Microsoft

Microsofts rapport om digitalt forsvar 2022

Belysning af trusselslandskabet
og forstærkning af et digitalt forsvar.

Indhold

Dataene, indsigten og hændelserne i denne rapport er fra juli 2021 til juni 2022 (Microsoft-regnskabsåret 2022), medmindre andet er angivet.

For at få den bedste oplevelse med at se og navigere i denne rapport anbefaler vi, at du bruger Adobe Reader, der kan downloades uden omkostninger fra Adobes websted.

Introduktion ved Tom Burt

Corporate Vice President, Customer Security & Trust

"Billionerne af signaler, vi analyserer fra vores verdensomspændende økosystem af produkter og tjenester, afslører brutaliteten og omfanget af digitale trusler over hele verden."

Et snapshot af vores landskab...

Omfanget af trussel-slandskabet

Mængden af adgangskodeangreb er steget til ca. 921 angreb hvert sekund – en stigning på 74 % på blot et år.

Afvikling af cyberkriminalitet

Til dato har Microsoft fjernet mere end 10.000 domæner, der blev anvendt af cyberkriminelle, og 600, der blev anvendt af nationalstatsaktører.

Håndtering af sårbarheder

93 % af vores indsats mod ransomware afslørede utilstrækkelig kontrol af rettigheder og tværgående bevægelser.

Den 23. februar 2022 startede der en ny æra for cybersikkerhedsverdenen, hybridkrigens æra. På denne dag – timer før missiler blev sendt af sted, og kampvogne rullede over grænser – indledte russiske aktører et massivt, destruktivt cyberangreb mod ukrainske myndigheder, teknologi og mål inden for finanssektoren. Du kan læse mere om disse angreb og de erfaringer, der kan drages af dem, i kapitlet Trusler fra nationalstater i denne tredje årlige udgave af Microsofts rapport om digitalt forsvar (også kaldet MDDR, som står for Microsoft Digital Defense Report). Den vigtigste af disse erfaringer er, at cloud-løsningen giver den bedste fysiske og logiske sikkerhed mod cyberangreb og skaber mulighed for fremskridt inden for trusselsintelligens og endpoint-beskyttelse, som har bevist sin værdi i Ukraine.

Selvom en undersøgelse af dette års udvikling inden for cybersikkerhed skal begynde der, er dette års rapport et dybdegående indblik i meget mere. I rapportens første kapitel fokuserer vi på cyberkriminelles aktiviteter, efterfulgt af trusler fra nationalstater i kapitel to. Begge grupper har i stadig stigende grad øget raffinementet af deres angreb, hvilket på dramatisk vis har øget virkningen af deres handlinger. Selvom Rusland skabte flest overskrifter, eskalerede iranske ransomware-aktører deres angreb efter et præsidentskifte og lancerede destruktive angreb mod Israel og ransomware og hack-and-leak-operationer mod kritisk infrastruktur i USA. Kina øgede også sin spionageindsats i Sydøstasien og andre steder i de sydlige lande for at forsøge at modvirke amerikansk indflydelse og stjæle kritiske data og oplysninger.

Udenlandske aktører anvender også meget effektive teknikker til at muliggøre propagandaindflydelse i områder over hele verden. Dette beskrives i tredje kapitel. Rusland har for eksempel gjort en stor indsats for at overbevise sine borgere og borgere i mange andre lande om, at deres invasion af Ukraine var berettiget – de sådede også propaganda, der miskrediterer Vestens COVID-vacciner og samtidig promoverer effekten af deres egne. Derudover fokuserer aktørerne i stigende grad på IoT-enheder (Internet of Things – Tingenes internet) og OT-kontrolenheder (Operational Technology – driftsteknologi) som indgangspunkter til netværk og kritisk infrastruktur. Dette beskrives i kapitel fire. I det sidste kapitel afslutter vi med indsigt og erfaringer fra det seneste år, hvor vi forsvarer os mod angreb, som er rettet mod Microsoft og vores kunder, mens vi gennemgår årets udvikling inden for cyberrobusthed.

Hvert kapitel indeholder de vigtigste erfaringer og indsigter baseret på Microsofts unikke synspunkt. De billioner af signaler, som vi analyserer fra vores verdensomspændende økosystem af produkter og tjenester, afslører brutaliteten i og omfanget af digitale trusler over hele verden. Microsoft tager skridt til at forsvare kunder og det digitale økosystem mod disse trusler. Du kan læse om vores teknologi, der identificerer og blokerer milliarder af phishingforsøg, identitetstyveri og andre trusler mod vores kunder.

Introduktion ved Tom Burt

fortsat

Vi bruger også juridiske og tekniske midler til at udnytte og nedlukke infrastruktur, der anvendes af cyberkriminelle og nationalstatsaktører, og underrette kunderne, når de bliver truet eller angrebet af en nationalstatsaktør. Vi arbejder på at udvikle mere effektive funktioner og tjenester, der identificerer og blokerer cybertrusler ved hjælp af AI/ML-teknologi, så sikkerhedsprofessionelle bliver hurtigere og mere effektive til at opdage og bekæmpe cyberangreb.

Men det måske vigtigste er, at vi i hele MDDR tilbyder vores bedste råd om, hvad enkeltpersoner, organisationer og virksomheder kan gøre for at forsvare sig mod disse voksende digitale trusler. Det at indføre en god cyberhygiejne er det bedste forsvar og kan reducere risikoen for cyberangreb betydeligt.

Status for cyberkriminalitet

Cyberkriminelle fortsætter med at fungere som sofistikerede profitvirksomheder. Angribere tilpasser sig og finder nye måder at implementere deres teknikker på. Dette gør det vanskeligere at vide, hvordan og hvor de har deres kampagneinfrastruktur Samtidig bliver cyberkriminelle mere og mere sparsommelige. For at sænke deres faste omkostninger og øge udseendet af legitimitet kompromitterer angriberne virksomhedsnetværk og -enheder for at hoste phishingkampagner, malware eller endda bruge deres computerkraft til mining af kryptovaluta.

Få mere at vide på side 6

"Implementeringen af cybervåben i hybridkrigen i Ukraine er starten på en ny tidsalder med konflikter".

Trusler på nationalstatsniveau

Nationalstatsaktører lancerer stadig mere sofistikerede cyberangreb, der er designet til at undgå afsløring og fremme deres strategiske prioriteter. Implementeringen af cybervåben i hybridkrigen i Ukraine er starten på en ny tidsalder med konflikter. Rusland har også støttet krigen med informationspåvirkningsaktiviteter ved at bruge propaganda til at påvirke holdningerne i Rusland, Ukraine og globalt. Uden for Ukraine har nationalstatsaktører øget aktiviteten og er begyndt at bruge fremskridt inden for automatisering, cloud-infrastruktur og fjernadgangsteknologier til at angribe et bredere sæt af mål. Virksomheders it-forsyningskæder, der giver adgang til slutmålene, bliver ofte angrebet. Cybersikkerhedshygiejne blev endnu mere kritisk, da aktører hurtigt udnyttede sårbarheder uden programrettelser, brugte både sofistikerede og brute force-teknikker til at stjæle legitimationsoplysninger og slørede deres aktiviteter ved hjælp af open source eller legitim software. Derudover slutter Iran sig til Rusland i brugen af destruktive cybervåben, herunder ransomware, som en vigtig bestanddel af deres angreb.

Denne udvikling kræver øjeblikkelig indførelse af en ensartet, global struktur, der prioriterer menneskerettigheder og beskytter folk mod den uforsvarlige statsadfærd online. Alle nationer skal samarbejde om at implementere normer og regler for ansvarlig statsadfærd.

Få mere at vide på side 30

Enheder og infrastruktur

Pandemien og den hurtige introduktion af internetforbundne enheder af enhver art som en del af den accelererende digitalisering har i høj grad øget angrebsfladen i vores digitale verden. Resultatet er, at cyberkriminelle og nationalstater er hurtige til at udnytte mulighederne Selvom sikkerheden for it-hardware og -software er blevet styrket i de senere år, er sikkerheden for IoT- og OT-enheder ikke fulgt med. Trusselsaktører udnytter sådanne enheder til at få adgang til netværk og til horisontal bevægelse, til at få fodfæste i supply chain eller til at afbryde målorganisationens OT-drift.

Få mere at vide på side 56

Introduktion ved Tom Burt

fortsat

Cyber-indflydelsesaktiviteter

Nationalstater bruger i stigende grad sofistikerede indflydelsesaktiviteter til at distribuere oplysninger og påvirke den offentlige mening både nationalt og internationalt. Disse kampagner underminerer tillid, øger polariseringen og truer demokratiske processer. Dygtige avancerede og vedholdende manipulatorer bruger traditionelle medier sammen med internettet og sociale medier til markant at øge omfanget og effektiviteten af deres kampagner og den store indvirkning, de har i det globale informationsøkosystem. I det forløbne år har vi set disse operationer blive brugt som en del af Ruslands hybridkrig i Ukraine, men vi har også set Rusland og andre nationer, herunder Kina og Iran, i stigende grad implementere propagandaaktiviteter på de sociale medier for at udvide deres globale indflydelse på en række spørgsmål.

Få mere at vide på side 71

Cyberrobusthed

Sikkerhed er vigtig for teknologisk succes. Innovation og øget produktivitet kan kun opnås ved at introducere sikkerhedsforanstaltninger, der gør organisationer så modstandsdygtige som muligt over for moderne angreb. Pandemien har udfordret os på Microsoft til at ændre vores sikkerhedspraksis og -teknologier for at beskytte vores medarbejdere, uanset hvor de arbejder. I det forløbne år fortsatte trusselsaktører med at udnytte sårbarheder, der blev eksponeret under pandemien og overgangen til et hybridarbejdsmiljø. Siden da har vores primære udfordring været at håndtere udbredelsen og kompleksiteten af forskellige angrebsmetoder og øget nationalstatsaktivitet. I dette kapitel beskriver vi de udfordringer, vi har stået over for, og det forsvar, vi har mobiliseret som reaktion sammen med vores mere end 15.000 partnere.

Få mere at vide på side 86

Vores unikke udgangspunkt

37 mia.
blokerede mailtrusler

34,7 mia.
identitetstrusler blokeret

43 bil.
signaler syntetiseredes dagligt ved hjælp af sofistikerede dataanalyser og AI-algoritmer for at opnå en bedre forståelse over for og beskyttelse mod digitale trusler og cyberkriminalitet.

2,5 mia.
endpointsignaler analyseret dagligt

8.500+
teknikere, forskere, dataforskere, cybersikkerhedseksperter, trusselsjægere, geopolitiske analytikere, efterforskere og frontlinjerespondenter i 77 lande.

15.000+
partnere i vores sikkerhedsøkosystem, der øger cyberrobustheden for vores kunder.

1. juli 2021 til og med 30. juni 2022

Introduktion ved Tom Burt
fortsat

Vi mener, at Microsoft – uafhængigt og gennem tætte partnerskaber med andre i den private sektor, det offentlige og civilsamfundet – har et ansvar for at beskytte de digitale systemer, der understøtter vores samfunds sociale struktur, og fremme sikre computermiljøer for alle mennesker, uanset hvor de befinder sig. Dette ansvar er årsagen til, at vi hvert år har udgivet MDDR siden 2020. Rapporten er kulminationen på Microsofts mange data og omfattende forskning. Den beskriver vores unikke indsigt i, hvordan det digitale trusselslandskab udvikler sig, og de vigtige foranstaltninger vi kan træffe for at forbedre sikkerheden i økosystemet.

Vi håber at kunne indgyde en fornemmelse af uopsættelighed, så læserne kan træffe øjeblikkelige foranstaltninger baseret på de data og indsigter, vi præsenterer både her og i vores mange cybersikkerhedspublikationer i løbet af året. Når vi tænker på alvoren af truslen mod det digitale landskab – og hvad det har af betydning i den fysiske verden – er det vigtigt at huske på, at vi alle kan træffe foranstaltninger for at beskytte os selv, vores organisationer og virksomheder mod digitale trusler.

Tak, fordi du tager dig tid til at gennemgå Microsofts rapport om digitalt forsvar for dette år. Vi håber, du vil få værdifuld indsigt og anbefalinger, der kan hjælpe os med kollektivt at forsvare det digitale økosystem.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Vi har to mål med denne rapport:

1. At belyse det skiftende digitale trusselslandskab for vores kunder, partnere og interessenter, der spænder over det bredere økosystem, og kaste lys over både nye cyberangreb og de skiftende tendenser i historisk vedvarende trusler.
2. At give vores kunder og partnere mulighed for at forbedre deres cyberrobusthed og reagere på disse trusler.

Status for cyber-kriminalitet

I takt med at cyberforsvaret forbedres, og flere organisationer tager en proaktiv tilgang til forebyggelse, tilpasser angriberne deres teknikker.

En oversigt over

status for cyberkriminalitet

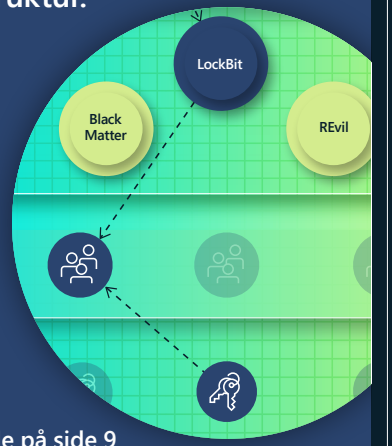
I takt med at cyberforsvaret forbedres, og flere organisationer tager en proaktiv tilgang til forebyggelse, tilpasser angriberne deres teknikker.

Cyberkriminelle fortsætter med at fungere som sofistikerede profitvirksomheder. Angribere tilpasser sig og finder nye måder at implementere deres teknikker på. Dette gør det vanskeligere at vide, hvordan og hvor de har deres kampagneinfrastruktur Samtidig bliver cyberkriminelle mere og mere sparsommelige. For at sænke deres faste omkostninger og øge udseendet af legitimitet kompromitterer angriberne virksomhedsnetværk og -enheder for at hoste phishingkampagner, malware eller endda bruge deres computerkraft til mining af kryptovaluta.

Cyberkriminalitet fortsætter med at stige, efterhånden som industrialiseringen af den cyberkriminelle økonomi sænker kompetencebarrieren ved at give bedre adgang til værktøjer og infrastruktur.

Få mere at vide på side 18

Truslen fra ransomware og afpresning bliver mere og mere aggressiv med angreb rettet mod offentlige myndigheder, virksomheder og kritisk infrastruktur.

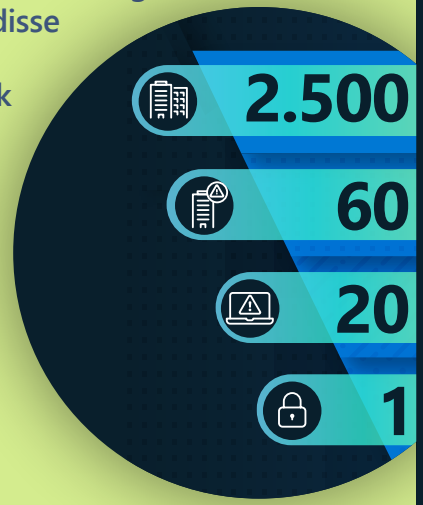


Få mere at vide på side 9

Angribere truer i stigende grad med at afsløre følsomme data for at tilskynde til udbetalinger af løsepenge.

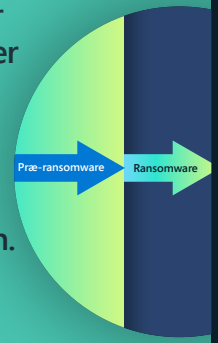
Få mere at vide på side 10

Ransomware, der drives af mennesker, er den mest udbredte variant. En tredjedel af målene kompromitteres af kriminelle, der bruger disse angreb, og 5% af disse er blevet økonomisk afpresset.



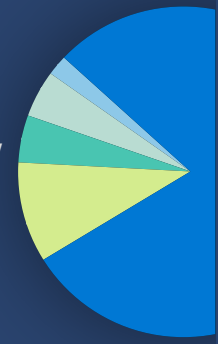
Få mere at vide på side 9

Det mest effektive forsvar mod ransomware omfatter multifaktorgodkendelse, hyppige sikkerhed-srettelser og Nul tillid-principper på hele netværksarkitekturen.



Få mere at vide på side 13

Der forekommer stadig flere og flere phishingforsøg med legitimationsoplysninger, som vilkårligt går efter alle indbakker, og kompromitterede forretningsmails, herunder fakturasvindel, udgør en betydelig cyberkriminalitetsrisiko for virksomheder.



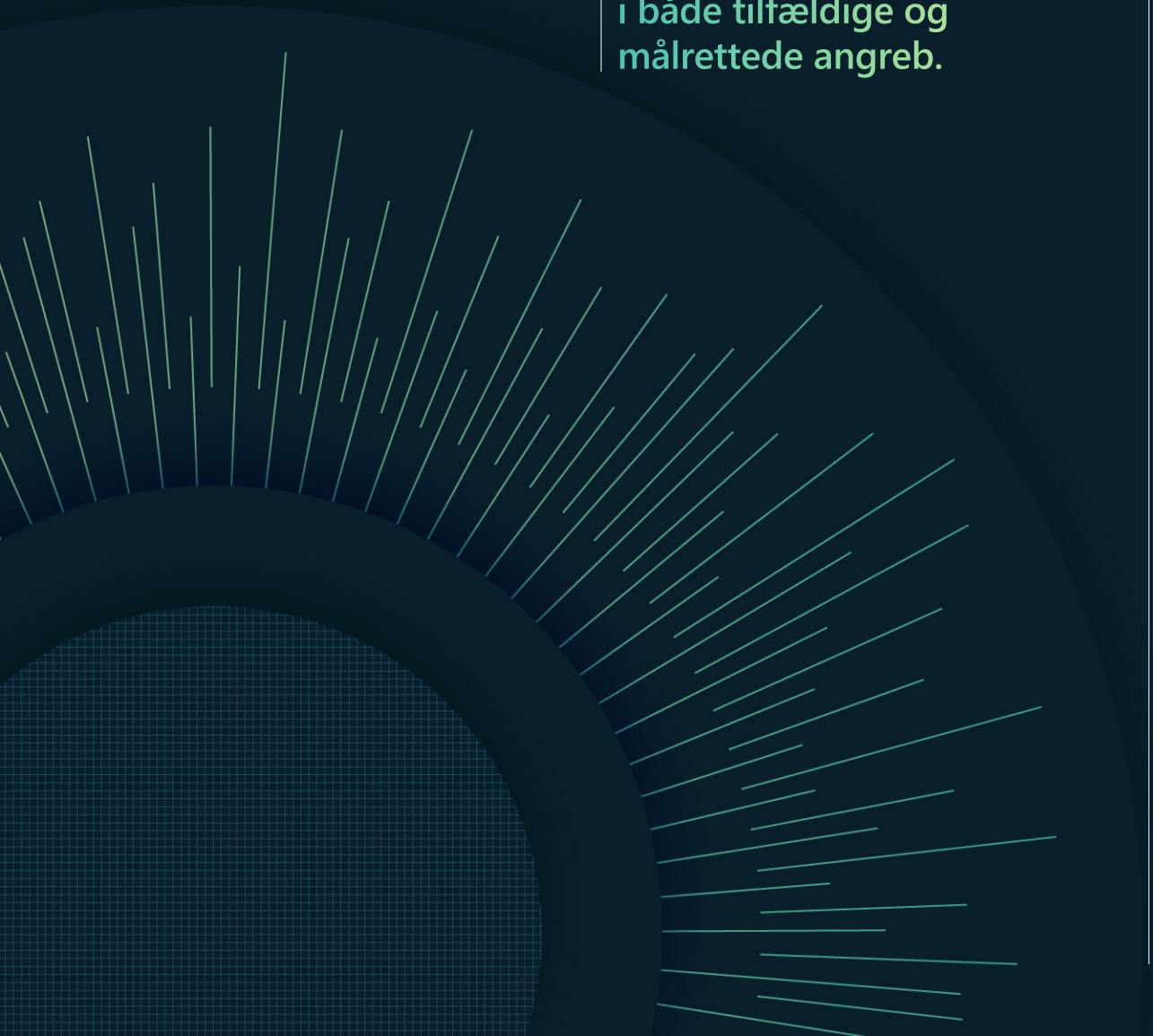
Få mere at vide på side 21

For at sætte en stopper for cyberkriminelles og nationalstatsaktørers ondsindede infrastrukturer er Microsoft afhængig af innovative juridiske lovlige tilgange og vores offentlige og private partnerskaber.

Få mere at vide på side 25

Introduktion

Der sker fortsat en stigning i cyberkriminalitet i både tilfældige og målrettede angreb.



Efterhånden som cyberforsvaret forbedres, og flere myndigheder og virksomheder benytter en proaktiv tilgang til forebyggelse, ser vi, at hackere benytter to strategier til at få den adgang, der er nødvendig for at udøve cyberkriminalitet. Én fremgangsmåde er en bredt målrettet kampagne, der er afhængig af mængde. Den anden bruger overvågning og mere selektiv målretning til at øge afkastet. Selv når målet ikke er at få indtægter – f.eks. nationalstatsaktivitet til geopolitiske formål – anvendes der både tilfældige og målrettede angreb. I det forløbne år anvendte cyberkriminelle stadig social engineering og udnyttelse af aktuelle problemstillinger til at maksimere kampagnesucces. Eksempel: Mens phishingfælder med COVID-tema blev brugt mindre hyppigt, observerede vi fælder, hvor folk blev bedt om donationer til at støtte borgerne i Ukraine.

Angribere tilpasser sig og finder nye måder at implementere deres teknikker på. Dette gør det vanskeligere at vide, hvordan og hvor de har deres kampagneinfrastruktur Vi har bemærket, at cyberkriminelle bliver mere og mere sparsommelige, og at hackere ikke længere betaler for teknologi. For at sænke deres faste omkostninger og øge udseendet af legitimitet forsøger nogle hackere at kompromittere virksomheder til at hoste phishingkampagner, malware eller endda bruge deres computerkraft til mining af kryptovaluta.

I dette kapitel undersøger vi også stigningen i hacktivisme, som er en afbrydelse forårsaget af privatpersoner, der udfører cyberangreb for at fremme sociale eller politiske mål. Tusindvis af mennesker rundt omkring i verden, både eksperter og nybegyndere, har siden februar 2022 mobiliseret sig for at starte angreb som f.eks. at deaktivere websteder og lække stjålne data som en del af krigen mellem Russia og Ukraine. Det er for tidligt at forudsige, om denne tendens vil fortsætte, når de aktive fjendtligheder ophører.

Organisationer skal regelmæssigt gennemgå og styrke adgangskontroller og implementere sikkerhedsstrategier for at forsvare sig mod cyberangreb. Men det er ikke alt, hvad de kan gøre. Vi forklarer, hvordan vores DCU (Digital Crimes Unit) har benyttet civile sager til at konfiskere ondsindet infrastruktur, der bruges af cyberkriminelle og nationalstatsaktører. Vi skal bekæmpe denne trussel i fællesskab gennem både offentlige og private partnerskaber. Vi håber, at vi ved at dele det, vi har erfaret i løbet af de sidste ti år, kan hjælpe andre med at forstå og overveje de proaktive foranstaltninger, de kan træffe for at beskytte sig selv og det bredere økosystem mod den konstant voksende trussel fra cyberkriminalitet.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

Ransomware og afpresning: En trussel på nationalt niveau

Ransomware-angreb udgør en stigende fare for alle enkeltpersoner, da kritisk infrastruktur, virksomheder i alle størrelser samt statslige og lokale myndigheder bliver ramt af kriminelle, der udnytter et voksende cyberkriminelt økosystem.

I de sidste to år har højt profilerede ransomware-hændelser – f.eks. dem, der involverer kritisk infrastruktur, sundhedspleje og it-tjenesteudbydere – opnået betydelig offentlig opmærksomhed. I takt med, at ransomware-angreb er blevet mere dristige i omfang, er deres virkninger blevet mere vidtrækkende. Følgende er eksempler på angreb, vi allerede har oplevet i 2022:

- I februar påvirkede et angreb mod to virksomheder betalingssystemerne på hundredvis af tankstationer i Nordtyskland.[1]
- I marts afbrød et angreb på Grækenlands posttjeneste midlertidigt mailleveringen og påvirkede behandlingen af finansielle transaktioner.[2]
- I slutningen af maj medførte et ransomware-angreb mod de costaricanske myndigheder, at der blev erklæret national nødsituation, efter at hospitalerne var blevet lukket ned, og told- og skatteopkrævningen var blevet afbrudt.[3]
- Også i maj forårsagede et angreb flyforsinkelser og aflysninger for et af Indiens største luftfartsselskaber, hvilket medførte, at hundredvis af passagerer strandede.[4]

Succesen med disse angreb og omfanget af deres konsekvenser i den virkelige verden er resultatet af en industrialisering af cyberkriminalitetsøkonomien, som giver adgang til værktøjer og infrastruktur og udvider de cyberkriminelles muligheder ved at sænke kompetencebarrieren.

I de seneste år er ransomware ændret fra en model, hvor en enkelt "bande" både udviklede og distribuerede ransomware-nyttedata til en ransomware as a service-model (RaaS). RaaS giver en gruppe mulighed for at administrere udviklingen af ransomware-nyttedata og levere tjenester til betaling og afpresning via datalækage til andre cyberkriminelle – dem, der rent faktisk lancerer ransomware-angrebene – også kaldet "associerede selskaber" – mod at få en del af fortjenesten. Denne franchisevirksomhed inden for cyberkriminalitetsøkonomien har udvidet angriberpuljen. Industrialiseringen af cyberkriminelles værktøjer har gjort det nemmere for angribere at udføre indtrængen, eksfiltrere data og implementere ransomware.

Menneskedrevet ransomware[5] er stadig en alvorlig trussel mod organisationer. Begrebet er opfundet af Microsoft-forskere til at beskrive trusler drevet af mennesker, der træffer beslutninger i alle faser af angrebene baseret på, hvad de opdager i deres målnetværk og begrænser de traditionelle ransomware-angreb.

Model baseret på Microsoft Defender for Endpoint-data (EDR) (januar-juni 2022).

Ransomware og afpresning: En trussel på nationalt niveau

Fortsat

Ransomware-angreb er blevet endnu mere virkningsfulde, efterhånden som indførelsen af en strategi med dobbeltafpresning af penge er blevet en standardpraksis. Dette omfatter eksfiltrering af data fra kompromitterede enheder, kryptering af data på enhederne og derefter sende eller true med at offentliggøre de stjålne data for at presse ofrene til at betale en løsesum.

Selvom de fleste ransomware-angribere opportunistisk implementerer ransomware i et hvilket som helst netværk, de får adgang til, køber nogle adgang fra andre cyberkriminelle og udnytter forbindelser mellem adgangsmæglere og ransomware-operatører.

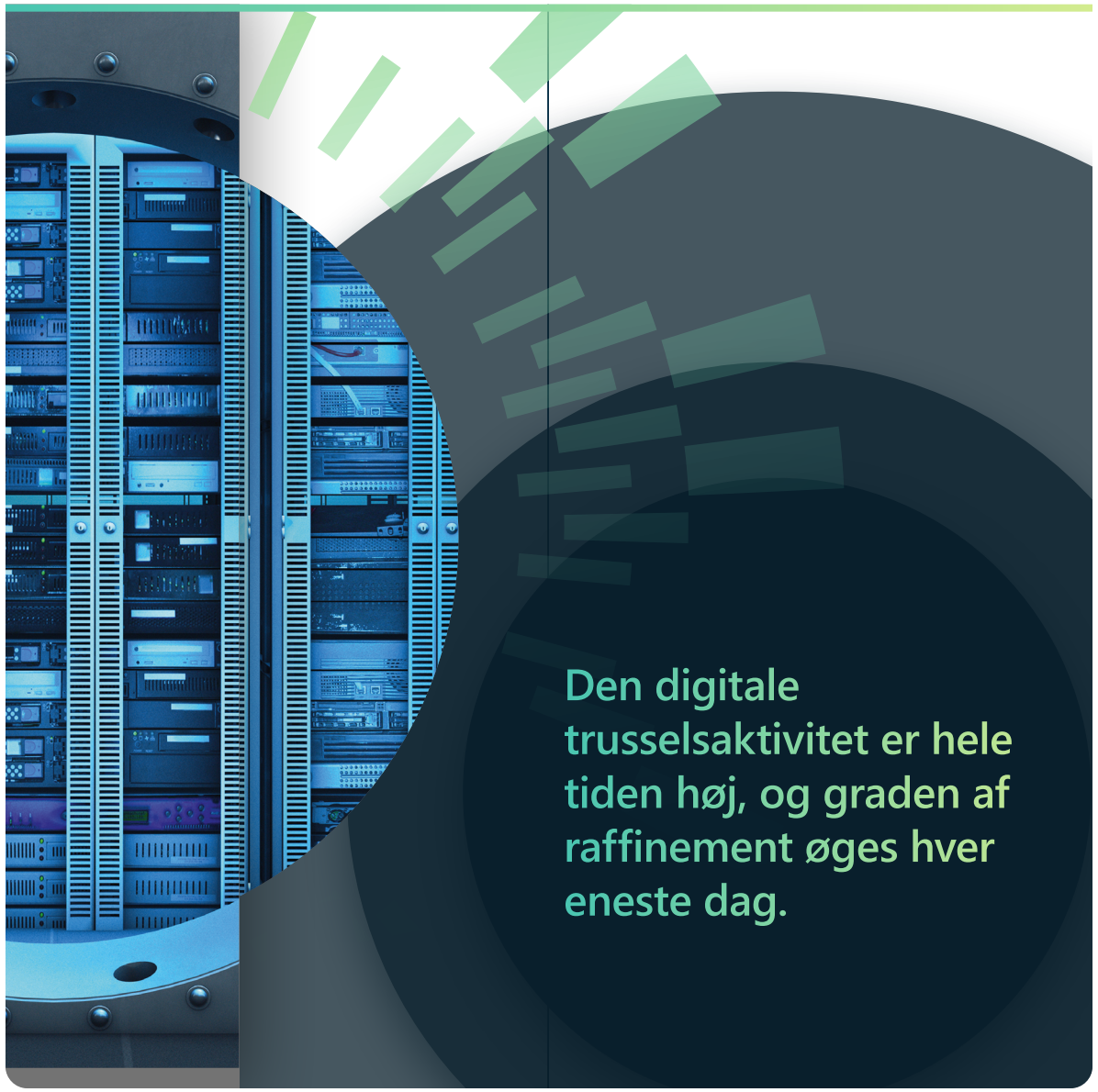
Vores unikke bredde af signalintelligens indsamles fra flere kilder – identitet, mail, endpoints og cloud-løsninger – og giver indsigt i den voksende ransomware-økonomi, komplet med et associeret system, som omfatter værktøjer designet til mindre teknisk dygtige angribere.

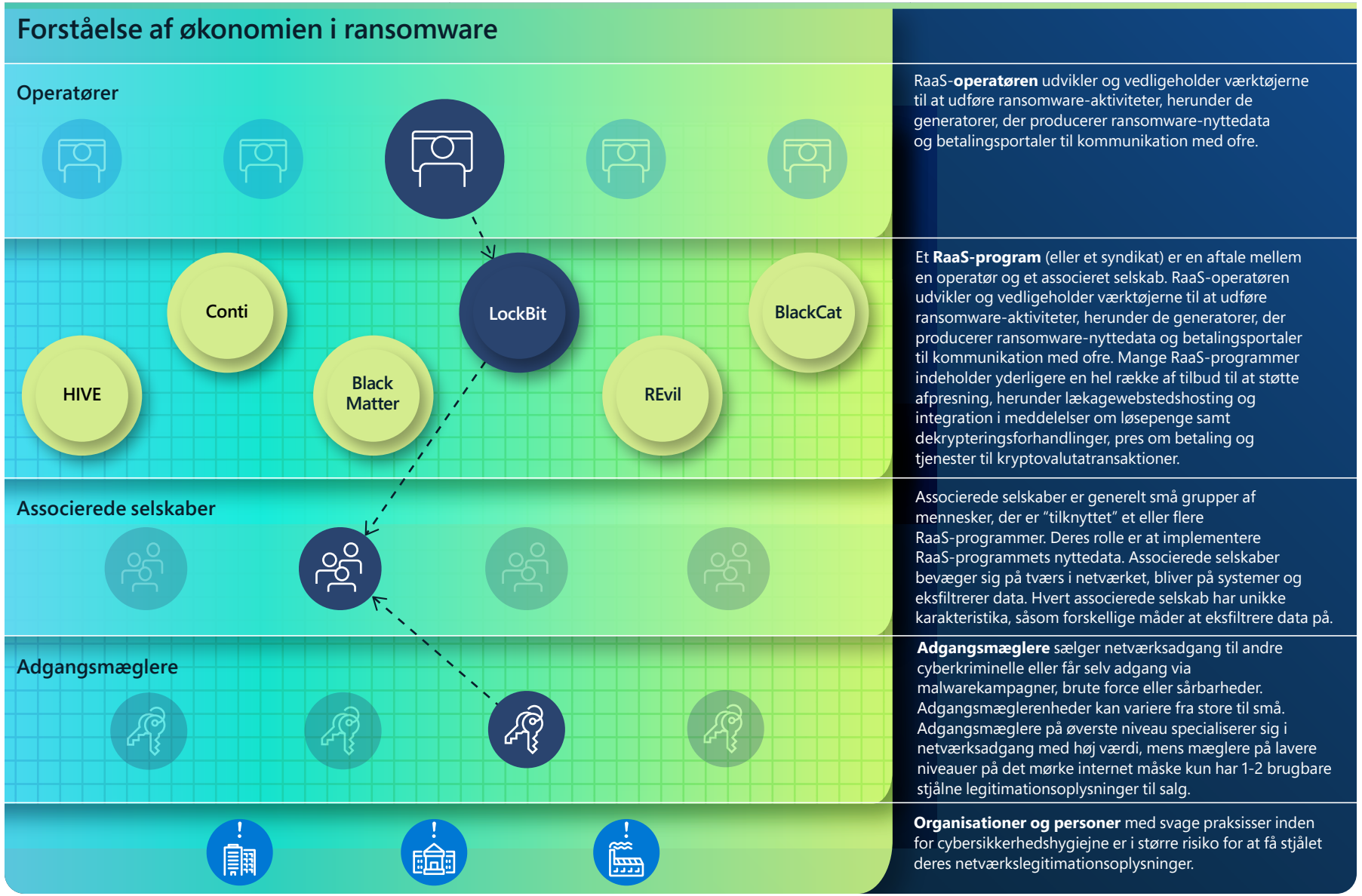
De udvidede relationer mellem specialiserede cyberkriminelle har gjort ransomware-angreb hyppigere, mere sofistikerede og succesfulde. Dette har drevet udviklingen af det cyberkriminelle økosystem til et netværk af aktører med forskellige teknikker, mål og kompetencer, der støtter hinanden i den indledende adgang til mål, betalingstjenester og dekrypterings- eller publikationsværktøjer eller -websteder.

Ransomware-operatører kan nu købe adgang til organisationer eller offentlige netværk online eller købe legitimationsoplysninger og adgang via personlige relationer med mæglere, hvis primære mål er udelukkende at tjene penge på den adgang, de har opnået.

Operatørerne bruger derefter den købte adgang til at implementere ransomware-nyttedata, der er købt via webmarkedspladser eller forummer på det mørke internet. I mange tilfælde foregår forhandlingerne med ofrene med RaaS-teamet, ikke operatørerne selv. Disse kriminelle transaktioner er problemfri, og deltagerne løber kun en lille risiko for at blive anholdt og sigtet. Dette skyldes anonymiteten på det mørke internet og problemer med at håndhæve tværnationale love.

En bæredygtig og vellykket indsats mod denne trussel vil kræve en helhedsstrategi mellem myndighederne i tæt partnerskab med den private sektor.





I modsætning til, hvordan ransomware nogle gange fremstilles i medierne, er det sjældent, at en enkelt ransomware-variant administreres fuldstændigt af en "ransomware-bande". I stedet er der særskilte enheder, der udvikler malware, andre, der får adgang til ofre, andre, der implementerer ransomware og endnu andre, der håndterer afpresningsforhandlinger. Industrialiseringen af det kriminelle økosystem har ført til:

- Adgangsmæglere, der bryder ind og giver adgang (adgang som en service).
- Malwareudviklere, der sælger værktøjer.
- Kriminelle operatører og associerede selskaber, der udfører indtrængen.
- Krypterings- og afpresningstjenester, der håndterer indtjeningen fra associerede selskaber (RaaS).

Alle menneskedrevne ransomware-kampagner er afhængige af sikkerhedssvagheder. Specifikt udnytter angriberne normalt en organisations dårlige cyberhygiejne, hvilket ofte omfatter sjældne programrettelser og manglende implementering af multifaktorgodkendelse (MFA).

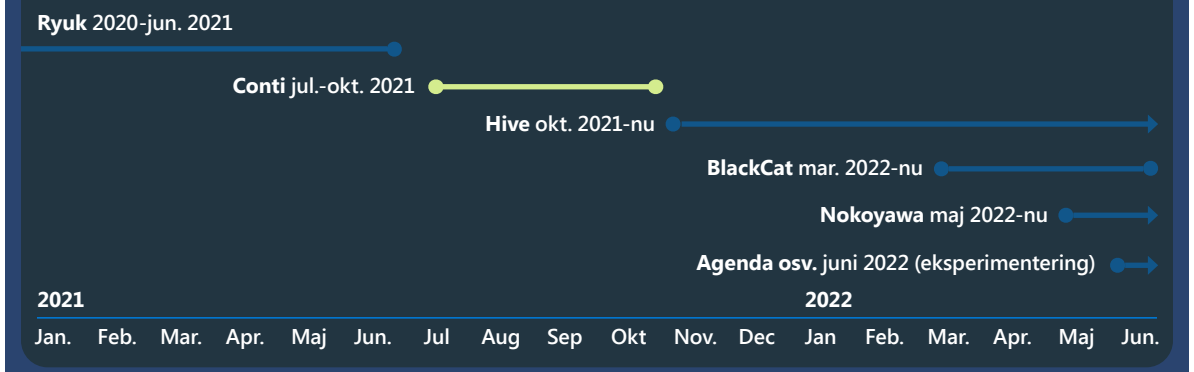
Case study: Opløsningen af Conti

Conti, en af de største ransomware-varianter i de sidste to år, begyndte at lukke for aktiviteter i midten af 2022, hvor MSTIC (Microsoft Threat Intelligence Center) observerede et betydeligt fald i aktiviteten i slutningen af marts og begyndelsen af april. Vi observerede de sidste Conti ransomware-implementeringer midt i april. Men ligesom lukningen af andre ransomware-aktiviteter havde Conti's opløsning ikke nogen betydelig indvirkning på ransomware-implementeringer. MSTIC observerede, at Conti-associerede selskaber omstillede sig og begyndte at implementere andre ransomware-nyttedata, herunder BlackBasta, Lockbit 2.0, LockbitBlack og HIVE. Dette er i overensstemmelse med data fra tidligere år og tyder på, at når ransomware-bander går offline, dukker de op igen flere måneder senere eller omfordeler deres tekniske kapacitet og ressourcer til nye grupper.

Microsofts trusselsefterretningsteam sporer ransomware-trusselsaktører som individuelle grupper (kaldet DEV'er) baseret på deres specifikke værktøjer i stedet for at spore dem efter den malware, de bruger. Det betød, at da Contis associerede selskaber spredte sig, kunne vi fortsætte med at spore disse DEV'er gennem deres brug af andre værktøjer eller RaaS-kits. Eksempel:

- DEV-0230, som er tilknyttet Trickbot, havde været en produktiv bruger af Conti. I slutningen af april observerede MSTIC det ved hjælp af QuantumLocker.
- DEV-0237 skiftede fra Conti's ransomware-kit til HIVE og Nokoyawa, herunder brug af HIVE i angrebet den 31. maj mod de costaricanske myndigheder.
- DEV-0506, en anden produktiv bruger af Conti's ransomware-kit, blev observeret ved hjælp af BlackBasta.

Eksempel på et associeret selskab (DEV-0237), der hurtigt skifter mellem RaaS-programmer



Når et RaaS-program som Conti er lukket ned, skifter ransomware-partneren til et andet (Hive) næsten øjeblikkeligt.

RaaS udvikler ransomware-økosystemet og forhindrer tilskrivning

Da menneskeligt drevet ransomware drives af individuelle operatører, varierer angrebsmønstrene baseret på mål og alternativer i hele angrebets varighed. Tidligere observerede vi en tæt relation mellem den indledende indgangsmetode, værktøjerne og valg af ransomware-nyttedata i hver kampagne for en enkelt ransomware-type. Dette gjorde tilskrivningen nemmere. RaaS-partnermodellen frakobler dog denne relation. Som et resultat sporer Microsoft ransomware-associerede selskaber, som implementerer nyttedata i specifikke angreb, i stedet for at spore udviklere af ransomware-nyttedata som operatører.

Vi antager med andre ord ikke længere, at HIVE-udvikleren er operatøren bag et HIVE-ransomware-angreb. Det er mere sandsynligt, at det er et associeret selskab.

Cybersikkerhedsbranchen har haft svært ved at registrere denne afgrænsning mellem udviklere og operatører i tilstrækkeligt omfang. Branchen rapporterer stadig ofte en ransomware-hændelse med dens nyttedatanavn, hvilket giver det falske indtryk, at en enkelt enhed, eller ransomware-bande, står bag alle angreb, som benytter disse særlige ransomware-nyttedata, og at alle hændelser, der er forbundet med den, anvender fælles teknikker og infrastruktur. For at støtte netværksforsvarere er det vigtigt at lære mere om de faser, der går forud for forskellige associerede selskabers angreb – f.eks. dataeksfiltrering og yderligere vedholdenhedsmekanismer – og de registrerings- og beskyttelsesmuligheder, der måtte findes.

Angribere skal bruge legitimationsoplysninger for at få succes med deres handlinger, ikke så meget skadelig kode. En vellykket menneskeligt drevet ransomware-infektion i en hel organisation er afhængig af adgang til en konto med et højt adgangsniveau.

Fokus på menneskedrevne ransomware-angreb

I løbet af det seneste år har Microsofts ransomware-eksperter gennemført dybdegående undersøgelser af mere end 100 menneskedrevne ransomware-hændelser for at spore angribernes teknikker og forstå, hvordan vi bedre kan beskytte vores kunder.

Det er vigtigt at bemærke, at den analyse, vi deler her, kun er mulig for onboardede, administrerede enheder. Ikke-onboardede, ikke-administrerede enheder udgør den mindst sikre del af en organisations hardwareaktiver.

Mest udbredte teknikker i ransomware-faser:

75 %
Bruger administratorværktøjer.

75 %
Bruger kompromitteret brugerkonto med højt rettighedsniveau til at sprede skadelige nyttedata via SMB-protokollen.

99 %
Forsøger at manipulere med opdagede sikkerheds- og backupprodukter ved hjælp af OS-opbyggede værktøjer.

Det typiske menneskedrevne angreb

Menneskedrevne ransomware-angreb kan kategoriseres i fasen for præ-ransomware og fasen for ransomware-implementering. I fasen for præ-ransomware forbereder angriberne sig på at infiltrere netværket ved at lære om organisationens typologi og sikkerhedsinfrastruktur.

Stop angriberne, før de når ransomware-implementering sfasen	**Implementering!**
Præ-ransomware	**Ransomware**
Denne fase kan variere fra et par dage til flere uger eller måneder, selvom den er blevet kortere i løbet af de sidste to år.	Denne fase kan vare i blot nogle få minutter
Angribere forbereder sig på at infiltrere netværket ved at lære så meget som muligt om topologien og sikkerhedsinfrastrukturen. Angribere kan også eksfiltrere data i denne fase..	Angribere sigter mod at kryptere så mange data som muligt

Vores undersøgelser viste, at de fleste aktører bag menneskedrevne ransomware-angreb udnytter lignende sikkerhedssvagheder og anvender de samme angrebsmønstre og -teknikker.

En holdbar sikkerhedsstrategi

Bekæmpelse og forhindring af angreb af denne art kræver et skift i organisationens tankegang for at fokusere på den omfattende beskyttelse, der kræves for at bremse og stoppe angribere, før de kan gå fra fasen for præ-ransomware til fasen for implementering af ransomware.

Virksomhederne skal anvende bedste sikkerhedspraksis konsekvent og aggressivt på deres netværk for at reducere mængden af angreb. På grund af den menneskelige beslutningstagning kan disse ransomware-angreb generere flere, tilsyneladende uensartede sikkerhedsproduktadvarsler, som nemt kan gå tabt eller ikke reageres på i tide. Advarselstræthed er reel, og SOC'er (Security Operations Centers) kan gøre livet nemmere ved at se på tendenser i deres advarsler eller gruppere advarsler i hændelser, så de kan se det store perspektiv. SOC'er kan reducere advarsler ved hjælp af hærdningsfunktioner som f.eks. regler for at reducere angrebsflader. Hærdning mod almindelige trusler kan ikke kun reducere advarselsmængden. De kan også stoppe mange angribere, før de får adgang til netværk.

Organisationer skal opretholde kontinuerlige høje standarder for sikkerhedsforhold og netværkshygiejne for at beskytte sig mod menneskedrevne ransomware-angreb.

Handlingsrettet indsigt

Ransomware-angribere er motiveret af nem fortjeneste, så øgede omkostninger ved at styrke sikkerheden er nøglen til at forstyrre cyberkriminalitetsøkonomien.

1. Opbyg større bevidsthed om beskyttelse af legitimationsoplysninger. Angribere skal bruge legitimationsoplysninger for at få succes med deres handlinger, ikke så meget skadelig kode. En vellykket menneskedrevet ransomware-infektion i en hel organisation afhænger af adgang til en konto med højt adgangsniveau, f.eks. en domæneadministrator, eller mulighed for at redigere en gruppepolitik.
2. Overvåg eksponering af legitimationsoplysninger.
3. Prioriter implementering af Active Directory-opdateringer.
4. Prioriter cloud-hærdning.
5. Reducer angrebsfladen.
6. Hærd internetbaserede aktiver, og forstå netværkets perimeter.
7. Reducer SOC-advarselstræthed ved at hærde dit netværk for at reducere mængden og have tilstrækkelig båndbredde til højt prioriterede hændelser.

Links til yderligere oplysninger

- RaaS: Forståelse af gig-økonomien for cyberkriminalitet, og hvordan du beskytter dig selv | Microsoft Security Blog
- Menneskedrevne ransomware-angreb: En katastrofe, der kan forhindres | Microsoft Security Blog

Ransomware-indsigt fra frontlinjerespondenter

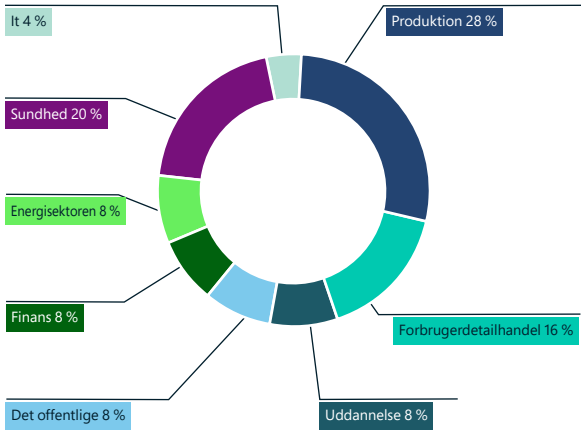
Organisationer over hele verden oplevede en støt vækst i menneskedrevne ransomware-angreb fra og med 2019. Men retshåndhævende myndigheder og geopolitiske begivenheder i det seneste år har haft en betydelig indvirkning på cyberkriminelle organisationer.

Microsofts Security Service Line understøtter kunderne gennem et helt cyberangreb, fra undersøgelse til inddæmning og genoprettelsesaktiviteter. Respons- og gendannelsestjenesterne tilbydes via to yderst integrerede teams, hvor det ene fokuserer på undersøgelsen og det grundlæggende arbejde med gendannelse, og det anden fokuserer på inddæmning og gendannelse. Dette afsnit indeholder en oversigt over resultaterne baseret på ransomware-aktiviteter i løbet af det seneste år.

93 %

af Microsofts undersøgelser under indvindingsengagementer afslørede utilstrækkelig kontrol af adgangsrettigheder og kontrol af tværgående bevægelser.

Ransomware-hændelser og indvindingsaktiviteter efter branche

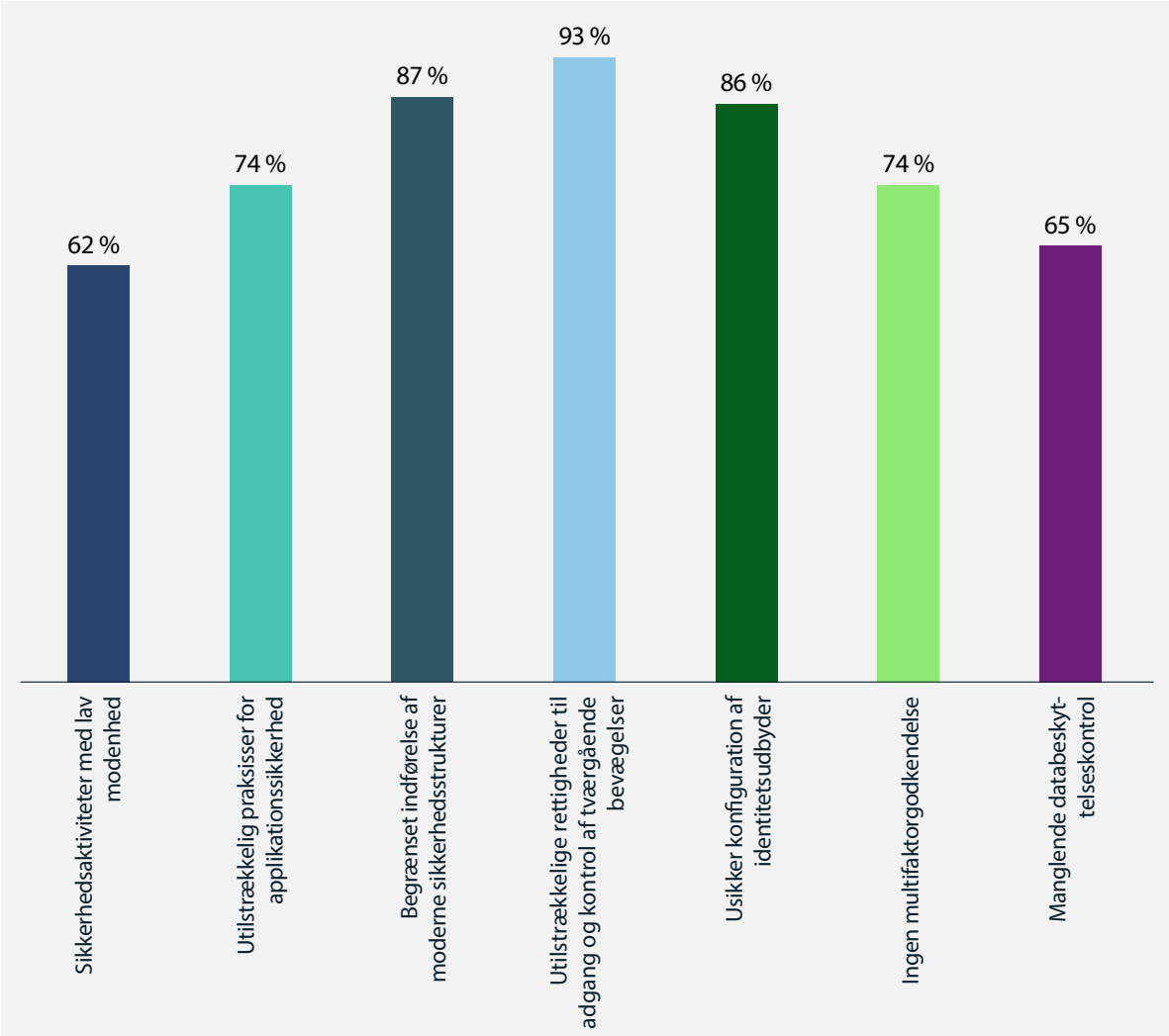


Efterhånden som der dukker nye mindre grupper og trusler op, skal forsvarsteamene være opmærksomme på nye ransomware-trusler, samtidig med at de beskytter mod tidligere ukendte malware-familier. Tilgangen med hurtig udvikling, som anvendes af kriminelle grupper, førte til oprettelsen af intelligent ransomware pakket i brugervenlige kits. Dette giver større fleksibilitet ved lancering af udbredte angreb mod et højere antal mål.

De følgende sider giver et dybere indblik i de mest almindeligt observerede medvirkende faktorer til svag beskyttelse mod ransomware, grupperet i tre kategorier af resultater:

1. Svage identitetskontroller
2. Ineffektive sikkerhedsaktiviteter
3. Begrænset databeskyttelse

Oversigt over de mest almindelige resultater i forbindelse med respons på ransomware



Det mest almindelige resultat blandt interaktioner med ransomware-hændelser var utilstrækkelig kontrol af adgangsrettigheder og kontrol af tværgående bevægelser

Ransomware-indsigt fra frontlinjerespondenter

Fortsat

De tre vigtigste faktorer, vi ser i vores interaktioner med onsite respons:

① **Svage identitetskontroller:** Tyveri af legitimationsoplysninger er fortsat en af de mest anvendte medvirkende faktorer

② **Ineffektive sikkerheds-processer** udgør ikke blot en mulighed for angribere, men påvirker i høj grad den tid, det tager at gendanne data

③ Det handler i bund og grund om data – organisationer kæmper for at implementere en effektiv databeskyttelsesstrategi, der passer til deres forretningsbehov

① Svage identitetskontroller

Menneskedrevet ransomware fortsætter med at udvikle sig og anvender tyveri af legitimationsoplysninger og metoder til tværgående bevægelse, hvilket traditionelt er forbundet med målrettede angreb. Vellykkede angreb er ofte resultatet af langvarige kampagner, der involverer kompromitterede identitetssystemer som Active Directory (AD), der giver menneskelige operatører mulighed for at stjæle legitimationsoplysninger, få adgang til systemer og forblive i netværket.

Active Directory (AD) og Azure AD-sikkerhed

88 %

af de påvirkede kunder brugte ikke bedste fremgangsmåder for AD- og Azure AD-sikkerhed. Dette er blevet en almindelig angrebsvektor, da angribere udnytter fejlkonfigurationer og svage sikkerhedsforhold i kritiske identitetssystemer til at få bredere adgang til og indvirkning på virksomheder.

Sikkerhed for privilegeret konto

88 %

af engagementer, hvor MFA ikke var implementeret for følsomme og højt privilegerede konti, hvilket udgør et sikkerhedshul, som angribere kan bruge til at kompromittere legitimationsoplysninger og starte yderligere angreb ved hjælp af lovlige legitimationsoplysninger.

Adgang med færrest mulige rettigheder og brug af arbejdsstationer med privilegeret adgang (PAW)

Ingen af de påvirkede organisationer implementerede korrekt adskilte administrative legitimationsoplysninger og principper for adgang med færrest mulige rettigheder via dedikerede arbejdsstationer under management af deres kritiske identitet og mest værdifulde aktiver, f.eks. egne systemer og forretningskritiske applikationer.

84 %

Administratorer på tværs af 84 % af organisationerne brugte ikke identitetskontroller for rettigheder, f.eks. just-in-time-adgang, til at forhindre yderligere misbrug af kompromitterede privilegerede legitimationsoplysninger.

Ransomware-indsigt fra frontlinjerespondenter

Fortsat

② Ineffektive sikkerhedsaktiviteter

Vores data viser, at organisationer, der har været udsat for ransomware-angreb, har betydelige huller, når det gælder management af sikkerhedsoperationer, værktøjer og livscyklussen for aktivers informationsteknologi. Baseret på de tilgængelige data blev følgende huller mest observeret:

Fejlretning:

68 %

af de påvirkede organisationer havde ikke en effektiv proces til administration af sårbarheder og programrettelser og en høj afhængighed af manuelle processer kontra automatiserede programrettelser førte til kritiske åbninger. Produktionsinfrastruktur og kritisk infrastruktur kæmper fortsat med vedligeholdelse og programrettelser af ældre driftsteknologisystemer (OT).

Mangel på værktøjer til sikkerhedsoperationer:

De fleste organisationer rapporterede en mangel på synlighed fra start til slut på grund af manglende eller forkert konfiguration af sikkerhedsværktøjer, hvilket førte til en mindre effektivitet i forbindelse med registrering og respons.

60 %

af organisationerne rapporterede, at de ikke havde brugt et EDR[6]-værktøj, som er en grundlæggende teknologi til registrering og respons.

60 %

investerede ikke i SIEM-teknologi (Security Information and Event Management), der førte til overvågningssiloer, begrænset evne til at registrere end-to-end-trusler og ineffektive sikkerhedsoperationer. Automatisering er stadig en central mangel i SOC-værktøjer og -processer, og dette tvinger SOC-medarbejderne til at bruge utallige timer på at forstå sikkerhedstelemetri.

84 %

af de påvirkede organisationer aktiverede ikke integration af deres multi-cloud-miljøer i deres værktøjer til sikkerhedsoperationer.

Respons- og gendannelsesprocesser:

76 %

Mangel på en effektiv responsplan var et kritisk område, der blev observeret i 76 % af de påvirkede organisationer, hvilket forhindrede en tilstrækkelig organisatorisk kriseparathed og havde en negativ indvirkning på tiden til at reagere og komme sig.

③ Begrænset databeskyttelse

Mange kompromitterede organisationer manglede tilstrækkelige databeskyttelsesprocesser, hvilket førte til alvorlige konsekvenser for gendannelsestider og muligheden for at vende tilbage til forretningsdrift. De mest almindelige huller, der blev opdaget, omfatter:

Uforanderlig backup:

44 %

af organisationerne havde ikke uforanderlige backups til de påvirkede systemer. Data viser også, at administratorer ikke havde backups og genopretningsplaner for kritiske aktiver som f.eks. AD.

Forebyggelse af datatab:

Angribere finder normalt deres måde at kompromittere systemer på ved at udnytte sårbarheder i organisationen, eksfiltrere kritiske data til afpresning, tyveri af immaterielle rettigheder eller indtægtsgenerering.

92 %

af de påvirkede organisationer implementerede ikke effektive kontroller til forebyggelse af datatab for at afbøde disse risici, og dette førte til kritisk datatab.

Ransomware har været faldende i nogle områder og er steget i andre

I år har vi observeret et fald i det samlede antal ransomware-sager, der er rapporteret af vores responsteams i Nordamerika og Europa, sammenlignet med året før. Samtidig steg antallet af rapporterede tilfælde i Latinamerika.

En fortolkning af denne observation er, at cyberkriminelle vender sig væk fra områder, der opfattes som havende en højere risiko for at udløse en undersøgelse fra retshåndhævende myndigheder til fordel for blødere mål. Da Microsoft ikke observerede en betydelig forbedring af sikkerheden i virksomhedsnetværk på verdensplan, som kunne forklare faldet i ransomware-relaterede supportopkald, mener vi, at den mest sandsynlige årsag er en kombination af retshåndhævende aktiviteter i 2021 og 2022, som øgede omkostningerne til kriminelle aktiviteter sammen med nogle geopolitiske begivenheder i 2022.

En af de mest almindelige RaaS-operationer er forbundet med en russisktalende kriminel gruppe med navnet REvil (også kendt som Sodinokibi), som har været aktiv siden 2019. I oktober 2021 blev REvils servere taget offline som en del af den internationale retshåndhævende GoldDust-kampagne.[7] I januar 2022 anholdt Rusland 14 påståede REvil-medlemmer og ransagede 25 steder, som havde forbindelse til dem.[8] Det var første gang, at russerne handlede mod ransomware-operatører på deres egen jord.

Mens retshåndhævende aktiviteter sandsynligvis satte en stopper for hyppigheden af angreb i 2022, kan trusselsaktører nemt udvikle nye strategier for at undgå at blive fanget i fremtiden. Derudover ser spændingerne mellem Rusland og USA ud til at have sat en stopper for det spirende russiske samarbejde i den globale kamp mod ransomware. Efter en kort periode med usikkerhed efter disse REvil-anholdelser indstillede USA og Rusland samarbejdet i jagten på ransomware-aktører. Dette betyder, at cyberkriminelle igen kan se Rusland som et sikkert sted.

Når vi ser fremad, forudser vi, at tempoet af ransomware-aktiviteter vil afhænge af resultatet af nogle vigtige spørgsmål:

1. Vil forskellige landes myndigheder træffe foranstaltninger til at forhindre ransomware-kriminelle i at operere inden for deres grænser eller forsøge at stoppe aktører, der opererer fra fremmed jord?
2. Vil ransomware-grupper ændre taktik for at fjerne behovet for ransomware og gribe til afpresningsangreb?
3. Vil organisationer kunne modernisere og transformere deres it-aktiviteter hurtigere, end kriminelle kan udnytte sårbarheder?
4. Vil fremskridt inden for sporing af løsesumsbetalinger tvinge løsesumsmodtagere til at ændre taktik og forhandlingsmetoder?

Mens retshåndhævende aktiviteter sandsynligvis satte en stopper for hyppigheden af angreb i 2022, kan trusselsaktører nemt udvikle nye strategier for at undgå at blive fanget i fremtiden.

2x

Antallet af ransomware-angreb faldt i nogle områder, men kravene om løsesum blev mere end fordoblet.

Handlingsrettet indsigt

1. Fokuser på holistiske sikkerhedsstrategier, da alle ransomware-familier udnytter de samme sikkerhedssvagheder til at påvirke et netværk.
2. Opdater og vedligehold sikkerhedsgrundlaget for at øge sikkerhedsforsvaret i dybden for at sikre beskyttelse og modernisere sikkerhedsdriften. Ved at flytte til cloud-løsningen kan du opdage trusler hurtigere og reagere hurtigere.

Links til yderligere oplysninger

- Beskyt din organisation mod ransomware | Microsoft Security
- 7 metoder til at hærde dit miljø mod kompromitteringer | Microsoft Security Blog
- Forbedring af AI-baseret forsvar for at afbryde menneskedrevet ransomware | Microsoft 365 Defender Research Team
- Security Insider: Udforsk den seneste indsigt og opdateringer om cybersikkerhed | Microsoft Security

Cyberkriminalitet som en tjeneste

Cyberkriminalitet som en tjeneste (CaaS) er en voksende trussel under udvikling mod kunder over hele verden. Microsoft Digital Crimes Unit (DCU) observerede fortsat vækst i CaaS-økosystemet med et stigende antal onlinetjenester, der muliggør forskellig cyberkriminalitet, herunder BEC og menneskedrevet ransomware. Phishing er fortsat en foretrukken angrebsmetode, da cyberkriminelle kan opnå betydelig værdi ved at stjæle og sælge adgang til stjålne konti.

Som reaktion på det voksende CaaS-marked forbedrede DCU sine lyttesystemer med det formål at registrere og identificere CaaS-tilbud på tværs af hele økosystemet af internettet, det dybe net, fora med adgangskrav,[9] dedikerede websteder, onlinediskussionsforummer og meddelelsesplatforme.

Cyberkriminelle samarbejder nu på tværs af tidszoner og sprog for at levere specifikke resultater. For eksempel vedligeholder et CaaS-websted, som administreres af en person i Asien, aktiviteter i Europa og opretter ondsindede konti i Afrika. Da disse operationer foregår i mange jurisdiktioner, skaber de komplekse lovgivningsmæssige og håndhævelsesmæssige udfordringer. Derfor fokuserer DCU sin indsats på at deaktivere ondsindet kriminel infrastruktur, der benyttes til at fremme CaaS-angreb, og samarbejde med retshåndhævende myndigheder over hele verden for at holde de kriminelle ansvarlige.

Cyberkriminelle benytter i stigende grad analyser til at maksimere rækkevidden, omfanget og gevinsten. Ligesom almindelige virksomheder skal CaaS sites sikre, at deres produkter og tjenester fungerer for at bevare et godt omdømme. CaaS-websteder automatiserer f.eks. rutinemæssigt adgangen til kompromitterede konti for at sikre, at de kompromitterede legitimationsoplysninger er gyldige. Cyberkriminelle afbryder salget af specifikke konti, når adgangskoder nulstilles eller sårbarheder afhjælpes. Vi har i stigende grad oplevet CaaS-websteder, som forsyner købere med on-demand-verificering som en kvalitetskontrolproces. Som følge heraf er købere sikret, at CaaS-webstedet sælger aktive konti og adgangskoder, og samtidig kan CaaS-forhandleren reducere potentielle omkostninger i tilfælde af, at stjålne legitimationsoplysninger bliver rettet inden salget.

DCU observerede også CaaS-websteder, som tilbyder købere mulighed for at købe kompromitterede konti fra specifikke geografiske placeringer, udvalgte onlinetjenesteudbydere og specifikt målrettede enkeltpersoner, erhverv og brancher. Ofte bestilte konti fokuserer på fagfolk eller afdelinger, der behandler fakturering, f.eks. økonomidirektører eller "Debitorafdelingen". På samme måde målrettes de brancher, der deltager i offentlige kontrakter, ofte på grund af den mængde oplysninger, der stilles til rådighed gennem den offentlige udbudsproces.

DCU-undersøgelser af CaaS viste en række vigtige tendenser:

Antallet og raffinementet af tjenester er stigende.

Et eksempel er udviklingen af webshells, som typisk består af kompromitterede webservere, der bruges til at automatisere phishingangreb. DCU observerede CaaS-forhandlere, der forenklede uploaden af phishingkits eller malware via specialiserede dashboards på internettet. CaaS-sælgere forsøger ofte efterfølgende at sælge yderligere tjenester til trusselsaktøren via dashboardet. Det kunne være spammeddelelsestjenester og specialiserede spammodtagerlister baseret på definerede attributter, herunder geografisk placering eller erhverv. I nogle tilfælde observerede vi, at en enkelt webshell blev benyttet i flere angrebskampagner, hvilket tyder på, at trusselsaktører kan opretholde vedvarende adgang til den kompromitterede server. Vi observerede også en stigning i anonymiseringstjenester, der er tilgængelige som en del af CaaS-økosystemet, samt tilbud på VPN-konti (virtual private networks) og VPNS-konti (virtual private server). I de fleste tilfælde blev VPN'et/VPS'en i første omgang indkøbt ved brug af stjålne kreditkort. CaaS-websteder tilbød også et større antal RDP (Remote Desktop Protocol), SSH (Secure Shell) og cPanels, der kan bruges som platform til at orkestrere cyberkriminalitetsangreb. CaaS-forhandlere konfigurerer RDP-, SSH- og cPanels med passende værktøjer og scripts til at muliggøre forskellige typer cyberangreb.

Tjenester til oprettelse af homoglyfdomæner kræver i stigende grad betaling i kryptovaluta.

Homoglyfdomæner udgiver sig for at være lovlige domænenavne ved at udnytte tegn, der er identiske eller næsten identiske i udseendet med et andet tegn. Målet er at bedrage brugeren til at tro, at homoglyfdomænet er det ægte domæne. Disse domæner findes næsten overalt og er en gateway til en betydelig mængde cyberkriminalitet. CaaS-websteder sælger nu tilpassede homoglyfdomænenavne, hvilket giver køberne mulighed for at anmode om specifikke firma- og domænenavne, som de kan udgive sig for at være. Når betaling er modtaget, bruger CaaS-forhandlere et homoglyfgenereringsværktøj til at vælge domænenavnet og derefter registrere den skadelige homoglyf. Betaling for denne tjeneste sker næsten udelukkende i kryptovaluta.

2.750.000

webstedsregistreringer blev blokeret af DCU i år for at få et forspring i forhold til kriminelle aktører, der planlagde at bruge dem til at engagere sig i global cyberkriminalitet.

Cyberkriminalitet som en tjeneste

Fortsat

CaaS-sælgere tilbyder i stigende grad kompromitterede legitimationsoplysninger.

Kompromitterede legitimationsoplysninger giver uautoriseret adgang til brugerkonti, herunder mailmeddelelsestjeneste, virksomhedens fildelingsressourcer og OneDrive for Business. Hvis en administrators legitimationsoplysninger kompromitteres, kan uautoriserede brugere få adgang til fortrolige filer, Azure-ressourcer og virksomhedens brugerkonti. I mange tilfælde identificerede DCU-undersøgelser uautoriseret brug af de samme legitimationsoplysninger på tværs af flere servere som en måde til at automatisere bekræftelse af legitimationsoplysninger på. Dette mønster tyder på, at den kompromitterede bruger kan være offer for flere phishingangreb eller have malware på sin enhed, som gør det muligt for botnet-keyloggers at indsamle legitimationsoplysninger.

Der dukker CaaS-tjenester og -produkter med forbedrede funktioner op for at undgå registrering.

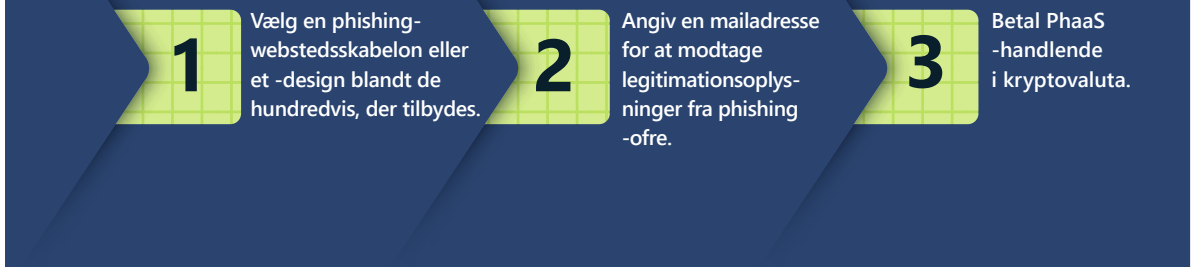
En CaaS-sælger tilbyder phishingkits med øgede lag af kompleksitets- og anonymiseringsfunktioner, der er designet til at omgå registrerings- og forebyggelsessystemer for helt ned til 6 USD pr. dag. Tjenesten tilbyder en række omdirigeringer, der udfører kontroller, før der tillades trafik til det næste lag eller websted. Én af disse kører over 90 kontroller for fingeraftryk på enheden, herunder om der benyttes en virtuel maskine, indsamling af detaljer om browseren og den anvendte hardware med mere. Hvis alle kontroller bestås, sendes trafikken til en landingsside, der bruges til phishing.

Komplette cyberkriminalitetstjenester sælger abonnementer til administrerede tjenester.

Typisk kan hvert enkelt trin i gennemførelsen af en onlinekriminalitet eksponere trusselsaktører, hvis driftssikkerheden er dårlig. Risikoen for eksponering og identifikation øges, hvis der købes tjenester fra flere CaaS-websteder. DCU observerede en bekymrende tendens på det mørke internet, hvor der ses en stigning i tjenesternes tilbud om at anonymisere softwarekode og generalisere webstedstekst for at reducere eksponeringen. Serviceudbydere af komplette abonnementstjenester for cyberkriminalitet administrerer alle tjenester og garanterer resultater, som yderligere reducerer eksponeringsrisici for det OCN, der abonneres på. Den reducerede risiko har øget populariteten af disse komplette tjenester.

Phishing som en tjeneste (PhaaS) er ét eksempel på en komplet cyberkriminalitetstjeneste. PhaaS er en udvikling af tidligere tjenester, der kaldes fuldt uregistrerbare tjenester (FUD), og tilbydes på abonnementsbasis. Typiske PhaaS-vilkår omfatter at holde phishingwebsteder aktive i en måned.

PhaaS, cyberkriminelle tilbyder flere tjenester i et enkelt abonnement. Generelt behøver en køber kun at udføre tre handlinger:



Når disse trin er fuldført, opretter den PhaaS-handlende tjenester med tre eller fire lag omdirigering og hosting af ressourcer for at målrette mod bestemte brugere. Kampagnen lanceres efterfølgende, og ofrenes legitimationsoplysninger høstes, bekræftes og sendes til den mailadresse, som køberen har angivet. Mod en merpris tilbyder mange PhaaS -handlende at hoste phishing-websteder på den offentlige blockchain, så de kan tilgås af enhver browser, og omdirigeringer kan sende brugere videre til en ressource i den distribuerede hovedbog.

DCU identificerede også en CaaS-forhandler, der tilbød DDoS (Distributed Denial of Service) i en abonnementsmodel. Denne model outsourcer oprettelsen og vedligeholdelsen af det botnet, der er nødvendigt for at udføre angreb, til CaaS-forhandleren. Hver DDoS-abonnementskunde modtager en krypteret tjeneste for at forbedre driftssikkerheden og et års 24/7-support. DDoS-abonnementstjenesten tilbyder forskellige arkitekturer og angrebsmetoder, så en køber vælger blot en ressource, der skal angribes. Derefter giver sælgeren adgang til en række kompromitterede enheder på sit botnet for at udføre angrebet. Prisen for DDoS-abonnementet er kun 500 USD.

DCU's arbejde med at udvikle værktøjer og teknikker, der identificerer og afbryder CaaS-cyberkriminelle, foregår på løbende basis. Udviklingen af CaaS-tjenester udgør betydelige udfordringer, især med hensyn til at afbryde betalinger i kryptovaluta.

Kriminel brug af kryptovaluta

Efterhånden som indførelsen af kryptovaluta bliver mere og mere almindelig, bruger de kriminelle den i stigende grad til at omgå retshåndhævende foranstaltninger og AML-foranstaltninger (anti-hvidvask). Dette skaber større udfordringer for retshåndhævende myndigheder i forbindelse med at spore betalinger til cyberkriminelle i kryptovaluta.

De globale udgifter til blockchain-løsninger er steget med ca. 340 % i løbet af de sidste fire år, mens nye kryptovalutategnebøger steg med omkring 270 %. Der er mere end 83 millioner unikke tegnebøger globalt, og den samlede markedskapitalisering af alle kryptovalutaer var ca. 1,1 billion USD pr. 28. juli 2022.[10]

Kilde: Twitter.com—@PeckShieldAlert (PeckShield er et blockchain-sikkerhedsselskab i Kina).

Sporing af ransomware-betalinger

Ransomware er en af de største kilder til ulovlig kryptovaluta. I et forsøg på at afbryde den skadelige tekniske infrastruktur, der benyttes i ransomware-angreb – f.eks. afbrydelsen af Zloader i april 2022[11] – sporer Microsofts DCU kriminelles tegnebøger for at gøre det muligt at aktivere sporing af kryptovaluta og genindvindingsfunktioner.

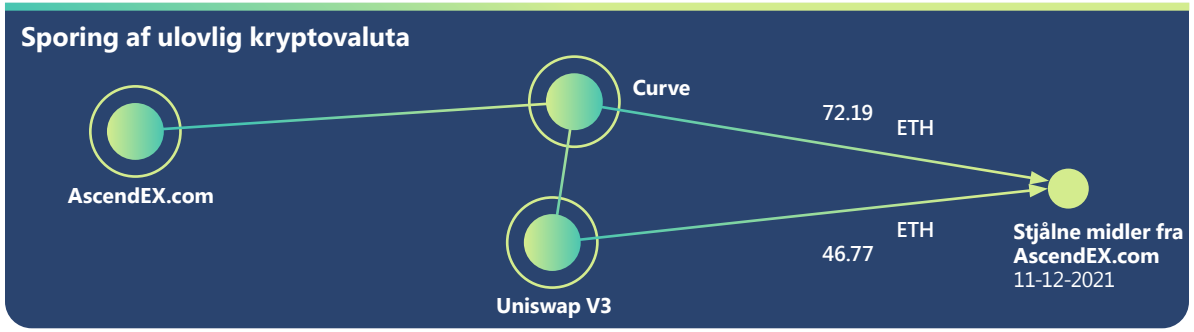
DCU-efterforskere har observeret, at ransomware-aktører udvikler deres kommunikationstaktik med ofre for at skjule pengesporet. Oprindeligt inkluderede cyberkriminelle Bitcoin-adresser i deres meddelelser om løsepenge. Dette gjorde det dog nemt at følge betalingstransaktioner på blockchain'en, så ransomware-aktører holdt op med at inkludere tegnebogsadresser og tilføjede i stedet mailadresser eller links til chatwebsteder for at kommunikere betalingsadresser til ofre. Nogle aktører oprettede endda unikke websider og logins til hvert offer for at forhindre sikkerhedsforskere og retshåndhævende myndigheder i at få fat i de kriminelles tegnebogsadresser ved at udgive sig for at være ofre. På trods af de kriminelles bestræbelser på at skjule deres spor, kan nogle løsepenge stadig indvindes ved at samarbejde med retshåndhævende myndigheder og kryptoanalysevirksomheder, der kan spore bevægelser på blockchain.

Tendens: DEX-hvidvaskning af ulovlig indtjening

Et centralt problem for cyberkriminelle er konvertering af kryptovaluta til fiatvaluta. Cyberkriminelle har flere potentielle muligheder for konvertering, som hver især indebærer en forskellig grad af risiko. En metode, der bruges til at reducere risikoen, er hvidvask af indtægter via en decentraliseret børs (DEX), før pengene udbetales via tilgængelige udbetalingsmuligheder, f.eks. centraliserede børser (CEX), peer-to-peer (P2P) og OTC (over the counter). DEXes er attraktive steder til hvidvask af penge, fordi de ofte ikke overholder foranstaltningerne til bekæmpelse af hvidvask.

I december 2021 angreb hackere den globale kryptovalutahandelsplatform AscendEx og stjal ca. 77,7 millioner USD i kryptovaluta, som tilhørte kunderne.[12] AscendEx hyrede blockchain-analysevirksomheder og kontaktede andre CEX'er, så de tegnebøger, som modtog stjålne midler, kunne blive sortlistet. Derudover blev adresser, hvor pengene blev sendt til, mærket som sådan på Ethereum-blockchain-udforskningen Etherscan.[13] For at omgå advarslen og sortlistningen sendte hackerne 1,5 millioner USD i Ethereum til Uniswap, en af verdens største DEX'er, den 18. februar 2022.[14]

Indførelse af stærkere foranstaltninger til bekæmpelse af hvidvask (AML) kan afhjælpe hvidvask af penge på deres platforme og tvinge cyberkriminelle til at bruge andre tilsløringsmetoder såsom mønttumbling eller udvekslinger uden licens. Som et eksempel annoncerede Uniswap for nylig, at de ville begynde at benytte sortlister til at blokere tegnebøger, der er kendt for at være involveret i ulovlige aktiviteter i forbindelse med transaktioner på børsen.[15]



Ved at benytte værktøjet Chainalysis til undersøgelse af kryptovaluta opdagede Microsofts enhed for digital kriminalitet, at AcendEX-hackerne vekslede deres stjålne midler hos en mindre DEX med navnet Curve ud over Uniswap. Dette diagram illustrerer de hvidvaskruter, som teamet afdækkede. Hver cirkel repræsenterer en klynge af tegnebøger, og tallene på hver linje repræsenterer den samlede mængde Ethereum, der er overført til hvidvaskformål.

Handlingsrettet indsigt

1. Hvis du er offer for cyberkriminalitet, og har betalt den kriminelle i kryptovaluta, skal du kontakte lokale retshåndhævende myndigheder, som kan hjælpe med at spore og inddrive mistede midler.
2. Bliv fortrolig med de ALM-foranstaltninger, der er implementeret, når du vælger en DEX.

Links til yderligere oplysninger

- Hardwarebaseret trusselsforsvar mod stadig mere komplekse cryptojackers | Microsoft 365 Defender Research-team

Phishingtrusselsland-skabet under udvikling

Metoder til phishing efter legitimation-soplysninger bliver stadig mere udbredte og udgør fortsat en betydelig trussel mod brugere overalt, fordi de kritikløst målretter mod alle indbakker. Blandt de trusler, som vores forskere sporer og beskytter mod, er phishingangreb meget større end alle andre trusler, når der er tale om mængder.

Ved at benytte data fra Defender til Office ser vi ondsindet mail og kompromitteret identitetsaktivitet. Azure Active Directory Identity Protection giver endnu flere oplysninger via advarsler om kompromitterede identitetshændelser. Ved at benytte Defender for Cloud Apps ser vi dataadgangshændelser med kompromitterede identiteter, og Microsoft 365 Defender (M365D) giver korrelation på tværs af produkter. Målingen for tværgående bevægelser kommer fra Defender for Endpoint (advarsler og hændelser om angrebsadfærd), Defender for Office (ondsindet mail) og igen M365D for korrelation på tværs af produkter.

710 millioner
phishingmails blokeret om ugen.

1 time 12 min.
Den gennemsnitlige tid, det tager for en angriber at få adgang til dine private data, hvis du bliver offer for en phishingmail.[16]

1 time 42 min.
Gennemsnitstiden, det tager for en angriber at begynde at bevæge sig på tværs inden for virksomhedens netværk, når en enhed er blevet kompromitteret.[17]

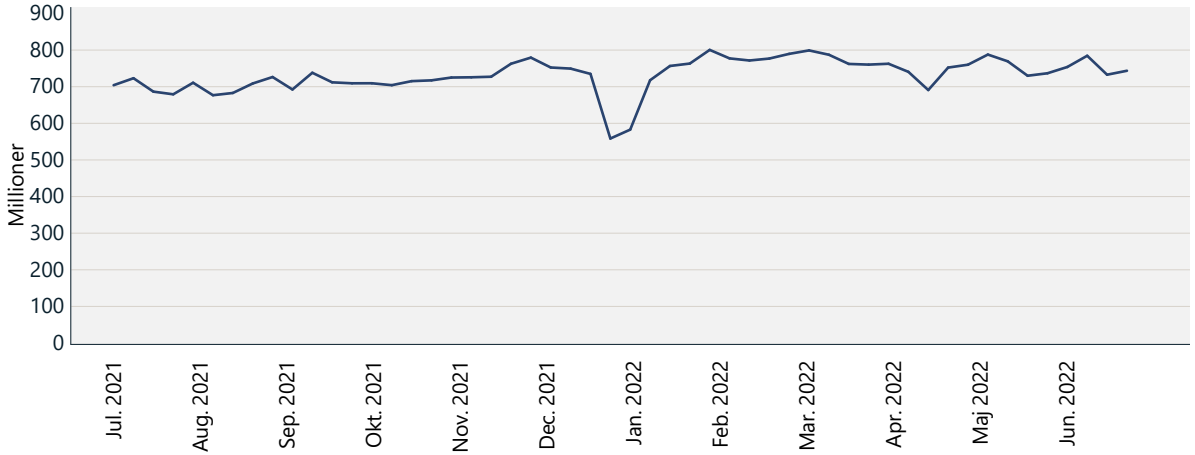
Microsoft 365-legitimationsoplysninger forbliver en af de mest efterspurgte kontotyper for hackere. Når legitimationsoplysninger er kompromitteret, kan angribere logge på virksomhedens forbundne computersystemer for at fremme infektion med malware og ransomware, stjæle fortrolige virksomhedsdata og -oplysninger ved at få adgang til SharePoint-filer og fortsætte udbredelsen af phishing ved at sende yderligere skadelige mails ved hjælp af Outlook, blandt andre handlinger.

Ud over kampagner med bredere mål, phishing efter legitimationsoplysninger, donationer og personlige oplysninger går hackere efter udvalgte virksomheder med henblik på større indtjening. Mail-phishingangreb mod virksomheder for at opnå økonomisk gevinst kaldes samlet for BEC-angreb. Microsoft registrerer millioner af BEC-mails hver måned, hvilket svarer til 0,6 % af alle observerede phishingmails. En rapport fra IC3[18], der blev offentliggjort i maj 2022, indikerer en stigende tendens i tab som følge af BEC-angreb.

De teknikker, der anvendes i phishingangreb, fortsætter med at blive mere komplekse. Som reaktion på modforanstaltninger indfører angribere nye måder at implementere deres teknikker på, og dette øger kompleksiteten af, hvordan og hvor de hoster deres kampagneinfrastruktur Dette betyder, at organisationer regelmæssigt skal revurdere deres strategi for implementering af sikkerhedsløsninger til at blokere skadelige mails og styrke adgangskontrol for individuelle brugerkonti.

531.000
Ud over de URL'er, som er blokeret af Defender for Office, stod vores Digital Crimes Unit for fjernelse af 531.000 unikke phishing-URL'er, der var hostet uden for Microsoft.

Registrerede phishingmails



Antallet af phishingregistreringer hver uge stiger fortsat. Faldet i december-januar er et forventet sæsonbestemt fald, som vi også så i sidste års rapport. Kilde: Exchange Online Protection-signaler.

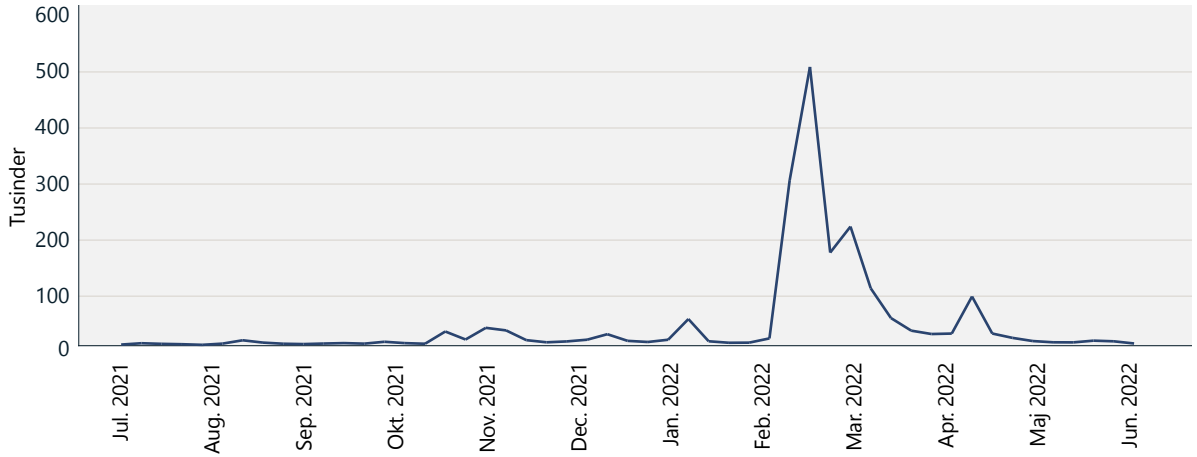
Phishingtrusselslan-dskabet under udvikling

Fortsat

Vi fortsætter med at observere en støt stigning i antallet af phishingmails fra år til år. I forbindelse med skiftet til fjernarbejde i 2020 og 2021 var der en betydelig stigning i phishingangreb, som havde til formål at udnytte det ændrede arbejdsmiljø. Phishingoperatører er hurtige til at indføre nye mailskabeloner med lokkemad, der er relateret til større verdensbegivenheder, f.eks. COVID-19-pandemien og temaer, der er knyttet til samarbejds- og produktivitetsværktøjer, f.eks. Google Drive eller OneDrive-fildeling. Mens der er blevet færre Covid-19-relaterede temaer, blev krigen i Ukraine en ny form for lokkemad, der startede i marts 2022. Vores forskere observerede en svimlende stigning i antallet af mails fra angiveligt lovlige organisationer, hvor man anmodede om donationer i kryptovalutaerne Bitcoin og Ethereum under påskud af at hjælpe borgerne i Ukraine.

Blot et par dage efter starten af krigen i Ukraine i slutningen af februar 2022 steg antallet af registrerede phishingmails, der indeholdt Ethereum-adresser, drastisk på tværs af virksomhedskunder. De samlede angreb toppede i den første uge af marts, hvor en halv million phishingmails indeholdt en Ethereum-tegnebogsadresse. Før starten af krigen var antallet af Ethereum-tegnebogsadresser på andre mails, der blev registreret som phishing, betydeligt mindre og nåede i gennemsnit op på nogle få tusinde mails om dagen.

Phishingmails med Ethereum-tegnebogsadresser



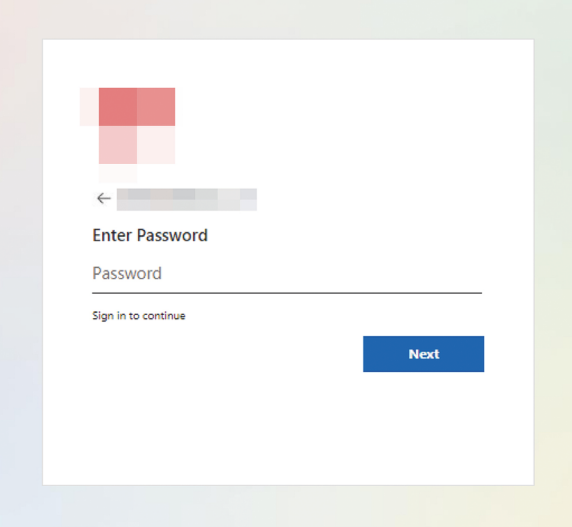
Det samlede antal mails, der blev opdaget som phishing, og som indeholder Ethereum-tegnebogsadresser, steg i starten af konflikten mellem Ukraine og Rusland efter det første fremstød.

Phishingbrugere benytter mere end nogensinde lovlig infrastruktur til deres aktiviteter. Dette fører til en stigning i phishingkampagner, der er rettet mod at kompromittere forskellige aspekter af en operation, så de ikke behøver at købe, hoste eller drive deres egne. Skadelige mails kan f.eks. stamme fra kompromitterede afsenderkonti. Angribere kan drage fordel af at bruge disse mailadresser, som har en højere omdømmescore og opfattes som mere troværdige end nyoprettede konti og domæner. I nogle mere avancerede phishingkampagner observerede vi, at angribere foretrækker at sende og spoofe fra domæner, hvor DMARC[19] er konfigureret forkert med en "ingen handling"-politik, hvilket åbner døren for mail-spoofing.

Store phishingaktiviteter har en tendens til at bruge cloud-tjenester og virtuelle maskiner i cloud-løsningen (VM'er) til at operationalisere angreb i stor skala. Angribere kan automatisere processen med at implementere og levere mails udelukkende fra VM'er ved hjælp af SMTP-mailvideresendelser eller cloud-mailinfrastruktur for at drage fordel af de høje leveringsrater og disse lovlige tjenesters positive omdømme. Hvis skadelig mail har tilladelse til at sendes via disse cloud-tjenester, skal forsvarere benytte stærke funktioner til mailfiltrering for at blokere mails mod at komme ind i deres miljø.

Microsoft forbliver et populært mål for phishingoperatører, hvilket fremgår af de talrige phishinglandingssider, der foregiver at være Microsoft 365-logonsiden. Phishere forsøger f.eks. at matche Microsofts logonoplevelse i deres phishingsæt ved at generere en entydig URL, der er tilpasset modtageren. Denne URL-adresse peger på et skadeligt websted, der er udviklet til at indsamle legitimationsoplysninger, men en parameter i URL'en indeholder den specifikke modtagers mailadresse. Når målet navigerer til siden, udfylder phishingsættet brugerens logondata på forhånd og indsætter et virksomhedslogo, der er tilpasset mailmodtageren, hvilket afspejler udseendet af den målrettede virksomheds tilpassede Microsoft 365-logonside.

En phishing-side, der udgiver sig for at være en Microsoft-logonside med dynamisk indhold

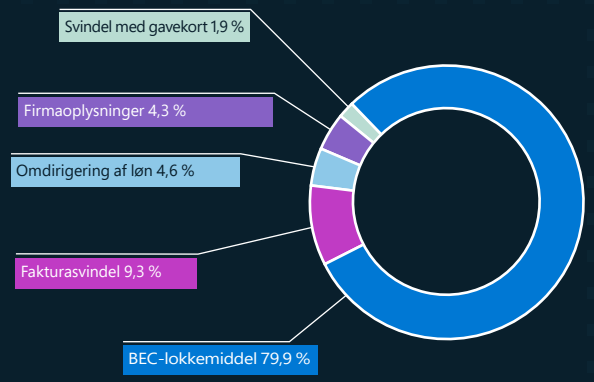


Fokus på kompromittering af virksomhedsmails

Cyberkriminelle udvikler stadig mere komplekse systemer og teknikker til at slippe udenom sikkerhedsindstillinger og målrette mod enkeltpersoner, virksomheder og organisationer. Som reaktion på dette investerer vi betydelige ressourcer for at forbedre vores BEC-håndhævelsesprogram.

BEC er den mest bekostelige finansielle cyberkriminalitet med en anslået værdi på 2,4 milliarder USD i justerede tab i 2021. Dette udgør mere end 59 % af de fem største tab inden for internetkriminalitet globalt.[20] For at forstå omfanget af problemet, og hvordan man bedst beskytter brugerne mod BEC, har Microsofts sikkerhedseksperter sporet de mest almindelige temaer, der anvendes i angreb.

BEC-temaer (januar-juni 2022)



BEC-temaer efter procentdel af forekomster

BEC-tendenser

Som udgangspunkt forsøger BEC-angribere normalt at starte en samtale med potentielle ofre for at etablere en relation. Angriberen udgiver sig for at være en kollega eller et forretningsmæssig bekendtskab og leder gradvist samtalen over på en pengeoverførsel Introduktionsmailen, som vi sporer som en BEC-fælde, repræsenterer tæt på 80 % af de registrerede BEC-mails. Andre tendenser, der er identificeret Microsofts sikkerhedseksperter i det forløbne år, omfatter:

- De hyppigst anvendte teknikker i BEC-angreb, der er observeret i 2022, var spoofing[21]og efterligning.[22]
- Den BEC-undertype, der forårsagede de mest økonomisk skade for ofrene, var fakturasvindel (baseret på mængden og de anmodede dollarbeløb, som vi så i vores BEC-kampagneundersøgelser).
- Tyveri af virksomhedsoplysninger, f.eks. kreditrapporter og kundekontakter, gør det muligt for angribere at begå fakturasvindel.
- De fleste anmodninger om omdirigering af løn blev sendt fra mailtjenester uden omkostninger og sjældent fra kompromitterede konti. Mængden af mails fra disse kilder toppede omkring den første og femtende i hver måned, som er de mest almindelige lønudbetalingsdatoer.
- På trods af at det er en velkendt metode til at begå svindel, udgjorde svindel med gavekort kun 1,9 % af de identificerede BEC-angreb.

Handlingsrettet indsigt

Forsvar mod phishing

For at reducere din organisations eksponering for phishing opfordres it-administratorer til at implementere følgende politikker og funktioner:

1. Kræv, at der benyttes MFA på tværs af alle konti for at begrænse uautoriseret adgang.
2. Aktivér funktioner med betinget adgang for konti med højt privilegeret adgang for at blokere adgang fra lande, regioner og IP-adresser, der typisk ikke genererer trafik i organisationen.
3. Overvej at bruge fysiske sikkerhedsnøgler til ledere, medarbejdere, der er involveret i betalings- eller købsaktiviteter, og andre privilegerede konti.
4. Håndhæv brugen af browsere, der understøtter tjenester som f.eks. Microsoft SmartScreen, for at analysere webadresser for mistænkelig adfærd og blokere adgang til kendte ondsindede websteder.[23]
5. Brug en sikkerhedsløsning baseret på maskinlæring, der sætter sandsynlige phishingmails i karantæne, og som placerer webadresser og vedhæftede filer i en sandkasse, før mailen når indbakken, f.eks. Microsoft Defender til Office 365.[24]
6. Aktivér beskyttelsesfunktioner mod efterligning og spoofing på tværs af organisationen.
7. Konfigurer DKIM- (DomainKeys Identified Mail) og DMARC-politikker (Domain-based Message Authentication Reporting & Conformance) for at forhindre levering af ikke-godkendte mails, der kan være forsøg på spoofing af velrenommerede afsendere.
8. Overvåg lejer og brugeroprettede tilladelsesregler, og fjern brede domæne- og IP-baserede undtagelser. Disse regler har ofte forrang og kan tillade kendte skadelige mails via mailfiltrering.
9. Kør regelmæssigt phishingsimulatorer for at måle den potentielle risiko på tværs af organisationen og for at identificere og uddanne sårbare brugere.

Links til yderligere oplysninger

- Fra cookie-tyveri til BEC: Angribere bruger AiTM-phishingwebsteder som indgangspunkt for yderligere økonomisk svindel | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Homoglyfbedrag

BEC og phishing er almindelige social engineering-taktikker. Social engineering spiller en væsentlig rolle inden for kriminalitet. Målet overtales til at interagere med den kriminelle ved at opnå tillid.

Inden for fysisk handel bruges varemærker til at sikre tillid til oprindelsen af et produkt eller en tjeneste, og forfalskede produkter er misbrug af varemærket. På samme måde udgiver cyberkriminelle sig for at være en kontakt, som offeret kender, under et phishingangreb og bruger homoglyffer til at bedrage potentielle ofre.

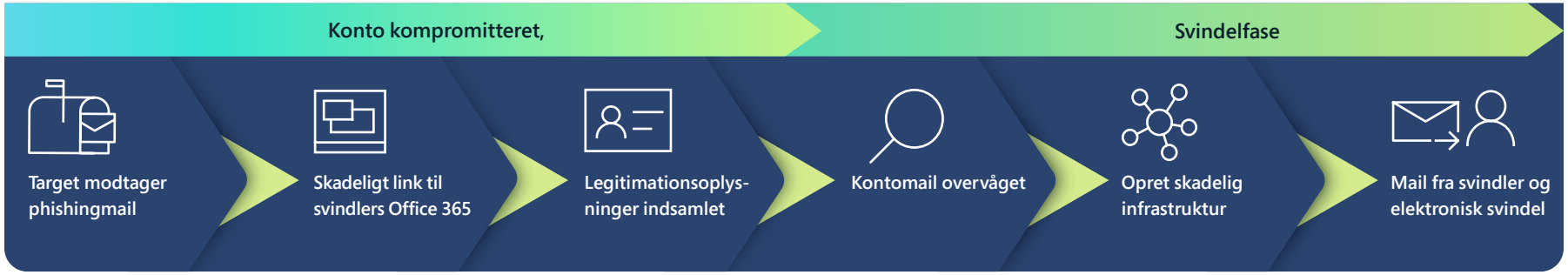
En homoglyf er et domænenavn, der bruges til mailkommunikation i BEC, hvor et tegn erstattes af et andet, der er identisk eller næsten identisk i udseende, for at bedrage målet.

Homoglyfteknikker, der anvendes i BEC-forsøg

BEC har generelt to faser, hvoraf den første involverer kompromittering af legitimationsoplysninger. Disse typer af lækager af legitimationsoplysninger kan være et resultat af phishingangreb eller store databrud. Legitimationsoplysningerne sælges eller handles derefter på det mørke internet.

Den anden fase er svindelfasen, hvor angriberen bruger kompromitterede legitimationsoplysninger til at engagere sig i sofistikeret social engineering ved hjælp af maildomæner med homoglyffer.

Forløbet af et BEC-angreb



Teknik	% af domæner, der benytter homoglyfteknik
erstat. l for I	25 %
erst. i for l	12 %
erst. q for g	7 %
erst. rn for m	6 %
erst. .cam for .com	6 %
erst. 0 for o	5 %
erst. ll for l	3 %
erst. ii for l	2 %
erst. vv for w	2 %
erst. l for ll	2 %
erst. e for a	2 %
erst. nn for m	1 %
erst. ll for I, sub l for i	1 %
erst. o for u	1 %

Analyse af over 1.700 homoglyfdomæner mellem januar-juli 2022. Der blev anvendt 170 homoglyfteknikker, men 75 % af domænerne brugte kun 14 teknikker.

En homoglyf i aktion

Et homoglyfdomæne, der ligner et maildomæne, som ofret genkender, er registreret hos en mailudbyder med et identisk brugernavn. Der sendes derefter en overtaget mail fra det overtagne domæne med nye betalingsinstruktioner.

Ved at udnytte open source-data og adgang til mailtråde identificerer den kriminelle personer, der har ansvar for fakturering og betalinger. Derefter efterligner de mailadressen på den person, der sender fakturaer. Denne efterligning består af et identisk brugernavn og et maildomæne, der er en homoglyf af den ægte afsender.

Angriberen kopierer en mailkæde, der indeholder en legitim faktura, og ændrer derefter fakturaen, så den indeholder angriberens egne bankoplysninger. Denne nye ændrede faktura sendes derefter igen fra mailen med en homoglyfefterligning til målet. Da konteksten giver mening, og mailen ser ægte ud, følger målet ofte de bedrageriske instruktioner.

Handlingsrettet indsigt

1. Håndhæv brugen af browsere, der understøtter tjenester som f.eks. Microsoft SmartScreen, for at analysere webadresser for mistænkelig adfærd og blokere adgang til kendte ondsindede websteder, f.eks. Safe Links og SmartScreen.[25]
2. Brug en sikkerhedsløsning baseret på maskinlæring, der sætter sandsynlige phishingmails i karantæne, og som placerer webadresser og vedhæftede filer i en sandkasse, før mailen når indbakken.

Links til yderligere oplysninger

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Indsigt i Spoof-intelligens – Office 365 | Microsoft Docs
- Indsigt i efterligning – Office 365 | Microsoft Docs

En tidslinje over afbrydelser af botnet fra begyndelsen af Microsoft-samarbejdet

I mere end ti år har DCU arbejdet på proaktivt at forhindre cyberkriminalitet, hvilket har resulteret i 26 malware- og nationalstatsafbrydelser. Da DCU-teamet bruger mere avancerede taktikker og værktøjer til at lukke disse ulovlige aktiviteter ned, ser vi, at cyberkriminelle også udvikler deres tilgange i et forsøg på at være et skridt foran. Her er en tidslinje, der viser et udvalg af de botnets, som er afbrudt af DCU, og de strategier, som Microsoft indførte for at lukke dem ned.

2008

Conficker-botnet

Beskrivelse: En orm, der spredte sig hurtigt og var målrettet mod Windows. Den inficerede millioner af computere og enheder på det samme netværk og forårsagede netværksafbrydelser i hele verden.

Samarbejde: Dannelse af Conficker-arbejdsgrupperne, det første konsortium af sin art. Microsoft samarbejdede med 16 organisationer over hele verden om at overvinde botten.

Microsofts reaktion: Gruppen samarbejdede på tværs af mange internationale jurisdiktioner, og det lykkedes dem at besejre Conficker.

2009

Waledac-botnet

Beskrivelse: Et komplekst spambotnet med amerikanske domæner, der indsamlede mailadresser og distribuerede spam, der inficerede op til 90.000 computere over hele verden.[26]

Samarbejde: Oprettelse af endnu et konsortium, MMPC (Microsoft Malware Protection Center) med fokus på tæt samarbejde med akademikere.[27]

Microsofts reaktion: Microsoft benyttede niveauinddeling af C2-baserede afbrydelser og overraskede cyberkriminelle ved at udnytte domæner med base i USA uden varsel[28] Microsoft blev tildelt midlertidigt ejerskab af næsten 280 domæner, der bruges af Waledacs servere.

2011

Microsoft Digital Crimes Unit (DCU) dannes

Samarbejde: Designet til at modarbejde cyberkriminalitet, der påvirker Microsoft-økosystemet, gennem tæt integration på tværs af et team af efterforskere, advokater og teknikere.

Microsofts tilgang: Målet er bedre at forstå de tekniske aspekter af forskellig malware og formidle denne indsigt til Microsofts juridiske team for at udvikle en effektiv afbrydelsesstrategi.

Rustock-botnet

Beskrivelse: En trojansk bagdørshest, der udsendte spam via en mailbot og benyttede internetudbydere som primære C2'er, udviklet til at sælge lægemidler.

Samarbejde: Microsoft etablerede et partnerskab med Pfizer Pharmaceuticals for at forstå de lægemidler, der blev solgt af Rustock, og arbejdede tæt sammen med de hollandske retshåndhævende embedsmænd.[29]

Microsofts reaktion: Microsoft samarbejdede med US Marshalls og de retshåndhævende myndigheder i Holland om at lukke C2-serverne i det pågældende land. Registrerede og blokerede alle fremtidige domænegenereringsalgoritmer (DGA'er).

2013

Sirefef/Zero Access-botnet

Beskrivelse: Et reklamebotnet, der var designet til at dirigere folk til farlige websteder, der ville installere malware eller stjæle personlige oplysninger, inficerede mere end to millioner computere og kostede annoncører mere end USD 2,7 millioner om måneden, primært i USA og Vesteuropa.

Samarbejde: Tæt samarbejde med FBI og Europol's Cybercrime Center for at nedbryde peer-to-peer-infrastrukturen.

Microsofts reaktion: Tilsluttede sig Zero Access-netværket, erstattede de kriminelle C2-servere og beslaglagde downloadserverdomæner.

2019

Trickbot-botnet

Beskrivelse: Et avanceret botnet med fragmenteret infrastruktur over hele verden, der var rettet mod finanssektoren og kompromitterede IoT-enheder.

Samarbejde: Microsoft samarbejdede med Financial Services Information Sharing and Analysis Center (FS-ISAC) for at lukke Trickbot.[30]

Microsofts reaktion: DCU byggede et system til at identificere og spore botinfrastruktur og genererede meddelelser til aktive internetudbydere under hensyntagen til specifikke love i forskellige lande.

Fortsat fokus på afbrydelse

Beskrivelse: Microsoft nedbrød infrastrukturen hos syv trusselsaktører i løbet af sidste år, og dette forhindrede dem i at distribuere yderligere malware, kontrollere ofrenes computere og målrette mod yderligere ofre.

Samarbejde: I samarbejde med internettjenesteudbydere, regeringer, retshåndhævende myndigheder og den private sektor delte Microsoft oplysninger for at hjælpe over 17 millioner ofre for malware over hele verden.

2022

Fremtiden

DCU fortsætter med at innovere og ønsker at bruge sin erfaring i afbrydelser af botnets til at udføre koordinerede operationer, der går længere end kun malware. Vores fortsatte succes kræver kreativ engineering, udveksling af oplysninger, innovative juridiske teorier og offentlige og private partnerskaber.

Cyberkriminelles misbrug af infrastruktur

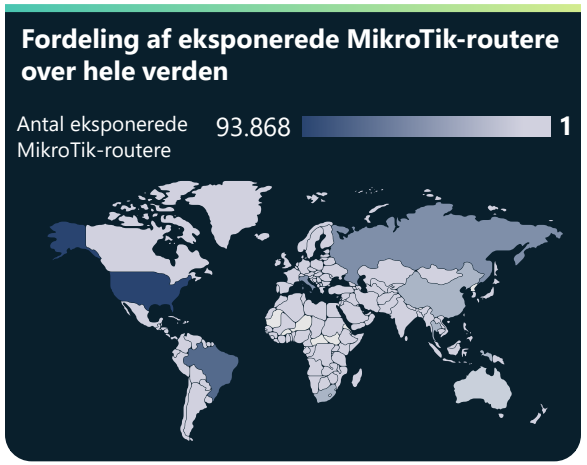
Internetgateways som kriminel kommando- og kontrolinfrastruktur

IoT-enheder bliver et stadig mere populært mål for cyberkriminelle, som benytter udbredte botnets. Når routere er uden programrettelser og vises direkte på internettet, kan trusselsaktører misbruge dem til at få adgang til netværk, udføre ondsindede angreb og endda støtte deres aktiviteter.

Microsoft Defender for IoT-teamet forsker i forskellige typer udstyr fra ældre industrielle kontrolsystemcontrollere til banebrydende IoT-sensorer. Teamet undersøger IoT- og OT-specifik malware, som de kan bidrage med til den fælles liste over kompromitteringsindikatorer.

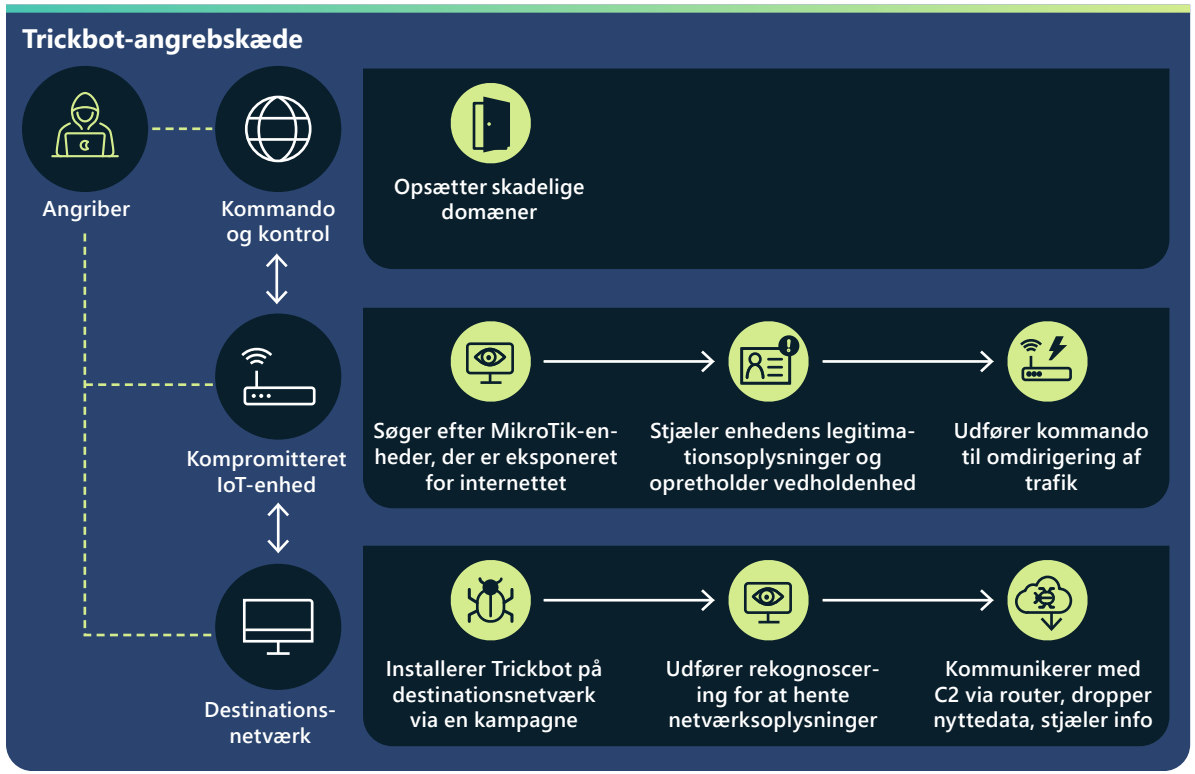
Routere er særligt sårbare angrebsvektorer, fordi de er allestedsnærværende på tværs af internettilsluttede hjem og organisationer. Vi har sporet aktiviteten af MikroTik-routere, en populær router rundt om i verden, som benyttes i både private boliger og kommercielt, og vi har identificeret, hvordan de udnyttes til kommando- og kontrolangreb (C2), DNS-angreb (domænenavnesystem) og kryptomining-aktiviteter.

Mere specifikt identificerede vi, hvordan Trickbot-operatører udnytter kompromitterede MikroTik-routere og omkonfigurerer dem, så de fungerer som en del af deres C2-infrastruktur. Populariteten af disse enheder gør Trickbots misbrug af dem alvorlig, og deres unikke hardware og software gør det muligt for trusselsaktører at omgå traditionelle sikkerhedsforanstaltninger, udvide deres infrastruktur og kompromittere flere enheder og netværk.



Eksponerede routere risikerer at få udnyttet potentielle sårbarheder.

Ved at spore og analysere trafik, der indeholder SSH-kommandoer (Secure Shell), observerede vi angribere, der bruger MikroTik-routere til at kommunikere med Trickbot-infrastruktur efter at have indhentet lovlige legitimationsoplysninger til enheder. Disse legitimationsoplysninger kan opnås gennem brute force-angreb, udnyttelse af kendte sårbarheder med let tilgængelige programrettelser og ved brug af standardadgangskoder. Når der er opnået



Trickbot-angrebskæden, der viser brugen af MikroTik IoT-enheder som proxyservere til C2.

adgang til en enhed, udsteder angriberen en unik kommando, der omdirigerer trafik mellem to porte i routeren og etablerer kommunikationslinjen mellem Trickbot-påvirkede enheder og C2.

Vi har samlet vores viden om de forskellige metoder til at angribe MikroTik-enheder, ud over blot Trickbot, samt kendte almindelige sårbarheder og eksponeringer (CVE'er) i et open source-værktøj til MikroTik-enheder, som kan udtrække de tekniske artefakter, som er relateret til angreb på disse enheder.[31]

Enheder, der fungerer som reverse proxyer for malware C2, er ikke kun unikke for Trickbot- og MikroTik-routere. I samarbejde med Microsoft RiskIQ-teamet sporede vi tilbage til den involverede C2 og ved at observere SSL-certifikater identificerede vi Ubiquiti- og LigoWave-enheder, der også påvirkes.[32] Dette er en stærk indikation på, at IoT-enheder er ved at blive aktive komponenter i nationalstatskoordinerede angreb og et populært mål for cyberkriminelle, der benytter udbredte botnets.

Kryptokriminelle misbruger IoT-enheder

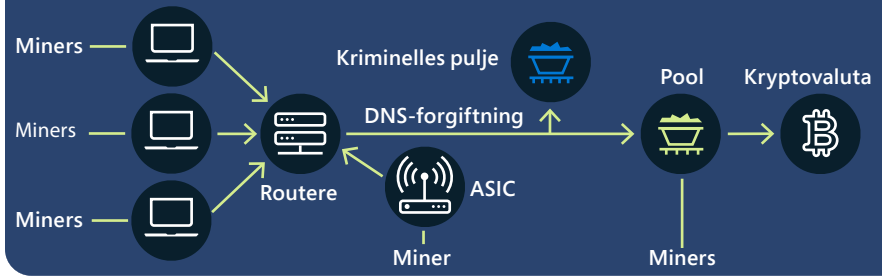
Gateway-enheder er et stadig mere værdifuldt mål for trusselsaktører, da antallet af kendte sårbarheder er øget støt fra år til år. De bruges til kryptomining og andre former for skadelig aktivitet.

Efterhånden som kryptovaluta er blevet mere populær, har mange mennesker og organisationer investeret computerkraft og netværksressourcer fra enheder såsom routere til at minere mønter på blockchain. Men mining af kryptovaluta er en tids- og ressourcekrævende proces med kun lidt sandsynlighed for succes. For at øge sandsynligheden for mining af en mønt samler minearbejdere sig i distribuerede, samarbejdsbaserede netværk og modtager hashes i forhold til den procentdel af mønten, som det lykkedes dem at minere med deres forbundne ressourcer.

I det forløbne år observerede Microsoft et stigende antal angreb, som misbruger routere til omdirigering med henblik på mining af kryptovaluta. Cyberkriminelle kompromitterer routere, der er forbundet med miningpuljer og omdirigerer miningtrafik til deres tilknyttede IP-adresser ved at benytte DNS-forgiftningsangreb, hvilket ændrer DNS-indstillingerne for målrettede enheder. De berørte routere registrerer den forkerte IP-adresse for et bestemt domænenavn og sender deres miningressourcer – eller hashes – til puljer, der bruges af trusselsaktører. Disse puljer kan minere anonyme mønter i forbindelse med kriminelle aktiviteter eller bruge lovlige hashes genereret af miners til at få en procentdel af den mønt, de har mineret, og dermed høste frugterne af deres arbejde.

Da mere end halvdelen af de kendte sårbarheder, der blev fundet i 2021, mangler en programrettelse, er opdatering og sikring af routere på virksomhedsnetværk og private netværk stadig en betydelig udfordring for enhedsejere og -administratorer.

Kompromittering af enheder til ulovlig kryptomining.



DNS-forgiftning af gatewayenheder kompromitterer lovlige miningaktiviteter og omdirigerer ressourcer til kriminelle miningaktiviteter.

Virtuelle maskiner som kriminalinfrastruktur

Den udbredte flytning til cloud-løsningen omfatter cyberkriminelle, der udnytter private aktiver fra uanende ofre, der er indsamlet via phishing eller distribution af malwareprogrammer, der indsamler legitimationsoplysninger. Mange cyberkriminelle vælger at oprette deres skadelige infrastrukturer på cloudbaserede virtuelle maskiner (VM'er), containere og mikrotjenester.

Når den cyberkriminelle har fået adgang, kan der opstå en sekvens af hændelser for at konfigurere infrastruktur – f.eks. en række virtuelle maskiner via scripting og automatiserede processer. Disse scriptede, automatiserede processer bruges til at starte skadelig aktivitet, herunder omfattende mailspamangreb, phishingangreb og websider, der hoster forbryderisk indhold. Det kan endda omfatte oprettelse af et skaleret virtuelt miljø, der udfører mining af kryptovaluta, hvilket medfører, at offeret får en regning på hundredtusindvis af dollars i slutningen af måneden.

Cyberkriminelle forstår, at deres skadelige aktivitet har en begrænset levetid, før den opdages og lukkes ned. Derfor har de opskaleret og opererer nu proaktivt med uforudsete aktiviteter i tankerne. De er blevet observeret forberede kompromitterede konti på forhånd og overvåge deres miljøer. Så snart en konto (der er oprettet med hundredtusindvis af virtuelle maskiner) registreres, går de videre til den næste konto – der allerede er forberedt af scripts, der aktiveres med det samme – og deres skadelige aktivitet fortsætter med lidt eller ingen afbrydelse.

På samme måde som cloud-infrastruktur kan on-premises-infrastruktur bruges i angreb med virtuelle lokale miljøer, der er ukendte for on-premises-brugeren. Dette kræver, at det første adgangspunkt forbliver åbent og tilgængeligt. Private on-premises-aktiver er også blevet misbrugt af cyberkriminelle til at starte en fremadrettet kæde af cloud-infrastruktur, der er konfigureret til at sløre deres oprindelse for at undgå registrering af oprettelse af mistænkelig infrastruktur.

Handlingsrettet indsigt

1. Implementer god cyberhygiejne, og giv medarbejderne vejledning i, hvordan de undgår social engineering.
2. Udfør regelmæssige automatiserede kontroller af brugeraktivitet gennem registreringer i stor skala for at reducere disse angrebstyper.
3. Opdater og sikr routere på virksomhedsnetværk og private netværk.

Er hacktivisme kommet for at blive?

Selvom hacktivisme ikke er et nyt fænomen, oplevede man en bølge af frivillige hackere i forbindelse med krigen i Ukraine, herunder nogle, der blev instrueret af myndigheder i at implementere cyberværktøjer for at skade politiske modstanderes omdømme eller aktiver, organisationer og endda nationalstater.

I februar 2022 opfordrede den ukrainske regering private civile rundt om i verden til at udføre cyberangreb på Rusland som en del af dens 300.000 personers stærke "it-hær".[33] Samtidig begyndte etablerede hacktivistgrupper som Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans og RaidForum2 at udføre angreb til støtte for Ukraine. Andre grupper, herunder nogle fra Conti ransomware-banden, valgte Ruslands side.[34]

I månederne, der fulgte, var Anonymous' aktiviteter meget synlige. Hackere, der agerede i gruppens navn – eller i et af dens associerede selskaber – deaktiverede midlertidigt tusindvis af russiske og hviderussiske websteder, lækkede hundredvis af gigabyte stjålne data, hackede russiske tv-kanaler for at vise pro-ukrainsk indhold og tilbød endda at betale Bitcoin for overdragne russiske tankvogne.

Stigning i antallet af medborger-hackere

Sociale medieplatforme gjorde det muligt at foretage en hurtig organisering og mobilisering af tusindvis af såkaldte medborgerhackere, der fik anvisninger i at udføre let eksekverbare angreb som f.eks. DDoS-angreb. Arrangørerne brugte Twitter, Telegram og private fora til at samle hackere, organisere aktiviteter og formidle instruktionsvejledninger om at hacke.

Men de fleste af disse hackere har sandsynligvis begrænsede færdigheder, selvom de får anvisninger. Dette tyder på to potentielle fremtider: en, hvor hundred- eller tusindvis af personer med rudimentær teknisk kapacitet bruger angrebsskabeloner til at udføre fremtidige koordinerede eller individuelle hacktivistangreb mod mål, eller en anden fremtid, hvor den endelige afslutning af fjendtlighederne i Ukraine får dem til at opgive deres hacktivisme, i det mindste indtil det næste politiske eller sociale spørgsmål inspirerer dem til at handle.

Politisering af hackere

Den største risiko ved denne politiske mobilisering er implementeringen af teknologikyndige hackere, der kan fortsætte med at udføre cyberangreb mod udenlandske offentlige mål for at støtte deres egne nationale prioriteter, enten på eget initiativ eller på foranledning af deres egne myndigheder.

Iran, Kina og Rusland bruger allerede hacktivisme til at rekruttere nye styrker til deres statslige hackergrupper. I april 2022 lancerede den prorussiske hackinggruppe Killnet f.eks. DDoS-angreb mod tjekkiske jernbaner, regionale lufthavne og Tjekkiets server for offentlige tjenester, selvom Tjekkiet ikke er direkte involveret i krigen.[35] Samtidig kan nogle myndigheder bruge hacktivisme som dække for traditionel cyberspionage eller sabotageoperationer – f.eks. iranske aktiviteter mod Israel.

I et miljø med en stigning i DDoS-angreb, som har forbindelse med hacktivisme, udfordres teknologibranchen til hurtigt at afkode forskellen mellem normal og unormal trafikstrøm til et websted. Microsoft og deres partnere har udviklet en samling værktøjer, der genkender skadelig DDoS-trafik og sporer den tilbage til oprindelsen. Microsoft Azure-platformen kan desuden identificere maskiner på platformen, der producerer ekstraordinært høje niveauer af udgående trafik, og lukke dem.

Fremkomst af protestware

Protestware er opstået som en direkte følge af følelsesmæssige reaktioner på krigen mellem Rusland og Ukraine. Nogle open source-softwareudviklere brugte deres softwares popularitet som et middel til at fremkomme med deres mening eller reagere på den geopolitiske situation, der udfolder sig. Dette omfattede harmløse tekstfiler, der blev åbnet på et skrivebord eller i en browser for at sprede meddelelser om fred, men omfattede også målrettede angreb baseret på den geografiske placering af IP-adresser og destruktive handlinger som f.eks. at slette en harddisk. Når andre globale begivenheder udfolder sig, kan vi forvente at se protestware igen i fremtiden. Da disse generelt er tilfælde, hvor velrenommerede open source-vedligeholdelsesmedarbejdere beslutter at komme med personlige udtalelser ved hjælp af deres egne open source-komponenter, er der i øjeblikket ingen beskyttelse, der kan forhindre, at denne type ændringer opstår i kildefilpakkerne, og brugerne bør være opmærksomme på potentielle effekter.

Sociale medieplatforme gjorde det muligt at foretage en hurtig organisering og mobilisering af tusindvis af såkaldte medborgerhackere, der fik anvisninger i at udføre let eksekverbare angreb som f.eks. DDoS-angreb.

Handlingsrettet indsigt

1. Teknologibranchen er nødt til at samarbejde om at udvikle en omfattende reaktion på denne nye trussel.
2. Førende teknologivirksomheder, herunder Microsoft, har værktøjer til at identificere skadelig trafik, der kan forbindes med DDoS-angreb, og deaktivere de ansvarlige maskiner.
3. Open source-brugere bør være ekstra på vagt i perioder med geopolitisk strid.

Slutnoter

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. Endpoint detection and response. 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. Et forum med adgangskrav er et onlinediskussionsforum, der kræver, at et eksisterende medlem står inde for, at et nyt medlem optages.
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. Datakilde: Defender for Office (skadelig mail/aktivitet med kompromitteret identitet), Azure Active Directory Identity Protection (hændelser relateret til kompromitterede identiteter/alarmer), Defender for Cloud Apps (dataadgangshændelser med kompromitterede identiteter) og M365D (korrelation på tværs af produkter).
17. Datakilde: Defender for Endpoint (advarsler/hændelser om angrebsadfærd), Defender for Office (skadelig mail) og M365D (korrelation på tværs af produkter).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Domænebaseret meddelelsesgodkendelse, rapportering og overensstemmelse: En protokol til mailgodkendelse, politik og rapportering, der er udviklet til at give ejere af maildomæner mulighed for at beskytte deres domæne mod uautoriseret brug.
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., Nr. 1:10CV156, (E.D.Va. 22. feb 2010).
27. Se Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27. sep. 2011.
28. Specifikt tillader regel 65 i Federal Rules of Civil Procedure en part at søge en sådan afhjælpning, hvis: 1) parten vil lide øjeblikkelig og uoprettelig skade, hvis afhjælpning ikke gives, og 2) parten forsøger at give den anden side rettidig varsel. Derudover kræver lovgivningen, at der anvendes en balanceringstest, som afvejer sagsøgtes varselsret i forhold til mængden af skade på offentligheden.
29. Microsoft Corporation v. John Does 1-11, et. al., Nr. 2:11cv222, (W.D. Wa. 9. feb 2011).
30. Microsoft Corp. v. Does, Nr. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12. aug. 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

Trusler på national-statsniveau

Nationalstatsaktører lancerer stadig mere sofistikerede cyberangreb for at undgå afsløring og fremme deres strategiske prioriteter.

En oversigt over

trusler fra nationalstater

Nationalstatsaktører lancerer stadig mere sofistikerede cyberangreb for at undgå afsløring og fremme deres strategiske prioriteter. Implementeringen af cybervåben i hybridkrigen i Ukraine er starten på en ny tidsalder med konflikter.

Rusland har også støttet krigen med informationsindflydelsesaktiviteter ved at bruge propaganda til at påvirke holdningerne i Rusland, Ukraine og globalt. Denne første hybridkonflikt i fuld skala har givet andre vigtige erfaringer. For det første kan sikkerheden i digitale operationer og data bedst beskyttes – både i cyberspace og i det fysiske rum – ved at flytte til cloud-løsningen. De første russiske angreb var målrettet mod on-premises-tjenester med wiper-malware, og et af de første missiler var rettet mod fysiske datacentre.

Ukraine reagerede ved hurtigt at flytte workloads og data til hyperskalerede cloud-løsninger, der hostes i datacentre uden for Ukraine. For det andet har fremskridt inden for cybertrusselsintelligens og endpoint-beskyttelse drevet af dataene og avancerede AI- og ML-tjenester i cloud-løsningen hjulpet med at forsvare sig mod russiske cyberangreb.

Andre steder har nationalstatsaktører øget aktiviteten og er begyndt at bruge fremskridt inden for automatisering, cloud-infrastruktur og fjernadgangsteknologier til at angribe et bredere sæt af mål. Virksomheders it-forsyningskæder, der giver adgang til slutmålene, bliver ofte angrebet. Cybersikkerhedshygiejne blev endnu mere kritisk, da aktører hurtigt udnyttede sårbarheder uden programrettelser, brugte både sofistikerede og brute force-teknikker til at stjæle legitimationsoplysninger og slørede deres aktiviteter ved hjælp af open source eller legitim software. Og Iran slutter sig til Rusland i brugen af destruktive cybervåben, herunder ransomware, som en vigtig bestanddel af deres angreb.

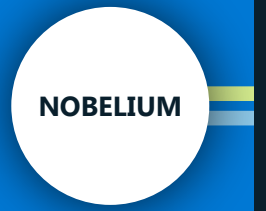
Denne udvikling kræver øjeblikkelig indførelse af en ensartet, global ramme, der prioriterer menneskerettigheder og beskytter folk mod den uforsvarlige statsadfærd online. Alle nationer skal samarbejde om at implementere aftalte normer og regler for ansvarlig statsadfærd.

Forsvare Ukraine: Tidlige erfaringer fra cyberkrigen – Microsoft On the Issues

Øget opmærksomhed mod kritisk infrastruktur, især it-sektor, finansielle tjenester, transportsystemer og kommunikationsinfrastruktur.

Få mere at vide på side 35

It-supply chain, der bruges som gateway til at få adgang til mål.



Få mere at vide på side 36

Kina udvider den globale målretning, især på mindre lande i Sydøstasien, for at opnå intelligens og konkurrence-mæssige fordele.

Få mere at vide på side 44

Iran blev stadig mere aggressiv efter magtovertagelsen, udvidede ransomware-angreb ud over regionale modstandere til ofre i USA og EU og målrettede mod højt profileret kritisk infrastruktur i USA.

Få mere at vide på side 46

Identifikation og hurtig udnyttelse af sårbarheder uden programrettelser er blevet en vigtig taktik. Hurtig implementering af sikkerhedsopdateringer er nøglen til forsvar.

Få mere at vide på side39

Nordkorea målrettede mod forsvars- og luftfartsvirksomheder, kryptovaluta, nyhedskanaler, afhoppere og hjælpeorganisationer for at nå regimets mål: at opbygge forsvar, styrke økonomien og sikre stabilitet i landet.

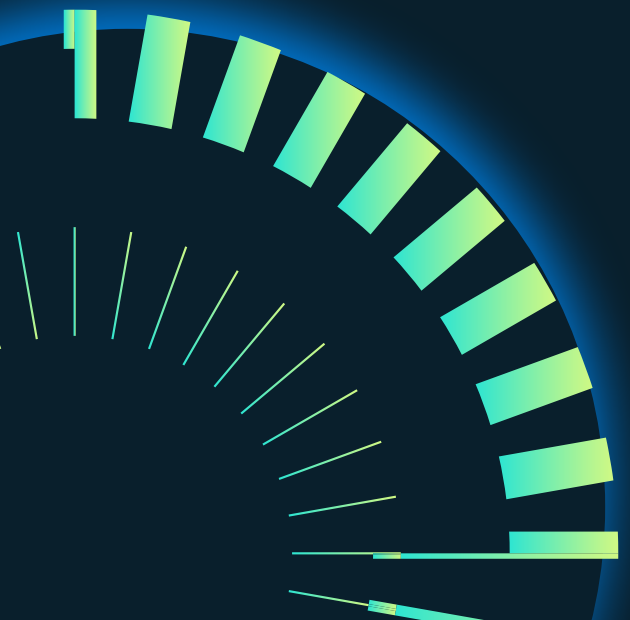
Få mere at vide på side 49

Cyberlejesoldater truer stabiliteten i cyberområdet, da denne voksende industri af private virksomheder udvikler og sælger avancerede værktøjer, teknikker og tjenester for at give deres kunder (ofte offentlige myndigheder) mulighed for at bryde ind i netværk og enheder.

Få mere at vide på side 52

Introduktion

Efter højt profilerede angreb i 2020 og 2021 brugte nationalstatstrusselsaktører betydelige ressourcer på at tilpasse sig ny sikkerhedsbeskyttelse, der blev implementeret af organisationer for at forsvare sig mod sofistikerede trusler.



Ligesom virksomhedsorganisationer begyndte modstanderne at bruge fremskridtene inden for automatisering, cloud-infrastruktur og fjernadgangsteknologier til at udvide deres angreb mod et bredere sæt af mål. Disse taktiske justeringer førte til nye tilgange og storstilede angreb på virksomhedernes supply chains. It-sikkerhedshygiejne fik endnu større betydning, da aktørerne udviklede nye metoder til hurtigt at udnytte sårbarheder uden sikkerhedsrettelser, udvidede teknikker til at kompromittere virksomhedsnetværk og slørede deres aktiviteter ved hjælp af open source-software eller lovlig software. Nye angrebsteknikker gav nye vektorer, der var vanskeligere at registrere, til at få adgang til et måls netværk. Endelig så vi, at i takt med at fysiske angreb under krigen eskalerede, indtog cyberangreb en fremtrædende rolle i militære aktiviteter.

Konflikten i Ukraine er et alt for brutalt eksempel på, hvordan cyberangreb udvikler sig til at påvirke verden parallelt med militær konflikt på jorden. Strømsystemer, telekommunikationssystemer, medier og anden kritisk infrastruktur er alle blevet mål for fysiske angreb og cyberangreb. Forsøg på netværkskompromittering, der normalt observeres som en del af spionage- og informationseksfiltreringskampagner, var i hybridkrigen fokuseret på destruktive wiper-malwareangreb mod kritiske infrastruktursystemer. Forbindelsen mellem disse systemers sikkerhed og cloud-løsningen resulterede i tidlig registrering og afbrydelse af potentielt ødelæggende angreb.[1]

For første gang i en større cyberhændelse brugte adfærdsregistreringer, der udnyttede maskinlæring, kendte angrebsmønstre til at identificere og stoppe yderligere angreb uden forudgående kendskab til den underliggende malware – selv før nogen mennesker var opmærksomme på truslerne. Vi fik også bekræftet værdien af at dele trusselsefterretninger i realtid med dem, der forsvarer disse systemer, og giver dem vigtige oplysninger, så de kan forudse og forsvare sig mod aktive angreb.

Nationalstatstrusselsaktører rundt omkring i verden fortsætter med at udvide deres operationer på nye og gamle måder. Kina, Nordkorea, Iran og Rusland udførte alle angreb på Microsofts kunder. It-tjenesternes supply chain blev et fælles mål, da aktører skiftede fokus til upstream-tjenester, der kan være adgangspunkter for flere organisationer. Vi forventer, at aktører fortsat vil udnytte betroede relationer i virksomheders supply chains, hvilket understreger vigtigheden af omfattende håndhævelse af godkendelsesregler, omhyggelig programrettelse og kontokonfiguration for infrastruktur til fjernadgang samt hyppig revision af partnerrelationer for at verificere autenticiteten.

Nationalstatsaktører, ligesom ransomware-operatører og kriminelle operatører, har reageret på øget eksponering ved at bevæge sig mod målretning mod forkert konfigurerede virksomhedssystemer eller systemer uden programrettelser (VPN/VPS-infrastruktur, on-premises servere, tredjepartssoftware) for at udføre living-off-the-land-angreb. Mange har øget anvendelsen af købt malware og open source red team-værktøjer til at sløre deres skadelige aktivitet.

Derfor er opretholdelse af en velfungerende it-sikkerhedshygiejne gennem prioriterede programrettelser, aktivering af anti-manipulationsfunktioner, brug af værktøjer til håndtering af angrebsoverflader som RiskIQ for at få et udefrakommende overblik over en angrebsoverflade og aktivering af multifaktorgodkendelse på tværs af hele virksomheden blevet grundlæggende principper til proaktivt at forsvare sig mod mange sofistikerede aktører.

Nationalstatsaktører er også begyndt at benytte ransomware som taktik i deres angreb, og de genbruger ofte ransom-malware, der er oprettet af det kriminelle økosystem i deres angreb. Vi har set aktører fra både Iran og Nordkorea udnytte kommercielt tilgængelige ransomware-værktøjer til at skade målrettede systemer, ofte herunder kritisk infrastruktur, hos regionale modstandere. Endelig har vi set den voksende trussel fra cyberlejesoldater, der udvikler og sælger værktøjer, teknikker og tjenester til at udvide udnyttelser mod sårbare tredjepartsløsninger. Nationalstatsaktørernes sofistikerede og smidige angreb vil fortsat udvikles for hvert år. Organisationer skal reagere ved at holde sig informeret om disse ændringer blandt aktører og udvikle sit forsvar parallelt.

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

Baggrund for nationalstatdata

Nationalstatstrusler defineres som trusselsaktiviteter, der stammer fra et bestemt land med den tilsyneladende hensigt at fremme nationale interesser. Nationalstatsaktører udgør nogle af de mest avancerede og vedvarende trusler, som vores kunder står over for, herunder tyveri af intellektuel ejendom, spionage, overvågning, legitimationstyveri, destruktive angreb og meget mere.

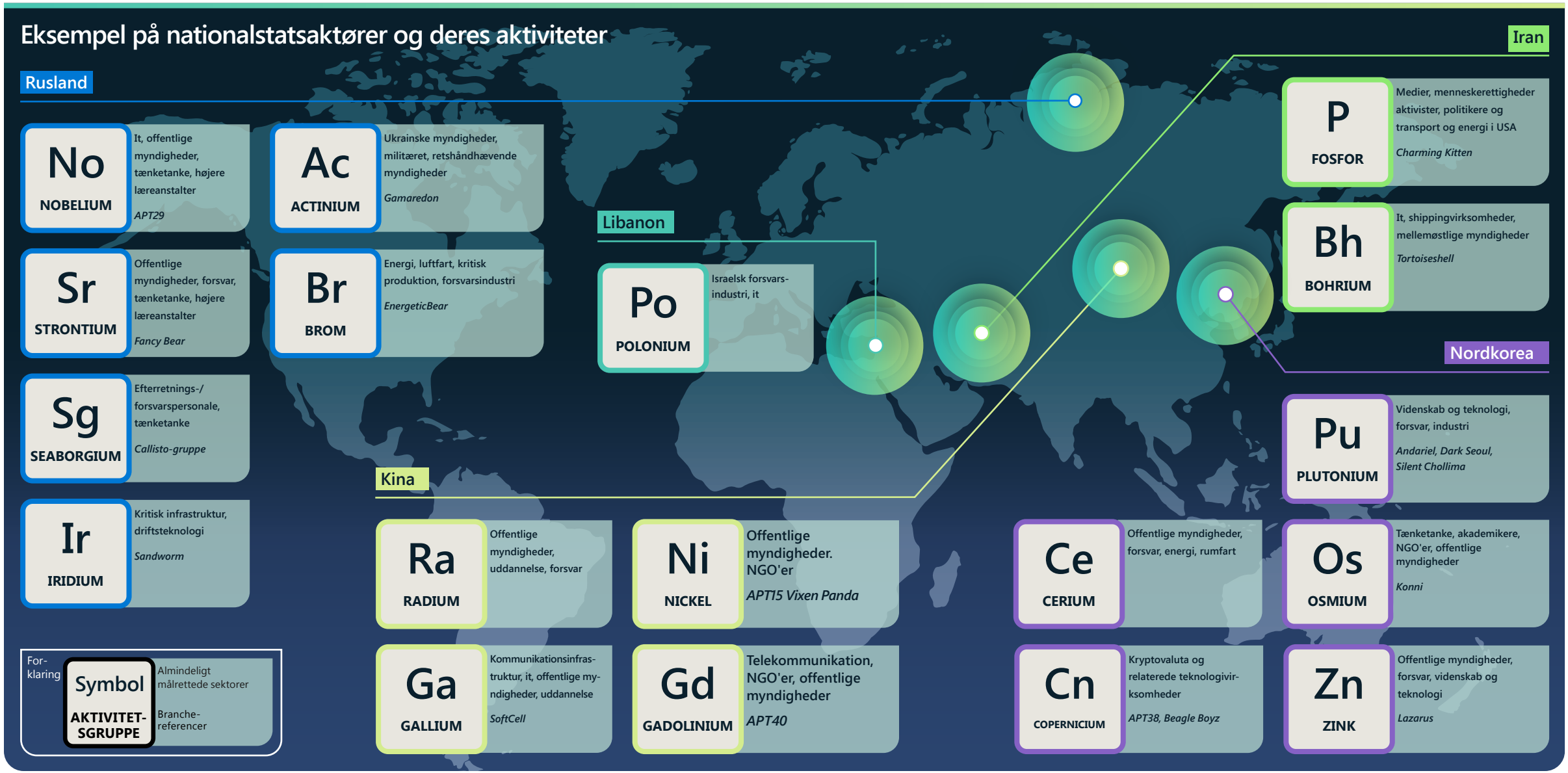
Vi investerer betydelige ressourcer i at opdage, forstå og imødegå disse trusler. Når en organisation eller en individuel kontoejer målrettes eller kompromitteres af observeret nationalstatsaktivitet, sender Microsoft en advarsel i form af en nationalstatsmeddelelse (NSN) direkte til den pågældende kunde, herunder de oplysninger, de har brug for for at undersøge aktiviteten. Pr. juni 2022 havde vi leveret over 67.000 NSN'er, siden vi begyndte i 2018.

Microsoft af NSN-advarselsdata præsenteres i dette kapitel for at give et overblik over målbar aktivitet. Niveauet af nationalstatsaktivitet, der vises i diagrammerne, er baseret på antallet af NSN'er, som Microsoft, udsendte til kunder som reaktion på registrering af nationalstatsaktører, der målretter mod eller kompromitterer mindst én konto i kundeorganisationen.

De fire primære nationalstater, hvis trusselsgrupper vi medtager i denne rapport, er Rusland, Kina, Iran og Nordkorea. Disse repræsenterer oprindelseslande for de mest almindeligt observerede aktører, der har målrettet mod Microsoft-kunder i løbet af det seneste år. Rapporten indeholder også vores observationer om trusselsgrupper fra Libanon og fra cyberlejesoldater eller fjendtlige aktører i den private sektor, der kan ansættes.

Microsoft identificerer nationalstatsgrupper efter kemiske elementnavne (f.eks. NOBELIUM), men der er kun vist nogle af dem på følgende side. Vi benytter DEV-####-betegnelser som et midlertidigt navn, der gives til en ukendt, ny eller klyngetrusselsaktivitet, der er under udvikling, så vi kan spore den som et unikt sæt af oplysninger, indtil vi er temmelig sikre på oprindelsen eller identiteten på aktøren bag aktiviteten.

Når den opfylder kriterierne, konverteres en DEV til en navngiven aktør eller flettes med eksisterende aktører. I dette kapitel nævner vi eksempler på nationalstats- og udviklingsgrupper for at give et dybere indblik i angrebsmål, -teknikker og -analyse af motiver. Selv om mange af disse grupper benytter de samme værktøjer som cyberkriminelle, udgør de unikke trusler i form af skræddersyet malware, evnen til at opdage og udnytte zero-day-sårbarheder og juridisk straffrihed.


Eksempel på nationalstatsaktører og deres aktiviteter
Rusland
No
NOBELIUM
It, offentlige myndigheder, tænketanke, højere læreanstalter
APT29
Ac
ACTINIUM
Ukrainske myndigheder, militæret, retshåndhævende myndigheder
Gamaredon
Sr
STRONTIUM
Offentlige myndigheder, forsvar, tænketanke, højere læreanstalter
Fancy Bear
Br
BROM
Energi, luftfart, kritisk produktion, forsvarsindustri
EnergeticBear
Sg
SEABORGIUM
Efterretnings-/ forsvarspersonale, tænketanke
Callisto-gruppe
Ir
IRIDIUM
Kritisk infrastruktur, driftsteknologi
Sandworm
Libanon
Po
POLONIUM
Israelsk forsvars-industri, it
Iran
P
FOSFOR
Medier, menneskerettigheder aktivister, politikere og transport og energi i USA
Charming Kitten
Bh
BOHRIUM
It, shippingvirksomheder, mellemøstlige myndigheder
Tortoiseshell
Nordkorea
Pu
PLUTONIUM
Videnskab og teknologi, forsvar, industri
Andariel, Dark Seoul, Silent Chollima
Kina
Ra
RADIUM
Offentlige myndigheder, uddannelse, forsvar
Ni
NICKEL
Offentlige myndigheder. NGO'er
APT15 Vixen Panda
Ce
CERIUM
Offentlige myndigheder, forsvar, energi, rumfart
Os
OSMIUM
Tænketanke, akademikere, NGO'er, offentlige myndigheder
Konni
Ga
GALLIUM
Kommunikationsinfras-truktur, it, offentlige myndigheder, uddannelse
SoftCell
Gd
GADOLINIUM
Telekommunikation, NGO'er, offentlige myndigheder
APT40
Cn
COPERNICIUM
Kryptovaluta og relaterede teknologivir-ksomheder
APT38, Beagle Boyz
Zn
ZINK
Offentlige myndigheder, forsvar, videnskab og teknologi
Lazarus
For-klaring
Symbol
AKTIVITET-SGRUPPE
Almindeligt målrettede sektorer
Branche-referencer

Trusselslandskab under udvikling

Microsofts mission om at spore nationalstatsaktivitet og underrette kunderne, når vi ser dem blive angrebet eller kompromitteret, er forankret i vores mission om at beskytte vores kunder mod angreb.

Denne meddelelse er en vigtig del af vores forpligtelse til at informere kunderne om, hvorvidt observerede angreb forhindres af vores sikkerhedsprodukter, eller om angrebene er effektive på grund af ukendte sikkerhedssvagheder. Sporingsmeddelelser over tid hjælper Microsoft med at identificere nye trusselstendenser efter aktør og fokusere produktbeskyttelse på proaktivt at afhjælpe trusler mod kunder på tværs af vores cloud-tjenester.

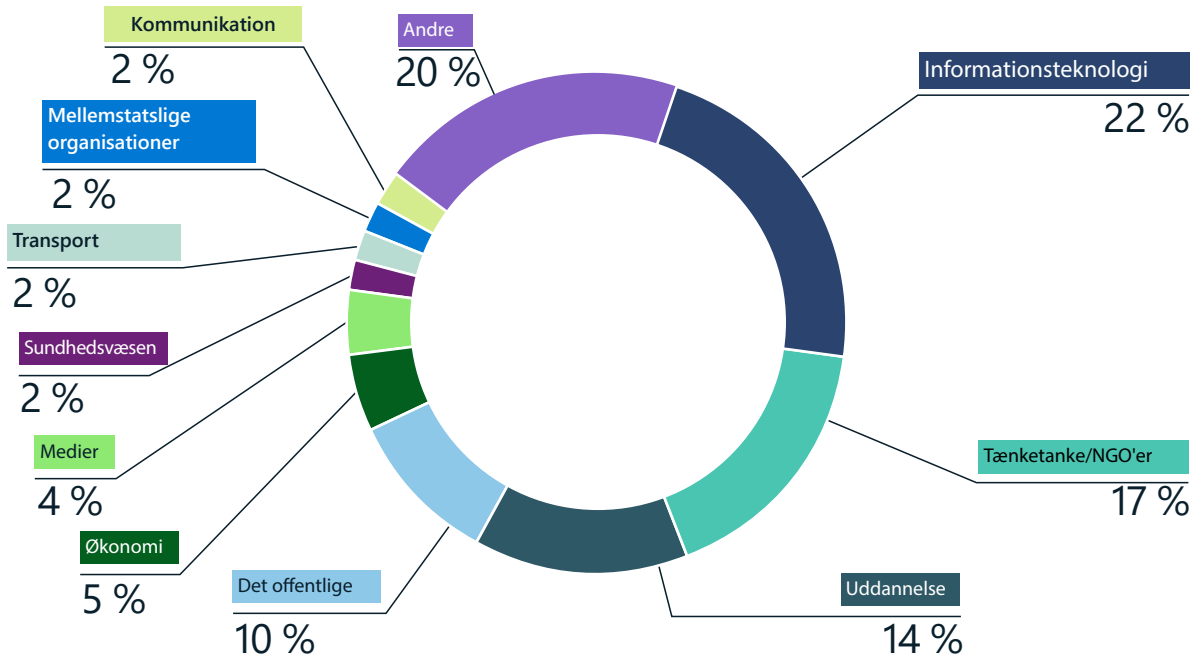
Denne sporing giver os også mulighed for at dele data og indsigt om det, vi ser. De analytikere, der sporer aktørerne og følger deres angreb, bruger en kombination af tekniske indikatorer og geopolitisk ekspertise til at forstå aktørernes motiver og kombinere teknisk og global kontekst i ny indsigt. Denne kurering giver et unikt indblik i nationalstatsaktørernes prioriteter, og hvordan deres motiver kan afspejle de politiske, militære og økonomiske prioriteter for de nationalstater, der ansætter dem.

De politiske udviklinger i det seneste år har formet prioriteterne og risikotolerancen for statssponsorerede trusselsgrupper på verdensplan. I takt med at geopolitiske relationer er brudt sammen, og "høge"-elementer har fået mere kontrol i nogle lande, er cyberaktører blevet mere dristige og aggressive. Eksempel:

- Rusland målrettede ubønhørligt mod den ukrainske regering og landets kritiske infrastruktur for at supplere deres militære indsats på jorden.[2]
- Iran forsøgte aggressivt at få adgang til kritisk infrastruktur i USA, f.eks. havnemyndigheder.
- Nordkorea fortsatte sin kampagne for at stjæle kryptovaluta fra finansielle og teknologiske virksomheder.
- Kina udvidede sine globale cyberespionageaktiviteter.

Selv om nationalstatsaktører kan være teknisk sofistikerede og anvende en bred vifte af taktikker, kan deres angreb ofte afbødes af god cyberhygiejne. Mange af disse aktører er afhængige af relativt lavteknologiske midler, f.eks. spear-phishingmails, til at levere sofistikeret malware i stedet for at investere i at udvikle tilpassede udnyttelser eller bruge målrettet social engineering til at nå deres mål.

Industrisektorer, som nationalstatsaktører målretter mod



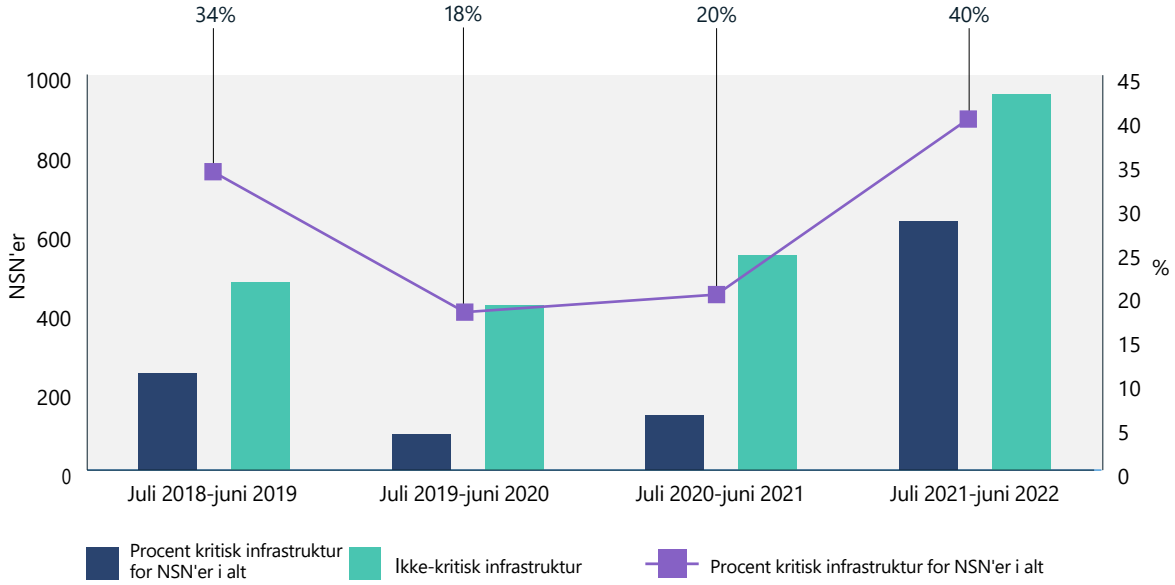
Nationalstatsgrupper målrettede mod en række sektorer. Russiske og iranske statsaktører målrettede mod it-branchen som et middel til at få adgang til it-virksomhedernes kunder. Tænketanke, ikke-statslige organisationer (NGO'er), universiteter og offentlige myndigheder forblev andre almindelige mål for nationalstatsaktører.

Nationalstatsaktører har en række mål, der kan resultere i målretning mod bestemte grupper af organisationer eller enkeltpersoner. I det seneste år er supply chain-angreb steget med et særligt fokus på it-virksomheder. Ved at kompromittere it-tjenesteudbydere kan trusselsaktører ofte nå deres oprindelige mål gennem en betroet relation til virksomheden, der administrerer forbundne systemer, eller potentielt udføre angreb i langt større skala ved at kompromittere hundredvis af downstream-kunder i ét enkelt angreb. Efter it-sektoren var de enheder, der oftest blev målrettet mod, tænketanke, akademikere, der var knyttet til universiteter, og embedsmænd. Disse er ønskværdige "bløde mål" for spionage for at indsamle oplysninger om geopolitiske spørgsmål.

Trusselslandskab under udvikling

Fortsat

Tendenser for kritisk infrastruktur

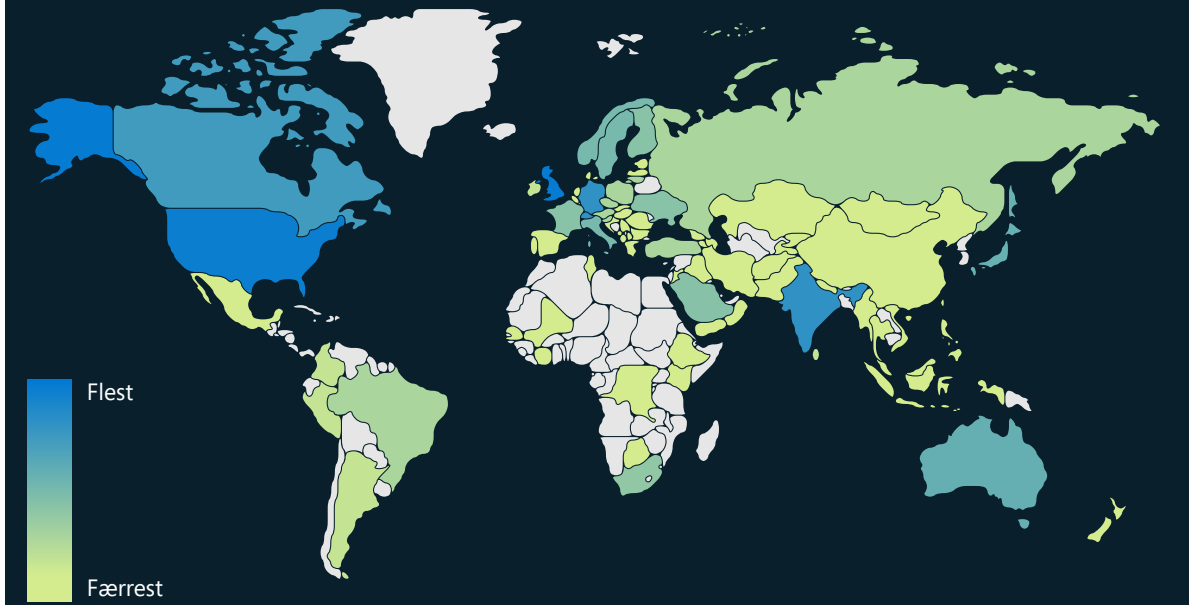


Nationalstatsgruppers målretning mod kritisk infrastruktur[3] steg i det forløbne år. Aktørerne havde fokus på virksomheder i it-sektoren, finansielle tjenester, transportsystemer og kommunikationsinfrastruktur.

"Før invasionen af Ukraine mente myndighederne, at data skulle forblive i et land for at være sikre. Efter invasionen er migrering af data til cloud-løsningen og flytning uden for de geografiske grænser nu en del af robusthedsplanlægning og god styring."

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

Nationalstatsaktørers geografiske målretning



Nationalstatsgruppers cybermålretning spændte over hele verden sidste år med et særligt stort fokus på amerikanske og britiske virksomheder. Organisationer i Israel, Forenede Arabiske Emirater, Canada, Tyskland, Indien, Schweiz og Japan var også blandt nogle af de hyppigst målrettede ifølge vores NSN-data.

Handlingsrettet indsigt

1. Identificer og beskyt dine potentielle datamål med høj værdi, teknologier i risikozonen, oplysninger og forretningsaktiviteter, der kan være i overensstemmelse med de strategiske prioriteter for nationalstatsgrupper.
2. Aktivér cloud-beskyttelser for at identificere og afbøde kendte og nye trusler mod dit netværk i stor skala.

It-supply chain som gateway til det digitale økosystem

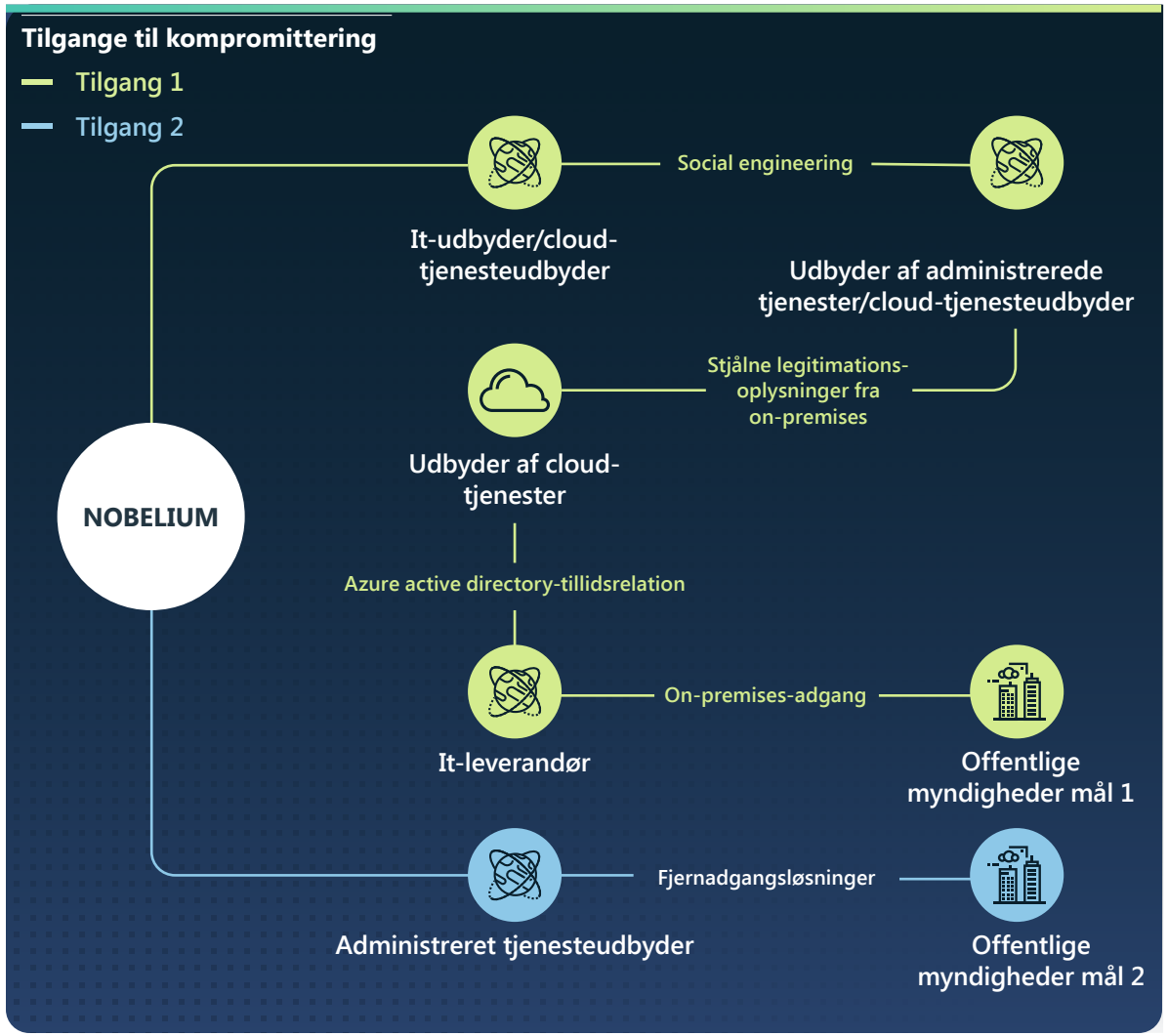
Målretning mod it-tjenesteudbydere fra nationalstaters side kan give trusselsaktørerne mulighed for at få adgang til andre organisationer af interesse ved at udnytte den tillid og adgang, der gives til disse supply chain-udbydere. I det forløbne år målrettede nationalstatslige cybertrusselsgrupper mod udbydere af it-tjenester for at angribe tredjepartsmål og få adgang til downstream-klienter inden for offentlige myndigheder, politik og kritiske infrastruktursektorer.

It-tjenesteudbydere er attraktive mellemmål, fordi de betjener hundredvis af direkte og tusindvis af indirekte kunder af interesse for udenlandske efterretningstjenester. Hvis disse virksomheder udnyttes, kan de rutinemæssige forretningspraksisser og de uddelegerede administrative rettigheder, som disse virksomheder nyder godt af, tillade ondsindede aktører at få adgang til og manipulere it-tjenesteudbyderens klientnetværk uden at det straks udløser advarsler.

I det forløbne år forsøgte NOBELIUM at kompromittere og udnytte privilegerede konti i cloud-løsninger og hos andre udbydere af administrerede tjenester til at forsøge at få målrettet downstream-adgang til primært amerikanske og europæiske offentlige myndigheder og politikkunder.

NOBELIUM demonstrerede, hvordan en "kompromitter en for at kompromittere mange"-tilgang kan rettes mod en opfattet geopolitisk modstander. I det forløbne år har trusselsaktøren engageret sig i både tredjepartsindtrængen og direkte indtrængen i følsomme organisationer, der er baseret i medlemslande i NATO (North Atlantic Treaty Organisation), som den russiske regering opfatter som en eksistentiel trussel. Mellem juli 2021 og begyndelsen af juni 2022 gik 48 % af Microsofts meddelelser til kunder om russisk trusselsaktivitet mod onlinetjenesters kunder til virksomheder i it-sektoren i NATO-medlemslande, sandsynligvis som mellemliggende adgangspunkter. Samlet set gik 90 % af meddelelser om russisk trusselsaktivitet i samme periode til kunder i NATO-medlemsstaterne, primært inden for it, tænketanke og ikke-statslige organisationer (NGO'er) og offentlige sektorer, hvilket antyder at der er brugt forskellige værktøjer til at få indledende adgang til disse mål.

Der er sket et skift fra udnyttelse af software-supply chain til udnyttelse af it-tjenesternes supply chain med målretning mod cloud-løsninger og udbydere af administrerede tjenester for at nå downstream-kunder.



Dette diagram viser NOBELIUM's multivektortilgang til at kompromittere sine ultimative mål og følgeskaderne på andre ofre undervejs. Ud over de handlinger, der er vist ovenfor, lancerede NOBELIUM adgangskodespray- og phishingangreb mod de involverede enheder og målrettede mod mindst én offentlig medarbejders personlige konto som en anden potentiel vej til kompromittering.

It-supply chain som gateway til det digitale økosystem

Fortsat

I løbet af året registrerede MSTIC (Microsoft Threat Intelligence Center) et stigende antal iranske statsaktører og Iran-tilknyttede aktører, som kompromitterede it-virksomheder. I mange tilfælde blev aktørerne fundet under forsøg på at stjæle logonoplysninger til at få adgang til downstream-klienter for en række mål, fra indsamling af oplysninger til destruktive gengældelsesangreb.

- I juli og august 2021 kompromitterede DEV-0228 en israelsk leverandør af software for senere at kompromittere downstream-kunder i det israelske forsvar, energisektoren og den juridiske sektor.[4]
- Fra august til september 2021 registrerede Microsoft en stigning i iranske statsaktører, der målrettede mod it-virksomheder baseret i Indien. Fraværet af relevante geopolitiske spørgsmål, der kunne retfærdiggøre et sådant skift, tyder på, at denne målretning er for at få indirekte adgang til datterselskaber og kunder uden for Indien.
- I januar 2022 kompromitterede DEV-0198, en gruppe, vi vurderer er tilknyttet regeringen i Iran, en israelsk leverandør af cloud-løsninger. Microsoft vurderer, at aktøren sandsynligvis har brugt kompromitterede legitimationsoplysninger fra udbyderen til at blive godkendt af det israelske logistikfirma. MSTIC observerede den samme aktør forsøge at udføre et destruktivt cyberangreb mod logistikvirksomheden senere på måneden.
- I april 2022 kompromitterede POLONIUM, en Libanon-baseret gruppe, som vi vurderer til at have samarbejdet med iranske statsgrupper om it-supply chain-teknikker, en anden israelsk it-virksomhed for at få adgang til det israelske forsvar og juridiske organisationer.[5]

Dette forløbne års aktivitet viser, at trusselsaktører som NOBELIUM and DEV-0228 kender landskabet for en organisations betroede relationer bedre end selve organisationerne. Denne øgede trussel understreger behovet for, at organisationer forstår dette og styrker deres digitale ejendommes grænser og indgangssteder. Det understreger også vigtigheden af, at it-tjenesteudbydere nøje overvåger deres egen cybersikkerhed. Organisationer bør f.eks. implementere politikker for multifaktorgodkendelse og betinget adgang, der gør det vanskeligere for ondsindede aktører at få adgang til privilegerede konti eller infiltrere hele netværket.

Med en grundig gennemgang og revision af partnerrelationer minimeres eventuelle unødvendige tilladelser mellem din organisation og upstream-udbydere, og adgangen til eventuelle relationer, der ser ukendt ud, kan straks fjernes. Øget kendskab til aktivitetslogfiler og gennemgang af tilgængelig aktivitet gør det lettere at opdage uregelmæssigheder, der kan føre til yderligere undersøgelser.

> Nationalstater, der målretter mod tredjeparter, giver dem mulighed for at udnytte følsomme organisationer ved at udnytte tillid og adgang i en supply chain.

Handlingsrettet indsigt

1. Gennemgå og overvåg upstream- og downstream-tjenesteudbyderrelationer og uddelegerede adgangsrettigheder for at minimere unødvendige tilladelser. Fjern adgang for partnerrelationer, der ikke forekommer bekendte eller endnu ikke er blevet overvåget.[6]
2. Aktivér logføring, og gennemgå alle godkendelsesaktiviteter for fjernadgangsinfrastruktur og VPN'er (virtuelle private netværk), og fokuser på konti, der er konfigureret med enkeltfaktorgodkendelse, for at bekræfte ægthed og undersøge unormal aktivitet.
3. Aktivér MFA for alle konti (herunder tjenestekonti), og sørg for, at MFA håndhæves for alle fjernforbindelser.
4. Brug adgangskodefri løsninger for at beskytte konti.[7]

Links til yderligere oplysninger

- NOBELIUM målretter mod delegerede administrative rettigheder for at gøre det nemmere at udføre bredere angreb | Microsoft Threat Intelligence Center (MSTIC)
- Irans målretning mod it-sektoren er stigende | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Eksponering af POLONIUM-aktivitet og -infrastruktur målrettet mod israelske organisationer | Microsoft Threat Intelligence Center (MSTIC)

Hurtig udnyttelse af sårbarheder

Efterhånden som organisationer styrker deres cybersikkerhedsforhold, reagerer nationalstatsaktører ved at benytte nye og unikke taktikker til at angribe og undgå afsløring. Identifikation og udnyttelse af tidligere ukendte sårbarheder – kaldet zero-day-sårbarheder – er en vigtig taktik i denne indsats.

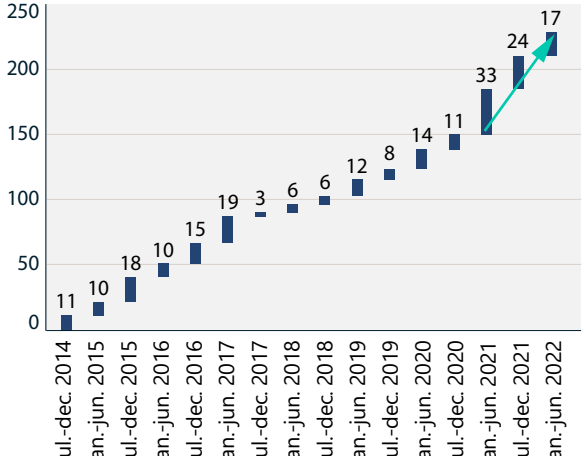
Zero-Day-sårbarheder er et særdeles effektivt middel til indledende udnyttelse, og når sårbarhederne først er blevet offentliggjort, kan de hurtigt genbruges af andre nationalstater og kriminelle aktører. Antallet af offentliggjorte zero-day-sårbarheder i det seneste år er på niveau med dem fra året før, hvilket er det højeste, der er registreret.

Da cybertrusselsaktører – både nationalstater og kriminelle – bliver mere dygtige til at udnytte disse sårbarheder, har vi observeret en reduktion i tiden mellem meddelelsen om en sårbarhed og kommercialiseringen af den pågældende sårbarhed. Derfor er det afgørende, at organisationer benytter programrettelser med det samme. Tilsvarende er det afgørende, at organisationer eller enkeltpersoner, der afdækker nye sårbarheder, på ansvarlig vis videregiver eller rapporterer dem til berørte leverandører så hurtigt som muligt i overensstemmelse med koordinerede procedurer for afsløring af sårbarhed.

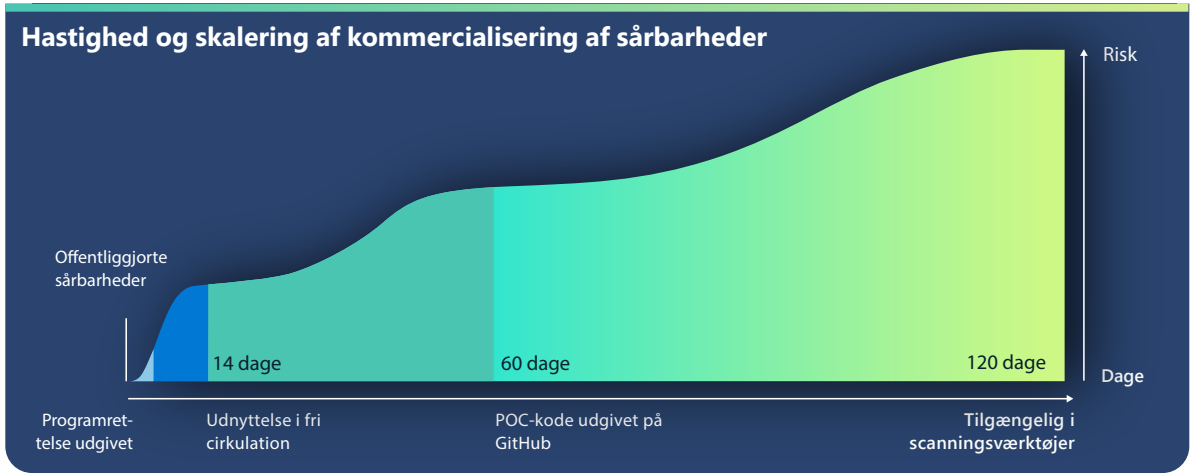
Dette sikrer, at sårbarheder identificeres, og programrettelser udvikles rettidigt for at beskytte kunderne mod tidligere ukendte trusler.

Mange organisationer antager, at de er mindre tilbøjelige til at blive ofre for zero-day-angreb, hvis sårbarhedsstyring er en integreret del af deres netværkssikkerhed. Men kommercialiseringen af udnyttelser fører til, at det sker meget hurtigere. Zero-day-udnyttelser opdages ofte af andre aktører og genbruges bredt i en kort periode, og dette betyder, at systemer uden programrettelser er i fare. Selv om det kan være vanskeligt at opdage zero-day-handlinger, er aktørernes handlinger efter udnyttelse ofte lettere at opdage, og hvis de kommer fra software med programrettelser, kan de fungere som et advarselstegn på en kompromittering.

Programrettelser udgivet for zero-day-sårbarheder



Antallet af offentliggjorte zero-day-udnyttelser fra listen over fælles sårbarheder og afsløringer (CVE'er – Common Vulnerabilities and Disclosures).



I gennemsnit tager det kun 14 dage for en udnyttelse at være i fri cirkulation, efter en sårbarhed er offentliggjort. Denne visning giver en analyse af tidslinjerne for udnyttelse af zero-day-sårbarheder sammen med antallet af systemer, der er sårbare over for den angivne udnyttelse og aktive på internettet fra tidspunktet for første offentliggørelse.

Selvom zero-day-sårbarhedsangreb har en tendens til i første omgang at være målrettet mod et begrænset antal organisationer, bliver de hurtigt indført i det større økosystem af trusselsaktører. Dette starter et kapløb, hvor trusselsaktører skal nå at udnytte sårbarheden så bredt som muligt, før deres potentielle mål installerer programrettelser.

Selvom vi observerer mange nationalstatsaktører, der udvikler udnyttelser fra ukendte sårbarheder, er nationalstatsaktører fra Kina særdeles dygtige til at opdage og udvikle zero-day-udnyttelser. Kinas rapporteringsbestemmelser om sårbarheder trådte i kraft i september 2021, og det var den første i verden, hvor en regering kræver rapportering af sårbarheder til en offentlig myndighed, før sårbarheden deles med produktet eller tjenesteejeren. Denne nye bestemmelse kan gøre det muligt for elementer i den kinesiske regering at oplagre rapporterede sårbarheder og benytte dem som våben. Den øgede anvendelse af zero-day-sårbarheder i løbet af det seneste år fra kinabaserede aktører afspejler sandsynligvis det første hele år af Kinas krav om offentliggørelse af sårbarheder, som er pålagt det kinesiske sikkerhedsfællesskab, og repræsenterer et stort skridt i brugen af zero-day-udnyttelse som en statslig prioritet. De sårbarheder, der er beskrevet nedenfor, blev først udviklet og implementeret i angreb af nationalstatsaktører i Kina, før de blev opdaget og udbredt blandt andre aktører i det større trusselsøkosystem.

Hurtig udnyttelse af sårbarheder

Fortsat

Selv organisationer, der ikke er et mål for nationalstatsangreb, har en begrænset periode til at programrette zero-day-sårbarheder i de berørte systemer, før sårbarhederne udnyttes af det bredere aktørøkosystem.

Disse eksempler på nyligt identificerede sårbarheder viser, at organisationer i gennemsnit har 60 dage fra det tidspunkt, hvor sårbarheden er blevet programrettet, og en POS-kode (proof of concept) er stillet til rådighed online og ofte er opfanget af andre aktører med henblik på genbrug. Tilsvarende har organisationer i gennemsnit 120 dage, før en sårbarhed er tilgængelig i automatiseret scanning af sårbarheder og udnyttelsesværktøjer som Metasploit – hvilket ofte resulterer i udnyttelse i et massivt omfang. Dette viser, at selv organisationer, der ikke er et mål for nationalstatstrusselsaktører, har en begrænset periode til at programrette zero-day-sårbarheder i de berørte systemer, før sårbarhederne udnyttes af det bredere aktørøkosystem.

CVE-2021-35211 SolarWinds Serv-U

I juli 2021 udgav SolarWinds en sikkerhedsrådgivning for CVE-2021-35211, hvor de gav Microsoft æren for meddelelsen.[8] På det tidspunkt opdagede vi, at nationalstatsaktøren DEV-0322 aktivt udnyttede SolarWinds Serv-U-sårbarheden. Vores RiskIQ-team observerede 12.646 IP-adresser, der var vært for internetforbundne versioner af de berørte enheder mellem den 15. juni og den 9. juli.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

I september 2021 observerede vores forskere aktører tilknyttet Kina, der udnyttede Zoho ManageEngine på flere enheder med base i USA. Sårbarheden blev offentligt rapporteret den 6. september som CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, som organisationer typisk bruger til at håndtere nulstilling af adgangskoder.[9] DEV-0322 udnyttede sårbarheden senere i september og brugte den som en indledende vektor til at få fodfæste i netværk og udføre yderligere handlinger, herunder dumping af legitimationsoplysninger, installation af tilpassede binære filer og implementering af malware for at opretholde vedholdenhed. På tidspunktet for afsløringen observerede RiskIQ 4.011 forekomster af disse systemer, der var aktive og på internettet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

I slutningen af oktober 2021 observerede vi DEV-0322 udnytte en sårbarhed (CVE-2021-44077) i et andet Zoho ManageEngine-produkt, ServiceDesk Plus – en it-helpdesk-software med aktivmanagement. DEV-0322 benyttede denne sårbarhed til at målrette mod og kompromittere enheder inden for sundhedssektoren, informationsteknologi, videregående uddannelser og kritiske produktionssektorer. Den 2. december udsendte FBI (Federal Bureau of Investigation) og CBOT (Cybersecurity and Infrastructure Security Agency) en fælles advarsel til offentligheden om nationalstatsaktører, der udnyttede sårbarheden. På tidspunktet for offentliggørelsen observerede RiskIQ 7.956 forekomster af disse systemer, der var aktive og på internettet.

CVE-2021-42321 Microsoft Exchange

En zero-day-udnyttelse af en Exchange-sårbarhed CVE-2021-42321 blev afsløret under Tianfu Cup, et internationalt cybersikkerhedsmøde og en hackingkonkurrence, der blev afholdt den 16. og 17. oktober 2021 i Chengdu i, Kina. Sikkerhedseksperter på Microsoft observerede udnyttelse af Exchange-sårbarheden, der var i fri cirkulation den 21. oktober, kun tre dage efter at sårbarheden blev afsløret. På tidspunktet for offentliggørelsen observerede RiskIQ 61.559 forekomster af disse systemer, der var aktive og på internettet. Vi fortsatte med at observere udnyttelsesaktivitet til november 2021.

CVE-2022-26134 Confluence

En aktør med tilknytning til Kina havde sandsynligvis zero-day-udnyttelseskoden til Confluence-sårbarheden (CVE-2022-26134), fire dage før sårbarheden blev offentliggjort den 2. juni, og udnyttede den sandsynligvis mod en amerikansk baseret enhed. På tidspunktet for offentliggørelsen observerede RiskIQ 53.621 forekomster af sårbare Confluence-systemer, der var aktive og på internettet.

Sårbarheder bliver hentet og udnyttet i et massivt omfang og inden for stadig kortere tidsrammer.

Handlingsrettet indsigt

1. Prioriter programrettelser af zero-day-sårbarheder, så snart de frigives. Vent ikke på, at administrationscyklussen for programrettelser implementeres.
2. Dokumentér og registrer alle virksomhedens hardware- og softwareaktiver for at bestemme risici og hurtigt bestemme, hvornår der skal handles på programrettelser.

Russiske statslige aktørers cybertaktik i krigstid truer Ukraine med flere

I år lancerede russiske stataktører cyberoperationer for at supplere militær indsats under den russiske invasion af Ukraine og benyttede ofte de samme taktikker og teknikker som mod mål uden for Ukraine. Det er afgørende, at organisationer over hele verden tager skridt til at styrke cybersikkerheden mod digitale trusler, der stammer fra trusselsaktører i Rusland.

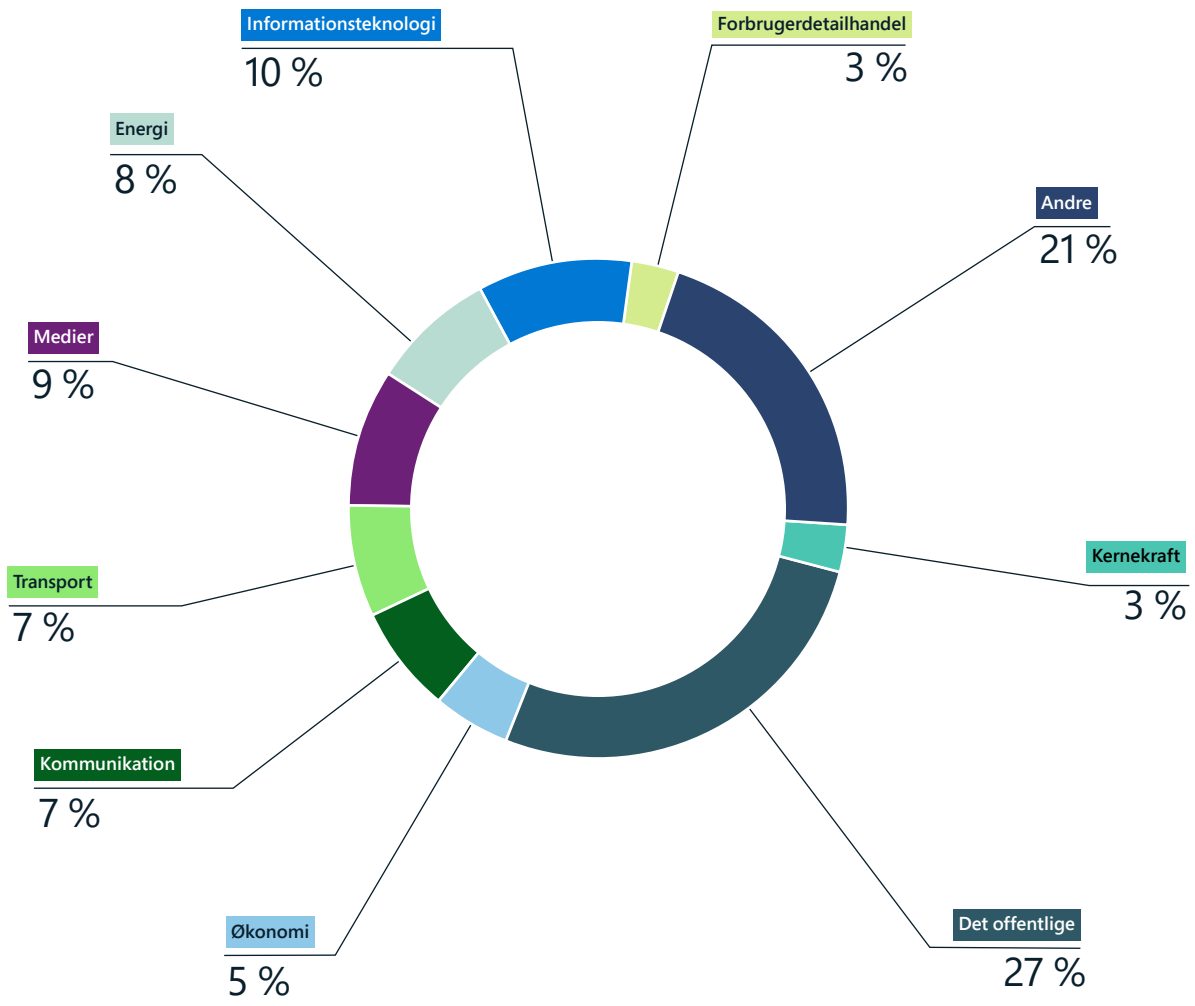
Situationen på stedet er fortsat ustabil på grund af den igangværende militære konflikt, og Ukraine og deres allierede skal være parate til at forsvare sig, hvis de russiske statslige cyberoperatører øger hyppigheden eller intensiteten af indtrængen i overensstemmelse med militære mål. I de første fire måneder af krigen observerede Microsoft trusselsaktører, der var knyttet til det russiske militær, lancere flere bølger af destruktive cyberangreb mod næsten 50 forskellige ukrainske bureauer og virksomheder og spionagefokuserede indtrængen mod mange andre. Med undtagelse af operationer mod kunder med onlinetjenester blev 64 % af den russiske trusselsaktivitet mod kendte mål rettet mod organisationer i Ukraine i perioden fra slutningen af februar til juni.

I hver operation benyttede de russiske trusselsaktører mange af de taktikker, teknikker og procedurer (TTP'er), som vi observerede før invasionen mod mål, både inden for og uden for Ukraine. Disse aktører havde til hensigt at destruere data og skabe ubalance inden for de offentlige myndigheder i den første periode af konflikten. De har siden forsøgt at spænde ben for transporten af militær og humanitær assistance til soldaterne, afskære den offentlige adgang til tjenester og medier og stjæle oplysninger om længerevarende efterretninger eller af økonomisk værdi for Rusland.

Målretning mod transport truer et område af afgørende betydning for ukrainske borgere, der forsøger at overleve konflikten. Ifølge en UNICEF-sponsoreret undersøgelse i maj var respondenterne i konfliktramte byområder mest bekymrede over transport og brændstof, forsyningsafbrydelser, sikkerhed og begrænset adgang til fødevarer, sundhedspleje og finansielle tjenesteydelser.[10] I juni sagde FN's krisekoordinator for Ukraine, at mindst 15,7 millioner mennesker i Ukraine havde akut behov for humanitær assistance, og at antallet ville stige, efterhånden som krigen fortsatte.[11]

Uden for Ukraine opdagede Microsoft russiske netværksindtrængningsforsøg mod 128 organisationer i 42 lande mellem slutningen af februar og juni. USA var Ruslands vigtigste mål. Polen, hvor en stor del af den internationale militære og humanitære assistance til Ukraine passerer igennem, var også et vigtigt mål i denne periode. Trusselsaktører med tilknytning til den russiske stat forsøgte også at infiltrere organisationer i de baltiske lande og computernetværk i Danmark, Norge, Finland og Sverige i april og maj.

De mest målrettede branchesektorer i Ukraine siden invasionen



Føderale, statslige og lokale myndigheder i Ukraine er forblevet prioriterede mål for russiske stats- og statstilknyttede trusselsgrupper under hele konflikten. Fokus på organisationer inden for transport, energi, finans og medier fremhæver den risiko, som disse cyberaktiviteter udgør for tjenester, som ukrainske borgere er afhængige af.

Russiske statslige aktørers cybertaktik i krigstid truer Ukraine med flere

Fortsat

Vi har set en stigning i lignende aktivitet målrettet mod udenrigsministerier i NATO-lande.

I det forløbne år har de russiske trusselsgrupper fortsat været interesserede i at kompromittere kritisk infrastruktur både inden for og uden for Ukraine. IRIDIUM implementerede Industroyer2-malwaren i et mislykket forsøg på at efterlade millioner af mennesker i Ukraine uden strøm. Uden for Ukraine udførte BROMINE indtrængningsforsøg mod organisationer, der er involveret i produktions- og industrielle kontrolsystemer, i begyndelsen af 2022.

Russiske stats- og statstilknyttede aktører udførte i år cyberoperationer mod Ukraine, deres allierede og andre mål af efterretningsværdi ved at benytte mange af følgende TTP'er:

Spear-phishing med skadelige vedhæftede filer eller links

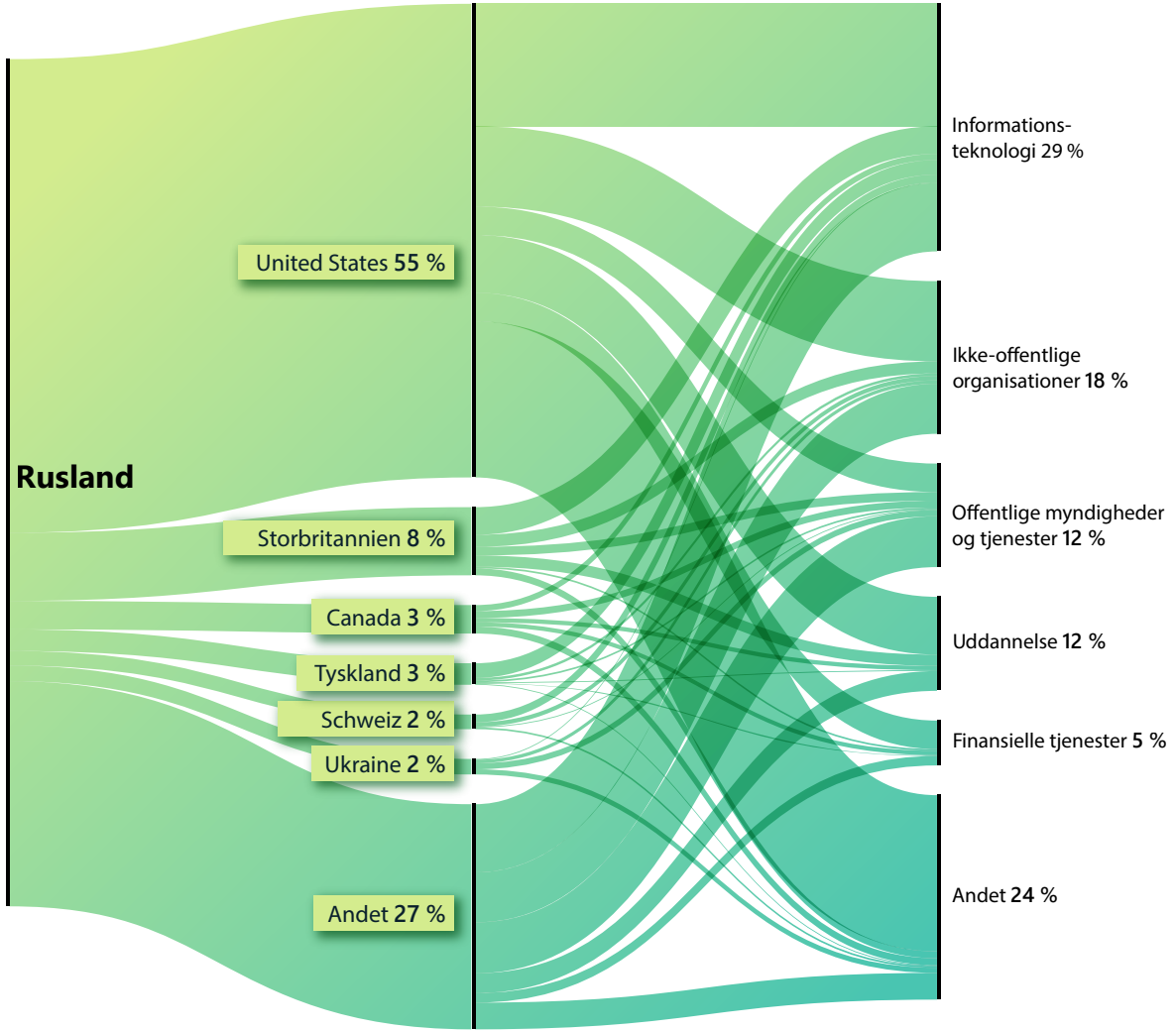
Russiske stats- og statstilknyttede grupper som ACTINIUM, AFSONIUM, STRONTIUM, DEV-0257, SEABORGIUM og IRIDIUM brugte alle phishing-kampagner til at få indledende adgang til ønskede konti og netværk i organisationer inden for og uden for Ukraine. Mange kampagner udnyttede kompromitterede eller spoofede konti i målrettede organisationer eller inden for samme branche og overbevisende temaer for at tiltrække ofre. NOBELIUM benyttede kompromitterede diplomatiske konti til at sende phishingmail forklædt som diplomatisk kommunikation til ansatte i udenrigsministerier i hele verden. STRONTIUM oprettede spoof-konti baseret på offentligt tilgængelige navne på kontoejere i tænketanke i USA og sendte phishingmeddelelser for at få adgang til konti i disse tænketanke. SEABORGIUM udførte phishing ved at benytte fælder relateret til rapportering om konflikten i Ukraine for at få adgang til konti i tænketanke for internationale anliggender i de nordiske lande.

Udnyttelse af supply chain for it-tjenester for at påvirke downstream-kunder

I slutningen af 2021 kompromitterede russiske statsaktører it-tjenesteudbydere og brugte adgangen til at ødelægge websteder og implementere den destruktive malware Whispergate via DEV-0586 i januar.[12] DEV-0586 kompromitterede også netværket i et it-firma, der byggede ressourcestyringssystemer for det ukrainske forsvarsministerium og andre organisationer inden for kommunikations- og transportsektoren, hvilket antyder, at gruppen også udforskede muligheder for tredjepartsangreb i disse sektorer.

På verdensplan, men især i USA og Vesteuropa, målrettede NOBELIUM mod it-tjenesteudbydere for at få adgang til offentlige myndigheder og andre følsomme netværk i hele 2021-2022 (se beskrivelsen af supply chain-sårbarheder tidligere i dette kapitel).

Rusland: De mest målrettede lande og brancher



På trods af et intensiveret fokus siden begyndelsen af 2022 på organisationer med base i Ukraine var virksomheder med base i Nordamerika og Vesteuropa stadig de onlineservicekunder, som russiske aktører målrettede mest. NOBELIUM's kampagne mod it-sektoren har gjort den til den mest målrettede sektor i det forløbne år.

Russiske statslige aktørers cybertaktik i krigstid truer Ukraine med flere

Fortsat

Udnyttelse af offentligt rettede applikationer til at få indledende adgang til netværk

Siden i hvert fald slutningen af 2021 har STRONTIUM arbejdet på at udvikle og forfine sine funktioner til at udnytte offentlige tjenester, f.eks. på Microsoft Exchange-servere, til at stjæle oplysninger. STRONTIUM udnyttede Exchange-servere uden programrettelser til at få adgang til ukrainske myndigheders konti samt militær- og forsvarsindustrirelaterede organisationer i USA, Libanon, Peru og Rumænien samt andre statslige organer i Armenien, Bosnien, Kosovo og Malaysia. DEV-0586, der også er tilknyttet det russiske militær, udnyttede Confluence-serversårbarheder til at få indledende adgang til organisationer i den offentlige sektor og it-sektoren i Ukraine og andre østeuropæiske lande.

Russiske stats- og tilknyttede trusselsaktører benytter mange af de samme TTP'er til at kompromittere organisationer af interesse i både krig og fred.

Brug af administrative konti og protokoller samt indbyggede hjælpeprogrammer til netværksregistrering og tværgående bevægelser

Efter at russiske statsaktører havde opnået indledende adgang til et netværk, observerede Microsoft, at de benyttede lovlige konti og softwareprogrammer til at udføre grundlæggende vedligeholdelsesopgaver for at undgå registrering så længe som muligt. De stolede på kompromitterede identiteter med administrative funktioner og gyldige administrationsprotokoller, værktøjer og metoder til at bevæge sig på tværs i netværk uden straks at tiltrække sig opmærksomhed fra automatiserede overvågninger og netværksforsvarere.

Grundlæggende cyberhygiejne og implementering af endpoint-registrerings- og responsværktøjer kan hjælpe med at afbøde de negative konsekvenser af disse typer aktiviteter i både freds- og krigstid.

Den uforudsigelighed, der er forbundet med den igangværende konflikt, kræver, at organisationer over hele verden træffer foranstaltninger til at styrke cybersikkerheden mod digitale trusler, der stammer fra den russiske stat og de trusselsaktører, der er tilknyttet Rusland.

Handlingsrettet indsigt

1. Minimer tyveri af legitimationsoplysninger og misbrug af konti ved at beskytte dine brugeres identiteter ved at implementere MFA-identitetsbeskyttelsesværktøjer og håndhæve adgang med færrest mulige rettigheder for at sikre de mest følsomme og privilegerede konti og systemer.
2. Anvend opdateringer for at sikre, at alle dine systemer får det højeste beskyttelsesniveau så hurtigt som muligt og kontinuerligt opdateres.
3. Implementer antimalware-, endpoint-registrerings- og identitetsbeskyttelsesløsninger på tværs af din organisation. En kombination af avancerede sikkerhedsløsninger kombineret med uddannet og kompetent personale, kan give din organisation mulighed for at identificere, opdage og forhindre indtrængen, der påvirker virksomhedens drift.
4. Iværksæt undersøgelser og genoprettelse i tilfælde af, at du registrerer eller modtager meddelelser om en trussel mod dit miljø ved at sikkerhedskopiere kritiske systemer og aktivere logføring. Der opfordres kraftigt til at udarbejde en handlingsplan.

Links til yderligere oplysninger

- Forsvare Ukraine: Tidlige erfaringer fra cyberkrigen | Microsoft On the Issues
- Hybridkrigen i Ukraine | Microsoft On the Issues
- Cybertrusselsaktivitet i Ukraine: analyse og ressourcer| Microsoft Security Response Center (MSRC)
- Afbrydelse af målretning af cyberangreb mod Ukraine | Microsoft On the Issues
- Malwareangreb, der målretter myndighederne i Ukraine | Microsoft On the Issues
- MagicWeb: NOBELIUM's trick til at godkende som enhver efter kompromittering | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

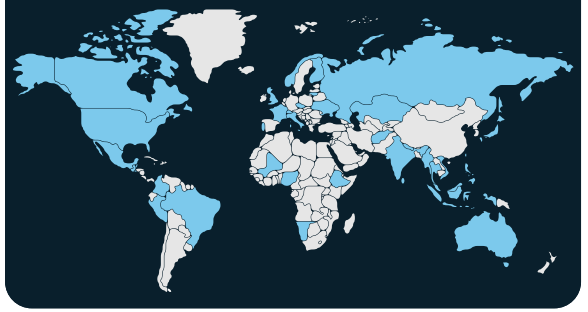
Kina udvider den globale målretning for at opnå konkurrencemæssige fordele

I nutidens komplekse geopolitiske klima forsøger kinesiske stats- og statstilknyttede trusselsaktører, der udfører cyberoperationer, ofte på at fremme landets strategiske mål for militær, økonomi og eksterne relationer som en del af Kinas mål om at opnå en konkurrencemæssig fordel. I det seneste år har Microsoft observeret udbredte kinesiske trusselsaktiviteter rettet mod lande rundt om i verden.

Siden midten af 2021 har Kina forsøgt at sikre økonomisk og finansiel stabilitet midt i den værste stigning af COVID-19 i to år.[13] Kina fortsatte med at jonglere rundt med deres holdninger til geopolitiske begivenheder, såsom kampen for at skabe balance mellem deres "ubegrænsede" partnerskab med Rusland[14] og fastholde deres position på den internationale scene.[15] Derudover fortsatte Kinas kamp mod USA og deres allierede i forbindelse med Taiwan[16] og Det Sydkinesiske Hav fortsatte med at belaste relationerne med mange lande.[17]

Kinesiske stats- og statstilknyttede trusselsgrupper øgede målretningen mod mindre lande rundt om i verden med fokus på Sydøstasien for at opnå konkurrencemæssige fordele på alle fronter.

Lande, som er målrettet af kinesiske stats- og statstilknyttede grupper

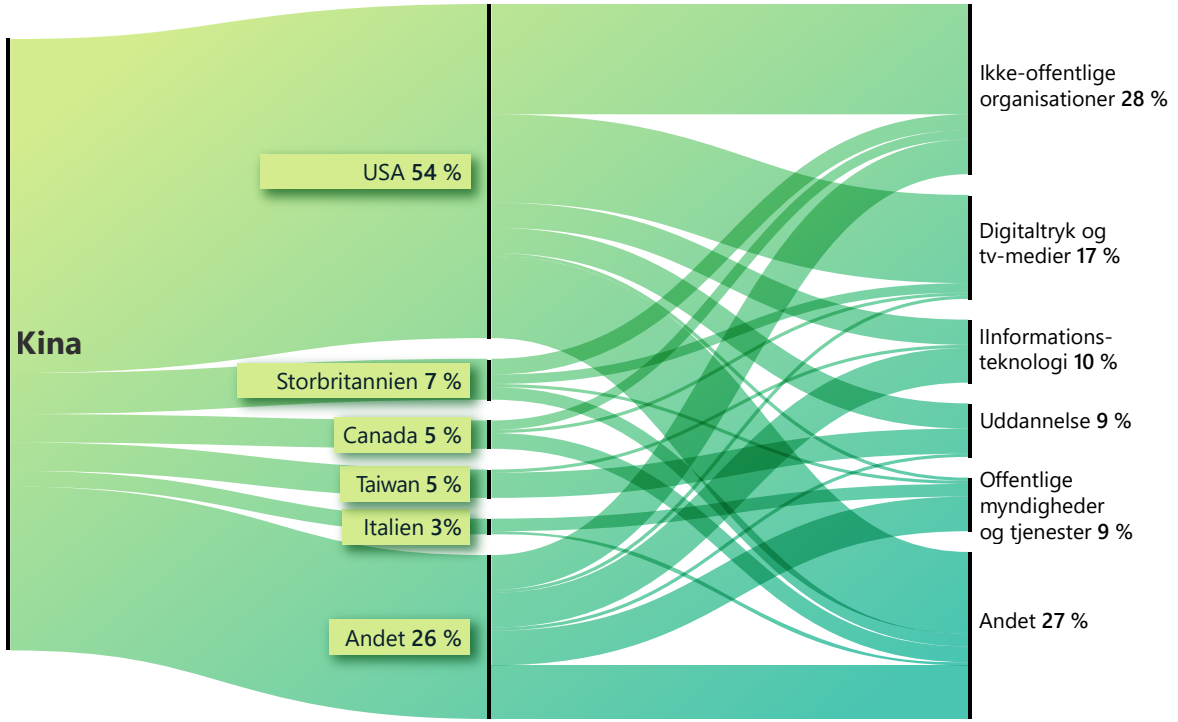


Kina fortsatte også med at udvide sin økonomiske indflydelse globalt gennem det tidligere etablerede Belt and Road-initiativ (BRI) og forsøgte at genoplive en omfattende investeringsramme med EU,[18] og forhandle en ny regional handelsaftale med 15 lande i Asien og Stillehavsområdet, også kaldet Regional Comprehensive Economic Partnership (det regionale vidtrækkende økonomiske partnerskab).[19] Microsoft vurderer, at Kina fortsat vil bruge cybersamling som et værktøj til at fremme sine strategiske politiske, militære og økonomiske mål på grund af observerede cyberaktiviteter og de mange målrettede enheder.

Cybermålretninger kan sandsynligvis fremme økonomiske og militære interesser.

Microsoft observerede udbredt målretning mod mindre lande rundt om i verden af kinesiske stats- og statstilknyttede trusselsgrupper, hvilket tyder på, at Kina sandsynligvis bruger cyberespionage som en komponent i sin globale økonomiske og militære indflydelse.

Kina: De mest målrettede lande og brancher



Tænketanke/NGO'er, medier, it, offentlige myndigheder og undervisningssektoren var blandt de sektorer, der var mest målrettede for kinesiske trusselsgrupper, sandsynligvis til vedvarende indsamling af efterretninger og rekognoscering.

Målene omfattede, men var ikke begrænset til, lande i Afrika, Caribien, Mellemøsten, Oceanien og Sydøstasien, med særligt fokus på disse lande i Sydøstasien og Stillehavsøerne.

I overensstemmelse med Kinas BRI-strategi målretter Kina-baserede trusselsgrupper enhederne i Afghanistan, Kazakhstan, Mauritius, Namibia og Trinidad og Tobago.[20] Trinidad og Tobago var f.eks. det første caribiske land, der støttede Kinas BRI-strategi i 2018, og Kina betragter dem som en vigtig partner i regionen. NICKEL har haft vedvarende netværksaktiviteter rettet mod Trinidad og Tobago siden 2021. I marts 2022 udførte NICKEL f.eks. rekognosceringsaktiviteter mod en offentlig instans, sandsynligvis med henblik på dataindsamlingsformål.

Kina udvider den globale målretning for at opnå konkurrencemæssige fordele

Fortsat

I mellemtiden observerede Microsoft kinesiske stats- og statstilknyttede trusselsgrupper, der fokuserede deres netværksaktiviteter mod enheder i Sydøstasien og udvidede til lande i Stillehavsområdet, da Kina ændrede sine militære og økonomiske prioriteter for at håndtere udfordringerne med USA's fornyede interesse i regionen. I januar 2022 observerede Microsoft, at RADIUM målrettede mod et energiselskab og en energitilknyttet offentlig myndighed i Vietnam og en indonesisk offentlig myndighed. RADIUM's aktiviteter er sandsynligvis i overensstemmelse med Kinas strategiske mål i Det Sydkinesiske Hav.[21] I slutningen af februar og begyndelsen af marts kompromitterede GALLIUM mere end 100 konti, der er tilknyttet en fremtrædende organisation (IGO) i Sydøstasien. Tidspunktet for GALLIUM's målretning mod IGO i regionen faldt sammen med annonceringen af et planlagt møde mellem USA og regionale ledere. GALLIUM-aktører fik sandsynligvis til opgave at overvåge kommunikationen og indsamle efterretninger før arrangementet.

Da Kina udvidede sin indflydelse i landene på Stillehavsøerne, fulgte de kinesiske trusselsgruppers aktiviteter med. I april underskrev Kina og Salomonøerne en sikkerhedsaftale, der havde til formål at "fremme fred og sikkerhed". Aftalen giver potentielt Kina mulighed for at indsætte bevæbnet politi og militær på Salomonøerne.[22] I maj var Kina vært for det andet udenrigsministermøde mellem Kina og landene på Stillehavsøerne (PIC'er) på Fiji, og foreslog at fremme et "omfattende strategisk partnerskab" for at fremme politiske, kulturelle, sociale, sikkerhedsmæssige og klimaændringsmæssige interesser samt for at bekæmpe pandemien.[23] Omkring samme tid i maj identificerede Microsoft GADOLINIUM's skadelige malware på Salomonøernes offentlige systemer. RADIUM kørte også skadelig kode på systemer i et telekommunikationsselskab i Papua Ny Guinea. Vi vurderer, at disse aktiviteter, at sandsynligvis var til dataindsamlingsformål for at støtte Kinas overordnede regionale strategi.

Microsoft afbryder NICKEL-aktiviteter, men trusselsgruppen viser sin vedholdenhed.

I december 2021 indsendte Microsoft DCU (Digital Crimes Unit) ansøgninger til den amerikanske distriktsdomstol i det østlige Virginia, om at få tilladelse til at beslaglægge 42 kommando- og kontroldomæner (C2), der kontrolleredes af NICKEL. Disse C2-domæner havde været anvendt i aktiviteter mod myndigheder, diplomatiske enheder og NGO'er i Central- og Sydamerika, Caribien, Europa og Nordamerika siden september 2019.[24] Ved hjælp af disse operationer havde NICKEL opnået langsigtet adgang til flere enheder og konsekvent eksfiltreret data fra visse ofre siden slutningen af 2019.

I takt med at Kina fortsætter med at etablere økonomiske relationer til flere lande – ofte i aftaler, der er knyttet til BRI – fortsætter Kinas globale indflydelse med at vokse. Vi vurderer, at kinesiske statslige og statstilknyttede trusselsaktører vil målrette mod deres offentlige myndigheder, diplomati og NGO-sektorer for at få ny indsigt, som sandsynligvis vil kunne bruges til økonomisk spionage eller traditionelle efterretningsindsamlingsmål. Siden Microsoft afbrydelse har NICKEL målrettet mod flere offentlige myndigheder, sandsynligvis i et forsøg på at genvinde mistet adgang. I perioden fra slutningen af marts til maj 2022 kompromitterede NICKEL igen mindst fem offentlige instanser over hele verden. Dette tyder på, at gruppen havde flere indgangspunkter til disse enheder eller genvandt adgangen via nye C2-domæner. NICKEL's vedholdenhed ved gentagne gange at kompromittere de samme offentlige myndigheder globalt fortæller noget om opgavens vigtighed på højt niveau.

Kina bliver mere selvsikker, når det gælder udenrigspolitik. Vi vurderer, at cyberbaseret økonomisk spionage og indsamling af efterretninger sandsynligvis vil fortsætte.

Handlingsrettet indsigt

1. Forstærk cyberforsvaret for proaktivt at afbøde cybertrusler. De kinesiske trusselsaktørers vedholdenhed kræver, at organisationer rettidigt identificerer, beskytter, registrerer og reagerer på mulig indtrængen.
2. Trusselsaktører misbruger planlagte opgaver[25] som en almindelig metode til vedholdenhed og forsvarsunddragelse. Sørg for, at dit miljø anvender yderligere sikkerhedsretningslinjer for at beskytte mod denne almindeligt anvendte teknik.[26]
3. Vi fortsætter med at observere brugen af webshells som en indledende vektor i målrettede netværk.[27] Organisationer bør styrke deres systemer mod web shells-angreb, der kan give angribere adgang til at køre fjernkommandoer.[28]

Links til yderligere oplysninger

- NICKEL målretter mod statslige organisationer i hele Latinamerika og Europa | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Protecting people from recent cyberattacks | Microsoft On the Issues

Iran bliver stadig mere aggressiv efter magtskifte

Microsoft har observeret, at iranske statsgrupper og tilknyttede aktører øger hastigheden og omfanget af cyberangreb mod Israel, udvider ransomware-angreb ud over regionale modstandere til amerikanske og europæiske ofre og målretter mod højt profilerede kritisk infrastruktur i USA for at forberede sig på potentielle destruktive cyberangreb.

Iranske statsaktørers voksende cyberaggression efter præsidentskifte. I sommeren 2021 erstattede den konservative præsident Ibrahim Raisi den moderate præsident Hassan Rouhani. I skarp modsætning til Raisi, der er en protégé af den øverste leder og en nær allieret med IRGC (Den Islamiske Revolutionsgarde), bragte den tidligere præsident Rouhanis tilbøjelighed til diplomati ham ofte på kant med den øverste leder og IRGC's topledere.[29] Raisi-administrationens høgeagtige synspunkter ser ud til at have gjort aktørerne mere villige til at udføre mere dristige aktiviteter mod Israel og Vesten, især USA, til trods for genoptagelsen af det diplomatiske engagement for at genoplive atomaftalen med Iran.

Øget hastighed og omfang af iranske cyberangreb mod Israel

Få uger efter at Raisi dannede sit udenrigspolitiske team[30], genoptog iranske statsaktører destruktive cyberangreb mod Israel i et hurtigere tempo end i de foregående år. Disse ransomware- og hack-and-leak-angreb blev udført med nogle få ugers mellemrum fra begyndelsen af september og omfattede mindst tre iransk tilknyttede aktører, hvilket antyder, at angrebene kan have været en del af en landsdækkende gengældelseskampagne mod Israel. I mindst ét tilfælde vurderede Microsoft, at et ransomware-angreb mod en israelsk organisation i slutningen af 2021 var beregnet på at skjule et underliggende datasletningsangreb. Microsofts malwareanalyse fandt frem til, at den ransomware, der blev leveret til ofret, var programmeret til at køre wiper-malware efter kryptering.

I 2022 eskalerede iranske malwareangreb i deres målvalg og form for angreb. I februar forsøgte DEV-0198 at udføre et destruktivt angreb mod kritisk israelsk infrastruktur. Microsoft vurderer også, at en iransk tilknyttet aktør sandsynligvis var ansvarlig for et sofistikeret cyberangreb, der startede nødraketsirener i Israel i juni, sandsynligvis ved hjælp af software, der justerer lyd via IP-netværk.

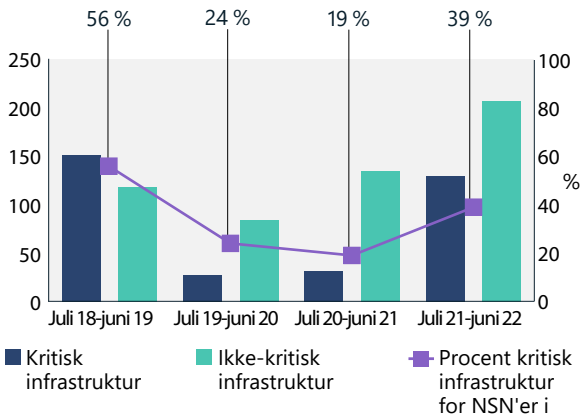
Iransk trussel mod kritisk infrastruktur i USA og Israel blev intensiveret i løbet af året

Iranske statsaktører, som Microsoft vurderer som tilknyttede til IRGC (PHOSPHORUS og DEV-0198), målrettede mod højt profileret kritisk infrastruktur i USA og Israel fra slutningen af 2021 og frem til midten af 2022. Det sandsynlige formål var at give Teheran mulighed for at gengælde de samme sektorer, som højtstående IRGC-embedsmænd beskyldte USA og Israel for at forstyrre i Iran.[31] Vi vurderer, at denne aktivitet er knyttet til erklæringer i slutningen af oktober 2021, som blev fremsat af IRGC's general Gholamreza Jalali, leder af Irans Passive Defense Organization, som gentog udtalelser fra andre indflydelsesrige personer i regimet, om at USA og Israel udførte cyberangreb på Irans havne, jernbaner og tankstationer.[32] Jalali fremsatte denne beskyldning for anden gang under en iscenesat fredagstale på et podie med billedet af et missil, der rammer ordet "USA", og antyder, at hans overordnede havde samme holdning.[33]

I oktober 2021 begyndte PHOSPHORUS en omfattende scanning af amerikanske organisationer for Fortinet- og ProxyShell-sårbarheder uden programrettelser. Når disse systemer uden programrettelser var kompromitteret, blev de brugt til at udføre ransomware-angreb i flere tilfælde mod kritisk infrastruktur i USA og andre vestlige lande. Disse markerede de første bekræftede tilfælde af iranske statstilknyttede ransomware-angreb uden for Mellemøsten. Efter cyberangrebet mod Irans tankstationer i slutningen af oktober observerede Microsoft en stigning i ransomware-angreb mod amerikanske virksomheder, hvilket tyder på mulig sammenhæng.

Samtidig skiftede PHOSPHORUS til direkte målretning – ofte via spear-phishing – mod højt profilerede amerikanske kritiske infrastrukturvirksomheder, herunder store havne og transitsystemer, forsyningsselskaber og olie- og gasselskaber. Denne målretning, der ofte blev udført via spear-phishing, varede indtil midten af 2022. Målene er i fuldstændig overensstemmelse med de sektorer, som Teheran har givet USA og Israel skylden for at have angrebet i Iran og har sandsynligvis givet Iran muligheder for gengældelse. Kompromitteringen af næsten identiske mål giver mulighed for at forhindre lignende fremtidige angreb, samtidig med at de forsøger at undgå eskalering ved at signalere årsagen til angreb uden at indrømme nogen skyld.

Genopblussen af iransk målretning mod infrastruktur



Iransk målretning mod kritisk infrastruktur steg til det højeste niveau, der er observeret siden slutningen af 2018 til starten af 2019. Vi brugte det amerikanske præsidentielle politiske direktiv 21 (PPD-21) til at afgøre, om en virksomhed opfyldte kriterierne for kritisk infrastruktur. (Juli 2021-juni 2022).

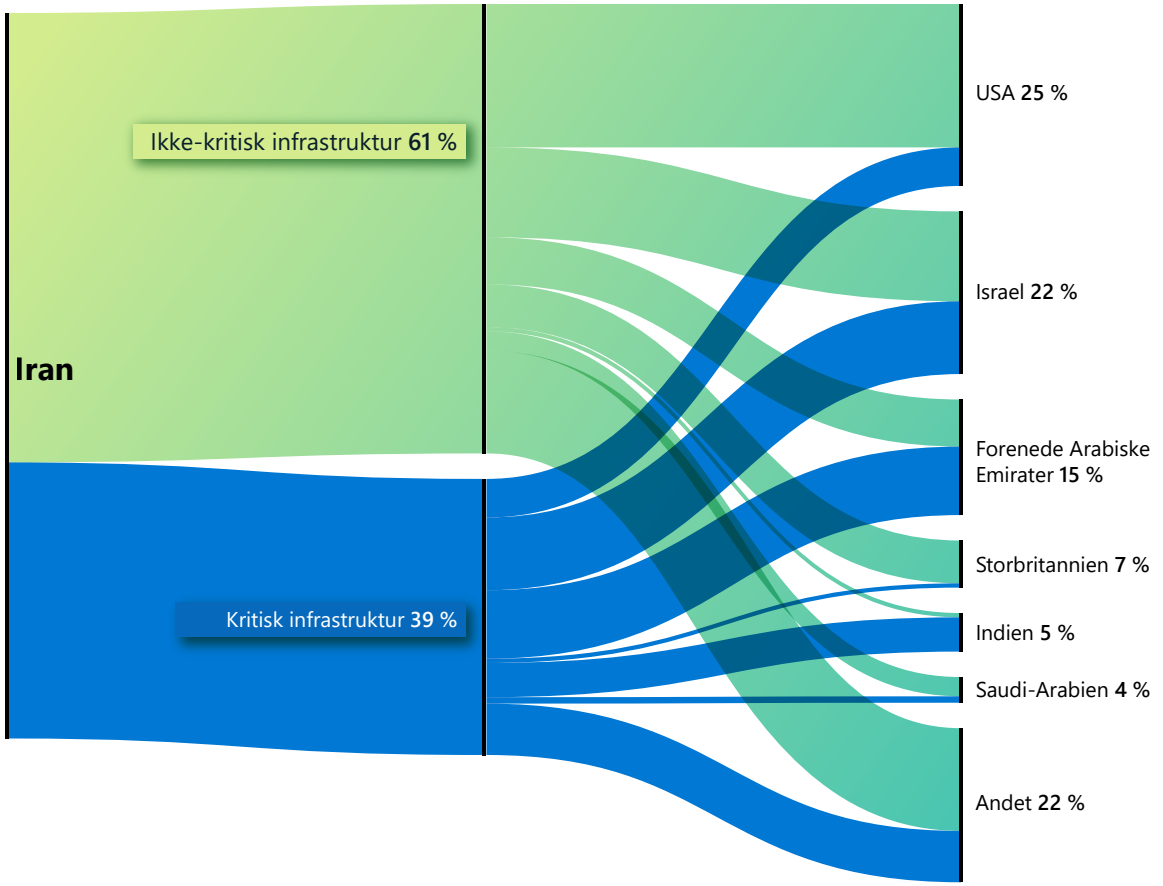
Iran bliver stadig mere aggressiv efter magtskifte

Fortsat

I Israel målrettede DEV-0198 mod israelske jernbaner, logistikvirksomheder, softwareudbydere af logistikvirksomheder og brændstofvirksomheder med fokus på tankstationer. I starten af 2022 udførte gruppen et angreb på netværket i en stor israelsk logistikvirksomhed, som tvang virksomheden til at lukke sine computere og nogle af dens aktiviteter for at begrænse angrebet. I et andet tilfælde observerede vi, at gruppen forsøgte at få adgang til netværket hos en stor israelsk transportudbyder med stjålne eller genbrugte legitimationsoplysninger. I mellemtiden kompromitterede en anden iransk aktør, DEV-0343, hvis målretning mod virksomheder inden for forsvar, søtransport og satellitbilleder antyder en tilknytning til IRGC, konti hos israelske transport- og havnerelaterede enheder i begyndelsen af 2021.

Iranske trusselsgrupper vil sandsynligvis forblive en trussel mod amerikanske og israelske transport- og energivirksomheder, især da diplomatiske bestræbelser på at genoplive atomaftalen med Iran går i hårdknude, og Washington, Tel Aviv og Teheran vil forsøge at anvende alternative tvangsmidler for at opnå indrømmelser.

Iransk målretning mod kritisk infrastruktur efter land



Irans målretning mod kritisk infrastruktur forekom hovedsageligt mod israelske, emiratiske og amerikanske organisationer.

Iranske aktører vil sandsynligvis forblive en trussel mod amerikanske og israelske transport- og energiselskaber i det kommende år.

Iranske grupper har udvidet ransomware-angreb ud over regionale modstandere og målretter mod højt profilerede kritiske infrastrukturmål i USA og Israel.

Handlingsrettet indsigt

1. Gør din organisations generelle cyberhygiejne bedre ved at aktivere adgangskodefri løsninger som MFA, og håndhæv brugen af det til alle fjernforbindelser for at afbøde eventuelle potentielt kompromitterede legitimationsoplysninger.
2. Evaluer ægtheden af al indgående mailtrafik for at sikre, at afsenderadressen er lovlig.
3. Implementer programrettelser tidligt og ofte.[34]
4. Gennemgå og overvåg hver enkelt af dine partnerrelationer med tjenesteudbydere for at minimere eventuelle unødvendige tilladelser mellem din organisation og upstream-leverandører. Microsoft anbefaler, at du omgående fjerner adgang for partnerrelationer, der ikke forekommer bekendte eller endnu ikke er blevet overvåget.[35]

Links til yderligere oplysninger

- Irans målretning mod it-sektoren er stigende | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Iran-tilknyttet DEV-0343 målretter mod forsvar, GIS og søfartssektorer | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Libanesisk gruppe med tilknytning til Iran målretter mod Israel

Microsoft overvåger cybertrusler uanset platform, målrettet offer eller geografisk region. Vi opretholder synlighed og aktiv trusselsjagt i hele verden for at skrive bedre registreringer til vores kunder.

Selvom trusler fra Rusland, Kina, Iran og Nordkorea udgør størstedelen af vores observerede aktiviteter fra nationalstatsaktører, sporer og kommunikerer vi også om trusler fra NATO-medlemslande og demokratiske nationer. Sidste år var der aktivitet fra en aktør i Tyrkiet (SILICON) og en aktør i Vietnam (BISMUTH). I år ser vi nærmere på en gruppe baseret i Libanon, som allerede er blevet offentliggjort tidligere.[36]

Microsoft afdækkede en hidtil udokumenteret Libanon-baseret gruppe, som vi med rimelighed mener samarbejdede med aktører tilknyttet Irans ministerie for efterretning og sikkerhed (MOIS) Et sådant samarbejde eller ordrer fra Teheran stemmer overens med afsløringer fra slutningen af 2020 om, at Irans regering benytter tredjeparter til at udføre cyberaktiviteter, så de bedre kan afvise, at de er involveret.

I den observerede aktivitet målrettede POLONIUM mod eller kompromitterede to dusin israelske organisationer og én IGO med aktiviteter i Libanon mellem februar og maj 2022, før Microsoft afbrød og afslørede deres aktivitet. Næsten halvdelen af de israelske organisationer var en del af Israels forsvarsindustri eller havde tilknytninger til forsvarsvirksomheder, hvilket antyder, at gruppen havde flere fælles interesser med Iran, når det handler om at indsamle efterretninger om og/eller direkte foretage modforanstaltninger over for Israel.[37]

POLONIUM's vurderede tilknytninger til MOIS-grupper er baseret på observerede overlap mellem ofre og fællestræk ved værktøjer og teknikker.

- Overlap mellem ofre: En iransk gruppe knyttet til Irans MOIS, som er døbt MERCURY af Microsoft, har tidligere kompromitteret flere ofre for POLONIUM, hvilket antyder, at der er en konvergens i missionskravene eller en mulig "overførsel" af ofre mellem grupperne.
- Fællestræk ved værktøjer og teknikker: I lighed med POLONIUM observerede MSTIC, at DEV-0588 (også kendt som CopyKittens) ofte benytter AirVPN til aktiviteter, og at DEV-0133 (også kendt som Lyceum[38]) benytter OneDrive til C2 og eksfiltrering. På samme måde som iranske statsaktører benyttede POLONIUM en cloud-tjenesteudbyder til at kompromittere et israelsk luftfartsselskab og et advokatfirma.[39]

POLONIUM implementerede en række tilpassede implanter ved hjælp af cloud-tjenester til C2 og dataeksfiltrering – især OneDrive og DropBox. POLONIUM oprettede ofte unikke OneDrive-applikationer til mål, sandsynligvis for at undgå at blive opdaget.

I juni 2022 suspenderede Microsoft mere end 20 OneDrive-applikationer, som POLONIUM havde oprettet, underrettede de berørte organisationer og implementerede en række opdateringer til sikkerhedsoplysninger til at sætte POLONIUM-udviklede værktøjer i karantæne.

Microsoft registrerede og deaktiverede POLONIUM's misbrug af OneDrive som C2.

Handlingsrettet indsigt

1. Opdater antivirusværktøjer[40], og sørg for, at aktivere cloud-beskyttelse[41], så det registrerer de relaterede indikatorer.
2. For kunder med tjenesteudbyderrelationer skal du sørge for at gennemgå og overvåge alle partnerrelationer for at minimere unødvendige tilladelser mellem din organisation og upstream-udbydere.[42] Fjern straks adgang for partnerrelationer, der ikke forekommer bekendte eller ikke er blevet overvåget.

Links til yderligere oplysninger

- Eksponering af POLONIUM-aktivitet og -infrastruktur målrettet mod israelske organisationer | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY udnytter Log4j 2-sårbarheder i systemer uden programrettelser for at målrette mod israelske organisationer | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Nordkoreas cyberkapacitet benyttes for at nå regimets tre primære mål

Nordkoreas cyberprioriteter i det forløbne år afspejler regeringens erklærede globale prioriteter. Kim Jong-un understregede tre prioriteter: opbygning af forsvarskapacitet, styrkelse af landets skrantende økonomi og sikring af intern stabilitet på flere nøgleområder.[43] De handlinger, som de nordkoreanske statsaktører har udført, viser tydeligt, at der anvendes cyberfunktionalitet til at nå disse tre mål.

Nordkoreanske statsaktører brugte en række forskellige taktikker til at forsøge at trænge ind i rumfartsvirksomheder over hele verden.

Nordkoreanske trusselsgrupper, primært CERIUM og ZINC, benyttede en række taktikker til at forsøge at trænge ind i netværk tilhørende forsvars- og rumfartsvirksomheder over hele verden. Under den mest aggressive missiltestkampagne nogensinde, i første halvdel af 2022, brugte Nordkorea cyberspionage til at hjælpe sine forskere med at fremme udviklingen af interne forsvarssystemer og modforanstaltninger for at imødegå modstanderes fremskridt.

Vi observerede COPERNICIUM målrettede mod en række kryptovaluta-relaterede virksomheder rundt om i verden, ofte med succes, for at støtte Nordkoreas skrantende økonomi. Selvom vi ikke kan bekræfte, om gruppen var i stand til at eksfiltrere penge efter en kompromittering, observerede vi, at COPERNICIUM inficerede masser af maskiner ved at sende skadelige dokumenter forklædt som tilbud fra andre kryptovalutafirmaer.

Endelig arbejdede en gruppe, som Microsoft sporede som DEV-0215, på at opretholde stabilitet og loyalitet i Nordkorea ved at målrette mod nyhedsorganisationer, der rapporterer om nordkoreanske problematikker. Disse nyhedsmedier har kilder både i Nordkorea og i lokalsamfund med afhoppere, som Pyongyang betragter som en eksistentiel trussel. Derudover har gruppen arbejdet på at få adgang til netværk af koreansktalende kristne grupper, som har en tendens til at udtale sig uforbeholdent om Nordkorea og aktivt samarbejde med nordkoreanske afhoppere.

Målretning mod forsvars- og rumfartsvirksomheder

Nordkoreas statsaktører, der ledes af CERIUM og ZINC, har ydet en stor indsats for at udvikle målrettede taktikker, der har til formål at trænge ind i forsvars- og rumfartsvirksomheder. CERIUM har flere gange forsøgt at ind på sydkoreanske virtuelle private netværk (VPN'er) ved at downloade klienter og søge efter svagheder. Den downloadede også almindelige applikationer, der bruges af sydkoreanske militær- og myndighedsklienter, sandsynligvis for at lede efter sårbarheder. Gruppen fulgte de aktuelle hændelser nøje og skrev nye lokkedokumenter, som brugte højt profilerede emner, for at narre målene til at klikke på deres eksekverbare malware og links.

Både ZINC og CERIUM brugte sociale medier og social engineering i kampagner. ZINC var især eksperter i at oprette falske profiler på LinkedIn og andre professionelle websteder på sociale medier, hvor operatørerne foregav at være rekrutteringsmedarbejdere til store forsvars- og luftfartsvirksomheder. Ved hjælp af disse profiler sendte de links eller skadelige vedhæftede filer til potentielle ofre via direkte meddelelser på sociale medier eller mail.

Ud over medarbejderne i selskaber målrettede CERIUM også bredt mod medlemmer af det sydkoreanske militær og viste særlig interesse for både sydkoreanske militærakademier og medlemmer af militæret, der arbejder i den akademiske verden.

Målretning mod kryptovaluta for at afveje tab

Siden indførelsen af FN-sanktioner i 2016, er Nordkoreas økonomi fortsat med at blive forværret af naturkatastrofer som f.eks. oversvømmelser[44] og tørke[45] samt en næsten total importblokade siden starten af COVID-19-pandemien i starten af 2020.[46] Selv om Nordkorea kort åbnede sine grænser for handel med Kina i starten af 2022, blev de hurtigt lukket igen.[47] I midten af maj rapporterede Nordkorea sit første nationale tilfælde af COVID-19.[48] De har siden anvendt en "nul COVID"-strategi med massenedlukninger for at bekæmpe den virus, der har svækket Nordkoreas allerede skrøbelige økonomi.

Den nordkoreanske statsgruppe, COPERNICIUM, forsøgte at kompensere for nogle af de mistede indtægter ved at stjæle penge – typisk i form af kryptovaluta – fra enhver virksomhed, hvis netværk den kunne trænge ind i. Vi så mange kompromitterede maskiner tilhørende kryptovaluta-relaterede virksomheder i USA, Canada, Europa og i hele Asien. COPERNICIUM kompromitterede endda maskiner tilhørende kryptovaluta-relaterede virksomheder i Kina, Nordkoreas stærkeste allierede, både på fastlandet og i Hongkong. Gruppen gjorde udstrakt brug af sociale medier til indledende rekognosceringsaktiviteter og måden at henvende sig til målene på. Aktørerne opbygger profiler og udgiver sig for at være udviklere eller ledende medarbejdere i virksomheder med relation til kryptovaluta. De etablerede derefter relationer til andre i branchen og sendte skadelige links eller filer, når de havde opbygget kontakt.

Nordkoreas cyberkapacitet benyttes for at nå regimets tre primære mål

Fortsat

En gruppe, der er relateret til PLUTONIUM, udvikler og implementerer ransomware

En gruppe aktører med oprindelse fra Nordkorea, som Microsoft sporer under navnet DEV-0530 begyndte at udvikle og bruge ransomware i angreb i juni 2021. Denne gruppe, som kaldte sig selv H0lyGh0st, udnyttede en ransomware-nyttedata med samme navn til sine kampagner og kompromitterede med succes små virksomheder i flere lande allerede i september 2021.

Microsoft vurderede, at DEV-0530 havde forbindelser med en anden nordkoreansk gruppe, der blev sporet som PLUTONIUM (også kendt som DarkSeoul eller Andariel). Selvom brugen af H0lyGh0st-ransomware i kampagner er unik for DEV-0530, observerede MSTIC kommunikation mellem de to grupper, samt at DEV-0530 benyttede værktøjer, der udelukkende var oprettet af PLUTONIUM.

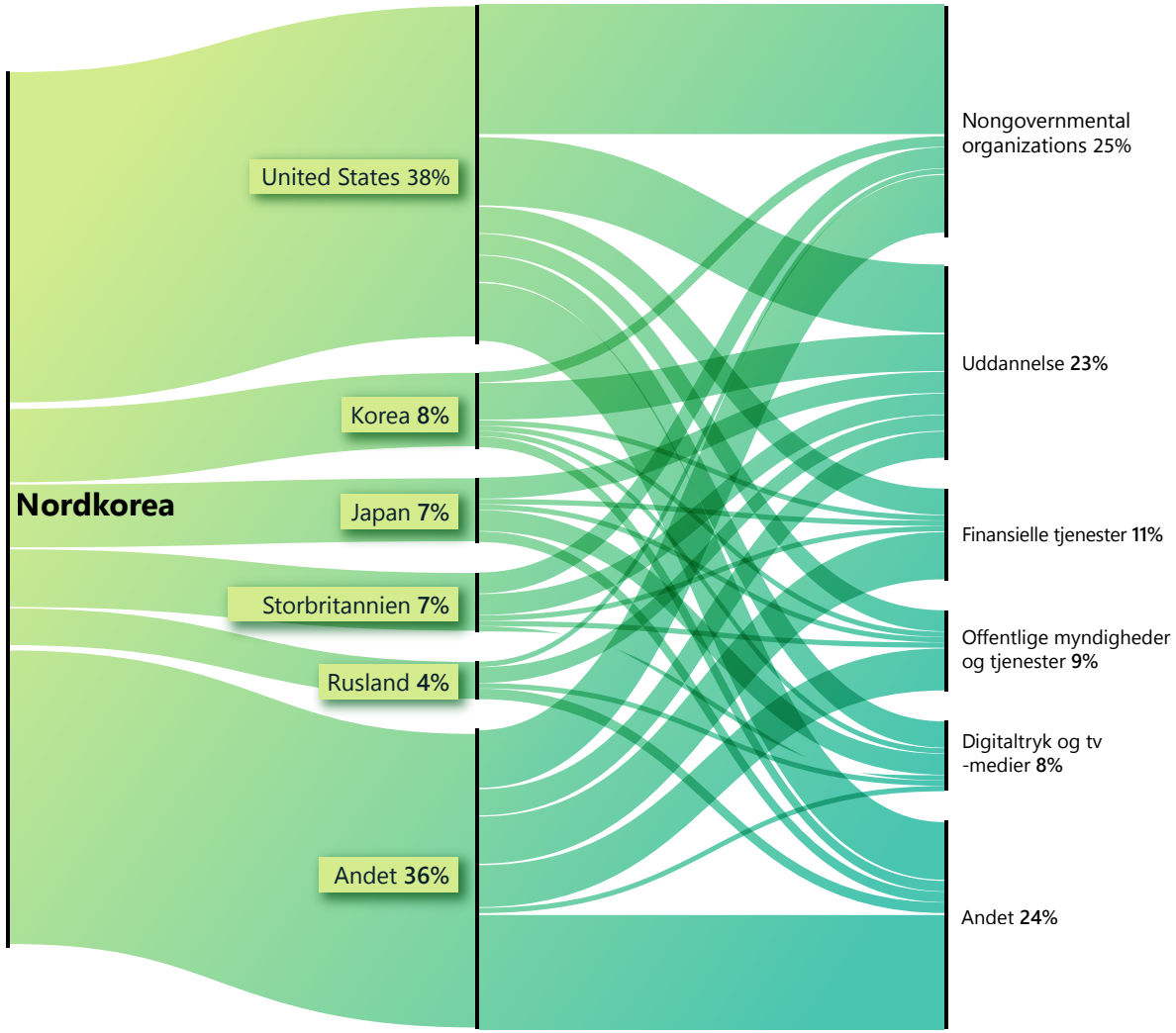
Det er ikke sikkert, at DEV-0530 -aktivitet var sponsoreret af myndighederne. Selv om ransomware-angreb kunne være blevet bestilt af myndighederne af samme grund som til, at de sponsorerede tyveri fra kryptovalutavirksomheder, er det også muligt, at aktørerne bag DEV-0530 handlede på egen hånd for selv at tjene penge. Hvis det var nordkoreanske hackere, der opererede selvstændigt, ville det forklare, hvorfor aktiviteten ikke var udbredt i forhold til offentligt sponsorerede tyveriaktiviteter mod kryptovalutavirksomheder.

Målretning mod nordkoreanske nyhedskanaler, afhoppere, religiøse grupper og hjælpeorganisationer

I det seneste år var den øverste leder, Kim Jong Un, offentligt mere fokuseret på intern sikkerhed og loyalitet end missiler og atomvåben. For at afspejle denne optagethed af indenlandske problemer fokuserede mindst to nordkoreanske statsgrupper på, hvad regimet ville se som indenlandske trusler.

Den første var en gruppe, som Microsoft sporer som DEV-0215, som målretter mod medieorganisationer, der nøje følger nordkoreanske nyheder. En sandsynlig årsag til denne målretning er, at disse mediekanaler får deres nyheder fra nordkoreanske afhoppere, kinesiske borgere, der arbejder tæt sammen med Nordkorea, og endda nogle nordkoreanske borgere med base i landet, som anvender en række metoder til at kommunikere med omverdenen. De nordkoreanske myndigheder betragter disse grupper som en eksistentiel trussel mod deres overlevelse, især borgere i Nordkorea bliver opfattet som forrædere og spioner. DEV-0215 forsøgte sandsynligvis at identificere disse mediekanalers kilder, så de kunne neutralisere potentielle informationslækager.

Nordkorea: De mest målrettede lande og branchesektorer



Nordkorea betragter USA, Sydkorea og Japan som sine primære fjender. Selvom Rusland er en langvarig allieret, målretter nordkoreanske trusselsaktører mod russiske tænketanke, akademikere og diplomater for at få oplysninger om Ruslands syn på globale anliggender.

Nordkoreas cyberkapacitet benyttes for at nå regimets tre primære mål

Fortsat

Microsoft så også bevis for, at DEV-0215 målretter mod koreansktalende, kristne samfund. Evangeliske, kristne koreanske kirker har en tendens til at være kritiske over for både Nordkorea og myndigheder i Sydkorea, der er tilhængere af engagement med Nordkorea. Disse kirker vil sandsynligvis opsøge afhoppere, og nogle engagerer sig i humanitært arbejde med Nordkorea. Nordkorea betragter dem som en trussel, selv om strømmen af afhoppere, der kommer fra Nordkorea, næsten er forsvundet under pandemien[49], spiller disse grupper ofte en afgørende rolle i at hjælpe afhoppere med at flygte. DEV-0215 har genereret falske dokumenter om kristne konferencer for koreansktalende som fælder for at målrette mod gruppen og opdage, hvem der hjælper med at organisere afhoppere.

Endelig viste statsgruppen OSMIUM en konstant interesse for internationale hjælpeorganisationer hele året, herunder organisationer, der tidligere har hjulpet Nordkorea. Selvom Nordkorea generelt har afvist tilbud om hjælp udefra, især siden COVID-19-udbruddet,[50] er det muligt, at Nordkorea overvejer at tage imod hjælp, men er på vagt over for de sikkerhedsmæssige følger ved at lade udenlandske hjælpearbejdere komme ind i landet. Nordkorea trænger muligvis ind i globale hjælpeorganisationers netværk for at afgøre, om de vil tillade en sådan hjælp i deres eget land.

Handlingsrettet indsigt

1. Nordkoreanske statsaktører er dygtige, nådesløse og kreative, men organisationer kan forsvare sig mod dem.
2. De fleste vellykkede angreb kan stoppes med grundlæggende cyberhygiejne, f.eks. godkendelse med to faktorer eller ved at undlade at åbne vedhæftede filer fra ukendte personer i et virtuelt miljø.

Links til yderligere oplysninger

- Nordkoreanske trusselsaktører målretter mod små og mellemstore virksomheder med H0lyGh0st-ransomware-| Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Blandt eksperter på Nordkorea har der længe været debat om, hvorvidt den nordkoreanske regering er ærlig, når de fremsætter sine offentlige erklæringer, eller om den bare lader som om. Tilpasningen af cyberangreb til Nordkoreas erklærede prioriteter underbygger troen på, at Nordkorea mener, hvad de siger, når de udtaler sig offentligt om deres mål.

Cyberlejesoldater truer stabiliteten af cyberspace

Det er et voksende privat antal virksomheder, der udvikler og sælger værktøjer, teknikker og tjenester, som sætter deres kunder – ofte myndigheder – i stand til at bryde ind i netværk, computere, telefoner og internetforbundne enheder. Disse virksomheder er et aktiv for nationalstatsaktører, men de sætter i mange tilfælde afhoppere, menneskerettighedsforkæmpere, journalister, civilsamfundsaktører og andre private borgeres liv i fare. Vi kalder disse for cyberlejesoldater eller offensive aktører i den private sektor.

En verden, hvor virksomheder i den private sektor skaber og sælger cybervåben, er mere farlig for forbrugere, virksomheder i alle størrelser og offentlige myndigheder. Disse stødende værktøjer kan bruges på måder, der er uforenelige med normerne og værdierne for god forvaltning og demokrati. Microsoft mener, at beskyttelse af menneskerettigheder er en grundlæggende forpligtelse, og vi tager dette alvorligt ved at begrænse "overvågning som en tjeneste" over hele verden.

Microsoft har vurderet visse statsaktører i demokratiske og autoritære regimer, der outsourcer udviklingen eller brugen af "overvågning som en tjeneste"-teknologi." Dette er måden, de undgår ansvarlighed og opsyn samt opnår kapaciteter, der ville være vanskelige at udvikle.

> Disse cybervåben giver nationalstater overvågningskapaciteter, som de ikke ville have været i stand til selv at udvikle.

Det marked, som cyberlejesoldater opererer på, er uigennemsigtigt. Ikke desto mindre fortsætter vi med at observere disse grupper, der udnytter zero-day-udnyttelser og endda zero-click-udnyttelser, der slet ikke kræver nogen interaktion fra ofrenes side, men som aktiverer overvågning som en tjeneste.

Microsoft annoncerede for nylig en offensiv aktør i den europæiske private sektor, som vi kalder KNOTWEED, som er en PSOA, der hedder DSIRF og er fra Østrig. Adskillige nyhedsrapporter har knyttet virksomheden til udvikling og forsøg på salg af et ondsindet kodesæt med navnet Subzero.[51] Ofrene omfatter advokatfirmaer, banker og strategiske konsulentvirksomheder i lande som Østrig, Storbritannien og Panama.[52]

Da disse offensive overvågningskapaciteter ikke længere er højt klassificerede kapaciteter, der er oprettet af forsvars- og efterretningstjenester, men snarere kommercielle produkter, der nu tilbydes til virksomheder og enkeltpersoner, skal enhver reguleringsramme for cybervåben gå ud over eksportkontrol. Effekten af disse cybervåben kan være ødelæggende.

Når en cyberlejesoldat udnytter en sårbarhed i et produkt eller en tjeneste, sætter de hele it-økosystemet i fare. Når sårbarheder er offentligt identificeret, er virksomheder i et kapløb om tid, før de skal have frigivet beskyttelser, før udbredte angreb følger (se vores tidligere beskrivelse om udnyttelse af sårbarheder). Dette er en farlig og vanskelig cyklus for både softwareleverandører (som hurtigt skal udvikle programrettelser) og forbrugerne af produkter (som skal implementere programrettelserne med det samme).

Som stiftende medlem af Cybersecurity Tech Accord[53] – en førende alliance med mere end 150 teknologivirksomheder – har Microsoft forpligtet sig til ikke at deltage i stødende aktiviteter online. Vi står ved denne forpligtelse og vores ansvar for menneskerettigheder på dette område. Vi har været involveret i tekniske afbrydelser og juridiske udfordringer for at fremhæve de negative konsekvenser af de tjenester, der leveres af cyberlejesoldater, og vi vil fortsætte med at beskytte vores kunder, når vi ser misbrug.

> Cyberlejesoldater opretter og leverer "overvågning som en tjeneste"-funktioner, der er teknologisk sofistikerede og bredt tilgængelige, herunder avanceret malware og en række teknikker.

Handlingsrettet indsigt for myndigheder

1. Implementer krav til gennemsigtighed og tilsyn for overvågning som en tjeneste, især i forbindelse med indkøb, herunder forbud mod disse offensive aktører, som USA har gjort med handelsministeriets liste over virksomheder på enhedslisten.
2. Indfør begrænsninger efter ansættelsen for tidligere medarbejdere i denne sektor.
3. Sigt mod at implementere "kend din kunde"-forpligtelser, og tilskynd virksomheder til at overholde deres forpligtelser vedrørende menneskerettigheder.

Links til yderligere oplysninger

- Udvikling af KNOTWEED: Offensiv aktør i den europæiske private sektor ved hjælp af 0-day-udnyttelse | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Fortsættelse af kampen mod cybervåben i den private sektor | Microsoft On the Issues

Operationalisering af cybersikkerhedsnormer for fred og sikkerhed i cyberspace

Vi har brug for øjeblikkelig indførelse af en ensartet, global ramme, der prioriterer menneskerettigheder og beskytter folk mod den uforsvarlige statsadfærd online. Dette behov demonstreres tydeligt under den igangværende krig i Ukraine. Ud over en global strategisk indsats kan myndighederne handle nu for at opnå en øjeblikkelig positiv indvirkning.

For fem år siden opfordrede Microsoft til oprettelse af en "digital Genève-konvention" til at fremme ansvarsområder og forpligtelser på tværs af sektorer for at forsvare fred og sikkerhed online. Cyberspace var ved at udvikle sig som et særskilt og ustabilt domæne bestående af konflikt og konkurrence mellem stater, hvor angrebene blev mere almindelige, selv i tider med fred.

I dag er der stadig et tydeligt behov for en sådan ramme – hvilket de russiske cyberangreb mod Ukraine som en del af den russiske invasion er bevis på. Denne kamp har skabt en ny frontlinje, som er noget anderledes end den, vi tidligere har kendt.

At bringe stabilitet til cyberspace vil kræve en styrke og nytænkning af globale styringsinstitutioner for at gøre dem egnede til formålet. Cyberspace er fundamentalt anderledes end andre domæner – det er grænseløst, syntetisk og vedligeholdes i vid udstrækning af den private sektor. Det betyder, at teknologibranchen skal tage et større ansvar for både sikkerheden for produkter og tjenester og det bredere digitale økosystem. Selvom der har været betydelige fremskridt på alle fronter, er udfordringerne vokset dramatisk.

Vi er nødt til at fordoble kollektive bestræbelser for at forsvare sikkerheden i cyberspace. Vi kan ikke tage de rettigheder og friheder, vi er kommet til at forvente online, for givet. Mens vi kæmper med disse udfordringer, planlægger kriminelle, hvordan og hvor de skal slå til ved hjælp af AI, udnyttelse af desinformation og at finde metoder til at underminere den spirende metaverse. Menneskerettighedsforkæmpere , teknologibranchen og regeringer, der respekterer rettigheder, skal arbejde sammen mod en bekræftende vision for en sikker onlineverden. Vejen frem er lang, men der er ting, som myndighederne kan gøre nu for straks at forbedre cybersikkerhedsøkosystemet:

- Citer normer, love og konsekvenser i tilskrivninger. En stor forbedring i løbet af de seneste fem år har været hastigheden og koordineringen af de offentlige tilskrivninger af cyberangreb. Ud over blot "naming and shaming" skal disse udsagn fremhæve, hvilke internationale love eller normer der overtrædes, og hvilken slags konsekvenser der vil blive pålagt for at styrke anerkendelse af internationale forventninger.
- Tydeliggør fortolkning af international lovgivning online. Selvom myndigheder er enige om, at international lovgivning gælder online, er der stadig spørgsmål om, hvordan den gælder i specifikke tilfælde. Dette er især relevant i kølvandet på invasionen i Ukraine. Myndigheder kan gøre meget for at skabe forventninger, undgå misforståelser og opbygge tillid ved at fremsætte, hvordan de ser på deres forpligtelser i henhold til international lov.
- Rådfør dig med andre interessenter. I takt med at internationale fora fortsætter med at identificere de bedste metoder til at muliggøre robust inklusion af flere interessenter, kan myndigheder støtte en informeret dialog ved at rådføre sig med fællesskaber med flere lag, især teknologibranchen, for at sikre at dialogen nyder godt af dem med nødvendig ekspertise.
- Opbyg et stående organ til at støtte ansvarlig tilstandsadfærd i cyberspace. Arbejdet i internationale diplomatiske fora for at fremme ansvarlig tilstandsadfærd online har aldrig været vigtigere. Der er et tydeligt behov for en permanent FN-mekanisme til at håndtere cyberspace som et konfliktområde.
- Definer nye normer for trusler under udvikling. Cyberspace-trusler udvikler sig hele tiden sammen med innovationer inden for teknologi. Selvom internationale normer bør være teknologineutrale, skal de opdateres og tilpasses på basis af ændringer i trusselslandskabet, og måden vi bruger teknologi på. Selv i dag ser vi mangler i den eksisterende internationale ramme, som misbruges. Stater bør forpligte sig til udtrykkeligt at beskytte kerneprocesser, der understøtter det digitale økosystem, som i øjeblikket ikke er beskyttet, f.eks. softwareopdateringsprocessen. Endvidere fortjener specifikke områder yderligere beskyttelse. Under pandemien har vi f.eks. erfaret, at normer for beskyttelse af sundhedspleje er vigtige.

Nationalstatsaktører og -angreb stiger i mængde og bliver stadig mere raffinerede, hvilket skaber en uholdbar situation.

Øjeblikkelig handling er bydende nødvendig – der er ting, som myndigheder kan gøre nu for straks at forbedre cybersikkerhedsøkosystemet, herunder implementering af vedtagne normer og regler for statsadfærd i cyberspace og samarbejde med det bredere fællesskab med flere interessenter for at håndtere nye mangler.

Multilaterale institutioner skal omdefineres for at imødegå den presserende udfordring med nationalstaters cyberangreb.

Links til yderligere oplysninger

- Et øjebliks vurdering: behovet for en stærk og global cybersikkerhedsrespons | Microsoft On the Issues
- Cyberangreb rettet mod sundhedspleje skal stoppe | Microsoft On the Issues
- Det næste kapitel af cyberdiplomati i FN kalder | Microsoft On the Issues

Slutnoter

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. Kritisk infrastruktur i dette kapitel defineres af Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (februar 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

Slutnoter fortsat

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. Ret især Exchange-servere for ProxyShell-sårbarheder (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 og CVE-2021-27065, CVE-2021-34473). Sørg også for at rette Fortinet FortiOS SSL VPN-apparater for sårbarheder.
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. Som nævnt i vores tekniske blog betyder identifikationen af mål i et land ikke nødvendigvis, at en DSIRF-kunde er bosat i samme land, da international målretning er almindelig.
53. Start | Cybersecurity Tech Accord (cybertechaccord.org)

Enheder og infrastruktur

På grund af hurtigheden af den digitale transformation er sikkerheden i digital infrastruktur vigtigere end nogensinde.

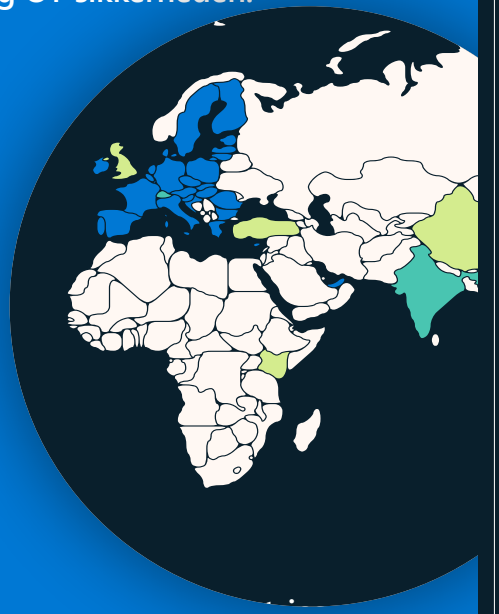
En oversigt over

enheder og infrastruktur

Pandemien og den hurtige introduktion af internetforbundne enheder af enhver art som en del af den accelererende digitalisering har i høj grad øget angrebsfladen i vores digitale verden.

Cyberkriminelle og nationalstater er hurtige til at udnytte mulighederne Selvom sikkerheden for it-hardware og -software er blevet styrket i de senere år, er sikkerheden for IoT- og OT-enheder ikke fulgt med. Trusselsaktører udnytter sådanne enheder til at få adgang til netværk og til horisontal bevægelse, til at få fodfæste i supply chain eller til at afbryde målorganisationens OT-drift.

Myndigheder over hele verden arbejder på at beskytte kritisk infrastruktur ved at forbedre IoT- og OT-sikkerheden.

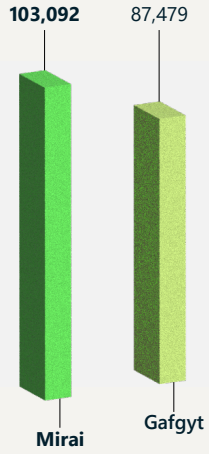


Få mere at vide på side 59

Globalt ensartede og kompatible sikkerhedspolitikker er nødvendige for at sikre en udbredt indførelse.

Få mere at vide på side 59

Malware som en tjeneste er blevet en storstilet operation mod udsat IoT og OT i infrastruktur og hjælpeprogrammer såvel som virksomhedsnetværk.



Få mere at vide på side 63

Angreb mod fjernstyringsenheder er voksende. Der blev observeret over 100 millioner angreb i maj 2022, en femdobling på et år.

Få mere at vide på side 62

Angribere udnytter i stigende grad sårbarheder i IoT-enhedens firmware til at infiltrere virksomhedens netværk og starte ødelæggende angreb.

Få mere at vide på side 65

32 % af den analyserede firmware indeholdt mindst ti kendte og kritiske sårbarheder.

Få mere at vide på side 66

Introduktion

Den accelererende digitalisering har øget cybersikkerhedsrisikoen for den vigtige infrastruktur og cyberfysiske systemer.

I de senere år har vi oplevet en hidtil uset ændring i den digitale verden. Organisationer udvikler sig for at udnytte fremskridt inden for computerbehandlingsegenskaber fra både den intelligente cloud-løsning og den intelligente grænseenhed. Som et resultat af pandemien, der tvinger enheder til at digitalisere for at overleve, og den hastighed, hvormed brancher over hele verden indfører internetrettede enheder, vokser angrebsfladen for den digitale verden eksponentielt.

Den hurtige migrering har oversteget sikkerhedsfællesskabet evne til at følge med. I løbet af de sidste år har vi fundet trusler, der udnytter enheder alle steder i organisationerne, fra traditionelt it-udstyr til controllere af driftsmæssig teknologi (OT - operational technology) - eller enkle IoT-sensorer (Internet of Things). Selvom sikkerheden for it-udstyr er blevet stærkere i de seneste år, har sikkerheden for IoT og OT-enheder ikke fulgt med. Trusselsaktører udnytter disse enheder til at få adgang til netværk og til tværgående bevægelse eller til at afbryde organisationens OT-drift. Vi har set angreb på elnet, ransomware-angreb, der forstyrrer OT-drift, IoT-routere, der benyttes til at øge vedvarenhed, og angreb rettet mod sårbarheder i firmware.

Udbredelsen af IoT- og OT-sårbarheder er en udfordring for alle organisationer, men kritisk infrastruktur er i øget risiko, fordi trusselsaktører har erfaret, at deaktivering af vigtige tjenester er et effektivt middel. Ransomware-angrebet på Colonial Pipeline Company i 2021 viste, hvordan kriminelle kan afbryde en vigtig tjeneste for at øge sandsynligheden for at modtage en løsesum. Og Ruslands cyberangreb på Ukraine viser, at nogle nationalstater betragter cyberangreb på vigtig infrastruktur som acceptabel, når det handler om at erobre militære mål.

Der er dog håb forude. Politikere og netværksforsvarere reagerer for at forbedre cybersikkerheden for vigtig infrastruktur, herunder de IoT- og OT-enheder, de er afhængige af. Politikere fremskynder udviklingen af love og regler for at opbygge offentlig tillid til cybersikkerheden af kritisk infrastruktur og enheder.

Microsoft samarbejder med myndigheder rundt omkring i verden for at benytte denne mulighed for at forbedre cybersikkerheden, og vi hilser yderligere engagement velkommen. Vi er dog bekymrede for, at inkonsekvente, specialtilpassede eller komplekse krav kan have utilsigtede virkninger, herunder at formindske sikkerheden i nogle tilfælde ved at omdirigere knappe sikkerhedsressourcer mod overholdelse af flere certificeringer, der overlapper hinanden.

Ud fra et sikkerhedsmæssigt synspunkt anvender alle, der forsvarer netværk, flere metoder til at forbedre deres organisations IoT/OT-sikkerhedsforhold. En af fremgangsmåderne er at implementere kontinuerlig overvågning af IoT- og OT-enheder. En anden metode er "skift til venstre", hvilket betyder at efterspørge og implementere bedre fremgangsmåder for cybersikkerhed for selve IoT- og OT-enhederne. En tredje metode er at implementere en løsning til sikkerhedsovervågning, der omfatter både IT- og OT-netværk. Denne holistiske tilgang har den betydelige ekstra fordel, at den bidrager til vigtige organisatoriske processer, f.eks. at "nedbryde siloerne" mellem OT og IT, hvilket igen gør det muligt for organisationen at opnå bedre sikkerhedsforhold og samtidig opfylde virksomhedens mål.

Michal Braverman-Blumenstyk
Corporate Vice President, teknologidirektør, cloud- og AI-sikkerhed

Myndigheder handler for at forbedre sikkerhed og modstandsdygtighed for vigtig infrastruktur

Myndigheder over hele verden udarbejder og udvikler politikker til at håndtere vigtige cybersikkerhedsrisici. Mange er også i gang med at vedtage politikker for at forbedre IoT- og OT-enhedssikkerheden. Den voksende globale bølge af politikinitiativer skaber store muligheder for at forbedre cybersikkerhed, men giver også udfordringer for interessenter på tværs af økosystemet.

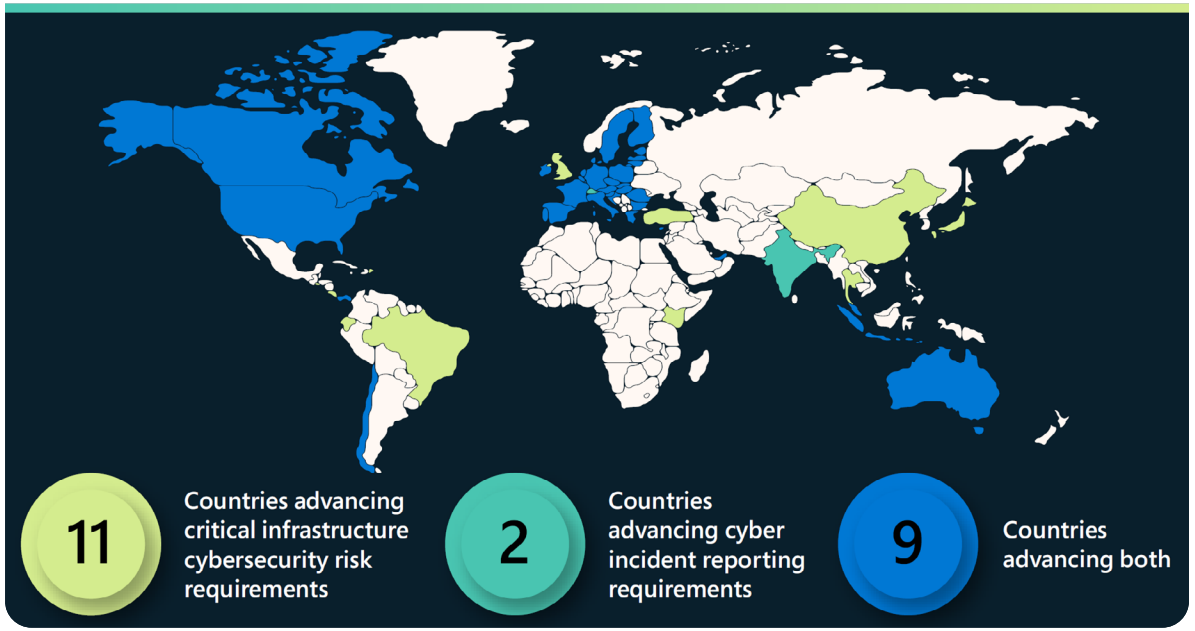
Det er vigtigt, men kompliceret at udarbejde en holistisk vision om håndtering af cyberrisici i den vigtige infrastruktur, især i betragtning af omfanget af forbindelserne mellem teknologier og globale leverandører, de forskellige måder at anvende teknologi på og de tilsvarende risici, og behovet for at investere i både kort- og langsigtede strategier. Effektive politikker, der fremmer iterativ læring og forbedring og understøtter global, tværsektorinteroperabilitet, kan lette håndteringen af kompleksitet og aktivere en mere sikkerhedsorienteret digital transformation. Men en fragmenteret tilgang til lovgivningen kan føre til overlappende og inkonsekvente lovkrav. Dette kan påvirke ressourcerne og i sidste ende underminere sikkerhedsmålene. Organisationer kan f.eks. omdirigere ressourcer fra innovation og sikkerhed til formalistiske overholdelsesøvelser.

Microsoft tilstræber at samarbejde med myndigheder overalt i verden for at få implementeret effektive cybersikkerhedsstrategier for vigtig infrastruktur, for bedre at forstå udfordringer og muligheder og for at støtte bestræbelser på at forbedre den kollektive holdning over for risici.

Politikudviklinger inden for risikomanagement af cybersikkerhed for vigtig infrastruktur

I løbet af det sidste år har mange jurisdiktioner, herunder Australien, Chile, EU (Den Europæiske Union), Japan, Singapore, Storbritannien og USA, udviklet, opdateret eller implementeret tværindustriel eller sektorspecifik cybersikkerhedskrav.[1] Mange af disse lande, f.eks. Indien[2] og Schweiz[3], har allerede udstedt eller er ved at udvikle krav til rapportering af cybersikkerhedshændelser for vigtig infrastruktur og væsentlige tjenesteudbydere.[4]

Der har fundet nogle bemærkelsesværdige politiske udviklinger sted i Australien, EU, Indonesien og USA i løbet af det seneste år. Australien har vedtaget to love, der skal hjælpe at håndtere vigtige cybersikkerhedsrisici på tværs af sektorer. Disse love udpeger blandt andet nye vigtige infrastruktursektorer, kræver udvikling af planer til risikostyring, giver mandat til rapportering af cybersikkerhedshændelser og giver myndighederne midlerne til at gribe ind, hvis en vigtig infrastrukturoperatør ikke ønsker eller ikke kan reagere tilstrækkeligt på en hændelse.



EU har arbejdet på at opdatere sit NIS-direktiv fra 2016, som udgør en ramme for EU-medlemslandene til at regulere teknologitjenester og -produkter, der betragtes som væsentlige for deres økonomi og samfundets funktion. NIS 2-forslaget omfatter revisioner, der ville skabe en ny kategori af kritisk digital infrastruktur, øge kravene til rapportering af cyberhændelser og pålægge yderligere krav til risikostyring af cybersikkerheden. EU har også udviklet et forslag til opdatering af sin DORA-lov (Digital Operational Resilience Act) om udarbejdelse af nye krav til teknologier for informationskommunikation, der anvendes i den finansielle sektor.

I maj udsendte den indonesiske regering en præsidentiel forordning om beskyttelse af vigtig informationsinfrastruktur ("IIV"), som træder i kraft i maj 2024 og dækker sektorer som energi, transport, finans og sundhed mm. Indonesiens mål med denne forordning er at beskytte kontinuiteten i implementeringen af IIV, forhindre cyberangreb og styrke beredskabet til håndtering af cyberhændelser. IIV-udbydere vil være ansvarlige for at implementere sikker og pålidelig beskyttelse, effektiv cyberrisikostyring og rapportering af cyberrisikoresultater til relevante offentlige myndigheder. Forordningen indeholder en forpligtelse til at rapportere cyberhændelser inden for 24 timer.

Myndigheder handler for at forbedre sikkerhed og modstandsdygtighed for vigtig infrastruktur

Fortsat

Den amerikanske kongres har vedtaget en lov, der giver CISA (Cybersecurity and Infrastructure Security Agency) bemyndigelse til at udstede regulativer, der kræver, at kritiske infrastrukturoperatører rapporterer cyberhændelser, og TSA (Transportation Security Administration) at etablere nye cybersikkerhedskrav, der er specifikke for transportsektoren. I 2021 udstedte TSA to sikkerhedsretningslinjer for operatører af farlige væsker og naturgasledninger som reaktion på ransomware-angrebet på Colonial Pipeline Company:

- Det første direktiv pålagde operatører at udpege en cybersikkerhedskoordinator, rapportere cyberhændelser inden for 12 timer og udføre en sårbarhedsvurdering af deres systemer.
- Det andet direktiv, som TSA reviderede i 2022, krævede, at de skulle implementere specifikke begrænsninger for at beskytte sig mod ransomware-angreb og andre kendte trusler mod it- og OT-systemer, udvikle og implementere en cybersikkerhedsberedskabs- og -handlingsplan inden for 30 dage samt foretage en årlig designgennemgang af cybersikkerhedsarkitekturen.

Med udgangspunkt i sine bestemmelser om rørledninger udgav TSA to yderligere sikkerhedsdirektiver senere i 2021, som offentliggjorde cybersikkerhedskrav til godstransport, passagerbefordring og jernbanetransitsystemer. Direktiverne krævede, at berørte operatører udpeger en cybersikkerhedskoordinator, rapporterer cybersikkerhedshændelser inden for 24 timer, udarbejder og implementerer en handlingsplan for cybersikkerhedshændelser og foretager en sårbarhedsvurdering af cybersikkerheden. TSA meddelte samtidig, at de også havde opdateret deres programmer for luftfartssikkerhed til at kræve, at lufthavne og luftfartsselskaber implementerer de to første bestemmelser, nemlig at de udpeger en koordinator og rapporterer hændelser inden for 24 timer.

Politikudviklinger inden for IoT- og OT-enhedssikkerhed

I masser af lande har myndigheder travlt med at udvikle krav til fremme af cybersikkerheden for ICT-produkter og -tjenester (information and communications technology), herunder IoT og OT-enheder. I forbindelse med ICT-produkter og -tjenester er de største bekymringer sikkerhed i software-supply chain og IoT-sikkerhed.

- Europa-Kommissionen foreslog Cyber Resilience Act, som ville etablere cybersikkerhedskrav for enkeltstående software og tilsluttede enheder og hjælpetjenester.[5] Relevant praksis for softwareleverandører er at udnytte en sikker softwareudviklingslivscyklus[6] og levere en softwarematerialeliste.[7] Nye sikkerhedskrav ville gælde for tilsluttede enheder, og alle producenter ville få til opgave at styre koordinerede processer for at afsløre sårbarheder[8] for frigivne produkter.

Politikere har også fokuseret på den fortsatte udbredelse af IoT-enheder og netværksbaserede OT-enheder.

- I Storbritannien vil den foreslåede lov om produktsikkerhed og telekommunikationsinfrastruktur kræve, at producenter af produkter, som forbrugerne kan tilslutte, f.eks. smart-tv'er, stopper med at bruge standardadgangskoder, som er lette mål for cyberkriminelle, etablerer en politik for afsløring af sårbarheder (f.eks. via en måde til at modtage meddelelser om sikkerhedsfejl) og for på en gennemsigtig måde at kommunikere den minimumsperiode, som de vil levere sikkerhedsopdateringer i.[9]
- I EU indføres nye sikkerhedsstandarder eller sikkerhedskrav gennem flere lovgivningsmæssige instrumenter, herunder en delegeret lov til radioudstyrsdirektivet, der gælder for trådløse enheder og har til formål at forbedre netværkets robusthed, beskytte forbrugernes privatliv og reducere risikoen for økonomisk svindel.[10] Derudover kan det kræve brug af et cloud-certificeringssystem,[11] som i øjeblikket udarbejdes på grund af EU-forordningen for cybersikkerhed fra 2019[12].

Behovet for konsekvens

I mange tilfælde udføres aktiviteter i alle regioner, sektorer, teknologier og operationelle risikostyringsområder samtidigt, hvilket fører til potentiel overlapning eller uoverensstemmelser i omfang, krav og kompleksitet for organisationer, der søger at anvende rådgivning eller demonstrere overholdelse. Uden en universelt accepteret definition af IoT er omfanget særligt udfordrende for IoT- og OT-enhedsregler. Eksemplerne ovenfor gælder muligvis for "tilsluttede produkter og hjælpetjenester", "produkter, som forbrugerne kan tilslutte" og "trådløse enheder". Samtidig tilstræber mange lande at indføre mere robuste vurderingssystemer for at få en bedre forståelse af, om og hvordan organisationer og produkter opfylder øjeblikkelige, fremtidige og skiftende krav. Efterhånden som disse tendenser flettes sammen, øges kompleksiteten. Det var opmuntrende, at de spørgsmål, der blev rejst under høringen af EU-loven om cyberrobusthed, undersøgte, hvordan nye regler potentielt kunne interagere med eksisterende cybersikkerhedsregler, hvilket tyder på, at hensigten er at undgå modstridende cybersikkerhedskrav.

Iterative risikobaserede og resultat- eller procesorienterede tilgange (kontra implementeringsspecifik) kunne styrke cybersikkerheden og fremme løbende forbedringer. På samme måde kan fokus på at aktivere interoperabilitet på tværs af sektorer, regioner og politikområder fremme cybersikkerheden på tværs af indbyrdes forbundne globale supply chains.

Myndigheder handler for at forbedre sikkerhed og modstandsdygtighed for vigtig infrastruktur

Fortsat

Der udarbejdes stadig mere komplekse cybersikkerhedsstrategier for vigtig infrastruktur på tværs af flere regioner, sektorer og områder. Denne aktivitet byder på store perspektiver, men rummer også betydelige udfordringer. Myndighedernes beslutninger vil være afgørende for fremtiden for digital transformation og økosystemsikkerhed.

Fremskyndelse af økosystemomfattende investeringer i softwaresikkerhed i supply chain og nul-tillid-arkitektur

Den amerikanske bekendtgørelse 14028 om forbedring af cybersikkerhed har fungeret som en katalysator til at fremme Microsofts igangværende initiativer til at investere i vores egen og økosystemdækkende supply chain-sikkerhed og til at give vores kunder mulighed for at nå nul tillid-mål.

I lang tid har vi ment, at forbedring af softwarens supply chain kræver deling af viden og bedste praksis, som det første gang blev demonstreret for ca. 15 år siden med vores offentliggørelse af Microsoft's Security Development Lifecycle.

Derudover arbejder vi tæt sammen med National Cybersecurity Center of Excellence for at demonstrere anvendelse af nul tillid-arkitekturtilgang på både on-premises- og cloud-teknologier og for at etablere nye produktfunktioner, herunder muligheden for at håndhæve phishingresistent godkendelse for hybrid- og multicloud-miljøer.

I dag går vi endnu længere end kravene i EO-bekendtgørelsen for at demonstrere overholdelse af sikkerhedskravene i supply chain for software og levere SBOM-oplysninger (Software Bill of Materials) på to måder

1. For det første deler vi en open source-version af vores SBOM-generatorværktøj, som vi har designet til nemt at blive integreret i CI/CD-pipelines, der understøtter builds på Windows, Linux, Mac, iOS og Android-platforme.[13]
2. For det andet bidrager vi til udviklingen af branchestandarder for supply chain-integritet, gennemsigtighed og tillid (SCITT). Dette gør det muligt automatisk at udveksle verificerbare oplysninger om supply chain, herunder artefakter, der viser overholdelse af krav, som dem der er et resultat af bekendtgørelsens vejledning om software-supply chain.

Handlingsrettet indsigt

1. Multilaterale institutioner skal omdefineres for at imødegå den presserende udfordring med nationalstaters cyberangreb.
2. Udvikle konsekvente og interoperable politikker for cybersikkerhed på tværs af områder, industrier og fagområder.

Links til yderligere oplysninger

- Fortsatte investeringer i supply chain-sikkerhed til støtte for cybersikkerhedsbekendtgørelse | Microsoft Tech Community
- Den amerikanske regering definerer strategi og krav til Nul tillid-arkitektur | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Integritet, gennemsigtighed og tillid i supply chain | github.com
- Implementering af en Nul tillid-arkitektur | NCCoE (nist.gov)

IoT og OT-eksponering: Tendenser og angreb

I en stadigt mere forbundet digital verden kommer enheder hurtigt online, kommunikerer med større systemer, indsamler data og skaber synlighed, hvor det før var sløret. Dette er en kilde til muligheder for både organisationer og cyberkriminelle, og cyberkriminalitet bliver både en industri og en risiko på flere milliarder dollar.

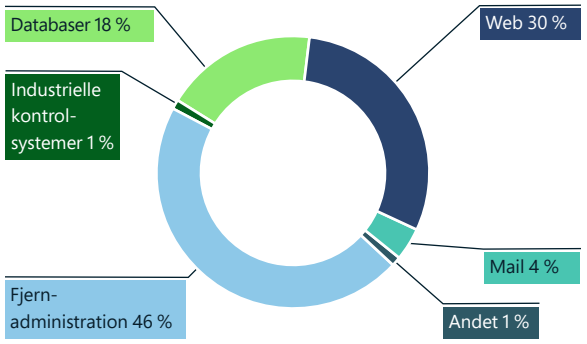
IoT-enheder – herunder alt fra printere til webkameraer, klimakontrolenheder og adgangskontrolenheder til bygninger – udgør unikke sikkerhedsrisici for enkeltpersoner, organisationer og netværk. Selvom de er afgørende for driften af mange organisationer, kan de hurtigt blive en belastning og en sikkerhedsrisiko. Den hurtige indførelse af IoT-løsninger i næsten alle brancher har øget antallet af angrebsvektorer og risikoen for eksponering for organisationer.

Malware som en tjeneste har været genstand for storstilede operationer mod civil infrastruktur og forsyningsselskaber (hospital, brændstof og gas, elnet, transport og anden kritisk infrastruktur) og mod virksomhedsnetværk. Cyberkriminelle skal udføre en betydelig forskningsindsats for at afdække og udnytte konfigurationen af driftsmiljøer og integrerede IoT- og OT-enheder.

IoT-enheder udgør unikke sikkerhedsrisici som indgangs- og omdrejningspunkter i netværket. Millioner af IoT-enheder er uden programrettelser eller er eksponerede.

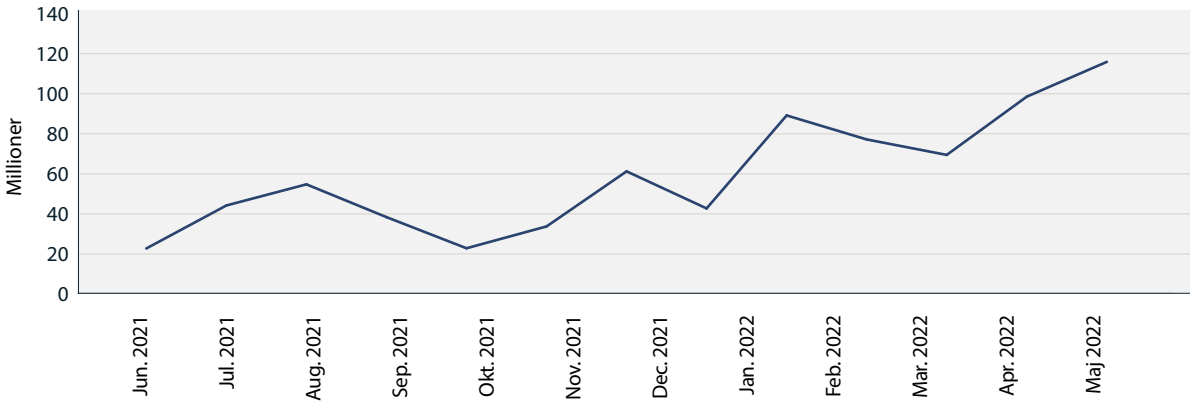
Udsatte enheder kan registreres gennem internetsøgeværktøjer ved at identificere tjenester, der overvåger åbne netværksporte. Disse porte bruges normalt til fjernadministration af enheder. Hvis en IoT-enhed ikke er korrekt sikret, kan den bruges som et omdrejningspunkt på et andet lag af virksomhedens netværk, da uautoriserede brugere kan få fjernadgang til porte. Vi har observeret en række cyberkriminelle, der forsøger at udnytte sårbarheder i enheder, der er eksponeret for internettet, lige fra kameraer til routere til termostater. Men på trods af risikoen er millioner af enheder uden programrettelser eller er eksponerede.

Oversigt over angrebstyper på IoT/OT



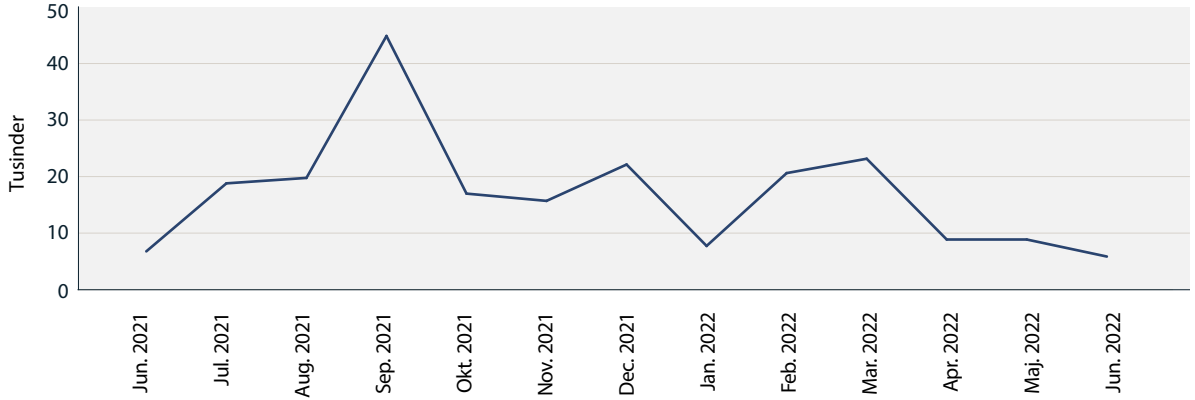
Typer af angreb observeret gennem MSTIC-sensornetværk. De mest udbredte angreb var angreb mod fjernstyringsenheder, webangreb og databaser (brute-force-teknikker eller udnyttelser).

Angreb mod fjernstyringsenheder



Stigning i angreb på fjernstyringsporte over tid, som set via MSTIC-sensornetværket.

Webangreb mod IoT og OT



Mængde af angreb på nettet over tid, som observeret af MSTIC-sensornetværket. Da antallet af enheder, der er direkte forbundet til nettet, fortsætter med at falde, kan angribere efterhånden være mindre tilbøjelige til at udnytte dem.

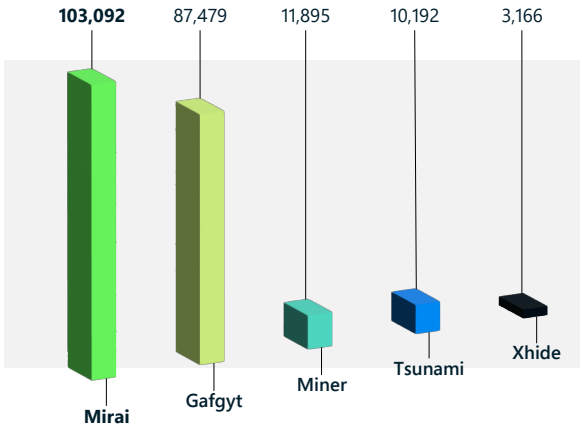
IoT og OT-eksponering: Tendenser og angreb

Fortsat

Moderniseret malwarefunktion

Efterhånden som cyberkriminelle grupper har udviklet sig, har deres implementering af malware og valg af mål også udviklet sig. I løbet af det seneste år har vi observeret, at angreb mod almindelige IoT-protokoller, som Telnet, er faldet markant, i nogle tilfælde med helt op til 60 %. Samtidig anvender cyberkriminelle grupper og nationalstatsaktører igen botnets Vedholdenheden af malware, som Mirai, fremhæver modulariteten af disse angreb og eksisterende truslers tilpasningsevne.

Top IoT-malware fundet i fri cirkulation



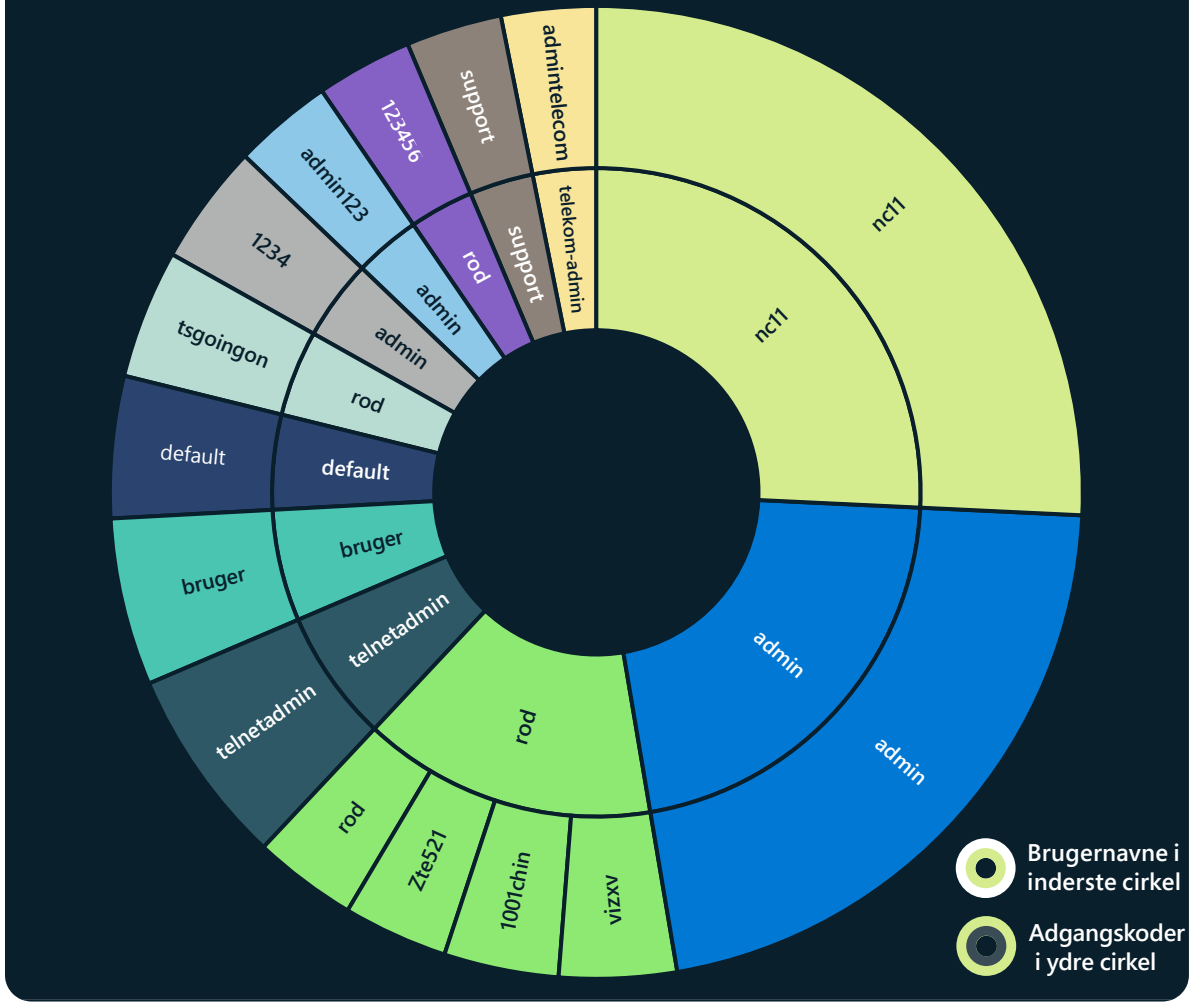
Mirai har udviklet sig til at inficere en lang række af IoT-enheder, herunder internetprotokolkameraer, digitale videooptagere til sikkerhedskameraer og routere. Angrebsvektoren omgår ældre sikkerhedskontroller og udgør en risiko for endpoints i netværket ved at udnytte yderligere sårbarheder og bevæge sig på tværs. Mirai er blevet redesignet flere gange. Der er varianter, der tilpasser sig forskellige arkitekturer og udnytter både kendte sårbarheder og zero-day-sårbarheder for at kunne kompromittere nye angrebsvektorer.

I løbet af det sidste år er anvendelsen af Miray vokset på både 32- og 64-bit x86 CPU-arkitekturer, og malwaren har fået nye funktioner, der hurtigt er blevet indført af nationalstater og kriminelle grupper. Nationalstatsangreb anvender nu nye varianter af eksisterende botnets i DDoS-angreb mod udenlandske fjender.

Da omsætningen fra angreb mod IoT-enheder faldt i 2022, observerede vi, at flere trusselsaktører udnyttede sårbarheder – såsom Log4j og Spring4Shell – til at levere en nyttelast mod enheder som servere, inficere dem og rekruttere dem til store botnets, der udfører DDoS-angreb. Den omarbejdede malware, der er designet til målretning mod sårbare IoT-enheder, har implikationer for både organisationer og lande, da tværgående bevægelser kan eksponere bagdøre for yderligere nyttelast og andre enheder på netværket.

Mange industrielle kontrolsystemprotokoller er uovervågede og derfor sårbare over for OT-specifikke angreb. Dette kan betyde øget risiko for kritisk infrastruktur.

Relativ udbredelse af brugernavn og adgangskodepar set blandt IoT/OT-enheder over 45 dages sensorsignaler



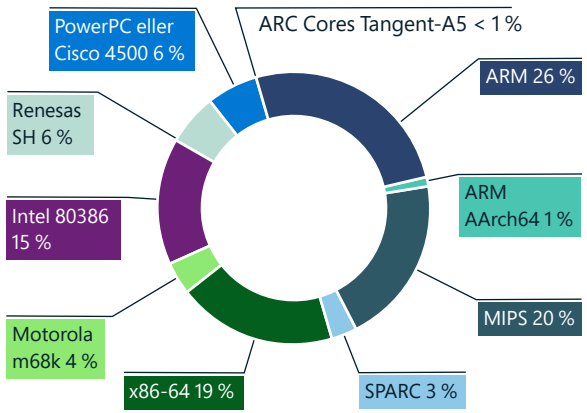
Brug af almindelige brugernavne og adgangskodepar øger risikoen for kompromitteringer. Baseret på en stikprøve på over 39 millioner IoT- og OT-enheder brugte cirka 20 % identiske brugernavne og adgangskoder.

IoT og OT-eksponering: Tendenser og angreb

Fortsat

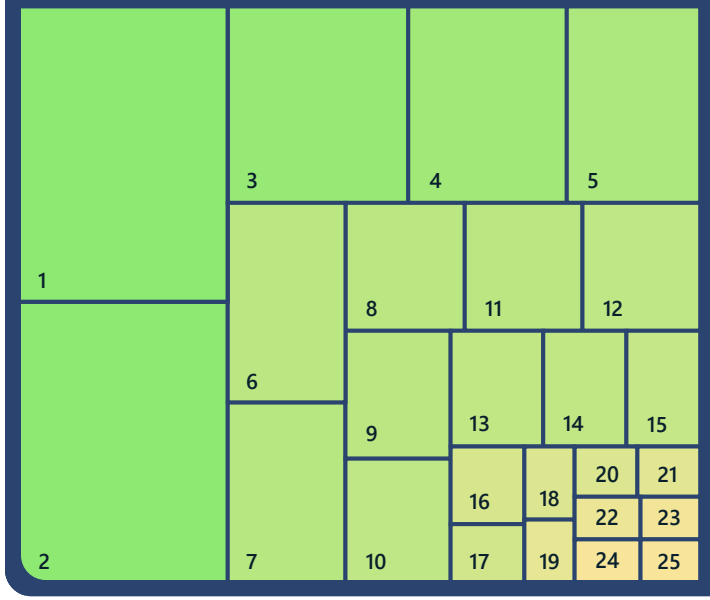
Mens svage konfigurationer og standardlegitimationsoplysninger altid er en risiko for netværk, har Microsoft observeret adskillige webbaserede udnyttelser, der anvender HTTP-protokollen. Vi har observeret denne stigning i angreb mod webbaserede tjenester, der anvender ældre botnets. Samtidig er antallet af åbne telnet-porte på internettet faldet, hvilket er et positivt tegn for netværkssikkerheden, da botnet-netværk, der tidligere udgjorde en risiko for enheder, mister deres relevans. På trods af dette fald i antallet af åbne telnet-porte observerede vi stadig vedvarende botnets i sensornetværkene.

Distribution af IoT-malware efter CPU-arkitektur



Microsoft observerede, at IoT-enheder, der kører på ARM, er mest målrettet af malware, efterfulgt af MIPS-, X86-64- og Intel 80386-processorer.

Udbredelse af industrielle kontrolsystemprotokoller



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

Sårbarheder i industrielle kontrolsystemprotokoller

Vi kiggede på OT-data fra vores cloud-forbundne sensorer og afslørede de mest almindelige ICS-protokoller (Industrial Control System). Med disse protokoller får du indsigt i arten af disse enheder og deres angrebsflade. Dette gælder især for sikkerheden i kritisk infrastruktur. Nogle vigtige erfaringer er:

1. De fleste af de repræsenterede protokoller er mærkevarebeskyttede, så standardværktøjer til it-overvågning giver ikke tilstrækkeligt overblik over sikkerheden for alle disse enheder og protokoller. Som et resultat er netværk uovervågede og dermed mere sårbare over for OT-specifikke angreb.
2. Der er en lang række leverandørspecifikke protokoller. Det betyder, at leverandørspecifikke sikkerhedsløsninger ikke vil være i stand til at dække hele netværket tilstrækkeligt. Microsoft har en leverandøragnostisk tilgang til at levere sikkerhedsdækning til en lang række forskellige enheder.
3. Organisationer bør sikre, at disse protokoller ikke eksponeres direkte for internettet fra deres netværk. Denne eksponering kan udgøre en stor sikkerhedsrisiko på grund af disse protokollers sårbarheder og usikre karakter.

Malware som Mirai fortsætter med at overleve gennem udvikling af nye funktioner og indføres af cyberkriminelle og nationalstatsgrupper, som udnytter nye varianter af eksisterende botnets i DDoS-angreb mod udenlandske fjender.

Handlingsrettet indsigt

1. Sørg for, at enheder er robuste ved at anvende programrettelser og ændre adgangskoder og SSH-standardporte.
2. Reducer angrebsfladen ved at udelukke unødvendige internetforbindelser og åbne porte, begrænse fjernadgang gennem portblokering, nægte fjernadgang og bruge VPN-tjenester.
3. Brug en IoT/OT-aktiveret NDR-løsning (network detection and response) og en SIEM- (security information and event management)/SOAR-løsning (Security Information and Event Management) til at overvåge unormal eller uautoriseret adfærd på enheder, f.eks. kommunikation med ukendte værter.
4. Segmentér netværk for at begrænse angriberes mulighed for at bevæge sig på tværs og kompromittere aktiver efter den første indtrængen. IoT-enheder og OT-netværk bør isoleres fra virksomhedens it-netværk gennem firewalls.
5. Sørg for, at ICS-protokoller ikke eksponeres for internettet.

Hacking af supply chain og firmware

Næsten alle internetforbundne enheder har firmware, som er software, der er integreret i enhedens hardware eller printkort. I løbet af de sidste få år har vi set en stigning i målretningen mod firmware for at starte ødelæggende angreb. Da firmware sandsynligvis vil fortsætte med at være værdifuldt mål for trusselsaktører, er organisationer nødt til at beskytte sig mod firmwareangreb.

Firmware er ansvarlig for en enheds primære funktioner, som at oprette forbindelse til et netværk eller lagre data. Firmware findes i routere, kameraer, fjernsyn og andre enheder, der bruges erhvervsmæssigt (IoT), sammen med industrielt kontroludstyr (OT), der bruges i kritisk infrastruktur. Historisk set er firmware skrevet med usikker kode, hvilket resulterede i betydelige sårbarheder, der kan udnyttes til at tage kontrol over enheden eller indsætte skadelig kode i firmwaren.

Denne risiko forværres, når det kommer til supply chain. De fleste enheder er bygget ved brug af software- og hardwarekomponenter fra mange producenter samt fra open source-biblioteker. I mange tilfælde har brugerne af enhederne ikke overblik over hardware- og softwarestyklister (H/SBOM), så de kan vurdere supply chain-risikoen for enheder i deres netværk. I juni 2020 blev der afsløret sårbarheder i en netværksstak, der blev brugt af mange forskellige producenter, hvilket påvirker hundrede millioner af IoT-enheder på forbruger- og industriudstyrsområdet.[14] I nogle tilfælde var netværksstakken blevet omdøbt af andre leverandører, og der var ingen indikation af, at enheden var sårbar. Vi ser en stigende trussel fra ondsindede aktører, der målretter supply chain for software- og hardware til IoT/OT-enheder for at kompromittere organisationer.

Firmwareopdateringsprocessen kan være meget forskellig på tværs af enheder, og kompleksiteten og den logistiske udfordring ved at udføre den påvirker opdateringshyppigheden. Det er ikke altid muligt at afgøre, om en enhed kører den nyeste firmware, hvilket gør det vanskeligt for sikkerhedsmedarbejdere at overvåge og garantere sikkerhedsniveauet for deres IoT- og OT-enheder. Derudover har nogle enheder firmware, der ikke er kryptografisk signeret, hvilket gør det muligt at opdatere dem uden brugerbekræftelse. Disse svagheder udsætter enhederne yderligere for supply chain-angreb gennem hele produktions- og distributionskæden.

For at imødegå disse trusler investerer Microsoft kraftigt i at garantere sikkerhed og integritet i firmwaren, når den gennemgår de forskellige faser af supply chain og ved at dokumentere, at der ikke er manipuleret med den under implementering eller senere. Dette vil give os mulighed for at validere tilliden i hvert segment af pipelinen og levere en certificeret og verificerbar komplet kæde af ansvar for hver komponent, vi leverer til kunderne. Vi samarbejder med vores partnere om at levere chip-til-cloud-sikkerhed på alle enheder på virksomhedens netværk og OT-netværket.

"Der målrettes i stigende grad mod ICT-infrastrukturudbydere, fordi de giver mulighed for udbredt replikering af et enkelt angreb. Samtidig er globale love og bestemmelser såvel som kundekrav til supply chain-sikkerhed og robusthed stigende, og kravene er ofte forskellige.

Løsningen er partnerskab. I samarbejde med leverandører og offentlige myndigheder i hele verden er Microsoft forpligtet til at håndtere sikkerhed på tværs af sit supply chain-økosystem på en måde, der overstiger krav fra kunder og lovgivende myndigheder. Det gør vi ved at anlægge en omfattende tilgang til sikkerhed og driftsmæssig robusthed, som implementeres fleksibelt i hele supply chain.

At styre firmwareintegritet fra design til enhedsdrift er nøglen til vores kollektive tilgang. At sikre leverandørernes SDL-processer og implementere innovation af hardwareindbygget tillid er eksempler på, hvordan vi kan "indbygge" integritet i supply chain.

Vores fællesskab er afhængig af kollektiv forskning og udvikling, der dækker nye anti-manipulationsteknikker og nye kryptografiske mekanismer, kombineret med kontinuerlig overvågning og registrering af uregelmæssigheder. Sammen gør vi fremskridt for at gøre supply chain mindre tiltrækkende som en angrebsflade".

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

Fokus på firmwaresårbarheder

Angribere udnytter i stigende grad sårbarheder i IoT-enheders firmware til at infiltrere virksomhedsnetværk. I modsætning til traditionelle it-endpoints, der anvender XDR-agenter til at identificere svagheder, er det meget vanskeligere at identificere sårbarheder på IoT/OT-enheder.

En nylig undersøgelse foretaget af Microsoft og Ponemon Institute fremhæver både mulighederne og sikkerhedsudfordringerne ved IoT/OT-enheder i en virksomhed.[15] Hvis 68 % af respondenterne mener, at IoT/OT-indførsel er afgørende for deres strategiske digitale transformation, anerkender 60 %, at IoT/OT-sikkerhed er et af de mindst sikre aspekter af IT/OT-infrastrukturen.

Et eksempel på angribere, der bruger sårbarheder i IoT-enhedsfirmware til at infiltrere netværk, er Trickbot-trojaneren, der udnyttede standardadgangskoder og sårbarheder i Mikrotik-routere[16] til at omgå virksomhedens forsvarssystemer. Den grundlæggende udfordring for IoT-enhedsfirmware er det manglende overblik over enheders sikkerhedsforhold og sårbarheder.

Selvom der er løsninger til at opbygge sikre enheder, er der allerede milliarder af enheder på markedet og implementeret i virksomheder. Enhederne kaldes brownfield-enheder. I 2021 hyrede Microsoft ReFirm Labs til at belyse sikkerheden i brownfield-enheder og gøre det muligt for enhedsproducenter at forbedre sikkerheden af deres produkter. ReFirm Labs analyserer en enheds binære firmwareafbildning og opretter en detaljeret rapport over potentielle sikkerhedssvagheder.[17] Denne teknologi indarbejdes i en fremtidig udgave af Microsoft Defender til IoT.

I det sidste år har vi gennemgået de samlede resultater af den unikke firmware, der er scannet af vores kunder. Selvom ikke alle de opdagede svagheder kan udnyttes, understreger de den grundlæggende udfordring ved sikkerheden af enhedsfirmware.

Bemærk, at de typer af svagheder, der findes i IoT/OT-enheder, aldrig ville være acceptable på traditionelle Windows- eller Linux-endpoints.

- Svage adgangskoder: 27 % af de scannede firmwareafbildninger indeholdt konti med adgangskoder, der er kodet ved hjælp af svage algoritmer (MD5/DES), som angribere nemt kan afkode.

Analyserede sikkerhedssvagheder i firmwareafbildninger

- Kendte sårbarheder: Ligesom andre systemer udnytter IoT/OT-enhedsfirmware i omfattende udstrækning open source-biblioteker. Enheder leveres dog ofte med forældede versioner af disse komponenter. Ifølge vores analyse indeholdt 32 % af afbildningerne mindst 10 kendte sårbarheder (CVE'er) klassificeret som kritiske (9,0 eller højere). Fire % indeholdt mindst 10 vigtige sårbarheder, der var mere end seks år gamle.
- Udløbne certifikater: Certifikater bruges til at godkende logins og identiteter og til at beskytte følsomme data, men 13 % af de scannede afbildninger havde 10 eller flere certifikater, der havde været udløbet i mere end 3 år.
- Softwarekomponenter: 36 % af billederne indeholder softwarekomponenter, som Microsoft anbefaler at ekskludere fra IoT-enheder, som pakkeindlæsningsværktøjer (tcpdump, libpcap), som kan udnyttes til netværksrekognoscering som en del af en angrebskæde.

Firmwareangreb

Viasat: Brug af en firmwaresårbarhed til at målrette satellitkommunikation

I februar 2022 afbrød en hændelse på et satellitnetværk et strategisk kommunikationsnetværk. Virkningerne kunne mærkes i hele Europa Viasats KA-SAT-system blev overvældet af en stor mængde trafik, der afbrød forbindelsen til mange modemer, og der blev iværksat et denial of service-angreb mod netværket. Da det faste bredbånd blev afbrudt, blev tusindvis af vindmøller utilgængelige for fjernoperatører, og ondsindet malware blev implementeret på berørte modemmer. Afbrydelsen ramte mere end 30.000 satellitterminaler, der blev brugt af virksomheder og organisationer til kommunikation.

Cyclops Blink: Brug af et firmwareangreb på supply chain til at målrette mod firewall-gateways

For trusselsaktører er udvikling og udvidelse af kommando og kontrol (C2) og angrebsinfrastruktur et vigtigt element for succes. Efterhånden som behovet for en stabil C2-infrastruktur er vokset, er routere blevet en efterspurgt angrebsvektor på grund af mangel på programrettelser og manglen på omfattende sikkerhedsløsninger.

Microsoft samarbejder med myndigheder og industrien om at udvikle firmwarescanningsteknologi, der kan give større indblik i enhedssikkerhed og garantere fuld livscyklussikkerhed for enhedsproducenter og -operatører.

Siden juni 2019 har en nationalstatsassocieret APT-gruppe (Advanced Persistent Threat) brugt modulær Cyclops Blink-malware til at målrette mod sårbare WatchGuard-firewallenheder og ASUS-routere ved at køre skadelige firmwareopdateringer og integrere dem i et stort botnet. Malwaren inficerer enheder ved at udnytte en kendt sårbarhed, der tillader eskalering af rettigheder, så det bliver muligt for trusselsaktørerne at administrere enheden. Når den er inficeret, gør malwaren det muligt for yderligere moduler at installere og undvige firmwareopdateringer. Der er observeret kompromitterede enheder, der opretter forbindelse med C2-servere, der er hostet på andre WatchGuard-enheder. Ved at udstede mange SSL-certifikater til deres C2 på forskellige TCP-porte fik Cyclops Blink-operatører privilegeret fjernadgang til netværk ved at køre skadelige firmwareopdateringer og omgå traditionelle sikkerhedsmetoder som scanning.

Sådan forbedrer Microsoft sikkerheden i supply chain

Microsoft samarbejder med myndigheder og industri om at løse disse sikkerhedsudfordringer i forbindelse med IoT og OT-enheder (se diskussionen på side 66). Vores bidrag vil inkludere firmwareanalyseteknologi til at give enhedsoperatører indsigt i sikkerhedsniveauet for enheder i deres netværk. Dette vil give kunderne mulighed for at identificere og prioritere enheder, der har brug for yderligere beskyttelse, opgraderinger eller udskiftning, og det vil tilskynde enhedsproducenter til at investere i enhedssikkerhed. Samtidig støtter vi udviklere med omfattende løsninger til at udvikle sikre enheder og indføre sikre udviklingslivscyklusser.

En anden nøglekomponent giver udviklere og operatører en robust infrastruktur, så enhedens firmware kan opdateres, efterhånden som sikkerhedsproblemer opdages og løses. Microsoft kombinerer firmwareanalyse og Defender for IoT med Device Update for IoT Hub for at levere en løsning til hele sikkerhedslivscyklussen for IoT- og OT-enheder. Disse er vigtige trin i realisering af vores vision om, at kunderne skal sikre infrastrukturen ved at bruge enheder, der understøtter en nul tillid-tilgang til deres IoT- og OT-løsninger.[18]

Angribere udnytter i stigende grad målsårbarheder i IoT-enhedsfirmware til at infiltrere virksomhedsnetværk.

Handlingsrettet indsigt

1. Få bedre indblik i IoT/OT-enheder på dit netværk, og prioriter dem ud fra den risiko, de udgør for virksomheden, hvis de kompromitteres.
2. Brug værktøjer til scanning af firmware for at forstå potentielle sikkerhedssvagheder, og samarbejd med leverandører for at afgøre, hvordan du kan reducere risikoen for højrisikoenheder.
3. Positiv påvirkning af sikkerheden af IoT/OT-enheder ved at stille krav om, at dine leverandører indfører bedste praksis for sikre udviklingslivscyklusser.

Links til yderligere oplysninger

- Vurdering af de vigtige supply chains, der understøtter den amerikanske industri for informations- og kommunikationsteknologi

Rekognoscerings-baserede OT-angreb

Komplekse supply chains bruger specifikke designoplysninger til at planlægge det faktiske system. Af de utallige aktiver, der udgør disse designoplysninger, er den mest følsomme fil projektfilen, som definerer miljøet og dets aktiver. Denne fil er et afgørende strategisk mål for trusselsaktører, der ønsker at få adgang og implementere et vellykket angreb, der er fuldstændigt tilpasset til miljøet.

Målretning mod industrielle systemer for at forstyrre driftsprocesser involverer to trin.

1. Først skal angriberen have adgang til OT-netværket. Dette kan gøres ved at gå ind via IoT-enheder på virksomhedssiden af netværket (Purdue Model Level 4) og krydse IT-OT-grænsen, traditionelt adskilt af firewalls og netværksudstyr, for at nå niveauerne for drift og kontrol.
2. Dernæst skal netværksenheder identificeres. Industrielle systemer anvender standardenheder og komponenter i tilpassede arkitekturer, der er designet specifikt til deres miljø. En af disse standardenheder er PLC (Programmable Logic Controller). Hver producent udvikler unikke grænseflader og funktioner til sine programmerbare logiske controllere (PLC), som er en vigtig komponent i industrielle systemer. Disse enheder er yderligere konfigureret med tilpassede skemaer, der er Specifikt designet til kundemiljøer.

Den unikke konfiguration af hver PLC er beskrevet i projektfilen, som indeholder definitionen af miljøet og dets aktiver, stigelogikken og meget mere.

I de fleste miljøer, der viser tegn på et angreb, viser analyse, at tidslinjen op til angrebet langt overstiger varigheden af selve angrebet. Trusselsaktører investerer ofte måneder i simulering af miljøet og dets aktiver eksternt ved at foretage utallige forsøg på at udvikle en model og forberede deres målrettede angreb. Da miljøer konstant ændres og integrerer nye enheder, skabes der sårbarheder specifikt omkring data i projekt- og konfigurationsfiler. Tyveri af en projektfil kan fremskynde et angreb med uger eller måneder og gøre det muligt for angribere at modellere målmiljøet hurtigt og præcist, hvilket gør det sværere at opdage skadelig aktivitet.

Industroyer og Incontroller

Vi har observeret en stigning i angreb mod mål, herunder organisationer, kritisk infrastruktur og offentlige administrationer fra statsstøttede aktører, der bruger modulær malware og angrebsstruktur. Nye forsøg på at forstyrre kritiske operationer i Ukraine understreger den voksende trussel fra rekognosceringsbaserede OT-angreb, der er yderst tilpassede til deres målmiljøer. Langvarige rekognoscerings- og undersøgelsesfaser udført af nationalstatslige cyberaktører peger på en strategi, der bruger cyberkrigsførelse til at fjernafbryde infrastruktur for at opnå specifikke strategiske eller operationelle mål i kombinerede cyberkinetiske operationer og politiske strategier.

Vi har observeret en voksende trussel om rekognoscerings-baserede OT-angreb, der er meget tilpassede til deres målmiljøer.

Rekognoscerings-baserede OT-angreb

Fortsat

I starten af 2022 blev der identificeret to fleksible, kritiske OT-angreb. Et cyberfysisk angreb på elektriske understationer og beskyttelsesrelæer i Ukraine blev udført via tilpasset malware, herunder via en variant af Industroyer, en malware, der er kendt for at forårsage strømafbrydelser i Ukraine, efter at den blev implementeret i 2016.

Industroyer2 er den første kendte genimplementering af skadelig OT-angrebsmalware på et nyt mål. Den udnyttede IEC104-protokolplugin'en (der er standardprotokol til overvågning og styring af strømsystemet), der blev udviklet til Industroyer og primært var målrettet mod PLC-lignende fjernterminalenheder med modelnummer ABB RTU540/560. Forfatteren til denne malware brugte viden om ofrets miljø til gentagne gange at udstede kommandoer til forudbestemte output for at sikre, at de ikke kunne aktiveres manuelt. Dette sikrede længerevarende strømafbrydelser og en mere skadelig påvirkning.

Incontroller, der er en modulopbygget angrebsstruktur, der blev identificeret i samme periode, er et modulært værktøjssæt, der i væsentlig grad reducerer, den tid det tager at trænge ind og angribe OT-enheder og omgå ældre sikkerhedsløsninger. Det generelle værktøjssæt har dataindsamlings-, rekognoscerings- og angrebskapaciteter, der er meget tilpasningsdygtige i forskellige miljøer og kan have en enorm indflydelse på undersøgelsesfasen af et OT-angreb, reducere den tid, der er nødvendig for at udføre rekognoscering og understøtte simuleringen af miljøer ved at udtrække oplysninger om enheder og deres konfigurationer.

Incontroller-strukturen understøtter protokoller for Schneider Electric- og Omron PLC'er og indsamler oplysninger, herunder firmwareversion, modeltype og tilsluttede enheder. Værktøjssættet kan udstede kommandoer til at ændre konfigurationer og aktivere eller deaktivere output. Når først der er opnået adgang til et miljø, understøtter strukturen indsættelse af bagdøre i enheder for at levere flere nyttedata, publicering af sårbarheder for at øge adgangspunkter, upload af stigelogik og evnen til at starte DoS-angreb. Værktøjssættets generiske karakter gør det muligt for en trusselsaktør hurtigt at angribe et miljø uden at skulle skrive nye angreb for hver PLC eller lokation. Dette gør det nemt for aktøren at interagere med forskellige maskintyper potentielt på tværs af flere brancher.

Handlingsrettet indsigt

1. Undgå at overføre filer, der indeholder systemdefinitioner, gennem usikre kanaler eller til personale, der ikke har brug for dem.
2. Hvis overførslen af sådanne filer er uundgåelig, skal du sørge for at overvåge netværksaktivitet og sikre, at aktiverne er sikre.
3. Beskyt teknikerstationer ved overvågning med EDR-løsninger.
4. Udfør hændelsesrespons for OT-netværk proaktivt.
5. Implementer kontinuerlig overvågning, f.eks. Defender til IoT.

Slutnoter

1. Se f.eks. Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1, Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au), Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance, Japan passes economic security bill to guard sensitive technology | The Japan Times, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg), Proposal for legislation to improve the UK's cyber resilience – GOV.UK (www.gov.uk), Telecommunications (Security) Act 2021 (legislation.gov.uk), Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST
2. Cert-In – startside
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Se f.eks. uden titel (house.gov)
5. Lov om cyberrobusthed | Forme Europas digitale fremtid (europa.eu)
6. Se f.eks. Microsoft Security Development Lifecycle
7. Se f.eks. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft – Engineering@Microsoft, se f.eks. også The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Se f.eks. https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill – faktaark om produktsikkerhed – GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe – ENISA (europa.eu)
12. Certificering – ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub - Microsoft/sbom-tool: SBOM-værktøjet er et yderst skalerbart og virksomhedsklart værktøj til at oprette SPDX 2.2-kompatible SBOM'er til alle typer af artefakter.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. IoT/OT Innovation Critical but Comes with Significant Risks (dec. 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. Uncovering Trickbot's use of IoT devices in C2 Infrastructure (mar 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show on Channel 9 Episode on IoT Firmware Scanning (maj 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. How to apply a Zero Trust approach to your IoT solutions (maj 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Cyber-indflydelses-aktiviteter

Nutidens udenlandske indflydelsesaktiviteter bruger nye metoder og teknikker. Deres kampagner har til formål at svække tilliden mere effektivt.

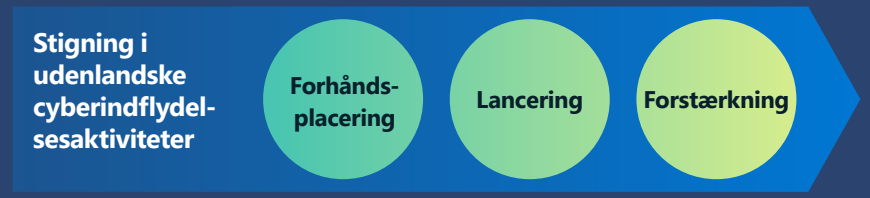
En oversigt over

cyberindflydel-sesaktiviteter

Nutidens udenlandske indflydelsesaktiviteter bruger nye metoder og teknikker. Deres kampagner har til formål at svække tilliden mere effektivt.

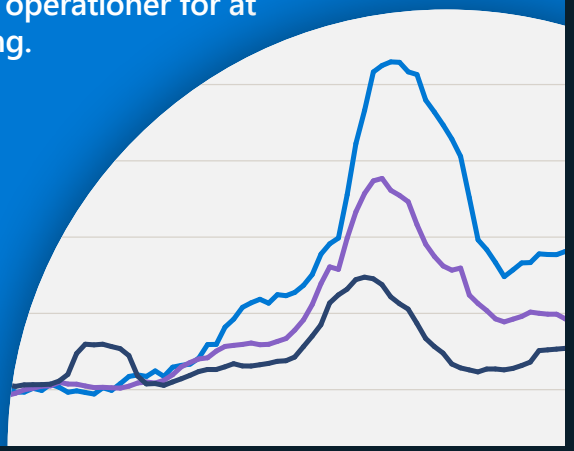
Nationalstater bruger i stigende grad sofistikerede indflydelsesaktiviteter til at distribuere oplysninger og påvirke den offentlige mening både nationalt og internationalt. Disse kampagner underminerer tillid, øger polariseringen og truer demokratiske processer. Dygtige avancerede og vedholdende manipulatorer bruger traditionelle medier sammen med internettet og sociale medier til markant at øge omfanget og effektiviteten af deres kampagner og den store indvirkning, de har i det globale informationsøkosystem. I det forløbne år har vi set disse aktiviteter blive brugt som en del af Ruslands hybridkrig i Ukraine, men vi har også set Rusland og andre nationer, herunder Kina og Iran, i stigende grad implementere propagandaaktiviteter på de sociale medier for at udvide deres globale indflydelse.

Cyberindflydelsesaktiviteter bliver mere og mere sofistikerede, efterhånden som flere myndigheder og nationalstater bruger sådanne aktiviteter til at forme meninger, miskreditere modstandere og fremme uoverensstemmelse.



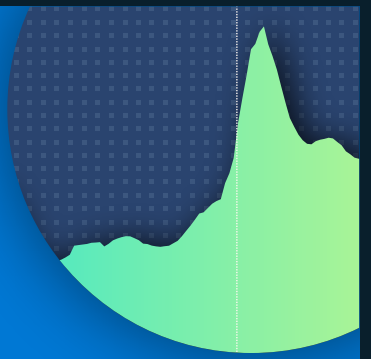
Få mere at vide på side 74

Ruslands invasion af Ukraine viser cyberindflydelsesaktiviteter integreret med mere traditionelle cyberangreb og kinetiske militære operationer for at maksimere indvirkning.



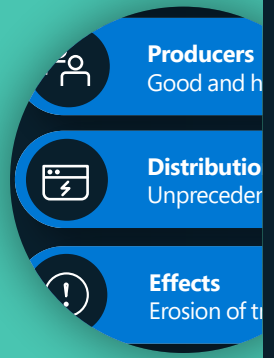
Få mere at vide på side 76

Rusland, Iran og Kina brugte hyppigt propaganda- og indflydelseskampagner under Covid-19-pandemien som en strategisk metode til at nå bredere politiske mål



Få mere at vide på side 76

Syntetiske medier bliver mere og mere almindelige på grund af udbredelsen af værktøjer, der gør det nemt at oprette og distribuere meget realistiske, kunstige billeder, film og lyde. Digital "herkomstteknologi", der certificerer oprindelsen af medieaktiver, lover at bekæmpe misbrug.



Få mere at vide på side 80

En holistisk tilgang til beskyttelse mod cyberindflydelsesaktiviteter

Microsoft bygger videre på sin allerede modne infrastruktur for cybertrusselsintelligens for at bekæmpe cyberindflydelsesaktiviteter. Vores strategi er at registrere, forstyrre, forsvare og afskrække propagandakampagner fra udenlandske angribere.

Få mere at vide på side 83

Introduktion

Demokrati har brug for pålidelige oplysninger for at blomstre. Et nøglefokusområde for Microsoft er indflydel-sesaktiviteter, der udvikles og videreføres af nationalstater. Disse kampagner underminerer tillid, øger polariseringen og truer demokratiske processer.

Aktiviteter med udenlandsk indflydelse har altid været en trussel mod informationsøkosystemet. Forskellen i internettets og de sociale mediers alder er imidlertid den stærkt forøgede rækkevidde, omfang og effektivitet af kampagner og den overordnede indvirkning, de kan have på det globale informationsøkosystems sundhed.

Det gamle ordsprog om, at "En løgn kan nå halvvejs rundt om jorden, mens sandheden tager sine sko på" kan nu bekræftes med data. Ifølge en undersøgelse foretaget af MIT (Massachusetts Institute of Technology[1] er der 70 % større sandsynlighed for, at falske nyheder bliver retweetet end sandheden, og at de når de første 1.500 mennesker seks gange hurtigere. Informationsøkosystemet er blevet mere og mere broget, efterhånden som propagandakampagner blomstrer på internettet og sociale medier og underminerer tilliden til traditionelle nyheder. I en undersøgelse fra 2021[2] sagde kun 7 % af voksne amerikanere, at de havde "en stor del tillid" til aviser, tv og radio, mens 34 % sagde, at de "slet ingen tillid" havde.

Microsoft har arbejdet på at identificere nøglespillere, trusler og taktikker i det udenlandske cyberindflydelsesområde og at dele erfaringerne. I juni i år offentliggjorde vi en omfattende rapport om erfaringer fra Ukraine, som indeholdt en detaljeret undersøgelse af Ruslands cyberindflydelsesaktiviteter.[3]

Vi undersøger også, hvordan avancerede teknologier, som deep fakes, kan bruges som våben, og hvordan de kan underminere journalisters troværdighed. Og vi samarbejder med industrien, de offentlige myndigheder og den akademiske verden om at udvikle metoder til at opdage syntetiske medier og genskabe tillid, som AI-systemer (kunstig intelligens), der kan opdage falske data.

Det hurtigt skiftende karakter af informationsøkosystemet og den nationalstatslige onlinepropaganda, herunder sammensmeltningen af traditionelle cyberangreb med indflydelsesaktiviteter og indblanding i demokratiske valg, kræver en omfattende tilgang fra hele samfundet for at afbøde online- og offlinetrusler mod demokratiet.

Microsoft er forpligtet til at opretholde et sundt informationsøkosystem, hvor pålidelige nyheder og information trives. Vi udvikler værktøjer og trusselsregistreringsfunktioner til at bekæmpe den udviklende og stadig voksende risiko for indflydelsesaktiviteter, der udføres af nationalstater. For at gøre dette arbejde muligt har vi for nylig erhvervet Miburo Solutions, vi har indgået partnerskab med tredjepartsvalidatorer som Global Disinformation Index og NewsGuard, og vi deltager i eller leder endda partnerskaber med flere interessenter, herunder C2PA (Coalition for Content Provenance and Authenticity).
Kun ved at samarbejde kan det lykkes os at besejre dem, der forsøger at underminere demokratiske processer og institutioner.

Teresa Hutson

Vice President, Technology and Corporate Responsibility

Tendenser inden for cyberindflydel-sesaktiviteter

Cyberindflydelsesaktiviteter bliver stadig mere sofistikerede, mens teknologien udvikler sig i samme tempo. Vi ser en overlapning og udvidelse af de værktøjer, der bruges i traditionelle cyberangreb, anvendt på cyberindflydelsesaktiviteter. Desuden ser vi en vækst i koordinering og forstærkning blandt nationalstaterne.

Microsoft investerede i bekæmpelse af udenlandsk indflydelse i år med opkøbet af Miburo Solutions, en virksomhed, der er specialiseret i analyse af udenlandske indflydelsesaktiviteter. Ved at kombinere disse analytikere med Microsofts analytikere af trusselslandskabet blev DTAC (Digital Threat Analysis Center) dannet. DTAC analyserer og rapporterer om trusler fra nationalstater, herunder både cyberangreb og indflydelsesaktiviteter. De kombinerer oplysninger og trusselsintelligens med geopolitisk analyse for at give indsigt og informere effektive svar og beskyttelser.

Mere end tre fjerdedele af mennesker verden over sagde, at de bekymrer sig om, at oplysninger bliver benyttet som et våben,[4] og vores data understøtter disse bekymringer. Microsoft og dets partnere har sporet, hvordan nationalstatsaktører anvender indflydelsesaktiviteter til at nå deres strategiske og politiske mål. Ud over destruktive cyberangreb og cyberspionagebestræbelser bruger autoritære regimer i stigende grad cyberindflydelsesaktiviteter til at forme den offentlige mening, miskreditere modstandere, indgyde frygt, fremme uoverensstemmelse og fordreje virkeligheden.

Disse udenlandske cyberindflydelsesaktiviteter har typisk tre faser:

Forhåndsplacering

Ligesom forhåndsplacering af malware i en organisations computernetværk forhåndsplacerer udenlandske cyberindflydelsesaktiviteter falske historier i det offentlige domæne på internettet. Forhåndsplaceringstaktikken har længe været nyttig til mere traditionelle cyberaktiviteter, især hvis it-administratorer scanner den seneste aktivitet på deres netværk. Malware, der ligger i dvale i lang tid på et netværk, kan gøre en senere anvendelse mere effektiv. Falske historier, der er gået ubemærket hen på internettet, kan få efterfølgende referencer til dem til at fremstå mere troværdige.

Lancering

På det tidspunkt, hvor det er mest gavnligt at nå aktørens mål, iværksættes der en koordineret kampagne for at sprede historier via offentligt statsstøttede og påvirkede mediekanaler og sociale mediekanaler.

Forstærkning

Endelig forstærker nationalstatskontrollerede medier og fuldmagter historier inden for målrettede målgrupper. Ofte udvider ufrivillige teknologiske hjælpeteknologier historiernes rækkevidde. For eksempel kan onlineannoncer hjælpe med at finansiere aktiviteter, og koordinerede indholdsleveringssystemer kan oversvømme søgemaskiner.

Denne tretrinstilgang blev anvendt i slutningen af 2021 til at støtte Ruslands falske historier om påståede biologiske våben og laboratorier i Ukraine. Denne historie blev første gang uploadet til YouTube den 29. november 2021 som en del af en programserie udarbejdet på engelsk af en Moskva-baseret amerikansk emigrant, der hævdede, at amerikansk-finansierede laboratorier i Ukraine havde forbindelse til biologiske våben. Historien gik ubemærket hen i flere måneder. Den 24. februar 2022, da russiske kampvogne krydsede grænsen, blev historien sendt i omløb. Et dataanalyseteam fra Microsoft identificerede 10 russisk-kontrollerede eller russisk-influerede nyhedswebsteder, som samtidig offentliggjorde rapporter den 24. februar, der refererede til "sidste års rapport" og forsøgte at give den troværdighed. Derudover holdt embedsmænd i det russiske udenrigsministerium pressekonferencer, hvor man udspredte falske påstande i informationsmiljøet om amerikanske laboratorier. De russisk-sponsorerede teams arbejdede derefter på at forstærke historien på sociale medier og internetsider mere bredt.

Vi ser autoritære regimer rundt om i verden samarbejde om at forurene informationsøkosystemet til gensidig fordel. Under hele COVID-19-pandemien brugte Rusland, Iran og Kina propaganda- og indflydelsesaktiviteter ved at bruge en blanding af åbenlyse, halvhemmelige og hemmelige formidlingsmetoder til at målrette mod demokratier og andre geopolitiske mål (som beskrives yderligere på side 76). De tre regimer forstærkede hinandens budskaber og informationsøkosystemer for at fastholde deres foretrukne historier. Meget af dette bestod af kritik eller konspirationsteorier om USA og deres allierede fremført af embedsmænd i officielle udtalelser, mens de udråbte deres egne vacciner og reaktion på covid-19 som overlegne i forhold til vacciner fra USA og andre demokratier. Ved at forstærke hinanden oprettede statsstyrede mediekanaler et økosystem, hvor negativ omtale af demokratier – eller positiv omtale af Rusland, Iran og Kina – produceret af det ene statslige mediebureau blev forstærket af de andre.

Illustration af, hvordan historier om amerikanske biologiske laboratorier og våben spredes via de tre brede faser af mange udenlandske magters indflydelsesaktiviteter: forhåndsplacering, lancering og forstærkning.

Tendenser inden for cyberindflydel-sesaktiviteter

Fortsat

Udfordringen kan blive endnu større, fordi teknologienheder i den private sektor uforvarende kan aktivere disse kampagner. Katalysatorer kan inkludere virksomheder, der registrerer internetdomæner,hoster websteder, promoverer materiale på sociale medier og søgesider, kanaliserer trafik og hjælper med at betale for disse øvelser gennem digital annoncering. Organisationer skal være opmærksomme på de værktøjer og metoder, der bruges af autoritære regimer til cyberindflydelsesaktiviteter, så de kan registrere og derefter forhindre spredning af kampagner. Det er også et voksende behov for at hjælpe kunder med at udvikle en mere sofistikeret evne til at identificere udenlandske indflydelsesaktiviteter og begrænse engagement med sådanne historier eller indhold.

Cyberindflydelsesaktiviteter, herunder autoritær propaganda, er en trussel mod demokratier over hele verden, da de undergraver tillid, øger polarisering og truer demokratiske processer.

Øget koordinering og informationsdeling på tværs af offentlige myndigheder, den private sektor og civilsamfundet er nødvendig for at øge gennemsigtigheden og eksponere og afbryde disse indflydelseskampagner.

På globalt plan bekymrer mere end tre fjerdedele af folk sig over, hvordan information bliver brugt som våben.

Fokus på indflydelsesaktiviteter under COVID-19 og russisk invasion af Ukraine

Nationalstater, der forsøgte at kontrollere informationsmiljøet gennem hele pandemien og under den russiske invasion af Ukraine, er konkrete eksempler på, hvordan autoritære regimer blander cyber- og informationsaktiviteter.

COVID-19-propaganda

Rusland, Iran og Kina anvendte propaganda og indflydelseskampagner under hele COVID-19-pandemien. COVID-19 har været fremtrædende i disse kampagner på to centrale måder:

1. Repræsentationer af selve pandemien.
2. Kampagner, der brugte COVID-19 som en strategisk enhed til at nå bredere politiske mål.

Det overordnede mål med disse kampagnetyper er todelt: For det første at underminere demokratier, demokratiske institutioner og billedet af USA og deres allierede på verdensscenen, og for det andet at styrke deres egen position nationalt og internationalt.

Du kan se et eksempel på dette i de beskeder, der blev udsendt af velkendte russiske konti og medieorganisationer målrettet mod engelsktalende læsere kontra de russiske myndigheders beskeder til egne borgere om vaccinen og alvoren af COVID-19.

Emner, der dækkes af de 10 mest sete coronavirushistorier på RT.com (oktober 2021-april 2022)

Anti-vaccinepropaganda målrettes mod ikke-russiske læsere

Russisk (oversat nedenfor til engelsk)	Engelsk
"Lockdowns og vaccineforstærkere forhindrer smittespredning"	"Vaccinationer begrænser ikke smitte og er ineffektive mod nye varianter"
"Russiske offentlige personer tester positive"	"Pfizer-vaccine har farlige bivirkninger"
"Tilfælde og dødsfald er stigende i Rusland"	"Massevaccination er politisk motiveret"
"Sputnik V-vaccinen er yderst effektiv"	"Pfizer og Moderna udfører uregulerede forsøg"
"Vaccinationsbeviser er nødvendige i offentlig transport"	

Russiske COVID-19-meddelelser varierer efter sprog.

Kampagner, der forsøgte at sløre oprindelsen af COVID-19-virussen er et andet eksempel. Siden starten af pandemien har den russiske, iranske og kinesiske COVID-19-propaganda øget dækningen fra de andre for at forstærke disse centrale temaer. En stor del af denne dækning bestod i at fremme kritik eller konspirationsteorier om USA. Ved at forstærke hinandens udtalelser udviklede de statslige mediekanaler et økosystem, hvor negative tekster om demokratier eller positive tekster om Rusland, Iran og Kina fra den ene statslige mediekanal blev forstærket af de andre gentagne gange.

Et sådant eksempel er det tidlige forslag fra russiske og iranske statsmedier om, at COVID-19 kunne være et biologisk våben skabt af USA. Denne påstand cirkulerede på yderliggående konspirationswebsteder tidligt i pandemien, efter et interview med en juraprofessor, der mente, at COVID-19-virussen var oprettet som et våben.[6] Efter interviewet blev offentliggjort på nogle få websteder med begrænset rækkevidde, blev historien opfanget af statsejede mediekanaler. PressTV, en engelsk- og franskproget iransk kanal, der blev støttet af den iranske regering,[7], offentliggjorde en historie på engelsk i februar 2020 med titlen "Er coronavirus et amerikansk biologisk krigsførelsesvåben, som Francis Boyle påstår?" Artiklen antydede, at USA stod bag COVID-19-udbruddet og skrev, at "i alle amerikanske krige blev der brugt radiologiske, kemiske, biologiske og andre forbudte våben, med en ødelæggende virkning for mennesker i målrettede områder".[8] Russiske statsejede mediekanaler og kinesiske regeringskonti gentog denne udtalelse. Russia Today (RT), en statsejet virksomhed, der er kendt for dets rolle i at formidle Kreml-propaganda[9], offentliggjorde mindst én artikel, der fremhævede udtalelser fra iranske embedsmænd, der hævdede, at COVID-19 kunne være "et produkt af amerikansk biologisk angreb rettet mod Iran og Kina"[10] og spredte indlæg på sociale medier, der bekræftede denne erklæring. For eksempel stod der i et RT-tweet fra den 27. februar 2020: "Ræk hånden op, hvis du ikke bliver overrasket, hvis det aldrig bliver afsløret, at #coronavirus er et biologisk våben".[11]

Krigen i Ukraine – propaganda som et krigsvåben

Ruslands invasion af Ukraine er et tydeligt eksempel på, hvordan cyberindflydelsesaktiviteter kan blive flettet sammen med mere traditionelle cyberangreb og militære aktiviteter for at maksimere deres indvirkning.

Under optakten til invasionen af Ukraine observerede Microsofts trusselsefterretningsanalytikere, at mindst seks separate pro-russiske aktører lancerede mere end 237 cyberangreb mod Ukraine. Disse kampagner forsøgte at nedværdige tjenester og institutioner, forstyrre ukrainernes adgang til pålidelige oplysninger og at så tvivl om landets lederskab.

Fokus på indflydelsesaktiviteter under COVID-19 og russisk invasion af Ukraine

Fortsat

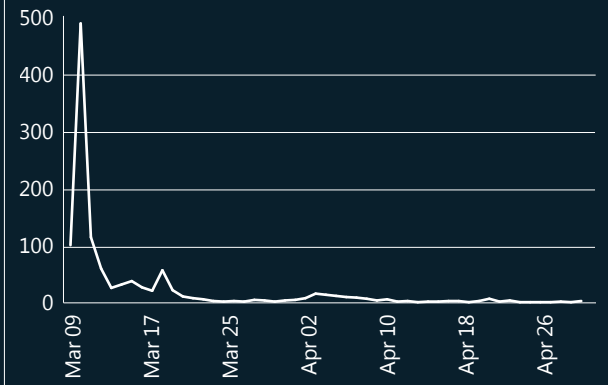
I en Microsoft-rapport offentliggjort i april 2022 viste vi, hvordan Rusland i et åbenlyst forsøg på at kontrollere oplysningerne i Kiev affyrede et missil mod et tv-tårn i Kiev samme dag, som de lancerede ødelæggende malware rettet mod et større ukrainsk medieselskab.[12]

I et andet eksempel på, hvordan cyberangreb og indflydelsesaktiviteter konvergerer, sendte en russisk trusselsaktør mails til ukrainske borgere, og foregav at de var fra indbyggere i Mariupol, der bebrejdede den ukrainske regering, at krigen eskalerede, og opfordrede deres landsmænd til at gå mod regeringen. Disse mails var specifikt adresseret (med navn) til dem, der modtog mailen, hvilket indikerer, at de måske har fået stjålet deres oplysninger i et tidligere spionagerelateret cyberangreb. Der blev ikke fundet skadelige links i mailen, hvilket synes at indikere, at det var rene indflydelsesaktiviteter.

Præsentation af angiveligt hackede, lækkede eller følsomme dokumenter er en almindelig taktik, som russiske aktører anvender i forbindelse med indflydelsesaktiviteter. Under hele krigen i Ukraine har pro-russiske sociale medier promoveret, hvad de hævder er lækkede eller på anden vis følsomme materialer fra ukrainske kilder. Lækkede eller følsomme dokumenter anvendes af pro-russiske sociale netværk og medier som led i en bredere indflydelsesstrategi, der sigter mod at mindske tilliden til institutioner og så tvivl om nyhedshistorierne. Disse oplysninger kan manipuleres til at skabe propaganda, der er rettet mod Ukraine og Vesten, mindske tilliden til digital sikkerhed og underminere støtte til vestlig hjælp til Ukraine.

Rusland benyttede andre informationsangreb til at påvirke den offentlige mening efter begivenheder på stedet for at skjule eller underminere fakta. Den 7. marts placerede Rusland f.eks. en forhåndsplaceret historie via en indberetning til FN om, at et barselshospital i Mariupol i Ukraine var blevet tømt og blev brugt som et militæranlæg. Den 9. marts bombede Rusland hospitalet. Da nyheden om bombningen brød ud, tweetede Ruslands FN-repræsentant, Dmitry Polyanskiy, at rapporter om bombningen var "falske nyheder", og citerede Ruslands tidligere påstande om, at det blev brugt som et militæranlæg. Rusland udbredte derefter denne historie bredt på russisk-kontrollerede websteder i to uger efter angrebet på hospitalet.

Domæner med trafik
(9. marts 2022-30. april 2022)



Propagandawebsteder publicerede artikler om barselshospitalet i ca. to uger med en kort genopblussen den 1. april 2022. Kilde: Microsoft AI for Good Lab.

Satellitbilleder af et perinatalhospital i Mariupol i februar og marts 2022

Microsofts satellitbilledanalyse viser, at perinatalhospitalet blev bombet. Det første billede er fra 24. februar 2022, og det andet er fra 24. marts 2022. Fotokilde: Planet Labs.

Ruslands dække over egne grusomheder er fortsat, efterhånden som krigen har udviklet sig. I slutningen af juni 2022 fremstillede de russiske medier og influencere f.eks. bombningen af et indkøbscenter som berettiget og nødvendigt og påstod fejlagtigt, at det ikke var i brug som et indkøbscenter, men snarere i brug af Ukraine som et våbenlager for de territoriale forsvarsstyrker.[13] Flere pro-Kremlin-bloggere på Telegram postede og forstærkede indhold, der underbyggede "falsk flag"-historien, og bloggere pegede på påståede indikatorer for fabrikation, herunder tilstedeværelsen af mennesker i uniform på billeder fra stedet[14] og fraværet af kvinder på billederne.[15] Rusland lancerede kampagner ved hjælp af en omfattende system af budbringere og propagandamidler og -medier. Forstærkning af disse historier online giver Rusland mulighed for at aflede skylden på den internationale scene og undgå ansvarlighed.

Nationalstater som Rusland har indset værdien af at bruge oplysninger fra lukkede kilder til at påvirke den offentlige mening ved at bruge "hack and leak"-kampagner til at sprede modhistorier og så mistillid.

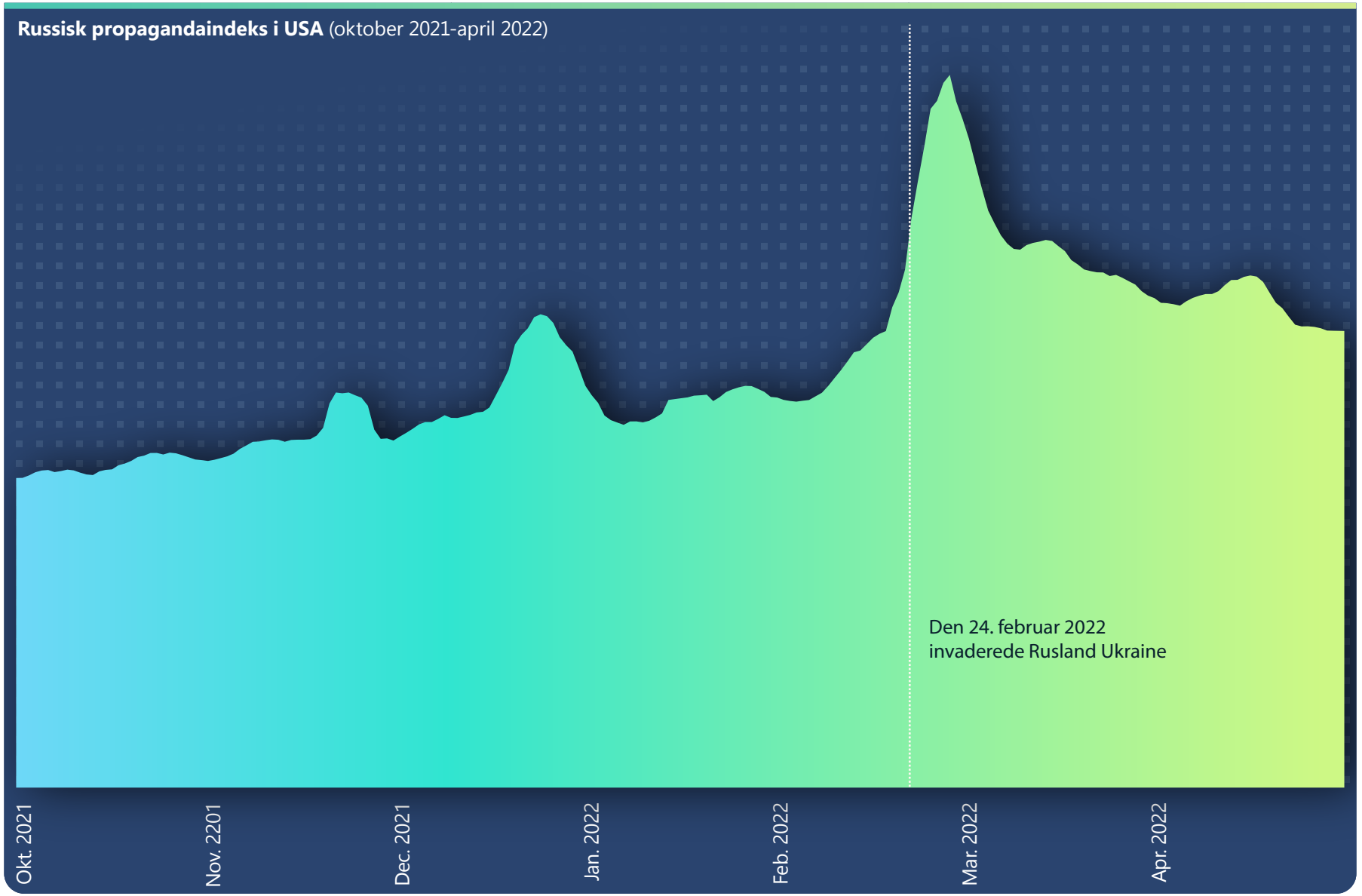
Links til yderligere oplysninger

- Forsvare Ukraine: Tidlige erfaringer fra cyberkrigen | Microsoft On the Issues
- En oversigt over Ruslands cyberangreb-saktivitet i Ukraine | Microsoft Special Report
- Afbrydelse af målretning af cyberangreb mod Ukraine | Microsoft On the Issues

Sporing af det russiske propagandaindeks

I januar 2022 henviste næsten 1.000 amerikanske websteder trafik til russiske propagandawebsteder. De mest almindelige emner for de russiske propagandawebsteder, der var målrettet et amerikansk publikum, var krigen i Ukraine, amerikansk indenrigspolitik (enten pro-Trump eller pro-Biden) samt COVID-19 og vaccinerelaterede historier.

RPI (Russian Propaganda Index) overvåger strømmen af nyheder fra russiske statskontrollerede og sponsorerede nyhedskanaler og forstærkninger som en del af den samlede nyhedstrafik på internettet. RPI'en kan benyttes til at kortlægge forbruget af den russiske propaganda på tværs af internettet og i forskellige geografiske områder på en nøjagtig tidslinje. Microsoft angiver, at det kun er muligt at observere den russiske propaganda, der offentliggøres på tidligere identificerede websteder. Vi har ikke indsigt i propaganda på andre typer af websteder, herunder autoritative nyhedswebsteder, uidentificerede websteder og sociale netværksgrupper.



Sporing af det russiske propagandaindeks

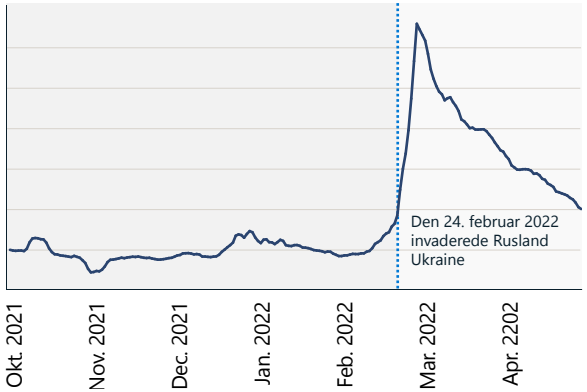
Fortsat

Russisk propagandaindeks: Ukraine

Da krigen i Ukraine begyndte, oplevede vi en stigning på 216 % i den russiske propaganda, og den toppede den 2. marts. Diagrammet herunder viser, hvordan denne pludselige stigning faldt sammen med invasionen. De to diagrammer viser, hvordan den russiske propaganda steg hurtigt, efter invasionen startede.

RPI, Ukraine

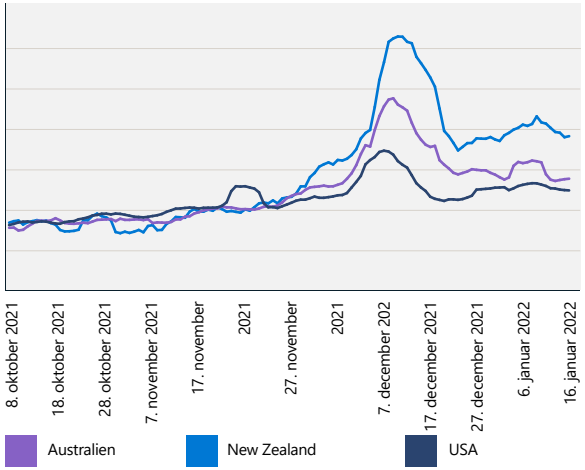
(7. oktober 2021-30. april 2022)



Det russiske propagandaindeks: New Zealand sammenlignet med Australien og USA.

En vurdering af RPI i New Zealand viste en stigning i slutningen af 2021, der var relateret til COVID-19-propaganda. Denne stigning i forbruget af russisk propaganda i New Zealand gik forud for en stigning i antallet af offentlige demonstrationer i starten af 2022 i Wellington. En anden stigning var klart relateret til den russiske invasion af Ukraine og overskred RPI'erne i Australien og USA.

RPI, New Zealand kontra Australien og USA



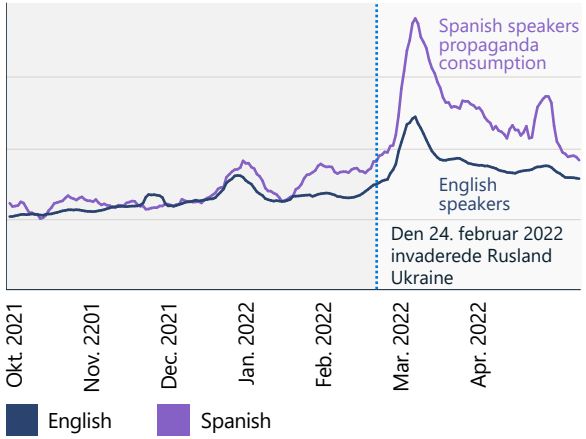
Forbruget af russisk propaganda i New Zealand svarer til Australiens forbrug indtil den første uge af december 2021. Efter december stiger forbruget af russisk propaganda i New Zealand med mere end 30 % sammenlignet med forbruget i Australien og USA.

Det russiske indeks i USA: engelsk og spansk

RPI'en sporer også propaganda på tværs af sprog. Flere kanaler, herunder RT og Sputnik News, er tilgængelige på over 20 sprog. Disse omfatter engelsk, spansk, tysk, fransk, græsk, italiensk, tjekkisk, polsk, serbisk, lettisk, litauisk, moldavisk, hviderussisk, armensk, ossetisk, georgisk, aserbajdsjansk, arabisk, tyrkisk, persisk og dari.

Følgende diagram viser, at RPI for de spanske sprognyheder i USA er meget højere end for de engelske nyheder.

Forbruget af russisk propaganda er 2 gange højere blandt spansktalende



Forbruget af russisk propaganda i USA er to gange højere blandt spansktalende.

Forbruget af russisk propaganda er højt i Latinamerika

RT på spansk er den internationale nyhedskanal med det højeste antal sidevisninger og Facebook-følgere.

Kilde: Microsoft AI for Good Research Lab

Syntetiske medier

Vi går ind i en guldalder for AI-aktiveret medieoprettelse og manipulation. Microsoft-analytikere bemærker, at denne udvikling skyldes to store tendenser: udbredelsen af letanvendelige værktøjer og tjenester til kunstigt at skabe yderst realistiske syntetiske billeder, videoer, lyd og tekst, og evnen til hurtigt at udsende indhold, der er optimeret til specifikke målgrupper.

Ingen af disse udviklinger er i sig selv problematisk. AI-baseret teknik kan bruges til at skabe sjovt og spændende digitalt indhold, hvad enten det gælder om at oprette rent syntetisk eller forbedre eksisterende materiale. Disse værktøjer bruges i stor udstrækning af virksomheder til annoncering og kommunikation og af enkeltpersoner til at skabe involverende indhold for deres følgere. Men syntetiske medier, der er skabt og distribueret med den hensigt at gøre skade, kan forårsage alvorlig skade på enkeltpersoner, virksomheder, institutioner og samfundet. Microsoft har været en drivkraft bag udviklingen af teknologier og praksis, både internt og i det overordnede medieøkosystem, for at begrænse denne skade.

I dette afsnit undersøger vi indsigt fra Microsofts analyse af den avancerede teknologi til at skabe skadeligt syntetisk indhold, den skade, der kan opstå, hvis dette indhold spredes bredt, og tekniske afbødende faktorer som et forsvar mod syntetiske mediebaserede cybertrusler.

Oprettelse af syntetiske medier

Feltet for syntetiske tekst og medier udvikler sig utroligt hurtigt, da teknikker, der engang kun var mulige med de enorme computerressourcer i store filmstudier, nu er integreret i telefonapps. Samtidig bliver værktøjerne nemmere at bruge og kan generere indhold med et realismeniveau, der kan narre selv retsvidenskabelige mediespecialister. Vi er meget tæt på at nå det punkt, hvor enhver kan oprette en syntetisk video af alle, der siger eller gør noget. Det er ikke urimeligt at tro, at vi går ind i en tidsalder, hvor en betydelig mængde af det indhold, vi ser online, er helt eller delvist syntetisk ved hjælp af AI-teknikker.

> Med fremkomsten af mere sofistikerede, brugervenlige og bredt tilgængelige værktøjer er oprettelsen af syntetisk indhold voksende og vil snart være umuligt at skelne fra virkeligheden.

Der er mange gratis og kommercielle værktøjer til billed-, video- og lydredigering i høj kvalitet. Disse værktøjer kan bruges til at foretage enkle, men potentielt skadelige ændringer i digitalt indhold, som tilføjelse af misvisende tekst, ombytning af ansigter og fjernelse eller ændring af konteksten. Disse "billige forfalskninger" benyttes i vid udstrækning til at sprede forbryderisk indhold, fremme politiske ideologier og til at skade menneskers omdømme. Et velkendt eksempel er videoen fra 2019[16] af formanden for Repræsentanternes hus, Nancy Pelosi, der taler sløret og optræder beruset.

Selv om det hurtigt blev afgjort, at videoens hastighed blev gjort langsommere for at skabe effekten, spredte den "billige forfalskning" sig vidt og bredt, før den oprindelige video og kontekst dukkede op.

Mere sofistikerede tilgange til at ændre medieindhold omfatter brugen af avancerede AI-teknikker til at (a) skabe rent syntetiske medier og til at (b) foretage mere avancerede redigeringer af eksisterende medier. Termen "deepfake" bruges ofte for syntetiske medier, der er genereret ved hjælp af banebrydende AI-teknikker (navnet kommer fra de dybe neurale netværk, der nogle gange benyttes). Disse teknologier udvikles som standalone apps, værktøjer og tjenester, og de integreres i etablerede kommercielle og open source-redigeringsværktøjer.

Disse teknologier anvendes af ondsindede aktører, der håber på at skade enkeltpersoner og institutioner. Eksempler på deepfake-teknikker inkluderer:

- **Face swap (video, billeder)** – udskiftning af et ansigt med et andet i en video. Denne teknik kan bruges til at prøve at afpresse en person, virksomhed eller institution eller placere enkeltpersoner på pinlige steder eller i pinlige situationer.
- **Dukkeføring (video, billeder)** – brug af en video til at animere et stillbillede eller anden video. Dette kan give det udseende af, at en person har sagt noget pinligt eller misvisende.
- **Generative fjendtlige netværk (video, billeder)** – en serie af teknikker til at generere fotorealistiske billeder.
- **Transformermodeller (video, billeder, tekst)** – oprettelse af avancerede billeder baseret på tekstbeskrivelser.

Sådanne avancerede AI-baserede teknikker bruges endnu ikke i vid udstrækning i cyberindflydelseskampagner i dag, men vi regner med, at problemet vil vokse, efterhånden som værktøjerne bliver nemmere at bruge og mere almindeligt tilgængelige.

Indvirkningen af manipulation med syntetiske medier

Anvendelsen af informationsaktiviteter til at forvolde skade eller få udvidet indflydelse er ikke ny. Når man tænker på, hvor hurtigt oplysninger kan blive spredt, og vores manglende evne til hurtigt at sortere fakta fra fiktion betyder det, at virkninger og skader, der er forårsaget af falske data og andre syntetisk genererede skadelige medier, kan blive meget større, som det blev vist i Pelosi-eksemplet.

Der er adskillige kategorier af skader: markedsmanipulation, svindel med betaling, vishing, efterligninger, skade på brands, skade på omdømme og botnets. For mange af disse kategorier har der været rapporteret om eksempler fra den virkelige verden, hvilket kan underminere vores evne til at skelne mellem fakta og fiktion.

En mere langsigtet og en mere lumsk trussel er vores forståelse af, hvad der er sandt, hvis vi ikke længere kan stole på det, vi ser og hører. På grund af dette kan alle kompromitterende billeder, lyd eller videoer af en offentlig eller privat person afvises som falsk – et resultat, der er kendt som The Liar's Dividend (Løgnerens udbytte).[17] Nyeste forskning[18] viser, at dette teknologimisbrug allerede benyttes til at angribe finansielle systemer, selvom mange andre misbrugsscenarier er plausible.

Syntetiske medier

Fortsat

Registrering af syntetiske medier

Der er bestræbelser undervejs på tværs af branchen, offentlige myndigheder og den akademiske verden på at udvikle bedre metoder til at registrere og afbøde syntetiske medier og for at genoprette tilliden. Der er adskillige lovende veje frem, samt barrierer der bør tages i betragtning.

En metode er at bygge AI-baserede systemer, der kan opdage forfalskninger – i det væsentlige "defensive" AI-systemer til at imødegå de offensive AI-systemer. Dette er et område med aktiv forskning, hvor de aktuelle systemer til oprettelse af syntetisk lyd og video efterlader afslørende artefakter, som trænede medieanalytikere og automatiserede værktøjer kan opdage.

Desværre er det sådan, at selvom de nuværende forfalskninger har afslørende fejl, har de nøjagtige artefakter en tendens til at være specifikke for et bestemt værktøj eller en bestemt algoritme. Det betyder, at undervisning i kendte forfalskninger normalt ikke kan generaliseres til andre algoritmer, som vist i en åben konkurrence i 2020 om at bygge deepfake-billeddetektorer.[19] Det er fristende at investere yderligere i udvikling af mere avancerede detektorer, men Microsoft tror ikke på, at dette vil resultere i meningsfulde forbedringer af to årsager:

For det første har vi fantastiske fysiske modeller, der afspejler den virkelige verden. De aktuelle udviklere af forfalskninger skærer hjørner, hvilket resulterer i registrerbare artefakter, men nyere modeller vil blive endnu mere realistiske. Der er i sig selv ikke noget specielt ved en scene fra den virkelige verden, der er optaget af et kamera, og som ikke kan modelleres af en computer.

For det andet bruger avancerede algoritmer til oprettelse af falske billeder en teknik ved navn GAN (Generative Adversarial Networks) som en del af oprettelsesprocessen. En GAN afspiller to AI-systemer parallelt ved brug af en generator til at skabe det falske billede og en diskriminator (et klassificeringssystem) til at finde falske billeder og træne generatoren. Alle investeringer i at udvikle en bedre detektor vil kun sætte generatoren i stand til at forbedre kvaliteten af forfalskningerne.

Syntetiske medier

Fortsat

Digitale aktivers herkomst

Hvis det er vanskeligt at opdage forfalskninger, hvad kan der så gøres for at beskytte mod skadelig brug af syntetiske medier? En vigtig ny teknologi er digital herkomst – en mekanisme, der gør det muligt for udviklere af digitale medier at certificere et aktiv og hjælpe forbrugerne med at afgøre, om der er blevet manipuleret med det digitale aktiv. Digital herkomst er specielt vigtig i forbindelse med nutidens sociale medienetværk i betragtning af den hastighed, hvormed indhold kan blive spredt på internettet, og muligheden for at ondsindede personer nemt kan manipulere indhold.

900 %

årlig stigning i udbredelsen af deepfakes siden 2019.[20]

Digital Provenance Technology er en moderne version af kryptografisk dokumentsignering. Den er udarbejdet til at registrere kilden, redigere historikken og metadataene for objekter, når de flyder gennem nutidens internet. Visionen og de tekniske metoder til at muliggøre denne type komplet manipulationssikker certificering af medier er udarbejdet af et team af forskere og videnskabsmænd hos Microsoft. Vi leder sammen med andre et partnerskab på tværs af brancher, der har til formål at udvikle herkomstteknologi for medier i Project Origin (grundlagt af Microsoft, BBC, CBC/Radio-Canada og New York Times) og engagere os i Content Authenticity Initiative (grundlagt af Adobe). Microsoft samarbejde også med teknologi- og medietjenestepartnere om at etablere koalitionen for C2PA (Coalition for Content Provenance and Authenticity). C2PA er en standardiseringsorganisation, der for nylig publicerede den mest avancerede specifikation for digital herkomst til brug med medieaktiver, inklusive billeder, videoer, lyd og tekst.

Et C2PA-aktiveret objekt bærer et manifest, der beskytter objektet og metadataene mod manipulation, og det medfølgende certifikat identificerer udgiveren.

Syntetiske medier var ikke oprindeligt udarbejdet til at gøre skade, men de bliver brugt som våben af ondsindede aktører til at underminere tilliden til enkeltpersoner og institutioner.

Digital herkomst er en lovende ny teknologi, der har potentialet til at genoprette folks tillid til online medieindhold ved at certificere oprindelsen af et medieaktiv.

Offentligt tilgængelige løsninger baseret på C2PA-specifikationen vises enten som en ny funktion i eksisterende produkter eller nye enkeltstående apps og tjenester. Vi forventer, at de fleste af de almindeligt anvendte værktøjer til registrering, redigering og oprettelse bliver aktiveret som C2PA i løbet af nogle få år. Dette giver selskaberne mulighed for at fastsætte deres behov og anvendelser for digital herkomst i dag og at kræve dette yderligere beskyttelseslag i de værktøjer, de bruger i eksisterende arbejdsgange.

Handlingsrettet indsigt

1. Tag proaktive skridt til at beskytte din organisation mod trusler om misinformation gennem proaktive overvejelser af dine PR- og kommunikationssvar.
2. Brug herkomstteknologi til at beskytte den officielle kommunikation.

Links til yderligere oplysninger

- Et lovende trin fremad om misinformation | Microsoft On the Issues
- A Milestone Reached, 31. januar 2022
- Project Origin | Microsoft ALT Innovation
- C2PA (Coalition for Content Provenance and Authenticity)
- Udforsk tekniske oplysninger om det system, som Project Origin bruger til mediegodkendelse | Microsoft ALT Innovation

En holistisk tilgang til beskyttelse mod cyberindflydel-sesaktiviteter

Microsoft bygger videre på den allerede veludviklede infrastruktur til cybertrusselsintelligens med henblik på at udvikle en bredere og mere inkluderende visning af cyberindflydelsesaktiviteter.

Vi bruger en struktur til at foreslå respons- og afbødningsstrategier til at bekæmpe den trussel, der er forbundet med handlinger. Denne kan opdeles i fire grundlæggende søjler: registrer, afbryd, forsvar og afskræk.

Desuden har Microsoft indført fire principper for at forankre vores arbejde i dette område. Det første princip er en forpligtelse til at respektere ytringsfriheden og opretholde vores kunders mulighed for at oprette, publicere og søge efter oplysninger via vores platforme, produkter og tjenester. Det andet er, at vi arbejder proaktivt på at forhindre, at vores platforme og produkter bruges til at forstærke udenlandske cyberindflydelsessteder og indhold. Det tredje er, at vi ikke med vilje vil profitere af udenlandsk cyberindflydelsesindhold eller -aktører. Endelig prioriterer vi at vise indhold for at imødegå udenlandske cyberindflydelsesaktiviteter ved at anvende interne og pålidelige tredjepartsdata i vores produkter.

Registrer

Ligesom med cyberforsvar er det første trin i at imødegå udenlandske cyberindflydelsesaktiviteter at udvikle kapaciteten til at registrere dem. Der er ingen enkelt virksomhed eller organisation, der kan gøre sig håb om, at de individuelt kan foretage de nødvendige fremskridt. Et nyt og bredere samarbejde på tværs af teknologisektoren vil være afgørende, da fremskridt i analysen og rapporteringen af cyberindflydelsesaktiviteter i høj grad afhænger af civilsamfundets rolle, herunder akademiske institutioner og nonprofitorganisationer.

I erkendelse af denne rolle har forskerne Jake Shapiro og Alicia Wanless på Princeton University og Carnegie Endowment for International Peace hver for sig lagt planer om at lancere det nye IRIE (Institute for Research on the Information Environment). Med støtte fra Microsoft, Knight Foundation og Craig Newmark Philanthropies vil IRIE oprette en inkluderende forskningsinstitution med deltagelse af flere interessenter med CERN (European Organization for Nuclear Research) som model. Den vil kombinere ekspertise inden for databehandling og -analyse for at sætte fart på og skalere nye opdagelser på dette område. Resultaterne vil blive publiceret for at formidle oplysningerne til politikere, teknologivirksomheder og forbrugere i bredere forstand.

Forsvar

Den anden grundlæggende søjle er at støtte det demokratiske forsvar, en langvarig prioritet med behov for investering og innovation. Den bør tage hensyn til de udfordringer, som teknologien har skabt for demokrati, og de muligheder, teknologien har skabt for at forsvare de demokratiske samfund mere effektivt.

Microsoft strategistruktur sigter mod at hjælpe interessenter på tværs af sektorer med at registrere, afbryde, forsvare og afskrække mod propaganda – især kampagner fra udenlandske angribere.

Det er passende at starte med en af de store teknologiske udfordringer i vores tidsalder – indvirkningen af internettet og den digitale annoncering på traditionel journalistik. Lige siden 1700-tallet har en fri og uafhængig presse haft en særlig rolle at spille i støtten til alle demokratier i verden. Den afslører korruption, dokumenterer krig og kaster lys over de største samfundsmæssige udfordringer i denne og alle andre tider. Men internettet har udhulet de lokale nyheder ved at udtrække reklameindtægter og narre betalende abonnenter væk. Mange lokale aviser er brudt sammen. En indsigt ud af flere fra vores seneste arbejde er, at byer, der ikke har nogen avis, uforvarende og uundgåeligt udsættes for en større mængde udenlandsk propaganda end gennemsnittet. Af disse årsager skal en af demokratiets vigtige forsvarstiltag være at styrke traditionel journalistik og den frie presse, især på lokalt plan. Dette kræver kontinuerlige investeringer og innovation, der skal afspejle de lokale behov i forskellige lande og på forskellige kontinenter. Disse problemer er ikke nemme at bearbejde, og de kræver indsatser fra flere interessenter, som Microsoft og andre teknologivirksomheder støtter i stigende grad.

Vi har også brug for nytænkning i den offentlige politik, og den skal prioriteres. Dette kan inkludere love, der tillader udgivere at forhandle reklameindtægter kollektivt med teknologivirksomheder, og lovgivning, der giver skattelettelser til at afhjælpe lokale nyhedsredaktioner med en del af deres skat for journalister, de ansætter. Journalister har brug for mange andre værktøjer til deres arbejde. De skal bl.a. kunne adskille indhold fra lovlige og svigagtige kilder.

Der er også et hurtigt voksende behov for at hjælpe forbrugerne med at blive bedre til at genkende nationalstatsdrevne informationsaktiviteter. Selvom dette kan virke overvældende, minder det om det arbejde, som teknologisektoren længe har udført for at bekæmpe andre former for cybertrusler. Overvej at oplære forbrugerne til at se nærmere på mailadresser for at hjælpe dem til at opdage spam eller anden svigagtig kommunikation. Initiativer i USA – f.eks. News Literacy Project og Trusted Journalism.

En mere langsigtet og en mere lumsk trussel er vores forståelse af, hvad der er sandt, hvis vi ikke længere kan stole på det, vi ser og hører.

En holistisk tilgang til beskyttelse mod cyberindflydel-sesaktiviteter

Fortsat

Program – hjælper med at udvikle bedre oplyste forbrugere af nyheder og information. Globalt kan ny teknologi som f.eks. browser-plugin fra NewsGuard hjælpe med til at fremme denne indsats meget hurtigere.

Det bør også erindre os om, at en del af grundlaget for demokrati er en uddannelse i medborgerskab. Som altid skal denne indsats starte i skolerne. Men vi lever i en verden, der kræver, at vi kontinuerligt modtager medborgerskabsuddannelse i hele vores levetid. Det nye Civics at Work-projekt, ledet af Center for Strategiske og Internationale Studier og med Microsoft som stiftende medlem og partner forsøger at styrke medborgerskabsuddannelse i virksomhedsfællesskaber. Det er et godt eksempel på bredden i muligheden for at styrke vores demokratiske forsvar.

Afbryd

I de seneste år har Microsoft's DCU (Digital Crimes Unit) forfinet deres taktikker og udviklet værktøjer til at afbryde cybertrusler rangerende fra ransomware til botnets og nationalstatsangreb. Vi har lært mange vigtige lektioner, startende med den rolle, som aktive afbrydelser spiller i imødegåelse af en lang række cyberangreb.

Når vi tænker på imødegåelse af cyberind-flydelsesaktiviteter, kan afbrydelse komme til at spille en endnu vigtigere rolle, og den bedste fremgangsmåde til afbrydelse bliver mere og mere tydelig. Den mest effektive modgift mod udbredt bedrageri er åbenhed. Det er grunden til, Microsoft øgede sin kapacitet til at registrere og afbryde nationalstatens indflydelsesaktiviteter ved at opkøbe Miburo Solutions, der er en førende virksomhed inden for cybertrusler og forskning, som har specialiseret sig i at registrere og reagere på udenlandske cyberindflydelsesaktiviteter.

Vores erfaring viser, at offentlige myndigheder, teknologivirksomheder og NGO'er bør tilskrive cyberangreb omhyggeligt og med tilstrækkelige beviser. Det er afgørende at forstå virkningen af en sådan afbrydelse, og det kan være endnu mere nyttigt i forbindelse med at afbryde cyberindflydelsen. Se blot på de amerikanske myndigheders måde at dele oplysninger på inden Ruslands invasion af Ukraine, hvor de brugte åbenhed til at handle effektivt – som at afsløre de russiske planer, herunder særlige kampagner som en plan om at bruge en falsk video.

Som det blev vist i sidste sommers publikation fra CyberPeace Institute i Geneve om igangværende cyberangreb i og uden for Ukraine, har mange organisationer i civilsamfundet og i den private sektor mulighed for at fremme åbenheden i forbindelse med cyberindflydelsesaktiviteter. Pålidelige rapporter om nyligt opdagede og veldokumenterede aktiviteter kan hjælpe offentligheden med bedre at vurdere, hvad de læser, ser og hører, især på internettet. Til dette formål vil Microsoft bygge videre på og udvide de eksisterende cyberrapporter og vil udgive nye rapporter, data og opdateringer relateret til, hvad vi opdager om cyberindflydelsesaktiviteter, herunder tilskrivningserklæringer, når det er relevant. Vi vil udgive en årsrapport, der bruger en datadrevet tilgang til at se på tilstedeværelsen af udenlandske informationsaktiviteter i hele virksomheden, og hvad der kan gøres for at sikre trinvise forbedringer. Vi vil også overveje yderligere skridt, der bygger på denne type åbenhed.

Den digitale annonceringsrolle er f.eks. særlig vigtig, da annoncer kan hjælpe med til at finansiere udenlandske aktiviteter og samtidig give legitimitet til udenlandsk sponsorerede propagandasteder. Det vil være nødvendigt med nye bestræbelser for at afbryde disse finansielle strømme.

Afskræk

Endelig kan vi ikke forvente, at nogen lande vil ændre deres adfærd, hvis der ikke kræves ansvarlighed for overtrædelser af internationale regler. Håndhævelse af en sådan ansvarlighed er alene et myndighedsansvar. Alligevel spiller stadig flere interessenter en vigtig rolle i forhold til at styrke og udvide de internationale normer. Mere end 30 onlineplatforme, annoncører og udgivere – inklusive Microsoft – har underskrevet Europa-Kommissionens nyligt opdaterede adfærdskodeks for misinformation og er enige om at styrke deres forpligtelse til at håndtere dette voksende problem. Ligesom det seneste møde i Paris, Christchurch Call, og deklarationen om internettets fremtid, kan multilaterale handlinger og aktiviteter fra flere interessenter samle myndighederne og offentligheden i demokratiske nationer. De offentlige myndigheder kan derefter bygge videre på disse normer og love for at fremme den ansvarlighed, som verdens demokratier har brug for og fortjener.

Gennem hurtig og radikal åbenhed kan demokratiske myndigheder og samfund effektivt svække indflydelseskampagner ved at nævne kilden til nationalstatsangreb, informere offentligheden og opbygge tillid til institutioner.

> Vi har øget den tekniske kapacitet til at opdage og afbryde aktiviteter med udenlandske indflydelsesaktiviteter og er forpligtet til åben rapportering om disse aktiviteter ligesom vores rapportering om cyberangreb.

Handlingsrettet indsigt

1. Implementer stærk digital hygiejneadfærd på tværs af organisationen.
2. Overvej metoder til at reducere utilsigtet aktivering af cyberindflydelseskampagner udført af dine medarbejdere eller din forretningspraksis. Det omfatter at reducere mængden af ressourcer til kendte udenlandske propagandasteder.
3. Understøt digitale kompetencer og medborgerskabskampagner som en nøglekomponent, der hjælper samfund med at forsvare sig mod propaganda og udenlandsk indflydelse.
4. Engager dig direkte i grupper, der er relevante for din branche og arbejder på at håndtere indflydelsesaktiviteter.

Slutnoter

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. Forsvare Ukraine: Tidlige erfaringer fra cyberkrigen (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Det russiske udenrigsministeriums talskvinde Maria Zakharova: 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. Russiske påstande om Kremenchuk kontra beviserne – bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi's video er manipuleret | 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 og Kristjan Peterson, oktober 2020

Cyber-robusthed

Forståelse af farerne og fordelene ved modernisering bliver afgørende for en holistisk tilgang til robusthed.

En oversigt over

cyberrobusthed

Cybersikkerhed er en vigtig katalysator for teknologisk succes. Innovation og øget produktivitet kan kun opnås ved at introducere sikkerhedsforanstaltninger, der gør organisationer så modstandsdygtige som muligt over for moderne angreb.

Pandemien har udfordret os til at omdesigne vores sikkerhedspraksis og -teknologier for at beskytte Microsofts medarbejdere, uanset hvor de arbejder. I det forløbne år fortsatte trusselsaktører med at udnytte sårbarheder, der blev eksponeret under pandemien og overgangen til et hybridarbejdsmiljø. Siden da har vores primære udfordring været at håndtere udbredelsen og kompleksiteten af forskellige angrebsmetoder og øget nationalstatsaktivitet.

Effektiv cyberrobusthed kræver en holistisk, tilpasningsdygtig tilgang for at modstå nye trusler mod kernetjenester og infrastruktur.

Få mere at vide på side 89

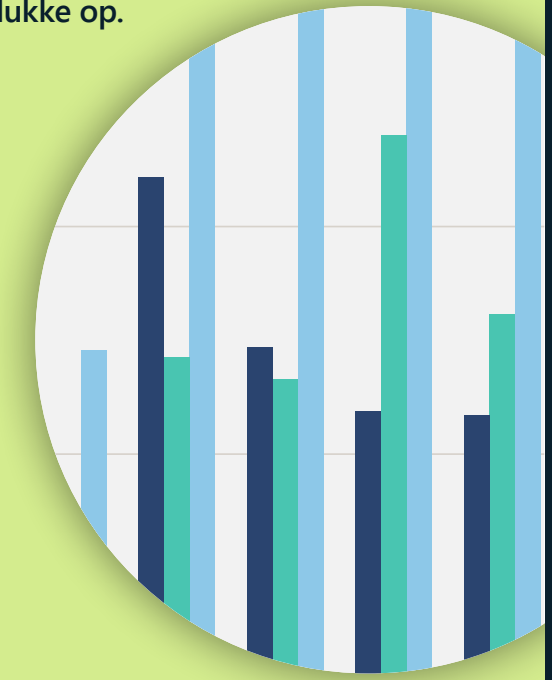
Moderniserede systemer og arkitekturer er vigtige for håndtering af trusler i en hyperforbundet verden.

Få mere at vide på side 90

Grundlæggende sikkerhedsforhold er en afgørende faktor for effektivitet af avancerede løsninger.

Få mere at vide på side 92

Selvom adgangskodebaserede angreb stadig er den vigtigste årsag til kompromitterede identiteter, begynder andre typer angreb at dukke op.



Få mere at vide på side 93

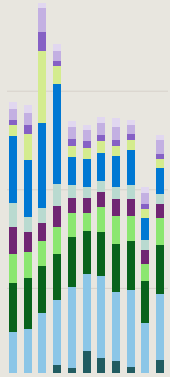
Den menneskelige dimension af robusthed over for cyberindflydel-sesaktiviteter er vores evne til at samarbejde.

Få mere at vide på side 102

Langt størstedelen af vellykkede cyberangreb kan forhindres ved brug af grundlæggende sikkerhedshygiejne.

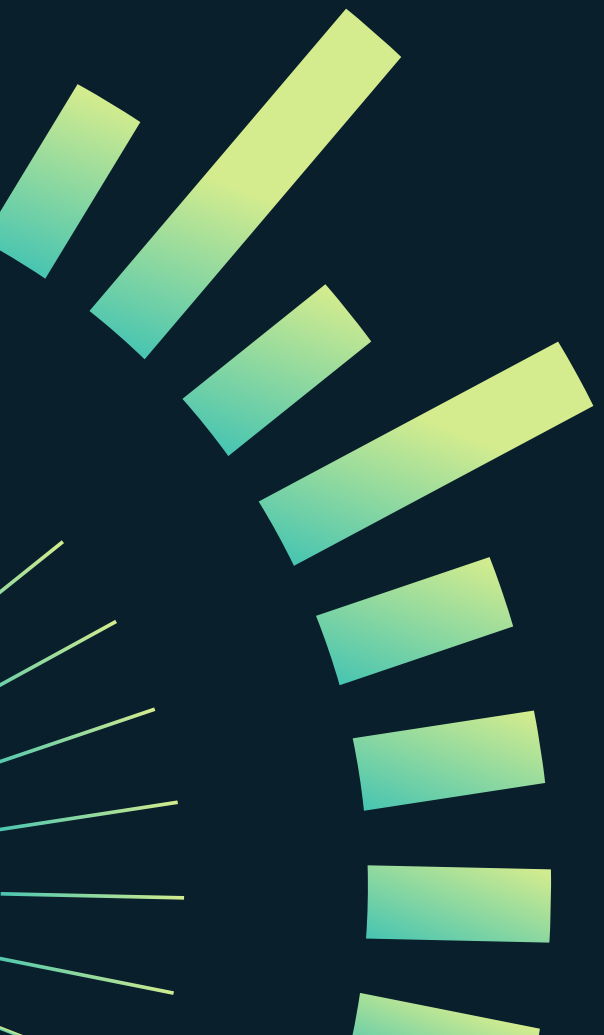
Få mere at vide på side 108

I løbet af det seneste år oplevede verden DDoS-aktivitet, der var uden fortilfælde i volumen, kompleksitet og frekvens.



Få mere at vide på side 98

Introduktion



Pandemien har udfordret os til at omdesigne vores sikkerhedspraksis og -teknologier for at beskytte Microsofts medarbejdere, uanset hvor de arbejder. I det forløbne år fortsatte trusselsaktører med at udnytte sårbarheder, der blev eksponeret under pandemien og overgangen til et hybridarbejdsmiljø. Siden da har vores primære udfordring været at håndtere udbredelsen og kompleksiteten af forskellige angrebsmetoder og øget nationalstatsaktivitet.

Den digitale trusselaktivitet og niveauet af sofistikering af cyberangreb vokser hver dag. Mange af nutidens avancerede angreb fokuserer på at kompromittere identitetsarkitekturer, supply chains og tredjeparter med forskellige grader af sikkerhedskontroller. Vi har især bemærket, at phishingidentitetsangreb er en klar og aktuel trussel. Men disse angrebstyper lykkes generelt ikke, hvis du har en god identitetsstyring, phishingkontrol og endpoint-managementpraksis. Derfor skal vi huske det grundlæggende: 98 % af angrebene kan stoppes med grundlæggende hygiejnemæssige foranstaltninger. Hos Microsoft administrerer vi identiteter og enheder som en del af vores Nul tillid-tilgang, som inkluderer mindst privilegeret adgang og phishingresistente legitimationsoplysninger for effektivt at stoppe trusselsaktører og beskytte vores data.

I dag kan selv trusselsaktører, der mangler sofistikerede tekniske færdigheder, iværksætte utroligt ødelæggende angreb, da adgang til avancerede taktikker, teknologi og procedurer alle er blevet en del af cyberkriminalitetsøkonomien. Krigen i Ukraine demonstrerede, hvordan nationalstatsaktører har eskaleret deres offensive cyberaktiviteter gennem øget brug af ransomware. Ransomware er nu en sofistikeret branche med trusselsaktører, der bruger dobbelte eller tredobbelte afpresningsmetoder til at få betaling, og udviklere, der tilbyder ransomware som en tjeneste (RaaS). Med RaaS udnytter trusselsaktører et tilknyttet netværk til at udføre angreb, hvilket sænker adgangsbarrieren for mindre kvalificerede cyberkriminelle og i sidste ende udvider puljen af angribere.

Som følge deraf har Microsoft designet et program til at eliminere ransomware. Målet med programmet er at afhjælpe mangler i kontroller og dækning, bidrage til funktionsforbedringer for tjenester og udvikle genoprettelsesstrategiplaner til vores sikkerhedsoperationer og tekniske teams i tilfælde af et ransomware-angreb.

Nylige angreb på supply chain og tredjepartsudbydere antyder et stort vendepunkt i branchen. De afbrydelser, som disse angreb medfører for vores kunder, partnere, offentlige myndigheder og Microsoft, fortsætter med at stige, hvilket illustrerer vigtigheden af at fokusere opmærksomheden på cyberrobusthed og samarbejde mellem sikkerhedsinteressenter. Modstanderne målretter også mod on-premises-systemer, hvilket fremmer behovet for, at organisationer håndterer sårbarheder forbundet med ældre systemer ved at modernisere og flytte infrastruktur til cloud-løsningen, hvor sikkerheden er mere robust.

Vi lever i en tidsalder, hvor sikkerhed er en vigtig facilitator til teknologisk succes. Innovation og øget produktivitet kan kun opnås ved at introducere sikkerhedsforanstaltninger, der gør organisationer så modstandsdygtige som muligt over for moderne angreb. Efterhånden som der kommer flere digitale trusler, og de udvikler sig, er det afgørende at indbygge cyberrobusthed i alle organisationers struktur.

Bret Arsenault
Chief Information Security Officer

Cyberrobusthed: Et nødvendigt fundament for et forbundet samfund

Revolutionen inden for digital teknologi har gjort, at organisationer transformeres til at blive stadig mere forbundne, både på den måde de opererer, og de tjenester de tilbyder. Efterhånden som truslerne i cyberlandskabet vokser, er det lige så vigtigt at indbygge cyberrobusthed i organisationens struktur som økonomisk og driftsmæssig robusthed.

Digital transformation har for evigt forandret den måde, som organisationer interagerer med kunder, partnere, medarbejdere og andre interessenter på. Nye teknologier giver enorme muligheder for at interagere med mennesker, transformere produkter og optimere driften. Pandemien accelererede digitaliseringen ved at fremme innovative teknologier, som giver folk mulighed for at samarbejde på nye måder og hvor som helst.

Efterhånden som cybertrusler bliver endemiske, bliver det vanskeligere at forhindre dem i at kompromittere en organisation i vores "altid forbundne" verden. Cyberrobusthed er en organisations evne til at fortsætte driften og bevare vækstaccelerationen på trods af angrebene. Forebyggende foranstaltninger skal afvejes mod overlevelses- og genoprettelsesfunktioner, og offentlige myndigheder og virksomheder udvikler omfattende modeller, der rækker ud over sikkerhed og beskyttelse af personlige oplysninger for at beskytte aktiver, data og andre ressourcer som en del af cyberrobusthed.

Udvikling af en holistisk tilgang til cyberrobusthed

Cyberrobusthed kræver en holistisk, tilpasningsdygtig og global tilgang, der kan modstå udvikling af trusler mod kernetjenester og infrastruktur, inklusive:

- Grundlæggende cyberhygiejne som beskrevet i vores klokkekurve for cyberrobusthed.
- Forståelse af og styring af risikoen/fordelen ved at gå på kompromis med digital transformation.
- Responsfunktioner i realtid, der muliggør proaktiv registrering af trusler og sårbarheder.
- Beskyttelse mod kendte angreb og forebyggende aktivitet mod nye og forventede angrebsvektorer, herunder muligheden for automatisk afbødning.
- Reduceret indvirkning af angreb og katastrofer gennem fejlisolering og segmentering
- Automatiseret genoprettelse og redundans i tilfælde af afbrydelser.
- Prioritering af operationelle test for at finde mangler og forstå fælles ansvarsområder og afhængigheder af eksterne ressourcer, f.eks. cloudbaserede sikkerhedsløsninger.

Et effektivt cyberrobusthedsprogram starter med grundlæggende ressourcer, som at forstå tilgængelige tjenester og have et pålideligt katalog over ressourcer, der kan tilkaldes i tilfælde af en afbrydelse. På basis af disse oplysninger skal programmet være i stand til at vurdere sin egen effektivitet, måle ydeevnen af kritiske tjenester og deres afhængigheder, teste og validere funktioner for on-premises- og cloud-tjenester og levere kontinuerlige forbedringer i hele organisationens digitale livscyklus.

For at kunne give en holistisk tilgang samarbejder vi med organisationer om at identificere deres vigtigste on-premises- og onlinetjenester, forretningsprocesser, afhængigheder, personale, forhandlere og leverandører. Vi forsøger også at identificere aktiver og ressourcer, der er knyttet til kundernes og markedets forventninger, lovgivningsmæssige og kontraktlige forpligtelser samt interne aktiviteter. Når disse kritiske ressourcer er identificeret, bør parallelle bestræbelser opdage og overvåge trusler, afbrydelser, potentielle angrebsvektorer samt system- og processårbarheder. Evnen til at gøre dette under den nuværende mangel på kompetencer kræver streng prioritering baseret på den samlede risiko for organisationen.

Denne type af holistisk tilgang skal kunne tilpasses i et trusselslandskab under konstant forandring med det mål at fremme målbar forbedring af ydeevnen, reduceret tid til at opdage, reagere og genoprette og reduceret radius for indvirkning i tilfælde af afbrydelser. Tilgangen skal også anerkende truslernes voksende forbundethed. En sikkerhedshændelse kan for eksempel resultere i et databrud med konsekvenser for beskyttelsen af personlige oplysninger, hvilket kræver, at mange interne og eksterne teams samarbejder for at reagere hurtigt og minimere indvirkningen.

Cyberrobusthed er en virksomheds evne til at fortsætte driften og opretholde accelerationen af væksten på trods af afbrydelser, inklusive cyberangreb.

Handlingsrettet indsigt

1. Opbyg og håndter teknologisystemer, der begrænser konsekvenserne af et brud og giver dem mulighed for at fortsætte med at fungere sikkert og effektivt, selv hvis et brud lykkes. Fokuser på almindelige kritiske aktiver, understøt smidighed og opbyg tilpasningsevne (f.eks. hybrid og multi-cloud, multiplatform), reducer angrebsflader (fjern f.eks. ubrugte applikationer og for store adgangsrettigheder), antag at ressourcer er kompromitteret og forvent, at fjenderne udvikler sig.
2. Når du planlægger digitale projekter, skal du overveje potentielle trusler sideløbende med muligheder og fælles ansvar for robusthed for hele den digitale teknologi-supply chain, herunder cloudbaserede sikkerhedsløsninger.
3. Byg systemer for at integrere sikkerhed gennem design, og tag skridt til at forudse, opdage, modstå, tilpasse og reagere på fremtidige nye trusler.
4. Sørg for, at virksomhedens ledere rådfører sig med sikkerhedsteams, når det er nødvendigt, for at forstå de risici, der er forbundet med nye udviklinger. Tilsvarende bør sikkerhedsteams overveje forretningsmål og rådgive ledere om, hvordan de kan indfri dem på en sikker måde.
5. Sørg for, at der er etableret klare operationelle praksisser og procedurer for organisatorisk robusthed for cyberhændelser.

Vigtigheden af at modernisere systemer og arkitektur

Når vi udvikler nye funktioner til en hyperforbundet verden, skal vi håndtere truslerne fra ældre systemer og software.

Ældre systemer – dem, der blev udviklet før moderne forbindelsesværktøjer som smartphones, tablets og cloud-tjenester blev normen – udgør en risiko for en organisation, der stadigvæk bruger dem. Denne risikoeksponering forstærkes af resultaterne fra Microsoft Security Services for Incident Response-teamet, en sikkerhedsekspertgruppe, der hjælper kunderne med reaktion på og genoprettelse efter angreb.

I løbet af det sidste år var de problemer, der blev fundet blandt kunder, som var i gang med genoprettelse efter angreb, relateret til seks kategorier som vist i diagrammet på denne side. Den følgende side skitserer handlingsrettede trin, der kan tages for at forbedre robustheden.

Over 80 % af sikkerhedshændelser kan spores tilbage til nogle få manglende elementer, der kan håndteres via moderne sikkerhedsmetoder.

Vigtige problemer, der påvirker cyberrobusthed

Dette diagram viser, hvor stor en procentdel af de påvirkede kunder, der mangler grundlæggende sikkerhedskontroller, som er afgørende for at øge organisationens cyberrobusthed. Resultaterne er baseret på Microsoft arbejde i løbet af det seneste år.

"Ledere bør betragte cyberrobusthed som et kritisk aspekt af virksomhedens robusthed. De bør planlægge cyberafbrydelser på samme måde, som de gør med naturkatastrofer eller andre uforudsete begivenheder, og samle interne interessenter som drift, kommunikation, jura med flere for at udarbejde strategier. Hvis de gør det, vil det hjælpe med at sikre, at organisationerne får deres kritiske forretningssystemer tilbage online så hurtigt som muligt for at genoptage den normale forretningsdrift.

Men det stopper ikke her.
Da mange organisationer er afhængige af tredjepartsleverandører og tjenesteudbydere, bør lederne udvide planlægningen af cyberrobusthed til hele deres værdikæde for yderligere at sikre forretningskontinuitet og robusthed".

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

Vigtigheden af at modernisere systemer og arkitektur

Fortsat

Der er tydelige områder, som organisationer kan håndtere for at modernisere deres tilgang og beskyttelse mod trusler:

Problem	Handlingsrettede trin
Usikker konfiguration af identitetsudbyder Fejlkonfiguration og eksponering af identitetsplatforme og dens komponenter er en almindelig metode til at få uautoriseret adgang med store rettigheder.	Følg grundlinjerne for sikkerhedskonfiguration og de bedste fremgangsmåder, når du implementerer og vedligeholder identitetssystemer som f.eks. AD- og Azure AD-infrastrukturen. Implementer adgangsbegrænsninger ved at gennemtvinge opdeling af rettigheder, mindst privilegeret adgang og anvendelse af arbejdsstationer med privilegeret adgang til administration af identitetssystemer.
Utilstrækkelige rettigheder til adgang og kontrol af tværgående bevægelser Administratorer har overdrevent mange tilladelser i det digitale miljø og eksponerer ofte administrative legitimationsoplysninger på arbejdsstationer, der er underlagt internet- og produktivitetsrisici.	Beskyt og begræns administrativ adgang for at gøre miljøet mere robust og begrænse omfanget af et angreb. Brug privilegerede adgangsstyringskontroller, som JIT-adgang (just-in-time) og JEA-administratoradgang (just-enough access).
Ingen multifaktorgodkendelse (MFA) Nutidens angribere bryder ikke ind, de logger på.	MFA er en meget vigtig og grundlæggende brugeradgangskontrol, som alle organisationer bør aktivere. Kombineret med betinget adgang kan MFA være uvurderlig til bekæmpelse af cybertrusler.
Sikkerhedsaktiviteter med lav modenhed De fleste berørte organisationer benyttede traditionelle trusselregistreringsværktøjer og manglede relevant indsigt til rettidig respons og afhjælpning.	En omfattende trusselregistreringsstrategi kræver investeringer i udvidet registrering og respons (XDR) og moderne cloudbaserede værktøjer, der bruger maskinlæring til at adskille støj fra signaler. Moderniser sikkerhedsdriftværktøjer ved at indarbejde XDR, som kan give dyb sikkerhedsindsigt på tværs af hele det digitale landskab.
Manglende databeskyttelseskontrol Organisationer kæmper fortsat med at sammensætte holistiske datasikkerhedskontroller, der har fuld dækning på tværs af alle dataplaceringer og forbliver effektive gennem hele informationslivscyklussen og er afstemt med, hvor virksomhedskritiske data er.	Identificer dine kritiske virksomhedsdata, og hvor de er placeret. Gennemgå processer for informationslivscyklussen, og håndhæv databeskyttelse, samtidig med at forretningskontinuiteten sikres.
Begrænset indførelse af moderne sikkerhedsstrukturer Identitet er den nye sikkerhedsgrænse, der giver adgang til forskellige digitale tjenester og computermiljøer. Ved at integrere Nul tillid-principper, applikationssikkerhed og andre moderne cyberstrukturer kan organisationer proaktivt håndtere risici, som de ellers ville have svært ved at forestille sig.	Nul tillid-strukturer håndhæver begreberne mindste rettighed, eksplicit bekræftelse af al adgang og det faktum, at ressourcer kan kompromitteres. Organisationer bør også implementere sikkerhedskontroller og sikkerhedsrutiner i DevOps- og applikationslivscyklusprocesser for at opnå højere sikkerhedsniveauer i deres virksomhedssystemer.

Grundlæggende sikkerhedsforhold er en afgørende faktor for effektivitet af avancerede løsninger

Gennem vores analyse opdagede vi en udbredelse af almindelige blinde vinkler i organisationers forsvar, der gjorde det muligt for angribere at få indledende adgang, etablere et brohoved og udføre et angreb, selv under tilstedeværelse af avancerede sikkerhedsløsninger.

I mange tilfælde bestemmes resultatet af et cyberangreb, længe før angrebet starter. Angribere udnytter sårbare miljøer til at få indledende adgang, udføre overvågning og skabe kaos via tværgående bevægelser, kryptering eller eksfiltrering. Det at kunne stoppe en angriber på et tidligt tidspunkt øger i høj grad muligheden for at reducere den samlede indvirkning.

Microsoft undersøgte specifikke konfigurationer i sikkerhedsforhold for at identificere de mest almindelige mangler i praksis i disse miljøer. Dette gjorde det muligt for os at se de mest almindelige sårbarheder, der blev udnyttet under menneskeskabte ransomware-angreb, og som gjorde det muligt for trusselsaktørerne at få adgang til og bevæge sig uopdaget rundt på et netværk.

Grundlæggende sikkerhedskonfigurationer skal aktiveres

En organisations enheder, der ikke er onboardet eller er forældede (både med hensyn til sårbarheder og status for sikkerhedsagenter), fungerer som potentielle indgangspunkter og adgangsruter for angribere. Vi opdagede, at selvom det er et vigtigt skridt, at organisatoriske enheder er onboardet med en opdateret EDR-registrering (endpoint detection and response)[1] og EPP-løsning (endpoint protection platform)[2], er der ikke garanti for, at det vil stoppe ransomware.

Avancerede løsninger som EDR og EPP er meget vigtige for at opdage en angriber tidligt i angrebsstrømmen og for at kunne aktivere automatisk afhjælpning og beskyttelse. Men da disse avancerede løsninger er afhængige af en grundlæggende evne til at registrere et angreb, kræver de, at grundlæggende sikkerhedskonfigurationer er aktiveret. Faktisk observerede vi en udbredt forekomst af etablerede avancerede løsninger, som blev undermineret af manglende grundlæggende sikkerhedskonfigurationer.

Bedste praksis i sikkerhedskonfigurationer er en bedre indikator for robusthed end SOC-analytikeres (Security Operations Center) responstid

Vi observerede en reduktion på 70 % i den tid, det tager en SOC-analytiker at se og reagere på en relevant advarsel over en periode på seks måneder på tværs af vores kunder og partnere. Denne øgede bevidsthed er et godt tegn. Men mens sikkerhedskonfigurationens synlighed har forbedret SOC-analytikernes ydeevne, har synlighed i produkter gennem onboarding og opdatering af organisationens enheder vist sig at være en meget mere effektiv forudsigelig indikator med hensyn til forebyggende arbejde.

Risiko forbundet med ukendte enheder

I modsætning til cloud-netværk, hvor kunderne ved, hvilke aktiver der kører på hvilke operativsystemer, kan on-premises-netværk indeholde en række forskellige enheder som IoT, stationære computere, servere og netværksenheder, der ikke overvåges eller administreres af organisationen.

Et gennemsnitligt virksomhedsnetværk har flere end 3.500 tilsluttede enheder, der ikke er beskyttet af en EDR-agent og kan have adgang til virksomhedens ressourcer eller endda meget værdifulde aktiver. MDE (Microsoft Defender for Endpoint) bruger netværksinspektion til at opdage enheder og levere enhedsklassifikationsoplysninger for dem, der er tilsluttet netværket, som f.eks. enhedsnavn, operativsystemsfordeling og enhedstype.

3.500

Gennemsnitligt antal tilsluttede enheder i en virksomhed, der ikke er beskyttet af en endpoint-registrerings- og responsagent.

For enheder, der ikke understøttes af nogen EDR-agent, bør du i det mindste være opmærksom på deres eksistens og handle for at beskytte dem ved at vurdere sårbarheder og begrænse netværksadgang.

Handlingsrettet indsigt

1. Selv avancerede løsninger kan undermineres ved ikke at bruge grundlæggende sikkerhed-skonfigurationer.
2. Invester i de bedste praksisser i sikkerhedskonfigurationer for at beskytte mod fremtidige angreb. Disse grundlæggende indstillinger giver et enormt investeringsafkast med hensyn til en organisations evne til at forsvare sig mod angreb.
3. Onboard alle relevante enheder for en EDR-løsning.
4. Sørg for at opdatere dine sikkerhedsagenter og sikre beskyttelse mod manipulation for at øge produktets synlighed og beskyttelsesfordele.

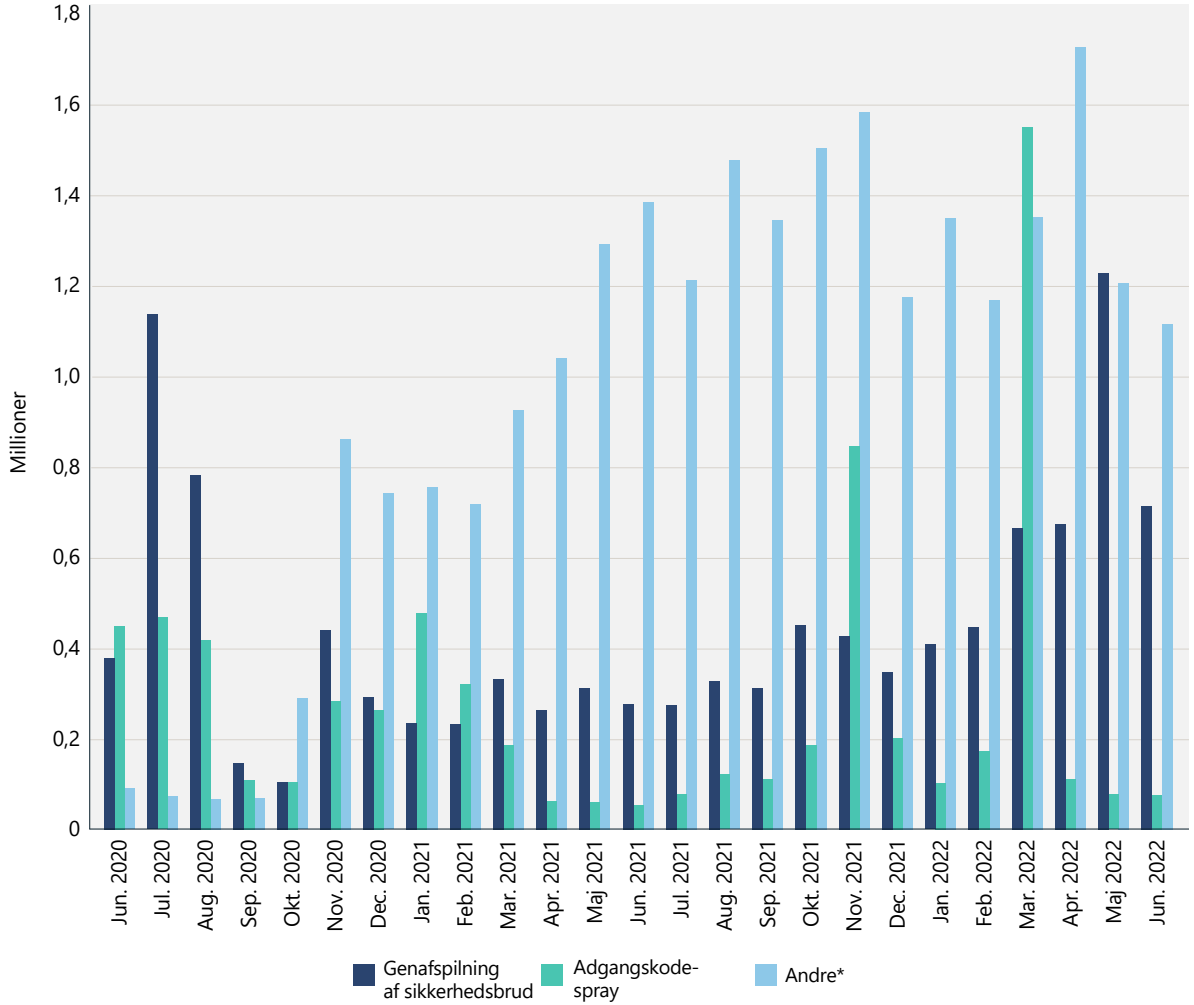
Vedligeholdelse af identitetssundhed er fundamentalt for organisationsmæssig trivsel

Beskyttelse af identitet er vigtigere end nogensinde. Selvom adgangskodebaserede angreb stadig er den vigtigste årsag til kompromitterede identiteter, begynder andre typer angreb at dukke op. Antallet af sofistikerede angreb fortsætter med at vokse i forhold til den tidligere norm for adgangskodespredning og efterligninger af sikkerhedsbrud.

Adgangskodebaserede angreb er stadig almindelige, og flere end 90 % af konti kompromitteret via disse metoder er ikke beskyttet med stærk godkendelse. Med stærk godkendelse bruges mere end én faktor til godkendelse, for eksempel adgangskode + SMS og FIDO2-sikkerhedsnøgler.

Vi har set en stigning i målrettede spredningsangreb med adgangskode med meget store stigninger i angriberens trafikmængde fordelt på tusindvis af IP-adresser.

Brugere kompromitteret efter angrebskategori



Brugere kompromitteret pr. måned efter angrebskategori. Mængden af spredningsangreb med adgangskode varierede meget, som det kan ses af stigningerne i november 2021 og marts 2022. Disse stigninger repræsenterer tusindvis af brugere og tusindvis af berørte IP-adresser. *"Andet" indikerer andre angreb end adgangskodespredning og gentagelse af brud, herunder phishing, malware, man-in-the-middle-angreb, kompromittering af on-premises-tokenudstedere og andre. KIlde: Azure AD Identity Protection.

4.500

I den tid, det tager dig at læse dette, har vi forsvaret os mod 4.500 adgangskodeangreb.

Vedligeholdelse af identitetssundhed er fundamentalt for organisationsmæssig trivsel

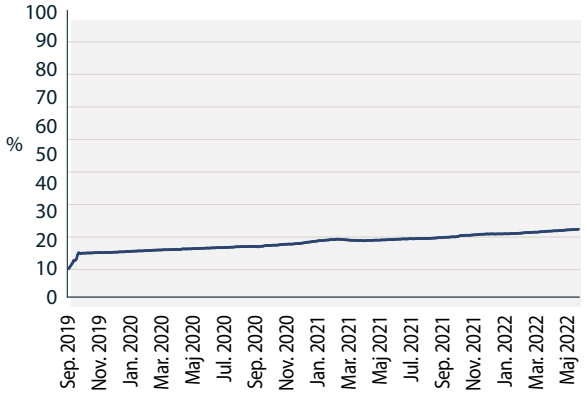
Fortsat

Benyttelse af stærk godkendelse

Som en positiv bemærkning ser vi en støt stigning i indførelsen af stærk godkendelse blandt vores Azure AD-virksomhedskunder (Azure Active Directory (Azure AD). For Azure AD steg månedlige stærke godkendelsesbrugere fra 19 til 26 % i løbet af det seneste år, mens månedlige stærke godkendelsesbrugere for administrative konti steg fra 30 til omkring 33 %.

Denne tendens er positiv, men mange flere skal tilføje stærk godkendelse, før flertallet bruger det. Kunder, der ikke allerede bruger stærk godkendelse i deres miljøer, bør begynde at planlægge og implementere stærk godkendelse for at beskytte deres brugere.[3] Mens du designer implementering af stærk godkendelse, bør godkendelse uden adgangskode overvejes, da det giver den mest sikre brugbare oplevelse og eliminerer risikoen for adgangskodeangreb.

Brug af stærk godkendelse
(september 2019-maj 2022)

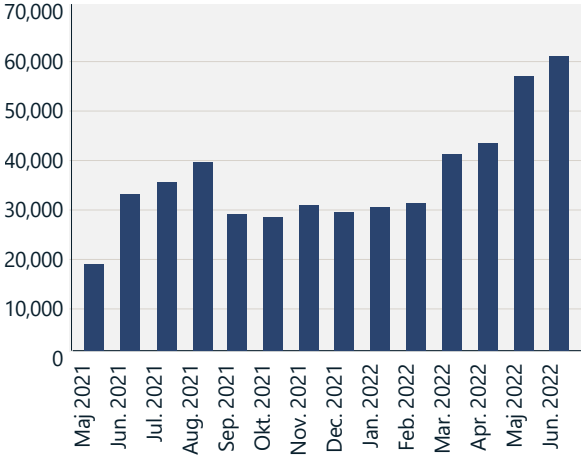


Selvom brugen af stærk godkendelse er fordoblet siden 2019, er det kun 26 % af brugerne og 33 % af administratorerne der benytter det. Kilde: Azure Active Directory.

Støt stigning i genafspilning af token-angreb

Andelen af andre former for angreb steg i 2022. Vi så en stigning i målrettede angreb, der specifikt undgår adgangskodebaseret godkendelse, hvilket mindskede risikoen for registrering. Disse angreb udnytter browser-SSO-cookies (single sign-on) eller opdateringstokens opnået gennem malware, phishing eller andre metoder. I nogle tilfælde vælger angriberne infrastruktur på steder tæt på den påtænkte brugers geografiske placering for yderligere at reducere risikoen for registrering. Vi har oplevet en støt stigning i genafspilning af token-angreb og har nået over 40.000 registreringer pr. måned i Azure AD Identity Protection. Genafspilning af token betyder, at en angriber, der har adgang til dem, benytter et token, der er udstedt til en legitim bruger. Tokenet opnås normalt via malware, for eksempel ved at eksfiltrere cookies fra brugerens browser eller gennem avancerede phishingmetoder.

Antal af registrerede genafspilning af token-angreb



Registrerede genafspilning af token-angreb pr. måned. Kilde: Azure AD Identity Protection, unikke sessioner, der er blevet markeret på grund af unormal registrering af tokener.

Vedligeholdelse af identitetssundhed er fundamentalt for organisationsmæssig trivsel

Fortsat

Udtrække tokener

Mere end malware har angribere brug for legitimationsoplysninger for at nå deres mål Faktisk inkluderer 100 % af alle menneskeskabte ransomware-angreb omfatter stjålne legitimationsoplysninger. Mange sofistikerede indtrængninger involverer legitimationsoplysninger, der er købt på det mørke internet. De blev oprindeligt stjålet af usofistikeret og bredt distribueret malware til tyveri af legitimationsoplysninger. Denne klasse af malware er udviklet til at stjæle tokens, herunder sessionsoplysninger og MFA-krav. Det betyder, at infektioner i hjemmesystemer, hvorfra brugere logger ind på virksomhedsaktiver, kan føre til alvorlige hændelser i virksomhedens netværk.

Angribere kan også udtrække tokens fra ofrenes enheder gennem man-in-the-middle-angreb, hvor ofret klikker på et skadeligt link i en phishingmail eller chatbesked og dirigeres til et websted, der ligner identitetsudbyderens legitime logonside. Faktisk er det en webtjeneste, der er opsat af angriberen, og som videresender og opsnapper al trafik mellem brugeren og identitetsudbyderen. Angriberen kan opsnappe brugernavne og adgangskoder og også videresende MFA-udfordringer. De resulterende tokener, der er udstedt af identitetsudbyderen og opsnappet af angriberen, kan indeholde MFA-krav, som kan bruges af angriberen til at opfylde MFA-kravene.

Microsoft Defender for Cloud-apps har i gennemsnit registreret 895 sådanne angreb pr. måned siden begyndelsen af 2022. Denne form for angreb kan forhindres ved at bruge phishingresistente MFA-faktorer, som certifikatbaseret godkendelse, Windows Hello for Business eller FIDO2-sikkerhedsnøgler.

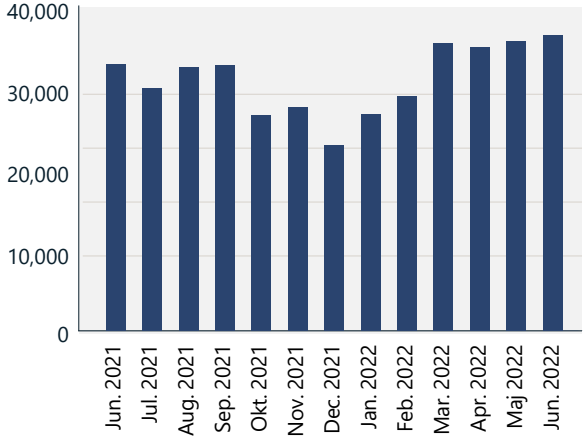
Adgangskodebaserede angreb er den primære metode, som konti kompromitteres med.

MFA-træthed

Ved at bruge konceptet "MFA-træthed" genererer angribere flere MFA-anmodninger til offerets enhed i håb om, at offeret vil acceptere anmodningen enten ved et uheld eller som et resultat af træthed. Dette angreb kan forhindres ved at anvende moderne godkenderapps som Microsoft Authenticator kombineret med funktioner som nummermatchning[4] og aktivering af yderligere kontekst.[5] Azure AD Identity Protection vurderede, at der forekommer 30.000 MFA-træthedsangreb pr. måned.

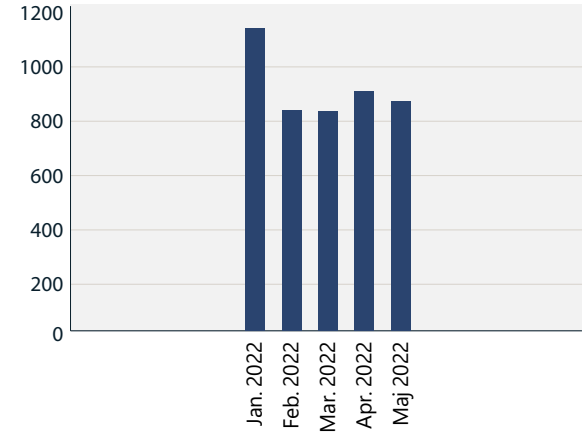
Andelen af sofistikerede angreb fortsætter med at stige, og understreger behovet for phishingresistente faktorer til multifaktorgodkendelse.

Anslåede forekomster af MFA-træthedsangreb



KIlde: Azure AD Identity Protection.

Registrerede forekomster af phishing efterfulgt af man-in-the-middle-angreb



Kilde: Microsoft Defender for Cloud Apps.

Handlingsrettet indsigt

1. Sørg for, at alle konti i organisationen er beskyttet af stærke godkendelse.
2. Godkendelse uden adgangskode tilbyder den mest sikre og brugervenlige oplevelse og eliminerer risikoen for adgangskodeangreb.
3. Deaktiver ældre godkendelse i hele organisationen.
4. Beskyt værdifulde og administrative konti med phishingresistente former for stærk godkendelse.
5. Moderniser fra en on-premises-identitetsudbyder til en cloud-identitetsudbyder, og tilslut alle apps til den cloud-baserede identitetsudbyder for at sikre ensartede brugeroplevelser og sikkerhed.

Links til yderligere oplysninger

- Denne World Password Day overvejer helt at droppe adgangskoder | Microsoft Security

Standardsikker-hedsindstillinger for operativsystem

Med det stadigt skiftende landskab for sikkerhedstrusler er der et stigende behov for computersikkerhed konfigureret som standard til at forbedre cyberrobustheden. Selvom operativsystemets sikkerhed er mere presserende, kompleks og forretningskritisk end nogensinde før, kan det være en udfordring at få styr på det og administrere det.

Tidligere inkluderede computer- og enhedssikkerhed indbyggede sikkerhedsfunktioner, som kunden eller it-medarbejderen forventedes at konfigurere til deres eget ønskede niveau. Denne tilgang er ikke længere tilstrækkelig, da angribere bruger mere avancerede værktøjer inden for automatisering, cloud-infrastruktur og fjernadgangsteknologier til at nå deres mål. Det er blevet afgørende, at alle sikkerhedslag, fra chippen til cloud-løsningen, konfigureres som standard. Microsoft konfigurerer nu Windows-operativsystemsikkerheden som standard.[6]

Kunder, der ønsker at forsvare sig selv – i dybden med en lagdelt sikkerhedsposition, nye sikkerhedsfunktioner, regelmæssige og konsekvente programrettelser og opdateringer samt sikkerhedstræning og sikkerhedsbevidsthed til at rapportere phishing og anden svindel – kan forvente mindre malware.

For at forenkle forsvaret i dybden har Windows 11 tæt integreret hardware- og softwarebeskyttelse aktiveret som standard, inklusive hukommelsesintegritet, Secure Boot og Trusted Platform Module 2.0. Windows 10-brugere på kompatibel hardware kan også aktivere disse funktioner i appen Windows-indstillinger eller i BIOS-menuen.

Generelt har ældre enheder ofte ikke så god tilpasning mellem hardwaresikkerheds- og softwaresikkerhedsteknikker. For enheder, hvor sikkerheden ikke er aktiveret som standard, kan den konfigureres manuelt i indstillinger, hvor det er muligt.[7]

For enheder, hvor sikkerhed ikke er aktiveret som standard, anbefaler Microsoft at konfigurere det manuelt i indstillinger, hvor det er muligt.

Vær proaktiv med at anvende løbende operativsystem-opdateringer og sikkerhedsrettelser, der beskytter gennem hele hardware- og softwarelivscyklussen.

Handlingsrettet indsigt

1. Brug en løsning uden adgangskode, der binder legitimationsoplysninger i Trusted Platform Module. Søg specifikt efter en løsning uden adgangskode, der opfylder branchestandarden for FIDO-alliancer (Faster Identity Online)[8].
2. Udfør rettidig oprydning af alle ubenyttede og forældede eksekverbare data på organisationers enheder.
3. Beskyt dig mod avancerede firmwareangreb ved at aktivere hukommelsesintegritet, Secure Boot og Trusted Platform Module 2.0, hvis det ikke er aktiveret som standard. Dette styrker opstart ved hjælp af funktioner, der er indbygget i moderne CPU'er.
4. Aktivér datakryptering og beskyttelse af legitimationsoplysninger.
5. Aktivér applikations- og browserkontroller for at aktivere avanceret, indbygget beskyttelse mod applikationer, der ikke er tillid til, og andre udnyttelser.
6. Aktivér beskyttelse af hukommelsesadgang som et forsvar mod almindelige fysiske angreb, f.eks. en person, der tilslutter en skadelig enhed i eksternt tilgængelige porte.

Links til yderligere oplysninger

- Windows Security Book | Commercial
- Nye sikkerhedsfunktioner til Windows 11 hjælper med at beskytte hybridarbejde | Microsoft Security Blog

Centralitet af software-supply chain

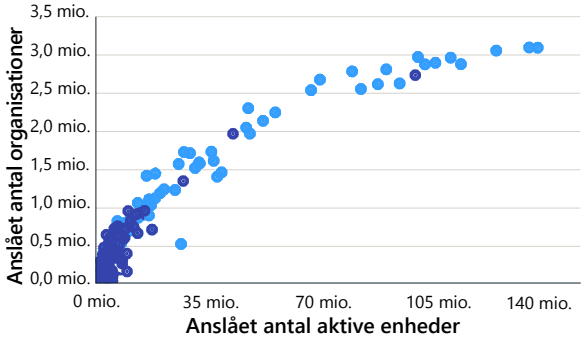
Angreb mod tredjepartsapps, plugins og udvidelser kan udhule kundernes tillid til leverandører, der spiller en central rolle i forsyningsøkosystemet. Brug af netværksteori til at se på softwarens centralitet gør det lettere at se vigtigheden af programrettelser, især for centrale apps.

Windows App-netværket, der består af 18 millioner eksekverbare filer installeret og brugt af fem millioner organisationer, giver et overblik over vores softwareøkosystem. Af de 100.000 mest benyttede applikationer er 97 % produceret af tredjepartsorganisationer, hvis opdateringer og sikkerhedsrettelser vedligeholdes af dem. Dette illustrerer to vigtige egenskaber ved vores økosystem af kommercielle applikationer.

Den første er centraliteten i økosystemet for kommercielle Windows-applikationer. Kun de 100.000 (ud af 18 millioner) mest populære applikationer anvendes på 1.000 eller flere enheder. Med andre ord har lidt over en halv procent af disse applikationer denne form for vidtrækkende effekt på enhedens økosystem.

For det andet styres disse applikationer på en række forskellige måder. De 10.000 softwareudbydere administrerer opdateringer og sikkerhedsrettelser til disse mest udbredte kommercielle applikationer. Dette viser den gensidige afhængighed, som en virksomhed har af et mangfoldigt sæt af softwareleverandørers sikkerheds-, overholdelses- og styringskontroller.

Kommerciel indtrængen af mest anvendte applikationer.



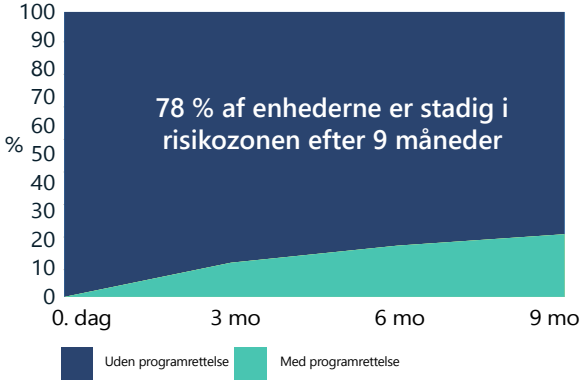
De mest populære applikationer bruges af millioner af organisationer og på millioner af enheder. Da de næsten er allestedsnærværende, er modstanderne konstant på udkig efter sårbarheder i disse applikationer, som kan påvirke millioner af brugeres enheder.

Vi ser millioner af kommercielle enheder, der stadig bruger sårbare applikationsversioner mange måneder efter udgivelse af programrettelser eller endda år efter, at produktsupport er afsluttet. For eksempel er der mere end en million aktive kommercielle Windows-enheder, der kører en version af en PDF-læser, der ikke har været understøttet siden 2017.

Gamle versioner af applikationer, der ikke understøttes, anvendes stadig på millioner af kommercielle enheder. Som et resultat er organisationer i fare for at have sårbarheder, der ikke vil blive rettet.

For understøttede applikationsversioner ser vi en udjævning af den hastighed, hvormed kritiske programrettelser indføres, hvilket er det modsatte af den tendens, der fremmer robusthed. I stedet bør kurven vise en eksponentiel stigende indførelse af programrettelser måned for måned for at opnå den nødvendige robusthed.

Hastighed for implementering af vigtige programrettelser



Efter at have undersøgt en kritisk sårbarhed, der påvirkede 134 versioner af et bestemt sæt browsere, opdagede vi, at 78 %, eller millioner af enheder, stadig brugte en af de berørte versioner ni måneder efter, at programrettelsen blev udgivet.

Vi brugte InterpretML-værktøjssættet[9] til at identificere kendetegn, der er forbundet med organisationer, der er mere tilbøjelige til at have enheder med ældre versioner af applikationerne. De vigtigste af disse indikatorer omfattede: få timers engagement på enheder, geografiske områder som Asien, Stillehavsområdet og Latinamerika og brancher som bilindustrien, kemikalier, telekommunikation, transport og logistik, sygeforsikringsvirksomheder (skadesbehandlere) og forsikring.

Vedligeholdelse af softwarerobusthed bør omfatte regelmæssig deaktivering eller afinstallation af ubenyttede applikationer.

En organisations sikkerhed og overholdelse af regler og standarder afhænger af virksomhedens egen indsats og af softwareleverandørernes indsats.

Handlingsrettet indsigt

1. Udfør rettidige opdateringer af alle applikationer og endpoints i hele din organisation.
2. Udfør rettidig oprydning af alle ubenyttede og forældede eksekverbare data på organisationers enheder.

Links til yderligere oplysninger

- Microsoft Intune-dokumentation | Microsoft Docs
- Administrer applikationer | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- Oss Secure supply chain-struktur | Microsoft Security Engineering
- Microsoft Open Source Software Secure supply chain-struktur | Github

Opbygning af robusthed over for nye DDoS-, webapplikations- og netværksangreb

Accelereret digital transformation har sat en stopper for den traditionelle perimetermodel for netværk og sikkerhed. Flytning til cloud-løsningen betyder, at virksomheder skal indføre cloudbaseret netværkssikkerhed for at beskytte digitale aktiver.

Kompleksiteten, hyppigheden og omfanget af angrebene vokser fortsat og er ikke længere begrænset til højtider, men finder nu sted hele året rundt. Dette fremhæver vigtigheden af kontinuerlig beskyttelse ud over traditionelle spidsbelastningsperioder.

DDoS-angreb (Distributed Denial of Service)

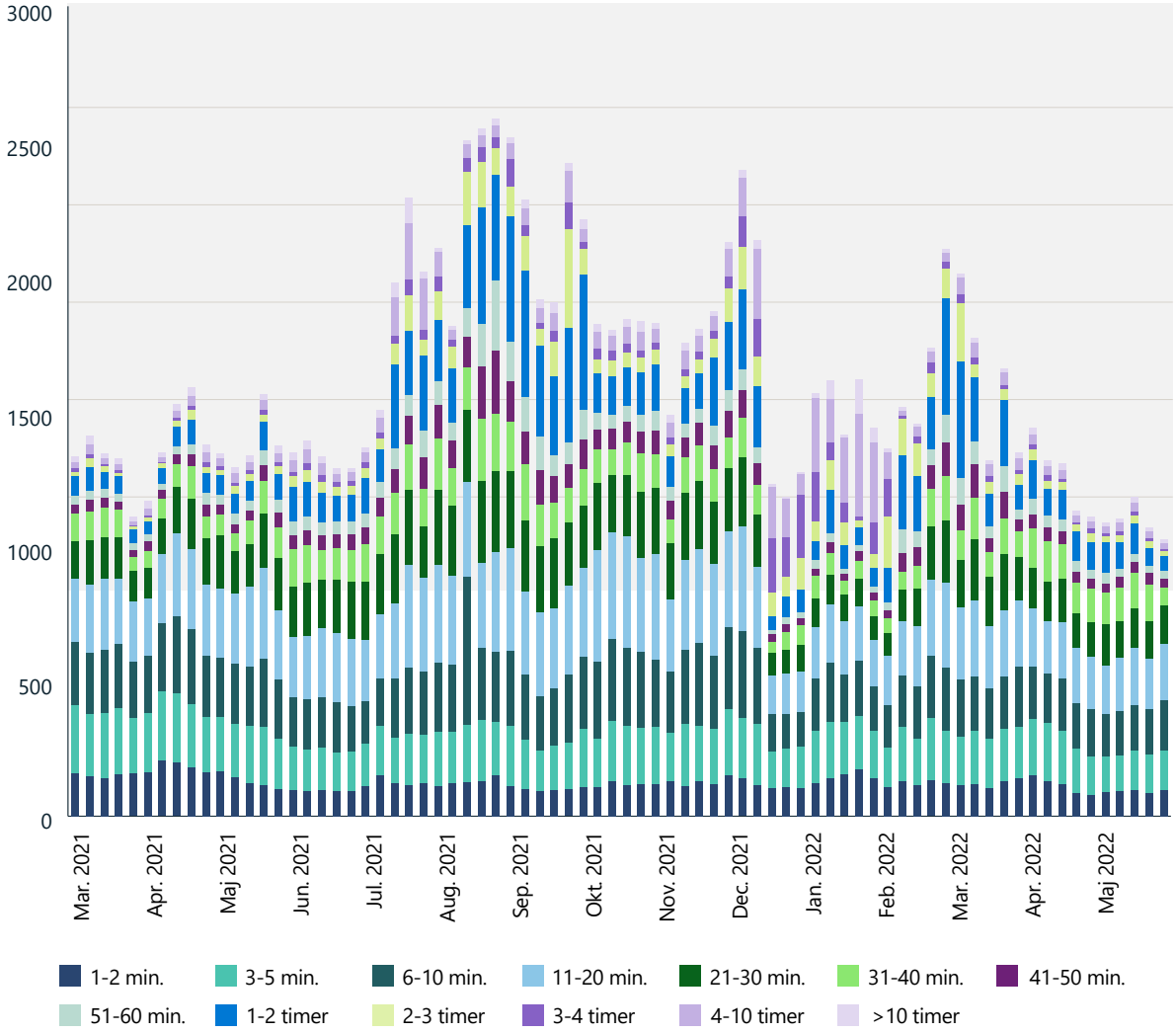
I løbet af det seneste år oplevede verden DDoS-aktivitet, der var uden fortilfælde i volumen, kompleksitet og frekvens. Denne DDoS-eksplosion blev drevet af en betydelig vækst i nationalstatsangreb og en fortsat spredning af billige DDoS-tjenester, der kan købes. Microsoft afbødede i gennemsnit 1.955 angreb pr. dag, en stigning på 40 % i forhold til det foregående år. Tidligere forekom det maksimale antal angreb normalt i højtiden i slutningen af året. I år blev der registreret flest den 10. august 2021. Dette kan indikere et skift til angreb hele året og fremhæver vigtigheden af kontinuerlig beskyttelse ud over traditionelle spidsbelastningsperioder.

I november 2021 stoppede Microsoft et omfangsrigt DDoS-angreb med en gennemstrømning på 3,4 TB pr. sekund fra omkring 10.000 kilder fordelt over flere lande. Lignende højvolumenangreb på mere end 2 TB/s blev afbødet i 2022, hvilket understreger, at det ikke kun er kompleksiteten og hyppigheden af angreb, der er stigende, men også antallet (båndbredden) af angrebene.

Angrebenes varighed

De fleste angreb, der er blevet observeret i løbet af det seneste år, var kortvarige. Omkring 28 % af angrebene varede i mindre end 10 minutter, 26 % varede 10-30 minutter, og 14 % varede 31-60 minutter. 32 % af angrebene varede mere end en time.

Antallet DDoS-angreb og varighedsfordeling
(marts 2021-maj 2022)



De fleste angreb i det seneste år var kortvarige. Omkring 28 % af angrebene varede mindre end 10 minutter.

Opbygning af modstands-dygtighed over for nye DDoS-, webapplikations- og netværksangreb

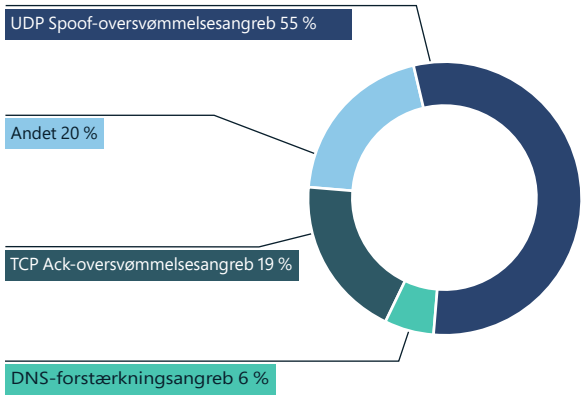
Fortsat

DDoS-angrebsvektorer

I det seneste år var de almindeligt anvendte angrebsvektorer UDP-refleksion (User Datagram Protocol) på port 80 ved hjælp af SSDP- (Simple Service Discovery Protocol), CLDAP- (Connectionless Lightweight Directory Access Protocol), DNS- (Domain Name System) og NTP-protokol (Network Time) med en enkelt top. Vi så også en stigning i DDoS-angreb i applikationslaget målrettet mod websteder med toppe på 16,3 millioner RPS (anmodninger pr. sekund) og en toptrafik på 9,89 TB/s.

I 2022 afbødede Microsoft næsten 2.000 DDoS-angreb dagligt og stoppede det største DDoS-angreb, der nogensinde er rapporteret i historien.

DDoS-angrebsvektorer



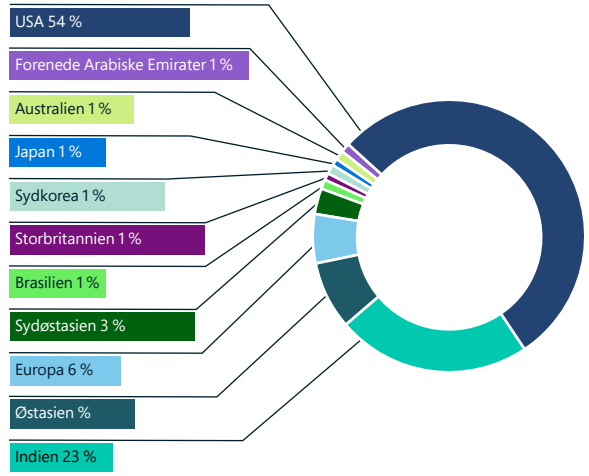
UDP Spoof-oversvømmelsesangreb voksede til den vigtigste angrebsmetode i første halvdel af 2022 fra 16 til 55 %. TCP Ack-oversvømmelsesangreb blev reduceret fra 54 % til 19 %.

Spilbranchen er fortsat det vigtigste mål for DDoS-angreb, primært gennem mutationer af Mirai-botnettet og UDP-protokolangreb med lav volumen. Da UDP er meget anvendt i spil- og streamingapplikationer, var et overvældende flertal af angrebsvektorer UDP-spoof-oversvømmelser, mens et mindretal var UDP-refleksion og forstærkningsangreb.

Geografiske målområder

Af de DDoS-angreb, der blev registreret i løbet af det seneste år, blev 54 % gennemført mod mål i USA, en tendens, der delvist kan forklares med det faktum, at de fleste Azure- og Microsoft-kunder er i USA. Vi oplevede også en markant stigning i angrebene mod Indien, fra kun 2 % af alle angreb i anden halvdel af 2021 til 23 % i første halvdel af 2022. Især Østasien, Hongkong, er stadigvæk et populært mål på 8 %. For Europa var angrebene koncentreret mod Amsterdam, Wien, Paris og Frankfurt.

DDoS-angrebsdestination

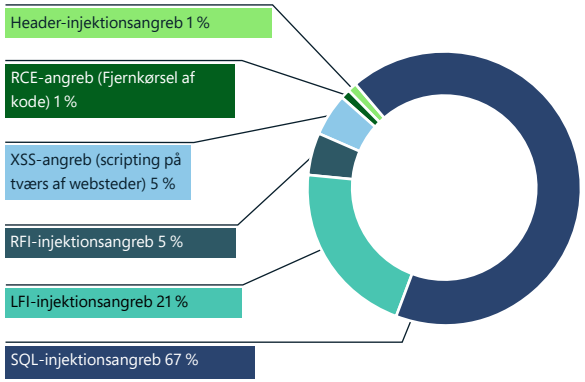


Vi tilskriver den store mængde angreb i Asien til områdets enorme spilmarkeder, især i Kina, Japan, Sydkorea og Indien. Dette marked vil blive ved med at vokse, da den stigende mængde smartphones gør det populært at spille på mobilenheder. Det tyder på, at dette geografiske mål kun vil fortsætte med at vokse.

Udnyttelse af webapplikationer

WAF (Web Application Firewall) udgør sammen med DDoS-beskyttelse en integreret del af en detaljeret forsvarsstrategi til beskyttelse af web- og API-aktiver (applikationsprogrammeringsgrænseflade). Microsoft observerede op mod 300 milliarder WAF-regler, der blev udløst pr. måned via Azure WAF'er.

Fordeling af de mest udbredte angrebstyper



Azure WAF registrerer milliarder af OWASP-topti[10]-angreb (Open Web Application Security Project) hver dag. Ifølge vores signaler forsøger angriberne for det meste SQL-injektionsangreb efterfulgt af lokal filinjektion og eksterne filinjektionsangreb. Dette er i overensstemmelse med OWASP's top ti-liste, der viser injektionsangreb som den tredje mest almindelige type webangreb.

Botangreb mod Azure-webapplikationer er også steget med et gennemsnit på 1,7 milliarder botanmodninger pr. måned. 4,6 % af denne trafik består af dårlige bots.

Opbygning af robusthed mod nye DDoS-, webapplikations- og netværksangreb

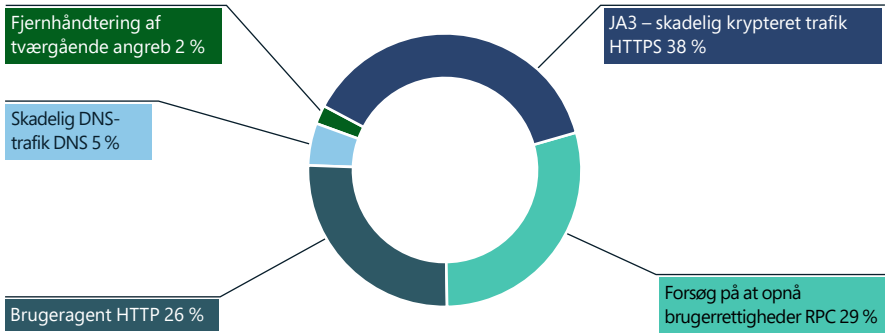
Fortsat

På grund af et stigende antal bots, der foretager angreb i form af credential stuffing-angreb, kreditkortsvindel, cyberindflydelseskampagner og supply chain-angreb, forventer vi at se en støt stigning i botangreb mod webapplikationer.

Netværksindtrængen: registrering og forebyggelse

Vi oplevede en betydelig stigning i angreb mod netværkslaget, især malware, i 2022. IdPS (Azure Firewall Intrusion Detection and Prevention System) blokerede mere end 150 millioner forbindelser alene i juni.

Årsag til IDPS Deny traffic



Årsager til IDPS Alert traffic

Analyse af IDPS Alert- og Deny traffic viser følgende metoder, der anvendes af angribere. I Deny traffic oplever vi, at angribere bruger SSL til at skjule deres aktiviteter, og fjernkørselsangreb bliver mere og mere almindelige. I Alert traffic ser vi SMB/SMB2-protokoller, der bruges til at udføre fjernkørselsangreb.

Handlingsrettet indsigt

1. Undersøg al trafik mellem systemer i et datacenter eller en cloud-tjeneste og trafik, der forsøger at få adgang til dem.
2. Udvikl en robust strategi for netværkssikkerhed hele året.
3. Brug cloud-baserede sikkerhedstjenester til at implementere en robust Nul tillid-netværkssikkerhedsforhold.

Links til yderligere oplysninger

- Forbedr dit sikkerhedsforsvar for ransomware-angreb med Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Et DDoS-forstærket angrebs anatomi | Microsoft Security Blog
- Intelligent applikationsbeskyttelse fra grænseenheder til cloud-løsning med Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Udvikling af en afbalanceret tilgang til datasikkerhed og cyberrobusthed

Den digitale transformation har givet brændstof til en enorm udvidelse af dataaktiver og en stigning i sikkerheds-, overholdelses- og fortrolighedsrisici. Cyberrobuste organisationer skal balancere investeringer i databeskyttelse, overholdelse og gendannelseskapaciteter og integrere dem i specialiserede regulatoriske responsprocesser for at håndtere forskellige typer brud.

Brud på datasikkerhed er ikke et spørgsmål om hvis, men om hvornår. IBM- og Ponemon Institute's "Cost of a Data Breach, 2021"-undersøgelse rapporterer en global gennemsnitlig omkostning til brud på datasikkerheden på 4,24 millioner USD (en stigning på 10 % i forhold til året før) og 9,05 millioner USD i USA. Manglende overholdelse af regler betragtes som den vigtigste omkostningsforstærkende faktor. Omvendt var omkostningsreduktioner i forbindelse med datasikkerhedsbrud knyttet til bedste praksis som planlægning af hændelsesrespons, Nul tillid-implementeringsmodenhed, sikkerheds-AI og automatisering og brug af kryptering.

Databrud er uundgåelige. Organisationer med en afbalanceret robusthedstilgang oplever reduceret hyppighed, virkning og omkostninger ved brud.

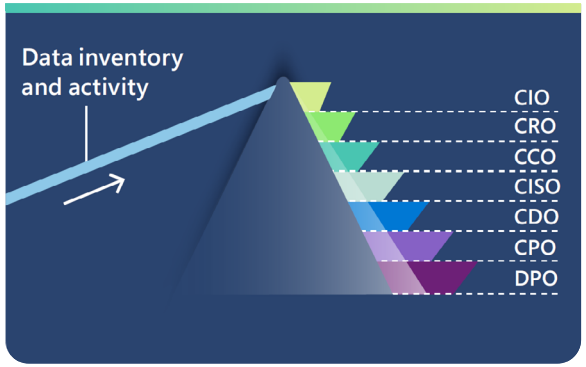
Datastyring, sikkerhed, overholdelse af regler og beskyttelse af personlige oplysninger er gensidigt afhængige

Vi har i de seneste år set data vinde som et afgørende værdiskabelsessystem for organisationer. Samtidig har stigningen i antallet af bestemmelser om beskyttelse af personlige oplysninger, der kræver både datastyring og sikkerhed, sløret grænserne mellem risikoroller. Selvom nye lederroller som CDO'er (Chief Data Officers) eller CPO'er (Chief Privacy Officers) har en personlig interesse i sikkerhed og overholdelse, er implementeringen og operationaliseringen af databeskyttelse ofte afhængig af teams ledet af CIO'er (Chief Information Officers) og/eller CISO (Chief Information Security Officer). Det er ikke en ensrettet vej, da datastyringsinitiativer ledet af CDO'er også har sikkerhedsfordele. På grund af denne indbyrdes sammenhæng skal teams i it, datastyring, sikkerhed, overholdelse og beskyttelse af personlige oplysninger samarbejde tættere for at opnå effektivitet og håndtere risici.

Samlede risikostyringsplatforme for data for hele organisationens datasamling er fremtiden

Det er vanskeligt at tilpasse processer for it, datastyring, sikkerhed, overholdelse og administration i et miljø med tilpassede applikationer til hver disciplin og inkonsekvent dækning på tværs af hybrid dataspredning over flere cloud-løsninger i en typisk organisation. Vi mener, at organisationer har brug for en enkelt "rude" for at finde og kende deres data, beskytte deres data, kontrollere adgangen til, anvendelsen og livscyklussen af data og forhindre tab af data på tværs af datasamlingen.

At arbejde med de samme datalager- og aktivitetsoplysninger letter processer på tværs af teams, giver et mere omfattende risikobillede og gør det muligt for organisationer bedre at forberede og strømline deres reaktioner på sikkerhedsbrud.



Den "enkelte rude" skal fungere som et prisme. Teams, der arbejder med datasikkerhed, overholdelse og beskyttelse af personlige oplysninger, har brug for forskellige men konsekvente perspektiver af det samme datalager og aktiviteter for at blive enige og samarbejde. Dataaktivitet omfatter dataadgang, ændring og bevægelseshændelser, som er en værdifuld del af datasikkerhedsligningen.

Effektiv datastyring, sikkerhed, overholdelse og beskyttelse af personlige oplysninger er indbyrdes afhængige og kræver samarbejde mellem forskellige teams.

Handlingsrettet indsigt

1. Balancer forsvar med genoprettelse, og minimer virkningen af brud på datasikkerheden ved at investere i overholdelse af angivne standarder, databeskyttelse og responsfunktioner.
2. Udvikl og indfør processer og værktøjer, der nedbryder datarisikosiloer og dækker hele datasamlingen.

Links til yderligere oplysninger

- Microsoft Purview – Databeskyttelsesløsninger | Microsoft Security
- Fremtiden for overholdelse af standarder og datastyring er her: Introduktion til Microsoft Purview | Microsoft blog om sikkerhed

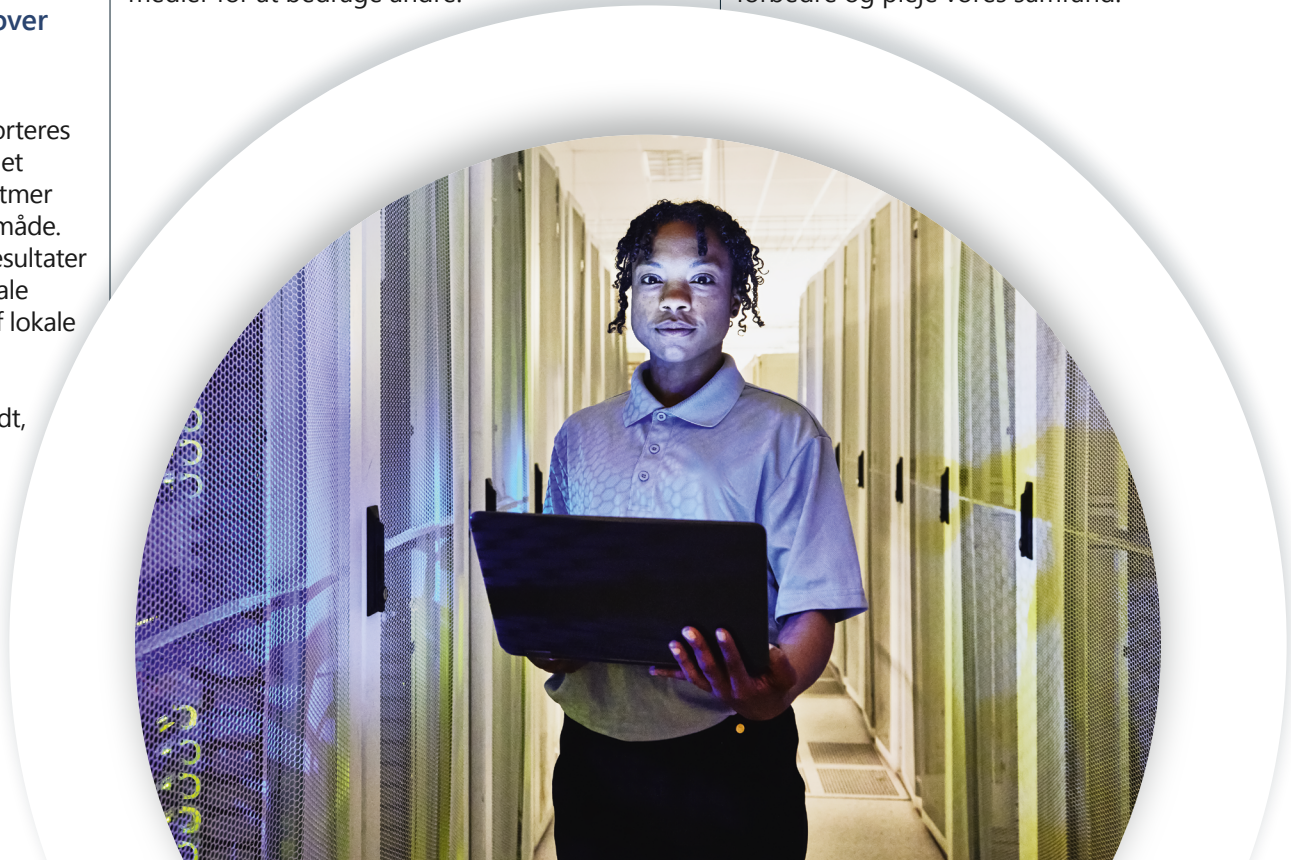
Robusthed over for cyberindflydel-sesaktiviteter: Den menneskelige dimension

I løbet af de sidste fem år har fremskridt inden for grafik og maskinlæring introduceret brugervenlige værktøjer, der hurtigt kan generere realistisk indhold i høj kvalitet, der kan spredes bredt over internettet på få sekunder.

Når det drejer sig om hændelser, der rapporteres via tekst, lyd og visuelt indhold, har vi nået et punkt, hvor hverken mennesker eller algoritmer kan skelne fakta fra fiktion på en pålidelig måde. Udbredelsen af disse værktøjer og deres resultater rejser tvivl om troværdigheden af alle digitale medier, hvilket forstyrrer vores forståelse af lokale begivenheder og verdensbegivenheder. Nye former for indflydelsesaktiviteter, som er muliggjort af teknologiske fremskridt, har alvorlige konsekvenser for de demokratiske processer.[11]

Der opstår spørgsmål om, hvad vi kan gøre for at forberede os på en mere robust fremtid mod disse cyberindflydelsesaktiviteter. Teknologi er kun én del af puslespillet. Det vil kræve indsats på flere fronter, herunder undervisning rettet mod større mediekendskab, bevidsthed og årvågenhed, investering i kvalitetsjournalistik – med velrenommerede journalister på stedet, lokalt, nationalt og internationalt – netværk til at dele og advare om indflydelsesaktiviteter og nye typer af bestemmelser, der straffer ondsindede aktører, der genererer eller manipulerer digitale medier for at bedrage andre.

Vi erkender også, at forsøget på at genskabe tilliden til digitalt indhold er et ambitiøst mål, som vil kræve mange forskellige perspektiver og deltagelse. Der er ikke én virksomhed, en institution eller en offentlig myndighed, der kan løse disse trusler på egen hånd. Vores superkræfter som mennesker er vores evne til at samarbejde. Dette er især vigtigt nu, fordi det vil kræve, at alle – globale myndigheder, brancher, den akademiske verden og især nyheds-, sociale organisationer og medieorganisationer – samarbejder om at forbedre og pleje vores samfund.



Links til yderligere oplysninger

- Applikationer til kunstig intelligens i forsvarsministeriets cybermissioner | Microsoft On the Issues
- Kunstig intelligens og cybersikkerhed: Stigende udfordringer og lovende retninger. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (3. maj 2022, Eric Horvitz' vidnesbyrd)

Forstærkning af den menneskelige faktor med kompetencer

Håndtering af den menneskelige faktor er en vigtig komponent i enhver strategi for at øge cybersikkerhedskompetencer. Ifølge en undersøgelse foretaget af Kaspersky Human Factor in IT Security[12], involverer 46 % af cybersikkerhedshændelser uopmærksomme eller uvidende medarbejdere, der gør angreb mulige.

Microsoft's Education and Awareness-team i Digital Security and Resilience-organisationen er ansvarlig for at styrke den menneskelige faktor i cybersikkerhed ved at give medarbejdere mulighed for at sikre vores egne og vores kunders systemer og data. Vores mål er at:

- Reducere risikoen for Microsoft og vores kunder ved at opbygge et centraliseret sikkerhedskompetencesæt for hele medarbejderstyrken.
- Styrke medarbejdernes sikkerhedsviden gennem en flerfaset undervisning, der understøtter de ønskede adfærdsresultater.
- Fremme kulturændringer ved at gøre bevidsthed om sikkerhed til en integreret del af Microsofts kultur gennem årlig obligatorisk sikkerhedstræning og -begivenheder.
- Fremme en centraliseret webressource for bedste praksis, virksomhedspolitikoplysninger og hændelsesrapportering for alt, hvad der omhandler cybersikkerhed.

Et målrettet, centraliseret kompetenceprogram for cybersikkerhed udsendes til alle Microsoft-medarbejdere mindst én gang om året. Undervisningsstilbud optimeres til at understøtte aktuelle cybersikkerhedsinitiativer og levere målbare adfærdsresultater. Microsoft IRMC (Information Risk Management Council) spiller en vigtig rolle i identificeringen af vigtige resultater for cybersikkerhedsadfærd, der skal håndteres i forbindelse med undervisning.

Med alle vores kompetenceprogrammer inden for cybersikkerhed måler vi løsningens effektivitet, virkning og resultater, når det er muligt. Vores tilbud om træning i insidertrusler har for eksempel 95 % overholdelse af undervisningskrav, ekstraordinær tilfredshed blandt studerende og har resulteret i en betydelig stigning blandt ledere, der rapporterer mulige sager om insidertrusler via virksomhedens Report It Now-værktøj. Programmet omfatter:

Grundlag for sikkerhed: Centraliseret, virksomhedsdækkende bevidsthed om cybersikkerhed og undervisning i overholdelse af angivne standarder, der omhandler centrale praksisser for sikkerhed og beskyttelse af personlige oplysninger. Denne længe ventede undervisningsserie anvender en edutainment-model til at gøre læring om cybersikkerhed involverende og interessant.

STRIKE: Microsofts krævede tekniske undervisning for teknikere, der udvikler og vedligeholder erhvervsløsninger. Denne undervisning, som man skal inviteres til, omhandler rettidige og kritiske områder inden for bedste praksis i cybersikkerhedshygiejne og bruger en hybrid leveringsmodel, der er tilpasset målgruppens behov.

Programspecifikt: Målrettede undervisningsprogrammer understøtter specifikke cybersikkerhedsinitiativer, inklusive Shadow IT, Insider Threat og Microsoft Federal. Disse tilbud er tæt integreret med den overordnede engagementsstrategi for deres respektive cybersikkerhedsinitiativer gennem ledelsessponsorering og scorecardrapportering for at forhindre en undervisningstilgang, hvor man kun skal krydse felter af.

MSProtect: Microsofts centraliserede webressource til bedste praksis, virksomhedspolitikoplysninger og hændelsesrapportering for alt, hvad der vedrører cybersikkerhed. Denne on-demand-ressource er til medarbejdere, der ikke deltager i formelle undervisningstilbud.

Sikkerhedskompetencer må ikke ses som en aktivitet, hvor man blot markerer nogle afkrydsningsfelter. Fokuser i stedet på adfærdsændringer for at tillade, at resultaterne kan kontrolleres op mod identificeret måladfærd, og etabler lyttesystemer til at fastsætte indvirkningen af tilbud.

Handlingsrettet indsigt

1. Giv medarbejderne sikkerhedsundervisning og -ressourcer, når og hvor de har brug for det.
2. Udarbejd en centraliseret kompetencestrategi ud fra, hvad interessenter i hele virksomheden siger.
3. Sørg for, at effekten af undervisningen spores og analyseres for nyttevirkning (mængde), effektivitet (kvalitet) og resultater (virksomhedsindvirkning).

Links til yderligere oplysninger

- Microsoft indleder næste fase af kompetenceinitiativet efter at have hjulpet 30 millioner mennesker

Indsigt fra vores program til eliminering af ransomware

Microsoft har i de sidste fem år arbejdet på at implementere Nul tillid[13] med henblik på at sikre, at identiteter og enheder er robust administrerede og sunde. I takt med at risikoen for ransomware vokser, har vi udviklet en dyb indsigt i, hvordan vi understøtter vores tilgang til at beskytte os selv og vores kunder.

Efter en grundig intern evaluering har vi udviklet et ransomware-elimineringsprogram for at afhjælpe mangler i kontroller og dækning, bidrage til funktionelle forbedringer af tjenester som Defender for Endpoint, Azure og M365 og udvikle regler for vores SOC- og teknologiteams om genoprettelse efter et ransomware-angreb.

Det første skridt var at forstå omfanget af vores beskyttelse mod et ransomware-angreb rettet mod Microsoft. Arbejdet var allerede godt i gang med at implementere Defender for Endpoint og sikre, at alle enheder blev administreret og overholdt vores Nul tillid-politikker, men vi var nødt til at finde en måde at forstå alle aspekter af det vigtigere spørgsmål om, hvorvidt vi effektivt kunne foretage genoprettelse efter et angreb. For at få indsigt evaluerede vi NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF)-profilen,[14], som stemmer overens med vores overordnede virksomhedspolitik i forhold til vores liste over kendte kontroller. Denne analyse identificerede hurtigt mangler i dækningen.

Dernæst prioriterede vi mangler i CSF-funktionerne Identificer, Registrer, Beskyt, Reager og Genopret. Vi fandt en strategisk overensstemmelse med Nul tillid og andre programmer og opdagede også mangler, der ikke havde nogen eksisterende workstream. Efter at have vurderet den mængde arbejde og indsats, der var nødvendig for at afhjælpe disse mangler, opdelte vi dem i to søjler:

- **PtE (Beskyt virksomheden):** Definer de arbejdspunkter, som vi skal foretage som virksomhed for at beskytte os selv og være i stand til at foretage genoprettelse efter et angreb, hvis det lykkedes.
- **PtC (Beskyt kunden):** Opbyg funktioner i vores tilbud for at beskytte både vores kunder og vores forretning.

Integrering af resultater i vores egen virksomhed

For at imødegå de største risici og beskytte vores kritiske tjenester mod ransomware-angreb, planlægger vi at fokusere investeringer over de næste 6 til 12 måneder på at gennemføre de fem scenarier nedenfor som en del af et dedikeret ransomware-program. Når vi har gennemført hvert af scenarierne, vil vi gradvist udvide programmets omfang til at nå ud til alle dele af virksomheden.

Scenarie 1: Medlemmer af sikkerhedsteamet forstår den overordnede risiko i forbindelse med et ransomware-angreb og har etableret en proces, der giver ledere kendskab til kontrolmangler og risikostatus.

Scenarie 2: Medlemmer af sikkerhedsteamet har adgang til strategiplaner, der er udviklet til at hjælpe dem og andre teams i Microsoft med at reagere på og genoprette kritiske tjenester efter et ransomware-angreb.

Scenarie 3: Enterprise Resilience-teammedlemmer har en standard, de skal følge for at sikkerhedskopiere kritiske systemer. Der findes strategiplaner, og der udføres regelmæssige øvelser i sikkerhedskopiering og genoprettelse for at sikre, at data kan genoprettes i tilfælde af et ransomware-angreb.

Scenarie 4: Tjenesteejere forstår og implementerer de nødvendige sikkerheds- og driftskontroller og -politikker for at beskytte deres tjenester, kundedata, endpoints og netværksaktiver mod ransomware-angreb med særligt fokus på tjenester, der prioriteres som kritiske Microsoft-tjenester.

Scenarie 5: Alle medarbejdere kan få adgang til undervisningsressourcer, der beskriver, hvordan et ransomware-angreb genkendes, hvordan sikkerhedsteamet underrettes, og hvordan respons påbegyndes.

Handlingsrettet indsigt

1. Dokumentér og valider komplette genoprettelses- og afhjælpningsaktiviteter relateret til ransomware-angreb mod kritiske tjenester.
2. Involver interessenter i opdatering af dine strategiplaner for virksomhedsmæssig krisehåndtering til at inkludere ransomware-specifikke aktiviteter og en beslutningsproces og vejledning i at afgøre, om/hvornår der skal betales løsesummer.
3. Få bedre registrerings- og beskyttelsesdækning ved at aktivere funktioner, der er tilgængelige i de implementerede sikkerhedsprodukter (f.eks. Defender for Endpoint Attack Surface Reduction-regler).
4. Samarbejd med teamet for sikkerhedsstandarder om at definere grundlæggende beskyttelse mod et ransomware-angreb, og giv tekniske teams undervisning i og dokumentation om, hvordan de beskytter sig mod et ransomware-angreb.
5. Benyt automatisering til at forenkle implementeringen af sikkerheds- og driftspolitikker for DevOps-teams, og sørg for, at systemer, der afviger fra standarden, hurtigt identificeres og korrigeres.

Links til yderligere oplysninger

- Deling af, hvordan Microsoft beskytter mod ransomware | Microsoft Inside Track

Reager nu på kvantesik-kerhedsimplikationer

Der er pres på for at håndtere den trussel, kvantecomputere udgør for nutidens kryptografi, og alt, hvad den beskytter. Det nyligt udsendte Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15], der bygger på US Executive Order 10428[16] for Improving the Nation's Cybersecurity, fremhæver sikkerhed i software-supply chain som afgørende for håndtering af fremtidige nationalstatsangreb.

Hvad er kvantecomputere?

Kvantecomputere er maskiner, der bruger egenskaberne fra kvantefysik til at lagre data og udføre beregninger. Dette kan være yderst fordelagtigt til visse opgaver, hvor de kan udkonkurrere selv vores bedste supercomputere markant. Kvantecomputere åbner allerede nye horisonter for datakryptering og -behandling. Undersøgelser forudsiger, at kvantecomputere vil blive en kvanteindustri på flere milliarder dollar (USD) allerede i 2030.[17] Faktisk er kvantecomputere og kvantekommunikation forberedt til at have en transformativ effekt på tværs af en lang række brancher, lige fra sundhedspleje og energi til økonomi og sikkerhed.

Kvantecomputere er en trussel mod nutidens kryptografi og alt, hvad den beskytter.

Truslen mod nutidens kryptografi

Med Shors algoritme fra 1994 og en kvantecomputer i industriel skala på mere end et par millioner fysiske qubits, kan alle vores nuværende bredt implementerede krypteringsalgoritmer for offentlige nøgler nemt brydes. Det er vigtigt at overveje, evaluere og standardisere "kvantesikre" kryptosystemer, der er effektive, fleksible og sikre over for et modsætningsfuldt kvantebaseret angreb. Migrering af software til "post-kvantekryptografi", dvs. klassiske algoritmer og protokoller, der allerede er tilgængelige og resistente over for kvanteangreb, vil tage år eller endda mere end et årti.[18]

Dette betyder, at presset øges for at håndtere truslen mod den moderne kryptografi og alt det, den beskytter. Modstandere kan registrere krypterede data nu og udnytte dem senere, når der er en kvantecomputer tilgængelig. Det vil være for sent at vente på kvantecomputere, før de kryptografiske konsekvenser håndteres.

Da kryptografi bruges i hele cyberøkosystemet, betyder det, at vores kryptografiske sikkerhedstjenester kan blive kompromitteret. Dette inkluderer for eksempel kommunikationstjenester (TLS, IPSec), meddelelser (mail, webkonferencer), identitets- og adgangsstyring, webbrowsing, kodesignering, betalingstransaktioner og andre tjenester, der er afhængige af kryptografi til beskyttelse.

Når kvantecomputere bliver en realitet, skal tredjeparts softwarekomponenter med implementeringer af kryptografiske algoritmer og funktioner også undersøges nærmere. Dette kræver, at alle organisationer i værdikæden gør deres del for at sikre, at kæden forbliver sikker. Brancheorganer og myndigheder øger deres indsats for at definere sikkerhedskrav til software-supply chain og introducerer i nogle tilfælde nye krav til sikring af kæden. National Security Memorandum NSM-8[19] etablerer krav og tidslinjer for implementering af kryptografi efter introduktionen af kvantecomputere i NSS (National Security Systems). Der omtales tidsforventninger på 180 dage til "moderniseringsplanlægning, brug af ikke-understøttet kryptering, godkendte missionsspecifikke protokoller, kvanteresistente protokoller og planlægning af brug af kvanteresistent kryptografi efter behov".

Standardisering er en langvarig aktivitet i overgangen til kvantesikker kryptografi. Standardiseringsmyndigheder, der arbejder på standarder ved hjælp af kryptografi til offentlige nøgler, skal begynde at eksperimentere med og indføre post-kvantealgoritmer nu.

Nye PQC-algoritmer (post-quantum cryptography) – klassiske algoritmer, der menes at være robuste over for kvanteangreb – bliver nu gennemgået under NIST's Post-Quantum Standardization Project.[20] Dette arbejde vil påvirke den globale indsats hos standardiseringsmyndighederne. Selvom der vil være en vis overlapning med den amerikanske regerings algoritmevalg, kan forskellige nationale organer/regulatoriske valg for kompatible algoritmer give internationale udfordringer. Denne fragmentering vil igen komplicere produkt- og serviceteknologi.

Nye post-kvantekryptografi-algoritmer er under gennemgang gennem NIST's Post-Quantum Cryptography-standardiseringsprogram. Dette arbejde vil påvirke den globale indsats hos standardiseringsorganer.

Handlingsrettet indsigt

Sammen med SAFECode og partnermedlemmer bør industrien øjeblikkeligt gå i gang med kortsigtede aktiviteter for at forberede overgangen til et post-kvantekryptografi.[21] Dette omfatter:

1. At få et overblik over dine produkter/koder, der bruger kryptografi.
2. Implementere en krypto-fleksibilitetsstrategi for hele din organisationen, der inkluderer minimering af den kodeudskiftning, der kræves, når kryptografi ændres.
3. Udføre en pilotundersøgelse af brugen af kvantesikre algoritmer i dine produkter eller tjenester, hvor der bruges kryptografi.
4. Være forberedt på at bruge forskellige offentlige nøglealgoritmer til kryptering, nøgleudveksling og signaturer.
5. Teste dine applikationer for indvirkningen af meget store nøglestørrelser, krypteringer og signaturer.

Links til yderligere oplysninger

- Microsoft har vist den underliggende fysik, der kræves for at skabe en ny type qubit | Microsoft Research

Integration af forretning, sikkerhed og it for at opnå større robusthed

Graden af cyberrobusthed afhænger af virksomhedsledere, der samarbejder med sikkerhedsteams om at implementere sikkerhed. Microsoft erfarer, at det er svært at være førende inden for sikkerhed, fordi det kræver støtte fra organisationens ledere at beskytte organisationen effektivt.

Sikkerhedsledere navigerer i et spektrum af dynamiske udfordringer, der spænder over emner som risiko, teknologi, økonomi, organisatoriske processer, forretningsmodeller, kulturtransformation, geopolitiske interesser, spionage og overholdelse af internationale sanktioner. Alle disse har nuancer, der skal forstås og håndteres omhyggeligt.

Sikkerhedsledere har også til opgave at undvige intelligente, velfinansierede og højt motiverede menneskelige angribere og effektive cyberkriminelle med kun ringe færdigheder. Deres teams skal forsvare komplekse tekniske områder, der ofte er blevet bygget i små trin over 30 år eller mere, da sikkerheden havde en lav eller ingen prioritet. Beslutninger, der blev truffet for år tilbage, kan udgøre risici i dag, indtil vi betaler af på den tekniske gæld og håndterer sikkerhedsmanglerne.

Organisatoriske ledere og politikere kan have en betydelig positiv indvirkning på sikkerheden ved aktivt at støtte sikkerhedsledere og være med til at bygge bro mellem integreret sikkerhed og resten af organisationen. Når Microsoft arbejder med kunder, der har denne tilpasning, ser vi dem opbygge en mere robust organisation, og de bliver også mere fleksible i forhold til at tilpasse og innovere.

Organisatorisk ledelse kan støtte sikkerhedsledere ved at fokusere på tre nøgleområder:

1. Opbyg sikkerhed gennem design

Sikkerhed ses nogle gange som en hindring eller en eftertanke i forretningsprocesser, der medtages ofte kun i beslutningsovervejelser, når det er for sent at undgå en risiko eller løse problemet billigt og nemt.

Organisatoriske ledere og politikere bør sørge for, at de:

Inkluderer sikkerhed tidligt i nye initiativer. Nye digitale initiativer og cloud-indførelse bør prioritere sikkerhed for at sikre, at de risici, som organisationen står over for, ikke øges med hver ny applikation eller digital funktion. Hvis sikkerhed er pålideligt inkluderet, kan disse processer bruges til at modernisere ældre systemer og opnå både sikkerheds- og produktivitetsfordele på samme tid.

Normaliser forebyggende vedligeholdelse af sikkerheden. Sørg for grundlæggende sikkerhedsvedligeholdelse – som at anvende sikkerhedsopdateringer og programrettelser og sikre konfigurationer – er fuldt understøttet af organisationen (herunder budgetter, planlagt nedetid og købskrav til leverandørens produktsupport).

Desværre forsinker, udskyder eller anvender mange organisationer kun delvist disse almindelige praksisser. Dette giver angribere omfattende muligheder, som de kan udnytte. Behovet for sikkerhedsnormalisering er registreret i US NIST 800-40.[22]

2. Engager dig i sikkerhed

Virksomhedsledere bør aktivt deltage i og sponsorere vigtige sikkerhedsprocesser for at sikre prioritering af ressourcer og beredskab i forbindelse med sikkerhedskatastrofer. Dette inkluderer at engagere sig i følgende:

Identificer kritiske virksomhedsaktiver. Sikkerhedsledere og -teams har brug for at vide, hvilke aktiver der er forretningskritiske for at fokusere sikkerhedsressourcer på det, der er vigtigst. Dette er ofte en ny øvelse, der omfatter at stille og besvare nye spørgsmål, der ikke er blevet håndteret tidligere.

Øvelser i cybersikkerhed for forretning-skontinuitet og disaster recovery. Cyberangreb kan blive store begivenheder, der afbryder eller stopper de fleste eller alle forretningsaktiviteter. At sikre, at teams i hele organisationen er parate til at håndtere disse situationer, vil reducere tiden til at genoprette virksomhedens drift, begrænse skaderne for organisationen og bidrage til at opretholde tilliden hos kunder, medborgere og interessenter. Dette bør integreres i en eksisterende forretningskontinuitet og disaster recovery-proces.

Beslutninger om sikkerheds-risici træffes bedst af virksomheds- eller missionsejere, der har fuld synlighed over alle risici og muligheder.

Integration af forretning, sikkerhed og it for at opnå større robusthed

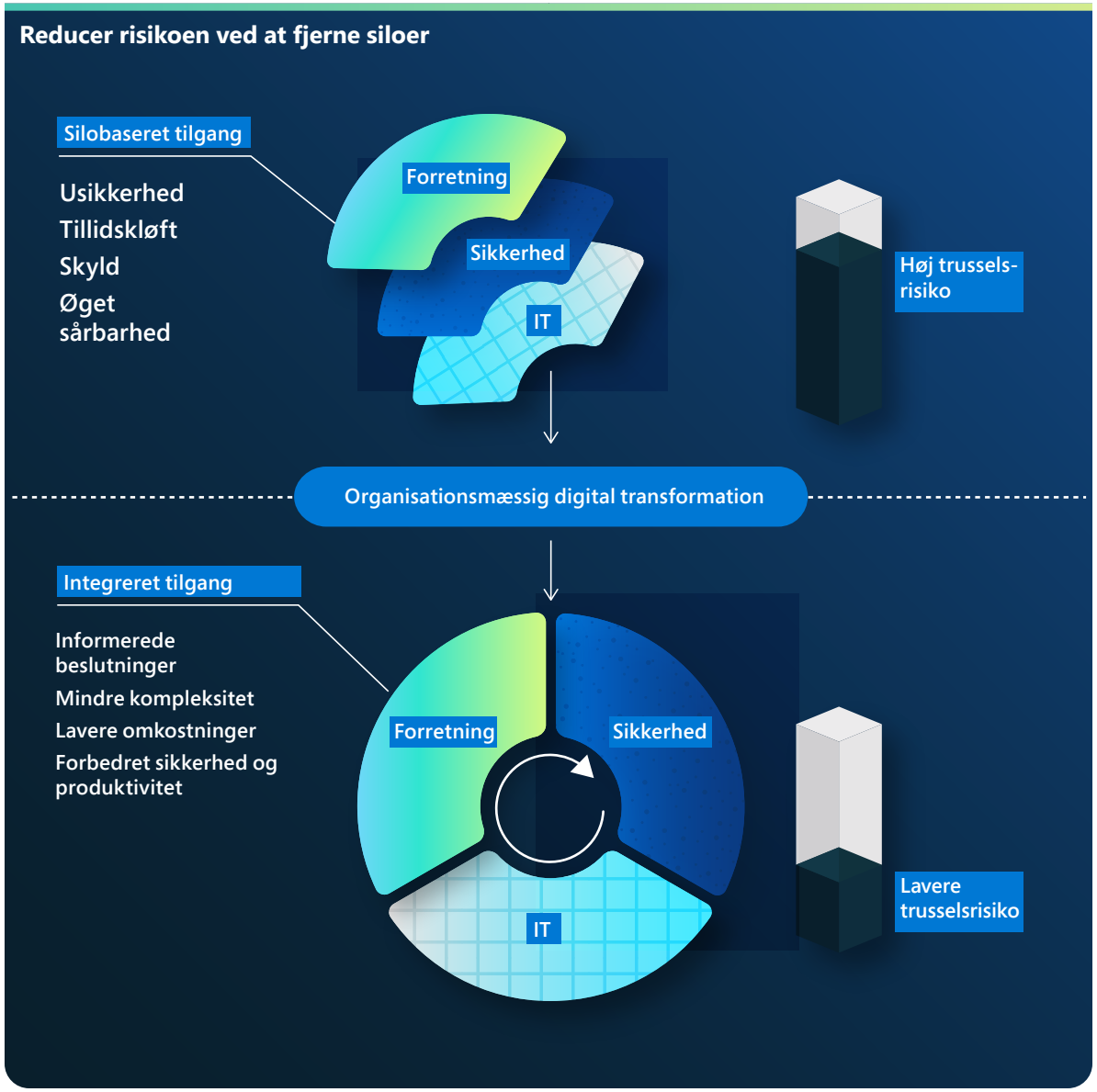
Fortsat

3. Placer sikkerheden korrekt

Den måde som organisationer strukturerer ansvaret for sikkerhedsrisici på gør dem ofte dårlige til at træffe beslutninger om sikkerhedsrisici. Risikobeslutninger træffes bedst af virksomheds- eller missionsejere, der har fuld synlighed over alle risici og muligheder, men mange organisationer tildeler (implicit eller eksplicit) ansvaret for sikkerhedsrisici til fageksperter i sikkerhedsteamet i stedet. Dette lægger en usund byrde på sikkerhedsteams og fratager virksomhedsejere synlighed og kontrol over en vigtig risiko, som deres virksomhed står over for. Organisationer kan ændre dette ved at:

Forberede virksomhedsejere: Undervis virksomhedsejere i den overordnede sikkerhedsrisiko, og hvordan disse trusler kan og vil påvirke deres virksomhed. Involvering af sikkerhedsteams direkte i dette arbejde øger også samarbejdsforholdet mellem sikkerhed og overordnet forretningsfleksibilitet.

Tildele sikkerhedsrisiko til virksomhedsejere: Efterhånden som virksomhedsejere bliver tilstrækkeligt informeret til at forstå og acceptere sikkerhedsrisici, bør organisationen eksplicit flytte ansvaret for sikkerhedsrisici til dem, mens de stadig holder sikkerhedsteams ansvarlige for at håndtere risikoen og levere informeret ekspertise og vejledning til ejeren.



"Cyberrobusthed findes på en glidende skala fra klassisk forretningskontinuitet og disaster recovery, startende med god sikkerhedskopiering af data, videre til genoprettelsesfunktioner for processer, teknologi og deres afhængigheder (inklusive personer og tredjeparter) og fortsætter til altid aktive selvhelbredende tjenester, robusthed over for kritiske roller og failovers for kritiske tredjeparter. De mest robuste organisationer fremmer integration mellem it, virksomhedsledere og sikkerhedsmedarbejdere. Stor robusthed omfatter design af robusthed fra starten, sikker ændringsmanagement og detaljeret fejlisolering. Cyberrobusthed er blot ét scenarie i et godt program, hvor du planlægger med alle risici. Efterhånden som antallet af cyberrisici vokser, og skæringspunktet mellem cybersikkerhed og robusthed bliver stadig vigtigere, styrkes forbindelsen mellem CISO'en (Chief Information Security Officer) og virksomhedens robusthedsprogram. Hvert år tager flere CISO'er kontrol over virksomhedens robusthed".

Lisa Reshaur
General Manager, Risk Management, Microsoft

Links til yderligere oplysninger

- Fra robusthed til digital vedholdenhed: Hvordan organisationer bruger digital teknologi til at komme igennem vanskelige tider | Officiel Microsoft Blog
- Hvordan it- og sikkerhedsteams kan samarbejde om at forbedre endpoint-sikkerhed | Microsoft Security

Klokkekurven for cyberrobusthed

Succesfaktorer for robusthed, som alle organisationer bør indføre

Som vi har set, lykkes mange cyberangreb, simpelthen fordi grundlæggende sikkerhedshygiejne ikke er blevet fulgt. De minimumsstandarder, som alle organisationer bør indføre, er:

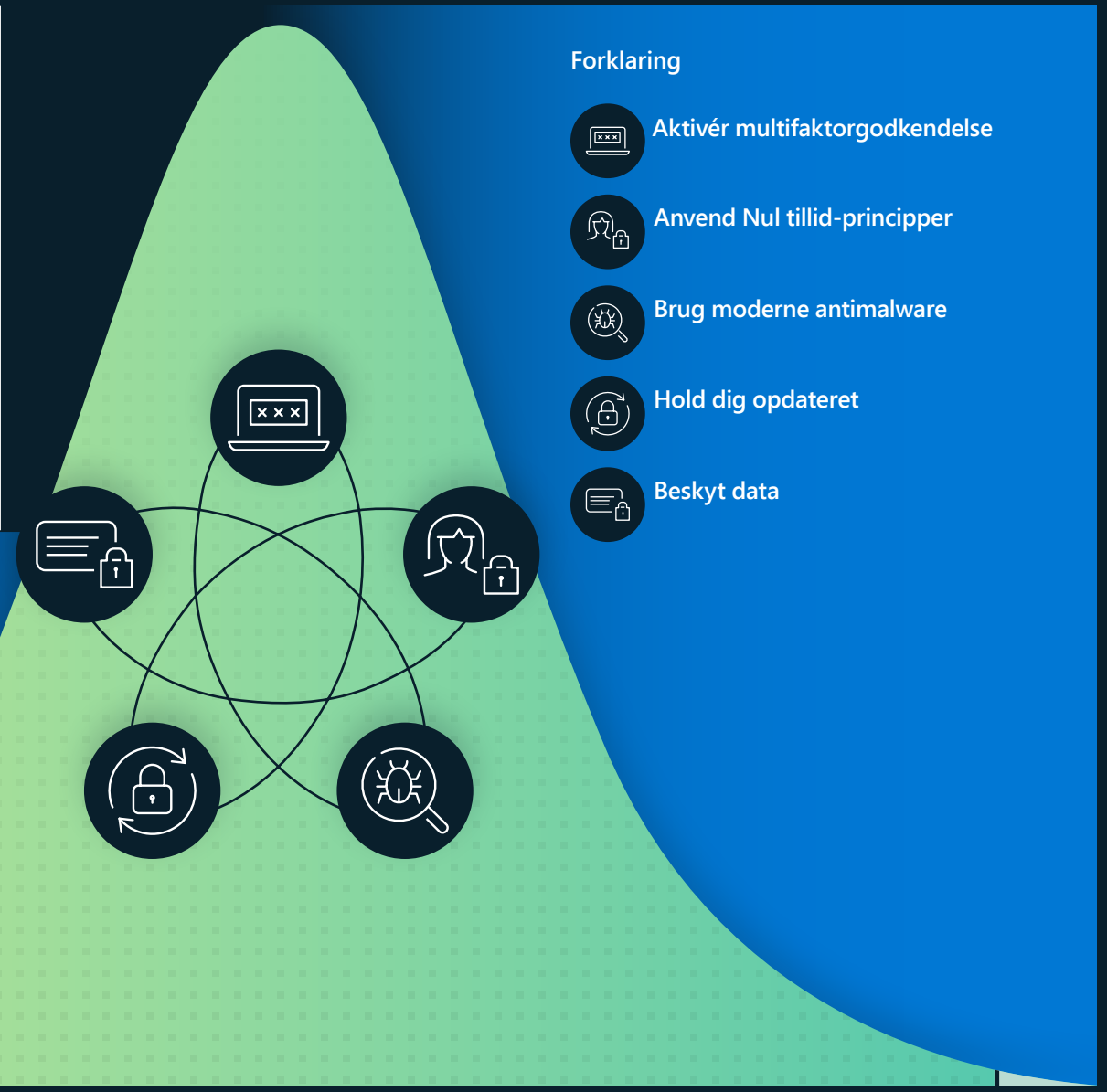
- **Aktiver MFA (multifaktorgodkendelse):** For at beskytte mod kompromitterede brugeradgangskoder og hjælpe med at give identiteter ekstra robusthed.
- **Anvend Nul tillid-principper:** Hjørnestenen i enhver robusthedsplan, der begrænser indvirkningen på en organisation. Disse principper er:

1. – Bekræft eksplicit – sørg for, at brugere og enheder er i god stand, før de får lov til at bruge ressourcer.
2. – Brug adgang med minimumrettigheder – tillad kun de rettigheder, der er nødvendige for at få adgang til en ressource, og ikke mere.
3. – Antag brud – antag, at systemforsvaret er blevet brudt, og at systemer kan blive kompromitteret. Dette betyder konstant overvågning af miljøet for mulige angreb.

- **Brug anti-malware med forbedrede registrering- og responsmuligheder:** Implementer software til at registrere og automatisk blokere angreb og give indsigt til sikkerhedsafdelingen. Overvågning af indsigt fra trusselsregistreringssystemer er afgørende for at kunne reagere rettidigt på trusler.
- **Hold dig opdateret:** Systemer uden fejlrettelse og forældede systemer er en vigtig årsag til, at mange organisationer bliver ofre for et angreb. Sørg for, at alle systemer holdes opdaterede, herunder firmware, operativsystemet og applikationer.
- **Beskyt data:** Det er afgørende at kende dine vigtige data, hvor de er placeret, og om de rigtige systemer er implementeret, for at kunne implementere en passende beskyttelse.

98 %

Grundlæggende sikkerhedshygiejne beskytter fortsat mod 98 % af angrebene.



Slutnoter

1. EDR (Endpoint Detection and Response) er en endpoint-sikkerhedsplatform til virksomheder, der er udviklet til at hjælpe virksomhedens netværk med at forebygge, registrere, undersøge og reagere på avancerede trusler. Endpoint-registrerings- og responsfunktioner tilbyder avancerede registreringer af angreb i næsten realtid og er handlingsrettet. Sikkerhedsanalytikere kan prioritere advarsler effektivt, få indblik i det fulde omfang af et sikkerhedsbrud og træffe foranstaltninger for at afbøde trusler.
2. En EPP (Endpoint Protection Platform) er en løsning, der er implementeret på endpoint-enheder for at forhindre filbaseret malware, for at opdage og blokere skadelig aktivitet fra pålidelige og upålidelige applikationer og for at levere de undersøgelses- og afhjælpningsfunktioner, der er nødvendige for at reagere dynamisk på sikkerhedshændelser og -advarsler.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows Security Book | Commercial
7. Nye sikkerhedsfunktioner til Windows 11 hjælper med at beskytte hybridarbejde | Microsoft Security Blog
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Executive Order 14028 Improving the Nation's Cybersecurity
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. "The Long Road Ahead to Transition to Post-Quantum Cryptography", https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Teams, der har bidraget

Teams, der har bidraget

Dataene og indsigterne i denne rapport er leveret af et væld af sikkerhedsfokuserede fagfolk, der arbejder på tværs af mange forskellige teams hos Microsoft. Samlet er deres mål at beskytte Microsoft, Microsofts kunder og hele verden mod truslen fra cyberangreb. Vi er stolte af at dele denne indsigt for at sikre transparens og med et fælles mål om at gøre den digitale verden til et sikrere sted for alle.

AI for Good Research Lab: Udnyttelse af styrken i data og AI for at håndtere mange af verdens udfordringer. Laboratoriet samarbejder med organisationer uden for Microsoft, der anvender AI til at forbedre levevilkår og miljøer. Fokusområder omfatter onlinesikkerhed (misinformation, cybersikkerhed, børns sikkerhed), katastrofeberedskab, bæredygtighed og AI i sundhedspleje.

Azure Edge & Platform, Enterprise & OS Security: Ansvarlig for sikkerheden for det centrale operativsystem og platformen på tværs af Windows, Azure og andre Microsoft-produkter. Teamet udvikler brancheførende sikkerheds- og hardwareløsninger til Microsoft-platforme for at reducere kompromitteringer via udnyttelse, identiteter og malware fra chip til cloud-løsningen. Skabere af Microsoft Secured-kerneplatform til pc, grænseenheder og server, Microsoft Pluton Security-processor og meget mere.

Azure-netværk, kerne: Et cloud-netværksteam, der fokuserer på Microsoft WAN, datacenternetværk og den softwaredefinerede netværksinfrastruktur i Azure, herunder DDoS-platformen, grænseenhedsplatformen for netværk og netværkssikkerhedsprodukter, f.eks. Azure WAF, Azure Firewall og Azure DDoS Protection Standard.

Cloud Security Research-team: Ved at sikre Microsoft Cloud, udvikle innovative sikkerhedsfunktioner og produkter og udføre undersøgelser beskytter og styrker dette team Microsoft-kunder til at transformere deres organisationer på en sikker måde.

CST (Customer Security and Trust): Et team, der løbende arbejder på at forbedre kundesikkerheden i Microsoft-produkter og -onlinetjenester. I samarbejde med tekniske og sikkerhedsfokuserede teams på tværs af hele virksomheden sikrer CST overholdelse, forbedrer sikkerheden og giver mere gennemsigtighed med henblik på at beskytte kunder og styrke den globale tillid til Microsoft.

Kundesucces: Sikkerhedsteams i kundesucces arbejder direkte med kunderne for at dele bedste praksis, erfaringer og vejledning for at fremskynde sikkerhedstransformation og modernisering. Dette team samler og organiserer bedste praksis og erfaringer fra Microsofts rejse – samt vores kunders – inden for referencestrategier, referencearkitekturer, referenceplaner og meget mere.

CDOC (Cyber Defense Operations Center): Microsofts cybersikkerheds- og forsvarscenter er et fusionscenter, der samler sikkerhedseksperter fra hele virksomheden for at beskytte vores virksomhedsinfrastruktur og den cloud-infrastruktur, som kunderne har adgang til. Responsmedarbejdere sidder sammen med dataeksperter og sikkerhedsteknikere fra alle Microsofts grupper af tjenester, produkter og enheder for at hjælpe med at beskytte, registrere og reagere på trusler døgnet rundt.

Democracy Forward Initiative: Et Microsoft-team, der arbejder på at bevare, beskytte og fremme demokratiets grundlæggende værdier ved at fremme et sundt informationsøkosystem, beskytte åbne og sikre demokratiske processer og være fortaler for virksomhedernes samfundsansvar.

DCU (Digital Crimes Unit): Et team af advokater, efterforskere, dataforskere, ingeniører, analytikere og erhvervsfolk, der er dedikeret til at bekæmpe cyberkriminalitet på verdensplan ved hjælp af teknologi, retsvidenskab, civile søgsmål, underretninger om kriminelle aktiviteter samt offentlige/private partnerskaber.

Digitalt diplomati: Et internationalt team af tidligere diplomater, strateger og juridiske eksperter, der arbejder for at fremme et fredeligt, stabilt og sikkert cyberspace i lyset af den stigende nationalstatskonflikt.

DSR (Digital Security & Resilience): En organisation, der er dedikeret til at give Microsoft mulighed for at udvikle de mest pålidelige enheder og tjenester, samtidig med at vi sikrer vores virksomhed og beskytter både vores virksomhedsdata og kundedata.

DSU (Digital Security Unit): Et team bestående af cybersikkerhedsadvokater og -analytikere, der leverer juridisk, geopolitisk og teknisk ekspertise for at beskytte Microsoft og deres kunder. DSU opbygger tillid til Microsofts sikkerhedsforsvar for virksomheder mod avancerede cyberkriminelle i hele verden.

DTAC (Digital Threat Analysis Center): Et team af eksperter, der analyserer og rapporterer om nationalstatstrusler, herunder cyberangreb og indflydelsesaktiviteter. Teamet kombinerer information og cybertrusselsdata med geopolitisk analyse for at tilbyde indsigt til vores kunder og Microsoft for at informere om effektiv respons og beskyttelse.

Virksomhed og sikkerhed: Et team, der er fokuseret på at levere en moderne, sikker og håndterbar platform til den intelligente cloud-løsning og intelligente grænseenheder.

Enterprise Mobility: Et team, der hjælper med at levere den moderne arbejdsplads og moderne management for at holde data sikre i cloud-løsningen og on-premises. Endpoint Manager omfatter de tjenester og værktøjer, Microsoft og kunderne bruger til at administrere og overvåge mobilenheder, stationære computere, virtuelle maskiner, integrerede enheder og servere.

Teams, der har bidraget

Fortsat

Enterprise Risk Management: Et team, der arbejder på tværs af forretningsenheder for at prioritere risikodiskussioner med Microsoft øverste ledelse. ERM forbinder flere driftsrisikoteams, administrerer Microsofts virksomhedsrisikostruktur og gør det nemmere at udføre virksomhedens interne sikkerhedsvurderinger ved hjælp af NIST Cybersecurity Framework.

Global Cybersecurity Policy: Et team, der samarbejder med myndigheder, NGO'er og partnere i branchen om at fremme offentlig cybersikkerhedspolitik, der giver kunderne mulighed for at styrke deres sikkerhed og robusthed, når de indfører og bruger Microsoft cybersikkerhed.

IDNA (Identity and Network Access) Security: Et team, der arbejder på at beskytte alle Microsoft-kunder mod uautoriseret adgang og svindel. IDNA Security er et tværfagligt team af ingeniører, produktchefer, dataforskere og sikkerhedsefterforskere.

M365 Security: Organisation, der udvikler sikkerhedsløsninger, herunder Microsoft Defender for Endpoint (MDE), Microsoft Defender for Identity (MDI) og andre for at beskytte virksomhedskunder.

Microsoft AETHER (AI, Ethics and Effects in Engineering and Research): En rådgivende bestyrelse hos Microsoft med missionen om at sikre, at nye teknologier udvikles og benyttes på en ansvarlig måde.

Microsoft Bing Search and Distribution: Et team, der er dedikeret til at levere et internetsøgeprogram i verdensklasse, der giver brugere over hele verden mulighed for hurtigt at finde pålidelige søgeresultater og oplysninger, herunder sporing af emner og populære historier, der betyder noget for dem, samtidig med at det giver brugerne kontrol over deres personlige oplysninger.

Microsoft Customer and Partner Solutions: Microsofts samlede, kommercielle lanceringsorganisation med ansvar for feltroller som f.eks. sikkerhedsmæssige og tekniske salgsspecialister og rådgivere.

Microsoft Defender Experts: Microsofts største globale organisation af produktfokuserede sikkerhedseksperter, praktisk funderede forskere og analytikere inden for trusselsefterretninger. Defender Experts leverer innovative funktioner inden for registrering og respons i Microsoft 365-sikkerhedsløsninger og administrerede Microsoft Defender Experts-tjenester.

Microsoft Defender for IoT: Et team bestående af domæneeksperter med speciale i reverse engineering af IoT/OT-malware, -protokoller og -firmware. Teamet jagter IoT/OT-trusler for at afdække skadelige tendenser og kampagner.

Microsoft Defender Threat Intelligence (RiskIQ): Et team, der producerer taktisk intelligens gennem analyse af Microsofts omfattende eksterne telemetrisamling, kortlægger trusselslandskabet, efterhånden som det udvikler sig for at opdage tidligere ukendt trusselsinfrastruktur, og føjer kontekst til trusselsaktører og -kampagner. Teamet udgiver regelmæssigt forskning, der er rettidig og tydelig, for at levere afgørende taktiske data til forsvarere.

Microsoft Security Business Development Team: Et team, der leder Microsofts strategi for vækst inden for cybersikkerhed, partnerskaber og strategiske investeringer.

Microsoft Security Response Center (MSRC): Et team, der er samarbejder med sikkerhedseksperter om at beskytte Microsofts kunder og partnerøkosystem. MSRC er en integreret del af Microsofts CDOC (Cyber Defense Operations Center) og samler eksperter inden for sikkerhedsrespons fra hele virksomheden for at hjælpe med at beskytte, registrere og reagere på trusler i realtid.

Microsoft Security Services for Incident Response: Et team af cybersikkerhedseksperter, der hjælper kunder gennem hele cyberangrebet fra undersøgelser til vellykkede aktiviteter relateret til inddæmning og genoprettelse. Tjenester tilbydes via to yderst integrerede teams, DART (Detection and Response Team) med fokus på undersøgelsen og det grundlæggende arbejde for genoprettelse og CRSP (Compromise Recovery Security Practice), som fokuserer på aspekterne for inddæmning og genoprettelse.

MSTIC (Microsoft Threat Intelligence Center): Et team, der er fokuseret på at identificere, spore og indsamle data, der er relateret til de mest sofistikerede modstandere, der påvirker Microsoft-kunder, herunder nationalstatstrusler, malware og phishing.

1ES (One Engineering System): Et team med en mission om at levere værktøjer i verdensklasse, der hjælper Microsoft-udviklerne med at være så produktive og sikre som muligt. Teamet leder den centrale strategi for at sikre Microsofts komplette software-supply chain.

OpTIC (Operational Threat Intelligence Center): Teamet, der er ansvarligt for at administrere og formidle oplysninger om cybertrusler, der understøtter Microsoft CDOC's (Cyber Defense Operation Center) mission om at beskytte Microsoft og vores kunder.

Microsoft

Belysning af trusselslandskabet og forstærkning af et digitalt forsvar.

- Få mere at vide: **https://microsoft.com/mddr**
- Gå i dybden: **https://blogs.microsoft.com/on-the-issues/**
- Hold dig opdateret: **@msftissues og @msftsecurity**