Microsoft

Zpráva společnosti Microsoft o digitální obraně 2022

Přehled prostředí hrozeb
a posílení digitální obrany.

Obsah

Pokud není uvedeno jinak, data, přehledy a události v této zprávě pocházejí z období od července 2021 do června 2022 (pro Microsoft je to fiskální rok 2022).

Pro nejpohodlnější zobrazení a prohlížení této zprávy doporučujeme použít software Adobe Reader, který si lze zdarma stáhnout na webu společnosti Adobe.

Úvodní slovo Toma Burta

Corporate Vice President, Customer Security & Trust

„Biliony signálů, které analyzujeme z našeho celosvětového ekosystému produktů a služeb, odhalují závažnost, dosah a rozsah digitálních hrozeb po celém světě“

Pohled na naše prostředí...

Rozsah a měřítko prostředí hrozeb

Objem útoků na hesla vrostl na odhadovaných 921 útoků každou sekundu – 74% nárůst za pouhý jeden rok.

Boj s kybernetickou kriminalitou

Do dnešního dne Microsoft odebral více než 10 000 domén využívaných kyberzločinci a 600 domén používaných aktéry národních států.

Řešení chyb v zabezpečení

93 % našich aktivit při reakci na ransomwarové incidenty odhalilo nedostatečné řídicí mechanismy pro privilegovaný přístup a taktiku lateral movement.

Dne 23. února 2022 vstoupil svět kybernetického zabezpečení do nového věku, věku hybridní války. Toho dne, hodiny před odpálením raket a přejezdem tanků přes hranice, zahájili ruští aktéři masivní ničivý kybernetický útok na ukrajinské cíle ve státní správě i v technologickém a finančním sektoru. Více se o těchto útocích a o tom, jak se z nich poučit, dozvíte v kapitole Hrozby ze strany národních států v tomto třetím ročním vydání Zprávy společnosti Microsoft o digitální obraně (MDDR). Nejdůležitějším poučením je to, že cloud nabízí nejlepší fyzické a logické zabezpečení před kybernetickými útoky a přináší inovace v analýze hrozeb a ochraně koncových bodů, jejichž hodnota se projevila na Ukrajině.

I když jakýkoli průzkum ročního vývoje v kybernetickém zabezpečení musí začínat právě tímto tématem, letošní zpráva se do problematiky ponoří mnohem hlouběji. V první kapitole této zprávy se zaměřujeme na aktivity kyberzločinců, po kterých následují hrozby ze strany národních států v kapitole druhé. Obě skupiny značně propracovaly své útoky, čímž dramaticky vzrostl dopad jejich operací. Zatímco Rusko moderovalo titulky článků, íránští aktéři v návaznosti na změnu prezidenta posílili své útoky a zahájili ničivé útoky na Izrael spolu s ransomwarovými a hackerskými operacemi, kterými cílili na kritickou infrastrukturu ve Spojených státech. Také Čína zintenzivnila své špionážní úsilí v jihovýchodní Asii a na jiných místech na jižní polokouli s cílem oponovat vlivu USA a ukrást důležitá data a informace.

Cizí aktéři navíc využívají vysoce efektivní techniky, které umožňují šířit propagandu v nejrůznějších oblastech světa. Tomu se věnujeme ve třetí kapitole. Rusko například intenzivně pracovalo na přesvědčování svých občanů i občanů mnoha jiných zemí, že jeho invaze na Ukrajinu byla oprávněná. K tomu šířilo propagandu, která měla na Západě zdiskreditovat očkování proti covidu a zároveň propagovat jejich účinnost na domácím území. Kromě toho aktéři stále častěji cílí na zařízení internetu věcí (IoT) nebo řídicí zařízení provozních technologií (OT), která využívají jako vstupní body do sítí a kritické infrastruktury. O tom pojednává čtvrtá kapitola. Poslední kapitola je pak věnována přehledům a poznatkům, ke kterým jsme došli za poslední rok při obraně před útoky cílenými na Microsoft a naše zákazníky. Projdeme si vývoj v kybernetické odolnosti za poslední rok.

Každá kapitola nabízí hlavní zjištěné poznatky a přehledy, které Microsoft může předložit díky svému jedinečnému úhlu pohledu. Biliony signálů z našeho celosvětového ekosystému produktů a služeb, které analyzujeme, odhalují dravost, rozsah a měřítko digitálních hrozeb po celém světě. Microsoft činí kroky, kterými před těmito hrozbami chrání své zákazníky a digitální ekosystém. Vy si teď můžete přečíst o naší technologii, která identifikuje a blokuje miliardy pokusů o phishing, krádež identity a další útoky na naše zákazníky.

Úvodní slovo Toma Burta

pokračování

Právními i technickými prostředky zajišťujeme a vypínáme infrastrukturu, kterou využívají aktéři kyberzločinu a národních států, a oznamujeme zákazníkům, že jsou ohroženi nebo napadeni aktérem národního státu. Pracujeme na vývoji stále efektivnějších funkcí a služeb, které pomocí technologií AI/ML identifikují a blokují kybernetické hrozby. Odborníci na zabezpečení rychleji a efektivněji zajišťují identifikaci kybernetických útoků a obranu před nimi.

A co je možná nejdůležitější, v celém MDDR nabízíme naše nejlepší rady, jak se jednotlivci, organizace a podniky můžou bránit před těmito stále závažnějšími digitálními hrozbami. Nejlepší obranou je přijmout osvědčené postupy kybernetické hygieny. Dá se tak významně snížit riziko kybernetických útoků.

Situace v oblasti kybernetické kriminality

Kyberzločinci nadále působí jako sofistikované ziskové podniky. Útočníci se přizpůsobují a hledají nové způsoby, jak své techniky uvést do praxe. Kvůli tomu jsou principy a místa hostování infrastruktury pro operace kampaní stále složitější. Kyberzločinci jsou zároveň stále hospodárnější. V rámci snižování režijních nákladů a posilování zdání legitimity útočníci napadají firemní sítě a zařízení, na kterých hostují phishingové kampaně či malware, nebo dokonce i využívají jejich výpočetní výkon k těžbě kryptoměn.

> **Více se dozvíte na str. 6**

„Nasazením kybernetických zbraní v hybridní válce na Ukrajině započal nový věk konfliktů.“

Hrozby ze strany národních států

Aktéři národních států zahajují své stále propracovanější kybernetické útoky navržené tak, aby se nedaly snadno zjistit a podpořily jejich strategické priority. Nasazením kybernetických zbraní v hybridní válce na Ukrajině započal nový věk konfliktů. Rusko svou válku podpořilo i operacemi ovlivňování informací, když pomocí propagandy ovlivňovalo názory v Rusku, na Ukrajině i po celém světě. Mimo Ukrajinu aktéři národních států zintenzivnili své aktivity a začali využívat pokroků v technologiích automatizace, cloudové infrastruktury a vzdáleného přístupu, s nimiž útočí na širší skupinu cílů. Častými cíli byly firemní dodavatelské řetězce pro IT, které umožňují přístup ke konečným cílům. Teď, když aktéři rychle zneužívají neopravené chyby v zabezpečení, používají důmyslné techniky i hrubou sílu ke krádeži přihlašovacích údajů a zakrývají své operace pomocí opensourcového nebo legitimního softwaru, je hygiena kybernetické bezpečnosti důležitější než kdy dříve. Kromě Ruska pak ničivé kybernetické zbraně, včetně ransomwaru, používá i Írán, který na nich zakládá své útoky.

Tato situace vyžaduje urychlené přijetí konzistentní celosvětové architektury, která upřednostňuje lidská práva a chrání lidi před bezohledným chováním států na internetu. Všechny národy musí spolupracovat na implementaci norem a pravidel pro odpovědné chování států.

> **Více se dozvíte na str. 30**

Zařízení a infrastruktura

Pandemie spolu s rychlým zaváděním nejrůznějších zařízení připojených k internetu, které tvoří součást stále rychlejší digitální transformace, značně rozšířily potenciální oblast útoku v našem digitálním světě. Toho kyberzločinci a národní státy rychle využívají. I když je zabezpečení IT hardwaru a softwaru v posledních letech důkladnější, zabezpečení zařízení IoT a OT se tak rychle nevyvíjí. Aktéři hrozeb tato zařízení zneužívají k zajištění přístupu do sítí a přípravě taktiky lateral movement, získání výchozího bodu v dodavatelském řetězci nebo k narušení operací OT v cílové organizaci.

> **Více se dozvíte na str. 56**

Úvodní slovo Toma Burta

pokračování

Operace ovlivňování v kyberprostoru

Národní státy ve stále větší míře využívají důmyslné operace ovlivňování, kterými šíří propagandu a ovlivňují veřejné mínění jak na svém vlastním území, tak za svými hranicemi. Tyto kampaně podkopávají důvěru, podporují polarizaci a ohrožují demokratické procesy. Zkušení aktéři pokročilých trvalých manipulací používají tradiční média spolu s internetem a sociálními médii ke značnému navýšení rozsahu, měřítka a efektivity svých kampaní. Díky tomu mají obrovský dopad na globální informační ekosystém. Za poslední rok jsme tyto operace pozorovali v rámci hybridní války Ruska na Ukrajině, ale zároveň jsme zjistili, že Rusko a jiné státy, třeba Čína a Írán, stále častěji nasazují operace propagandy a využívají k tomu sociální média. Rozšiřují tak svůj globální vliv na nejrůznější problémy.

Více se dozvíte na str. 71

Kybernetická odolnost

Zabezpečení představuje stěžejní prvek technologického úspěchu. Inovací a vyšší produktivity je možné dosáhnout jen zavedením bezpečnostních opatření, s nimiž budou organizace co nejodolnější vůči moderním útokům. Pandemie pro nás v Microsoftu představovala výzvu, jak upravit postupy a technologie zabezpečení tak, aby chránily naše zaměstnance bez ohledu na místo, odkud pracují. V tomto uplynulém roce aktéři hrozeb i nadále využívali chyb v zabezpečení objevených během pandemie a přesunu do hybridního pracovního prostředí. Od té doby je největším problémem převaha a složitost různých metod útoku a větší aktivita národních států. V této kapitole podrobně rozebereme výzvy, kterým jsme čelili, a obranu zavedenou ve spolupráci s našimi více než 15 000 partnery.

Více se dozvíte na str. 86

Náš jedinečný úhel pohledu

37 mld.
zablokovaných e-mailových hrozeb

34,7 mld.
zablokovaných hrozeb pro identitu

43 bil.
signálů každý den syntetizovaných pomocí propracované analýzy dat a algoritmů AI, s nimiž získáváme informace k obraně před digitálními hrozbami a zločinnou kybernetickou aktivitou

2,5 mld.
signálů z koncových bodů analyzovaných každý den

Přes 8500
inženýrů, výzkumníků, datových vědců, odborníků na kybernetickou bezpečnost, analytiků hrozeb, geopolitických analytiků, vyšetřovatelů a respondérů v předních liniích ve více než 77 zemích

Přes 15 000
partnerů v našem ekosystému zabezpečení, kteří zvyšují kybernetickou odolnost našich zákazníků

od 1. července 2021 do 30. června 2022

Úvodní slovo Toma Burta

pokračování

Myslíme si, že Microsoft sám i prostřednictvím blízkých partnerství s ostatními v privátním sektoru, státní správě a občanské společnosti nese odpovědnost za ochranu digitálních systémů, které jsou základem naší společnosti a podporují bezpečná výpočetní prostředí pro kohokoli, ať už pochází odkudkoli. Tato odpovědnost je důvodem, proč od roku 2020 každý rok vydáváme MDDR. Zpráva představuje vyvrcholení poznatků z obrovských dat a komplexního výzkumu Microsoftu. Najdete v ní naše jedinečné přehledy o tom, jak se vyvíjí prostředí digitálních hrozeb a jakými nezbytnými opatřeními je možné už dnes zlepšit zabezpečení ekosystému.

Doufáme, že se nám podaří vysvětlit naléhavost, s jakou by čtenáři měli okamžitě zavést opatření na základě dat a přehledů, které představujeme jak tady, tak v mnoha našich publikacích o kybernetické bezpečnosti vydávaných v průběhu roku. Až budeme přemýšlet nad závažností hrozeb digitálního prostředí a nad jejich dopady na fyzický svět, je důležité nezapomenout, že všichni máme ve své moci podniknout kroky, abychom ochránili sami sebe, naše organizace a podniky před digitálními hrozbami.

Děkujeme, že jste si udělali čas a přečetli si letošní Zprávu společnosti Microsoft o digitální obraně. Doufáme, že v ní najdete cenné poznatky a doporučení, která nám společně pomůžou bránit digitální ekosystém.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Touto zprávou sledujeme dva cíle:

1. Chceme vysvětlit vyvíjející se prostředí digitálních hrozeb pro naše zákazníky, partnery a zúčastněné strany v širším ekosystému a vrhnout světlo jak na nové kybernetické útoky, tak na nové trendy v historicky přetrvávajících hrozbách.
2. Chceme našim zákazníkům a partnerům umožnit vylepšit kybernetickou odolnost a reakce na tyto hrozby.

Situace v oblasti kybernetické kriminality

Se stále dokonalejší obranou před kybernetickými útoky a se stále větším počtem organizací, které zaujímají aktivní postoj k prevenci, musí útočníci přizpůsobovat své techniky.

Přehled

situace v oblasti kybernetické kriminality

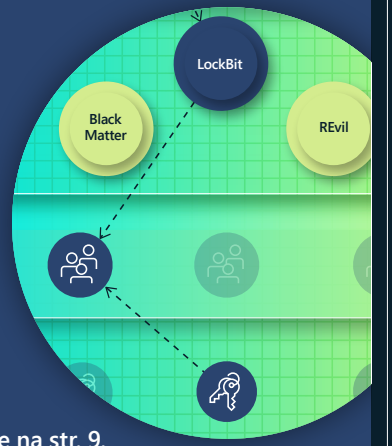
Se stále dokonalejší obranou před kybernetickými útoky a se stále větším počtem organizací, které zaujímají aktivní postoj k prevenci, musí útočníci přizpůsobovat své techniky.

Kyberzločinci nadále působí jako sofistikované ziskové podniky. Útočníci se přizpůsobují a hledají nové způsoby, jak své techniky uvést do praxe. Kvůli tomu jsou principy a místa hostování infrastruktury pro operace kampaní stále složitější. Kyberzločinci jsou zároveň stále hospodárnější. V rámci snižování režijních nákladů a posilování zdání legitimity útočníci napadají firemní sítě a zařízení, na kterých hostují phishingové kampaně či malware, nebo dokonce i využívají jejich výpočetní výkon k těžbě kryptoměn.

Kybernetická kriminalita je i nadále na vzestupu, protože industrializace ekonomiky kybernetického zločinu snižuje nároky na dovednosti. Je totiž snazší získat přístup k potřebným nástrojům a infrastruktuře.

Více se dozvíte na str. 18.

Hrozba ransomwaru a vydírání je pak o to smělejší, když je zacílena na státní správy, firmy a kritickou infrastrukturu.

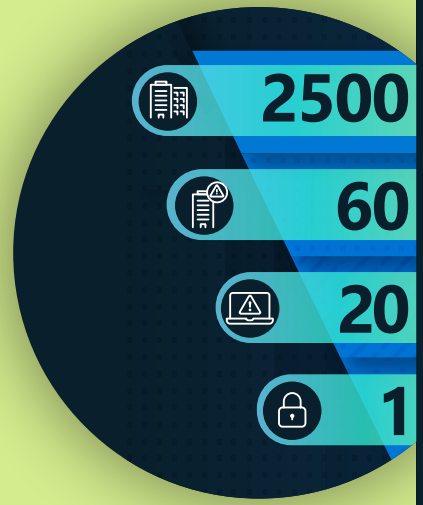


Více se dozvíte na str. 9.

Útočníci stále častěji vyhrožují zveřejněním citlivých údajů, aby dosáhli zaplacení výkupného.

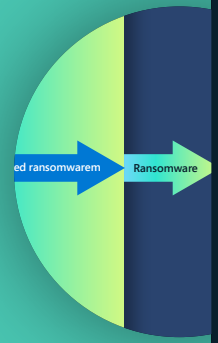
Více se dozvíte na str. 10.

Nejčastějším útokem je člověkem řízený ransomware. Třetina cílů je úspěšně napadena zločinci, které tyto útoky používají, a 5 % z nich zaplatí výkupné.



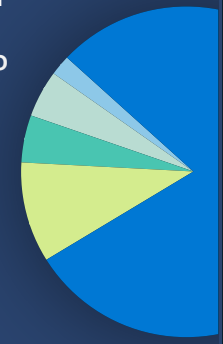
Více se dozvíte na str.9

Mezi nejúčinnější způsoby, jak se bránit ransomwaru, patří vícefaktorové ověřování, časté opravy zabezpečení a principy Zero Trust (nulové důvěry) v celé síťové architektuře.



Více se dozvíte na str. 13

Schémata phishingu přihlašovacích údajů, které bez rozdílu cílí na všechny schránky, zažívají rozmach. Napadání firemních schránek, včetně podvodů s fakturami, představuje pro podniky výrazné riziko kybernetické kriminality.



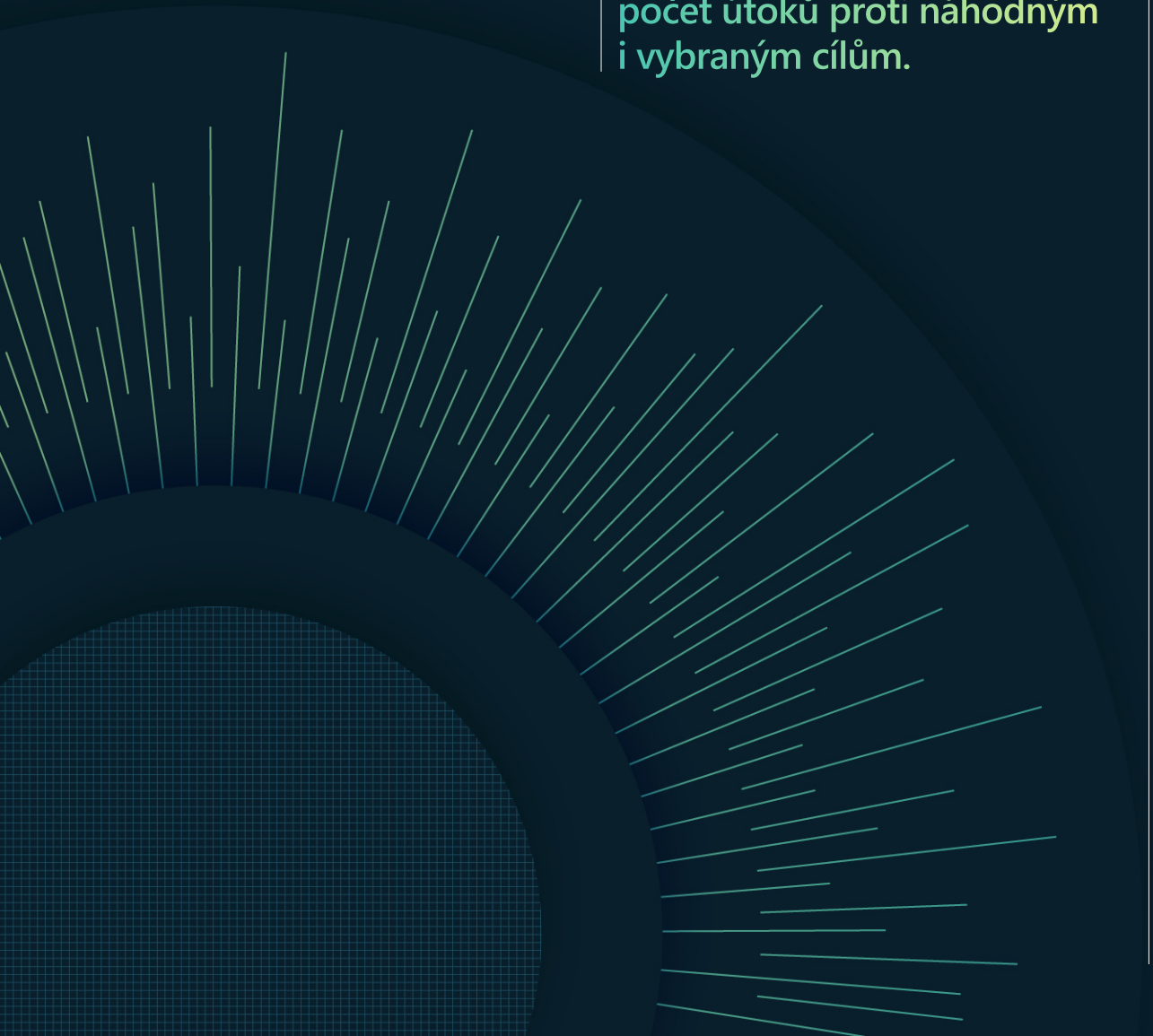
Více se dozvíte na str. 21.

Aby mohl Microsoft narušovat škodlivé infrastruktury kyberzločinců a aktérů národních států, spoléhá na inovativní právní přístupy a svá veřejná a privátní partnerství.

Více se dozvíte na str. 25.

Úvod

Kybernetická kriminalita je stále na vzestupu, narůstá počet útoků proti náhodným i vybraným cílům.



Se stále dokonalejší obranou před kybernetickými útoky a se stále větším počtem státních správ a firem, které zaujímají aktivní postoj k prevenci, využívají útočníci dvě strategie, jak získat přístup potřebný k usnadnění kybernetického zločinu. Jedním z přístupů je kampaň se širokou škálou cílů, která spoléhá na množství. Ten druhý používá průzkum a selektivnější cílení, jehož cílem je zvýšit návratnost. I v případě, že cílem není vygenerovat výnos, třeba při aktivitách národních států z geopolitických důvodů, se používají náhodné i cílené útoky. V uplynulém roce kyberzločinci i nadále spoléhali na sociální inženýrství a zneužívání tematických problémů, aby maximalizovali úspěch kampaní. Například i když se phishingové nástrahy s tématikou covidu používaly méně často, zpozorovali jsme nárůst nástrah, které žádají o dar na podporu občanů Ukrajiny.

Útočníci se přizpůsobují a hledají nové způsoby, jak své techniky uvést do praxe. Kvůli tomu jsou principy a místa hostování infrastruktury pro operace kampaní stále složitější. Zjistili jsme, že kyberzločinci začínají být hospodárnější a útočníci už za technologie neplatí. V rámci snižování režijních nákladů a posilování zdání legitimity se někteří útočníci stále častěji pokoušejí napadnout firmy, aby mohli hostovat phishingové kampaně či malware, nebo dokonce i využívat jejich výpočetní výkon k těžbě kryptoměn.

V této kapitole prozkoumáme rizika hacktivismu, tedy narušení způsobených soukromými občany, kteří kybernetické útoky provádějí s cílem podpořit určité společenské nebo politické cíle. Od února 2022 začaly v rámci rusko-ukrajinské války útočit tisíce jednotlivců po celém světě z řad odborníků i začátečníků, například s cílem vyřadit weby a zveřejnit kradená data. Ještě je brzy předvídat, jak se tento trend bude dále vyvíjet po ukončení aktivit znesvářených stran.

Organizace musí pravidelně kontrolovat a posilovat řídicí mechanismy přístupu a implementovat bezpečnostní strategie, kterými se brání před kybernetickými útoky. Můžou ale udělat i více. Vysvětlíme, jak náš tým Digital Crimes Unit (DCU) využil civilní případy k zajištění škodlivé infrastruktury, kterou používají kyberzločinci a aktéři národních států. Této hrozbě musíme čelit společně prostřednictvím veřejných i privátních partnerství. Naší nadějí je, že sdílením našich poznatků z posledních 10 let pomůžeme jiným porozumět situaci a zvážit aktivní opatření, která můžou zavést pro ochranu sebe samých i širšího ekosystému před stále rostoucí hrozbou kybernetické kriminality.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

Ransomware a vydírání: Hrozba na národní úrovni

Ransomwarové útoky představují značné nebezpečí pro všechny jednotlivce, protože zločinci cílí na kritickou infrastrukturu, firmy všech velikostí a státní i místní správy. Při tom využívají rostoucí ekosystém kybernetické kriminality.

V posledních dvou letech si velkou pozornost veřejnosti získaly známé ransomwarové incidenty, třeba ty, které se týkaly kritické infrastruktury, zdravotnictví a poskytovatelů IT služeb. S rostoucími ambicemi ransomwarových útoků se stále více různí i jejich účinky. Následují příklady útoků, které jsme již zaznamenali v roce 2022:

- V únoru došlo k útoku na dvě společnosti, který ovlivnil systémy zpracování plateb stovek čerpacích stanic na severu Německa.[1]
- Březnový útok na řecké poštovní služby dočasně narušil doručování pošty a měl dopad na zpracovávání finančních transakcí.[2]
- Ke konci května způsobil ransomwarový útok na státní úřady Kostariky vyhlášení národního nouzového stavu, protože přestaly fungovat nemocnice a došlo k narušení výběru cla a daní.[3]
- Rovněž v květnu došlo k útoku, který způsobil zpoždění a zrušení letů jedné z největších indických leteckých společností, kvůli čemuž uvízly stovky pasažérů.[4]

Úspěch těchto útoků a rozsah jejich dopadů na skutečný svět jsou výsledkem industrializace ekonomiky kybernetické kriminality, která umožňuje přístup k nástrojům a infrastruktuře a rozšiřuje možností kyberzločinců tím, že už nemusí být tak technicky zdatní.

V posledních letech se ransomware přesunul z modelu, kdy jeden „gang" vyvinul a distribuoval škodlivý ransomwarový program, na model ransomwaru jako služby (RaaS). RaaS umožňuje jedné skupině výměnou za podíl na zisku spravovat vývoj škodlivého ransomwarového programu a platební a vyděračské služby prostřednictvím úniků dat jiným kyberzločincům. Těm se říká „partneři" a jsou to oni, kdo ve skutečnosti zahajují ransomwarové útoky. Tento franšízing ekonomiky kybernetického zločinu rozšířil působnost útočníků. Industrializace nástrojů pro kybernetickou kriminalitu usnadnila útočníkům průniky do systémů, exfiltraci dat a nasazování ransomwaru.

Člověkem řízený ransomware[5] – pojem zavedený výzkumníky Microsoftu, kterým popisují hrozby řízené osobami, které v každé fázi útoku činí rozhodnutí podle nových zjištění v cílové síti, a odlišují tuto hrozbu od komoditních ransomwarových útoků – zůstává pro organizace významným nebezpečím.

Model založený na datech Microsoft Defenderu for Endpoint (EDR) (leden–červen 2022)

Ransomware a vydírání: Hrozba na národní úrovni

pokračování

Ransomwarové útoky teď mají ještě větší dopad díky tomu, že se standardním postupem stala monetizační strategie dvojího vydírání. Ta zahrnuje exfiltraci dat z napadaných zařízení, jejich zašifrování na zařízení a pak zveřejnění nebo vyhrožování zveřejněním kradených dat, aby oběť musela zaplatit výkupné.

I když většina ransomwarových útočníků nasazuje ransomware podle naskytnuté příležitosti do jakékoli sítě, ke které získají přístup, někteří si kupují přístup od jiných kyberzločinců a využívají propojení mezi zprostředkovateli přístupu a operátory ransomwaru.

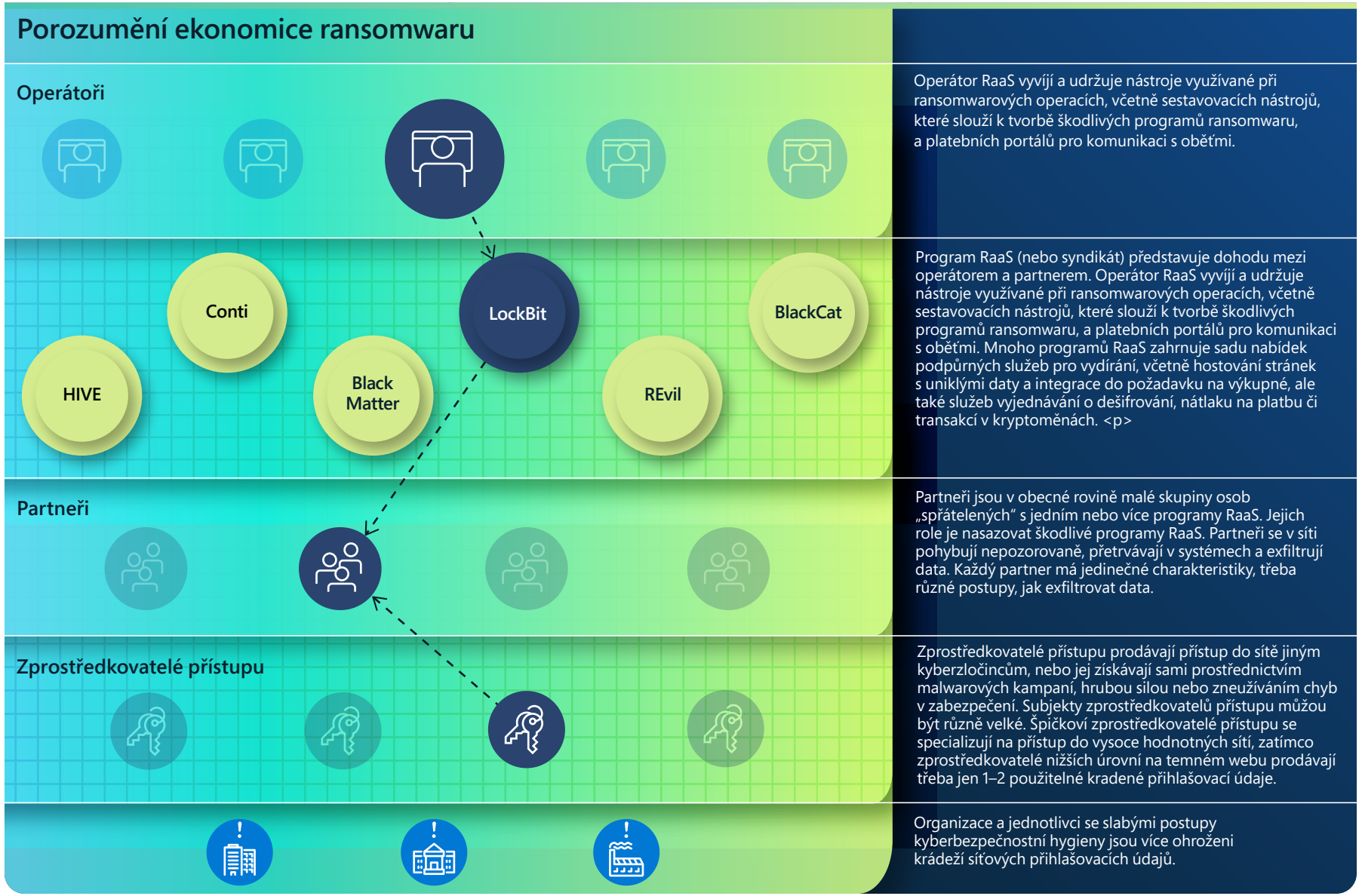
Naše jedinečná škála informací o signálech pochází z několika zdrojů – identit, e-mailů, koncových bodů a cloudu – a nabízí přehledy o rostoucí ekonomice ransomwaru, včetně systému partnerů a nástrojů navržených pro méně technicky zdatné útočníky.

Prohlubování vztahů mezi specializovanými kyberzločinci přineslo rychlejší, důmyslnější a úspěšnější ransomwarové útoky. To pak vedlo k tomu, že se ekosystém kybernetické kriminality přetvořil na systém propojených aktérů s různými technikami, cíli a dovednostmi, kteří se vzájemně podporují v prvotním přístupu k cílům, platebním službám a nástrojům nebo webům pro dešifrování či zveřejňování.

Operátoři ransomwaru si teď můžou koupit přístup k sítím organizací nebo státní správy online nebo získat přihlašovací údaje a přístup prostřednictvím mezilidských vztahů se zprostředkovateli, jejichž hlavním cílem je jen zpeněžit získaný přístup.

Operátoři pak zakoupený přístup využijí k nasazení škodlivého ransomwarového programu pořízeného na tržištích nebo fórech na temném webu. V mnoha případech jednání s oběťmi vede tým RaaS, nikoli samotní operátoři. Tyto zločinné transakce jsou velmi propracované a riziko pro účastníky, že by byli zatčeni a obviněni, je kvůli anonymitě temného webu a problémům při vynucování práva na mezinárodní úrovni nízké.

Udržitelné a úspěšné úsilí proti této hrozbě bude vyžadovat implementaci strategie, na které se bude podílet celá státní správa v úzkém partnerství se soukromým sektorem.



Navzdory tomu, jak je ransomware někdy vyobrazen v médiích, není obvyklé, aby jednu variantu ransomwaru spravoval jeden komplexní „ransomwarový gang“. Existují samostatné subjekty, které vytvářejí malware, získávají přístup k obětem, nasazují ransomware a vedou vydírací vyjednávání. Industrializace zločinného ekosystému dala vzniknout:

- zprostředkovatelům přístupu, kteří získávají přístup a ten pak předávají dále (přístup jako služba)
- vývojářům malwaru, kteří prodávají nástroje
- zločinným operátorům a partnerům, kteří provádějí útoky
- poskytovatelům služeb šifrování a vydírání, kteří přebírají monetizaci od partnerů (RaaS)

Všechny kampaně člověkem řízeného ransomwaru spolu sdílí závislost na slabých stránkách zabezpečení. Konkrétně útočníci zpravidla využívají nedostatečnou kybernetickou hygienu společnosti, která často obnáší nepříliš časté aktualizace a chybějící implementaci vícefaktorového ověřování (MFA).

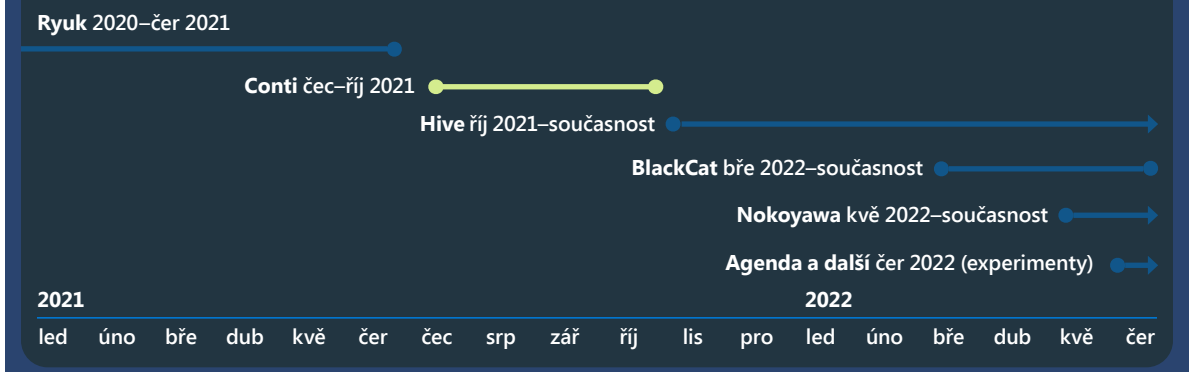
Případová studie: Zánik programu Conti

Conti je jednou z nejúspěšnějších variant ransomwaru za poslední dva roky. V polovině roku 2022 začalo ukončovat svou činnost a centrum Microsoft Threat Intelligence Center (MSTIC) zjistilo výrazný pokles aktivity ke konci března a na začátku dubna. Poslední nasazení ransomwaru Conti jsme zaznamenali v polovině dubna. Nicméně stejně jako u jiných ukončených operací ransomwaru nemělo zrušení programu Conti významný dopad na nasazování ransomwaru. Centrum MSTIC zjistilo, že partneři Conti přešli na nasazování jiných škodlivých ransomwarových programů, například BlackBasta, Lockbit 2.0, LockbitBlack a HIVE. To je v souladu s údaji z předchozích let a naznačuje to, že když dojde k ukončení činnosti ransomwarových gangů, o několik měsíců později se objevují znovu nebo přerozdělují své technické možnosti a prostředky novým skupinám.

Naše týmy pro analýzu hrozeb v Microsoftu sledují aktéry ransomwarových hrozeb jako jednotlivé skupiny (označené jako DEV) spíše podle jejich konkrétních nástrojů než podle malwaru, který používají. To znamená, že když byli partneři programu Conti rozpuštěni, mohli jsme i nadále tyto DEV sledovat podle toho, jak používali jiné nástroje nebo sady RaaS. Například:

- DEV-0230, který je partnerem Trickbotu, byl velmi aktivním uživatelem programu Conti. Ke konci dubna jej centrum MSTIC zpozorovalo při používání QuantumLockeru.
- DEV-0237 přešel ze sady ransomwaru Conti na HIVE a Nokoyawu. 31. května pak použil HIVE k útoku na státní úřady na Kostarice.
- DEV-0506, další aktivní uživatel ransomwarové sady Conti, byl přistižen při používání malwaru BlackBasta.

Příklad partnera (DEV-0237) a jeho rychlých přechodů mezi programy RaaS



Jakmile je program RaaS, jako je Conti, ukončen, partneři ransomwaru přecházejí téměř okamžitě na jiný (Hive).

RaaS rozvíjí ekosystém ransomwaru a znesnadňuje hledání viníků

Jelikož člověkem řízený ransomware je ovládán konkrétními operátory, způsoby útoku se liší podle cíle a v průběhu útoku se mění. V minulosti jsme zaznamenali těsnou souvislost mezi volbami počátečního vektoru průniku, nástrojů a škodlivého ransomwarového programu v jednotlivých kampaních konkrétního kmene ransomwaru. Díky tomu bylo hledání viníka snazší. Model partnerů RaaS však tento vztah rozděluje. Kvůli tomu Microsoft nesleduje vývojáře škodlivého ransomwarového programu jako operátory, sleduje spíše partnery ransomwaru, kteří programy nasazují při konkrétních útocích.

Jinými slovy už nepředpokládáme, že operátorem za ransomwarovým útokem HIVE je vývojář HIVE. Je pravděpodobnější, že to bude nějaký partner.

Odvětví kybernetické bezpečnosti se usilovně snaží vhodně toto odlišení vývojářů a operátorů zachytit. Často se v tomto odvětví ransomwarové incidenty hlásí podle názvu škodlivého programu, kvůli čemuž vzniká mylný dojem, že za všemi útoky s využitím toho konkrétního programu může jeden subjekt, jeden ransomwarový gang, a že všechny související incidenty používají společné techniky a infrastrukturu. Pro podporu obránců sítí je důležité zjistit více o fázích, které předcházejí útokům různých partnerů (třeba exfiltrace dat a další mechanismy trvalosti), a také o případných příležitostech k detekci a ochraně.

Ještě více než malware útočníci potřebují přihlašovací údaje, se kterými zajistí úspěch svých operací. Úspěšné napadení celé organizace člověkem řízeným ransomwarem závisí na přístupu k vysoce privilegovanému účtu.

Vybrané útoky člověkem řízeným ransomwarem

Za poslední rok odborníci Microsoftu na ransomware provedli hloubkové šetření více než 100 incidentů člověkem řízeného ransomwaru s cílem sledovat techniky útočníků a porozumět, jak lépe chránit naše zákazníky.

Je důležité si uvědomit, že analýzu, kterou tady uvádíme, je možné provést jen pro nasazená spravovaná zařízení. Nenasazená a nespravovaná zařízení představují nejméně zabezpečenou část hardwarových prostředků organizace.

Nejčastější techniky ransomwarové fáze:

75 %
používá nástroje pro správu.

75 %
používá získaný napadený účet se zvýšenými oprávněními k šíření škodlivých programů přes protokol SMB.

99 %
se pokouší upravit zjištěné zabezpečení a zálohovat produkty pomocí nástrojů integrovaných do operačního systému.

Typický útok řízený člověkem

Útoky člověkem řízeným ransomwarem se dají rozdělit do dvou kategorií: fáze před ransomwarem a fáze nasazení ransomwaru. Během fáze před ransomwarem se útočníci připravují na průnik do sítě. Během těchto příprav zkoumají typologii a infrastrukturu zabezpečení organizace.

Zastavení útočníků dříve, než se dostanou do fáze nasazení ransomwaru	**Nasazení!**
Před ransomwarem	**Ransomware**
Tato fáze může trvat od několika dní po několik týdnů až měsíců, i když se v posledních dvou letech její doba trvání zkracovala.	Tato fáze může trvat jen minuty.
Příprava útočníků na průnik do sítě spočívá ve zjišťování co největšího množství informací o topologii a infrastruktuře zabezpečení. V této fázi můžou útočníci také exfiltrovat data.	Útočníci se snaží zašifrovat co největší množství dat.

Během šetření jsme zjistili, že většina aktérů stojících za útoky člověkem řízeným ransomwarem využívá podobné slabé stránky zabezpečení a má shodné způsoby a techniky útoku.

Odolná strategie zabezpečení

Boj s takovými útoky a prevence před nimi vyžaduje změnu v procesech organizace tak, aby se zaměřovala na komplexní ochranu potřebnou ke zpomalení a zastavení útočníků ještě předtím, než se dostanou z fáze před ransomwarem do fáze nasazení ransomwaru.

Podniky musí konzistentně a aktivně zavádět ve svých sítích osvědčené postupy zabezpečení s cílem zmírnit různé třídy útoků. Kvůli lidskému rozhodování dokážou tyto ransomwarové útoky generovat více zdánlivě nesouvisejících upozornění bezpečnostních produktů, která se snadno ztratí nebo na ně není včas reagováno. K zahlcení upozorněními skutečně dochází a centra Security Operations Center (SOC) si můžou usnadnit práci tím, že se podívají na trendy ve svých upozorněních nebo seskupí upozornění do incidentů. Tak získají celkový nadhled. Pak můžou SOC upozornění zmírnit funkcemi posílení zabezpečení, třeba pomocí pravidel pro omezení potenciální oblasti útoku. Posílení zabezpečení před běžnými hrozbami dokáže nejen snížit počet upozornění, ale i zastavit mnoho útočníků dříve, než získají přístup do sítí.

Organizace musí neustále udržovat vysoké standardy stavu zabezpečení a síťové hygieny, aby se chránily před útoky člověkem řízeným ransomwarem.

Poznatky a jejich využití

Útočníci, kteří využívají ransomware, jsou motivováni snadným ziskem. Proto je pro narušení ekonomiky kybernetické kriminality klíčové zvýšit jejich náklady tím, že posílíte zabezpečení.

1. Zaveďte hygienu přihlašovacích údajů. Ještě více než malware útočníci potřebují přihlašovací údaje, se kterými zajistí úspěch svých operací. Úspěšné napadení celé organizace člověkem řízeným ransomwarem závisí na přístupu k vysoce privilegovanému účtu, třeba ke správci domény, nebo na schopnosti upravit zásady skupiny.
2. Proveďte audit zpřístupňování přihlašovacích údajů.
3. Považujte nasazování aktualizací služby Active Directory za jednu z priorit.
4. Jako prioritu zaveďte i posílení zabezpečení cloudu.
5. Zmenšete potenciální oblast útoku.
6. Posilte zabezpečení k internetu připojených prostředků a důkladně se seznamte se svým perimetrem.
7. Snižte zahlcení SOC upozorněními posílením sítě tak, aby se snížil počet upozornění a zachovala šířka pásma pro incidenty s vysokou prioritou.

Odkazy na další informace

- RaaS: Seznámení se zakázkovou ekonomikou a způsoby ochrany | Microsoft Security Blog
- Útoky člověkem řízeným ransomwarem: Katastrofa, které se dá předejít | Microsoft Security Blog

Poznatky o ransomwaru od respondérů v první linii

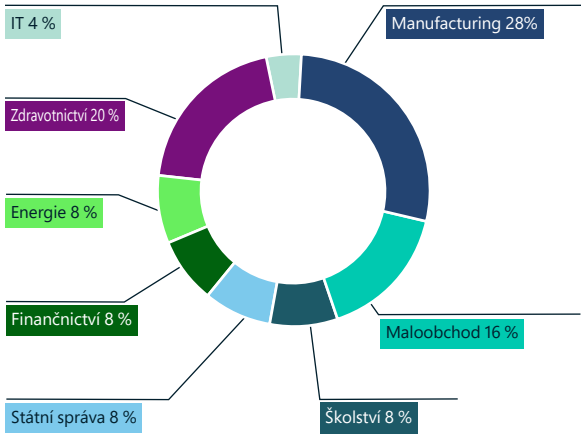
Organizace po celém světě čelí už od roku 2019 stabilnímu nárůstu útoků člověkem řízeným ransomwarem. Významný dopad na organizace kybernetického zločinu však měly operace policejních složek a geopolitické události za poslední rok.

Linka služby zabezpečení Microsoftu podporuje zákazníky v průběhu celého kybernetického útoku, od vyšetřování až po úspěšnou obranu a činnosti při zotavení. Služby reakce a zotavení se nabízejí prostřednictvím dvou vysoce integrovaných týmů. Jeden se zaměřuje na vyšetřování a připravuje zotavení, druhý se zabývá obranou a zotavením samotným. Tato část nabízí shrnutí poznatků z ransomwarových případů za poslední rok.

93 %

vyšetřování Microsoftu během zotavování z ransomwaru odhalilo nedostatečné řídicí mechanismy pro privilegovaný přístup a taktiku lateral movement.

Aktivity při ransomwarovém incidentu a zotavování podle odvětví

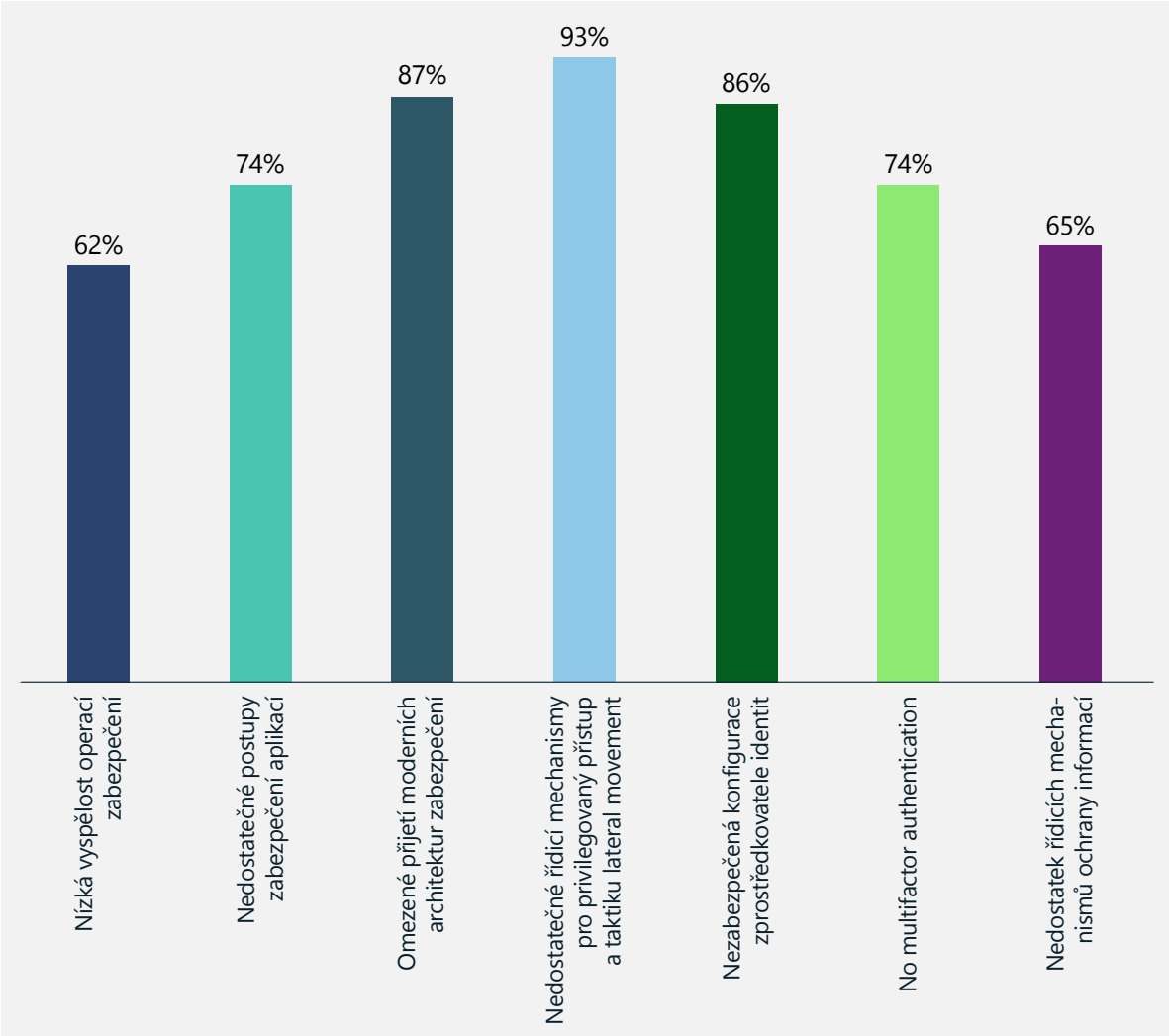


S příchodem malých skupin a hrozeb musí mít obranné týmy povědomí o měnících se hrozbách ransomwaru a zároveň se musí bránit dříve neznámým rodinám ransomwarového malwaru. Taktika rychlého vývoje, kterou používají zločinecké skupiny, vedla k vytvoření inteligentního ransomwaru zabaleného do snadno použitelných sad. Ten nabízí větší flexibilitu při zahajování rozsáhlých útoků na velký počet cílů.

Následující stránky nabízejí podrobnější pohled na nejčastěji zjišťované aspekty, kvůli kterým není obrana před ransomwarem moc silná. Jsou seskupeny do tří kategorií poznatků:

1. Slabé kontrolní mechanismy identit
2. Neúčinné operace zabezpečení
3. Omezená ochrana dat

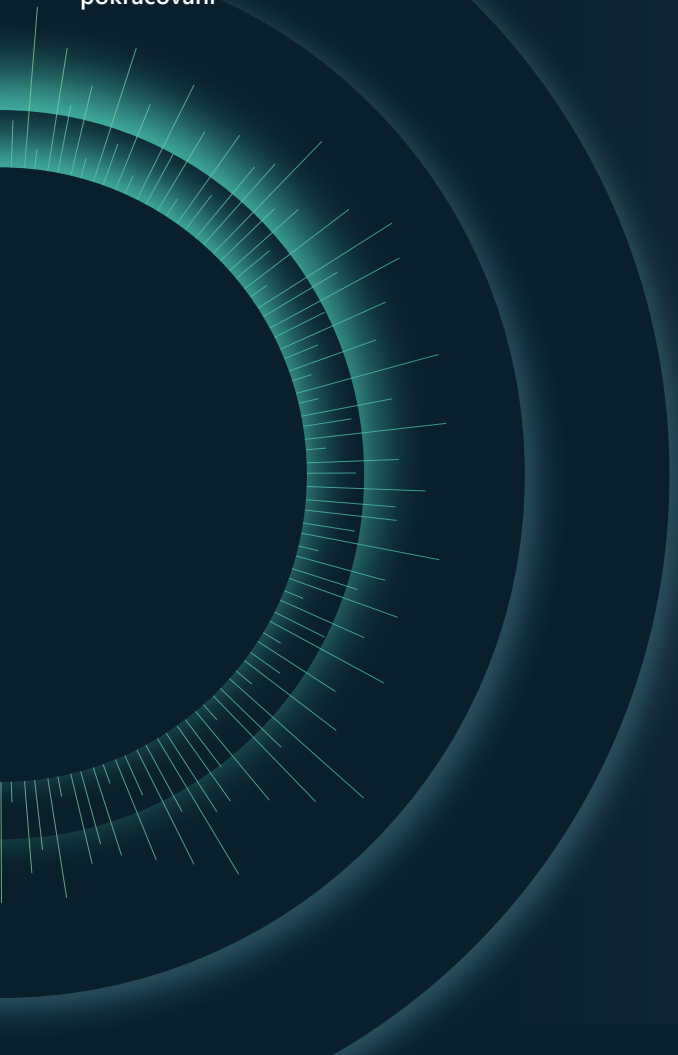
Shrnutí nejčastějších zjištění při reakcích na ransomware



Nejčastějším zjištěním při činnostech v reakci na ransomwarový incident byly nedostatečné řídicí mechanismy pro privilegovaný přístup a taktiku lateral movement.

Poznatky o ransomwaru od respondérů v první linii

pokračování



Tři hlavní problémové aspekty zjištěné při řešení ransomwaru u zákazníků:

① **Slabé kontrolní mechanismy identit:** Jedním z hlavních problémových aspektů zůstávají útoky s cílem ukrást přihlašovací údaje.

② **Neúčinné procesy operací zabezpečení** nepředstavují jen příležitost pro útočníky, ale mají zároveň i významný dopad na délku zotavování.

③ Nakonec vše směřuje k datům – organizacím se nedaří implementovat účinnou **strategii ochrany dat,** která by odpovídala jejich firemním potřebám.

① Slabé kontrolní mechanismy identit

Člověkem řízený ransomware se nadále vyvíjí a využívá metody krádeže přihlašovacích údajů a taktiky lateral movement, které obvykle souvisejí s cílenými útoky. Úspěšné útoky jsou často výsledkem dlouhotrvajících kampaní, které zahrnují napadení systémů identit, třeba Active Directory (AD), jež lidským operátorům umožňují ukrást přihlašovací údaje, přistupovat do systémů a zůstat v síti trvale aktivní.

Zabezpečení Active Directory (AD) a Azure AD

88 %

napadených zákazníků nepoužívalo osvědčené postupy zabezpečení AD a Azure AD. To se stalo běžným vektorem útoku, protože útočníci díky chybné konfiguraci a horšímu stavu zabezpečení v kritických systémech identit získávají širší přístup do firem, kde pak mají větší dopad.

Přístup s nejmenšími možnými oprávněními a používání pracovních stanic s privilegovaným přístupem (PAW)

Žádná z napadených organizací neimplementovala při správě nejdůležitějších identit a hodnotných prostředků, jako jsou proprietární systémy a důležité obchodní aplikace, správné oddělení přihlašovacích údajů pro správu a principy přístupu s nejnižší možnou úrovní oprávnění přes vyhrazené pracovní stanice.

Zabezpečení privilegovaných účtů

88 %

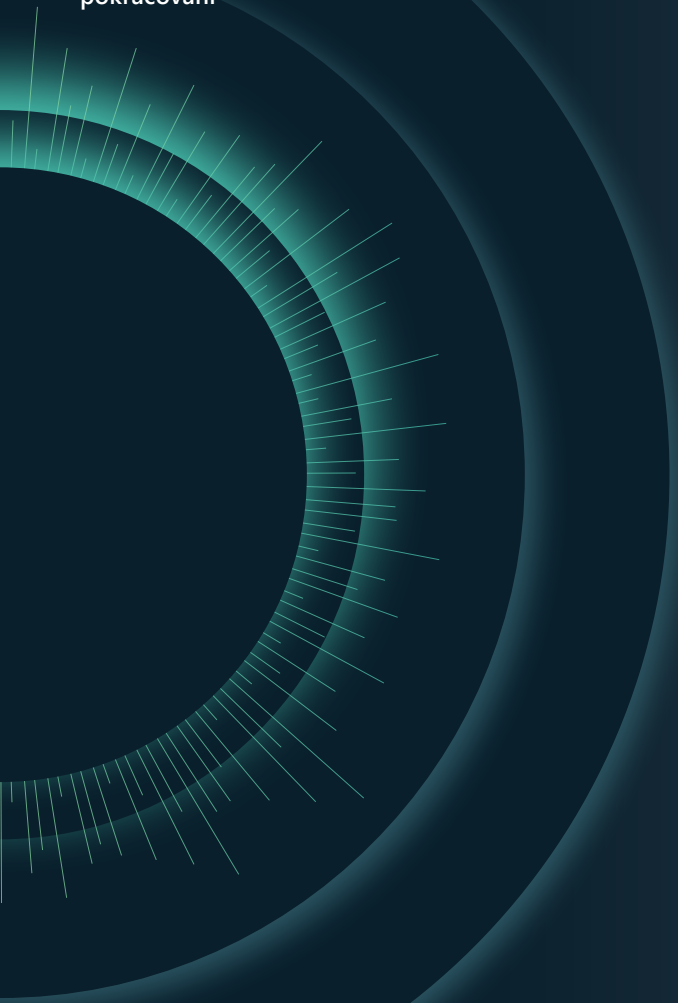
případů odhalilo absenci implementace MFA pro citlivé a vysoce privilegované účty. Tím vznikl v zabezpečení prostor, kterým útočníci mohli napadnout přihlašovací údaje a podpořit další útoky pravými přihlašovacími údaji.

84 %

Správci v 84 % organizací nepoužívali řídicí mechanismy pro privilegované identity, třeba přístup podle potřeby, které by zabránily dalšímu škodlivému využití kradených privilegovaných přihlašovacích údajů.

Poznatky o ransomwaru od respondérů v první linii

pokračování



② Neúčinné operace zabezpečení

Z našich dat je patrné, že organizace, na které zaútočil ransomware, měly významné nedostatky v operacích zabezpečení, nástrojích a správě životního cyklu prostředků informačních technologií. Na základě dostupných dat byly nejčastěji pozorovány tyto nedostatky:

Opravy:

68 %

napadených organizací nemělo zavedený účinný proces správy oprav a ohrožení zabezpečení. Vysoká závislost na ručních procesech namísto automatizovaných oprav vedla ke kritickým nedostatkům. Výroba a kritická infrastruktura stále čelí problémům s údržbou a opravou starších systémů provozních technologií (OT).

Nedostatek nástrojů pro operace zabezpečení:

Většina organizací oznámila nedostatek komplexních informací o zabezpečení, protože jim chyběly nástroje pro zabezpečení nebo je měly nesprávně nakonfigurované. To pak vedlo ke snížení efektivity detekce a reakcí.

60 %

organizací oznámilo, že nepoužívá žádný nástroj EDR[6], což je stěžejní technologie pro detekci a reakce.

60 %

neinvestovalo do technologie správy akcí a informací o zabezpečení (SIEM), což vedlo k silům monitorování, omezeným možnostem detekce komplexních hrozeb a neefektivním operacím zabezpečení. Nejvýznamnějším nedostatkem v nástrojích a procesech SOC zůstává automatizace. Kvůli tomu musí zaměstnanci SOC trávit nespočet hodin analýzou telemetrie ze systémů zabezpečení.

84 %

napadených organizací nezavedlo integraci vícecloudových prostředí do svých nástrojů pro operace zabezpečení.

Procesy reakcí a zotavení:

76 %

Absence účinného plánu reakcí byla kritická oblast zjištěná u 76 procent napadených organizací, což znemožnilo jejich správnou přípravu a nepříznivě ovlivnilo dobu trvání reakce a zotavování.

③ Omezená ochrana dat

Mnoha napadeným organizacím chyběly správné procesy ochrany dat, což mělo značný dopad na délku zotavování a schopnost vrátit se k obchodním operacím. Mezi nejčastější zjištěné nedostatky patří:

Neměnná záloha:

44 %

organizací nemělo neměnné zálohy napadených systémů. Data navíc ukazují, že správci neměli plány zálohování a obnovování pro kritické prostředky, jako je AD.

Ochrana před únikem informací:

Útočníci obvykle najdou způsob, jak napadnout systémy, zneužitím chyb v zabezpečení organizace, exfiltrací kritických dat pro vydírání, krádeží duševního vlastnictví nebo monetizací.

92 %

napadených organizací neimplementovalo účinné řídicí mechanismy ochrany před únikem informací ke zmírnění těchto rizik. To vedlo ke kritické ztrátě dat.

Někde byl ransomware na ústupu, jinde na vzestupu

Letos jsme v porovnání s předchozím rokem pozorovali pokles celkového počtu ransomwarových případů oznámených našim reakčním týmům v Severní Americe a Evropě. Ve stejnou chvíli došlo k nárůstu hlášených případů v Latinské Americe.

Ačkoli aktivity policejních složek pravděpodobně snížily v roce 2022 četnost útoků, aktéři hrozeb nejspíše vyvinou nové strategie, jak se v budoucnu nenechat chytit.

Jednou z možných interpretací tohoto zjištění je, že se kyberzločinci odchýlili od oblastí, u kterých je zřejmě vyšší riziko prověřování ze strany policejních složek, ve prospěch méně chráněných cílů. Jelikož Microsoft nezaznamenal výrazné zlepšení v zabezpečení firemních sítí po celém světě, které by vysvětlilo pokles počtu hovorů s podporou v souvislosti s ransomwarem, domníváme se, že nejpravděpodobnější příčinou je kombinace aktivity policejních složek v letech 2021 a 2022, která prodražila kriminální činnost, a některých geopolitických událostí roku 2022.

Jedny z nejrozšířenějších operací RaaS patří rusky mluvícímu zločineckému uskupení známému jako REvil (také jako Sodinokibi), jehož aktivita započala v roce 2019. V říjnu 2021 byly servery skupiny REvil vyřazeny v rámci mezinárodní policejní operace Operation GoldDust.[7] V lednu 2022 Rusko zatklo 14 údajných členů skupiny REvil a provedlo razii 25 míst, kde skupina působila.[8] Bylo to poprvé, kdy Rusko zasáhlo proti operátorům ransomwaru na svém území.

2krát

Počet ransomwarových útoků v některých oblastech klesl, ale požadovaná výkupná jsou více než dvojnásobná.

Ačkoli aktivity policejních složek pravděpodobně snížily v roce 2022 četnost útoků, aktéři hrozeb nejspíše vyvinou nové strategie, jak se v budoucnu nenechat chytit. K tomu se zdá, že napětí mezi Ruskem a Spojenými státy kvůli ruské invazi na Ukrajinu ukončilo nadějné začátky spolupráce Ruska v globálním boji proti ransomwaru. Po krátkém období nejistoty po zatčení členů skupiny REvil přestaly Spojené státy a Rusko spolupracovat na pronásledování ransomwarových aktérů. To znamená, že kyberzločinci můžou Rusko opět považovat za bezpečné území.

Pro budoucnost předvídáme, že míra ransomwarových aktivit bude záviset na odpovědích na některé zásadní otázky:

1. Budou vlády činit kroky, které ransomwarovým kyberzločincům zabrání operovat na jejich území, nebo hledat způsoby, jak narušit činnost aktérů v zahraničí?
2. Budou ransomwarové skupiny měnit strategii, aby nebylo zapotřebí ransomware používat, a přejdou na útoky vydíráním?
3. Dokážou organizace modernizovat a transformovat své IT operace rychleji, než zločinci dokáží zneužívat chyby v zabezpečení?
4. Donutí pokroky ve vyhledávání a sledování plateb výkupného jejich příjemce změnit strategii a způsob vyjednávání?

Poznatky a jejich využití

1. Zaměřte se na holistické strategie zabezpečení, protože všechny rodiny ransomwaru k napadení sítě zneužívají stejné slabé stránky zabezpečení.
2. Aktualizujte a dodržujte základy zabezpečení, abyste si zajistili vyšší základní úroveň ochrany důkladnou obranou, a modernizujte operace zabezpečení. Přesun do cloudu umožní rychleji detekovat hrozby a reagovat.

Odkazy na další informace

- Ochrana organizace před ransomwarem | Microsoft Security
- 7 způsobů, jak posílit zabezpečení prostředí před napadením | Microsoft Security Blog
- Zlepšení obrany založené na AI pro narušení člověkem řízeného ransomwaru | Microsoft 365 Defender Research Team
- Security Insider: Nejnovější poznatky a aktuální informace o kybernetické bezpečnosti | Microsoft Security

Kybernetická kriminalita jako služba

Kybernetická kriminalita jako služba (CaaS) je rostoucí a neustále se vyvíjející hrozbou pro zákazníky po celém světě. Tým Digital Crimes Unit (DCU) v Microsoftu zjistil, že ekosystém CaaS stále roste, stejně jako počet online služeb, které usnadňují různé kybernetické zločiny, včetně BEC a člověkem řízeného ransomwaru. Oblíbenou metodou útoku je i nadále phishing, protože pro kyberzločince má úspěšná krádež a prodej přístupu k ukradeným účtům významnou hodnotu.

V reakci na rostoucí trh CaaS vylepšil tým DCU pozorovací systémy, které zjišťují a identifikují nabídky CaaS v celém ekosystému internetu, hlubokého webu, důkladně prověřených fór[9], vyhrazených webů, online diskuzních fór a platforem pro zasílání zpráv.

Kyberzločinci teď na konkrétních výsledcích spolupracují i napříč časovými pásmy a jazyky. Například jeden web CaaS spravovaný jednou osobou v Asii udržuje operace v Evropě a vytváří škodlivé účty v Africe. Vícejurisdikční povaha těchto operací představuje z pohledu zákona a dohledu nad jeho dodržováním složité problémy. V reakci na to DCU zaměřuje své úsilí na likvidaci škodlivé zločinecké infrastruktury, kterou se usnadňují útoky CaaS, a na spolupráci s policejními orgány po celém světě, které můžou zločince postavit před spravedlnost.

Kyberzločinci stále častěji využívají analytické nástroje k maximalizaci dosahu, rozsahu a zisku. Stejně jako legitimní firmy musí weby CaaS zajistit kvalitu produktů a služeb, aby si zachovaly dobrou pověst. Weby CaaS například rutinně automatizují přístup k napadeným účtům, aby ověřily platnost kompromitovaných přihlašovacích údajů. Pokud dojde k resetování hesla nebo opravě chyb v zabezpečení, kyberzločinci přestávají prodávat konkrétní účty. Ve stále větší míře jsme nacházeli weby CaaS, které v rámci procesu kontroly kvality zajišťují kupujícím ověření na vyžádání. Kupující tak v důsledku toho můžou mít jistotu, že web CaaS prodává aktivní účty a hesla, a zároveň se tím snižují případné náklady obchodníka CaaS, pokud by byly kradené přihlašovací údaje před prodejem vyřazeny.

Dále tým DCU zjistil, že weby CaaS nabízejí kupujícím možnost nakoupit napadené účty z konkrétních geografických oblastí, od stanovených poskytovatelů online služeb a od konkrétních napadených jednotlivců, profesí a oborů. Často se objednané účty zaměřují na odborníky nebo oddělení, kteří zpracovávají faktury, třeba na CFO nebo pohledávky. Obdobně se cílem stávají i odvětví, která se účastní veřejných zakázek, a to kvůli množství informací, které bývají zveřejněny v rámci procesu veřejných nabídek.

Vyšetřování CaaS týmem DCU odhalila několik hlavních trendů:

Zvyšuje se počet a složitost služeb.

Příkladem je vývoj webových prostředí, která obvykle sestávají z napadených webových serverů, jimiž se automatizují phishingové útoky. Tým DCU zjistil, že prodejci CaaS zjednodušují nahrávání phishingových sad nebo malwaru prostřednictvím specializovaných webových řídicích panelů. Přes takový řídicí panel se pak prodejci CaaS často následně pokusí prodat aktérovi hrozeb i další služby, například spamové zprávy a specializované seznamy příjemců spamu podle definovaných atributů, jako je geografická poloha nebo profese. V některých případech jsme zjistili, že se jedno webové prostředí používalo v několika kampaních útoků. To naznačuje, že by aktéři hrozeb mohli udržovat trvalý přístup k napadenému serveru. Dále jsme zjistili jak nárůst anonymizačních služeb dostupných v rámci ekosystému CaaS, tak nabídek účtů virtuálních privátních sítí (VPN) a virtuálních privátních serverů (VPS). Ve většině případů byly nabízené VPN/VPS zajištěny kradenými platebními kartami. K tomu weby CaaS nabízely více prostředků protokolů RDP (Remote Desktop Protocol), SSH (Secure Shell) a cPanel, které slouží jako platforma k orchestraci kybernetických útoků. Obchodníci CaaS nakonfigurují RDP, SSH a cPanely pomocí vhodných nástrojů a skriptů, které usnadňují různé typy kybernetických útoků.

Služby pro vytváření homoglyfických domén stále častěji požadují platbu v kryptoměnách.

Homoglyfické domény napodobují legitimní názvy domény pomocí znaků, které jsou vzhledově totožné nebo téměř totožné s jiným znakem. Cílem je oklamat uživatele, aby si myslel, že homoglyfická doména je ta pravá. Takové domény jsou všudypřítomnou hrozbou a bránou pro značný objem kybernetické kriminality. Weby CaaS teď prodávají vlastní homoglyfické názvy domén. To kupujícím umožňuje požádat o napodobení názvů konkrétních domén a společností. Jakmile obchodníci CaaS obdrží platbu, použijí nástroj pro generování homoglyfických domén, vyberou název domény a škodlivý homoglyf zaregistrují. Platby za tuto službu probíhají téměř výhradně v kryptoměně.

2 750 000

registrací webů letos úspěšně zablokovaných týmem DCU, což přineslo náskok před zločinnými aktéry, kteří je plánovali použít ke globální kybernetické kriminalitě.

Kybernetická kriminalita jako služba

pokračování

Prodejci CaaS stále častěji nabízejí ke koupi kradené přihlašovací údaje.

Takové přihlašovací údaje umožňují neautorizovaný přístup k uživatelským účtům, včetně služby pro zasílání e-mailových zpráv, prostředků pro sdílení firemních souborů a OneDrivu pro firmy. Pokud jsou ukradeny přihlašovací údaje správce, neautorizovaní uživatelé by mohli získat přístup k důvěrným souborům, prostředkům Azure a uživatelským účtům firmy. V mnoha případech šetření týmu DCU zjistilo neoprávněné použití stejných přihlašovacích údajů na různých serverech jako způsob, jak automatizovat ověřování přihlašovacích údajů. Tento model naznačuje, že se napadený uživatel mohl stát obětí nejednoho phishingového útoku nebo má na zařízení malware, který umožňuje botnetovým keyloggerům sbírat přihlašovací údaje.

Objevují se služby a produkty CaaS s vylepšenými funkcemi, které pomáhají uniknout odhalení.

Jeden prodejce CaaS nabízí phishingové sady s větší složitostí a vylepšenými anonymizačními funkcemi navrženými tak, aby obešly detekci a systémy prevence, za pouhých 6 USD denně. Služba nabízí řadu přesměrování, kterými se provádí kontroly, než se povolí přenos na další vrstvu nebo web. V jednom případě probíhá přes 90 kontrol, které poskytnou identifikační údaje o zařízení. Mezi ty patří informace, jestli jde o virtuální počítač, podrobnosti o používaném prohlížeči a hardwaru a další. Pokud všechny kontroly proběhnou úspěšně, komunikace se odešle na cílovou phishingovou stránku.

Komplexní služby kybernetické kriminality prodávají předplatná spravovaných služeb.

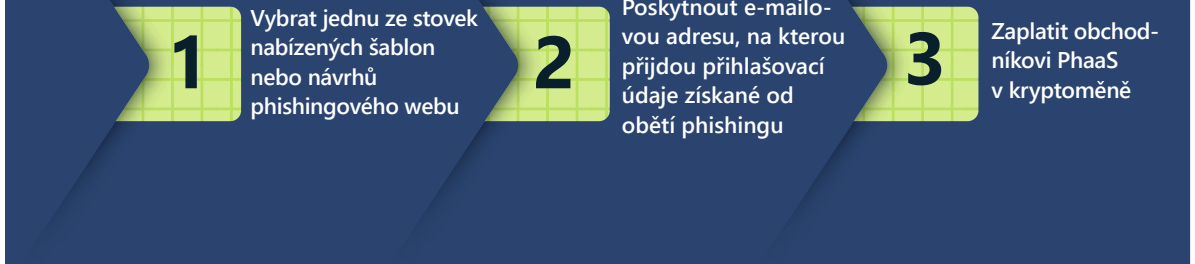
Pokud je zabezpečení operací aktérů hrozeb nedostatečné, obvykle je může každý krok online zločinu odhalit. Riziko odhalení a identifikace se zvyšuje, pokud dojde k nákupu služeb z více webů CaaS. Tým DCU zaznamenal na temném webu znepokojivý trend, kdy dochází k nárůstu počtu služeb, které nabízejí anonymizaci softwarového kódu a zobecnění textu webu, aby se snížilo riziko odhalení. Poskytovatelé komplexních předplacených služeb kybernetické kriminality spravují všechny služby a zaručují výsledky, které riziko odhalení předplácejícího OCN ještě dále snižují. Nižší riziko pak vedlo k větší oblibě těchto komplexních služeb.

Phishing jako služba (PhaaS) je jedním příkladem komplexní služby kybernetické kriminality. PhaaS je evolucí předchozích služeb, kterým se říká zcela nedetekovatelné služby (fully undetectable services – FUD) a nabízí se na principu předplatného. Mezi typické podmínky PhaaS patří zajištění aktivity phishingového webu na jeden měsíc.

Tým DCU identifikoval i obchodníka CaaS, který jako předplatné nabízí útoky DDoS. V tomto modelu slouží obchodník CaaS jako externí zdroj pro vytváření a údržbu botnetu potřebného k provedení útoků. Každý zákazník předplatného DDoS získává šifrovanou službu, která vylepší zabezpečení operací, a nepřetržitou podporu po dobu jednoho roku. Služba předplatného DDoS nabízí různé architektury a metody útoků, aby si kupující mohl jednoduše vybrat prostředek, na který se zaútočí, a prodejce zajistí přístup k množství napadených zařízení v botnetu, ze kterých útok proběhne. Náklady na předplatné DDoS jsou pouhých 500 USD.

DCU aktivně pracuje na vývoji nástrojů a technik, které identifikují kyberzločince CaaS a narušují jejich činnost. Vývoj služeb CaaS s sebou nese značné překážky, obzvláště v případě narušení kryptoměnových plateb.

PhaaS, kyberzločinci nabízejí několik služeb v rámci jednoho předplatného. Kupující musí v obecné rovině udělat jen tři věci:



Jakmile je tento postup dokončen, obchodník PhaaS vytváří služby se třemi nebo čtyřmi vrstvami přesměrování a hostováním prostředků, kterými cílí na konkrétní uživatele. Následně je kampaň spuštěna a zjištěny přihlašovací údaje oběti, které jsou pak ověřeny a odeslány na e-mailovou adresu zadanou kupujícím. Za příplatek mnoho obchodníků PhaaS nabízí hostování phishingových webů na veřejném blockchainu, aby k nim bylo možné přistupovat z libovolného prohlížeče, a přesměrováním můžou tito obchodníci navést uživatele na prostředek v distribuovaném registru.

Trestné využití kryptoměn

V současné době se používání kryptoměn stává běžnou záležitostí a zločinci je stále více používají k úniku před policejními složkami a opatřeními proti praní špinavých peněz (AML). Pro policejní složky je pak obtížnější dohledat a vysledovat kryptoměnovou platbu ke kyberzločincům.

Celosvětové investice do blockchainových řešení za poslední čtyři roky zaznamenaly růst o přibližně 340 procent. Počet nových kryptopeněženek narostl přibližně o 270 procent. Na celém světě existuje více než 83 milionů jedinečných peněženek a celková kapitalizace trhu všech kryptoměn dosáhla k 28. červenci 2022 přibližně 1,1 bilionu USD.[10]

Zdroj: Twitter.com—@PeckShieldAlert (PeckShield je čínská společnost zabývající se bezpečnostní blockchainu.)

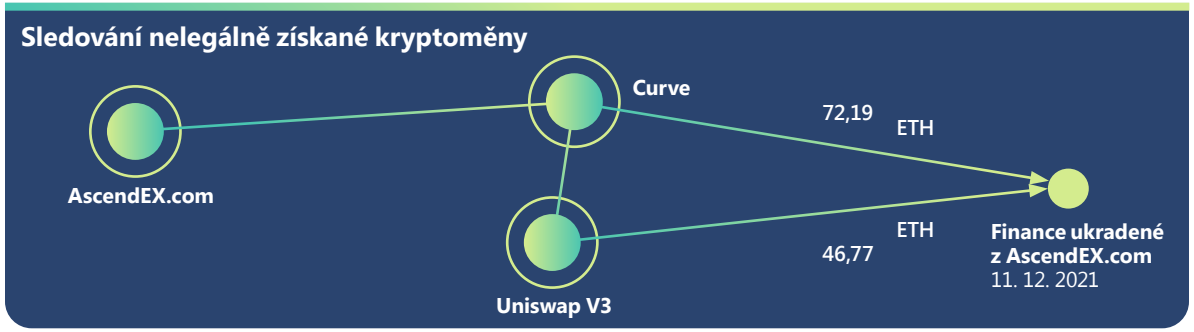
Sledování ransomwarových plateb

Ransomware je jedním z největších zdrojů nelegálně získaných kryptoměn. Ve snaze narušit škodlivou technickou infrastrukturu, která se používá při ransomwarových útocích (příkladem může být narušení Zloaderu v dubnu 2022[11]), tým DCU Microsoftu sleduje zločinecké peněženky. Chce tak umožnit sledování kryptoměn a zajistit možnosti zotavení po útoku.

Vyšetřovatelé z týmu DCU zjistili, že ransomwaroví aktéři vyvíjejí své strategie komunikace s oběťmi tak, aby zakryli finanční stopu. Původně kyberzločinci ve svých požadavcích na výkupné uváděli bitcoinové adresy. Kvůli tomu však bylo snadné sledovat platební transakce na blockchainu, proto ransomwaroví aktéři přestali uvádět adresy peněženek a namísto toho připojují e-mailové adresy nebo odkazy na chatovací weby, na kterých obětem adresy pro platbu výkupného sdělují. Někteří aktéři dokonce vytvořili jedinečné webové stránky a přihlašovací údaje pro jednotlivé oběti, aby výzkumníci zabezpečení a policejní složky nemohli získat adresy peněženek zločinců předstíráním, že jsou oběťmi. I přes veškeré snahy zločinců zakrýt své stopy je stále možné některé platby výkupného získat zpět v součinnosti s policejními složkami a společnostmi pro analýzu kryptotrhu, které dokáží sledovat pohyb na blockchainu.

Trend: Praní nelegálních výnosů přes decentralizované směnárny

Hlavním problémem pro kyberzločince je převod kryptoměny na zákonné platidlo. Kyberzločinci k tomu mají několik možností a každá představuje jiný stupeň nebezpečí. Jedním ze způsobů, jak riziko omezit, je praní výnosů přes decentralizovanou směnárnu (decentralized exchange – DEX) a následný vývod peněz dostupnými možnostmi výplaty, třeba přes centralizované směnárny (centralized exchange – CEX) nebo směnou přímo mezi uživateli (peer to peer – P2P) či přes prostředníka (over the counter – OTC). DEX jsou atraktivním místem pro praní špinavých peněz, neboť často nedodržují opatření AML.



Tým Digital Crimes Unit v Microsoftu pomocí nástroje pro prověřování kryptoměn Chainalysis odhalil, že hackeři AscendEX vyměnili své kradené finance kromě Uniswapu i na menší DEX s názvem Curve. Tento diagram znázorňuje cesty praní špinavých peněz, které tým objevil. Každý kruh představuje několik peněženek a čísla na každém řádku uvádějí celkový počet etherů převedených pro účely praní.

V prosinci 2021 hackeři zaútočili na globální platformu pro obchodování kryptoměn AscendEx a ukradli jejím zákazníkům přibližně 77,7 milionu USD v kryptoměnách.[12] Společnost AscendEx najala firmy zabývající se analýzou blockchainů a obrátila se na jiné CEX, aby zablokovaly peněženky přijímající kradené finance. Adresy, na které byly mince poslány, pak byly příslušně označeny na ethereovém průzkumníkovi blockchainu Etherscan.[13] Aby hackeři obešli upozorňování a seznamy blokovaných adres, poslali 18. února 2022 1,5 milionu USD v etherech směnárně Uniswap, což je jedna z největších DEX na světě.[14]

Pokud by DEX přijaly silnější opatření AML, mohlo by to omezit aktivitu praní špinavých peněz na jejich platformách a přinutit kyberzločince používat jiné metody obfuskace, třeba kombinování mincí nebo nelicencované směnárny. Směnárna Uniswap například v nedávné době oznámila, že pomocí seznamů začne blokovat směnárenské transakce peněženek, o kterých je známo, že byly používány při nelegálních činnostech.[15]

Poznatky a jejich využití

1. Pokud jste se stali obětí kybernetické kriminality a zaplatili jste zločinci pomocí kryptoměn, obraťte se na policejní složku, která by vám mohla pomoct sledovat a získat zpět ztracené peníze.
2. Při výběru DEX se seznamte se zavedenými opatřeními AML.

Odkazy na další informace

- Hardwarová obrana před hrozbami stále složitějšího napadání počítačů s cílem těžit kryptoměny | Microsoft 365 Defender Research Team

Vyvíjející se prostředí phishingových hrozeb

Schémata phishingu přihlašovacích údajů zažívají rozmach a zůstávají významnou hrozbou pro uživatele, ať už jsou kdekoli, protože bez rozdílů cílí na všechny schránky. Objem phishingových útoků je řádově větší než u všech ostatních hrozeb, které náš výzkumný tým sleduje a chrání před nimi.

Díky datům z Defenderu pro Office vidíme škodlivý e-mail a aktivitu napadené identity. Služba Azure Active Directory Identity Protection poskytuje stále více informací prostřednictvím upozornění na události napadení identity. Defender for Cloud Apps nám ukazuje události přístupu k datům napadené identity a Microsoft 365 Defender (M365D) nabízí korelaci mezi produkty. Metrika taktiky lateral movement pochází z Defenderu for Endpoint (upozornění a události útočného chování), Defenderu pro Office (škodlivý e-mail) a opět z M365D pro korelaci mezi produkty.

710 milionů
phishingových e-mailů zablokovaných každý týden

1 h 12 m
Medián doby, jak dlouho útočníkovi trvá získat přístup k soukromým datům, pokud se stanete obětí phishingového e-mailu.[16]

1 h 42 m
Medián doby, za jakou se útočník začne po napadení zařízení nepozorovaně pohybovat ve firemní síti.[17]

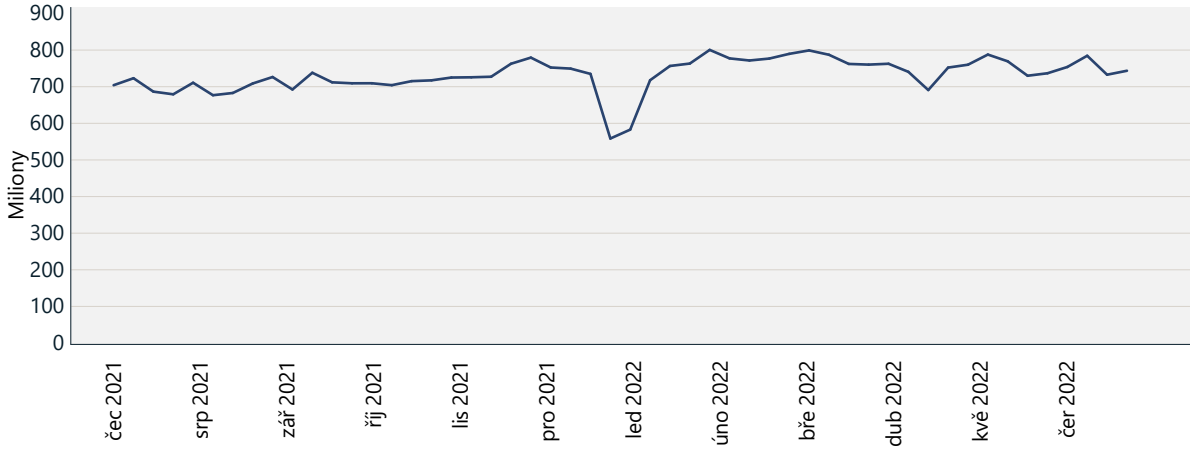
Přihlašovací údaje Microsoftu 365 zůstávají pro útočníky stále jedním z nejžádanějších typů účtů. Jakmile dojde k napadení přihlašovacích údajů, útočníci se můžou přihlásit k firemním počítačovým systémům a usnadnit nákazu malwarem a ransomwarem, ukrást důvěrné informace a data společnosti uložené v sharepointových souborech, pokračovat v šíření phishingových zpráv dalšími škodlivými e-maily pomocí Outlooku a podobně.

Kromě kampaní s širšími cíli a phishingu přihlašovacích údajů, darů a osobních údajů útočníci cílí na konkrétní firmy, které můžou zaplatit větší výkupné. E-mailovým phishingovým útokům na firmy za účelem finančního zisku se souhrnně říká útoky BEC. Každý měsíc Microsoft detekuje miliony e-mailů BEC, což představuje 0,6 procenta všech zjištěných phishingových e-mailů. Zpráva oddělení IC3[18] publikovaná v květnu 2022 ukazuje vzestupný trend exponovaných ztrát způsobených útoky BEC.

Techniky používané při phishingových útocích jsou stále složitější. V reakci na protiopatření se útočníci přizpůsobují a hledají nové způsoby, jak své techniky uvést do praxe a ještě více propracovat principy a místa hostování infrastruktury pro operace kampaní. To znamená, že organizace musí pravidelně přehodnocovat svou strategii, jak implementovat řešení zabezpečení tak, aby blokovaly škodlivé e-maily a posílily řídicí mechanismy přístupu pro účty jednotlivých uživatelů.

531 000
Kromě adres URL zablokovaných Defenderem pro Office náš tým Digital Crimes Unit organizoval vyřazení 531 000 jedinečných phishingových adres URL hostovaných mimo Microsoft.

Zjištěné phishingové e-maily



Počet každý týden zjištěných phishingů stále narůstá. Pokles mezi prosincem a lednem je očekávaný sezónní pokles, který byl patrný i v loňské zprávě. Zdroj: Signály Exchange Online Protection

Vyvíjející se prostředí phishingových hrozeb

pokračování

I nadále sledujeme stabilní meziroční nárůst počtu phishingových e-mailů. Přechod na vzdálenou práci v letech 2020 a 2021 s sebou přinesl značný nárůst phishingových útoků, které chtějí využít měnícího se pracovního prostředí. Phishingoví operátoři rychle zavádějí nové e-mailové šablony, ve kterých se využívají nástrahy související s velkými světovými událostmi, třeba pandemií covidu-19, a témata spojená se spoluprací a nástroji pro produktivitu, třeba sdílení souborů přes Disk Google nebo OneDrive. I když už motivy covidu-19 nejsou tak časté, stala se novou nástrahou od počátku března 2022 válka na Ukrajině. Naši výzkumníci zjistili ohromující nárůst e-mailů, které napodobují legitimní organizace a žádají o dary v bitcoinech a etherech, údajně na podporu občanů Ukrajiny.

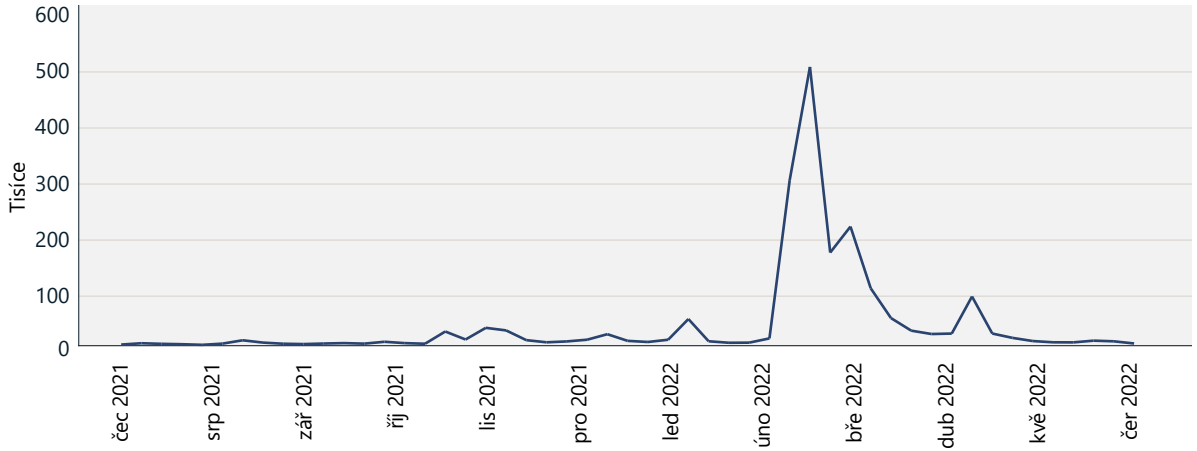
Jen několik dní od začátku války na Ukrajině na konci února 2022 výrazně vzrostl počet zjištěných phishingových e-mailů obsahujících etherové adresy mezi firemními zákazníky. Nejvíce phishingových e-mailů s adresou peněženky Ethereum, a to půl milionu, bylo rozesláno v prvním březnovém týdnu. Před začátkem války byl počet adres etherových peněženek v jiných e-mailech vyhodnocených jako phishing výrazně nižší, průměrně několik tisíc e-mailů denně.

Více než kdy dříve phishingoví útočníci používají legitimní infrastrukturu, s níž stále častěji vedou phishingové kampaně zaměřené na napadení různých částí provozní techniky, aby nemuseli kupovat, hostovat nebo provozovat svou vlastní. Škodlivé e-maily tak můžou pocházet třeba z napadených účtů odesílatelů. Útočníkům tyto e-mailové adresy poskytují výhody, protože mají vyšší reputační skóre a považují se za důvěryhodnější než nově vytvořené účty a domény. V některých pokročilejších phishingových kampaních jsme zjistili, že útočníci dávají přednost odesílání a podvádění z domén, které mají nesprávně nastavený mechanismus DMARC[19] se zásadami „nečinnosti“. Tím vzniká prostor pro falšování e-mailů.

Velké phishingové operace mají tendenci využívat k rozsáhlým útokům cloudové služby a cloudové virtuální počítače. Útočníci dokážou plně automatizovat proces nasazování a doručování e-mailů z virtuálních počítačů pomocí přenosů e-mailů protokolem SMTP nebo cloudové e-mailové infrastruktury. Přináší jim to výhodu rychlého doručování a dobré pověsti těchto legitimních služeb. Pokud se podaří škodlivý e-mail poslat prostřednictvím těchto cloudových služeb, obránci se musí spoléhat na silné funkce filtrování e-mailů, aby mohli e-mailům zablokovat vstup do jejich prostředí.

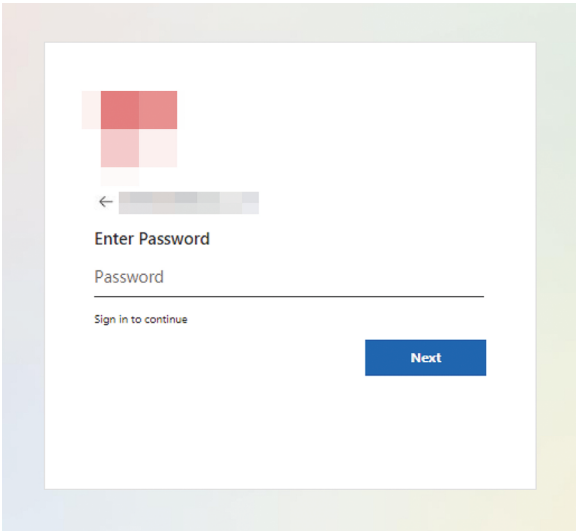
Hlavním cílem phishingových operátorů zůstávají účty Microsoft, jak dosvědčují mnohé phishingové cílové stránky, které napodobují přihlašovací stránku Microsoftu 365. Phishingoví útočníci se například ve svých phishingových sadách pokoušejí věrně napodobit přihlašovací prostředí Microsoftu generováním jedinečné adresy URL, která je přizpůsobena příjemci. Tato adresa URL vede na škodlivou webovou stránku, která sbírá přihlašovací údaje, ale parametr v adrese URL bude obsahovat konkrétní e-mailovou adresu příjemce. Jakmile cíl na tuto stránku přejde, phishingová sada předem vyplní přihlašovací údaje uživatele a firemní logo přizpůsobené podle e-mailu příjemce a zrcadlí tak vzhled vlastní přihlašovací stránky Microsoftu 365 cílové společnosti.

Phishingové e-maily s adresou ethereové peněženky



Na začátku ukrajinsko-ruského konfliktu se celkový počet zjištěných phishingových e-mailů obsahujících adresy peněženek Ethereum zvýšil, aby pak následně začal opět klesat.

Phishingová stránka, která napodobuje přihlašování Microsoftu s dynamickým obsahem

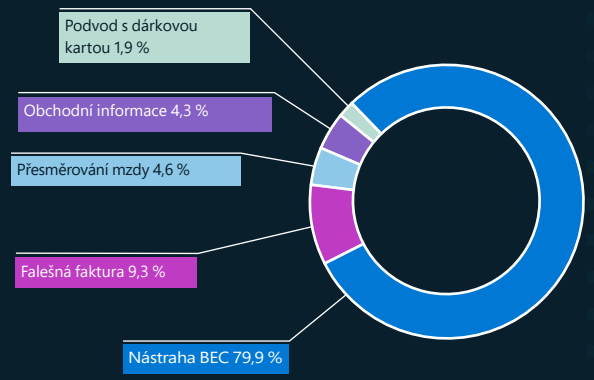


Útoky na firemní e-maily

Kyberzločinci vyvíjejí stále složitější schémata a techniky, kterými překonávají nastavení zabezpečení a cílí na jednotlivce, firmy a organizace. V reakci na to investujeme významné prostředky do dalšího vylepšování našeho programu pro ochranu před BEC.

BEC představuje nejnákladnější kybernetický zločin. Odhaduje se, že v roce 2021 dosáhly ztráty přibližně 2,4 miliardy USD, což představuje více než 59 procent z hlavních pěti ztrát způsobených internetovým zločinem.[20] Abychom porozuměli rozsahu tohoto problému a způsobům, jak uživatele před BEC nejlépe chránit, výzkumníci zabezpečení v Microsoftu sledují nejběžnější schémata, která se používají při útocích.

Témata BEC (leden–červen 2022)



Témata BEC podle procenta výskytu

Trendy BEC

Jako vstupní bod se útočníci BEC obvykle pokoušejí zahájit konverzaci a navázat dobrý vztah s potenciálními oběťmi. Útočník předstírá, že je kolega nebo obchodní partner, a postupně vede konverzaci směrem k peněžnímu převodu. Úvodní e-mail, který sledujeme jako nástrahu BEC, představuje téměř 80 procent zjištěných e-mailů BEC. Mezi další trendy, které výzkumníci zabezpečení v Microsoftu odhalili za poslední rok, patří:

- Nejčastěji používanými technikami při útocích BEC zjištěnými v roce 2022 bylo falšování[21] a napodobování.[22]
- Podtyp BEC, který obětem způsobil největší finanční škody, byly falešné faktury (podle objemu a požadovaných částek v dolarech zjištěných při našich šetřeních kampaní BEC).
- Krádež obchodních informací, třeba zpráv o závazcích a kontaktů na zákazníky, umožňuje útočníkům připravit přesvědčivou falešnou fakturu.
- Většina požadavků na přesměrování mzdy byla odeslána z bezplatných e-mailových služeb, jen málokdy z napadených účtů. Objem e-mailů z těchto zdrojů byl nejvyšší kolem prvního a patnáctého dne v měsíci, což jsou nejčastější výplatní dny.
- Navzdory tomu, že podvody s dárkovými kartami jsou dobře známou technikou podvodu, představují jen 1,9 procenta zjištěných útoků BEC.

Poznatky a jejich využití

Obrana před phishingem

V rámci snižování rizika napadení organizace phishingem je správcům IT doporučováno implementovat následující zásady a funkce:

1. Požadovat používání MFA pro všechny účty, aby se omezily neautorizované přístupy
2. Umožnit funkce podmíněného přístupu pro vysoce privilegované účty, aby byl blokován přístup ze zemí, oblastí a IP adres, z nichž obvykle provoz v organizaci nepochází
3. Zvážit používání fyzických bezpečnostních klíčů pro vedoucí pracovníky, zaměstnance pracující s platbami nebo nákupy a další privilegované účty
4. Vynutit používání prohlížečů, které podporují služby jako Microsoft SmartScreen pro analýzu podezřelého chování na adresách URL a blokování přístupu ke známým škodlivým webům[23]
5. Používat řešení zabezpečení založené na strojovém učení, třeba Microsoft Defender pro Office 365, které přesune vysoce pravděpodobný phishing do karantény a spustí adresy URL a přílohy v sandboxu dříve, než se e-mail dostane mezi příchozí poštu[24]
6. Povolit funkce ochrany před napodobováním a falšováním v celé organizaci
7. Nakonfigurovat zásady akcí DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication Reporting & Conformance), které zabrání doručení neověřených e-mailů, jež by mohly falšovat renomované odesílatele
8. Auditovat tenanty a uživateli vytvořená povolující pravidla a odebrat široké výjimky založené na doménách a IP adresách. Tato pravidla mají často přednost a můžou umožnit známým škodlivým e-mailům projít přes e-mailové filtry.
9. Pravidelně spouštět phishingové simulátory, změřit potenciální riziko v celé organizaci a identifikovat a vzdělávat ohrožené uživatele

Odkazy na další informace

- Od krádeže souborů cookie po BEC: Útočníci používají phishingové weby AiTM jako vstupní bod pro další finanční podvody | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Klamání homoglyfem

BEC a phishing jsou běžné techniky sociálního inženýrství. Ve zločinu hraje sociální inženýrství významnou roli, protože zločinec si dokáže získat důvěru cíle a přesvědčit jej ke spolupráci.

Ve fyzickém obchodě se k zajištění důvěry v původ produktu nebo služby používají ochranné známky a falešné výrobky představují zneužití příslušné známky. Obdobně se kyberzločinci při phishingovém útoku tváří jako kontakt, se kterým je cíl obeznámen. Slouží k tomu homoglyfy, které potenciální oběti oklamou.

Homoglyf je název domény, který se používá pro e-mailovou komunikaci při BEC. V tomto názvu domény je určitý znak nahrazen jiným, který je vzhledově téměř nebo zcela totožný, s cílem oklamat oběť.

Homoglyfické techniky používané při pokusech o BEC

BEC má v obecné rovině dvě fáze. Součástí první z nich je napadení přihlašovacích údajů. Tyto typy úniku přihlašovacích údajů můžou být důsledkem phishingových útoků nebo velkých úniků dat. Přihlašovací údaje jsou pak prodávány nebo obchodovány na temném webu.

Druhá fáze je fáze podvodu, kdy útočníci používají napadené přihlašovací údaje k sofistikovanému sociálnímu inženýrství s využitím homoglyfických e-mailových domén.

Průběh útoku BEC

Technika	% domén vykazujících homoglyfickou techniku
náhr. l za I	25 %
náhr. i za l	12 %
náhr. q za g	7 %
náhr. rn za m	6 %
náhr. .cam za .com	6 %
náhr. 0 za o	5 %
náhr. ll za l	3 %
náhr. ii za i	2 %
náhr. vv za w	2 %
náhr. l za ll	2 %
náhr. e za a	2 %
náhr. nn za m	1 %
náhr. ll za I, náhr. l za i	1 %
náhr. o za u	1 %

Analýza více než 1700 homoglyfických domén v období leden–červenec 2022. Ačkoli bylo využito 170 homoglyfických technik, 75 % domén jich používalo pouze 14.

Homoglyf v praxi

Homoglyfická doména, která vypadá totožně jako poštovní doména, kterou oběť pozná, je zaregistrována u poskytovatele e-mailu se stejným uživatelským jménem. Z napadené domény je pak odeslán zfalšovaný e-mail s novými platebními pokyny.

S využitím opensourcových informací a přístupu k e-mailovým vláknům zločinec identifikuje osoby, které odpovídají za fakturaci a platby. Pak vytvoří napodobeninu e-mailové adresy osoby, která odesílá faktury. Tato napodobenina sestává ze stejného uživatelského jména a poštovní domény, která je homoglyfem skutečného odesílatele.

Útočník zkopíruje e-mailový řetězec obsahující skutečnou fakturu a následně tuto fakturu pozmění tak, aby na ní bylo uvedeno jeho vlastní bankovní spojení. Tato nová, upravená faktura je pak odeslána z homoglyfické napodobeniny e-mailu na cíl. Jelikož kontext dává smysl a e-mail vypadá jako pravý, cíl se často řídí falešnými pokyny.

Poznatky a jejich využití

1. Vynucujte používání prohlížečů, které podporují služby jako Bezpečné odkazy a SmartScreen pro analýzu podezřelého chování na adresách URL a blokování přístupu ke známým škodlivým webům.[25]
2. Používejte řešení zabezpečení založené na strojovém učení, které přesune vysoce pravděpodobný phishing do karantény a spustí adresy URL a přílohy v sandboxu dříve, než se e-mail dostane mezi příchozí poštu.

Odkazy na další informace

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Přehled falšování informací – Office 365 | Microsoft Docs
- Přehled napodobování – Office 365 | Microsoft Docs

Časová osa narušení botnetu z raného období spolupráce s Microsoftem

Více než 10 let DCU pracuje na aktivním boji s kybernetickou kriminalitou. Výsledkem je 26 narušení malwarem a ze strany národních států. S tím, jak tým DCU používá stále pokročilejší techniky a nástroje, se kterými tyto nelegální operace ukončuje, pozorujeme i vývoj na straně kyberzločinců, kteří upravují své postupy ve snaze zůstat o krok napřed. Tady je časová osa, která znázorňuje příklad botnetů narušených jednotkou DCU a strategie, které Microsoft přijal, aby je mohl vyřadit.

2008

Botnet Conficker

Popis: Rychle se šířící červ, který cílil na operační systém Windows a nakazil miliony počítačů a zařízení ve společné síti, čímž po celém světě způsoboval výpadky sítí.

Spolupráce: Sestavení pracovní skupiny Conficker, prvního konsorcia svého druhu. Microsoft navázal partnerství s 16 organizacemi po celém světě, aby botnet porazil.

Reakce Microsoftu: Skupina spolupracovala v mnoha mezinárodních jurisdikcích a úspěšně zlikvidovala Conficker.

2009

Botnet Waledac

Popis: Složitý spamovací botnet s doménami USA, který shromažďoval e-mailové adresy a distribuoval spam, jímž bylo nakaženo po celém světě až 90 tisíc počítačů.[26]

Spolupráce: Vytvoření dalšího konsorcia, centra Microsoft Malware Protection Center (MMPC), které se zaměřuje na úzkou spolupráci s akademickým sektorem.[27]

Reakce Microsoftu: Microsoft k narušení využil vrstvený přístup C2 a překvapil škodlivé aktéry zajištěním domén v USA bez předchozího oznámení.[28] Microsoft udělil dočasné vlastnictví téměř 280 domén používaných servery sítě Waledac.

2011

Sestavení týmu Digital Crimes Unit v Microsoftu

Spolupráce: Navržena jako prostředek boje proti kybernetické kriminalitě, která má vliv na ekosystém Microsoftu, prostřednictvím těsné integrace týmů vyšetřovatelů, právníků a techniků.

Přístup Microsoftu: Cílem je lépe porozumět technickým aspektům různých malwarů a nabízet tyto poznatky právnímu týmu Microsoftu, aby mohla vzniknout účinná strategie narušení.

2013

Botnet Rustock

Popis: Bot pro rozesílání spamu s trojským koněm instalujícím zadní vrátka, který jako primární C2 používal poskytovatele internetu a byl navržen na prodej léčiv.

Spolupráce: Microsoft navázal partnerství se společností Pfizer Pharmaceuticals, aby porozuměl lékům prodávaným v síti Rustock, a úzce spolupracoval s nizozemskými policejními složkami.[29]

Reakce Microsoftu: Microsoft spolupracoval s US Marshals a policejními složkami v Nizozemsku na likvidaci nizozemských serverů C2. Zaregistroval a zablokoval všechny budoucí algoritmy generování domén (DGA).

Botnet Sirefef/ZeroAccess

Popis: Reklamní botnet navržený na přesměrování uživatelů na nebezpečné weby, které by nainstalovaly malware nebo ukradly osobní údaje, napadl více než dva miliony počítačů a stál inzerenty více než 2,7 milionu USD měsíčně, především ve Spojených státech a v západní Evropě.

Spolupráce: Úzká spolupráce s FBI a Centrem pro boj proti kybernetické kriminalitě Europolu při likvidaci partnerské infrastruktury.

Reakce Microsoftu: Připojil se k síti Zero Access, nahradil servery C2 zločinců a úspěšně zajistil domény stahovacích serverů.

2019

Botnet Trickbot

Popis: Důmyslný botnet s infrastrukturou rozmístěnou po celém světě, který cílil na odvětví finančních služeb a napadal zařízení IoT.

Spolupráce: Microsoft se spojil s konsorciem Financial Services Information Sharing and Analysis Center (FS-ISAC) s cílem vyřadit Trickbot.[30]

Reakce Microsoftu: Tým DCU sestavil systém pro identifikaci a sledování infrastruktury robotů a generoval oznámení pro aktivní poskytovatele internetu, přičemž zohledňoval konkrétní zákony v různých zemích.

2022

Pokračující zaměření na narušování

Popis: Microsoft v posledním roce narušil infrastrukturu sedmi aktérů hrozeb, čímž jim zabránil distribuovat další malware, převzít kontrolu nad počítači obětí a cílit na další oběti.

Spolupráce: Ve spolupráci s poskytovateli internetových služeb, státními správami, policejními složkami a soukromým sektorem se Microsoft podělil o informace, které pomohly více než 17 milionům obětí malwaru po celém světě.

Další kroky

DCU pokračuje v inovacích a snaží se využít své zkušenosti z narušování botnetů k organizaci koordinovaných operací i nad rámec malwaru. Abychom byli úspěšní i v budoucnu, potřebujeme kreativní inženýrství, sdílení informací, inovativní právní teorie a veřejná a soukromá partnerství.

Kybernetické zneužití infrastruktury

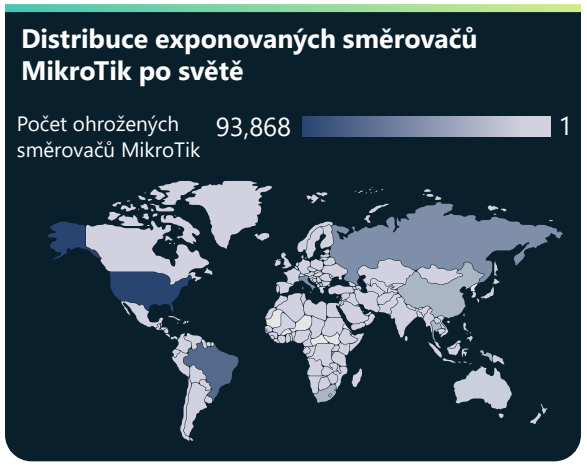
Internetové brány jako infrastruktura pro organizování zločinu

Zařízení IoT se stávají stále oblíbenějším cílem kyberzločinců, kteří využívají rozsáhlé botnety. Pokud uživatelé neinstalují opravy na své směrovače a nechávají je připojené přímo k internetu, aktéři hrozeb je můžou zneužít k přístupu do sítě, zahajování škodlivých útoků, a dokonce i k podpoře jejich operací.

Tým Microsoft Defender for IoT provádí výzkum zařízení od starších kontrolerů průmyslových řídicích systémů až po nejmodernější senzory IoT. Zkoumá malware specifický pro IoT a OT, aby rozšířil sdílený seznam ukazatelů napadení.

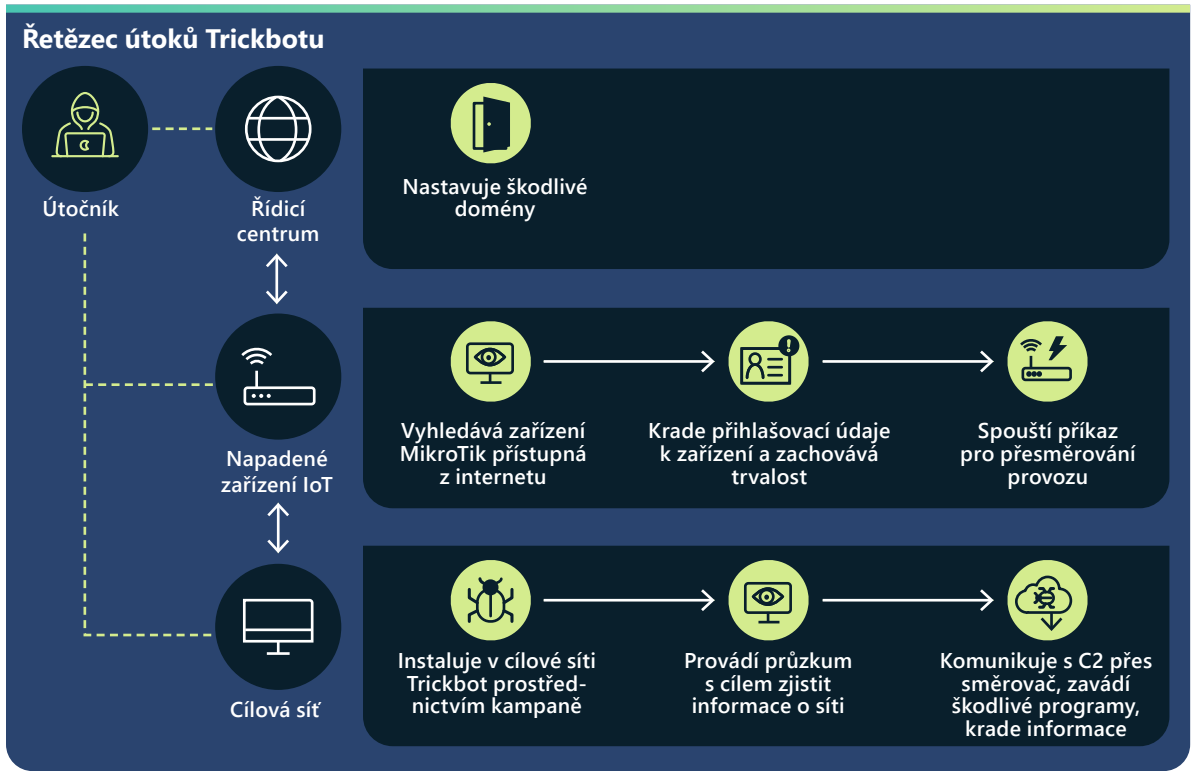
Směrovače jsou obzvláště ohrožené vektory útoku, protože jsou všudypřítomné – nacházejí se v domácnostech i organizacích připojených k internetu. Sledovali jsme aktivitu směrovačů MikroTik, které jsou oblíbené po celém světě u domácích i firemních zákazníků, a zjišťovali jsme, jak se využívají k ovládání a řízení (C2), útokům na DNS (Domain Name System) a neužívání počítačů k těžbě kryptoměn.

Konkrétně jsme zjistili, jak operátoři Trickbotu využívají napadené směrovače MikroTik a mění jejich konfiguraci tak, aby je mohli použít jako součást své infrastruktury C2. Oblíbenost těchto zařízení přispívá k závažnosti jejich zneužití Trickbotem a jejich jedinečný hardware a software umožňují aktérům hrozeb vyhnout se tradičním bezpečnostním opatřením, rozšířit svou infrastrukturu a napadat další zařízení a sítě.



Odhalené směrovače jsou ohroženy zneužitím možných chyb v zabezpečení.

Sledováním a analýzou provozu obsahujícího příkazy Secure Shell (SSH) jsme pozorovali útočníky, kteří používají směrovače MikroTik ke komunikaci s infrastrukturou Trickbotu poté, co získali legitimní přihlašovací údaje k zařízením. Tyto přihlašovací údaje lze získat prostřednictvím útoků hrubou silou, zneužitím známých chyb v zabezpečení, které mají k dispozici opravy, a používáním výchozích hesel. Po získání přístupu k zařízení útočník spustí jedinečný



Řetězec útoků Trickbotu znázorňující používání IoT zařízení MikroTik jako proxy serverů pro C2

příkaz, který přesměruje provoz mezi dvěma porty na směrovači. Tím naváže komunikaci mezi zařízeními napadenými Trickbotem a C2.

Naše znalosti různých metod útoků na zařízení MikroTik, nejen Trickbotu, a známých běžných chyb zabezpečení a rizik (CVE) jsme sloučili do opensourcového nástroje pro zařízení MikroTik, který dokáže extrahovat forenzní artefakty související s útoky na tato zařízení.[31]

Zařízení fungující jako reverzní proxy pro C2 malwaru nejsou jedinečná jen pro Trickbot a směrovače MikroTik. Ve spolupráci s týmem RiskIQ v Microsoftu jsme vysledovali zapojená C2 a pozorováním certifikátů SSL jsme identifikovali zařízení Ubiquiti a LigoWave, která byla napadena také.[32] Z toho zřejmě vyplývá, že se zařízení IoT stávají aktivními součástmi útoků koordinovaných národními státy a oblíbenými cíli kyberzločinců, kteří používají velké botnety.

Kryptozločinci zneužívají zařízení IoT

Zařízení bran jsou stále hodnotnější cíl pro aktéry hrozeb, protože počet známých chyb v zabezpečení rok od roku soustavně roste. Používají se pro těžbu kryptoměn a další typy škodlivých aktivit.

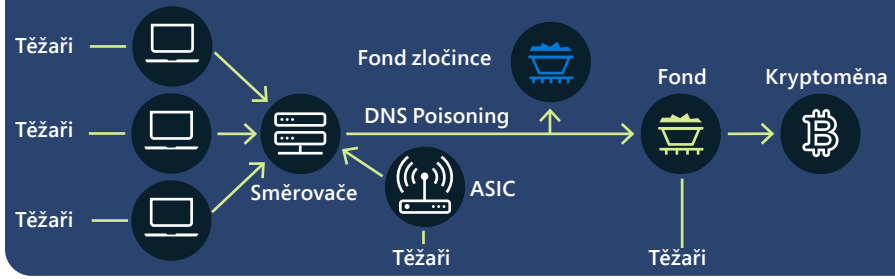
Se stále rostoucí oblibou kryptoměn mnoho lidí i organizací investovalo výpočetní výkon a síťové prostředky ze zařízení, jako jsou směrovače, k těžbě mincí na blockchainu. Těžba kryptoměn je ale proces náročný na čas i prostředky s nízkou pravděpodobností úspěchu. Aby těžaři zvýšili pravděpodobnost vytěžení mince, seskupují se do distribuovaných sítí pro spolupráci, ve kterých získávají procentuální podíl na úspěšně vytěžené minci podle počtu hodnot hash vypočítaných jejich připojenými prostředky.

Za poslední rok Microsoft zjistil, že narůstá počet útoků, které zneužívají směrovače pro přesměrování těžby kryptoměn.

Kyberzločinci napadají směrovače připojené k těžařským skupinám a pomocí útoků DNS Poisoning, které upravují nastavení DNS cílových zařízení, přesměrovávají komunikaci těžby na své IP adresy. Napadené směrovače zaregistrují pro daný název domény nesprávnou IP adresu a odešlou své těžební prostředky – nebo hodnoty hash – do skupin aktérů hrozeb. Tyto skupiny můžou těžit anonymní mince související s trestnou činností nebo používat legitimní hodnoty hash vygenerované těžaři, aby získaly procento z vytěžené mince. Tím si zajišťují svou odměnu.

> Jelikož více než polovina známých chyb v zabezpečení objevených v roce 2021 nemá opravu, aktualizace a zabezpečení směrovačů ve firemních i soukromých sítích zůstává významným problémem vlastníků a správců zařízení.

Napadání zařízení pro nelegální těžbu kryptoměn



Útok DNS Poisoning na zařízení bran ohrožuje legitimní těžební činnosti a přesměrovává prostředky na trestné těžební aktivity.

Virtuální počítače jako infrastruktura pro zločiny

K hromadnému přechodu do cloudu se přidávají i kyberzločinci, kteří využívají privátní prostředky nic netušících obětí získané prostřednictvím phishingu nebo distribuovaných nástrojů pro krádež přihlašovacích údajů. Mnoho kyberzločinců volí jako základ svých škodlivých infrastruktur cloudové virtuální počítače, kontejnery a mikroslužby.

Jakmile kyberzločinec získá přístup, k zavedení infrastruktury může vést posloupnost událostí, třeba vytvoření řady virtuálních počítačů skriptováním a automatizovaných procesů. Tyto skriptované automatizované procesy se používají k zahajování škodlivých aktivit, včetně rozsáhlých útoků e-mailovým spamem, phishingových útoků a webových stránek hostujících škodlivý obsah. Mezi škodlivé aktivity může patřit i nastavení škálovaného virtuální prostředí, které těží kryptoměny. To pak pro koncovou oběť může znamenat účet ve výši stovek tisíc dolarů na konci měsíce.

Kyberzločinci jsou si vědomi, že jejich škodlivá aktivita má omezenou životnost, než bude detekována a zablokována. Proto pokročili dále a teď aktivně pracují i s připravenými náhradními plány. Bylo zpozorováno, jak předem připravují napadené účty a monitorují jejich prostředí. Hned jak je účet (nastavený pomocí stovek tisíc virtuálních počítačů) detekován, přejdou na další účet, který je už připraven na okamžitou aktivaci skriptem, a škodlivá aktivita pokračuje dále jen s krátkou, nebo dokonce vůbec žádnou přestávkou.

Podobně jako cloudovou infrastrukturu je možné i místní infrastrukturu použít při útocích virtuálními místními prostředími, která jsou místnímu uživateli neznámá. To vyžaduje, aby počáteční vstupní bod zůstal otevřený a přístupný. Dále kyberzločinci zneužívají místní privátní prostředky k vytvoření následného řetězce cloudové infrastruktury nastavené na zakrytí jejich původu tak, aby nedošlo k detekci vytvoření podezřelé infrastruktury.

Poznatky a jejich využití

1. Implementujte dobrou kybernetickou hygienu a zajišťujte zaměstnancům školení v oblasti kybernetické bezpečnosti, aby věděli, jak se bránit sociálnímu inženýrství.
2. Provádějte pravidelné automatizované kontroly anomálií v aktivitě uživatelů prostřednictvím škálovatelných detekcí, které omezí tyto typy útoků.
3. Aktualizujte a zabezpečte směrovače ve firemních a privátních sítích.

Je hacktivismus nezvratný trend?

Ačkoli hacktivismus není nový jev, válka na Ukrajině s sebou přinesla prudký nárůst dobrovolných hackerů. Patří mezi ně i takoví, jejichž činnost řídila státní správa a kteří nasazovali kybernetické nástroje k poškozování pověsti nebo prostředků politických protivníků, organizací, nebo dokonce i národních států.

V únoru 2022 ukrajinská státní správa vybídla soukromé osoby po celém světě, aby jako součást její 300tisícové „IT armády" prováděly kybernetické útoky na Rusko.[33] Ve stejnou chvíli zavedené haktivistické skupiny, třeba Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans a RaidForum2, začaly provádět útoky na podporu Ukrajiny. Jiné skupiny, včetně některých členů ransomwarového gangu Conti, se postavily na stranu Ruska.[34]

V následujících měsících byly aktivity skupiny Anonymous velmi patrné. Hackeři, kteří jednali jménem skupiny – nebo jménem jednoho z jejích partnerů – dočasně vyřadili tisíce ruských a běloruských webů, zveřejnili stovky gigabajtů kradených dat, napadli ruské televizní kanály a nasadili proukrajinský obsah, a dokonce i nabídli bitcoinovou platbu za odevzdané ruské tanky.

Vzestup hackerů z řad občanů

Platformy sociálních médií umožnily rychlou organizaci a mobilizaci tisíců potenciálních občanských hackerů, kterým byly poskytnuty informace, jak vést snadné útoky, jako je DDoS. Organizátoři využívali Twitter, Telegram a privátní fóra, kde shromažďovali hackery, organizovali operace a šířili pokyny, jak hackovat.

Většina těchto hackerů však měla pravděpodobně jen omezené dovednosti, a to i s pokyny. Plynou z toho dvě možné varianty budoucnosti: jedna zahrnuje stovky tisíc jednotlivců se základními technickými dovednostmi, kteří budou s pomocí šablon útoků provádět budoucí koordinované nebo individuální haktivistické útoky proti cílům. V druhé budoucnosti nakonec dojde k ukončení nepřátelských aktivit na Ukrajině, čímž se hacktivismus stane minulostí, alespoň do dalšího politického nebo společenského problému, který opět podnítí akci.

Politizace hackerů

Větší riziko, které tato politická mobilizace představuje, je nasazení technicky zdatných hackerů, kteří budou pokračovat v kybernetických útocích proti cizím státním cílům na podporu svých vlastních národních priorit, ať už ze své vlastní iniciativy, nebo na pokyn své státní správy.

Írán, Čína a Rusko už hacktivismus používají jako prostředek náboru do státních hackerských skupin. Například v dubnu roku 2022 zahájila proruská hackerská skupina Killnet útoky DDoS na České dráhy, místní letiště a server české veřejné služby, i když Česko není přímo zapojeno do války.[35] Ve stejnou chvíli některé státní správy můžou používat hacktivismus jako krytí tradičních operací kybernetické špionáže nebo sabotáže – například íránské aktivity proti Izraeli.

V prostředí s vyšším počtem útoků DDoS spojených s hacktivismem má technologický průmysl před sebou náročný úkol rychle porozumět rozdílu mezi běžným a neobvyklým tokem dat na web. Microsoft a jeho partneři vyvinuli sadu nástrojů, které odliší škodlivý provoz DDoS a sledují jej zpět k jeho zdroji. Kromě toho dokáže platforma Azure od Microsoftu identifikovat počítače, které se na ní nacházejí a vytvářejí neobvykle vysoké úrovně odchozího provozu. Takové počítače pak vypíná.

Vznik protestwaru

Protestware vznikl jako přímý důsledek citové odezvy na válku mezi Ruskem a Ukrajinou. Někteří vývojáři opensourcového softwaru využili oblíbenosti svého softwaru jako prostředek, jak vyjádřit svůj názor nebo udělat něco proti nastávající geopolitické situaci. Takovými prostředky mohly být neškodné textové soubory otevřené na ploše nebo v prohlížeči, které hlásaly mír, ale třeba i cílené útoky podle geografické polohy IP adresy a ničivé akce, jako je vymazání pevného disku. S postupným vývojem celosvětových událostí můžeme očekávat, že se v budoucnu protestware opět objeví. Jelikož jde v obecné rovině o případy, kdy se uznávaní opensourcoví vývojáři rozhodují vyjadřovat pomocí svých vlastních opensourcových součástí osobní názory, neexistuje v současné době žádný způsob, jak v balíčcích zdrojových souborů těmto změnám zabránit. Uživatelé by měli mít na paměti možný dopad.

> Platformy sociálních médií umožnily organizaci a mobilizaci tisíců potenciálních občanských hackerů, kterým byly poskytnuty informace, jak vést snadné útoky, jako je DDoS.

Poznatky a jejich využití

1. Technologický průmysl se musí spojit a navrhnout komplexní odpověď na tuto novou hrozbu.
2. Přední technologické společnosti, mezi které patří i Microsoft, mají nástroje k identifikaci škodlivého provozu souvisejícího s útoky DDoS a vyřazují počítače, ze kterých pocházejí.
3. Uživatelé opensourcového softwaru by měli během geopolitických konfliktů dbát zvýšené opatrnosti.

Poznámky na závěr

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. Detekce a reakce u koncových bodů. 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. Prověřené fórum je online diskuzní fórum, které vyžaduje, aby se stávající člen zaručil za nově přidávaného člena.
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. Zdroj dat: Defender pro Office (škodlivý e-mail / aktivita napadeného účtu), Azure Active Directory Identity Protection (události/upozornění napadených identit), Defender for Cloud Apps (události přístupu k datům napadených identit) a M365D (korelace mezi produkty).
17. Zdroj dat: Defender for Endpoint (události/upozornění na průběh útoku), Defender pro Office (škodlivý e-mail) a M365D (korelace mezi produkty).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Ověřování, vykazování a dodržování shody zpráv podle domény: Protokol pro ověřování e-mailů, zásady a vykazování, které vlastníkům e-mailových domén umožňuje chránit doménu před neoprávněným použitím.
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. 22. února 2010).
27. Viz Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27. září 2011.
28. Konkrétně rozsudek 65 sbírky Federal Rules of Civil Procedure umožňuje účastníkovi zajistit takovou nápravu, pokud: 1) účastník utrpí bezprostřední a neodčinitelnou újmu, nebude-li náprava učiněna, a 2) účastník se pokusí zaslat protistraně včas oznámení. Zákon navíc vyžaduje, aby byl proveden test vyváženosti, který vyvažuje právo obžalovaného na oznámení s mírou újmy veřejnosti.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9. února 2011).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12. srpna 2021).
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

Hrozby ze strany národních států

Aktéři národních států zahajují své stále propracovanější kybernetické útoky, aby se nedali snadno přistihnout a podpořili své strategické priority.

Přehled hrozeb

ze strany národních států

Aktéři národních států zahajují své stále propracovanější kybernetické útoky, aby se nedali snadno přistihnout a podpořili své strategické priority. Nasazením kybernetických zbraní v hybridní válce na Ukrajině započal nový věk konfliktů.

Rusko svou válku podpořilo i operacemi ovlivňování informací, když pomocí propagandy ovlivňovalo názory v Rusku, na Ukrajině i po celém světě. Z prvního hybridního konfliktu v plném rozsahu jsme získali i další důležité poznatky. Zaprvé, zabezpečení digitálních operací a dat, a to v kyberprostoru i ve fyzickém světě, lze nejlépe zajistit přesunem do cloudu. Počáteční ruské útoky cílily na místní služby, do kterých nasazovaly malware určený k mazání dat, a jedna z prvních vystřelených raket mířila na fyzická datacentra.

Ukrajina zareagovala urychleným přesunem úloh a dat do hyperškálovatelných cloudů hostovaných v datacentrech mimo Ukrajinu. Zadruhé, pokroky v získávání informací o kybernetických hrozbách a ochrana koncových bodů založená na datech a pokročilých službách AI a ML v cloudu pomohly Ukrajině v obraně před kybernetickými útoky Ruska.

Jinde aktéři národních států zintenzivnili své aktivity a využívají pokroků v technologiích automatizace, cloudové infrastruktury a vzdáleného přístupu, s nimiž útočí na širší skupinu cílů. Častými cíli byly firemní dodavatelské řetězce pro IT, které umožňují přístup ke konečným cílům. Teď, když aktéři rychle zneužívají neopravené chyby v zabezpečení, používají důmyslné techniky i hrubou sílu ke krádeži přihlašovacích údajů a zakrývají své operace pomocí opensourcového nebo legitimního softwaru, je hygiena kybernetické bezpečnosti důležitější než kdy dříve. A kromě Ruska pak ničivé kybernetické zbraně, včetně ransomwaru, používá i Írán, který na nich zakládá své útoky.

Tato situace vyžaduje urychlené přijetí konzistentní celosvětové architektury, která upřednostňuje lidská práva a chrání lidi před bezohledným chováním států na internetu. Všechny národy musí spolupracovat na implementaci uznávaných norem a pravidel pro odpovědné chování států.

Obrana Ukrajiny: První ponaučení z kybernetické války – Microsoft On the Issues

Častější cílení na kritickou infrastrukturu, obzvláště pak sektor IT, finanční služby, dopravní systémy a komunikační infrastrukturu

Více se dozvíte na str. 35

Dodavatelský řetězec IT se používá jako brána pro přístup k cílům.

NOBELIUM

Více se dozvíte na str. 36

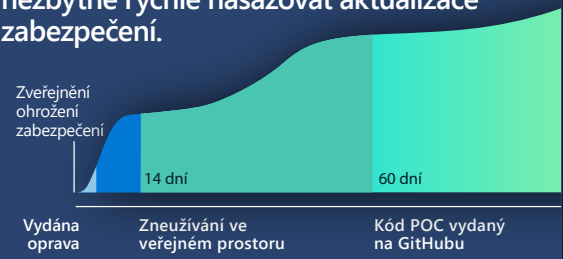
Čína rozšiřuje globální cílení, obzvláště na malé státy v jihovýchodní Asii, aby získala informace a konkurenční výhodu.

Více se dozvíte na str. 44

Írán je od převodu moci stále agresivnější, rozšířil ransomwarové útoky za hranice místních protivníků na USA a EU a cílí na exponovanou kritickou infrastrukturu v USA.

Více se dozvíte na str. 46

Hlavní taktikou se staly identifikace a rychlé zneužívání neopravených chyb v zabezpečení. Pro úspěšnou obranu je nezbytné rychle nasazovat aktualizace zabezpečení.



Více se dozvíte na str. 39

Severní Korea cílí na obranné a letecké společnosti, kryptoměny, zpravodajské kanály, zběhy a humanitární organizace, aby dosáhla cílů režimu: vybudovat obranu, posílit ekonomiku a zajistit domácí stabilitu.

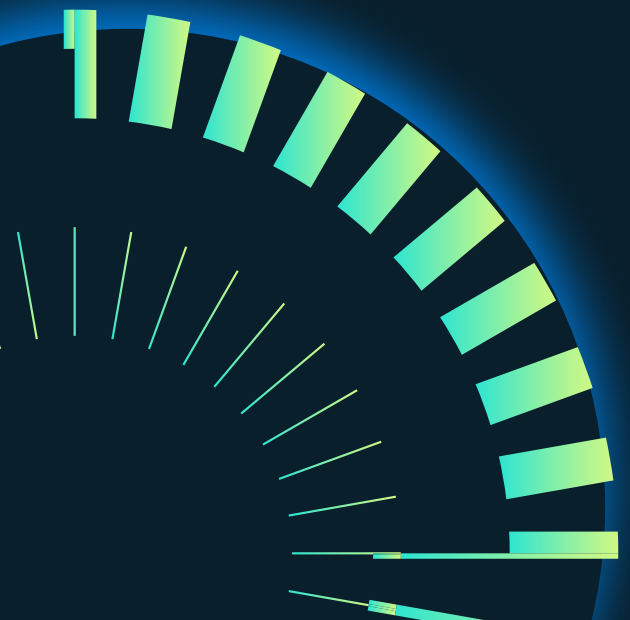
Více se dozvíte na str. 49

Kybernetičtí žoldnéři ohrožují stabilitu kyberprostoru, protože tento rostoucí obor soukromých společností vyvíjí a prodává pokročilé nástroje, techniky a služby, které klientům (jimiž jsou často státní správy) umožňují proniknout do sítí a na zařízení.

Více se dozvíte na str. 52

Úvod

V návaznosti na známé útoky v letech 2020 a 2021 aktéři hrozeb národních států vynaložili značné prostředky na nové bezpečnostní ochrany, které organizace implementují v rámci obrany před propracovanými hrozbami.



Podobně jako podnikové organizace také protivníci začali používat pokroky v automatizaci, cloudové infrastruktuře a technologiích vzdáleného přístupu k rozšíření útoků na větší okruh cílů. Tyto změny v taktice vyústily v nové přístupy a rozsáhlé útoky proti firemním dodavatelským řetězcům. Hygiena zabezpečení IT začala být o to důležitější, protože aktéři vyvinuli nové způsoby rychlého zneužívání neopravených chyb v zabezpečení, rozšířili techniky napadání firemních sítí a zakryli své operace opensourcovým nebo legitimním softwarem. Nové techniky útoku zajistily nové a hůře zjistitelné vektory, kterými je možné získat přístup do sítě cíle. A se stále silnějšími válečnými fyzickými útoky jsme zaznamenali, že kybernetické útoky začaly hrát významnou roli ve vojenské aktivitě.

Konflikt na Ukrajině předvedl až příliš hořkou ukázku, jak se kybernetické útoky vyvíjejí tak, aby ovlivnily svět bok po boku vojenského střetu na zemi. Energetické systémy, telekomunikační systémy, média a další kritická infrastruktura se staly cílem fyzických i kybernetických útoků. Pokusy o napadení sítě, ke kterým běžně docházelo v rámci kampaní špionáže a exfiltrace informací, se v hybridní válce zaměřovaly na ničivé útoky malwarem určeným k mazání dat na systémy kritické infrastruktury. Propojení zabezpečení těchto systémů s cloudem umožnilo včas zjišťovat a narušovat útoky s potenciálně devastujícími následky.[1]

Vůbec poprvé byly při velké kybernetické události použity detekce chování, které využívají strojové učení a známé vzory útoků. Úspěšně jimi byly identifikovány a zastaveny další útoky, aniž by byl předem znám používaný malware, a to dokonce dříve, než si hrozeb byli vědomi lidé. Kromě toho jsme potvrdili, že má význam v reálném čase sdílet informace o hrozbách s obránci, kteří tyto systémy chrání. Získají tak totiž stěžejní informace, s nimiž můžou očekávat aktivní útoky a bránit se jim.

Aktéři hrozeb národních států po celém světě i nadále rozšiřují svou působnost novými i zavedenými způsoby. Čína, Severní Korea, Írán i Rusko podnikaly útoky na zákazníky Microsoftu. Běžným cílem se stal dodavatelský řetězec IT služeb, protože aktéři přesunuli svou pozornost k navazujícím službám, které se můžou stát přístupovými body hned do několika organizací. Očekáváme, že aktéři budou i nadále zneužívat důvěrné vztahy ve firemních dodavatelských řetězcích. To jen zdůrazňuje důležitost uceleného vynucování pravidel ověřování, důsledného opravování a konfigurace účtů pro infrastrukturu vzdáleného přístupu a časté auditování vztahů s partnery, které ověří jejich pravost.

Jak aktéři národních států, tak operátoři ransomwaru a kyberzločinci zareagovali na větší expozici tím, že cílí na chybně nakonfigurované nebo neopravené podnikové systémy (infrastrukturu VPN/VPS, místní servery, software třetích stran) a provádějí útoky pomocí čehokoli, co v systémech najdou. Mnoho z nich začalo častěji používat komoditní malware a opensourcové nástroje červených týmů, kterými kryjí svou škodlivou aktivitu.

Kvůli tomu je zachování silného standardu hygieny zabezpečení IT prostřednictvím prioritních oprav, zaváděním funkcí proti neoprávněné manipulaci, používáním nástrojů pro správu potenciálních oblastí útoků, třeba RiskIQ, s nimiž lze získat ucelený pohled na oblast útoku, a povolením vícefaktorového ověřování v celé firmě základním předpokladem pro aktivní obranu před mnoha důmyslnými aktéry.

Aktéři národních států také ve větší míře využívají ransomware jako taktiku při svých útocích a častěji pro ně přebírají vyděračský malware vytvořený daným zločineckým ekosystémem. Pozorovali jsme aktéry z Íránu i Severní Korey, kteří pomocí komoditních ransomwarových nástrojů poškozovali cílové systémy, často i kritickou infrastrukturu, svých místních protivníků. A viděli jsme i narůstající hrozbu kybernetických žoldnéřů, kteří vyvíjejí a prodávají nástroje, techniky a služby, s nimiž lze rozšířit zneužívání na ohrožená řešení třetích stran. Důmyslnost a pružnost útoků aktérů národních států se bude každým rokem rozvíjet. Organizace musí zareagovat získáváním informací o těchto změnách u aktérů a ve stejné chvíli vyvíjet obranné prostředky.

John Lambert
Corporate Vice President and Distinguished Engineer, Microsoft Threat Intelligence Center

Pozadí dat národních států

Hrozby národních států jsou nebezpečné kybernetické aktivity, jejichž původem je konkrétní země se zřejmým cílem podpořit národní zájmy. Aktéři národních států patří mezi nejvyspělejší a nejtrvalejší hrozby, kterým naši zákazníci čelí. Patří mezi ně krádež duševního vlastnictví, špionáž, sledování, krádež přihlašovacích údajů, ničivé útoky a podobně.

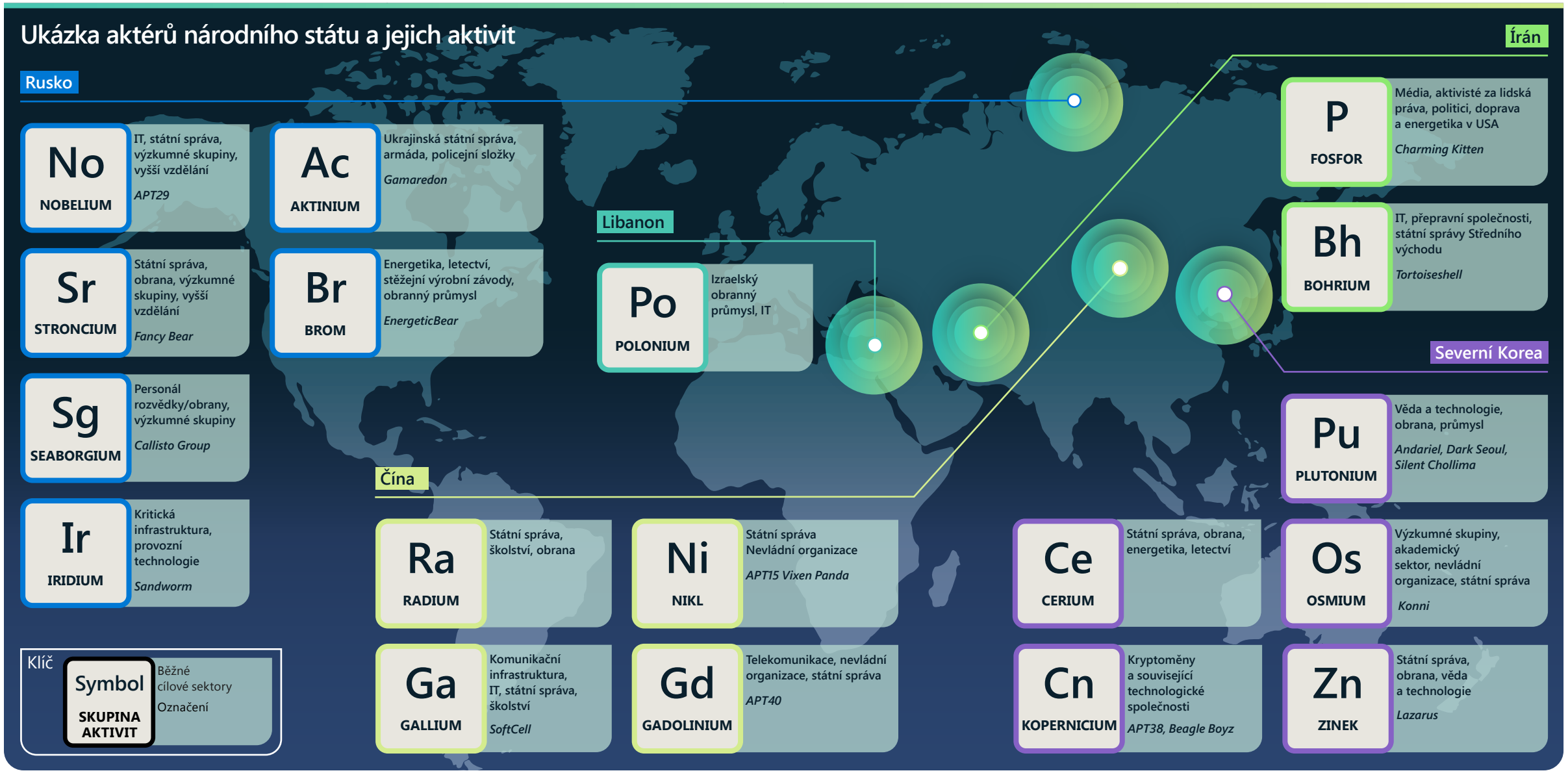
Investujeme značné prostředky do objevování, zkoumání a potírání těchto hrozeb. Pokud na organizaci nebo jednotlivce se zaregistrovaným účtem cílí nebo útočí pozorované aktivity národního státu, Microsoft přímo zákazníkovi zašle upozornění ve tvaru oznámení o národním státu (NSN), ve kterém zákazník najde informace potřebné k prověření dané aktivity. K červnu 2022 jsme doručili více než 67 000 NSN. Začali jsme v roce 2018.

V této kapitole představíme data upozornění NSN od Microsoftu a nabídneme tak pohled na měřitelnou aktivitu. Úroveň aktivity národního státu vyobrazená v grafech se zakládá na počtu NSN, které Microsoft zaslal zákazníkům v reakci na detekci aktérů národních států, kteří cílili nebo napadli alespoň jeden účet v organizaci zákazníka.

Čtyři hlavní národní státy, jejichž skupiny hrozeb zahrnujeme do této zprávy, jsou Rusko, Čína, Írán a Severní Korea. Z těchto zemí pochází nejčastěji pozorovaní aktéři, kteří za poslední rok cílili na zákazníky Microsoftu. Zpráva uvádí i naše poznatky o skupinách hrozeb z Libanonu a od kybernetických žoldnéřů, případně nájemných útočníků ze soukromého sektoru.

Skupiny národních států Microsoft identifikuje názvy chemických prvků (například NOBELIUM), z nichž některé jsou uvedeny na následující stránce. Označení DEV-#### pak používáme jako dočasný název pro neznámé, objevující se nebo rozvíjející se shluky nebezpečné aktivity. Umožňuje nám to sledovat je jako jedinečnou sadu informací, než dosáhneme vysoké míry jistoty o jejich původu nebo o identitě aktéra, který za nimi stojí.

Jakmile DEV splní kritéria, je převeden na pojmenovaného aktéra nebo sloučen s existujícími aktéry. V průběhu této kapitoly budeme citovat příklady skupin národních států a DEV a nabídneme hlubší pohled na cíle útoků, techniky a analýzy jejich motivací. Ačkoli mnoho z těchto skupin používá stejné nástroje jako kyberzločinci, představují jedinečné hrozby ve formě malwaru na míru, schopnosti objevit a využít ohrožení zabezpečení nultého dne a právní beztrestnosti.


Ukázka aktérů národního státu a jejich aktivit
Rusko
No
NOBELIUM
IT, státní správa, výzkumné skupiny, vyšší vzdělání
APT29
Ac
AKTINIUM
Ukrajinská státní správa, armáda, policejní složky
Gamaredon
Sr
STRONCIUM
Státní správa, obrana, výzkumné skupiny, vyšší vzdělání
Fancy Bear
Br
BROM
Energetika, letectví, stěžejní výrobní závody, obranný průmysl
EnergeticBear
Sg
SEABORGIUM
Personál rozvědky/obrany, výzkumné skupiny
Callisto Group
Ir
IRIDIUM
Kritická infrastruktura, provozní technologie
Sandworm
Libanon
Po
POLONIUM
Izraelský obranný průmysl, IT
Írán
P
FOSFOR
Média, aktivisté za lidská práva, politici, doprava a energetika v USA
Charming Kitten
Bh
BOHRIUM
IT, přepravní společnosti, státní správy Středního východu
Tortoiseshell
Severní Korea
Pu
PLUTONIUM
Věda a technologie, obrana, průmysl
Andariel, Dark Seoul, Silent Chollima
Čína
Ra
RADIUM
Státní správa, školství, obrana
Ni
NIKL
Státní správa Nevládní organizace
APT15 Vixen Panda
Ce
CERIUM
Státní správa, obrana, energetika, letectví
Os
OSMIUM
Výzkumné skupiny, akademický sektor, nevládní organizace, státní správa
Konni
Ga
GALLIUM
Komunikační infrastruktura, IT, státní správa, školství
SoftCell
Gd
GADOLINIUM
Telekomunikace, nevládní organizace, státní správa
APT40
Cn
KOPERNICIUM
Kryptoměny a související technologické společnosti
APT38, Beagle Boyz
Zn
ZINEK
Státní správa, obrana, věda a technologie
Lazarus
Klíč
Symbol
SKUPINA AKTIVIT
Běžné cílové sektory
Označení

Vyvíjející se prostředí hrozeb

Poslání Microsoftu sledovat aktivitu aktérů národních států a oznamovat zákazníkům, že jsme zjistili cílení a útoky na ně, je součástí naší mise chránit zákazníky před útoky.

Toto oznámení je stěžejní součástí našeho závazku informovat zákazníky, jestli bylo zjištěným útokům úspěšně zabráněno ochranami našich bezpečnostních produktů, nebo jestli byly útoky účinné kvůli neznámému nedostatku v zabezpečení. Sledování oznámení v průběhu času pomáhá Microsoftu identifikovat proměnlivé trendy hrozeb ze strany aktérů a zacílit ochranu produktů na aktivní zmírňování hrozeb pro zákazníky v našich cloudových službách.

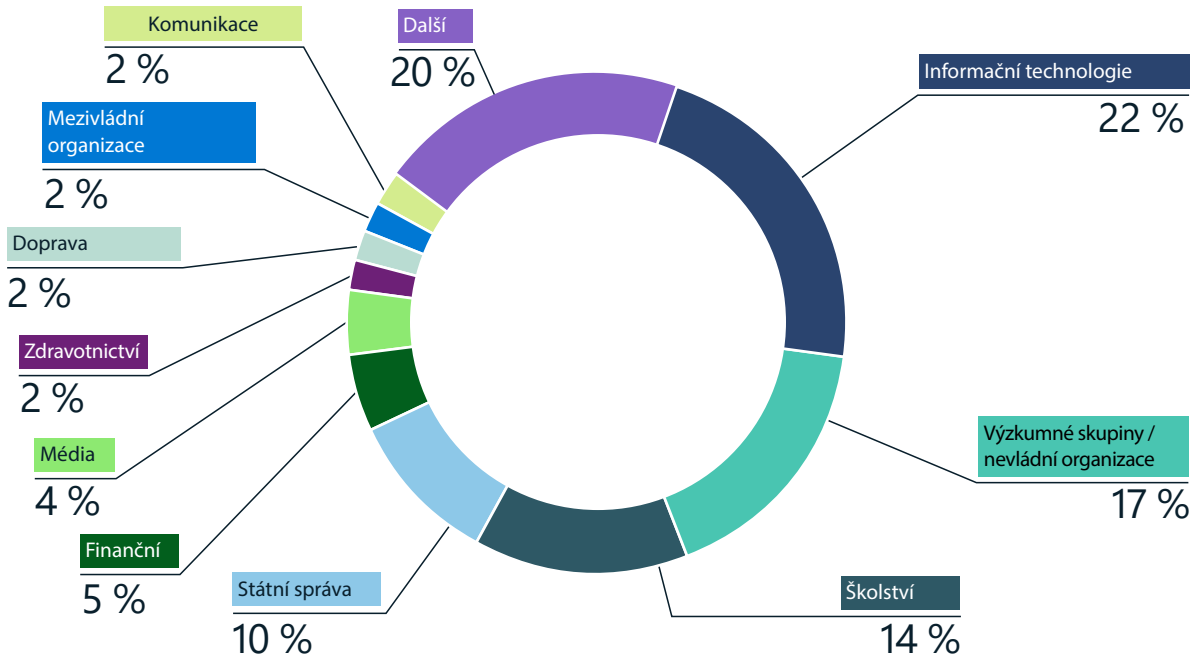
Díky takovému sledování můžeme navíc sdílet data a přehledy o tom, co zjišťujeme. Analytici, kteří sledují aktéry a jejich útoky, spoléhají na kombinaci technických indikátorů a odbornost v geopolitických záležitostech, která jim umožňuje porozumět motivacím aktérů. Technický a globální kontext tak spojují do nových poznatků. Toto kurátorování nabízí jedinečný pohled na priority kybernetických aktérů národních států a na to, jak jejich motivace můžou odrážet politické, vojenské a ekonomické priority národních států, které je zaměstnávají.

Politický vývoj za poslední rok stanovil priority a postoj k rizikům státem sponzorovaných skupin hrozeb po celém světě. S tím, jak se oslabují geopolitické vztahy a jak průbojní jedinci získávají v některých státech větší vliv, jsou kybernetičtí aktéři otrlejší a agresivnější. Například:

- Rusko neúnavně útočilo na ukrajinskou státní správu a kritickou infrastrukturu země, čímž doplňovalo pozemní vojenské operace.[2]
- Írán agresivně hledal přístupové cesty ke kritické infrastruktuře v USA, třeba k přístavním správám.
- Severní Korea pokračovala ve své kampani krádeže kryptoměn od finančních a technologických společností.
- Čína rozšířila své globální operace kybernetické špionáže.

I když aktéři národních států dokážou být technicky zdatní a využívají širokou paletu taktik, jejich útoky je často možné zmírnit dobrou kybernetickou hygienou. Mnoho z těchto aktérů spoléhá na vcelku jednoduché technické prostředky, třeba e-maily pro cílený phishing, kterými doručují důmyslný malware. K dosažení svých cílů neinvestují do vývoje útoků na míru ani nepoužívají cílené sociální inženýrství.

Průmyslová odvětví, na které cílí aktéři národních států



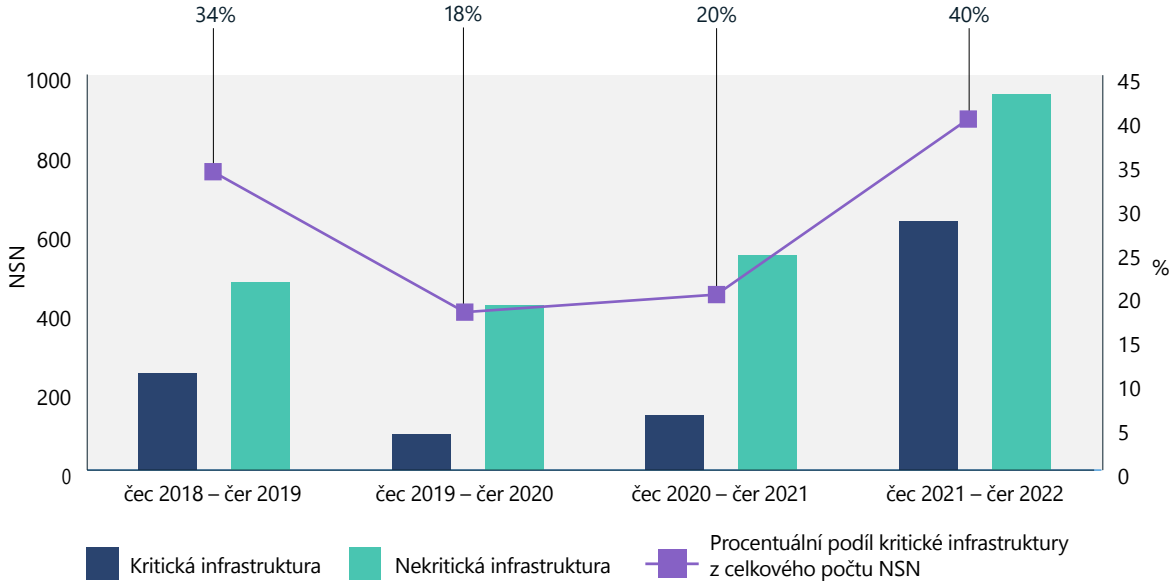
Skupiny národních států cílily na různé sektory. Ruští a íránští státní aktéři cílili na IT průmysl, který pro ně představoval způsob, jak se dostat k zákazníkům IT firem. Výzkumné skupiny, nevládní organizace (NGO), univerzity a státní úřady také zůstaly mezi běžnými cíli aktérů národních států.

Aktéři národních států mají spousty cílů, jejichž výsledkem může být zaměření na konkrétní skupiny organizací nebo jednotlivců. V minulém roce došlo k nárůstu útoků na dodavatelské řetězce, které se zaměřovaly především na IT firmy. Napadením poskytovatelů IT služeb často aktéři hrozeb zvládnou napadnout původní cíl prostřednictvím důvěrného vztahu se společností, která spravuje propojené systémy, nebo případně zahajují útoky v mnohem větším měřítku tím, že jediným útokem napadnou stovky přidružených zákazníků. Po IT sektoru jsou nejčastěji napadanými subjekty výzkumné skupiny, akademici pracující pro univerzity a státní úředníci. Tito lidé představují lákavé „měkké cíle“ špionáže, od kterých lze získat informace o geopolitických problémech.

Vyvíjející se prostředí hrozeb

pokračování

Trendy pro kritickou infrastrukturu

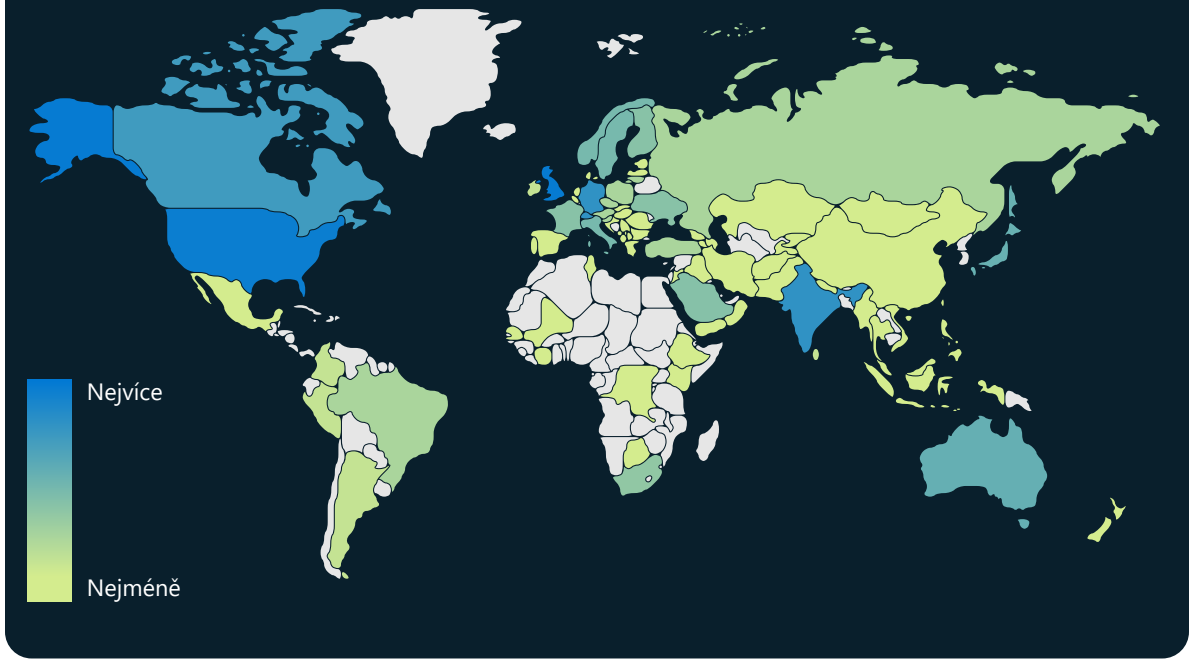


Za poslední rok skupiny národních států cílily na kritickou infrastrukturu[3] častěji. Aktéři se zaměřovali na společnosti v IT sektoru, finanční služby, dopravní systémy a komunikační infrastrukturu.

„Před invazí na Ukrajinu se státní správy domnívaly, že aby data zůstala v bezpečí, nesmí opustit hranice. Po invazi je migrace dat do cloudu a přesun mimo územní hranice součástí plánování odolnosti a zásad správného řízení."

Cristin Flynn Goodwin,
Associate General Counsel, Customer Security & Trust

Geografické cílení aktérů národních států



Kybernetické cílení skupin národních států se v tomto roce týkalo celého světa. Obzvláště silně se skupiny zaměřovaly na americké a britské podniky. Podle našich dat NSN patřily mezi jedny z nejčastěji napadaných organizací i ty v Izraeli, SAE, Kanadě, Německu, Indii, Švýcarsku a Japonsku.

Poznatky a jejich využití

1. Identifikujte a chraňte potenciální cíle s hodnotnými daty, ohrožené technologie, informace a obchodní operace, které by mohly být součástí strategických priorit skupin národních států.
2. Zajistěte ochrany cloudu, které nabídnou identifikaci a zmírnění známých i nových hrozeb pro síť ve velkém.

Dodavatelský řetězec IT jako brána k digitálnímu ekosystému

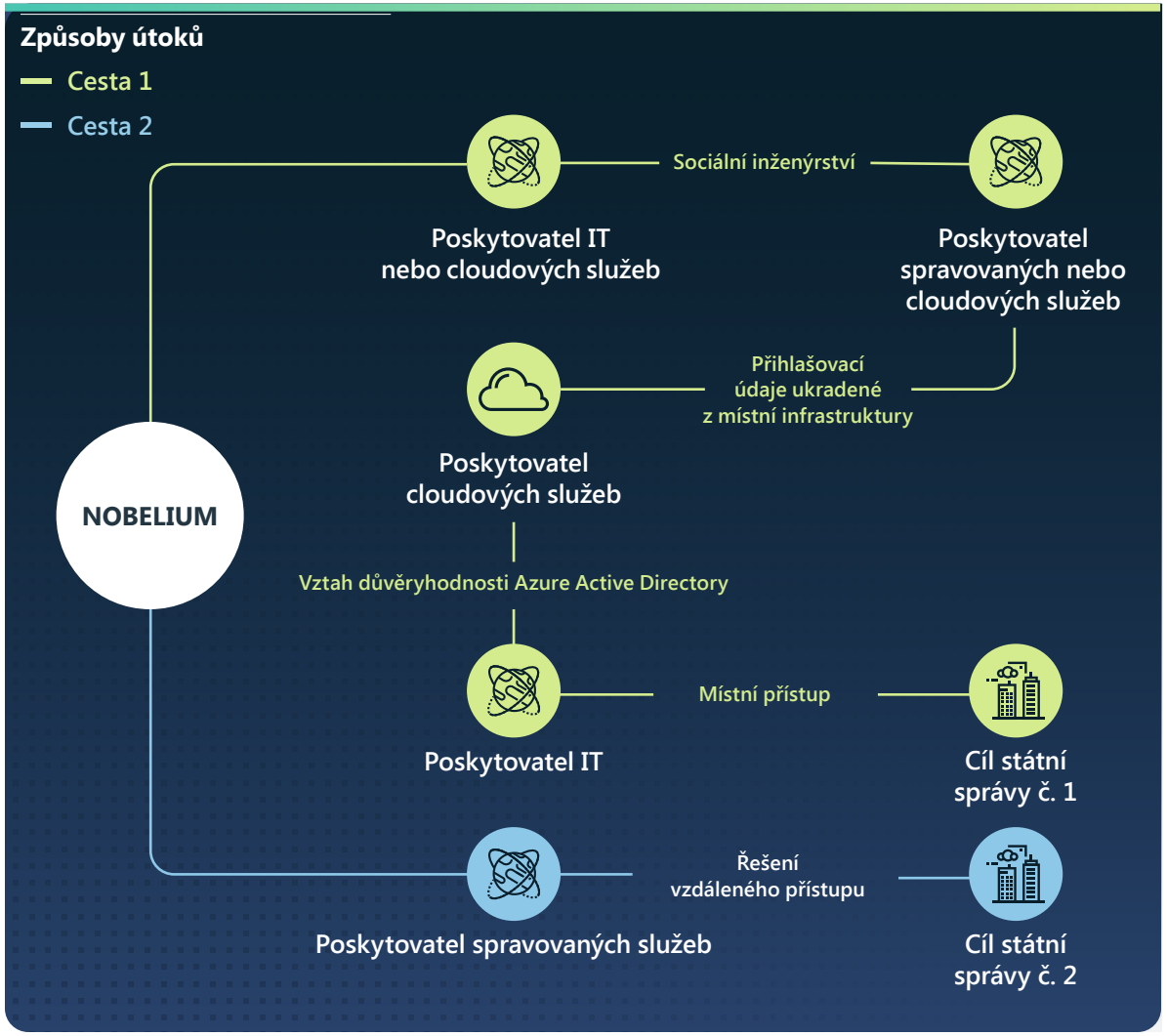
Cílení národních států na poskytovatele IT služeb může umožnit aktérům hrozeb zneužívat jiné zajímavé organizace tím, že využijí důvěry a přístupu získaného k těmto poskytovatelům dodavatelského řetězce. V posledním roce skupiny kybernetických hrozeb ze strany národních států cílily na poskytovatele IT služeb, aby mohly zaútočit na cíle třetích stran a získat přístup k napojeným klientům v sektorech státní správy, politiky a kritické infrastruktury.

Poskytovatelé IT služeb jsou lákavými přechodnými cíli, protože obsluhují stovky přímých a tisíce nepřímých klientů, kteří jsou pro zahraniční zpravodajské služby zajímaví. Pokud dojde ke zneužití, rutinní obchodní postupy a delegovaná oprávnění pro správu, která tyto firmy používají, můžou umožnit škodlivým aktérům získat přístup do sítí poskytovatele IT služeb a manipulovat s nimi, aniž by na sebe hned upozornili.

Loni se NOBELIUM pokusilo napadnout a zneužít privilegované účty u poskytovatelů cloudových řešení a jiných spravovaných služeb se záměrem získat cílený přístup především k americkým a evropským státním a politickým zákazníkům.

NOBELIUM ukázalo, že přístup, kdy je napaden jeden subjekt s cílem napadnout mnoho jiných, lze zacílit na domnělé geopolitické protivníky. V tomto uplynulém roce aktér hrozeb usiloval o průnik do systémů třetích stran i o přímé narušení citlivých organizací se sídlem v členských státech Severoatlantické aliance (NATO), kterou ruská státní správa vnímá jako existenční hrozbu. Mezi červencem 2021 a začátkem června 2022 směřovalo 48 procent oznámení zákazníkům Microsoftu na ruské aktivity, které zákazníky online služeb ohrožovaly, k firmám z IT sektoru se sídlem v členských zemích NATO. Pravděpodobně mělo jít o přechodné přístupové body. Celkově 90 procent oznámení o ruských nebezpečných aktivitách ve stejném období směřovalo k zákazníkům v členských zemích NATO, především v IT průmyslu, výzkumných skupinách, nevládních organizacích (NGO) a státních sektorech. To naznačuje, že byla využita strategie hledání několika způsobů, jak získat prvotní přístup k těmto cílům.

Došlo k posunu od zneužívání dodavatelského řetězce softwaru ke zneužívání dodavatelského řetězce IT služeb, kdy jsou cílem poskytovatelé cloudových řešení a spravovaných služeb, přes které se útočník dostává k cílovým zákazníkům.



Tento diagram znázorňuje vícevektorový přístup NOBELIA k napadení svých konečných cílů a vedlejší škody, které během útoků utrpěly jiné oběti. Kromě činností uvedených výše NOBELIUM zahájilo útok password spray a phishingové útoky na související subjekty, a dokonce i na osobní účet nejméně jednoho státního zaměstnance, který měl poskytnout další možnou cestu, kudy útočit.

Dodavatelský řetězec IT jako brána k digitálnímu ekosystému

pokračování

V průběhu roku centrum Microsoft Threat Intelligence Center (MSTIC) zaznamenalo rostoucí počet aktérů íránského státu a jeho partnerů, kteří napadají IT společnosti. V mnoha případech byli aktéři přistiženi při krádeži přihlašovacích údajů, aby získali přístup k propojeným klientům a dosáhli tak různých cílů, od získávání informací po odvetné ničivé útoky.

- V červenci a srpnu 2021 DEV-0228 napadl izraelského poskytovatele firemního softwaru, aby následně napadl propojené zákazníky v izraelských obranných, energetických a právních sektorech.[4]
- Od srpna do září 2021 Microsoft zaznamenal prudký nárůst počtu íránských státních aktérů zaměřených na IT společnosti se sídlem v Indii. Absence naléhavých geopolitických problémů, které by takovou změnu vysvětlovaly, naznačuje, že toto cílení slouží k nepřímému přístupu k dceřiným společnostem a klientům mimo Indii.
- V lednu 2022 skupina DEV-0198, pro kterou jsme vyhodnotili, že spolupracuje s íránskou státní správou, napadla izraelského poskytovatele cloudových služeb. Microsoft usuzuje, že aktér pravděpodobně využil přihlašovací údaje neoprávněně získané od poskytovatele k ověření u izraelské logistické společnosti. Centrum MSTIC zjistilo, že později ve stejném měsíci se tentýž aktér pokoušel zaútočit na tuto logistickou společnost ničivými kybernetickými útoky.
- Skupina POLONIUM z Libanonu, kterou jsme vyhodnotili jako spolupracovníka íránských státních skupin na technikách dodavatelského řetězce IT, napadla v dubnu 2022 izraelskou IT společnost s cílem získat přístup k obranným a právním organizacím v Izraeli.[5]

Uplynulý rok aktivity ukazuje, že se aktéři hrozeb, jako jsou NOBELIUM a DEV-0228, seznamují s prostředím důvěryhodných vztahů organizace lépe než organizace samy. Tato větší hrozba zdůrazňuje potřebu organizací porozumět hranicím a vstupním bodům do svých digitálních prostředků a posílit jejich zabezpečení. Podtrhuje to i důležitost důsledného monitorování stavu kybernetického zabezpečení u poskytovatelů IT služeb. Organizace by například měly implementovat vícefaktorové ověřování a zásady podmíněného přístupu, které škodlivým aktérům ztíží zachytávání privilegovaných účtů nebo šíření v síti.

Důkladné revize a audity partnerských vztahů pomáhají minimalizovat nepotřebná oprávnění mezi vaší organizací a poskytovateli a okamžitě odebrat přístup u vztahů, které nepoznáváte. Podrobnější seznámení s protokoly aktivit a prohlížení dostupné aktivity usnadňuje hledání anomálií, které můžou podnítit podrobnější prověřování.

> Cílení národních států na třetí strany jim umožňuje zneužívat citlivé organizace využíváním důvěryhodnosti a přístupu v dodavatelském řetězci.

Poznatky a jejich využití

1. Kontrolujte a auditujte vztahy se všemi poskytovateli služeb a delegované privilegované přístupy, aby bylo uděleno co nejméně nepotřebných oprávnění. Odeberte přístup všem partnerským vztahům, které nepoznáváte nebo ještě nebyly auditovány.[6]
2. Povolte protokolování a kontrolu veškeré aktivity ověřování pro infrastrukturu vzdáleného přístupu a virtuální privátní sítě (VPN). Zaměřte se na účty, které mají nakonfigurované jen jednofaktorové ověřování, abyste mohli potvrdit jejich pravost a prověřit neobvyklou aktivitu.
3. Povolte všem účtům (včetně účtů služeb) MFA a zajistěte, že se bude MFA vynucovat pro všechna vzdálená připojení.
4. K zabezpečení účtů používejte řešení bez hesel.[7]

Odkazy na další informace

- NOBELIUM cílí na delegovaná oprávnění pro správu, aby usnadnilo rozsáhlejší útoky | Microsoft Threat Intelligence Center (MSTIC)
- Íránské cílení na IT sektor na vzestupu | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Odhalování aktivity a infrastruktury skupiny POLONIUM, která cílí na izraelské organizace | Microsoft Threat Intelligence Center (MSTIC)

Rychlé zneužití chyb v zabezpečení

Organizace zlepšují stav svého kybernetického zabezpečení a aktéři národních států na to reagují hledáním nových a jedinečných taktik, jak vést útoky a vyhýbat se odhalení. Hlavní technikou je při tom identifikace a zneužívání dříve neznámých chyb v zabezpečení, kterým se říká ohrožení zabezpečení nultého dne.

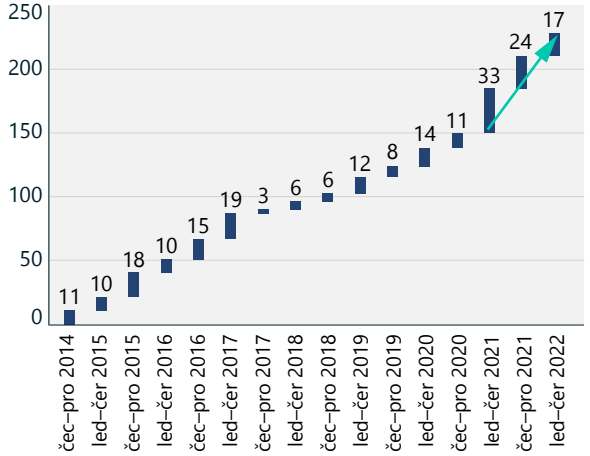
Ohrožení zabezpečení nultého dne jsou obzvláště účinný způsob, jak zahájit zneužívání. Chyby v zabezpečení můžou totiž po zveřejnění rychle začít používat i jiní aktéři z řad národních států a zločinců. Počet veřejně odhalených ohrožení zabezpečení nultého dne za poslední rok je přibližně stejný jako loni, kdy byl ze všech předchozích nejvyšší.

Aktéři kybernetických hrozeb – národní státy i zločinci – dokáží tyto chyby v zabezpečení využívat stále zdatněji. Zjistili jsme zkrácení doby mezi oznámením chyby v zabezpečení a její komoditizací. Proto je zcela nezbytné, aby organizace zneužitelná místa okamžitě opravily. Obdobně je důležité, aby organizace nebo jednotlivci, kteří odhalí nové chyby v zabezpečení, tyto chyby co nejdříve odpovědně zveřejnili nebo nahlásili příslušným dodavatelům v souladu s koordinovanými postupy pro zveřejňování chyb v zabezpečení.

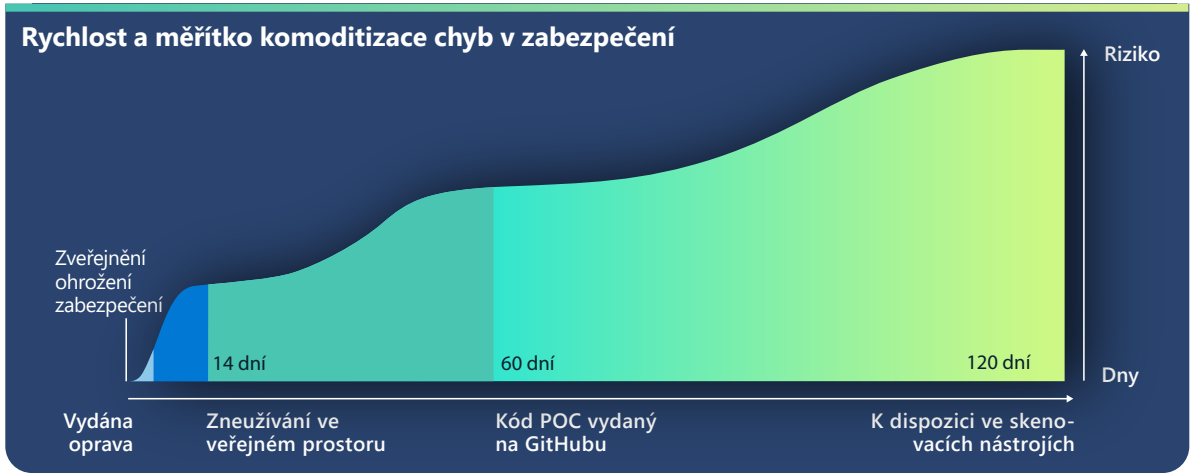
Tak se zajišťuje, že se chyby identifikují a že pro ně vzniknou včas opravy, které zákazníky ochrání před dříve neznámými hrozbami.

Mnoho organizací předpokládá, že je méně pravděpodobné, že by se staly obětí útoků zneužívajících ohrožení zabezpečení nultého dne, když je nedílnou součástí zabezpečení sítě i správa chyb v zabezpečení. Komoditizace zneužití však vede k tomu, že se chyby využívají mnohem rychleji. Zneužití nultého dne často najdou jiní aktéři, kteří umožní, aby se v krátkém časovém období hojně využívala. To představuje riziko pro neopravené systémy. I když může být obtížné zjistit, že došlo ke zneužití nultého dne, bývá snazší detekovat činnost aktérů po zneužití, a pokud je detekována ve zcela opraveném softwaru, bývá také varovným příznakem napadení.

Opravy vydané pro ohrožení zabezpečení nultého dne



Počet zveřejněných zneužití nultého dne na seznamu Běžné chyby zabezpečení a rizika (CVEs)



Průměrně trvá jen 14 dnů od zveřejnění chyby v zabezpečení, než je zneužití k dispozici široké veřejnosti. Tento diagram nabízí analýzu časových os zneužití ohrožení zabezpečení nultého dne spolu s počtem systémů ohrožených daným zneužitím a aktivních na internetu od chvíle prvního zveřejnění.

Ačkoli útoky prostřednictvím ohrožení zabezpečení nultého dne cílí spíše na určité množství organizací, často jsou zavedeny do většího ekosystému aktérů hrozeb. Tím startuje závod, kdy aktéři hrozeb chtějí zneužít chybu v zabezpečení v co největším měřítku dříve, než potenciální cíle nainstalují opravy.

Vývoj zneužití neznámých ohrožení zabezpečení pozorujeme u mnoha aktérů národních států, ale aktéři hrozeb národních států v Číně jsou obzvláště schopní hledat a vyvíjet zneužití nultého dne. V září 2021 vešel v platnost regulační předpis o vykazování chyb v zabezpečení. Je to vůbec poprvé, co státní správa vyžaduje hlášení chyb v zabezpečení, aby je státní úřad mohl zkontrolovat dříve, než budou sděleny vlastníkovi produktu nebo služby. Toto nové nařízení může umožnit některým prvkům čínské státní správy hromadit nahlášené chyby v zabezpečení s cílem použít je jako zbraň. Častější využívání nultých dnů za poslední rok mezi čínskými aktéry je pravděpodobně důsledkem prvního celého roku platnosti požadavku Číny na odhalování chyb v zabezpečení pro čínskou bezpečnostní komunitu. Je to velký krok ve zneužívání ohrožení zabezpečení nultého dne jako státní priority. Chyby v zabezpečení popsané níže byly nejdříve vyvinuty a nasazeny aktéry národních států v Číně při útocích a až pak je odhalili a rozšířili jiní aktéři v rozsáhlejším ekosystému hrozeb.

Rychlé zneužití chyb v zabezpečení

pokračování

Dokonce i organizace, které nejsou cílem útoků národních států, mají omezený čas na opravu ohrožení zabezpečení nultého dne v ohrožených systémech, než dojde ke zneužití širším ekosystémem aktérů.

Tyto příklady nově identifikovaných chyb v zabezpečení ukazují, že organizace mají průměrně 60 dní od nalezení chyby v zabezpečení, než bude online k dispozici kód pro testování konceptu (POC). Ten je často dále používán jinými aktéry. Podobně mají organizace v průměru 120 dní, než bude chyba v zabezpečení k dispozici v automatizovaných nástrojích pro skenování a zneužívání chyb, třeba v nástroji Metasploit. To pak často vede ke zneužívání v masivním měřítku. To poukazuje na to, že dokonce i organizace, které nejsou cílem aktérů hrozeb národních států, mají omezený čas na opravu ohrožení zabezpečení nultého dne v ohrožených systémech, než dojde ke zneužití chyb v širším ekosystému aktérů.

CVE-2021-35211 SolarWinds Serv-U

V červenci 2021 společnost SolarWinds vydala poradce pro zabezpečení kvůli CVE-2021-35211 s poděkováním Microsoftu za oznámení.[8] Tou dobou jsme zjistili, že aktér hrozeb DEV-0322 spolupracující s národním státem aktivně zneužíval chybu v zabezpečení produktu SolarWinds Serv-U. Náš tým RiskIQ zaznamenal mezi 15. červnem a 9. červencem 12 646 IP adres, které hostovaly verze napadených zařízení připojené k internetu.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

V září 2021 naši výzkumníci zaznamenali aktéry spřátelené s Čínou, kteří zneužívali Zoho ManageEngine u několika subjektů se sídlem v USA. Chyba v zabezpečení byla veřejně oznámena 6. září jako CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, které organizace obvykle používají ke zpracování resetů hesel.[9] Později v září tuto chybu zneužíval DEV-0322, který ji používal jako počáteční vektor, přes který získal oporu v sítích a prováděl další akce, včetně stahování přihlašovacích údajů, instalace vlastních binárních souborů a zavádění malwaru pro zachování trvalé přítomnosti. V době zveřejnění skupina RiskQ pozorovala 4011 případů těchto aktivních a k internetu připojených systémů.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Ke konci října 2021 jsme zjistili, že DEV-0322 využíval chybu v zabezpečení (CVE-2021-44077) v druhém produktu Zoho ManageEngine, ServiceDesk Plus – software pro IT help desk se správou prostředků. DEV-0322 tuto chybu v zabezpečení využil k cílení a napadení subjektů v sektorech zdravotnictví, informačních technologiích, vyššího vzdělávání a stěžejních výrobních závodů. 2. prosince Federální úřad pro vyšetřování (FBI) a úřad Cybersecurity and Infrastructure Security Agency (CISA) vydaly pro veřejnost společné upozornění o aktérech hrozeb národních států, kteří tuto chybu využívají. V době zveřejnění skupina RiskQ pozorovala 7956 případů těchto aktivních a k internetu připojených systémů.

CVE-2021-42321 Microsoft Exchange

Během soutěže Tianfu Cup, mezinárodního setkání ke kybernetické bezpečnosti a soutěže v hackování konané 16. a 17. října 2021 v čínském Čcheng-tu, bylo odhaleno zneužití nultého dne pro chybu v zabezpečení Exchange CVE-2021-42321. Výzkumníci zabezpečení v Microsoftu zjistili, že chyba v Exchangi začala být veřejně zneužívána 21. října, jen tři dny po jejím odhalení. V době zveřejnění skupina RiskQ pozorovala 61 559 případů těchto aktivních a k internetu připojených systémů. Aktivitu zneužívání jsme pozorovali ještě v listopadu 2021.

CVE-2022-26134 Confluence

Aktér s vazbami na Čínu pravděpodobně měl kód pro zneužití nultého dne v produktu Confluence (CVE-2022-26134) čtyři dny před zveřejněním chyby, které proběhlo dne 2. června. Pravděpodobně chybu využil proti subjektu se sídlem v USA. V době zveřejnění skupina RiskQ pozorovala 53 621 případů těchto ohrožených systémů Confluence na internetu.

Chyby v zabezpečení se sdílejí a zneužívají v masivním měřítku a se stále kratšími prodlevami.

Poznatky a jejich využití

1. Opravujte prioritně ohrožení zabezpečení nultého dne hned po jejich zveřejnění, nečekejte s nasazením na cyklus správy oprav.
2. Dokumentujte a inventarizujte veškeré hardwarové a softwarové prostředky podniku, abyste mohli zjistit riziko a rychle určit, kdy pracovat na opravách.

Kybernetické strategie ruských státních aktérů v době války ohrožují nejen Ukrajinu

Letos ruští státní aktéři zahajovali kybernetické operace, kterými doplňovali vojenské akce během ruské invaze na Ukrajinu. Často používali stejnou taktiku a techniky nasazované proti cílům mimo Ukrajinu. Je nezbytně nutné, aby organizace po celém světě přijaly opatření k posílení kybernetického zabezpečení před digitálními hrozbami pocházejícími od aktérů hrozeb spolupracujících s Ruskem.

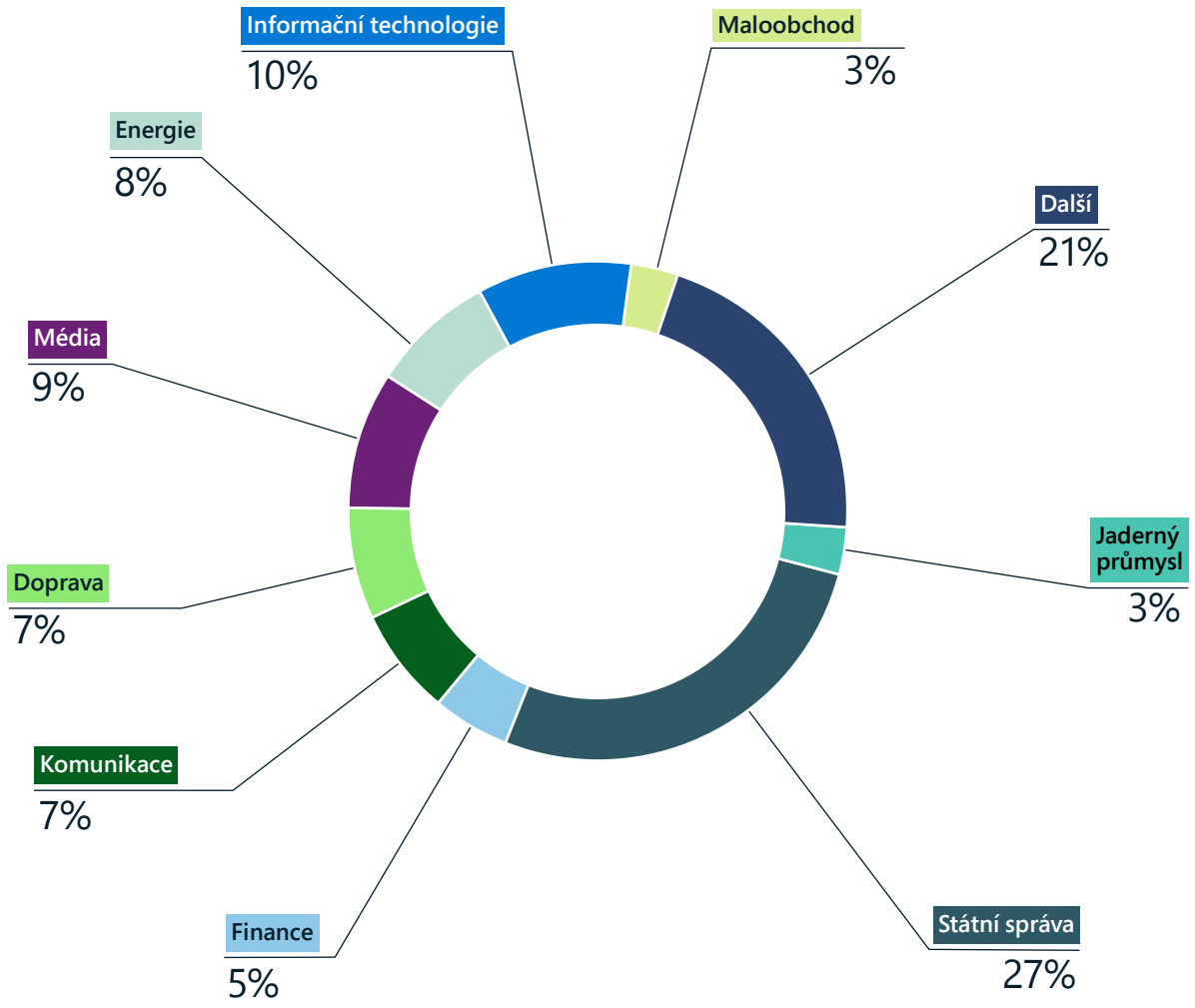
Situace na zemi se i nadále stále mění, jelikož ozbrojený konflikt přetrvává, a Ukrajina a její spojenci by měli být připraveni se bránit, pokud ruští státní kybernetičtí operátoři navýší četnost nebo intenzitu svých útoků v souladu s vojenskými cíli. Během prvních čtyř měsíců války Microsoft zjistil, že aktéři hrozeb spojení s ruskou armádou zahajují nejednu vlnu ničivých kybernetických útoků proti téměř 50 různým ukrajinským úřadům a podnikům. K mnoha dalším pak pronikali za účelem špionáže. Nebudou-li se počítat operace proti zákazníkům online služeb, 64 procent ruské nebezpečné aktivity proti známým cílům bylo v době od února do června mířeno na ukrajinské organizace.

V každé operaci ruští aktéři hrozeb použili mnohé z taktik, technik a postupů (TTP), které jsme pozorovali ještě před invazí. Probíhaly na cíle na Ukrajině i mimo ni. Tito aktéři měli za cíl zničit data a zaskočit ukrajinské státní úřady v počátečních fázích konfliktu. Od té doby se pokouší mařit přepravu vojenské a humanitární pomoci na Ukrajinu, narušovat veřejný přístup ke službám a médiím a krást informace, které mají pro Rusko dlouhodobou informační i ekonomickou hodnotu.

Cílení na přepravu ohrožuje oblast, která je pro přežití ukrajinských občanů kriticky důležitá. Podle květnového průzkumu sponzorovaného organizací UNICEF se respondenti ve válkou zasažených městských oblastech nejvíce obávali o dopravu a paliva, narušení dodávek, bezpečí a volný přístup k potravinám nebo lékařským a finančním službám.[10] V červnu krizový koordinátor OSN pro Ukrajinu řekl, že nejméně 15,7 milionu lidí na Ukrajině potřebuje rychlou humanitární pomoc a počet bude s pokračující válkou dále narůstat.[11]

Mimo Ukrajinu Microsoft detekoval v období od konce února do června ruské snahy o narušení sítí 128 organizací ve 42 zemích. Spojené státy byly hlavním cílem Ruska. Polsko, přes které prochází značná část mezinárodní vojenské a humanitární pomoci Ukrajině, bylo během tohoto období také významným cílem. I v dubnu a květnu se aktéři hrozeb napojení na ruský stát zaměřili na organizace v Pobaltí a počítačové sítě v Dánsku, Norsku, Finsku a Švédsku.

Nejčastější cílová průmyslová odvětví na Ukrajině od invaze



Federální, státní a místní vládní organizace na Ukrajině zůstaly hlavním cílem ruských státních a se státem propojených skupin hrozeb po celou dobu konfliktu. Zaměření na organizace v oblasti dopravy, energetiky, finančnictví a médií upozorňuje na riziko, které tyto kybernetické operace představují pro služby, na které se spoléhají ukrajinští občané.

Kybernetické strategie ruských státních aktérů v době války ohrožují nejen Ukrajinu

pokračování

Zaznamenali jsme nárůst podobné aktivity, která cílila na ministerstva zahraničí zemí NATO.

Ruské státní skupiny hrozeb se v posledním roce stále zajímaly o napadání kritické infrastruktury jak na Ukrajině, tak mimo ni. IRIDIUM nasadilo malware Industroyer2 při neúspěšném pokusu zanechat miliony lidí na Ukrajině bez elektřiny. Mimo Ukrajinu vedl BROM z počátku roku 2022 útoky na organizace, které se zabývají výrobou, a průmyslové řídicí systémy.

Ruští státní a se státem spolupracující aktéři tento rok směřovali kybernetické operace proti Ukrajině, jejím spojencům a dalším cílům, které mají informační hodnotu. Používali k tomu mnohé z následujících TTP:

Cílený phishing se škodlivými přílohami nebo odkazy

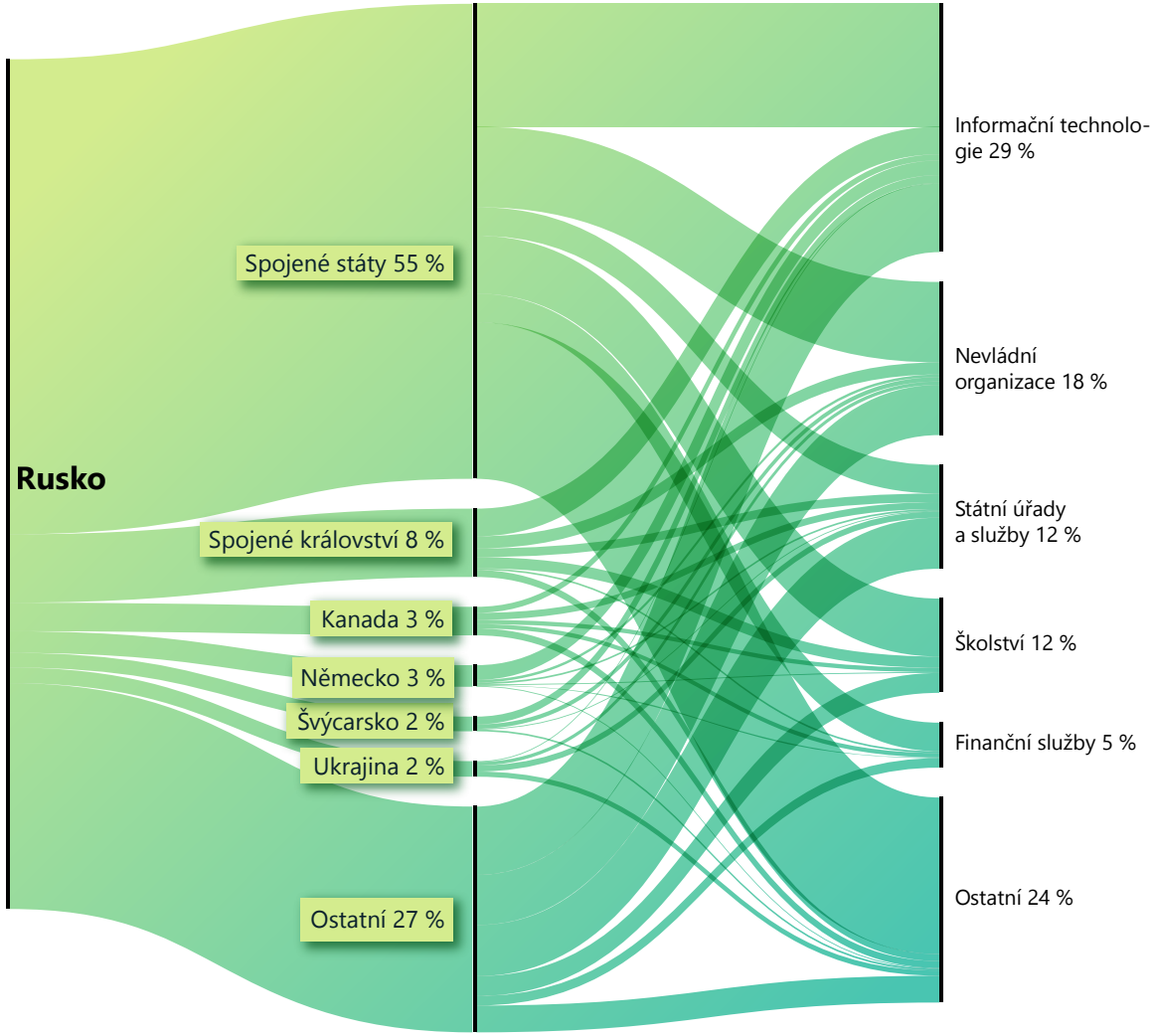
Ruský stát a skupiny spojené s Ruskem, třeba AKTINIUM, NOBELIUM, STRONCIUM, DEV-0257, SEABORGIUM a IRIDIUM používaly phishingové kampaně, pomocí kterých získávaly počáteční přístup k požadovaným účtům a sítím v organizacích na Ukrajině i mimo ni. Mnoho kampaní využívalo jako nástrahu na oběti napadené nebo falšované účty v cílových organizacích nebo ve stejném průmyslu a zajímavé motivy. NOBELIUM použilo napadené diplomatické účty, ze kterých rozesílalo phishingovou poštu maskovanou jako diplomatická komunikace zaměstnancům ministerstev zahraničí po celém světě. STRONCIUM vytvořilo falešné účty na základě veřejně dostupných názvů držitelů účtů ve výzkumných skupinách ve Spojených státech a rozesílalo phishingové zprávy, kterými získávalo přístup k účtům těchto výzkumných skupin. SEABORGIUM jako phishingovou nástrahu využívalo zprávy o konfliktu na Ukrajině, kterými získávalo přístup k účtům ve výzkumných skupinách pro mezinárodní záležitosti v severských zemích.

Zneužívání dodavatelského řetězce IT služeb k ovlivňování propojených zákazníků

V závěru roku 2021 ruští státní aktéři napadli poskytovatele IT služeb a využili získaný přístup, kterým si usnadnili neoprávněné změny webů a díky kterému mohl DEV-0586 v lednu nasadit destruktivní malware Whispergate.[12] DEV-0586 navíc napadl síť IT firmy, která vytváří systémy pro správu prostředků pro ukrajinské ministerstvo obrany a další organizace v komunikačním a dopravním odvětví. Naznačuje to, že skupina i v těchto oblastech zneužívá možnosti útoků třetích stran.

Na celém světě, ale obzvláště ve Spojených státech a v západní Evropě, NOBELIUM cílilo v letech 2021 a 2022 na poskytovatele IT služeb se záměrem získat přístup ke státním a jiným citlivým sítím (viz diskuze k ohrožením zabezpečení dodavatelského řetězce výše v této kapitole).

Rusko: Nejčastější cílové země a průmyslová odvětví



I přes silnější zaměření na ukrajinské organizace od začátku roku 2022 byly podniky se sídlem v Severní Americe a západní Evropě zákazníky online služeb, na které ruští aktéři cílili nejčastěji. Kampaň skupiny NOBELIUM vedená proti IT sektoru udělala z tohoto sektoru nejčastější cíl za poslední rok.

Kybernetické strategie ruských státních aktérů v době války ohrožují nejen Ukrajinu

pokračování

Zneužívání veřejných aplikací k získání počátečního přístupu k sítím

Nejméně od konce roku 2021 skupina STRONCIUM pracovala na vývoji a zdokonalování svých schopností zneužívat veřejné služby, třeba servery Microsoft Exchange, ke krádeži informací. STRONCIUM zneužilo neopravené servery Exchange k přístupu k ukrajinským státním účtům i organizacím napojeným na vojenský a obranný průmysl ve Spojených státech, Libanonu, Peru a Rumunsku a další státní úřady v Arménii, Bosně, Kosovu a Malajsii. DEV-0586, který je propojen s ruskou armádou, zneužil chyby v zabezpečení serveru Confluence a získal počáteční přístup ke státním a IT organizacím na Ukrajině a v dalších zemích východní Evropy.

Ruský stát a na něj napojení aktéři hrozeb používají mnoho TTP, kterými napadali pro ně zajímavé organizace v dobách války i míru.

Používání účtů a protokolů pro správu a nativních nástrojů pro zjišťování sítě a taktiku lateral movement

Microsoft zjistil, že jakmile ruští státní aktéři získali počáteční přístup do sítě, využívali legitimní účty a softwarové nástroje sloužící k základní údržbě, aby se co nejdéle vyhnuli svému odhalení. Spoléhali na napadené identity s funkcemi pro správu a platné administrativní protokoly, nástroje a metody, s jejichž pomocí aplikovali v sítích taktiku lateral movement, aniž by okamžitě přitáhli pozornost automatických nástrojů pro monitorování a ochranu sítě.

Základní kybernetická hygiena a zavedení detekce a reakce u koncových bodů dokáží zmírnit negativní dopad těchto typů operací v dobách míru i během válečných konfliktů.

Nepředvídatelnost aktuálního konfliktu vyžaduje, aby organizace po celém světě zaváděly opatření, kterými posílí kybernetické zabezpečení před digitálními hrozbami ze strany ruských státních a s Ruskem spolupracujících aktérů hrozeb.

Poznatky a jejich využití

1. Minimalizujte krádeže přihlašovacích údajů a zneužívání účtů tak, že pomocí nástrojů MFA na ochranu identity a vynucováním přístupu s nejnižší možnou úrovní oprávnění ochráníte identity svých uživatelů a zabezpečíte nejcitlivější a privilegované účty a systémy.
2. Instalujte aktualizace, aby všechny systémy měly co nejdříve tu nejvyšší úroveň ochrany a byly stále aktuální.
3. Nasazujte v celé organizaci řešení antimalwaru, detekce koncových bodů a ochrany identity. Kombinace bezpečnostních řešení pro důkladnou obranu a vyškolených a schopných zaměstnanců může organizaci umožnit identifikovat a detekovat hrozby, které by měly vliv na její podnikání, a předcházet jim.
4. Zálohujte kritické systémy a povolte protokolování, aby bylo možné prověřovat případnou zjištěnou nebo oznámenou hrozbu prostředí a zotavit se z ní. Důrazně se doporučuje zavést plán reakce na incidenty.

Odkazy na další informace

- Obrana Ukrajiny: První ponaučení z kybernetické války | Microsoft On the Issues
- Hybridní válka na Ukrajině | Microsoft On the Issues
- Aktivita kybernetických hrozeb na Ukrajině: analýza a prostředky | Microsoft Security Response Center (MSRC)
- Narušování kybernetických útoků cílených na Ukrajinu | Microsoft On the Issues
- Malwarové útoky cílené na ukrajinskou státní správu | Microsoft On the Issues
- MagicWeb: Trik skupiny NOBELIUM, jak se po napadení ověřit jako kdokoli | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

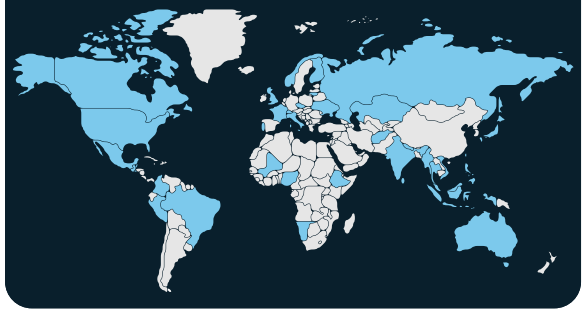
Čína rozšiřuje globální cíle pro svou konkurenční výhodu

V dnešním složitém geopolitickém prostředí se čínští státní a s Čínou spolupracující aktéři hrozeb, kteří provádějí kybernetické operace, často zaměřují na podporu strategických vojenských, ekonomických a zahraničních cílů země v souladu se snahou Číny získat konkurenční výhodu. V posledním roce Microsoft zpozoroval rozsáhlou aktivitu čínských hrozeb, které cílí na země po celém světě.

Od poloviny roku 2021 Čína jedná s cílem zajistit ekonomickou a finanční stabilitu v době největších nárůstů případů covidu-19 za poslední dva roky.[13] Čína nadále upravuje svá stanoviska ke geopolitickým událostem, například snahou najít rovnováhu mezi svým „neomezeným" partnerstvím s Ruskem[14] a zachováním svého postavení ve světovém dění.[15] Kromě toho postoj Číny proti Spojeným státům a jejich spojencům ve vztahu k Tchaj-wanu[16] a Jihočínskému moři nadále narušuje zahraniční vztahy s mnoha zeměmi.[17]

Čínské státní a se státem spolupracující skupiny hrozeb posílily své cílení na menší země po celém světě a zaměřují se na Jihovýchodní Asii, kde chtějí ve všech oblastech získat konkurenční výhodu.

Země, na které cílí čínské státní a se státem spolupracující skupiny

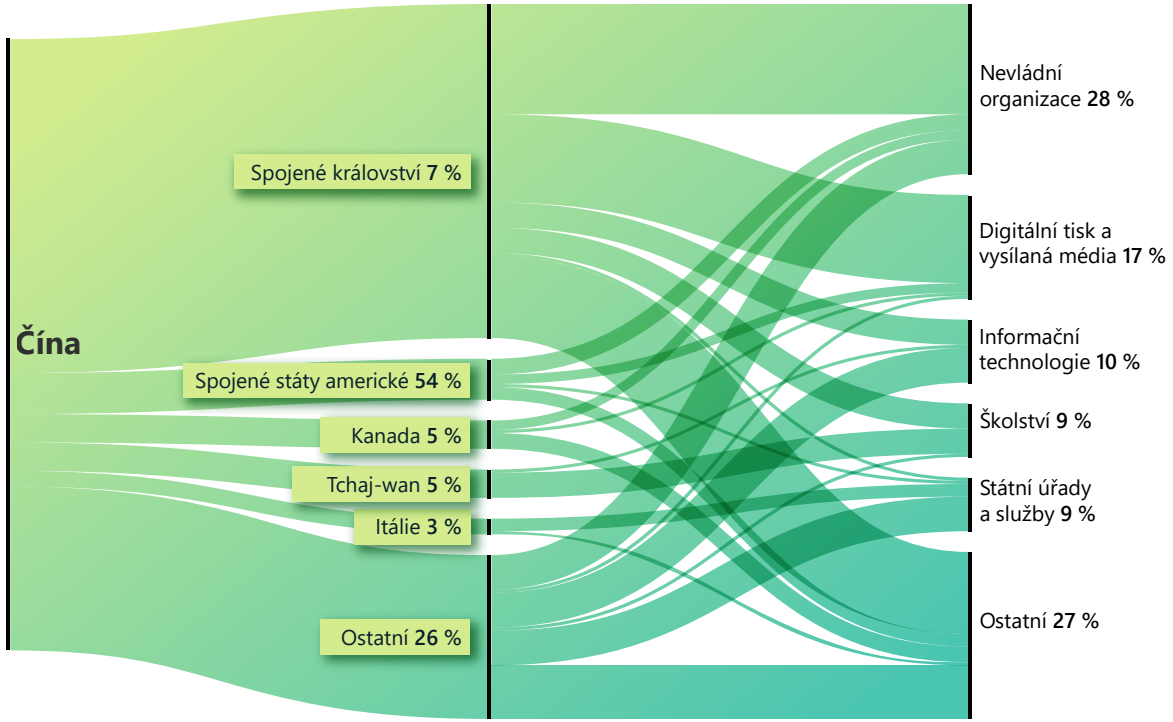


Čína navíc i nadále rozšiřuje svůj ekonomických vliv po celém světě prostřednictvím dříve zavedené tzv. Nové Hedvábné stezky (NHS), kterou se pokouší obnovit komplexní investiční rámec s EU[18] a vyjednat nové smlouvy o místním obchodu v 15 zemích asijsko-pacifického regionu. Tomuto rámci se říká Regionální ekonomické partnerství.[19] Z pozorovaných kybernetických operací a rozsahu cílových subjektů Microsoft usuzuje, že Čína bude i nadále využívat kybernetické shromažďování jako nástroj, kterým podpoří své strategické politické, vojenské a ekonomické cíle.

Kybernetické cílení pravděpodobně podporuje ekonomické a vojenské zájmy.

Microsoft pozoroval čínské státní a se státem spolupracující skupiny hrozeb, které ve velkém měřítku cílily na menší země po celém světě. To naznačuje, že Čína pravděpodobně využívá kybernetickou špionáž jako součást svého globálního ekonomického a vojenského vlivu.

Čína: Nejčastější cílové země a průmyslová odvětví



Sektory výzkumných skupin a nevládních organizací, médií, IT, státní správy a školství byly mezi nejčastějšími cílovými sektory pro skupiny hrozeb v Číně, pravděpodobně se záměrem zajistit trvalé shromažďování informací a průzkum.

Mezi cíle patřily například země v Africe, Karibské oblasti, na Středním východě, v Oceánii a Jižní Asii. Na země v Jihovýchodní Asii a na tichomořských ostrovech se Čína zaměřovala obzvlášť.

V souladu s čínskou strategií NHS se skupiny hrozeb v Číně zaměřují na subjekty v Afghánistánu, Kazachstánu, Mauriciu, Namibii a Trinidadu a Tobagu.[20] Například Republika Trinidad a Tobago byla první karibská země, která v roce 2018 podpořila strategii NHS Číny, a Čína ji považuje za důležitého oblastního partnera. Od roku 2021 podnikal NIKL trvalé síťové operace, kterými cílil na Trinidad a Tobago. Například v březnu 2022 NIKL prováděl průzkumné aktivity zaměřené na státní úřad, pravděpodobně za účelem shromažďování informací.

Čína rozšiřuje globální cíle pro svou konkurenční výhodu

pokračování

Dále Microsoft pozoroval, jak čínské státní a se státem spolupracující skupiny hrozeb zaměřují své síťové operace proti subjektům v Jihovýchodní Asii a rozšiřují se do tichomořských ostrovních zemí v souladu s tím, jak Čína mění své vojenské a ekonomické priority s ohledem na obnovený zájem Spojených států o tuto oblast. V lednu 2022 Microsoft sledoval RADIUM, jak cílí na energetickou společnost a státní úřad zabývající se energetikou ve Vietnamu a na státní úřad v Indonésii. Aktivity skupiny RADIUM byly pravděpodobně v souladu se strategickými cíli Číny v Jihočínském moři.[21] Ke konci února a na začátku března skupina GALLIUM napadla více než 100 účtů napojených na přední mezivládní organizace (IGO) v oblasti Jihovýchodní Asie. GALLIUM zacílilo na IGO v oblasti ve stejnou chvíli, kdy byla oznámena plánovaná schůze mezi Spojenými státy a místními lídry. Aktéři skupiny GALLIUM pravděpodobně dostali za úkol monitorovat před událostí komunikaci a shromáždit informace.

Tam, kde Čína rozšiřuje svůj vliv v tichomořských ostrovních zemích, lze pozorovat aktivity čínských skupin hrozeb. V dubnu Čína a Šalamounovy ostrovy podepsaly dohodu o zabezpečení s cílem „udržet mír a bezpečí". Tato dohoda by mohla Číně umožnit nasazovat ozbrojené policejní a vojenské složky na Šalamounovy ostrovy.[22] V květnu Čína uspořádala druhý summit ministrů zahraničních věcí z ostrovních států v čínském tichomoří na Fidži a navrhla rozšířit „komplexní strategické partnerství", které podpoří politické, kulturní, společenské, bezpečnostní a klimatické zájmy a boj s pandemií.[23] Přibližně ve stejnou dobu v květnu Microsoft identifikoval malware skupiny GADOLINIUM v systémech státní správy Šalamounových ostrovů. RADIUM také provozovalo škodlivý kód na systémech telekomunikační společnosti v Papui-Nové Guineji. Usuzujeme, že tyto aktivity sloužily pravděpodobně ke shromažďování informací, které podpoří celkovou místní strategii Číny.

Microsoft narušuje operace skupiny NIKL, je však vytrvalá.

V prosinci 2021 tým Digital Crimes Unit (DCU) v Microsoftu zaslal soudu US District Court v Eastern District of Virginia žádost o oprávnění zajistit 42 domén řídicích center (C2) ovládaných skupinou NIKL. Tyto domény C2 byly využívány při operacích proti státním správám, diplomatickým subjektům a nevládním organizacím ve Střední a Jižní Americe, karibské oblasti, Evropě a Severní Americe od září 2019.[24] Tyto operace skupině NIKL zajistily dlouhodobý přístup k několika subjektům a od konce roku 2019 umožnily průběžně exfiltrovat data některých obětí.

Čína i nadále navazuje dvoustranné ekonomické vztahy s dalšími zeměmi, často v dohodách souvisejícími s NHS, a její globální vliv dále poroste. Usuzujeme, že čínští státní a se státem spolupracující aktéři budou hledat cíle v oblastech státní správy, diplomacie a nevládních organizací, aby získali nové poznatky, pravděpodobně pro ekonomickou špionáž nebo tradiční cíle shromažďování informací. Od narušení Microsoftem se NIKL zaměřil na několik státních úřadů, pravděpodobně za účelem získat zpět ztracený přístup. Mezi koncem března a květnem 2022 NIKL opět napadl nejméně pět státních úřadů po celém světě. To naznačuje, že skupina měla k těmto subjektům další vstupní body nebo znovu získala přístup prostřednictvím nových domén C2. Vytrvalost skupiny NIKL v opakovaném napadání stejných státních úřadů po celém světě ukazuje na důležitost této úlohy na vysoké úrovni.

Čína zaujímá pevnější postoj k zahraniční politice. Usuzujeme, že kybernetická ekonomická špionáž a shromažďování dat budou i nadále pokračovat.

Poznatky a jejich využití

1. Posilte kybernetickou obranu a aktivně tak zmírněte kybernetické hrozby. Vytrvalost čínských aktérů hrozeb vyžaduje, aby organizace včas identifikovaly a detekovaly možná narušení, chránily před nimi a reagovaly na ně.
2. Aktéři hrozeb zneužívají plánované úlohy[25], což je pro ně běžný způsob, jak se vyhýbat odhalení a zajistit si trvalý přístup. Zaveďte ve svém prostředí dodatečnou ochranu, aby bylo chráněno před touto běžně používanou technikou.[26]
3. I nadále pozorujeme, že se jako počáteční vektory do cílových sítí používají webová prostředí.[27] Organizace by měly posílit zabezpečení svých systémů před útoky přes webová prostředí, která můžou útočníkům zajistit přístup a možnost vzdáleně spouštět příkazy.[28]

Odkazy na další informace

- NIKL cílí na státní organizace v Latinské Americe a Evropě | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Ochrana lidí před nedávnými kybernetickými útoky | Microsoft On the Issues

Írán je po převodu moci stále agresivnější

Microsoft zaznamenal, že íránské státní skupiny a spolupracující aktéři začali častěji a ve větším měřítku kyberneticky útočit na Izrael, rozšiřovat ransomwarové útoky za hranice místních protivníků na oběti v USA a EU a cílit na exponovanou kritickou infrastrukturu v USA, kde si chtějí přinejmenším zajistit výchozí pozici pro případné ničivé kybernetické útoky.

Po převzetí prezidentského úřadu novým prezidentem začala narůstat kybernetická agresivita íránských státních aktérů. V létě 2021 vystřídal neoblomný prezident Ebráhím Raísí umírněného prezidenta Hasana Rúháního. Na rozdíl od Raísího, který je pobočníkem nejvyššího představitele a blízký spojenec Íránské revoluční gardy (IRGC), ochota bývalého prezidenta Rúháního k diplomatickým jednáním často způsobovala konflikt s nejvyšším představitelem a vrchními vůdci IRGC.[29] Ostré postoje Raísího správy zřejmě podpořily ochotu íránských aktérů podnikat smělejší akce proti Izraeli a Západu, obzvláště Spojeným státům, a to navzdory pokračujícím diplomatickým jednáním, která mají za cíl obnovit dohodu o jaderných zbraních v Íránu.

Častější a rozsáhlejší kybernetické útoky Íránu proti Izraeli

Během týdnů, kdy Raísí dokončil sestavování své skupiny pro zahraniční politiku,[30] íránští státní aktéři začali provádět své destruktivní kybernetické útoky proti Izraeli častěji než v předchozím roce. Tyto ransomwarové útoky a útoky typu hack-and-leak probíhaly v několikatýdenních intervalech od září. Měly souvislost s nejméně třemi aktéry spolupracujícími s Íránem, což naznačuje, že útoky mohly být součástí celonárodní odvetné kampaně proti Izraeli. Nejméně v jednom případě Microsoft vyhodnotil, že ransomwarový útok proti izraelské organizaci na konci roku 2021 měl za úkol zakrýt útok, který měl vymazat data. Analýza malwaru provedená Microsoftem zjistila, že ransomware nasazený oběti byl naprogramován tak, aby po zašifrování spustil malware schopný vymazat data.

V roce 2022 začaly íránské kybernetické útoky mířit na více cílů a používat více technik. V únoru se DEV-0198 pokusil provést ničivý útok na izraelskou kritickou infrastrukturu. Microsoft dále usuzuje, že aktér spolupracující s Íránem byl s největší pravděpodobností zodpovědný za sofistikovaný kybernetický útok, který v Izraeli v červnu spustil nouzové raketové sirény, pravděpodobně pomocí softwaru upravujícího zvuk přes IP sítě.

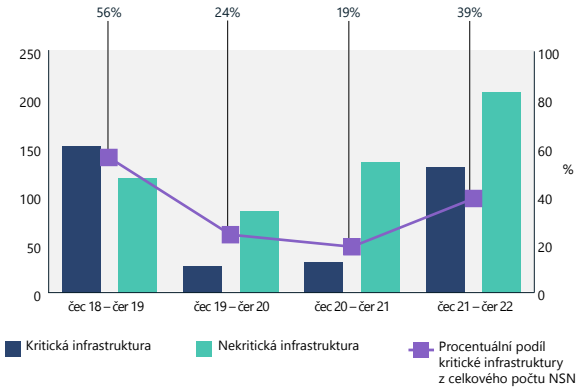
Íránská hrozba pro kritickou infrastrukturu v USA a Izraeli se v průběhu roku zvyšovala

Íránští státní aktéři, které Microsoft vyhodnotil jako partnery IRGC (FOSFOR a DEV-0198), cílili od konce roku 2021 do poloviny roku 2022 na veřejnou americkou a izraelskou kritickou infrastrukturu. Pravděpodobným cílem bylo nabídnout Teheránu možnosti, jak provést odvetnou akci proti stejným odvětvím, z jejichž narušení v Íránu vysocí úředníci IRGC viní Spojené státy a Izrael.[31] Usuzujeme, že tato aktivita souvisí s prohlášeními generála IRGC Golamrezy Džalálího, nejvyššího představitele íránské organizace pro pasivní obranu, z konce října 2021, který opakoval slova jiných vlivných osob v daném režimu, že Spojené státy a Izrael prováděly kybernetické útoky na íránské přístavy, železnice a čerpací stanice.[32] Džalálí toto obvinění pronesl podruhé připravenými poznámkami v inscenované páteční modlitbě na pódiu s obrázkem, na kterém řízená střela dopadá na slova „USA". Naznačuje to, že jeho vrchní představitelé sdíleli jeho názor.[33]

FOSFOR začal v říjnu 2021 ve velké míře hledat v amerických organizacích neopravené chyby v zabezpečení Fortinet a ProxyShell. Po napadení byly tyto neopravené systémy využity k zahajování ransomwarových útoků, v několika případech proti kritické infrastruktuře ve Spojených státech a dalších západních zemích. Šlo o první potvrzené případy ransomwarových útoků souvisejících s íránským státem mimo Střední východ. V návaznosti na kybernetický útok proti íránským čerpacím stanicím, ke kterému došlo na konci října, Microsoft pozoroval prudký nárůst ransomwarových útoků proti americkým společnostem. To naznačuje možnou korelaci.

Ve stejnou dobu FOSFOR přešel na přímé cílení, často prostřednictvím cíleného phishingu, na známé americké společnosti pro kritickou infrastrukturu, včetně velkých námořních přístavů a vstupních letišť, přepravních systémů, společností dodavatelů veřejných služeb a ropných a plynárenských společností. Toto cílení, při kterém byl často využíván cílený phishing, trvalo až do poloviny roku 2022. Cíle přesně odpovídaly odvětvím, na která v Íránu podle Teheránu útočily Spojené státy a Izrael, a pravděpodobně poskytly Íránu možnosti odvety. Napadení téměř totožných cílů by otevřelo příležitost odradit v budoucnu od podobných útoků a zároveň se pokusit vyhnout eskalaci stanovením příčiny útoku, aniž by to znamenalo přiznání viny.

Oživení cílení Íránu na infrastrukturu



Na nejvyšší úrovně se cílení Íránu na kritickou infrastrukturu dostalo od konce roku 2018 do začátku roku 2019. Při určování, zda společnost odpovídá kritériu kritické infrastruktury, jsme využili směrnici US Presidential Policy Directive 21 (PPD-21). (červenec 2021 – červen 2022)

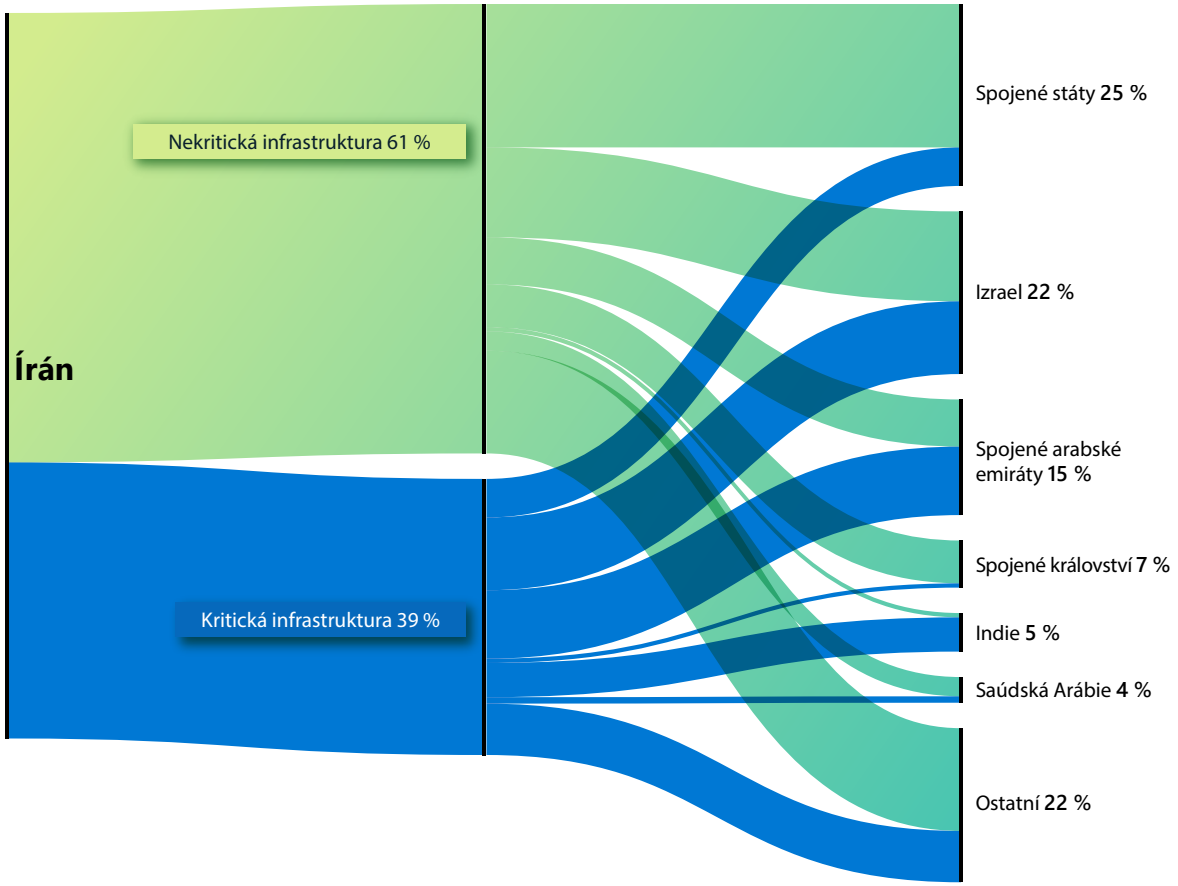
Írán je po převodu moci stále agresivnější

pokračování

V Izraeli DEV-0198 cílil na izraelské železnice, logistické společnosti, poskytovatele softwaru logistických společností a společnosti z oblasti paliv se zaměřením na čerpací stanice. Na začátku roku 2022 tato skupina provedla narušující útoky na síť velké izraelské logistické společnosti, čímž ji donutila vypnout své počítače a ukončit některé činnosti, aby útok zastavila. V jiném případě jsme skupinu pozorovali při pokusu získat přístup do sítě velkého izraelského přepravce prostřednictvím ukradených nebo opakovaně použitých přihlašovacích údajů. Mezitím jiný íránský aktér, DEV-0343, jehož cílení na společnosti z oblasti obrany, námořní přepravy a satelitního snímkování naznačuje propojení na IRGC, napadl ze začátku roku 2021 účty izraelských subjektů zabývajících se dopravou a provozem přístavů.

Íránské skupiny hrozeb pravděpodobně i nadále zůstávají hrozbou pro přepravní a energetické společnosti v USA a Izraeli, obzvláště ve chvíli, kdy ustávají diplomatická jednání o obnovení dohody o jaderných zbraních s Íránem a Washington, Tel Aviv a Teherán hledají jiné, agresivní způsoby, jak si vynutit ústupky.

Cílení Íránu na kritickou infrastrukturu podle země



K cílení Íránu na kritickou infrastrukturu docházelo nejčastěji proti organizacím v Izraeli, Emirátech a USA.

Íránští aktéři pravděpodobně i v nadcházejícím roce zůstanou hrozbou pro přepravní a energetické společnosti v USA a Izraeli.

Íránské skupiny rozšířily ransomwarové útoky za hranice místních protivníků a míří na exponované cíle americké a izraelské kritické infrastruktury.

Poznatky a jejich využití

1. Zlepšete celkovou kybernetickou hygienu organizace tím, že zavedete řešení bez hesel, třeba MFA, a vynutíte jejich používání pro všechna vzdálená připojení, aby se zmírnily dopady případného napadení přihlašovacích údajů.
2. Vyhodnocujte pravost všech příchozích e-mailů a ujistěte se, že adresa odesílatele je pravá.
3. Včas a často opravujte chyby.[34]
4. Provádějte kontroly a audity všech partnerských vztahů s poskytovateli služeb, abyste minimalizovali množství nepotřebných udělených oprávnění mezi organizací a jejími poskytovateli. Microsoft doporučuje okamžitě odebrat přístup všem partnerským vztahům, které nepoznáváte nebo ještě nebyly auditovány.[35]

Odkazy na další informace

- Íránské cílení na IT sektor na vzestupu | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- DEV-0343 ve spojení s Íránem cílí na obranná a námořní odvětví a GIS | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Skupina z Libanonu s napojením na Írán cílí na Izrael

Microsoft monitoruje aktivity kybernetických hrozeb bez ohledu na platformu, cílovou oběť nebo geografickou oblast. Po celém světě si udržujeme přehled a aktivně vyhledáváme hrozby, abychom mohli pro naše zákazníky vytvářet lepší systémy detekce.

Ačkoli hrozby z Ruska, Číny, Íránu a Severní Korey představují většinu námi pozorovaných aktivit aktérů národních států, sledujeme také hrozby ze strany členských států NATO a demokratických zemí a komunikujeme s nimi o nich. Loni jsme popisovali aktivitu aktéra z Turecka (KŘEMÍK) a z Vietnamu (BISMUT). Tento rok uvádíme podrobnosti o skupině z Libanonu, kterou jsme již dříve odhalili veřejnosti.[36]

Microsoft odhalil dříve nezaznamenanou libanonskou skupinu, o které se střední jistotou usuzujeme, že jednala ve spolupráci s aktéry spřátelenými s íránským Ministerstvem informací a bezpečnosti (MOIS). Taková spolupráce nebo řízení z Teheránu by byla v souladu se zjištěními z konce roku 2020, že státní správa Íránu využívá ke kybernetickým operacím třetí strany, pravděpodobně jako prostředek, jak Íránu zajistit důvěryhodnější možnost události popírat.

Při pozorované aktivitě skupina POLONIUM hodlala napadnout nebo napadla mezi únorem a květnem 2022 více než dvě desítky organizací z Izraele a jedno IGO s operacemi v Libanonu dříve, než Microsoft aktivitu skupiny narušil a zveřejnil. Téměř polovina těchto izraelských organizací byla součástí obranného průmyslu Izraele nebo měla vazby na izraelské obranné společnosti, což naznačuje, že skupina měla podobný zájem na shromažďování informací nebo přímý boj s Izraelem jako Írán.[37]

Posuzovaná napojení skupiny POLONIUM na skupiny MOIS se zakládají na společných pozorovaných obětech a využitých nástrojích a technikách.

- Společné oběti: Íránská státní skupina napojená na íránský MOIS, kterou Microsoft sleduje jako RTUŤ, dříve napadla několik obětí skupiny POLONIUM, což naznačuje sbližování požadavků mise nebo možné „předávání“ obětí mezi skupinami.
- Společné nástroje a techniky: Podobně jako POLONIUM skupina MSTIC pozorovala DEV-0588 (známého také jako CopyKittens), jak běžně používá AirVPN, a DEV-0133 (známého také jako Lyceum[38]) využívajícího OneDrive pro C2 a exfiltraci. Obdobně jako íránští státní aktéři POLONIUM využilo poskytovatele cloudových služeb k napadení izraelské letecké společnosti a právnické firmy.[39]

POLONIUM nasadilo řadu vlastních škodlivých prostředků pomocí cloudových služeb pro C2 a exfiltraci dat – především OneDrive a Dropbox. Často pro cíle vytvářelo jedinečné aplikace OneDrive, pravděpodobně jako způsob, jak se vyhnout odhalení.

K červnu 2022 Microsoft pozastavil více než 20 aplikací OneDrive vytvořených skupinou POLONIUM, zaslal oznámení napadeným organizacím a nasadil řadu aktualizací bezpečnostních informací, které uvrhly nástroje vyvinuté skupinou POLONIUM do karantény.

Microsoft úspěšně zjistil a ukončil zneužívání OneDrivu jako C2 skupinou POLONIUM.

Poznatky a jejich využití

1. Aktualizujte antivirové nástroje[40] a ujistěte se, že je zapnutá ochrana cloudu,[41] abyste mohli detekovat související indikátory.
2. U zákazníků, kteří mají vztahy s poskytovateli služeb, zajistěte kontrolu a audit všech vztahů s partnery, aby se minimalizoval počet zbytečně udělených oprávnění mezi vaší organizací a jejími poskytovateli.[42] Okamžitě odeberte přístup u každého partnerského vztahu, který nepoznáváte nebo nebyl auditován.

Odkazy na další informace

- Odhalování aktivity a infrastruktury skupiny POLONIUM, která cílí na izraelské organizace | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- RTUŤ využívá chyby v zabezpečení Log4j 2 v neopravených systémech k cílení na izraelské organizace | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Severokorejské dovednosti v kyberprostoru využité k dosažení tří hlavních cílů režimu

Priority Severní Korey v kyberprostoru za poslední rok odrážely globální priority stanovené státní správou. Kim Čong-un zdůraznil tři priority: vybudovat obranné schopnosti, posílit problémovou ekonomiku země a zajistit domácí stabilitu v několika klíčových oblastech.[43] Činnosti severokorejských státních aktérů zřetelně ukazují, že k dosažení těchto cílů je využíván kyberprostor.

Severokorejští státní aktéři používali různé strategie, kterými se pokoušeli proniknout do leteckých společností po celém světě.

Severokorejské státní skupiny hrozeb, především CER a ZINEK, využívaly různé strategie, kterými se pokoušely proniknout do sítí obranných a leteckých společností po celém světě. Když pak v první polovině roku 2022 Severní Korea započala své dosud nejagresivnější období testování raket, využila kybernetické špionáže, aby pomohla severokorejským výzkumníkům získat výhodu při vývoji vlastních obranných systémů a protiopatření v reakci na pokroky svých protivníků.

Zjistili jsme, skupina KOPERNICIUM cílí na různé společnosti z oblasti kryptoměn po celém světě, často úspěšně, a pomáhá tak zlepšit neuspokojivý stav severokorejské ekonomiky. Ačkoli nedokážeme potvrdit, jestli se skupině podařilo po napadení exfiltrovat peníze, zaznamenali jsme, jak KOPERNICIUM nakazilo desítky počítačů rozesláním škodlivých dokumentů, které se maskovaly jako návrhy jiných kryptoměnových společností.

Dále pak skupina, kterou Microsoft sleduje jako DEV-0215, usilovala o zajištění stability a sounáležitosti v Severní Koreji cílením na zpravodajské organizace, které informují o severokorejských záležitostech. Tyto kanály mají zdroje jak v Severní Koreji, tak v komunitách zběhů, které Pchjongjang považuje za existenční hrozbu. K tomu skupina pracovala na přístupu do sítí korejsky mluvících křesťanských skupin, které v Severní Koreji nebývají schvalovány a aktivně spolupracují se severokorejskými zběhy.

Cílení na obranné a letecké společnosti

Severokorejští státní aktéři vedení skupinami CER a ZINEK vynaložili značné úsilí na vývoj strategií cílených na průnik do obranných a leteckých společností. CER opakovaně zkoumal jihokorejské virtuální privátní sítě (VPN) stahováním klientů a hledáním slabých stránek. Dále stahoval běžné aplikace, které používají jihokorejští armádní a vládní klienti, zřejmě se záměrem najít chyby v zabezpečení. Skupina důsledně sledovala aktuální události a psala nové falešné dokumenty zabývající se významnými tématy. Ty pak sloužily jako nástraha, kterou se skupina snažila přimět cíle kliknout na spustitelné soubory a odkazy svého malwaru.

ZINEK i CER používaly v kampaních sociální média a sociální inženýrství. ZINEK byl obzvláště zdatný ve vytváření falešných profilů na LinkedInu a dalších webech profesních sociálních sítí, kde jeho operátoři vystupovali jako náboráři velkých obranných a leteckých společností. Pomocí těchto profilů rozesílal potenciálním obětem přímými zprávami na sociálních médiích nebo e-mailem odkazy nebo škodlivé souborové přílohy.

Kromě zaměstnanců korporací CER ve velkém cílil i na členy jihokorejské armády. Zvláštní zájem měl jak o jihokorejské vojenské akademie, tak členy armády, kteří v akademickém prostředí pracují.

Cílení na kryptoměny pro vyvážení ztrát

V roce 2016 OSN uvalilo na Severní Koreu sankce, které způsobily další pokles severokorejské ekonomiky. K němu dále přispěly přírodní katastrofy jako povodně[44] a sucho[45], ale i téměř úplné uzavření hranic od vypuknutí pandemie covidu-19 na začátku roku 2020.[46] I když začátkem roku 2022 Severní Korea na nějakou dobu otevřela své hranice, aby mohla obchodovat s Čínou, brzy byly zase uzavřeny.[47] V polovině května Severní Korea ohlásila svůj první případ covidu-19.[48] Následně podobně jako Čína zavedla strategii nulového covidu, při které v rámci boje s virem hromadně uzavírala města. To mělo opět nepříznivý vliv na už tak křehkou ekonomiku.

Severokorejská státní skupina KOPERNICIUM se pokusila ztrátu příjmů zmírnit kradením peněz, obvykle ve formě kryptoměn, od jakékoli společnosti, do jejichž sítí dokázala proniknout. Byli jsme svědky desítek napadených počítačů, které patřily kryptoměnovým společnostem ve Spojených státech, Kanadě, Evropě a po celé Asii. KOPERNICIUM dokonce napadlo počítače ve vlastnictví kryptoměnových společností u nejsilnějšího spojence Severní Korey, Číny, a to jak na pevnině, tak v Hongkongu. Pro svůj prvotní průzkum a přístup k cílům se skupina velmi spoléhala na sociální média. Aktéři si vytvářeli profily, které předstíraly, že jsou vývojáři nebo vysoce postavení zaměstnanci firem z oblasti kryptoměn. Následně navázali vztahy s lidmi v oboru, a jakmile si získali důvěru, posílali škodlivé odkazy nebo soubory.

Severokorejské dovednosti v kyberprostoru využité k dosažení tří hlavních cílů režimu

pokračování

Skupina související se skupinou PLUTONIUM vyvíjí a nasazuje ransomware

Skupina aktérů, kteří pocházejí ze Severní Korey a Microsoft je sleduje jako DEV-0530, začala v červnu 2021 vyvíjet a používat při útocích ransomware. Tato skupina, která si říká H0lyGh0st, využila ve svých kampaních stejnojmenný škodlivý ransomwarový program a už v září 2021 úspěšně napadla malé firmy v několika zemích.

Microsoft usoudil, že DEV-0530 měl vazby na jinou severokorejskou skupinu sledovanou jako PLUTONIUM, která je známá také jako DarkSeoul nebo Andariel. I když je používání ransomwaru H0lyGh0st v kampaních jedinečné pro DEV-0530, skupina MSTIC pozorovala komunikaci mezi těmito dvěma skupinami i skutečnost, že DEV-0530 používá nástroje vytvořené výhradně ve skupině PLUTONIUM.

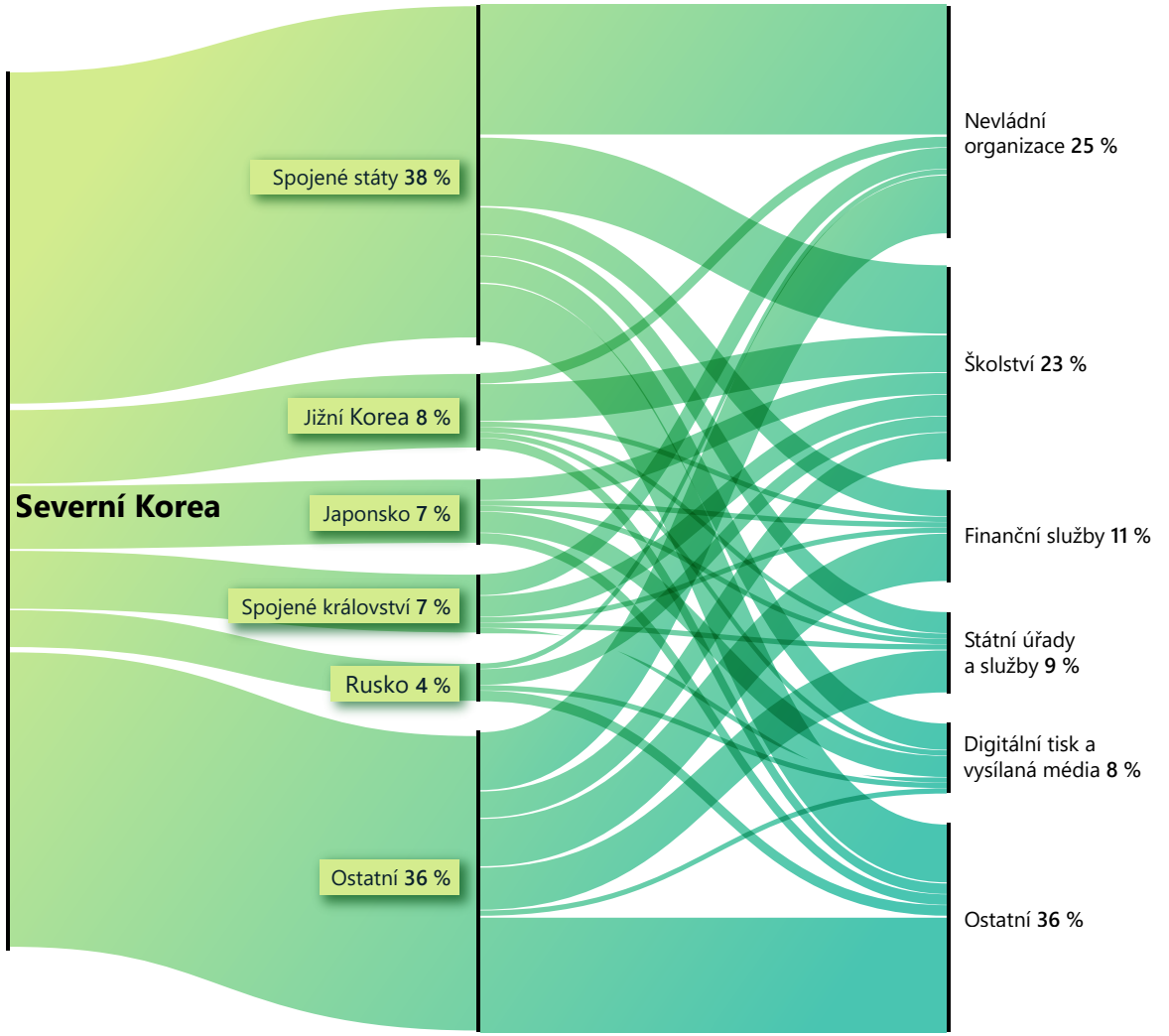
Není jisté, jestli je aktivita DEV-0530 sponzorována státní správou. Je sice možné, že ransomwarové útoky byly státní správou objednány ze stejného důvodu, z jakého sponzoruje krádeže od kryptoměnových společností, stejně tak je ale možné, že aktéři z DEV-0530 pracují nezávisle, aby si vydělali peníze pro sebe. Pokud jde o severokorejské hackery, kteří pracují nezávisle, vysvětlovalo by to, proč jejich aktivita nebyla tak rozsáhlá jako státní správou sponzorované krádeže u kryptoměnových společností.

Cílení na severokorejské zpravodajské kanály, zběhy, náboženské skupiny a humanitární organizace

Loni se nejvyšší vůdce Kim Čong-un veřejně zaměřoval více na domácí bezpečnost a sounáležitost než na řízené střely a jaderné zbraně. V souvislosti s tímto zaneprázdněním domácími problémy se nejméně dvě severokorejské státní skupiny zaměřily na aspekty, které by režim považoval za domácí hrozby.

První byla skupina, kterou Microsoft sleduje jako DEV-0215 a která cílí na mediální organizace, jež pozorně sledují severokorejské zpravodajství. Jedním z pravděpodobných důvodů tohoto cílení je, že tyto mediální kanály získávají své zprávy od severokorejských zběhů, čínských občanů, kteří se Severní Koreou úzce spolupracují, a dokonce i od některých severokorejských občanů, kteří stále žijí v zemi. Ke komunikaci s okolním světem využívají nejrůznější způsoby. Severokorejská státní správa tyto skupiny, a obzvláště pak občany žijící v Severní Koreji, kteří by byli považováni za zrádce a špehy, vnímá jako existenční hrozbu. DEV-0215 se pravděpodobně pokoušel identifikovat zdroje těchto kanálů, aby mohl případně zastavit možné úniky informací.

Severní Korea: Hlavní cílové země a průmyslová odvětví



Severní Korea vnímá jako své hlavní nepřátele Spojené státy, Jižní Koreu a Japonsko. I když je Rusko dlouhodobým spojencem, severokorejští aktéři hrozeb cílí na ruské výzkumné skupiny, akademiky a diplomaty, od kterých chce získat informace o ruském pohledu na světové události.

Severokorejské dovednosti v kyberprostoru využité k dosažení tří hlavních cílů režimu

pokračování

Microsoft našel důkaz o tom, že DEV-0215 cílil na korejsky mluvící křesťanské komunity. Evangelicko-křesťanské korejské církve mají tendenci se kriticky vyjadřovat o státních správách v Severní i Jižní Koreji, které dávají přednost jednáním se Severní Koreou. U těchto církví je pravděpodobné, že umožní zběhům uniknout ze země, a některé se zapojují do humanitárních činností v Severní Koreji. Severní Korea je vnímá jako hrozbu, protože tyto křesťanské skupiny často hrají důležitou roli při útěku zběhů, i když během pandemie jejich počet klesl téměř k nule.[49] DEV-0215 vygeneroval falešné dokumenty o křesťanských konferencích pro korejsky mluvící občany, kterými se snaží nalákat cílovou skupinu a zjistit, kdo pomáhá úniky organizovat.

Státní skupina OSMIUM projevila v průběhu roku stálý zájem o mezinárodní humanitární organizace, včetně těch, které v minulosti pomáhaly Severní Koreji. Severní Korea sice obecně odmítala nabídky pomoci ze zahraničí, obzvlášť od vypuknutí covidu-19,[50] je však možné, že využití nabídek pomoci zvažuje. Obává se ale důsledků, které by vstup zahraničních humanitárních pracovníků do země měl pro bezpečnost. Je možné, že Severní Korea proniká do sítí humanitárních organizací po celém světě, aby zjistila, jestli takovou pomoc do své země pustit.

Poznatky a jejich využití

1. Severokorejští státní aktéři jsou zkušení, vytrvalí a kreativní, ale organizace se jim můžou bránit.
2. Nejúspěšnější útoky lze zastavit základní kybernetickou hygienou, například dvojúrovňovým ověřováním nebo neotevíráním příloh od neznámých jednotlivců ve virtuálním prostředí.

Odkazy na další informace

- Severokorejský aktér hrozeb cílí na malé a střední firmy ransomwarem H0lyGh0st | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Mezi odborníky na Severní Koreu probíhá už dlouho diskuze, jestli je severokorejská státní správa při svých veřejných prohlášeních upřímná, nebo jestli se jedná jen o pózy. Souhra kybernetických útoků s oznámenými prioritami Severní Korey utvrzuje domnění, že Severní Korea myslí svá slova k veřejnosti o svých cílech vážně.

Kybernetičtí žoldnéři ohrožují stabilitu kyberprostoru

Existuje rostoucí odvětví privátních společností, které vyvíjejí a prodávají nástroje, techniky a služby, s nimiž jejich klienti – často státní správy – pronikají do sítí, počítačů, telefonů a zařízení připojených k internetu. Tyto subjekty jsou přínosem pro aktéry národních států a často ohrožují disidenty, obránce lidských práv, novináře, obhájce občanské společnosti a další soukromé občany. Těmto subjektům říkáme kybernetičtí žoldnéři nebo škodliví aktéři ze soukromého sektoru.

Svět, ve kterém soukromé společnosti vytvářejí a prodávají kybernetické zbraně, je pro zákazníky, firmy všech velikostí a státní správy nebezpečnější. Tyto útočné nástroje je možné použít způsoby, které nejsou v souladu s normami a hodnotami řádné správy a demokracie. Microsoft se domnívá, že ochrana lidských práv je základní povinností, kterou bereme velmi vážně. Proto po celém světě bojujeme proti sledování jako službě.

Microsoft usoudil, že určití státní aktéři v demokratických i autoritativních režimech využívají externí vývoj nebo používají technologii pro sledování jako službu. Takto se vyhýbají odpovědnosti a dohledu a zároveň získávají možnosti, které by bylo obtížné vyvinout svépomocí.

> Tyto kybernetické zbraně nabízejí národním státům možnosti sledování, které by nemohly vyvinout samy.

Trh, na kterém operují kybernetičtí žoldnéři, je neprůhledný. I přesto nadále pozorujeme, jak si tyto skupiny zajišťují sledování jako službu zneužíváním chyb nultého dne nebo i neinteraktivním zneužíváním, které nevyžaduje žádnou spolupráci oběti.

Nedávno Microsoft oznámil evropského škodlivého aktéra ze soukromého sektoru, kterému říkáme KNOTWEED. Je to PSOA z Rakouska s názvem DSIRF. Nejedna zpráva spojovala tuto společnost s vývojem a pokusem o prodej sady malwarových nástrojů jménem Subzero.[51] Mezi oběťmi se nacházejí právnické firmy, banky a strategické poradenské společnosti v zemích jako Rakousko, Spojené království a Panama.[52]

Jelikož už tyto možnosti útočného sledování nejsou vysoce utajovanými možnostmi vytvářenými obrannými a zpravodajskými úřady, ale spíše komerční produkty nyní prodávané společnostem a jednotlivcům, musí jakýkoli režim regulace kybernetických zbraní představovat více než jen řízení exportu. Dopad těchto kybernetických zbraní může být zničující.

Když kybernetický žoldnéř zneužije chybu v zabezpečení produktu nebo služby, ohrožuje celý výpočetní ekosystém. Jakmile dojde ke zveřejnění chyb v zabezpečení, začne společnostem běžet čas, za který musí vydat ochranu, než přijdou rozsáhlé útoky (viz naše dřívější diskuze o zneužívání chyb v zabezpečení). Toto je nebezpečný a obtížný cyklus jak pro dodavatele softwaru (kteří musí účelně vyvíjet opravy), tak pro uživatele produktů (ti musí okamžitě opravy zavádět).

Jako zakládající člen sdružení Cybersecurity Tech Accord[53] – předního spojenectví, které spojuje více než 150 technologických společností – se Microsoft zavázal neúčastnit se útočných operací online. Za tímto závazkem a naší odpovědností v oblasti lidských práv si stojíme. Zapojili jsme se do technického narušování a právních problémů, abychom zdůraznili nepříznivé dopady způsobené službami poskytovanými kybernetickými žoldnéři, a budeme nadále chránit své zákazníky proti zjištěnému zneužívání.

> Kybernetičtí žoldnéři vytvářejí a nabízejí mnoho různých technik a možností sledování jako služby, které jsou technologicky propracované a široce dostupné, včetně pokročilého malwaru.

Poznatky a jejich využití ve státních správách

1. Implementujte požadavky na transparentnost a dohled pro sledování jako službu, obzvláště v zásobování, včetně zákazu těchto škodlivých aktérů, jak to zajistilo americké ministerstvo obchodu uváděním společností na seznamu Entity List.
2. Zaveďte pro bývalé zaměstnance v tomto odvětví omezení platná i po skončení pracovního poměru.
3. Snažte se implementovat povinnosti KYC (Know Your Customer) a motivovat společnosti, aby dodržovaly své závazky v oblasti lidských práv.

Odkazy na další informace

- Rozplétání skupiny KNOTWEED: Evropský škodlivý aktér ze soukromého sektoru, který zneužívá chyby nultého dne | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Pokračování v boji proti kybernetickým zbraním v soukromém sektoru | Microsoft On the Issues

Zavedení norem kybernetické bezpečnosti pro mír a bezpečí v kyberprostoru

Nutně potřebujeme konzistentní celosvětový rámec, který upřednostňuje lidská práva a chrání lidi před bezohledným chováním států na internetu. Nikde to není více zřetelné než na právě probíhající válce na Ukrajině. Kromě globálního strategického úsilí můžou státní správy hned učinit opatření, která budou mít příznivý dopad.

Před pěti lety Microsoft vyzýval k ustanovení „Digitální Ženevské úmluvy", která by rozšířila odpovědnost a povinnosti v různých odvětvích s cílem chránit mír a bezpečnost online. Z kyberprostoru se začala stávat samostatná a nestálá doména konfliktu a soupeření mezi státy a útoky jsou stále častější, a to i v dobách míru.

I dnes je stále zřejmé, že takový rámec je nezbytný – dosvědčují to ruské kybernetické útoky na Ukrajinu provedené v rámci ruské invaze. Tato válka vytvořila novou přední linii, která se značně liší od toho, co známe z dřívějších dob.

Má-li být kyberprostor stabilní, bude to vyžadovat posílení a přepracování globálních řídicích institucí tak, aby tento úkol zvládly. Kyberprostor se zásadně liší od ostatních domén – nemá hranice, je umělý a udržuje jej z velké části soukromý průmysl. To znamená, že je nutné požádat technologický průmysl, aby přijal větší odpovědnost jak za zabezpečení produktů a služeb, tak za širší digitální ekosystém. I když na všech frontách došlo k významnému pokroku, výzvy jsou výrazně větší.

Musíme zdvojnásobit společné úsilí při ochraně bezpečí kyberprostoru. Nemůžeme považovat práva a svobodu, kterou už od online prostředí očekáváme, za samozřejmé. Zatímco my se snažíme tyto problémy řešit, škodliví aktéři plánují, jak a kde znovu udeří pomocí umělé inteligence a jak při tom využijí dezinformace. Zároveň hledají způsoby, jak podkopat vznikající oblast metavesmíru. Ochránci lidských práv, technologický průmysl a státní správy, které respektují lidská práva, musí spolupracovat na společně uznávané vizi bezpečného a zabezpečeného online světa. Cesta před námi je dlouhá, ale státní správy už teď můžou něco udělat pro lepší ekosystém kybernetického zabezpečení:

- Uplatňovat normy, zákony a důsledky, když se zjistí zdroj. Jedním z hlavních zlepšení za posledních pět let je rychlost a koordinace, s jakými státní správy určují zdroje kybernetických útoků. Kromě pouhého určení a slovního odsouzení musí taková vyjádření zdůraznit, které mezinárodní zákony nebo normy byly porušeny a jaký důsledek to bude mít. Díky tomu bude zřetelnější, jaká jsou v dané věci očekávání na mezinárodní úrovni.
- Vyjasnit v online prostoru interpretaci mezinárodních zákonů. Ačkoli státní správy souhlasí, že mezinárodní právo platí i online, zůstává nejasné, jak jej uplatňovat na konkrétní případy. Obzvláště relevantní je to s ohledem na důsledky ukrajinské invaze. Státní správy můžou významně přispět k nastavení očekávání, prevenci nedorozumění a budování důvěry tím, že stanoví, jak rozumí svým povinnostem s ohledem na mezinárodní právo.
- Konzultovat s jiným zúčastněnými stranami. Mezinárodní fóra nadále objevují nejlepší způsoby, jak usnadnit robustní začleňování většího množství zúčastněných stran, a státní správy můžou podporovat fundovaný dialog konzultací s komunitami s mnoha účastníky, obzvláště s technologickým průmyslem. Měly by se snažit zajistit, že v dialogu budou moct promluvit i ti, kteří mají nedocenitelné zkušenosti.
- Utvořit stálé uskupení, které bude podporovat odpovědné chování států v kyberprostoru. Činnost mezinárodních diplomatických fór, která podpoří odpovědné chování států online, nebyla nikdy důležitější. Existuje zřetelná potřeba trvalého mechanismu v OSN, který by se zabýval kyberprostorem jako sférou konfliktu.
- Definovat nové normy pro vyvíjející se hrozby. Kybernetické hrozby se neustále vyvíjejí stejně jako inovace v technologiích. I když by měly být mezinárodní normy technologicky neutrální, bude nutné je aktualizovat a upravovat podle změn v prostředí hrozeb a způsobu, jakým používáme technologie. I v dnešní době pozorujeme mezery ve stávajícím mezinárodním rámci, který je zneužíván. Státy by se měly zavázat, že budou výslovně chránit hlavní procesy, které stojí za digitálním ekosystémem a v současné době nejsou chráněny. Jedním takovým je proces aktualizace softwaru. Konkrétní oblasti by si navíc zasloužily i další ochranu. Jak jsme například zjistili během pandemie, stěžejní jsou normy pro ochranu zdraví.

Aktérů národních států i útoků je stále více a jsou důmyslnější, čímž vzniká neudržitelná situace.

Je zapotřebí co nejdříve něco udělat. Existují věci, které má v moci státní správa a které okamžitě vylepší ekosystém kybernetické bezpečnosti. Patří mezi ně implementace uznávaných norem a pravidel pro chování států v kyberprostoru a spolupráce se širší komunitou s mnoha účastníky na řešení odhalovaných nedostatků.

Nadnárodní instituce musí být přepracovány tak, aby se mohly postavit naléhavému problému kybernetických útoků národních států.

Odkazy na další informace

- Chvíle k zamyšlení: Potřeba silné a globální reakce na kybernetické zabezpečení | Microsoft On the Issues
- Kybernetické útoky zaměřené na zdravotní péči musí přestat | Microsoft On the Issues
- Další kapitola kybernetické diplomacie v Organizaci spojených národů přichází | Microsoft On the Issues

Poznámky na závěr

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. Kritická infrastruktura v této kapitole je definována podle směrnice Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (z února 2013).
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

Pokračování poznámek na závěr

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. Zejména jde o opravy chyb v zabezpečení ProxyShell v serverech Exchange (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 a CVE-2021-27065, CVE-2021-34473). Nezapomeňte opravit chyby v zabezpečení i na zařízeních Fortinet s SSL VPN a FortiOS.
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/; Andre Meister, We unveil the state Trojan „Subzero" from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Jak je uvedeno na našem technickém blogu, identifikace cílů v zemi nutně neznamená, že zákazník DSIRF sídlí ve stejné zemi, neboť mezinárodní cílení není ničím neobvyklým.
53. Domovská stránka | Cybersecurity Tech Accord (cybertechaccord.org)

Zařízení a infrastruktura

Se zrychlováním digitální transformace je zabezpečení digitální infrastruktury důležitější než kdy jindy.

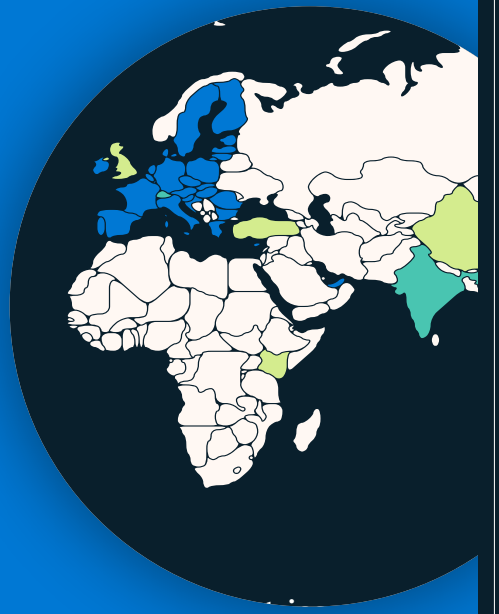
Přehled

zařízení a infrastraktury

Pandemie spolu s rychlým zaváděním nejrůznějších zařízení připojených k internetu, které tvoří součást stále rychlejší digitální transformace, značně rozšířily potenciální oblast útoku v digitálním světě.

Toho kyberzločinci a národní státy rychle využívají. I když je zabezpečení IT hardwaru a softwaru v posledních letech důkladnější, zabezpečení zařízení Internetu věcí (IoT) a provozní technologie (OT) se tak rychle nevyvíjí. Aktéři hrozeb tato zařízení zneužívají k zajištění přístupu do sítí a přípravě taktiky lateral movement, získání výchozího bodu v dodavatelském řetězci nebo k narušení operací OT v cílové organizaci.

Státní správy po celém světě začínají chránit kritickou infrastrukturu posílením zabezpečení IoT a OT.

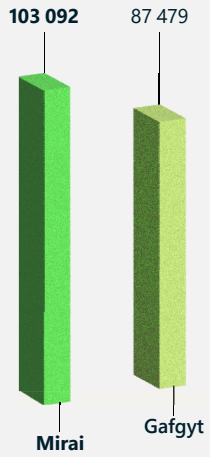


Více se dozvíte na str. 59

Pro široké přijetí je zapotřebí stanovit globálně konzistentní a interoperabilní zásady zabezpečení.

Více se dozvíte na str. 59

Malware jako služba teď představuje rozsáhlé operace proti exponovaným zařízením IoT a OT jak v infrastruktuře a veřejných službách, tak ve firemních sítích.



Více se dozvíte na str. 63

Útoky na zařízení pro vzdálenou správu jsou na vzestupu. V květnu 2022 jich bylo zaznamenáno více než 100 milionů, což je za poslední rok pětinásobný nárůst.

Více se dozvíte na str. 62

Útočníci stále častěji využívají chyb v zabezpečení firmwaru zařízení IoT, pomocí kterých pronikají do firemních sítí a zahajují ničivé útoky.

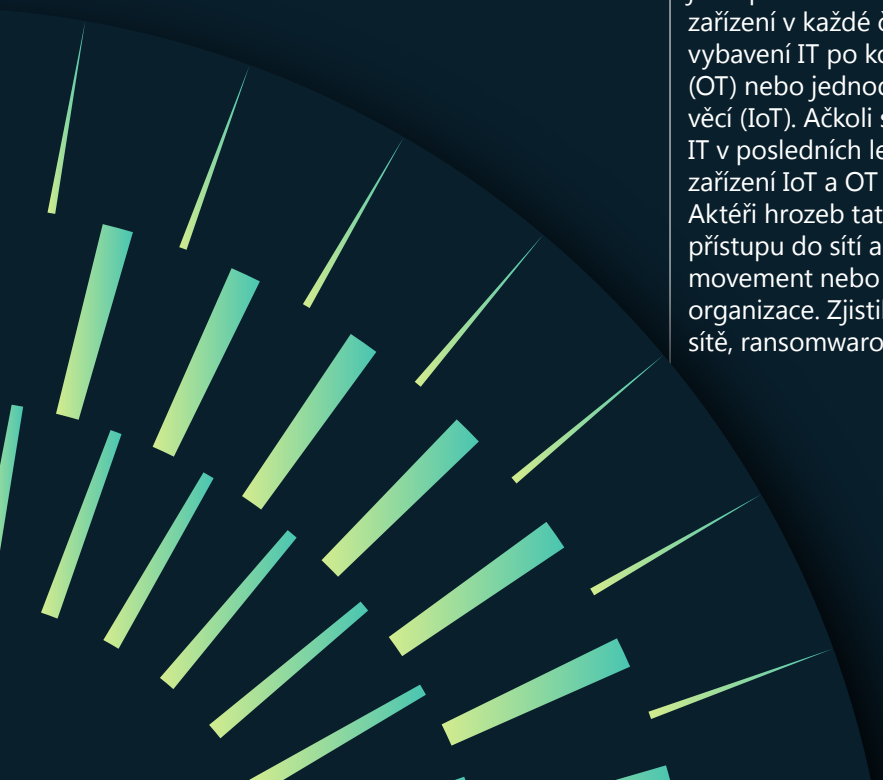
Více se dozvíte na str. 65

32 % z analyzovaných imagí firmwaru obsahovalo alespoň 10 známých kritických zranitelností.

Více se dozvíte na str. 66

Úvod

Zrychlující digitální transformace zvýšila riziko kybernetického zabezpečení kritické infrastruktury a kyberneticko-fyzických systémů.



Za posledních několik let se v digitálním světě udály nevídané změny. Organizace mění své postupy, aby využily pokroky ve výpočetních schopnostech v inteligentním cloudu i na inteligentních hraničních zařízeních. V důsledku pandemie, která si vyžádala digitalizaci subjektů bojujících o přežití, a kvůli rychlosti, s jakou odvětví na celém světě zavádějí k internetu připojená zařízení, se exponenciálně rozšiřuje potenciální oblast útoku digitálního světa.

Tato prudká migrace proběhla tak rychle, že s ní komunita zabývající se zabezpečením nedokázala udržet krok. V posledním roce jsme pozorovali hrozby, které zneužívají zařízení v každé části organizace, od tradičního vybavení IT po kontrolery provozní technologie (OT) nebo jednoduché senzory Internetu věcí (IoT). Ačkoli se zabezpečení vybavení IT v posledních letech zlepšilo, zabezpečení zařízení IoT a OT se tak rychle nevyvíjelo. Aktéři hrozeb tato zařízení zneužívají k zajištění přístupu do sítí a přípravě taktiky lateral movement nebo k narušení operací OT organizace. Zjistili jsme útoky na elektrické sítě, ransomwarové útoky narušující operace OT, směrovače IoT zneužívané k zajištění trvalé přítomnosti a útoky zaměřené na chyby v zabezpečení ve firmwaru.

Zatímco výskyt chyb v zabezpečení IoT a OT představuje problém pro všechny organizace, zvýšenému riziku čelí i kritická infrastruktura, protože aktéři hrozeb zjistili, že vyřazením kritických služeb se dá získat silná vyjednávací pozice. V roce 2021 proběhl ransomwarový útok na společnost Colonial Pipeline, který ukázal, jak zločinci dokáží narušit kritickou službu a zvýšit tím pravděpodobnost, že bude zaplaceno výkupné. A kybernetické útoky Ruska proti Ukrajině ukazují, že některé národní státy vnímají kybernetické útoky na kritickou infrastrukturu jako přípustnou sabotáž na podporu vojenských cílů.

V dálce je však vidět naděje. Tvůrci zásad a obránci sítí podnikají činnosti, které mají zlepšit kybernetické zabezpečení kritické infrastruktury, včetně zařízení IoT a OT, na která se spoléhá. Tvůrci zásad urychlují vývoj zákonů a regulačních předpisů, aby vybudovali veřejnou důvěru v kybernetické zabezpečení kritické infrastruktury a zařízení.

Microsoft spolupracuje se státními správami po celém světě, aby této příležitosti využil k posílení kybernetického zabezpečí. Vítáme další posily. Obáváme se však, že nekonzistentní, účelové nebo komplexní požadavky by mohly mít neočekávané účinky, například v některých případech zhoršení úrovně zabezpečení v důsledku přesměrování omezených bezpečnostních zdrojů na dodržování předpisů s nejednou duplicitní certifikací.

Z hlediska bezpečnostních operací musí obránci sítí přistupovat ke zlepšení stavu zabezpečení IoT a OT organizace z různých úhlů. Jedním z nich je implementace nepřetržitého monitorování zařízení IoT a OT. Dalším je tzv. „posun doleva" – tedy požadavek a implementace lepších technik kybernetického zabezpečení pro samotná zařízení IoT a OTA. Třetím přístupem je implementace řešení monitorování zabezpečení, které bude aktivní v sítích IT i OT. Tento holistický přístup má významnou výhodu v tom, že rozšiřuje kritické procesy organizace, například „odstraňování sil" mezi OT a IT. To pak zase organizaci umožňuje zajistit si lepší stav zabezpečení a při tom plnit cíle firmy.

Michal Braverman-Blumenstyk
Corporate Vice President, Chief Technology Officer, Cloud and AI Security

Státní správy činí kroky k lepšímu zabezpečení a odolnosti kritické infrastruktury

Státní správy po celém světě vyvíjejí a vylepšují zásady řízení rizik kybernetického zabezpečení kritické infrastruktury. Mnoho z nich také zavádí zásady ke zlepšení zabezpečení zařízení IoT a OT. Rostoucí globální vlna politických iniciativ vytváří ohromnou příležitost zlepšit kybernetické zabezpečení, ale představuje i výzvu pro zúčastněné strany v celém ekosystému.

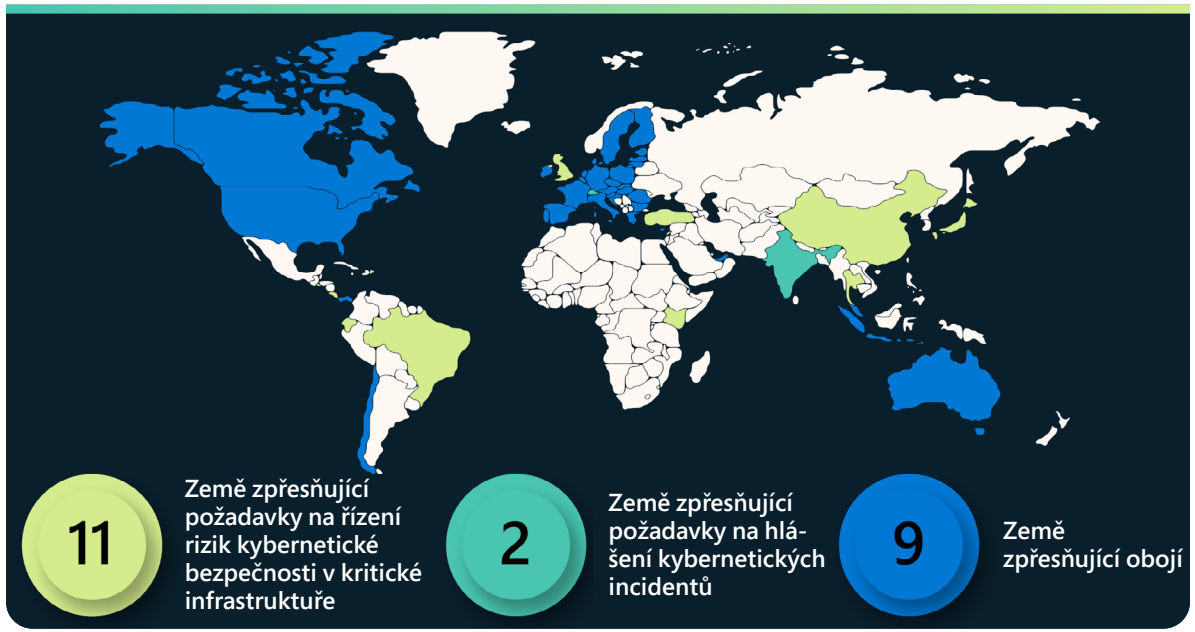
Vývoj holistické vize řízení kybernetických rizik pro kritickou infrastrukturu je nezbytně důležitý, ale složitý, obzvláště s ohledem na míru propojení mezi technologiemi a globálními dodavateli, škálu používaných technologií a souvisejících rizik a potřebu investovat do krátkodobých i dlouhodobých strategií. Vhodně vymezené zásady, které podporují iterativní zdokonalování a vylepšení a podporují globální interoperabilitu mezi odvětvími, můžou pomoct při řízení složitosti a umožnit digitální transformaci s větším důrazem na zabezpečení. Roztříštěný přístup k právním předpisům by mohl vést k překrývajícím se a nekonzistentním regulačním požadavkům. To by mohlo mít vliv na zdroje a nakonec být v rozporu s cíli zabezpečení. Organizace by například mohly být nuceny převést prostředky z inovací a zabezpečení na formalistická cvičení k dodržování předpisů.

Microsoft se chce spojit se státními správami po celém světě a hledat s nimi efektivní zásady kybernetického zabezpečení kritické infrastruktury. Při tom je možné lépe porozumět problémům a příležitostem a podpořit úsilí při zlepšování celkového stavu zajištění před riziky.

Vývoj zásad při řízení rizik kybernetického zabezpečení kritické infrastruktury

V průběhu loňska několik jurisdikcí, například Austrálie, Chile, Evropská unie (EU), Japonsko, Singapur, Spojené království (UK) a Spojené státy, vyvinulo, aktualizovalo nebo implementovalo požadavky na kybernetické zabezpečení mezi odvětvími nebo v rámci konkrétního odvětví.[1] Mnoho z těchto státních správ – a dalších, třeba Indie[2] a Švýcarsko[3] – už vydalo nebo vyvíjí požadavky na hlášení incidentů kybernetického zabezpečení pro kritickou infrastrukturu a poskytovatele nezbytných služeb.[4]

Některé z významných vývojů za poslední rok jsou k vidění v Austrálii, Evropské unii, Indonésii a Spojených státech. Austrálie schválila dva zákony, které jí pomůžou řídit rizika kybernetického zabezpečení kritické infrastruktury mezi odvětvími. Zákony mimo jiné stanovují nová odvětví kritické infrastruktury, vyžadují vývoj plánů řízení rizik, zavádějí hlášení incidentů kybernetického zabezpečení a umožňují státní správě zasáhnout, pokud vyhodnotí, že operátor kritické infrastruktury není ochoten nebo schopen adekvátně reagovat na incident.



Evropská unie pracovala na aktualizaci směrnice NIS z roku 2016, která zavádí rámec pro členské státy EU k regulaci technologických služeb a produktů považovaných za nezbytné pro ekonomiku a fungování společnosti. Navrhovaná směrnice NIS 2 obsahuje změny, které by vytvořily novou kategorii kritické digitální infrastruktury, upřesnily požadavky na hlášení kybernetických incidentů a zavedly další požadavky na řízení rizik kybernetického zabezpečení. EU dále vyvinula navrhovanou aktualizaci svého Nařízení o digitální provozní odolnosti (DORA), kterým vznikají nové požadavky na informační a komunikační technologie používané v sektoru finančních služeb.

V květnu Indonésie vydala prezidentský regulativ na ochranu infrastruktury důležitých informací (IIV), který vejde v platnost v květnu 2024 a bude se zabývat odvětvími jako energetika, doprava, finančnictví, zdravotnictví a další. Cílem tohoto indonéského regulativu je chránit kontinuitu implementace IIV, bránit kybernetickým útokům a zvýšit připravenost na řešení kybernetických incidentů. Poskytovatelé IIV budou odpovídat za bezpečnou a spolehlivou ochranu, implementovat efektivní řízení kybernetických rizik a hlásit výsledky kybernetických rizik příslušným státním úřadům. Regulativ stanovuje požadavek na hlášení kybernetických incidentů do 24 hodin.

Státní správy činí kroky k lepšímu zabezpečení a odolnosti kritické infrastruktury

pokračování

Americký Kongres schválil zákon, který opravňuje úřad Cybersecurity and Infrastructure Security Agency (CISA) vydávat předpisy vyžadující hlášení kybernetických incidentů ze strany operátorů kritické infrastruktury, a americký úřad Transportation Security Administration (TSA) vydal nové požadavky na kybernetické zabezpečení v oboru dopravy. V roce 2021 úřad TSA vydal v reakci na ransomwarový útok na společnost Colonial Pipeline dvě bezpečnostní směrnice pro operátory distribučních sítí pro nebezpečné kapaliny a plyn:

- První směrnice zavedla požadavek, aby operátoři stanovili koordinátora kybernetického zabezpečení, hlásili kybernetické incidenty do 12 hodin a posuzovali ohrožení zabezpečení ve svých systémech.
- Druhá směrnice, kterou úřad TSA revidoval v roce 2022, vyžaduje implementovat konkrétní zmírňující opatření, která budou chránit před ransomwarovými útoky a dalšími známými hrozbami pro systémy IT a OT, do 30 dní vyvinout a implementovat pohotovostní a reakční plán a projít každoroční kontrolou architektonického návrhu kybernetického zabezpečení.

V návaznosti na své regulativy pro distribuční sítě úřad TSA vydal později v roce 2021 další dvě bezpečnostní směrnice, které stanovily požadavky na kybernetické zabezpečení systémů nákladní železniční přepravy, osobních železničních přepravců a železničního tranzitu. Směrnice vyžadovaly, aby příslušní operátoři ustanovili koordinátora kybernetického zabezpečení, hlásili incidenty kybernetického zabezpečení do 24 hodin, vyvinuli a implementovali plán reakce na incident kybernetického zabezpečení a provedli posouzení ohrožení kybernetického zabezpečení. Současně s tím úřad TSA oznámil, že aktualizoval své bezpečnostní programy pro letový provoz tak, aby letiště a letečtí dopravci implementovali první dvě ustanovení, tedy aby jmenovali koordinátora a do 24 hodin hlásili incidenty.

Vývoj zásad v oblasti zabezpečení zařízení IoT a OT

V několika desítkách zemí státní správy aktivně vyvíjejí požadavky, které posílí kybernetické zabezpečení produktů a služeb informačních a komunikačních technologií (ICT), včetně zařízení IoT a OT. V kontextu produktů a služeb ICT je největším problémem zabezpečení dodavatelského řetězce softwaru a zabezpečení IoT.

- Evropská komise navrhla Akt o kybernetické bezpečnosti, který by zavedl požadavky na kybernetické zabezpečení samostatného softwaru, připojených zařízení a doplňkových služeb.[5] Mezi relevantní postupy výrobců softwaru patří využití bezpečného životního cyklu vývoje softwaru[6] a poskytování softwarového kusovníku.[7] Nové požadavky na zabezpečení by se vztahovaly na připojená zařízení a všichni výrobci by měli za úkol řídit procesy koordinovaného zveřejňování chyb v zabezpečení[8] u produktů uvedených na trh.

Tvůrci zásad svou pozornost zaměřili i na stále širší využívání zařízení IoT a zařízení OT pracujících v síti.

- Ve Spojeném království vznikl koncept zákona Product Security and Telecommunications Infrastructure Bill, který bude vyžadovat, aby výrobci spotřebitelských připojitelných produktů, třeba chytrých televizorů, přestali používat výchozí hesla, na která snadno zacílí kyberzločinci. Mezi dalšími požadavky je zavedení zásad zveřejňování chyb v zabezpečení (například zasíláním oznámení o těchto chybách) a zajištění transparentnosti o minimální době, po kterou budou výrobci poskytovat aktualizace zabezpečení.[9]
- V EU jsou nové standardy nebo požadavky na zabezpečení implementovány několika legislativními nástroji, například aktem v přenesené pravomoci ke Směrnici o rádiových zařízeních, který se vztahuje na bezdrátová zařízení a jehož cílem je zlepšit odolnost sítí, chránit osobní údaje spotřebitelů a omezit riziko finančních podvodů.[10] Kromě toho může být zapotřebí používat schéma certifikace cloudů,[11] které je v současné době ve vývoji na základě evropské Směrnice o kybernetické bezpečnosti[12] z roku 2019.

Potřeba konsistence

V mnoha případech se nejrůznější aktivity mezi oblastmi, odvětvími, technologiemi a řízením provozních rizik řeší najednou, což může organizacím, které chtějí využít pokyny nebo prokázat dodržování předpisů, způsobit překryv a nekonzistenci v rozsahu, požadavcích a složitosti. Bez všeobecně uznávané definice IoT je pro regulace zařízení IoT a OT obzvláště velkým problémem rozsah. Výše uvedené příklady by se mohly vztahovat na propojené produkty a doplňkové služby, spotřebitelské připojitelné produkty a bezdrátová zařízení. Zároveň se mnoho státních správ zaměřuje na implementaci robustnějších režimů posuzování, aby lépe porozuměly, jestli a jak organizace a produkty plní aktuální, vznikající a měnící se požadavky. Tyto trendy se postupně slučují a s tím roste složitost. Je však povzbudivé, že se otázky položené během konzultačního období k evropskému Aktu o kybernetické bezpečnosti zabývaly tím, jak by nová regulace mohla ovlivnit stávající regulaci kybernetického zabezpečení. To naznačuje záměr předejít konfliktům požadavků na kybernetické zabezpečení.

Iterativní přístupy, jejichž základem je riziko a orientují se na výsledek nebo proces (v kontrastu se zaměřením na implementaci), by mohly podpořit lepší kybernetické zabezpečení a průběžné zdokonalování. Obdobně zaměření na podporu interoperability mezi odvětvími, oblastmi a zásadami by mohlo konzistentně posílit kybernetické zabezpečení mezi propojenými globálními dodavatelskými řetězci.

Státní správy činí kroky k lepšímu zabezpečení a odolnosti kritické infrastruktury

pokračování

V různých regionech, odvětvích a tématických oblastech se vyvíjejí stále složitější zásady kybernetického zabezpečení kritické infrastruktury. Tato aktivita přináší velké příležitosti a významné problémy. Další postup státních správ bude mít zásadní význam na budoucnost digitální transformace a zabezpečení v celém ekosystému.

Zrychlující investice v celém ekosystému zabezpečení dodavatelského řetězce softwaru a architektury Zero Trust (nulové důvěry)

Americké výkonné nařízení (EO) 14028 o zlepšení kybernetického zabezpečení umožnilo urychlit stávající iniciativu Microsoftu při investicích do zabezpečení svého dodavatelského řetězce softwaru i celého ekosystému a umožnit našim zákazníkům plnit cíle Zero Trust (nulové důvěry).

Již dlouho věříme, že aby došlo ke zlepšení dodavatelského řetězce softwaru, je zapotřebí sdílet poznatky a osvědčené postupy. Začali jsme uveřejněním našeho procesu Microsoft Security Development Lifecycle přibližně před 15 lety.

Dále úzce spolupracujeme s centrem National Cybersecurity Center of Excellence, abychom ukázali přístupy k architektuře Zero Trust (nulové důvěry) zavedené jak pro místní, tak cloudové technologie a předvedli nové funkce produktů, mezi které patří schopnost vynutit ověřování odolné proti phishingu pro hybridní a vícecloudová prostředí.

V současnosti překračujeme rámec požadavků EO na prokazování souladu s požadavky zabezpečení dodavatelského řetězce softwaru. Dvěma způsoby poskytujeme informace softwarového kusovníku (Software Bill of Materials – SBOM):

1. Nejprve sdílíme opensourcovou verzi našeho generátoru SBOM, který jsme vytvořili tak, aby se dal snadno integrovat do kanálů CI/CD podporujících sestavování na platformách Windows, Linux, Mac, iOS a Android.[13]
2. Dále přispíváme k vývoji oborových standardů pro integritu, transparentnost a důvěryhodnost dodavatelských řetězců (SCITT). To umožní automatizovanou výměnu ověřitelných informací o dodavatelském řetězci, včetně artefaktů, které prokazují dodržování požadavků, třeba těch vyplývajících z pokynů pro dodavatelské řetězce softwaru v EO.

Poznatky a jejich využití

1. Nadnárodní instituce musí být přepracovány tak, aby se mohly postavit naléhavému problému kybernetických útoků národních států.
2. Vyvíjejte zásady kybernetického zabezpečení, které jsou konzistentní a interoperabilní mezi regiony, odvětvími a tématickými oblastmi.

Odkazy na další informace

- Stávající investice do zabezpečení dodavatelských řetězců na podporu výkonného nařízení o kybernetickém zabezpečení | Microsoft Tech Community
- Vláda USA stanovuje strategii a požadavky pro architektury Zero Trust (nulové důvěry) | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Integrita, transparentnost a důvěryhodnost dodavatelského řetězce | github.com
- Implementace architektury Zero Trust (nulové důvěry) | NCCoE (nist.gov)

Exponované IoT a OT: trendy a útoky

Stále více a více propojený digitální svět znamená, že se zařízení rychle připojují, komunikují s většími systémy, shromažďují data a nabízejí přístup na dříve špatně dostupná místa. To nabízí příležitosti jak organizacím, tak aktérům hrozeb a podnikání v kybernetické kriminalitě se stalo oborem a rizikem hodnoceným na miliardy dolarů.

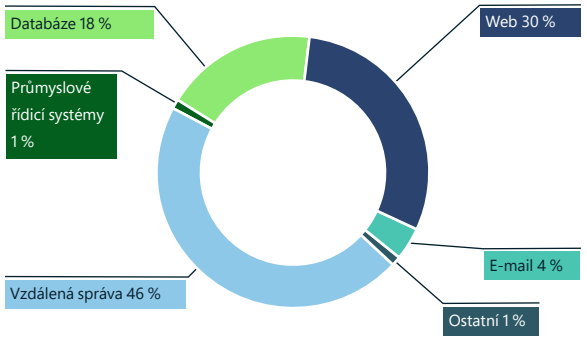
Zařízení IoT, mezi která patří vše od tiskáren po webové kamery, klimatizace a přístupové systémy pro budovy, představují jedinečná bezpečnostní rizika pro jednotlivce, organizace a sítě. Ačkoli jsou nezbytně důležitá pro provoz mnoha organizací, můžou se rychle stát přítěží a bezpečnostním rizikem. Rychlé zavádění řešení IoT v téměř všech oborech navýšilo počet vektorů útoků a rizika odhalení organizací.

Malware jako služba se v současné době využívá pro rozsáhlé operace jak proti civilní infrastruktuře a veřejným službám (včetně nemocnic, čerpacích stanic, elektrických rozvodných sítí, dopravních služeb a další kritické infrastruktury), tak firemním sítím. Aby aktéři hrozeb mohli objevit a zneužít konfiguraci provozních prostředí a integrovaných zařízení IoT a OT, musí vynaložit značné úsilí.

Zařízení IoS představují jedinečná bezpečnostní rizika jako vstupní a výchozí body v síti. Miliony zařízení IoT zůstávají bez oprav nebo jsou exponovány.

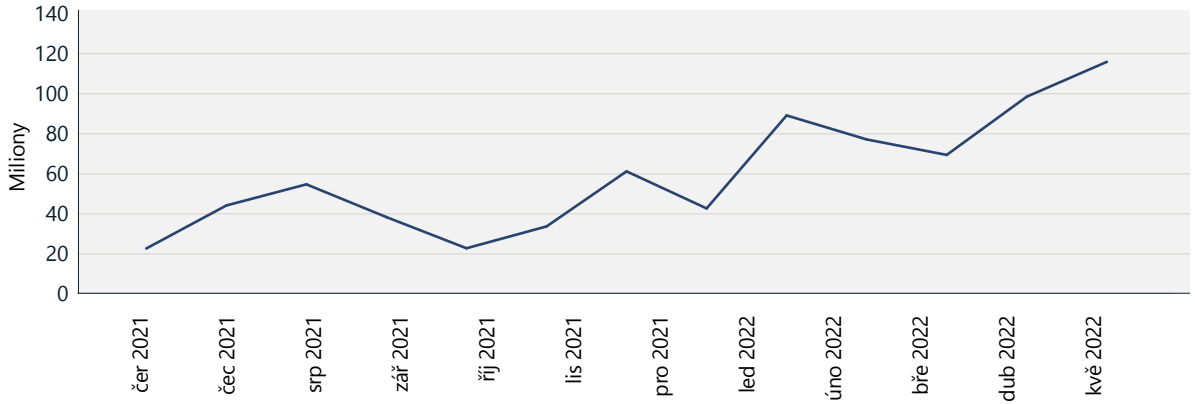
Exponovaná zařízení se dají najít pomocí nástrojů pro prohledávání internetu, které identifikují služby naslouchající na otevřených síťových portech. Tyto porty se běžně používají pro vzdálenou správu zařízení. Nesprávně zabezpečené exponované zařízení IoT se dá využít jako výchozí bod do další vrstvy firemní sítě, protože neautorizovaní uživatelé můžou k portům přistupovat na dálku. Zaznamenali jsme, jak se různí aktéři hrozeb pokoušejí zneužít chyby v zabezpečení zařízení připojených k internetu, od kamer přes směrovače až po termostaty. Navzdory riziku však zůstávají miliony zařízení neopravené nebo exponované.

Shrnutí typů útoků na IoT a OT



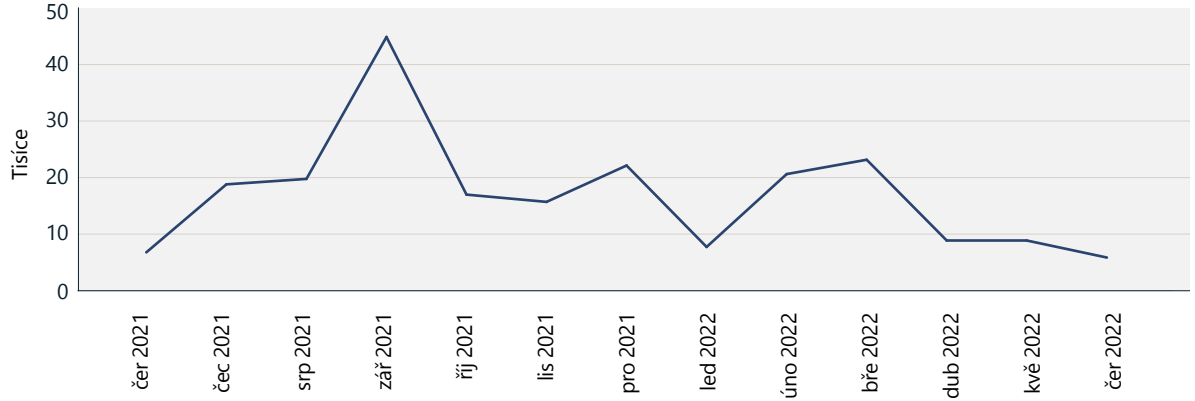
Typy útoků pozorované prostřednictvím sítě senzorů MSTIC. Nejčastějšími útoky byly útoky na zařízení pro vzdálenou správu, útoky přes web a útoky na databáze (hrubá síla nebo zneužití chyb).

Útoky na zařízení pro vzdálenou správu



Rostoucí počet útoků na porty pro vzdálenou správu v průběhu času zaznamenaný sítí senzorů MSTIC.

Webové útoky na IoT a OT



Objem webových útoků v průběhu času zaznamenaný sítí senzorů MSTIC. Čím méně je zařízení připojených přímo k webu, tím méně pravděpodobné nakonec může být, že je budou útočníci prohledávat.

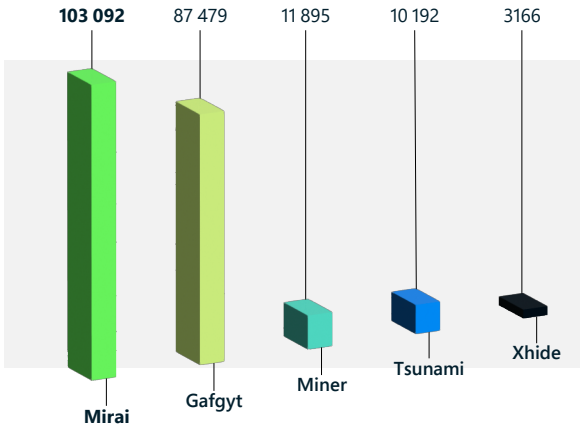
Exponované IoT a OT: trendy a útoky

pokračování

Přepracovaný malwarový nástroj

S vývojem kyberzločineckých skupin se vyvíjely i malware a volba cílů. V uplynulém roce jsme pozorovali, že počet útoků na běžné protokoly IoT, například Telnet, výrazně poklesl. V některých případech dokonce o 60 procent. Zároveň kyberzločinecké skupiny a aktéři národních států přepracovali botnety. Vytrvalost malwaru, jako je Mirai, podtrhuje modularitu těchto útoků a přizpůsobitelnost existujících hrozeb.

Malware pro IoT nejčastěji detekovaný ve veřejném prostoru



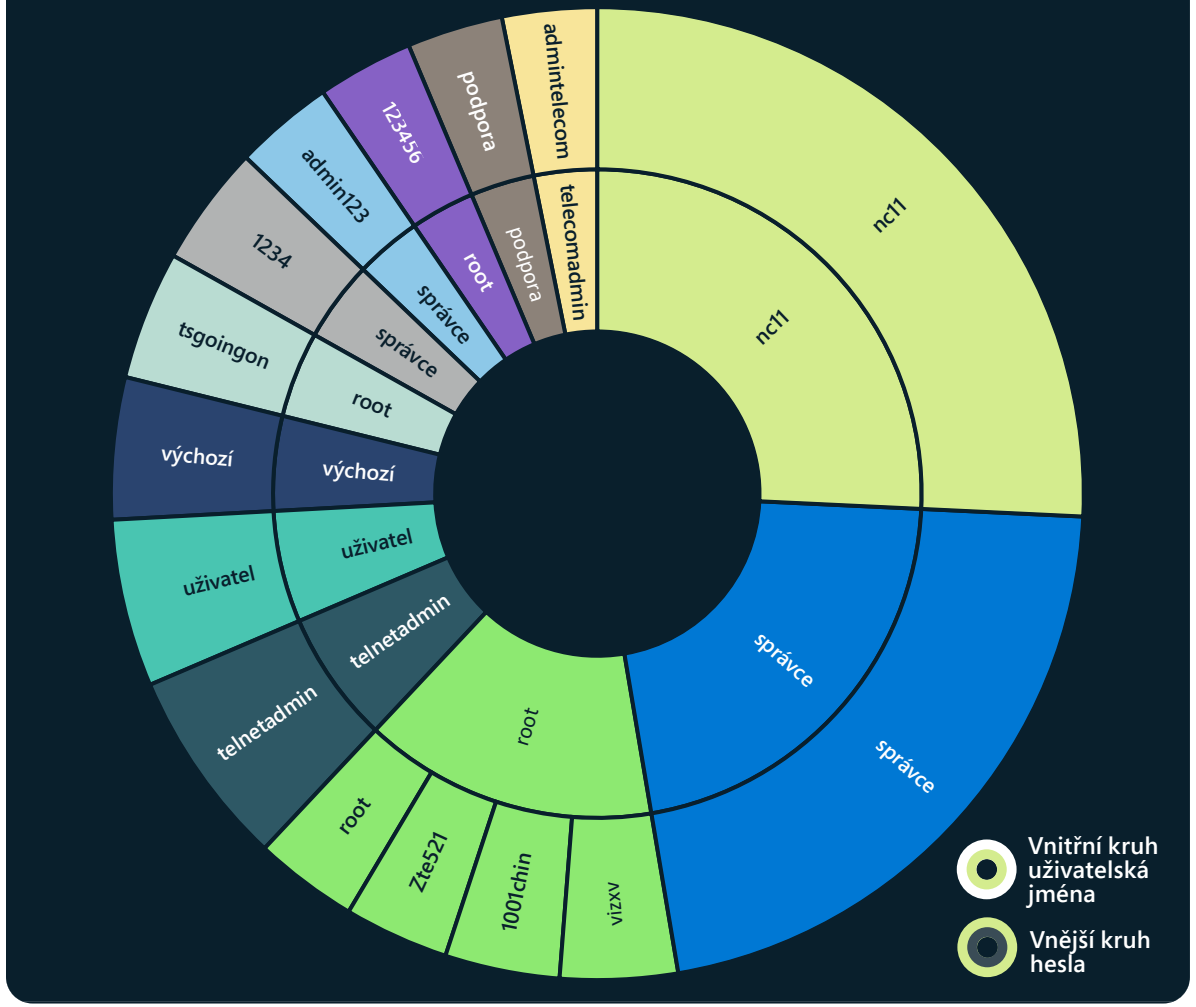
Mirai se vyvinul tak, aby napadal širokou paletu zařízení IoT, třeba IP kamery, bezpečnostní kamery, digitální videorekordéry a směrovače. Vektor útoku obcházel starší mechanismy zabezpečení a představuje riziko pro koncové body v sítích, neboť zneužívá další chyby v zabezpečení a pohybuje se taktikou lateral movement. Mirai byl několikrát přepracován. Jeho varianty se přizpůsobují různým architekturám a zneužívají známé chyby zabezpečení i chyby nultého dne, přes které zajišťují nové vektory útoku.

Mirai byl za poslední rok stále častěji využíván na 32- i 64bitové architektuře procesorů x86 a získal nové funkce, které velmi rychle zavedly skupiny národních států a zločinců. Útoky národních států teď využívají nové varianty existujících botnetů při útocích DDoS na cizí protivníky.

V roce 2022 došlo k poklesu výnosů z útoků na zařízení IoT. Zjistili jsme, že několik skupin aktérů hrozeb zneužívá chyby v zabezpečení, například Log4j a Spring4Shell, k doručování škodlivých programů na zařízení, jako jsou servery. Aktéři tato zařízení napadají a začleňují je do velkých botnetů, které provádějí útoky DDoS. Přepracovaný malwarový nástroj navržený na cílení ohrožených zařízení IoT má vážné dopady jak na organizace, tak na státy, protože taktika lateral movement může odhalit zadní vrátka pro další škodlivé programy a jiná zařízení na síti.

Mnoho protokolů pro průmyslové řídicí systémy není monitorováno, což je vystavuje hrozbám útoků na konkrétní OT. To může znamenat zvýšené riziko pro kritickou infrastrukturu.

Relativní výskyty dvojic uživatelského jména a hesla zjištěných na zařízeních IoT/OT v signálech senzorů shromážděných za 45 dní.



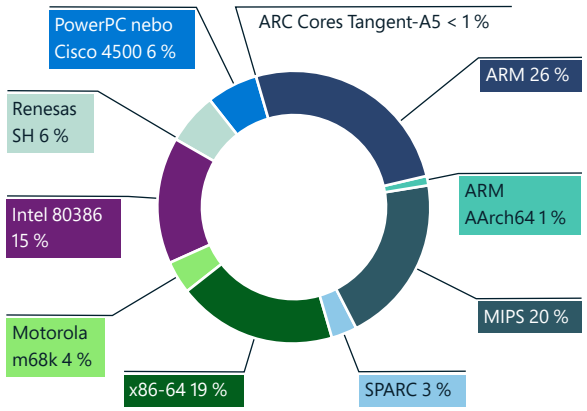
Používání běžných dvojic uživatelského jména a hesla zvyšuje riziko napadení. Na základě vzorku více než 39 milionů zařízení IoT a OT představovala ta, která používá stejná uživatelská jména a hesla, přibližně 20 procent.

Exponované IoT a OT: trendy a útoky

pokračování

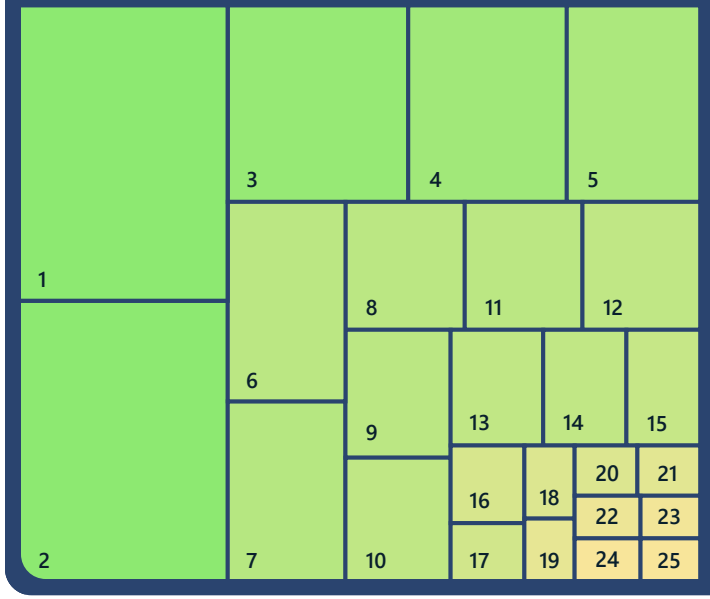
I když slabé konfigurace a výchozí přihlašovací údaje stále představují pro sítě nebezpečí, Microsoft zaznamenal mnoho webových útoků, které využívaly protokol HTTP. Tento nárůst počtu útoku jsme zpozorovali na webových službách, které používají starší verze botnetů. Mezitím došlo k poklesu počtu otevřených portů pro Telnet na internetu, což je pozitivní vývoj zabezpečení sítí, protože botnety, které v minulosti ohrožovaly zařízení, ztrácejí na významu. I přes tento pokles otevřených telnetových portů jsme v síti senzorů stále zaznamenávali trvalé botnety.

Rozdělení malwaru IoT podle architektury CPU



Microsoft zjistil, že malware nejčastěji cílí na zařízení IoT, která používají architekturu ARM. Následují architektury MIPS, X86-64 a procesory Intel 80386.

Výskyt protokolů průmyslových řídicích systémů



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

Ohrožení zabezpečení protokolů průmyslových řídicích systémů

Prohlédli jsme si data o OT z našich senzorů připojených do cloudu a zjistili jsme, které protokoly průmyslových řídicích systémů (ICS) se používají nejčastěji. Tyto protokoly nabízejí poznatky o povaze těchto zařízení a jejich potenciální oblasti útoku. Je to obzvláště důležité z pohledu zabezpečení kritické infrastruktury. Mezi hlavní poznatky patří:

1. Většina zastoupených protokolů je proprietární, proto standardní monitorovací nástroje IT nebudou mít patřičné informace o zabezpečení těchto zařízení a protokolů. Kvůli tomu zůstávají sítě bez monitorování a jsou tak více ohroženy útoky na konkrétní OT.
2. Protokoly různých dodavatelů se značně liší. To znamená, že řešení zabezpečení konkrétního dodavatele nebude moct vhodným způsobem pokrýt celou síť. Microsoft upřednostňuje přístup nezávislý na dodavateli, který nabízí zabezpečení pro širokou škálu různých zařízení.
3. Organizace by ve svých sítích měly zajistit, že tyto protokoly nebudou přístupné přímo z internetu. Taková expozice by mohla kvůli chybám a nezabezpečené povaze těchto protokolů představovat významné bezpečnostní riziko.

Malware, jako je Mirai, přetrvává díky vývoji nových funkcí. Používají jej kyberzločinecké skupiny a aktéři národních států, kteří využívají nové varianty stávajících botnetů při útocích DDoS na cizí protivníky.

Poznatky a jejich využití

1. Zajistěte robustnost zařízení instalací oprav a změnou výchozích hesel a výchozích portů SSH.
2. Omezte potenciální oblast útoku odstraněním nepotřebných internetových připojení a otevřených portů, omezením vzdáleného přístupu blokováním portů, zákazem vzdáleného přístupu a používáním služeb VPN.
3. Používejte v síti řešení pro detekci a reakce (NDR), které umí pracovat s IoT a OT, řešení správy akcí a informací o zabezpečení (SIEM) a řešení pro orchestraci zabezpečení a reakce (SOAR), kterými budete monitorovat neobvyklé nebo neautorizované chování zařízení, třeba komunikaci s neznámými hostiteli.
4. Rozdělte sítě s cílem omezit schopnost útočníka používat taktiku lateral movement a napadnout prostředky po počátečním průniku. Zařízení IoT a sítě OT by měly být izolovány od podnikových IT sítí prostřednictvím bran firewall.
5. Zajistěte, že protokoly ICS nebudou přístupné přímo z internetu.

Hackování dodavatelského řetězce a firmwaru

Skoro každé zařízení připojené k internetu má firmware, což je software integrovaný do hardwaru nebo obvodové desky zařízení. V průběhu posledních několika let jsme zjistili, že se stále častěji cílí na firmware s cílem zahájit ničivé útoky. Jelikož firmware bude pravděpodobně i nadále cenným cílem aktérů hrozeb, musí se organizace chránit před jeho hackováním.

Firmware odpovídá za primární funkce zařízení, například připojování k síti a ukládání dat. Firmware se nachází ve směrovačích, kamerách, televizích a dalších zařízeních, která se používají ve firmách (IoT), spolu s průmyslovými řídicími zařízeními (OT), která se používají v kritické infrastruktuře. V minulosti byl firmware psán nezabezpečeným kódem, čímž vznikaly vážné chyby v zabezpečení. Ty se dají využít k převzetí kontroly nad zařízením nebo vložení škodlivého kódu do firmwaru.

Toto riziko se stupňuje ve chvíli, kdy se začne dotýkat dodavatelského řetězce. Většina zařízení je vyráběna se softwarovými a hardwarovými součástmi různých výrobců a opensourcovými knihovnami. V mnoha případech provozovatelé zařízení nemají informace o hardwarovém a softwarovém kusovníku (H/SBOM), aby mohli vyhodnotit riziko dodavatelského řetězce pro zařízení ve své síti. V červnu 2020 byly v síťové infrastruktuře používané mnoha různými výrobci odhaleny chyby v zabezpečení, které měly vliv na miliony zařízení IoT ve spotřebitelském i průmyslovém sektoru.[14] V některých případech jiní dodavatelé síťovou infrastrukturu přejmenovali a nebylo nijak patrné, že zařízení bylo ohroženo. Pozorujeme rostoucí hrozbu škodlivých aktérů, kteří na tento dodavatelský řetězec softwaru a hardwaru zařízení IoT a OT cílí, aby mohli napadnout organizace.

Proces aktualizace firmwaru se mezi jednotlivými zařízeními značně liší a složitost a logistické překážky při jeho provádění mají vliv na četnost aktualizací. Není vždy možné určit, jestli zařízení používá nejnovější firmware. Proto je taky pro odborníky na zabezpečení obtížné monitorovat a zajistit stav zabezpečení svých zařízení IoT a OT. Kromě toho některá zařízení mají firmware, který není kryptograficky podepsaný, což jim umožňuje aktualizace bez ověření uživatelem. Tyto slabé stránky ještě více otevírají zařízení útokům na dodavatelský řetězec v celém produkčním a distribučním řetězci.

Aby Microsoft na tyto hrozby reagoval, investuje nemalé prostředky do zajištění zabezpečení a integrity firmwaru v různých fázích dodavatelského řetězce. Kdykoli dokáže ověřit, že během jeho činnosti s ním nebylo manipulováno. To nám umožní ověřovat důvěryhodnost jednotlivých částí kanálu a poskytovat certifikované a prokazatelné sledování původu každé součásti, kterou dodáváme zákazníkům. Spolupracujeme s partnery na zavádění tohoto komplexního zabezpečení od prvního čipu až po cloud na všechna zařízení ve firemní a OT síti.

„Dodavatelé ICT infrastruktury jsou stále častějšími cíli, protože umožňují ve velkém měřítku replikovat jeden útok. Současně se stále upřesňují regulace, globální legislativa a požadavky zákazníků na zabezpečení a odolnost dodavatelského řetězce, které se však často rozcházejí.

Řešením je partnerství. Spolu s dodavateli a státními správami po celém světě se Microsoft zavázal řešit zabezpečení v celém ekosystému dodavatelského řetězce. Tím chce překonat požadavky zákazníků i regulátorů. Za tímto účelem podporujeme ucelený přístup k zabezpečení a provozní odolnosti, který je flexibilně nasazován v celém dodavatelském řetězci.

Klíčem k našemu kolektivnímu přístupu je podpora integrity firmwaru od návrhu až po zprovoznění zařízení. Jako příklad, jak dokážeme ‚zabudovat' integritu dodavatelského řetězce, můžeme uvést zajištění procesů SDL dodavatelů a nasazení inovací v oblasti hardwarových důvěryhodných kořenových certifikátů.

Naše komunita využívá společného výzkumu a vývoje, který se zabývá technikami ochrany před manipulací a kryptografickými mechanismy v kombinaci se stávajícím monitorování a detekcí anomálií. Společně pracujeme na minimalizaci atraktivity dodavatelského řetězce jako potenciální oblasti útoku."

Edna Conway,
Vice President, Security & Risk Officer,
Cloud Infrastructure

Vybrané chyby v zabezpečení firmwaru

Útočníci stále častěji využívají chyb v zabezpečení firmwaru zařízení IoT, pomocí kterých pronikají do firemních sítí. Na rozdíl od tradičních koncových bodů IT, které k identifikaci slabých stránek používají agenty XDR, je identifikace slabých stránek zařízení IoT nebo OT mnohem obtížnější.

Nedávný průzkum společností Microsoft a Ponemon Institute zdůrazňuje příležitost i problematiku zabezpečení zařízení IoT a OT ve firmě.[15] Ačkoli se 68 % respondentů domnívá, že zavést IoT nebo OT je nezbytné pro strategickou digitální transformaci, 60 procent uznává, že IoT a OT představují nejméně zabezpečený aspekt IT/OT infrastruktury.

Příkladem, kdy útočníci využili chyby v zabezpečení firmwaru zařízení IoT k průniku do sítě, je trojský kůň Trickbot. Ten využíval výchozí hesla a chyby v zabezpečení směrovačů Mikrotik,[16] pomocí nichž obcházel firemní obranné systémy. Nejzákladnějším problémem s firmwarem zařízení IoT je nedostatek informací o stavu zabezpečení a chyb v zabezpečení zařízení.

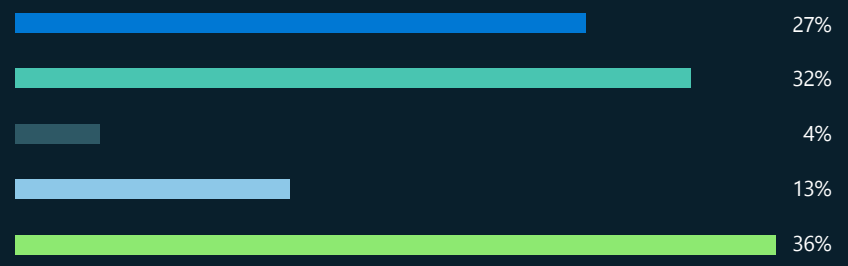
I když jsou k dispozici řešení, jak vyrábět zabezpečená zařízení, na trhu a ve firmách se už vyskytují miliardy zařízení. Těm se říká brownfieldová zařízení. V roce 2021 Microsoft koupil společnost ReFirm Labs, se kterou chce vrhnout na zabezpečení brownfieldových zařízení světlo a umožnit výrobcům zařízení zlepšit zabezpečení svých produktů. ReFirm Labs analyzuje binární image firmwaru zařízení a vytváří podrobnou sestavu o možných slabých stránkách zabezpečení.[17] Tato technologie je začleňována do budoucích verzí Microsoft Defenderu for IoT.

Za poslední rok jsme si prošli souhrnné výsledky jedinečných firmwarů, které prohledali naši zákazníci. Ne každá objevená slabá stránka musí být nutně zneužitelná, je z toho však patrné, kde spočívá nejzákladnější problém zabezpečení firmwaru zařízení.

Stojí za zmínku, že typy slabých stránek, které se vyskytují na zařízeních IoT nebo OT, by nikdy nebyly přijatelné na tradičních koncových bodech s Windows nebo Linuxem.

- Slabá hesla: Dvacet sedm procent prohledaných imagí firmwaru obsahovalo účty s hesly kódovanými slabými algoritmy (MD5/DES), které útočníci dokáží snadno prolomit.

Analyzované slabé stránky zabezpečení v imagích firmwaru



- Známé chyby v zabezpečení: Stejně jako jiné systémy i firmware zařízení IoT a OT ve velké míře využíval opensourcové knihovny. Zařízení se však často dodávají se zastaralými verzemi těchto součástí. V naší analýze 32 procent imagí obsahovalo alespoň 10 známých chyb v zabezpečení (CVE) hodnocených jako kritické (9,0 a více). Čtyři procenta obsahovala alespoň 10 kritických chyb v zabezpečení, které byly starší než šest let.
- Certifikáty s ukončenou platností: Certifikáty se používají k ověřování připojení a identit i k ochraně citlivých dat, ale 13 procent analyzovaných imagí obsahovalo nejméně 10 certifikátů, jejichž platnost vypršela před více než třemi lety.
- Softwarové komponenty: Třicet šest procent imagí obsahovalo softwarové součásti, které Microsoft doporučuje vyloučit ze zařízení IoT, například nástroje pro zachytávání paketů (tcpdump, libpcap). Dají se totiž využít k průzkumu sítě v rámci řetězce útoků.

Útoky na firmware ve veřejném prostoru

Viasat: Využití chyby v zabezpečení firmwaru k zacílení na satelitní komunikaci

V únoru 2022 došlo k incidentu satelitní sítě, který odpojil strategickou komunikační síť a měl dopad na celou Evropu. Systém KA-SAT společnosti Viasat obdržel značný objem provozu, který odpojil mnoho modemů. Proti síti byl zahájen útok přerušením služby (denial of service). Pevné širokopásmové připojení bylo narušeno a provozovatelé se nemohli vzdáleně připojit k tisícům větrných turbín. Na modemy, na které to mělo vliv, byl nasazen škodlivý malware pro vymazávání dat. Narušení mělo vliv na více než 30 000 satelitních terminálů, které používají společnosti a organizace ke komunikaci.

Cyclops Blink: Využití útoku na dodavatelský řetězec firmwaru k zacílení na brány firmwaru

Pro aktéry hrozeb je vývoj a šíření řídicích center (C2) a infrastruktury pro útoky nezbytným prostředkem k úspěchu. Se stále větší potřebou stabilní infrastruktury C2 začaly být žádoucím vektorem útoku směrovače, protože nejsou často opravovány a chybí jim komplexní řešení zabezpečení.

Microsoft navazuje partnerství se státními správami a průmyslem, aby s nimi spolupracoval na technologii pro analýzu firmwarů. Díky této technologii bude k dispozici více informací o zabezpečení zařízení. Výrobcům a provozovatelům zařízení bude možné nabídnout zabezpečení v rámci celého životního cyklu.

Od června 2019 používala skupina rozšířené trvalé hrozby (ATP) spolupracující s národním státem modulární malware Cyclops Blink, s nímž cílila na ohrožená zařízení brány firewall WatchGuard a směrovače ASUS. Instalovala aktualizace se škodlivým firmwarem a začleňovala je do velkého botnetu. Tento malware úspěšně napadá zařízení zneužíváním známé chyby v zabezpečení, která umožňuje zvýšit oprávnění. Díky tomu můžou aktéři hrozeb zařízení spravovat. Po nákaze malware umožňuje nainstalovat další moduly a vyhýbá se aktualizacím firmwaru. Bylo zjištěno, že napadená zařízení se připojují k serverům C2 hostovaným na jiných zařízeních WatchGuard. Operátoři Cyclops Blink vystavovali pro své C2 mnoho certifikátů SSL na různých portech TCP a získali privilegovaný vzdálený přístup do sítí. Zajistila jim jej instalace aktualizací se škodlivým firmwarem a vyhýbání se tradičním způsobům zabezpečení, jako je prohledávání.

Jak Microsoft zlepšuje zabezpečení dodavatelského řetězce

Microsoft spolupracuje se státními správami a průmyslem na řešení těchto problémů se zabezpečením zařízení IoT a OT (přečtěte si diskuzi na straně 66). Jedním z našich příspěvků bude využití technologie pro analýzu firmwaru, která provozovatelům zařízení nabídne informace o stavu zabezpečení zařízení v jejich síti. Díky tomu budou moct zákazníci identifikovat a stanovovat priority zařízení, která je zapotřebí důkladněji chránit, upgradovat nebo vyměnit. Zvyšuje se tím zároveň poptávka, aby výrobci zařízení investovali do zabezpečení výrobků. Současně výrobce podporujeme komplexními řešeními k návrhu zabezpečených zařízení a přijímání bezpečných životních cyklů vývoje.

Další klíčovou součástí je poskytnout výrobcům a provozovatelům robustní infrastrukturu, která umožní aktualizovat firmware zařízení podle toho, jak jsou objevovány a řešeny problémy se zabezpečením. Microsoft spojuje analýzu firmwaru a Defender for IoT se službou Device Update for IoT Hub, aby nabídl řešení celého životního cyklu zabezpečení zařízení IoT a OT. To jsou důležité kroky v realizaci naší vize, v níž zákazníci zabezpečují infrastrukturu zaváděním zařízení podporujících přístup Zero Trust (nulové důvěry) do svých řešení IoT a OT.[18]

Útočníci stále častěji cílí na chyby v zabezpečení firmwaru zařízení IoT, pomocí kterých pronikají do firemních sítí.

Poznatky a jejich využití

1. Zjistěte si podrobnější informace o zařízeních IoT a OT v síti, a pokud byla napadena, nastavte jim priority podle rizik pro firmu.
2. Používejte nástroje pro prohledávání firmwaru, abyste mohli porozumět možným slabým stránkám zabezpečení a spolupracovat s dodavateli na identifikaci a zmírnění rizik vysoce rizikových zařízení.
3. Vyžadujte, aby vaši dodavatelé používali osvědčené postupy pro životní cyklus vývoje softwaru. Příznivě tak ovlivníte zabezpečení zařízení IoT a OT.

Odkazy na další informace

- Posouzení kritických dodavatelských řetězců podporujících americký průmysl informačních a komunikačních technologií

Útoky na OT založené na průzkumech

Komplexní dodavatelské řetězce používají při plánování skutečného systému konkrétní informace o návrhu. Z toho obrovského množství prvků, ze kterých se tyto informace o návrhu skládají, je nejcitlivějším soubor projektu, který definuje prostředí a jeho prostředky. Tento soubor je klíčovým strategickým cílem pro aktéry hrozeb, kteří chtějí získat přístup a nasadit úspěšný útok zcela přizpůsobený danému prostředí.

Cílení na průmyslové systémy za účelem narušení provozních procesů má dva kroky.

1. Nejdříve musí útočník získat přístup do sítě OT. Toho může docílit vstupem na provozní a řídicí úrovně přes zařízení IoT na firemní straně sítě (úroveň 4 modelu Purdue) a překročením hranice mezi IT a OT, kterou tradičně oddělují brány firewall a síťová zařízení.
2. Dále je zapotřebí identifikovat síťová zařízení. Průmyslové systémy používají v přizpůsobených architekturách navržených speciálně pro jejich prostředí standardní zařízení a součásti. Jedním z těchto standardních zařízení je programovatelná logická řídicí jednotka (PLC). Každý výrobce pro svá PLC vyvíjí jedinečná rozhraní a funkce, které jsou nedílnou součástí průmyslových systémů. Tato zařízení se dále konfigurují přizpůsobenými schématy speciálně navrženými pro prostředí zákazníků.

Jedinečná konfigurace každého PLC je popsána v souboru projektu, který obsahuje definici prostředí a jeho prostředků, žebříkovou logiku a podobně.

Ve většině prostředí, která vykazují známky útoku, analýza ukazuje, že délka činností před útokem dalece přesahuje dobu trvání samotného útoku. Aktéři hrozeb často tráví měsíce vzdálenou simulací prostředí a jeho prostředků. Provádějí mnoho pokusů o vytvoření modelu a připravují svůj cílený útok. Prostředí neustále mění a integrují nová zařízení, což s sebou přináší nové chyby v zabezpečení, obzvláště v oblasti dat v projektových a konfiguračních souborech. Krádež souboru projektu může útok urychlit o týdny nebo měsíce a umožnit útočníkům rychle a přesně vymodelovat cílové prostředí, čímž se zvyšuje obtížnost detekce škodlivé aktivity.

Industroyer a Incontroller

Zaznamenali jsme větší počet útoků na organizace, kritickou infrastrukturu a státní cíle ze strany státy sponzorovaných aktérů, kteří používají modulární malware a architektury útoků. Nové pokusy o zásah do kritických operací na Ukrajině jen podtrhují rostoucí hrozbu útoků na OT založených na průzkumech, které jsou do značné míry přizpůsobené svým cílovým prostředím. Delší fáze průzkumu a výzkumu, které kybernetičtí aktéři národních států používají, poukazují na strategii využití kybernetické války ke vzdálenému ochromení infrastruktury a splnění konkrétních strategických nebo operačních cílů ve spojených kybernetico-kinetických operacích a politických strategiích.

Zaznamenali jsme stále větší hrozbu útoků na OT založených na průzkumu, které byly značně přizpůsobené cílovým prostředím.

Útoky na OT založené na průzkumech

pokračování

Na začátku roku 2022 byly identifikovány dva proměnlivé útoky na OT. Při kybernetické-fyzickém útoku na elektrické rozvodny a ochranná relé na Ukrajině byl použit přizpůsobený malware, včetně varianty Industroyeru. To je malware známý tím, že po svém nasazení v roce 2016 způsobil na Ukrajině výpadky elektřiny.

Industroyer2 je první známé opětovné nasazení škodlivého malwaru pro útoky na OT proti novému cíli. Využíval modul plug-in protokolu IEC104 (standardního protokolu pro monitorování a řízení energie) vyvinutý pro Industroyer a jeho cílem byly především vzdálené terminálové jednotky podobné PLC s modelovým číslem ABB RTU540/560. Autor tohoto malwaru využil znalosti prostředí oběti, aby opakovaně zadával příkazy na předem stanovené výstupy. Tím zajistil, že nebude možné je zapnout ručně. Způsobil tak dlouhodobé výpadky elektřiny s ještě ničivějším dopadem.

Incontroller, modulární architektura útoků identifikovaná ve stejném období, je modulární sada nástrojů, která významně snižuje čas potřebný k překonání starších verzí řešení zabezpečení a k průniku a útoku na zařízení OT. Tato obecná sada nástrojů obsahuje funkce pro shromažďování dat, průzkum a útoky, které je možné do značné míry přizpůsobit různým prostředím a mají velký dopad na výzkumnou fázi útoku na OT. Zkracuje se tím doba potřebná na průzkum a díky extrakci informací o zařízeních a jejich konfiguracích to podporuje simulaci prostředí.

Architektura Incontroller podporuje protokoly pro PLC Schneider Electric a Omron a sbírá informace, jako jsou verze firmwaru, typ modelu a připojená zařízení. Sada nástrojů dokáže vydávat příkazy, které mění konfiguraci a zapínají nebo vypínají výstupy. Jakmile útočník získá přístup do prostředí, architektura podporuje zavedení zadních vrátek do zařízení, aby bylo možné doručit další škodlivý software, hledat slabé stránky jako vstupní body, nahrávat žebříkovou logiku a zahajovat útoky DoS. Díky obecné povaze této sady nástrojů může aktér hrozeb rychle zaútočit na prostředí, aniž by musel psát nové útoky pro každé PLC nebo místo. Tak aktér může snadno pracovat s různými typy počítačů, potenciálně i v mnoha různých oblastech.

Poznatky a jejich využití

1. Nepřenášejte soubory, které obsahují definice systému, přes nezabezpečené kanály ani je nepředávejte personálu, který je nepotřebuje.
2. Pokud je přenos takových souborů nezbytný, důkladně monitorujte aktivitu na síti a zajistěte, že jsou prostředky zabezpečené.
3. Chraňte technické stanice monitorováním pomocí řešení EDR.
4. Aktivně reagujte na incidenty v sítích OT.
5. Nasaďte průběžné monitorování, třeba Defender for IoT.

Poznámky na závěr

1. Přečtěte si např. Revised Directive on Security of Network and Information Systems (NIS2) | Utváření digitální budoucnosti Evropy (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 – Domovská stránka
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Přečtěte si např. untitled (house.gov).
5. Akt o kybernetické odolnosti | Utváření digitální budoucnosti Evropy (europa.eu)
6. Přečtěte si např. Microsoft Security Development Lifecycle.
7. Přečtěte si např. Generování softwarových kusovníků (SBOM) pomocí SPDX v Microsoftu – Engineering@Microsoft a dále The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Přečtěte si např. 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. Komise posiluje kybernetickou bezpečnost bezdrátových zařízení a výrobků (europa.eu)
11. Certifikační schéma pro cloud: Budování důvěryhodných cloudových služeb v celé Evropě – ENISA (europa.eu)
12. Certifikace – ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool"GitHub-Microsoft/sbom-Tool: nástroj SBOM je vysoce škálovatelný a podnikový nástroj, který umožňuje vytvářet kompatibilní Sbomy SPDX 2,2 pro nejrůznější artefakty.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. Inovace IoT a OT je nezbytná, ale přináší značná rizika (prosinec 2021): 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. Odhalování používání IoT zařízení v infrastruktuře C2 Trickbotem (březen 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. Seriál IoT na Channel 9, epizoda o prohledávání firmwaru IoT (květen 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. Jak do svých řešení IoT zavést přístup Zero Trust (nulové důvěry) (květen 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Operace ovlivňování v kyberprostoru

Dnešní zahraniční operace ovlivňování používají nové metody a technologie, díky kterým jsou jejich kampaně navržené k podkopávání důvěry účinnější.

Přehled

operací ovlivňování v kyberprostoru

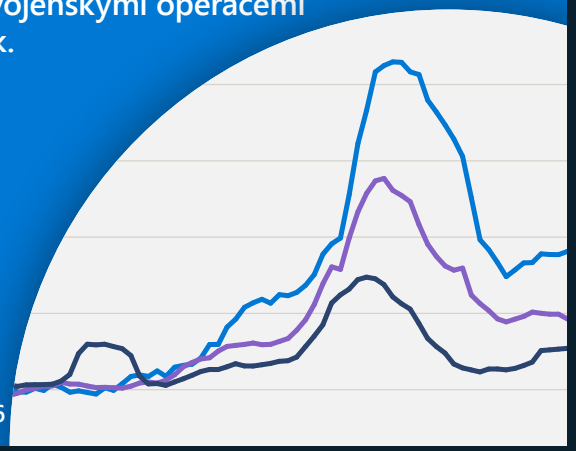
Dnešní zahraniční operace ovlivňování používají nové metody a technologie, díky kterým jsou jejich kampaně navržené k podkopávání důvěry účinnější.

Národní státy ve stále větší míře využívají důmyslné operace ovlivňování, kterými šíří propagandu a ovlivňují veřejné mínění jak na svém vlastním území, tak za svými hranicemi. Tyto kampaně podkopávají důvěru, podporují polarizaci a ohrožují demokratické procesy. Zkušení aktéři pokročilých trvalých manipulací používají tradiční média spolu s internetem a sociálními médii ke značnému navýšení rozsahu, měřítka a efektivity svých kampaní. Díky tomu mají obrovský dopad na globální informační ekosystém. Za poslední rok jsme tyto operace pozorovali v rámci hybridní války Ruska na Ukrajině, ale zároveň jsme zjistili, že Rusko a jiné státy, třeba Čína a Írán, se stále častěji spoléhají na operace propagandy využívající sociální média. Rozšiřují tak svůj globální vliv.

Operace ovlivňování v kyberprostoru jsou stále propracovanější a stále více státních správ a národních států tyto operace používají k utváření názorů, diskreditaci protivníků a podpoře vzdoru.

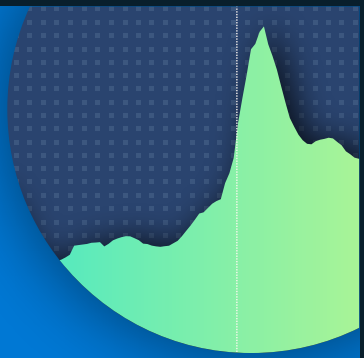
Více se dozvíte na str. 74

Ruská invaze na Ukrajinu ukazuje, jak jsou operace ovlivňování v kyberprostoru integrovány s tradičnějšími kybernetickými útoky a kinetickými vojenskými operacemi pro maximální účinek.



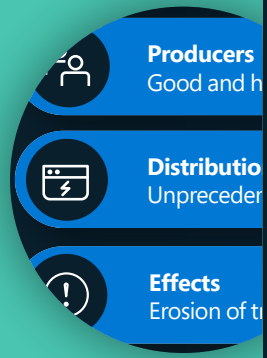
Více se dozvíte na str. 76

Rusko, Írán a Čína často používaly propagandu a ovlivňující kampaně během pandemie covidu-19. Byl to pro ně strategický prostředek, jak dosáhnout širších politických cílů.



Více se dozvíte na str.76

Syntetická média jsou k vidění stále častěji, protože se snadno šíří nástroje, které bez námahy vytvářejí a rozšiřují velmi realistické umělé obrázky, videa a zvuk. Jako prostředek pro boj se zneužíváním vypadá slibně technologie digitálního původu, která certifikuje původ mediálních materiálů.



Více se dozvíte na str. 80

Holistický přístup k ochraně před operacemi ovlivňování v kyberprostoru

Microsoft staví na své už nyní vyspělé infrastruktuře pro zjišťování kybernetických hrozeb a bojuje s operacemi ovlivňování v kyberprostoru. Naší strategií je zjišťovat kampaně propagandy cizích agresorů, narušovat je, bránit před nimi a odrazovat od jejich používání.

Více se dozvíte na str. 83

Úvod

Aby demokracie vzkvétala, potřebuje důvěryhodné informace. Klíčovou oblastí, na kterou se Microsoft zaměřuje, jsou operace ovlivňování, které vyvíjejí a provozují národní státy. Tyto kampaně podkopávají důvěru, podporují polarizaci a ohrožují demokratické procesy.

Zahraniční operace ovlivňování vždy představovaly hrozbu informačnímu ekosystému. Co se však v době internetu a sociálních médií změnilo, je značně větší rozsah, měřítko a efektivita kampaní, které teď můžou mít obrovský dopad na stav globálního informačního ekosystému.

Staré rčení praví, že lež procestuje půlku světa, než si pravda stihne nazout boty, a dnes přesně totéž platí pro data. Studie z Massachusetts Institute of Technology (MIT)[1] zjistila, že nepravdy mají o 70 % větší pravděpodobnost, že budou retweetovány, než pravda. K prvním 1500 lidem se dostanou šestkrát rychleji. Informační ekosystém je méně a méně přehledný, protože na internetu a sociálních médiích se daří kampaním propagandy, které podrývají důvěru v tradiční zpravodajství. Ve studii z roku 2021[2] pouze sedm procent amerických dospělých řeklo, že mají „velkou“ důvěru v novinové, televizní a rádiové zpravodajství, zatímco 34 procent odpovědělo, že nemají „vůbec žádnou“.

Microsoft pracuje na identifikaci hlavních aktérů, hrozeb a taktik v prostředí ovlivňování kyberprostoru v zahraničí a o získané poznatky se dělí. Letos v červnu jsme publikovali ucelenou zprávu o nových zjištěních z Ukrajiny, která obsahovala podrobné informace o ruských operacích ovlivňování v kyberprostoru.[3]

Dále studujeme, jak se dají pokročilé technologie, třeba deepfake, používat jako zbraň a jak podkopávají důvěryhodnost novinářů. A spolupracujeme s průmyslem, státní správou a akademickým sektorem na vývoji lepších způsobů, jak detekovat syntetická média a obnovit důvěru – třeba pomocí systémů umělé inteligence (AI), které dokáží rozpoznat podvrhy.

Rychle se měnící povaha informačního ekosystému a online propagandy národních států, včetně spojování tradičních kybernetických útoků s operacemi ovlivňování a vměšování do demokratických voleb, vyžaduje celospolečenský přístup ke zmírňování online a offline hrozeb pro demokracii.

Microsoft je odhodlán podporovat zdravý informační ekosystém, ve kterém prospívají důvěryhodné zprávy a informace. Vyvíjíme nástroje a funkce pro detekci hrozeb, které pomůžou v boji proti stále většímu a vyvíjejícímu se riziku operací ovlivňování řízených národními státy. Abychom se této činnosti mohli věnovat, získali jsme nedávno společnost Miburo Solutions a spolupracujeme s validátory třetích stran, třeba s organizacemi Global Disinformation Index a NewsGuard. Dále se účastníme, a někdy i vedeme, partnerství více účastníků, jako je asociace Coalition for Content Provenance and Authenticity (C2PA). Jen spolupráce nám může přinést úspěch v boji proti těm, kdo chtějí podrýt demokratické procesy a instituce.

Teresa Hutson

Vice President, Technology and Corporate Responsibility

Trendy v operacích ovlivňování v kyberprostoru

Operace ovlivňování v kyberprostoru jsou stále důmyslnější. Odpovídá to rychlosti, s jakou se vyvíjí technologie. Sledujeme překrývání a rozšiřování nástrojů, které se používají při tradičních kybernetických útocích a teď i v operacích ovlivňování v kyberprostoru. Dále pozorujeme větší koordinaci a zesílení mezi národními státy.

Microsoft tento rok investoval do boje se zahraničními operacemi ovlivňování akvizicí společnosti Miburo Solutions, která se specializuje na analýzu operací ovlivňování na cizím území. Spojením těchto analytiků s analytiky kontextu hrozeb Microsoftu vzniklo v Microsoftu centrum Digital Threat Analysis Center (DTAC). DTAC analyzuje a píše zprávy o hrozbách národních států, mezi které patří kybernetické útoky a operace ovlivňování, kombinuje informace a analýzu hrozeb s geopolitickou analýzou, čímž nabízí přehledy a poskytuje informace o účinných reakcích a ochranách.

Více než tři čtvrtiny lidí po celém světě vyjádřilo své obavy o využívání informací jako zbraně[4] a z našich dat vyplývá oprávněnost těchto obav. Microsoft a jeho partneři sledovali, jak aktéři národních států používají operace ovlivňování k dosažení svých strategických a politických cílů. Kromě ničivých kybernetických útoků a pokusů o kybernetickou špionáž autoritativní režimy stále více využívají operace ovlivňování v kyberprostoru, kterými utvářejí mínění, diskreditují protivníky, podněcují strach, podporují vzdor a deformují realitu.

Tyto zahraniční operace ovlivňování v kyberprostoru mají obvykle tři fáze:

Příprava pozice

Stejně jako příprava pozice malwaru v počítačové síti nějaké organizace zahraniční operace ovlivňování v kyberprostoru připravují falešné příběhy ve veřejném internetovém prostoru. Taktika přípravy pozice už dlouho pomáhá při tradičních kybernetických aktivitách, obzvláště pokud správci IT kontrolují nejnovější aktivitu v síti. Malware, který dlouhou dobu zůstává v síti nečinný, může být při svém následném použití účinnější. Falešné příběhy, které na internetu zůstávají bez povšimnutí, můžou působit důvěryhodněji, až se na ně začne odkazovat v budoucnu.

Zahájení

Často je ve chvíli, kdy je pro aktéra nejvhodnější doba dosáhnout svých cílů, spuštěna koordinovaná kampaň, která šíří příběhy prostřednictvím státem podporovaných a ovlivněných mediálních kanálů a sociálních médií.

Zesílení

Národním státem řízená média a předsunuté kanály nakonec zesílí příběhy u cílových skupin. Dosah takových příběhů je často nevědomě rozšířen i technickými prostředky. Například online reklama může pomoct financovat aktivity a koordinované systémy pro doručování obsahu dokáží zaplavit vyhledávače.

Tento třífázový postup byl využit ke konci roku 2021 na podporu ruského nepravdivého tvrzení o domnělých biologických zbraních a laboratořích na Ukrajině. Toto tvrzení bylo poprvé nahráno na YouTube 29. listopadu 2021 v rámci pravidelného anglicky mluveného pořadu uváděného Američanem žijícím v Moskvě, který tvrdil, že biologické laboratoře financované Spojenými státy mají souvislost s biologickými zbraněmi. Měsíce zůstal tento příběh povětšinou bez povšimnutí. 24. února 2022, kdy ruské tanky překročily hranice, byl do boje vyslán i tento příběh. Tým pro analýzu dat v Microsoftu identifikoval 10 Ruskem řízených nebo ovlivněných zpravodajských webů, které všechny najednou 24. února publikovaly zprávy poukazující na zprávu z loňského roku. Tím se snažily zajistit její důvěryhodnost. Kromě toho představitelé ruského ministerstva zahraničních věcí pořádali tiskové konference, na kterých byla v informačním prostředí dále šířena tvrzení o amerických biologických laboratořích. Ruskem financované týmy pak pracovaly na širším posilování příběhu na sociálních médiích a internetových stránkách.

Vidíme, jak autoritativní režimy po celém světě spolupracují na znečištění informačního ekosystému k jejich vzájemnému prospěchu. Například během pandemie covidu-19 Rusko, Írán a Čína používaly propagandu a operace ovlivňování, při kterých kombinovaly zřejmé, částečně nenápadné a zcela nenápadné způsoby šíření na cílové demokracie a další geopolitické cíle (podrobněji diskutováno na straně 76). Tyto tři režimy si vzájemně přispívaly v ekosystémech pro zasílání zpráv a informací, kde šířily upřednostňované příběhy. Většina obsahu představovala kritiku nebo konspirační teorie o Spojených státech a jejich spojencích, kterou utvrzovali vládní činitelé v oficiálních prohlášeních, když propagovali své vlastní vakcíny a reakce na covid-19 jako účinnější než ty ve Spojených státech a jiných demokraciích. Vzájemným zesilováním mediální kanály provozované státy vytvořily ekosystém, ve kterém byla negativní vyobrazení demokracie – nebo pozitivní vyobrazení Ruska, Íránu a Číny – vytvořená jedním státním mediálním kanálem utvrzena jinými.

Je to ukázka, jak se zprávy o biologických laboratořích a zbraních Spojených států šířily ve třech obsáhlých fázích mnoha zahraničních operací ovlivňování – příprava pozice, zahájení a zesílení.

Trendy v operacích ovlivňování v kyberprostoru

pokračování

Problém je pak o to složitější, že technologické subjekty ze soukromého sektoru mohou tyto kampaně nevědomě umožňovat. Takovými subjekty můžou být společnosti, které registrují internetové domény, hostují weby, šíří obsah na sociálních médiích a vyhledávačích, sdružují provoz a pomáhají platit za tyto činnosti prostřednictvím digitální reklamy. Organizace musí znát nástroje a metody, které autoritativní režimy používají při operacích ovlivňování v kyberprostoru, aby je mohly detekovat. Pak budou moct bránit šíření kampaní. Existuje také rostoucí potřeba pomoct spotřebitelům rozvinout sofistikovanější schopnost identifikovat zahraniční operace ovlivňování a omezit zapojení do jejich příběhů nebo obsahu.

Operace ovlivňování v kyberprostoru, včetně autoritářské propagandy, jsou hrozbou pro demokracie po celém světě, protože narušují důvěru, rozdělují společnost a ohrožují demokratické procesy.

K větší transparentnosti a pro odhalování a narušování těchto ovlivňujících kampaní je zapotřebí intenzivnější koordinace a sdílení informací mezi státními správami, soukromým sektorem a občanskou společností.

Po celém světě se více než tři čtvrtiny lidí obávají využití informací jako zbraní.

Operace ovlivňování během covidu-19 a invaze Ruska na Ukrajinu

Národní státy, které chtěly v průběhu pandemie a během ruské invaze na Ukrajinu získat kontrolu nad informačním prostředím, jsou zářným příkladem, jak autoritativní režimy spojují kybernetické a informatické operace.

Propaganda ke covidu-19

Rusko, Írán a Čína využívaly v době pandemie covidu-19 propagandu a ovlivňující kampaně. Covid-19 se v těchto kampaních objevoval jako hlavní téma dvěma ústředními způsoby:

1. Reprezentací samotné pandemie
2. Kampaněmi, které používaly covid-19 jako strategický prostředek k dosažení širších politických cílů

Široký cíl těchto typů kampaní má dvojí účel: zaprvé podkopat demokracie, demokratické instituce a veřejné mínění o Spojených státech a jeho spojencích na globální scéně a zadruhé posílit své vlastní postavení doma i v zahraničí.

Příkladem můžou být zprávy známých ruských účtů a mediálních organizací, které cílí na anglicky mluvící čtenáře, v porovnání s tím, jak ruská státní správa komunikovala se svými vlastními občany v souvislosti s očkováním a závažností covidu-19.

Témata, kterými se zabývá 10 nejčtenějších článků o koronaviru na webu RT.com
(říjen 2021 – duben 2022)

Propaganda proti očkování cílí na neruské čtenáře

Rusky (níže přeloženo do češtiny)	Čeština
„Lockdowny a posilovací dávky zabraňují šíření“	„Očkování nedokáže zamezit šíření a je neúčinné proti novým kmenům“
„Ruští veřejní činitelé mají pozitivní testy“	„Očkování Pfizeru má nebezpečné vedlejší účinky“
„V Rusku roste počet případů a úmrtí“	„Hromadné očkování je motivováno politikou“
„Vakcína Sputnik V je vysoce efektivní“	„Pfizer a Moderna provádějí neregulované testy“
„Ve veřejné dopravě je vyžadován doklad o očkování“	

Zprávy Ruska o covidu-19 se liší podle jazyka.

Jiným příkladem jsou kampaně, které se pokoušely zastřít původ viru covid-19. Od začátku pandemie si ruská, íránská a čínská propaganda ke covidu-19 vzájemně pomáhaly v šíření obsahu, aby zdůraznily význam těchto ústředních témat. Většina tohoto obsahu sestávala z propagace kritiky nebo konspiračních teorií o Spojených státech. Pravidelným vzájemným zesilováním státní mediální kanály vyvinuly ekosystém, ve kterém byla negativní vyobrazení demokracie – nebo pozitivní vyobrazení Ruska, Íránu a Číny – vytvořená jedním státním mediálním kanálem opakovaně utvrzována jinými.

Příkladem může být brzký návrh ruských a íránských státních médií, že covid-19 by mohl být biologickou zbraní vytvořenou Spojenými státy. Toto tvrzení kolovalo na okrajových konspiračních webech v počátečních fázích pandemie po rozhovoru s profesorem práv, který tvrdil, že věří, že covid-19 byl vytvořen jako zbraň.[6] Po zveřejnění rozhovoru na několika webech s omezeným dosahem příběh zachytily mediální kanály vlastněné státy. PressTV, íránský anglicko-francouzský kanál financovaný íránskou státní správou,[7] zveřejnila v únoru 2020 příběh v angličtině s názvem Is coronavirus a US biowarfare weapon as Francis Boyle believes? (Je koronavirus biologickou zbraní USA, jak se domnívá Francis Boyle?). V článku bylo naznačováno, že Spojené státy stojí za vypuknutím covidu-19: „Ve všech válkách USA jsou používány radiologické, chemické, biologické a jiné zakázané zbraně, které mají na lidi v cílových oblastech ničivé následky.“[8] Ruské státní mediální kanály a čínská vláda tento postoj vyjádřily také. Stanice Russia Today (RT) – státem vlastněný kanál známý pro svou roli při šíření kremelské propagandy[9] – publikovala nejméně jeden příběh, který přebíral vyjádření íránských úředníků. Ti tvrdili, že covid-19 může být „výsledkem biologického útoku USA cíleného na Írán a Čínu“[10]. Takové náznaky pak stanice vypouštěla v příspěvcích na sociálních médiích. Například tweet RT z 27. února 2020 obsahoval zprávu, „ať zvedne ruku ten, kdo by nebyl překvapený, kdyby se zjistilo, že #coronavirus je biologická zbraň.“[11]

Válka na Ukrajině – propaganda jako válečná zbraň

Ruská invaze na Ukrajinu je příkladem toho, jak se operace ovlivňování v kyberprostoru dají spojit s tradičnějšími kybernetickými útoky a pozemními vojenskými operacemi s cílem maximalizovat jejich dopad.

V době před invazí na Ukrajinu analytici hrozeb v Microsoftu zaznamenali nejméně šest samostatných aktérů spolupracujících s Ruskem, jak provedli více než 237 kybernetických útoků na Ukrajinu. Tyto kampaně usilovaly o omezení služeb a institucí, narušení přístupu Ukrajinců ke spolehlivým informacím a zakořenění pochybností o vedení země.

Operace ovlivňování během covidu-19 a invaze Ruska na Ukrajinu

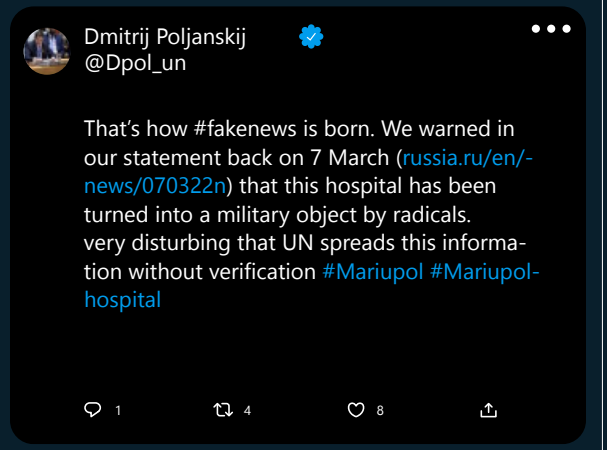
pokračování

Ve zprávě Microsoftu vydané v dubnu 2022 jsme ukázali, jak Rusko při zřejmém pokusu získat kontrolu nad informačním prostředím v Kyjevě zahájilo raketový útok na kyjevskou televizní věž ve stejný den, kdy zároveň vypustilo ničivý malware na velké ukrajinské mediální společnosti.[12]

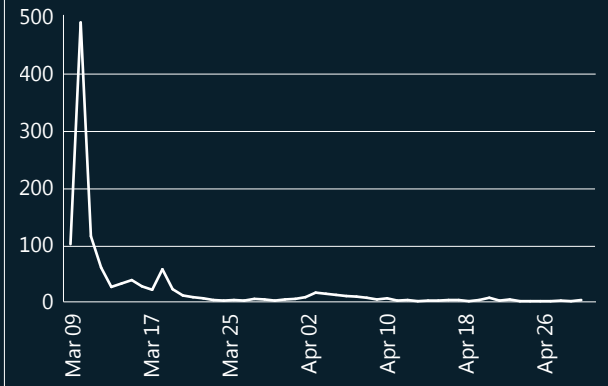
V další ukázce, jak se k sobě přibližují kybernetické útoky a operace ovlivňování, ruský aktér hrozeb poslal ukrajinským občanům e-maily, které údajně pocházely od obyvatel Mariupolu a obviňovaly ukrajinskou vládu z eskalace válečného konfliktu. Vyzývaly krajany, aby se vzbouřili proti vládě. Tyto e-maily byly zasílány adresně (jmenovitě) na ty, kteří je obdrželi. To naznačuje, že jejich údaje mohly být ukradeny již při dřívějším špionážním kybernetickém útoku. V e-mailech se nenacházely žádné škodlivé odkazy, z čehož plyne, že byly součástí jen operací ovlivňování.

Využívání údajně hacknutého, uniklého nebo jinak citlivého materiálu je běžnou taktikou, kterou ruští aktéři používají při operacích ovlivňování. V průběhu války na Ukrajině proruské kanály sociálních médií šířily něco, o čem tvrdily, že to jsou uniklé nebo jinak citlivé materiály z ukrajinských zdrojů. Proruské kanály sociálních médií a zdroje používají uniklé nebo citlivé materiály v rámci širší strategie ovlivňování, jejímž cílem je narušit důvěru v instituce a zpochybnit příběhy pro širokou veřejnost. Tyto informace se dají zkreslit tak, aby z nich vznikla propaganda cílená na Ukrajinu a Západ, aby narušila důvěru v digitální zabezpečení a oslabila podporu západní pomoci Ukrajině.

Po událostech, které se odehrály na zemi, Rusko využilo další útoky na informace, aby utvářelo veřejné mínění a zakrylo nebo podkopávalo fakta. Například 7. března Rusko připravilo příběh zaslaný Organizaci spojených národů (OSN), že porodnice v ukrajinském Mariupolu byla evakuována a využita jako vojenský objekt. 9. března Rusko nemocnici bombardovalo. Jakmile vyšly o tomto bombardování zprávy, ruský diplomat při OSN Dmitrij Poljanskij zveřejnil tweet, že záběry z bombardování byly falešné zprávy, a citoval dřívější tvrzení Ruska o údajném využití jako vojenského objektu. Rusko tehdy svou verzi dva týdny po útoku na nemocnici šířilo prostřednictvím Ruskem ovládaných webů.



Domény s provozem
(9. března 2022 – 30. dubna 2022)



Propagační webové stránky přibližně dva týdny publikovaly příběhy o porodnici, ke kterým se počínaje 1. dubnem 2022 na chvíli vracely. Zdroj: Microsoft AI for Good Lab

Satelitní snímky porodnice v Mariupolu v únoru a březnu 2022

Analýza vlastních satelitních snímků Microsoftu ukazuje, že proběhl bombový útok na porodnici. První fotka pochází z 24. února 2022, druhá pak z 24. března 2022. Zdroj snímků: Planet Labs

I v dalších obdobích války Rusko odmítá přijmout odpovědnost za krutost. Například na konci června 2022 ruské mediální kanály a influenceři vyobrazili bombový útok na nákupní centrum jako oprávněný a nezbytný, když nepravdivě tvrdili, že nebylo používáno jako obchodní centrum, ale jako zbrojnice pro ukrajinské územní obranné síly.[13] Několik proruských blogerů na Telegramu zveřejňovalo a zesilovalo obsah, který utvrzoval příběh o „falešné vlajce". Blogeři poukazovali na údajné indicie falšování, například na přítomnost osob ve vojenských uniformách v záběrech z místa[14] a absenci žen na záznamu.[15] Rusko zahájilo kampaně, s nimiž spoléhalo na připravený systém šiřitelů propagandy a propagačních médií. Zesilování těchto příběhů online přináší Rusku možnost odvrátit vinu na mezinárodní scéně a vyhnout se odpovědnosti.

Národní státy, jako je Rusko, rozumí přínosu informací vyvozených z uzavřených zdrojů, kterými se dá ovlivnit vnímání veřejnosti, a využití kampaní typu hack-and-leak k šíření opačných příběhů a nedůvěry.

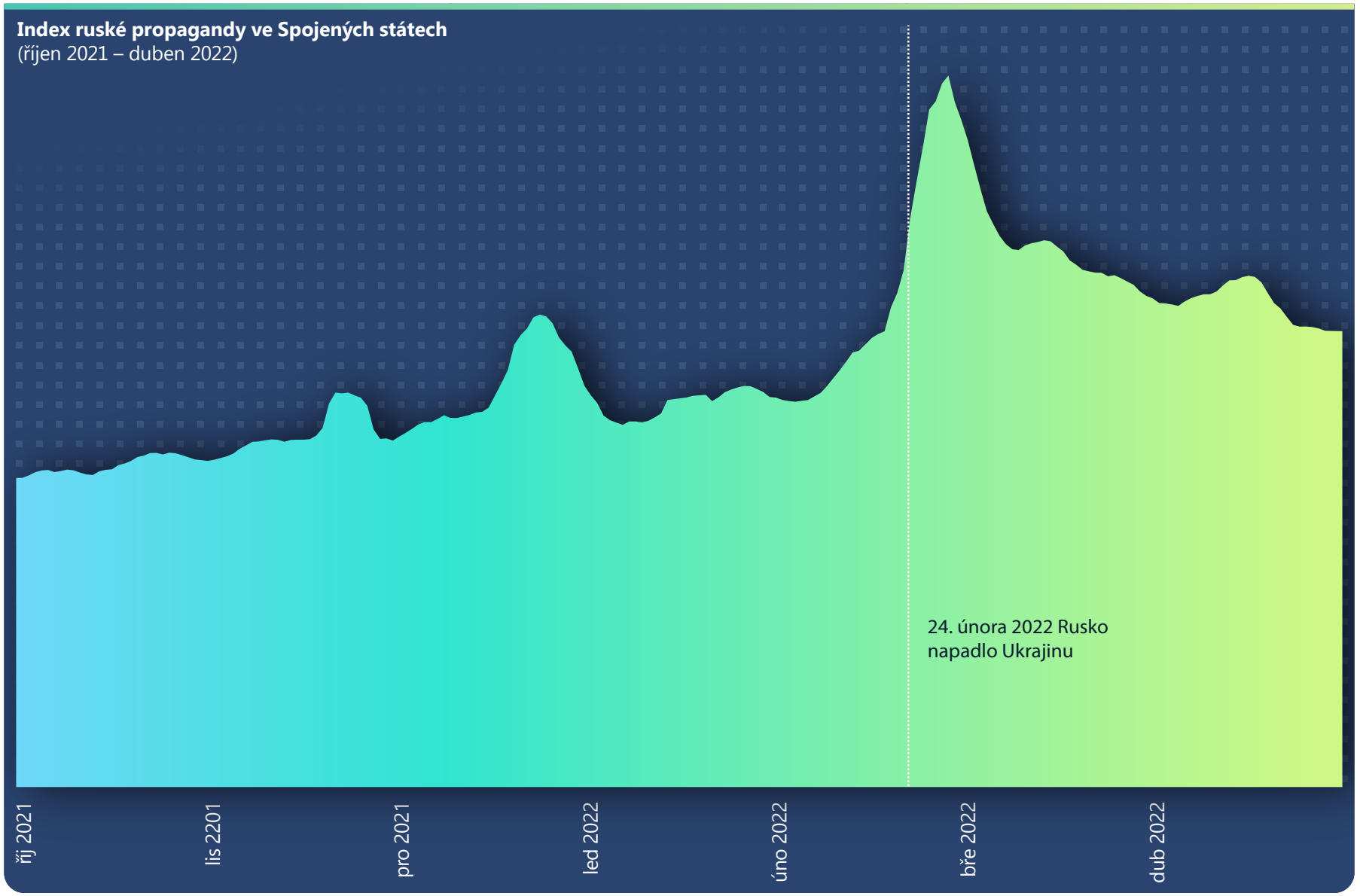
Odkazy na další informace

- Obrana Ukrajiny: První ponaučení z kybernetické války | Microsoft On the Issues
- Přehled ruské aktivity při kybernetických útocích na Ukrajině | Microsoft Special Report
- Narušování kybernetických útoků cílených na Ukrajinu | Microsoft On the Issues

Sledování indexu ruské propagandy

V lednu 2022 téměř tisíc amerických webů přesměrovávalo provoz na ruské propagační weby. Nejčastějšími tématy ruských propagačních webů, které cílily na americké cílové skupiny, byly válka na Ukrajině, domácí politika USA (podporující buď Trumpa, nebo Bidena) a příběhy o covidu-19 a očkování.

Index ruské propagandy (RPI) monitoruje tok zpráv z ruských státem ovládaných a financovaných zpravodajských kanálů a zesilovačů jako podíl na celkovém zpravodajském provozu na internetu. Pomocí RPI se dá do grafu na přesnou časovou osu vykreslit sledování ruské propagandy po celém internetu a v různých geografických oblastech. Microsoft však dodává, že ruskou propagandu můžeme pozorovat jen na dříve identifikovaných webech. Nemáme informace o propagandě na jiných typech webů, mezi které patří zpravodajské weby autoritativních režimů, neidentifikované weby a skupiny na sociálních sítích.



Sledování indexu ruské propagandy

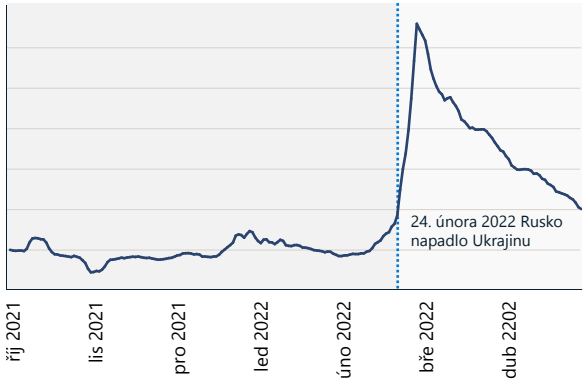
pokračování

Index ruské propagandy: Ukrajina

Když začala válka na Ukrajině, zaznamenali jsme 216procentní nárůst ruské propagandy, který dosáhl svého vrcholu 2. března. Graf níže ukazuje, jak tento náhlý nárůst koresponduje s invazí. Tyto dva grafy ukazují, jak vzrostlo používání ruské propagandy krátce po začátku války.

RPI, Ukrajina

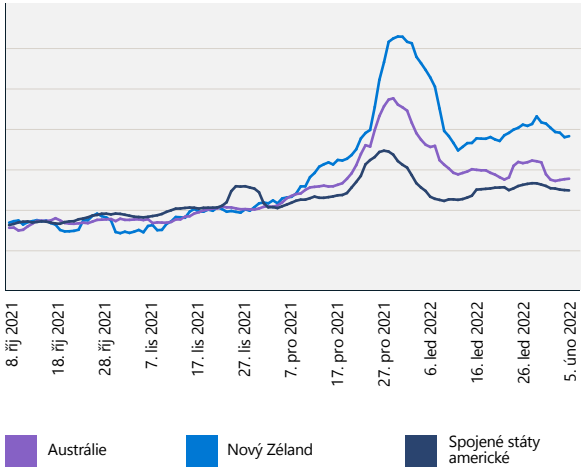
(7. října 2021 – 30. dubna 2022)



Index ruské propagandy: Nový Zéland proti Austrálii a Spojeným státům

Posouzení RPI na Novém Zélandu ukázalo prudký nárůst na konci roku 2021, který souvisel s propagandou ke covidu-19. Po tomto nárůstu sledování ruské propagandy na Novém Zélandu došlo ke zintenzivnění veřejných protestů na začátku roku 2022 ve Wellingtonu. Druhý nárůst jasně souvisel s ruskou invazí na Ukrajinu a překročil RPI Austrálie a Spojených států.

RPI, Nový Zéland proti Austrálii a Spojeným státům



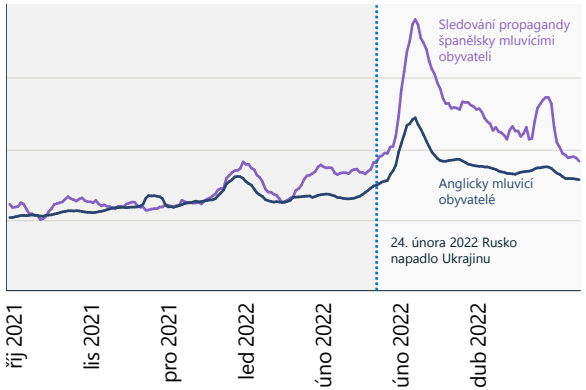
Sledování ruské propagandy na Novém Zélandu je až do prvního týdne prosince roku 2021 podobné tomu v Austrálii. Po prosinci se sledování ruské propagandy na Novém Zélandu zvýšilo ve srovnání se sledováním v Austrálii a Spojených státech o více než 30 procent.

Index ruské propagandy ve Spojených státech: angličtina a španělština

RPI sleduje propagandu i v různých jazycích. Několik kanálů, včetně RT a Sputnik News, je k dispozici ve více než 20 jazycích. Patří mezi ně angličtina, španělština, němčina, francouzština, řečtina, italština, čeština, polština, srbština, lotyšština, litevština, moldavština, běloruština, arménština, osetština, gruzínština, ázerbájdžánština, arabština, turečtina, perština a dari.

Následující graf znázorňuje, že RPI pro španělsky mluvící zpravodajství ve Spojených státech je mnohem vyšší než pro zpravodajství v angličtině.

Sledování ruské propagandy je 2× vyšší mezi španělský mluvícími obyvateli



Sledování ruské propagandy ve Spojených státech je dvakrát vyšší mezi španělsky mluvícími obyvateli.

Ruská propaganda má vysoké zastoupení v Latinské Americe

RT ve španělštině je mezinárodní zpravodajský kanál s nejvyšším počtem zobrazení stránek a sledujících na Facebooku.

Zdroj: Microsoft AI for Good Research Lab

Syntetická média

Vstupujeme do zlaté éry vytváření a manipulací s médií pomocí AI. Analytici Microsoftu poznamenávají, že hnacím motorem jsou dva hlavní trendy: šíření snadno použitelných nástrojů a služeb pro umělou tvorbu vysoce realistických syntetických obrázků, videí, zvuku a textu a možnost rychle šířit obsah optimalizovaný pro konkrétní cílové skupiny.

Žádný z těchto trendů není sám o sobě problematický. Technologie založené na AI se dají využít k vytváření zábavného a zajímavého digitálního obsahu, ať už ve formě čistě umělého, nebo vylepšeného stávajícího materiálu. Firmy tyto nástroje běžně používají pro reklamní a komunikační účely, jednotlivci pak k vytváření poutavého obsahu pro své sledující. Pokud však syntetická média vzniknou a šíří se s cílem způsobit újmu, mají potenciál zanechat na jednotlivcích, společnostech, institucích a veřejnosti závažné škody. Microsoft je hnací silou při vývoji technologií a postupů, a to interně i v širším mediálním ekosystému, které tyto škody mají omezit.

Tato část se zabývá poznatky analytiků Microsoftu o aktuálních nejmodernějších technologiích pro vytváření škodlivého syntetického obsahu, škodami, které může tento obsah způsobit v případě velkého rozšíření, a technickými opatřeními, která pomáhají bránit se před kybernetickými hrozbami založenými na syntetických médiích.

Vytváření syntetických médií

Oblast syntetického textu a médií se neuvěřitelně rychle vyvíjí, protože techniky, které byly dříve realistické jen s obrovskými výpočetními prostředky velkých filmových studií, jsou dnes integrovány do aplikací pro telefony. Zároveň je stále snazší používat nástroje, které dokáží generovat obsah na takové úrovni realismu, že dokáží oklamat i forenzní specialisty na média. Velmi jsme se přiblížili bodu, kdy může kdokoli vytvořit syntetické video, na kterém kdokoli říká nebo dělá cokoli. Není daleko od věci se domnívat, že vstupujeme do éry, kdy značná část obsahu dostupného online bude zcela nebo částečně syntetická díky technikám AI.

> S dostupností sofistikovanějších, snadno použitelných a široce dostupných nástrojů je stále běžnější i vytváření syntetického obsahu, který zanedlouho nepůjde rozeznat od skutečnosti.

Existuje mnoho velmi kvalitních bezplatných i komerčních nástrojů pro úpravu obrázků, videí a zvuku. Tyto nástroje se dají používat k jednoduchým, ale potenciálně škodlivým změnám digitálního obsahu, například k přidání zavádějícího textu, záměně tváří nebo odebrání či změně kontextu. Takové „levné podvrhy" se běžně používají k šíření škodlivého obsahu, propagaci politických ideologií a poškozování pověsti. Dobře známým případem je video z roku 2019,[16] na němž předsedkyně americké Sněmovny reprezentantů Nancy Pelosi pronesla nezřetelně svou řeč a působila opile. Ačkoli bylo rychle zjištěno, že efekt vznikl zpomalením videa, tento „levný podvrh" se rozšířil široko daleko dříve, než se objevily původní video a kontext.

Mezi důmyslnější přístupy k úpravě mediálního obsahu patří využití pokročilých technik AI k (a) vytvoření čistě syntetického média a (b) provedení propracovanějších změn existujícího média. Pro syntetická média vytvořená pomocí špičkových technik AI se často používá pojem deepfake (název je odvozen od hlubokých (deep) neurálních sítí, které se někdy používají). Tyto technologie se vyvíjejí jako samostatné aplikace, nástroje a služby a integrují se do zavedených komerčních a opensourcových editačních nástrojů.

Zlomyslní aktéři tyto technologie používají jako zbraň v naději, že způsobí jednotlivcům a institucím škody. Příkladem technik deepfake může být:

- **Záměna tváří (video, obrázky)** – nahrazení tváře ve videu jinou tváří. Tato technika může sloužit k pokusu o vydírání jednotlivce, společnosti nebo instituce nebo ke vložení jednotlivce na hanebná místa nebo do trapných situací.
- **Loutkaření (video, obrázky)** – využití videa k animaci nepohyblivého obrázku nebo druhého videa. Tato technika může vyvolat dojem, že jednotlivec řekl něco ostudného nebo zavádějícího.
- **Generativní kompetitivní sítě (video, obrázky)** – rodina technik pro generování fotorealistických snímků.
- **Transformační modely (video, obrázky, text)** – vytváření propracovaných obrázků z textových popisů.

Takto pokročilé techniky AI se v současné době ještě nepoužívají běžně při kampaních ovlivňování v kyberprostoru, ale očekáváme, že čím bude nástroje snazší používat a čím snáze dostupné budou, tím bude problém větší.

Dopad manipulace syntetickými médii

Používání informačních operací s cílem způsobit škody nebo rozšířit vliv není novinka. Avšak rychlost, s jakou se informace dokáží šířit, a naše neschopnost rychle odlišit fakta od fikce znamenají, že dopad a škody způsobené podvrhy a dalšími synteticky generovanými škodlivými médii můžou být daleko větší. Poukazuje na to příklad Pelosi.

Existuje několik kategorií škod, které bereme v úvahu: manipulace s trhem, platební podvody, vishing, zosobnění, poškození značky, poškození pověsti a botnety. Pro mnoho z těchto kategorií existují často hlášené příklady z reálného světa, které by mohly narušit naši schopnost rozlišit fakta od fikce.

Pokud už nemůžeme důvěřovat tomu, co vidíme a slyšíme, čelí naše vnímání skutečnosti dlouhodobější a zákeřnější hrozbě. Kvůli tomu může být jakýkoli kompromitující obrázek, zvukový záznam nebo video veřejné nebo soukromé osoby ignorován jako falešný. Tomuto jevu se říká lhářova dividenda.[17] Nedávný výzkum[18] ukázal, že toto zneužívání technologie se už objevuje v útocích na finanční systémy, i když scénářů zneužití je zřejmě daleko více.

Syntetická média

pokračování

Detekce syntetických médií

V průmyslu, ve státních správách i v akademickém prostředí probíhají snahy o vývoj lepších způsobů, jak detekovat a zmírňovat syntetická média a obnovit důvěru. Existuje několik slibných způsobů, ale i překážek, které stojí za zvážení.

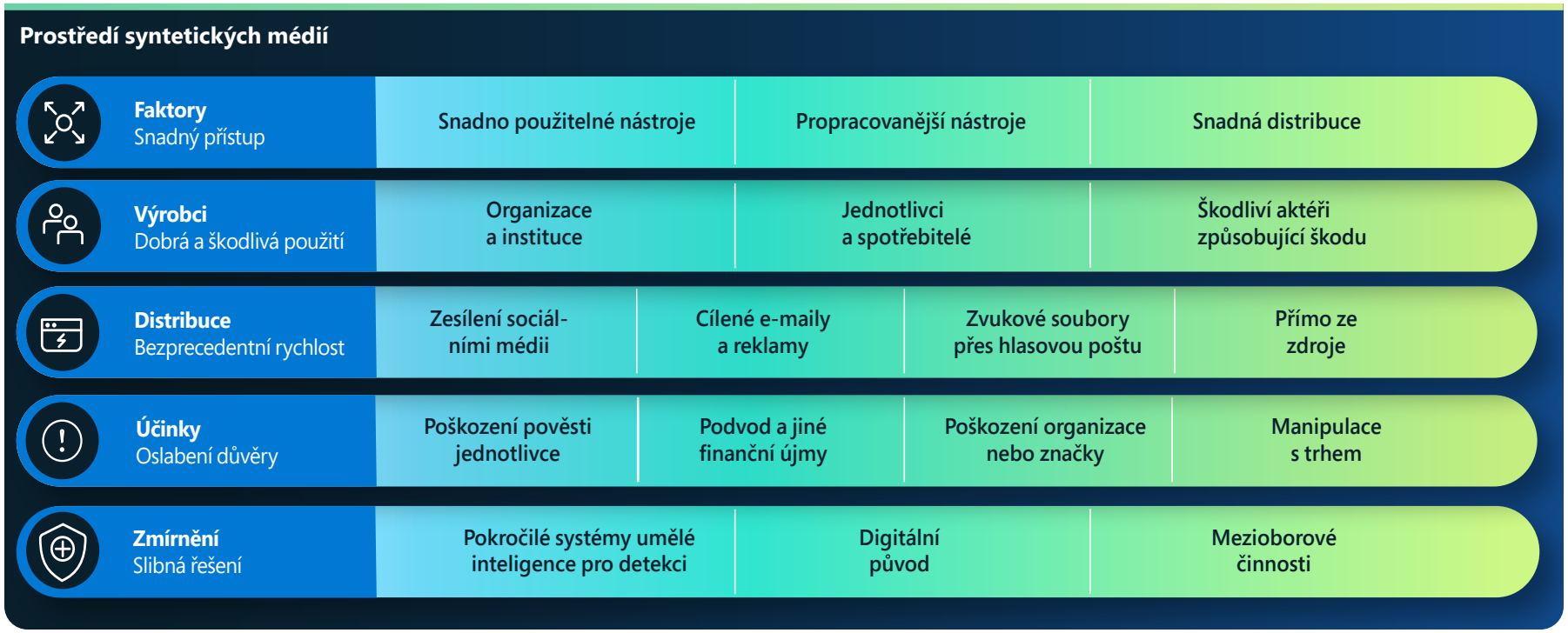
Jedním ze způsobů je vytvořit systémy založené na AI, které dokáží rozpoznat podvrhy – v podstatě „obranné" systémy AI, které budou bojovat proti útočným systémům AI. Toto je stále aktivní oblast výzkumu, kde aktuální systémy pro vytváření syntetického zvuku a videa zanechávají výmluvné artefakty. Ty dokážou odhalit zkušení forenzní analytici médií a automatizované nástroje.

Naneštěstí, i když aktuální podvrhy mají zřetelné nedostatky, konkrétní artefakty bývají specifické pro určitý nástroj nebo algoritmus. To znamená, že trénování na známých podvrzích obvykle nenabídne zobecnění na další algoritmy.

To ukázala otevřená soutěž z roku 2020, ve které bylo za úkol vytvořit detektory deepfake obrázků.[19] Je lákavé navýšit investice do vývoje pokročilejších detektorů, ale Microsoft je velmi skeptický ohledně smysluplných vylepšení, a to ze dvou důvodů:

Zaprvé, máme vynikající fyzické modely, které odrážejí skutečný svět. V současné době si autoři podvrhů usnadňují práci, což vede ke zjistitelným artefaktům, ale novější modely jsou stále realističtější. Na skutečné scéně zachycené kamerami není v zásadě nic natolik zvláštního, aby se to nedalo modelovat počítačem.

Zadruhé, pokročilé algoritmy pro vytváření podvrhů používají ve svém tvůrčím procesu techniku jménem generativní kompetitivní sítě (GAN). GAN proti sobě spouští dva systémy AI. Pomocí generátoru vytváří podvrh a diskriminátorem se detekují falešné obrázky pro trénování generátoru. Jakákoli investice do vývoje lepšího detektoru pouze umožní generátoru zlepšit kvalitu podvrhů.



Syntetická média

pokračování

Původ pro digitální prostředky

Pokud je detekce podvrhů nespolehlivá, co se dá udělat pro ochranu před škodlivým využitím syntetických médií? Jednou z důležitých vyvíjených technologií je digitální původ – mechanismus, který umožňuje autorům digitálních médií certifikovat prostředek a pomáhá uživatelům identifikovat, jestli bylo s digitálním prostředkem manipulováno. Digitální původ je obzvláště důležitý v kontextu dnešních sítí sociálních médií s ohledem na rychlost, jakou se obsah dokáže šířit internetem, a příležitosti ke snadné manipulaci s obsahem ze strany zlomyslných aktérů.

900%

meziroční nárůst šíření deepfake obsahu od roku 2019[20]

Technologie digitálního původu je moderní verze kryptografického podepisování dokumentů navržená k zaznamenávání zdroje, historie úprav a metadat objektů přenášených dnešním webem. Vize a technické způsoby, jak tento typ komplexní certifikace médií odolné proti manipulaci umožnit, vyvinuly společné týmy výzkumníků a vědců v Microsoftu. Podílíme se na vedení mezioborového partnerství zaměřeného na uvedení technologie původu médií do praxe v projektu s názvem Project Origin (založen společnostmi Microsoft, BBC, CBC/Radio-Canada a New York Times) a zapojujeme se do iniciativy Content Authenticity Initiative (založené společností Adobe). Microsoft navíc spolupracoval s partnery v oblasti technologií a mediálních služeb na založení asociace Coalition for Content Provenance and Authenticity (C2PA). C2PA je standardizační organizace, která nedávno publikovala nejpokročilejší specifikaci digitálního původu, kterou lze využít pro mediální prostředky, včetně obrázků, videí, zvuku a textu.

Objekt podporující C2PA obsahuje manifest, který chrání objekt a metadata před manipulací, a průvodní certifikát identifikuje vydavatele.

Syntetická média původně nebyla určena k šíření škod, ale zlomyslní aktéři je používají jako zbraň, kterou podkopávají důvěru v jednotlivce a instituce.

Digitální původ je slibná vyvíjející se technologie, která má potenciál pomoct obnovit důvěru obyvatel v online mediální obsah certifikací původu mediálního prostředku.

Veřejně dostupná řešení, která se zakládají na specifikaci C2PA, se objevují buď jako nová funkce ve stávajících produktech, nebo jako nové samostatné aplikace a služby. Očekáváme, že do několika let bude C2PA podporovat většina běžně používaných nástrojů pro nahrávání, úpravy a tvorbu obsahu. Vzniká tak příležitost, aby firmy už dnes stanovily své potřeby a možná využití digitálního původu a aby vyžadovaly tuto další úroveň ochrany v nástrojích, které používají ve stávajících pracovních postupech.

Poznatky a jejich využití

1. Buďte aktivní při ochraně organizace před hrozbami dezinformací a zvažujte aktivně reakce v PR a při komunikaci.
2. Chraňte oficiální komunikace pomocí technologie původu.

Odkazy na další informace

- Slibný krok vpřed v oblasti dezinformací | Microsoft On the Issues
- Dosažený milník, 31. ledna 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Průzkum technických podrobností o využití systému Project Origin k ověřování médií | Microsoft ALT Innovation

Holistický přístup k ochraně před operacemi ovlivňování v kyberprostoru

Microsoft staví na své již vyspělé infrastruktuře pro získávání informací o kybernetických hrozbách a vyvíjí širší, obsáhlejší pohled na operace ovlivňování v kyberprostoru.

Používáme architekturu, s jejíž pomocí navrhujeme strategie reakcí a zmírňování v boji proti hrozbám ze strany operací. Tyto strategie se dají rozdělit na čtyři hlavní pilíře: detekce, narušení, obrana a odrazování.

Kromě toho Microsoft přijal za své čtyři principy, které se staly základem jeho práce v této oblasti. Prvním z nich je závazek respektovat svobodu projevu a zachovat našim zákazníkům možnost vytvářet, publikovat a hledat informace na našich platformách, v produktech a službách. Dále aktivně pracujeme na obraně našich platforem a produktů před využitím k zesilování webů a obsahu sloužících k šíření cizího vlivu v kyberprostoru. Třetím závazkem je, že z obsahu nebo činnosti aktérů šířících cizí vliv v kyberprostoru nebudeme vědomě profitovat. A nakonec upřednostňujeme zpřístupňování obsahu, který umožňuje čelit operacím ovlivňování v kyberprostoru. Využíváme k tomu interní a důvěryhodná data třetích stran o našich produktech.

Detekce

Stejně jako v případě kybernetické obrany je prvním krokem v boji proti cizím operacím ovlivňování v kyberprostoru vývoj schopnosti je detekovat. Žádná společnost ani organizace není schopna samostatně dosáhnout potřebného pokroku. Stěžejní bude nová, širší spolupráce v celém technologickém odvětví. Pokrok v analýzách a hlášení operací ovlivňování v kyberprostoru bude značně spoléhat na roli občanské společnosti, včetně akademických institucí a neziskových organizací.

Výzkumníci Jake Shapiro a Alicia Wanless z Princetonské univerzity a organizace Carnegie Endowment for International Peace jsou si této role vědomi a prozkoumali plány na vytvoření nové instituce s názvem Institute for Research on the Information Environment (IRIE). S podporou Microsoftu, nadace Knight Foundation a organizace Craig Newmark Philanthropies IRIE vytvoří inkluzivní výzkumnou instituci s mnoha účastníky, pro kterou byla vzorem Evropská organizace pro jaderný výzkum (CERN). Bude kombinovat odbornost ve zpracování a analýze dat a zvýší nejen rychlost nových objevů v této oblasti, ale i jejich rozsah. Poznatky budou obsáhleji sdíleny s tvůrci zásad, technologickými společnostmi a spotřebiteli.

Obrana

Druhým strategickým pilířem je posílit obranné mechanismy demokracie. To je dlouhodobou prioritou, která vyžaduje investice a inovace. Tento pilíř by se měl zaměřit na výzvy pro demokracii, které technologie vytvořila, a příležitosti, které technologie přináší při účinnější obraně demokratických společností.

Architektura strategie Microsoftu se zaměřuje na pomoc mezioborovým účastníkům detekovat a narušovat propagandu, bránit se před ní a odrazovat od ní, především pak od kampaní cizích agresorů.

Je vhodné začít jedním z největších technologických problémů dnešní doby – dopadu internetu a digitální reklamy na tradiční žurnalistiku. Od 18. století měl svobodný a nezávislý tisk zvláštní roli při podpoře všech demokracií na planetě – odhaloval totiž korupci, dokumentoval války a vrhal světlo na největší problémy společnosti této i kterékoli jiné doby. Internet však pro místní zpravodajství představuje značnou překážku, protože pohltil výnosy z reklamy a odlákal předplatitele. Mnoho místních novin přestalo existovat. Jedním z mnoha poznatků z naší nedávné práce je, že města, ve kterých nejsou k dispozici noviny, jsou nevědomky a nevyhnutelně vystavena více než průměrnému objemu cizí propagandy. Z těchto důvodů musí být jedním z nejdůležitějších bodů obrany demokracie posílení tradiční žurnalistiky a svobodného tisku, obzvláště na místní úrovni. To si žádá průběžné investice a inovace, které musí zohledňovat místní požadavky různých zemí a kontinentů. Tyto problémy nejsou jednoduché a vyžadují přístupy s více účastníky. Tyto přístupy Microsoft a jiné technologické společnosti podporují stále více.

Kromě toho potřebujeme inovace v oblasti veřejné politiky, která se musí stát veřejnou prioritou. Její součástí můžou být zákony, které umožní vydavatelům kolektivně vyjednávat o výnosech z reklamy s technologickými společnostmi, a legislativa umožňující daňové úlevy, které místní zpravodajské domy uplatní na část daňového zatížení jimi zaměstnaných novinářů. Novináři potřebují pro své řemeslo spoustu dalších nástrojů, například možnost rozlišit obsah z legitimních a podvodných zdrojů.

Velmi rychle se také vyvíjí nutnost pomoct zákazníkům rozvinout schopnost identifikovat informační operace řízené národními státy. Může se to zdát jako velmi náročný úkol, dost se to ale podobá činnostem, kterými se technologický sektor už dlouho zabývá při boji s jinými kybernetickými hrozbami. Představte si, že by byli spotřebitelé vzděláváni tak, aby se pozorněji dívali na e-mailovou adresu a snadněji tak odhalili spam nebo jiné podvodné komunikace. Tím se zabývají některé iniciativy ve Spojených státech – například News Literacy Project a Trusted Journalism

Pokud už nemůžeme důvěřovat tomu, co vidíme a slyšíme, čelí naše vnímání skutečnosti dlouhodobější a zákeřnější hrozbě.

Holistický přístup k ochraně před operacemi ovlivňování v kyberprostoru

pokračování

Program – a pomáhají u spotřebitelů rozvíjet lepší povědomí o novinkách a informacích. Na celém světě můžou technologie jako modul plug-in prohlížeče společnosti NewsGuard pomoct daleko rychleji posouvat toto úsilí vpřed.

Mělo by nám to také připomenout, že základem demokracie je i vzdělání v oblasti občanské výchovy. Jako vždy musí toto úsilí začít už ve školách. Žijeme však ve světě, který vyžaduje, abychom byli vzděláváni jako občané celoživotně. Nový závazek iniciativy Civics at Work, kterou vede centrum Center for Strategic and International Studies a pro kterou byl Microsoft zakládajícím signatářem a partnerem, má za cíl obnovit občanskou gramotnost ve firemních komunitách. Je to dobrá ukázka toho, jak velká je příležitost posílit naši demokratickou obranu.

Narušení

V posledních letech tým Digital Crimes Unit (DCU) v Microsoftu zdokonalil taktiku a vyvinul nástroje, jak narušovat kybernetické útoky od ransomwaru po botnety a útoky národních států. Získali jsme mnoho důležitých poznatků, od důležitosti aktivního narušování až po boj s rozsáhlými kybernetickými útoky.

Když přemýšlíme o způsobech, jak bojovat s operacemi ovlivňování v kyberprostoru, narušování může hrát ještě důležitější roli a nejlepší přístup k němu začíná být zřetelnější. Tou nejúčinnější protilátkou rozsáhlého klamání je transparentnost. Proto Microsoft posílil svou schopnost detekovat a narušovat operace ovlivňování ze strany národních států akvizicí společnosti Miburo Solutions, přední společnosti zabývající se analýzou a výzkumem kybernetických hrozeb. Ta se specializuje na detekci zahraničních operací ovlivňování v kyberprostoru a reakce na ně.

Naše zkušenosti ukazují, že státní správy, technologické společnosti a nevládní organizace by měly přisuzovat kybernetické útoky konkrétním činitelům opatrně a s velkým množstvím důkazů. Velice důležité je pochopit dopad takového narušení. Pak takové porozumění může být ještě užitečnější při narušování ovlivňování v kyberprostoru. Příkladem může být sdílení informací ze strany americké vlády krátce před invazí Ruska na Ukrajinu, která transparentnost uvedla do praxe – třeba odhalení ruských plánů, včetně konkrétních kampaní jako záměr použít falešné grafické video.

Jak bylo patrné v publikaci ženevského institutu CyberPeace Institute z minulého léta o probíhajících kybernetických útocích na Ukrajině i mimo ni, existuje příležitost, jak spousta organizací občanské společnosti a soukromého sektoru může přispět k transparentnosti v souvislosti s operacemi ovlivňování v kyberprostoru. Spolehlivé zprávy o nově zjištěných a dobře zdokumentovaných operacích můžou veřejnosti pomoct lépe vyhodnotit, co čte, vidí a slyší, obzvlášť na internetu. S tímto cílem Microsoft využije stávající zprávy o kyberprostoru, rozšíří je a vydá nové zprávy, data a aktualizace o nových zjištěních k operacím ovlivňování v kyberprostoru. Součástí budou i prohlášení o činitelích, budou-li vhodná. Budeme publikovat každoroční zprávy, které přístupem založeným na datech budou zkoumat výskyt cizích informačních operací v celé firmě a další kroky, jak zajistit postupné zlepšení. Budeme zvažovat i další kroky, které z tohoto typu transparentnosti budou vycházet.

Obzvláště důležitou roli hraje například digitální reklama, protože reklamní sdělení můžou pomoct financovat cizí operace a zároveň vytvářet dojem pravosti propagačních webů podporovaných ze zahraničí. K narušení těchto finančních toků bude zapotřebí nových přístupů.

Odrazování

A nakonec, nemůžeme očekávat, že státy změní chování, pokud za porušování mezinárodních pravidel nebudou vedeny k odpovědnosti. Prosazování takové odpovědnosti patří do rukou výhradně státním správám. I přesto mají stále silnější vliv činnosti asociací s více účastníky, které hrají důležitou roli při upevňování a rozšiřování mezinárodních norem. Více než 30 online platforem, inzerentů a vydavatelů, včetně Microsoftu, podepsalo nedávno aktualizovaný Kodex zásad boje proti dezinformacím vydaný Evropskou komisí a souhlasilo s posílením závazků řešit tuto stále větší výzvu. Stejně jako v poslední době Paris Call, Christchurch Call a Prohlášení o budoucnosti internetu můžou aktivity asociací více účastníků spojit státní správy a veřejnost demokratických zemí. Pak budou moct státní správy využít tyto normy a zákony k prosazování odpovědnosti, kterou světové demokracie potřebují a zasluhují.

Rychlou a prudkou transparentností můžou demokratické státní správy a společnosti účinně oslabit kampaně ovlivňování tím, že stanoví zdroj útoků ze strany národních států, informují veřejnost a budou budovat důvěru v instituce.

> Rozšířili jsme naše technické možnosti, jak detekovat a narušovat zahraniční operace ovlivňování, a zavázali jsme se transparentně oznamovat tyto operace, podobně jako teď oznamujeme kybernetické útoky.

Poznatky a jejich využití

1. V celé organizaci zaveďte důsledné postupy digitální hygieny.
2. Zvažte způsoby, jak omezit neúmyslnou podporu kampaní ovlivňování v kyberprostoru zaměstnanci nebo obchodními postupy. Sem patří omezení zdrojů známých webů šířících cizí propagandu.
3. Podpořte informační gramotnost a kampaně občanské angažovanosti jako prioritu, která pomůže společnostem bránit se propagandě a cizím vlivům.
4. Spolupracujte napřímo se skupinami z vašeho oboru na řešení operací ovlivňování.

Poznámky na závěr

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. Obrana Ukrajiny: První ponaučení z kybernetické války (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Mluvčí ruského ministerstva zahraničí Marija Zacharovová: 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 a Kristjan Peterson, říjen 2020

Kybernetická odolnost

Porozumění rizikům a přínosům modernizace začíná být stěžejní pro holistický přístup k odolnosti.

Přehled

kybernetické odolnosti

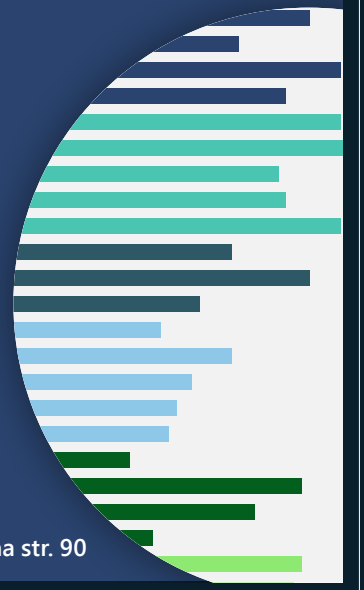
Kybernetické zabezpečení je stěžejní prvek technologického úspěchu. Inovací a vyšší produktivity je možné dosáhnout jen zavedením bezpečnostních opatření, s nimiž budou organizace co nejodolnější vůči moderním útokům.

Pandemie pro nás představovala výzvu, jak upravit postupy a technologie zabezpečení tak, aby chránily zaměstnance Microsoftu bez ohledu na místo, odkud pracují. V tomto uplynulém roce aktéři hrozeb i nadále využívali chyb v zabezpečení objevených během pandemie a přesunu do hybridního pracovního prostředí. Od té doby je největším problémem převaha a složitost různých metod útoku a větší aktivita národních států.

Efektivní kybernetická odolnost vyžaduje holistický, přizpůsobivý přístup, který odolá rozvíjejícím se hrozbám pro základní služby a infrastrukturu.

Více se dozvíte na str. 89

Modernizované systémy a architektura jsou důležitou součástí řízení hrozeb v hyperpropojeném světě.

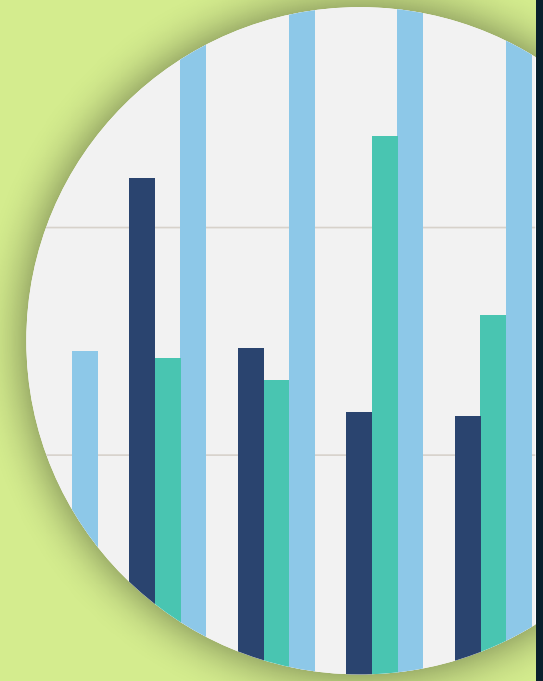


Více se dozvíte na str. 90

Základní stav zabezpečení je stěžejním faktorem pro účinnost pokročilého řešení.

Více se dozvíte na str. 92

I když útoky založené na heslech zůstávají hlavním zdrojem napadení identity, objevují se i další typy útoků.



Více se dozvíte na str. 93

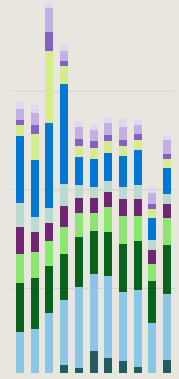
Lidským rozměrem odolnosti vůči operacím ovlivňování v kyberprostoru je naše schopnost spolupracovat.

Více se dozvíte na str. 102

Naprosté většině úspěšných kybernetických útoků šlo zabránit základní bezpečnostní hygienou.

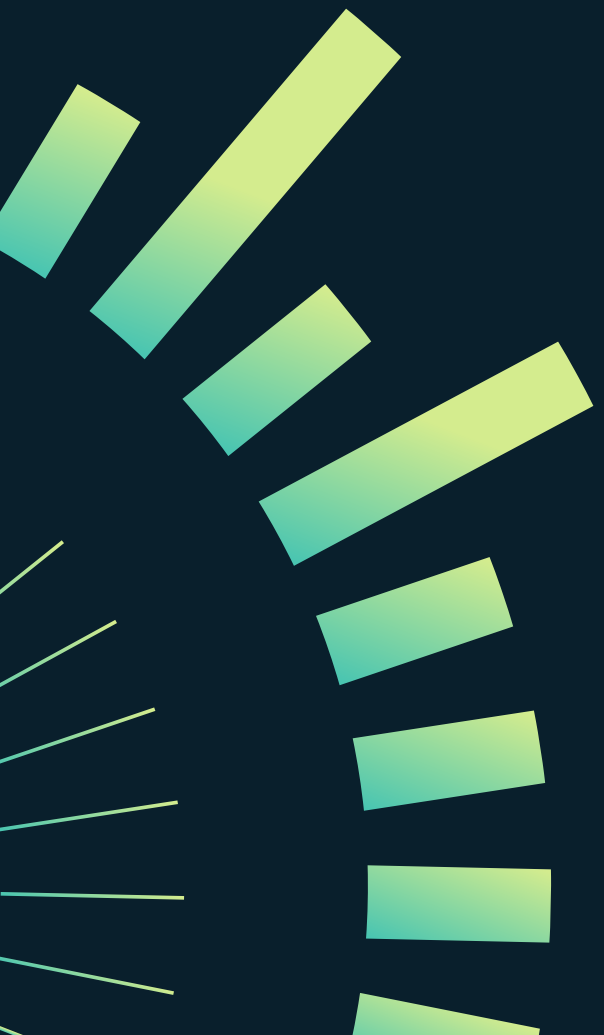
Více se dozvíte na str. 108

Za poslední rok ve světě docházelo k aktivitě útoků DDoS, která byla co do objemu, složitosti a četnosti nevídaná.



Více se dozvíte na str. 98

Úvod



Pandemie pro nás představovala výzvu, jak upravit postupy a technologie zabezpečení tak, aby chránily zaměstnance Microsoftu bez ohledu na místo, odkud pracují. V tomto uplynulém roce aktéři hrozeb i nadále využívali chyb v zabezpečení objevených během pandemie a přesunu do hybridního pracovního prostředí. Od té doby je největším problémem převaha a složitost různých metod útoku a větší aktivita národních států.

Aktivita digitálních hrozeb je v současné době nejvyšší v historii a každý den narůstá úroveň sofistikovanosti kybernetických útoků. Mnoho dnešních složitých útoků se zaměřuje na napadení architektur identit, dodavatelských řetězců a třetích stran s různými úrovněmi bezpečnostních mechanismů. Konkrétně jsme zaznamenali, že jasnou a stávající hrozbou jsou phishingové útoky na identitu. S dobrou správou identit, řízením phishingu a technikami správy koncových bodů jsou však tyto útoky obvykle neúspěšné. Kvůli tomu nesmíme zapomenout na základy: 98 procent útoků lze zastavit zavedením základních hygienických opatření. V Microsoftu spravujeme identity a zařízení jako součást našeho přístupu Zero Trust (nulové důvěry), do kterého patří přístup s nejnižší možnou úrovní oprávnění a přihlašovací údaje odolné proti phishingu. Tak účinně zastavujeme aktéry hrozeb a udržujeme svá data v bezpečí.

V dnešní době můžou nesmírně ničivé útoky zahájit i aktéři hrozeb, kteří nemají nijak velké technické dovednosti. Přístup k pokročilým strategiím, technikám a postupům je totiž v ekonomice kyberzločinu snadný. Válka na Ukrajině ukázala, jak aktéři národních hrozeb stupňovali své útočné kybernetické operace větší mírou ransomwaru. Ransomware je teď propracovaný obor, v němž aktéři hrozeb využívají taktiku dvojitého nebo trojitého vydírání, aby dostali zaplaceno, a vývojáři nabízejí ransomware jako službu (RaaS). S RaaS můžou aktéři hrozeb využít k útokům síť partnerů, díky čemuž není tak těžké začít i pro méně schopné kyberzločince. V konečném důsledku se tak rozšiřuje okruh útočníků.

Proto Microsoft přepracoval program eliminace ransomwaru. Cílem programu je napravit mezery v řízení a pokrytí, přispět k rozšíření funkcí služeb a vyvinout playbooky zotavení pro naše centrum Security Operations Center a technické týmy pro případ ransomwarového útoku.

Nedávné útoky na dodavatelské řetězce a externí dodavatele naznačují velký zlom v oboru. Problémy, které tyto útoky způsobují našim zákazníkům, partnerům, státním správám a Microsoftu, jsou stále větší. Je tedy patrné, jak důležité je zaměřit pozornost na kybernetickou odolnost a spolupráci se stranami, které se podílejí na zabezpečení. Protivníci cílí i na místní systémy, proto organizace potřebují spravovat chyby v zabezpečení starších systémů a modernizovat, případně přesunout infrastrukturu do cloudu, který nabízí robustnější zabezpečení.

Žijeme v době, kdy klíčem k technologickému úspěchu je zabezpečení. Inovací a vyšší produktivity je možné dosáhnout jen zavedením bezpečnostních opatření, s nimiž budou organizace co nejodolnější vůči moderním útokům. Digitální hrozby jsou stále větší a vyvíjejí se, proto je zcela zásadní integrovat kybernetickou odolnost do struktury všech organizací.

Bret Arsenault
Chief Information Security Officer

Kybernetická odolnost: Nezbytný základ propojené společnosti

Revoluce v digitálních technologiích měla za následek transformaci organizací tak, aby byly ještě více propojené jak ve způsobu, jakým fungují, tak ve službách, které nabízejí. Se stále většími hrozbami v kybernetickém prostředí je integrace kybernetické odolnosti do samotných základů organizace zrovna tak důležitá jako finanční a provozní odolnost.

Digitální transformace navždy změnila způsob, jakým organizace komunikují se zákazníky, partnery, zaměstnanci a dalšími účastníky. Nové technologie nabízejí obrovské příležitosti, jak být v kontaktu s lidmi, transformovat produkty a optimalizovat provoz. Pandemie urychlila digitální transformaci, protože umožnila vznik inovativních technologií, které lidem umožňují spolupracovat novými způsoby a z jakéhokoli místa.

Kybernetické hrozby se stávají všudypřítomnými a v našem vždy propojeném světě je stále obtížnější jim zabránit, aby ohrozily nějakou organizaci. Kybernetická odolnost představuje schopnost organizace pokračovat ve své činnosti a zachovat rychlost růstu bez ohledu na tíhu útoků, kterým čelí. Prevence musí být v rovnováze se schopností přežít a zotavit se a státní správy a firmy vyvíjejí komplexní modely, které se zabývají více oblastmi než jen zabezpečením a ochranou osobních údajů. V rámci kybernetické odolnosti mají tyto modely chránit prostředky, data a další zdroje.

Vývoj holistického přístupu ke kybernetické odolnosti

Kybernetická odolnost vyžaduje holistický, přizpůsobivý a globální přístup, který odolá rozvíjejícím se hrozbám pro základní služby a infrastrukturu. Do takového přístupu patří:

- Základní kybernetická hygiena popsaná naší zvonovou křivkou kybernetické odolnosti
- Porozumění a řízení kompromisu mezi riziky a přínosy digitální transformace
- Možnosti reakce v reálném čase, které umožňují aktivně detekovat hrozby a chyby v zabezpečení
- Ochrana před známými útoky a preventivní činnosti proti novým a očekávaným vektorům útoku, včetně možnosti automatické nápravy
- Snížený dopad útoků a katastrof izolací a segmentací chyb
- Automatizované zotavení a redundance pro případ narušení
- Upřednostnění provozního testování, které odhalí mezery, a porozumění sdílené odpovědnosti a závislostem na externích prostředcích, třeba cloudových řešeních zabezpečení

Efektivní program kybernetické odolnosti začíná u základních informací o prostředcích, například porozumění dostupným službám a zajištění spolehlivého katalogu prostředků, které se dají využít v případě narušení. S takovými základy pak musí být program schopen posoudit svou vlastní účinnost, změřit výkon kritických služeb a jejich závislostí, otestovat a ověřit funkce místních a cloudových služeb a pomáhat neustále zlepšovat celý digitální životní cyklus organizace.

Abychom mohli nabízet holistický přístup, spolupracujeme s organizacemi na identifikaci nejdůležitějších místních a online služeb, obchodních procesů, závislostí, zaměstnanců, prodejců a dodavatelů. Zároveň se snažíme identifikovat prostředky související s očekáváními zákazníka a trhu, regulačními a smluvními závazky a vnitřním provozem. V průběhu identifikace těchto kritických prostředků by současně měly probíhat činnosti, které detekují a monitorují hrozby, narušení, potenciální vektory útoku a chyby v zabezpečení systémů a procesů. Schopnost toto vše zajistit i přes aktuální nedostatek kvalifikovaných pracovníků vyžaduje důsledné stanovení priorit podle celkového rizika pro organizaci.

Takový holistický přístup se musí umět přizpůsobit neustálému vývoji prostředí hrozeb s cílem zajistit měřitelná zlepšení ve výkonu, snížení doby detekce, reakcí a zotavení a omezení dopadu v případě narušení. Navíc tento přístup musí reagovat na stále větší propojenost hrozeb. Incident zabezpečení může například způsobit únik dat s následky pro ochranu osobních údajů a vyžadovat spolupráci velkého množství interních a externích týmů na rychlé reakci a minimalizaci dopadu.

> Kybernetická odolnost je schopnost firmy pokračovat v provozu a zachovat zrychlování růstu navzdory narušením, mezi které patří i kybernetické útoky.

Poznatky a jejich využití

1. Vytvářejte a spravujte technologické systémy, které omezují dopad narušení a umožňují jejich další bezpečný a efektivní provoz i v případě, že dojde k úspěšnému narušení. Zaměřte se na společné kritické prostředky, podporujte pružnost a navrhujte systémy tak, aby se dokázaly přizpůsobovat (například hybridní a vícecloudová prostředí, multiplatformní systémy), omezovaly potenciální oblast útoku (odeberte například nepoužívané aplikace a příliš benevolentní přístupová práva), předpokládejte napadení prostředků a očekávejte, že protivníci budou používat nové taktiky.
2. Při plánování digitálních projektů zvažujte kromě příležitostí i možné hrozby a sdílenou odpovědnost za odolnost v celém dodavatelském řetězci digitálních technologií, včetně cloudových řešení zabezpečení.
3. Vytvářejte systémy, do kterých bude zabezpečení integrováno už při návrhu, a snažte se předvídat a detekovat budoucí vyvíjející se hrozby a odolávat jim, přizpůsobovat se jim a reagovat na ně.
4. Zajistěte, že se obchodní vedoucí představitelé budou podle potřeby radit s bezpečnostními týmy, aby byli seznámeni s riziky spojenými s novými situacemi. Obdobně by bezpečnostní týmy měly mít na paměti firemní cíle a radit vedoucím pracovníkům, jak se k nim přibližovat bezpečně.
5. Zajistěte zavedení zřetelných provozních praktik a postupů pro odolnost organizace vůči kybernetickým incidentům.

Význam modernizace systémů a architektury

S vývojem nových funkcí pro hyperpropojený svět musíme řešit hrozby, které vznikají kvůli starším systémům a softwaru.

Starší systémy – tedy ty, které byly vyvinuty dříve, než se standardem staly moderní komunikační nástroje jako smartphony, tablety a cloudové služby – představují pro organizace, které je stále používají, riziko. Toto vystavení riziku umocňují zjištění týmu Microsoft Security Services for Incident Response. To je skupina odborníků na zabezpečení, která zákazníkům pomáhá reagovat na útoky a zotavit se z nich.

V posledním roce souvisely problémy nalezené u zákazníků, kteří se zotavovali z útoků, se šesti kategoriemi. Znázorňuje je graf na této stránce. Na další stránce jsou uvedeny kroky, kterými je možné zvýšit odolnost.

Přes 80 procent incidentů zabezpečení je možné vysledovat k několika chybějícím prvkům, které se dají řešit moderními přístupy k zabezpečení.

Hlavní problémy ovlivňující kybernetickou odolnost

Tento graf ukazuje procento napadených zákazníků, kterým chybí základní mechanismy zabezpečení nezbytné ke zvýšení kybernetické odolnosti organizace. Zjištění se zakládají na zásazích Microsoftu za poslední rok.

„Vedoucí pracovníci by měli o kybernetické odolnosti přemýšlet jako o kriticky důležitém aspektu odolnosti firem. Měli by mít plán pro kybernetická narušení, stejně jako jej mají pro přírodní katastrofy a jiné nepředpokládané události. Měli by umožnit spolupráci interních účastníků, třeba provozního, komunikačního, právního i dalších oddělení, na tvorbě strategií. Pomůže to organizacím zajistit, že jejich kritické systémy budou zpět online v nejkratším možném čase a organizace se tak vrátí k běžnému obchodnímu provozu.

Tím to ale nekončí. Mnoho organizací totiž spoléhá na dodavatele třetích stran a poskytovatele služeb, proto by vedoucí pracovníci měli plánování kybernetické odolnosti rozšířit na svůj komplexní řetězec hodnot, aby ještě více zajistili nepřetržitý chod a odolnost podniku."

Ann Johnson,
Corporate Vice President of Security, Compliance, Identity, and Management Business Development

Význam modernizace systémů a architektury

pokračování

Existují zřetelné oblasti, kterým se organizace můžou věnovat, aby modernizovaly svůj přístup a chránily se před hrozbami:

Problém	Aktivní postup
Nezabezpečená konfigurace zprostředkovatele identit Chybná konfigurace a odhalení platforem identit a jejich součástí jsou běžný vektor, kterým lze získat neautorizovaný vysoce privilegovaný přístup.	Při nasazování a údržbě systémů identity, jako jsou infrastruktura AD a Azure AD, dodržujte základy a osvědčené postupy konfigurace zabezpečení. Implementujte omezení přístupu vynucováním oddělení oprávnění, přístupem s nejnižší možnou úrovní oprávnění a využitím pracovních stanic s privilegovaným přístupem ke správě systémů identit.
Nedostatečné řídicí mechanismy pro privilegovaný přístup a taktiku lateral movement Správci mají v digitálním prostředí nadbytečná oprávnění a často odhalují přihlašovací údaje pro správu na pracovních stanicích ohrožených riziky z internetu a riziky pro produktivitu.	Zabezpečte a omezte přístup pro správu tak, aby bylo prostředí odolnější a omezil se rozsah útoku. Využívejte kontrolní mechanismy správy privilegovaného přístupu, například přístup podle potřeby nebo správu jen v adekvátní míře.
Absence vícefaktorového ověřování (MFA) Dnešní útočníci se nevloupávají, ale přihlašují.	MFA je kritickým a základním kontrolním mechanismem uživatelského přístupu, který by měly mít zavedený všechny organizace. Spolu s podmíněným přístupem může být MFA nedocenitelným prostředkem při boji s kybernetickými hrozbami.
Nízká vyspělost operací zabezpečení Většina zasažených organizací používala tradiční nástroje pro detekci hrozeb a neměla relevantní informace, díky kterým by mohla včas zareagovat a zjednat nápravu.	Komplexní strategie detekce hrozeb vyžaduje investice do rozšířené detekce a reakce (XDR) a moderních cloudových nativních nástrojů, které pomocí strojového učení oddělují signály od šumu. Modernizujte nástroje pro operace zabezpečení začleněním XDR, které dokáže nabídnout podrobné informace o zabezpečení v celém digitálním prostředí.
Nedostatek řídicích mechanismů ochrany informací Organizace i nadále bojují se zavedením holistických řídicích mechanismů pro ochranu informací, které by plně pokrývaly všechna umístění dat, byly účinné po celou dobu životního cyklu informací a odpovídaly důležitosti dat pro firmu.	Identifikujte nejdůležitější firemní data a místa, kde se ukládají. Zkontrolujte procesy životního cyklu informací a posilte ochranu dat se zajištěním nepřetržitého chodu podniku.
Omezené přijetí moderních architektur zabezpečení Identita je nový bezpečnostní perimetr, který umožňuje přístup k různým digitálním službám a výpočetním prostředím. Integrace principů Zero Trust (nulové důvěry), zabezpečení aplikací a další moderní kybernetické architektury umožňují organizacím aktivně řídit rizika, která by se organizacím jinak jen obtížně předvídala.	Architektury Zero Trust vynucují koncepty nejnižší možné úrovně oprávnění a explicitního ověřování veškerého přístupu a vždy předpokládají napadení. K tomu by organizace měly implementovat kontrolní mechanismy a osvědčené postupy zabezpečení v DevOps a procesech životního cyklu aplikací, aby získaly vyšší úrovně kontrol ve firemních systémech.

Základní stav zabezpečení je stěžejním faktorem pro účinnost pokročilého řešení

Prostřednictvím naší analýzy jsme zjistili výskyt běžných nechráněných míst organizací, která útočníkům umožňují získat počáteční přístup, zajistit si oporu a implementovat útok, a to i v případě přítomnosti pokročilých řešení zabezpečení.

Často je výsledek kybernetického útoku rozhodnut dlouho předtím, než k útoku dojde. Útočníci využívají ohrožená prostředí, pomocí kterých získávají počáteční přístup, provádějí průzkum a vytvářejí chaos taktikou lateral movement a šifrováním nebo exfiltrací. Když se podaří útočníka zastavit v počátečních fázích, razantně se zvětší příležitost omezit celkový dopad.

Microsoft studoval konkrétní konfigurace stavů zabezpečení a identifikoval nejběžnější nedostatky ve skutečné praxi v těchto prostředích. To nám umožnilo spatřit nejběžnější chyby v zabezpečení zneužívané během útoků člověkem řízeným ransomwarem, které aktérům hrozeb umožnily získat přístup a bez povšimnutí se pohybovat v síti.

Základní konfigurace zabezpečení musí být zapnuté

Zařízení organizace, která nejsou zavedena nebo jsou zastaralá (jak v souvislosti s chybami v zabezpečení, tak ve stavu agenta zabezpečení), slouží útočníkům jako potenciální vstupní body a způsoby zavedení přístupu. Jak jsme zjistili, zajištění onboardingu zařízení organizace do aktualizovaného řešení detekce a reakce u koncových bodů[1] (EDR) a platformy ochrany koncových bodů[2] (EPP) je sice důležitý krok, ale není zaručeno, že dokáže ransomware zastavit.

Pokročilá řešení, jako jsou EDR a EPP, mají zásadní význam při detekci útočníka v prvních fázích toku útoku a zajištění automatické nápravy a ochrany. Jelikož ale tato pokročilá řešení zcela spoléhají na schopnost detekovat útok, vyžadují, aby byly zapnuty základní konfigurace zabezpečení. Zaznamenali jsme dokonce existenci scénářů se zavedenými pokročilými řešeními, která byla neúčinná kvůli chybějícím základním konfiguracím zabezpečení.

Osvědčené postupy při konfiguracích zabezpečení jsou lepší indikátor odolnosti než rychlost reakce analytiků ze Security Operations Center (SOC).

Mezi našimi zákazníky a partnery jsme v období šesti měsíců zpozorovali 70procentní snížení doby, kterou analytik SOC potřebuje k seznámení se s relevantním upozorněním a k zahájení jeho řešení. Toto zvýšené povědomí je dobré znamení. Ale i když informace o konfiguraci zabezpečení zvýšily výkonnost analytiků SOC, zajištění dostupnosti informací o produktech onboardingem a aktualizací zařízení organizace bylo větším prediktorem úspěšné prevence.

Riziko neznámých zařízení

Na rozdíl od cloudových sítí, kde zákazníci vědí, které prostředky běží na jakém operačním sytému, můžou místní sítě obsahovat pestrou paletu zařízení, třeba IoT, desktopy, servery a síťová zařízení, která organizace nemonitoruje ani nespravuje.

Průměrná podniková síť má přes 3500 připojených zařízení, která nejsou chráněna agentem EDR a můžou mít přístup k firemním prostředkům, nebo dokonce i k vysoce hodnotným zdrojům. Microsoft Defender for Endpoint (MDE) používá inspekci sítě, s jejíž pomocí zjišťuje zařízení a poskytuje informace o klasifikacích k síti připojených zařízení, třeba název zařízení, distribuci operačního systému a typ zařízení.

3500

průměrně připojených zařízení ve firmě, která nejsou chráněna agentem detekce a reakce u koncových bodů.

V případě zařízení nepodporovaných agentem EDR buďte alespoň seznámeni s jejich existencí a chraňte je posouzením chyb v zabezpečení a omezením přístupu k síti.

Poznatky a jejich využití

1. I propracovaná řešení můžou být neúčinná kvůli absenci základních konfigurací zabezpečení.
2. Investujte do osvědčených postupů v konfiguracích stavu zabezpečení, abyste se chránili před budoucími útoky. Tato základní nastavení zajišťují značnou návratnost investic, protože se organizace dokáže bránit před útoky.
3. Zaveďte všechna vhodná zařízení do řešení EDR.
4. Nezapomeňte aktualizovat agenty zabezpečení a zajistěte ochranu před manipulací, abyste získali více informací a lépe využili výhody ochrany v produktech.

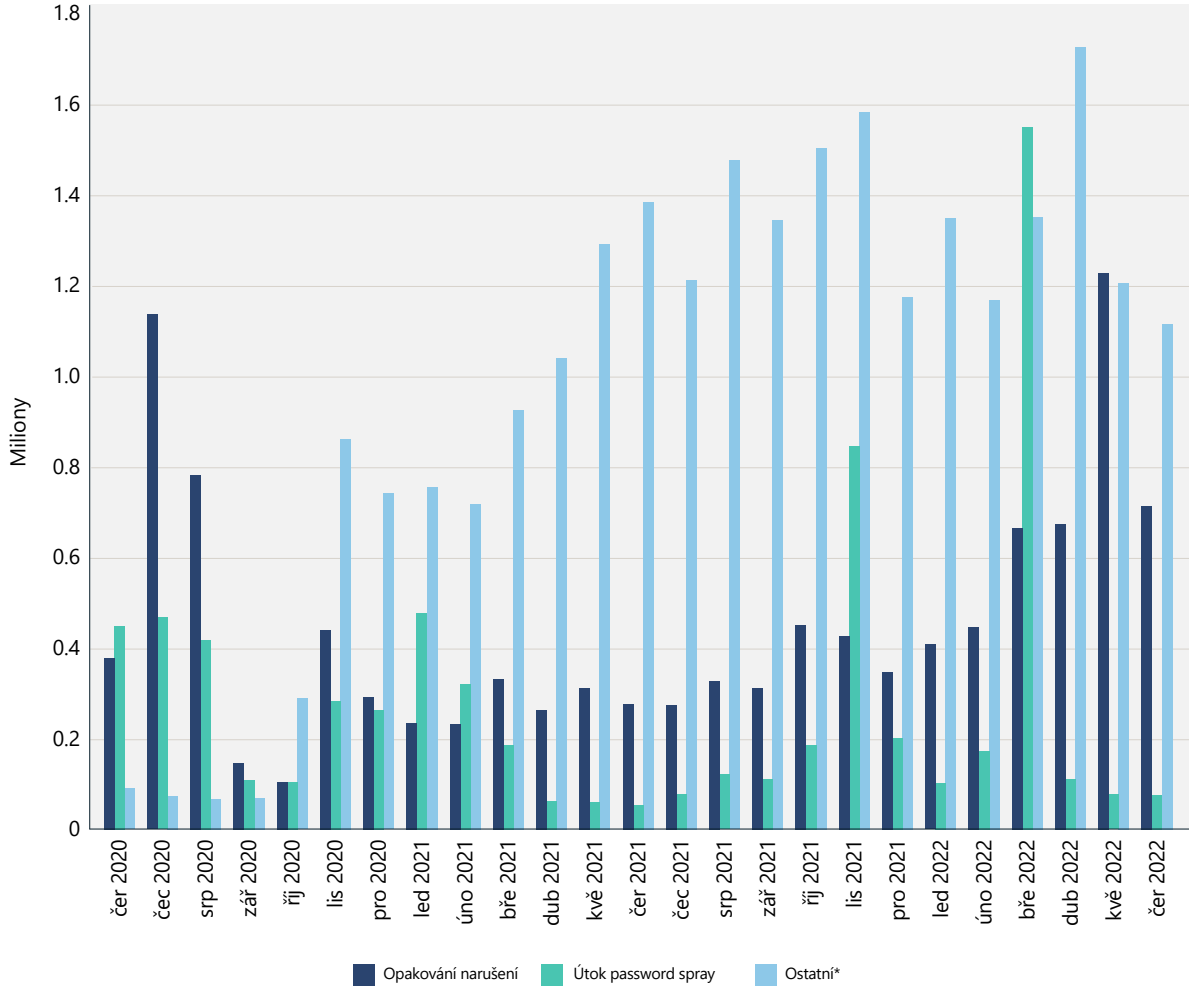
Dobrý stav identit je základem dobrého stavu organizace

Ochrana identit je teď důležitější než kdy jindy. I když útoky založené na heslech zůstávají hlavním zdrojem napadení identity, objevují se i další typy útoků. Objem sofistikovaných útoků je ve srovnání s předchozím běžným stavem útoků password spray a breach replay stále větší.

Útoky založené na heslech jsou stále běžné a více než 90 procent účtů napadených těmito metodami není chráněno silným ověřováním. Silné ověřování používá více než jeden faktor ověřování, například heslo a SMS a klíče zabezpečení FIDO2.

Zaznamenali jsme zvýšení počtu cílených útoků password spray s velmi vysokým nárůstem objemu provozu útočníků rozděleného mezi tisíce IP adres.

Ohrožení uživatelé podle kategorie útoků



Ohrožení uživatelé podle měsíců a kategorie útoků Objemy útoků password spray byly značně nestálé, jak ukazují výkyvy v listopadu 2021 a březnu 2022. Tyto výkyvy představují tisíce uživatelů a tisíce dotčených IP adres.* Kategorie Ostatní označuje útoky odlišné od password spray a breach replay. Patří mezi ně phishing, malware, man-in-the-middle, napadení místního vydavatele tokenů a další. Zdroj: Azure AD Identity Protection

4500

Za dobu, po kterou čtete toto prohlášení, jsme se ubránili 4500 útokům na hesla.

Dobrý stav identit je základem dobrého stavu organizace

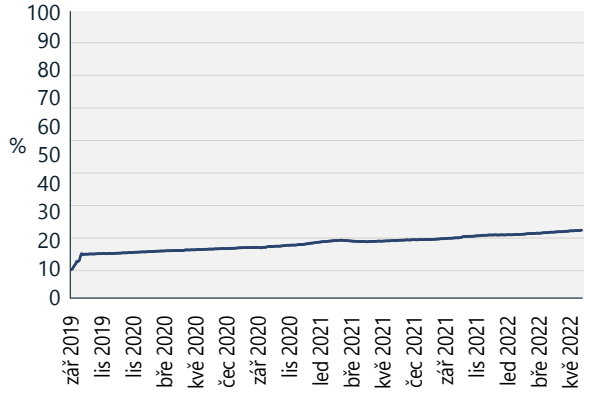
pokračování

Přijetí silného ověřování

Dobrou zprávou je, že u firemních zákazníků služby Azure Active Directory (Azure AD) pozorujeme stabilní nárůst přijetí silného ověřování. Pro Azure AD počet měsíčních aktivních uživatelů (MAU) silného ověřování vzrostl za poslední rok z 19 procent na 26 procent, zatímco MAU silného ověřování účtů pro správu vzrostlo z 30 na přibližně 33 procent.

Tento trend je příznivý, ale aby bylo dosaženo většinového pokrytí silným ověřováním, je stále zapotřebí výrazný nárůst. Pokud zákazníci ještě ve svých prostředích silné ověřování nepoužívají, měli by jej začít plánovat a nasazovat, aby chránili své uživatele.[3] Při návrhu nasazení silného ověřování by se mělo zvážit ověřování bez hesla, protože nabízí nejbezpečnější použitelné prostředí a eliminuje riziko útoků na hesla.

Používání silného ověřování
(září 2019 – květen 2022)

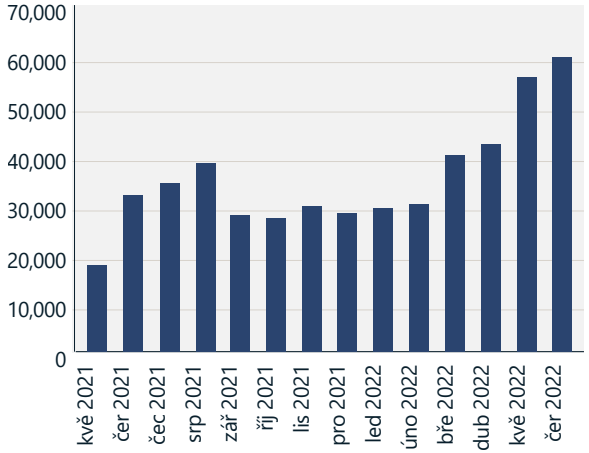


I když se silné ověřování používá od roku 2019 ve dvojnásobné míře, využívá jej jen 26 procent uživatelů a 33 procent správců. Zdroj: Azure Active Directory

Stálý nárůst počtu útoků token replay

Podíl ostatních forem útoku se v roce 2022 zvýšil. Došlo k nárůstu cílených útoků, které se záměrně vyhýbají ověřování založenému na heslech, aby se snížilo riziko jejich odhalení. Tyto útoky využívají soubory cookie jednotného přihlašování (SSO) v prohlížečích nebo obnovovací tokeny získané prostřednictvím malwaru, phishingu a jinými způsoby. V některých případech útočníci volí infrastrukturu v lokalitách blízko geografické polohy cílového uživatele, aby byla pravděpodobnost odhalení ještě nižší. Zpozorovali jsme stabilní nárůst útoků token replay. V Azure AD Identity Protection jich bylo za měsíc zjištěno 40 000. Při útoku token replay útočník používá tokeny vydané legitimnímu uživateli, ke kterým tento útočník získal přístup. Běžně se tokeny získávají malwarem, například exfiltrací souborů cookie z prohlížeče uživatele nebo prostřednictvím pokročilých metod phishingu.

Objem zjištěných útoků token replay



Zjištěné útoky token replay podle měsíců. Zdroj: Azure AD Identity Protection, jedinečné relace jsou označeny detekcí neobvyklých tokenů.

Dobrý stav identit je základem dobrého stavu organizace

pokračování

Extrakce tokenů

Více než malware útočníci potřebují k dosažení svých cílů přihlašovací údaje. Ve skutečnosti 100 procent všech útoků člověkem řízeným ransomwarem využívá kradené přihlašovací údaje. Mnoho sofistikovaných narušení používá přihlašovací údaje koupené na temném webu, ukradené z nepříliš propracovaného a široce distribuovaného malwaru pro krádež přihlašovacích údajů. Tato třída malwaru se vyvinula tak, aby kradla tokeny, včetně informací o relacích a deklarace MFA. To znamená, že nákazy domácích systémů, kde se uživatelé přihlašují k firemním prostředkům, můžou vést k závažným incidentům ve firemních sítích.

Útočníci můžou extrahovat tokeny ze zařízení obětí i pomocí útoků man-in-the-middle, při kterých oběť klikne na škodlivý odkaz ve phishingovém e-mailu nebo rychlé zprávě a je přesměrována na web, který vypadá jako pravá přihlašovací stránka zprostředkovatele identit. Ve skutečnosti je to ale webová služba zprovozněná útočníkem, která přesměrovává a zachytává všechen provoz mezi uživatelem a zprostředkovatelem identit. Útočník dokáže zachytit uživatelské jméno a heslo a předávat výzvy MFA. Tokeny vydané zprostředkovatelem identity a zachycené útočníkem tak můžou obsahovat deklarace MFA, které pak útočník může použít ke splnění požadavku na MFA.

Microsoft Defender for Cloud Apps od začátku roku 2022 zjistil průměrně 895 takových útoků za měsíc. Tomuto typu útoku se dá předcházet používáním faktorů MFA odolných proti phishingu, třeba ověřování na základě certifikátů, služby Windows Hello for Business nebo klíčů zabezpečení FIDO2.

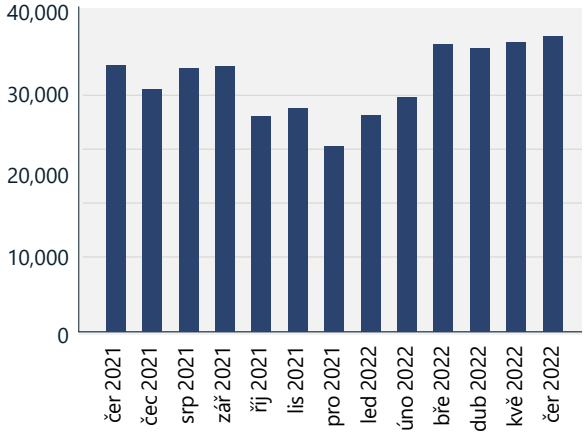
> Útoky založené na heslech jsou primárním způsobem napadání účtů.

MFA fatigue

Když útočníci využijí koncept MFA fatigue, vygenerují pro zařízení oběti mnoho požadavků na MFA v naději, že oběť přijme požadavek buď omylem, nebo v důsledku zahlcení. Tomuto útoku je možné předcházet používáním moderních ověřovacích aplikací, třeba Microsoft Authenticatoru, ve spojení s funkcemi jako porovnávání čísel[4] a poskytnutím dalšího kontextu.[5] Azure AD Identity Protection odhaduje, že za měsíc dojde k 30 000 útoků MFA fatigue.

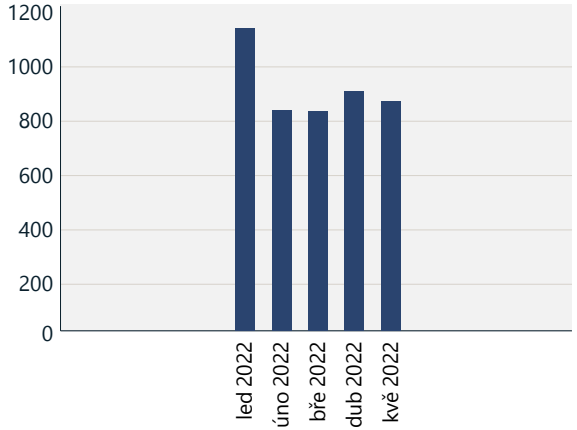
> Podíl propracovaných útoků i nadále roste, což jen dokazuje nutnost používat faktory vícefaktorového ověřování, které jsou odolné proti phishingu.

Odhadované případy útoků MFA fatigue



Zdroj: Azure AD Identity Protection

Zjištěné případy phishingu s následnými útoky man-in-the-middle



Zdroj: Microsoft Defender for Cloud Apps

Poznatky a jejich využití

1. Zajistěte, že všechny účty v celé organizaci budou chráněny opatřeními silného ověřování.
2. Ověřování bez hesla nabízí nejbezpečnější a pro uživatele příjemné prostředí, které eliminuje riziko útoků na hesla.
3. Zakažte v celé organizaci starší verze ověřování.
4. Chraňte vysoce hodnotné účty a účty pro správu silným ověřováním odolným proti phishingu.
5. Přejděte z místního zprostředkovatele identit na cloudového a propojte všechny své aplikace s cloudovým zprostředkovatelem identit, který zajistí konzistentní uživatelské prostředí a zabezpečení.

Odkazy na další informace

- Letošní Světový den hesel zvažte možnost zbavit se zcela všech hesel | Microsoft Security

Výchozí nastavení zabezpečení operačního systému

Ve stále se měnícím prostředí bezpečnostních rizik pozorujeme, že je stále důležitější mít i ve výchozím stavu nakonfigurované zabezpečení počítačů s cílem zvýšit kybernetickou odolnost. A i když je zabezpečení operačního systému naléhavější, složitější a pro firmy důležitější než kdy dříve, může být problematické jej zajistit a spravovat správným způsobem.

V minulosti k zabezpečení počítačů a zařízení patřily integrované funkce zabezpečení, u kterých se očekávalo, že si je zákazník nebo odborník na IT nakonfiguruje na svou vlastní požadovanou úroveň. Tento přístup už není adekvátní, protože útočníci ke splnění svých cílů používají pokročilejší nástroje pro automatizaci, cloudovou infrastrukturu a technologie vzdáleného přístupu. V dnešní době je už velmi důležité, aby všechny vrstvy zabezpečení, od čipu po cloud, byly nakonfigurovány už ve výchozím nastavení. Microsoft už považuje konfiguraci zabezpečení operačního systému Windows za standard.[6]

Zákazníci, kteří zavádějí obranu – a to důkladnou, včetně vrstveného zabezpečení, nových funkcí zabezpečení, pravidelných a konzistentních oprav a aktualizací i školení a povědomí o zabezpečení, aby byl hlášen phishing a další podvody – můžou očekávat méně malwaru.

Aby byla důkladná obrana jednodušší, systém Windows 11 úzce integruje hardwarové a softwarové ochrany, které jsou ve výchozím nastavení zapnuté, včetně integrity paměti, zabezpečeného spouštění a čipu TPM (Trusted Platform Module) 2.0. Uživatelé Windows 10 s podporovaným hardwarem můžou tyto funkce zapnout také. Najdou je v aplikaci Nastavení Windows nebo v nabídce systému BIOS.

Starší zařízení obecně často nemají takový soulad mezi zabezpečením hardwaru a softwarovými technikami zabezpečení. Na zařízeních, která nemají zabezpečení povolené ve výchozím nastavení, nakonfigurujte zabezpečení ručně v nastaveních, je-li to možné.[7]

Na zařízeních, která nemají zabezpečení povolené ve výchozím nastavení, Microsoft doporučuje nakonfigurovat zabezpečení ručně v nastaveních, je-li to možné.

Buďte aktivní při zavádění průběžných aktualizací operačního systému a oprav zabezpečení, které pomůžou zajistit ochranu v celém životním cyklu hardwaru a softwaru.

Poznatky a jejich využití

1. Používejte bezheslové řešení, které uloží přihlašovací údaje do čipu TPM (Trusted Platform Module). Vyhledávejte konkrétně bezheslové řešení, které splňuje průmyslový standard aliance Faster Identity Online (FIDO) Alliance[8].
2. Odstraňujte včas všechny nepoužívané a zastaralé spustitelné soubory, které se nacházejí na zařízeních organizace.
3. Braňte se pokročilým útokům na firmware povolením integrity paměti, zabezpečeného spouštění a čipu TPM (Trusted Platform Module) 2.0, pokud nejsou povoleny už ve výchozím nastavení. Posílí se tím zabezpečení spouštění pomocí funkcí integrovaných do moderních procesorů.
4. Zapněte šifrování dat a ochranu přihlašovacích údajů.
5. Povolte kontrolní mechanismy pro aplikace a prohlížeč, které nabídnou rozšířenou ochranu před nedůvěryhodnými aplikacemi, a další integrované ochrany před zneužitím.
6. Povolte ochranu přístupu k paměti, která pomůže chránit před příležitostnými fyzickými útoky, například před připojením škodlivého zařízení k externě přístupným portům.

Odkazy na další informace

- Kniha o zabezpečení Windows | Commercial
- Nové funkce zabezpečení pro Windows 11 pomůžou ochránit hybridní práci | Microsoft Security Blog

Centralizace dodavatelského řetězce softwaru

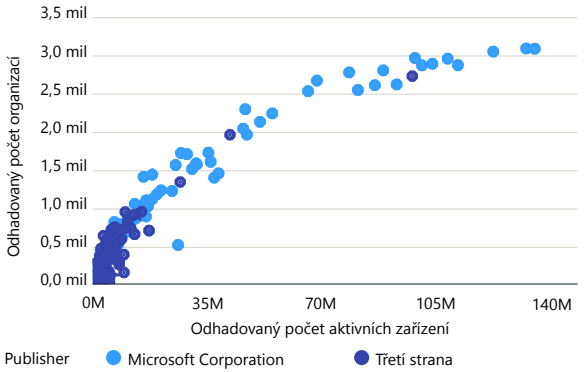
Útoky na aplikace, moduly plug-in a rozšíření třetích stran dokáží narušit důvěru zákazníků v dodavatele, kteří hrají ústřední roli v ekosystému dodavatelů. Když se podíváme na centralizaci softwaru optikou teorie sítí, pomůže nám to porozumět důležitosti oprav, obzvláště pro centrální aplikace.

Síť aplikací pro Windows, která obsahuje 18 milionů spustitelných souborů aplikací, je nainstalovaná a používaná v pěti milionech organizací a nabízí nám celkový pohled na náš ekosystém softwaru. Celkem 97 procent ze 100 000 nejpoužívanějších aplikací pochází od organizací třetí strany, které samy zajišťují aktualizace a opravy zabezpečení. Jsou tak patrné dva důležité rysy našeho ekosystému komerčních aplikací.

Zaprvé, v ekosystému komerčních aplikací pro Windows existuje centralizace. Jen horních 100 000 (z 18 milionů) aplikací se používá na nejméně 1000 zařízeních. Jinými slovy, jen něco málo přes polovinu procenta těchto aplikací má tento typ dalekosáhlého účinku v ekosystému zařízení.

Zadruhé, existuje rozmanitost v možnostech spravovat tyto aplikace, kde horních 10 000 dodavatelů aplikací spravuje aktualizace a opravy zabezpečení nejpoužívanějších komerčních aplikací. To ukazuje, jak je jedna společnost závislá na různorodé skupině kontrolních mechanismů zabezpečení, dodržování předpisů a správy dodavatelů softwaru.

Komerční dosah nejpoužívanějších aplikací



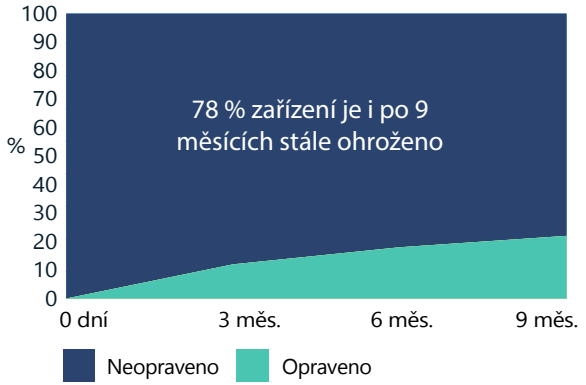
Hlavní aplikace se používají v milionech organizací a na desítkách milionů zařízení. Jelikož jsou tyto aplikace téměř všudypřítomné, protivníci neustále hledají způsoby, jak zneužít jejich chyby v zabezpečení a mít tak vliv na miliony zařízení mezi uživateli.

Pozorujeme, že miliony komerčních zařízení stále používají ohrožené verze aplikací, a to i mnoho měsíců po vydání oprav, nebo dokonce i roky po ukončení podpory produktu. Existuje například více než jeden milion aktivních komerčních zařízení s Windows, které používají verzi čtečky PDF, která se nepodporuje už od roku 2017.

Staré a nepodporované verze aplikací jsou i nadále aktivně používány na milionech komerčních zařízení. Kvůli tomu jsou organizace ohroženy neopravenými chybami v zabezpečení.

U stále podporovaných verzí aplikací pozorujeme stabilizaci rychlosti přijímání důležitých oprav, což je opačný trend, než který podpoří odolnost. K zajištění potřebné odolnosti by křivka měla vykazovat mezi měsíci spíše exponenciálně rychlejší zavádění oprav.

Míra nasazování důležitých oprav



Po prověření kritické chyby v zabezpečení, která ovlivnila 134 verzí několika prohlížečů, jsme zjistili, že 78 procent zařízení, tedy několik milionů, používá ohrožené verze ještě devět měsíců po vydání opravy.

K identifikaci charakteristik souvisejících s organizacemi, u kterých je větší pravděpodobnost, že mají zařízení se staršími verzemi aplikací, jsme použili sadu nástrojů InterpretML[9]. Mezi nejdůležitější z těchto prediktorů patří: nízký počet hodin používání zařízení, geografické oblasti, třeba Asie, Tichomoří a Latinská Amerika, a obory jako automobilový průmysl, chemické obory, telekomunikace, přeprava a logistika, plátci zdravotní péče (likvidátoři událostí) a pojištění.

Součástí údržby odolnosti softwaru by mělo být pravidelné zakazování nebo odinstalovávání nepoužívaných aplikací.

Zabezpečení a dodržování předpisů v organizaci závisí na jejích vlastních činnostech a na činnostech jejích dodavatelů softwaru.

Poznatky a jejich využití

1. Zajišťujte včasné aktualizace všech aplikací a koncových bodů v celé organizaci.
2. Odstraňujte včas všechny nepoužívané a zastaralé spustitelné soubory, které se nacházejí na zařízeních organizace.

Odkazy na další informace

- Dokumentace k Microsoft Intune | Microsoft Docs
- Správa aplikací | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- Zabezpečená architektura dodavatelského řetězce OSS | Microsoft Security Engineering
- Architektura zabezpečeného dodavatelského řetězce opensourcového softwaru Microsoftu | GitHub

Budování odolnosti vůči vznikajícím útokům DDoS a útokům na webové aplikace a sítě

Urychlená digitální transformace přinesla konec tradiční práce v síti a modelu perimetru zabezpečení. Přesun do cloudu znamená, že firmy musí pro ochranu digitálních prostředků přijmout cloudové zabezpečení sítě.

Složitost, četnost a objem útoků i nadále roste a není už omezený na sváteční období. Naznačuje to přesun k celoročním útokům. Je proto důležité zajistit nepřetržitou ochranu i mimo období tradičních nárůstů aktivity.

Distribuované útoky s cílem odepření služeb (DDoS)

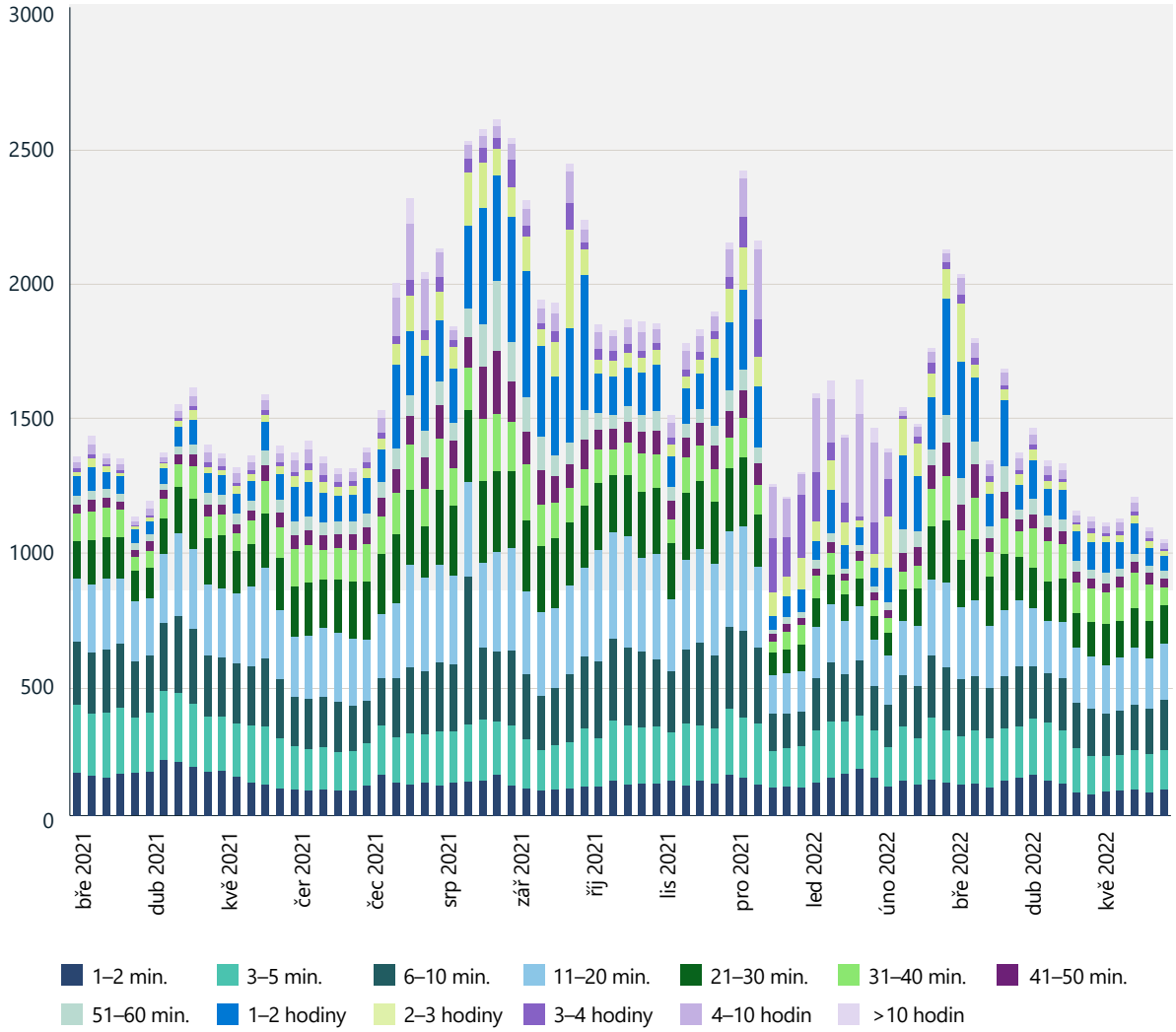
Za poslední rok ve světě docházelo k aktivitě útoků DDoS, která byla co do objemu, složitosti a četnosti nevídaná. Tento prudký nárůst útoků DDoS byl následkem značného nárůstu útoků národních států a pokračujícího šíření levných služeb pronájmu DDoS. Průměrně Microsoft zmírňoval 1955 útoků každý den, což oproti předešlému roku představuje nárůst o 40 procent. Dříve k nejvyššímu počtu útoků docházelo během svátečního období na konci roku. Pro letošek jich však bylo za jeden den nejvíce zaznamenáno 10. srpna 2021. To může znamenat posun k celoročním útokům a zdůrazňuje to důležitost nepřetržité ochrany i mimo období tradičních nárůstů aktivity.

V listopadu 2021 Microsoft zmařil rozsáhlý útok DDoS, jehož propustnost byla 3,4 terabitu za sekundu (Tb/s) a pocházel z přibližně 10 000 zdrojů v několika zemích. Podobné útoky s provozem vyšším než 2 Tb/s byly zmírněny i v roce 2022, z čehož vyplývá, že se nezvyšuje jen složitost a četnost útoků, ale také jejich objem (šířka pásma).

Trvání útoků

Většina útoků zaznamenaných v uplynulém roce trvala jen chvíli. Přibližně 28 procent útoků trvalo méně než 10 minut, 26 procent trvalo 10–30 minut a 14 procent bylo dlouhých 31–60 minut. 32 procent útoků trvalo déle než hodinu.

Distribuce počtu útoků DDoS a jejich trvání
(březen 2021 – květen 2022)



Většina útoků v minulém roce byla krátkodobá. Přibližně 28 procent útoků trvalo necelých 10 minut.

Budování odolnosti vůči vznikajícím útokům DDoS a útokům na webové aplikace a sítě

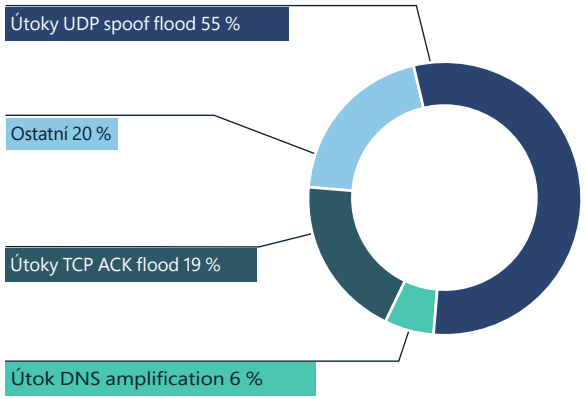
pokračování

Vektory útoků DDoS

V uplynulém roce patřily mezi běžně používané vektory útoku UDP (User Datagram Protocol) reflection na portu 80, který používá protokol SSDP (Simple Service Discovery Protocol), protokol CLDAP (Connectionless Lightweight Directory Access Protocol), systém DNS (Domain Name System) a protokol NTP (Network Time Protocol), z nichž sestávala jedna špička. Navíc jsme zjistili nárůst útoků DDoS na aplikační vrstvě, které cílily na webové stránky. V době největší aktivity proběhlo 16,3 milionu RPS (požadavků za sekundu) a protékalo 9,89 Tb/s dat.

V roce 2022 Microsoft zmírnil skoro 2000 útoků DDoS za den a zmařil vůbec největší zaznamenaný útok DDoS v historii.

Vektory útoků DDoS



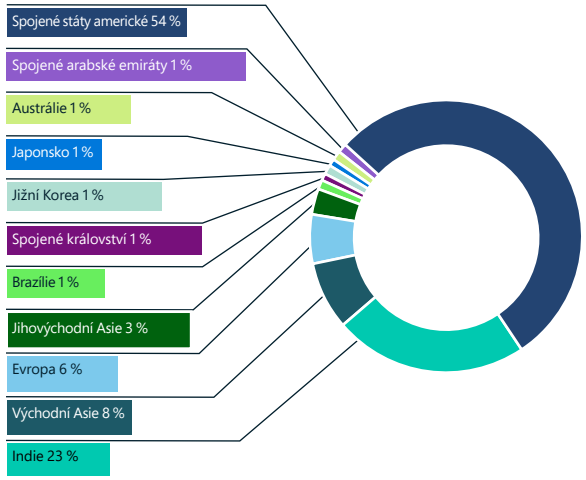
Útok UDP spoof flood se v první polovině roku 2022 stal nejčastějším vektorem, když narostl z 16 na 55 procent. Útok TCP ACK flood klesl z 54 na 19 procent.

Herní průmysl je i nadále nejčastějším cílem útoků DDoS, povětšinou mutacemi botnetu Mirai a útoky přes protokol UDP s nízkým objemem. Jelikož se protokol UDP běžně používá v herních a streamovacích aplikacích, drtivá většina vektorů útoků byly UDP spoof flood a jen malou část představovaly útoky UDP reflection a amplification.

Geografické cílové oblasti

Ze všech útoků DDoS zjištěných za poslední rok bylo 54 procent mířeno na cíle ve Spojených státech. Tento trend lze částečně vysvětlit skutečností, že většina zákazníků Azure a Microsoftu pochází ze Spojených států. Zaznamenali jsme také výrazný nárůst počtů útoků na Indii, z původních 2 procent všech útoků v druhé polovině roku 2021 na 23 procent v první polovině roku 2022. Východní Asie, a především Hongkong, zůstává oblíbeným cílem s 8 procenty. U Evropy jsme zjistili koncentraci útoků na oblasti v Amsterdamu, Vídni, Paříži a Frankfurtu.

Cíl útoků DDoS

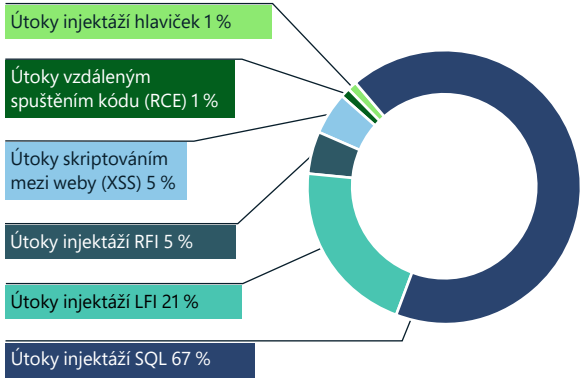


Vysoký objem útoků v Asii připisujeme značně rozšířenému hraní her v oblasti, obzvláště v Číně, Japonsku, Jižní Koreji a Indii. Herní průmysl i nadále poroste, protože stále více lidí používá smartphony, které podporují oblíbenost mobilních her. Proto tento geografický cíl bude zřejmě dále nabývat na významu.

Zneužívání webových aplikací

Firewall webových aplikací (WAF) v kombinaci s ochranou před útoky DDoS je nedílnou součástí strategie důsledné obrany, která chrání prostředky webových stránek a aplikačních programovacích rozhraní (API). Microsoft prostřednictvím firewallů Azure WAF zaznamenal více než 300 miliard aktivovaných pravidel WAF za měsíc.

Distribuce nejrozšířenějších typů útoků



Azure WAF detekuje každý den miliardy útoků identifikovaných v projektu OWASP (Open Web Application Security Project)[10] jako 10 nejčastějších útoků. Podle našich signálů se útočníci pokoušeli nejčastěji o útoky injektáží SQL, za kterými následovaly útoky injektáží místních souborů a injektáží vzdálených souborů. To je v souladu se seznamem nejčastějších deseti útoků projektu OWASP, který ukazuje, že útoky injektáží představují nejčastější tři typy webových útoků.

Došlo také k navýšení počtu útoků botů proti webovým aplikacím Azure. Průměrně boty zaslaly 1,7 miliardy požadavků měsíčně, 4,6 procenta z nich pocházelo od škodlivých botů.

Budování odolnosti vůči vznikajícím útokům DDoS a útokům na webové aplikace a sítě

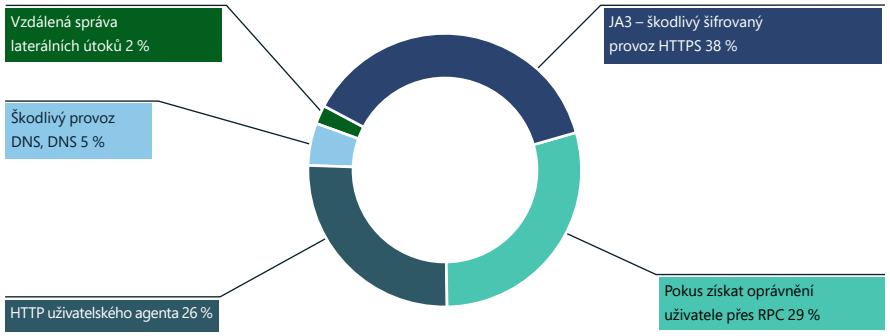
pokračování

Kvůli rostoucímu počtu botů, které provádějí útoky credential stuffing, podvody s platebními kartami, kampaně ovlivňování v kyberprostoru a útoky na dodavatelský řetězec, očekáváme stabilní nárůst útoků botů na webové aplikace.

Narušení sítě: detekce a prevence

V roce 2022 jsme zpozorovali výrazný nárůst zneužití na síťové vrstvě, obzvláště malwarem. Systém detekce a prevence narušení (IDPS) v Azure Firewallu zablokoval jen v měsíci červnu více než 150 milionů připojení.

Odůvodnění zamítnutí přenosů IDPS



Odůvodnění upozornění na přenosy IDPS

Analýza upozornění a zamítnutí přenosů IDPS ukazuje, že útočníci používají následující přístupy. V případě zamítnutí přenosů pozorujeme, že útočníci využívají protokol SSL, s jehož pomocí zakrývají své aktivity. Stále častěji jsou využívány útoky vzdáleným spouštěním. U upozornění na přenosy zjišťujeme, že k provádění útoků vzdáleným spouštěním se využívají protokoly SMB/SMB2.

Poznatky a jejich využití

1. Prověřujte veškerý provoz mezi systémy v datacentru nebo cloudové službě a provoz, který se k nim pokouší přistupovat.
2. Vypracujte robustní celoroční strategii reakcí pro zabezpečení sítě.
3. Používejte cloudové služby zabezpečení a implementujte robustní zabezpečení sítě na principu Zero Trust (nulové důvěry).

Odkazy na další informace

- Vylepšení bezpečnostní obrany před ransomwarovými útoky pomocí Azure Firewallu | Azure Blog and Updates | Microsoft Azure
- Anatomie útoku DDoS amplification | Microsoft Security Blog
- Inteligentní ochrana aplikací od hraničních zařízení po cloud pomocí služby Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Vytvoření vyváženého přístupu k zabezpečení dat a kybernetické odolnosti

Digitální transformace způsobila značné rozšíření datových prostředků a nárůst rizik pro zabezpečení, dodržování předpisů a ochranu osobních údajů. Kyberneticky odolné organizace musí najít rovnováhu mezi investicemi do ochrany dat, dodržování předpisů a funkcí obnovení a integrovat je do specializovaných procesů reakcí na regulativy, aby mohly řešit různé typy narušení zabezpečení.

Není otázkou, jestli nastanou úniky dat, ale kdy. Studie společností IBM a Ponemon Institute s názvem Cost of a Data Breach, 2021 uvádí, že v celosvětovém průměru stojí únik dat 4,24 milionu USD (10procentní nárůst v porovnání s předchozím rokem) a 9,05 milionu USD ve Spojených státech. Bylo zjištěno, že chyby v dodržování předpisů byly faktorem, který zvyšoval náklady nejvíce. Naopak snížení nákladů vzniklých únikem dat souviselo s osvědčenými postupy, například plánováním reakcí na incidenty, vyspělostí nasazení Zero Trust (nulové důvěry), AI a automatizací zabezpečení a používáním šifrování.

Únikům dat se nedá zabránit. Organizace, které k odolnosti přistupují vyváženým způsobem, omezí četnost, dopad a finanční ztráty způsobené úniky.

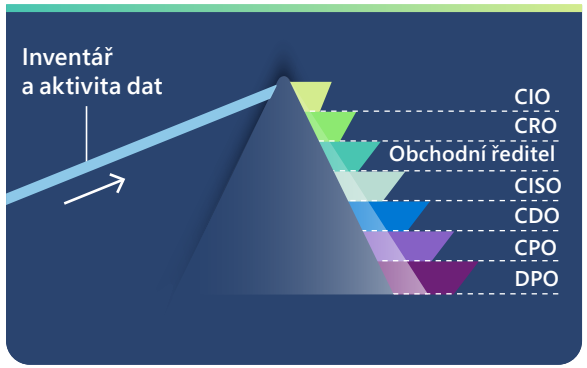
Řízení dat, zabezpečení, dodržování předpisů a ochrana osobních údajů jsou na sobě vzájemně závislé

Zjistili jsme, že se v posledních letech uchovává stále více dat, která pro organizace představují zásadní prostředek pro vytváření hodnoty. Současně zpřísnění regulačních požadavků na ochranu osobních údajů, které vyžaduje řízení a zabezpečení dat, rozostřilo hranici mezi rizikovými pozicemi. Zatímco novější pozice na úrovni C, třeba Chief Data Officer (CDO) nebo Chief Privacy Officer (CPO), mají svůj vlastní zájem na zabezpečení a dodržování předpisů, implementace a operacionalizace ochrany dat často spoléhá na týmy vedené pracovníky na pozicích Chief Information Officer (CIO) nebo Chief Information Security Officer (CISO). Není to ale jednostranné, protože iniciativy řízení dat vedené pracovníky na pozici CDO mají své výhody v zabezpečení také. Kvůli tomuto vzájemnému propojení musí týmy v oblasti IT, řízení dat, zabezpečení, dodržování předpisů a ochrany osobních údajů spolupracovat ještě úžeji. Jen tak můžou zajistit efektivitu a řízení rizik.

Budoucností jsou sjednocené platformy pro řízení rizik souvisejících s daty určené pro celou datovou infrastrukturu organizace

Není jednoduché sladit proces správy IT, řízení dat, zabezpečení, dodržování předpisů a ochrany osobních údajů v prostředí zakázkových aplikací pro každou oblast a při nekonzistentním rozložení dat v typickém hybridním, vícecloudovém prostředí organizace. Domníváme se, že organizace potřebují ucelené informace, které jim umožní najít jejich data a porozumět jim, chránit je, řídit přístup k datům, jejich využití a životní cyklus a předcházet ztrátě dat v celé datové infrastruktuře.

Práce se stejným inventářem dat a informacemi o aktivitách usnadňuje procesy mezi týmy, přináší ucelenější informace o rizicích a umožňuje organizacím lépe připravit a zjednodušit svou reakci na únik.



Ucelený pohled by měl sloužit jako optický hranol. Aby týmy, které se zabývají zabezpečením dat, dodržováním předpisů a ochranou osobních údajů, mohly účinně spolupracovat, potřebují jiné, a přitom konzistentní informace o stejném inventáři dat a aktivitách. Do aktivity dat patří přístup k datům, jejich úprava a události přesunu, které jsou cennou složkou rovnice zabezpečení dat.

Účinné řízení dat, zabezpečení, dodržování předpisů a ochrana osobních údajů jsou vzájemně provázané a vyžadují spolupráci mezi týmy.

Poznatky a jejich využití

1. Najděte rovnováhu mezi obranou a zotavením a minimalizujte dopad úniku dat investicemi do dodržování předpisů, ochrany dat a možností reakce.
2. Vypracujte a zaveďte procesy a nástroje, které odstraní riziková datová sila a pokryjí celou datovou infrastrukturu.

Odkazy na další informace

- Microsoft Purview – řešení ochrany dat | Microsoft Security
- Budoucnost dodržování předpisů a řízení dat je tu: Představujeme Microsoft Purview | Microsoft Security Blog

Odolnost vůči operacím ovlivňování v kyberprostoru: lidský rozměr

Pokroky v grafice a strojovém učení za posledních pět let přinesly snadno použitelné nástroje, které dokáží rychle vygenerovat vysoce kvalitní, realistický obsah, který se může po celém internetu rozšířit během sekund.

V souvislosti s událostmi oznamovanými prostřednictvím textového, zvukového a vizuálního obsahu jsme se dostali do bodu, kdy ani lidé, ani algoritmy nedokáží spolehlivě rozlišit skutečnost od fikce. Šíření těchto nástrojů a jejich výstupů vrhají pochyby na důvěryhodnost všech digitálních médií a narušují naše porozumění místních a světových událostí. Nové formy operací ovlivňování, které jsou možné díky pokrokům v technologiích, mají závažné důsledky pro demokratické procesy.[11]

Vznikají otázky, co můžeme dělat, abychom se připravili na budoucnost, která dokáže lépe odolávat těmto operacím ovlivňování v kyberprostoru. Technologie jsou pouze jedna část hádanky. Bude to vyžadovat úsilí na více stranách, například vzdělávání zaměřené na mediální gramotnost, povědomí a opatrnost, investice do kvalitní žurnalistiky s důvěryhodnými novináři na místní, národní i mezinárodní scéně a sítě pro sdílení a upozorňování na operace ovlivňování. Důležité budou i nové druhy předpisů umožňující trestat zlomyslné aktéry, kteří generují digitální obsah nebo s ním manipulují s cílem klamat.

Jsme si také vědomi, že obnovit důvěru v digitální obsah je ambiciózní cíl, který bude vyžadovat různé úhly pohledu a účastníky. Neexistuje žádná jedna společnost, instituce ani státní správa, která dokáže tyto hrozby vyřešit sama. Naše superschopnost, kterou máme jako lidé, je schopnost spolupracovat. Ta je v současné době obzvláště důležitá, protože bude vyžadovat, aby všichni – státní správy, průmyslové obory, akademický sektor a obzvláště zpravodajské, sociální a mediální organizace – spolupracovali na zlepšování úrovně a zdraví naší společnosti.

Odkazy na další informace

- Využití umělé inteligence při kybernetických misích Ministerstva obrany | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (3. května 2022; svědectví Erica Horvitze)

Posílení lidského faktoru zlepšováním dovedností

Lidský faktor je stěžejní součástí jakékoli strategie zvyšování kvalifikace v oblasti kybernetického zabezpečení. Podle studie Kaspersky Human Factor in IT Security[12] lze ve 46 procentech incidentů kybernetického zabezpečení pozorovat neopatrné nebo neinformované zaměstnance, kteří neúmyslně usnadní útok.

Tým Education and Awareness Microsoftu v organizaci Digital Security and Resilience odpovídá za posílení lidského faktoru v kybernetickém zabezpečení. Pomáhá zaměstnancům zabezpečit data a systémy své i našich zákazníků. Mezi naše cíle patří:

- Snížení rizika pro Microsoft a naše zákazníky budováním centralizované sady dovedností v oblasti základního zabezpečení v celém podniku u všech zaměstnanců
- Rozšíření znalostí zaměstnanců o zabezpečení vícefázovým přístupem ke školení, který podpoří žádoucí výsledky chování
- Podporovat změnu kultury začleněním myšlenek o zabezpečení jako nedílné součásti kultury Microsoftu každoročním povinným školením a akcemi zaměřenými na zabezpečení
- Podpora centralizovaného webového prostředku pro osvědčené postupy, informace o zásadách společnosti a hlášení incidentů pro cokoli, co se týká kybernetického zabezpečení

Nejméně jednou ročně každý zaměstnanec Microsoftu absolvuje program cíleného a centralizovaného školení zaměřeného na kybernetické zabezpečení. Nabídky školení jsou optimalizovány s ohledem na podporu aktuálních iniciativ kybernetického zabezpečení a zajištění měřitelných výsledků chování. Microsoft's Information Risk Management Council (IRMC) hraje klíčovou roli v identifikaci důležitých výsledků změn chování v oblasti kybernetického zabezpečení, kterými by se školení měla zabývat.

U všech našich programů školení v oblasti kybernetického zabezpečení, kde je to možné, měříme účinnost, efektivitu a výsledky řešení. Například naše nabídka školení k insiderským rizikům má 95procentní soulad s předpisy pro školení a výjimečnou spokojenost školených osob. Díky tomuto školení výrazně narostl počet hlášení, kterými manažeři oznamovali možné případy insiderských hrozeb prostřednictvím nástroje Report It Now společnosti. Součástí programu je:

Základy zabezpečení: Centralizované školení k dodržování předpisů a povědomí o kybernetickém zabezpečení v celém podniku, které se zabývá základními postupy zabezpečení a ochrany osobních údajů. Tato velmi očekávaná řada školení využívá model zábavné výuky, díky kterému je získávání informací o kybernetickém zabezpečení poutavé a zajímavé.

STRIKE: Povinné technické školení Microsoftu pro techniky, kteří vytvářejí a udržují obchodní řešení. Toto školení, které je dostupné jen na pozvání, se zabývá včasnými a kritickými oblastmi osvědčených postupů hygieny kybernetického zabezpečení a využívá hybridní model doručování přizpůsobený požadavkům cílové skupiny.

Pro konkrétní program: Cílené programy školení podporují konkrétní iniciativy kybernetického zabezpečení, včetně stínového IT, insiderských hrozeb a Microsoft Federal. Tyto nabídky jsou úzce integrovány s celkovou strategií zapojení pro příslušné iniciativy kybernetického zabezpečení prostřednictvím financování z vedení a vykazování výsledků, aby školení neprobíhalo jen formálně.

MSProtect: Centralizovaný webový prostředek Microsoftu nabízí osvědčené postupy, informace o zásadách společnosti a hlášení incidentů pro cokoli, co se týká kybernetického zabezpečení. Tento prostředek na vyžádání je doporučován zaměstnancům mimo formální nabídky školení.

Trénování dovedností v oblasti zabezpečení nesmí být vnímáno jen jako formální aktivita pro dodržování předpisů. Zaměřte se místo toho na změnu chování, aby bylo možné monitorovat výsledky u všech identifikovaných cílových chování, a zaveďte systémy, s nimiž dokážete určit dopad nabídek.

Poznatky a jejich využití

1. Zajistěte zaměstnancům školení a materiály k zabezpečení, kdykoli a kdekoli je potřebují.
2. Vypracujte strategii centralizovaného budování dovedností, k níž se vyjádří zúčastněné strany z celé firmy.
3. Zajistěte sledování a analýzu dopadu školení z pohledu účinnosti (množství), efektivity (kvality) a výsledků (dopad na firmu).

Odkazy na další informace

- Microsoft zahajuje další fázi iniciativy zlepšování dovedností poté, co pomohl 30 milionům lidí

Poznatky z našeho programu pro eliminaci ransomwaru

Microsoft v posledních pěti letech sám rozvíjel své principy Zero Trust (nulové důvěry)[13], aby zajistil robustní správu a dobrý stav identit a zařízení. S rostoucí hrozbou ransomwaru jsme vyvinuli podrobný pohled, který podpoří náš přístup k ochraně nás i našich zákazníků.

Po důkladném interním vyhodnocení jsme vytvořili program na eliminaci ransomwaru, který řeší nedostatky v řízení a pokrytí, přispívá k vylepšení funkcí pro služby jako Defender for Endpoint, Azure a M365 a vyvíjí playbooky pro naše týmy SOC a technické týmy, jak se zotavit v případě ransomwarového útoku.

Prvním krokem bylo porozumět rozsahu naší ochrany před ransomwarovým útokem cíleným na Microsoft. Už nějakou dobu probíhaly aktivity k nasazení Defenderu for Endpoint a k zajištění, že všechna zařízení budou spravována a budou dodržovat zásady Zero Trust (nulové důvěry), ale potřebovali jsme najít způsob, jak porozumět všem aspektům otázky, jestli bychom se dokázali efektivně zotavit z útoku. Abychom získali přehled, porovnali jsme profil NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile,[14] který je v souladu s našimi celofiremními zásadami, s naším seznamem známých kontrolních mechanismů. Tato analýza rychle identifikovala nedostatky v pokrytí.

Dále jsme upřednostnili nedostatky ve funkcích identifikace, detekce, ochrany, reakce a zotavení profilu CSF. Našli jsme strategický soulad s principem Zero Trust (nulové důvěry) a dalšími programy a objevili jsme nedostatky, kterými se nezabýval žádný stávající pracovní proces. Po vyhodnocení množství práce a úsilí potřebných k nápravě těchto nedostatků jsme je rozdělili na dva pilíře:

- **Ochrana firmy (Protect the enterprise, PtE):** Definice pracovních položek, které potřebujeme zajistit jako firma, abychom se chránili a mohli se zotavit z případného úspěšného útoku
- **Ochrana zákazníka (Protect the customer, PtC):** Začlenění funkcí ochrany zákazníků i naší firmy do nabídek

Integrace poznatků do vlastního podniku

Abychom napravili největší rizika a chránili naše důležité služby před ransomwarovým útokem, chystáme se zaměřit investice v dalších 6 až 12 měsících na dosažení pěti níže uvedených scénářů, které jsou součástí vyhrazeného ransomwarového programu. Jakmile v každém z těchto scénářů uspějeme, budeme postupně rozšiřovat rozsah programu tak, aby se dostal do všech částí firmy.

Scénář 1: Členové bezpečnostního týmu rozumí celkovému riziku souvisejícímu s ransomwarovým útokem a mají zavedený proces, jak u vedoucích pracovníků zajistit povědomí o nedostatcích v kontrolních mechanismech a o stavu rizik.

Scénář 2: Členové bezpečnostního týmu mají přístup k playbookům navrženým tak, aby jim i ostatním týmům v Microsoftu pomohly reagovat na ransomwarový útok na kritické služby a tyto služby obnovit.

Scénář 3: Členové týmu Enterprise Resilience mají ustanoven standard pro zálohování kritických systémů. Existují playbooky a provádějí se pravidelná cvičení zálohování a obnovování s cílem zajistit, že data půjde obnovit v případě ransomwarového útoku.

Scénář 4: Vlastníci služeb rozumí potřebným bezpečnostním a provozním kontrolním mechanismům a zásadám a implementují je, aby chránili svou službu, data zákazníků, koncové body a síťové prostředky před ransomwarovými útoky. Obzvláště se zaměřují na prioritní služby, které jsou považovány za kritické služby Microsoftu.

Scénář 5: Všichni zaměstnanci mají přístup ke vzdělávacím a školicím materiálům, které popisují, jak rozpoznat ransomwarový útok, jak jej oznámit bezpečnostnímu týmu a jak začít reagovat.

Poznatky a jejich využití

1. Dokumentujte a ověřujte komplexní aktivity zotavení a nápravy související s ransomwarovými útoky na kritické služby.
2. Zapojte účastníky do procesu aktualizace playbooku firemního krizového řízení tak, aby obsahoval činnosti specifické pro ransomware a proces rozhodování a pokyny, kterými se vyhodnotí, jestli, případně kdy zaplatit výkupné.
3. Zlepšete pokrytí detekce a ochrany povolením funkcí dostupných v nasazených produktech zabezpečení (např. pravidla pro omezení potenciální oblasti útoku v Defenderu for Endpoint).
4. Spolupracujte s týmem pro bezpečnostní standardy na definici základního nastavení ochrany před ransomwarovým útokem a pro technické týmy zajistěte školení a dokumentaci, jak se bránit ransomwarovému útoku.
5. Zaveďte automatizaci, která usnadní nasazování zásad zabezpečení a provozu v týmech DevOps, a zajistěte, že pokud systém přestane dodržovat předpisy, bude rychle označen a napraven.

Odkazy na další informace

- Jak Microsoft chrání před ransomwarem | Microsoft Inside Track

Reakce na význam kvantového zabezpečení

Existuje tlak na řízení hrozeb, které představují kvantové počítače pro dnešní kryptografii a vše, co se s její pomocí chrání. Nedávno zveřejněný dokument Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] navazuje na nařízení US Executive Order 10428[16] for Improving the Nation's Cybersecurity a stanovuje zabezpečení dodavatelského řetězce softwaru jako nezbytné při řešení budoucích útoků národních států.

Co jsou kvantové počítače?

Kvantové počítače jsou stroje, které k ukládání dat a výpočtům využívají vlastností kvantové fyziky. Můžou být extrémně užitečné pro určité úlohy, ve kterých dokáží být daleko výkonnější než nejlepší superpočítače. Kvantové výpočty už otevírají nové obzory šifrování a zpracování dat. Studie předpovídají, že kvantové výpočty budou už v roce 2030 představovat kvantový průmysl s hodnotou v řádech miliard dolarů (USD).[17] Dokonce to vypadá, že kvantové výpočty a kvantová komunikace budou mít transformativní účinek v mnoha různých odvětvích, od zdravotnictví přes energetiku až po finančnictví a zabezpečení.

Kvantové výpočty jsou hrozbou pro dnešní kryptografii a vše, co se s její pomocí chrání.

Hrozba pro dnešní kryptografii

Se Shorovým algoritmem z roku 1994 a průmyslovým kvantovým počítačem s více než několika miliony fyzických qubitů by mohly být všechny současné široce nasazené kryptografické algoritmy, které využívají veřejné klíče, prakticky prolomeny. Je nezbytně důležité zvážit, vyhodnotit a standardizovat „kvantově bezpečné" kryptografické systémy, které jsou efektivní, pružné a zabezpečené proti nepřátelskému kvantovému útoku. Migrace softwaru na „post-kvantovou kryptografii", především s ohledem na stávající klasické algoritmy a protokoly odolné proti kvantovému útoku, potrvá roky, ne-li desetiletí a déle.[18]

To znamená, že existuje tlak na řízení hrozeb, které představují kvantové počítače pro dnešní kryptografii a vše, co se s její pomocí chrání. Protivníci můžou už teď zaznamenat šifrovaná data a zneužít je později, až bude k dispozici kvantový počítač. Když budeme s řešením dopadů na kryptografii čekat až na dostupnost kvantových výpočtů, bude příliš pozdě.

Kryptografie se používá v celém kybernetickém ekosystému, proto by mohly být naše služby zabezpečení založené na kryptografii ohroženy. Patří sem například služby pro komunikace (TLS, IPSec), zasílání zpráv (e-mail, webové konference), správa identit a přístupu, prohlížení webu, podepisování kódu, platební transakce a další služby, které spoléhají na kryptografickou ochranu.

S uváděním kvantových počítačů do praxe bude nutné podrobněji prověřit součásti softwaru třetích stran, které obsahují implementace kryptografických algoritmů a funkcí. To znamená, že se všechny organizace v hodnotovém řetězci budou muset podílet na jeho zabezpečení. Průmyslové organizace a státní správy stále intenzivněji pracují na definici požadavků na zabezpečení dodavatelského řetězce softwaru a v některých případech stanovují nové mandáty na zabezpečení řetězce. National Security Memorandum NSM-8[19] stanovuje požadavky a časové harmonogramy implementace post-kvantové kryptografie v systémech National Security Systems (NSS). Stanovuje časovou lhůtu 180 dní na plánování modernizace, používání nepodporovaného šifrování, schválené protokoly jedinečné pro poslání, kvantově odolné protokoly a plánování pro používání kvantově odolné kryptografie tam, kde je to zapotřebí.

Standardizace představuje pro přechod na kvantově bezpečnou kryptografii časově velice náročnou aktivitu. Standardizační organizace, které pracují na standardech ohledně kryptografie s veřejnými klíči, musejí začít bezodkladně experimentovat s post-kvantovými algoritmy a zavádět je.

Nové algoritmy post-kvantové kryptografie (PQC) – klasické algoritmy, o kterých se předpokládalo, že jsou odolné proti kvantovému útoku – jsou nyní přezkoumávány v projektu Post-Quantum Standardization Project pod záštitou Národního institutu standardů a technologie.[20] Výsledky této práce budou mít vliv na celosvětové úsilí ve standardizačních organizacích. I když dojde k určitému překryvu s výběrem algoritmů vládou USA, odlišná volba vyhovujících algoritmů ze strany národních a regulačních orgánů by mohla představovat určité překážky na mezinárodní úrovni. Tato fragmentace pak zkomplikuje vývoj produktů a služeb.

Nové algoritmy post-kvantové kryptografie jsou přezkoumávány v programu Post-Quantum Cryptography Standardization pod záštitou Národního institutu standardů a technologie. Výsledky této práce budou mít vliv na celosvětové úsilí ve standardizačních organizacích.

Poznatky a jejich využití

Průmysl spolu se SAFECode a partnerskými členy by měl okamžitě podniknout krátkodobé aktivity, které jej připraví na přechod na PQC.[21] Mezi takové aktivity patří:

1. Sestavení inventáře produktů a kódů, které používají kryptografii
2. Implementace strategie kryptografické flexibility v celé organizaci, jejíž součástí je minimalizace změn kódu nutných při změně kryptografie
3. Předběžné využití algoritmů, které by mohly být kvantově bezpečné, v produktech a službách používajících kryptografii
4. Připravenost použít k šifrování, výměně klíčů a podpisům jiné algoritmy s veřejnými klíči
5. Testování vlivu velmi velkých klíčů, šifer a podpisů na aplikace

Odkazy na další informace

- Microsoft předvedl fyzikální principy pro vytvoření nového typu qubitu | Microsoft Research

Integrace podnikání, zabezpečení a IT pro vyšší odolnost

Robustní kybernetická odolnost závisí na spolupráci firemních představitelů a bezpečnostních týmů na implementaci zabezpečení. Dle zkušeností Microsoftu je vedení v oblasti zabezpečení náročnou disciplínou, která pro efektivní ochranu organizace vyžaduje podporu jejích vedoucích pracovníků.

Vedoucí pracovníci v zabezpečení řeší celou řadu dynamických problémů, které se týkají témat souvisejících s riziky, technologiemi, ekonomikou, organizačním procesem, obchodními modely, transformací kultury, geopolitickými zájmy, špionáží a dodržováním mezinárodních sankcí. Každé toto téma má své nuance, kterým se musí porozumět a které se musí důkladně řídit.

Na vedoucí pracovníky v zabezpečení spadá také úkol mařit činnost inteligentních, dobře placených a velmi motivovaných lidských útočníků i málo kvalifikovaných, ale účinných kyberzločinců. Jejich týmy musí bránit složitou technickou infrastrukturu, která byla často průběžně budována 30 i více let, kdy zabezpečení představovalo nízkou nebo zcela neexistující prioritu. Rozhodnutí učiněná před lety můžou v dnešní době představovat rizika, dokud nesplatíme svůj technologický dluh a nevyřešíme nedostatky v zabezpečení.

Představitelé organizací a tvůrci zásad můžou mít významný příznivý dopad na zabezpečení, když budou aktivně podporovat vedoucí pracovníky v zabezpečení a pomáhat s propojováním integrovaného zabezpečení a zbytku organizace. Když Microsoft pracuje se zákazníky, kteří jsou takto nastaveni, pozorujeme, jak vytvářejí odolnější organizaci a zlepšuje se jejich schopnost se přizpůsobit a inovovat.

Vedení organizace může vedoucí pracovníky v zabezpečení podporovat tím, že se zaměří na tři hlavní oblasti:

1. Budování zabezpečení od základů

Na zabezpečení se někdy pohlíží jako na překážku nebo něco, o čem se v obchodních procesech přemýšlí až v druhé řadě. Často se rozhoduje o zabezpečení, až když je příliš pozdě na prevenci rizik nebo snadnou a levnou opravu.

Představitelé organizací a tvůrci zásad by měli zajistit:

Zahrnutí zabezpečení do počátečních fází nových iniciativ. V nových digitálních iniciativách a při zavádění cloudu by mělo mít zabezpečení prioritu, aby se zajistilo, že organizace nebude s každou novou aplikací nebo digitální funkcí stále více ohrožována riziky. Jakmile se zabezpečení spolehlivě začlení do návrhu, dají se tyto procesy využít k modernizaci starších systémů a v jednu chvíli tím získat výhody jak ze strany zabezpečení, tak z pohledu produktivity.

Normalizovat preventivní údržbu zabezpečení. Zajistěte, že základní údržba zabezpečení, třeba instalace aktualizací zabezpečení a oprav a bezpečné konfigurace, má plnou podporu celé organizace (například rozpočtů, plánovaných výpadků, požadavků na akvizice pro podporu produktů dodavatelů).

Mnoho organizací bohužel tyto běžné postupy odkládá, pozdržuje nebo zavádí jen částečně. Tak útočníci získávají velké příležitosti ke zneužívání. Potřeba standardizovat zabezpečení je zohledněna v US NIST 800-40.[22]

2. Interakce s bezpečností

Vedoucí pracovníci organizací by se měli aktivně účastnit důležitých procesů zabezpečení a financovat je, aby se mezi prioritami objevovaly i materiály a připravenost na bezpečnostní katastrofy. To zahrnuje zapojení do:

Identifikace nepostradatelných obchodních prostředků. Vedoucí pracovníci v zabezpečení a týmy potřebují vědět, které prostředky jsou pro firmu nepostradatelné, aby soustředili prostředky tam, kde budou mít největší přínos. To je často nový problém, který vyžaduje ptát se na nové, dříve neřešené otázky a nacházet na ně odpovědi.

Cvičení nepřetržitého chodu podniku a obnovení po havárii kybernetického zabezpečení. Kybernetické útoky můžou představovat významnou událost, která naruší nebo zastaví velkou část firemních operací, nebo dokonce všechny. Když bude zajištěno, že týmy v celé organizaci budou připraveny vypořádat se s těmito situacemi, sníží se doba obnovování provozu firmy, omezí se škody v organizaci a pomůže to zachovat důvěru zákazníků, občanů a voličů. Taková příprava by měla být integrována do existujícího procesu nepřetržitého chodu podniku a obnovení po havárii.

Rozhodování o bezpečnostních rizicích by měli v ideálním případě dělat majitelé firmy nebo mise, kteří mají všechny informace o všech rizicích a příležitostech.

Integrace podnikání, zabezpečení a IT pro vyšší odolnost

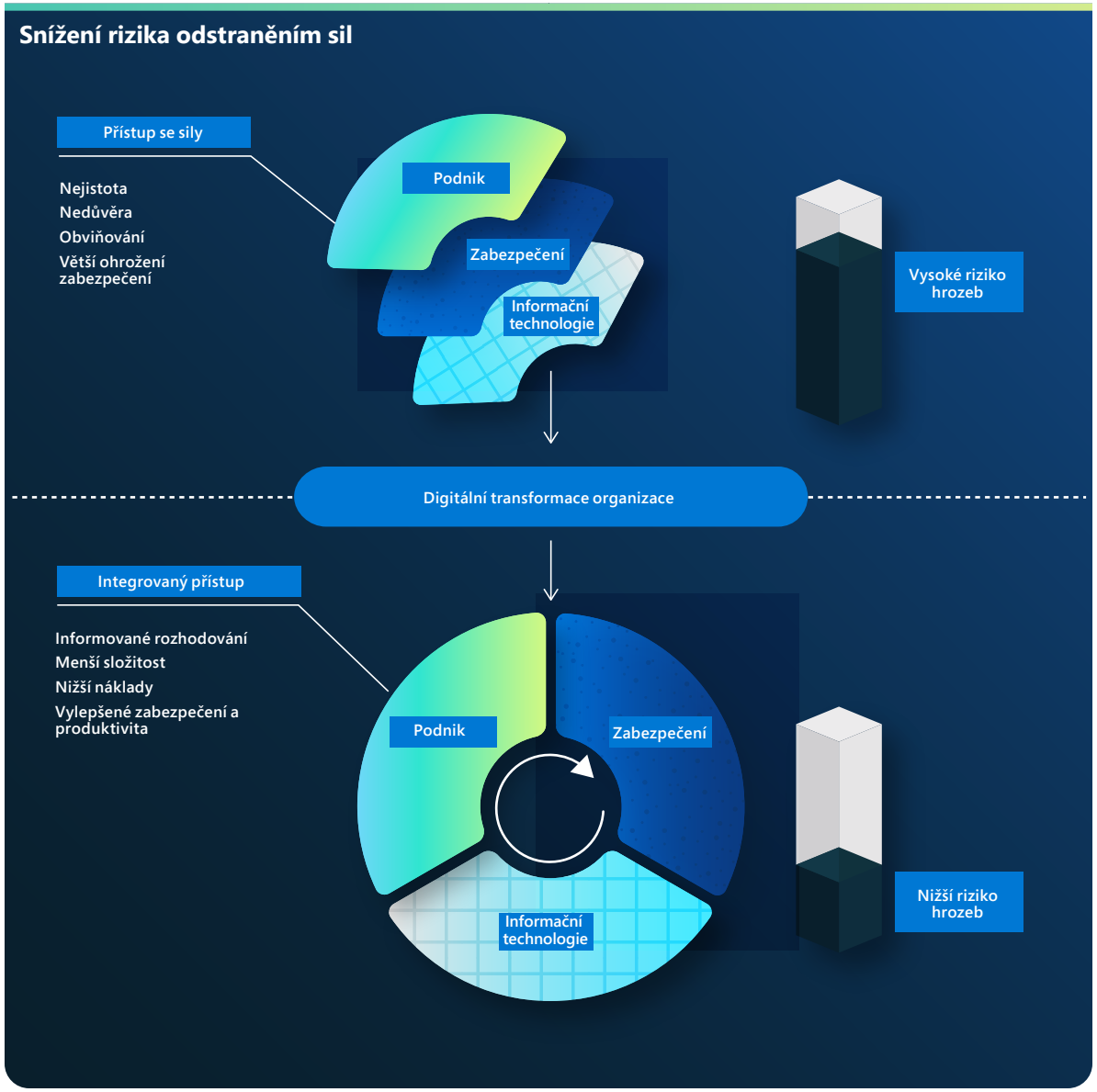
pokračování

3. Správné umístění zabezpečení

Způsob, jakým organizace strukturují odpovědnost za bezpečnostní rizika, často připravuje půdu pro nevhodná rozhodnutí o těchto rizicích. O rizicích by měli rozhodovat majitelé firmy nebo mise, kteří mají kompletní informace o všech rizicích a příležitostech, ale organizace často (implicitně i explicitně) místo toho přiřazují odpovědnost za bezpečnostní rizika odborníkům na příslušnou oblast v bezpečnostním týmu. To je pro bezpečnostní týmy nezdravá zátěž, která navíc majitele firmy připravuje o informace a kontrolu nad největším rizikem pro jejich podnikání. To můžou organizace napravit takto:

Přípravou majitelů firmy: Vzdělávejte majitele firmy o celkovém bezpečnostním riziku a o tom, jak tyto hrozby můžou ovlivnit a ovlivní jejich podnikání. Když do těchto činností zapojíte přímo i bezpečnostní týmy, posílí se tím vztahy při spolupráci na zabezpečení a celková pružnost firmy.

Přiřazením bezpečnostních rizik majitelům firmy: Jakmile budou mít majitelé firmy více informací a budou rozumět bezpečnostnímu riziku a přijímat jej, měla by organizace explicitně přenést odpovědnost za bezpečnostní riziko na ně, ale zároveň trvat na odpovědnosti bezpečnostních týmů za řízení tohoto rizika a poskytování odborných informací a poradenství majitelům.



„Kybernetická odolnost představuje klouzavou stupnici od klasického nepřetržitého chodu podniku a obnovení po havárii, které začínají u dobrého zálohování dat, pokračují funkcemi zotavení pro procesy, technologie a jejich závislosti (včetně lidí a třetích stran) a končí u nepřetržité dostupnosti, služeb automatických oprav, odolnosti důležitých rolí a přebírání služeb při selhání nejdůležitějších třetích stran. Nejodolnější organizace podporují integraci mezi IT, obchodními manažery a odborníky na zabezpečení. K velké odolnosti patří návrh pro odolnost od samotného počátku, bezpečná správa změn a podrobná izolace chyb. Kybernetická odolnost je jen jedním scénářem v dobrém programu plánování na všechna rizika. Kybernetická rizika jsou na vzestupu a průnik kybernetického zabezpečení s odolností je stále důležitější, proto také posiluje vazba pracovníka na pozici Chief Information Security Officer (CISO) na program firemní odolnosti. Každý rok přebírá stále více pracovníků CISO odpovědnost za odolnost v celé společnosti."

Lisa Reshaur
General Manager, Risk Management, Microsoft

Odkazy na další informace

- Od odolnosti po digitální vytrvalost: Jak organizace využívají digitální technologie při překonávání nezvykle obtížných období | Official Microsoft Blog
- Jak IT a bezpečnostní týmy dokáží spolupracovat na zlepšení zabezpečení koncových bodů | Microsoft Security

Zvonová křivka kybernetické odolnosti

Faktory úspěšné odolnosti, které by měla přijmout každá organizace

Jak jsme byli svědky, mnoho kybernetických útoků je úspěšných jednoduše proto, že nebyla dodržována základní hygiena zabezpečení. Mezi minimální standardy každé organizace by měly patřit tyto:

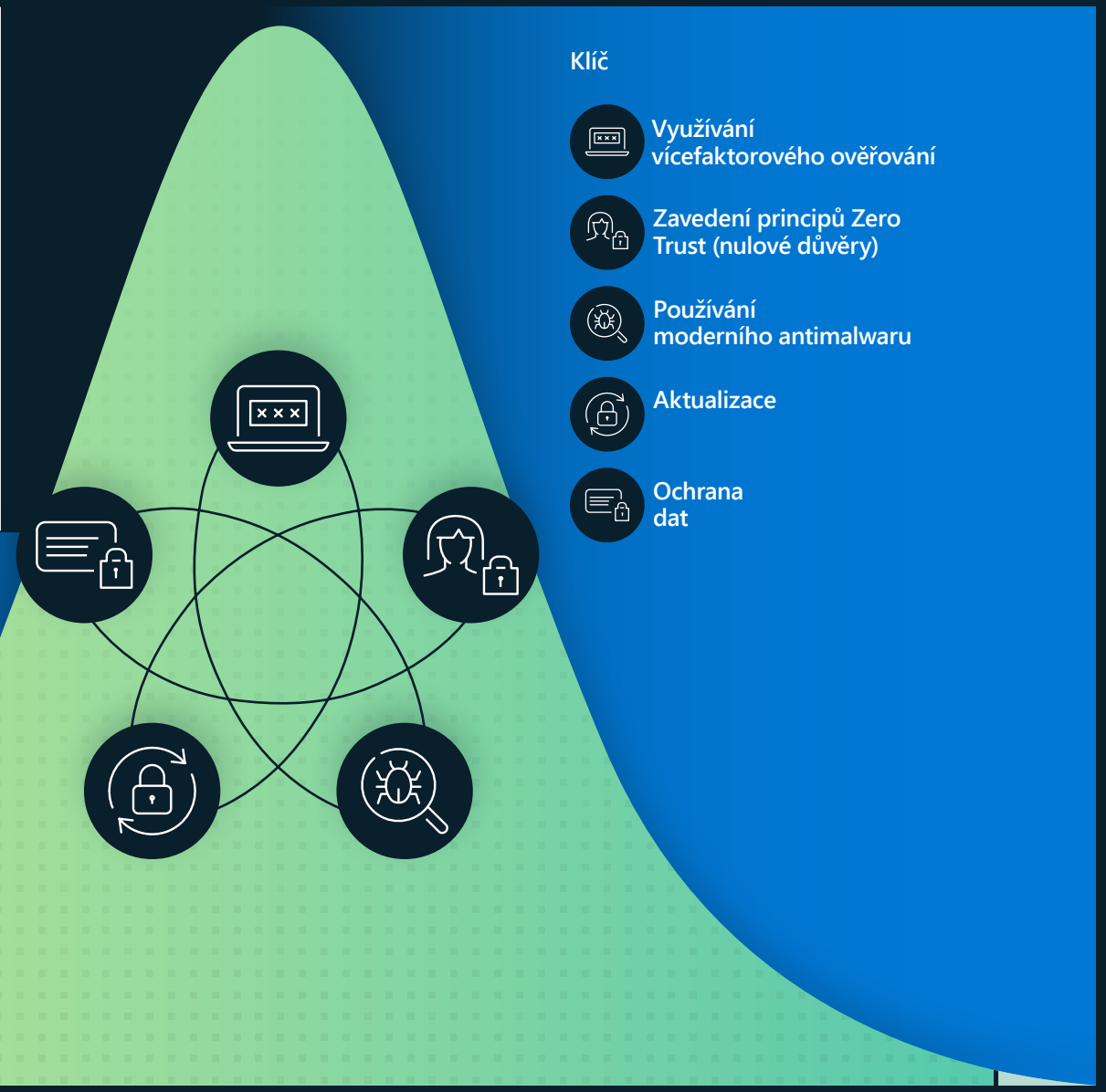
- **Povolení vícefaktorového ověřování (MFA):** Zajišťuje ochranu před napadenými uživatelskými hesly a pomáhá zajistit větší odolnost identit.
- **Zavedení principů Zero Trust (nulové důvěry):** Základní kámen jakéhokoli plánu odolnosti, který omezuje dopad na organizaci. Těmito principy jsou:

1. – Explicitně ověřujte – než povolíte uživatelům a zařízením přístup k prostředkům, ověřte jejich dobrý stav.
2. – Používejte přístup s nejnižší možnou úrovní oprávnění – povolte jen oprávnění nezbytně nutná pro přístup k prostředku a žádná jiná.
3. – Předpokládejte narušení – předpokládejte, že obrana systému byla prolomena a systém může být napadený. To znamená nepřetržité monitorování možných útoků v prostředí.

- **Používání antimalwaru pro rozšířenou detekci a reakci:** Implementujte software, který bude detekovat a automaticky blokovat útoky a poskytovat informace o operacích zabezpečení. Monitorování přehledů ze systémů detekce hrozeb je důležité, aby bylo možné na hrozby reagovat včas.
- **Aktualizace:** Neopravené a zastaralé systémy jsou hlavním důvodem, proč se mnoho organizací stává oběťmi útoku. Zajistěte, že všechny systémy budou aktuální, včetně firmwaru, operačního systému a aplikací.
- **Ochrana dat:** Znalost důležitých dat, jejich umístění a jestli jsou implementovány správné systémy je nezbytná pro implementaci vhodné ochrany.

98 %

Základní hygiena zabezpečení stále chrání před 98 % útoků.



Poznámky na závěr

1. Endpoint Detection and Response (EDR) je platforma pro zabezpečení koncových bodů určená k prevenci, odhalování a prověřování pokročilých hrozeb v podnikových sítích a k reakcím na ně. Funkce detekce a reakce u koncových bodů nabízejí pokročilé detekce útoků, které probíhají téměř v reálném čase a na jejichž základě lze jednat. Bezpečnostní analytici můžou efektivně stanovovat priority upozornění, získat informace o celém rozsahu narušení a svými reakcemi napravovat hrozby.
2. Platforma ochrany koncových bodů (EPP) je řešení nasazené na zařízeních koncových bodů, které slouží jako prevence před souborovým malwarem, detekuje a blokuje škodlivou aktivitu z důvěryhodných i nedůvěryhodných aplikací a poskytuje funkce pro prověřování a nápravy potřebné k dynamické reakci na incidenty a upozornění zabezpečení.
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. Kniha o zabezpečení Windows: Commercial
7. Nové funkce zabezpečení pro Windows 11 pomůžou ochránit hybridní práci | Microsoft Security Blog
8. FIDO Alliance: Otevřené standardy ověřování bezpečnější než hesla
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

Přispívající týmy

Přispívající týmy

Data a poznatky v této sestavě poskytla rozmanitá skupina odborníků na zabezpečení, kteří pracují v mnoha různých týmech Microsoftu. Jejich společným cílem je chránit Microsoft, jeho zákazníky a celý svět před hrozbou kybernetických útoků. Jsme hrdí na to, že se o tyto poznatky můžeme podělit v duchu transparentnosti a se společným cílem učinit svět bezpečnějším místem pro všechny.

AI for Good Research Lab: Využívá potenciál dat a AI k řešení mnoha problémů světa. Laboratoř spolupracuje s organizacemi mimo Microsoft a zavádí AI, které zlepšuje životní podmínky a prostředí. Mezi její oblasti zájmu patří online bezpečnost (dezinformace, kybernetické zabezpečení, bezpečí dětí), reakce na katastrofy, udržitelnost a AI pro zdraví.

Azure Edge & Platform, Enterprise & OS Security: Odpovídá za zabezpečení základního operačního systému a platformy ve Windows, Azure a dalších produktech Microsoftu. Tým vytváří přední řešení zabezpečení a hardwaru pro platformy Microsoftu, která omezují zneužívání, krádeže identit a napadání malwarem od nejmenších zařízení po cloud. Stojí za platformou Secured-Core od Microsoftu pro PC, hraniční zařízení a servery, Microsoft Pluton Security Processorem a dalšími produkty.

Azure Networking, Core: Tým pro cloudovou síť, který se zaměřuje na Microsoft WAN, sítě datacenter a softwarem definovanou síťovou infrastrukturu Azure, včetně platformy DDoS, platformy hraniční sítě a produktů zabezpečení sítě, jako jsou Azure WAF, Azure Firewall a Azure DDoS Protection Standard.

Tým Cloud Security Research: Tento tým chrání zákazníky Microsoftu a umožňuje jim bezpečně transformovat organizace, protože zabezpečuje cloud Microsoftu, vytváří inovativní funkce a produkty zabezpečení a provádí výzkum.

Customer Security and Trust (CST): Mezioborový tým, který se stará o neustálé zlepšování bezpečnosti zákazníků v produktech a online službách Microsoftu. CST ve spolupráci s inženýrskými a bezpečnostními týmy napříč společností zajišťuje dodržování předpisů, zlepšuje zabezpečení a poskytuje větší transparentnost s cílem chránit zákazníky a podporovat celosvětovou důvěru v Microsoft.

Customer Success: Bezpečnostní týmy v Customer Success pracují přímo se zákazníky, s nimiž se dělí o osvědčené postupy, zjištěné poznatky a pokyny, jak urychlit transformaci a modernizaci zabezpečení. Tento tým sestavuje a organizuje osvědčené postupy a poznatky zjištěné na cestě Microsoftu i jeho zákazníků k referenčním strategiím, referenčním architekturám, referenčním plánům a dalším materiálům.

Cyber Defense Operations Center (CDOC): Oddělení Microsoftu pro kybernetické zabezpečení a obranu funguje na bázi fúze a sdružuje bezpečnostní odborníky z celé společnosti, aby chránili naši podnikovou infrastrukturu a cloudovou infrastrukturu, ke které mají přístup zákazníci. Pracovníci pro řešení incidentů pracují společně s datovými vědci a bezpečnostními inženýry ze skupin služeb, produktů a zařízení Microsoftu a pomáhají nepřetržitě chránit, odhalovat i reagovat na hrozby.

Democracy Forward Initiative: Tým Microsoftu pracující na zachování, ochraně a rozšiřování základů demokracie. Za tímto účelem podporuje zdravý informační ekosystém, chrání otevřené a bezpečné demokratické procesy a zasazuje se o odpovědnost korporací vůči občanům.

Digital Crimes Unit (DCU): Tým advokátů, vyšetřovatelů, datových vědců, techniků, analytiků a obchodních specialistů odhodlaných bojovat s kyberzločinem na globální úrovni pomocí technologií, forenzní analýzy, občanskoprávních činností, trestních oznámení a veřejných i soukromých partnerství.

Digital Diplomacy: Mezinárodní tým bývalých diplomatů, tvůrců zásad a právníků, kteří pracují na prosazování poklidného, stabilního a bezpečného kyberprostoru, který čelí narůstajícímu vlivu konfliktu s národními státy.

Digital Security & Resilience (DSR): Organizace, která má za cíl umožnit Microsoftu vytvářet nejdůvěryhodnější zařízení a služby, udržovat naši společnost v bezpečí a chránit data Microsoftu i zákazníků.

Digital Security Unit (DSU): Tým advokátů a analytiků z oblasti kybernetického zabezpečení, kteří nabízejí právní, geopolitickou a technickou odbornost pro ochranu Microsoftu a jeho zákazníků. DSU buduje důvěru v podnikovou bezpečnostní obranu Microsoftu před důmyslnými kybernetickými protivníky po celém světě.

Digital Threat Analysis Center (DTAC): Tým odborníků, kteří analyzují a hlásí hrozby ze strany národních států, včetně kybernetických útoků a operací ovlivňování. Tento tým kombinuje informace a zjištění o kybernetických hrozbách s geopolitickou analýzou a přináší našim zákazníkům i nám samotným poznatky, podle nichž lze zajistit účinnou reakci a ochranu.

Enterprise and Security: Tým zaměřený na poskytování moderní, bezpečné a spravovatelné platformy pro inteligentní cloud a inteligentní hranici.

Enterprise Mobility: Tým, který pomáhá doručovat moderní pracovní prostředí s moderní správou a zachovat cloudová i místní data v bezpečí. Endpoint Manager obsahuje služby a nástroje, které Microsoft a zákazníci používají ke správě a monitorování mobilních zařízení, desktopových počítačů, virtuálních počítačů, vestavěných zařízení a serverů.

Přispívající týmy

pokračování

Enterprise Risk Management: Tým pracující v různých firemních jednotkách na prioritizaci diskuzí o rizicích se seniorním vedením Microsoftu. ERM propojuje několik týmů operačního rizika, spravuje rámec rizik pro podnikání Microsoftu a usnadňuje posuzování vnitřního zabezpečení společnosti prostřednictvím rámce NIST Cybersecurity Framework.

Global Cybersecurity Policy: Tým, který spolupracuje s vládami, nevládními organizacemi a průmyslovými partnery na podpoře veřejných zásad v oblasti kybernetického zabezpečení. Tyto zásady zákazníkům umožňují posílit jejich zabezpečení a odolnost při zavádění technologií Microsoftu.

Identity and Network Access (IDNA) Security: Tým pracující na ochraně všech zákazníků Microsoftu před neoprávněným přístupem a podvodem. IDNA Security je mezioborový tým techniků, produktových manažerů, datových vědců a bezpečnostních vyšetřovatelů.

M365 Security: Organizace, která vyvíjí bezpečnostní řešení, včetně Microsoft Defenderu for Endpoint (MDE), Microsoft Defenderu for Identity (MDI) a dalších. Tato řešení slouží k zabezpečení firemních zákazníků.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Poradní výbor v Microsoftu s posláním zajistit, že nové technologie budou vyvíjeny a uváděny do praxe odpovědným způsobem.

Microsoft Bing Search and Distribution: Tým, zabývající se výhradně poskytováním špičkového internetového vyhledávače, který uživatelům po celém světě umožňuje rychle vyhledávat důvěryhodné informace. Zahrnuje funkce sledování témat a aktuálních příběhů, které jsou pro uživatele významné, a přitom uživatelům umožňuje kontrolu nad jejich soukromím.

Microsoft Customer and Partner Solutions: Sjednocená obchodní organizace Microsoftu pro uvádění produktů na trh, která je zodpovědná za role v terénu, jako jsou specialisté a poradci v oblasti zabezpečení a technického prodeje.

Microsoft Defender Experts: Největší globální organizace společnosti Microsoft, která sdružuje výzkumné pracovníky v oblasti zabezpečení, vědce a analytiky hrozeb. Tým Defender Experts zajišťuje inovativní funkce detekce a reakce v produktech zabezpečení Microsoft 365 a službách, které tým Microsoft Defender Experts spravuje.

Microsoft Defender for IoT: Tým složený ze špičkových oborových výzkumníků, kteří se specializují na reverzní inženýrství malwaru, protokolů a firmwaru pro IoT a OT. Tento tým aktivně vyhledává hrozby pro IoT a OT a odhaluje škodlivé trendy a kampaně.

Microsoft Defender Threat Intelligence (RiskIQ): Tým, který získává taktické informace analýzou rozsáhlé kolekce externí telemetrie Microsoftu. Při tom mapuje měnící se prostředí hrozeb, objevuje dříve neznámou infrastrukturu hrozeb a zjišťuje kontextové informace k aktérům hrozeb a kampaním. Tým pravidelně a včas publikuje výsledky jedinečného výzkumu, s nimiž obránci získávají důležité taktické informace.

Microsoft Security Business Development Team: Tým, který vede strategii růstu kybernetického zabezpečení, partnerství a strategické investice Microsoftu.

Microsoft Security Response Center (MSRC): Tým spolupracující s výzkumníky zabezpečení pracujícími na ochraně zákazníků Microsoftu a partnerského ekosystému. MSRC je nedílnou součástí centra CDOC (Cyber Defense Operations Center) Microsoftu a sdružuje odborníky na reakce na incidenty v zabezpečení, kteří odhalují hrozby a reagují na ně v reálném čase

Microsoft Security Services for Incident Response: Tým specialistů na kybernetické zabezpečení, kteří pomáhají zákazníkům v průběhu kybernetického útoku od prověřování přes úspěšnou izolaci po aktivity související s obnovením. Služby se nabízejí prostřednictvím dvou důkladně propojených týmů. Těmi jsou Detection and Response Team (DART), který se zaměřuje na prověřování a přípravu pro zotavení, a Compromise Recovery Security Practice (CRSP), který se zabývá izolací útoků a aspekty zotavování.

Microsoft Threat Intelligence Center (MSTIC): Tým Microsoftu zaměřený na identifikaci, sledování a shromažďování informací souvisejících s nejsofistikovanějšími protivníky, kteří mají dopad na zákazníky Microsoftu, včetně hrozeb ze strany národních států, malwaru, a phishingu.

One Engineering System (1ES): Tým s posláním doručovat špičkové nástroje, které vývojářům v Microsoftu pomáhají zajistit co nejvyšší produktivitu a zabezpečení. Tento tým vede centrální strategii pro zabezpečení komplexního dodavatelského řetězce softwaru Microsoftu.

Operational Threat Intelligence Center (OpTIC): Tým odpovědný za řízení a šíření informací o kybernetických hrozbách, které podporují poslání týmu Microsoft Cyber Defense Operation Center's (CDOC) chránit Microsoft a jeho zákazníky.

Microsoft

Zjišťování povahy hrozeb a pomoc s digitální obranou

- Další informace: **https://microsoft.com/mddr**
- Podrobnější informace: **https://blogs.microsoft.com/on-the-issues/**
- Zůstaňte ve spojení: **@msftissues a @msftsecurity**

© 2022 Microsoft. Všechna práva vyhrazena.