Microsoft

A Microsoft digitális védelmi jelentése, 2022

Bepillantást nyerhet a fenyegetések világába, és segítséget kaphat a digitális védekezéshez.

Tartalom

A jelentésben szereplő adatok, információk és események a 2021. július és 2022. június közötti időszakra vonatkoznak (ez a Microsoft 2022-es pénzügyi éve), kivéve, ha a jelentésben más szerepel.

A jelentés optimális megtekintése és használata érdekében javasoljuk, hogy használja az Adobe Reader alkalmazást, amely ingyenesen letölthető az Adobe weboldaláról.

Tom Burt,

ügyfélbiztonságért és bizalomért felelős vállalati alelnök bevezetője

„A termékeink és szolgáltatásaink világméretű hálójából származó több billió jelzés elemzésével feltárul a digitális fenyegetések valódi súlyossága, kiterjedése és hatóköre”

Pillanatkép az aktuális helyzetről...

A fenyegetések kiterjedése és hatóköre

A jelszavak elleni támadások száma másodpercenként körülbelül 921-re emelkedett – ez mindössze egy év alatt 74%-os növekedés.

A kiberbűnözés felszámolása

A Microsoft a mai napig több mint 10 000 kiberbűnözők által és 600 állami csoportok által használt tartományt távolított el.

A biztonsági rések bezárása

A zsarolótámadások elhárítása során az esetek 93%-ában kiemelt jogosultságú hozzáférések nem megfelelő szabályozására derítettünk fényt, ami a támadók oldalirányú mozgására adott lehetőséget.

2022. február 23-án a kiberbiztonság új korszakba lépett: beköszöntött a hibrid háborúk kora. Ezen a napon, órákkal azelőtt, hogy egyetlen rakéta becsapódott volna, és egyetlen tank is átlépte az ukrán határt, az oroszok pusztító kibertámadást indítottak ukrán kormányzati, technológiai és pénzügyi célpontok ellen. Ezekről a támadásokról és a levonható tanulságokról többet is megtudhat a nemzetállami fenyegetésekkel foglalkozó fejezetben, ha tovább olvassa a Microsoft éves digitális védelmi jelentésének (MDDR) harmadik kiadását. A legfontosabbat azonban itt is szeretném kiemelni: a felhő kínálja a leghatékonyabb fizikai és logikai védelmet a kibertámadások ellen, és az általa biztosított veszélyforrás-felderítési intelligencia és végpontvédelem már Ukrajnában is bizonyította, hogy mire képes.

Az év kiberbiztonsági eseményeiről készült körkép nem kezdődhet mással, mint a háborúval, de idei jelentésünk emellett is számtalan területtel foglalkozik. Az első fejezetben a kiberbűnözőkre összpontosítunk, majd a második fejezetben rátérünk a kiberhadviselésre. Idén a bűnözők és a nemzetállamok egyaránt jóval kifinomultabb támadásokat indítottak, így tevékenységük káros hatásai is megsokszorozódtak. A címlapokon elsősorban Oroszország szerepelt, de az új elnök beiktatását követően Irán pusztító kiberhadereje is egyre gyakrabban vette célba Izraelt, valamint zsarolótámadásokat és kiszivárogtatási műveleteket is végrehajtottak az Egyesült Államokban. Kína fokozta kémtevékenységét Dél-kelet-Ázsiában és a déli félteke egyéb területein: az ázsiai ország az amerikai befolyás ellensúlyozására törekszik, és fontos adatokra és információkra leselkedik.

A külföldi szereplők rendkívül hatékony módszerekkel terjesztették propagandájukat a világ minden táján: erről szól a harmadik fejezet. Oroszország például keményen dolgozott rajta, hogy meggyőzze a saját és számos más ország polgárait: az Ukrajna elleni invázió indokolt volt – közben pedig álhíreket terjesztett, amelyek kétségbe vonták a nyugati koronavírus-védőoltások hatékonyságát, és az orosz oltásokat éltették. A támadók ráadásul egyre gyakrabban veszik célba a számos hálózat és kritikus infrastruktúra belépési pontjának számító IoT-eszközöket és operatív technológiai (OT) vezérlőeszközöket – ezeket a negyedik fejezetben vizsgáljuk meg. Az utolsó fejezetben megosztjuk az olvasóval azokat az információkat és tanulságokat, amelyeket az elmúlt év során, a Microsoft és az ügyfeleink ellen irányuló támadások kivédése során gyűjtöttünk össze, és áttekintjük a kiberreziliencia terén elért idei eredményeket.

A fejezetek megírása során a Microsoft egyedülálló piaci helyzetének segítségével feltárt fontos tanulságokra és információkra támaszkodtunk. A termékeink és szolgáltatásaink világméretű hálójából származó több billió jelzés elemzésével feltárul a digitális fenyegetések valódi súlyossága, kiterjedése és hatóköre. A Microsoft ezért folyamatosan azon dolgozik, hogy megóvja ügyfeleit és digitális ökoszisztémáját a fenyegetésektől: technológiáinkról is olvashat, amelyek idén is több milliárd adathalász kísérletet, identitáslopást és más súlyos veszélyforrást azonosítottak és blokkoltak.

Tom Burt bevezetője

(folytatás)

Jogi és technikai módszerekre támaszkodunk, hogy elfoglaljuk és leállítsuk a kiberbűnözők és az államilag szponzorált csoportok által használt infrastruktúrát, és értesítjük az ügyfeleinket, ha egy állami támogatású csoport célba vette vagy megtámadta őket. Folyamatosan egyre hatékonyabb funkciók és szolgáltatások kifejlesztésén dolgozunk, amelyek AI és gépi tanulás segítségével képesek azonosítani és blokkolni a kiberfenyegetéseket, és lehetővé teszik, hogy a biztonsági szakemberek gyorsabban és hatékonyabban azonosítsák és megállítsák a kibertámadásokat.

De ami talán a legfontosabb, a Microsoft digitális védelmi jelentésében hasznos tanácsokat adunk a magánszemélyeknek, a szervezeteknek és a vállalatoknak azzal kapcsolatban, hogy milyen lépéseket érdemes tenni az egyre fokozódó digitális fenyegetéssel szemben. A megfelelő kiberhigiéniai gyakorlatok alkalmazása a legjobb védekezés, ami jelentősen csökkenti a kibertámadások kockázatát.

Kiberbűnözési körkép

A jellemző kiberbűnöző ma kifinomult, profitorientált vállalkozóként működik. A támadók folyamatosan új módszereket dolgoznak ki, új utakat találnak technikáik alkalmazására, és egyre kifinomultabb megoldásokkal és helyszíneken hosztolják a kampányaikhoz szükséges infrastruktúrát. Eközben egyre takarékosabbá is válnak. A többletköltségek csökkentése és a legitimitás látszatának fenntartása érdekében a támadók gyakran vállalati hálózatokat és eszközöket törnek fel adathalász kampányaik lebonyolításához és rosszindulatú szoftvereik bevetéséhez, sőt sokszor e hálózatok számítási teljesítményét kihasználva kriptovalutát bányásznak.

> **További információt a 6. oldalon talál**

„Az Ukrajnában zajló hibrid háborúban bevetett kiberfegyverek már a konfliktus új korszakának elérkeztét jelzik.”

Kiberhadviselés

A nemzetállami szereplők egyre kifinomultabb kibertámadásokat indítanak, amelyeket úgy alakítanak ki, hogy kerüljék a lelepleződést, és megvalósítsák stratégiai prioritásaikat. Az Ukrajnában zajló hibrid háborúban bevetett kiberfegyverek már a konfliktus új korszakának elérkeztét jelzik. Oroszország olyan propagandaműveletekkel is támogatja háborús tevékenységét, amelyek célja, hogy Oroszországban, Ukrajnában és világszerte befolyásolja az emberek véleményét. A nemzetállami szereplők Ukrajnán kívül is fokozták aktivitásukat, és az automatizálás, a felhő-infrastruktúra és a távoli hozzáférésre alapuló technológiák fejlődését kihasználva egyre szélesebb csoportokat céloznak meg. Gyakran a tényleges cél elérését megkönnyítő vállalati IT-ellátási láncokat is támadások érik. A támadók könyörtelenül kihasználják a be nem foltozott biztonsági réseket, a kifinomult és a nyers erőre épülő módszerektől sem riadnak vissza, és sokszor nyílt forráskódú, akár legitim szoftverekkel fedik el a tevékenységüket – a kiberbiztonsági higiénia ezért ma fontosabb, mint valaha. Oroszországhoz mellett Irán is pusztító kiberfegyvereket vetett be, előszeretettel nyúl például zsarolóvírusokhoz.

E fejlemények is jelzik, mennyire sürgős volna elfogadni egy átfogó, globális keretrendszert, amely az emberi jogokat helyezi előtérbe, és védelmet nyújt a felelőtlen állami cselekmények veszélyeivel szemben. A világ országainak együtt kell működnie a normák és a felelősségteljes állami magatartásra vonatkozó szabályok alkalmazása érdekében.

> **Tudjon meg többet a 30. oldalon**

Eszközök és infrastruktúra

A világjárvány és az internetre kapcsolódó eszközök digitális átalakulás gyorsításának részeként történt tömeges bevezetése nagymértékben megnövelte digitális világunk támadási felületét. A kiberbűnözők és a nemzetállamok gyorsan kihasználták ezt a helyzetet. Az IT-hardverek és -szoftverek az elmúlt években egyre biztonságosabbá váltak, de az IoT- és OT-eszközök védelmi funkciói nem fejlődtek ilyen ütemben. A támadók sokszor ezeken az eszközökön keresztül jutnak be a hálózatokba, ahol oldalirányú mozgásba kezdenek, megvetik a lábukat az ellátási láncban, és megakadályozzák a szervezet OT-tevékenységeit.

> **Tudjon meg többet az 56. oldalon**

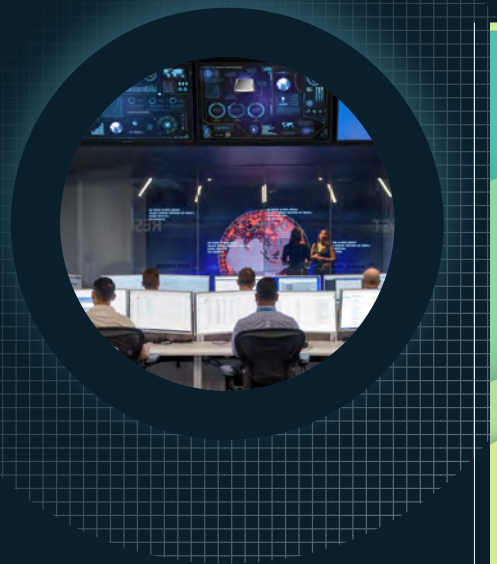
Tom Burt bevezetője

(folytatás)

Kiberbefolyásolási műveletek

A nemzetállamok egyre gyakrabban kifinomult befolyásolási műveleteket alkalmaznak propagandájuk terjesztésére és a közvélemény befolyásolására, mind belföldön, mind nemzetközi szinten. Ezek a kampányok aláássák a bizalmat, növelik a polarizációt, és fenyegetést jelentenek a demokratikus folyamatokra. A képzett, ügyes és kitartó manipulátorok a hagyományos, az internetes és a közösségi média felhasználásával jelentős mértékben növelni tudták kampányaik kiterjedését és társadalmi hatását, így erőforrásaikhoz képest jelentős hatást tudnak kifejteni a globális információs ökoszisztémára. Az elmúlt évben elsősorban Oroszország Ukrajna ellen folytatott hibrid háborújának részeként láthattunk ilyen műveleteket, de Oroszország más államok, köztük Kína és Irán ellen is egyre fokozódó mértékben alkalmaz közösségi médián alapuló propagandát, ezzel igyekszik növelni a befolyását a különböző globális ügyekben.

› További információt a 71. oldalon talál



Védekezés a kibertámadásokkal szemben

A biztonság a technológia sikeres kihasználásának kulcsfontosságú eleme. Az innováció és a hatékonyság fokozásához olyan biztonsági intézkedéseket kell bevezetnünk, amelyekkel a lehető legellenállóbbá tehetjük szervezetünket a modern támadásokkal szemben. A világjárvány a Microsoftot is komoly kihívás elé állította: át kellett alakítanunk biztonsági gyakorlatainkat és technológiáinkat, hogy megóvhassuk munkatársainkat, bárhol is dolgozzanak. Az elmúlt évben a támadók változatlanul kihasználták a világjárvány és a hibrid munkarend miatt keletkezett biztonsági réseket. Ma a különböző támadási módok kiterjedése és összetettsége, valamint az államilag szponzorált csoportok fokozott tevékenysége jelenti a legnagyobb kihívást. Ebben a fejezetben részletesen bemutatjuk, hogy milyen kihívásokkal néztünk szembe, és hogy milyen védelmi intézkedéseket mobilizáltunk ellenük több mint 15 000 partnerünknél.

› Tudjon meg többet a 86. oldalon

A Microsoft egyedülálló pozíciója

37 milliárd
veszélyes e-mailt blokkoltunk

34,7 milliárd
identitás elleni támadás blokkolva

43 billió
jelet szintetizálunk naponta kifinomult adatanalitikai módszerek és AI-algoritmusok segítségével, hogy megértsük a digitális fenyegetéseke és a kiberbűnözők tevékenységét, és hatékonyan védekezhessünk ellenük.

2,5 milliárd
végpontjelzést elemzünk naponta

Több mint 8500
mérnök, kutató, adatmérnök, kiberbiztonsági szakértő, veszélyforrás-elhárítással foglalkozó szakember, geopolitikai elemző, nyomozó és első vonalbeli reagáló 77 országban.

Több mint 15 000
partner vesz részt biztonsági ökoszisztémánkban, akik azon dolgoznak, hogy megvédjék ügyfeleinket a kibertámadásoktól

2021. július 1. – 2022. június 30.

Tom Burt bevezetője

(folytatás)

Hiszünk benne, hogy a Microsoft – önállóan, valamint a más magánvállalatokkal, kormányzati és civil szereplőkkel folytatott szoros együttműködés révén – felelősséggel tartozik azért, hogy megóvja a társadalmunk szövetének szerves részét képező digitális rendszereket, és a világ minden pontján biztonságos IT-környezeteket nyújtson mindenkinek. Ezért is tesszük közzé 2020 óta minden évben a Microsoft digitális védelmi jelentését (MDDR), amely a Microsoft által gyűjtött jelentős adatmennyiségeken végzett részletes kutatásokon alapul. A jelentésben egyedülálló információkat osztunk meg a digitális fenyegetések változásairól, és bemutatjuk, hogy milyen fontos intézkedéseket lehet tenni az ökoszisztéma fokozott védelme érdekében.

Reméljük, sikerült átadnunk, mennyire sürgető kérdés ez, és olvasóink a lehető leghamarabb megteszik a szükséges intézkedéseket az itt és az év során közreadott további kiberbiztonsági publikációinkban megosztott adatok és információk alapján. Nem lehet eléggé hangsúlyozni a digitális környezetre leselkedő fenyegetések súlyosságát – és ezek fizikai világra gyakorolt hatását –, ugyanakkor fontos leszögezni, hogy mindannyian tehetünk azért, hogy megóvjuk magunkat, szervezeteinket és vállalatainkat a digitális fenyegetésektől.

Köszönjük, hogy időt szán a Microsoft digitális védelmi jelentésének elolvasására! Reméljük, hogy hasznosnak találja az itt szereplő információkat és javaslatokat, és Ön is hozzájárul, hogy közösen megvédjük a digitális ökoszisztémát!

Tom Burt
ügyfélbiztonságért és -bizalomért felelős vállalati alelnök bevezetője

Ennek a jelentésnek kettős célja van:

1. Szeretnénk felhívni ügyfeleink, partnereink és az egyéb érdekeltek figyelmét a tágabb ökoszisztémára kiterjedő, fejlődő digitális fenyegetésekre, és az új típusú kibertámadásokra és az ismert fenyegetések körében megfigyelhető trendekre egyaránt rávilágítani.
2. Emellett szeretnénk támogatni ügyfeleinket és partnereinket a kibertámadásokkal szembeni hatékony védekezésben.

Kiberbűnözési körkép

A kibervédelem folyamatosan fejlődik, és egyre több vállalat támaszkodik proaktív megközelítésre a megelőzés, valamint a támadókkal és módszereikkel szembeni védekezés terén.

A kiberbűnözés aktuális helyzetének áttekintése

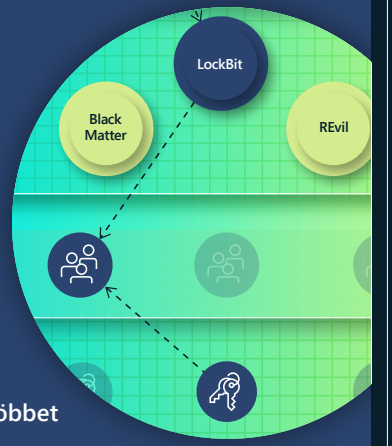
A kibervédelem folyamatosan fejlődik, és egyre több vállalat támaszkodik proaktív megközelítésre a megelőzés, valamint a támadókkal és módszereikkel szembeni védekezés terén.

A jellemző kiberbűnöző ma kifinomult, profitorientált vállalkozóként működik. A támadók folyamatosan új módszereket dolgoznak ki, új utakat találnak technikáik alkalmazására, és egyre kifinomultabb megoldásokkal és helyszíneken hosztolják a kampányaikhoz szükséges infrastruktúrát. Eközben egyre takarékosabbá is válnak. A többletköltségek csökkentése és a legitimitás látszatának fenntartása érdekében a támadók gyakran vállalati hálózatokat és eszközöket törnek fel adathalász kampányaik lebonyolításához és rosszindulatú szoftvereik bevetéséhez, sőt sokszor e hálózatok számítási teljesítményét kihasználva kriptovalutát bányásznak.

A kiberbűnözés egyre elterjedtebb, az ágazat iparosodásával és az egyszerűen elérhető támadóeszközöknek és infrastruktúráknak köszönhetően ráadásul egyre kisebb szakértelem szükséges ahhoz, hogy valaki sikeres támadást indítson.

Tudjon meg többet a 18. oldalon

A zsarolók egyre bátrabban lépnek fel: kormányzatokat, vállalatokat és létfontosságú infrastruktúrákat egyaránt célba vesznek.

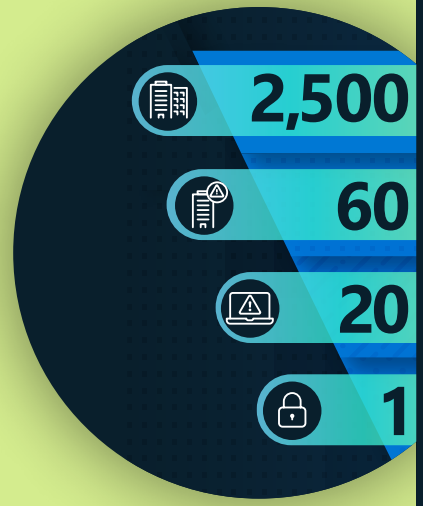


Tudjon meg többet a 9. oldalon

A támadók egyre gyakrabban fenyegetőznek azzal, hogy bizalmas adatokat fednek fel, ha az áldozat nem fizet váltságdíjat.

Tudjon meg többet a 10. oldalon

Az ember által működtetett zsarolószoftverek a legelterjedtebbek, az ilyen támadások egyharmada sikeres, és 5%-nál a váltságdíjat is kifizették.

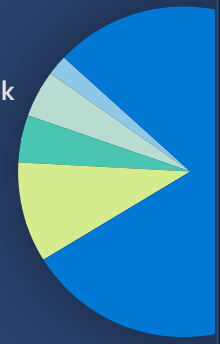


Tudjon meg többet a 9. oldalon

A zsarolótámadásokkal szembeni leghatékonyabb védekezés része a többfaktoros hitelesítés, a biztonsági javítások gyakori kiadása és az egész hálózati architektúrában alkalmazott Zero Trust elv.

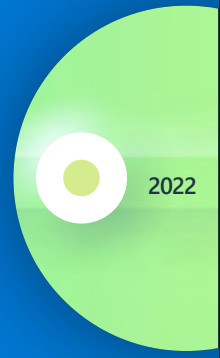
További információt a 13. oldalon talál

Egyre gyakoribb a hitelesítési adatokkal kapcsolatos adathalászat, amelyek válogatás nélkül az összes elérhető postafiókot célba veszik, emellett az üzleti e-mailekkel és számlákkal kapcsolatos csalások is komoly kockázatot jelentenek a vállalatok számára.



Tudjon meg többet a 21. oldalon

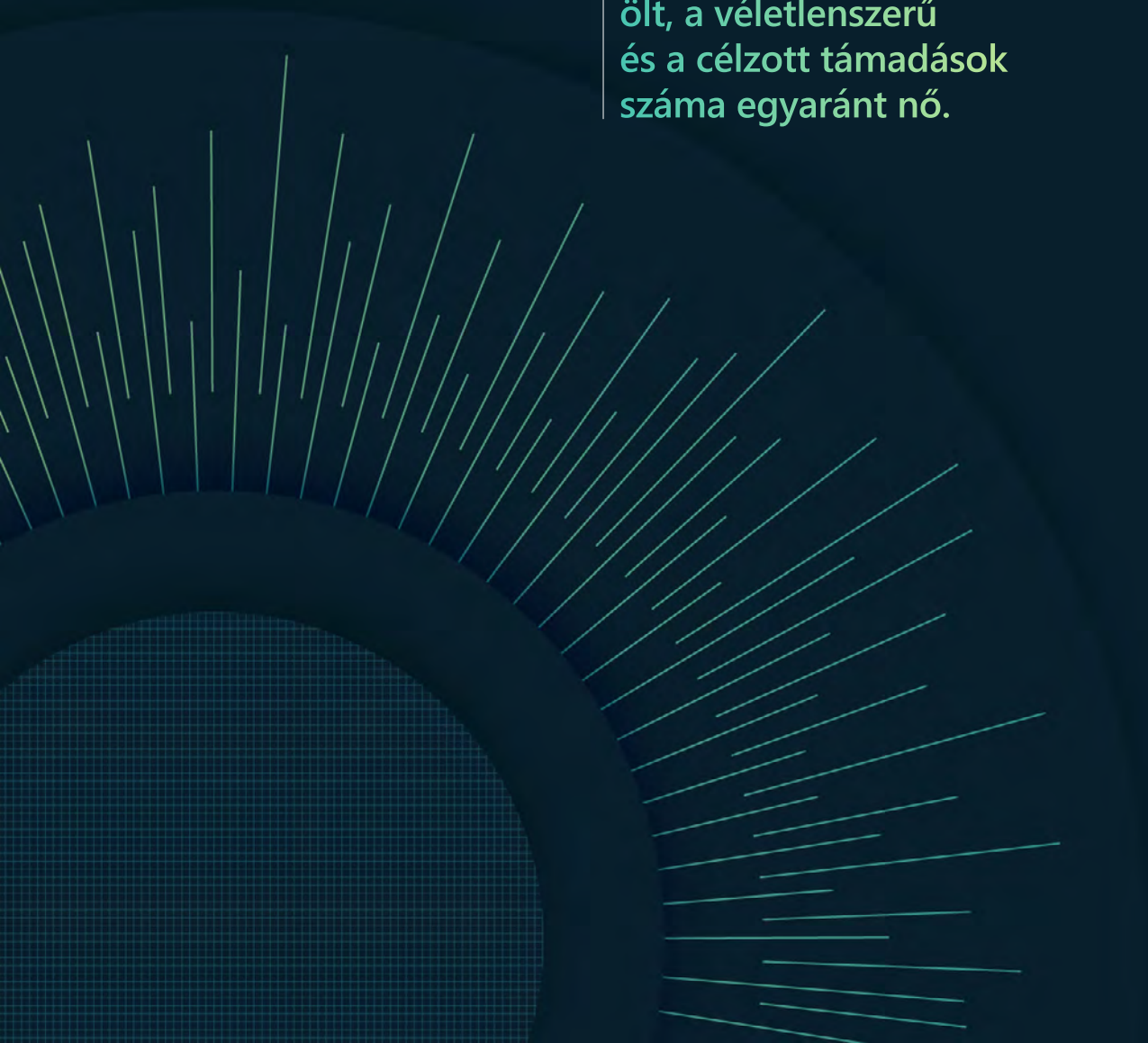
A Microsoft innovatív jogi módszerekre és az állami és a privát szférában működő partnereire hagyatkozik, hogy felszámolja a kiberbűnözők és az államilag szponzorált csoportok rosszindulatú infrastruktúráit.



Tudjon meg többet a 25. oldalon

Bevezető

A kiberbűnözés egyre súlyosabb méreteket ölt, a véletlenszerű és a célzott támadások száma egyaránt nő.



A kibervédelem folyamatosan fejlődik, és egyre több kormány és vállalat alkalmaz proaktív megközelítést a megelőzésre. A támadók ma elsősorban két stratégiát alkalmaznak a hozzáférés megszerzésére. Az egyik megközelítés a széles körű, mennyiségen alapuló kampány. A másik megközelítés megfigyelést és pontosabb célzást alkalmaz a profitráta növelése érdekében. Sokszor nem is kifejezetten a bevételszerzés a cél – például a geopolitikai célokat szolgáló nemzetállami tevékenységeknél –, de ezekben az esetekben is egyaránt látunk véletlenszerű és célzottabb támadásokat. A kiberbűnözők az elmúlt évben is alkalmaztak pszichológiai manipulációt, és kihasználták a közbeszédben aktuális témákat, hogy növeljék kampányaik sikerét. A koronavírust idén ritkábban használták csaliként, de számos esetben láttuk például, hogy a csalók azt állították, Ukrajna lakóinak gyűjtenek adományokat.

A támadók folyamatosan új módszereket dolgoznak ki, új utakat találnak technikáik alkalmazására, és egyre kifinomultabb megoldásokkal és helyszíneken hosztolják a kampányaikhoz szükséges infrastruktúrát. Megfigyeltük, hogy a kiberbűnözők egyre jobban odafigyelnek a költségekre, és ma már nem szívesen fizetnek a technológiákért. A többletköltségek csökkentése és a legitimitás látszatának fenntartása érdekében egyes támadók vállalati hálózatokat és eszközöket törnek fel adathalász kampányaik lebonyolításához és rosszindulatú szoftvereik bevetéséhez, sőt sokszor e hálózatok számítási teljesítményét kihasználva kriptovalutát bányásznak.

Ebben a fejezetben megvizsgáljuk a hacktivizmus előretörését is, ami alatt azt értjük, amikor az állampolgárok társadalmi vagy politikai célok megvalósítása érdekében követnek el kibertámadásokat. 2022 februárja óta világszerte több ezer ember ragadott billentyűzetet (szakértők és hobbisták egyaránt) az orosz-ukrán háború hatására – többek között webhelyeket bénítottak meg és lopott adatokat szivárogtattak ki. Egyelőre nehéz megmondani, hogy ez a trend a hadi cselekmények lezárulta után is fennmarad-e.

A vállalatoknak rendszeresen felül kell vizsgálniuk és meg kell erősíteniük a hozzáférési kontrollokat, és olyan biztonsági stratégiát kell bevezetniük, amely hatékony védelmet nyújt a kibertámadások ellen. Ez azonban csak a kezdet. Elmagyarázzuk, hogyan indított polgári pereket digitális bűnüldözési egységünk (DCU), hogy felszámolja a kiberbűnözők és nemzetállami aktorok által rosszindulatú célokra használt infrastruktúrát. Kormányzati és magánvállalati partnereinkkel együtt a jövőben is küzdeni fogunk e fenyegetések ellen. Reményeink szerint azzal, hogy megosztjuk velük az elmúlt 10 év tanulságait, másoknak is segíthetünk, hogy megértsék, milyen proaktív lépésekre van szükség a hatékony védekezéshez, és ahhoz, hogy megóvják magukat és a szélesebb ökoszisztémát a kibertámadások egyre súlyosbodó fenyegetésétől.

Amy Hogan-Burney
ügyvezető igazgató, digitális bűnüldözési egység

Zsarolóvírusok: nemzetbiztonsági fenyegetés

A zsarolótámadások mindannyiunkra egyre nagyobb veszélyt jelentenek, hiszen a bűnözők a burjánzó kiberalvilági ökoszisztémára támaszkodva a kritikus infrastruktúrát, a legkülönbözőbb méretű vállalkozásokat, valamint a kormányzatokat és a helyi önkormányzatokat egyaránt célpontnak tekintik.

Az elmúlt két évben több zsarolóvírusos támadás is igen nagy visszhanggal járt – elsősorban azok, amelyeknek a kritikus infrastruktúra, valamint egészségügyi és IT-szolgáltatók estek áldozatául. A zsarolók egyre nagyobb szervezeteket vesznek célba, támadásaik hatásait pedig egyre többen érzik. Csupán néhány példa 2022-ben bekövetkezett támadásokra:

- Februárban támadást indítottak két vállalat ellen, amelynek hatására több száz észak-németországi benzinkút fizetésfeldolgozó rendszerében következtek be zavarok.[1]
- Márciusban a görög postaszolgálat elleni támadás hatására átmenetileg szüneteltek a kézbesítések, valamint a pénzügyi tranzakciók feldolgozása is akadozott.[2]
- Májusban a costa ricai kormány elleni zsarolóvírusos támadás hatására országos vészhelyzetet hirdettek az országban: kórházakat kellett bezárni, és a vámok és adók behajtása is szünetelt.[3]
- Egy másik májusi támadás hatására számtalan járat késett, másokat pedig törölni kellett India egyik legnagyobb légitársaságánál, és több száz utas nem tudott hazajutni.[4]

E támadások sikere és a fizikai világra gyakorolt hatásaik mértéke is szemlélteti, hogy a kiberbűnözés egyfajta iparággá vált, amelynek szereplő számos különböző eszközhöz és infrastruktúrához hozzáférnek – a kiberbűnözők ma kevesebb szakértelem birtokában is több kárt tudnak tenni.

Az elmúlt években a zsarolószoftverek piaca is megváltozott: míg korábban egyetlen „banda” fejlesztette a vírust és indította a támadást, mára szinte szolgáltatásként kínálják a zsarolószoftvereket (RaaS modell). Az RaaS révén a fejlesztői csoport csupán a vírus előállításáért felel, amelyet szolgáltatásként, a haszon egy részéért cserébe ad el a zsarolótámadást ténylegesen végrehajtó kiberbűnözőknek. A kiberbűnözői franchise-ok kialakulásának hatására egyre többen tudnak ilyen támadásokat indítani. A kiberbűnözés iparággá válásával a támadók könnyebben be tudnak jutni a rendszerekbe, ahol hozzáférnek a bizalmas adatokhoz, és telepítik a zsarolóvírust.

Továbbra is komoly fenyegetést jelentenek az ember által irányított zsarolótámadások[5]. Ezt a kifejezést a Microsoft kutatói dolgozták ki az előzőekben leírt „hozott anyagból” dolgozó támadásokkal szemben, és azokra a támadásokra használják, amelyeket emberek irányítanak, akik minden lépésnél döntéseket hoznak, az alapján, hogy mit fedeznek fel a célpont hálózatában.

A Végponthoz készült Microsoft Defender (EDR) adatain alapuló modell (2022. január és június között).

Zsarolóprogramok és zsarolás: nemzetbiztonsági fenyegetés

Folytatás

A kettős zsarolásra épülő monetizációs stratégia bevetté válásával a zsarolótámadások még súlyosabb hatást tudnak kifejteni. Ennek lényege, hogy a támadók ellopják az adatokat a feltört eszközökről, majd titkosítják az eszközökön található adatokat, és azzal fenyegetőznek, hogy nyilvánosságra hozott az ellopott információkat – kivéve, ha az áldozat kifizeti a váltságdíjat.

A legtöbb támadó a kínálkozó lehetőségeket keresi, és azokon a hálózatokon telepíti a vírusát, amelyekhez valahogy hozzáférést szerez, míg mások úgynevezett brókerektől vásárolnak hozzáférést.

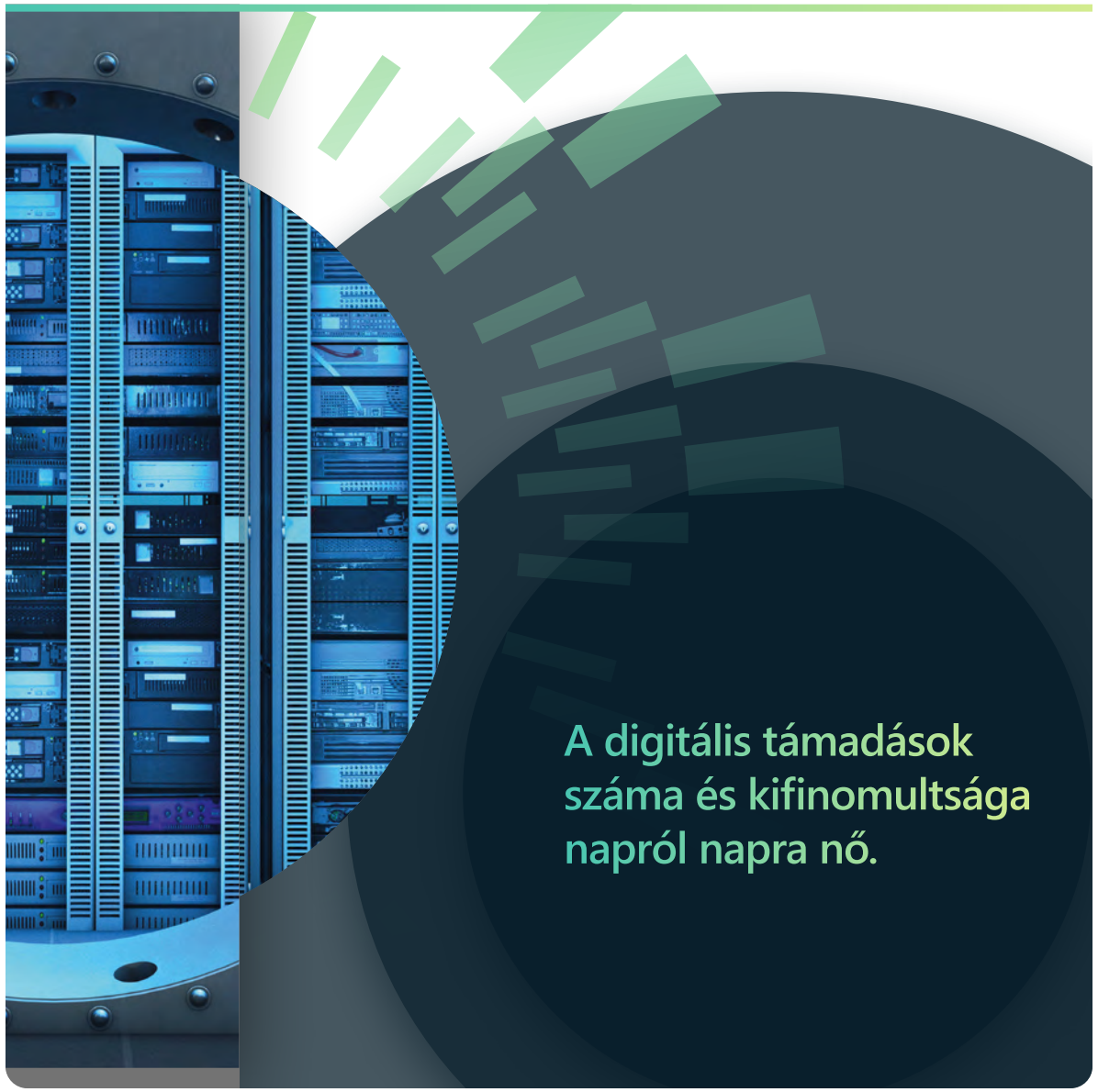
A Microsoft a jelek különlegesen gazdag gyűjteményére támaszkodhat, amelyeket számos forrásból gyűjtünk (identitásokból, e-mailekből, végpontokról és a felhőből), így hasznos információkat szerezhetünk az egyre növekvő zsarolóvírusos iparágról – amelyben ma már úgynevezett beszállítók is működnek, akik eszközöket fejlesztenek az informatikához kevésbé értő bűnözőknek.

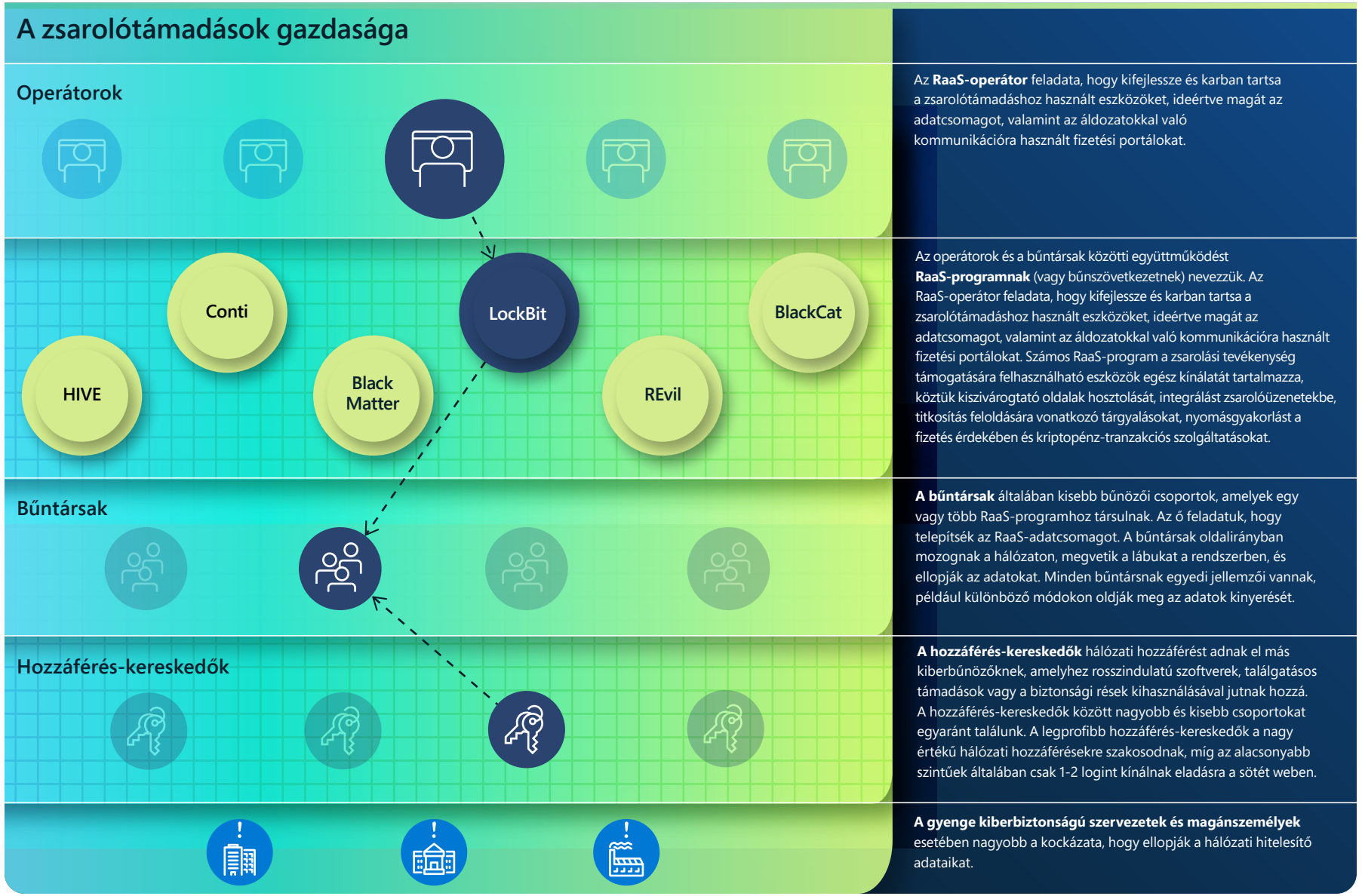
Az egyes területekre szakosodott kiberbűnözők közötti kapcsolatok bővülésének hatására a zsarolótámadások üteme, kifinomultsága és sikere egyaránt megnőtt. A kiberbűnözői ökoszisztémában ma különböző módszerekkel, célokkal és kapcsolatokkal rendelkező, de egymással kapcsolatban álló csoportok működnek, amelyek segítik egymást a célpontok, fizetési szolgáltatások, titkosításfeloldási vagy publikációs eszközök és webhelyek kezdeti feltörésében.

A zsarolóvírusok üzemeltetői emellett most már akár meg is vásárolhatják a vállalati vagy a kormányzati hálózatokhoz való hozzáférést, de a brókerekkel ápolt személyes kapcsolatuknak köszönhetően is hozzájuthatnak a hitelesítő adatokhoz. A brókerek kizárólag azzal foglalkoznak, hogy monetizálják az egyszer már megszerzett hozzáférést.

A támadás lebonyolítói a megvásárolt hozzáférés birtokában már könnyen telepíthetik a sötét weben működő piactereken vagy fórumokon vásárolt vírust. Sok esetben az áldozatokkal folytatott tárgyalást is az RaaS-csapat vezeti, és nem maguk a támadók. Ezek a törvénytelen tranzakciók gördülékenyen zajlanak, és kicsi rá az esély, hogy résztvevőiket letartóztatják és vád elé helyezik, mivel a sötét web anonimitást biztosít, és ezekben a nemzeteken felüli terekben nehéz betartatni a törvényeket.

Az ilyen támadások hosszú távú és sikeres megfékezéséhez a kormányzati szereplők és a magánszektor szoros együttműködése szükséges.





A zsarolóvírusokról a médiában bemutatott képpel ellentétben ritkán fordul elő, hogy a zsarolóvírusos támadást az elejétől a végéi egyetlen „bűnbanda” menedzseli. Ehelyett általában több különböző csoport működik együtt: az egyik kifejleszti a zsarolóvírust, a másik feltöri az áldozat rendszerét, telepíti a vírust, majd lebonyolítja a tárgyalásokat. A bűnügyi ökoszisztéma iparággá válásával a következő szerepkörök alakultak ki:

- Hozzáférésbrókerek, amelyek feltörik az áldozat rendszerét, majd eladják a hozzáférést (ún. hozzáférési szolgáltatás).
- Rosszindulatú szoftvereket készítő és értékesítő fejlesztők.
- A támadást lebonyolító bűnözők és bűntársaik.
- Titkosítási és zsarolási szolgáltatásokat biztosító felek, akik a monetizációért felelnek (RaaS).

Az ember által irányított zsarolótámadásokban az a közös, hogy mindegyik valamilyen biztonsági rést használ ki. A támadók azért tudnak bejutni a rendszerbe, mert nem megfelelő a szervezet kiberbiztonsági állapota, például nem telepítik elég gyakran a javításokat, vagy nem vezettek be többfaktoros hitelesítést (MFA).

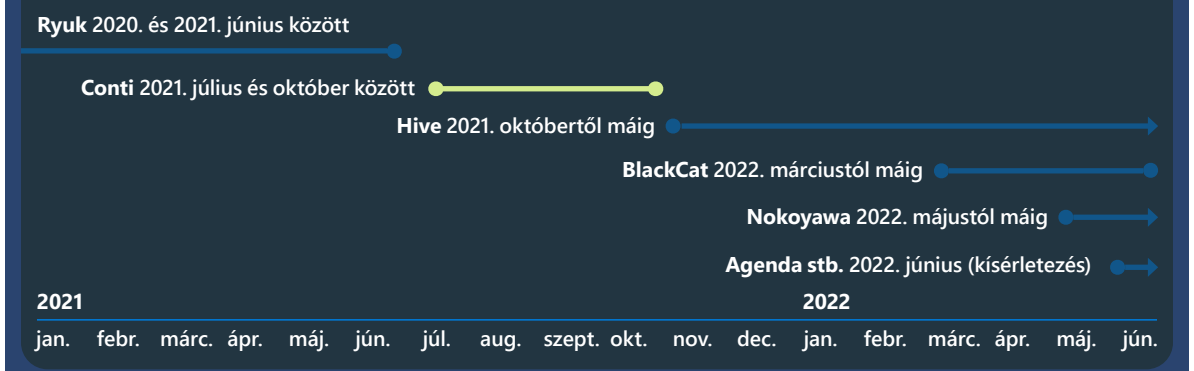
Esettanulmány: A Conti felszámolása

A Conti az elmúlt két év egyik legnépszerűbb zsarolóvírus-változata volt, de 2022 közepétől kezdve fokozatosan megszűnt, a Microsoft Threat Intelligence Center (MSTIC) már március végén és április elején is arról számolt be, hogy jóval kevesebben használják. Április közepe óta egyáltalán nem használják a Conti zsarolóvírust. Ahogyan más hasonló zsarolóvírusoknál is tapasztaltuk, a Conti megszűnésével nem csökkent jelentősen a zsarolóvírusos támadások száma, az MSTIC megfigyelései szerint az addig Contival dolgozó bűnözők egyszerűen áttértek más megoldásokra (ilyen volt a BlackBasta, a Lockbit 2.0, a LockbitBlack és a HIVE). Ez összhangban van az előző évekből származó adatokkal, és azt sugallja, hogy ha a zsarolóbanda egyik megoldását sikerül is felszámolni, hónapokkal később újra megjelennek, vagy új csoportokba rendeződve kamatoztatják hozzáértésüket és erőforrásaikat.

A Microsoft veszélyforrás-felderítési csapatai a használt eszközök, és nem a használt rosszindulatú szoftverek alapján különböztetik meg a zsarolással foglalkozó bűnözői csoportokat (amelyeket DEV-eknek neveznek). Ez azt jelenti, hogy amikor a Conti csoporthoz tartozó bűnözők szétszéledtek, az általuk használt más eszközök és RaaS-készletek alapján folytatni tudtuk ezeknek a DEV-eknek a nyomon követését. Például:

- DEV-0230, aki a Trickbottal hozható összefüggésbe, korábban a Conti lelkes felhasználója volt. Április végén az MSTIC szerint ez a DEV már a QuantumLockert használta.
- DEV-0237 a Conti zsarolókészletéről a HIVE és a Nokoyawa megoldásokra tért át, és a HIVE segítségével a costa ricai kormányzat ellen május 31-én végrehajtott támadásban is részt vett.
- DEV-0506, szintén a Conti lelkes felhasználója pedig a BlackBasta használatára tért át.

Példa: Egy támadó (DEV-0237) rendkívül gyorsan áttér egyik RaaS-programról a másikra



Az egyik RaaS-program (esetünkben a Conti) felszámolását követően a zsarolóvírusokkal dolgozó bűnöző szinte azonnal elkezdett egy másikat használni (Hive).

A RaaS lendületet adott a zsarolószoftverek ökoszisztémájának, és megnehezítette a felelősök megtalálását

Az ember által irányított zsarolótámadások mögött konkrét személyek állnak, ezért támadási mintáik is a célponthoz igazodnak, sőt akár a támadás közben is megváltozhatnak. A múltban az azonos „családhoz" tartozó zsarolóvírusoknál általában hasonló kezdeti bejutási pontokat, eszközöket és szoftveres kialakítást figyelhettünk meg. Ez megkönnyítette a felelősök megkeresését. A bűntársak által szolgáltatott RaaS-modellben azonban nincs kapcsolat a támadás különböző részei között. A Microsoft ezért nem a támadás lebonyolítóit követi nyomon, hanem az egyes támadások során használt adatcsomagot biztosító bűntársakat figyeli.

Más szóval: a HIVE zsarolóvírussal indított támadások mögött valószínűleg nem a HIVE fejlesztője áll, hanem egy bűntárs.

A kiberbiztonsági iparág számára nehézséget jelent, hogy különválassza a vírus fejlesztőjét a támadások lebonyolítójától. Az ágazatban gyakran még mindig a zsarolóvírus nevével kötik össze a támadást, ezzel azt a hamis látszatot keltve, hogy az adott vírussal végrehajtott összes támadás mögött egyetlen entitás vagy „zsarolóbanda" áll, és hogy az összes ilyen incidensnél hasonló módszerekre és infrastruktúrára lehet számítani. A hálózatokat védő szakemberek támogatása érdekében fontos, hogy megismerjük a különböző bűntársak támadásait megelőző fázisokat, például azt, hogyan lopják el az adatokat a bűnözők, és miként vetik meg a lábukat a rendszerben – és hogy mely pontokat lehet azonosítani és elhárítani a támadásokat.

A rosszindulatú szoftverek mellett a támadóknak hitelesítő adatokra is szükségük van a sikeres működéshez. Ahhoz, hogy az ember által irányított zsarolóvírusos támadások az egész szervezetre kiterjedjenek, a támadóknak hozzáférést kell szerezniük egy magas jogosultsági szintű fiókhoz.

Reflektorfényben az ember által irányított zsarolóvírusos támadások

Az elmúlt évben a Microsoft zsarolótámadásokkal foglalkozói szakértői több mint 100 ember által irányított zsarolóvírusos incidenst vizsgáltak ki, ennek során nyomon követték a támadók módszereit, és igyekeztek feltárni, hogyan tudnánk jobban megvédeni az ügyfeleinket.

Fontos megjegyezni, hogy az itt megosztott elemzést csak regisztrált és felügyelt eszközök esetében lehet használni. A nem regisztrált, nem felügyelt eszközök a vállalat hardverparkjának legkevésbé biztonságos részét képviselik.

A legnépszerűbb módszerek a zsarolóvírus telepítésének szakaszában:

75%

Rendszergazdai eszközök használata.

75%

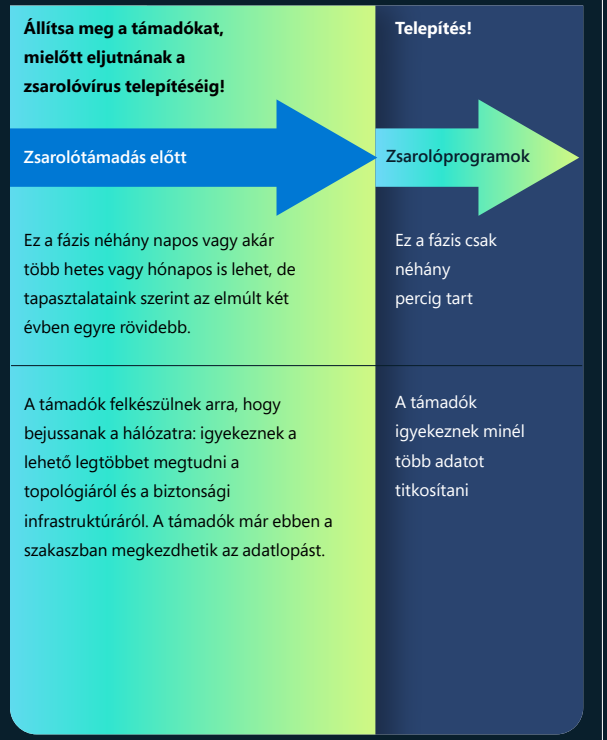
A vírus terjesztése az SMB protokoll segítségével a feltört magas jogosultsági szintű felhasználói fiókok használatával.

99%

A felfedezett biztonsági és biztonsági mentési termékek manipulálása az operációs rendszerhez fejlesztett eszközökkel.

Egy jellemző ember által irányított támadás

Az ember által irányított zsarolótámadások esetében megkülönböztethetjük a megelőző fázist, valamint a zsarolóvírus telepítésének fázisát. A megelőző fázisban a támadók felkészülnek a hálózat feltörésére: elemzik a szervezet tipológiáját és biztonsági infrastruktúráját.



Az általunk vizsgált ember által irányított zsarolótámadások nagy része hasonló biztonsági hiányosságokon alapult, és a támadási minták és módszerek is nagyrészt megegyeztek.

Tartós biztonsági stratégia

Az ilyen jellegű támadások leküzdéséhez és megakadályozásához át kell alakítani a vállalat gondolkodásmódját: átfogó védelemre van szükség, amely lelassítja, sőt meg is állítja a támadókat, mielőtt a megelőző fázisból áttérnének a zsarolóvírus telepítésére.

A nagyvállalatoknak következetesen és agresszíven kell alkalmazniuk a bevált biztonsági gyakorlatokat a hálózataikban, hogy képesek legyenek enyhíteni ezeknek a támadásoknak a kockázatát. Mivel e zsarolótámadásokat emberi döntések irányítják, számos, látszólag különálló biztonsági riasztást is generálhatnak, amelyeket a szakemberek könnyen figyelmen kívül hagynak vagy elodáznak. A legtöbb biztonsági műveleti központ (SOC) túl sok riasztást kénytelen kezelni. Ha azonban a trendek felderítésére fókuszálnak, vagy incidensek szerint csoportosítják a riasztásokat, jobban átláthatják a teljes képet. Az SOC-k ezt követően biztonságerősítési lépésekkel, például a támadási felületet csökkentő szabályokkal csökkenthetik a riasztások számát. A gyakori fenyegetések elleni védekezéssel nem csupán a riasztások mennyiségét csökkentheti, hanem számos támadót megakadályozhat abban, hogy hozzáférjen a hálózathoz.

A vállalatoknak folyamatosan kiváló állapotban kell tartaniuk biztonsági rendszereiket és hálózataikat, hogy megvédjék magukat az ember által irányított zsarolótámadásoktól.

Gyakorlati tanácsok

A zsarolótámadók célja az egyszerű haszonszerzés, ezért kulcsfontosságú, hogy a biztonság megerősítéssel megnöveljük a költségeiket, és ezzel ellehetetlenítsük gazdasági modelljüket.

1. Hitelesítő adatok higiéniájának biztosítása. A rosszindulatú szoftverek mellett a támadóknak hitelesítő adatokra is szükségük van a sikeres működéshez. Ahhoz, hogy az ember által irányított zsarolóvírusos támadások az egész szervezetre kiterjedjenek, a támadóknak hozzáférést kell szerezniük egy magas jogosultsági szintű fiókhoz (ilyen például a tartományi rendszergazda), vagy olyan fiókhoz, amely jogosult a csoportszabályzatok szerkesztésére.
2. Hitelesítő adatok kitettségének ellenőrzése.
3. Az Active Directory-frissítések telepítésének előtérbe helyezése.
4. A felhő megerősítése.
5. A támadási felület csökkentése.
6. Az internettel érintkező eszközök megerősítése és a hálózati határvonal megértése.
7. A hálózati védelem megerősítésével csökkentheti az SOC-ra nehezedő nyomást és a riasztások mennyiségét, így több sávszélesség marad a fontosabb incidensek leküzdésére.

További információra mutató hivatkozások

- RaaS: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog
- Human-operated ransomware attacks: A preventable disaster | Microsoft Security Blog

Információk a zsarolóvírusokról olyanoktól, akiknek már volt velük dolguk

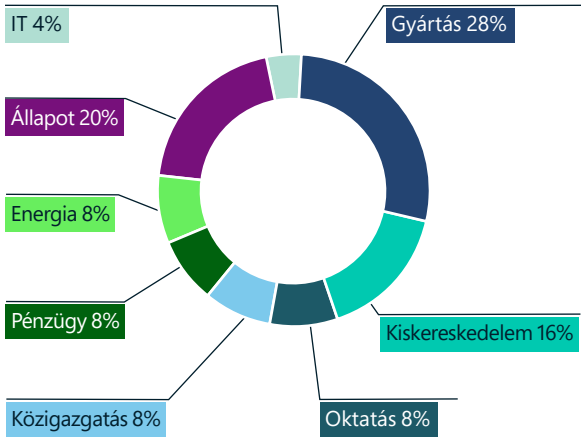
2019-től kezdődően a legtöbb vállalat egyre több ember által irányított zsarolótámadással néz szembe. A tavalyi évben azonban a bűnüldöző hatások működése és a geopolitikai helyzet egyaránt komoly hatást gyakorolt a kiberbűnözői csoportokra.

A Microsoft Security Service Line a kibertámadás minden fázisában támogatja az ügyfeleket, a kivizsgálástól a sikeres megfékezésig, majd a helyreállítási tevékenységekig. A reagálási és helyreállítási szolgáltatások két, szorosan együttműködő csapat biztosítja, az egyik a kivizsgálásra és a helyreállítás előkészítésére, a másik pedig a támadás megállítására és a helyreállításra fókuszál. Ebben a részben az elmúlt év során kezelt zsarolótámadások alapján levont tanulságokat összegezzük.

93%

a Microsoft által zsarolóvírusos támadások kapcsán lefolytatott vizsgálatok közül ennyi esetben nem felügyelte megfelelően a vállalat a magas szintű hozzáféréseket és a laterális mozgást.

Zsarolótámadások és helyreállítási tevékenységek iparág szerint

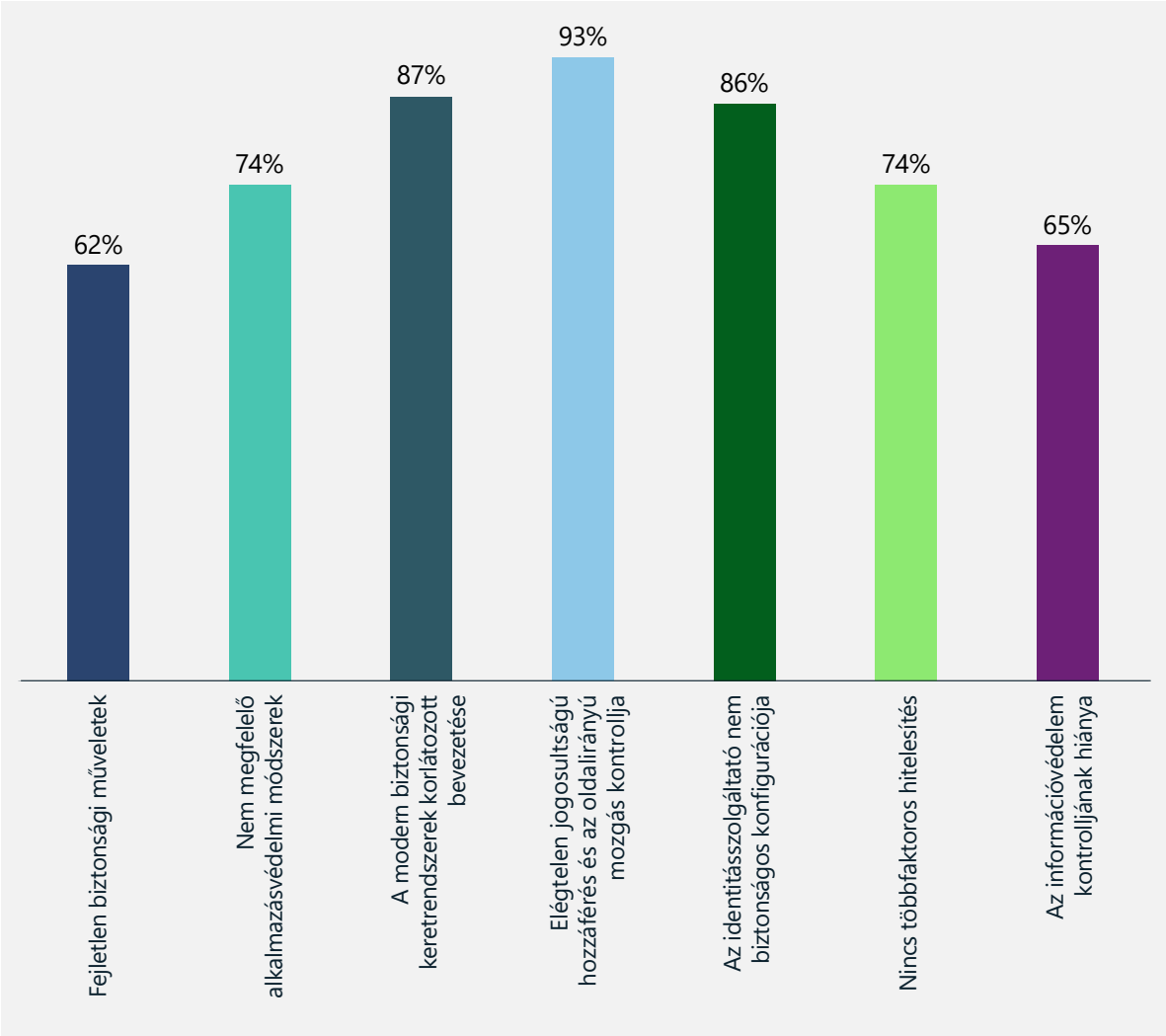


Folyamatosan új, kisebb csoportok és fenyegetések ütik fel a fejüket, a biztonsági csapatoknak ezért figyelemmel kell követniük a veszélyforrások fejlődését, és közben a korábban ismeretlen rosszindulatú szoftverek ellen is védekezniük kell. A bűnözői csoportok gyorsan kifejleszthető, intelligens, egyszerűen használható készlet formájában elérhető zsarolóvírusokat értékesítenek. Így rugalmasabban működhetnek, és több célpont ellen irányuló, szélesebb körű támadásokat indíthatnak.

A következő oldalakon megvizsgáljuk, melyek azok a leggyakoribb tényezők, amelyek meggyengítik a vállalati rendszereket a zsarolótámadásokkal szemben. Ezeket három kategóriába soroljuk:

1. Gyenge identitásszabályozás
2. Nem hatékony biztonsági műveletek
3. Gyenge adatvédelem

A zsarolóvírusok elhárítása során levont tanulságok



A zsarolóvírusos incidensek elhárítása során levont leggyakoribb tanulság, hogy az áldozatul esett szervezet nem felügyelte megfelelően a magas szintű hozzáféréseket és a laterális mozgást.

Információk a zsarolóvírusokról olyanoktól, akiknek már volt velük dolguk

Folytatás

A vállalatunkon belül látott három fő tényező a következő:

① **Gyenge identitásszabályozás:** A lopott hitelesítő adatokra épülő támadások ma is különösen gyakoriak

② **Nem hatékony biztonsági műveletek** – az ilyen folyamatok támadási felületet kínálnak, és a helyreállítást is meghosszabbítják

③ Végső soron az adatok a legfontosabbak: a probléma az, hogy a szervezetek nem tudtak olyan hatékony **adatvédelmi stratégiát kidolgozni,** amely üzleti igényeiknek is megfelelt

① Gyenge identitásszabályozás

Az ember által irányított zsarolótámadások folyamatosan fejlődnek, és általában hitelesítőadat-lopást és laterális mozgást is alkalmaznak, ami a célzott műveletek esetében gyakori. A sikeres támadások mögött gyakran hosszú ideje tartó kampányok húzódnak meg, amelyek részeként a bűnözők feltörik az identitáskezelő rendszereket, amilyen például az Active Directory (AD), így az emberi irányítók ellophatják a hitelesítő adatokat, hozzáféréshez juthatnak a rendszerekhez, és megvethetik a lábukat a hálózatban.

Az Active Directory (AD) és az Azure AD biztonsága

88%

a megtámadott ügyfelek közül nem használta az AD és az Azure AD bevált gyakorlatait. Ez gyakori támadási vektorrá vált, hiszen a támadók a kritikus identitáskezelő rendszerek helytelen konfigurációit és gyengébb biztonsági állapotát kihasználva szélesebb körű hozzáférést szerezhetnek, és komoly károkat okozhatnak a vállalatoknak.

A szükséges legkisebb jogosultságú hozzáférések és a kiemelt jogosultsághoz kötött hozzáférési munkaállomások (PAW) használata

Az érintett vállalatok egyike sem választotta el megfelelően a rendszergazdai hitelesítő adatokat, és nem használtak dedikált munkaállomásokat a kritikus identitások és a saját fejlesztésű rendszerek, üzletkritikus alkalmazások és más, különösen értékes eszközök kezelésére (pedig a legkisebb jogosultságok elve ezt írja elő).

Kiemelt biztonságú fiókok

88%

az érintettek közül nem használt MFA-t a bizalmas és magas jogosultsági szintű fiókokhoz – ez olyan biztonsági rést jelent, amelyet kihasználva a bűnözők hozzájuthattak a hitelesítő adatokhoz, és a további támadásokat már legitim hitelesítő adatok birtokában indíthatták.

84%

A szervezetek 84%-ánál a rendszergazdák nem szabályozták a kiemelt hozzáférésű identitásokat, például időben korlátozható hozzáféréssel – pedig ez segíthetett volna elkerülni az ellopott hitelesítő adatokkal való visszaélést.

Információk a zsarolóvírus-sokról olyanoktól, akiknek már volt velük dolguk

Folytatás

② Nem hatékony biztonsági műveletek

Adataink komoly biztonsági réseket mutatnak a zsarolótámadás áldozatává vált szervezetek biztonsági műveleteiben, eszközkészletében és az IT-eszközök életciklusának menedzselésében. A rendelkezésre álló információk alapján a következő hiányosságokat figyeltük meg a legtöbbször:

Javítások:

68%

az érintett szervezetek közül nem használt hatékony folyamatokat a biztonsági rések és a javítások menedzselésére, ezeknél a vállalatoknál elsősorban manuális eljárásokra hagyatkoztak a javítások automatikus telepítése helyett, ami kritikus hézagokhoz vezetett. A gyártóiparban és a kritikus infrastruktúrák területén továbbra is komoly nehézséget jelent a régebbi OT-rendszerek karbantartása és patchelése.

Megfelelő biztonsági eszközkészlet hiánya:

A legtöbb szervezet nem rendelkezett átfogó képpel a biztonsági eseményekről: a helytelenül konfigurált biztonsági eszközök révén jelentősen csökkent az észlelés és a reagálás hatékonysága.

60%

a szervezetek közül nem használt EDR[6] eszközt, amely pedig alapvető észlelési és reagálási technológiának számít.

60%

nem fektetett információ- és eseménykezelő (SIEM) rendszerekbe, ami megnehezítette az átfogó monitorozást és a fenyegetések észlelését, és a biztonsági műveleteket is megnehezítette. Az automatizálás fontos, de továbbra is jórészt hiányzik a biztonsági műveleti központok eszközkészleteiből és folyamataiból, a szakembereknek így komoly erőfeszítésbe telik a biztonsági telemetria értelmezése.

84%

az érintett szervezetek közül nem integrálta biztonsági eszközeit a többfelhős környezetével.

Reagálási és helyreállítási folyamatok:

76%

A hatékony reagálási terv hiánya az érintett szervezetek 76%-ánál kritikus problémának számított, hiszen így felkészületlenül érte őket a krízis, ami negatívan befolyásolta a reagálási és helyreállítási időt.

③ Gyenge adatvédelem

Számos megtámadott szervezet nem rendelkezett megfelelő adatvédelmi folyamatokkal, ami jelentősen meghosszabbította a helyreállításhoz szükséges időt, és megnehezítette a normál üzletmenethez való visszatérést. A következő hiányosságokat figyeltük meg a leggyakrabban:

Megváltoztathatatlan biztonsági mentések:

44%

a szervezeteknek közül nem alkalmazott megváltozhatatlan biztonsági mentést az érintett rendszerekhez. Az adatokból az is kiderül, hogy a rendszergazdák nem rendelkezte biztonsági mentési és helyreállítási tervvel a kritikus fontosságú eszközökhöz (például az AD-hoz).

Adatvesztés-megelőzés:

A támadók általában a szervezeti hézagokat kihasználva jutnak be a rendszerekbe, ellopják a zsarolásra használható kritikus adatokat és szellemi tulajdont, majd monetizálják ezeket.

92%

az érintett szervezetek közül nem alkalmazott hatékony adatszivárgás-megelőzési kontrollokat e kockázatok mérséklésére, ami kritikus adatvesztéshez vezetett.

Egyes régiókban csökkent a zsarolótámadások száma, míg máshol nőtt

Reagálási csapatainkhoz idén kevesebb zsarolótámadással kapcsolatos bejelentés érkezett az észak-amerikai és európai régióban, mint tavaly. Latin-Amerikában azonban nőtt az esetek száma.

Az egyik értelmezés lehet, hogy a kiberbűnözők felismerték, ezen a területen nagyobb a veszély, hogy magukra vonják a bűnüldöző szervek figyelmét, ezért inkább más, „puhább" célokat választottak. A Microsoft megfigyelései szerint a globális nagyvállalatok hálózati biztonsága nem javult jelentős mértékben (ami szintén megmagyarázhatná a zsarolóvírusokkal kapcsolatos támogatási hívások ritkulását), ezért azt tartjuk a legvalószínűbbnek, hogy a 2021-es és 2022-es csökkenő trendért a hatóságok aktivitása (amely megnövelte a bűnözés költségét) és bizonyos 2022-es geopolitikai események felelősek.

Az egyik legelterjedtebb RaaS-operációt egy orosz nyelvű bűnözői csoport, a REvil (más néven Sodinokibi) irányítja, amely 2019 óta aktív. 2021 októberében a GoldDust nevű nemzetközi rendőri művelet keretében lekapcsolták a REvil szervereit.[7] 2022 januárjában Oroszországban letartóztatták a REvil 14 állítólagos tagját, és a hatóságok kiszálltak 25, hozzájuk köthető helyszínre.[8] Ez volt az első alkalom, hogy Oroszország fellépett a határain belül működő zsarolócsoportokkal szemben.

2022-ben tehát a bűnüldöző hatóságok akciói valószínűleg lelassították a támadásokat, de megvan a kockázata, hogy a bűnözők hamarosan új stratégiákat dolgoznak ki, hogy elkerüljék a lebukást. Emellett Oroszország éppen most kapcsolódott be a globális zsarolóvírusok elleni küzdelembe, de az Ukrajna elleni invázió miatt feszült orosz-amerikai viszony miatt ez az együttműködés máris hamvába holt. A REvil csoporttal kapcsolatos letartóztatásokat követő rövid bizonytalanság után az Egyesült Államok és Oroszország megszakította az együttműködést a zsarolással foglalkozó bűnözők üldözésében, ami azt jelenti, hogy a kiberbűnözők ismét biztonságos menedékként tekinthetnek Oroszországra.

A jövőbe tekintve úgy véljük, hogy a zsarolótámadások helyzete attól függően fog alakulni, hogy mi lesz a válasz az alábbi fontos kérdésekre:

1. Megteszik a kormányzatok a szükséges lépéseket, hogy a zsarolóprogramok irányítói ne operálhassanak a határaikon belül, és hogy a külföldről működő bűnözők tevékenységét is megakadályozzák?
2. Elképzelhető, hogy a bűnözői csoportok módszert váltanak, kivezetve a vírusokat, és tisztán zsarolásos támadásokra támaszkodnak majd?
3. Képesek lesznek a szervezetek olyan ütemben modernizálni és átalakítani IT-műveleteiket, mint ahogy a bűnözők felfedezik a biztonsági réseket?
4. Elképzelhető, hogy a váltságdíjat követelő felek módszert váltanak a kifizetett összegek nyomon követése és felderítése terén elért előrelépések hatására?

2022-ben tehát a bűnüldöző hatóságok akciói valószínűleg lelassították a támadásokat, de megvan a kockázata, hogy a bűnözők hamarosan új stratégiákat dolgoznak ki, hogy elkerüljék a lebukást.

2X

A zsarolóvírusos támadások egyes régiókban ritkultak, de az átlagosan követelt váltságdíj több mint a kétszeresére nőtt.

Gyakorlati tanácsok

1. Összpontosítson a holisztikus biztonsági stratégiákra, hiszen minden zsarolóvírus ugyanazokat a biztonsági hiányosságokat használva jut be a hálózatra.
2. Fejlessze tovább és tartsa megfelelő állapotban a biztonsági alapokat a mélységi védelem fokozása és a biztonsági műveletek modernizálása érdekében! A felhőbe költözéssel gyorsabban észlelheti a fenyegetéseket, és hatékonyabban reagálhat rájuk.

További információra mutató hivatkozások

- Protect your organization from ransomware | Microsoft Security
- 7 ways to harden your environment against compromise | Microsoft Security Blog
- Improving AI-based defenses to disrupt human-operated ransomware | A Microsoft 365 Defender kutatócsapata
- Security Insider: Explore the latest cybersecurity insights and updates | Microsoft Security

Szolgáltatásként elérhető kiberbűnözés

A szolgáltatásként elérhető kiberbűnözés (CaaS) világszerte fokozódó és folyamatosan változó fenyegetést jelent. A Microsoft digitális bűnüldözési egysége (DCU) a CaaS-ökoszisztéma növekedéséről számolt be: egyre többen kínálnak online kiberbűnözési szolgáltatásokat, ideértve a BEC és az ember által irányított zsarolótámadásokat is. Az adathalászat ma is népszerű támadási módszer, mivel a kiberbűnözők komoly összegeket zsebelhetnek be az ellopott, majd eladott fiókokért.

A CaaS bővülő piacára válaszul a DCU továbbfejlesztette felügyeleti rendszereit, amelyek az internet minden részében képesek észlelni és azonosítani a CaaS-ajánlatokat, a deep webet, a regisztrációhoz kötött fórumokat[9], a dedikált webhelyeket, az online vitafórumokat és az üzenetküldési platformokat is ideértve.

Ma már a különböző időzónákban élő és más-más nyelven beszélő kiberbűnözők is együttműködnek a kitűzött célok elérése érdekében. Például az egyik Ázsiából irányított CaaS-webhely Európában is jelen van, de még Afrikában is létrehozott rosszindulatú célokra használt fiókokat. Ezek a tevékenységek több joghatóságot is lefednek, ami összetett kihívást jelent a törvénykezők és a hatóságok számára. A DCU ezért arra fókuszál, hogy felszámolja a bűnözők által a CaaS-támadások lebonyolítására használt infrastruktúrát, és világszerte együttműködik a bűnüldöző szervekkel, támogatva a bűnözők felelősségre vonását.

A kiberbűnözők egyre gyakrabban analitikai módszereket is bevetnek az elérés, a hatókör és a haszon maximalizálása érdekében. A törvényes vállalkozásokhoz hasonlóan a CaaS-webhelyeknek is oda kell figyelniük a jó hírükre, ezért rendszeresen ellenőrzik termékeik és szolgáltatásaik validitását. A CaaS-webhelyek például gyakran automatizálják a hozzáférést a feltört fiókokhoz, hogy ellenőrizzék a feltört hitelesítő adatok érvényességét. Ha a szervezet visszaállítják a jelszavakat vagy kijavítja a sebezhetőséget, a kiberbűnözők beszüntetik a kapcsolódó fiókok értékesítését. Egyre gyakrabban látjuk, hogy a CaaS-webhelyek egyfajta minőség-ellenőrzési folyamatként igény szerinti ellenőrzést kínálnak a vásárlók számára. A vevők ennek hatására jobban megbíznak a CaaS-webhelyben, és tudják, hogy valóban aktív fiókokat és jelszavakat vásárolnak, így a CaaS-kereskedőnek sem kell amiatt aggódnia, hogy az üzlet nyélbe ütéséig a cég törli az ellopott hitelesítő adatokat.

A DCU emellett megfigyelte, hogy sok CaaS-webhelyen a vásárlók akár a feltört fiókok földrajzi helyét is megválaszthatják, de konkrét online szolgáltatókat, magánszemélyeket, foglalkozásokat és iparágakat is megadhatnak preferenciaként. Népszerűek a számlázással foglalkozó szakemberek és részlegek, például a CFO-k és a kinnlevőségekkel foglalkozó személyek. Emellett gyakran a közbeszerzési eljárásokban érintett iparágak is gyakran kerülnek a célkeresztbe, hiszen e folyamat során rengeteg információt kell rögzíteni és átadni.

A DCU által a CaaS-szolgáltatók után indított nyomozások az alábbi fontos trendeket tárták fel:

A szolgáltatások száma és kifinomultsága egyre fokozódik.

Jó példa erre a webshellek fejlődése, amelyek általában feltört, automatizált adathalász támadásokra használt webszerverekből állnak. A DCU megfigyelte, hogy a CaaS-kereskedők speciális webes irányítópultokat használnak, amelyekkel egyszerűbb az adathalász készletek és vírusok feltöltése. A CaaS-értékesítők aztán később további szolgáltatásokat is megpróbálnak eladni a támadóknak az irányítópulton keresztül, például spammelési szolgáltatásokat és igény szerinti attribútumok (például földrajzi hely vagy szakma) alapján összeállított címlistákat. Előfordult, hogy egyetlen webshellt több kampányban is felhasználtak, ami arra utal, hogy a támadók perzisztens hozzáférést szereztek a feltört a szerverhez. Emellett a CaaS-ökoszisztémában egyre népszerűbbek az anonimizálási szolgáltatások, valamint a virtuális magánhálózatokhoz (VPN) és a virtuális magánszerverekhez (VPS) tartozó fiókok. A felkínált VPN-t/VPS-t a legtöbbször eredetileg ellopott hitelkártyák révén szerezték meg. A CaaS-webhelyek emellett nagyszámú remote desktop protocol (RDP), secure shell (SSH) és cPanel-komponenst is kínálnak, amelyek platformként használva kiválóan alkalmasak a kibertámadások lebonyolítására. A CaaS-kereskedők fel is szerelik az RDP-t, az SSH-t és a cPanelst az adott kibertámadási típushoz megfelelő eszközökkel és szkriptekkel.

A bűnözők egyre inkább kriptodevizában kérik a fizetséget a megtévesztő tartományok létrehozásáért.

A megtévesztő tartományok legitim tartományneveket utánoznak, és ehhez olyan karaktereket használnak, amelyek nagyon hasonlítanak egy másik karakterre, vagy akár teljesen ugyanúgy néznek ki. A cél, hogy a felhasználó azt higgye a megtévesztő tartományra, hogy valódi. Ezek a tartományok mindennapos fenyegetést jelentenek az interneten, és rengeteg kiberbűnöző használja őket. A CaaS-webhelyek ma gyakran kínálnak személyre szabott megtévesztő tartományneveket: a vevő mondhatja meg, hogy mely vállalatot és tartományneveket szeretné leutánozni. A fizetést követően a CaaS-kereskedő egy generátorral kiválasztja a csalárd célú tartománynevet, majd regisztrálja. Ezért a szolgáltatásért szinte minden esetben kriptodevizában kell fizetni.

2 750 000

oldalregisztrációt blokkolt idén a DCU, megelőzve így a bűnözőket, akik csalárd célokra akarták felhasználni őket világszerte.

Szolgáltatásként elérhető kiberbűnözés

Folytatás

A CaaS-kereskedők egyre gyakrabban értékesítenek feltört hitelesítő adatokat.

A feltört hitelesítő adatokkal illetéktelen személyek is hozzáférhetnek a felhasználói fiókokhoz, például az e-mail-szolgáltatásokhoz, a vállalati fájlmegosztási erőforrásokhoz és a OneDrive Vállalati verzióhoz. Ha rendszergazdai hitelesítő adatokat sikerül ellopni, a jogosulatlan felhasználók akár a bizalmas fájlokat, az Azure-erőforrásokat és a vállalati felhasználói fiókokat is elérhetik. A DCU vizsgálatai sok esetben arra jutottak, hogy a támadók több szerveren is felhasználják a jogtalanul megszerzett loginokat, automatizálva ezzel a hitelesítő adatok ellenőrzését. Ez a mintázat arra utal, hogy a feltört felhasználó több adathalász támadás áldozatává vált, vagy botnetes billentyűzetfigyelőket telepítettek az eszközére, és így jutottak hozzá a hitelesítő adataihoz.

A CaaS-szolgáltatások és -termékek ma továbbfejlesztett funkciókat kínálnak, amelyek segítenek rejtve maradni.

Az egyik CaaS-kereskedő rendkívül összetett, anonimizálási funkciókat is tartalmazó adathalász készleteket kínál, amelyek képesek rejtve maradni az észlelési és reagálási rendszerek előtt – ez a szolgáltatás akár már napi 6 USD-ért elérhető. A megoldás átirányítások sorozatát alkalmazza, amelyek ellenőrzéseket végeznek, mielőtt továbbengedik a forgalmat a következő rétegbe vagy webhelyre. Az egyik ilyen szolgáltatás több mint 90 ellenőrzést végez az eszköz ujjlenyomattal történő feloldásakor, például hogy virtuális gépről van-e szó, emellett adatokat gyűjt a használt böngészőről, hardverről stb. Ha minden ellenőrzés sikeresen teljesül, megnyílik az adathalász webhely.

Teljes körű kiberbűnözési szolgáltatások, előfizetések és felügyelt szolgáltatások.

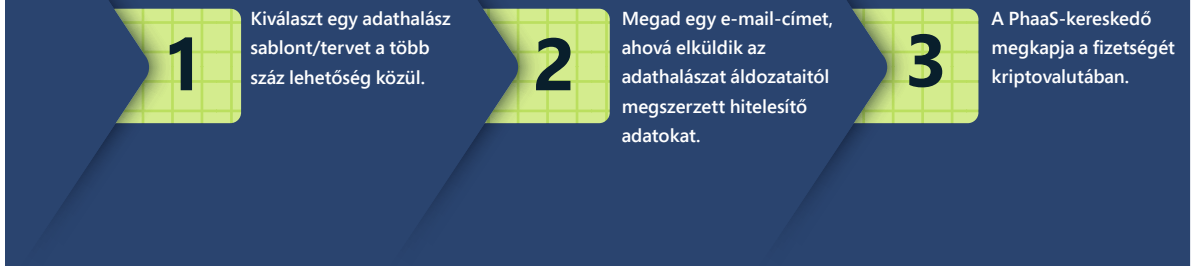
Normál esetben az online bűncselekmények minden lépésénél fény derülhet a támadók kilétére, ha nem figyelnek oda kellően az operatív védekezésre. A felderítés és az azonosítás kockázata nő, ha a támadók több CaaS-webhelytől is vásárolnak szolgáltatásokat. A DCU aggasztó trendet figyelt meg a sötét weben: egyre több szolgáltatás érhető el a szoftverkód anonimizálására és a webhelyeken használt szövegek általánosítására – a cél a lebukás elkerülése. A teljes körű, előfizetéses szolgáltatásokat kínáló kiberbűnözők maguk menedzselik az összes szolgáltatást, és garantált eredményeket kínálnak – ez tovább csökkenti a kockázatot az előfizető OCN számára. Az alacsonyabb kockázatok miatt ezek a teljes körű szolgáltatások rendkívül népszerűek.

A szolgáltatásként kínált adathalászat (PhaaS) jó példa a teljes körű kiberbűnözési szolgáltatásra. A PhaaS a korábban „nem észlelhető szolgáltatások” (FUD) néven ismert megoldás fejlődésével jött létre, és előfizetéses alapon érhető el. A PhaaS keretében a szolgáltató általában egy hónapig tartja fenn az adathalász webhelyet.

A DCU emellett olyan CaaS-kereskedőket is talált, amelyek előfizetéses alapú szolgáltatásmegtagadásos támadásokat (DDoS) kínálnak. Ebben a modellben a támadásokhoz használt botnet létrehozásáért és fenntartásáért a CaaS-kereskedő felel. A DDoS-előfizetést vásárló ügyfelek az operatív biztonság fokozása érdekében titkosított szolgáltatást, valamint egy évre szóló, éjjel-nappal elérhető támogatást kapnak. A DDoS-előfizetés különböző architektúrákhoz és támadási módszerekhez kínál hozzáférést, így a vásárló egyszerűen kiválasztja a megtámadni kívánt erőforrást, és a kereskedő rendelkezésére bocsátja a botnethez tartozó feltört eszközök egy részét. Az ilyen DDoS-előfizetés ára mindössze 500 USD.

A DCU folyamatosan azon dolgozik, hogy olyan eszközöket és technikákat fejlesszen ki, amelyek képesek felderíteni és felszámolni a CaaS-kiberbűnözőket. A CaaS-szolgáltatások fejlődése azonban komoly kihívásokat jelent, különösen a kriptodevizás kifizetések megakadályozása okoz nehézséget.

PhaaS – több kiberbűnözői szolgáltatás egyetlen előfizetésen belül. A vásárlónak általában csak három dolgot kell tennie:



Ha ezek a lépések befejeződtek, a PhaaS-kereskedő létrehoz egy három vagy négy átirányítási és hosztolási réteggel rendelkező szolgáltatást, amellyel konkrét felhasználókat lehet célba venni. Ezután elindul a támadás, megszerzik és ellenőrzik az áldozat hitelesítő adatait, majd elküldik a vásárló által megadott e-mail-címre. Felárért számos PhaaS-kereskedő a nyilvános blockchainben is hajlandó hosztolni az adathalász webhelyet, amely így bármilyen böngészőből megnyitható, és az átirányításokkal az elosztott nyilvántartásban található erőforrások is megcélozhatók.

A kriptodevizák használata bűncselekményekhez

A kriptodevizák mára széles körben elterjedt megoldásnak számítanak, ezért egyre több bűnöző támaszkodik rájuk, hogy elkerülje a hatóságokat és a pénzmosás elleni intézkedéseket. A bűnüldöző szervek számára ezért komoly kihívást jelent a kiberbűnözőkhöz irányuló kriptodevizás kifizetések nyomon követése és felderítése.

Az elmúlt négy évben körülbelül 340%-kal nőtt a blockchain-megoldásokkal megvalósított kifizetések volumene, az új kriptodeviza-pénztárcák száma pedig kb. 270%-kal emelkedett. Ma világszerte több mint 83 millió egyedi pénztárca létezik, a kriptodevizák teljes piaci kapitalizációja pedig körülbelül 1,1 billió USD (2022. július 28-án).[10]

Forrás: Twitter.com—@PeckShieldAlert (aPeckShield egy kínai vállalat, amely a blockchain biztonságával foglalkozik).

A zsarolótámadásokhoz kapcsolódó kifizetésének nyomon követése

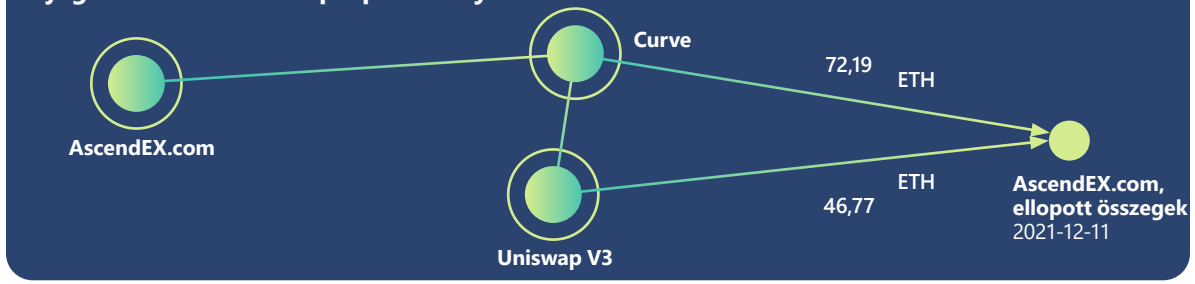
A zsarolótámadások a jogszerűtlenül szerzett kriptopénzek egyik legnagyobb forrását jelentik. A törvénytelen célokra, például zsarolótámadásokra használt technikai infrastruktúra felszámolása érdekében a Microsoft DCU nyomon követi a bűnözők pénztárcáit, hogy elősegítse a kriptopénzek visszaszerzését (ilyen akció volt a Zloader elleni fellépés 2022 áprilisában[11]).

A DCU nyomozói megfigyelték, hogy a zsarolók egyre fejlettebb kommunikációs módszereket alkalmaznak az áldozatokkal történő egyeztetés során, hogy elfedjék a pénz útját. A kiberbűnözők kezdetben bitcoin-címeket adtak meg a váltságdíjat követelő üzeneteikben. Ez azonban megkönnyítette a fizetési tranzakciók nyomon követését a blockchainben, így a zsarolók ma már inkább e-mail-címeket vagy csevegési webhelyekre mutató hivatkozásokat küldenek, és ezeken keresztül tárgyalnak a váltságdíjról. Olyat is láttunk, hogy a támadók egyedi weboldalakat és bejelentkezési adatokat hoztak létre az egyes áldozatokhoz, hogy a biztonsági kutatók és a hatóságok ne tudják megszerezni a bűnözők pénztárcájának címét azáltal, hogy áldozatnak adják ki magukat. A bűnözők tehát mindent megtesznek, hogy eltöröljék a nyomaikat, de a blockchain-mozgások nyomon követésével a bűnüldöző szervek és a kriptoelemzők esetenként továbbra is képesek visszaszerezni a váltságdíjat.

Trend: DEX – a jogszerűtlenül szerzett pénz tisztára mosása

A kiberbűnözők előtt álló egyik legnagyobb kihívás, hogy a megszerzett kriptodevizát fiat valutára váltsák. A kiberbűnözők több különböző módszert is bevethetnek, amelyek mindegyike eltérő kockázatokat rejt. A kockázatok csökkentésének egyik módja, ha a pénzt átvezetik egy decentralizált tőzsdén (DEX), majd készpénzzé alakítják a különféle kivételi opciók, például a centralizált tőzsdék (CEX), társközi (P2) megoldások és over the counter (OTC) tőzsdék segítségével. A DEX azért jelent vonzó megoldást a pénzmosásra, mert ezek a tőzsdék gyakran nem alkalmaznak AML-intézkedéseket.

A jogtalanul szerzett kriptopénzek nyomon követése



A Microsoft digitális bűnüldözési egysége a kriptodeviza-nyomozásokhoz készült Chainalysis eszköz segítségével rájött, hogy az AscendEX hackerei az Uniswap mellett egy Curve nevű kisebb DEX-et is felhasználták a pénzmosáshoz. Az itt szereplő ábra bemutatja a felderített pénzmosási útvonalakat. Mindegyik kör egy pénztárcaklasztert képvisel, a vonalakon jelzett számok pedig a pénzmosási célból átutalt ethereum-összeget adják meg.

2021 decemberében hackerek támadták meg az AscendEx nevű globális kriptodeviza-platformot, és mintegy 77,7 millió dollár értékű kriptodevizát loptak el a platform ügyfeleitől.[12] Az AscendEx blockchain-analitikai vállalatokat bízott meg a nyomozással, és felvette a kapcsolatot más CEX tőzsdékkel, és kérte, hogy helyezzék feketelistára az ellopott pénzt tartalmazó pénztárcákat. Emellett az Etherscan nevű, ethereum blockchainnel foglalkozó felderítő megjelölte azokat a címeket, ahová az ellopott coint küldték.[13] A riasztások és a feketelisták megkerülése érdekében a hackerek 2022. február 18-án 1,5 millió dollár értékű ethereumot küldtek az Uniswapra, a világ egyik legnagyobb DEX tőzsdéjére.[14]

Ha a DEX-ek erősebb pénzmosás elleni intézkedéseket vezetnek be, kiránthatják a talajt a bűnözők lába alól, akik így kénytelenek lesznek más módszerekhez folyamodni a lopott összegek elrejtéséhez, ilyen lehet például a coin tumbling vagy az engedély nélküli tőzsdék használata. Jó példa erre, hogy az Uniswap a közelmúltban bejelentette, feketelistákat fog felállítani, és kitiltja a tőzsdéről a jogszerűtlen tevékenységekben érintett pénztárcákat.[15]

Gyakorlati tanácsok

1. Ha áldozattá vált, és kriptodevizában fizetett a bűnözőknek, forduljon a helyi bűnüldöző szervekhez – elképzelhető, hogy tudnak segíteni az elvesztett pénz visszaszerzésében.
2. Amikor DEX-et választ, nézzen utána, hogy milyen pénzmosásellenes intézkedéseket alkalmaz az adott tőzsde.

További információra mutató hivatkozások

- Hardware-based threat defense against increasingly complex cryptojackers | A Microsoft 365 Defender kutatócsoportja

Az adathalászat változásai

Egyre gyakoribbak a hitelesítő adatokat célzó adathalász támadások, amelyek továbbra is komoly fenyegetést jelentenek a felhasználókra, hiszen válogatás nélkül minden lehetséges postafiókot megcéloznak. A kutatóink által követett és leküzdött támadások közül az adathalászok minden más bűnözőnél jóval nagyobb szeletet képviselnek.

A Defender for Office adataiból kiderül, a rosszindulatú e-mailek és a feltört identitások is súlyos problémákat okoznak. Az Azure Active Directory Identity Protection további információkat nyújt erről a feltört identitásokkal kapcsolatos riasztások révén. A Defender for Cloud Apps segítségével felderíthetjük, hogy milyen adatokhoz férnek hozzá a feltört identitásokkal, a Microsoft 365 Defender (M365D) pedig lehetővé teszi a különböző termékek közötti korrelációt. A laterális mozgásokkal kapcsolatos metrikák a Végponthoz készült Defenderből (támadási viselkedés és események), a Defender for Office-ból (rosszindulatú e-mailek) származnak, az M365D pedig lehetővé teszi a termékek közötti korrelációt.

710 millió
blokkolt adathalász e-mail hetente.

1 óra 12 perc
Átlagosan ennyi időre volt szükségük a támadóknak, hogy hozzájussanak az adathalász e-mailek áldozatául esett személyek privát adataihoz.[16]

1 óra 42 perc
Átlagosan ennyi időre volt szükségük a támadóknak, hogy laterális mozgásba kezdjenek a vállalati hálózaton, miután sikerült feltörniük egy eszközt.[17]

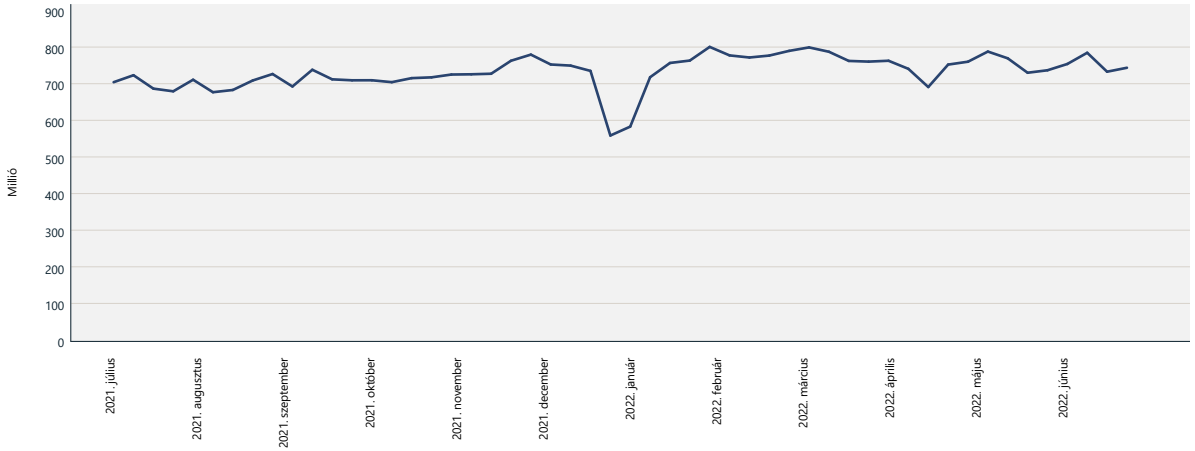
A támadók továbbra is gyakran próbálnak hozzájutni a Microsoft 365-fiókok hitelesítő adataihoz. Ha sikerült ellopniuk a hitelesítő adatokat, a támadók bejelentkezhetnek a vállalati szintű számítógépes rendszerekbe, majd kártevők és zsarolóprogramok segítségével megfertőzhetik ezeket, ellophatják a SharePoint-fájlokban rejlő bizalmas vállalati adatokat és információkat, és az Outlook segítségével további csalárd e-maileket küldhetnek, így kiterjeszthetik adathalász tevékenységüket.

A szélesebb körű kampányok (amelyek hitelesítő és személyes adatokat céloznak, valamint adományokat kérnek) mellett a támadók szelektívebb műveleteket is folytatnak, amelyekkel egy adott vállalatot céloznak meg a nagyobb nyereség reményében. A cégek elleni, pénzügyi haszonszerzés céljából indított e-mailes adathalász támadásokat BEC támadásoknak is nevezzük. A Microsoft havonta több millió ilyen e-mailt fedez fel, a BEC az összes adathalász levél 0,6%-át teszi ki. Az IC3[18] által 2022 májusában publikált jelentés szerint a vállalatok egyre súlyosabb veszteségeket szenvednek el a BEC-támadások miatt.

Az adathalász támadásokhoz használt módszerek egyre fejlettebbé válnak. Az ellenintézkedésekre reagálva a támadók folyamatosan új módszereket dolgoznak ki, és egyre összetettebb megoldásokkal és helyszíneken hosztolják a kampányaikhoz szükséges infrastruktúrát. Ez azt jelenti, hogy a vállalatoknak is rendszeresen felül kell vizsgálniuk a biztonsági megoldások implementálására vonatkozó stratégiájukat, hogy blokkolják a rosszindulatú e-maileket, és megerősítsék a felhasználói fiókok hozzáférés-szabályozását.

531 000
A Defender for Office által blokkolt URL-címek mellett a digitális bűnüldözési egység 531 000 egyedi, a Microsoft rendszerein kívül hosztolt adathalász URL felszámolását is levezényelte.

Észlelt adathalász e-mailek



A hetente észlelt adathalász támadások száma folyamatosan nő. A decemberi-januári csökkenés várható szezonális trend, amelyet a tavalyi jelentésben is megfigyeltünk. Forrás: Exchange Online védelmi jelek.

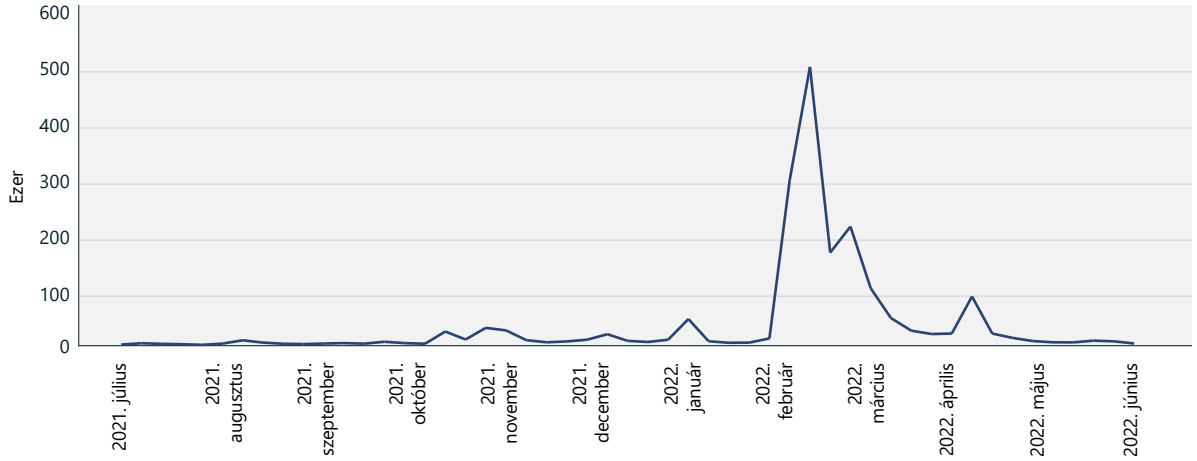
Az adathalászat változásai

Folytatás

Az adathalász e-mailek száma továbbra is évről évre nő. A távmunkára való 2020-as és 2021-es átállás hatására az adathalász támadások csak még gyakoribbá váltak, a bűnözők igyekeztek kihasználni a munkakörnyezet megváltozását. Az adathalászok gyorsan új e-mail-sablonokat dolgoztak ki a világban zajló jelentős eseményekre reagálva: ezt láttuk a koronavírus-világjárvány során, amikor gyakran együttműködési és hatékonyságnövelő eszközökhöz, például a Google Drive-hoz és a OneDrive-fájlmegosztáshoz kapcsolódó csalikat használtak. A koronavírus ma már kevésbé népszerű téma, 2022 márciusának elejétől átvette a helyét az ukrajnai háború. A kutatók hatalmas mennyiségű csalárd e-mailt láttak, amelyek valódi szervezetek nevében arra kérték a címzetteket, hogy adományozzanak bitcoint, ethereumot és más kriptodevizákat az ukrán lakosság megsegítésére.

Még csak néhány nap telt el az ukrajnai háború kirobbanása után, amikor 2022 februárjának végén már azt tapasztaltuk, hogy jelentősen megnőtt a nagyvállalati ügyfeleknek küldött, ethereum-címeket tartalmazó adathalász e-mailek száma. A csúcs március első hetében érkezett el, amikor félmillió olyan levelet küldtek, amely valamilyen ethereum-pénztárcára mutatott. A háború előtt az adathalászathoz köthető e-mailek jóval ritkábban tartalmaztak ethereum-címeket, átlagosan hetente néhány ezer ilyen levelet észleltünk.

Adathalász e-mailek, amelyek ethereum-pénztárcára mutatnak



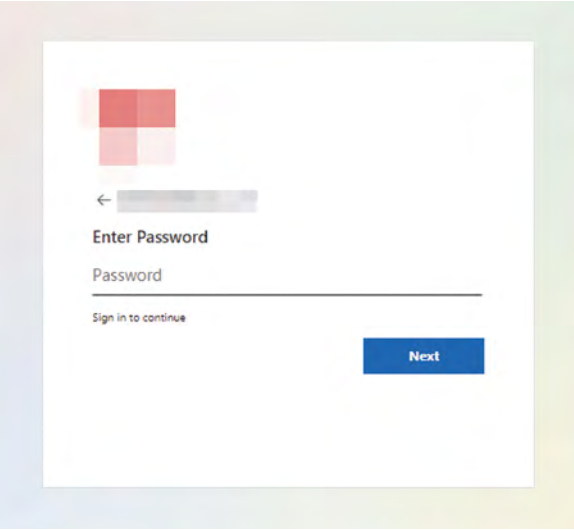
Az ukrán-orosz háború kirobbanását követő napokban megnőtt az ethereumcímet tartalmazó adathalász e-mailek száma, de ez a lendület a kezdeti csúcsok után viszonylag hamar alábbhagyott.

Az adathalászok ma minden korábbinál nagyobb mértékben támaszkodnak a legitim infrastruktúrákra, ezért egyre több olyan kampányt látunk, amelyek célja, hogy feltörjék valamilyen szervezet rendszerének bizonyos elemeit, és így megspórolják a saját környezet megvásárlásának, hosztolásának és üzemeltetésének költségeit. A rosszindulatú e-mailek gyakran feltört fiókokból származnak. A támadók számára azért is előnyösek ezek az e-mail-címek, mert magasabb reputációs pontszámmal rendelkeznek, és megbízhatóbbnak tartják őket, mint az újonnan létrehozott fiókokat és tartományokat. Néhány kifinomultabb adathalász kampánynál azt is megfigyeltük, hogy a támadók azokat a tartományokat részesítik előnyben, amelyeknél a DMARC[19] esetében helytelenül a „nincs művelet" értékre van állítva, ami megkönnyíti az e-mailek hamisítását.

A nagy léptékű adathalász tevékenységek általában felhőszolgáltatásokra és felhős virtuális gépekre hagyatkoznak. A támadók virtuális gépek, SMTP-üzenettovábbítók és felhős e-mail-infrastruktúrák segítségével akár teljes mértékben automatizálhatják az e-mailek küldését, így az ezekhez a legitim szolgáltatásokhoz köthető magas kézbesíthetőségi arányt és pozitív hírnevet is kihasználhatják. Az ilyen felhőszolgáltatásokon keresztül küldött rosszindulatú e-mailek esetében erős e-mail-szűrési funkciókat kell implementálni, hogy a csalárd levelek ne is juthassanak be a környezetbe.

A Microsoft-fiókok továbbra is népszerű célpontot jelentenek az adathalászok számára. Ezt bizonyítja, hogy számos adathalász operáció a Microsoft 365 bejelentkezési oldalát utánozza. Az adathalászok emellett a Microsoft bejelentkezési módszerét is igyekeznek leutánozni: programjaik gyakran egyedi, a címzettre szabott URL-címet generálnak. Ez az URL egy rosszindulatú webhelyre mutat, amelyet hitelesítő adatok gyűjtésére fejlesztettek ki, de az URL-címben megadott paraméter az adott címzett e-mail-címét tartalmazza. Ha a célpont megnyitja ezt az oldalt, az adathalász készlet kitölti a felhasználói bejelentkezési adatokat, és megjelenít egy, a címzettre szabott vállalati logót, hogy elhitesse vele, az adott vállalat egyedi Microsoft 365 bejelentkezési oldalán van.

Egy dinamikus tartalmat használó adathalász oldal, amely a Microsoft-bejelentkezést utánozza

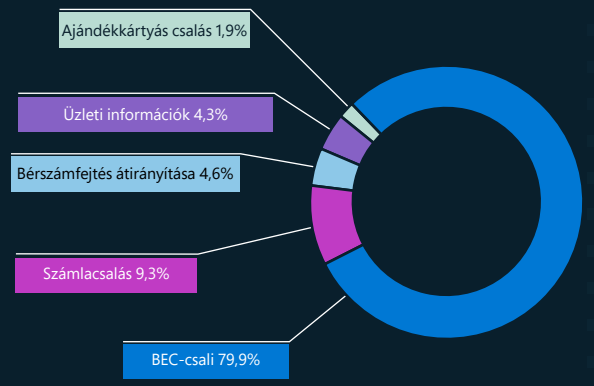


Reflektorfényben az üzleti e-mailek feltörése

A kiberbűnözők egyre összetettebb terveket és módszereket dolgoznak ki, hogy megkerüljék a biztonsági beállításokat. Magánszemélyek, gazdasági és más szervezetek egyaránt a célpontjaikká válhatnak. A Microsoft ezért komoly erőforrásokat fordít a BEC elleni védekezésre.

A BEC a kiberbűnözés legnagyobb károkat okozó fajtája: 2021-ben 2,4 milliárd USD veszteség köthető ezekhez a támadásokhoz, ami az öt legsúlyosabb kiberbűnözés által okozott kár 59%-át lefedi.[20] A Microsoft biztonsági kutatói folyamatosan figyelik az ilyen támadások során használt módszereket, hogy pontos képet kapjanak a probléma súlyáról, és megtalálják a BEC elleni védekezés optimális módját.

Trendek a BEC terén (2022. január és június között)



A BEC-trendek százalékos előfordulása

BEC-trendek

A folyamat első lépéseként a BEC-támadók általában megpróbálnak beszélgetésbe elegyedni az áldozattal. Munkatársnak vagy üzleti ismerősnek adják ki magukat, és idővel valamilyen pénzösszeg átutalására terelik a szót. A bemutatkozó e-mail, amelyet a BEC csalijának nevezünk, az észlelt BEC-üzenetek 80%-át teszi ki. A Microsoft biztonsági kutatói az alábbi trendeket is megfigyelték az elmúlt év során:

- 2022-ben a BEC-támadások elsősorban hamisításra[21] és megszemélyesítésre alapultak.[22]
- A legtöbb anyagi kárért felelős BEC-altípus a számlával kapcsolatos csalás volt (a BEC-kampányokkal kapcsolatos vizsgálataink során látott mennyiségek és követelt összegek alapján).
- Ha a támadók üzleti információkhoz (például a kötelezettségekkel kapcsolatos beszámolókhoz és az ügyfelek elérhetőségeihez) jutnak, meggyőzőbben tudják végrehajtani a számlacsalást.
- A bérszámfejtés átirányításával kapcsolatos legtöbb kérést ingyenes e-mail-szolgáltatásból küldték, ezen a területen ritkán használtak feltört fiókokat. Az ilyen típusú e-mailek volumene minden hónap első és tizenötödik napja körül megugrott – ezek a leggyakoribb fizetésnapok.
- Az ajándékkártyás csalások közismertek, de csak az észlelt BEC-támadások 1,9%-át tették ki.

Gyakorlati tanácsok

Védekezés az adathalászok ellen

A vállalat adathalászattal szembeni kitettségének csökkentése érdekében javasoljuk, hogy az IT-adminisztrátorok vezessék be az alábbi szabályzatokat és funkciókat:

1. A korlátlan hozzáférés megakadályozása érdekében írják elő az MFA-t minden fióknál.
2. A magas jogosultsági szintű fiókoknál használjanak feltételes hozzáférést, amely letiltja a hozzáférést az olyan országokból, régiókból és IP-címekről, amelyek általában nem generálnak forgalmat a szervezetnél.
3. Ha lehetséges, a vállalat vezetői, a fizetési és beszerzési tevékenységekkel foglalkozó munkatársak és más, magas jogosultsági szintű felhasználók használjanak fizikai biztonsági kulcsokat.
4. Tegye kötelezővé az olyan böngészők használatát, amelyek támogatják például a Microsoft SmartScreent (vagy más, hasonló szolgáltatásokat). Ezek az URL-ek elemzésével kiszűrik a gyanús viselkedést, és letiltják a hozzáférést az ismert rosszindulatú webhelyekhez.[23]
5. Használjanak gépi tanulásra épülő biztonsági megoldást, amely karanténba helyezi a nagy valószínűséggel adathalász üzeneteket, és egy tesztkörnyezetben aktiválja az URL-eket és a mellékleteket, mielőtt az e-mail megérkezne a postaládába (ilyen például a Microsoft Defender for Office 365).[24]
6. Használjanak megszemélyesítés és hamisítás elleni védelmi funkciókat a szervezet minden pontján.
7. Konfigurálják úgy a DomainKeys Identified Mail (DKIM) és a Domain-based Message Authentication Reporting & Conformance (DMARC) szabályzatokat, hogy megakadályozzák a nem hitelesített e-mailek kézbesítését, amelyeknél fennáll a kockázat, hogy legitim feladóknak próbálják kiadni magukat.
8. Auditálják a tenantok és a felhasználók által létrehozott engedélyezési szabályokat, és távolítsák el a széles körű, tartomány- és IP-alapú kivételeket. Ezek a szabályok gyakran elsőbbséget élveznek, és átengedhetik a tudottan kártékony e-maileket az e-mail-szűrőkön.
9. Végezzenek folyamatos adathalászati szimulációkat, amellyel felmérhető a kockázat szintje a vállalatnál, és azonosíthatók és továbbképezhetők a sérülékeny felhasználók.

További információra mutató hivatkozások

- From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | A Microsoft 365 Defender kutatócsoportja, Microsoft Threat Intelligence Center (MSTIC)

Megtévesztés

A BEC és az adathalászat gyakori manipulációs módszerek. A pszichológiai manipuláció a bűnözők fontos fegyvere: megpróbálják elnyerni az áldozat bizalmát, hogy aztán rávegyék valamire.

A fizikai kereskedelemben a védjegyek jelzik, hogy az adott termék vagy szolgáltatás megbízható, és a termékek hamisítása egyben a védjeggyel való visszaélést is jelenti. A kiberbűnözők is hasonlóan járnak el: a célpont ismerősének adják ki magukat, így igyekeznek megtéveszteni a potenciális áldozatot.

A BEC-üzenetek gyakran megtévesztő tartományneveket is tartalmaznak, amelyeknél a valódi tartománynév egyik karakterét lecserélték egy azonos vagy nagyon hasonló megjelenésű másik karakterre.

A BEC-támadások során használt megtévesztési technikák

A BEC általában két fázisból áll: a bűnözők először valahogyan megszerzik a hitelesítő adatokat, például adathalász támadással vagy nagy léptékű adatvédelmi incidensek során. A hitelesítő adatokat ezután a sötét weben értékesítik vagy elcserélik.

A második fázis a csalási fázis, amelyben a támadók a megszerzett hitelesítő adatokat használva kifinomult pszichológiai manipulációs technikákat alkalmaznak, és a valóshoz hasonló e-mail-tartományokat használnak.

Egy BEC-támadás előrehaladása

Technika	A megtévesztési technikát alkalmazó tartományok %-os aránya
I helyett l	25%
l helyett i	12%
g helyett q	7%
m helyett rn	6%
.com helyett .cam	6%
o helyett 0	5%
l helyett ll	3%
i helyett ii	2%
w helyett vv	2%
ll helyett l	2%
a helyett e	2%
m helyett nn	1%
I helyett ll, i helyett l	1%
u helyett o	1%

Több mint 1700 ilyen megtévesztő tartományt elemeztünk 2022 januárja és júliusa között. Míg a támadók összesen 170 megtévesztő technikát alkalmaztak, a tartományok 75%-a mindössze 14 technikát használt.

Egy megtévesztő tartomány működés közben

Egy e-mail-szolgáltatónál regisztrálnak egy olyan megtévesztő tartományt, amely hasonlít az áldozat által ismert egyik tartományra, és mindehhez a valóshoz megtévesztően hasonlító felhasználónevet választanak. Ezután eltérített e-mailt küldenek az eltérített tartományból az új fizetési utasításokkal.

A nyílt forrású intelligenciát és az e-mail-szálakhoz való hozzáférést kiaknázva a bűnöző beazonosítja a számlázásért és fizetésért felelős felhasználókat. Ezután létrehoz a számlákat küldő felhasználót megszemélyesítő e-mail-címet. A megszemélyesítéshez a valódi feladó felhasználónevéhez és e-mail-tartományához megtévesztően hasonló címet használ.

A támadó lemásol egy valódi számlát tartalmazó e-mail-láncot, majd úgy módosítja a számlát, hogy az a saját banki adatait tartalmazza. Ezt az új, módosított számlát ezután a megtévesztő, az eredeti feladót megszemélyesítő e-mail-címről küldi el a kiszemelt célszemélynek. Mivel a kontextus és az e-mail valódinak tűnik, a megcélzott felhasználó gyakran követi a csalárd utasításokat.

Gyakorlati tanácsok

1. Tegye kötelezővé az szolgáltatásokat támogató böngészők használatát, amelyek az URL-ek elemzésével kiszűrik a gyanús viselkedést, és letiltják a hozzáférést az ismert rosszindulatú webhelyekhez. Ilyen szolgáltatás például a Safe Links és a SmartScreen.[25]
2. Használjon gépi tanulásra épülő biztonsági megoldást, amely karanténba helyezi a nagy valószínűséggel adathalász üzeneteket, és egy sandboxban detonálja az URL-eket és a mellékleteket, mielőtt az e-mail megérkezne a postaládába.

További információra mutató hivatkozások

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Spoof intelligence insight— Office 365 | Microsoft Docs
- Impersonation insight—Office 365 | Microsoft Docs

A botnetes támadások idővonala a Microsoft együttműködésének korai időszakától

A DCU több mint egy évtizede azon dolgozik, hogy proaktív módon megálljt parancsoljon a kiberbűnözésnek, amelynek során 26 rosszindulatú szoftver és nemzetállami rosszindulatú programot számolt fel. Ahogy a DCU csapata is egy fejlettebb taktikákat és eszközöket használ ezeknek az illegális műveleteknek letöréséhez, azt láthattuk, hogy a kiberbűnözők is egyre fejlettebb megközelítést alkalmazva próbálnak meg előnyben maradni. Ezen az idővonalon a DCU által leállított botnetekre, és a Microsoft által a felszámolásukhoz használt stratégiákra láthatók példák.

2008

Conficker botnet

Leírás: A Windows operációs rendszert célzó, gyorsan terjedő féreg, amelyek számítógépek és az eszközök millióit fertőzte meg egy közös hálózaton, és világszerte hálózati kimaradásokat okozott.

Együttműködés: Megalakult a Conficker munkacsoport – egy, a maga nemében elsőnek számító konzorcium. A Microsoft világszerte 16 szervezettel lépett partnerségre a bot legyőzéséhez.

A Microsoft válasza: A csoport számos a világ számos joghatóságával együttműködve végül sikeresen legyőzte a Conficker.

2009

Waledac botnet

Leírás: Összetett spambotnet egyesült államokbeli tartományokkal, amelyek e-mail-címeket gyűjtöttek, és spameket terjesztettek, melyek révén világszerte 90 000 számítógépet fertőztek meg.[26]

Együttműködés: Egy másik konzorcium, a Microsoft Malware Protection Center (MMPC) létrehozása, amely az akadémiai szférával való szoros együttműködésre összpontosított.[27]

A Microsoft válasza: A Microsoft többszintű megközelítést használt a C2 felszámolásához, és meglepte a rosszindulatú szereplőket az egyesült államokbeli tartományok figyelmeztetés nélküli lefoglalásával.[28] A Microsoft ideiglenes tulajdonjogot kapott a Waledac szerverei által használt közel 280 tartományra.

2011

Megalakult a Microsoft Digital Crimes Unit

Együttműködés: A Microsoft ökoszisztémáját befolyásoló kiberbűnözés kiküszöbölése érdekében szoros integráció jött létre egy nyomozókból, jogászokból és mérnökökből álló csapaton belül.

A Microsoft megközelítése: A cél az, hogy jobban megértsük a különböző rosszindulatú szoftverek technikai aspektusait, és ezeket az információkat a Microsoft jogi csapatának rendelkezésére bocsássuk, egy hatékony felszámolási stratégia kialakításához.

2013

Rustock botnet

Leírás: Egy backdoor típusú trójai, spam-e-mailekben terjedő bot, amely az internetszolgáltatókat használta elsődleges C2-ként, és a célja gyógyszerek értékesítése volt.

Együttműködés: A Microsoft a Pfizer Pharmaceuticals vállalattal lépett partnerségre, hogy megismerje a Rustock által árusított gyógyszereket, és szorosan együttműködött a holland bűnüldöző szervek tisztviselőivel.[29]

A Microsoft válasza: A Microsoft a US Marshals Service-szel és a holland bűnüldöző szervekkel együttműködve kapcsolta le az országban működő C2-szervereket. Regisztrálta és letiltotta az összes jövőbeli tartománygenerátor algoritmust (DGA-t).

Sirefef/Zero Access botnet

Leírás: Reklámbotnet, amelyet úgy alakítottak ki, hogy az embereket veszélyes webhelyekre irányítsa, amelyek kártevőket telepítenek vagy személyes adatokat lopnak. Több mint két millió számítógépet fertőzött meg, és a hirdetőknek több mint 2,7 millió dollárjába került havonta. Elsősorban az Egyesült Államokban és Nyugat-Európában okozott károkat.

Együttműködés: Szorosan együttműködtünk az FBI-jal és az Europol Kiberbűnözési Központjával a P2P-infrastruktúra felszámolása érdekében.

A Microsoft válasza: Csatlakozott a Zero Access-hálózathoz, lecserélte a bűnözők C2-szervereit, és sikeresen lefoglalta letöltési szerverek tartományait.

2019

Trickbot botnet

Leírás: Kifinomult botnet, amely a pénzügyi szolgáltatási ágazatot vette célba egy világszerte széttagolt infrastruktúrával, és az IoT-eszközöket törte fel.

Együttműködés: A Microsoft a Financial Services Information Sharing and Analysis Center (FS-ISAC) szervezettel lépett partnerségre a Trickbot felszámolásához.[30]

A Microsoft válasza: A DCU olyan rendszert épített ki, amely azonosítja és a nyomon követi a botinfrastruktúrát, és ez a rendszer értesítéseket küldött az aktív internetszolgáltatóknak, figyelembe véve a különböző országok hatályos törvényeit.

2022

További összpontosítás a káros tevékenységek zavarására

Leírás: A Microsoft az elmúlt év során hét támadó infrastruktúráját számolta fel, megakadályozva őket a további kártevők terjesztésében, az áldozatok számítógépének ellenőrzésében és a további áldozatok kiválasztásában.

Együttműködés: Az internetszolgáltatókkal, a kormányokkal, a bűnüldöző szervekkel és az ipari magánszektorral együttműködve a Microsoft olyan információkat osztott meg, amelyek világszerte a kártevők több mint 17 millió áldozatának nyújtottak segítséget.

A jövő

A DCU folytatja az innovációt, és arra törekszik, hogy a botnetek felszámolásában szerzett tapasztalatait a rosszindulatú szoftvereken túlmutató koordinált műveletek során is kamatoztassa. Folyamatos sikerünkhöz kreatív tervezésre, az információk megosztására és az innovatív jogi elméletekre éppúgy szükség van, mint a köz- és a privát szféra közötti partnerségekre.

Visszaélés legitim infrastruktúrákkal

Internetes átjárók használata a bűnözők irányítási infrastruktúrájaként

Az IoT-eszközök egyre népszerűbb célpontok a kiterjedt botneteket használó kiberbűnözők körében. A javítások telepítése nélkül az interneten elérhetővé tett útválasztókat a támadóok arra használhatják, hogy hozzáférést szerezzenek a hálózatokhoz, rosszindulatú támadásokat indítsanak, vagy akár támogassák a saját műveleteiket.

A Microsoft Defender for IoT csapata a régi típusú ipari vezérlőrendszerek kontrollereitől a legmodernebb IoT-szenzorokig számos készüléket elemez. A csapat vizsgálja az IoT- és OT-specifikus rosszindulatú szoftvereket, hogy hozzájáruljon a biztonsági incidensekre utaló jelzések közös listájához.

Az útválasztók különösen sebezhető támadási vektorok, mert az internetre kapcsolódó háztartásokban és szervezeteknél mindenütt megtalálhatók. Nyomon követtük a lakossági és üzleti környezetben egyaránt népszerű MikroTik útválasztók tevékenységét világszerte, és beazonosítottuk, hogyan használják őket irányítási (C2) és a tartománynévrendszerrel (DNS) kapcsolatos támadásokhoz, és hogyan térítik el őket kriptobányászat céljából.

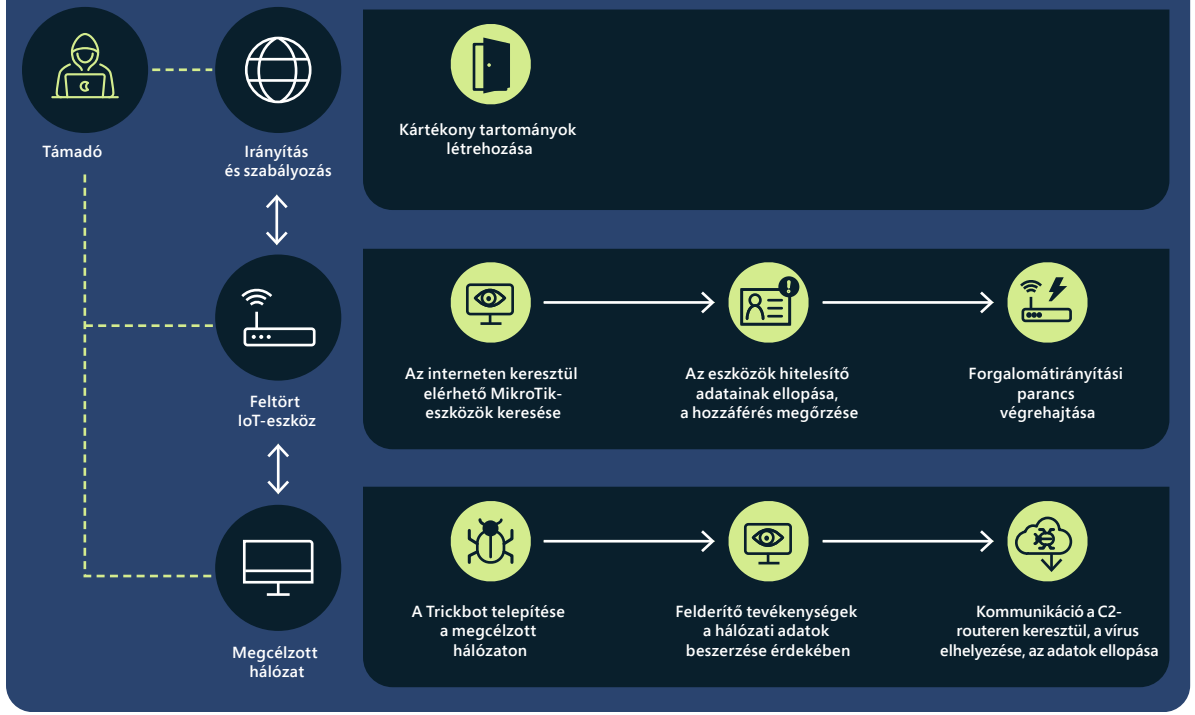
Pontosabban azt azonosítottuk, hogy a Trickbot operátorai hogyan használják a feltört MikroTik útválasztókat, és hogyan konfigurálják őket át úgy, hogy saját C2-infrastruktúrájuk részeként működjenek. Ezeknek az eszközöknek népszerűsége súlyosbítja a Trickbot által velük elkövetett visszaéléseket, egyedi hardverük és szoftverük pedig lehetővé teszi a támadók számára, hogy megkerüljék a hagyományos biztonsági intézkedéseket, és további eszközöket és hálózatot törjenek fel.

A kitett MikroTik útválasztók megoszlása világszerte

Az interneten nyilvánosan elérhetővé tett útválasztók ki vannak téve a potenciális sebezhetőségek kihasználásának.

Az SSH- (Secure Shell-) parancsokat tartalmazó forgalom nyomon követésével és elemzésével megfigyeltük, hogy a támadók MikroTik útválasztók használatával kommunikálnak a Trickbot infrastruktúrájával, miután megszerezték az eszközökhöz használható hitelesítő adatokat. Ezeket a hitelesítő adatokat megszerezhetik találgatásos támadásokkal, rendelkezésre álló javításokkal orvosolható ismert sebezhetőségek kihasználásával, valamint alapértelmezett jelszavak használatával. Amint hozzáfér egy eszközhöz,

A Trickbot támadási lánca



A Trickbot támadáslánca, amelyen látható a MikroTik IoT-eszközök C2-proxyszerverként való használata.

a támadó kiad egy olyan egyedi parancsot, amely átirányítja a forgalmat az útválasztó két portja között, így kommunikációs csatornát nyit a Trickbottal fertőzött eszközök és a C2 között.

A MikroTik eszközöket célzó különböző támadásokról (nem csupán a Trickbot vizsgálata során) szerzett ismereteinkre, valamint az ismert gyakori sebezhetőségekre és kitettségekre (CVE) alapozva készítettünk egy olyan nyílt forráskódú eszközt a MikroTik eszközökhöz, amely kinyeri az ezeket az eszközöket célzó támadásokhoz kapcsolódó bűnelemzési műtermékeket.[31]

Az eszközök fordított proxyként való felhasználása a kártevők irányításához nem korlátozódik a Trickbotra és a MikroTik útválasztókra. A Microsoft RiskIQ csapattal együttműködve visszakövettük az érintett C2-eszközöket, és az SSL-tanúsítványok vizsgálatával megállapítottuk, hogy az Ubiquiti és a LigoWave eszközök is érintettek.[32] Ez fontos jelzés arról, hogy az IoT-eszközök a nemzetállamok által koordinált támadások aktív összetevőivé és a kiterjedt botneteket használó kiberbűnözők kedvelt célpontjaivá váltak.

A kriptobűnözők visszaélnek az IoT-eszközökkel

Az átjáróeszközök egyre értékesebb célpontnak számítanak a támadók körében, mivel az ismert sebezhetőségek száma évről évre konzisztensen növekszik. Ezeket az eszközöket kriptovaluta-bányászathoz és más rosszindulatú tevékenységekhez használják.

Mivel a kriptovaluták egyre népszerűbbé váltak, sok magánszemély és szervezet fektetett be számítási teljesítményt és hálózati erőforrásokat útválasztókról és hasonló eszközökről, hogy a blokchainen kriptovalutát bányásszanak. A kriptovaluta-bányászat azonban idő- és erőforrás-igényes folyamat, amelynek sikerrátája alacsony. A sikeres érmebányászat esélyének növeléséhez a bányászok elosztott, együttműködő hálózatokba, „poolokba" tömörülnek, és annak alapján kapnak hasheket, hogy mennyi összekapcsolat erőforrással járultak hozzá a sikeres bányászathoz.

Az elmúlt évben a Microsoft egyre több olyan támadást figyelt meg, amely útválasztókat használt a kriptovaluta-bányászati erőfeszítések átirányítására. A kiberbűnözők feltörik a bányászok pooljaihoz csatlakoztatott útválasztókat, és átirányítják a bányászati forgalmat a hozzájuk tartozó IP-címekről DNS-mérgezéses támadásokkal, amelyek során megváltoztatják a megcélzott eszközök DNS-beállításait. Az érintett útválasztók nem megfelelő IP-címet regisztrálnak egy adott tartománynévhez, és a bányászati erőforrásokat – vagy hasheket – a támadók által használt poolokba küldik. Ezek a poolok anonim, bűnelkövetéshez használható érméket bányászhatnak, vagy a bányászok által használt valódi hashek használatával részesedést szerezhetnek az általuk bányászott érméből – más szóval ellopják a befektetésük eredményét.

A 2021-ben felfedezett sebezhetőségek több mint feléhez nem áll rendelkezésre javítás, így a vállalati és privát hálózatokon használt útválasztók frissítése és védelme továbbra is jelentős kihívást jelent az eszközök tulajdonosai és a rendszergazdák számára.

Eszközök feltörése illegális kriptobányászat céljából.

Az átjáróeszközök DNS-mérgezéses eltérítése során a jogszerű bányászati tevékenységeket támadják, és átirányítják az erőforrásokat az illegális bányászati tevékenységekhez.

A bűnözők infrastruktúrájaként használt virtuális gépek

A felhőbe költözés széles körű terjedésével a kiberbűnözők is lépést tartanak, és az adathalász támadások vagy hitelesítő adatokat lopó rosszindulatú szoftverek révén ellopott magáneszközöket az áldozatok tudta nélkül használják. Számos kiberbűnöző választja rosszindulatú infrastruktúrája alapjául a felhőalapú virtuális gépeket (VM-eket), konténereket és mikroszolgáltatásokat.

Miután a kiberbűnöző hozzáférést szerzett, események láncolata vezet az infrastruktúra beállításához – például egy sor virtuális gép szkripteken és automatizált folyamatokon keresztüli létrehozásához. Ezeket a szkriptelt, automatizált folyamatokat olyan rosszindulatú tevékenységek elindításához használják, mint a nagyszabású e-mailes spamtámadások, az adathalász támadások és a rosszindulatú tartalmakat tároló weboldalak létrehozása. Akár egy skálázott virtuális környezetet is beállíthatnak a kriptovaluta-bányászathoz, melynek eredményeképpen a gyanútlan áldozat több százezer dolláros számlát kap a hó végén.

A kiberbűnözők tisztában vannak vele, hogy rosszindulatú tevékenységük csak korlátozott ideig működhet, mielőtt felfedeznék és meghiúsítanák. Emiatt ők is szintet léptek, és már proaktívan tevékenykednek, felkészülve a problémákra. A megfigyelések szerint feltört fiókokat készítenek elő és figyelik a környezetüket. Amint az egyik (virtuális gépek százezreivel beállított) fiókot felfedezik, már lépnek is tovább a következőre – amelyet szkriptekkel már előre beállítottak azonnal aktiválhatóra –, és szinte megszakítás nélkül folytatják rosszindulatú tevékenységüket.

A felhőinfrastruktúrához hasonlóan a helyi infrastruktúra is felhasználható a támadásokhoz a helyi felhasználó számára észrevétlenül maradó virtuális helyi környezetekkel. Ehhez arra van szükség, hogy a kezdeti hozzáférési pont nyílt és hozzáférhető maradjon. A kiberbűnözők a helyi magáneszközökkel is visszaélnek, és a felhőinfrastruktúra létrehozását indítják el velük, elfedve a tevékenységek valódi forrását, hogy elkerüljék a gyanús infrastruktúra-létrehozás észlelését.

Gyakorlati tanácsok

1. Vezessen megfelelő kiberhigiéniai intézkedéseket, és biztosítson kiberbiztonsági képzést a munkatársak számára a pszichológiai manipuláció elkerüléséhez.
2. Rendszeresen keressen rendellenességeket a felhasználói tevékenységekben automatizált, nagy léptékű ellenőrzésekkel, hogy csökkentse az ilyen típusú támadások esélyét.
3. Frissítse és védje meg az útválasztókat a vállalati és magánhálózatokon.

Hacktivizmus – hosszú távon is számolnunk kell vele?

Bár a hacktivizmus nem új jelenség, az ukrajnai háború kezdete óta megugrott az önkéntes hackerek száma, és az olyan, kormányzati irányítás alatt álló műveletek is megszaporodtak, amelyek célja a politikai ellenfelek, szervezetek, sőt nemzetállamok hírnevének vagy eszközeinek rombolására hivatott kibereszközök terjesztése.

2022 februárjában az ukrán kormány felszólította a civil hackereket világszerte, hogy indítsanak kibertámadásokat Oroszország ellen egy a 300 000 fős „IT-hadsereg" részeként.[33] Ugyanekkor a már korábban is ismert hacktivistacsoportok, például az Anonymous, a Ghostsec, az Against the West, a Belarusian Cyber Partisans és a RaidForum2 is elkezdtek Ukrajnát támogató kibertámadásokat indítani. Más csoportok, köztük a Conti zsarolócsoport, Oroszország mellé álltak.[34]

Az ezt követő hónapokban az Anonymous tevékenysége nagyon látványos volt. A csoport – vagy társult csoportjai – nevében tevékenykedő hackerek egy időre elérhetetlenné tettek több ezer orosz és fehérorosz weboldalt, több száz gigabájtnyi lopott adatot tettek közzé, orosz tévécsatornákat törtek fel, hogy ukránbarát tartalmakat játsszanak le rajtuk, sőt Bitcoinban fizetett jutalmat ajánlottak a magukat megadó orosz harckocsik legénységének.

A civil hackerek felemelkedése

A közösségimédia-platformok lehetővé tették a gyors szervezést és több ezer civil hacker mozgósítását, akik egyszerűen végrehajtható támadásokhoz – például DDoS-támadásokhoz – kaptak utasításokat. A szervezők a Twittert, a Telegramot és a privát fórumokat használták a hackerek összegyűjtéséhez, a tevékenységek szervezéséhez, valamint a hackelési útmutatók terjesztéséhez.

Azonban ezeknek a hackereknek a többsége feltehetőleg csak korlátozott tudással rendelkezik – még az útmutatók ellenére is. Ez két potenciális jövőképet vetít előre: az egyik szerint alapszintű technikai képességekkel rendelkező emberek százai vagy ezrei fognak sablonok alapján összehangolt vagy egyéni hacktivistatámadásokat indítani a célpontok ellen, a másik forgatókönyv szerint, ha végül véget érnek a harcok Ukrajnában, ezek az emberek felhagynak a hacktivistatevékenységükkel – legalábbi addig, amíg egy újabb politikai vagy társadalmi ügy nem sarkallja őket újabb hackertámadásokra.

A hackerek átpolitizálódása

Ez a fajta politikai mozgósítás azért jelent nagyobb kockázatot, mert számos, a technológia iránt érdeklődő hackert aktivizál, akik folytathatják a külföldi kormányzati célok elleni kibertámadásokat a saját nemzeti prioritásaik mentén – akár önállóan, akár saját kormányuk utasítására.

Irán, Kína és Oroszország már jelenleg is felhasználja a hacktivizmust arra, hogy új tagokat toborozzon állami hackercsoportjaiba. Például a 2022 áprilisában az oroszbarát Killnet hackercsoport DDoS-támadásokat indított a cseh vasutak, regionális repülőterek és a cseh közigazgatás szerverei ellen, annak ellenére, hogy Csehország közvetlenül nem érintett a háborúban.[35] Ugyanakkor egyes kormányok a hacktivizmust használják álcának hagyományos kiberkémkedési vagy szabotázsműveleteikhez – ezt figyelhettük meg például az Izraelt támadó iráni hackerek esetében.

A hacktivizmushoz kapcsolódó DDoS-támadások számának növekedésével a technológiai ágazat jelentős kihívással találta szemben magát: gyorsan meg kell állapítani a webhelyekre irányuló forgalomról, hogy normális vagy rendellenes-e. A Microsoft és partnerei kifejlesztettek egy olyan eszközgyűjteményt, amely megkülönbözteti a rosszindulatú DDoS-forgalmat, és vissza tudja követni egészen a kiindulópontjáig. Ezenkívül a Microsoft Azure platform képes azonosítani a platformon lévő olyan gépeket, amelyek rendkívül nagy kimenő forgalmat generálnak, és le tudja állítani őket.

A protestware felemelkedése

A protestware szoftverek az Oroszország és Ukrajna között kitört háború által kiváltott érzelmi reakciók közvetlen leképeződései. Egyes nyílt forráskódú szoftverek fejlesztői arra használták szoftvereik népszerűségét, hogy szót emeljenek vagy konkrét lépéseket tegyenek a kibontakozó geopolitikai helyzet ellen. Ezek között az asztalon vagy a böngészőben megjelenített, békeüzeneteket tartalmazó ártalmatlan szövegfájlok éppúgy megtalálhatók voltak, mint az IP-geolokációs adatokon alapuló célzott támadások és az olyan káros tevékenységek, mint a merevlemezek teljes törlése. Más globális események kibontakozása esetén is számíthatunk rá, hogy a protestware-ek ismét felbukkannak. Mivel ezek általában olyan esetek, amikor egy nyílt forrású szoftver köztiszteletben álló karbantartója úgy dönt, hogy saját nyílt forrású szoftverösszetevőjét személyes üzenetek megjelenítésére használja, jelenleg nincs olyan védekezési megoldás, amely megakadályozhatná a forrásfájlcsomagok ilyen típusú módosítását, ezért a felhasználóknak kell figyelniük a potenciális következményekre.

> A közösségimédia-platformok lehetővé tették több ezer civil hacker mozgósítását és szervezését, akik egyszerűen végrehajtható támadásokhoz – például DDoS-támadásokhoz – kaptak utasításokat.

Gyakorlati tanácsok

1. A technológiai ágazatnak együtt kell működnie, hogy átfogó választ dolgozzon ki erre az új fenyegetésre.
2. A vezető technológiai vállalatoknak, többek között a Microsoftnak, olyan eszközökkel kell rendelkezniük, amelyekkel azonosítható a DDoS-támadásokhoz kapcsolódó rosszindulatú forgalom, és letilthatók az azt generáló gépeket.
3. A nyílt forráskódú szoftverek felhasználóinak fokozott figyelemmel kell eljárniuk a geopolitikai konfliktusok idején.

Végjegyzet

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. Végponti észlelés és reagálás. https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. Az ellenőrzött fórum olyan online vitafórum, amelyben a meglévő tagoknak kell kezeskedniük az újonnan felvett tagokért.
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. Adatforrás: Defender for Office (rosszindulatú e-mailek/sérült biztonságú identitásokkal kapcsolatos tevékenységek), Azure Active Directory Identity Protection (sérült biztonságú identitásokkal kapcsolatos események/riasztások), Defender for Cloud Apps (sérült biztonságú identitásokkal kapcsolatos adathozzáférési események) és M365D (termékek közötti korreláció).
17. Adatforrás: Defender for Endpoint (támadási viselkedéssel kapcsolatos riasztások/események), Defender for Office (rosszindulatú e-mailek) és M365D (termékek közötti korreláció).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Tartományalapú üzenethitelesítés, jelentéskészítés és megfelelőség: E-mail-hitelesítési, szabályzat- és jelentési protokoll, amelyet úgy terveztek, hogy segítségével az e-mail-tartományok tulajdonosai megvédhessék a tartományukat a jogosulatlan felhasználástól.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10cv156 (E.D.Va. 2010. feb. 22.)
27. Lásd: Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 2011. szept. 27.
28. Pontosabban a Szövetségi Polgári Perrendtartás 65-ös szabálya teszi lehetővé, hogy egy fél ilyen jogorvoslatot kérjen, ha: 1) a fél azonnali és helyrehozhatatlan kárt szenvedne el, ha a mentességet nem biztosítanák, és 2) a fél időben megpróbálja átadni a másik félnek az értesítést. Ezenfelül a törvény megköveteli az egyensúlyvizsgálat alkalmazását is, amely kiegyensúlyozza az alperes tájékoztatáshoz való jogát és a közérdek elleni sérelem mértékét.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 2011. feb. 9.)
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 2021. aug. 12.).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Kiberhadviselés

A nemzetállami szereplők egyre kifinomultabb kibertámadásokat indítanak, hogy elkerüljék a lelepleződést, és támogassák stratégiai prioritásaikat.

Áttekintés

a nemzetállamok általi fenyegetésekről

A nemzetállami szereplők egyre kifinomultabb kibertámadásokat indítanak, hogy elkerüljék a lelepleződést, és támogassák stratégiai prioritásaikat. Az Ukrajnában zajló hibrid háborúban bevetett kiberfegyverek már a konfliktus új korszakának elérkeztét jelzik.

Oroszország is támogatta saját háborús erőfeszítéseit olyan információs befolyásolásszerzési műveletekkel, amelyek során propagandán keresztül igyekezett hatást gyakorolni az Oroszországban, Ukrajnában és világszerte kialakuló véleményekre. Ebből az első teljes körű hibrid konfliktusból más fontos tanulságokat is levonhattunk. Először is, a digitális műveletek és adatok védelme leginkább a felhőbe költözéssel biztosítható – igaz ez a kibertérben éppúgy, mint a fizikai térben. A kezdeti orosz támadások során helyi szolgáltatásokat céloztak adattörlő rosszindulatú szoftverekkel, az egyik elsőként kilőtt rakéta pedig egy adatközpontot vett célba.

Ukrajna gyorsan reagált, és a workloadokat hiperskálázható, Ukrajnán kívül üzemeltetett hiperskálázható felhőkbe helyezte át. A második tanulság, hogy az adatokon és fejlett AI- és ML-szolgáltatásokon alapuló és a felhőben futó kiberfenyegetés-észlelési és végpontvédelmi megoldások segítettek Ukrajnának védekezni az orosz kibertámadások ellen.

Máshol a nemzetállami szereplők fokozták aktivitásukat, és az automatizálás, a felhőinfrastruktúra, valamint a távoli hozzáférési technológiák fejlődését kihasználva szélesebb célcsoportok támadását indították meg. Gyakran a tényleges cél elérését megkönnyítő vállalati IT-ellátási láncokat is támadások érik. A támadók könyörtelenül kihasználják a be nem foltozott biztonsági réseket, a kifinomult és a nyers erőre épülő módszerektől sem riadnak vissza, és sokszor nyílt forráskódú, akár legitim szoftverekkel fedik el a tevékenységüket – a kiberbiztonsági higiénia ezért ma fontosabb, mint valaha. Ezenkívül Irán csatlakozott Oroszországhoz a pusztító kiberfegyverek, köztük a legfontosabb eszköznek számító rosszindulatú szoftverek használatában.

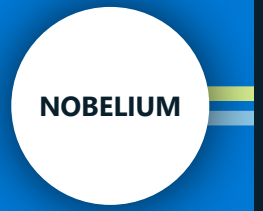
E fejlemények is jelzik, mennyire sürgős volna elfogadni egy átfogó, globális keretrendszert, amely az emberi jogokat helyezi előtérbe, és védelmet nyújt a felelőtlen állami cselekmények veszélyeivel szemben. Minden országnak együtt kell működnie az egyeztetett normák és a felelősségteljes állami magatartásra vonatkozó szabályok alkalmazása terén.

Defending Ukraine: Early Lessons from the Cyber War — Microsoft On the Issues

A létfontosságú infrastruktúra – különösen az informatikai szektor, a pénzügyi szolgáltatások, atömegközlekedési rendszerek és a kommunikációs infrastruktúra – egyre nagyobb arányban válik a kibertámadások célpontjává.

Tudjon meg többet a 35. oldalon

Az informatikai ellátási láncot átjáróként használják a célpontokhoz való hozzáféréshez.



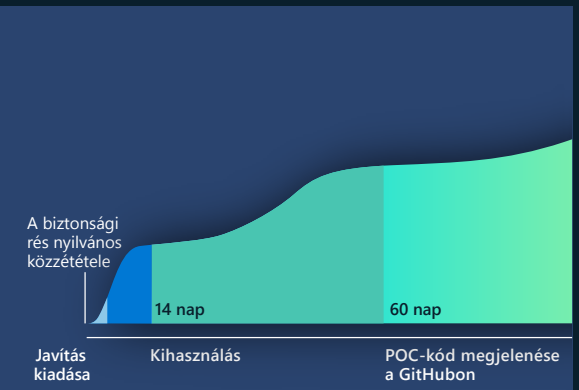
Tudjon meg többet a 36. oldalon

Kína a globálisan szélesíti célpontjai körét, különösen a kisebb délkelet-ázsiai országokban próbál információkhoz és versenyelőnyhöz jutni.

További információt a 44. oldalon talál

Irán egyre agresszívabbá vált a hatalmi átmenetet követően, és a regionális ellenfelein túl egyesült államokbeli és európai áldozatokat is megcélzott zsarolóprogramos támadásaival, sőt az Egyesült Államok kulcsfontosságú infrastruktúrájának legnagyobb szereplőit sem kímélte.

Tudjon meg többet a 46. oldalon



Tudjon meg többet a 39. oldalon

Észak-Korea védelmi és repülőipari vállalatokat, kriptodevizákat, hírügynökségeket, disszidenseket és segélyszervezeteket vett célba, hogy elérje a rezsim céljait: a védekezési képességek fokozását, a gazdaság erősítését és a belföldi stabilitás biztosítását.

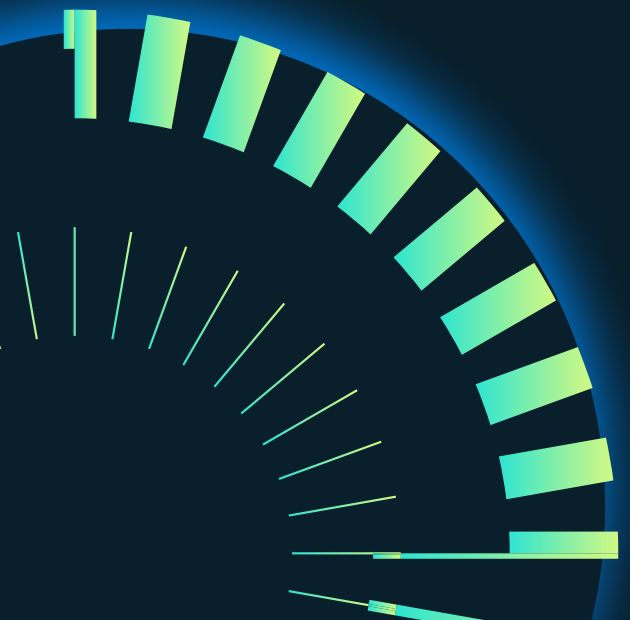
Tudjon meg többet a 49. oldalon

A kiberzsoldosok veszélyeztetik a kibertér stabilitását, mivel a szektor egyre szaporodó magánvállalatai fejlett eszközöket, technikákat és szolgáltatásokat fejlesztenek ki és értékesítenek, amelyekkel az ügyfeleik (gyakran kormányok) hálózatokra és eszközökre törhetnek be.

További információt az 52. oldalon talál

Bevezető

A 2020-as és 2021-es nagy horderejű támadások után a nemzetállami támadók jelentős erőforrásokat fordítottak a vállalatok által a kifinomult fenyegetések elleni védekezés érdekében bevezetett új biztonsági intézkedések kijátszására.



Akárcsak a nagyvállalatok, a támadók is elkezdték alkalmazni az automatizálás, a felhő-infrastruktúra és a távoli hozzáférési technológiák terén történt előrelépéseket, hogy bővítsék áldozataik körét. Ezek a taktikaváltások új megközelítéseket és a vállalati ellátási láncok elleni nagy volumenű támadásokat hoztak. Az IT-biztonsági higiénia még fontosabbá vált, mivel a támadók új módszereket fejlesztettek ki a javítás nélkül hagyott sebezhetőségek kiaknázására, kibővítették a vállalati hálózatok feltörésére használt módszerek palettáját, és a nyílt forráskódú vagy legitim szoftverek segítségével fedték el a működésüket. Az új támadási módszerek új és nehezebben felfedezhető vektorokat biztosítottak a célpont hálózatához való hozzáféréshez. Végül pedig – a fizikai háborús támadások eszkalálódásával – azt is láthattuk, hogy a kibertámadások kiemelkedő szerepet kaptak a katonai műveletekben is.

Az ukrajnai konfliktus megrendítő példát szolgáltatott arra, hogy a kibertámadások hogyan fejlődnek, és a fizikai katonai konfliktusokkal párhuzamosan hogyan befolyásolják egyre nagyobb mértékben a világot. Az energiaellátási és telekommunikációs rendszerek, a média és más létfontosságú infrastruktúrák a fizikai támadások mellett a kibertámadások célpontjaivá is váltak. Az általában a kémkedés és az információkiszivárogtatási műveletek részeként elkövetett hálózatfeltörési kísérletek fókuszálttá váltak a kritikus infrastruktúrát célzó, pusztító adattörlő rosszindulatú szoftverek elleni hibrid háborúban. Ezeknek a rendszereknek a biztonságát a felhőhöz kapcsolva lehetővé vált a betörések korai észlelése és a potenciálisan pusztító hatású támadások letörése.[1]

Ez volt az első alkalom, hogy egy jelentős kibertámadás során a gépi tanulást alkalmazó viselkedési észlelőrendszerek az ismert támadási minták alapján azonosították és megakadályozták a további támadásokat az alapul szolgáló rosszindulatú szoftverről szerzett korábbi ismeretek nélkül – ráadásul mindezt azelőtt, hogy az emberi operátorok tudomást szereztek volna a fenyegetésekről. Emellett arról is meggyőződhettünk, mennyire fontos a fenyegetésfelderítési adatok valós idejű megosztása a rendszerek védőivel, akik így létfontosságú információkhoz jutottak az aktív támadások elhárításához és az ellenük való védekezéshez.

Az állami támadók régi és új módszerekkel világszerte szélesítik tevékenységeik körét. Kína, Észak-Korea, Irán és Oroszország egyaránt támadásokat hajtott végre a Microsoft-ügyfelekkel szemben. Az informatikai szolgáltatások ellátási lánca általános célponttá vált, mivel a támadók most már olyan szolgáltatásokra összpontosítják erőfeszítéseiket, amelyeken keresztül több vállalathoz is bejuthatnak. Várakozásaink szerint ezek a támadók továbbra is igyekezni fognak kihasználni a vállalati ellátási láncok bizalmon alapuló kapcsolatait, ami kiemeli a hitelesítési szabályok érvényre juttatásának, a javítások gondos telepítésének, a távoli hozzáférési infrastruktúrához végzett fiókkonfigurációnak és a partneri kapcsolatok megbízhatóságát vizsgáló gyakori auditoknak az átfogó fontosságát.

Az állami szereplők – a zsarolószoftverek üzemeltetőihez és más kiberbűnözőkhöz hasonlóan – úgy reagáltak a nagyobb kitettségre, hogy egyre inkább a rosszul konfigurált vagy javítatlanul hagyott vállalati rendszereket (VPN-/VPS-infrastruktúrát, helyi szervereket, külső szállítótól származó szoftvereket) veszik célba az ott talált eszközöket felhasználó (LoTL) támadásaik során. Sok támadó a rosszindulatú tevékenysége elfedése érdekében egyre nagyobb mértékben támaszkodik a készen megvásárolható rosszindulatú szoftverekre és a nyílt forrású támadásszimulációs eszközökre.

Ennek eredményeképpen az informatikai biztonsági higiénia terén stabil alapokat kell teremteni a javítástelepítés előnyben részesítése, a manipulációellenes funkciók engedélyezése, valamint a támadási felületek menedzselésére szolgáló eszközök, például a RiskIQ használata révén, amelyek külső nézetből mutatják meg a támadási felületeket. Ezenkívül az egész vállalatnál a biztonság alapkövévé kell emelni a többfaktoros hitelesítést, amellyel proaktívan lehet védekezni számos, kifinomult taktikákat alkalmazó támadó ellen.

A nemzetállami szereplők is egyre nagyobb mértékben használják a zsarolóprogramokat a támadásaik során, gyakran újrahasznosítva a bűnözői ökoszisztémában létrehozott zsaroló rosszindulatú szoftvereket. Iráni és észak-koreai szereplők esetében is láthattuk, hogy készen kapható zsarolóeszközöket használtak a megcélzott – gyakran a kritikus infrastruktúra részét képező – rendszereken való károkozásra a regionális riválisoknál. Végül azt i láthattuk, hogy a kiberzsoldosok egyre nagyobb fenyegetést jelentenek, mivel olyan eszközöket, technológiákat és szolgáltatásokat fejlesztenek ki és értékesítenek, amelyekkel nagyobb léptékben használhatók ki a külső féltől származó sebezhető megoldások. A nemzetállami szereplők által elkövetett támadások évről évre kifinomultabbak és agilisabbak lesznek. A vállalatok erre reagálva tájékozódniuk kell ezeknek a szereplőknek a fejlődéséről, és ezzel párhuzamosan fejleszteniük kell védelmi rendszereiket is.

John Lambert
a Microsoft veszélyfelderítő központjának kiemelt mérnöke és vállalati alelnöke

Nemzetállami adatok háttere

A nemzetállami fenyegetések olyan, kiberfenyegetést jelentő tevékenységek, amelyek egy adott országból indulnak, és nyilvánvalóan az adott ország érdekeinek érvényesítését célozzák. A nemzetállami szereplők jelentik az egyik legfejlettebb és folyamatosan fennálló fenyegetést az ügyfelekre – tevékenységeik között szerepel a szellemi tulajdon ellopása, a kémkedés, a megfigyelés, a hitelesítő adatok ellopása, a pusztító támadások és egyebek.

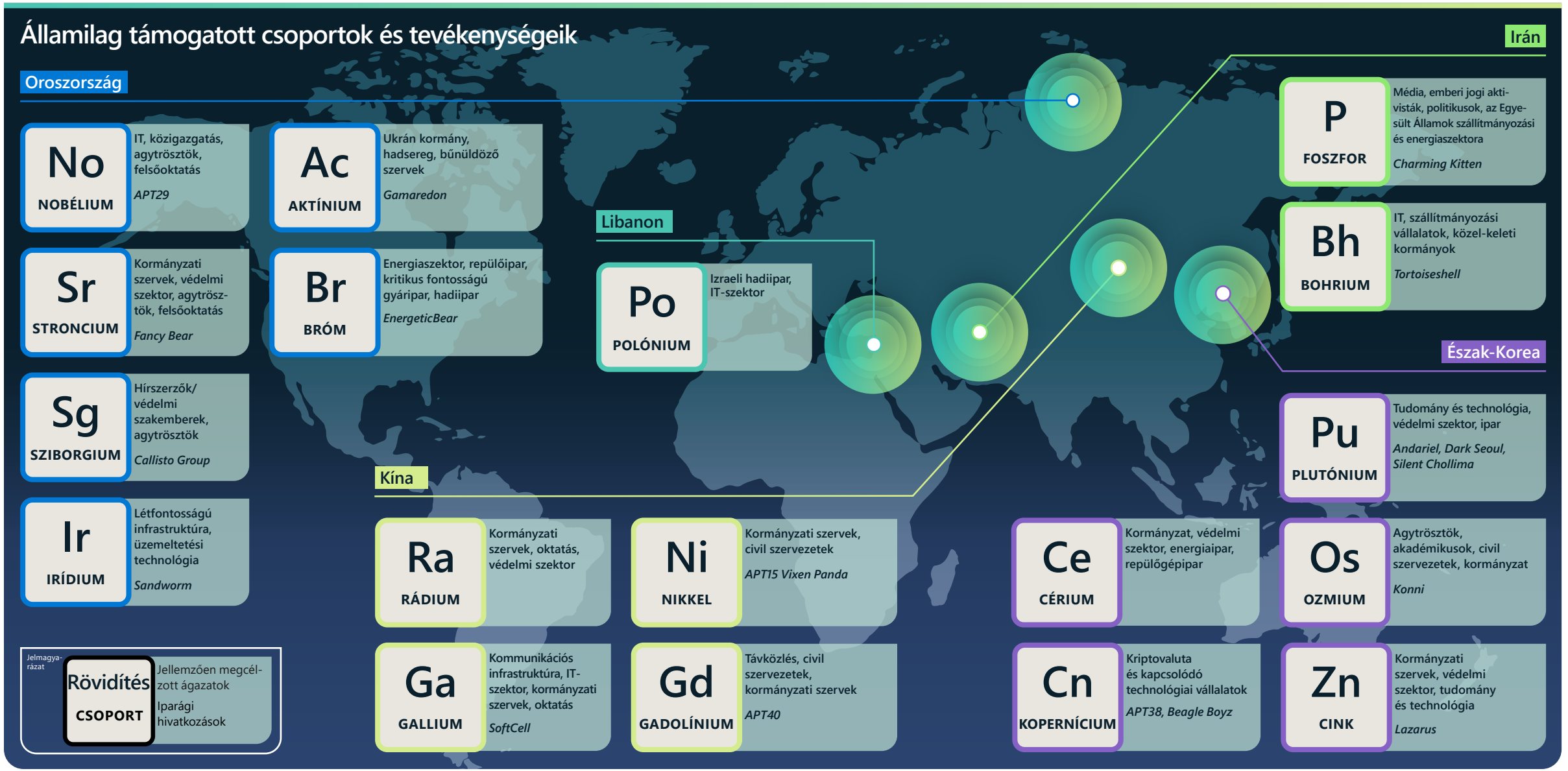
Jelentős erőforrásokat fordítunk az ilyen típusú fenyegetések felderítésére, megismerésére és elhárítására. Amikor egy vállalati vagy magánszemély fióktulajdonos a megfigyelt nemzetállami tevékenységek célkeresztjébe kerül vagy áldozatává válik, a Microsoft értesíti az ügyfelet egy állami csoportok támadásával kapcsolatos figyelmeztetésben, amelyhez az adott tevékenység kivizsgálását segítő információkat is mellékel. A funkció 2018-as bevezetésétől 2022. júniusáig több mint 67 000 ilyen figyelmeztetést küldtünk.

A Microsoft állami támadókkal kapcsolatos adatait azért szerepeltetjük ebben a fejezetben, hogy képet adjunk erről a mérhetőn tevékenységről. A grafikonokon látható nemzetállami tevékenységek szintjének alapjául a Microsoft által az ügyfeleknek küldött, nemzetállami támadással kapcsolatos figyelmeztetések szolgálnak, amelyeket az ügyfél szervezetén belül legalább egy fiók megtámadása vagy feltörése nyomán adtunk ki.

A jelentésben szereplő, veszélyt jelentő nemzetállamok közül Oroszország, Kína, Irán és Észak-Korea a négy legfontosabb. Ezek az elmúlt évben a Microsoft-ügyfeleket célzó leggyakrabban megfigyelt támadók származási országai. A jelentésben a libanoni és a kiberzsoldosok – azaz felbérelhető, privát szektorbeli támadók – megbízásából dolgozó bűnözői csoportokkal kapcsolatos megfigyeléseinket is olvashatja.

A Microsoft a nemzetállami csoportokat kémiai elemek (például NOBÉLIUM) után nevezi el – ezek közül néhány látható a következő oldalon is. Az ismeretlen, feltörekvő vagy fejlődő fenyegetések klaszterei a DEV-#### jelölést kapják, ami lehetővé teszi számunkra, hogy egyedi információhalmazként kezeljük őket, amíg megbízhatóan meg nem tudjuk állapítani az adott tevékenység mögött álló szereplő származását vagy kilétét.

Miután megfelel a kritériumoknak, a DEV nevet kap, vagy összevonjuk egy meglévő szereplővel. Ebben a fejezetben a nemzetállami és DEV-csoportokat hozunk példaként ahhoz, hogy részletesebben bemutassuk a támadások célpontjait, technikáit és motivációinak elemzését. Bár a csoportok többsége ugyanazokat az eszközöket használja, mint a kiberbűnözők, egyedi fenyegetést jelentenek a személyre szabott kártevők alkalmazása, a nulladik napi sebezhetőségek felfedezésének és kihasználásának képessége és a jogi következmények hiánya miatt.


Államilag támogatott csoportok és tevékenységeik
Oroszország
No
NOBÉLIUM
IT, közigazgatás, agytrösztök, felsőoktatás
APT29
Ac
AKTÍNIUM
Ukrán kormány, hadsereg, bűnüldöző szervek
Gamaredon
Sr
STRONCIUM
Kormányzati szervek, védelmi szektor, agytrösztök, felsőoktatás
Fancy Bear
Br
BRÓM
Energiaszektor, repülőipar, kritikus fontosságú gyáripar, hadiipar
EnergeticBear
Sg
SZIBORGIUM
Hírszerzők/ védelmi szakemberek, agytrösztök
Callisto Group
Ir
IRÍDIUM
Létfontosságú infrastruktúra, üzemeltetési technológia
Sandworm
Jelmagyarázat
Rövidítés
CSOPORT
Jellemzően megcélzott ágazatok
Iparági hivatkozások
Libanon
Po
POLÓNIUM
Izraeli hadiipar, IT-szektor
Kína
Ra
RÁDIUM
Kormányzati szervek, oktatás, védelmi szektor
Ni
NIKKEL
Kormányzati szervek, civil szervezetek
APT15 Vixen Panda
Ga
GALLIUM
Kommunikációs infrastruktúra, IT-szektor, kormányzati szervek, oktatás
SoftCell
Gd
GADOLÍNIUM
Távközlés, civil szervezetek, kormányzati szervek
APT40
Irán
P
FOSZFOR
Média, emberi jogi aktivisták, politikusok, az Egyesült Államok szállítmányozási és energiaszektora
Charming Kitten
Bh
BOHRIUM
IT, szállítmányozási vállalatok, közel-keleti kormányok
Tortoiseshell
Észak-Korea
Pu
PLUTÓNIUM
Tudomány és technológia, védelmi szektor, ipar
Andariel, Dark Seoul, Silent Chollima
Ce
CÉRIUM
Kormányzat, védelmi szektor, energiaipar, repülőgépipar
Os
OZMIUM
Agytrösztök, akadémikusok, civil szervezetek, kormányzat
Konni
Cn
KOPERNÍCIUM
Kriptovaluta és kapcsolódó technológiai vállalatok
APT38, Beagle Boyz
Zn
CINK
Kormányzati szervek, védelmi szektor, tudomány és technológia
Lazarus

Változások a fenyegetések világában

A Microsoft küldetése az ügyfelei védelme, és ennek keretében nyomon követi az állami szereplők tevékenységét, és értesíti azokat az ügyfeleit, akik az ilyen támadók célkeresztjébe kerültek vagy áldozatául estek.

Ez az értesítés fontos része az iránti elkötelezettségünknek, hogy informáljuk az ügyfeleket, hogy a megfigyelt támadásokat sikeresen kivédték-e termékeink védelmi mechanizmusai, vagy a támadások sikerrel jártak valamilyen ismeretlen biztonsági gyengeség miatt. Az értesítéseket időben nyomon követve a Microsoft azonosítani tudja a támadók körében feltörekvő fenyegetési trendeket, és a termékekbe épített olyan védelmi mechanizmusok kifejlesztésére tud összpontosítani, amelyek proaktívan mérséklik az ügyfelekre leselkedő fenyegetéseket felhőszolgálatásainkban.

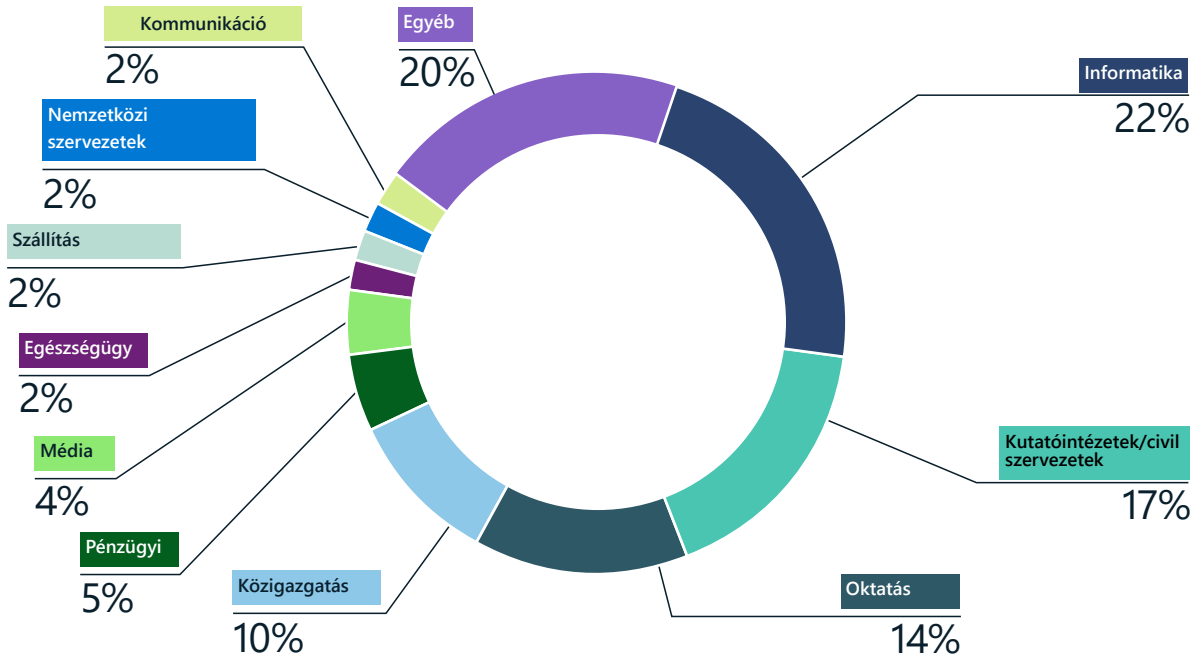
Ez a követés azt is lehetővé teszi számunkra, hogy adatokat és statisztikákat osszunk meg az általunk megfigyelt folyamatokról. Az ezeket a szereplőket és támadásaikat nyomon követő elemzők a technikai indikátorok és a geopolitikai szakértelem kombinációjára támaszkodnak a szereplők motivációinak megértésében, és a technikai és a globális összefüggéseket ötvözve új ismeretekhez jutnak. Ez az adatválogatás egyedülálló képet ad a nemzetiállami hátterű kibertámadók prioritásairól, és arról, hogy a motivációik hogyan tükrözhetik az őket alkalmazó nemzetállamok politikai, katonai és gazdasági érdekeit.

Az elmúlt év politikai fejleményei világszerte meghatározták az államilag finanszírozott támadócsoportok prioritásait és kockázattűrését. A geopolitikai kapcsolatok degradálódásával és az erőszakos elemek egyes országokban történt befolyásszerzésével a kibertámadók is merészebbé és agresszívabbá váltak. Például:

- Oroszország könyörtelenül támadta az ukrán kormányzati szerveket és az ország létfontosságú infrastruktúráját, kiegészítve a szárazföldi katonai inváziójával.[2]
- Irán agresszív támadásokat indított az Egyesült Államok infrastruktúrájának olyan létfontosságú elemei ellen, mint a kikötői hatóságok.
- Észak-Korea folytatta műveleteit, amelyek során kriptovalutát lop a pénzügyi és technológiai cégektől.
- Kína kiterjesztette globális kiberkémkedési tevékenységét.

Bár a nemzetállami szereplők technikailag kifinomult módszereket és sokféle taktikát alkalmaznak, támadásaik sokszor kivédhetők a megfelelő kiberhigiéniai gyakorlatokkal. Számos ilyen szereplő viszonylag egyszerű technológiákat alkalmaz, például célzott adathalász e-mailekben próbálja célba juttatni a fejlett rosszindulatú szoftvereket ahelyett, hogy személyre szabná a támadásokat, vagy célzott pszichológiai befolyásolással próbálná meg elérni a céljait.

A nemzetállami szereplők által megcélzott iparágak



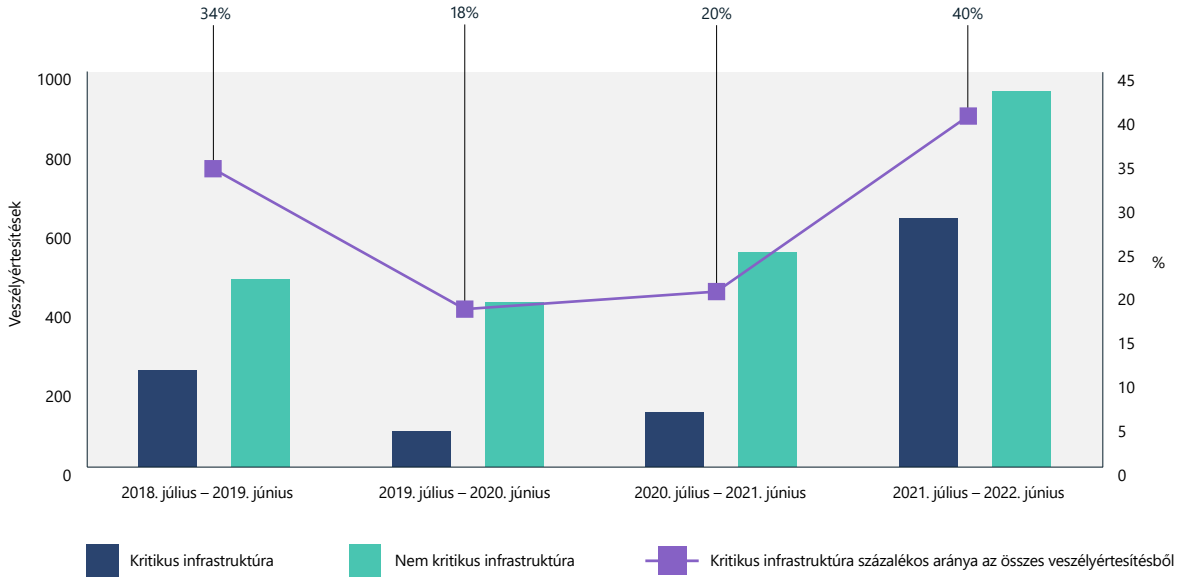
Az állami csoportok számos szektort céloznak. Az orosz és iráni állami szereplők az IT-ágazatot vették célba, hogy hozzáférhessenek az IT-cégek ügyfeleihez. Az agytrösztök, a civil szervezetek, az egyetemek és a kormányzati szervek maradtak a nemzetállami szereplők további gyakori célpontjai.

A nemzetállami szereplők különböző célokat próbálnak elérni, ami azt eredményezheti, hogy szervezetek vagy magánszemélyek adott csoportját célozzák meg. Az elmúlt évben az ellátási láncot érintő támadások egyre nagyobb teret nyertek, és különösen az IT-cégekre összpontosítottak. Az informatikai szolgáltatók feltörésével a támadók gyakran egy bizalomra épülő kapcsolaton keresztül, az összekapcsolt rendszereket üzemeltető cégen át tudják elérni az eredeti célpontjukat, esetleg sokkal nagyobb léptékű támadásokat hajthat végre azáltal, hogy egyetlen támadás során több száz ügyfél rendszerébe jutnak be. Az IT-szektor után leggyakrabban megcélzott szervezetek az agytrösztök, az egyetemekhez kapcsolódó akadémikusok és a kormányzati tisztviselők voltak. Ezek kívánatos „könnyű célpontokat" jelentenek a kémek számára, ahonnan geopolitikai kérdésekkel kapcsolatos információkat szerezhetnek.

Változások a fenyegetések világában

Folytatás

Kritikus infrastruktúrákat érintő trendek

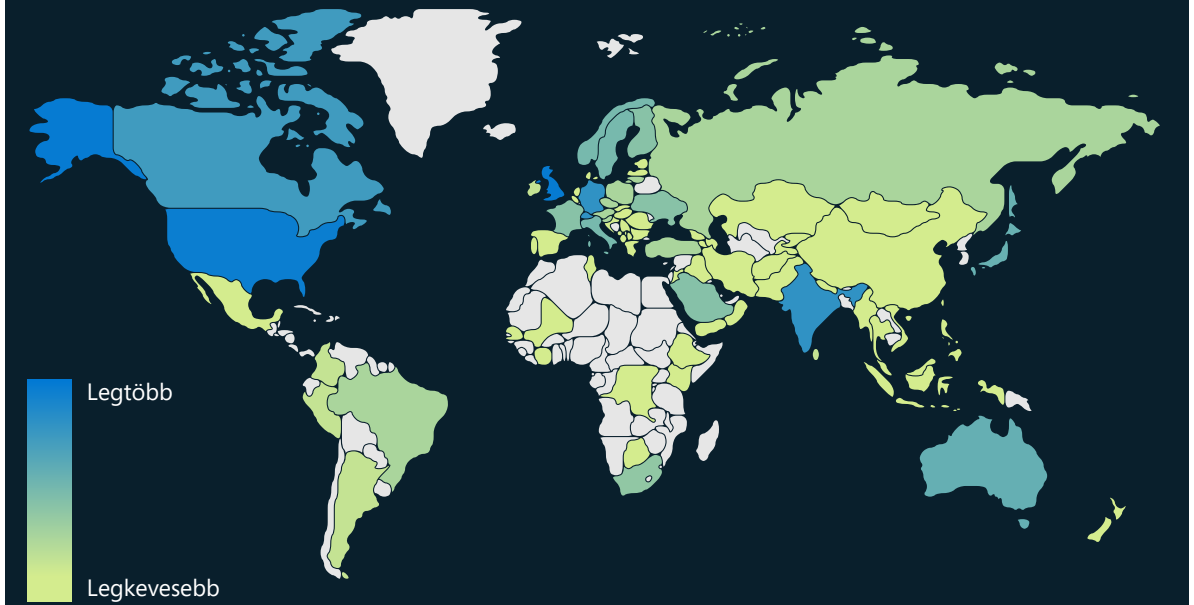


Az elmúlt évben egyre nagyobb mértékben vált a nemzetállami szereplők célpontjává a létfontosságú infrastruktúra[3], és a támadók elsősorban az IT-szektor, a pénzügyi szolgáltatások, a tömegközlekedési rendszerek és a kommunikációs infrastruktúra vállalataira koncentrálnak.

„Az Ukrajna elleni inváziót megelőzően a kormányok úgy gondolták, hogy az adatok csak akkor lehetnek biztonságban, ha az országhatáron belül maradnak. Az invázió tanulságainak levonása után az adatok felhőbe költöztetése és a területi határokon kívüli tárolása ma már a rugalmassági tervezés és a felelősségteljes adatgazdálkodás bevált gyakorlatai."

Cristin Flynn Goodwin,
Általános jogtanácsos munkatárs, Ügyfélbiztonság és -bizalom

A nemzetállami szereplők földrajzi célzása



A nemzetállami csoportok kibertámadásai az elmúlt évben az egész világra kiterjedtek, de különösen nagy hangsúlyt kaptak az egyesült államokbeli és brit vállalatok. Az állami támadásokkal kapcsolatos figyelmeztetéseink adatai alapján az Izraelben, az Egyesült Arab Emírségekben, Kanadában, Németországban, Indiában, Svájcban és Japánban működő cégek is a gyakori célpontok között voltak.

Gyakorlati tanácsok

1. Azonosítsa és védje meg a potenciálisan értékes adatcélpontokat, a kockázatoknak kitett technológiákat, valamint az egyéb olyan információkat és üzleti tevékenységeket, amelyek fontosak lehetnek a nemzetállami csoportok stratégiai prioritásai szempontjából.
2. Engedélyezze a felhővédelmi funkciókat, amelyek nagy léptékben azonosíthatják és mérsékelhetik a hálózatára leselkedő ismert és új fenyegetéseket.

Az informatikai ellátási lánc mint a digitális ökoszisztéma kapuja

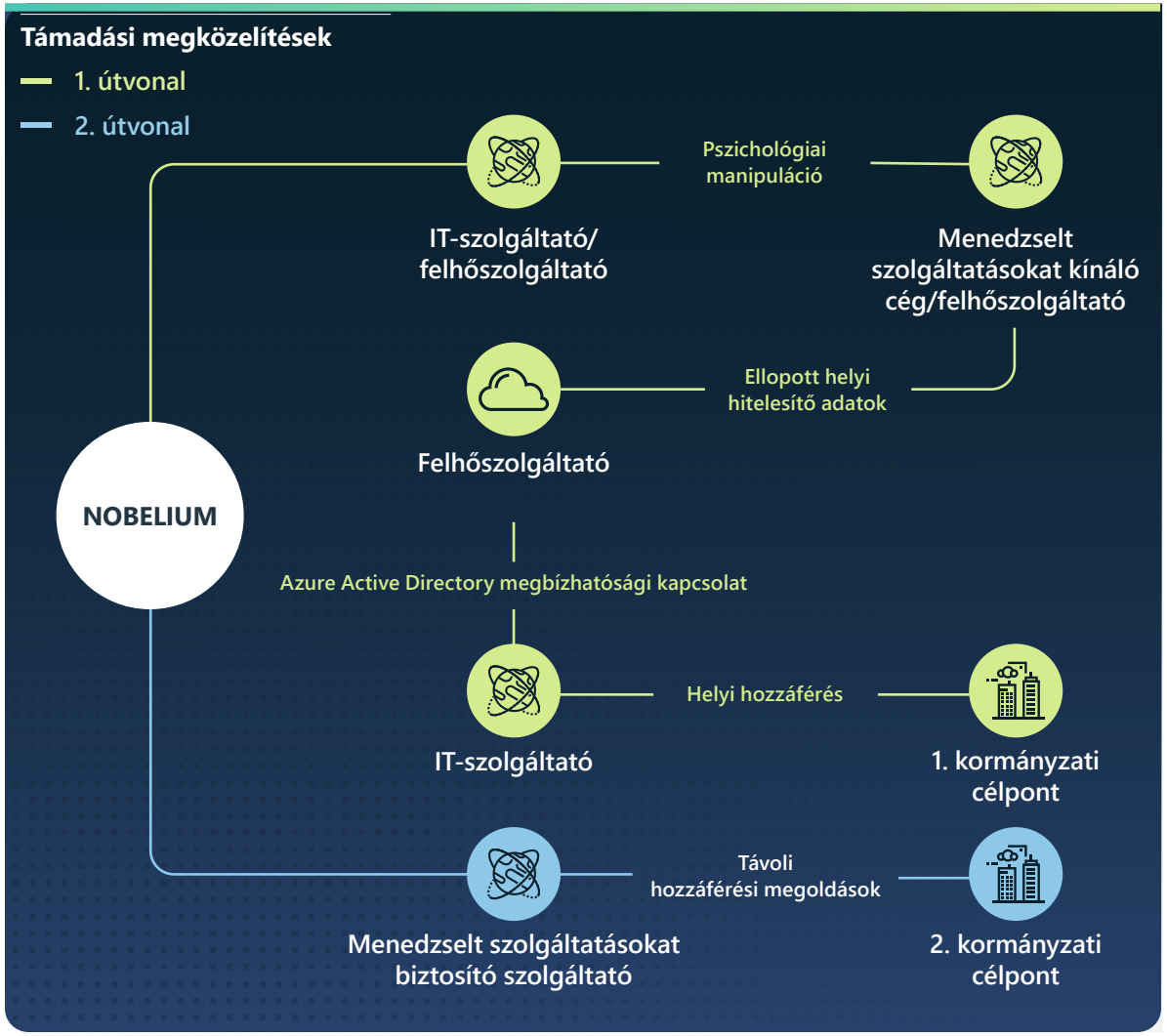
Az informatikai szolgáltatók nemzetállamok általi megcélzása lehetővé teheti a támadók számára, hogy megtámadjanak más, számukra fontos szervezeteket is, kihasználva az ellátási láncbeli szolgáltató iránti bizalmat és a számára biztosított hozzáférést. Az elmúlt évben a nemzetállami támadócsoportok IT-szolgáltatókat támadtak meg azért, hogy harmadik fél célpontok rendszereibe hatolhassanak be, és hozzáférjenek a szolgáltatók ügyfelei között szereplő, kormányzati, politikai és a kritikus infrastruktúrához tartozó szektorokban tevékenykedő szervezetek rendszereihez.

Az informatikai szolgáltatók vonzó köztes célpontnak számítanak, mivel több száz közvetlen és több ezer közvetett, a külföldi hírszerző szolgálatok számára fontos ügyfelet szolgálnak ki. Ha sikerül őket feltörni, az ezek által a cégek által alkalmazott megszokott üzleti gyakorlat és a számukra delegált adminisztratív jogosultságok kihasználása révén a rosszindulatú szereplők hozzáférhetnek az IT-szolgáltató ügyfeleinek hálózataihoz anélkül, hogy azonnal riasztásokat váltanának ki.

Az elmúlt évben a NOBÉLIUM megpróbálta feltörni és kihasználni felhőmegoldások és más menedzselt szolgáltatásokat biztosító szolgáltatók kiemelt jogosultságú fiókjait, hogy így kíséreljen meg hozzáférést szerezni ezeknek a szolgáltatóknak az egyesült államokbeli és európai kormányzati és politikai ügyfeleihez.

A NOBÉLIUM bizonyította, hogyan fordítható az „sok ellen egyen keresztül” megközelítés a vélt geopolitikai ellenfél ellen. Az elmúlt évben ez a támadó a külső felek megcélzása mellett közvetlenül is megpróbált behatolni a NATO-tagállamok fontos szervezeteihez, amelyet az orosz kormány a létét fenyegető veszélynek tekint. 2021 júliusa és 2022 június eleje között a Microsoft által az orosz fenyegetésekkel kapcsolatban kiküldött figyelmeztetések 48 százalékát a NATO-tagállamokban tevékenykedő online szolgáltató ügyfelek kapták, amelyeket nagy valószínűséggel köztes hozzáférési pontként akartak használni. Összességében az ugyanezen időszak alatt az orosz fenyegetéssel kapcsolatos figyelmeztetések 90 százalékát NATO-tagállamokban működő ügyfelek kapták, elsősorban az informatikai szektor cégei, agytrösztök és civil szervezetek, valamint az állami szektor szereplői, ami arra utal, hogy többféleképpen is megpróbáltak hozzáférést szerezni ezeknek a célpontoknak a rendszereihez.

Ez elmozdulást jelent a korábbi stratégiához képest, amikor a szoftverellátási lánc tagjait próbálták feltörni – helyettük most már az informatikai ellátási lánc tagjai, a felhőmegoldásokat és a menedzselt szolgáltatásokat biztosító cégek kerültek a célkeresztbe annak reményében, hogy rajtuk keresztül hozzáférést lehet szerezni az ügyfeleikhez.



Ez az ábra a NOBÉLIUM többvektoros megközelítését ábrázolja, amit a végső célpontjai ellen alkalmaz, és amellyel az egyéb áldozatoknak is járulékos károkat okoz. A fent bemutatott módszerek mellett a NOBÉLIUM szórásos jelszófeltörési és adathalász támadásokat is indított az érintett szervezetekkel szemben, sőt legalább egy kormányzati dolgozó személyes fiókját is célba vette, ami egy újabb potenciális behatolási útvonalat jelez.

Az informatikai ellátási lánc mint a digitális ökoszisztéma kapuja

Folytatás

Az idei év során a Microsoft Threat Intelligence Center (MSTIC) egyre több iráni állami és Iránnal kapcsolatban álló támadót észlelt, amelyek IT-cégekhez törtek be. Sok esetben azt észleltük, hogy ezek a támadók bejelentkezési adatokat loptak el, hogy hozzáférjenek a cégek ügyfeleihez különböző célok megvalósításához, amelyek a hírszerzéstől a destruktív megtorló támadásokig terjedtek.

- 2021. júliusában és augusztusában, a DEV-0228 egy izraeli üzleti szoftverszolgáltatót tört fel, hogy később behatolhasson annak ügyfeleihez, amelyek az izraeli védelmi, energia- és jogi szektorban tevékenykednek.[4]
- 2021 augusztus és szeptember között a Microsoft kiugróan sok iráni állami támadást regisztrált indiai informatikai cégek ellen. A változást indokló geopolitikai konfliktusok hiányában, ezt valószínűleg az indokolta, hogy a támadók a cégek Indián kívüli leányvállalataihoz és ügyfeleihez akartak hozzáférést szerezni.
- 2022 januárjában a DEV-0198 nevű, vizsgálataink szerint az iráni kormányhoz köthető csoport feltört egy izraeli felhőmegoldás-szolgáltatót. A Microsoft vizsgálata szerint a támadók valószínűleg a szolgáltatótól ellopott hitelesítő adatokat használtak arra, hogy bejelentkezzenek egy izraeli logisztikai cég rendszerébe. A MSTIC megfigyelte, hogy ugyanez a csoport még abban a hónapban megpróbált destruktív kibertámadást indítani a logisztikai vállalat ellen.
- 2022 áprilisában a POLÓNIUM, egy libanoni csoport, amelyről kiderítettük, hogy az iráni állami támadócsoportokkal működik együtt az IT-ellátási lánc elleni technikák alkalmazásában, feltört egy másik izraeli IT-céget, hogy hozzáférést szerezzen az izraeli védelmi és jogi szervezetekhez.[5]

Ezek az elmúlt évben észlelt tevékenységek bizonyítják, hogy az olyan támadók, mint a NOBÉLIUM és a DEV-0228, jobban ismerik a kiszemelt vállalat bizalmi kapcsolatait, mint maga a vállalat. Ez a megnövekedett fenyegetés kiemeli, mennyire fontos megerősíteni a vállalati digitális vagyon határait és belépési pontjait. Annak a fontosságára is felhívják a figyelmet, hogy az IT-szolgáltatóknak is kiemelten fontos szigorúan ellenőrizni saját kiberbiztonsági állapotukat. A szervezeteknek például többfaktoros hitelesítést és feltételes hozzáférési szabályzatokat kell bevezetniük, amelyek megnehezítik a rosszindulatú támadók számára, hogy megszerezzék az ellenőrzést a kiemelt hozzáféréssel rendelkező fiókokat felett, vagy a hálózaton keresztül további rendszerekhez szerezzen hozzáférést.

A partneri kapcsolatok alapos ellenőrzésével és auditálásával csökkenthető a vállalat és az általa igénybe vett szolgáltatók közötti szükségtelen engedélyek száma, és azonnal megvonható az ismeretlenek kapcsolatok hozzáférése. A tevékenységnaplók alaposabb ismerete és a rendelkezésre álló tevékenységek áttekintése megkönnyíti a további vizsgálatot kiváltó rendellenességek észlelését.

> Az állami támadók a külső feleket megcélozva fontos szervezetekhez törhetnek be az ellátási láncon belüli bizalmat és hozzáférést kiaknázva.

Gyakorlati tanácsok

1. Tekintse át és auditálja mindkét irányú szolgáltatói kapcsolatait, valamint a delegált jogosultságokat a szükségtelen engedélyek számának minimalizálásához. Vonja meg az ismeretlennek tűnő vagy még nem auditált partneri kapcsolatok hozzáférését.[6]
2. Engedélyezze a naplózást és tekintse át az összes, távoli hozzáférési infrastruktúrához és virtuális magánhálózatokhoz (VPN) kapcsolódó hitelesítési tevékenységet – különösen figyeljen az egyfaktoros hitelesítésre beállított fiókokra, győződjön meg a valódiságukról, és vizsgáljon ki minden rendellenes tevékenységet.
3. Engedélyezze az MFA-t az összes fiókhoz (beleértve a szolgáltatásfiókokat is), és ügyeljen rá, hogy minden távoli kapcsolat esetén megkövetelje az MFA használatát.
4. Használjon jelszó nélküli megoldásokat a fiókok védelméhez.[7]

További információra mutató hivatkozások

- NOBÉLIUM targeting delegated administrative privileges to facilitate broader attacks | Microsoft Threat Intelligence Center (MSTIC)
- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC)

A biztonsági rések gyors kiaknázása

Ahogy szervezetek erősítik kiberbiztonsági helyzetüket, a nemzetállami szereplők is új és egyedi taktikákat keresnek a támadások indítására és a lelepleződés elkerülésére. Ennek során a korábban ismeretlen biztonsági rések – más néven a nulladik napi sebezhetőségek – keresése és kihasználása kulcsfontosságú taktika.

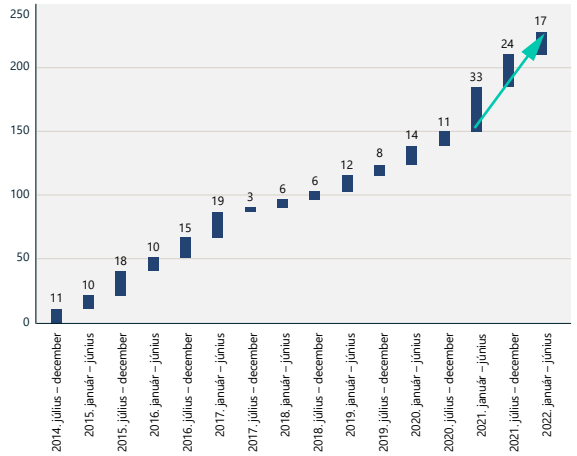
A nulladik napi sebezhetőségek különösen hatékonyak, ha elsőként használják ki őket, és ha nyilvánosan elérhetővé válnak, más nemzetállami és bűnügyi szereplők is gyorsan kihasználhatják ezeket. Az elmúlt évben a nyilvánosan közzétett nulladik napi sebezhetőség mennyisége nagyságrendileg azonos volt az előző évivel, amely minden korábbi rekordot megdöntött.

Mivel a kiberfenyegetést jelentő szereplők – mind az állami, mind a bűnözői csoportok – egyre ügyesebben használják ki ezeket a biztonsági réseket, megfigyelhető, hogy a sebezhetőségek bejelentése és kommodizációja között egyre rövidebb idő telik el. Ez létfontosságúvá teszi, hogy a szervezet haladéktalanul javítsák a felfedezett biztonsági réseket. Hasonlóképpen igen fontos, hogy az új sebezhetőségeket felfedező szervezetek és magánszemélyek a lehető leghamarabb, felelős módon tegyék ezeket közzé, vagy jelentsék az érintett szállítónak – a sebezhetőségek összehangolt közzétételi eljárásaival összehangban.

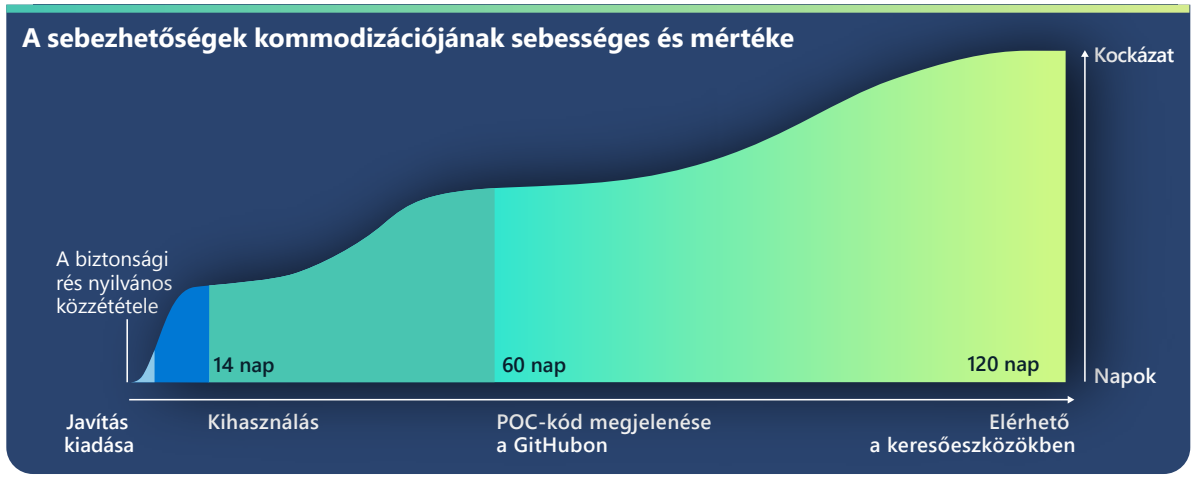
Ez biztosítja a sebezhetőségek azonosítását, illetve azt, hogy időben elkészüljön rájuk a javítás, amely megvédi az ügyfeleket a korábban ismeretlen fenyegetésektől.

Sok szervezet azt feltételezi, hogy a sebezhetőségek menedzselése szerves része hálózatbiztonsági eljárásaiknak, azzal csökkenthetik annak a valószínűségét, hogy egy nulladik napi sebezhetőségen alapuló támadás áldozataivá váljanak. A biztonsági rések kommodizációja azonban azzal jár, hogy sokkal gyakrabban kell szembenézni ilyen típusú támadásokkal. A nulladik napi sebezhetőségeket gyakran más szereplők fedezik fel, és rövid idő alatt sor kerül széles körű kihasználásukra, ami miatt a javítás nélküli rendszerek veszélybe kerülnek. Annak ellenére, hogy a nulladik napi sebezhetőségek kihasználását nem könnyű észlelni, a támadók behatolás utáni tevékenységei gyakran sokkal könnyebben felfedezhetők – ezek különösen akkor lehetnek erős figyelmeztető jelek, ha olyan rendszeren történnek, amelyre minden javítást telepítettek.

A nulladik napi sebezhetőségekre kiadott javítások



A biztonsági réseket listázó Common Vulnerabilities and Disclosures (CVEs) listáján szereplő, nyilvánosan közzétett nulladik napi sebezhetőségek.



Átlagosan mindössze 14 napot vesz igénybe, ha egy nyilvános bejelentett sebezhetőséget elkezdjenek kihasználni. Ezen az ábrán a nulladik napi sebezhetőségek kihasználási idővonalának elemzése látható azoknak a rendszereknek a számával együtt, amelyeket az adott sebezhetőség érintett és amelyek aktívak voltak az interneten a sebezhetőség nyilvánosságra hozatalának időpontjában.

> Bár a nulladik napi sebezhetőségekre alapuló támadások elsőként jellemzően csak szervezetek szűkebb körét érintik, gyorsan beépülnek a tágabb támadói ökoszisztémába. Ez olyan versengést indít, amelyben a támadók igyekeznek minél szélesebb körben kihasználni a sebezhetőséget, mielőtt a potenciális célpontjaik telepítenék a javításokat.

Bár minden nemzetállami szereplőnél megfigyeltük, hogy ismeretlen sebezhetőségeket használ ki a támadásai során, a kínai állami hátterű támadók különösen nagy tapasztalatra tettek szert a nulladik napi biztonsági rések feltárásában és kihasználásában.

Kína sebezhetőségbejelentési rendelete 2021 szeptemberében lépett hatályba, és a világon elsőként előírja, hogy a sebezhetőségeket egy állami hatóságnak kell bejelenteni, mielőtt megoszthatnák őket a termék vagy szolgáltatás tulajdonosával. Ez az új rendelet lehetővé teszi, hogy bizonyos kínai kormányzati szervek összegyűjtsék a bejelentett sebezhetőségeket, hogy később kiberfegyverként használhassák őket. Az elmúlt évben azt láthattuk, hogy a kínai szereplők körében megnőtt a nulladik napi sebezhetőségek használatának gyakorisága, ami valószínűleg a kínai biztonsági közösség számára előírt új bejelentési követelmény első évének eredménye, és nagy lépés a nulladik napi sebezhetőségek állami prioritások közé emelésében. Az alábbiakban ismertetett biztonsági réseket először a kínai nemzetállami szereplők használták fel a támadásaik során, mielőtt a támadói ökoszisztéma más tagjai is felfedezték és szélesebb körűen alkalmazták volna őket.

A biztonsági rések gyors kiaknázása

Folytatás

Még a nemzetállami támadások célpontjai között nem szereplő szervezeteknek is korlátozott idejük van a nulladik napi sebezhetőségek javítására az érintett rendszerekben, mielőtt az adott sebezhetőséget a szélesebb támadói ökoszisztéma is elkezdené kihasználni.

Az újonnan azonosított sebezhetőségek e példái bizonyítják, hogy a szervezeteknek a sebezhetőség javításától a koncepcióigazoló (POC) kód online közzétételéig (amelyet gyorsan átvesznek és újrahasznosítanak mások is) átlagosan 60 napjuk van. Ehhez hasonlóan átlagosan 120 nap telik el addig, amíg egy sebezhetőség bekerül a biztonsági rések keresésére és kihasználására szolgáló olyan automatikus eszközökbe, mint a Metasploit – ami gyakran a sebezhetőség igen széles körű kihasználását eredményezi. Ez rávilágít arra, hogy még a nemzetállami támadók célpontjai között nem szereplő szervezeteknek is korlátozott idejük van a nulladik napi sebezhetőségek javítására az érintett rendszerekben, mielőtt a sebezhetőséget a szélesebb támadói ökoszisztéma is elkezdené kihasználni.

CVE-2021-35211 SolarWinds Serv-U

2021 júliusában a SolarWinds kiadott egy biztonsági figyelmeztetést a CVE-2021-35211 jelű sebezhetőséggel kapcsolatban, amelynek felfedezését a Microsoftnak tulajdonította.[8] Ekkoriban ugyanis felfedeztük, hogy a nemzetállami érdekek mentén tevékenykedő DEV-0322 aktívan kihasználja a SolarWinds Serv-U biztonsági résést. A RiskIQ-csapat június 15. és július 9. között 12 646 olyan IP-címet figyelt meg, amelyet az érintett eszközök internetkapcsolattal rendelkező verziói használtak.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

2021 szeptemberében kutatóink megfigyelték, hogy kínai kapcsolatokkal rendelkező támadók több egyesült államokbeli szervezetnél aktívan kihasználják a Zoho ManageEngine sebezhetőségét. A biztonsági rést szeptember 6-án jelentették be nyilvánosan, és a CVE-2021-40539 Zoho ManageEngine ADSelfService Plus nevet kapta – ez a komponenst a szervezetek jellemzően a jelszavak átállításához használtál.[9] A DEV-0322 még szeptember folyamán kihasznált a biztonsági rést, és kiinduló vektorként használta fel arra, hogy megvesse a lábát a megcélzott hálózatokon, és olyan műveleteket végezzen, mint a hitelesítő adatok kinyerése, egyéni binárisok telepítése, valamint a tartós jelenlétüket biztosító rosszindulatú szoftverek elhelyezése. A közzétételkor a RiskIQ az ilyen rendszerek 4011 aktív, internetre csatlakozó példányát figyelte meg.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

2021. október végén észleltük, hogy a DEV-0322 egy második Zoho ManageEngine termékben, a ServiceDesk Plus-ban – ez egy eszközkezeléssel rendelkező IT-ügyfélszolgálati szoftver – lévő sebezhetőséget (CVE-2021-44077) is kihasznál. A DEV-0322 ezt a sebezhetőséget egészségügyi, információtechnológiai, felsőoktatási és kritikus fontosságú gyártóipari szereplők ellen vetette be. December 2-án a Szövetségi Nyomozó Iroda (FBI) és a Cybersecurity and Infrastructure Security Agency (CISA) közös, a nagyközönségnek szóló figyelmeztetést adott ki arról, hogy a nemzetállami támadók kihasználják ezt a sebezhetőséget. A közzétételkor a RiskIQ az ilyen rendszerek 7956 aktív, internetre csatlakozó példányát figyelte meg.

CVE-2021-42321 Microsoft Exchange

Az Exchange CVE-2021-42321 jelű nulladik napi sebezhetőséget a 2021. október 16. és 17. között a kínai Csengtuban tartott, Tianfu Cup nevű nemzetközi kiberbiztonsági csúcstalálkozó alatt fedezték fel. A Microsoft biztonsági kutatói megfigyelték, hogy az Exchange sebezhetőségét már október 21-én – mindössze három nappal a sebezhetőség bejelentése után már kihasználták. A közzétételkor a RiskIQ az ilyen rendszerek 61559 aktív, internetre csatlakozó példányát figyelte meg. A sebezhetőség kihasználása 2021 novemberében tovább folytatódott.

CVE-2022-26134 Confluence

Egy kínai kapcsolatokkal rendelkező támadó valószínűleg már rendelkezett a Confluence sebezhetőségét (CVE-2022-26134) kihasználó kóddal négy nappal a sebezhetőség június 2-ai nyilvánosságra hozatala előtt, és valószínűleg fel is használta egy egyesült államokbeli célpont ellen. A közzétételkor a RiskIQ a sebezhető Confluence-rendszerek 53 621 aktív, internetre csatlakozó példányát figyelte meg.

A sebezhetőségeket hatalmas léptékben találják meg és használják ki – egyre rövidebb idő alatt.

Gyakorlati tanácsok

1. A nulladik napi sérülékenységek javításait telepítse elsőbbséggel, amint megjelennek – ne várja meg, amíg a javításmenedzselési ciklusban sorra kerülnek.
2. Dokumentáljon és vegyen leltárba minden vállalati hardver- és szoftvereszközt a kockázatok meghatározása, valamint a javításokkal kapcsolatos gyors intézkedés érdekében.

Az orosz állam kiberháborús taktikája Ukrajna ellen és azon túl

Az idei évben az orosz állami szereplők az ukrajnai invázió katonai akcióit kiegészítő kiberhadműveleteket indítottak, gyakran ugyanazokat a taktikákat és technikákat alkalmazva, amelyeket az Ukrajnán kívüli célpontok ellen is bevetettek. Létfontosságú, hogy a szervezetek világszerte a kiberbiztonságot erősítő lépéseket tegyenek az Oroszország érdekei mentén tevékenykedő digitális támadók ellen.

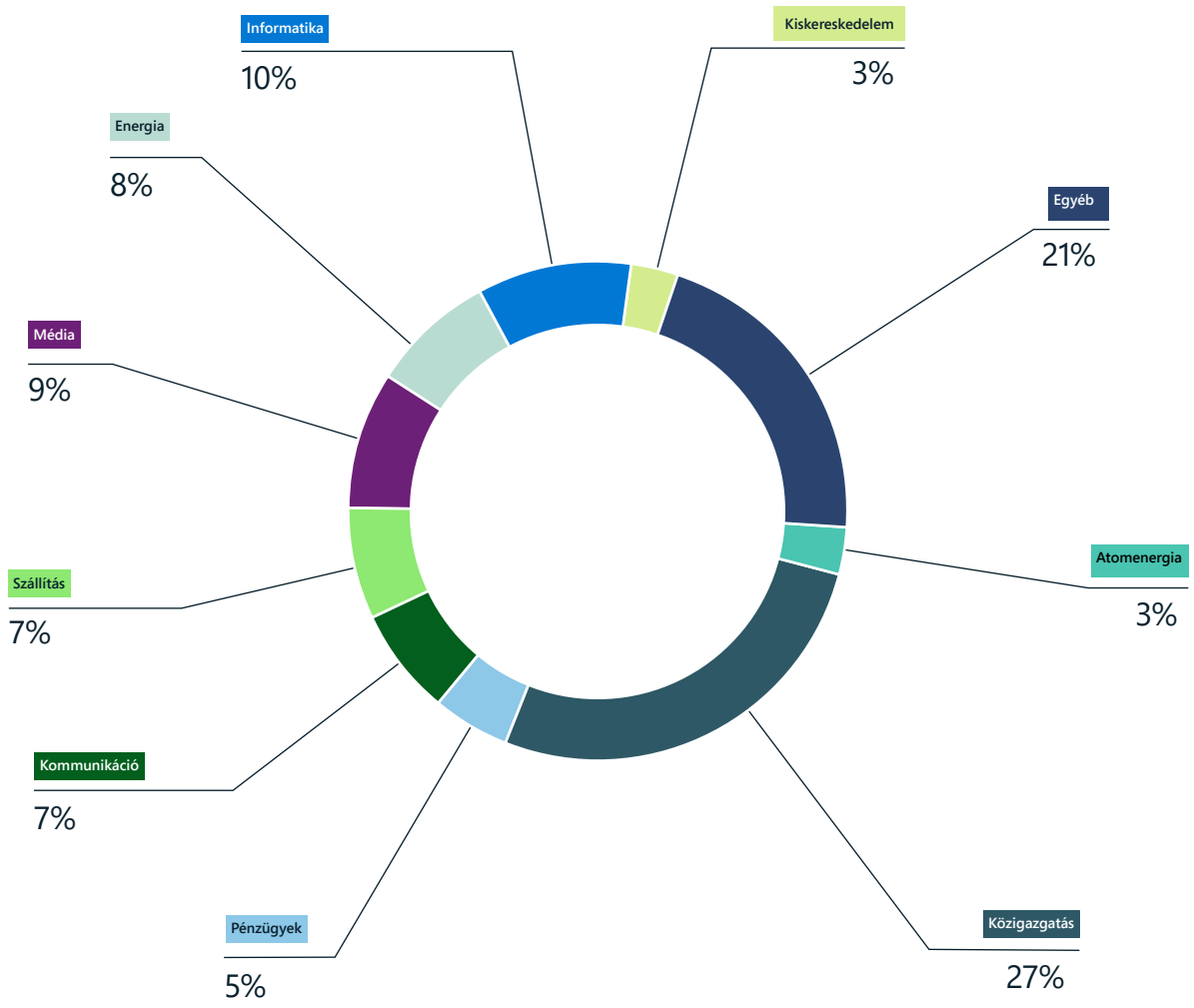
A katonai konfliktus folytatódásával a harctéri helyzet továbbra is hullámzó, ezért Ukrajnának és szövetségeseinek fel készülni arra, hogy megvédjék magukat, ha az orosz állami kibertámadók a katonai célokkal összhangban megnövelik a támadások gyakoriságát vagy intenzitását. A háború első négy hónapja alatt a Microsoft megfigyelte, hogy az orosz hadsereghez kötődő támadók több hullámban is pusztító kibertámadásokat indítottak közel 50 különböző ukrán ügynökség és vállalat ellen, valamint kémkedési céllal támadtak sok másikat. Az online szolgáltatások ügyfelei elleni műveleteket leszámítva az ismert célpontok ellen irányuló orosz támadások 64 százalékát február vége és június között Ukrajnában tevékenykedő szervezetek ellen követték el.

Az orosz támadók minden ilyen műveletekben számos olyan taktikát, technikát és eljárást (TTP-t) alkalmaztak, amelyet már az invázió előtt is megfigyeltünk az Ukrajnán belüli és kívüli célok elleni támadások során. A konfliktus kezdeti szakaszában a támadók célja az volt, hogy adatokat semmisítsenek meg, és kibillentsék az egyensúlyukból az ukrán kormányzati ügynökségeket. Azóta megkísérelték megakadályozni a katonai és humanitárius segélyszállítmányok Ukrajnába való eljuttatását, megzavarni a szolgáltatásokhoz és a médiához való nyilvános hozzáférést, valamint Oroszország számára hosszabb távú hírszerzési vagy gazdasági értékkel bíró információkat próbáltak lopni.

A szállítás megcélzása a konfliktust túlélni próbáló ukrán emberek számára létfontosságú területet fenyeget. Egy májusi, az UNICEF által szponzorált felmérés keretében a konfliktus által sújtott városokban megkérdezettek leginkább a közlekedés és az üzemanyag-ellátás, a szállítmányozás fennakadásai, a biztonság és az élelmiszerekhez, az orvosi ellátásához és a pénzügyi szolgáltatásokhoz való korlátozott hozzáférés miatt aggódtak.[10] Júniusban az ENSZ Ukrajnáért felelős válságkoordinátora arról számolt be, hogy az országban legalább 15,7 millió ember szorul sürgős humanitárius segítségre, és ez a szám a háború folytatódásával csak nőni fog.[11]

Ukrajnán kívül a Microsoft február és június között a világ 42 országának 128 szervezeténél észlelt az orosz szereplők számlájára írható hálózati behatolási kísérletet. Az Egyesült Államok volt Oroszország első számú célpontja. Ugyanebben az időszakban Lengyelország is fontos célpont volt, mivel ezen az országon halad keresztül az Ukrajnába tartó nemzetközi katonai és humanitárius segítség nagy része. Az orosz állammal kapcsolatban álló támadók áprilisban és májusban a balti országokban működő szervezeteket, valami dán, norvég, finn és svéd számítógépes hálózatokat is célba vettek.

A legnagyobb arányban támadott ágazatok Ukrajnában az invázió kezdete óta



A konfliktus során az orosz állami és állami kapcsolatokkal rendelkező támadók elsődleges célpontjai között továbbra is első helyen szerepelnek az ukrán szövetségi, állami és helyi kormányzati szervezetek. A közlekedési, az energiaipai, a pénzügyi és a médiaszektor szervezeteinek célkeresztbe kerülése rávilágított arra, hogy milyen kockázatokat jelentenek ezek a kiberműveletek az ukrán polgárok számára fontos ágazatokra.

Az orosz állam kiberháborús taktikája Ukrajna ellen és azon túl

Folytatás

Megfigyeléseink szerint a NATO-tagországok külügyminisztériumai elleni hasonló műveletek száma is megnövekedett.

Az orosz állami támadócsoportok az elmúlt évben is érdekeltek voltak abban, megzavarják a kritikus fontosságú infrastruktúra működését Ukrajnán belül és kívül. Az IRÍDIUM a Industroyer2 nevű rosszindulatú szoftverrel indított meghiúsult támadást azzal a céllal, hogy több millió ukránt fosszon meg az energiaellátástól. Ukrajnán kívül 2022 elején a BRÓM gyártóipari és ipari vezérlőrendszerekkel foglalkozó vállalatokhoz hatolt be.

Az orosz állami és állami kapcsolatokkal rendelkező szereplők az Ukrajna, a szövetségesei és más, hírszerzési szempontból fontos célpontok ellen indított idei támadások során a következő TTP-k közül sokat alkalmaztak:

Célzott adathalászat rosszindulatú mellékletekkel vagy hivatkozásokkal

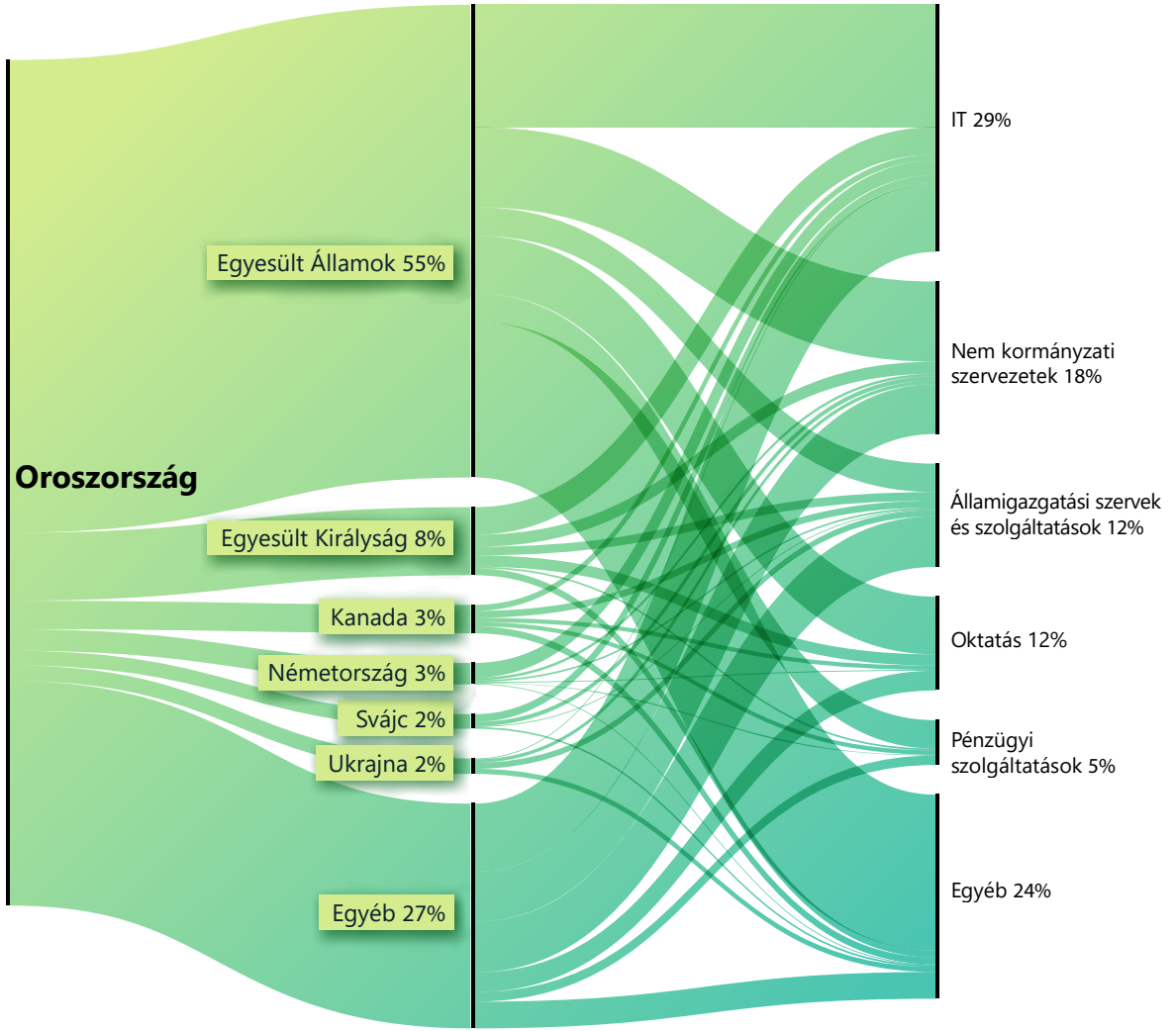
Az orosz állami és orosz kapcsolatokkal rendelkező csoportok – például az AKTÍNIUM, a NOBÉLIUM, a STROCIUM, a DEV-0257, a SZIBORGIUM és az IRÍDIUM – mind alkalmaztak adathalász kampányokat ahhoz, hogy kezdeti hozzáférést szerezzenek az Ukrajnán belüli és kívüli szervezetek fiókjaihoz és hálózataihoz. Számos kampány feltört vagy hamisított fiókokat használt a megcélzott vállalatoknál vagy az adott iparágon belül, és ezeket meggyőző témákkal kombinálta az áldozatok megtévesztéséhez. A NOBÉLIUM feltört diplomáciai fiókokból küldött diplomáciai levélnek álcázott e-maileket más országok külügyminisztériumi dolgozóinak világszerte. A STRONCIUM hamisított fiókokat hozott létre egyesült államokbeli agytrösztök tagjainak nyilvánosan közzétett nevét használva, és adathalászati üzenetet küldött azzal a céllal, hogy hozzáférjen az adott agytröszt fiókjaihoz. A SZIBORGIUM az ukrajnai konfliktussal kapcsolatos jelentéseket használt csaliként az adathalász támadásai során, amelyekkel kezdeti hozzáférést próbált szerezni az északi országokban működő, nemzetközi ügyekkel foglalkozó agytrösztök rendszereihez.

Az IT-szolgáltatások ellátási láncának kihasználása a szolgáltatók ügyfeleinek támadása érdekében

2021. végén az orosz állami szereplők IT-szolgáltatókat törtek fel, és a megszerzett hozzáférést webhelyek megrongálásához használták, a DEV-0586 pedig januárban a Whispergate nevű, destruktív rosszindulatú szoftvert telepítette a segítségével.[12] A DEV-0586 egy olyan IT-cég hálózatát is feltörte, amely erőforrás-menedzsment rendszereket készített Ukrajna Hadügyminisztériumának, valamint a kommunikációs és a szállítmányozási szektor vállalatainak – ebből már akkor következtetni lehetett rá, hogy a csoport ezekben az ágazatokban is a külső félen keresztüli támadások lehetőségét keresi.

2021 és 2022 során a NOBÉLIUM világszerte, de különösen az Egyesült Államokban és Nyugat-Európában informatikai szolgáltatókat célzott meg, hogy hozzáférést szerezzen kormányzati és más bizalmas hálózatokhoz (lásd a fejezet korábbi, az ellátási lánc sebezhetőségeivel foglalkozó részét).

Oroszország: a legfontosabb célországok és -iparágak



Annak ellenére, hogy a 2022 eleje óta egyre inkább az ukrán szervezetek kerültek középpontba, az Észak-Amerikában és Nyugat-Európában működő, szolgáltatásokat igénybe vevő vállalatok továbbra is az orosz támadók legfontosabb célpontjai között vannak. A NOBÉLIUM IT-szektor elleni műveletsorozata nyomán ez az ágazat szenvedte el a legtöbb támadást az elmúlt évben.

Az orosz állam kiberháborús taktikája Ukrajna ellen és azon túl

Folytatás

Nyilvánosan hozzáférhető alkalmazások kihasználása a hálózatokhoz való kezdeti hozzáféréshez

Legalább 2021 vége óta a STRONCIUM azon dolgozott, hogy fejlessze és finomítsa a nyilvánosan hozzáférhető szolgáltatások – például a Microsoft Exchange-szerverek – kihasználásának képességét, amelynek révén információkat tud lopni. A STRONCIUM javítatlanul hagyott Exchange-szervereket kihasználva szerzett hozzáférést ukrán kormányzati fiókokhoz, valamint katonai és hadiiparral kapcsolatos szervezetek rendszereihez az Egyesült Államokban, Libanonban, Peruban és Romániában, valamint egyéb kormányzati ügynökségek rendszereihez Örményországban, Boszniában, Koszovóban és Malajziában. A DEV-0586, amely szintén az orosz hadsereggel áll kapcsolatban, a Confluence-szerverek sebezhetőségeit kihasználva szerzett kezdeti hozzáférést a kormányzati és IT-szektorbeli szervezetek rendszereihez Ukrajnában és más kelet-európai országokban.

Az orosz állami és állami kapcsolatokkal rendelkező támadók nagyrészt azonos TTP-ket alkalmaznak a célul kiszemelt szervezetek feltöréséhez háborúban és békeidőben egyaránt.

Rendszergazdai fiókok és protokollok, natív hálózatfelderítési segédprogramok és oldalirányú mozgás használata

A hálózathoz való kezdeti hozzáférés megszerzése után a Microsoft megfigyelései szerint az orosz állami szereplők az alapvető karbantartási feladatok elvégzéséhez szükséges legitim fiókokat és segédprogramokat használják, hogy a lehető legtovább észrevétlenek maradjanak. Rendszergazdai képességekkel rendelkező feltört identitásokra érvényes felügyeleti protokollokra, eszközökre, illetve módszerekre támaszkodva mozognak oldalirányban a hálózatokon anélkül, hogy ezzel azonnal magukra vonnák az automatikus figyelőrendszerek és hálózatvédelmi eszközök figyelmét.

Az alapvető kiberhigiénia és a végponti észlelési és reagálási eszközök alkalmazása enyhítheti az ilyen típusú műveletek negatív hatásait úgy békeidőben, mint háborús konfliktusok idején.

A folyamatban lévő konfliktusok kiszámíthatatlansága világszerte megköveteli a vállalatoktól, hogy megerősítsék kiberbiztonsági rendszerüket az orosz állami és állami kapcsolatokkal rendelkező támadók jelentette digitális fenyegetések enyhítéséhez.

Gyakorlati tanácsok

1. Minimalizálja a hitelesítő adatok ellopásának és a fiókokkal való visszaélések kockázatát a felhasználók identitását védő MFA-identitásvédelmi eszközök bevezetésével, és tartassa be a legkisebb jogosultság elvét a legérzékenyebb és kiemelt jogosultságokkal rendelkező fiókok és rendszerek esetén.
2. Telepítse a frissítéseket annak biztosítása érdekében, hogy minden rendszere a lehető legkorábban a lehető legmagasabb szintű védelmet élvezhesse, és mindig naprakész legyen.
3. Telepítsen vírusirtó, végponti észlelési és identitásvédelmi megoldásokat az egész vállalatnál. A mélyreható biztonsági megoldások kombinációja a jól képzett és megfelelő készségekkel rendelkező személyzettel párosítva lehetővé teheti a szervezet számára az üzletmenetet befolyásoló betörések azonosítását, észlelését és megelőzését.
4. Tegye lehetővé a vizsgálatot és a helyreállítást abban az esetben, ha a környezetére leselkedő fenyegetést észlel, vagy ilyenről kap értesítést: készítsen biztonsági mentést a kritikus rendszerekről, és engedélyezze a naplózást. Kifejezetten ajánlott megtervezni az incidensek esetén elvégzendő válaszlépéseket.

További információra mutató hivatkozások

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- The hybrid war in Ukraine | Microsoft On the Issues
- Cyber threat activity in Ukraine: analysis and resources | Microsoft Security Response Center (MSRC)
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues
- Malware attacks targeting Ukraine government | Microsoft On the Issues
- MagicWeb: NOBÉLIUM's post-compromise trick to authenticate as anyone | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

Kína: egyre több globális célpont a versenyelőny megszerzése érdekébe

Napjaink komplex geopolitikai környezetében a kínai állami és állammal kapcsolatban álló támadók kiberhadműveleteiket gyakran azzal a céllal folytatják, hogy előmozdítsák országuk stratégiai katonai, gazdasági és külpolitikai céljainak megvalósítását – mindez jól illeszkedik Kína versenyelőny megszerzésére irányuló erőfeszítéseibe. Az elmúlt évben a Microsoft kiterjedt kínai kiberfenyegetéseket észlelt, amelyek a világ számos országát célba vették.

2021 közepe óta Kína a gazdasági és pénzügyi stabilitás biztosítása érdekében manőverezik, miközben a koronavírus-járvány két éve nem látott súlyossággal lángolt fel ismét az országban.[13] Kína továbbra is egyensúlyozó álláspontot van a geopolitikai eseményekkel kapcsolatban, például igyekszik fenntartani „korlátok nélküli" partnerségét Oroszországgal[14], miközben próbálja megőrizni globális politikai színtéren elfoglalt pozícióját is.[15] Emellett Kína az Egyesült Államokkal és szövetségeseivel is szembehelyezkedett Tajvan[16] és a Dél-kínai-tenger feletti ellenőrzés okán, emiatt számos országgal kiéleződött a viszonya.[17]

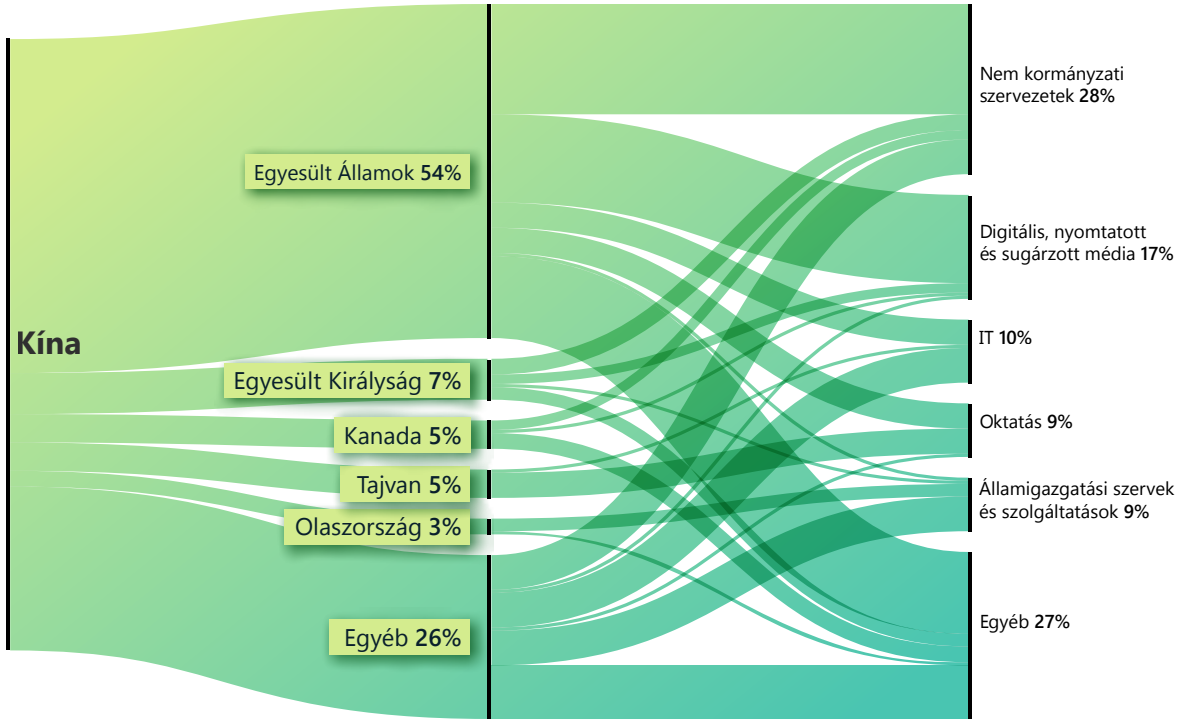
A kínai állami és állami kapcsolatokkal rendelkező csoportok növekvő mértékben célozzák meg a kisebb országokat világszerte, de főleg Délkelet-Ázsiára összpontosítanak, hogy Kína minden fronton versenyelőnyhöz jusson.

Kína továbbra is folytatja gazdasági befolyása globális kiterjesztését a korábban létrehozott Egy övezet, egy út kezdeményezés révén, megpróbál újraéleszteni egy, az EU-val létrehozandó átfogó beruházási keretrendszert[18], továbbá új regionális kereskedelmi megállapodásokról folytat tárgyalásokat az ázsiai és csendes-óceáni térségben Regionális Átfogó Gazdasági Partnerség néven.[19] A Microsoft a megfigyelt kiberműveletek és a megcélzott szervezetek sokfélesége alapján úgy véli, hogy Kína továbbra is fel fogja használni a kiberhadviselés eszközeit kémkedési célokra, hogy előmozdítsa stratégiai politikai, katonai és gazdasági céljainak megvalósítását.

A kibertámadások célzása valószínűleg előmozdítja gazdasági és katonai érdekek érvényesítését.

A Microsoft megfigyelései szerint a kínai állami és állami kapcsolatokkal rendelkező támadócsoportok gyakorta veszik célba a kisebb országokat világszerte, ami arra enged következtetni, hogy Kína nagy valószínűséggel a kiberkémkedést is a globális gazdasági és katonai befolyásszerzés egyik eszközeként használja.

Kína: a legfontosabb célországok és -iparágak



A kínai támadók leggyakrabban az agytrösztöket/civil szervezeteket, valamint a média, az informatika, a közigazgatás és az oktatási szereplőit veszik célba, feltehetően hírszerzési és felderítési célból.

Célkeresztbe kerültek többek között afrikai, karibi, közel-keleti, óceániai és dél-ázsiai államok, melyek közül kifejezetten nagy hangsúlyt kaptak Délkelet-Ázsia és Óceánia országai.

Kína Egy övezet, egy út kezdeményezésével összhangban a kínai csoportok Afganisztánban, Kazahsztánban, Mauritiuson, Namíbiában, valamint Trinidad és Tobagóban működő szervezeteket vettek célba.[20] Például Trinidad és Tobago volt az első olyan karibi ország, amely támogatta Kína Egy övezet, egy út kezdeményezését 2018-ben, és Kína fontos partnerként tekint rá a régióban. A NIKKEL 2021 óta folyamatosan Trinidad és Tobagót célzó hálózati műveleteket folytat. Például 2022 márciusában a NIKKEL felderítési tevékenységet folytatott az ország egyik kormányzati ügynöksége ellen, valószínűleg hírszerzési és adatgyűjtési céllal.

Kína: egyre több globális célpont a versenyelőny megszerzése érdekébe

Folytatás

Eközben a Microsoft megfigyelései szerint a kínai állami és állami kapcsolatokkal rendelkező csoportok hálózati műveletei a délkelet-ázsiai térségben koncentrálódnak, és egyre nagyobb mértékben kiterjednek a csendes-óceáni szigetországokra, ahogy Kína katonai és gazdasági prioritásai eltolódnak, hogy választ adjanak az Egyesült Államok régió iránti megújult érdeklődése által támasztott kihívásokra. 2022 januárjában Microsoft megfigyelte, hogy a RÁDIUM egy vietnámi energetikai vállalatot és egy energiaügyi kormányhivatalt, valamint egy indonéz kormányhivatalt vett célba. A RÁDIUM tevékenysége feltehetően összhangban van Kína Dél-kínai-tengerrel kapcsolatos stratégiai céljaival.[21] Február végén és március elején a GALLIUM több mint 100 fiókot tört fel, amelyek a délkelet-ázsiai régió egy fontos kormányközi szervezetével voltak kapcsolatban. A GALLIUM támadása időben egybeesett az Egyesült Államok és a regionális vezetők közötti tárgyalások bejelentésével. A GALLIUM támadói valószínűleg azt a feladatot kapták, hogy kísérjék figyelemmel a felek kommunikációját, és gyűjtsenek információkat az esemény előtt.

Ahogy Kína kiterjesztette befolyását a csendes-óceáni szigeteken, a kínai támadók is célba vették a területet. Áprilisban Kína és a Salamon-szigetek aláírt egy biztonsági megállapodást, amelynek célja „a béke és a biztonság előmozdítása". A megállapodás lehetővé teszi, hogy Kína fegyveres rendőri és katonai erőket telepítsen a Salamon-szigetekre.[22] Májusában Kína volt a házigazdája a Kína és a csendes óceáni szigetországok külügyminisztereinek közötti találkozónak Fidzsin, ahol „átfogó stratégiai partnerséget" javasolt a politikai, kulturális, társadalmi, biztonsági és éghajlatváltozással kapcsolatos érdekek előmozdítása, valamint a világjárvány leküzdése céljából.[23] Szintén májusban, körülbelül ezzel egyidőben, a Microsoft azonosította a GADOLÍNIUM rosszindulatú szoftverét a Salamon-szigetek kormányzati rendszereiben. A RÁDIUM szintén rosszindulatú kódot futtatott egy telekommunikációs vállalat rendszerein Pápua Új-Guineában. Felmérésünk szerint ezeknek a tevékenységeknek a célja a Kína átfogó regionális stratégiáját támogató információgyűjtés.

A Microsoft felszámolta a NIKKEL tevékenységét, de a csoport nem adja fel.

2021 decemberében a Microsoft Digital Crimes Unit (DCU) a Virginia Keleti körzetében illetékes bíróságtól 42, a NIKKEL által használt irányítási (C2) tartomány elkobzását kérte. Ezeket a C2-tartományokat kormányok, diplomáciai testületek és a civil szervezetek elleni műveletekhez használták Közép- és Dél-Amerikában, a Karib-térségben, Európában és Észak-Amerikában 2019 szeptembere óta.[24] Ezen műveletek során a NIKKEL hosszú távú hozzáférést szerzett számos szervezet rendszereihez, és folyamatosan adatokat szivárogtatott ki áldozataitól 2019 vége óta.

Mivel Kína továbbra is folytatja a kétoldalú gazdasági kapcsolatok kialakítását más országokkal – gyakran az Egy övezet, egy út kezdeményezés részeként –, Kína globális befolyása tovább fog növekedni. Értékelésünk szerint a kínai állami és állami kapcsolatokkal rendelkező csoportok a továbbiakban is célba fogják venni a kormányzati, a diplomáciai és a civil szervezeteket, hogy új információkat szerezzenek, feltehetően gazdasági kémkedési vagy hagyományos hírszerzési céllal. Amióta a Microsoft felszámolta a NIKKEL hálózatát, a csoport számos kormányügynökséget vett célba, vélhetően az elveszett hozzáférés visszaszerzésének szándékával. 2022. március vége és május között a NIKKEL legalább öt kormányügynökség rendszereit törte fel újra. Ez arra enged következtetni, hogy a csoportnak további belépési pontjai is voltak ezekhez a szervezetekhez, vagy új C2-tartományokon keresztül szereztek ismét hozzáférést. A NIKKEL kitartása, amellyel ismételten ugyanazokhoz a kormányügynökségekhez tör be világszerte, azt jelzi, hogy fontos feladatot hajt végre.

Kína külpolitikája egyre rámenősebbé válik. Értékelésünk szerint tovább fogja folytatni a kiberműveletekre alapuló gazdasági kémkedést és hírszerzést.

Gyakorlati tanácsok

1. Erősítse meg a kibervédelmet a kiberfenyegetések proaktív mérsékléséhez. A kínai támadók kitartó működése miatt a vállalatoknak időben azonosítaniuk kell a lehetséges behatolási kísérleteket, védekezniük kell ellenük, valamint megfelelő válaszlépéseket kell tenniük.
2. A támadók gyakori módszere, hogy az ütemezett feladatokat[25] használják arra, hogy tartósan megvessék a lábukat a rendszerben, és elkerüljék a védelmet, ezért fontos, hogy olyan kiegészítő biztonsági irányelveket vezessen be környezetében, amely védelmet nyújt ez ellen az elterjedt módszer ellen.[26]
3. Továbbra is gyakran látjuk, hogy a webshelleket használják elsődleges vektorként a megcélzott hálózatokra való bejutáshoz.[27] A szervezetnek meg kell erősíteniük rendszereik webshellalapú támadások elleni védelmét, amelyeken keresztül a támadók távoli parancsok futtatására alkalmas hozzáférést szerezhetnek.[28]

További információra mutató hivatkozások

- NICKEL targeting government organizations across Latin America and Europe | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Protecting people from recent cyberattacks | Microsoft On the Issues

Az őrségváltást követően egyre agresszívabbá váló Irán

A Microsoft megfigyelései szerint az iráni állami és állami kapcsolatokkal rendelkező támadók növelik az Izraellel szembeni kibertámadások ütemét és terjedelmét, és a zsarolótámadásaikat a regionális ellenfeleken túl egyesült államokbeli és az EU-s célpontokra is kiterjesztik, továbbá az Egyesült Államok létfontosságú infrastruktúrájának részét képező szereplőket is célba vesznek, hogy legalábbis előkészítsék a terepet potenciális destruktív kibertámadások számára.

Az iráni állami szereplők kibertámadásai az országban nemrégiben lezajlott hatalomátvételt követően váltak agresszívabbá. 2021 nyarán a keményvonalas Ibrahim Raisi elnök lépett a mérsékelt Ibrahim Raisi helyébe. Raisi az ország legfelsőbb vezetőjének pártfogoltja és az Iszlám Forradalmi Gárda szövetségese. Szöges ellentéte elődjének, Rouhani elnöknek, aki diplomáciai megoldások iránti vonzalma miatt gyakran került ellentétbe a legfelsőbb vezetővel és a Forradalmi Gárda felső vezetésével.[29] A Raisi-kormányzat erőszakos nézetei láthatóan Izrael és a Nyugat elleni merészebb akciókra sarkallták az iráni kibertámadókat. Különösen az Egyesült Államok elleni tevékenységük fokozódott annak ellenére, hogy a két ország visszaállított diplomáciai kapcsolatait az iráni atomalku felélesztése érdekében.

Az Izraellel szembeni iráni kibertámadások megnövekedett üteme és terjedelme

Néhány héttel azután, hogy Raisi összeállította külpolitikai csapatát[30], az iráni állami szereplők újraindították Izrael elleni kibertámadásaikat – az előző évhez képest megnövelt ütemmel. Ezek a zsarolásos és rendszerfeltöréses-adatszivárogtatásos támadások szeptembertől kezdve néhány hetenként követték egymást, és legalább három, Iránhoz köthető szereplő vett részt bennük, ami arra enged következtetni, hogy egy országos szintű megtorló akció részét képezték Izrael ellen. Legalább egy esetben a Microsoft arra jutott, hogy egy izraeli szervezetet ért zsarolóprogramos támadás 2021 végén egy mögöttes adattörléses támadás elfedésére szolgált. A Microsoft a kártevők elemzése során megállapította, hogy az áldozatnál aktivált zsarolószoftvert úgy programozták, hogy az adatok titkosítása után egy adattörlő rosszindulatú szoftvert futtasson.

2022-re az iráni kibertámadások mind a célok kiválasztása, mint a támadások formája terén szintet léptek. Februárban a DEV-0198 megpróbált destruktív támadást intézni Izrael létfontosságú infrastruktúrája ellen. Az Microsoft vizsgálata azt is kiderítette, hogy valószínűleg egy Iránhoz köthető szereplő volt a felelős azért a kifinomult kibertámadásért is, amely aktiválta a rakétatámadásra figyelmeztető szirénákat júniusban egy olyan szoftverrel, amely a hangjeleket IP-hálózatokon keresztül módosítja.

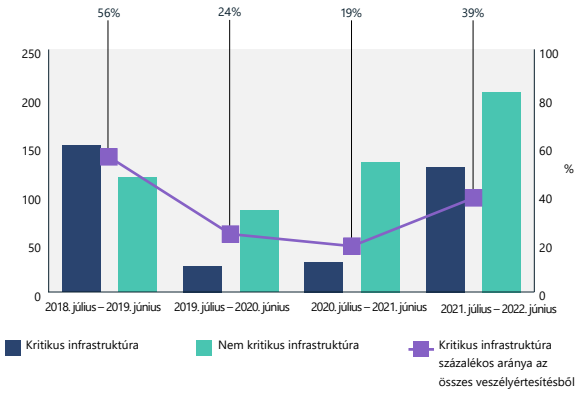
Az Egyesült Államok és Izrael létfontosságú infrastruktúrájára leselkedő iráni fenyegetés az év során fokozódott

A Microsoft felmérése szerint a Forradalmi Gárdához kapcsolódó iráni állami szereplők (FOSZFOR és DEV-0198) 2021 vége és 2022 közepe között az Egyesült Államok és Izrael létfontosságú infrastruktúrájának fontos részeit célozták meg. Valószínűsíthető céljuk az volt, hogy lehetőséget biztosítsanak Teheránnak arra, hogy bosszút álljon azokon a szektorokon, amelyek működését a Forradalmi Gárda vezető körei szerint az Egyesült Államok és Izrael akadályozza Iránban.[31] Elemzésünk szerint ezek a tevékenységek Gholamreza Jalali, a Forradalmi Gárda tábornoka és az iráni Passzív Védelmi Szervezet vezetője által 2021. október végén tett azon kijelentésekhez kapcsolódnak, amelyek a rezsim más befolyásos szereplőinek véleményét tükrözve arról szóltak, hogy az Egyesült Államok és Izrael kibertámadásokat hajtott végre iráni kikötők, vasutak és üzemanyagtöltő állomások ellen.[32] Jalali ezeket a vádakat másodszor is elismételte egy pénteki imabeszéd során, miközben a pódium hátterében az „USA" szót eltaláló rakéta volt látható, jelezve, hogy felettesei is osztják ezt a véleményt.[33]

A FOSZFOR 2021 októberében nagyszabású akciót indított, melynek keretében az egyesült államokbeli szervezeteknél kereste a javítás nélkül hagyott Fortinet- és ProxyShell-sebezhetőségeket. A sebezhetőségek kihasználása után ezeket a javítás nélkül maradt rendszereket zsarolóprogramos támadásokhoz használták, számos esetben az Egyesült Államok és más nyugati országok létfontosságú infrastruktúrája ellen. Ezek voltak az első megerősített esetek, amikor az iráni államhoz kapcsolódó szereplők zsarolótámadásokat hajtottak végre a Közel-Keleten kívül. Az iráni üzemanyagtöltő állomások elleni október végi kibertámadást követően a Microsoft megfigyelései szerint megugrott az amerikai vállalatokat célzó zsarolótámadások száma, ami a kettő közötti összefüggést sejtet.

Ugyanakkor a FOSZFOR konkrét célok támadására állt át, és gyakran a célzott adathalászat módszeréhez folyamodott az Egyesült Államok létfontosságú infrastruktúrájához tartozó fontos cégek, köztük jelentősebb tengeri kikötők és nemzetközi repülőterek, tömegközlekedési rendszerek, közműszolgáltatók, valamint olaj- és gázipari vállalatok elleni támadások során. Ez a fajta célzás, amelyhez gyakran célzott adathalászatot alkalmaztak, 2022 közepéig tartott. A célpontok közvetlenül egybeestek azokkal a szektorokkal, amelyeknek a megtámadását Iránban Teherán az Egyesült Államok és Izrael számlájára írta, és valószínűleg lehetőséget biztosítottak Irán számára a válaszcsapásra. A közel azonos célok feltörése lehetőséget biztosíthat a hasonló jövőbeli támadásoktól való elrettentésre, miközben az eszkalációt is megpróbálja elkerülni azzal, hogy a felelősség felvállalása nélkül jelzi a támadások okát.

Az infrastruktúrát célzó iránit támadások újjáéledése



A létfontosságú infrastruktúrát érő iráni támadások intenzitása a 2018 végi – 2019 eleji időszakban megfigyelthez képest a legmagasabb szintet érte el. A US Presidential Policy Directive 21 (PPD-21) alapján határoztuk meg, hogy egy adott vállalat a létfontosságú infrastruktúra része-e. (2021. július – 2022. június)

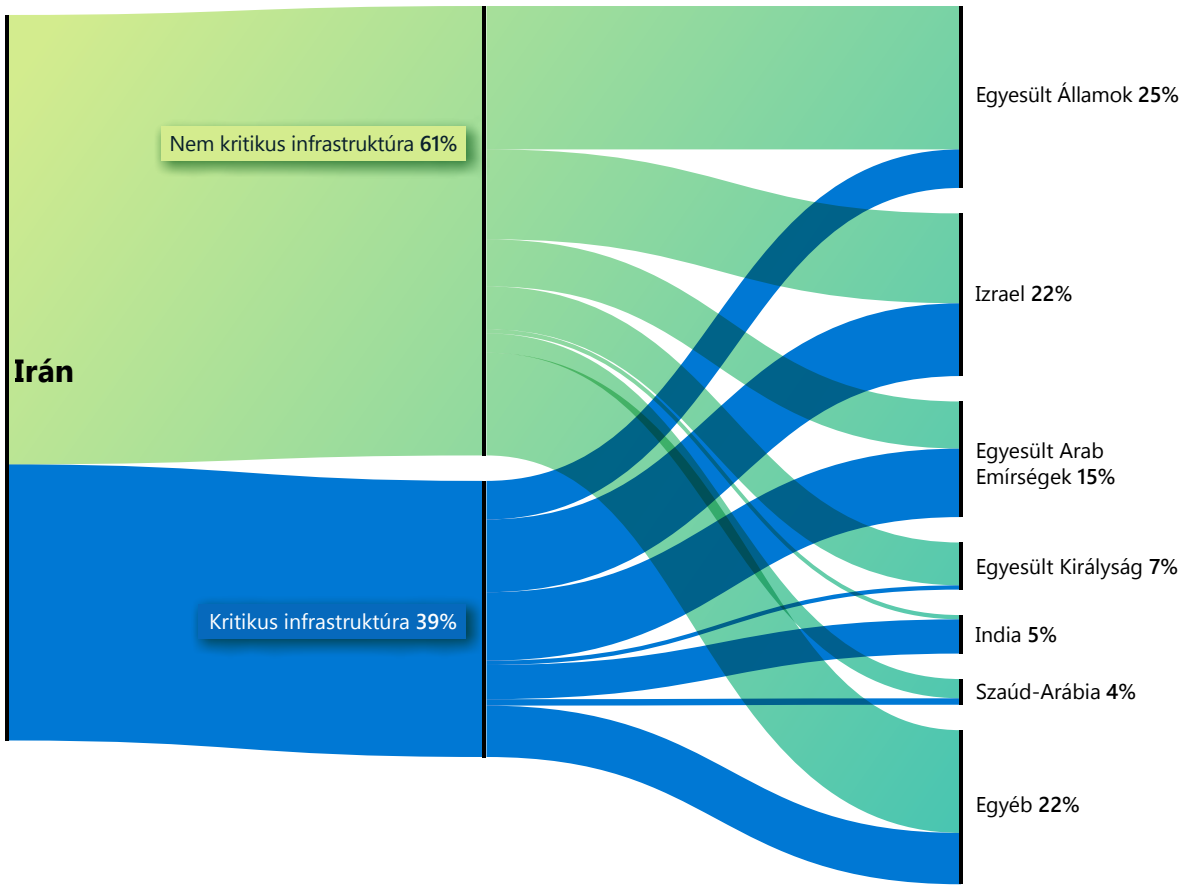
Az őrségváltást követően egyre agresszívabbá váló Irán

Folytatás

Izraelben a DEV-0198 vasúttársaságokat, logisztikai vállalatokat, a logisztikai vállalatok szoftverszolgáltatóit és üzemanyagforgalmazó vállalatokat (különösen üzemanyagtöltő állomásokat) vett célba. 2022 elején a csoport jelentős zavarokat okozó támadást indított egy izraeli logisztikai vállalat hálózatán, amelynek hatására a vállalat kénytelen volt leállítani számítógépeit és bizonyos tevékenységeit a támadás elleni védekezés érdekében. Egy másik esetben azt figyeltük meg, hogy a csoport megkísérelt hozzáférni egy jelentős izraeli szállítóvállalat hálózatához ellopott vagy újrafelhasznált hitelesítő adatokkal. Eközben egy másik iráni csoport, a DEV-0343 – amely a hadiipari, tengeri szállítási és a műholdképekkel foglalkozó vállalatokat vette célba, így valószínűleg a Forradalmi Gárdához kapcsolódik – 2021 elején izraeli szállítmányozó és kikötőkhöz kapcsolódó szervezetek fiókjait törte fel.

Az iráni támadók várhatóan továbbra is fenyegetést jelentenek majd az Egyesült Államok és Izrael közlekedési és energetikai vállalatai számára – különösen annak fényében, hogy az iráni atomalku felélesztésére irányuló diplomáciai erőfeszítések kifulladni látszanak, és Washington, Tel Aviv és Teherán alternatív nyomásgyakorlási módszerekkel próbálják érvényesíteni az érdekeiket.

Iráni támadások a létfontosságú infrastruktúra ellen ország szerint



Irán elsősorban Izrael, az Emírségek és az Egyesült Államok létfontosságú infrastruktúráját célozta meg.

Az iráni szereplők valószínűleg az elkövetkező évben is fenyegetést fognak jelenteni az Egyesült Államok és Izrael szállítmányozási és energetikai vállalataira.

Az iráni csoportok kiterjesztették zsarolótámadásaikat a regionális ellenfeleken túlra, és jelenleg az Egyesült Államok és Izrael létfontosságú infrastruktúrájának fontos részeit célozzák.

Gyakorlati tanácsok

1. Fokozza a szervezet általános kiberhigiéniai képességét azáltal, hogy engedélyezi a jelszó nélkül megoldásokat, például az MFA-t, és kötelezővé teszi a használatukat az összes távoli kapcsolat esetén, ezzel mérsékelve az esetlegesen feltört hitelesítő adatok használatának káros következményeit.
2. Értékelje ki az összes bejövő e-mail-forgalom eredetiségét annak ellenőrzéséhez, hogy a küldő címe valódi-e.
3. Telepítse a javításokat korán és gyakran.[34]
4. Tekintse át és auditálja partneri kapcsolatait a szolgáltatókkal, hogy minimálisra csökkentse a saját szervezete és a szolgáltatók közötti szükségtelen jogosultságok számát. A Microsoft azt javasolja, hogy haladéktalanul vonja meg az ismeretlennek tűnő vagy még nem auditált partneri kapcsolatok hozzáférését.[35]

További információra mutató hivatkozások

- Szaporodnak az informatikai rendszereket érő iráni támadások | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Egy Iránhoz köthető libanoni csoport Izraelt célozza

A Microsoft a kiberfenyegetési tevékenységeket platformtól, megcélzott áldozattól és földrajzi régiótól függetlenül monitorozza. Világszerte biztosítjuk a láthatóságot, és aktív keressük a fenyegetéseket, hogy hatékonyabb észlelési szolgáltatást tudjunk nyújtani ügyfeleink számára.

Bár az általunk megfigyelt állami szereplők nagyrészt Oroszországhoz, Kínához, Iránhoz és Észak-Koreához kapcsolódnak, a NATO-tagországok és demokratikus berendezkedésű országok által végrehajtott akciókat is figyeljük és jelentjük. Tavaly egy törökországi (SZILÍCIUM) és egy vietnámi (BIZMUT) csoportra is felhívtuk a figyelmet. Idén egy olyan libanoni alapú csoport adatait részleteztük, amelynek a tevékenységét már korábban felfedtük.[36]

A Microsoft felfedezett egy korábban nem dokumentált libanoni csoportot, amelyről mérsékelt megbízhatósággal azt állapítottuk meg, hogy az iráni Hírszerzési és Biztonsági Minisztériumhoz köthető szereplőkkel működik együtt. Az ilyen fajta együttműködési vagy irányítási kapcsolat beleillik abba a 2020 vége óta megfigyelt mintázatba, mely szerint az iráni kormány külső feleket használ fel kiberműveletei végrehajtásához, feltehetően azért, hogy hitelesebben tudja tagadni ezek létezését.

A megfigyelt tevékenység keretében a POLÓNIUM célba vett két tucat izraeli szervezetet és egy nemzetközi szervezetet Libanonban 2022. február és május között, mielőtt a Microsoft felszámolta és nyilvánosságra hozta volna a csoport tevékenységét. Az izraeli szervezetek közel fele az izraeli hadiipar szereplője vagy izraeli hadiipari cégekkel áll kapcsolatban – ez azt jelzi, hogy a csoport az Irán által megcélzottakhoz hasonló szervezetek körében végez hírszerző tevékenységet, és/vagy közvetlenül Izraelt támadja.[37]

A POLÓNIUM és az iráni Hírszerzési és Biztonsági Minisztérium közötti kapcsolatokat az áldozatok közötti átfedések, valamint a felhasznált eszközök és módszerek hasonlósága alapján valószínűsítjük.

- Átfedés az áldozatok között: A Microsoft által HIGANY néven nyomon követett iráni állami hátterű, a Hírszerzési és a Biztonsági Minisztériumhoz kapcsolódó csoport korábban a POLÓNIUM számos áldozatának rendszerét feltörte, ez pedig a csoportok feladatai közötti konvergenciára, valamint az áldozatok csoportok közötti lehetséges „átadására" utal.
- Gyakori eszközök és technikák: Az MSTIC megfigyelései szerint a POLÓNIUM csoporthoz hasonlóan a DEV-0588 (más néven CopyKittens) is gyakran használja az AirVPN-t a műveleteihez, a DEV-0133 (más néven Lyceum[38]) pedig a OneDrive-ot alkalmazza C2-feladatokra és az adatok kiszivárogtatására. Az iráni állami szereplőkhöz hasonlóan a POLÓNIUM is felhőszolgáltatót használt egy izraeli légiközlekedési vállalat és egy ügyvédi iroda feltöréséhez.[39]

A POLÓNIUM több egyéni „implantátumot" is telepített felhőszolgáltatásokkal a C2- és adatkiszivárogtatási célokra – ezek közül külön említést érdemel a OneDrive és a DropBox használata. A POLÓNIUM gyakran hozott létre egyedi OneDrive-alkalmazásokat a célpontokhoz, valószínűleg a lelepleződése elkerülése érdekében.

2022 júniusára a Microsoft több mint 20, a POLÓNIUM által készített OneDrive-alkalmazást függesztett fel, értesítette az érintett szervezeteket, és egy sor biztonsági frissítést telepített a POLÓNIUM által fejlesztett eszközök karanténba zárásához.

A Microsoft sikeresen észlelte és megakadályozta, hogy a POLÓNIUM OneDrive-ot használja irányítási célokra.

Gyakorlati tanácsok

1. Frissítse a vírusirtó eszközöket[40], és gondoskodjon a felhővédelem[41] bekapcsolásáról, mivel az észlelni tudja a kapcsolódó indikátorokat.
2. A szolgáltatói kapcsolatokkal rendelkező ügyfelek számára biztosítsa az összes partneri kapcsolat felülvizsgálatát és auditját, hogy minimalizálni lehessen a szükségtelen jogosultságokat a szervezet és az általa igénybe vett szolgáltatók között.[42] Haladéktalanul vonja meg az ismeretlennek tűnő vagy még nem auditált partneri kapcsolatok hozzáférését.

További információra mutató hivatkozások

- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Észak-Korea kiberhadereje a rezsim három fő célkitűzésének szolgálatában

Az elmúlt évben Észak-Korea kiberműveleteinek iránya a kormányzat által hangoztatott globális prioritásokat tükrözte. Kim Dzsongun három célt fogalmazott meg: a védelmi kapacitás kiépítését, az ország problémás gazdasági helyzetének javítását, valamint a belföldi stabilitás biztosítását.[43] Az észak-koreai állami szereplők tevékenységeiből jól láthatóan kirajzolódik, hogy a kibertevékenységeket e három cél elérésére használják.

Az észak-koreai állami szereplők különböző taktikákkal próbáltak behatolni a repülőipari cégekhez világszerte.

Az észak-koreai állami támadócsoportok, elsősorban a CERIUM és a ZINC, különböző taktikákkal próbálnak behatolni a hadi- és repülőipari cégek hálózataira világszerte. Amellett, hogy Észak-Korea 2022 első felében minden eddiginél agresszívabb rakétateszteket folytatott, a kiberkémkedési tevékenységek ahhoz is hozzásegítették az észak-koreai kutatókat, hogy előnyt szerezzenek a saját fejlesztésű védelmi rendszerek terén, és az ellenfeleik új fejlesztéseire válaszul ellenintézkedéseket hozzanak.

Megfigyeltük, hogy a KOPERNÍCIUM világszerte különböző, kriptovalutákkal foglalkozó cégeket támadott – gyakran sikeresen –, hogy támogassa Észak-Korea nehézségekkel küzdő gazdaságát. Bár azt nem tudjuk megerősíteni, hogy a csoport a betörés után képes volt-e kicsempészni pénzt, megfigyeltük, hogy a KOPERNÍCIUM több tucat gépet fertőzött meg úgy, hogy más kriptovaluta-vállalkozásoktól érkező ajánlatnak álcázva rosszindulatú dokumentumokat küldött.

Végül a Microsoft által DEV-0215 néven regisztrált csoport az észak-koreai rezsim stabilitása és a hozzá való hűség fenntartása érdekében az észak-koreai ügyekkel foglalkozó hírügynökségeket támadott. Ezek a hírügynökségek mind Észak-Koreán belül, mind pedig a disszidens közösségekben rendelkeznek forrásokkal, amelyeket a Phenjan a létét fenyegető veszélyeknek tekint. Ezenkívül a csoport igyekezett hozzáférni koreai nyelvű keresztény csoportok hálózataihoz is, amelyek általában nyíltan Észak-Korea elleni foglalnak állást, és aktívan együttműködnek az észak-koreai disszidensekkel.

A hadi- és repülőipari vállalatok megcélzása

Az észak-koreai állami szereplők, élükön a CÉRIUM és a CINK csoporttal, jelentős erőfeszítéseket tesznek a hadi- és repülőipari cégekhez való behatolásra alkalmas taktikák kifejlesztésébe. A CÉRIUM ismételten tesztelte a dél-koreai virtuális magánhálózatokat (VPN-eket) – ehhez letöltötték a szolgáltatások kliensprogramjait, és gyenge pontokat kerestek az infrastruktúrában. Letöltötték a dél-koreai katonai és kormányzati ügyfelek által széles körben használt alkalmazásokat is, amelyekben valószínűleg sebezhetőségeket kerestek. A csoport a jelenlegi eseményeket naprakészen követve új csalidokumentumokat készített felkapott témákkal, hogy ezzel ösztönözze a célpontokat a rosszindulatú szoftverekre és hivatkozásokra kattintásra.

Mind a CINK, mind a CÉRIUM felhasználta a közösségi médiát és a pszichológiai befolyásolást a műveletei során. A CINK különösen ügyesen hozott létre hamis profilokat a LinkedInen és más szakmai közösségi oldalakon, ahol a csoport tagjai jelentős hadi- és repülőipari vállalatok toborzójának adták ki magukat. Ezeknek a profiloknak a használatával hivatkozásokat vagy rosszindulatú fájlmellékleteket küldtek a potenciális áldozatoknak, a közösségi oldalakon közvetlen üzenetben vagy e-mailben.

A vállalatok munkatársai mellett a CÉRIUM a dél-koreai hadsereg tagjait is széles körben megcélozta, különös érdeklődést mutatva a dél-koreai katonai akadémiák és a hadsereg akadémiai területen dolgozó tagjai iránt.

A kriptovaluták megcélzása a veszteségek ellensúlyozásához

Mióta 2016-ban ENSZ-szankciókat vezettek be Észak-Korea ellen, az ország gazdasága folyamatosan zsugorodik, amelyet a természeti csapások, például az árvizek[44] és aszályok [45], valamint a koronavírus-járvány 2020 eleji kirobbanása óta a határok import előli csaknem teljes lezárása tovább súlyosbítottak.[46] Bár 2022 elején Észak-Korea rövid időre megnyitotta határait a Kínával való kereskedelem előtt, hamarosan ismét határzárat vezetett be.[47] Május közepén Észak-Korea jelentette első belföldi koronavírusos esetét.[48] Azóta a kínaihoz hasonló „zéró COVID" stratégiát alkalmaz, és tömeges lezárásokkal próbálja megfékezni a vírus terjedését, amely negatívan befolyásolja Észak-Korea már jelenleg is törékeny gazdaságát.

A KOPERNÍCIUM nevű észak-koreai állami csoport a kiesett bevétel egy részét lopott pénzzel – jellemzően kriptovalutával – próbálta kipótolni bármely olyan cégtől, amelynek a hálózataira be tudott hatolni. Több tucatnyi feltört gépet találtunk az Egyesült Államokban, Kanadában, Európában és Ázsiában működő kriptovaluta-vállalatoknál. A KOPERNÍCIUM még Észak-Korea legerősebb szövetségesén, Kínán belül is feltörte kriptovalutával foglalkozó cégek számítógépeit – mind Kontinentális Kína, mind Hongkong területén. A csoport nagymértékben támaszkodott a közösségi médiára a korai felderítés és a célszemélyek megközelítése során. A csoport olyan profilokat készített, amelyek kriptovalutával foglalkozó cégek fejlesztőinek vagy felső vezetőinek adták ki magukat. Ezután kapcsolatokat építettek az iparágon belül, és a bizalom megteremtése után rosszindulatú hivatkozásokat és fájlokat küldtek.

Észak-Korea kiberhadereje a rezsim három fő célkitűzésének szolgálatában

Folytatás

A PLUTÓNIUM csoporthoz kapcsolódó szereplő zsarolószoftvert fejleszt és telepít

Észak-Koreából származó szereplők egy csoportja, amelyet a Microsoft DEV-0530 néven követ nyomon, 2021 júniusában zsarolószoftvert kezdett fejleszteni és felhasználni támadásaiban. A magát H0lyGh0st néven emlegető csoport azonos nevű zsarolóeszközt használ támadásaiban már legalább 2021 szeptembere óta, és több országban is sikeresen feltörte kisvállalkozások rendszereit.

A Microsoft értékelése szerint a DEV-0530 egy másik észak-koreai székhelyű, PLUTÓNIUM (vagy DarkSeoul, illetve Andariel) néven ismert csoporthoz kapcsolódik. Bár a H0lyGh0st zsarolószoftvert csak a DEV-0530 használja fel támadásaiban, az MSTIC kommunikációt figyelt meg a két csoport között, valamint azt is észrevette, hogy a DEV-0530 kizárólag a PLUTÓNIUM által létrehozott eszközöket is használ.

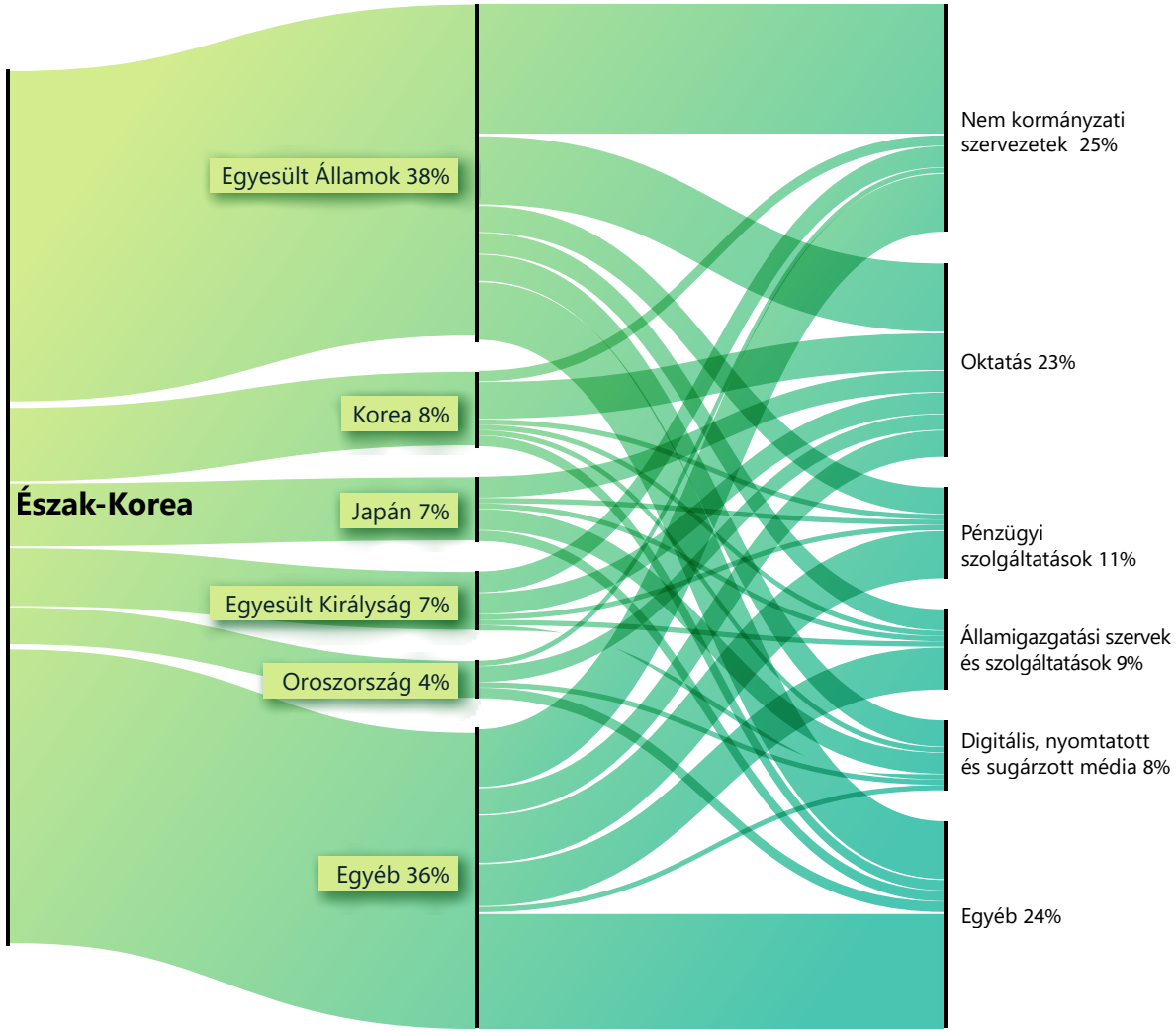
Nem biztos, hogy a DEV-0530 állami támogatással tevékenykedett. Bár elképzelhető, hogy a zsarolótámadásokat a kormány rendelte meg ugyanazért, amiért a kriptovaluta-lopást is szponzorálja, az is elképzelhető, hogy a DEV-0530 tagjait saját nyereségvágyuk motiválta. Ha ezek az észak-koreai hackerek önállóan dolgoztak, az magyarázatot kínálna arra, hogy miért nem volt tevékenységük annyira kiterjedt, mint az államilag támogatott támadások a kriptovállalatok ellen.

Észak-Koreával foglalkozó hírügynökségek, disszidensek, vallási csoportok és segélyszervezetek megcélzása

Az elmúlt évben az ország vezetője, Kim Dzsongun nyilvánosan a rakéták és a nukleáris fegyverek helyett inkább a belbiztonságra és a hűségre helyezte a hangsúlyt. Ezeket a belföldi problémákkal kapcsolatos aggodalmakat tükrözve legalább két észak-koreai állami csoport olyan ügyekre összpontosított, amelyeket a rezsim belföldi fenyegetésnek érez.

Az első csoport a Microsoft által DEV-0215 néven nyomon követett szereplő, amely az észak-koreai híreket szorosan követő hírügynökségeket vett célba. Ennek az érdeklődésnek az egyik valószínűsíthető oka az, hogy ezek a médiatermékek észak-koreai disszidensektől, Észak-Koreával szorosan együttműködő kínai állampolgároktól, sőt egyes esetekben olyan észak-koreai állampolgároktól szerzik információikat, akik különböző módszerekkel kommunikálnak a külvilággal. Az észak-koreai kormány ezekre a csoportokra a létét és fennmaradását fenyegető veszélyként tekint – különösen az Észak-Koreán belüli informátorok zavarják, akiket árulónak és kémnek tart. A DEV-0215 valószínűleg megpróbálta azonosítani ezeknek a hírügynökségeknek a forrásait, hogy kiiktathassák az információkat szivárogtató elemeket.

Észak-Korea: A leggyakrabban támadott országok és szektorok



Észak-Korea az Egyesült Államokat, Dél-Koreát és Japánt tekinti elsődleges ellenségének. Bár Oroszország régi szövetséges, ez nem akadályozza meg az észak-koreai támadókat abban, hogy célba vegyék az orosz agytrösztöket, akadémikusokat és diplomáciai tisztviselőket annak érdekében, hogy információt szerezzenek a globális ügyekkel kapcsolatos orosz álláspontról.

Észak-Korea kiberhadereje a rezsim három fő célkitűzésének szolgálatában

Folytatás

A Microsoft arra is bizonyítékot talált, hogy a DEV-0215 koreai nyelvű keresztény közösségeket is célba vett. A koreai evangéliumi keresztény egyházak általában mind az észak-koreai, mind az olyan dél-koreai kormányokkal szemben kritikusak, amelyek nyitottak a kapcsolatfelvételre Észak-Koreával. Ezek az egyházak valószínűleg segítséget nyújtanak a disszidenseknek, és egyesek humanitárius munkát folytatnak Észak-Koreával. Észak-Korea azért tekint fenyegetésként ezekre az egyházakra, mivel – bár az észak-koreai disszidensek száma a világjárvány során szinte nullára csökkent[49] – ezek a keresztény csoportok gyakran kritikus szerepet játszanak a disszidensek szökésének támogatásában. A DEV-0215 hamis dokumentumokat készített koreai nyelvű keresztény találkozókról, amelyeket csaliként használt fel a csoport megcélzásához és annak kiderítéséhez, hogy ki segít a disszidálások szervezésében.

Végül az állami, OZMIUM nevű csoport az év során folyamatos érdeklődést tanúsított a nemzetközi segélyszervezetek, köztük az Észak-Koreát korábban segítő szervezetek, iránt. Bár Észak-Korea általában elutasított minden, az országon kívülről érkező segítséget, különösen a koronavírus-járvány kitörése óta[50], lehetséges, hogy az ázsiai ország fontolóra vette a felkínált segítség elfogadását, de aggodalommal töltik el a külföldi szervezetek munkatársainak belépése miatti biztonsági kockázatok. Észak-Korea világszerte behatolhat a globális segélyszervezetek hálózataira annak eldöntése érdekében, hogy elfogadja-e ezt a fajta segítséget.

Gyakorlati tanácsok

1. Az észak-koreai állami szereplők gyakorlottak, rendíthetetlenek és kreatívak, de a szervezetek tudnak ellenük védekezni.
2. A legtöbb sikeres támadás megakadályozható az alapvető kiberhigiéniai gyakorlatok betartásával, például kétfaktoros hitelesítés használatával, vagy az ismeretlen feladótól származó virtuális környezetben való megnyitásával.

További információra mutató hivatkozások

- North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Az Észak-Korea-szakértők hosszú ideje vitatkoznak arról, hogy az észak-koreai kormány nyilvános megszólalásai a rezsim valódi céljait tükrözik-e, vagy hatásvadász céllal hangzanak el. A kibertámadások és az Észak-Korea által meghirdetett prioritások összehangja azt látszik igazolni, hogy Észak-Korea komolyan gondolja nyilvánosan meghirdetett céljait.

Kiberzsoldosok veszélyeztetik a kibertér stabilitását

Egyre bővül azon magánvállalatok köre, amelyek olyan eszközöket, technológiákat és szolgáltatásokat fejlesztenek ki és értékesítenek, amelyek lehetővé teszik az ügyfelek – gyakran kormányok – számára a hálózatokra, számítógépekre, telefonokra és internetre kapcsolódó eszközökre való betörést. Ezek a nemzetállami szereplők számára hasznos vállalatok gyakran veszélyt jelentenek a disszidensekre, az emberi jogi aktivistákra, az újságírókra, a civil szervezetek szószólóira és más magánszemélyekre. Ezek a cégeket kiberzsoldosoknak vagy magánszektorbeli támadóknak nevezzük.

Egy olyan világ, amelyben magánvállalatok készítenek és árusítanak kiberfegyvereket, sokkal veszélyesebb a fogyasztók, a különböző méretű cégek és a kormányok számára. Ezeket a támadóeszközöket olyan módokon lehet felhasználni, amelyek nem egyeztethetők össze a felelősségteljes kormányzás és a demokrácia normáival és értékeivel. A Microsoft úgy véli, hogy az emberi jogok védelme alapvető kötelezettség, és cégünk világszerte komolyan veszi a „megfigyelési szolgáltatások" visszaszorítását.

A Microsoft elemzése szerint bizonyos állami szereplők mind a demokratikus, mind a tekintélyuralmi rendszerekben kiszervezik a „megfigyelési szolgáltatások" fejlesztését és használatát. Így el tudják kerülni az elszámoltatási kötelezettséget és a felügyeletet, valamint olyan képességekhez juthatnak, amelyeket nehezen tudnának önállóan kifejleszteni.

> Ezek a kiberfegyverek olyan megfigyelési képességeket biztosítanak a nemzetállamok számára, amelyeket önállóan nem tudtak volna kifejleszteni.

A kiberzsoldosok piaca átláthatatlanul működik. Mindazonáltal továbbra is látjuk, hogy ezek a csoportok nulladik napi sebezhetőségeket, sőt kattintás nélkül kihasználható – azaz az áldozat interakcióját nem igénylő – eszközöket használnak a megfigyelési szolgáltatások biztosításához.

A Microsoft nemrégiben jelentette be egy európai magánszektorbeli támadó felfedezését, amelynek a KNOTWEED nevet adta. Az osztrák központú szereplő DSIRF néven is ismert, és több jelentés is összekapcsolta a vállalatot egy Subzero nevű kártevő eszközkészlet fejlesztésével és értékesítési kísérletével.[51] Az eszközkészlet áldozatai közé tartoznak jogi cégek, bankok, valamint stratégiai tanácsadócégek több országban, például Ausztriában, az Egyesült Királyságban és Panamában.[52]

Mivel ezek az offenzív megfigyelési képességek már csupán a védelmi és hírszerző ügynökségek titkos műhelyeiben készülnek, hanem cégek és magánszemélyek által megvásárolható kereskedelmi termékek, minden kiberfegyverekkel kapcsolatos szabályozásnak túl kell lépnie az exportkorlátozásokon. Ezek a kiberfegyverek pusztító hatásúak lehetnek.

Amikor egy kiberzsoldos kihasználja egy termék vagy szolgáltatás sebezhetőségét, az egész számítógépes ökoszisztémát kockázatnak teszi ki. A sebezhetőségek nyilvános közzétételekor a vállalatok versenyt futnak az idővel, hogy megfelelő védekezőeszközöket adjanak ki, mielőtt széles körben megindulnak a sebezhetőséget kihasználó támadások (lásd a sebezhetőségekkel kapcsolatos korábbi szakaszt). Ez egy veszélyes és nehéz körforgás mind a szoftverszállítók (amelyeknek gyorsan elő kell állnia a javítással), mind a termékeket használó fogyasztók (akiknek azonnal telepíteniük kell a javításokat) számára.

A Cybersecurity Tech Accord[53] – egy több mint 150 technológiai céget egyesítő vezető szövetség – alapító tagjaként a Microsoft kötelezettséget vállalt arra nézve, hogy nem folytat offenzív tevékenységet az interneten. Kitartunk ezen vállalásunk és a területet érinti emberi jogi felelősségvállalásunk mellett. Részt vettünk a rosszindulatú szereplők tevékenységének felszámolásában mind technikai, mind jogi síkon, hogy felhívjuk a figyelmet a kiberzsoldosok által nyújtott szolgáltatások negatív hatásaira, és a továbbiakban is meg fogjuk védeni ügyfeleinket, ha visszaélésről szerzünk tudomást.

> A kiberzsoldosok olyan megfigyelési szolgáltatásokat hoznak létre és kínálnak, amelyek technikailag kifinomultak és széles körben elérhetők, és fejlett rosszindulatú szoftvereket, valamint számos különböző technikát alkalmaznak.

Gyakorlati tanácsok a kormányok számára

1. Vezessen be átláthatósági és felügyeleti követelményeket a megfigyelési szolgáltatások terén, különös tekintettel a beszerzésre, többek között tiltsa ki ezeket a támadó szereplőket, ahogyan az Egyesült Államok is tette, ahol a Kereskedelmi Minisztérium tiltólistára teszi az érintett vállalatokat.
2. Vezessen be a munkaviszony megszűnése utáni korlátozásokat a volt dolgozók szektorbeli elhelyezkedésére vonatkozóan.
3. Igyekezzen az ügyfelek megismerését célzó kötelezettségeket bevezetni, és bátorítsa a cégeket arra, hogy tartsák fenn az emberi jogokkal kapcsolatos elkötelezettségüket.

További információra mutató hivatkozások

- Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Continuing the fight against private sector cyberweapons | Microsoft On the Issues

A kibertér békéjét és biztonságát szolgáló kiberbiztonsági normák alkalmazása

Égető szükség van egy átfogó, globális keretrendszerre, amely előtérbe helyezi az emberi jogokat, és megvédi az embereket a meggondolatlan állami magatartás okozta online veszélyektől. A folyamatban lévő ukrajnai háború fájóan ékes bizonyíték erre. A globális stratégiai erőfeszítés mellett a kormányok gyorsan cselekedve azonnali pozitív hatást érhetnek el.

Öt évvel ezelőtt a Microsoft felvetette egy „digitális genfi egyezmény" aláírását, amely előmozdítaná a különböző szektorok felelősségének és kötelezettségeinek szabályozását az online tér békéjének és biztonságának megóvása érdekében. A kibertér az államok közötti konfliktusok és verseny jól körülhatárolható és bizonytalan színterévé kezdett válni, ahol a támadások békeidőben is egyre gyakoribbá váltak.

Napjainkban még mindig egyértelmű, hogy szükség van egy ilyen keretrendszerre – ezt mi sem támasztja alá látványosabban, mint az Ukrajna elleni orosz invázió részeként indított kibertámadások. Ebben a háborúban olyan új frontvonal nyílt, amely drámaian különbözik minden eddig látottól.

A kibertér stabilitásának megteremtéséhez meg kell erősíteni és úgy kell átalakítani a globális irányítási intézményeket, hogy teljesíteni tudják ezt a feladatot. A kibertér alapvetően eltér más területektől – határok nélküli, szintetikus és nagyrészt a magánszektor tartja karban. Ez azzal jár, hogy nagyobb felelősségvállalást kell kérni a technológiai ágazat szereplőitől a saját termékeik és szolgáltatásaik, valamint az egész digitális ökoszisztéma biztonsága terén. Bár minden fronton jelentős előrelépés történt, a kihívások drámain súlyosbodtak.

A kibertér védelme érdekében meg kell dupláznunk kollektív erőfeszítéseinket. Nem vehetjük természetesnek az online térben megszokott jogokat és szabadságokat. Miközben mi a kihívásokkal küzdünk, a rosszindulatú szereplők a következő csapást tervezik mesterséges intelligencia segítségével, dezinformációt bevetve, és arra is módot találva, hogy aláássák a bimbózó metaverzum biztonságát. Az emberi jogi aktivistáknak, a technológiai iparnak és az emberi jogokat tiszteletben tartó kormányoknak együtt kell működniük a biztonságos online világ víziójának megvalósításában. Hosszú út áll előttünk, de vannak néhány dolog, amit a kormányok már ma megtehetnek a kiberbiztonsági ökoszisztéma azonnali javítása érdekében:

- A normák, törvények és következmények felsorolása a közleményekben. Az elmúlt öt év egyik jelentős előrelépését a kiberbűnözők kormányzati beazonosításának sebessége és koordinációja terén láthattuk. Az elkövetők megnevezésén és az elkövetett támadások megnevezésén felül a kormányzati nyilatkozatokban kell emelni, hogy mely nemzetközi törvényeket vagy normákat szegték meg, és hogy milyen válaszintézkedésekkel fogják erősíteni a nemzetközi elvárások betartatását.
- Tisztázza a nemzetközi jog online térre való értelmezését. Bár a kormányok egyetértenek abban, hogy a nemzetközi jog online is érvényes, nyitva állnak bizonyos kérdések azzal kapcsolatban, hogy értelmezendő ez az egyes konkrét esetekben. Ez különösen fontos az ukrajnai inváziót követően. A kormányok sokat tehetnek az elvárásaik megfogalmazása, a félreértések elkerülése, valamint a bizalomépítés terén, ha leszögezik, hogyan értelmezik a nemzetközi jog szerint kötelezettségeiket.
- Egyeztessen más érintettekkel. Ahogyan a nemzetközi fórumok továbbra is a lehető legjobb módszereket keresik a különböző érintettek hatékony bevonására, a kormányok támogathatják a megalapozott párbeszédet a több érintettet magukban foglaló közösségekkel, különösen a technológiai ágazattal, így biztosítva, hogy a párbeszéd profitálhasson a nélkülözhetetlen szakértelemmel rendelkező felek részvételéből.
- Hozzon létre egy állandó testületet a kibertérbeli felelős állami viselkedés támogatására. A nemzetközi diplomáciai fórumok felelősségteljes állami online viselkedést előmozdító munkája még sosem volt ennyire fontos. Egyértelmű, hogy szükség van egy állandó ENSZ-mechanizmusra a kibertér konfliktushelyszínként való kezeléséhez.
- Határozza meg a folyamatosan változó fenyegetések új normáit. A technológiai innovációkkal párhuzamosan a kibertérbeli fenyegetések is folyamatosan fejlődnek. Bár a nemzetközi normáknak technológiasemlegesnek kell lenniük, folyamatosan frissíteni és finomítani kell őket a fenyegetési környezet változásaira és a technológia használatára reagálva. Még ma is láthatjuk a meglévő nemzetközi keretrendszerek hiányosságainak kiaknázását. Az államoknak el kell kötelezniük magukat a digitális ökoszisztéma alapvető, ám jelenleg nem védett folyamatainak – például a szoftverfrissítési folyamatnak – a szabályozása mellett. Ráadásul egyes területek további védelmet igényelnek. Például a világjárvány során megtanultuk, az egészségügy védelmének normái alapvető fontosságúak.

A nemzetállami szereplők és támadásaik volumene és kifinomultsága is egyre nő, tarthatatlan helyzetet eredményezve.

Elengedhetetlen az azonnali cselekvés – a kormányok azonnal meghozhatnak bizonyos intézkedéseket a kiberbiztonsági ökoszisztéma fejlesztése érdekében, például egyeztetett normákat és szabályokat vezethetnek be az állam kibertérbeli viselkedésére vonatkozóan, és együttműködhetnek a szélesebb, többszereplős közösséggel a felmerülő hiányosságok kezelése érdekében.

A többoldalú intézményeket úgy átformálni, hogy választ tudjanak adni a nemzetállami kibertámadások sürgető kihívásaira.

További információra mutató hivatkozások

- A moment of reckoning: the need for a strong and global cybersecurity response | Microsoft On the Issues
- Cyberattacks targeting health care must stop | Microsoft On the Issues
- The next chapter of cyber diplomacy at the United Nations beckons | Microsoft On the Issues

Végjegyzet

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. A létfontosságú infrastruktúrát ebben a fejezetben a Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (2013. február) rendelet alapján határoztuk meg.
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

A végjegyzet folytatása

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. Különösen a ProxyShell-sebezhetőségek (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 és CVE-2021-34473) elleni javításokat kell telepíteni az Exchange-szerverekhez. Továbbá a Fortinet FortiOS SSL VPN-készülékek sebezhetőségeit is javítani kell.
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the „Subzero" state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; We unveil the state Trojan „Subzero" from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Ahogy technikai blogunkon is kifejtettük, a célpontok országa nem feltétlenül egyezik meg a DSIRF-ügyfél országával, mivel gyakori a nemzetközi célzás.
53. Kezdőlap | Cybersecurity Tech Accord (cybertechaccord.org)

Eszközök és infrastruktúra

A digitális átalakulás felgyorsulásával a digitális infrastruktúra védelme fontosabb, mint valaha.

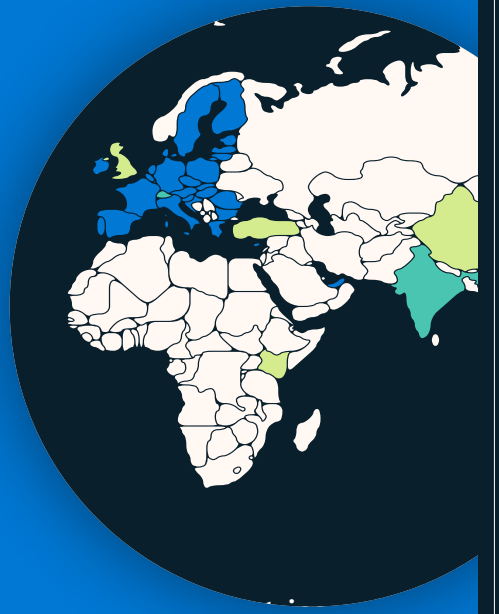
Eszközök

és infrastruktúra – áttekintés

A világjárvány és az internetre kapcsolódó eszközök digitális átalakulás gyorsításának részeként történt tömeges bevezetése nagymértékben megnövelte digitális világunk támadási felületét.

A kiberbűnözők és a nemzetállamok gyorsan kihasználták a helyzetet. Míg az informatikai hardverek és szoftverek biztonsága javult az elmúlt években, az IoT- és OT-eszközök biztonsága nem tartott lépést a fejlődéssel. A támadók sokszor ezeken az eszközökön keresztül jutnak be a hálózatokba, ahol oldalirányú mozgásba kezdenek, megvetik a lábukat az ellátási láncban, és megakadályozzák a szervezet OT-tevékenységeit.

A kormányok világszerte egyre inkább az IoT- és az OT-technológia biztonságának erősítésével próbálják javítani a létfontosságú infrastruktúra védelmét.

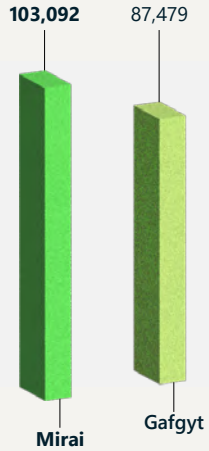


Tudjon meg többet az 59. oldalon talál

A széles körű bevezetéshez globális szinten következetes és egységes biztonsági irányelvekre van szükség.

Tudjon meg többet az 59. oldalon talál

A szolgáltatásként elérhető rosszindulatú szoftvereket az IoT- és OT-infrastruktúra és a közművek, valamint a vállalati hálózatok elleni nagy volumenű támadásokhoz használják.



További információt a 63. oldalon talál

Növekszik a távoli felügyeleti eszközök ellen irányuló támadások száma. 2022 májusában 100 milliónál is több ilyen támadást figyeltek meg – ez ötszörös emelkedést jelent csak az elmúlt évben.

További információt a 62. oldalon talál

A támadók egyre nagyobb mértékben használják ki az IoT-eszközök firmware-ének sebezhetőségeit arra, hogy beszivárogjanak a vállalati hálózatokra, és pusztító támadásokat indítsanak.

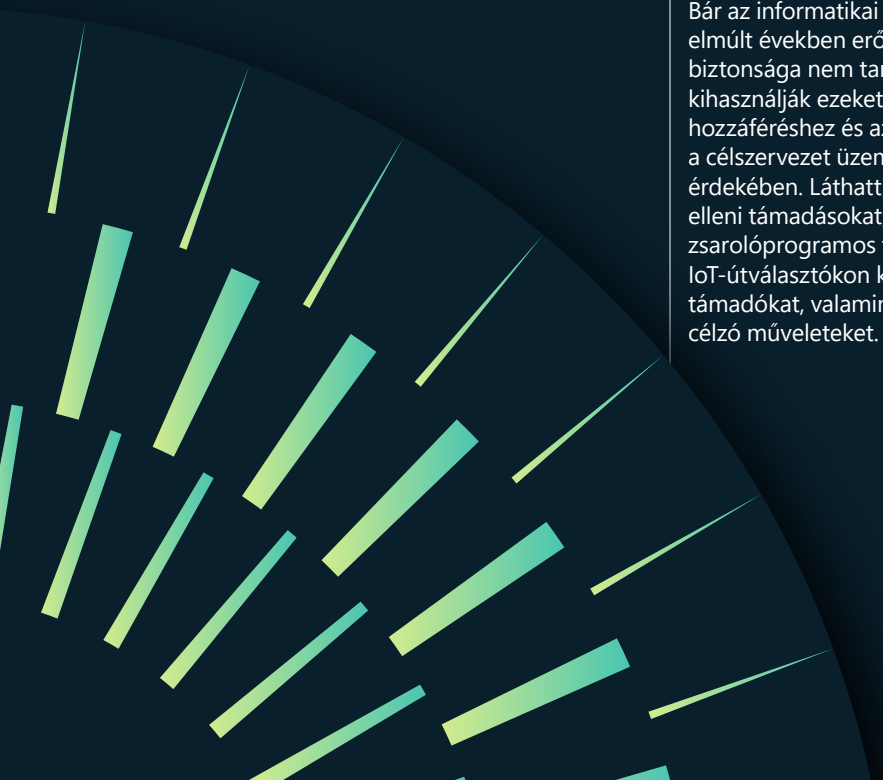
Tudjon meg többet a 65. oldalon talál

Az elemzett firmware-képek 32%-a legalább 10 ismert kritikus sebezhetőséget tartalmazott.

Tudjon meg többet a 66. oldalon talál

Bevezető

A digitális átalakulás felgyorsulásával megnövekedett a kritikus infrastruktúrára és a kiber-fizikai rendszerekre leselkedő kiberbiztonsági kockázat.



Az elmúlt néhány évben eddig példa nélkül álló változást tapasztalhattunk a digitális világban. A szervezetek folyamatosan fejlődve kiaknázzák mind az intelligens felhő, mind az intelligens peremhálózat számítási képessége terén elért fejlődést. A világjárvány hatására a vállalatok a túlélés érdekében digitalizálásra kényszerültek, és a különböző ágazatok világszerte rohamtempóban vezették be az internetre kapcsolódó eszközöket, ami miatt a digitális világ támadási felülete exponenciálisan megnőtt.

A biztonsági közösség nem tudott lépést tartani ezzel a gyors átállással. Az elmúlt év során a szervezet minden részében észleltünk az eszközök sebezhetőségeit kihasználó fenyegetéseket – a hagyományos IT-berendezésektől az üzemeltetési (OT) vezérlőkön át az egyszerű IoT-érzékelőkig. Bár az informatikai berendezések védelme az elmúlt években erősödött, az IoT- és OT-eszközök biztonsága nem tartott lépést ezzel. A támadók kihasználják ezeket az eszközöket a hálózatokhoz való hozzáféréshez és az oldalirányú mozgáshoz, valamint a célszervezet üzemeltetési műveleteinek megzavarása érdekében. Láthattunk a villamosenergia-hálózatok elleni támadásokat, az üzemeltetést megzavaró zsarolóprogramos támadásokat, a rendszerben IoT-útválasztókon keresztül a lábukat megvető támadókat, valamint a firmware-ek sebezhetőségeit célzó műveleteket.

Bár az IoT- és OT-sebezhetőségek nagy száma minden cég számára kihívást jelent, a létfontosságú infrastruktúra fokozott kockázatnak van kitéve, mivel a támadók már megtanulták, hogy a létfontosságú szolgáltatások leállítása hatékony eszköz a nyomásgyakorlásra. A Colonial Pipeline Company elleni 2021-es zsarolószoftveres támadás bizonyította, hogy a bűnözők megzavarhatják a létfontosságú szolgáltatások működését, hogy nagyobb eséllyel jussanak hozzá a követelt váltságdíjhoz. Oroszország Ukrajna elleni kibertámadásai pedig az bizonyítják, hogy egyes országok elfogadható eszköznek tartják a létfontosságú infrastruktúra elleni kibertámadásokat a katonai céljaik eléréséhez.

Azonban van remény a láthatáron. A politikai döntéshozók és a hálózatvédelemmel foglalkozó szereplők dolgoznak a létfontosságú infrastruktúra kiberbiztonságának fejlesztésén, beleértve az alapul szolgáló IoT- és OT-eszközök védelmét is. A politikai döntéshozók igyekeznek meggyorsítani azoknak a törvényeknek és szabályozásoknak az elfogadását, amelyek elmélyítik a létfontosságú infrastruktúra és eszközök kiberbiztonságával szembeni közbizalmat.

A Microsoft világszerte együttműködik a kormányokkal a kiberbiztonság erősítése érdekében, és szívesen látja a további együttműködő partnereket. Aggasztónak tartjuk azonban az inkonzisztens, egyedi vagy bonyolult követelmények bevezetésének nem várt mellékhatásait, melyek bizonyos esetekben akár a biztonság gyengülését is magukkal hozhatják, ha a szűkös biztonsági erőforrásokat a több párhuzamos minősítésnek való megfelelés köti le.

Biztonsági műveleti szempontból a hálózatvédelmi szakértők többféle megközelítést is alkalmaznak a szervezetük IoT-/OT-biztonságának fokozására. Az egyik ilyen megközelítés az IoT- és az OT-eszközök folyamatos monitorozásának megvalósítása. A másik a korai tesztelés bevezetése – azaz a hatékonyabb kiberbiztonsági gyakorlatok megkövetelése és megvalósítása magukon az IoT- és OT-eszközökön. A harmadik megközelítés olyan biztonsági monitorozó megoldás megvalósítása, amely az IT- és az OT-hálózatokra is kiterjed. Ennek az átfogó megközelítésnek további előnye, hogy elősegíti az alapvető fontosságú szervezeti folyamatokat, például hozzájárul az OT és az IT elszigetelt működésének megszüntetéséhez, ami lehetővé teszi a vállalat számára, hogy az üzleti célkitűzések teljesítése mellett erősítse a biztonságot is.

Michal Braverman-Blumenstyk
alelnök, a felhő és az AI biztonságáért felelős műszaki igazgató

A kormányok lépéseket tesznek a létfontosságú infrastruktúra biztonságának és a rugalmasságának javítása érdekében

A kormányok világszerte olyan szabályzatokon dolgoznak, amelyekkel mérsékelhető a létfontosságú infrastruktúrát fenyegető kiberbiztonsági kockázat. Sok helyen már most is érvényben vannak az IoT- és az OT-eszközök biztonságát szolgáló szabályozások. A politikai kezdeményezések globális hulláma nagyszerű lehetőséget kínál a kiberbiztonság fokozására, ám kihívásokat is rejt magában az ökoszisztémán belüli érintett felek számára.

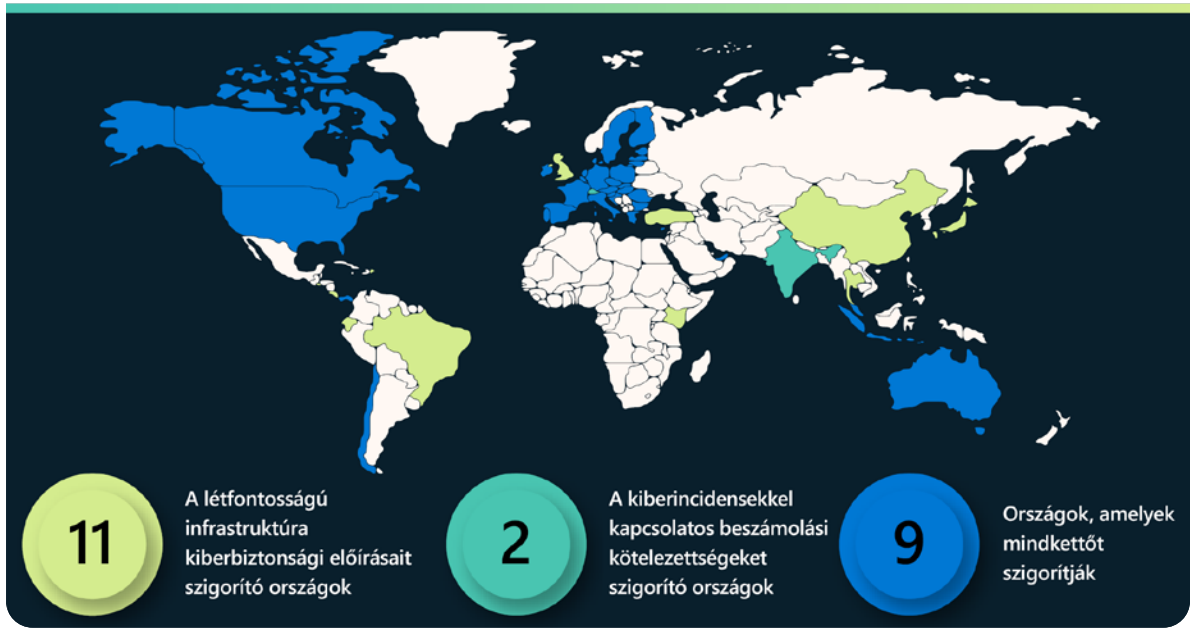
A létfontosságú infrastruktúrát fenyegető kiberkockázatok menedzselésére vonatkozó átfogó jövőkép kidolgozása kritikus fontosságú, de különösen a technológiák és a globális beszállítók közötti összefonódások mértéke, a technológia használatának kiterjedtsége és az ezzel járó kockázatok, valamint a rövid és hosszú távú stratégiák kidolgozásába való befektetés szükségessége miatt igen összetett feladat. A megfelelő hatókörű, az iteratív tanulást és fejlődést elősegítő, valamint a globális, ágazatokon átívelő interoperabilitást támogató szabályzatok azonban lehetővé teszik az összetettség menedzselését, és biztonságtudatosabb digitális átalakulást tesznek lehetővé. Azonban a széttagolt jogalkotási megközelítés egymással átfedésben lévő és inkonzisztens szabályozási követelmények meghatározásához vezethet. Ez negatívan befolyásolhatja az erőforrások felhasználását, és végső soron aláásható a biztonsági célkitűzéseket. Előfordulhat például, hogy a vállalatoknak az innovációtól és a biztonságtól kell átcsoportosítaniuk erőforrásokat, hogy teljesíteni tudják a formális megfelelőségi követelményeket.

A Microsoft világszerte partnerségre törekszik a kormányokkal, hogy segíthessen hatékony kiberbiztonsági szabályokat kidolgozni a létfontosságú infrastruktúra védelmére, információkat biztosíthasson a kihívásokról és a lehetőségekről, valamint támogathassa a kollektív kockázatkezelési erőfeszítéseket.

A létfontosságú infrastruktúrát fenyegető kiberbiztonsági kockázatok menedzselésére irányuló szakpolitika alakulása

Az elmúlt évben több joghatóság – köztük Ausztrália, Chile, az Európai Unió (EU), Japán, Szingapúr, az Egyesült Királyság és az Egyesült Államok – dolgozott ki, módosított vagy vezetett be ágazatközi vagy ágazatspecifikus kiberbiztonsági követelményeket.[1] Számos ilyen országban – és máshol, például Indiában[2] és Svájcban[3] – már bevezettek, vagy éppen most dolgoznak ki a kiberbiztonsági incidensek bejelentésére vonatkozó előírásokat a létfontosságú infrastruktúra szereplői és az alapvető szolgáltatók számára.[4]

Az elmúlt évben Ausztráliában, az EU-ban, Indonéziában és az Egyesült Államokban láthattunk néhány figyelemre méltó fejleményt a szabályozások területén. Ausztrália két olyan törvényt is bevezetett, amelyek segítenek mérsékelni az ágazatközi, létfontosságú infrastruktúrát fenyegető kiberbiztonsági kockázatokat. A törvények többek között új szektorokat emeltek be a létfontosságú infrastruktúrát alkotó ágazatok közé, előírják a kockázatmenedzselési tervek készítését, kötelezővé teszik a kiberbiztonsági incidensek jelentését, valamint felhatalmazzák a kormányt arra, hogy beavatkozzon, amennyiben úgy ítéli meg, hogy a létfontosságú infrastruktúra valamely szolgáltatója nem hajlandó vagy nem képes megfelelő választ adni egy incidensre.



Az EU módosítást dolgozott ki a 2016-os NIS irányelvéhez, amely keretrendszert biztosít az EU tagállamai számára a technológiai szolgáltatások, valamint a gazdaság és a társadalom működése szempontjából kritikus fontosságúnak ítélt szolgáltatások és termékek szabályozására. Az előterjesztett NIS 2 olyan módosításokat tartalmaz, amelyek megteremtik az új kritikus digitális infrastruktúra kategóriát, szigorítják a kiberbiztonsági incidensek jelentésének követelményeit, valamint további kiberbiztonsági kockázatkezelési követelményeket írnak elő. Az EU a pénzügyi ágazat digitális működési rezilienciájáról szóló törvényhez (DORA) is kidolgozott egy módosítást, amelyben a pénzügyi szolgáltatási szektorban használt infokommunikációs technológiákkal kapcsolatos új követelményeket javasol.

Májusban Indonézia kiadta a létfontosságú információs infrastruktúra („IIV") védelméről szóló elnöki rendeletet, amely 2024 májusában lép hatályba, és többek között kiterjed az energetikai, a közlekedési, a pénzügyi és az egészségügyi szektorra. Indonézia célja a rendelettel az, hogy biztosítsa az IIV folytonos működését, megakadályozza a kibertámadásokat, valamint hogy javítsa a kiberincidensekre való felkészültséget. Az IIV-szolgáltatók számára kötelező lesz biztonságos és megbízható védelmet alkalmazni, hatékony kiberkockázat-kezelési megoldásokat bevezetni, valamint jelenteni a kiberkockázati felmérések eredményét a megfelelő kormányzati szerveknek. A rendelet egy olyan előírást is tartalmaz, amely szerint a kiberincidensekről 24 órán belül jelentést kell tenni.

A kormányok lépéseket tesznek a létfontosságú infrastruktúra biztonságának és a rugalmasságának javítása érdekében

Folytatás

Az Egyesült Államok kongresszusa elfogadott egy törvényt, amely felhatalmazást ad a Cybersecurity and Infrastructure Security Agency (CISA) számára olyan szabályozás bevezetésére, amely előírja, hogy a létfontosságú infrastruktúrát alkotó szolgáltatóknak jelenteniük kell a kiberincidenseket; a US Transportation Security Administration (TSA) pedig új ágazatspecifikus kiberbiztonsági előírásokat adott ki a szállítmányozás területén. 2021-ben a TSA a Colonial Pipeline Companyt ért zsarolótámadásra reagálva két biztonsági irányelvet adott ki a veszélyes folyékony anyagokat továbbító és földgázvezetékek üzemeltetőinek:

- Az első irányelv értelmében az üzemeltetőknek ki kell jelölniük egy kiberbiztonsági koordinátort, 12 órán belül jelenteniük kell be a kiberincidenseket, és fel kell mérniük rendszerük sérülékenységeit.
- A második, a TSA által 2022-ben átdolgozott irányelv azt írja elő a vállalatok számára, hogy meghatározott kockázatcsökkentő intézkedéseket kell megvalósítaniuk a zsarolótámadások és az IT- és OT-rendszereket fenyegető más ismert fenyegetések elleni védekezéshez, valamint 30 napon belül kiberbiztonsági vészhelyzeti intézkedési és reagálási tervet kell készíteniük, továbbá évente át kell esniük a kiberbiztonsági architektúra felülvizsgálatán.

A csővezetékek üzemeltetőire vonatkozó rendeleteire alapozva a TSA még 2021-ben két további biztonsági irányelvet vezetett be, amelyek a kiberbiztonsági követelményeket a vasúti teher- és személyszállítási szolgáltatókra és vasúti szállítási rendszerekre is kiterjesztik. Az irányelvek előírják az érintett üzemeltetők számára, hogy kijelöljenek egy kiberbiztonsági koordinátort, 24 órán belül jelentsék a kiberbiztonsági incidenseket, dolgozzanak ki és vezessenek be egy cselekvési tervet a kiberbiztonsági incidensek esetére, továbbá hogy végezzenek kiberbiztonsági sebezhetőségi felmérést. A TSA ezzel egyidejűleg azt is bejelentette, hogy módosította repülésbiztonsági programjait, és megköveteli a légitársaságoktól és a repülőterek üzemeltetőitől az első két rendelkezés végrehajtását, azaz egy koordinátor kijelölését az incidensek 24 órán belüli jelentését.

Az IoT- és az OT-eszközök biztonságát érintő szabályozások fejlődése

Több tucat ország kormánya dolgozik aktívan az információs és kommunikációs technológiai (ICT) termékek és szolgáltatások – többek között az IoT- és az OT-eszközök – kiberbiztonságának előmozdítását szolgáló követelményeken. Az ICT-termékek és -szolgáltatások összefüggésében a legnagyobb aggodalom a szoftveres ellátási lánc biztonságát és az IoT-biztonságot övezi.

- Az Európai Bizottság által kidolgozott kiberreziliencia-törvény az önálló szoftverekre és a csatlakoztatott eszközökre és a kapcsolódó szolgáltatásokra vonatkozó kiberbiztonsági előírásokat javasol.[5] A szoftvergyártók szempontjából releváns gyakorlatok közé tartozik a biztonságos szoftverfejlesztési életciklus[6] és a szoftveres anyagjegyzék biztosítása.[7] A javaslat értelmében a csatlakoztatott eszközökre új biztonsági követelmények vonatkoznának, és az összes gyártó számára kötelező lenne a sérülékenységek összehangolt jelentésére[8] szolgáló folyamatok menedzselése a kiadott termékeikkel kapcsolatban.

A döntéshozók figyelme kiterjed az IoT-eszközök és a hálózatra kapcsolódó OT-eszközök számának folyamatos emelkedésére is.

- Az Egyesült Királyságban a termékbiztonsági és távközlési infrastruktúrákra vonatkozó törvény tervezete megköveteli a fogyasztók által összekapcsolható termékek – például az okostévék – gyártóitól, hogy ne használjanak a kiberbűnözők számára könnyű célpontot jelentő alapértelmezett jelszavakat, vezessenek be sebezhetőség-közzétételi irányelveket (például biztosítsanak lehetőséget a biztonsági hiányosságokkal kapcsolatos értesítések fogadására), valamint átláthatóan adjanak információt arról, hogy legalább mennyi ideig fognak biztonsági frissítéseket nyújtani a termékhez.[9]
- Az EU-ban az új biztonsági előírásokat és követelményeket több jogi eszközzel is megvalósítják, beleértve egy felhatalmazáson alapuló jogi aktust a rádióberendezésekről szóló irányelvhez, amely a vezeték nélküli eszközökre vonatkozik, és a hálózati rugalmasság javítását, a fogyasztói adatok védelmét, valamint a pénzügyi csalások kockázatának csökkentését szolgálja.[10] Továbbá bevezetésre kerülhet egy felhőtanúsítási rendszer[11] is, amely az 2019 EU-s kiberbiztonsági törvény[12] nyomán jelenleg kidolgozás alatt áll.

Az egységesség igénye

Sok esetben a régiókat, a szektorokat, a technológiákat és a működési kockázatkezelési területeket lefedő tevékenységeket egyszerre próbálják szabályozni, ami ahhoz vezethet, hogy az iránymutatásokat követni próbáló vagy a megfelelőség demonstrálására törekvő vállalatoknak inkonzisztens vagy egymást átfedő hatókörű és követelményeket támasztó bonyolult szabályrendszereknek kell megfelelniük. Az IoT általánosan elfogadott definíciója hiányában a hatókör meghatározása különösen nagy kihívást jelent az IoT- és az OT-eszközök szabályozása terén. A fenti példákban a szabályok a „csatlakoztatott termékekre és kapcsolódó szolgáltatásokra", a „fogyasztó által összekapcsolható termékekre" és a „vezeték nélküli eszközökre" vonatkoznak. Ugyanakkor számos kormány célja, hogy hatékonyabb értékelési rendszereket vezessenek be annak pontosabb megértéséhez, hogy a vállalatok és a termékek hogyan teljesítik a jelenlegi, felmerülő és változó követelményeket. Ezeknek a trendeknek az összeolvadásával növekszik a komplexitás. Bizakodásra ad okot, hogy az EU-s kiberreziliencia-törvény tárgyalása során feltett kérdések azt is vizsgálták, hogy az új szabályozások hogyan érinthetik a jelenlegi kiberbiztonsági szabályozást, mivel ez az ütköző kiberbiztonsági intézkedések elkerülésének szándékát jelzi.

Az iteratív, kockázatalapú és eredmény-, illetve folyamatorientált (nem pedig implementációspecifikus) megközelítések elősegítik a kiberbiztonság erősítését és a folyamatos fejlődést. Hasonlóképpen az ágazatok, a régiók és a szabályozási területek közötti együttműködés lehetővé tétele egységesen elősegítheti a jobb kiberbiztonságot az egymással összefonódó globális ellátási láncokban.

A kormányok lépéseket tesznek a létfontosságú infrastruktúra biztonságának és a rugalmasságának javítása érdekében

Folytatás

A különböző régiókban, ágazatokban és tematikus területeken egyre bonyolultabb szabályozásokat dolgoznak ki a létfontosságú infrastruktúra kiberbiztonságának erősítéséhez. Ez a nagyszerű lehetőségek mellett jelentős kihívásokat is eredményez. A digitális átalakulás és az egész ökoszisztémára kiterjedő biztonság jövője szempontjából döntő fontosságú, hogyan folytatják a szabályozások kidolgozását a kormányok.

A szoftverellátási lánc biztonságába és a Zero Trust architektúrába való ökoszisztémaszintű befektetés gyorsítása

Az Egyesült Államok kiberbiztonság javításáról szóló 14028-as elnöki rendelete (EO) hozzájárult ahhoz, hogy a Microsoftnál felgyorsuljanak azok a folyamatban lévő kezdeményezések, amelyek a saját és az ökoszisztémaszintű ellátási lánc biztonságába, valamint az abba történő befektetésre irányultak, hogy lehetővé tegyük az ügyfeleink számára a Zero Trust-célok megvalósítását.

Régóta úgy gondoljuk, hogy a szoftveres ellátási lánc fejlesztése megköveteli a tanulságok és a bevált módszerek megosztását, amely felé az első lépést 15 évvel ezelőtt, a Microsoft biztonságos fejlesztési módszertanának kiadásával tettük meg.

Emellett szorosan együttműködünk a National Cybersecurity Center of Excellence központtal, hogy bemutassuk a Zero Trust architektúra helyi és felhőtechnológiákban való alkalmazásának különböző megközelítéseit, valamint új termékfunkciókat dolgozzunk ki, például az adathalászatnak ellenálló hitelesítést a hibrid és többfelhős környezetekhez.

Napjainkban az EO követelményein túlmutatóan tanúsítjuk a szoftveres ellátási lánc biztonságával kapcsolatos követelmények betartását, és kétféleképpen biztosítjuk a szoftveres anyagjegyzékre (SBOM) vonatkozó információkat:

1. Először is megosztjuk SBOM-generátor eszközünk nyílt forráskódú változatát, amelyet úgy alakítottunk ki, hogy könnyen integrálható legyen a CI/CD-pipeline-okba, és támogatja a buildek készítését Windows, Linux, Mac, iOS és Android platformra.[13]
2. Ezenkívül hozzájárulunk az ellátási lánc integritására, átláthatóságára és megbízhatóságára (SCITT) vonatkozó iparági szabványok kidolgozásához. Ez lehetővé fogja tenni az ellátási lánc igazolható adatainak automatikus cseréjét, beleértve az olyan műtermékeket is, amelyek bizonyítják a követelmények – például az EO szoftveres ellátási láncra vonatkozó javaslatai nyomán bevezetett előírások – teljesítését.

Gyakorlati tanácsok

1. A többoldalú intézményeket úgy átformálni, hogy választ tudjanak adni a nemzetállami kibertámadások sürgető kihívásaira.
2. Dolgozzon ki olyan kiberbiztonsági irányelveket, amelyek konzisztensek és kompatibilisek a különböző régiók, szektorok és tematikus területek között.

További információra mutató hivatkozások

- Continued investments in supply chain security in support of the cybersecurity Executive Order | Microsoft Tech Community
- US Government sets forth Zero Trust architecture strategy and requirements | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Supply Chain Integrity, Transparency, and Trust | github.com
- Implementing a Zero Trust Architecture | NCCoE (nist.gov)

Az IoT és az üzemeltetési technológia (OT) kiszolgáltatottsága: trendek és támadások

Egyre nagyobb mértékben összekapcsolódó digitális világunkban az eszközök gyorsan érkeznek az internetre, nagyobb rendszerekkel kommunikálnak, adatokat gyűjtenek, és korábban rejtve maradt területeket tesznek láthatóvá. Ez a vállalatok mellett a kibertámadók számára is nagy lehetőségeket kínál, ami ahhoz vezetett, hogy mára a kiberbűnözés több milliárd dolláros iparággá és kockázattá nőtte ki magát.

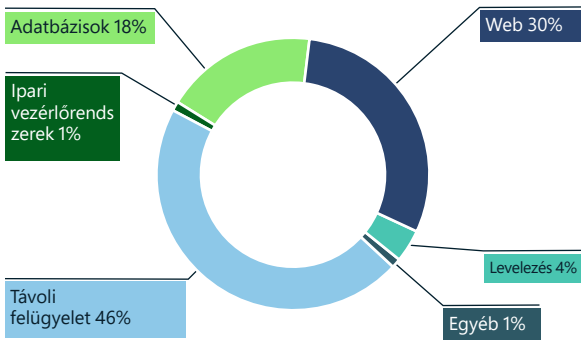
Az IoT-eszközök – a nyomtatóktól a webkamerákon át a klímavezérlőkig és az épületek beléptetőrendszereiig – egyedi biztonsági kockázatot jelentenek az egyénekre, a szervezetekre és a hálózatokra. Sok vállalat számára ezek az eszközök létfontosságúak, ám gyorsan kockázattá és biztonsági problémává válhatnak. Az IoT-megoldások gyors bevezetése szinte minden iparágban növelte a támadási vektorok számát és a vállalatok kitettségét.

A szolgáltatásként kínált rosszindulatú szoftverek nagyszabású támadásokat tesznek lehetővé a közösségi infrastruktúra és a közművek (többek között a kórházak, az olaj- és gázhálózatok, az elektromos hálózatok, a közlekedési szolgáltatások és a létfontosságú infrastruktúra más részei), valamint a vállalati hálózatok ellen egyaránt. A támadóknak jelentős kutatási erőfeszítéseket kell tenniük az üzemeltetési környezetek és a beágyazott IoT- és OT-eszközök sebezhetőségeinek és konfigurációjának feltárásához és kihasználásához.

Az IoT-eszközök egyedi biztonsági kockázatot jelentenek, mivel belépési és sarokpontokként használható a hálózatok támadása során. IoT-eszközök millió futnak javítás nélkül vagy nyilvánosan elérhető módon.

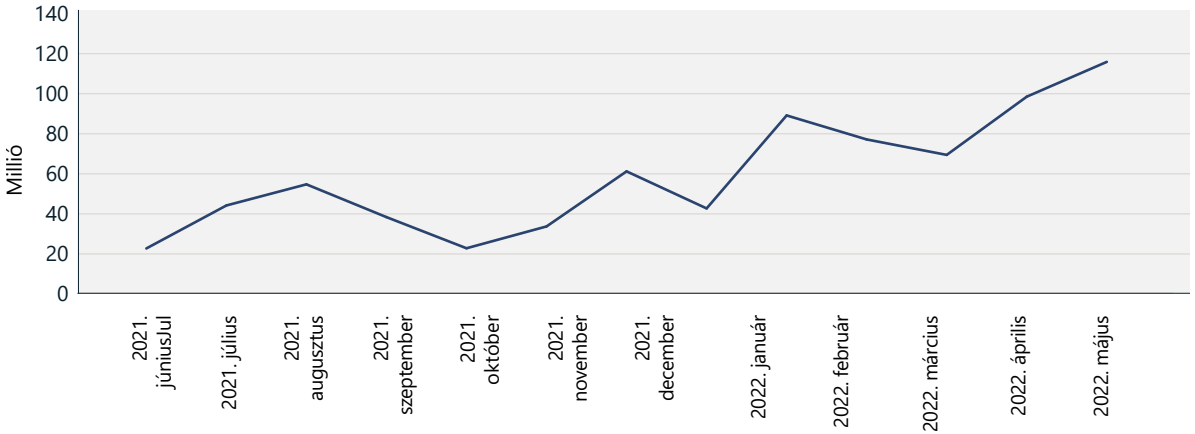
A nyilvánosan elérhető eszközök felfedezhetők a nyitott hálózati portokat figyelő szolgáltatásokat felderítő internetes keresőeszközökkel. Ezeket a portokat gyakran az eszközök távoli menedzselésére használják. Megfelelő védelem hiányában a nyilvánosan elérhető IoT-eszközökre támaszkodva a jogosulatlan felhasználók távolról elérhetik ezeket a portokat, és hozzáférést szerezhetnek a vállalati hálózat más rétegeihez. Számos különböző támadótól láthattuk, hogy megkísérlték kihasználni az interneten nyilvánosan elérhető olyan eszközök sebezhetőségeit, mint a kamerák, az útválasztók vagy éppen a termosztátok. A kockázatok ellenére azonban több millió eszköz továbbra is javítás nélkül vagy nyilvánosan hozzáférhető módon üzemel.

Az IoT-/OT-támadási típusok összefoglalása



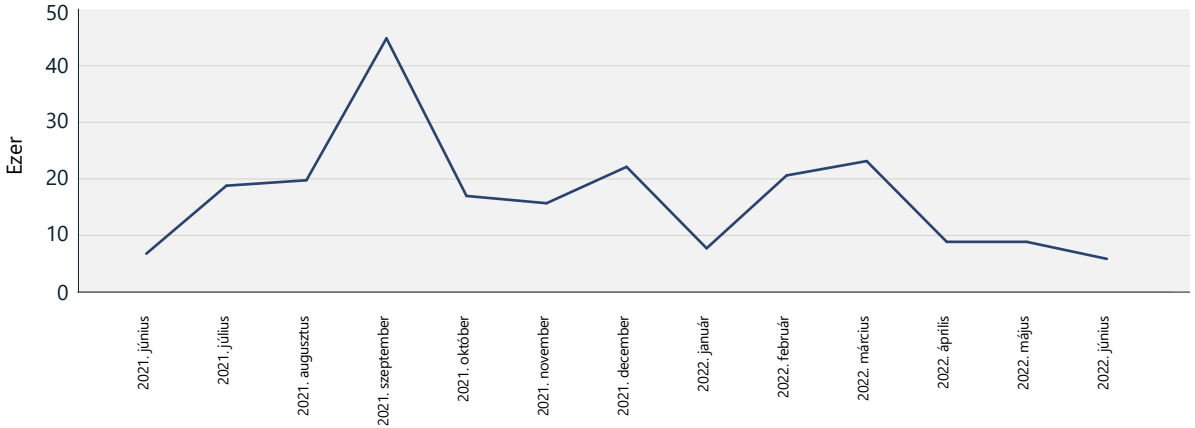
A MSTIC érzékelőhálózaton keresztül megfigyelt támadástípusok. A leggyakoribbak a távoli menedzsmenteszközöket érő, a weben keresztüli, valamint az adatbázisok elleni (találgatásos vagy biztonsági rést kihasználó) támadások.

Távoli menedzsmenteszközök elleni támadások



A távfelügyeleti portok elleni támadások számának az MSTIC érzékelőhálózaton keresztül észlelt növekedése az idők során.

Weben keresztüli támadások IoT- és OT-eszközök ellen



A webes támadások mennyiségének időbeli alakulása az MSTIC érzékelőhálózatán keresztül gyűjtött adatok alapján. Folytatódik a közvetlenül a hálózatra csatlakozó eszközök számának csökkenése, így a támadók egyre kevésbé tudják őket szkenneléssel megtalálni.

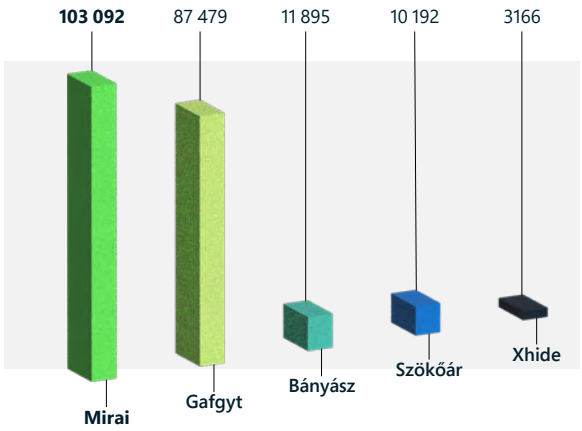
Az IoT és az üzemeltetési technológia (OT) kiszolgáltatottsága: trendek és támadások

Folytatás

A rosszindulatú szoftverek megújulása

A kiberbűnözői csoportok fejlődésével a rosszindulatú szoftverek telepítése és a célpontok kiválasztása is átalakult. Az elmúlt évben jelentős csökkenést figyeltünk meg a gyakori IoT-protokollok – például a Telnet – elleni támadások terén, néhány esetben akár 60 százalékos csökkenésre is sor került. Ugyanakkor a kiberbűnözői csoportok és a nemzetállami szereplők is új célokra kezdték el felhasználni a botneteket. A kártevők (például a Mirai) fennmaradása rávilágít a támadások moduláris természetére és a meglévő fenyegetések alkalmazkodóképességére.

Leggyakrabban észlelt IoT-kártevők



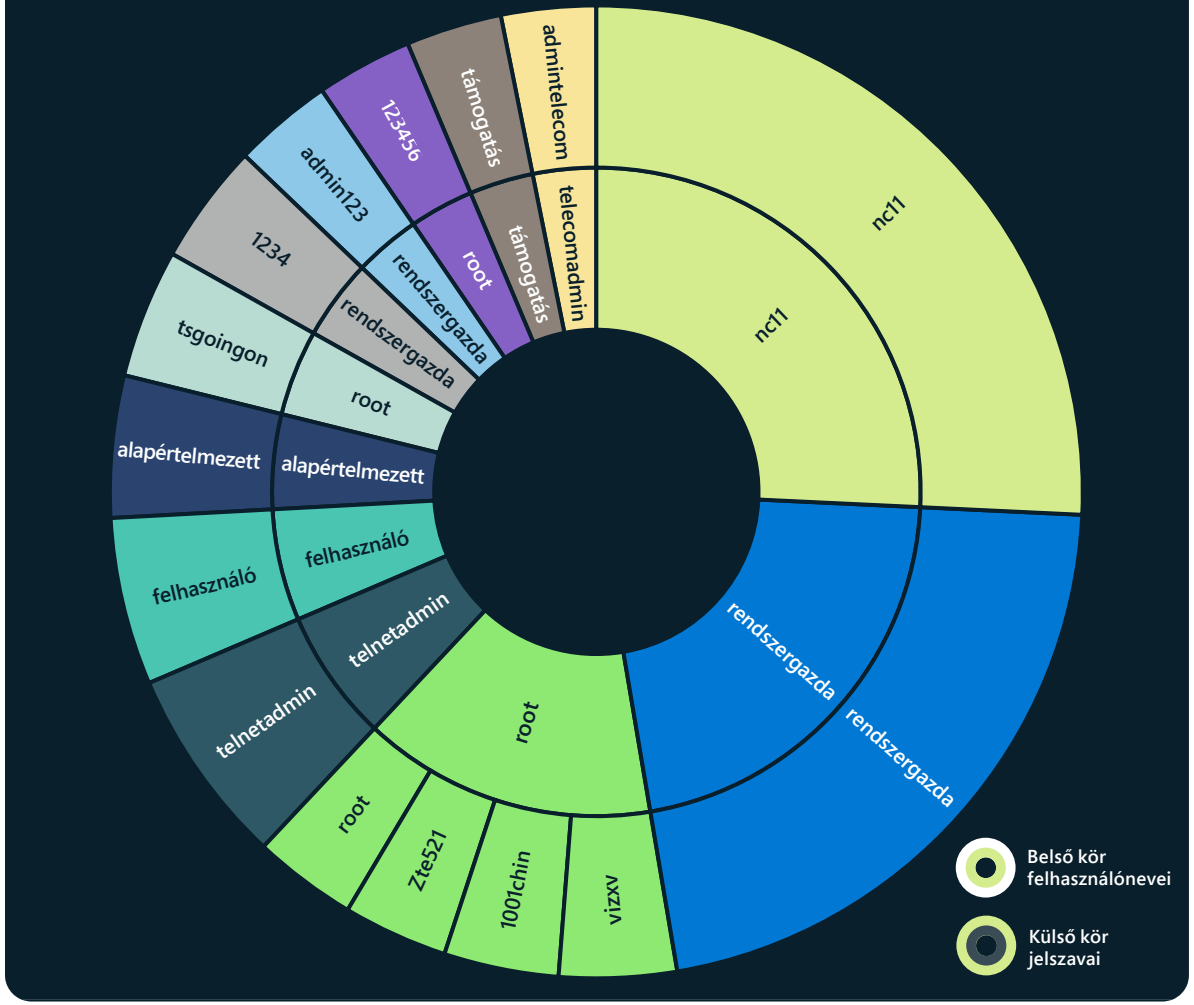
A Mirai továbbfejlődött, és már az IoT-eszközök széles körét képes megfertőzni, beleértve az IP-kamerákat, a biztonsági kamerák digitális videorögzítőit és az útválasztókat. A támadási vektor megkerülte a régi biztonsági ellenőrzési pontokat, és veszélyt jelent a hálózaton belüli végpontok számára a további sebezhetőségek kihasználásával és oldalirányú terjedéssel. A Mirait többször is átalakították, és a különböző architektúrákra szabott változatai jelentek meg, amelyek ismert és nulladik napi sebezhetőségek kihasználásával fertőznek meg új támadási vektorokat.

A Mirai 32 és 64 bites x86 CPU-architektúrák elleni használata növekedett az elmúlt évben, és a rosszindulatú szoftver új képességeket is kapott, amelyeket az nemzetállami és a bűnözői csoportok is gyorsan használatba vettek. A nemzetállami támadók most a meglévő botnetek új variánsait aknázzák ki az ellenfeleikkel szemben indított elosztott szolgáltatásmegtagadásos (DDoS) támadások során.

Mivel az IoT-eszközök elleni támadásokból származó bevétel 2022-ben visszaesett, megfigyeltük, hogy számos támadócsoport sebezhetőségek – például a Log4j és a Spring4Shell – kihasználásával visznek be rosszindulatú tartalmat az eszközökre (például szerverekre), amelyekkel megfertőzik és DDoS-támadásokhoz használt kiterjedt botnetekbe tagolják be őket. A sérülékeny IoT-eszközökhöz kifejlesztett rosszindulatú szoftverek újfajta használata komoly következményekkel jár mind a vállalatok, mind az országok számára, mivel az oldalirányú mozgás során további, újabb rosszindulatú tartalmak elhelyezésére alkalmas backdoorok és a hálózatra kapcsolódó más eszközök felfedezését teheti lehetővé.

Számos ipari vezérlőrendszer protokolljait nem monitorozzák, így sebezhetők az OT-specifikus támadásokkal szemben. Ez fokozott veszélyt jelent a létfontosságú infrastruktúrára.

A felhasználónév-jelszó párok relatív gyakorisága az IoT-/OT-eszközök körében 45 napnyi érzékelőjelben



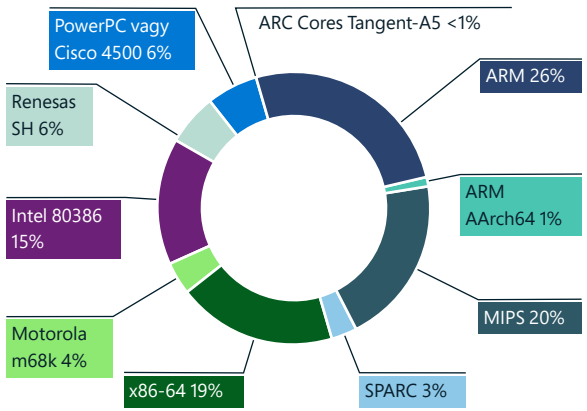
A gyakori felhasználónév-jelszó párok használata növeli a sikeres támadás esélyét. Egy több mint 39 millió IoT- és OT-eszközt tartalmazó minta alapján az azonos felhasználónevet és jelszót használó eszközök aránya 20 százalék körül van.

Az IoT és az üzemeltetési technológia (OT) kiszolgáltatottsága: trendek és támadások

Folytatás

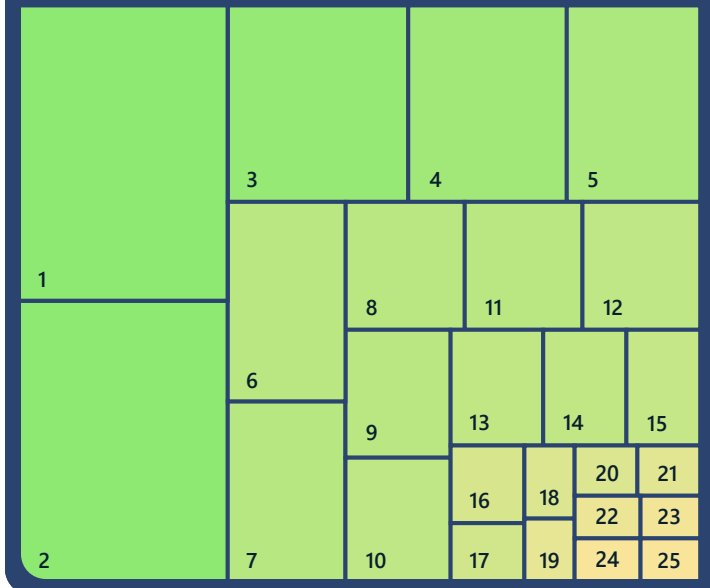
Bár a gyenge konfigurációk és az alapértelmezett hitelesítő adatok továbbra is kockázatot jelentenek a hálózatokra nézve, a Microsoft számos olyan webes támadási kísérletet észlelt, amely a HTTP-protokollt használta. Azt figyeltük meg, hogy ezekhez a webes szolgáltatások elleni támadásokhoz régi botneteket használtak. Mindeközben csökkent a nyílt Telnet-portok száma az interneten, ami mindenképpen pozitív fejlemény a hálózatbiztonság terén, mivel ezzel a korábban az eszközökre kockázatot jelentő botnetek is visszaszorulnak. A nyílt Telnet-portok számának csökkenése ellenére azonban továbbra is megfigyelhető a botnetek jelenléte az érzékelőhálózatokban.

IoT-kártevők CPU-architektúra szerinti eloszlása



A Microsoft megfigyelései szerint az ARM architektúrájú IoT-eszközöket célozta meg a legtöbb rosszindulatú szoftver, majd ezt követte a sorban a MIPS, az X86-64 és az Intel 80386.

Az ipari vezérlőrendszerek protokolljaink elterjedtsége



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Az ipari vezérlőrendszerek protokolljaink sebezhetőségei

Megvizsgáltuk a felhőhöz kapcsolt érzékelőktől származó OT-adatokat, és feltártuk az ipari vezérlőrendszerekben (ICS) leggyakrabban használt protokollokat. Ezek a protokollok betekintést nyújtanak az eszközök és támadási felületeik természetébe. Ez különösen fontos a létfontosságú infrastruktúra biztonsága szempontjából. Néhány fontos tanulság:

1. A protokollok többsége zárt fejlesztésű, így a szabványos IT-monitorozó eszközök nem fognak megfelelő biztonsági rálátást elérni ezeknek az eszközöknek és protokolloknak a körében. Ennek eredményeképpen a hálózatok továbbra is monitorozás nélkül maradnak, így sebezhetőbbek lesznek az OT-specifikus támadásokkal szemben.
2. Számos különböző szállítóspecifikus protokoll van használatban. Ez azt jelenti, hogy a szállítóspecifikus biztonsági megoldások nem képesek megfelelően lefedni a teljes hálózatot. Microsoft a szállítófüggetlen megközelítést részesíti előnyben, hogy eszközök széles köre számára biztosíthasson biztonsági lefedettséget.
3. A vállalatoknak gondoskodniuk kell, hogy ezek a hálózatukon belül használt protokollok ne legyenek közvetlenül hozzáférhetők az interneten keresztül. A nyilvános hozzáférhetőség a protokollok sebezhetőségei és nem biztonságos jellege miatt jelentős biztonsági kockázatot rejt magában.

Az olyan rosszindulatú szoftverek, mint a Mirai továbbra is velünk vannak, mivel folyamatosan új képességeket fejlesztenek hozzájuk, és kiberbűnözői, valamint nemzetállami csoportok is előszeretettel alkalmazzák őket, a meglévő botnetek új variánsait külföldi ellenfelekkel szembeni DDoS-támadásokhoz használva.

Gyakorlati tanácsok

1. Biztosítsa az eszközök ellenálló képességét a javítások alkalmazásával, valamint az alapértelmezett jelszavak és az alapértelmezett SSH-portok módosításával.
2. Csökkentse a támadási felületet azáltal, hogy lezárja a szükségtelen internetkapcsolatokat és nyílt portokat, a portok letiltásával korlátozza a távoli hozzáférést, elutasítja a távoli hozzáférési kísérleteket, valamint VPN-szolgáltatásokat használ.
3. Használjon IoT-/OT-kompatibilis hálózatészlelési és reagálási (NDR) megoldást, valamint biztonsági információ- és eseménykezelő (SIEM)/ biztonsági orkesztrációs és válaszautomatizáló (SOAR) megoldást az eszközök rendellenes vagy nem engedélyezett viselkedésének – például az ismeretlen hosztokkal való kommunikációnak – az észleléséhez.
4. Bontsa szegmensekre a hálózatot, hogy korlátozza az esetleges támadók oldalirányú mozgását, illetve a kezdeti behatolás után a eszközök feltörését. Az IoT-eszközöket és az OT-hálózatokat tűzfalakkal kell elválasztani a vállalati IT-hálózatoktól.
5. Gondoskodjon róla, hogy az ICS-protokollok ne legyenek közvetlenül hozzáférhetők az internetről.

Hackertámadások az ellátási láncok és a firmware-ek ellen

Szinte minden internetre csatlakozó eszközön található firmware, azaz az eszköz hardverébe vagy áramköri lapjára beágyazott szoftver. Az elmúlt néhány év során egyre többször láttuk, hogy a támadók a firmware-t vették célba pusztító támadásaik indításához. Mivel az eszközök firmware-e várhatóan továbbra is értékes célpontot fog jelenteni a támadók számára, a vállalatoknak védekezniük kell a firmware feltörése ellen.

A firmware biztosítja az eszközök elsődleges funkcióit, például a hálózati csatlakozást vagy az adatok tárolását. Firmware-t találunk az útválasztókban, a kamerákban, a televíziókban és más, nagyvállalati környezetben használt (IoT) eszközökben, akárcsak a létfontosságú infrastruktúra részét képező vezérlőberendezésekben (OT). Történelmileg úgy alakult, hogy a firmware-t nem biztonságos kódban írják, ami jelentős sebezhetőségekhez vezetett, amelyeket kihasználva átvehető az irányítás az eszköz felett, vagy rosszindulatú kód helyezhető el a firmware-ben.

Ezek a kockázatok az ellátási lánc esetén továbbiakkal egészülnek ki. A legtöbb eszközben több gyártót szoftveres és hardveres komponenseit is megtaláljuk, valamint gyakori a nyílt forráskódú függvénytárak használata is. Sok esetben az eszközök üzemeltetőinek nincs rálátásuk a hardveres és szoftveres anyagjegyzékekre (H/SBOM), amely alapján kiértékelhetnék a hálózatuk részét képező eszközök ellátási láncból eredő kockázatait. 2020 júniusában sebezhetőségeket találtak egy olyan hálózati stackben, amelyet számos különböző gyártó használt, így a probléma több százmillió IoT-eszközt érintett a fogyasztói és ipari eszközparkban.[14] Egyes esetekben a hálózati stacket más szállítók márkajelzésével látták el, így semmilyen jele nem volt annak, hogy az adott eszközt veszélyeztett. Egyre többször látjuk, hogy a támadók az IoT-/OT-eszközök ezen szoftveres és hardveres ellátási láncát célozzák meg a vállalatok feltöréséhez.

A firmware-frissítési folyamat nagy mértékben eltér a különböző eszközökön, és a frissítés bonyolultsága, illetve logisztikai kihívása negatívan befolyásolja a frissítési gyakoriságot. Nem mindig lehet megállapítani, hogy egy eszköz a legújabb firmware-t futtatja-e, ez pedig megnehezíti a biztonsági szakemberek számára az IoT- és OT-eszközök monitorozását és védelmét. Ezenkívül egyes eszközöknek olyan firmware-t futtatnak, amely nem rendelkezik kriptográfiai aláírással, így lehetőség nyílik a firmware felhasználó ellenőrzése nélküli frissítésére. Ezek a gyengeségek még sebezhetőbbé teszik az eszközöket az ellátási a termelési és a disztribúciós láncon keresztül érő támadásokkal szemben.

Ezeknek a fenyegetéseknek a mérséklése érdekében a Microsoft jelentős befektetéseket eszközöl a firmware biztonságának és integritásának biztosításába, ahogyan az szakaszról szakaszra halad az ellátási láncban, továbbá annak igazolásába, hogy a firmware-t sem a felhasználása során, sem az odáig vezető úton nem manipulálták. Ez lehetővé teszi számunkra a pipeline-szegmensek közötti bizalom ellenőrzését és azt, hogy igazolt és bizonyítható átfogó felügyeleti láncot biztosítsunk az ügyfeleinknek szállított minden összetevőhöz. Partnereinkkel azon dolgozunk, hogy ezt a chiptől a felhőig terjedő biztonságot minden eszközön megvalósítsuk a vállalati és az OT-hálózaton.

„Az ICT-infrastruktúra szállítói egyre gyakrabban válnak célponttá, mivel lehetővé teszik egyetlen sikeres támadás széles körű replikációját. Ugyanakkor világszerte a törvények és szabályok, valamint az ügyfelek ellátási lánc biztonságával és rugalmasságával kapcsolatos követelményei is egyre szigorúbbak, és gyakran meglehetősen eltérő követelményeket támasztanak.

A megoldás a partnerség. A beszállítókkal és a világ kormányaival együtt a Microsoft elkötelezett aziránt, hogy megoldja az ellátási lánc ökoszisztémájának biztonsági problémáit, és mind az ügyfelek, mind a szabályozó testületek követelményeit túlszárnyaló megoldásokkal álljon elő. Ehhez átfogó megközelítést alkalmazunk a biztonság és a működési rugalmasság terén, amely rugalmasan alkalmazunk az ellátási láncban.

Kollektív megközelítésünk kulcsa a firmware sértetlenségének biztosítása a tervezéstől az eszközüzemeltetésig. A beszállítók SDL-folyamatainak biztosítása és a hardveralapú megbízhatóság innovációinak alkalmazása jó példák arra, hogyan „építjük be" az ellátási lánc sértetlenségét.

Közösségünk kihasználja a kollektív kutatás-fejlesztés előnyeit, amelyek kiterjednek az új manipulációellenes technikákra és kriptográfiai mechanizmusokra, és folyamatos monitorozással, illetve anomáliaészleléssel párosítja őket. Együtt haladunk afelé, hogy csökkentsük az ellátási lánc mint támadási felület vonzerejét."

Edna Conway,
alelnök, a felhőinfrastruktúra biztonságáért és kockázatkezelésért felelős vezető

Reflektorfényben a firmware biztonsági rései

A támadók egyre nagyobb mértékben használják ki az IoT-eszközök firmware-ének sebezhetőségeit arra, hogy beszivárogjanak a vállalati hálózatokra. A hagyományos informatikai végpontokkal szemben – amelyek XDR-ügynököket használnak a gyengeségek azonosításához – az IoT-/OT-eszközök sebezhetőségeinek azonosítása sokkal nehezebben megfogható.

A Microsoft és a Ponemon Institute által nemrégiben készített felmérés rávilágít arra, hogy az IoT-/OT-eszközök milyen lehetőségeket és biztonsági kihívásokat jelentenek egy vállalatnál.[15] A válaszadók 68 százaléka hisz abban, hogy az IoT/OT bevezetése kritikus fontosságú a stratégiai digitális átalakulás szempontjából, 60 százaléka pedig tisztában van vele, hogy az IoT/OT-biztonság az IT-/OT-infrastruktúra egyik legkevésbé biztonságos területe.

A Trickbot trójai program jó példa arra, hogy a támadók hogyan használták ki az IoT-eszközök firmware-ének sebezhetőségeit arra, hogy beszivárogjanak a hálózatra. Ez a rosszindulatú szoftver a Mikrotik útválasztók alapértelmezett jelszavait és sebezhetőségeit használta ki[16] a vállalati védelmi rendszerek megkerüléséhez. Az IoT-eszközök firmware-évél fennálló alapvető kihívás a láthatóság hiánya: nagyon nehéz meghatározni az eszközök biztonsági helyzetét és sebezhetőségeit.

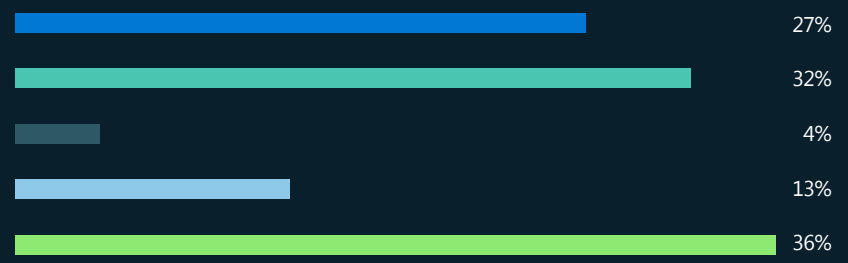
Bár vannak olyan megoldások, amelyekkel biztonságos eszközük építhetők, kész eszközök milliárdjai vannak jelenleg a piacon, illetve használatban a vállalatoknál. Ezeket „barnamezős" eszközöknek nevezzük. 2021-ben a Microsoft felvásárolta a ReFirm Labs nevű céget, hogy ráirányítsa a figyelmet a barnamezős eszközök biztonságára, és lehetővé tegye az eszközépítők számára, hogy fokozzák termékeik biztonságát. A ReFirm Labs elemzi az eszközök bináris firmware-képét, és részletes jelentést készít a potenciális biztonsági hiányosságokról.[17] Ez a technológia része lesz a Microsoft Defender for IoT egy későbbi kiadásának.

Az elmúlt év során elemeztük az ügyfeleink által megvizsgált egyedi firmware-ek összesített eredményeit. Bár nem minden felfedezett gyengeséget lehet kihasználni, az eredményekből jól látható, hogy az eszközök firmware-e alapvető biztonsági kihívást jelent.

Fontos megjegyezni az IoT-/OT-eszközökben megtalálható hiányosságok sosem lennének elfogadhatóak egy hagyományos Windows- vagy Linux-végponton.

- Gyenge jelszó: A megvizsgált firmware-képek 27 százaléka olyan fiókokat tartalmazott, amelyek gyenge, a támadók által könnyedén feltörhető algoritmusokkal (MD5/DES) kódolták a jelszavakat.

Az elemzett firmware-képekben talált biztonsági hiányosságok



- Ismert sebezhetőségek: Akárcsak más rendszerekben, az IoT-/OT-eszközök firmware-eiben is gyakran használnak nyílt forráskódú függvénytárakat. Az eszközöket azonban gyakran az ilyen összetevők elavult verziójával szállítják. Elemzésünk szerint a firmware-képek 32 százaléka legalább 10 olyan ismert sebezhetőséget (CVE-t) tartalmazott, amely kritikus (9,0-s vagy magasabb) besorolású. Négy százalékuk tartalmazott legalább 10 olyan kritikus sebezhetőséget, amely több mint hat éves.
- Lejárt tanúsítványok: A tanúsítványok a kapcsolatok és az identitások hitelesítéséhez, valamint a bizalmas adatok védelméhez használatosak, de az elemzett firmware-képek 13 százaléka tartalmazott legalább 10 olyan tanúsítványt, amely több mint három éve lejárt.
- Szoftverösszetevők: A firmware-képek 36 százaléka tartalmazott olyan szoftveres összetevőket, amelyeket a Microsoft ajánlása szerint nem lenne szabad beépíteni az IoT-eszközökbe. Ilyenek például a csomagrögzítő eszközök (tcpdump, libpcap), amelyek egy esetleges támadási láncban hálózatfelderítésre használhatók.

Néhány firmware-alapú támadás

Viasat: A műholdas kommunikáció megcélzása egy firmware-sebezhetőség kihasználásával

2022 februárjában egy műholdas hálózati incidens miatt megszakadt a kapcsolat egy stratégiai kommunikációs hálózattal, melynek hatásai egész Európában érezhetőek voltak. A Viasat KA-SAT rendszerébe jelentős formalom irányult, ami miatt számos modemmel megszakadt a kapcsolat, és egy szolgáltatásmegtagadásos támadás bontakozott ki a hálózat ellen. A vezetékes szélessávú kapcsolat zavara miatt az operátorok több ezer szélturbinához nem fértek hozzá távolról, és a támadók az érintett modemekre adattörlő rosszindulatú szoftvert telepítettek. A zavar több mint 30 000, a cégek és más szervezetek által kommunikációs célokra használt műholdas terminált érintett.

Cyclops Blink: Tűzfalátjárók megcélzása a firmware-ellátási lánc támadásán keresztül

A támadók sikerének egyik sarkalatos pontja az irányítási (C2) és a támadási infrastruktúra fejlesztése és bővítése. Ahogy növekedett a stabil C2-infrastruktúra iránti igény, az útválasztók a javítások ritka telepítése és az átfogó biztonsági megoldások hiánya miatt kívánatos támadási vektorrá váltak.

A Microsoft együttműködik a kormánnyal és az iparági szereplőkkel a firmware-elemzési technológiák területén, amelyek jobban rálátást tesznek lehetővé az eszközbiztonságra, és a teljes életciklusra kiterjedő biztonságot biztosítanak az eszközök készítői és felhasználói számára.

2019 júniusa óta egy nemzetállami kapcsolatokkal rendelkező, fejlett, tartós fenyegetést jelentő (APT) csoport a Cyclops Blink nevű moduláris rosszindulatú szoftverrel célozza meg a sérülékeny WatchGuard tűzfaleszközöket és az ASUS routereket úgy, hogy rosszindulatú firmware-frissítéseket futtat rajtuk, majd betagozza őket egy nagy kiterjedésű botnetbe. A rosszindulatú szoftver sikeresen fertőzi meg ezeket az eszközöket egy ismert sebezhetőség kihasználásával, amely lehetővé teszi a jogosultságemelést, így a támadó képes lesz az eszköz menedzselésére. A fertőzés után a rosszindulatú szoftver lehetővé teszi további modulok telepítését és a firmware-frissítések elkerülését. Megfigyelték, hogy a feltört eszközök más WatchGuard eszközökön futtatott C2-szerverekhez csatlakoznak. Különböző TCP-portokon C2-céljaikhoz számos SSL-tanúsítványt kiadva a Cyclops Blink üzemeltetői kiemelt jogosultságú távoli hozzáférést szereztek a hálózatokhoz rosszindulatú firmware-frissítések telepítésével és a hagyományos biztonsági módszerek – például a szkennelés – elkerülésével.

Hogyan teszi biztonságosabbá a Microsoft az ellátási láncot?

A Microsoft kormányzati és iparági szereplőkkel együttműködve ad választ az IoT- és OT-eszközök biztonsági kihívásaira (lásd az erről szóló részt a 66. oldalon). Hozzájárulásunk tartalmazni fogja firmware-elemzési technológiánkat, amely az ezközök üzemeltetői számára láthatóbbá teszi a hálózatukon található eszközök biztonsági állapotát. Ez lehetővé fogja tenni az ügyfelek számára a további védelmet, frissítést vagy cserét igénylő eszközök azonosítását és rangsorolását – és olyan igényeket fog támasztani, amelyek rákényszerítik az eszközgyártókat az eszközbiztonság fejlesztésére. Ugyanakkor az eszközgyártóknak is a rendelkezésére bocsátunk olyan átfogó megoldásokat, amelyekkel biztonságos eszközöket tervezhetnek, és biztonságos fejlesztési életciklust valósíthatnak meg.

Egy másik kulcsfontosságú összetevő a robosztus infrastruktúra biztosítása a gyártók és az üzemeltetők számára, amely lehetővé teszi az eszközök firmware-ének frissítését, amint a biztonsági problémákat felfedezik és megoldják. A Microsoft a Device Update for IoT Hub termékben egyesíti a firmware-elemzést a Defender for IoT szolgáltatással, így megoldást kínál az IoT- és OT-eszközök teljes életciklus alatti védelmére. Ezek fontos lépések azon elképzelésünk megvalósításához, amely szerint az ügyfelek számára biztonságos infrastruktúrát kínálunk olyan eszközök használatával, amelyek támogatják az IoT- és OT-megoldások Zero Trust megközelítését.[18]

A támadók egyre gyakrabban célozzák meg az IoT-eszközök firmware-ének sebezhetőségeit annak érdekében, hogy beszivárogjanak a vállalati hálózatokra.

Gyakorlati tanácsok

1. Alkosson pontosabb képet a hálózatán található IoT-/OT-eszközökről, és rangsorolja őket aszerint, hogy mekkora kockázatot jelentenek a vállalatára a feltörésük esetén.
2. Használjon firmware-szkennelő eszközöket a potenciális biztonsági problémák azonosításához, és a szállítókkal együttműködve keresse meg a kockázat mérséklésének módját a magas kockázatú eszközök esetén.
3. Legyen pozitív befolyással az IoT-/OT-eszközök biztonságára azáltal, hogy a beszállítóktól megköveteli a biztonságos fejlesztési életciklusra vonatkozó bevált gyakorlatok követését.

További információra mutató hivatkozások

- Az amerikai információs és kommunikációs technológiai ágazatot támogató kritikus ellátási láncok felmérése

Felderítésalapú támadások az üzemeltetési technológia ellen

Az összetett ellátási láncok egyedi tervezési információkat használnak a tényleges rendszerek megtervezéséhez. A tervezési információkat alkotó számtalan eszköz közül a legérzékenyebb a projektfájl, amely a környezet és eszközeinek meghatározását tartalmazza. Ez a fájl kulcsfontosságú stratégiai célpont azon támadók számára, akik hozzáférést próbálnak szerezni, hogy teljes mértékben a környezetre szabott támadást indíthassanak.

Az ipari rendszerek operatív folyamatok megzavarására irányuló megcélzása két lépésből áll.

1. Először a támadónak hozzá kell férnie az OT-hálózathoz. Ez úgy valósítható meg, hogy a hálózat vállalati oldalának (Purdue-modell, 4. szint) IoT-eszközein keresztül a támadó hozzáfér a hálózathoz, majd átlépi az IT-OT határvonalat, amelyet hagyományosan tűzfalak és hálózati eszközök védenek, és eljut a műveleti és szabályozási szintekre.
2. A második lépésben azonosítani kell a hálózati eszközöket. Az ipari rendszerekben szabványos eszközöket és összetevőket használnak a kifejezetten a környezethez tervezett, személyre szabott architektúrákban. Az egyik ilyen szabványos eszköz a programozható logikai vezérlő (PLC). Minden gyártó egyedi interfészeket és funkciókat fejleszt a PLC-i számára, amelyek az ipari rendszerek alapvető fontosságú összetevői. Ezeket az eszközöket azután tovább konfigurálják kifejezetten az ügyfél környezetére szabott egyéni sémákkal.

Az egyes PLC-k egyedi konfigurációját a projektfájl írja le, amely tartalmazza a környezet és az eszközök, a létralogika és egyebek meghatározását.

A legtöbb olyan rendszerben, amelyben támadásra utaló jeleket találtunk, az elemzések szerint a támadás előkészítése jóval meghaladta magának a támadásnak az időtartamát. A támadók gyakran hónapokat is rászánnak a környezet és a benne található eszközök távoli szimulálására, és számos kísérletet tesznek a modell rekonstruálására, valamint a célzott támadás előkészítésére. Ahogy a környezetek folyamatosan változnak és új eszközöket integrálnak, sebezhetőségek keletkeznek kifejezetten a projekt- és konfigurációs fájlokban található adatok körül. A projektfájl ellopása heteket vagy akár hónapokat is megtakaríthat a támadónak, mivel lehetővé teszi számára, hogy gyorsan és pontosan modellezze a célkörnyezetet, és megnehezítse a rosszindulatú tevékenység észlelését.

Industroyer és Incontroller

Megfigyeléseink szerint megszaporodtak a vállalatok, a létfontosságú infrastruktúra és a kormányzati célpontok elleni támadások, amelyeket állami támogatással rendelkező támadók követnek el moduláris rosszindulatú szoftverekkel és támadási keretrendszerekkel. Az Ukrajnában a létfontosságú infrastruktúra működésének megzavarására irányuló új kísérletek rávilágítottak, hogy egyre nagyobb veszélyt jelentenek az OT-rendszerek elleni, felderítésen alapuló és a célkörnyezetre szabott támadások. A nemzetállami kibertámadók által végzett alapos felderítés és kutatás olyan stratégiára utal, amelynek célja az infrastruktúra távoli megbénítása a kiberhadviselés eszközeivel – a kevert, kiber- és valóságos térbeli műveletek és a politikai stratégia műveleti és stratégiai céljainak megvalósítása érdekében.

Megfigyeléseink szerint növekszik a nagy mértékben a célkörnyezetre szabott, felderítésalapú OT-támadások esélye.

Felderítésalapú támadások az üzemeltetési technológia ellen

Folytatás

2022 elején két, adaptálható eszközzel elkövetett támadást észleltünk a kritikus fontosságú OT-infrastruktúra ellen. Az ukrajnai elektromos alállomások és védőrelék ellen kiber- és fizikai támadást indítottak testreszabott rosszindulatú szoftverekkel, többek között az Industroyer nevű szoftver egy variánsával, amely már 2016-os bevetése után is áramkimaradásokat okozott Ukrajnában.

A Industroyer2 az első ismert olyan eset, amikor egy rosszindulatú OT-támadó szoftvert új cél ellen vetettek be. A támadás során az Industroyerhez készült IEC104-protokoll (ez az energiaellátó rendszerek monitorozására és vezérlésére szolgáló standard protokoll) beépülő modult használták, és elsősorban az ABB RTU540/560 típusú, PLC-szerű távoli terminálegységeket célozták meg. A rosszindulatú szoftver írója az áldozat környezetére vonatkozó ismeretekre alapozva ismételten, előre meghatározott kimenetekre küldött parancsokat, így biztosítva, hogy az egységeket ne lehessen manuálisan bekapcsolni. Ezzel hosszabb idejű és pusztítóbb következményekkel járó áramkimaradásokat sikerült elérni.

Az ugyanebben az időszakban észlelt Incontroller nevű moduláris támadási keretrendszer egy olyan moduláris eszközkészlet, amely jelentősen lerövidíti az OT-eszközökre való behatolást, illetve az eszközök megtámadását megelőző előkészítést, mivel segít megkerülni a régi biztonsági megoldásokat. Az általános célú eszközkészlet olyan adatgyűjtési, felderítési és támadási képességekkel rendelkezik, amelyek nagymértékben a különböző környezetekre szabhatók, és jelentősen befolyásolhatják az OT-támadások kutatási fázisát, mivel lerövidítik a felderítéshez szükséges időt, valamint az eszközökkel és konfigurációikkal kapcsolatos információk kinyerésével támogatják a környezetek szimulálását.

Az Incontroller keretrendszer támogatja a Schneider Electric és az Omron PLC-k protokolljait, és információkat gyűjt a firmware-verzióról, a modelltípusról és a csatlakoztatott eszközökről. Az eszközkészlet képes a konfigurációt módosító és a kimeneteket be- és kikapcsoló utasításokat küldeni. Miután hozzáférést szerzett a környezethez, a keretrendszer támogatja a backdoorok elhelyezését az eszközökön, így lehetővé teszi további tartalmak küldését, sebezhetőségek elhelyezését a hozzáférési pontok számának növeléséhez, létralogika feltöltését, valamint DoS-támadások indítását. Az eszközkészlet általános jellegéből fakadóan a támadók gyorsan előkészíthetik az új rendszerek elleni támadásokat, mivel nem kell minden PLC-hez és helyhez új támadószoftvert írni. Így a támadók egyszerűen kommunikálhatnak a különböző típusú gépekkel, akár több ágazatból is.

Gyakorlati tanácsok

1. Kerülje a rendszerdefiníciókat tartalmazó fájlok nem biztonságos csatornákon keresztüli vagy nem alapvető dolgozóknak történő átvitelét.
2. Ha az ilyen fájlok átvitele elkerülhetetlen, ügyeljen arra, hogy monitorozza a hálózati tevékenységet, és megfelelő védelmet biztosítson az eszközöknek.
3. Védje a mérnöki állomásokat EDR-megoldásokkal történő monitorozás révén.
4. Reagáljon proaktívan az eseményekre az OT-hálózatokon.
5. Vezessen be folyamatos monitorozó megoldást, amilyen például a Defender for IoT.

Végjegyzet

1. Lásd pl.: Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST
2. Cert-In – kezdőoldal
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Lásd pl.: cím nélkül (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Lásd pl.: A Microsoft biztonságos fejlesztési módszertana
7. Lásd pl.: Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft – Engineering@Microsoft; lásd még: pl.: The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Lásd pl.: https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet – GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe – ENISA (europa.eu)
12. Certification – ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool„GitHub - microsoft/sbom-tool: The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. Az IoT-/OT-innováció kritikus fontosságú, de jelentős kockázatokat is hordoz magában (2021. dec.): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. A Trickbot IoT-eszközökből álló C2-infrastruktúrájának leleplezése (2022. márc.): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show a 9-es csatornán – az IoT-firmware szkenneléséről szóló epizód (2022. máj.): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. A Zero Trust megközelítés alkalmazás a IoT-megoldásokra (2021. máj.): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Kiberbefolyásolási műveletek

Napjaink külföldi befolyásolási kísérletei során új módszereket és technológiákat használnak, így a bizalom rombolását célzó műveletek hatékonyabbá és hatásosabbá váltak.

Kiberbefolyásolási

műveletek – áttekintés

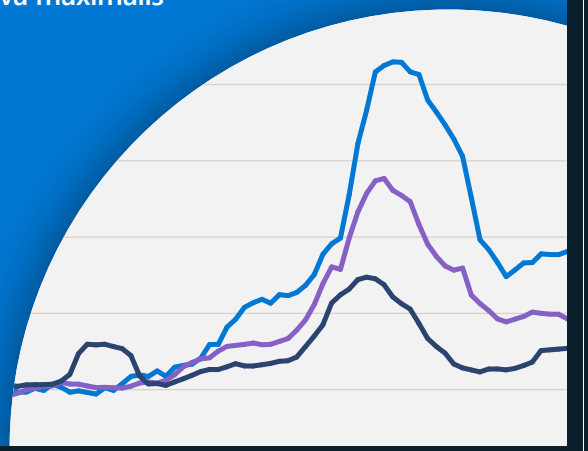
Napjaink külföldi befolyásolási kísérletei során új módszereket és technológiákat használnak, így a bizalom rombolását célzó műveletek hatékonyabbá és hatásosabbá váltak.

A nemzetállamok egyre gyakrabban kifinomult befolyásolási műveleteket alkalmaznak propagandájuk terjesztésére és a közvélemény befolyásolására, mind belföldön, mind nemzetközi szinten. Ezek a kampányok aláássák a bizalmat, növelik a polarizációt, és fenyegetést jelentenek a demokratikus folyamatokra. A képzett, ügyes és kitartó manipulátorok a hagyományos, az internetes és a közösségi média felhasználásával jelentős mértékben növelni tudták kampányaik kiterjedését és társadalmi hatását, így erőforrásaikhoz képest jelentős hatást tudnak kifejteni a globális információs ökoszisztémára. Az elmúlt évben ezeket a műveleteket az oroszok Ukrajna ellen folytatott hibrid háborújának részeként láthattuk, illetve Oroszország és más nemzetek – köztük Kína és Irán – egyre szívesebben alkalmaznak közösségi médián alapuló propagandaműveleteket, hogy kiterjesszék globális befolyásukat.

A kiberbefolyásolási műveletek egyre kifinomultabbá válnak, mivel egyre több kormány és nemzetállam használ ilyen műveleteket a közvélemény befolyásolására, az ellenfelei hiteltelenítésére és viszály szítására.

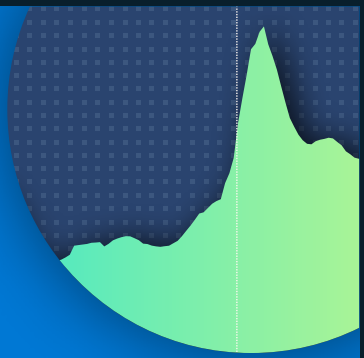
További információt a 74. oldalon talál

Ukrajna orosz inváziója jól példázza, hogy a kiberbefolyásolást a hagyományosabb kibertámadásokkal és a fizikai katonai műveletekkel kombinálva maximális hatás érhető el.



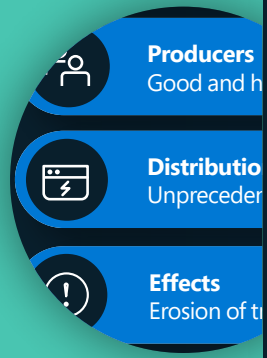
Tudjon meg többet a 76. oldalon

Oroszország, Irán és Kína propaganda- és befolyásolási kampányokat indított a COVID-19-világjárvány során – gyakran a szélesebb politikai céljai elérésének stratégiai eszközeként.



Tudjon meg többet a 76. oldalon

A szintetikus média egyre nagyobb hangsúlyt kap az olyan eszközök elterjedése miatt, amelyekkel könnyedén hozhatók létre és terjeszthetők realisztikusnak ható mesterséges képek, videók és hanganyagok. A médiaanyagok eredetét igazoló digitális technológiák azonban reményt jelentenek a visszaélések elleni harcban.



Tudjon meg többet a 80. oldalon

A kiberbefolyásolási műveletek elleni védekezés holisztikus megközelítése

A Microsoft már jelenleg is fejlett kiberveszély-felderítési infrastruktúrájára építkezve veszi fel a harcot a kiberbefolyásolási műveletek ellen. Stratégiánk, hogy észleljük és leállítsuk a külföldi agresszorok propagandakampányait, illetve védekezzünk ellenük, és elrettentsük őket az ilyen akcióktól.

További információt a 83. oldalon talál

Bevezető

A demokrácia csak megbízható információkra alapozva tud jól működni. A Microsoft számára kiemelten fontos területnek tartja a nemzetállamok által összeállított és kivitelezett befolyásolási műveleteket. Ezek a kampányok aláássák a bizalmat, növelik a polarizációt, és fenyegetést jelentenek a demokratikus folyamatokra.

A külföldi befolyásolási műveletek mindig is veszélyeztették az információs ökoszisztémát. Ami azonban az internet és a közösségi média korában más, az a kampányok jelentősen megnövekedett hatóköre, skálája és hatékonysága, valamint az a túlzott hatás, amelyet a globális információs ökoszisztéma állapotára gyakorolnak.

Az ősrégi bölcsesség, mely szerint „egy hazugság már félig körbejárta a világot, miközben az igazság még csak a cipőjét húzza" már adatokkal is alátámasztható. A Massachusetts Institute of Technology (MIT) tanulmánya[1] megállapította, hogy a hamis információkat az igazsághoz képest 70 százalékkal nagyobb valószínűséggel retweetelik, és az első 1500 emberhez hatszor gyorsabban jutnak el. Az információs ökoszisztéma egyre zavarosabbá vált, mivel az interneten és a közösségi médiában virágoznak a propagandakampányok, amelyek aláássák a hagyományos hírforrásokba vetett bizalmat. Egy 2021-es tanulmányban[2] csupán az egyesült államokbeli felnőttek hét százaléka nyilatkozott úgy, „nagyon megbízik" az újságokban, illetve a televíziós és rádiós hírszolgáltatásban, miközben 34 százalékuk nyilatkozott úgy, „egyáltalán nem" bízik ezekben.

A Microsoft folyamatosan azon dolgozik, hogy azonosítsa a külföldi kiberbefolyásolási szcéna szereplőit, fenyegetéseit és taktikáit, és közzéteszi a tanulságokat. Idén júniusban átfogó jelentést tettünk közzé az ukrajnai tanulságokról, amelyben részletesen áttekintettük Oroszország kiberbefolyásolási műveleteit.[3]

Azt is tanulmányozzuk, hogy a fejlett – például deep fake – technológiák hogyan használhatók fegyverként, és hogyan ássák alá az újságírók hitelét. Továbbá az iparági, kormányzati és akadémiai szereplőkkel együttműködve keressük a szintetikus média észlelésének hatékonyabb módszereit – ilyenek lehetnek például azok az AI-rendszerek, amelyek képesek a hamisítványok kiszűrésére.

Az információs ökoszisztéma gyorsan változó jellege és a nemzetállami online propaganda – ideértve a hagyományos kibertámadások befolyásolási műveletekkel és a demokratikus választásokba való beavatkozással való ötvözését – miatt a teljes társadalomnak ki kell vennie a részét a demokráciára leselkedő online és offline fenyegetések mérsékléséből.

Microsoft elkötelezett egy olyan egészséges információs ökoszisztéma támogatása mellett, amelyben a megbízható hírek és információk kapnak vezető szerepet. Olyan eszközöket és fenyegetésészlelési képességeket fejlesztünk, amelyek felveszik a harcot a nemzetállami befolyásolási műveletek jelentette egyre fejlődő és bővülő kockázatokkal. Ahhoz, hogy lehetővé tegyük ezt a munkát, a közelmúltban felvásároltuk a Miburo Solutions nevű céget, külső ellenőrökkel – például a Global Disinformation Indexszel és a NewsGuarddal – léptünk partnerségre, valamint több érdekelt felet tömörítő partnerségekben veszük részt, egyes esetekben vezetőként – ilyen például a Coalition for Content Provenance and Authenticity (C2PA). Csak együtt tudjuk sikerrel felvenni a harcot azok ellen, akik megpróbálják aláásni a demokratikus folyamatokat és intézményeket.

Teresa Hutson
technológiai és vállalati felelősségvállalási alelnök

Trendek a kiberbefolyásolási műveletekben

A technológia rohamos fejlődésével a kiberbefolyásolási műveletek egyre kifinomultabbá válnak. Megfigyeltük, hogy a hagyományos kibertámadásokhoz használt eszközöket elkezdték a kiberbefolyásolási műveletekhez is felhasználni. Emellett növekvő együttműködést és támogatást látunk a nemzetállamok között.

A Microsoft a Miburo Solutions felvásárlásával fektetett be a külföldi befolyásolási műveletek elleni harcba, mivel ez a cég pontosan az ilyen befolyásolási műveletek elemzésére szakosodott. A cég elemzőiből és Microsoft fenyegetésikontextus-elemzőiből a Microsoft létrehozta a Digital Threat Analysis Centert (DTAC). A DTAC elemzéseket és jelentéseket készít a nemzetállami fenyegetésekről – többek között a kibertámadásokról és a befolyásolási műveletekről –, amelyekhez az információkat és a fenyegetésfelderítési adatokat geopolitikai elemzéssel egyesíti, majd ezek alapján a hatékony reagálás és védelem kidolgozásához szükséges anyagokat állít össze.

Világszerte az emberek több mint háromnegyede nyilatkozta azt, hogy aggódik az információk fegyverként való felhasználása miatt,[4], és ezeket az aggályokat az adataink is alátámasztják. A Microsoft és partnerei nyomon követik, hogy a nemzetállami szereplők hogyan használják a befolyásolási műveleteket stratégiai célkitűzéseik és politikai céljaik eléréséhez. A pusztító kibertámadások és kiberkémkedés mellett a tekintélyuralmi rezsimek egyre gyakrabban használják a kiberbefolyásolási műveleteket a közvélemény alakítására, az ellenfeleik hiteltelenítésére, félelemkeltésre, viszályok szítására és a valóság torzítására.

Ezeknek a külföldi kiberbefolyásolási műveleteknek általában három fázisuk van:

Felvezetés

Ahogyan egy támadás során elsőként rosszindulatú szoftvereket helyeznek el a célpont számítógépes hálózatán, úgy a külföldi kiberbefolyásolási műveletek során is hamis narratívákat terjesztenek el az internet nyilvános terében. Az előzetes elhelyezés taktikája régóta segíti a hagyományos kibertámadásokat, különösen akkor, ha a rendszergazdák a legutóbbi hálózati tevékenységeket vizsgálják. A hálózaton hosszabb ideig tétlen rosszindulatú szoftvert később hatékonyabban lehet felhasználni. Ugyanígy az interneten észrevétlenül elhelyezett hamis narratívák is hitelesebb színben tüntetik fel a később rájuk hivatkozó tartalmakat.

Indítás

Gyakran az adott szereplő céljainak elérése szempontjából legjobbkor összehangolt kampány indul a narratívák kormányzati hátterű, illetve a kormányzattal szimpatizáló médiaforrásokon és közösségimédia-csatornákon keresztüli terjesztéséhez.

Erősítés

Végül a nemzetállam által vezérelt média és a proxyk erősítik a narratívákat a célközönségben. Gyakran a techszektorbeli szereplők tudtukon kívül hozzájárulnak a narratívák elérésének növeléséhez. Például a tevékenységeket online hirdetési bevételekből finanszírozhatják, a koordinált tartalomszolgáltató rendszerek pedig elárasztathatják a tartalommal a keresőket.

Ezt a három lépésből álló megközelítést alkalmazták 2021 végén is az állítólagos ukrán biológiai fegyverekről és biológiai laborokról szóló hamis orosz narratíva támogatásához. Ezt a narratívát először egy 2021. november 29-én a YouTube-ra feltöltött videóban láthattuk. Rendszeresen megjelenő angol nyelvű műsorában egy Moszkvában élő amerikai állította azt, hogy az Egyesült Államok által finanszírozott ukrajnai biolaborok biológiai fegyverekhez köthetők. A történetre hónapokig szinte senki sem figyelt fel. Amikor 2022. február 24-én az orosz tankok átlépték a határt, a biológiai fegyverek elméletét is bevetették. A Microsoft adatelemző csapata tíz, Oroszország által kontrollált vagy befolyásolt híroldalt azonosított, amelyek február 24-én egyidejűleg jelentettek meg cikkeket a témáról, visszautalva „a tavalyi beszámolóra", amelynek hitelt próbáltak adni. Ezenkívül az orosz Külügyminisztérium tisztviselői is sajtótájékoztatókat tartottak, amelyeken további hamis állításokat kürtöltek szét az információs térben az amerikai biolaborokról. Orosz támogatást élvező csapatok ezután azon dolgoztak, hogy a közösségi médiában és az internetes oldalakon minél szélesebb körben terjesszék ezt a narratívát.

Világszerte láthatjuk, hogy a tekintélyuralmi rezsimek együttműködve szennyezik az információs ökoszisztémát kölcsönösen előnyükre. Például a koronavírus-világjárvány alatt Oroszország, Irán és Kína a propaganda- és befolyásolási műveletei során nyílt, félig rejtett és titkos terjesztési módszereket ötvözött a demokráciák megcélzásához és saját geopolitikai céljai előmozdításához (További információt a 76. oldalon talál). A három rezsim egymás üzenetküldési és információs ökoszisztémáját használta a számára kedvező narratívák terjesztéséhez. Ezeknek a nagy része az Egyesült Államokkal és a szövetségeseivel kapcsolatos kritikákat vagy összeesküvés-elméleteket tartalmazott, amelyeket a kormányzat tisztviselők is terjesztettek hivatalos nyilatkozataikban, miközben a saját vakcináikat és koronavírus-járványra adott reakcióikat az Egyesült Államokéval és demokráciákéval szemben hatékonyabbnak tüntették fel. Egymást erősítve ezek az állami üzemeltetésű hírforrások olyan ökoszisztémát hoztak létre, amelyben az egyik állami sajtótermék által készített, a demokráciákról szóló negatív – és az Oroszországról, Iránról vagy Kínáról szóló pozitív – híreket a többi ország hasonló hírügynökségei erősítették meg.

Illusztráció arról, hogyan terjedt el az Egyesült Államok biolaborjairól és biológiai fegyvereiről szóló narratíva a számos külföldi befolyásolási műveletre jellemző három fő szakaszban – azaz a felvezetés, az indítás és az erősítés során.

Trendek a kiberbefolyásolási műveletekben

Folytatás

A kihívást nehezíti, hogy a magánszektor technológiai társaságai akaratlanul is támogathatják ezeket a kampányokat. Támogatók lehetnek például azok a cégek, amelyek internetes tartományokat regisztrálnak, webhelyeket hosztolnak, anyagokat népszerűsítenek a közösségi médiában és a keresőoldalakon, becsatornázzák a forgalmat, valamint segítenek finanszírozni ezeket a gyakorlatokat digitális hirdetések útján. A vállalatoknak tisztában kell lenniük a tekintélyuralmi rezsimek által a kiberbefolyásolási műveletekhez használ eszközökkel és módszerekkel, hogy észrevehessék, majd megakadályozhassák a kampányok terjesztését. Emellett egyre nagyobb szükség van arra, hogy a fogyasztók is pontosabban fel tudják ismerni a külföldi befolyásolási műveleteket, és korlátozni tudják az interakciójuk ezekkel a narratívákkal vagy tartalmakkal.

A kiberbefolyásolási műveletek, köztük az autoriter rendszerek propagandája világszerte veszélyt jelent a demokráciára, mivel csökkentik a bizalmat, növelik a megosztottságot, valamint fenyegetik a demokratikus folyamatokat.

Nagyobb fokú koordinációra és információmegosztásra van szükség a kormányzat, a magánszektor és a civil társadalom között az átláthatóság növeléséhez és az ilyen típusú befolyásoló kampányok felfedéséhez és feltartóztatásához.

Világszerte az emberek háromnegyede aggódik amiatt, hogy az információkat fegyverként használják fel.

Reflektorfényben a koronavírus-járvány és az Ukrajna elleni orosz invázió idején indított befolyásolási műveletek

A világjárvány és Ukrajna orosz inváziója során az információs környezetet kontrollálni próbáló nemzetállamok élesen kiemelik, hogyan ötvözik a tekintélyuralmi rendszerek a kiber- és az információs műveleteket.

Koronavírus-járvánnyal kapcsolatos propaganda

Oroszország, Irán és Kína propaganda- és befolyásolási kampányokat alkalmazott a koronavírus-világjárvány idején. A koronavírus-járvány kiemelt helyet kapott ezekben a kampányokban, amelyekben elsősorban kétféleképpen jelent meg:

1. Magának a világjárványnak a bemutatása.
2. Az átfogóbb politikai célok eléréséhez a koronavírus-járványt stratégiai eszközként használó kampányok.

Az ilyen típusú kampányok kettős célt szolgálnak: először is aláássák a demokráciák, a demokratikus intézmények, valamint az Egyesült Államok és szövetségesei nemzetközi megítélését; másodsorban pedig erősítik az adott ország belföldi és nemzetközi imázsát.

Ez jól tetten érhető az angol nyelvű olvasókat megcélzó ismert orosz hírforrások és sajtótermékek koronavírus elleni vakcinákkal és a járvány súlyosságával kapcsolatos üzeneteinek és a orosz kormány által ugyanebben a témában a saját állampolgárainak kommunikált üzeneteinek összehasonlítása során.

Az RT.com koronavírusról szóló 10 legolvasottabb cikkében szereplő témák
(2021. október – 2022. április)

A vakcinaellenes propaganda a nem orosz nyelvű olvasókat célozza

Orosz (magyarra fordítva)	Angol (magyarra fordítva)
„A lezárások és az emlékeztető oltások megelőzik a terjedést”	„Az oltások nem képesek megfékezni a terjedést, és hatástalanok az új variánsokkal szemben”
„Orosz közéleti személyiségek tesztje pozitív lett”	„A Pfizer vakcinájának veszélyes mellékhatásai vannak”
„Oroszországban növekszenek az esetszámok és a halálozás”	„A tömeges oltási kampányok politikailag motiváltak”
„A Szputnyik V vakcina rendkívül hatékony”	„A Pfizer és a Moderna szabályozatlan kísérleteket végez”
„A tömegközlekedési eszközökön oltási bizonyítványt kell bemutatni”	

A koronavírus-járvánnyal kapcsolatos orosz üzenetek nyelv szerint eltérnek.

A koronavírus-járvány eredetének elfedésével próbálkozó kampányok hasonlóan jó példát szolgáltatnak a jelenségre. A világjárvány kezdete óta a koronavírussal kapcsolatos orosz, iráni és kínai propaganda egymást erősítve terjeszti ezeket a központi témákat. Az ilyen hírek nagyrészt az Egyesült Államokkal kapcsolatos kritikákból és összeesküvés-elméletekből állnak. Rendszeresen egymást erősítve ezek az állami üzemeltetésű hírforrások olyan ökoszisztémát alakítottak ki, amelyben az egyik állami sajtótermék által készített, a demokráciákról szóló negatív – és az Oroszországról, Iránról vagy Kínáról szóló pozitív – híreket időről időre a többi ország hasonló hírügynökségei erősítették meg.

Az egyik ilyen példa az orosz és iráni médiában már korán megjelent feltételezés, mely szerint a koronavírus-járvány az Egyesült Államok által létrehozott biológiai fegyver lehet. Ez az állítás a világjárvány első szakaszában az alternatív, összeesküvés-elméleteket hangoztató weboldalakon kezdett terjedni, miután interjú készült egy jogászprofesszorral, aki szerint a koronavírus-járványt fegyverként hozták létre.[6] Miután az interjút közzétették néhány korlátozott elérésű webhelyen, az állami médiatermékek is átvették. Az iráni kormány által finanszírozott[7] PressTV nevű iráni, angol és francia nyelvű médiahálózat 2020 februárjában leadott egy angol nyelvű híradást „Is coronavirus a US biowarfare weapon as Francis Boyle believes?” (A koronavírus valóban az USA biológiai fegyvere, ahogyan Francis Boyle hiszi?) címmel. A cikkben arról írtak, hogy a koronavírus-járvány kitörése mögött az Egyesült Államok állt: „Amerika minden háborújában bevetettek radioaktív, kémiai, biológiai és más tiltott fegyvereket, amelyek számtalan áldozatot szedtek a célterületek lakói közül”.[8] Az orosz állami médiaügynökségek és a kínai kormányzati források is megosztották ezt a feltételezést. A Russia Today (RT) – egy állami tulajdonú orosz hírcsatorna, amely a Kreml propagandájának terjesztéséről ismert[9] – lehozott legalább egy történetet, amely az iráni vezetők azon nézeteit terjesztette, melyek szerint a koronavírus-járvány „az Egyesült Államok Irán és Kínát célzó »biológiai támadásának« következménye" lehet[10], és ezt sugalló bejegyzéseket is közzétett a közösségi médiában. Például a RT 2020. február 27-én a következőt tweetelte: „Tegye fel a kezét, aki nem lesz meglepve, ha egyszer kiderül, hogy a #coronavirus biológiai fegyver?”[11]

Ukrajnai háború – a propaganda mint háborús fegyver

Ukrajna orosz inváziója különösen szemléletes példát kínál arra, hogyan lehet a kiberbefolyásolási műveleteket a hagyományos kibertámadásokkal és a katonai műveletekkel ötvözve maximális hatást elérni.

Ukrajna inváziójának előestéjén a Microsoft fenyegetéselemzői legalább hat különböző, Oroszország érdekei mentén tevékenykedő szereplő több mint 237, Ukrajna ellen irányuló kibertámadását regisztrálták. Ezeknek a kampányoknak a szolgáltatások és intézmények bomlasztása, az ukrán közvélemény megbízható információkhoz való hozzáférésének megzavarása, valamint az ország vezetése iránti bizalmatlanság elültetése volt a célja.

Reflektorfényben a koronavírus-járvány és az Ukrajna elleni orosz invázió idején indított befolyásolási műveletek

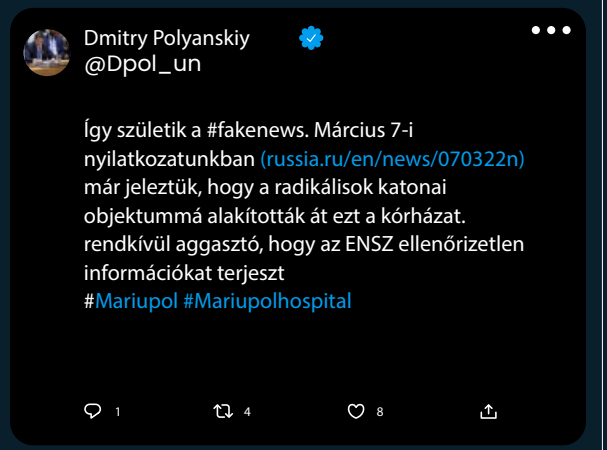
Folytatás

A Microsoft egy 2022 áprilisában kiadott jelentésében bemutattuk, hogy a kijevi információs környezet befolyásolására tett nyilvánvaló kísérletben hogyan mért Oroszország rakétacsapást egy kijevi tévétoronyra ugyanazon a napon, amikor destruktív rosszindulatú szoftverrel támadott meg egy vezető ukrán médiavállalatot.[12]

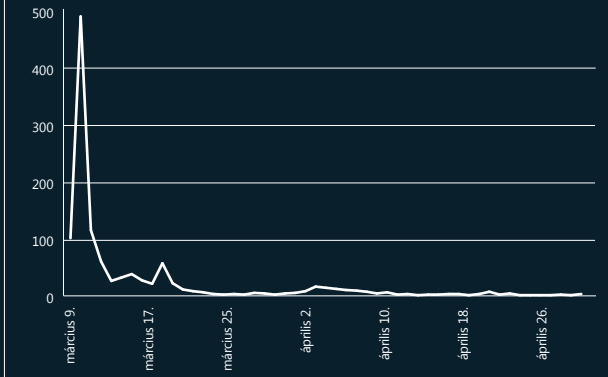
A kibertámadások és a befolyásolási műveletek ötvözésének másik eklatáns példája volt, amikor egy orosz támadó ukrán állampolgároknak küldött e-maileket a mariupoli lakosok nevében, amelyekben az ukrán kormányt hibáztatta a háború eszkalációjáért, és arra szólította fel „honfitársait", hogy álljanak ellen a kormány intézkedéseinek. Ezeket az e-maileket kifejezetten a címzettekre szabták (név szerint megszólítva őket), ami arra utal, hogy az adataikat egy korábbi, kémkedési célú kibertámadás során lopták el. Az e-mailek nem tartalmaztak rosszindulatú hivatkozások, ami azt sugallja, hogy a kampány célja teljes mértékben a befolyásolás volt.

Az állítólagosan feltört rendszerekből származó, kiszivárgott vagy egyéb bizalmasnak kikiáltott anyagok felhasználása az orosz szereplők gyakori taktikája a befolyásolási műveletekben. Az ukrajnai háború során az oroszbarát közösségimédia-csatornák az állításuk szerint ukrán források által kiszivárogtatott és más, bizalmasként bemutatott anyagokat népszerűsítenek. A kiszivárgott és bizalmas anyagokat az oroszbarát közösségimédia-csatornák és hírforrások egy kiterjedtebb befolyásolási stratégia részeként használják fel az intézményekbe vetett bizalom aláásására és a fősodorbeli narratívákkal szembeni kétségek elültetésére. Ezeket az információkat manipulálva Ukrajnát és a Nyugatot célzó propagandaanyagokat készíthetnek, csökkenthetik a digitális biztonságba vetett hitet, valamint az Ukrajnának biztosított nyugati segítség támogatottságát.

Oroszország egyéb információs támadásokkal is igyekezett formálni a közvéleményt a harctéri cselekmények után, hogy elfedje vagy hiteltelenítse a tényeket. Például március 7-én Oroszország egy ENSZ-beadvánnyal vezette fel azt a történetet, mely szerint egy mariupoli szülészeti klinikát az ukránok kiürítettek, és hadászati célokra használták fel. Március 9-én Oroszország lebombázta a kórházat. A bombázásról szóló híradások megjelenése után Oroszország ENSZ-nagykövetének helyettese, Dmitrij Poljanszkij arról írt a Twitteren, hogy a bombázásról szóló tudósítások álhírek, és Oroszország korábbi állításait idézte a kórház katonai felhasználásáról. Oroszország a támadás után két hétig széles körben terjesztette ezt a narratívát az általa kontrollált webhelyeken.



Forgalommal rendelkező tartományok
(2022. március 9. – 2022. április 30.)



A propagandawebhelyek körülbelül két hétig jelentettek meg cikkeket a szülészeti klinikáról, majd 2022. április 1-jén rövid időre leporolták a történetet. Forrás: AI for Good Lab.

Műholdképek a mariupoli szülészeti klinikáról 2022 februárjában és márciusában.

A Microsoft saját műholdképelemzése kimutatta, hogy a szülészeti klinikát lebombázták. Az első kép 2022. február 24-én készült, a második pedig 2022. március 24-én. Fotó forrása: Planet Labs.

Az Oroszország által elkövetett atrocitások tisztára mosása a háború előrehaladtával folytatódott. Például 2022. június végén az orosz médiaforrások és influenszerek egy bevásárlóközpont bombázását szükségesnek állították be, és azzal a hamis állítással indokolták, hogy az épületet nem bevásárlóközpontként, hanem az ukrán területvédelmi erők fegyverraktáraként használták.[13] Számos oroszbarát blogger posztolt az esetről a Telegramon, erősítve a „hamis zászló" narratívát. A bloggerek a hír meghamisításának állítólagos jeleit emelték ki, többek között a helyszínen készített felvételeken látható katonai egyenruhás emberek jelenlétét[14], valamint a nők hiányát.[15] Oroszország a már kiépített propagandaüzenetek és -média rendszerére támaszkodva indított kampányokat. A történetek online felerősítése révén Oroszország képes elhárítani a felelősséget a nemzetközi színtéren, és el tudja kerülni az elszámoltatást.

Oroszország és a hasonló államok átlátták, hogy mennyire hatékonyan befolyásolható a közvélemény a zárt forrásokból származó információkkal, és rendszerek feltörésén, illetve adatok kiszivárogtatásán alapuló kampányokkal terjeszti a számára kedvező ellennarratívát, és szítja a bizalmatlanságot.

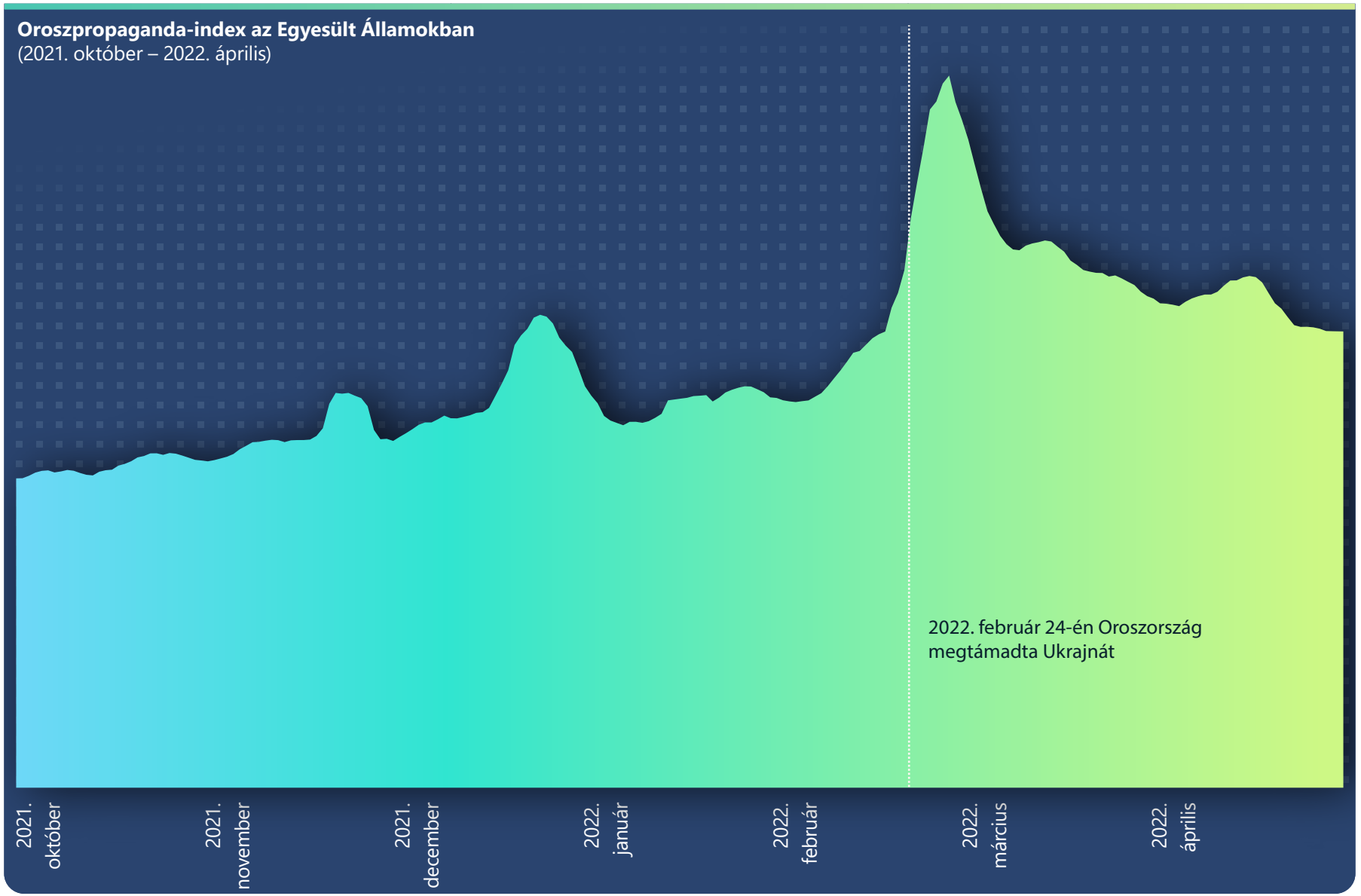
További információra mutató hivatkozások

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- Oroszország Ukrajnában indított kibertámadásainak áttekintése | A Microsoft speciális jelentése
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues

Az oroszpropaganda-index nyomon követése

2022 januárjában közel 1000 amerikai webhely irányított forgalmat orosz propagandawebhelyekre. Az amerikai közönséget megcélzó orosz propagandawebhelyek leggyakoribb témái az ukrán háború, az Egyesült Államok belpolitikája (Trumpot vagy Bident támogató állásponttal), valamint a koronavírus-járvány és a vakcinával kapcsolatos anyagok voltak.

Az oroszpropaganda-index (RPI) monitorozza, hogy mekkora részt képeznek az orosz államilag irányított és szponzorált hírforrásokból és az azokat erősítő szereplőktől származó hírek a teljes internetes hírforgalomban. Az RPI segítségével felmérhető és pontos idővonalra helyezhető az orosz propaganda fogyasztása az interneten és a különböző földrajzi régiókban. A Microsoft azonban felhívja a figyelmet arra, hogy csak a korábban azonosított webhelyeken tudja figyelni az orosz propagandát. A más típusú webhelyeken, például a hiteles híroldalakon, az azonosítatlan webhelyeken és a közösségi hálózati csoportokban terjesztett propagandára nem látunk rá.



Az oroszpropaganda-index nyomon követése

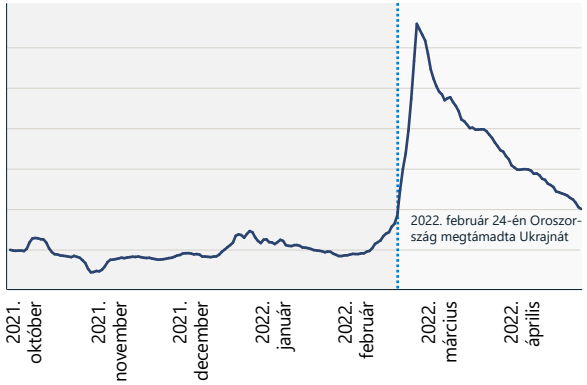
Folytatás

Oroszpropaganda-index: Ukrajna

Az ukrajnai háború indulásakor 216 százalékos növekedést láthattunk, amely március 2-án tetőzött. Az alábbi táblázatban látható, hogyan esett egybe ez a hirtelen növekedés az invázióval. A két grafikonon az látható, hogyan ugrott meg az orosz propaganda az invázió megindulása után.

RPI, Ukrajna

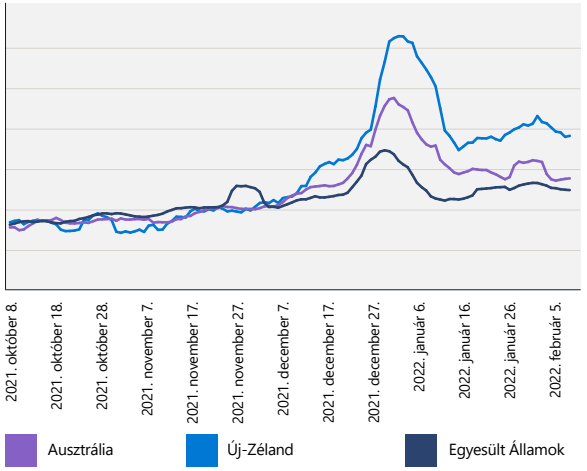
(2021. október 7. – 2022. április 30.)



Oroszpropaganda-index: Új-Zéland és Ausztrália, valamint az Egyesült Államok

Az új-zélandi RPI 2021 végén mutatott kiugrást, ami a koronavírus-járvánnyal kapcsolatos propagandához köthető. Az orosz propaganda új-zélandi fogyasztásának megnövekedése megelőzte a 2022 elején Wellingtonban zajlott nyilvános tiltakozásokat. A második kiugró érték egyértelműen Ukrajna orosz inváziójához kapcsolódik, és meghaladta Ausztrália és az Egyesült Államok RPI-értékeit.

RPI, Új-Zéland és Ausztrália, valamint az Egyesült Államok



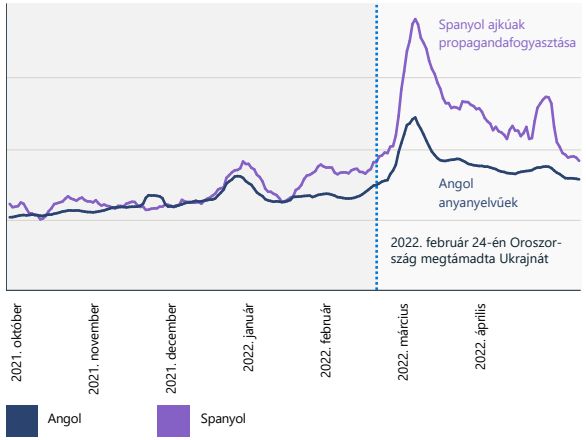
Az orosz propaganda fogyasztása Új-Zélandon Ausztráliához hasonlóan alakult 2021 decemberének első hetéig. December után azonban az orosz propaganda új-zélandi fogyasztása több mint 30 százalékkal megnövekedett az ausztrál és az egyesült államokbeli értékhez képest.

Oroszpropaganda-index az Egyesült Államokban: az angol és a spanyol nyelv megoszlása

Az RPI a propagandafogyasztást különböző nyelveken is nyomon követi. Több hírforrás, például az RT és a Sputnik News több mint 20 nyelven elérhető Sputnik News. Ezek között megtalálható az angol, a spanyol, a német, a francia, a görög, az olasz, a cseh, a lengyel, a szerb, a lett, a litván, a moldáv, a fehérorosz, az örmény, az oszét, a grúz, az azeri, az arab, a török, a perzsa és a dari.

Az alábbi grafikon látható, hogy az Egyesült Államokban a spanyol nyelvű hírek esetén az RPI sokkal magasabb, mint az angol nyelvű híreknél.

Az orosz propaganda fogyasztása kétszer magasabb a spanyol ajkúak körében



Az orosz propaganda fogyasztása az Egyesült Államokban kétszer magasabb a spanyol ajkúak körében.

Latin-Amerikában népszerű az orosz propaganda

Az RT spanyol nyelvű kiadása a legtöbb oldalmegtekintéssel és Facebook-követővel rendelkező nemzetközi hírforrás.

Forrás: Microsoft AI for Good Research Lab

Szintetikus média

Napjainkban kezdődik az AI-alapú médiakészítés és -manipuláció aranykora. A Microsoft elemzői szerint ezt két alapvető tendencia segíti elő: a rendkívül valósághű szintetikus képek, videók, hanganyagok és szövegek mesterséges létrehozásához rendelkezésre álló felhasználóbarát eszközök és szolgáltatások elterjedése, valamint a tartalmak meghatározott közönség számára történő optimalizált terjesztésének lehetősége.

Önmagában egyik fejlemény sem eredendően problematikus. Az AI-alapú technológiával szórakoztató és izgalmas digitális tartalmak hozhatók létre, akár tisztán szintetikus formában, akár meglévő anyagokat felhasználva. Ezeket az eszközöket széles körben használják a cégek hirdetések és kommunikációs anyagok készítéséhez, valamint a magánfelhasználók is, akik magával ragadó tartalmakat hoznak létre követőik számára. Ha azonban a szintetikus médiát károkozási szándékkal állítják elő és terjesztik, komoly károkat okozhat mind a magánembereknek, mind a vállalatoknak, az intézményeknek és az egész társadalomnak. A Microsoft az egyik vezetője az ilyen károk enyhítésére szolgáló technológiák és eljárások fejlesztésének. Fejlesztéseink között belső és a szélesebb média-ökoszisztémát érintő projektek is akadnak.

Ebben a szakaszban megismerhetjük a Microsoft elemzéseinek eredményeit a káros szintetikus média előállításához használt legkorszerűbb technológiákról, az ilyen tartalmak széles körben történő terjesztése által okozott károkat, valamint azokat a technikai megoldásokat, amelyekkel mérsékelhetjük a szintetikus médián alapuló kiberfenyegetéseket.

Szintetikus média készítése

A szintetikus szöveges és médiatartalmak területén hihetetlenül gyors fejlődést tapasztalhatunk: a korábban csak a legnagyobb filmstúdiók hatalmas számítási erőforrásaival elérhető lehetőségek ma már az okostelefonos alkalmazások beépített funkciói. Ugyanakkor az eszközök egyre könnyebben használhatók, és olyan realisztikus tartalmak előállítására képesek, amelyek még a bűnügyi médiaszakértőket is meg tudják téveszteni. Nagyon közel vagyunk ahhoz a pillanathoz, amikor bárki létrehozhat olyan szintetikus videót bárkiről, amelyen tetszőleges dolgot csinál vagy mond. Nem a valóságtól elrugaszkodott elképzelés úgy gondolni, hogy olyan korszakba lépünk, amelyben az online látott tartalmak jelentős része részben vagy egészben AI-technológiával előállított szintetikus tartalom.

> A kifinomultabb, könnyen használható és széles körben elérhető eszközök rendelkezésre állása révén a szintetikus tartalmak létrehozása felfutóban van, és a tartalmakat hamarosan nem lehet majd megkülönböztetni valóságtól.

Számos kiváló minőségű ingyenes és kereskedelmi kép-, videó- és hangszerkesztő eszköz létezik. Ezekkel az eszközökkel egyszerűen végezhetők potenciálisan káros változtatások a digitális tartalmakon, például megtévesztő szöveg adható hozzájuk, kicserélhető a szereplők arca, valamint eltávolítható és megváltoztatható a kontextus. Az ilyen „olcsó hamisítványok" széles körben használatosak a rosszindulatú tartalmak terjesztéséhez, a politikai ideológiák népszerűsítéséhez és mások hitelének rontásához. Egy jól ismert példa az a 2019-es[16] videó, amelyen az Amerikai Egyesült Államok Kongresszusának képviselőházi elnökének, Nancy Pelosinak a hangját változtatták el úgy, hogy kásásnak hangozzon, azt a benyomást keltve, hogy az elnök ittas. Bár hamar kiderült, hogy ennek a hatásnak az eléréséhez a videót lelassították, ez az „olcsó hamisítvány" széles körben elterjedt, mielőtt az eredeti videót és a kontextust közzétehették volna.

A médiatartalmak módosításának kifinomultabb megközelítései között szerepel a fejlett AI-technikák használata (a) tisztán szintetikus média készítéséhez, valamint (b) a meglévő médiaanyagok kifinomultabb módosításához. A deepfake kifejezést gyakran a legmodernebb AI-technikákkal létrehozott szintetikus médiaanyagokra használják (a név a mély (angolul deep) neurális hálózatok nevéből származik, amelyeket néha felhasználnak az ilyen tartalmak készítéséhez). Ezeket a technológiákat önálló alkalmazásokként, eszközökként és szolgáltatásokként fejlesztik ki, és integrálják a népszerű kereskedelmi és nyílt forrású szerkesztőeszközökbe.

A rosszindulatú szereplők fegyverként használják ezeket a technológiákat, hogy károkat okozzanak embereknek és intézményeknek. Néhány példa a deepfake technikákra:

- **Arccsere (videó, képek)** – egy arcot egy másikra cserélnek a videóban. Ezzel a technikával megkísérelhetnek megzsarolni magánszemélyeket, cégeket vagy intézményeket, illetve az embereket kellemetlen helyeken vagy helyzetekben játszódó videókba helyezhetik.
- **Bábjáték (videó, képek)** – állókép vagy másik videó animálása egy videóval. Ez olyan tartalmak készíthetők, amelyen úgy látszik, hogy valaki valami kínosat vagy félrevezetőt mond.
- **Generatív ellenséges hálózatok (videók, képek)** – olyan technikák családja, amelyekkel fotorealisztikus képek készíthetők.
- **Transzformer modellek (videó, képek, szöveg)** – részletes képek létrehozása szöveges leírás alapján.

Az ilyen fejlett AI-alapú technikákat ma még nem használják széles körben a kiberbefolyásolási műveletekben, de várhatóan az eszközök kezelésének egyszerűsödésével és elterjedésével a probléma fokozódni fog.

A szintetikus médiamanipuláció hatása

A károkozási és befolyásolási céllal indított információs műveletek nem jelentenek újdonságot. Az információk terjedésének sebessége és az, hogy nem tudjuk gyorsan megkülönböztetni a tényeket a fikciótól azt eredményezi, hogy a hamisítványok és más szintetikusan előállított rosszindulatú média által okozott hatás sokkal nagyobb lehet – ahogyan ezt Pelosi példáján is láthattuk.

A káros tevékenységek számos különböző kategóriába sorolhatók: piaci manipuláció, fizetési csalások, hangalapú adathalászat, személyazonosság-lopás, márkaimázs rontása, hírnévrontás és botnetek. E kategóriák közül sokra számos valós példát is láthattunk, ez pedig alááshatja azt a képességünket, hogy meg tudjuk különböztetni a tények és a fiktív információkat.

Hosszabb távú és sokkal súlyosabb probléma, hogy ha már nem hihetünk a szemünknek és a fülünknek, hogyan dönthetjük el, mi az igazság. Emiatt minden közszereplőről vagy magánemberről készült kép-, hang- és videófelvétel hamisítványnak kiáltható ki – ez az úgynevezett „Liar's Dividend" jelenség („a hazugság haszna", vagyis amikor az álhírekkel telített környezet bizonyos szereplők hasznára válik).[17] Nemrégiben végzett kutatások[18] szerint a technológiával való ilyen típusú visszaélések már előfordultak a pénzügyi rendszerek elleni támadások során, ám számos más esetben is elképzelhető az alkalmazásuk.

Szintetikus média

Folytatás

A szintetikus média észlelése

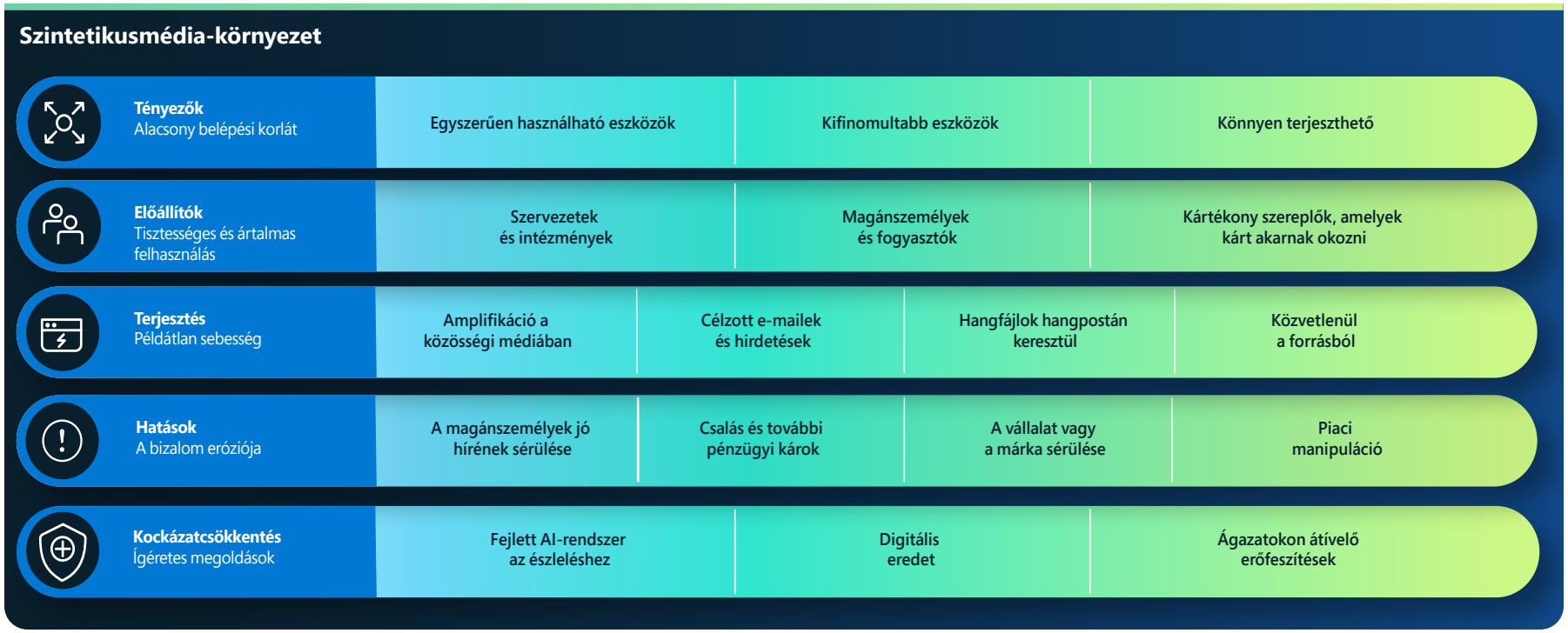
Az ágazati, kormányzati és egyetemi szférában is folyamatban vannak olyan programok, amelyek célja a szintetikus média hatékonyabb felismerése és hatásainak mérséklése, így a bizalom helyreállítása. Számos ígéretes irány van, de megfontolandó akadályokban is bővelkedik a terület.

Az egyik megközelítés AI-alapú rendszerekkel ismertetné fel a hamisítványokat – lényegében „védekező" AI-rendszerekkel venné fel a küzdelmet a támadó AI-rendszerekkel. Ezt a területet aktívan kutatják, mivel a szintetikus hang- és videoanyagokat készítő jelenlegi rendszerek árulkodó jeleket hagynak, amelyeket a képzett igazságügyi médiaelemzők és az automatikus eszközök észrevesznek.

Bár a jelenlegi hamisítványok árulkodó hibákat tartalmaznak, sajnos a pontos hibák egy adott eszközre vagy algoritmusra jellemzők. Ez azt jelenti, hogy az ismert hamisítványokon történő betanítás nem ad általános, más algoritmusoknál is használható ismereteket – ahogyan ezt egy 2020-as verseny is bizonyította, amelyen deepfake-képeket észlelő eszközöket kellett készíteni.[19] Bár jó ötletnek tűnhet többet fektetni a fejlettebb érzékelőeszközökbe, a Microsoft két okból is meglehetősen szkeptikus ezzel kapcsolatban:

Először is kiváló, a valóságot pontosan leíró fizikai modellekkel rendelkezünk. A jelenlegi hamisítványkészítők egyszerűsítenek bizonyos feladatokat, ezzel észlelhető műtermékeket hagynak a kész anyagban, ám az újabb modellek még élethűbbek lesznek. Semmi eredendően különleges nincs egy valós helyszínről kamerával rögzített jelenetben, amit ne lehetne számítógéppel modellezni.

Másodszor a fejlett hamisítványkészítő algoritmusok a generatív ellenséges hálózatok (GAN) nevű technikát használják a létrehozási folyamat részeként. Egy GAN két AI-rendszert állít szembe egymással: az egyik egy generátort használva elkészíti a hamisítványt, a másik pedig egy diszkriminátorral észleli a hamis képeket, és tanítja a generátort. A jobb észlelőeszközökre fordított minden befektetéssel csak a generátort segítjük a jobb hamisítványok létrehozásában.



Szintetikus média

Folytatás

A digitális eszközök származásigazolása

Ha a hamisítványok észlelése megbízhatatlan, hogyan védekezhetünk a szintetikus média káros felhasználása ellen? Az egyik fontos kialakulóban lévő technológia a digitális eredetigazolás – egy olyan mechanizmus, amely lehetővé teszi a digitális média alkotói számára, hogy hitelesítsenek egy anyagot, a fogyasztóknak pedig segít annak azonosításában, hogy az adott anyagot manipulálták-e. A digitális eredetigazolás különösen fontos napjaink közösségimédia-hálózatain, amelyeken szédületes sebességgel terjednek a tartalmak, és a rosszindulatú szereplőknek lehetőségük van egyszerűen manipulálni ezeket a tartalmakat.

900%

éves növekedés a deepfake-tartalmak számában 2019 óta.[20]

A digitális eredetigazolási technológia a kriptográfiai dokumentumaláírás modern változata, amelynek célja az objektumok forrásának, szerkesztési előzményeinek és metaadatainak rögzítése, miközben napjaink webes környezetében terjednek. Az ennek a végponttól végpontig terjedő manipulációbiztos médiatanúsítványnak az alapjául szolgáló elképzelést és technikai módszereket egy kutatókból és tudósokból álló csapat fejlesztette ki a Microsoftnál. Cégünk egy olyan ágazatközi partnerség társvezetője is, amelynek célja a médiaeredet-igazolási technológia gyakorlatba ültetése a Project Origin keretében (a partnerség alapítói a Microsoft, a BBC, a CBC/Radio-Canada és a new York Times). A Microsoft a technológiai és a médiaszolgáltatások területén is együttműködött más partnerekkel a Coalition for Content Provenance and Authenticity (C2PA) életre hívásában. A C2PA szabványügyi szervezetként működik, amely nemrég közzétette a médiafájlokkal – többek között képekkel, videókkal, hanganyagokkal és szövegekkel – használható legfejlettebb digitális eredetigazolási specifikációt.

A C2PA szabványának megfelelő objektumban manifest található, amely megvédi az objektumot és metaadatait a manipulációtól, és a hozzárendelt tanúsítvány azonosítja a közzétevőt.

A szintetikus média célja eredetileg nem a károkozás, azonban a rosszindulatú szereplők fegyverként használják az emberekbe és intézményekbe vetett bizalom aláásásához.

A digitális eredetigazolás ígéretes új technológia, amely a médiaanyagok eredetének tanúsításával visszaállíthatja az emberek bizalmát az online médiatartalmakban.

A C2PA-specifikáción alapuló nyilvánosan elérhető megoldások bekerülnek meglévő termékekbe új funkcióként, valamint új, önálló alkalmazások és szolgáltatások formájában is elérhetők. Arra számítunk, hogy néhány éven belül a legtöbb elterjedt rögzítő-, szerkesztő- és tartalomkészítő eszköz C2PA-kompatibilis lesz. Ez lehetőséget nyújt a vállalatoknak arra, hogy már most meghatározzák a digitális eredetigazolással kapcsolatos igényeiket és a technológia felhasználási módjait, és kérjék ennek a plusz védelmi rétegnek a beépítését a meglévő munkafolyamataikban használt eszközökbe.

Gyakorlati tanácsok

1. Tegyen proaktív lépéseket, hogy megvédje vállalatát a hamis információkkal kapcsolatos fenyegetésektől a PR- és kommunikációs válaszainak proaktív kidolgozásával.
2. Használja az eredetigazolási technológiát a hivatalos kommunikáció védelmére.

További információra mutató hivatkozások

- Ígéretes előrelépés a dezinformációval kapcsolatban | Microsoft On the Issues
- A Milestone Reached, 2022. január 31.
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- A Project Origin által a médiatartalmak hitelesítéséhez használt rendszer technikai részletei | Microsoft ALT Innovation

A kiberbefolyásolási műveletek elleni védekezés holisztikus megközelítése

A Microsoft már most is fejlett kiberfenyegetés-észlelő infrastruktúrájára építkezve szélesebb, inkluzívabb rálátást tesz lehetővé a kiberbefolyásolási műveletekre.

Az ilyen műveletek által jelentett fenyegetések elhárításához javasolt válasz- és mérséklési stratégiákból álló keretrendszert alkalmazunk, amely négy fő pillérre támaszkodik: az észlelésre, az elhárításra, a védelmére és az elrettentésre.

Ezenkívül a Microsoft négy alapelvet dolgozott ki, amellyel megszilárdítja munkáját ezen a területen. Az első a véleménynyilvánítás szabadsága iránti elkötelezettségünk, és annak biztosítása, hogy az ügyfelek információkat hozhassanak létre, tehessenek közzé és kereshessenek platformjainkon, termékeinkben és szolgáltatásainkban. A második, hogy proaktívan dolgozunk annak elkerülésén, hogy platformjainkat és termékeinket külföldi kiberbefolyásolási webhelyek és tartalmak üzenetének erősítésére használják. A harmadik, hogy szándékosan nem húzunk hasznot külföldi kiberbefolyásolási tartalmakból vagy szereplőkből. A negyedik, egyben utolsó alapelvünk: előnyben részesítjük a külföldi kiberbefolyásolási műveletek hatását mérséklő tartalmakat, belső és megbízható külső adatokat használva termékeinkben.

Észlelés

Akárcsak a kibervédelem területén, a külföldi kiberbefolyásolási műveletek elleni első lépés a felismerésükre szolgáló képesség fejlesztése. Egyetlen vállalat vagy szervezet sem remélheti, hogy egyedül el tudja érni a szükséges előrelépést. A technológiai ágazatban új, szélesebb körű együttműködésre lesz szükség, hogy előreléphessünk a külföldi kiberbefolyásolási műveletek elemzésében és jelentésében, nagymértékben támaszkodva a civil társadalom – többek között az akadémiai intézmények és a nonprofit szervezetek – szerepére.

Felismerve ezt a szerepet, Jake Shapiro és Alicia Wanless, a Princetoni Egyetem és a Carnegie Endowment for International Peace kutatói felvázolták az új „Institute for Research on the Information Environment" (IRIG, Információs környezetet kutató intézet) felállításának terveit. A Microsoft, a Knight Foundation és a Craig Newmark Philanthropies támogatásával az IRIE az Európai Nukleáris Kutatási Szervezethez (CERN) hasonló modellben működő, befogadó, több érintettet tömörítő kutatóintézet lesz. Az intézet az adatfeldolgozás és az elemzés terén szerzett szakértelmet ötvözve gyorsabb és nagyobb felfedezéseket fog tenni a területen. A megállapításait szélesebb körben meg fogja osztani a politikai döntéshozókkal, a technológiai vállalatokkal és a fogyasztókkal.

Védekezés

A második stratégiai pillér a demokratikus védelmi mechanizmusok fejlesztése. Ezt a régóta fennálló prioritást befektetésekkel és innovációval kell támogatni. Figyelembe kell vennie a technológia demokrácia elé állított kihívásait, valamint azokat a lehetőségeket, amelyeket a technológia a demokratikus társadalmak hatékonyabb védelmére kínál.

A Microsoft stratégiai keretrendszerének célja, hogy támogassa a különböző ágazatok szereplőit a propaganda észlelésében, megállításában, az ellene való védekezésben, valamint a terjesztőinek elrettentésében – különös tekintettel a külföldi agresszorok által indított műveletekre.

Érdemes korunk egyik nagy technológiai kihívásával kezdeni: az internet és a digitális hirdetések hagyományos újságírásra gyakorolt hatásával. Az 1700-as évektől kezdve a szabad és független sajtó különleges szerepet töltött a világ összes demokráciájának támogatásában a korrupció felfedésével, a háborúk dokumentálásával, és az aktuális vagy korábbi nagy társadalmi kihívások bemutatásával. Az internet azonban megfojtotta a helyi sajtót a hirdetési bevételek bekebelezésével és az előfizetők eltérítésével. Számos helyi újság összeomlott. A közelmúltban végzett munkánk egyik legfontosabb tanulsága, hogy a helyi újság nélkül maradt városok észrevétlenül és elkerülhetetlenül olyan helyzetbe kerültek, amelyben az átlagosnál jobban ki vannak téve a külföldi propagandának. Ezen okokból kifolyólag a demokrácia egyik legfontosabb védekező mechanizmusának megerősítéséhez támogatni kell a hagyományos újságírást és a szabad sajtót, különösen helyi szinten. Ehhez folyamatos beruházásokra és innovációra van szükség, amely tükrözi a különböző országok és kontinensek helyi szükségleteit. Ezeket a problémákat nem egyszerű kezelni, és több érintettet is be kell vonni, amit a Microsoft és más technológiai vállalatok is egyre nagyobb mértékben támogatnak.

A közpolitikai színtéren is új innovációkra van szükség, amelyeknek társadalmi prioritást kell kapniuk. Ez magában foglalhat olyan jogszabályokat, amelyek lehetővé teszik, hogy a kiadók kollektíven tárgyalhassanak a technológiai vállalatokkal a hirdetési bevételekről, valamint olyan törvényi környezetet, amely adókedvezményt biztosít a helyi sajtóorgánumok számára, könnyítve az újságírók alkalmazásával járó adóterheket. Az újságíróknak számos más eszközre is szükségük van hivatásuk gyakorlásához, például el kell tudniuk különíteni a valós és a csaló forrásokból származó tartalmakat.

Emellett arra is egyre égetőbb szükség van, hogy segítsünk a fogyasztóknak pontosabban felismerni az állami információs műveleteket. Bár ez elsőre ijesztően nagy feladatnak tűnhet, hasonló ahhoz a munkához, amelyet a technológiai szektor régóta végez a más kiberfenyegetések elleni védekezés jegyében. Gondoljunk csak arra, hogy már jelenleg is arra tanítjuk a fogyasztókat, hogy alaposan nézzék meg az e-mail-címet a spamek és más csalások felismeréséhez. Az Egyesült Államokban az olyan kezdeményezések, mint a News Literacy Project és a Trusted Journalism

Hosszabb távú és sokkal súlyosabb probléma, hogy ha már nem hihetünk a szemünknek és a fülünknek, hogyan dönthetjük el, mi az igazság.

A kiberbefolyásolási műveletek elleni védekezés holisztikus megközelítése

Folytatás

Program, azt a célt tűzték ki, hogy tájékozottabbá tegyék a fogyasztókat a hírekkel és az információkkal kapcsolatban. Globális szinten új technológiák, például a NewsGuard böngészőbővítménye is segíthetnek gyorsabb előrelépést elérni ezekkel az erőfeszítésekkel.

Ennek arra is emlékeztetnie kell minket, hogy a demokrácia egyik alapköve az állampolgári ismeretek oktatása. Sok máshoz hasonlóan ennek is az iskolában kell kezdődnie. Azonban olyan világban élünk, amely megköveteli, hogy élethosszig tanuljuk állampolgári jogainkat és kötelezettségeinket. Az állampolgári ismeretek nagyvállalati közegben való terjesztését célul kitűző új Civics at Work vállalást a Center for Strategic and International Studies jegyzi, de a Microsoft is szerepel az első aláírók és partnerek listáján. Ez jó példa arra, hogy milyen széles körű a demokratikus védelmi mechanizmusok erősítéséhez rendelkezésre álló lehetőségek skálája.

Megállítás

Az elmúlt években a Microsoft digitális bűncselekményekkel foglalkozó egysége, a Digital Crimes Unit (DCU) kifinomult taktikákat és olyan eszközöket fejlesztett ki, amelyekkel megálljt lehet parancsolni a kiberfenyegetéseknek – legyen szó zsarolóprogramot támadásról, botnetekről vagy állami támadásokról. Számos fontos tanulságot levontunk, melyek közül az egyik legfontosabb az, hogy az aktív védekezés rendkívül fontos számos különféle kibertámadás visszaveréséhez.

A kiberbefolyásolási műveletek elleni védekezésben talán még fontosabb szerepet kap a műveletek felszámolása, és egyre tisztábban látszik, mi a legjobb megközelítés. A széles körű megtévesztés elleni leghatékonyabb ellenszer az átláthatóság. Éppen ezért erősítette a Microsoft az állami befolyásolási műveletek észlelésének és felszámolásának képességét a Miburo Solutions felvásárlásával. Ez a vezető kiberfenyegetés-elemző és -kutató cég a külföldi kiberbefolyásolási műveletek felderítésére és az ellenük való védekezésre specializálódott.

Tapasztalataink azt mutatják, hogy a kormányoknak, a technológiai vállalatoknak és a civil szervezeteknek gondosan és megfelelő bizonyítékokra alapozva kell megtalálniuk a kibertámadások felelőseit. Az ilyen vizsgálatok és intézkedések hatásának megértése létfontosságú, és még hasznosabb lehet a kiberbefolyásolási műveletek kivédése során. Az átláthatóság gyakorlatba ültetésének ékes példája, hogy Ukrajna orosz inváziója előtt az Egyesült Államok kormánya megosztotta a rendelkezésére álló információkat – például a különböző műveletek orosz terveit, melyek között szerepelt egy hamisított felkavaró videó felhasználása is.

Amint azt a genfi CyberPeace Institute múlt nyáron az Ukrajnán belüli és kívüli kibertámadásokról közzétett tanulmányában láthattuk, a civil társadalom és a magánszektor cégei sokat tehetnek a kiberbefolyásolási műveletekkel kapcsolatos átláthatóság előmozdításáért. Az újonnan felfedezett és a jól dokumentált műveletekkel kapcsolatos megbízható jelentések révén a nagyközönség helyesebben meg tudja ítélni az olvasottak, látottak és hallottak hitelességét – különösen az interneten. Ennek érdekében a Microsoft a meglévő kiberjelentéseire építkezve, illetve azokat bővítve új jelentéseket, adatokat és frissítéseket fog kiadni arról, amit a kiberbefolyásolási műveletekkel kapcsolatban felfedezett, ideértve adott esetben a felelősöket megnevező közleményeket is.

Éves jelentést fogunk közzétenni, amely adatokon alapuló megközelítést alkalmazva tekinti át a vállalatot a külföldi információs műveletek gyakorisága tekintetében, és javaslatot tesz a következő lépésekre is a fokozatos fejlődés érdekében. Olyan további lépéseket is fontolóra veszünk, amelyek az ilyen típusú átláthatóságra építkeznek.

Például a digitális hirdetés szerepe különösen fontos, mert a hirdetések segíthetnek a külföldi műveletek finanszírozásban, egyúttal a külföldi hatalmak által szponzorált propagandawebhelyeket is legitim színben tüntetheti fel. Ezeknek a bevételi csatornáknak a felszámolásához új erőfeszítésekre van szükség.

Elrettentés

Végül nem várhatjuk el, hogy az államok megváltoztassák viselkedésüket, ha a nemzetközi szabályok megsértésekor elmarad a felelősségre vonás. Az elszámoltathatóság kikényszerítése kifejezetten kormányzati felelősség. A több érdekeltet felvonultató fellépés mégis fontos szerepet játszik a nemzetközi normák megerősítésében és kiterjesztésében. Több mint 30 online platform, hirdető és kiadó – köztük a Microsoft – írta alá az Európai Bizottság nemrég frissített, dezinformáció visszaszorítását célzó gyakorlati kódexét, és egyezett meg abban, hogy erősíti ennek a növekvő kihívásnak a leküzdése iránti elkötelezettségét. A nemrégiben életre hívott Paris Call és Christchurch Call kezdeményezéshez, valamint az internet jövőjéről szóló nyilatkozathoz hasonló többoldalú és több érintett részvételével történő cselekvés összehozhatja a kormányokat és a nyilvánosságot a demokratikus országokban. A kormányok ezután ezekre a normákra és jogszabályokra építkezve előmozdíthatják az elszámoltathatóságot, amelyet a világ demokráciái igényelnek és megérdemelnek.

A gyors és radikális átláthatóság révén a demokratikus kormányok és társadalmak hatékonyan képesek tompítani a befolyásolási kampányokat azáltal, hogy megnevezik az államilag támogatott támadások felelőseit, tájékoztatják a nagyközönséget, és erősítik az intézményekbe vetett hitet.

> Megnöveltük a külföldi befolyásolási műveletek észlelésére és megállítására szolgáló technikai kapacitásunkat, és más kibertámadásokhoz hasonlóan elkötelezettek vagyunk ezeknek a műveleteknek az átlátható jelentése iránt.

Gyakorlati tanácsok

1. Vezessen be hatékony digitális higiéniai gyakorlatokat szervezetén belül.
2. Érdemes lehet olyan módszereket bevezetni, amelyekkel csökkenthető annak az esélye, hogy a munkavállalók vagy az alkalmazott üzleti gyakorlatok véletlenül elősegítsék a kiberbefolyásolási kampányokat. Ez magában foglalja az ismert külföldi propagandaoldalak támogatásának csökkentését.
3. Támogassa az információs műveltséggel és az állampolgári részvétellel kapcsolatos kampányokat, mivel ezek kulcsfontosságú összetevői a propaganda és a külföldi befolyásolás elleni védekezésnek.
4. Működjön együtt közvetlenül az ágazata releváns csoportjaival a befolyásolási műveletekre adott válasz kidolgozásához.

Végjegyzet

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. Ukrajna védelme: A kiberháború első tanulságai (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. A Orosz Külügyminisztérium szóvivője, Marija Zaharova: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Russia's Kremenchuk Claims Versus the Evidence – bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas és Kristjan Peterson, 2020. október

Védekezés a kibertámadásokkal szemben

A modernizálás kockázatainak és előnyeinek megismerése elengedhetetlen a rugalmasság átfogó megközelítéséhez.

Védekezés a kibertámadásokkal szemben – áttekintés

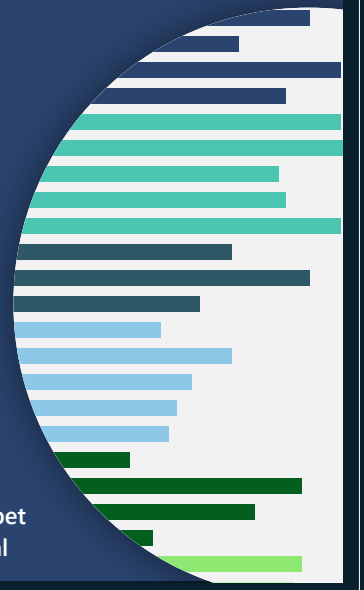
A kiberbiztonság kulcsfontosságú eleme a technológiai sikernek. Az innováció és a hatékonyság fokozásához olyan biztonsági intézkedéseket kell bevezetnünk, amelyekkel a lehető legellenállóbbá tehetjük szervezetünket a modern támadásokkal szemben.

A világjárvány komoly kihívás elé állított bennünket, és át kellett alakítanunk biztonsági gyakorlatainkat és technológiáinkat, hogy megóvhassuk a Microsoft munkatársait, bárhol is dolgozzanak. Az elmúlt évben a támadók változatlanul kihasználták a világjárvány és a hibrid munkarend miatt keletkezett biztonsági réseket. Ma a különböző támadási módok kiterjedése és összetettsége, valamint az államilag szponzorált csoportok fokozott tevékenysége jelenti a legnagyobb kihívást.

A kiberreziliencia holisztikus, adaptív megközelítést igényel, hogy ellenálljon az alapvető szolgáltatásokra és infrastruktúrára leselkedő, állandóan változó fenyegetéseknek.

Tudjon meg többet a 89. oldalon talál

Hiperösszekapcsolt világunkban a fenyegetések kezeléséhez kiemelten fontosak a modernizált rendszerek és architektúrák.

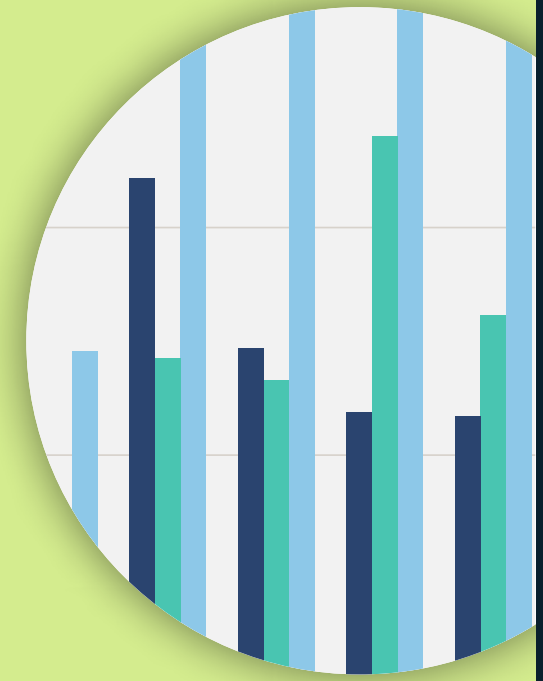


Tudjon meg többet a 90. oldalon talál

Az alapszintű biztonsági állapot a speciális megoldások hatékonyságának meghatározó tényezője.

További információt a 92. oldalon talál

Bár továbbra is a jelszóalapú támadások jelentik az identitásvédelem fő problémáját, más támadástípusok is felfutóban vannak.



További információt a 93. oldalon talál

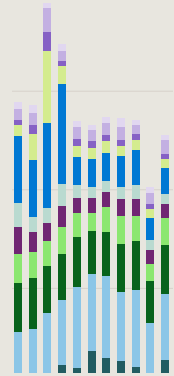
A kiberbefolyásolási műveletekkel szembeni rugalmasság emberi dimenziója az együttműködés és az együtt dolgozás képessége.

További információt a 102. oldalon talál

A sikeres kibertámadások túlnyomó többsége megelőzhető lett volna az alapvető biztonsági higiénia betartásával.

További információt a 108. oldalon talál

Az elmúlt évben a világ eddig soha nem látott volumenű, összetettségű és gyakoriságú DDoS-tevékenységet tapasztalt.



Tudjon meg többet a 98. oldalon talál

Bevezető

A világjárvány komoly kihívás elé állított bennünket, és át kellett alakítanunk biztonsági gyakorlatainkat és technológiáinkat, hogy megóvhassuk a Microsoft munkatársait, bárhol is dolgozzanak. Az elmúlt évben a támadók változatlanul kihasználták a világjárvány és a hibrid munkarend miatt keletkezett biztonsági réseket. Ma a különböző támadási módok kiterjedése és összetettsége, valamint az államilag szponzorált csoportok fokozott tevékenysége jelenti a legnagyobb kihívást.

A digitális fenyegetések aktivitása és a kibertámadások kifinomultsága napról napra növekszik. Napjainkban számos bonyolult támadása az identitásarchitektúrák, az ellátási láncok és a különböző szintű biztonsági kontrollal rendelkező külső felek ellen irányul. Különösen az identitáslopási célú adathalász támadások tűnnek egyértelmű és aktuális fenyegetésnek. Az ilyen típusú támadások azonban általában sikertelenek maradnak, ha a szervezetnél megfelelő identitásmenedzselési, adathalászat elleni és végpontmenedzsment-eljárásokat követnek. Emiatt fontos emlékeznünk az alapokra is: a támadások 98 százaléka alapvető higiéniai intézkedésekkel meghiúsítható. A Microsoftnál az identitások és az eszközök menedzselése a Zero Trust megközelítés része, amely magában foglalja a legkisebb jogosultságú hozzáférést és az adathalászatnak ellenálló hitelesítési adatok használatát a támadók hatékony megállítása és az adataink védelme érdekében.

Napjainkban még a haladó technikai ismeretekkel nem rendelkező támadók is rendkívül pusztító támadásokat tudnak indítani, mivel a fejlett taktikák, technikák és eljárások széles k9rben hozzáférhetővé váltak a kiberbűnözői közösségben. Az ukrajnai háború megmutatta, hogy hogyan fokozták a nemzetállami szereplők a támadó kiberműveleteket a zsarolóeszközök kiterjedtebb alkalmazása révén. A zsarolóeszközök mára fejlett iparággá vált, amelyben a támadó kettős vagy hármas zsarolótaktikákat alkalmaznak a váltságdíj kicsikarásához, a fejlesztők pedig szolgáltatásként kínálják a zsarolószoftvereket (RaaS). A RaaS modell segítségével a támadók egy partnerhálózatot alkalmaznak a támadások lebonyolításához, így a kevésbé képzett kiberbűnözők is belevághatnak is indíthatnak ilyen támadásokat, azaz végső soron bővül a támadók köre.

Erre válaszul Microsoft zsarolóvírusokat eltávolító programot állított össze. A program célja az ellenőrzés és a lefedettség hiányosságainak megszüntetése, hozzájárulás a szolgáltatások funkcióinak fejlesztéséhez, valamint a zsarolószoftveres támadás esetén követendő helyreállítási forgatókönyvek készítése biztonsági üzemeltetési központunk és mérnöki csapataink számára.

Az utóbbi időben megszaporodott, az ellátási láncot és a külső beszállítókat célzó támadások jelentős fordulópontot jelentenek az ágazat számára. A támadások miatt az ügyfeleinknél, partnereinknél, a kormányzati szerveknél és a Microsoftnál bekövetkezett fennakadások egyre súlyosbodnak, és rávilágítanak a kiberreziliencia és a biztonság terén érdekelt felek együttműködésének fontosságára. A támadók a helyi rendszereket is célba veszik, rákényszerítve a vállalatokat arra, hogy menedzseljék a régi rendszerek jelentette sebezhetőségeket modernizálással és az infrastruktúra felhőbe költöztetésével, ahol hatékonyabb biztonsági rendszerek védik.

Korunkban a biztonság a technológiai siker egyik kulcsfontosságú feltétele. Az innováció és a hatékonyság fokozásához olyan biztonsági intézkedéseket kell bevezetnünk, amelyekkel a lehető legellenállóbbá tehetjük szervezetünket a modern támadásokkal szemben. A digitális fenyegetések növekedésével és fejlődésével elengedhetetlen beépíteni a kiberrezilienciát minden szervezetbe.

Bret Arsenault
információbiztonsági igazgató

Kiberreziliencia: Az összekapcsolt társadalom alapköve

A digitális technológia forradalma közepette a vállalatok a nagyobb mértékű összekapcsolás irányába mozdultak el – mind működésük, mind az általuk kínált szolgáltatások terén. Ahogyan a kiberkörnyezet fenyegetései egyre fenyegetőbbé váltak, a kiberreziliencia szerepe is felértékelődött: ma már ugyanannyira fontos beépíteni a szervezetbe, mint a pénzügyi és a működési rugalmasságot.

A digitális átalakulás véglegesen megváltoztatta a vállalatok együttműködését az ügyfelekkel, a partnerekkel, a dolgozókkal és más érdekeltekkel. Az új technológiák hatalmas lehetőségeket kínálnak az emberekkel való interakcióhoz, a termékek átalakításához és az üzemeltetés optimalizálásához. A világjárvány felgyorsította a digitális átalakulást olyan innovatív technológiák fejlesztésének fellendítésével, amelyek lehetővé teszik az emberek számára az új módokon és bárhonnan történő együttműködést.

Mivel a kibertámadások helyi fenyegetéssé váltak, „mindig összekapcsolt" világunkban egyre nehezebb megakadályozni, hogy a támadók sikerrel hatoljanak be a vállalati rendszerekbe. A kiberreziliencia a szervezet azon képességét jelenti, hogy a támadások keresztüzében is folytatni tudja működését és fenn tudja tartani a növekedés lendületét. A megelőzést túlélési és helyreállítási képességekkel kell kiegyensúlyozni, és a kormányok, valamint a vállalatok olyan átfogó modelleket fejlesztenek, amelyek a kiberreziliencia jegyében túlmutatnak a biztonságon és az adatvédelmen az eszközök, az adatok és egyéb erőforrások védelme terén.

A kiberreziliencia átfogó megközelítésének kialakítása

A kiberreziliencia holisztikus, adaptív és globális megközelítést igényel, amely képes ellenállni az alapvető szolgáltatásokra és infrastruktúrára leselkedő, állandóan változó fenyegetéseknek. Ez a megközelítés többek között a következőket fedi le:

- Alapvető kiberhigiénia a kiberreziliencia haranggörbéjénélleírtak szerint.
- A digitális átalakulás kockázati/megtérülési arányának megismerése és menedzselése.
- Valós idejű válaszadási képességek, amelyek lehetővé teszik a fenyegetések és a sebezhetőségek proaktív észlelését.
- Védelem az ismert támadásokkal szemben és preventív tevékenység az új és várható támadási vektorok ellen, beleértve az automatikus javítást is.
- A támadások és katasztrófák hatásának mérséklése a hibák elkülönítésével és a szegmentálásával.
- Automatikus helyreállítás és redundancia zavar esetére.
- Az üzemeltetési tesztelés előtérbe helyezése a hiányosságok megtalálásához, valamint a külső erőforrásokkal, például felhőalapú biztonsággal kapcsolatos megosztott felelősségek és függőségek megismeréséhez.

A hatékony kiberreziliencia-program az erőforrások alapjainak lefektetésével kezdődik – például a rendelkezésre álló szolgáltatások felmérésével, valamint a fennakadás esetén igénybe vehető erőforrásokat tartalmazó megbízható katalógus összeállításával. Erre az alapra építkezve a programnak fel kell tudnia mérni saját hatékonyságát, fel kell tudnia mérni a kritikus fontosságú szolgáltatások teljesítményét és függőségeit, tudnia kell tesztelni és érvényesíteni a helyi és a felhőszolgáltatásokban rendelkezésre álló képességeket, valamint támogatnia kell a folyamatos fejlődést a szervezet egész digitális életciklusán keresztül.

A holisztikus megközelítés érdekében a vállalatokkal együttműködve azonosítjuk a legfontosabb helyi és online szolgáltatásaikat, üzleti folyamataikat, függőségeiket, személyzetüket, szolgáltatóikat és beszállítóikat. Megvizsgáljuk az ügyfél- és piaci elvárásokhoz, a szabályozási és szerződéses kötelezettségekhez, valamint a belső működéshez kapcsolódó eszközöket és erőforrásokat is. Ezeknek a kritikus fontosságú erőforrásoknak az azonosítása után, párhuzamos erőfeszítések keretében kell észlelni és monitorozni a fenyegetéseket, a zavarokat, a potenciális támadási vektorokat, valamint a rendszerek és a folyamatok sebezhetőségeit. A jelenlegi szakemberhiány mellett ez a vállalatra jelentett átfogó kockázat szerinti szigorú rangsorolást követel meg.

Az ilyen típusú holisztikus megközelítésnek a folyamatosan változó fenyegetési környezet miatt adaptívnak kell lennie, és a mérhető teljesítményfokozást, a rövidebb észlelési, válaszadási és helyreállítási időt, valamint a fennakadások hatásainak mérséklését kell céloznia. A megközelítésnek emellett azt is számításba kell vennie, hogy a fenyegetések is egy nagyobb mértékben összekapcsolódnak. Például egy biztonsági incidens adatvédelmi következményekkel járhat, és azt eredményezheti, hogy számos belső és külső csapatnak kell együttműködnie a gyors reagálás és a hatás minimalizálása érdekében.

> A kiberreziliencia a vállalat azon képessége, hogy zavarok – többek között kibertámadások – esetén is tudja folytatni a működését, és fenn tudja tartani a növekedés lendületét.

Gyakorlati tanácsok

1. Építsen ki olyan technológiai rendszert, amely korlátozza a betörések hatásait, és gondoskodjon róla, hogy még egy esetlegesen sikeres betörés esetén is biztonságosan és hatékonyan tudjanak tovább működni. Összpontosítson a leggyakoribb kritikus eszközökre, támogassa az agilitást, és a tervezés során tartsa szem előtt az alkalmazkodóképességet (pl. hibrid és többfelhős, többplatformos környezet kialakítása), csökkentse a támadási felületeket (pl. távolítsa el a nem használt alkalmazásokat és a felesleges hozzáférési jogosultságokat), számoljon feltört erőforrásokkal, és készüljön a támadók fejlődésére.
2. A digitális projektek tervezése során a lehetőségek mellett vegye figyelembe a potenciális fenyegetéseket, valamint a rugalmasságot szolgáló közös felelősségvállalásokat a digitális technológiai ellátási láncban, beleértve a felhőalapú biztonsági megoldásokat is.
3. Készítsen biztonságosra tervezett rendszereket, és tegyen lépéseket a jövőbeli változó fenyegetésekre való felkészülés és válaszadás, valamint a fenyegetések észlelése, a nekik való ellenállás, illetve a hozzájuk való alkalmazkodás felé.
4. Ügyeljen rá, hogy az üzleti vezetők szükség szerint konzultáljanak a biztonsági csapatokkal az új fejlesztésekhez kapcsolódó kockázatok megismerése érdekében. Hasonlóképpen a biztonsági csapatoknak is figyelembe kell venniük az üzleti célokat, és tanácsokkal kell ellátniuk a vezetőket e célok biztonságos megvalósításával kapcsolatban.
5. Gondoskodjon arról, hogy a kibertámadások esetére pontosan meghatározott üzemeltetési gyakorlatok és eljárások álljanak rendelkezésre az üzleti rugalmasság fenntartásához.

A rendszerek és az architektúra modernizálásának jelentősége

Amikor új képességeket fejlesztünk egy hiperösszekapcsolt világ számára, menedzselnünk kell a régi rendszerek és szoftverek által jelentett fenyegetéseket.

A régi rendszerek – amelyeket a modern csatlakozási eszközök, például az okostelefonok, a táblagépek és a felhőszolgáltatások széles körű elterjedése előtt fejlesztettek – kockázatot jelentenek azokra a cégekre, amelyek még mindig használják őket. Ezeknek a kockázatoknak a fennállását támasztják alá a Microsoft Security Services for Incident Response csapat eredményei is, amely biztonsági szakemberekből áll, és az ügyfeleket segíti a támadásokra való reagálásban, illetve az ezt követő helyreállításban.

Az elmúlt év során a támadás utáni helyreállításban támogatott ügyfeleknél talált problémák hat fő kategóriához kapcsolódtak, ahogyan ez az ezen az oldalon lévő diagramon is jól látható. A következő oldalon felvázoljuk a rugalmasság javítását célzó gyakorlati lépéseket.

A biztonsági incidensek több mint 80 százaléka visszavezethető néhány hiányzó elemre, amelyek modern biztonsági megközelítést alkalmazva pótolhatók.

A kiberrezilienciát érintő alapvető problémák

Ebben a diagramon látható, hogy az érintett ügyfeleknek hány százalékánál hiányzik az alapvető biztonsági kontroll, ami kulcsfontosságú a vállalati kiberreziliencia szempontjából. Az adatokat a Microsoft ügyfelekkel végzett munkája során gyűjtöttük a tavalyi évben.

„A vezetőknek a kiberrezilienciát az üzleti rugalmasság egyik alapvető fontosságú komponenseként kell felfogniuk. Ugyanúgy terveket kell készíteniük a kiberbiztonsági zavarok esetére, mint a természeti katasztrófák vagy egyéb előre nem látható események esetére, és a stratégiák kidolgozásához össze kell hívniuk a belső érdekelteket az üzemeltetési, a kommunikációs, a jogi és egyéb területekről. Így biztosítható, hogy a vállalatok a lehető leggyorsabban vissza tudják állítani a kritikus fontosságú üzleti rendszereket a normál üzletmenet folytatásához.

De ez még nem minden. Mivel számos vállalat támaszkodik külső beszállítókra és szolgáltatókra, a vezetőknek ki kell bővíteniük a kiberreziliencia tervezését a teljes értéklánc, hogy hatékonyabban biztosíthassák az üzletmenet folytonosságát és az üzleti rugalmasságot."

Ann Johnson,
biztonságért, megfelelőségért, identitásért és menedzsmentért felelős vállalati alelnök, Üzletfejlesztési részleg

A rendszerek és az architektúra modernizálásának jelentősége

Folytatás

Vannak olyan jól kivehető területek, amelyekre összpontosítva a vállalatok modernizálhatják megközelítésüket, és védekezhetnek a fenyegetések ellen:

Probléma	Gyakorlati lépések
Az identitásszolgáltató nem biztonságos konfigurációja Az identitáskezelő platformok és összetevőik helytelen konfigurációja és kitettsége gyakori vektor a magas jogosultsági szintű hozzáférés illetéktelen megszerzéséhez.	Az identitáskezelő rendszerek, például az AD és az Azure AD infrastruktúra bevezetésekor és karbantartásakor kövesse a biztonsági konfigurációs alapszabályokat és bevált gyakorlatokat. Vezessen be hozzáférési korlátozásokat az identitásrendszerek menedzseléséhez a jogosultságok elkülönítésének, a legkisebb jogosultsággal rendelkező hozzáférésnek és a kiemelt jogosultságú hozzáféréssel rendelkező munkaállomások (PAW) használatának kötelezővé tételével.
Elégtelen jogosultságú hozzáférés és az oldalirányú mozgás kontrollja A rendszergazdák túlzottan magas szintű jogosultságokkal rendelkeznek a digitális környezetben, és a rendszergazdai hitelesítő adatokat gyakran az internetes és hatékonysági kockázatoknak kitett munkaállomásokon használják.	Védje meg és korlátozza a rendszergazdai hozzáférést a környezet rugalmasságának növeléséhez, valamint az esetleges támadások hatókörének korlátozásához. Alkalmazzon a kiemelt jogosultságú hozzáférést szabályozó technikákat, például igény szerinti hozzáférést és az éppen elégséges adminisztráció biztosítását.
Nincs többfaktoros hitelesítés (MFA) Napjaink támadói nem betörnek, hanem bejelentkeznek.	Az MFA kritikus fontosságú és alapvető felhasználóihozzáférés-szabályozó eszköz, amelyet minden szervezetnek használnia kell. A feltételes hozzáféréssel párosítva az MFA felbecsülhetetlen értéket képvisel a kibertámadások elleni küzdelemben.
Fejletlen biztonsági műveletek A legtöbb érintett vállalat hagyományos fenyegetésészlelési eszközöket használt, és nem rendelkezett a időszerű reagáláshoz és kárelhárításhoz szükséges információkkal.	Az átfogó fenyegetésészlelési stratégia megalkotásához be kell fektetni a kiterjesztett észlelési és reagálási (XDR) rendszerekbe, és modern felhőnatív eszközöket kell használni, amelyek gépi tanulással különítik el a zajt és a fontos jeleket. Modernizálja a biztonsági üzemeltetési eszközöket az XDR beépítésével, amely mélyreható biztonsági elemzéseket kínál a digitális környezetről.
Az információvédelem kontrolljának hiánya A vállalatoknak továbbra is nehézséget okoz a holisztikus információvédelmi kontroll megalkotása, amely teljesen lefedi az adatok tárolási helyeit, az információk teljes életciklusa során érvényben marad, valamint összhangban van az adatok üzleti szempontból értelmezett fontosságával.	Azonosítsa a kritikus fontosságú üzleti adatokat és a tárolásuk helyét. Tekintse át az információ-életciklussal kapcsolatos folyamatokat, és az üzletmenet folytonossága mellett helyezzen nagy hangsúlyt az adatvédelemre is.
A modern biztonsági keretrendszerek korlátozott bevezetése Az identitás az új külső biztonsági védvonal, amely lehetővé teszi a különböző digitális szolgáltatásokhoz és a számítástechnikai környezetekhez való hozzáférést. A Zero Trust elveit alkalmazó alkalmazásbiztonsági és egyéb modern kiberbiztonsági keretrendszerek használata lehetővé teszi a vállalatok számára, hogy proaktív módon kezeljék azokat a kockázatokat, amelyeket egyébként nehezen látnának előre.	A Zero Trust Framework keretrendszerek a legkisebb jogosultság elvét alkalmazzák, explicit módon ellenőriznek minden hozzáférést, és mindig azt feltételezik, hogy sikeres támadás történt. A vállalatoknak biztonsági ellenőrzéseket és gyakorlatokat kell alkalmazniuk a DevOps- és alkalmazáséletciklus-folyamatokban is, hogy magasabb szintű védelmet biztosítsanak a céges üzleti rendszerekben.

Az alapszintű biztonsági állapot a speciális megoldások hatékonyságának meghatározó tényezője

Elemzéseink során felfedeztünk néhány gyakori vakfoltot a vállalatok védelmi rendszereiben, amelyek lehetővé teszik a támadók számára, hogy kezdeti hozzáférést szerezzenek, megvessék a lábukat, és támadást indítsanak még a fejlett biztonsági megoldások jelenléte esetén is.

Sok esetben a kibertámadások eredménye már jóval a tényleges támadás előtt eldől. A támadók a sebezhető környezeteket kihasználva kezdeti hozzáférést szereznek, megfigyelést végeznek, majd oldalirányban mozogva titkosítással vagy kiszivárogtatással okoznak károkat. A támadók korai megállítása nagyban növeli a teljes hatás mérséklésének esélyét.

A Microsoft tanulmányozta a különböző biztonsági állapotok konkrét konfigurációit, hogy azonosítsa a ténylegesen alkalmazott gyakorlatok legtöbbször előforduló hiányosságait ezekben a környezetekben. Így azonosítani tudtuk az emberi irányítású zsarolószoftveres támadások során leggyakrabban kihasznált sebezhetőségeket, amelyek lehetővé tették a támadók számára az észrevétlen hozzáférést és hálózaton történő mozgást.

Be kell kapcsolni az alapszintű biztonsági konfigurációkat

A vállalat nem regisztrált vagy elavult eszközei (mindkettő a sebezhetőségek és a biztonsági ügynökök állapota miatt) a támadók potenciális belépési pontjai és hozzáférésszerzési útvonalai. Megállapítottuk, hogy bár a vállalati eszközök frissített végponti észlelési és elhárítási[1] (EDR) és végpontvédelmi[2] (EPP) platformon való regisztrálása fontos lépés, nem garantálja a zsarolóprogramok feltartóztatását.

Az olyan fejlett megoldások, mint az EDR és az EPP, kritikus fontosságúak a támadások korai szakaszban történő felderítéséhez, valamint az automatikus helyreállítás és védelem lehetővé tételéhez. Mivel azonban ezek a fejlett megoldások a támadások észlelésének alapvető képességén alapulnak, működésükhöz be kell kapcsolni az alapvető biztonsági konfigurációkat. Számos olyan szituációt figyeltünk meg, amikor ugyan fejlett megoldásokat használtak, de ezek hatékonyságát aláásta az alapvető biztonsági konfigurációk hiánya.

A biztonsági konfigurációkkal kapcsolatos bevált gyakorlatok pontosabban jelzik a rugalmasság szintjét, mint a biztonsági műveleti központ (SOC) elemzőinek válaszideje

Ügyfeleink és partnereink körében hat hónap alatt 70 százalékos csökkenést figyeltünk meg abban, hogy a SOC-elemzők a releváns riasztás beérkezésétől számítva mennyi idő alatt tekintik meg azt, illetve reagálnak rá. Ez a megnövekedett tudatosság jó jel. Mindemellett, bár a biztonsági konfiguráció láthatósága javította a SOC-elemzők teljesítményét, a termékek láthatóságának vállalati eszközök regisztrálásával és frissítésével való biztosítása hatékonyabban előre jelezte a támadások sikeres megelőzését.

Az ismeretlen eszközök által jelentett kockázatok

A felhőalapú hálózatokkal szemben, ahol az ügyfelek tudják, hogy mely eszközök milyen operációs rendszeren futnak, a helyi hálózatok sokféle eszközt tartalmazhatnak, például IoT-eszközöket, asztali gépeket, szervereket és hálózati eszközöket, amelyeket a vállalat nem monitoroz vagy menedzsel.

Egy átlagos nagyvállalati hálózat több mint 3500 csatlakoztatott eszközt tartalmaz, amelyeket nem védenek EDR-ügynökök, és amelyek hozzáférhetnek a vállalati erőforrásokhoz, sőt akár a nagy értékű eszközökhöz is. A Végponthoz készült Microsoft Defender (MDE) hálózatvizsgálattal fedezi fel az eszközöket, és biztosít információt a hálózatra csatlakozó eszközök osztályozásáról, például az eszközök nevéről, az operációs rendszerek megoszlásáról és az eszköztípusról.

3500

– átlagosan ennyi olyan csatlakoztatott eszközt tartalmaz egy nagyvállalati hálózat, amelyet nem véd végponti észlelési és elhárítási ügynök.

Az EDR-ügynök által nem támogatott eszközök tekintetében legyen tisztában legalább a létezésükkel, és intézkedjen a védelmükről a sebezhetőségeik felmérésével, valamint a hálózati hozzáférés korlátozásával.

Gyakorlati tanácsok

1. Még a fejlett megoldásokat képességeit is alááshatja az alapvető biztonsági konfigurációk hiánya.
2. Fektessen be a biztonsági állapotot javító bevált módszerekbe, hogy sikeresen k tudja védeni a jövőbeli támadásokat. Ezek az alapvető beállítások busásan megtérülnek a vállalat számára, mivel a vállalat hatékonyan tud védekezni a támadások ellen.
3. Regisztrálja az összes erre alkalmas eszközt egy EDR-megoldásba.
4. Ügyeljen a biztonsági ügynökök frissítésére, és biztosítsa a manipuláció elleni védelmet a nagyobb láthatóság és a termékek teljesebb körű védelme érdekében.

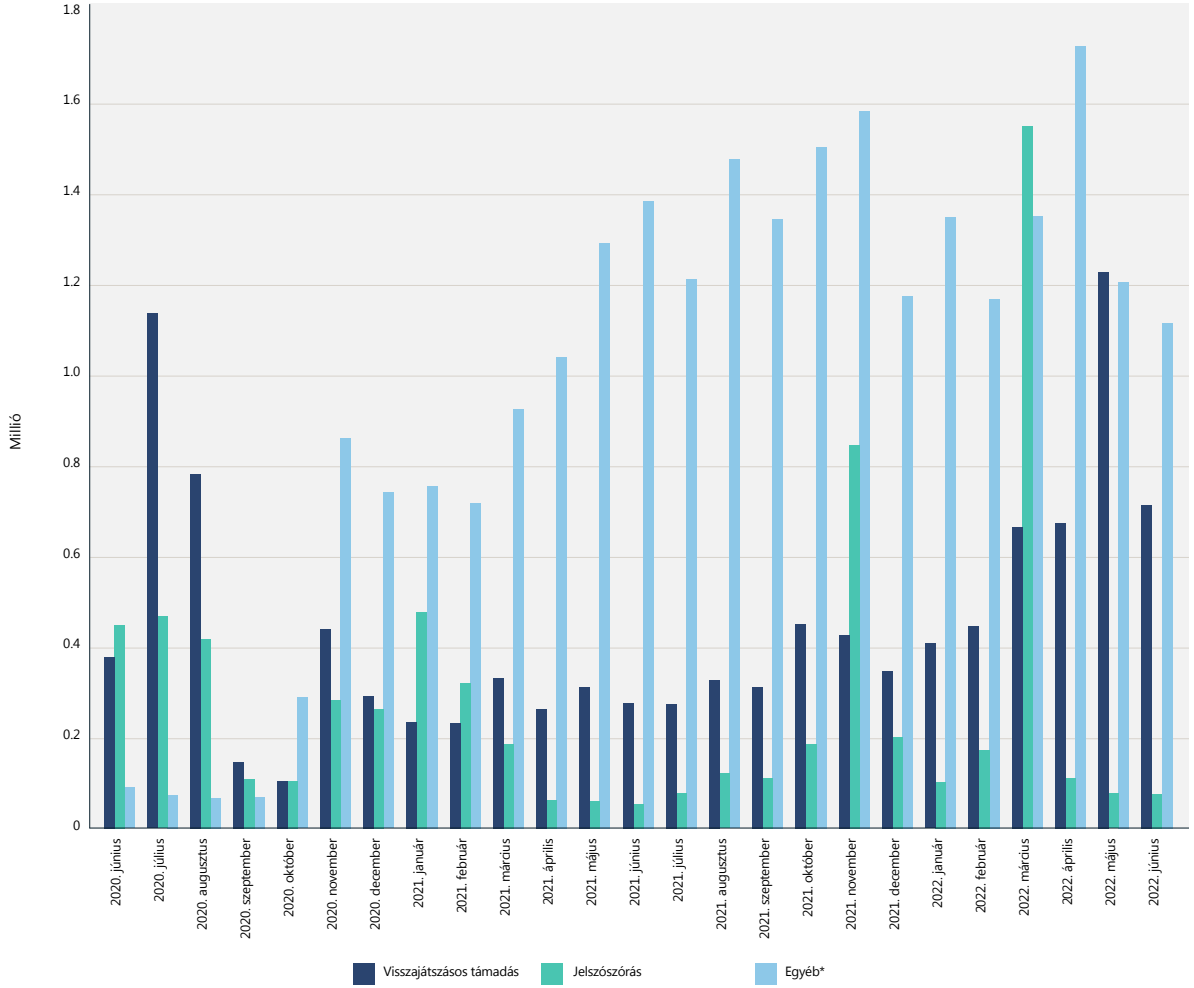
A megfelelő identitásállapot alapvető fontosságú a szervezeti jólléthez

A identitás védelme minden eddiginél fontosabb. Bár továbbra is a jelszóalapú támadások jelentik az identitásvédelem fő problémáját, más támadástípusok is felfutóban vannak. A kifinomult támadások aránya továbbra is emelkedik a korábban elterjedt szórásos jelszófeltöréses és visszajátszásos támadásokéhoz képest.

A jelszóalapú támadások még mindig gyakoriak, és az ilyen módszerekkel feltört fiókok több mint 90 százalékát nem védi erős hitelesítés. Az erős hitelesítés több hitelesítési faktort is használ, például jelszót és SMS-t, illetve FIDO2 biztonsági kulcsokat.

Emelkedést tapasztaltunk a célzott szórásos jelszófeltörést alkalmazó támadások számában, és különösen kiugró volumenűek voltak az olyan támadások, amelyek során a támadói forgalom több ezer IP-cím között oszlott meg.

A különböző támadási kategóriákkal feltört felhasználói fiókok megoszlása



A különböző támadási kategóriákkal feltört felhasználói fiókok száma havonta. A szórásos jelszófeltöréses támadások volumene jelentős ingadozást mutat, ahogyan ezt a 2021 novemberében és 2022 márciusában regisztrált kiugró értékek is tanúsítják. Ezek a kiugrások a gyakorlatban több ezer érintett felhasználót és IP-címet jelentenek. * Az „Egyéb" besorolás a szórásos jelszófeltöréstől és a visszajátszásos támadástól eltérő technikával megvalósított támadásokat jelöl, amelyek között megtalálható az adathalászat, a rosszindulatú szoftverek, a közbeékelődés, a helyi tokenkibocsátó feltörése és egyéb módszerek. Forrás: Azure AD Identity Protection.

4500

Amíg elolvassa ezt a részt, mi 4500 jelszófeltörési kísérletet védünk ki.

A megfelelő identitásállapot alapvető fontosságú a szervezeti jólléthez

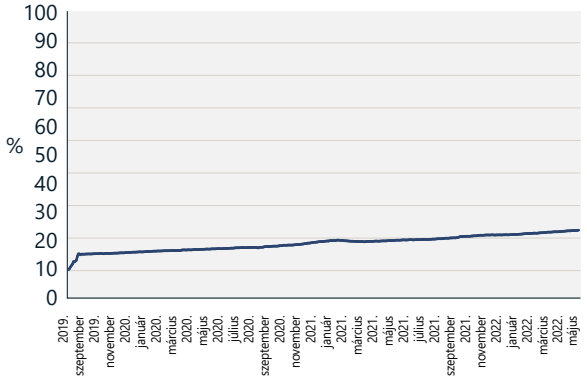
Folytatás

Az erős hitelesítés bevezetése

Pozitív fejlemény, hogy az Azure Active Directory (Azure AD) vállalati ügyfélbázisán belül folyamatosan növekszik az erős hitelesítést bevezető ügyfelek száma. Az Azure AD esetében az erős hitelesítést használó havi aktív felhasználók aránya 19 százalékról 26 százalékra nőtt az elmúlt évben, míg ugyanez az arány az adminisztratív fiókok esetében 30 százalékról mintegy 33 százalékra nőtt.

Ez mindenképpen pozitív tendencia, ám még mindig jelentős növekedésre van szükség ahhoz, hogy az erős hitelesítést használók többségbe kerüljenek. A felhasználóik védelme érdekében azoknak az ügyfeleknek is el kell kezdeniük megtervezni, majd megvalósítani az erős hitelesítés bevezetését, akik jelenleg nem használják a környezetükben.[3] Az erős hitelesítés bevezetésének tervezése során fontolóra kell venni a jelszó nélküli hitelesítés használatát is, mivel ez kínálja a legbiztonságosabb használható élményt, és kiküszöböli a jelszóalapú támadások kockázatát.

Erős hitelesítés használata
(2019. szeptember – 2022. május)

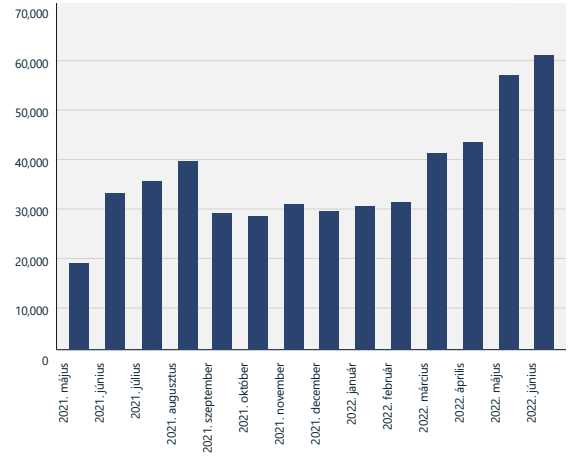


Bár az erős hitelesítés használata megduplázódott 2019 óta, mindössze a felhasználók 26 százaléka és a rendszergazdák 33 százaléka használja. Forrás: Azure Active Directory.

Folyamatosan növekszik a token-visszajátszási támadások száma

2022-ben megnövekedett az egyéb támadási formák aránya. Megfigyeltük, hogy felfutott az olyan célzott támadások száma, amelyek megkerülik a jelszóalapú hitelesítést, hogy csökkentsék az észlelésük esélyét. Ezek a támadások a böngésző egyszeri bejelentkezési (SSO) cookie-jait használják ki, vagy a rosszindulatú szoftverekkel, adathalászattal vagy más módon megszerzett tokeneket frissítenek. Bizonyos esetekben a támadók a megcélzott felhasználóhoz földrajzilag közel eső infrastruktúrát választanak, hogy tovább csökkentsék az észlelés esélyét. Folyamatos emelkedést észleltünk a token-visszajátszási támadások számában, az Azure AD Identity Protection szolgáltatásban immár havonta több mint 40 ezer ilyen támadást regisztrálunk. A token-visszajátszási támadások során jogosult felhasználó számára kiállított tokeneket használ fel a támadó, akinek birtokába jutottak ilyen tokenek. A tokeneket általában rosszindulatú szoftverekkel szerzik meg – például kiszivárogtatják a cookie-kat a felhasználó böngészőjéből, vagy fejlett adathalász módszereket alkalmaznak.

Az észlelt token-visszajátszási támadások mennyisége



Észlelt token-visszajátszási támadások havi száma. Forrás: Azure AD Identity Protection, a rendellenes tokeneket észlelő funkció által megjelölt egyedi munkamenetek.

A megfelelő identitásállapot alapvető fontosságú a szervezeti jólléthez

Folytatás

Tokenek kinyerése

A rosszindulatú szoftvereken kívül a támadóknak hitelesítő adatokra is szükségük van céljaik eléréséhez. Az ember által irányított zsarolótámadások 100 százalékában felhasználtak lopott hitelesítő adatokat. A kifinomult behatolási technikákat alkalmazó támadások során a dark weben vásárolt hitelesítő adatokat használnak fel, amelyeket eredetileg nem kifinomult, tömeges célzású rosszindulatú szoftverekkel loptak el. A rosszindulatú szoftverek e kategóriáját úgy fejlesztették tovább, hogy tokeneket – többek között munkamenetadatokat és MFA-jogcímeket – lopjon. Emiatt a vállalati hálózatokra nézve nagyon súlyos incidensekhez vezethet, ha sikerül megfertőzni olyan otthoni számítógépeket, amelyekről a felhasználók vállalati eszközökbe jelentkeznek be.

A támadók közbeékelődéses támadásokkal is megszerezhetik a tokeneket az áldozatok eszközeiről – ez a fajta támadás úgy működik, hogy az áldozatnak adathalász e-mailben vagy csevegőüzenetben rosszindulatú hivatkozást küldenek, amelyre kattintva az identitásszolgáltató valódi oldalához megtévesztően hasonlító webhelyre jut. Valójában a megnyitott oldal a támadó által készített webszolgáltatás, amely továbbítja és elfogja a felhasználó és az identitásszolgáltató közötti teljes forgalmat. A támadó képes elfogni a felhasználónevet és a jelszót, és az MFA-ellenőrzéseket is továbbítani tudja. Az identitásszolgáltató által kiállított és a támadó által elfogott tokenek olyan MFA-jogcímeket tartalmazhatnak, amelyekkel a támadó sikeresen elvégezheti az MFA-hitelesítést.

A Microsoft Defender for Cloud Apps 2022 eleje óta havonta átlagosan 895 ilyen támadást észlelt. Ez a támadási formát ki lehet védeni adathalászatnak ellenálló MFA-faktorok, például a Tanúsítványalapú hitelesítés, a Vállalati Windows Hello vagy a FIDO2 biztonsági kulcsok használatával.

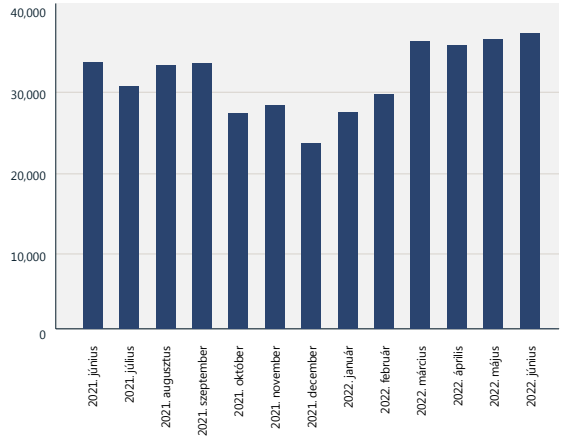
> A jelszóalapú támadások a fiókok feltörésének elsődleges módszerei.

MFA-kifárasztás

Az „MFA-kifárasztás” elvét használva a támadók több MFA-kérelmet küldenek az áldozat eszközére, remélve, hogy az áldozat véletlenül, vagy a kérelmek számába belefáradva elfogadja valamelyiket. Ez a támadás megakadályozható modern hitelesítő alkalmazásokat, például a Microsoft Authenticatort olyan funkciókkal kombinálva, mint a számegyeztetés[4] és a további kontextus engedélyezése.[5] Az Azure AD Identity Protection becslése szerint havonta 30 000 MFA-kifárasztásos támadásra kerül sor.

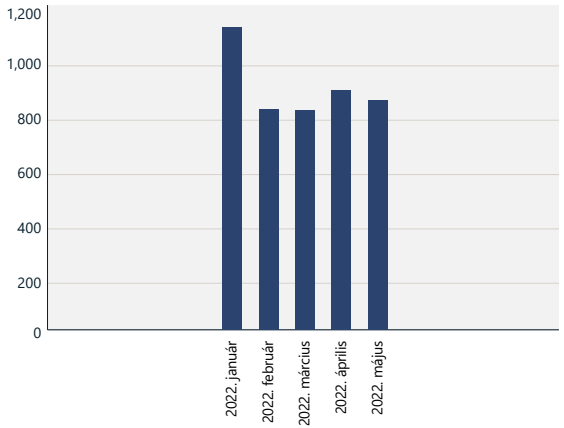
> A kifinomult támadások aránya továbbra növekszik, ami rávilágít arra, milyen fontos adathalászatnak ellenálló faktorokat használni a többfaktoros hitelesítéshez.

Az MFA-kifárasztásos támadások becsült száma



Forrás: Azure AD Identity Protection.

Észlelt adathalász támadások, amelyeket közbeékelődéses támadás követett



Forrás: Microsoft Defender for Cloud Apps.

Gyakorlati tanácsok

1. Gondoskodjon róla, hogy a vállalat minden fiókját erős hitelesítés védje.
2. A jelszó nélküli hitelesítés nyújtja a legbiztonságosabb és leginkább felhasználóbarát élményt, miközben kizárja a jelszóalapú támadások lehetőségét.
3. Tiltsa le a régi hitelesítési módszereket a teljes vállalatnál.
4. A különösen értékes és rendszergazdai fiókokat védje adathalászatnak ellenálló erős hitelesítéssel.
5. Modernizálja identitásszolgáltatóját: váltson helyi megoldásról felhőbeli identitásszolgáltatóra, és kapcsolja össze az összes alkalmazását ezzel a felhőalapú identitásszolgáltatóval a konzisztens felhasználói élmény és a biztonság érdekében.

További információra mutató hivatkozások

- A jelszavak idei világnapján fontolja meg a jelszavak teljes kiiktatását | Microsoft Security

Az operációs rendszer alapértelmezett biztonsági beállításai

A folyamatosan változó biztonsági fenyegetések világában a kiberreziliencia biztosításához egyre nagyobb szükség van az alapértelmezés szerint biztonságosra konfigurált számítógépes rendszerekre. Ugyan az operációs rendszerek biztonsága sürgetőbb, összetettebb és üzleti szempontból fontosabb, mint valaha, nem mindig egyszerű megtalálni és menedzselni a megfelelő konfigurációt.

A múltban a számítógépek és eszközök védelmét olyan beépített biztonsági funkciók látták el, amelyeket az ügyfélnek vagy egy informatikai szakembernek kellett a kívánt szintre konfigurálnia. Ez a megközelítés már nem megfelelő, mivel a támadók egyre fejlettebb eszközöket használnak céljaik eléréséhez az automatizálás, a felhőalapú infrastruktúra és a távoli hozzáférési technológiák terén. Létfontosságúvá vált, hogy a chiptől a felhőig minden réteg alapértelmezetten biztonságos beállításokkal érkezzen. A Microsoft is fejlődött ezen a téren, és a Windows operációs rendszert már alapértelmezetten biztonságos beállításokkal kínálja.[6]

Azok az ügyfelek, akik alaposabb figyelmet fordítanak a védelemre – többek között rétegesen építik fel biztonsági megközelítésüket, új biztonsági funkciókat használnak, rendszeresen és konzisztensen telepítik a javításokat és frissítéseket, valamint biztonsági tréningeket tartanak, illetve tudatosan jelentik az adathalászatot és más csalásokat – kevesebb rosszindulatú szoftverre számíthatnak.

A mélységi védelem egyszerűsítése érdekében a Windows 11 alapértelmezés szerint bekapcsolt, szorosan integrált hardveres és szoftveres védelmet biztosít, többek között memóriaintegritási funkciókat, biztonságos rendszerindítást és a Platformmegbízhatósági modul 2.0-s verzióját. A Windows 10 rendszert kompatibilis hardveren futtató felhasználók is bekapcsolhatják ezeket a funkciókat a Windows Gépház alkalmazásán vagy a BIOS-menüben.

A régebbi eszközökön gyakran nincsenek megfelelően összehangolva a hardveres és a szoftveres biztonsági technikák. Az olyan eszközökön, amelyeken alapértelmezés szerint nincsenek bekapcsolva a biztonsági funkciók, konfigurálja őket manuálisan a beállításokban, amennyiben lehetséges.[7]

Az olyan eszközökön, amelyeken alapértelmezés szerint nincsenek bekapcsolva a biztonsági funkciók, a Microsoft azt javasolja, hogy lehetőség szerint konfigurálja őket manuálisan.

Telepítse proaktívan az operációs rendszerhez folyamatosan érkező frissítéseket és biztonsági javításokat, amelyek elősegítik a támadások elleni védekezést a hardver és a szoftveres teljes életciklusa alatt.

Gyakorlati tanácsok

1. Használjon olyan, jelszó nélküli megoldást, amely a bejelentkezési hitelesítő adatokat a Platformmegbízhatósági modulban kapcsolja össze – keressen kifejezetten olyan megoldást, amely megfelel a Faster Identity Online (FIDO) szövetség[8] iparági szabványának.
2. Távolítsa el időben a vállalati eszközökön lévő összes nem használt és elavult végrehajtható fájlt.
3. Védekezzen a fejlett firmware-támadások ellen a memóriaintegritás, a biztonságos rendszerindítás és a Platformmegbízhatósági modul 2.0 bekapcsolásával, ha alapértelmezés szerint nincsenek engedélyezve, mivel ezek a modern CPU-kba beépített képességek erősítik a rendszerindítási folyamat védelmét.
4. Kapcsolja be az adattitkosítást és a hitelesítő adatok védelmét.
5. Engedélyezze az alkalmazások és böngészők nem megbízható alkalmazások elleni vezérlőit és egyéb beépített védelmi funkcióit.
6. Engedélyezze a memória-hozzáférés elleni védelmet, amely segít kivédeni az alkalmi fizikai támadásokat, például amikor valaki egy rosszindulatú eszközt csatlakoztat a számítógép egy kívülről elérhető portjához.

További információra mutató hivatkozások

- Windows biztonsági kézikönyv | Kereskedelmi
- A Windows 11 új biztonsági funkciói segítenek a hibrid munka védelmében | Microsoft Security Blog

A szoftverellátási lánc központi jellege

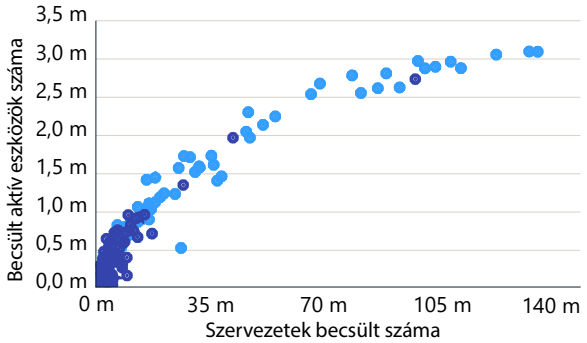
A külső alkalmazások, beépülő modulok és bővítmények elleni támadások alááshatják az ellátási ökoszisztémában központi szerepet betöltő bizalmat az ügyfelek és a beszállítók között. Ha bevonjuk a hálózatelméletet a szoftver központi szerepének vizsgálatába, tisztán látszik, mennyire fontos a javítások telepítése – különösen a központi alkalmazások esetén.

A Windows App Network 18 millió végrehajtható alkalmazásfájlját ötmillió szervezetnél telepítették és használják, így magas szintű nézetet biztosít szoftveres ökoszisztémánkról. A 100 000 legtöbbet használt alkalmazás 97 százalékát olyan külső cégek készítették, amelyeknek a frissítéseit és a biztonsági javításait saját maguk tartják karban. Ez kereskedelmi alkalmazás-ökoszisztémánk két fontos jellemzőjét szemlélteti.

Először is, centralitás figyelhető meg a kereskedelmi Windows-alkalmazások ökoszisztémájában. A 18 millió közül csak a top 100 ezer alkalmazást használják legalább 1000 eszközön. Más szóval ezeknek az alkalmazásoknak csupán valamivel több mint fél százaléka rendelkezik ilyen széles körű eléréssel az eszközök ökoszisztémájában.

Másodszor, ezen alkalmazások menedzselhetősége is változatos, mivel a top 10 ezer alkalmazásgyártó menedzseli a legnépszerűbb kereskedelmi alkalmazások frissítéseit és biztonsági javításait. Ennek alapján jól látszik, mennyire rá vannak utalva a cégek a szoftvergyártók kontrolljára a biztonság, a megfelelőségi és a menedzsment terén.

A leggyakrabban használt alkalmazások kereskedelmi penetrációja



A legnépszerűbb alkalmazásokat több millió szervezet használja eszközök tízmillióin. Mivel ennyire elterjedtek, a támadók is folyamatosan keresik a kihasználható biztonsági réseket ezekben a népszerű alkalmazásokban, amelyek sikeres kihasználása a felhasználói bázis több millió eszközét érintené.

Megfigyeléseink szerint kereskedelmi eszközök millióin használnak sebezhető alkalmazásverziókat hónapokkal a javítás kiadása után – vagy akár évekkel a terméktámogatás megszűnése után is. Például több mint egymillió aktív kereskedelmi Windows-eszközön fut egy PDF-olvasó olyan verziója, amelyet 2017 óta nem támogatnak.

Az alkalmazások nem támogatott régi verzióit továbbra is több millió kereskedelmi eszközön használják aktívan. Így a vállalatok olyan sebezhetőségeket hordoznak magukkal, amelyekre már nem is fog megjelenni javítás.

A támogatott alkalmazásverziók esetén azt látjuk, hogy a kritikus javítások alkalmazásának sebessége stagnál, ez pedig pont a rugalmasságot elősegítő trend ellenében hat. A szükséges rugalmasság eléréséhez a görbének a javítások alkalmazásának exponenciális növekedését kellene mutatnia hónapról hónapra.

A kritikus javítások telepítésének sebessége

Egy bizonyos böngészőcsoport 134 verzióját érintő kritikus sebezhetőséget megvizsgálva arra jutottunk, hogy az eszközök 78 százalékán – azaz több millió eszközön – a javítás kiadása után kilenc hónappal is valamelyik érintett verzió futott.

Az InterpretML[9] eszközkészlet segítségével azonosítottuk azokat a jellemzőket, amelyek korreláltak a legnagyobb valószínűséggel régebbi verziót futtató eszközökkel rendelkező vállalatokkal. A legfontosabbak indikátorok közé a következő tartoznak: alacsony eszközhasználati idő; olyan földrajzi régiók, mint Ázsia és a csendes-óceáni térség, valamint Latin-Amerika; továbbá olyan ágazatok, mint a gépjárműipar, a vegyipar, a távközlés, a szállítás és a logisztika, az egészségpénztárak (biztosítási ügykezelők) és a biztosítók.

A szoftveres rugalmasság fenntartásának részeként rendszeresen le kell tiltani és el kell távolítani a nem használt alkalmazásokat.

A szervezet biztonsága és megfelelősége a saját és a szoftverbeszállítóinak erőfeszítésein áll vagy bukik.

Gyakorlati tanácsok

1. Frissítse időben a szervezet összes alkalmazását és végpontját.
2. Távolítsa el időben a vállalati eszközökön lévő összes nem használt és elavult végrehajtható fájlt.

További információra mutató hivatkozások

- Microsoft Intune-dokumentáció | Microsoft Docs
- Alkalmazások menedzselése | Microsoft Docs
- Végponthoz készült Microsoft Defender | Microsoft Security
- OSS biztonságos ellátásilánc-keretrendszer | Microsoft Security Engineering
- A Microsoft nyílt forráskódú szoftvere védi az ellátásilánc-keretrendszert | Github

Üzleti rugalmasság kiépítése az erősödő DDoS-, webalkalmazás- és hálózati támadások korában

A felgyorsult digitális átalakulás elsöpörte a hagyományos hálózati és biztonsági perem modellt. A felhőbe költözés azt jelenti, hogy a vállalatoknak felhőnatív hálózatbiztonsági megoldást kell bevezetniük a digitális eszközök védelme érdekében.

A támadások összetettsége, gyakorisága és mennyisége folyamatosan nő, és már nem csupán az ünnepi szezonra korlátozódik – jelezve, hogy immár egész évben számítani kell támadásokra. Ez rávilágít arra, milyen fontos a hagyományos, csúcsszezonra összpontosító védelmet meghaladó folyamatos védelem megvalósítása.

Elosztott szolgáltatás-megtagadásos (DDoS) támadások

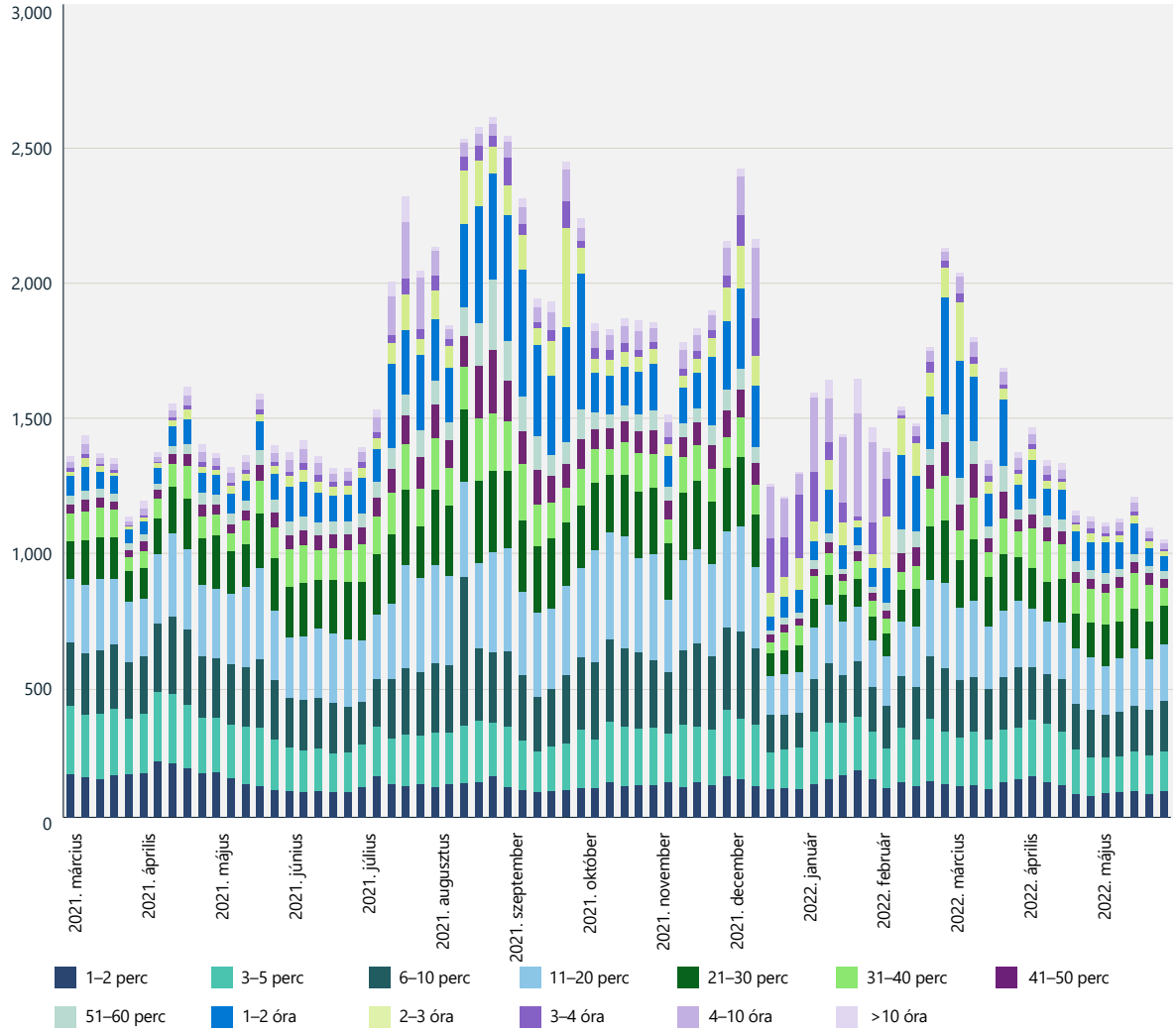
Az elmúlt évben a világ eddig soha nem látott volumenű, összetettségű és gyakoriságú DDoS-tevékenységet tapasztalt. A DDoS-támadások számának robbanásszerű növekedését a nemzetállami támadások jelentős megszaporodása váltotta ki, ami az olcsó, bérelhető DDoS-szolgáltatások elszaporodását is magával hozta. A Microsoft átlagosan 1955 támadást hárított el naponta – ezt 40 százalékos növekedést jelent az előző évhez képest. Korábban a támadások száma jellemzően az évvégi ünnepi szezonban tetőzött. Idén azonban a legtöbb támadást 2021. augusztus 10-én regisztráltuk. Ez arra utal, hogy a támadók elmozdultak az egész éves támadási szezon felé, és rávilágít, milyen fontos a hagyományos, csúcsszezonra összpontosító védelmet meghaladó folyamatos védelem megvalósítása.

2021 novemberében a Microsoft meghiúsított egy hatalmas volumenű DDoS-támadást, amely 3,4 terabit/másodperces (Tb/s) kapacitást vonultatott fel a világ számos országában található, körülbelül 10 000 forrására alapozva. Hasonlóan nagy volumenű (2 Tb/s feletti teljesítményű) támadásokat hiúsítottunk meg 2022-ben, amiből jól látható, hogy nemcsak a támadások összetettsége és gyakorisága növekszik, hanem a támadások volumene (sávszélessége) is.

Támadások hossza

Az elmúlt év során megfigyelt legtöbb támadás rövid életű volt. A támadások körülbelül 28 százaléka kevesebb mint 10 percig tartott, 26 százaléka 10–30 percig, 14 százaléka pedig 31–60 percig. A támadások 32 százaléka tartott egy óránál tovább.

A DDoS-támadások számának és időtartamának elosztása
(2021. március – 2022. május)



Az elmúlt évben a legtöbb támadás rövid életű volt. A támadások körülbelül 28 százaléka kevesebb mint 10 percig tartott.

Üzleti rugalmasság kiépítése az erősödő DDoS-, webalkalmazás- és hálózati támadások korában

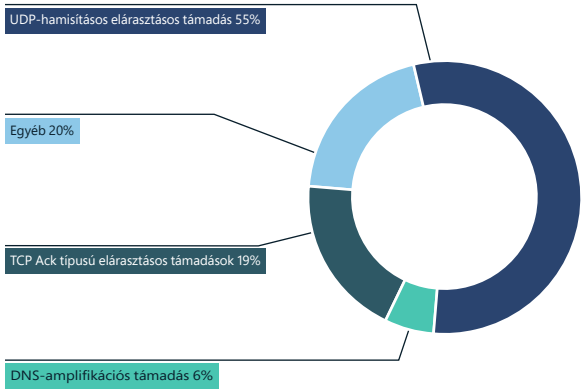
Folytatás

DDoS – támadás vektorok

Az elmúlt évben az általánosan használt támadási vektorok a 80-as porton keresztüli UDP-tükrözéssel használt SSDP (simple service discovery protocol), CLDAP (Connectionless Lightweight Directory Access Protocol), DNS (tartománynévrendszer) és egyetlen kiugró hullámban az NTP (Network Time Protocol) voltak. Növekedést tapasztaltunk a webhelyeket célzó, alkalmazásrétegbeli DDoS-támadások számában is, 16,3 milliós csúcs-RPS-értékkel (ez a kérelmek másodpercenkénti számát jelöl) és a csúcson 9,89 Tb/s forgalommal.

2022-ben a Microsoft közel 2000 DDoS-támadást hiúsított meg naponta, és az eddig dokumentált legnagyobb DDoS-támadást is sikerült megakadályoznia.

DDoS – támadás vektorok



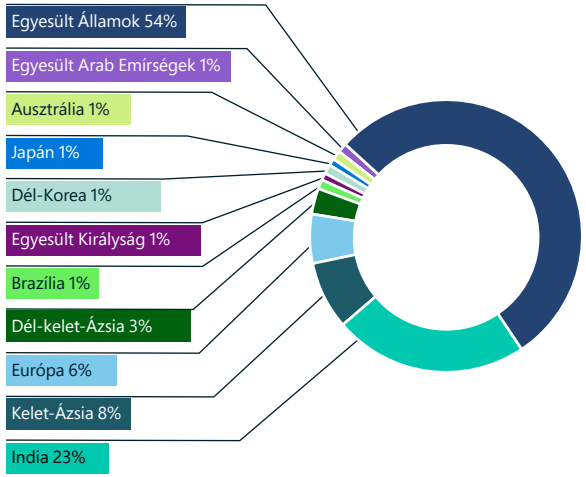
Az UDP-hamisításos elárasztásos támadás a legfontosabb vektorrá lépett elő 2022 első felében: részesedése 16 százalékról 55 százalékra nőtt. A TCP Ack típusú elárasztásos támadások aránya 54 százalékról 19 százalékra szorulta vissza.

A DDoS-támadások legfontosabb célpontja továbbra is a játékipar, amelyet többnyire a Mirai botnet valamilyen mutációjával támadnak, illetve alacsony volumenű, UDP-protokollon keresztüli támadások érnek. Mivel az UDP használata elterjedt a játékok és a streamelőalkalmazások körében, a támadások túlnyomó többsége az UDP-hamisításos elárasztásos vektort alkalmazta, míg kisebb része az UDP-tükrözéses és -erősítéses módszerhez folyamodott.

Földrajzi célrégiók

Az elmúlt év során észlelt DDoS-támadások 54%-át egyesült államokbeli célok ellen indították, amit részben az magyaráz, hogy a legtöbb Azure- és Microsoft-ügyfél az Egyesült Államokban van. Jelentős növekedést láttunk az indiai célpontok ellen intézett támadások arányában: míg 2021 második felében csupán a támadások 2 százaléka célozta Indiát, 2022 első felében ez az arány 23 százalékra növekedett. Kelet-Ázsia, különösen Hongkong továbbra is népszerű célpont a maga 8 százalékos részesedésével. Európában a támadások az amszterdami, bécsi, párizsi és frankfurti régióban koncentrálódtak.

DDoS-támadások célja

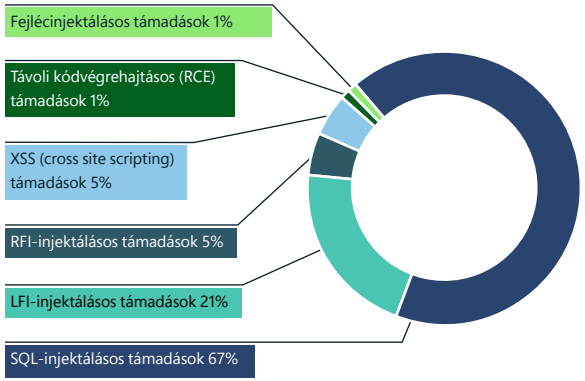


Az ázsiai támadások nagy számát annak tulajdonítjuk, hogy a régió – különösen Kína, Japán, Dél-Korea és India – jelentős részesedést mondhat magáénak a játékszcénában. Ez a részesedés az okostelefonok penetrációjának és azzal együtt a mobiljátékok népszerűségének felfutásával csak növekedni fog, így várhatóan ez a földrajzi régió a továbbiakban is egyre több támadás célpontja lesz.

Webalkalmazások sebezhetőségeinek kihasználása

A webalkalmazási tűzfal (WAF) a DDoS-védelemmel kombinálva szerves részét képezi annak a mélységi védelmi stratégiának, amely a webes és alkalmazásprogramozási felületek (API) eszközeinek védelmét hivatott szolgálni. A Microsoft adatai szerint havonta több mint 300 milliárd WAF-szabály aktiválódik az Azure WAF-eken.

A legelterjedtebb támadástípusok eloszlása



Az Azure WAF több milliárd, az Open Web Application Security Project (OWASP) top 10-es listáján[10] szereplő támadást észlel naponta. A jelek szerint a támadók leggyakrabban SQL-injektálásos támadásokkal próbálkoznak, amelyet a helyi fájl injektálására és a távoli fájl injektálására alapuló támadások követnek. Ez összhangban van az OWASP top tízes listájával, amely szerint az injektálásos támadások képviselik a webes támadások harmadik leggyakoribb típusát.

Emellett nőtt az Azure-webalkalmazások elleni bottámadások száma is, havonta átlagosan 1,7 milliárd botkérelemmel és a rossz botokból álló forgalom 4,6 százalékos részesedésével.

Üzleti rugalmasság kiépítése az erősödő DDoS-, webalkalmazás- és hálózati támadások korában

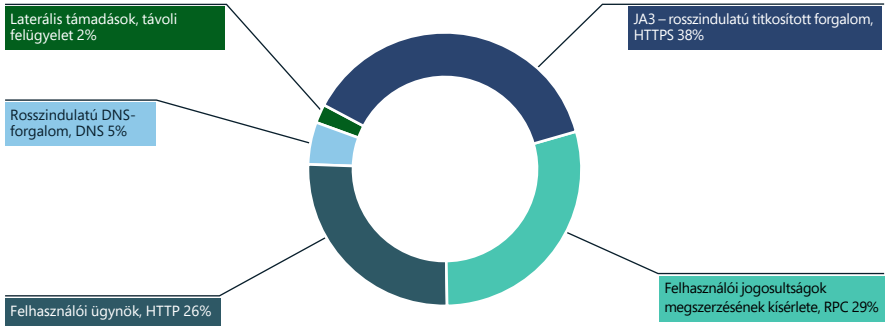
Folytatás

Mivel egyre több bot hajt végre lopott hitelesítő adatokat automatikusan felhasználó („credential stuffing”) támadásokat, hitelkártyacsalásokat, kiberbefolyásolási műveleteket és az ellátási láncot célzó támadásokat, várhatóan folyamatosan növekedni fog a webalkalmazások ellen botokkal elkövetett támadások száma.

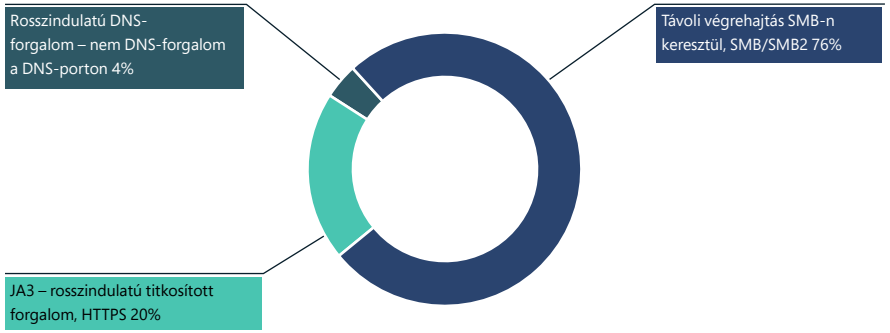
Hálózati behatolás: észlelés és megelőzés

Megfigyeltük, hogy 2022 során jelentős mértékben megnövekedett a hálózati réteget célzó támadások, különösen a rosszindulatú szoftverek száma. Az Azure Firewall behatolásérzékelő és -megelőzési rendszere (IDPS) csak júniusban több mint 150 millió kapcsolatot tiltott le.

Az IDPS általi forgalomletiltás oka



Az IDPS által küldött forgalmi riasztások okai



Az IDPS-riasztásokat és letiltást kiváltó forgalom elemzése azt mutatja, hogy a támadók a következő megközelítéseket alkalmazzák. A letiltott forgalomban láthattuk, hogy a támadók SSL használatával rejtik el tevékenységeiket, és szaporodnak a távoli kódfuttatásos támadások. A riasztást kiváltó forgalomban azt figyeltük meg, hogy az SMB/SMB2 protokollt használják távoli kódfuttatásos támadásokhoz.

Gyakorlati tanácsok

1. Vizsgálja meg a rendszerek és az adatközpont vagy a felhőszolgáltatás közötti összes forgalmat, valamint az ezekhez hozzáférni próbáló forgalmat is.
2. Dolgozzon ki robusztus, a teljes évet lefedő hálózati biztonsági reagálási stratégiát.
3. Használjon felhőnatív biztonsági szolgáltatásokat a robusztus, Zero Trust megközelítést alkalmazó hálózatbiztonsági állapot eléréséhez.

További információra mutató hivatkozások

- A zsarolóprogramos támadások elleni védelem erősítése az Azure Firewall segítségével | Azure Blog and Updates | Microsoft Azure
- Egy DDoS-erősítéses támadás anatómiája | Microsoft Security Blog
- Intelligens alkalmazásvédelem a peremtől a felhőig az Azure Web Application Firewall használatával | Azure Blog and Updates | Microsoft Azure

Az adatbiztonság és a kiberreziliencia kiegyensúlyozott megközelítésének fejlesztése

A digitális átalakulás az adateszközök hatalmas mértékű bővülését és új biztonsági, megfelelőségi és adatvédelmi kockázatok felmerülését hozta magával. A kiberreziliencia kialakítását megcélzó vállalatoknak egyensúlyt kell teremteniük az adatvédelmi, megfelelőségi és helyreállítási képességekbe fektetett erőforrások között, és specializált szabályozási válaszfolyamatokba kell integrálniuk ezeket a különböző típusú betörések kezeléséhez.

Az adatvédelmi incidensekkel kapcsolatban csak az a kérdés, hogy mikor következnek be. Az IBM és a Ponemon Institute „Cost of a Data Breach, 2021" című tanulmánya globális átlagban az adatvédelmi incidensek költségét 4,24 millió dollárra teszi (ami akár 10 százalékos növekedést jelent az előző évhez képest) – ugyanez az érték a tanulmány szerint az Egyesült Államokban 9,05 millió dollár. Megállapították, hogy a megfelelőségi problémák jelentik a legnagyobb költségtöbbszöröző tényezőt. A másik oldalon az adatvédelmi incidensek költségét csökkentő faktorok között említették az olyan bevált módszereket, mint az eseményválasz (IR) megtervezése, a Zero Trust előrehaladott megvalósítása, a biztonsági AI és automatizálás alkalmazása, valamint a titkosítás használata.

Az adatvédelmi incidensek elkerülhetetlenek. A kiegyensúlyozott rugalmassági megközelítést alkalmazó vállalatok azonban csökkenthetik az incidensek gyakoriságát, hatását és költségét.

Az adatgazdálkodás, a biztonság, a megfelelőség és az adatvédelem kölcsönösen függenek egymástól

Láthattuk, hogy az elmúlt években az adatok előtérbe kerültek, és a vállalatok alapvető értékteremtő eszközévé váltak. Ugyanakkor az adatgazdálkodást és az adatbiztonságot előíró adatvédelmi szabályozások erősödésével elmosódott a kockázatkezelési szerepkörök közötti határvonal. Míg az újabb felső vezető szerepkörök, például az adatkezelésért felelős igazgató (CDO) vagy az adatvédelmi vezető (CPO) érdekelt a biztonság és a megfelelőség megteremtésében, az adatvédelem megvalósítása és a napi működésbe való beépítése gyakran az informatikai igazgató (CIO) és/vagy az információbiztonsági igazgató (CISO) által irányított csapatokra marad. Ez azonban nem egyirányú út, hiszen a CDO-k által vezetett adatgazdálkodási kezdeményezések biztonsági előnyökkel is járnak. Ennek az összekapcsolódásnak köszönhetően az informatikai, adatgazdálkodási, biztonsági, megfelelőségi és adatvédelmi csapatoknak még szorosabban együtt kell működniük a hatékonyság érdekében és a kockázatok menedzseléséhez.

A vállalat teljes adatvagyonára kiterjedő adatkockázat-kezelő platformok jelentik a jövőt

Az informatika, az adatgazdálkodás, a biztonság, a megfelelőség és az adatvédelem menedzselését célzó folyamatok összehangolása nehéz feladat egy olyan környezetben, amelyben minden területen testreszabott alkalmazásokat használnak, és inkonzisztens a tipikus vállalati hibrid, többfelhős adatmassza lefedettsége. Úgy gondoljuk, hogy a vállalatoknak egyetlen felületre van szükségük, amelyen keresztül megtalálhatják és megismerhetik az adataikat, megvédhetik őket, szabályozhatják az adatok elérését, használatát és életciklusát, valamint megakadályozhatják az adatvesztést az egész adatvagyonra kiterjedően. A közös adatleltár és tevékenységi információk használata megkönnyíti a csapatközi folyamatokat, átfogóbb képet ad a kockázatokról, és lehetővé teszi a vállalatok számára, hogy jobban előkészítsék és egyszerűsítsék a biztonsági incidensekre adott válaszukat.

Az egyesített felületnek prizmaként kell működnie. Az adatbiztonságban, a megfelelőségben és az adatvédelemben érdekelt csapatoknak eltérő, ám egységes nézetekre van szüksége ugyanarról az adatleltárról és tevékenységekről az összehangolt munkához és együttműködéshez. Az adattevékenységekbe beletartoznak az adatelérési, -módosítási és -mozgatási eseményeket, amelyek fontos részei az adatbiztonsági képletnek.

A hatékony adatgazdálkodás, a biztonság, a megfelelőség és az adatvédelem kölcsönösen függenek egymástól, és a csapatközi együttműködést igényelnek.

Gyakorlati tanácsok

1. Egyensúlyozza ki a védelmet helyreállítási képességekkel, és minimalizálja az adatvédelmi incidensek hatását azzal, hogy befektet a megfelelőségi, adatvédelemi és válaszadási képességekbe.
2. Dolgozzon ki és vezessen be olyan folyamatokat és eszközöket, amelyek lebontják az adatkockázati falakat, és a teljes adatvagyonra kiterjednek.

További információra mutató hivatkozások

- Microsoft Purview – adatvédelmi megoldások | Microsoft Security
- Megérkezett a megfelelőség és az adatgazdálkodás jövője: bemutatkozik a Microsoft Purview | Microsoft Security Blog

A kiberbefolyásolási műveletek kivédése: az emberi tényező

Az elmúlt öt év során a grafika és a gépi tanulás fejlődése olyan, könnyen használható eszközök készítését tette lehetővé, amelyek gyorsan képesek az interneten pillanatok alatt elterjedő, kiváló minőségű, valósághű tartalmakat készíteni.

Az eseményekről szóló szöveges, hangalapú és vizuális híradások terén elérkeztünk egy olyan ponthoz, ahol többé sem emberek, sem algoritmusok nem tudják megbízhatóan megkülönböztetheti a tényeket a fikciótól. Az ilyen eszközök és az általuk előállított tartalmak elterjedése megrengeti a bizalmat a teljes digitális médiában, és felforgatja a helyi és globális események értelmezését. A befolyásolási műveletek technológia fejlődése által lehetővé tett új formái súlyos következményekkel járnak a demokratikus folyamatokra nézve.[11]

Rengeteg kérdés merül fel azzal kapcsolatban, hogy mit tehetünk azért, hogy a jövőben jobban ki tudjuk védeni ezeket a kiberbefolyásolási műveleteket. A technológia csak a kirakó egyik része. Sok területen kell erőfeszítéseket tennünk, többek között médiaműveltségi képzésekre, a tudatosság erősítésére, fokozott éberségre és a minőségi újságírásba – amelynek keretében megbízható tudósítók vannak jelen a helyi, az országos és a nemzetközi színtéren is – való befektetésekre lesz szükség, továbbá a befolyásolási műveletekkel kapcsolatos információmegosztási és riasztási hálózatokat kell kiépíteni, valamint olyan új szabályozást kell megalkotni, amely bünteti a digitális tartalmakat megtévesztési céllal előállító vagy manipuláló rosszindulatú szereplőket.

Azt is tudjuk, hogy a digitális tartalmak iránti bizalom helyreállítása ambiciózus cél, amely különböző perspektívákat és sok szereplő részvételét igényli. Egyetlen vállalat, intézmény vagy kormány sem tudja megoldani ezeket a fenyegetéseket önállóan. Emberként az a szuperképességünk, hogy képesek vagyunk az együttműködésre és a közös munkára. Ez most különösen fontos, mivel mindenkinek – a kormányoknak, a különböző ágazatoknak, az akadémiai szcénának és különösen a hírügynökségeknek és a közösségi, valamint sajtóorgánumoknak világszerte – együtt kell dolgozni a társadalom jobbá és egészségesebbé tételén.

További információra mutató hivatkozások

- A mesterséges intelligencia alkalmazási módjai a Védelmi Minisztérium kiberküldetéseiben | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. A Szenátus fegyveres erőkkel foglalkozó bizottsága alá tartozó kiberbiztonsági albizottság előtti meghallgatás a mesterséges intelligencia kibertérbeli műveletekben való felhasználásáról, 117. kongresszus (2022. május 3., Eric Horvitz tanúvallomása)

Az emberi tényező megerősítése továbbképzésekkel

Az emberi tényező figyelembevétele kulcsfontosságú eleme a kiberbiztonsági készségek fejlesztését célzó stratégiának. A Kaspersky Human Factor in IT Security című tanulmánya[12] szerint a kiberbiztonsági incidensek 46 százalékában része volt egy olyan óvatlan vagy képzetlen munkatársnak, aki akaratán kívül elősegítette a támadást.

A Microsoft Digital Security and Resilience szervezetének oktatási és tudatossági csapata felelős a kiberbiztonság emberi tényezőjének megerősítéséért, amelynek keretében támogatja a munkavállalókat saját és ügyfeleink rendszereinek és adatainak védelmében. Céljaink a következők:

- Csökkenteni szeretnénk a Microsoftra és ügyeleire leselkedő kockázatokat azáltal, hogy összes munkavállalónkat ellátjuk egy központosított, vállalati szintű alapvető biztonsági készségkészlettel.
- Meg szeretnénk erősíteni a munkavállalók biztonsági ismereteit többfázisú megerősítő képzés keretében, hogy elérjük a kívánt viselkedési eredményeket.
- Elő szeretnénk segíti a vállalati kultúra változását azáltal, hogy a biztonságközpontú gondolkodásmódot a Microsoft kultúrájának szerves részévé tesszük évente elvégzendő biztonsági képzésekkel és eseményekkel.
- Be szeretnénk vezetni egy központi, webes erőforrást, amely a bevált gyakorlatoktól a vállalati irányelvekkel kapcsolatos információkon át az incidensek bejelentéséig minden kiberbiztonsági igényt lefed.

Egy célirányos, központi kiberbiztonsági információs program legalább évente egyszer elér minden Microsoft-munkatársat. A képzési ajánlatok a jelenlegi kiberbiztonsági kezdeményezések támogatására és a mérhető viselkedési eredmények elérésére vannak optimalizálva. Microsoft informatikai kockázatkezelési tanácsa (IRMC) kulcsszerepet játszik a kiberbiztonsági magatartás fontos és elérendő változásainak azonosításában, amelyek alapján összeállítjuk a képzéseket.

Az összes kiberbiztonsági képzési programunk esetén mérjük a megoldás hatékonyságát, hatásosságát és kimenetelét. Például belső fenyegetési képzési kínálatunk 95 százalékos képzési megfelelőséget és kivételes tanulói elégedettséget tud felmutatni, valamint azt eredményezte, hogy a vezetők sokkal nagyobb arányban jelentik a belső fenyegetéseket a vállalati Report It Now eszközön keresztül. A program tartalma:

Biztonsági alapok: Központosított, nagyvállalati szintű kiberbiztonsági tudatossági és megfelelőségi képzése, amely az alapvető biztonsági és adatvédelmi gyakorlatokkal foglalkozik. A képzéssorozatot nagy várakozás előzte meg, és az alkalmazott „edutainment" modellnek köszönhetően a kiberbiztonsági ismeretek átadása lebilincselő és érdekes.

STRIKE: A Microsoft kötelező technikai képzése az üzletági megoldásokat készítő és karbantartó mérnököknek. Ez a csak meghívásos alapon elvégezhető képzés a kiberbiztonsági higiénia bevált gyakorlatainak időszerű és kritikus fontosságú területeivel foglalkozik, és a közönség igényeire szabott élő hibrid képzési modellt alkalmaz.

Programspecifikus: A célzott képzési programok támogatják a kiberbiztonsági kezdeményezéseket, többek között az árnyékinfrastruktúrával és a belső fenyegetésekkel kapcsolatos, valamint a Microsoft Federal kezdeményezést. Ezek az ajánlatok szorosan integrálva vannak a vonatkozó kiberbiztonsági kezdeményezések átfogó elkötelezettségi stratégiájába, melynek keretében vezetői szponzorálás és pontozókártyás jelentés segítségével előzzük meg, hogy a résztvevők csak a képzés „kipipálására" törekedjenek.

MSProtect: A Microsoft központi, webes erőforrása a bevált gyakorlatoktól a vállalati irányelvekkel kapcsolatos információkon át az incidensek bejelentéséig minden kiberbiztonsági igényt lefed. Ez a igény szerint elérhető portál a munkatársak formális képzési kínálaton kívüli általános információforrása.

A biztonsági készségeket fejlesztő képzésre nem szabad megfelelőségi, kipipálandó tevékenységként tekinteni. Ehelyett a viselkedés megváltoztatására kell összpontosítani, hogy monitorozni lehessen az eredményeket az azonosított kívánt viselkedési mintáknak való megfelelés szempontjából, és olyan figyelőrendszereket kell kialakítani, amelyekkel meghatározható a képzési ajánlatok hatása.

Gyakorlati tanácsok

1. Biztosítson biztonsági képzést és erőforrásokat a munkavállalóknak, amikor és ahol szükségük van rá.
2. Dolgozzon ki központosított készségfejlesztési stratégiát a vállalat összes érdekeltjének bevonásával.
3. Gondoskodjon a képzés hatásának nyomon követéséről és elemzéséről a hatékonyság (mennyiség), a hatásosság (minőség) és az eredmények (üzleti hatás) szempontjából.

További információra mutató hivatkozások

- A Microsoft elindítja a készségfejlesztési kezdeményezése következő szakaszát, miután 30 millió embernek segített

A zsarolóvírusokat eltávolító programunkból levont tanulságok

A Microsoft az elmúlt öt évben saját, Zero Trust felé vezető útját járta[13] annak érdekében, hogy az identitásokat és az eszközöket robusztus és egészséges módon tudja menedzselni. Ahogyan a zsarolóprogramok jelentette kockázat növekszik, mélyreható ismereteket szereztünk a saját és ügyfeleink védelmét szolgáló megközelítésünk támogatásához.

Alapos belső értékelést követően olyan, zsarolóprogramok elleni programot dolgoztunk ki, amely megszünteti az ellenőrzés és a lefedettség hiányosságait, hozzájárul a szolgáltatások – például a Defender for Endpoint, az Azure és az M365 – funkcióinak fejlesztéséhez, valamint amelynek keretében forgatókönyveket állítottunk össze SOC- és mérnöki csapataink számára a zsarolószoftveres támadás utáni helyreállításhoz.

Az első lépés a Microsoft elleni zsarolóprogramos támadások elleni védelem mértékének felmérése volt. Már régóta folyamatban voltak a Defender for Endpoint bevezetése, valamint annak irányába tett erőfeszítések, hogy minden eszközt menedzseljünk, illetve biztosítsuk Zero Trust-irányelveinknek való megfelelőségüket, azonban módot kellett találnunk rá, hogy megértsük annak az átfogóbb kérdésnek minden aspektusát, hogy valóban hatékonyan helyre tudnánk-e állni egy támadás után. Ennek megértéséhez kiértékeltük a NIST 8374: Zsarolóprogramok jelentette kockázatok kezelése: kiberbiztonsági keretrendszer (CSF) profil[14] ajánlást, amely összhangban van általános vállalati irányelvünkkel az ismert vezérlők tekintetében. Az elemzés gyorsan fényt derített a lefedettség hiányosságaira.

A következő lépésben a CSF észlelési, védelmi, válaszadási és helyreállítási funkciói terén feltárt hiányosságokra összpontosítottunk. Úgy találtuk, hogy stratégiai szinten követjük a Zero Trust és más programok elveit, de olyan hiányosságokat is találtunk, amelyekhez nem rendelkeztünk meglévő munkafolyamattal. Miután felmértük az ezeknek a hiányosságoknak a megszüntetéséhez szükséges munka és erőfeszítés mértékét, két pillérre osztottuk fel őket:

- **A vállalat védelme (PtE):** Olyan munkaelemek meghatározása, amelyeket vállalatként kell elvégeznünk, hogy megvédjük magunkat, és helyre tudjuk állítani működésünket egy esetlegesen sikeres támadás után.
- **Az ügyfél védelme (PtC):** Az ügyfeleink, valamint üzleti tevékenységeink védelmét szolgáló képességek beépítése ajánlatainkba.

Az eredmények beépítése saját vállalatunkba

A legfontosabb kockázatok csökkentéséhez, valamint a kritikus fontosságú szolgáltatásaink zsarolóprogramos támadásokkal szembeni védelméhez azt tervezzük, hogy a következő 6–12 hónapban befektetéseinket a dedikált, zsarolóprogramok elleni programunk részeként az alábbi öt forgatókönyv megvalósítására fogjuk összpontosítani. A forgatókönyvek sikeres megvalósítása után a programot fokozatosan kiterjesztjük a vállalat minden részére.

1. forgatókönyv: A biztonsági csapat tagjai tisztában vannak a zsarolószoftveres támadásokhoz kapcsolódó átfogó kockázattal, és olyan kidolgozott folyamattal rendelkeznek, amely a vezetők figyelmét az ellenőrzési hiányosságokra és a kockázati állapotra irányítja.

2. forgatókönyv: A biztonsági csapat tagjai hozzáférnek olyan forgatókönyvekhez, amelyeket úgy állítottunk össze, hogy segítsék őket és a Microsoft más csapatait egy esetleges zsarolószoftveres támadásra való reagálásban, valamint a kritikus fontosságú szolgáltatások helyreállításában.

3. forgatókönyv: A vállalati rugalmassági csapat tagjai számára rendelkezésre áll egy követendő szabvány a kritikus fontosságú rendszerek biztonsági mentése tekintetében. Kész forgatókönyvek állnak rendelkezésre, és rendszeres biztonsági mentési és helyreállítási gyakorlatokat végeznek annak érdekében, hogy az adatokat helyre lehessen állítani egy zsarolószoftveres támadás esetén.

4. forgatókönyv: A szolgáltatástulajdonosok megértik és implementálják a szükséges biztonsági és üzemeltetési ellenőrzéseket és irányelveket a szolgáltatás, az ügyféladatok, a végpontok és a hálózati eszközök zsarolószoftveres támadások elleni védelme érdekében, különös figyelmet fordítva a Microsoft kritikus fontosságúnak minősített szolgáltatásaira.

5. forgatókönyv: Az összes alkalmazott hozzáférhet az oktatási és képzési erőforrásokhoz, amelyek leírják, hogyan lehet felismerni a zsarolószoftveres támadásokat, és hogyan kell értesíteni a biztonsági csapatot, illetve válaszlépéseket kezdeményezni.

Gyakorlati tanácsok

1. Dokumentálja és validálja a kritikus fontosságú szolgáltatások elleni zsarolóprogramos támadásokkal kapcsolatos, végponttól végpontig tartó helyreállítási és javítási tevékenységeket.
2. Vonja be az érdekelteket a vállalati válságmenedzselési forgatókönyvek frissítésébe, és foglaljanak bele a zsarolóprogramos támadások esetén végzendő specifikus tevékenységeket, és olyan döntési folyamatot és iránymutatást, amelynek segítségével meghatározható, hogy kell-e, és ha igen, mikor kell a zsarolóknak fizetni.
3. Javítsa az észlelési és a védelmi lefedettséget a telepített biztonsági rendszereiben rendelkezésre álló képességek (pl. a Defender for Endpoint támadásifelület-csökkentési szabályai) engedélyezésével.
4. Dolgozzon együtt a biztonsági szabványokat kidolgozó csapattal a zsarolóprogramos támadások elleni védelem alapkonfigurációjának meghatározásához, és biztosítson képzést és dokumentációt a mérnöki csapatok számára az ilyen típusú támadások elleni védekezés módjáról.
5. Állítson be automatizálást a biztonsági és üzemeltetési szabályzatok bevezetésének DevOps-csapatok számára történő megkönnyítéséhez, és gondoskodjon róla, hogy a csökkent megfelelőségű rendszereket gyorsan megjelöljék és kijavítsák.

További információra mutató hivatkozások

Megosztjuk, hogyan védekezik a Microsoft a zsarolóeszközök ellen | Microsoft Inside Track

Nem lehet elég korán cselekedni: a kvantum-számítástechnika biztonsági szempontjai

Egyre sürgetőbb, hogy menedzseljük a kvantum-számítástechnika által a mai kriptográfiai megoldásokra és a velük védett minden adatra jelentett fenyegetést. A nemrégiben kiadott Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] a nemzeti kiberbiztonság fejlesztéséről szóló 10428-as amerikai elnöki rendeletre[16] építkezve kiemeli, hogy a szoftveres ellátási lánc biztonsága kritikus fontosságú a jövő nemzetállami támadásaival szembeni védekezés szempontjából.

Mik azok a kvantumszámítógépek?

A kvantumszámítógépek olyan gépek, amelyek a kvantumfizika tulajdonságait használják az adatok tárolásához és a számítások elvégzéséhez. Ez rendkívül előnyös lehet bizonyos feladatok esetén, amelyekben még a legjobb hagyományos szuperszámítógépek teljesítményét is jelentősen felülmúlhatják. A kvantum-számítástechnika már most is új távlatokat nyit az adattitkosítás és a -feldolgozás területén. A tanulmányok jóslatai szerint a kvantum-számítástechnika már 2030-re több milliárd dolláros (USD) iparággá növi ki magát.[17] A kvantum-számítástechnika és kvantumkommunikáció várhatóan gyökeresen át fog alakítani számos ágazatot az egészségügytől az energiaszektoron át a biztonságig.

A kvantum-számítástechnika veszélyt jelent napjaink kriptográfiai megoldásaira, és mindenre, amit ezekkel védünk.

A mai kriptográfiai megoldásokra jelentett veszély

A Shor 1994-es algoritmusa és egy ipari méretű, néhány millió fizikai qubitnél többel rendelkező kvantumszámítógép segítségével minden jelenleg széles körben használt nyilvános kulcsos kriptográfiai algoritmus hatékonyan feltörhető. Fontos megvizsgálni, kiértékelni és szabványosítani a „kvantumbiztos" titkosítási rendszereket, amely hatékony, agilis és biztonságos megoldást jelentenek az ellenséges kvantumalapú támadások ellen. A szoftverek átállítása „posztkvantum kriptográfiára", azaz a meglévő klasszikus algoritmusok és protokollok kvantumtámadásokkal szembeni megerősítése évekbe – ha nem egy évtizedbe vagy még többe – fog telni.[18]

Ezt azt jelenti, hogy egyre sürgetőbb menedzseljük a mai kriptográfiai megoldásokra és a velük védett minden adatra jelentett fenyegetést. A támadók már most rögzíthetik a titkosított adatokat, hogy később, ha már rendelkezésükre áll egy kvantumszámítógép, feltörjék őket. A kvantum-számítástechnika berobbanása után már túl késő lesz ahhoz, hogy menedzseljük a kriptográfiai kihívásokat.

Mivel a kriptográfia használata átszövi az egész kiber-ökoszisztémát, kriptográfián alapuló biztonsági szolgáltatásaink feltörhetővé válnak. Ez érinteni fogja például a kommunikációs szolgáltatásokat (TLS, IPSec), az üzeneteket (e-mailek, webkonferenciák), az identitás- és hozzáférés-menedzsmentet, a webböngészést, a kódaláírás, a fizetési tranzakciókat és egyéb olyan szolgáltatásokat, amelyek kriptográfiai védelemtől függenek.

Ahogyan a kvantumszámítógépek valósággá válnak, a kriptográfiai algoritmusokat és képességeket implementáló külső szoftverösszetevőket is további ellenőrzésnek kell alávetni. Az értéklánc összes szereplőjének ki kell venni a részét a lánc biztonságossá tételéből. Az iparági testületek és a kormányok egyre nagyobb erőfeszítéseket tesznek a szoftveres ellátási lánc biztonsági követelményeinek meghatározása érdekében, valamint bizonyos esetekben a lánc védelmét szolgáló új szabályokat is bevezetnek. Az NSM-8 nemzetbiztonsági memorandum[19] írja elő posztkvantum kriptográfia nemzetbiztonsági rendszerekben (NSS) való implementációjának követelményeit és ütemtervét. 180 napos időzítési elvárást szab meg a „modernizáció megtervezése, a nem támogatott titkosítás használata, a jóváhagyott feladatspecifikus protokollok, a kvantumtámadásoknak ellenálló protokollok, valamint a kvantumtámadásoknak ellenálló kriptográfia használatának szükség szerinti megtervezése" tekintetében.

A kvantumbiztos kriptográfiára való áttérés szabványosítása hosszú átfutási idejű feladat. A nyilvános kulcsú kriptográfiát használó szabványokon dolgozó szabványügyi testületeknek már most el kell kezdeniük a kísérletezést a posztkvantum algoritmusokkal, illetve a hozzájuk való alkalmazkodást.

Az új posztkvantum kriptográfiai (PQC) algoritmusokat – vagyis a várhatóan a kvantumtámadásoknak ellenálló klasszikus algoritmusokat – már vizsgálják a NIST Post-Quantum Standardization Project keretében.[20] Ez a munka hatással lesz a szabványügyi testületek globális erőfeszítéseire. Bár lesznek átfedések az USA kormányzata által választott algoritmusokkal, a különböző országos tesztületek/szabályozó szervek által megfelelőként választott algoritmusok nemzetközi kihívásokhoz vezethetnek. Ez a széttagoltság pedig meg fogja nehezíti a termékek és szolgáltatások tervezését.

Az új posztkvantum kriptográfiai algoritmusokat már vizsgálják a NIST Post-Quantum Cryptography Standardization programja keretében. Ez a munka hatással lesz a szabványügyi testületek globális erőfeszítéseire.

Gyakorlati tanácsok

A SAFECode és a tagokkal való partnerség mellett az iparágnak azonnali, rövidebb távú lépéseket is kell tennie a PQC-átállásra való felkészülés érdekében.[21] Ezek a következők:

1. Leltárba kell venni a kriptográfiát használó termékeket/kódokat.
2. Olyan kriptoagilitási stratégiát kell megvalósítani a vállalaton belül, amely többek között minimalizálja a kódlemorzsolódást a kriptográfiai változások bekövetkezésekor.
3. Tesztelni kell a kiválasztott kvantumbiztos algoritmusok alkalmazását a kriptográfiát használó termékekben és szolgáltatásokban.
4. Fel kell készülni arra, hogy a titkostáshoz, a kulcsok cseréjéhez és az aláíráshoz különböző nyilvános kulcsú algoritmusokat használunk.
5. Tesztelni kell, hogy milyen hatással van az alkalmazásokra a nagyon nagy méretű kulcsok, rejtjelek és aláírások használata.

További információra mutató hivatkozások

- A Microsoft bemutatta egy újfajta qubit létrehozásához szükséges fizikai alapokat | Microsoft Research

Az üzlet, a biztonság és az információtechnológia egyesítése a nagyobb rugalmasság érdekében

A robusztus kiberreziliencia azon múlik, mennyire tudnak jól együttműködni az üzleti vezetők a biztonsági csapatokokkal a biztonság megvalósítása terén. A Microsoft tapasztalatai szerint a biztonsági vezetők munkája kihívást jelentő terület, amely a vállalati vezetők támogatását igényli a szervezet lehető leghatékonyabb védelme érdekében.

A biztonsági vezetőknek a kihívások dinamikusan változó spektruma mentén kell navigálniuk, és ennek során a kockázatokkal, a technológiával, a közgazdasággal, a szervezeti folyamatokkal, az üzleti modellekkel, a kulturális átalakulással, a geopolitikai érdekekkel, a kémkedéssel és a nemzetközi szankcióknak való megfelelőséggel kapcsolatos témák között kell eligazodniuk. Ezek mindegyikéhez számtalan apró tényezőt kell megismerni és szorosan menedzselni.

A biztonsági vezetők feladatai közé tartozik emellett az intelligens, bőségesen finanszírozott, erősen motivált emberi támadók és az alacsonyan képzett, mégis hatékony, kiberbűnözők támadásainak elhárítása is. Csapataiknak összetett technológiai vagyont kell megvédeniük, amelynek alapjait akár 30 éve vagy még korábban rakták le, amikor a biztonság még nem vagy csak alacsony prioritást kapott – és azóta csak fokozatosan növekedett. Az évekkel ezelőtt hozott döntések ma is kockázatot jelenthetnek, amíg ki nem egyenlítjük a múlt technikai adósságait, és nem szüntetjük meg a biztonság hiányosságokat.

A vállalati vezetők és döntéshozók jelentős pozitív hatást gyakorolhatnak a biztonságra a biztonsági vezetők aktív támogatásával, valamint az integrált biztonság és a vállalati szervezet többi része közötti hídépítés elősegítésével. Amikor a Microsoft olyan ügyfelekkel dolgozik, amelyeknél megvan ez az összhang, akkor a vállalati rugalmasság erősödésének lehetünk tanúi, amely az adott vállalat agilisabb alkalmazkodási és innovációs képességét is magával hozza.

A szervezeti vezetés három fő területre összpontosítva támogathatja a biztonsági vezetőket:

1. Beépített védelem kialakítása

A biztonságot időnként akadálynak vagy valamilyen utólag beépítendő elemnek tekintik az üzleti folyamatokban, és gyakran csak akkor veszik figyelembe a döntésekben, amikor már túl késő van a kockázatok elkerüléséhez, illetve a problémák egyszerű és olcsó javításához.

A szervezeti vezetőknek és a döntéshozóknak biztosítaniuk kell, hogy:

Az új kezdeményezések esetén a biztonságot már a korai szakaszban is figyelembe veszik. Az új digitális kezdeményezések és felhőbevezetések során prioritásként kell kezelni a biztonságot, hogy ne növeljük a szervezeti kockázatot minden új alkalmazással és digitális képességgel. A biztonság megbízható beépítése után ezeket a folyamatokat felhasználva modernizálhatók a régi rendszerek, így egyszerre érhetők el biztonsági és hatékonysági előnyök.

Normalizálják a biztonságot fokozó megelőző karbantartást. Gondoskodni kell róla, hogy az alapvető biztonsági karbantartás – például a biztonsági frissítések és javítások, valamint a biztonságos konfigurációk telepítése – teljes szervezeti támogatást kapjon (beleértve a költségvetést, az ütemezett leállást, valamint a beszállítói terméktámogatási szolgáltatások beszerzési követelményeit).

Sajnos számos vállalat késlelteti, elhalasztja vagy csak részlegesen alkalmazza ezeket az általános gyakorlatokat. Ez számos kihasználható lehetőséget kínál a támadók számára. A biztonság normalizálásának szükségességét az US NIST 800-40 szabvány is rögzíti.[22]

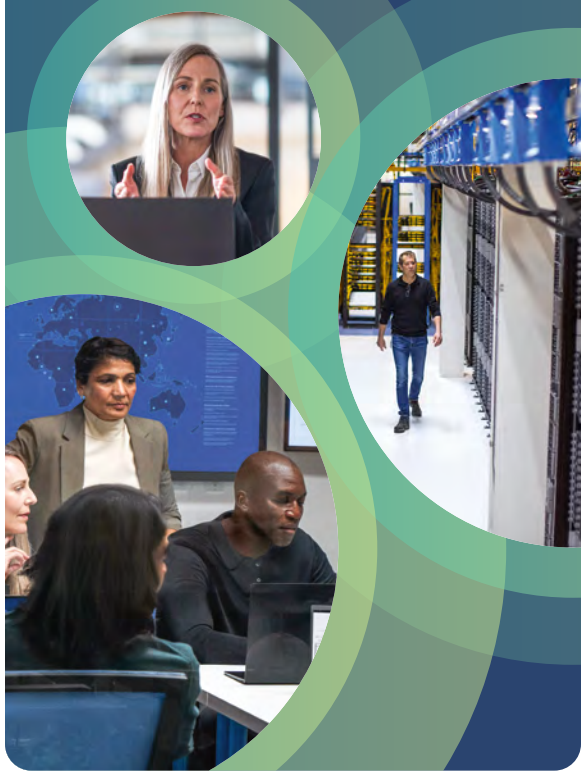
2. Részvétel a biztonság megteremtésében

A szervezeti vezetőknek aktívan részt kell venniük a kulcsfontosságú biztonsági folyamatokban, illetve szponzorálniuk kell őket, hogy biztosítsák az erőforrások priorizálását és a biztonsági katasztrófákra való felkészülést. Ez magában foglalja a következőkben való részvételt:

A kritikus fontosságú üzleti eszközök azonosítása. A biztonsági vezetőknek és csapatoknak tudniuk kell, hogy mely eszközök számítanak üzleti szempontból kritikus fontosságúnak, hogy a biztonsági erőforrásokat a megfelelő helyre összpontosíthassák. Ez gyakran olyan új feladat, amelynek során korábban még nem érintett új kérdéseket kell megfogalmazni és megválaszolni.

Kiberbiztonsági üzletmenet-folytonossági és vészhelyreállítási feladatok. A kibertámadások jelentős eseményekké nőhetik ki magukat, amelyek a legtöbb vagy akár az összes üzleti tevékenységet megzavarják vagy leállítják. A szervezet csapatainak ilyen eseményekre való felkészítése lerövidíti az üzleti működés helyreállításához szükséges időt, mérsékli a szervezet által elszenvedett károkat, valamint segít megtartani az ügyfelek, az állampolgárok és a választók bizalmát.Mindezt be kell építeni a meglévő üzletmenet-folytonossági és vészhelyreállítási folyamatba.

A biztonsági kockázatokkal kapcsolatos döntéseket leg-jobb, ha a cég- vagy küldetéstulaj-donosok hozzák meg, akik teljes rálátással rendelkeznek minden kockázatra és lehetőségre.



Az üzlet, a biztonság és az információtechnológia egyesítése a nagyobb rugalmasság érdekében

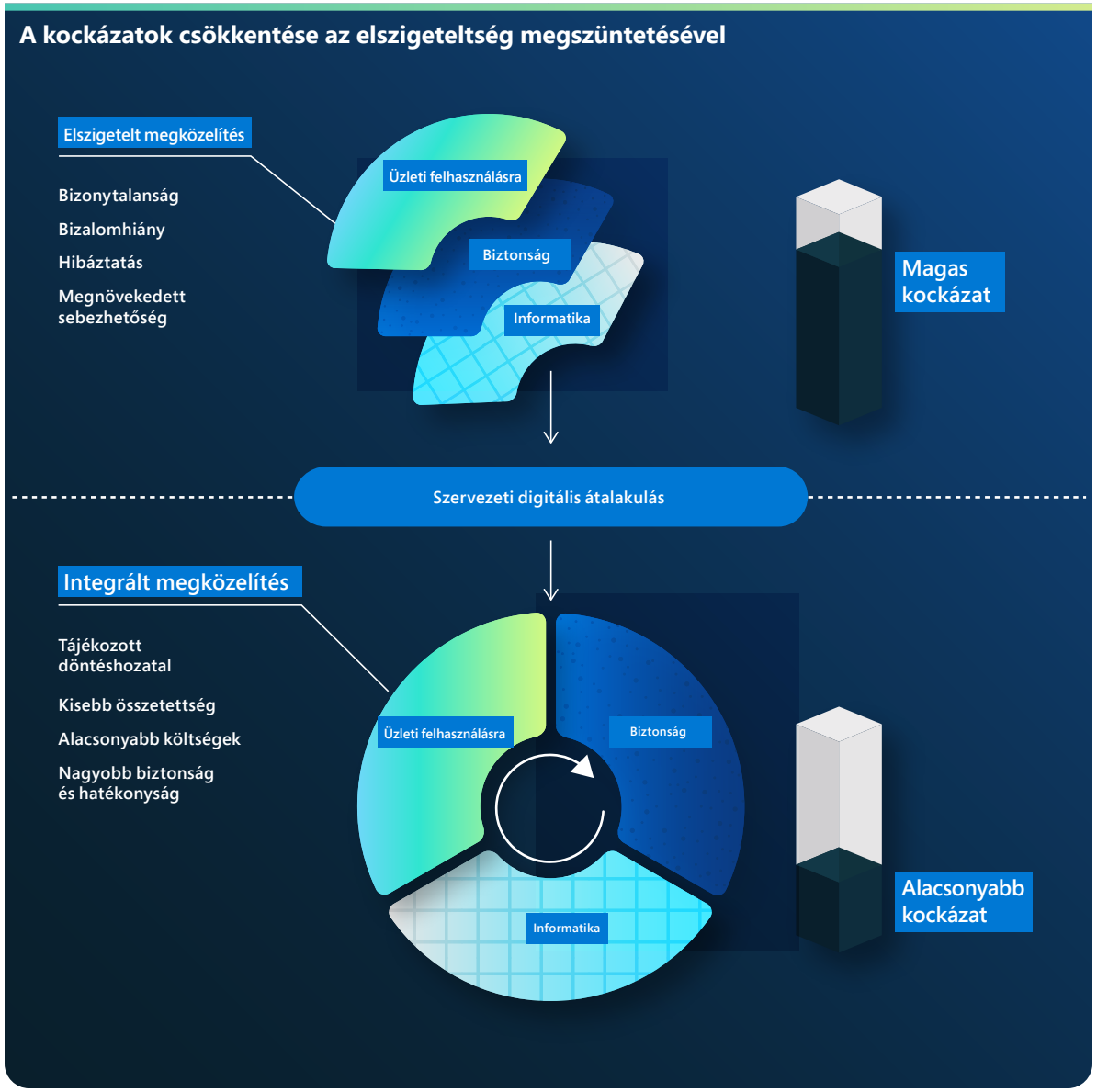
Folytatás

3. A biztonság megfelelő pozicionálása

A biztonsági kockázatokkal kapcsolatos elszámoltathatóság strukturálása a szervezeteknél gyakran vezet ahhoz, hogy rossz döntéseket hoznak a biztonsági kockázatokkal kapcsolatban. A legjobb, ha kockázatokkal kapcsolatos döntéseket a cég- vagy küldetéstulajdonosok hozzák meg, akik teljes rálátással rendelkeznek minden kockázatra és lehetőségre, ám ehelyett a szervezetek gyakran (implicit vagy explicit módon) a biztonsági csapat témaszakértőire hárítják a biztonsági kockázatokkal kapcsolatos felelősséget. Ez egészségtelen terhet ró a biztonsági csapatokra, miközben megfosztja a cégtulajdonosokat a cégükre kockázatot jelentő tényezők megismerésének és kontrollálásának lehetőségétől. A cégek ezt a következő módokon korrigálhatják:

A cégtulajdonosok felkészítése: A cégtulajdonosok tájékoztatása a biztonsági kockázatról, valamint arról, hogy ezek a fenyegetések hogyan befolyásolhatják és befolyásolják a vállalatot. A biztonsági csapatok közvetlen bevonása ebbe az erőfeszítésbe erősíti a biztonsággal és az általános üzleti agilitással fennálló együttműködést.

A biztonsági kockázatok hozzárendelése a cégtulajdonosokhoz: Ha a cégtulajdonosok megfelelő tájékoztatást kapnak a biztonsági kockázatok megismeréséhez és elfogadásához, a szervezeten belül explicit módon rájuk kell osztani a biztonsági kockázatokkal kapcsolatos felelősséget, miközben a kockázatok gyakorlati kezelésének, valamint a tulajdonos szakértő tájékoztatásának és az iránymutatás biztosításának felelősségét továbbra is a biztonsági csapatnál kell hagyni.



„A kiberreziliencia a klasszikus üzleti folytonossággal és vészhelyreállítással kezdődő mozgó skálán helyezkedik el, amelyen az adatok megfelelő biztonsági mentése az első lépcsőfok; majd a folyamatok, a technológia és azok függőségeinek helyreállítási képességeivel (beleértve az embereket és a külső feleket) következik; végül pedig a folyamatosan működő, önjavító szolgáltatásokban, a kritikus szerepkörök rugalmasságában és a kritikus fontosságú külső felekre való átállásban teljesedik ki. A leginkább ellenálló szervezetek elősegítik az integrációt az IT, a vállalatvezetők és a biztonsági szakemberek között. A kiváló rugalmasság eléréséhez a kezdetektől fogva rugalmasra kell tervezni a folyamatokat, továbbá biztonságos változásmenedzsmentet és részletes hibaelkülönítést kell megvalósítani. A kiberreziliencia csupán egy jó, minden veszélyre felkészülő tervezési program egyik forgatókönyve. A kiberkockázatok növekedésével és a kiberbiztonság és a rugalmasság metszetének egyre fontosabbá válásával az információbiztonsági igazgató (CISO) és a vállalati rugalmassági program közötti kapcsolat is erősödik. Évről évre egyre több információbiztonsági igazgató veszi kezébe a vállalati szintű rugalmasságot."

Lisa Reshaur
általános igazgató, kockázatkezelési részleg, Microsoft

További információra mutató hivatkozások

- A rugalmasságtól a digitális boldogulásig: Hogyan használják a szervezetek a digitális technológiát a helyzetük javításához ezekben a példa nélküli időkben | Hivatalos Microsoft blog
- Hogyan működhetnek együtt az IT- és a biztonsági csapatok a végponti biztonság javítása érdekében? | Microsoft Security

A kiberreziliencia haranggörbéje

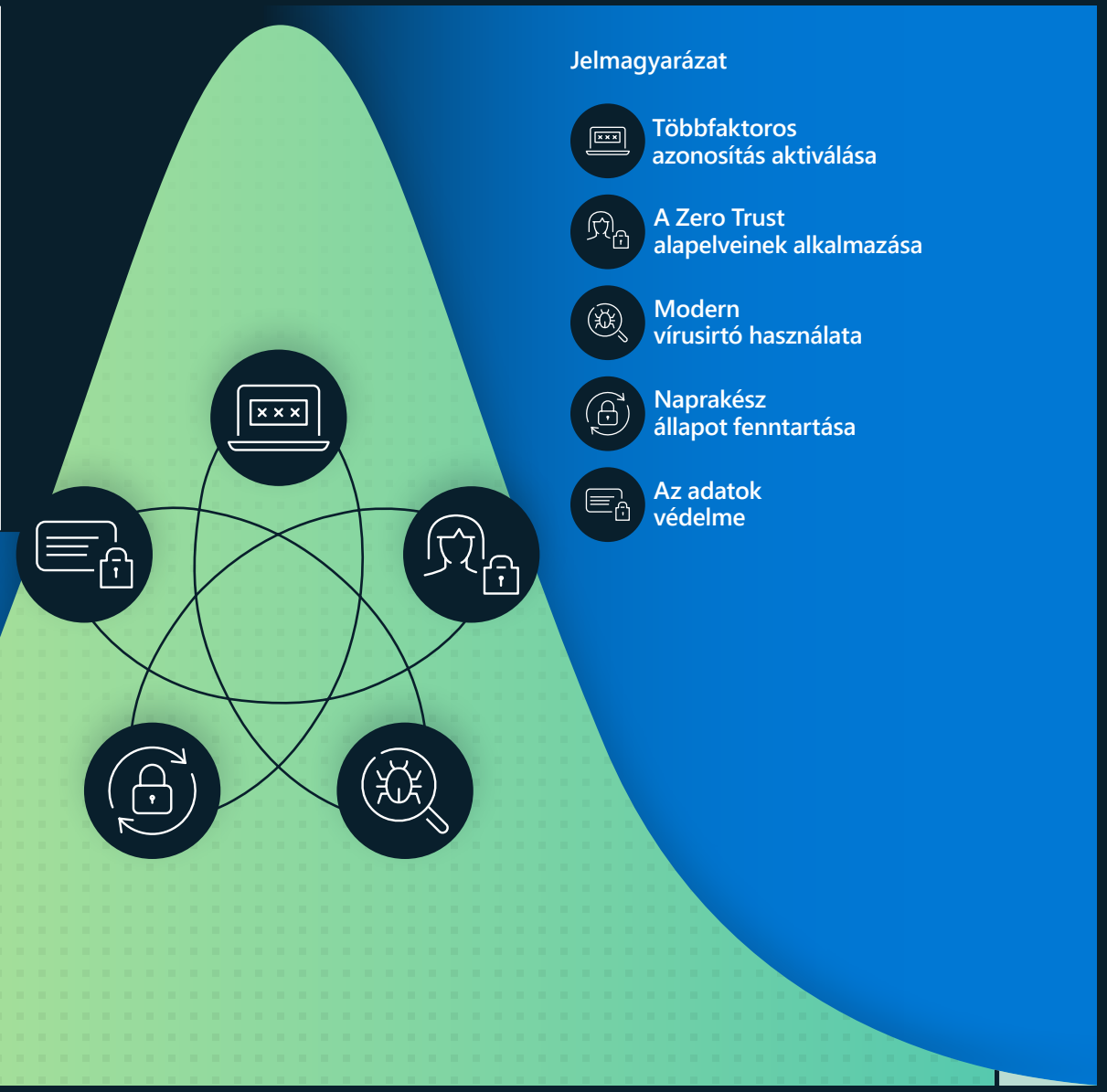
Rugalmassági sikertényezők, amelyeket minden szervezetnek alkalmaznia kell

Mint láttuk, sok kibertámadás csak azért sikeres, mert a célponttá vált szervezetnél nem tartják be az alapvető biztonsági higiéniát. A minden szervezetnél betartandó minimumkövetelmények a következők:

- **A többfaktoros hitelesítés (MFA) bekapcsolása:** Az illetéktelen kezekbe került felhasználói jelszavakkal való visszaélés elleni védekezéshez és kiegészítő védelmi vonalként az identitásokhoz.
- **A Zero Trust alapelveinek alkalmazása:** Minden rugalmassági terv sarokköve a szervezetre gyakorolt hatás mérséklése. Ezek az alapelvek a következők:
  1. – Explicit ellenőrzés – a felhasználók és az eszközök megfelelő állapotának ellenőrzése, mielőtt hozzáférést kapnának az erőforrásokhoz.
  2. – Legalább jogosultságú hozzáférés használata – kizárólag az adott erőforráshoz való hozzáférést és nem többet lehetővé tévő jogosultság biztosítása.
  3. – Biztonsági incidens feltételezése – annak feltételezése, hogy a rendszerek védelmét feltörték, és illetéktelenek szereztek hozzáférést. Ez azt jelenti, hogy folyamatosan figyelni kell a környezetet egy esetleges támadás jeleit keresve.
- **Bővített észlelési és reagálási képességeket biztosító vírusirtó használata:** Olyan szoftverek bevezetése, amelyek észlelik és automatikusan blokkolják a támadásokat, és rálátást biztosítanak a biztonsági műveletekre. A fenyegetésészlelési rendszerekből származó elemzések monitorozása elengedhetetlen a fenyegetésekre való időszerű reagáláshoz.
- **Naprakész állapot fenntartása:** A javítás nélkül maradt és elavult rendszerek a leggyakoribb okai annak, hogy a szervezetek támadások áldozatául esnek. Gondoskodjon az összes rendszer naprakészen tartásáról, beleértve a firmware-t, az operációs rendszert és az alkalmazásokat.
- **Az adatok védelme:** A fontos adatok, a tárolási helyük, valamint annak megismerése, hogy a megfelelő rendszerek vannak-e üzembe állítva, elengedhetetlen a megfelelő védelem megvalósításához.

98%

Az alapvető biztonsági higiénia továbbra is véd a támadások 98%-a ellen.



Végjegyzet

1. A végponti észlelés és reagálás (EDR) egy vállalati végpontvédelmi platform, amelynek célja, hogy segítse a vállalati hálózatokat a speciális fenyegetésekkel szembeni megelőzésben, észlelésben, kivizsgálásban és reagálásban. A végponti észlelési és reagálási képességek fejlett, közel valós idejű támadásészlelést biztosítanak, amely a gyakorlatban használható eredményt ad. A biztonsági elemzők hatékonyan rangsorolhatják a riasztásokat, rálátást kaphatnak a biztonsági incidensek teljes hatókörére, és megfelelő választ adhatnak a fenyegetések elhárításához.
2. A végpontvédelmi platform (EPP) a végponti eszközökre telepített olyan megoldás, amely megakadályozza a fájlalapú kártevők bejutását, észleli és letiltja a megbízható és nem megbízható alkalmazások rosszindulatú tevékenységeit, valamint biztosítja azokat a vizsgálati és javítási képességeket, amelyek a biztonsági incidensekre és riasztásokra való dinamikus válaszadáshoz szükségesek.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows biztonsági kézikönyv: Kereskedelmi
7. A Windows 11 új biztonsági funkciói segítenek a hibrid munka védelmében | Microsoft Security Blog
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Executive Order 14028 – Improving the Nation's Cybersecurity
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. „The Long Road Ahead to Transition to Post-Quantum Cryptography", https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Közreműködő csoportok

Közreműködő csoportok

A jelentésben szereplő adatokat és információkat biztonságfókuszú szakemberek sokszínű csoportjától kaptuk, melynek tagjai különböző Microsoft-csapatokban dolgoztak. Közös céljuk a Microsoft és ügyfelei, illetve az egész világ kibertámadások elleni védelme. A transzparencia jegyében büszkén osztjuk meg ismereteinket, amelyek reményeink szerint mindenki számára segítenek biztonságosabbá tenni a világot.

AI for Good Research Lab: Az adatok és az AI erejét használja fel a világ számos kihívásának leküzdéséhez. A labor a Microsofton kívüli szervezetekkel is együttműködik, és az AI-t a megélhetés és a környezet javításához használja. Fókuszterületei közé tartozik az online biztonság (a dezinformáció, a kiberbiztonság és a gyermekek védelme), a katasztrófaelhárítás, a fenntarthatóság és az AI for Health program.

Azure Edge & Platform, Enterprise & OS Security: A Windows, az Azure és egyéb Microsoft-termékek alapvető operációsrendszer- és platformbiztonságáért felelős. A csapat iparágvezető biztonsági és hardveres megoldásokat épít be a Microsoft-platformokba, amelyekkel a chiptől a felhőig terjedően visszaszorítja a sebezhetőségek kihasználását, az identitásokkal való visszaélését és a rosszindulatú szoftvereket. Ez a csapat hozta létre a Microsoft személyi számítógépeken, peremhálózaton és szervereken használt Secured-core platformját, a Microsoft Pluton Security Processor architektúrát és más technológiákat.

Azure Networking, Core: Felhőbeli hálózatkezelésre összpontosító csapat, amely elsősorban a Microsoft WAN-hálózattal, az adatközponti hálózatokkal, valamint az Azure szoftveresen meghatározott hálózati infrastruktúrájával – köztük a DDoS-platformmal, a hálózatiszegély-platformmal és az olyan hálózatbiztonsági termékekkel foglalkozik, mint az Azure WAF, az Azure Firewall és Azure DDoS Protection Standard.

Cloud Security Research csapat: A Microsoft-felhő védelme, innovatív biztonsági funkciók és termékek fejlesztése, valamint kutatások révén ez a csapat védi és támogatja a Microsoft ügyfeleit abban, hogy biztonságos módon alakulhassanak át.

Customer Security and Trust (CST): Ez a csapat vásárlóink biztonságát hivatott fokozni a Microsoft termékeiben és internetes szolgáltatásaiban. Céljuk, hogy a cég különböző tervező- és biztonsági csoportjaival együttműködve biztosítsák a szabályozási környezetnek való megfelelést, továbbá hogy fejlesszék a védelmet és a transzparenciát, ezzel védve ügyfeleinket, és növelve a Microsoft iránti globális bizalmat.

Customer Success: A Customer Success, azaz ügyfélsikerek területén tevékenykedő biztonsági csapatok közvetlenül az ügyfelekkel dolgoznak, hogy megosszák velük a bevált gyakorlatokat, tanulságokat és útmutatásokat a biztonsági átalakítás és a modernizálás felgyorsításához. Ez a csapat összegyűjti a Microsoft – és az ügyfelei – útja során kidolgozott bevált módszereket és tanulságokat, és referenciastratégiákba, referenciaarchitektúrákba, referenciatervekbe és egyebekbe rendszerezi őket.

Cyber Defense Operations Center (CDOC): A Microsoft kiberbiztonsági és védelmi szervezete a cég biztonsági szakembereit összegyűjtő központ. Céljuk a vállalati infrastruktúránk és a vásárlóink által használt felhőinfrastruktúránk védelme. A Microsoft különböző szolgáltatásain, termékein és készülékein dolgozó vészelhárítók, adattudósok és biztonsági szakértők közösen fejtik ki nonstop védelmi, detekciós és reakciós tevékenységüket.

Democracy Forward Initiative: A Microsoft azon csapata, amelynek feladata a demokrácia alapjainak megőrzése, védelme és előmozdítása azáltal, hogy elősegíti az egészséges információs ökoszisztéma megteremtését, a nyílt és biztonságos demokratikus folyamatok védelmét, valamint támogatja a vállalatok társadalmi felelősségvállalását.

Digital Crimes Unit (DCU): Jogászokból, nyomozókból, adattudósokból, mérnökökből, elemzőkből és üzleti szakemberekből álló csapat, amely globális szinten veszi fel a harcot a kiberbűnözés ellen technológiai és kriminalisztikai eszközök alkalmazásával, polgári perekkel, bűnügyi beszámolókkal, illetve köz- és magánszférabeli partnerségekkel.

Digital Diplomacy: Volt diplomatákból, politikai döntéshozókból és jogi szakértőkből álló nemzetközi csapat, amely a békés, stabil és biztonságos kibertér megteremtésén dolgozik az egyre erősödő nemzetállami konfliktusok közepette.

Digital Security & Resilience (DSR): Ez a szervezet azzal a céllal jött létre, hogy a Microsoft a lehető legmegbízhatóbb készülékeket és szolgáltatásokat készíthesse, miközben a cég, valamint a cég és ügyfelei adatai biztonságban maradnak.

Digital Security Unit (DSU): Kiberbiztonságra szakosodott jogászokból és elemzőkből álló csoport, amely jogi, geopolitikai és műszaki ismereteivel segíti a Microsoft és vásárlói védelmét. A DSU segíti a Microsoft fejlett kibertámadások elleni védelme iránti bizalom elmélyítésében.

Digital Threat Analysis Center (DTAC): Olyan szakértőkből álló csapat, amely elemzéseket és jelentéseket készít a nemzetállami fenyegetésekről – többek között a kibertámadásokról és a befolyásolási műveletekről. A csapat az információkat és a fenyegetésfelderítési adatokat geopolitikai elemzéssel egyesíti, majd ezek alapján a hatékony reagálás és védelem kidolgozásához szükséges anyagokat állít össze a Microsoft és ügyfelei számára.

Enterprise and Security: Ez a csapat az intelligens felhő és az intelligens peremhálózat számára biztosít modern, biztonságos és kezelhető platformot.

Enterprise Mobility: Olyan csapat, amely segít modern munkahelyet és menedzsmentet biztosítani az adatok védelméhez – úgy a felhőben, mint helyben. A Endpoint Manager tartalmazza azokat a szolgáltatásokat és eszközöket, amelyeket a Microsoft és az ügyfelei használnak a mobileszközök, az asztali gépek, a virtuális gépek, a beágyazott eszközök és szerverek menedzseléséhez és monitorozásához.

Közreműködő csoportok

Folytatás

Enterprise Risk Management: Ez a csapat üzleti egységeken átívelően dolgozik azon, hogy priorizálja a kockázatokkal kapcsolatos párbeszédet a Microsoft felső vezetésével. Az ERM több operatív kockázatot kezelő csoporttal működik együtt, menedzseli a Microsoft vállalati kockázati keretrendszerét, és elősegíti a cég belső biztonsági értékelését a NIST kiberbiztonsági keretrendszerének használatával.

Global Cybersecurity Policy: Ez a csoport állami szervekkel, civil szervezetekkel és ipari partnerekkel karöltve népszerűsíti azt a kiberbiztonsági politikát, ami lehetővé teszi ügyfeleinknek biztonságuk és ellenállóképességük erősítését a Microsoft technológiáival.

Identity and Network Access (IDNA) Security: Ez a csoport védi az összes Microsoft-ügyfelet a jogosulatlan hozzáféréstől és a csalásoktól. Az IDNA Security mérnökök, termékmenedzserekből, adattudósokból és biztonsági nyomozókból álló multidiszciplináris csapat.

M365 Security: Ez a szervezet biztonsági megoldásokat fejleszt, többek között a Végponthoz készült Microsoft Defender (MDE), a Microsoft Defender for Identity (MDI) és más, a vállalati ügyfelek biztonságát szolgáló termékeket.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Az Microsoft új technológiák felelős felhasználásában segítő tanácsadó testülete.

Microsoft Bing Search and Distribution: A csapat célja, hogy világszínvonalú internetes keresőmotort kínáljon, amely világszerte lehetővé tesz a felhasználóknak, hogy megbízható keresési találatokból gyorsan informálódjanak, és kövessék azokat a témaköröket és felkapott sztorikat, amelyek fontosak számukra, miközben kézben tarthatják az adataik védelme feletti kontrollt.

Microsoft Customer and Partner Solutions: A Microsoft egységes piaci bevezetési szervezete, amelynek ügyfeleknél dolgozó IT-biztonsági és műszaki értékesítési specialisták és tanácsadók a tagjai.

Microsoft Defender Experts: A Microsoft legnagyobb globális szervezete, amelyet a termékekre fókuszáló kiberbiztonsági kutatók, alkalmazott kutatók és a veszélyfelderítési elemzők alkotnak. A Defender Experts innovatív észlelési és reagálási funkciókat fejleszt az Microsoft 365 biztonsági termékeihez és a Microsoft Defender Experts menedzselt szolgáltatásokhoz.

Microsoft Defender for IoT: Szakértő kutatókból álló csapat, amely az IoT-/OT-kártevők, -protokollok és -firmware-ek visszafejtésére szakosodott. A csapat az IoT-/OT-fenyegetésekre vadászik, hogy felfedje a rosszindulatú trendeket és műveleteket.

Microsoft Defender Threat Intelligence (RiskIQ): Ez a csapat taktikai felderítési adatokat állít össze a Microsoft kiterjedt külső telemetriai adatgyűjtése alapján, valamint felméri a változó fenyegetési környezetet, hogy felfedje a korábban ismeretlen fenyegetési infrastruktúrát, és kontextusba helyezze a rosszindulatú szereplőket és műveleteket. A csapat rendszeresen tesz közzé időszerű és egyedi kutatásokat, hogy létfontosságú taktikai információkkal lássa el a védekezőket.

Microsoft Security Business Development Team: Ez a csapat vezeti a Microsoft kiberbiztonsági növekedési stratégiáját, partnerségeit és stratégiai beruházásait.

Microsoft Security Response Center (MSRC): A csapat biztonsági kutatókkal közösen dolgozik a Microsoft ügyfeleiből és partnereiből álló ökoszisztéma védelmén. A Microsoft Cyber Defense Operations Center (CDOC) szerves részét képező MSRC összefogja a biztonsági vészelhárítókat a valós idejű védelem, észlelés és reagálás érdekében.

Microsoft Security Services for Incident Response: Kiberbiztonsági szakértőkből álló csapat, amely a kibertámadás teljes feldolgozásán végigvezeti az ügyfeleket a kivizsgálástól kezdve a sikeres elszigetelési és helyreállítással kapcsolatos tevékenységekig. A szolgáltatásokat két, magasan szinten integrált csapat biztosítja: a Detection and Response Team (DART), amely a vizsgálatra és a helyreállítás alapjaira összpontosít, valamint a Compromise Recovery Security Practice (CRSP), amely az elszigetelési és helyreállítási szempontokat helyezi előtérbe.

Microsoft Threat Intelligence Center (MSTIC): A Microsoft ügyfeleit veszélyeztető legkifinomultabb és legfejlettebb ellenfelekkel – állami csoportokkal, kártevőgyártókkal, adathalászokkal stb. – kapcsolatos azonosítási, nyilvántartási és hírszerzési tevékenységekkel foglalkozik.

One Engineering System (1ES): Ennek a csapatnak a küldetése, hogy világszínvonalú eszközöket biztosítson a Microsoft fejlesztői számára, amelyekkel a lehető leghatékonyabban és legbiztonságosabban dolgozhatnak. A csapat vezeti a Microsoft teljes szoftverellátási láncának védelmét célzó központi stratégiát.

Operational Threat Intelligence Center (OpTIC): Ez a csapat felelős a kiberfenyegetésekkel kapcsolatos információk terjesztéséért, amelyek támogatják a Microsoft Cyber Defense Operation Center (CDOC) küldetését, azaz a Microsoft és ügyfelei védelmét.

Microsoft

Bepillantást nyerhet a fenyegetések világába, és segítséget kaphat a digitális védekezéshez.

- További információ: **https://microsoft.com/mddr**
- Merüljön el a témában: **https://blogs.microsoft.com/on-the-issues/**
- Maradjunk kapcsolatban: **@msftissues és @msftsecurity**