Microsoft

Microsofts rapport om digitalt forsvar 2022

Fremhev trussellandskapet og styrk et digitalt forsvar.

Innhold

Dataene, innsikten og hendelsene i denne rapporten er fra juli 2021 til juni 2022 (Microsoft-regnskapsåret 2022), med mindre annet er angitt.

For best mulig opplevelse når du leser og navigerer i denne rapporten, anbefaler vi at du bruker Adobe Reader, som kan lastes ned fra Adobe-nettstedet.

Innledning av Tom Burt

Viseadministrerende direktør, kundesikkerhet og -tillit

«De mange billionene signaler vi analyserer fra vårt verdensomspennende økosystem av produkter og tjenester, avslører aggressiviteten, omfanget og skalaen av digitale trusler over hele verden»

Et øyeblikksbilde av landskapet vårt ...

Omfanget av og skalaen til trussellandskapet

Volumet av passordangrep har steget til anslagsvis 921 angrep hvert sekund – en 74 % økning på bare ett år.

Demontering av nettkriminalitet

Hittil har Microsoft fjernet mer enn 10 000 domener som brukes av nettkriminelle, og 600 som brukes av statlige aktører.

Håndtering av sårbarheter

93 % av engasjementene våre innen hendelsesre-spons ved løsepengevirus avslørte utilstrekkelig kontroll over tilgang til rettigheter og sideveis bevegelse.

23. februar 2022 gikk cybersikkerhet inn i en ny tidsalder, hybridkrigens tidsalder. Den dagen, timer før raketter ble skutt ut og stridsvogner rullet over landegrensene, lanserte russiske aktører et massivt destruktivt nettangrep mot de ukrainske myndighetene, teknologi og mål i finanssektoren i Ukraina. Du kan lese mer om disse angrepene og erfaringene fra dem i kapittelet «Statlige trusler» i denne tredje årlige utgaven av Microsofts rapport om digitalt forsvar (MDDR). Det viktigste blant disse erfaringene er at skyen gir den beste fysiske og logiske sikkerheten mot nettangrep, og muliggjør fremskritt innen trusselintelligens og sluttpunktbeskyttelse som har bevist sin verdi i Ukraina.

Selv om alle undersøkelser av utviklingen i år innen nettsikkerhet må begynne der, gir årets rapport et dypdykk i mye mer enn dette. I første kapittel i rapporten fokuserer vi på aktiviteter til nettkriminelle, etterfulgt av statlige trusler i kapittel to. Begge gruppene har angrepet på betydelig mer sofistikerte måter, noe som dramatisk har økt virkningen av handlingene deres. Mens Russland skapte overskrifter, eskalerte iranske aktører angrepene etter innsettelsen av en ny president i landet, og de iverksatte destruktive angrep rettet mot Israel og løsepengevirus og hacking-og-lekkasje-operasjoner rettet mot kritisk infrastruktur i USA. Kina økte også sin spionasjeinnsats i Sørøst-Asia og andre steder i den sørlige del av verden for å motvirke den amerikanske innflytelsen og stjele kritiske data og informasjon.

Utenlandske aktører bruker også svært effektive teknikker for å muliggjøre innflytelsespåvirkning i områder over hele verden, som omtalt i tredje kapittel. Russland har for eksempel jobbet hardt for å overbevise sine egne innbyggere, og innbyggerne i mange andre land, om at invasjonen av landet var berettiget – mens de også sådde propaganda som diskrediterte COVID-vaksiner i Vesten og samtidig fremmet effektiviteten av sine egne vaksiner i hjemlandet. I tillegg målretter aktører i økende grad mot IoT-enheter (Internet of Things) eller OT-kontrollenheter (driftsteknologi) som inngangspunkter til nettverk og kritisk infrastruktur som omtales i kapittel fire. Til slutt, i det siste kapittelet, skal vi vise innsikten og erfaringene vi har lært det siste året, når det gjelder å forsvare oss mot angrep rettet mot Microsoft og kundene våre, når vi gjennomgår årets utvikling innen cybersikkerhet.

Hvert kapittel inneholder de viktigste erfaringene og innsiktene basert på Microsofts unike oversikt. De mange billionene signaler vi analyserer fra vårt verdensomspennende økosystem av produkter og tjenester, avslører aggressiviteten, omfanget og skalaen av digitale trusler over hele verden. Microsoft iverksetter tiltak for å forsvare kundene våre og det digitale økosystemet mot disse truslene, og du kan lese om teknologien vår som identifiserer og blokkerer milliarder av phishing-forsøk, identitetstyverier og andre trusler mot kundene våre.

Innledning av Tom Burt

Fortsettelse

Vi bruker også juridiske og tekniske metoder for å overta og stenge ned infrastrukturen som brukes av nettkriminelle og statlige aktører, og varsle kunder når de blir truet eller angrepet av en statlig aktør. Vi arbeider med å utvikle stadig mer effektive funksjoner og tjenester som bruker AI-/ML-teknologi til å identifisere og blokkere cybertrusler og sikkerhetspersonell som forsvarer seg mot og identifiserer inntrenging på nettet raskere og mer effektivt.

Det som kanskje er viktigst, er at vi gjennom MDDR tilbyr våre beste råd om hva enkeltpersoner, organisasjoner og bedrifter kan gjøre for å forsvare seg mot disse økende digitale truslene. Det beste forsvaret er å innføre gode rutiner for netthygiene og redusere risikoen for nettangrep betydelig.

Statusen på nettkriminalitet

Nettkriminelle fortsetter å agere som sofistikerte profittbedrifter. Angripere tilpasser seg og finner nye måter å implementere teknikkene sine på, noe som øker kompleksiteten i hvordan og hvor de drifter infrastruktur for kampanjeoperasjoner. Samtidig blir de nettkriminelle mer nøysomme. For å redusere innsatsen og få angrepene til å se mer legitime ut kompromitterer angripere bedriftsnettverk og -enheter for å drifte phishing-kampanjer, skadelig programvare eller til og med bruke datakraften til å utvinne kryptovaluta.

Finn ut mer på side 6

«Distribusjonen av cybervåpen under hybridkrigen i Ukraina utgjør starten på en ny tidsalder med konflikt.»

Statlige trusler

Statlige aktører lanserer stadig mer sofistikerte nettangrep som er utformet for å unngå deteksjon og fremme sine strategiske prioriteringer. Distribusjonen av cybervåpen under hybridkrigen i Ukraina utgjør starten på en ny tidsalder med konflikt. Russland har også understøttet krigen med informasjonspåvirkningsoperasjoner, ved å bruke propaganda for å påvirke meninger i Russland, Ukraina og globalt. Utenfor Ukraina har statlige aktører økt aktiviteten og begynt å bruke fremskritt innen automatisering, skyinfrastruktur og teknologi for ekstern tilgang til å angripe et bredere sett med mål. IT-forsyningskjeder i bedrifter som gir tilgang til endelige mål, har ofte blitt angrepet. Det har blitt enda viktigere med nettsikkerhetshygiene etter hvert som aktører raskt utnytter ikke-oppdaterte sårbarheter, bruker både sofistikerte teknikker og rå kraft-teknikker til å stjele legitimasjon og tilslører operasjonene ved hjelp av åpen kildekode eller legitim programvare. I tillegg har Iran slått seg sammen med Russland i bruk av destruktive cybertrusler, inkludert løsepengevirus, som et fast innslag i angrepene.

Denne utviklingen krever presserende implementering av et konsistent, globalt rammeverk som prioriterer menneskerettigheter og beskytter mennesker mot hensynsløs statlig atferd på nettet. Alle nasjoner må arbeide sammen for å implementere normer og regler for ansvarlig statlig atferd.

Finn ut mer på side 30

Enheter og infrastruktur

Pandemien, kombinert med rask innføring av alle typer enheter rettet mot Internett som en komponent i den digitale transformasjonen, har i stor grad økt angrepsoverflaten i den digitale verden. Som et resultat av dette kan nettkriminelle og nasjonsstater raskt dra nytte av det. Sikkerheten til IT-maskinvare og -programvare har styrket seg de siste årene, men sikkerheten til IoT- og OT-enheter har ikke holdt tritt. Trusselaktører utnytter disse enhetene til å etablere tilgang på nettverk og muliggjøre sideveis bevegelse, for å etablere et fotfeste i en forsyningskjede eller for å forstyrre målorganisasjonens OT-operasjoner.

Finn ut mer på side 56

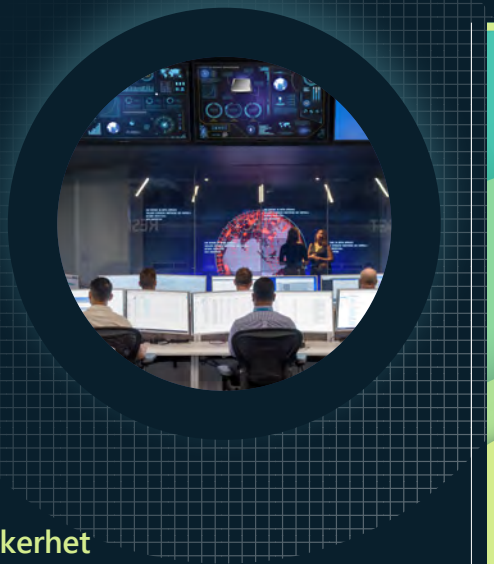
Innledning av Tom Burt

Fortsettelse

Cyberpåvirkningsoperasjoner

Nasjonalstater bruker i økende grad sofistikerte påvirkningsoperasjoner til å distribuere propaganda og påvirke opinionen i befolkningen både innenlands og internasjonalt. Disse kampanjene svekker tilliten, øker polariseringen og truer demokratiske prosesser. Dyktige, avanserte og vedvarende manipulatorer bruker tradisjonelle medier sammen med Internett og sosiale medier for å øke omfanget av, skalaen og effektiviteten til kampanjene vesentlig, og de har en enorm innvirkning i det globale informasjonsøkosystemet. I løpet av det siste året har vi sett disse operasjonene brukt som en del av Russlands hybride krig i Ukraina, men vi har også sett Russland og andre nasjoner, inkludert Kina og Iran, i økende grad ta i bruk operasjoner drevet av sosiale medier for å utvide sin globale innflytelse i en rekke saker.

Finn ut mer på side 71



Cybersikkerhet

Sikkerhet er en viktig faktor for teknologisk suksess. Innovasjon og forbedret produktivitet kan bare oppnås ved å innføre sikkerhetstiltak som gjør organisasjoner så robuste som mulig mot moderne angrep. Pandemien har utfordret oss hos Microsoft til å endre vår sikkerhetspraksis og teknologi for å beskytte våre ansatte uansett hvor de arbeider. Det siste året har trusselaktører fortsatt å dra nytte av sårbarheter eksponert under pandemien og overgangen til et hybrid arbeidsmiljø. Siden den gang har hovedutfordringen vår vært å håndtere utbredelsen og kompleksiteten til ulike angrepsmetoder og økt statlig aktivitet. I dette kapittelet gir vi detaljert informasjon om utfordringene vi har møtt, og forsvaret vi har mobilisert i respons, sammen med våre over 15 000 partnere.

Finn ut mer på side 86

Vårt unike utsiktspunkt

37 milliarder
e-posttrusler blokkert

34,7 milliarder
identitetstrusler blokkert

43 billioner
signaler syntetisert daglig, ved hjelp av sofistikert dataanalyse og AI-algoritmer for å forstå og beskytte mot digitale trusler og kriminell cyberaktivitet.

2,5 milliarder
endepunktssignaler analysert daglig

Over 8 500
ingeniører, forskere, dataforskere, eksperter på cybersikkerhet, trusseljegere, geopolitiske analytikere, etterforskere og respondenter i frontlinjen i 77 land.

Over 15 000
partnere i sikkerhetsøkosystemet vårt som øker cybersikkerheten for kundene våre.

1. juli 2021 til og med 30. juni 2022

Innledning av Tom Burt

Fortsettelse

Vi tror at Microsoft – uavhengig og gjennom våre nære partnerskap med andre i privat industri, det offentlige og det sivile samfunnet – har et ansvar for å beskytte de digitale systemene som underbygger det sosiale nettverket i samfunnet og fremmer trygge, sikre datamiljøer for enhver person, uansett hvor de befinner seg. Dette ansvaret er årsaken til at vi har publisert MDDR hvert år siden 2020. Rapporten er kulminasjonen av Microsofts mange data og omfattende forskning. Den deler vår unike innsikt i hvordan det digitale trussellandskapet utvikler seg, og de viktige tiltakene som kan iverksettes i dag for å forbedre sikkerheten i økosystemet.

Vi håper å skape en følelse av at det haster, slik at leserne iverksetter umiddelbare tiltak basert på dataene og innsikten vi presenterer både her og i våre mange nettsikkerhetspublikasjoner gjennom hele året. Når vi vurderer alvoret i trusselen mot det digitale landskapet – og hvordan dette kan overføres til den fysiske verden – er det viktig å huske at vi alle kan iverksette tiltak for å beskytte oss selv, våre organisasjoner og bedrifter mot digitale trusler.

Takk for at du tok deg tid til å gå gjennom årets Microsoft-rapport om digitalt forsvar. Vi håper du finner nyttig innsikt og verdifulle anbefalinger som kan hjelpe oss med å kollektivt forsvare det digitale økosystemet.

Tom Burt
Viseadministrerende direktør,
kundesikkerhet og -tillit

Målet vårt med denne rapporten er todelt:

1. Belyse det stadig skiftende digitale trussellandskapet for våre kunder, partnere og interessenter som spenner over det bredere økosystemet, og som kaster lys over både nye cyberangrep og utviklingstrender i historisk vedvarende trusler.
2. Gi våre kunder og partnere mulighet til å forbedre cybersikkerheten og reagere på disse truslene.

Statusen på nettkriminalitet

Etter hvert som cyberforsvaret forbedres og flere organisasjoner tar en proaktiv tilnærming til forebygging, tilpasser angriperne teknikkene sine.

En oversikt over

Statusen på nettkriminalitet

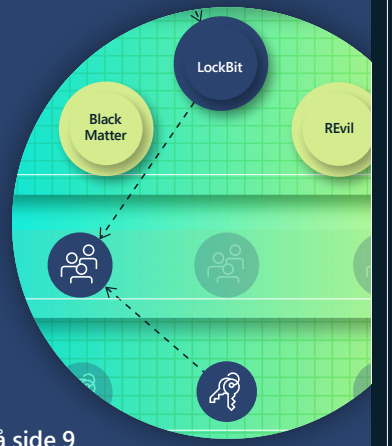
Etter hvert som cyberforsvaret forbedres og flere organisasjoner tar en proaktiv tilnærming til forebygging, tilpasser angriperne teknikkene sine.

Nettkriminelle fortsetter å agere som sofistikerte profittbedrifter. Angripere tilpasser seg og finner nye måter å implementere teknikkene sine på, noe som øker kompleksiteten i hvordan og hvor de drifter infrastruktur for kampanjeoperasjoner. Samtidig blir de nettkriminelle mer nøysomme. For å redusere innsatsen og få angrepene til å se mer legitime ut kompromitterer angripere bedriftsnettverk og -enheter for å drifte phishing-kampanjer, skadelig programvare eller til og med bruke datakraften til å utvinne kryptovaluta.

Cyberkriminalitet fortsetter å øke etter hvert som industrialiseringen av cyberkriminalitetsøkonomien senker kompetansebarrieren for å komme i gang, ved å gi økt tilgang til verktøy og infrastruktur.

Finn ut mer på side 18

Trusselen om løsepengevirus og utpressing blir stadig mer merkbar med angrep rettet mot regjeringer, bedrifter og kritisk infrastruktur.

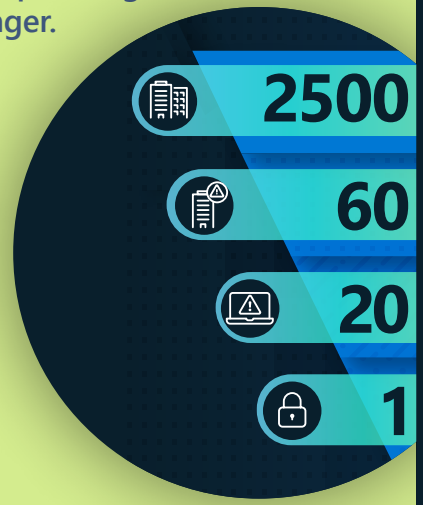


Finn ut mer på side 9

Angripere truer i økende grad med å avsløre sensitive data for å oppmuntre til betaling av løsepenger.

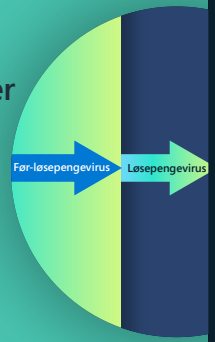
Finn ut mer på side 10

Menneskelig operert løsepengevirus er mest utbredt, da en tredjedel av målene er kompromittert av kriminelle aktører som bruker disse angrepene, og 5 % av disse er løsepenger.



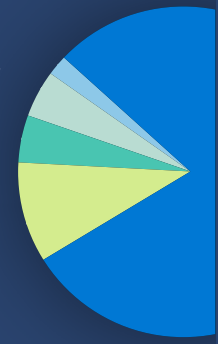
Finn ut mer på side 9

Det mest effektive forsvaret mot løsepengevirus inkluderer flerfaktorautentisering, hyppige sikkerhets-oppdateringer og prinsipper for nulltillit over hele nettverks-arkitekturen.



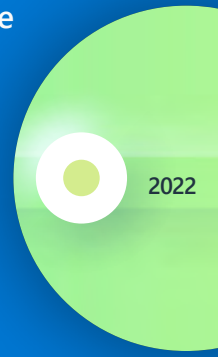
Finn ut mer på side 13

Phishing etter påloggingsinformasjon som ukritisk målretter alle innbokser, er økende, og bedrifts-e-postinnbrudd, inkludert fakturasvindel, utgjør en betydelig cyberkriminalitetsrisiko for bedrifter.



Finn ut mer på side 21

For å forstyrre den ondsinnede infrastrukturen til nettkriminelle og statlige aktører er Microsoft avhengig av innovative tilnærminger innenfor loven og våre offentlige og private partnerskap.



Finn ut mer på side 25

Innledning

Cyberkriminalitet fortsetter å øke, med økninger i både tilfeldige og målrettede angrep.

Etter hvert som cyberforsvaret forbedres og flere regjeringer og bedrifter bruker en proaktiv tilnærming til forebygging, ser vi at angripere bruker to strategier for å få tilgangen som kreves for å legge til rette for cyberkriminalitet. Den ene tilnærmingen er en kampanje med brede mål som avhenger av volum. Den andre bruker overvåking og mer selektiv målretting for å øke avkastningsraten. Selv når inntektsgenerering ikke er målet – for eksempel statlig aktivitet for geopolitiske formål – brukes både tilfeldige og målrettede angrep. Det siste året har nettkriminelle fortsatt å stole på sosial manipulering og utnyttelse av aktuelle saker for å maksimere suksessen til kampanjer. Eksempel: Mens phishing-lokkemidler med COVID-tema ble brukt sjeldnere, observerte vi at lokkemidler som pengegaver for å støtte innbyggerne i Ukrainia, ble brukt i økende grad.

Angripere tilpasser seg og finner nye måter å implementere teknikkene sine på, noe som øker kompleksiteten i hvordan og hvor de drifter infrastruktur for kampanjeoperasjoner. Vi har observert at nettkriminelle blir mer nøysomme, og angripere betaler ikke lenger for teknologi. For å redusere innsatsen og få angrepene til å se mer legitime ut forsøker enkelte angripere i stadig større grad å kompromittere bedrifter for å drifte phishing-kampanjer, skadelig programvare eller til og med bruke datakraften til å utvinne kryptovaluta.

I dette kapittelet undersøker vi også økningen av hacktivisme, en forstyrrelse forårsaket av at private innbyggere utfører cyberangrep for å fremme sosiale eller politiske mål. Tusenvis av enkeltpersoner over hele verden, både eksperter og nybegynnere, har mobilisert siden februar 2022 for å starte angrep, som for eksempel deaktivering av nettsteder og lekkasje av stjålne data, som en del av krigen mellom Russland og Ukraina. Det er for tidlig å forutsi om denne trenden vil fortsette etter slutten på den aktive krigføringen.

Organisasjoner må jevnlig gå gjennom og forsterke tilgangskontroller og implementere sikkerhetsstrategier for å forsvare seg mot cyberangrep. Det er imidlertid ikke alt de kan gjøre. Vi forklarer hvordan vår avdeling for digital kriminalitet (DCU) har brukt sivile saker til å ta over ondsinnet infrastruktur som brukes av nettkriminelle og statlige aktører. Vi må bekjempe denne trusselen sammen gjennom både offentlige og private partnerskap. Vi håper at vi kan hjelpe andre med å forstå og vurdere de proaktive tiltakene de kan iverksette for å beskytte seg selv og det bredere økosystemet mot den stadig økende trusselen om cyberkriminalitet, ved å dele det vi har lært de siste 10 årene.

Amy Hogan-Burney
Daglig leder, avdeling for digital kriminalitet

Løsepengevirus og utpressing: en trussel på nasjonsnivå

Angrep med løsepengevirus utgjør en økt fare for alle personer, siden kriminelle som utnytter et stadig voksende økosystem for nettkriminalitet, retter seg inn mot kritisk infrastruktur, bedrifter av alle størrelser og statlige og lokale myndigheter.

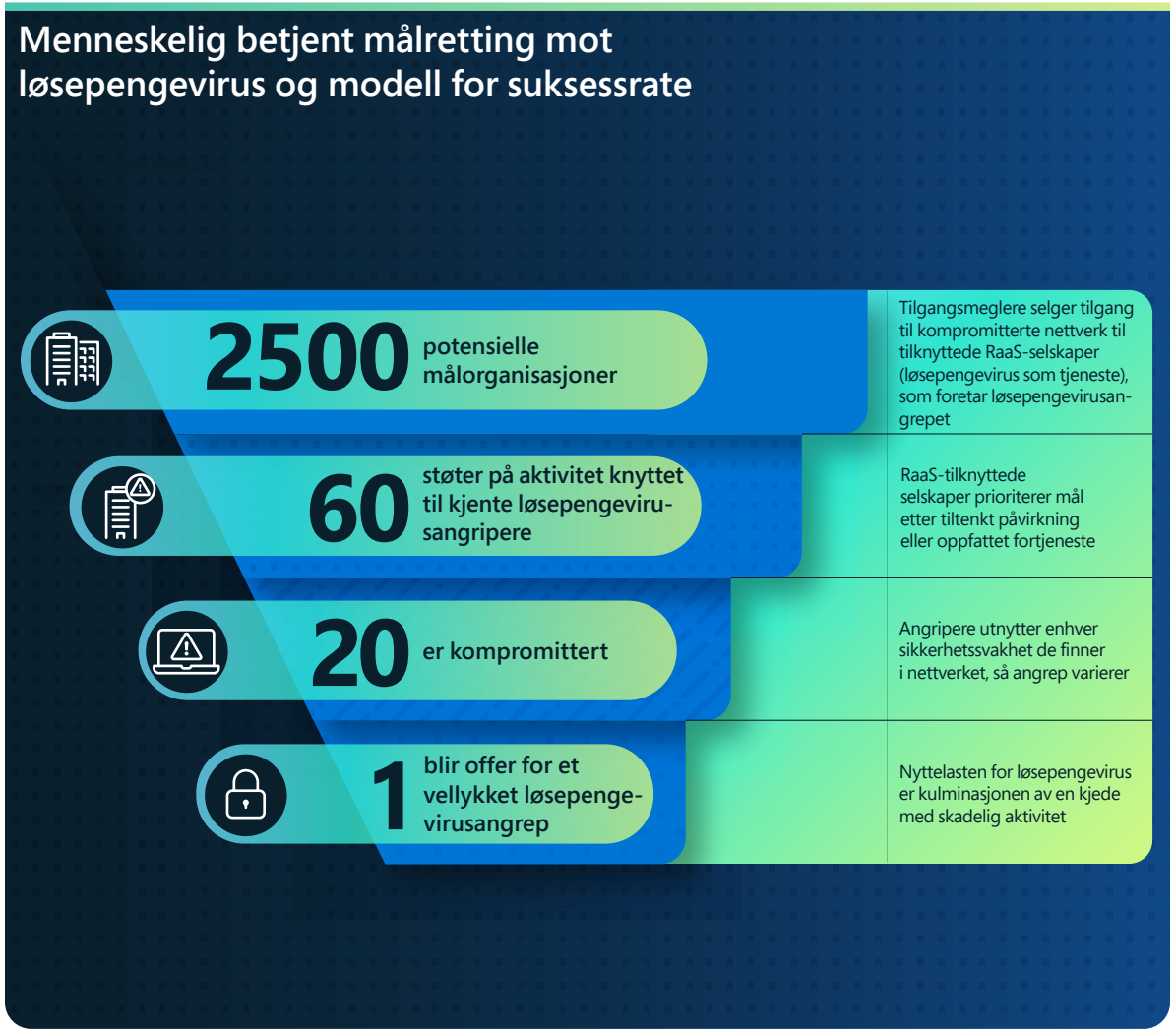
I løpet av de siste to årene har høyprofilerte hendelser med løsepengevirus – for eksempel hendelser som involverer kritisk infrastruktur, helsevesen og IT-tjenesteleverandører – fått stor offentlig oppmerksomhet. Etter hvert som omfanget av angrep med løsepengevirus har blitt mer merkbart, har effektene blitt mer omfattende. Følgende er eksempler på angrep vi har sett så langt i 2022:

- I februar rammet et angrep på to selskaper betalingsbehandlingssystemene til hundrevis av bensinstasjoner i Nord-Tyskland.[1]
- I mars lyktes et angrep mot postvesenet i Hellas midlertidig med å forstyrre leveringen av post og påvirket behandlingen av finansielle transaksjoner.[2]
- Sent i mai tvang et løsepengevirusangrep mot statlige byråer i Costa Rica frem en nasjonal nødsituasjon etter at sykehusene ble stengt og toll- og skatteinnkrevingen ble avbrutt.[3]
- I mai forårsaket også et angrep forsinkelser og kanselleringer for et av Indias største flyselskaper, noe som gjorde at hundrevis av passasjerer ble rammet.[4]

Suksessen til disse angrepene og omfanget av innvirkningen i den virkelige verden er resultatet av en industrialisering av cyberkriminalitetsøkonomien, noe som har gitt tilgang til verktøy og infrastruktur og en økning av kapasiteten til nettkriminelle grunnet en lavere kompetansebarriere for å komme i gang.

De siste årene har løsepengevirus gått fra en modell der én enkelt «gjeng» både utviklet og distribuerte en nyttelast for løsepengevirus, til RaaS-modellen (løsepengevirus som tjeneste). Med RaaS kan én gruppe administrere utviklingen av nyttelasten for løsepengeviruset og tilby tjenester for betaling og utpressing via datalekkasje til andre nettkriminelle – de som faktisk lanserer angrep fra løsepengevirus – referert til som «tilknyttede selskaper», for en del av fortjenesten. Denne utkontraheringen av cyberkriminalitetsøkonomien har utvidet angriperutvalget. Industrialiseringen av verktøy for nettkriminelle har gjort det enklere for angripere å utføre inntrenging, eksfiltrere data og ta i bruk løsepengevirus.

Løsepengevirus betjent av mennesker[5] – et begrep innført av Microsoft-forskere for å beskrive trusler drevet av mennesker som tar avgjørelser på hvert trinn i angrepene, basert på det de oppdager i målets nettverk, og avgrenser trusselen fra vanlige angrep med løsepengevirus – er fortsatt en betydelig trussel mot organisasjoner.



Modell basert på Microsoft Defender for endepunkt-data (EDR) (januar–juni 2022).

Løsepengevirus og utpressing: en trussel på nasjonsnivå

Fortsettelse

Angrep med løsepengevirus har blitt enda mer virkningsfulle etter hvert som innføringen av en inntjeningsstrategi med dobbel utpressing har blitt en standardpraksis. Dette innebærer å eksfiltrere data fra kompromitterte enheter, kryptere dataene på enhetene og deretter publisere eller true med å publisere de stjålne dataene offentlig for å presse ofrene til å betale løsepenger.

Selv om de fleste løsepengevirusangripere opportunistisk distribuerer løsepengevirus til det nettverket de får tilgang til, kan enkelte kjøpe tilgang fra andre nettkriminelle og utnytte forbindelser mellom tilgangsmeglere og operatører av løsepengevirus.

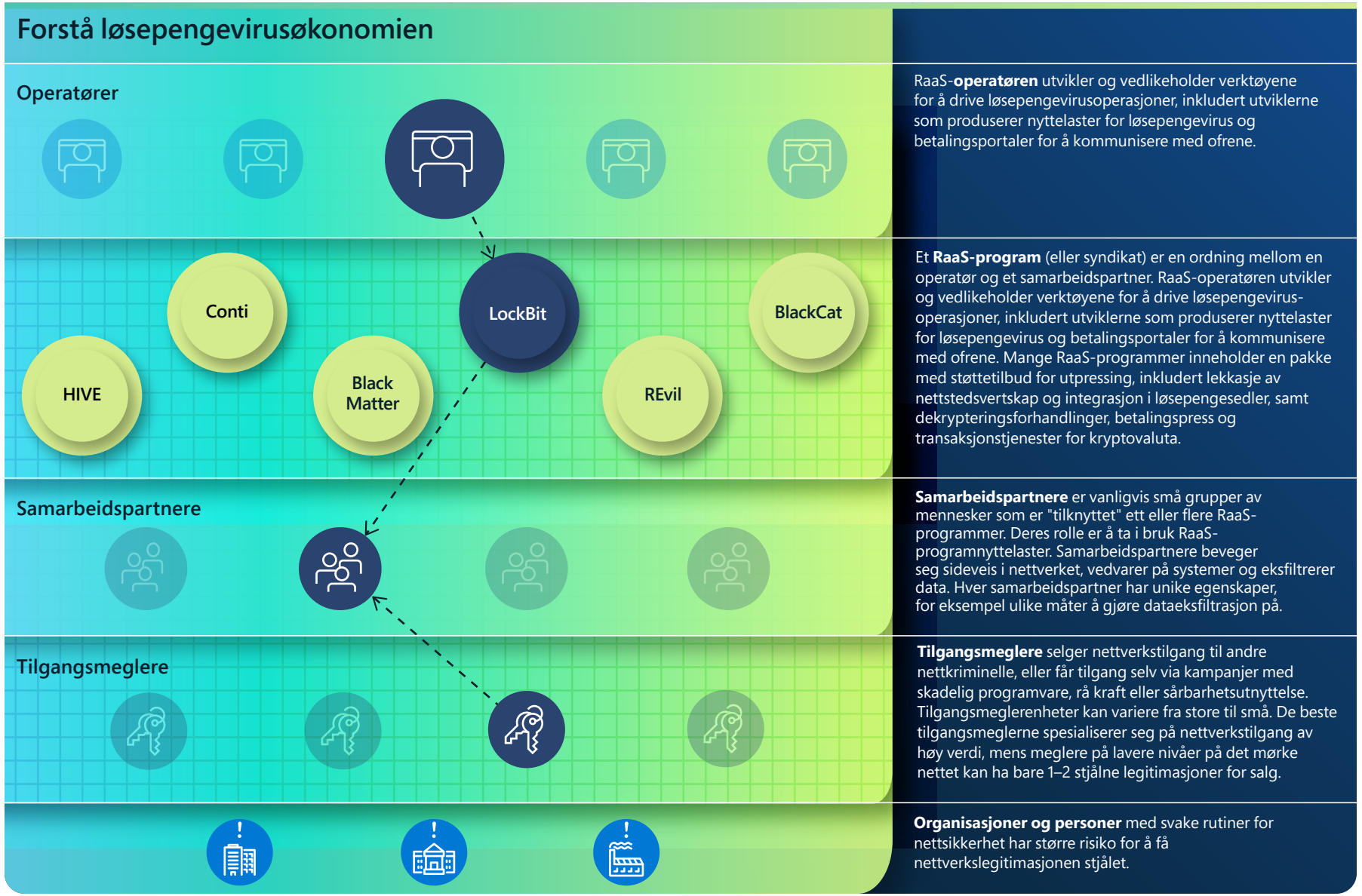
Vår unike bredde av signalintelligens er samlet inn fra flere kilder – identitet, e-post, endepunkter og skyen – og gir innsikt i den voksende løsepengevirusøkonomien, med et samarbeidssystem som inneholder verktøy utviklet for angripere med mindre teknisk innsikt.

Utvidede relasjoner mellom spesialiserte nettkriminelle har økt tempoet, kompleksiteten og suksessen til angrep fra løsepengevirus. Dette har drevet utviklingen av det nettkriminelle økosystemet til tilkoblede aktører med ulike teknikker, mål og ferdigheter som støtter hverandre ved innledende tilgang til mål, betalingstjenester og verktøy eller nettsteder for dekryptering eller publikasjon.

Operatører av løsepengevirus kan nå kjøpe tilgang til organisasjoner eller offentlige nettverk direkte på nettet eller få legitimasjon og tilgang via mellommenneskelige relasjoner med meglere, der hovedmålet utelukkende er å tjene penger på tilgangen de har fått.

Operatørene bruker deretter den kjøpte tilgangen til å distribuere en nyttelast for løsepengevirus kjøpt via mørke markedsplasser eller fora på nettet. I mange tilfeller gjennomføres forhandlinger med ofrene av RaaS-teamet, ikke av selve operatørene. Disse kriminelle transaksjonene er sømløse, og deltakerne risikerer liten sjanse for å bli pågrepet og straffet på grunn av anonymiteten i det mørke nettet og vanskeligheter med å håndheve lover på tvers av nasjoner.

En bærekraftig og vellykket innsats mot denne trusselen vil kreve at en helhetlig offentlig strategi gjennomføres i nært samarbeid med privat sektor.



I motsetning til hvordan løsepengevirus enkelte ganger fremstilles i media, er det sjeldent at én enkelt variant av løsepengevirus administreres av en «løsepengevirusgjeng» som gjør alt selv. I stedet finnes det separate enheter som utvikler skadelig programvare, får tilgang til ofre, distribuerer løsepengevirus og håndterer utpressingsforhandlinger. Industrialiseringen av det kriminelle økosystemet har ført til følgende:

- Tilgangsmeglere som bryter inn og gir tilgang (tilgang som tjeneste).
- Utviklere av skadelig programvare som selger verktøy.
- Kriminelle operatører og tilknyttede selskaper som utfører inntrenging.
- Leverandører av krypterings- og utpressingstjenester som overtar inntektsmuligheter fra tilknyttede selskaper (RaaS).

Alle menneskeopererte kampanjer for løsepengevirus deler felles avhengigheter av sikkerhetssvakheter. Spesielt drar angripere vanligvis nytte av den dårlige netthygienen til en organisasjon, som ofte inkluderer sjelden oppdatering og manglende implementering av flerfaktorautentisering (MFA).

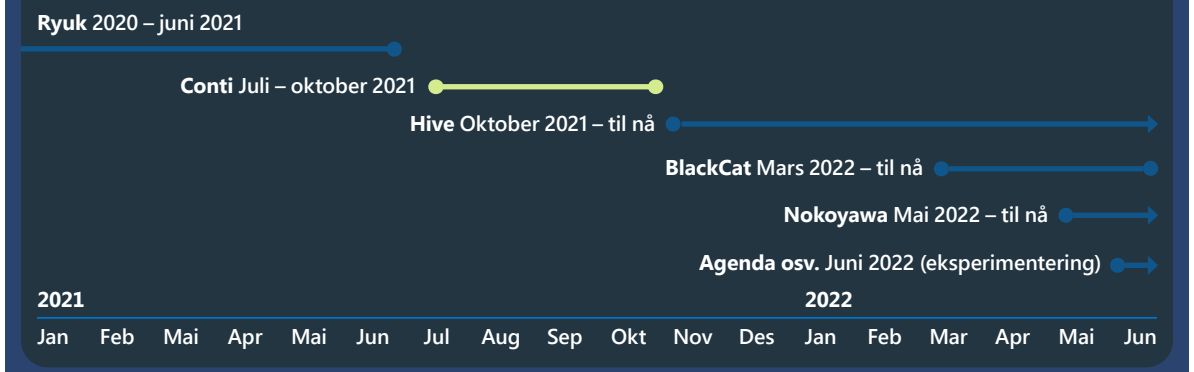
Kundehistorie: Oppløsningen av Conti

Conti, en av de mest populære variantene av løsepengevirus de siste to årene, begynte å stenge driften i midten av 2022. Microsoft Threat Intelligence Center (MSTIC) observerte en betydelig nedgang i aktiviteten i slutten av mars og begynnelsen av april. Vi observerte de siste utrullingene av løsepengevirus fra Conti i midten av april. På samme måte som avstengingen av andre løsepengevirusoperasjoner hadde Contis oppløsning imidlertid ikke en betydelig innvirkning på utrulling av løsepengevirus, da MSTIC observerte at selskaper tilknyttet Conti snudde på hælen og tok i bruk andre nyttelaster for løsepengevirus, inkludert BlackBasta, Lockbit 2.0, LockbitBlack og HIVE. Dette samsvarer med data fra tidligere år og antyder at når løsepengevirusgjenger blir frakoblet, dukker de opp igjen måneder senere eller videredistribuerer sine tekniske funksjoner og ressurser til nye grupper.

Våre Microsoft-grupper for trusselintelligens sporer aktører som truer med løsepengevirus, som individuelle grupper (merket som DEV-er) basert på deres spesifikke verktøy, i stedet for å spore dem etter den skadelige programvaren de bruker. Da selskaper tilknyttet Conti fortsatte å spre seg, kunne vi dermed fortsette å spore disse DEV-ene gjennom deres bruk av andre verktøy eller RaaS-pakker. Eksempler:

- DEV-0230, som er tilknyttet Trickbot, var en profilert bruker av Conti. I slutten av april observerte MSTIC dette ved hjelp av QuantumLocker.
- DEV-0237 byttet fra Contis løsepengeviruspakker til HIVE og Nokoyawa, inkludert bruk av HIVE i angrepet 31. mai mot myndighetene i Costa Rica.
- DEV-0506, en annen profilert bruker av Contis løsepengeviruspakke, ble observert ved hjelp av BlackBasta.

Eksempel på en samarbeidspartner (DEV-0237) som raskt bytter mellom RaaS-programmer



Etter at et RaaS-program som Conti er stengt ned, bytter samarbeidspartneren for løsepengevirus til et annet (Hive) nesten umiddelbart.

RaaS utvikler økosystemet for løsepengevirus og hindrer tilskrivelse

Siden menneskeoperert løsepengevirus drives av individuelle operatører, varierer angrepsmønstrene basert på målet og alternerer gjennom angrepets varighet. Tidligere observerte vi en nær sammenheng mellom den første inngangsvektoren, verktøyene og nyttelastvalgene for løsepengevirus i hver kampanje med én enkelt belastning for løsepengevirus. Dette gjorde tilskrivelsen enklere. RaaS-samarbeidsmodellen frakobler imidlertid dette forholdet. Som et resultat sporer Microsoft løsepengevirus fra samarbeidspartnere som distribuerer nyttelast i bestemte angrep, i stedet for å spore utviklerne av løsepengevirusnyttelaster som operatører.

Sagt på en annen måte antar vi ikke lenger at HIVE-utvikleren er operatøren bak et HIVE-angrep med løsepengevirus. Det er mer sannsynlig at det er en samarbeidspartner.

Nettsikkerhetsbransjen har slitt med å fange opp denne avgrensningen mellom utviklere og operatører i tilstrekkelig grad. Bransjen rapporterer fortsatt ofte om en løsepenge-virushendelse etter navnet på nyttelasten, noe som gir det falske inntrykket av at én enkelt enhet, eller en løsepengevirusgjeng, står bak alle angrep som bruker den aktuelle nyttelasten for løsepengevirus, og alle hendelser knyttet til den deler felles teknikker og infrastruktur. For å understøtte forsvarere på nettverket er det viktig å lære mer om fasene før et angrep fra ulike samarbeidspartnere – for eksempel dataeksfiltrasjon og ytterligere utholdenhetsmekanismer – samt gjenkjennings- og beskyttelsesmulighetene som kan eksistere.

I tillegg til skadelig programvare trenger angripere legitimasjon for å lykkes i operasjonene sine. En vellykket menneskelig operert infisering av løsepengevirus i en hel organisasjon er avhengig av tilgang til en høyprivilegert konto.

Søkelys på menneskedrevet løsepengevirusangrep

I løpet av det siste året gjennomførte Microsofts eksperter på løsepengevirus grundige undersøkelser av over 100 menneskelig opererte hendelser med løsepengevirus for å spore angripers teknikker og forstå hvordan vi kan beskytte kundene våre bedre.

Det er viktig å merke seg at analysen vi deler her, bare er mulig for klargjorte, administrerte enheter. Ikke-klargjorte, uadministrerte enheter representerer den minst sikre delen av maskinvareressursene i en organisasjon.

Mest utbredte faseteknikker for løsepengevirus:

75 %
Bruk administrasjonsverktøy.

75 %
Bruk anskaffet opphøyd kompromittert brukerkonto til å spre skadelige nyttelaster gjennom SMB-protokollen.

99 %
Forsøk på å tukle med oppdagede sikkerhets- og sikkerhetskopieringsprodukter ved hjelp av verktøy bygd i et OS.

Det typiske menneskeopererte angrepet

Menneskeopererert løsepengevirusangrep kan kategoriseres i fasen før løsepengevirus og utrullingsfasen for løsepengevirus. I fasen før løsepengevirus forbereder angripere seg på å infiltrere nettverket ved å lære om organisasjonens typologi og sikkerhetsinfrastruktur.

Stopp angriperne før de når utrullingsfasen for løsepengevirus	**Utplassering!**
Før-løsepengevirus	**Løsepengevirus**
Denne fasen kan variere fra noen dager til flere uker eller måneder, selv om den har blitt kortere i løpet av de siste to årene.	Denne fasen kan vare i kun noen minutter
Angripere forbereder seg på å infiltrere nettverket ved å lære så mye som mulig om topologien og sikkerhetsinfrastrukturen. Angripere kan også eksfiltrere data i denne fasen.	Angripere har som mål å kryptere så mye data som mulig

Undersøkelsene våre avdekket at de fleste aktører bak menneskelig opererte løsepengevirusangrep utnytter sikkerhetssårbarheter som ligner på hverandre, og deler vanlige angrepsmønstre og teknikker.

En holdbar sikkerhetsstrategi

Bekjemping og forebygging av slike angrep krever et skifte i organisasjonens tankesett for å fokusere på den omfattende beskyttelsen som kreves for å bremse og stoppe angripere før de kan gå fra fasen før løsepengevirus til utrullingsfasen for løsepengevirus.

Bedrifter må bruke beste praksiser for sikkerhet konsekvent og aggressivt på nettverkene sine, der målet må være å begrense angrepsklasser. Fordi beslutningene blir tatt av mennesker kan disse løsepengevirusangrepene generere flere, tilsynelatende atskilte sikkerhetsproduktvarsler som lett kan gå tapt eller ikke bli respondert på i tide. Varselstretthet er reelt, og sikkerhetsoperasjonssentre (SOC-er) kan forenkle ting ved å se på trender i varslene eller gruppere varsler i hendelser, slik at de kan se det større bildet. SOC-er kan deretter begrense varslene ved hjelp av herdingsfunksjoner, for eksempel regler for reduksjon av angrepsoverflaten. Herding mot vanlige trusler kan ikke bare redusere varselvolumet, men også stoppe mange angripere før de får tilgang til nettverkene.

Organisasjoner må opprettholde kontinuerlige høye standarder for sikkerhetsholdning og nettverks-hygiene for å beskytte seg mot menneskeopererte løsepenge-virusangrep.

Handlingsrettet innsikt

Angripere med løsepengevirus er motivert av enkel fortjeneste, så å øke kostnadene via sikkerhetsforsterkning er nøkkelen til å ødelegge for den cyberkriminelle økonomien.

1. Bygg legitimasjonshygiene. I tillegg til skadelig programvare trenger angripere legitimasjon for å lykkes i operasjonene sine. En vellykket menneskeopererert løsepengevirusinfeksjonen i en hel organisasjon avhenger av tilgang til en konto med høye privilegier, for eksempel en domeneadministrator, eller muligheten til å redigere grupperetningslinjer.
2. Eksponering for revisjonslegitimasjon.
3. Prioriter distribusjon av Active Directory-oppdateringer.
4. Prioriter forsterkning i skyen.
5. Reduser angrepsoverflaten.
6. Forsterk ressurser vendt mot Internett og forstå perimeteren din.
7. Reduser alarmtretthet fra sikkerhets-senteret ved å forsterke nettverket for å redusere volumet og bevare båndbredden for høyprioritetshendelser.

Koblinger til mer informasjon

- RaaS: Forstå nettkriminalitetsøkonomien og hvordan du beskytter deg selv | Microsoft Security Blog
- Menneskeopererert løsepengevirusangrep: en katastrofe som kan forebygges | Microsoft Security Blog

Innsikt i løsepengevirus fra frontlinjepersonalet

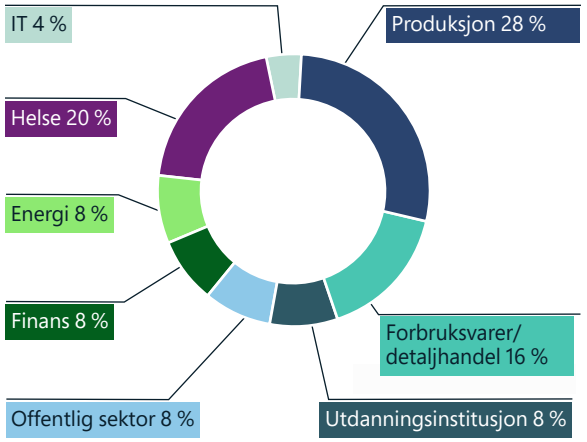
Organisasjoner over hele verden opplevde en jevn vekst i menneskeopererte løsepengevirusangrep fra og med 2019. Operasjoner fra politimyndigheter og geopolitiske hendelser i fjor hadde imidlertid en betydelig innvirkning på cyberkriminelle organisasjoner.

Microsofts servicetelefon for sikkerhet understøtter kunder gjennom et helt cyberangrep, fra undersøkelse til vellykket begrensning og gjenoppretting. Responsen og gjenopprettingstjenestene tilbys via to svært integrerte arbeidsgrupper, der den ene fokuserer på undersøkelse og grunnarbeid for gjenoppretting, og den andre på begrensning og gjenoppretting. Denne delen inneholder et sammendrag av funn basert på engasjement rundt løsepengevirus det siste året.

93 %

av Microsofts undersøkelser under engasjementer for gjenoppretting etter løsepengevirus avslørte utilstrekkelig kontroll av rettighetstilgang og sideveis bevegelse.

Løsepengevirushendelser og gjenopprettingsengasjementer etter bransje

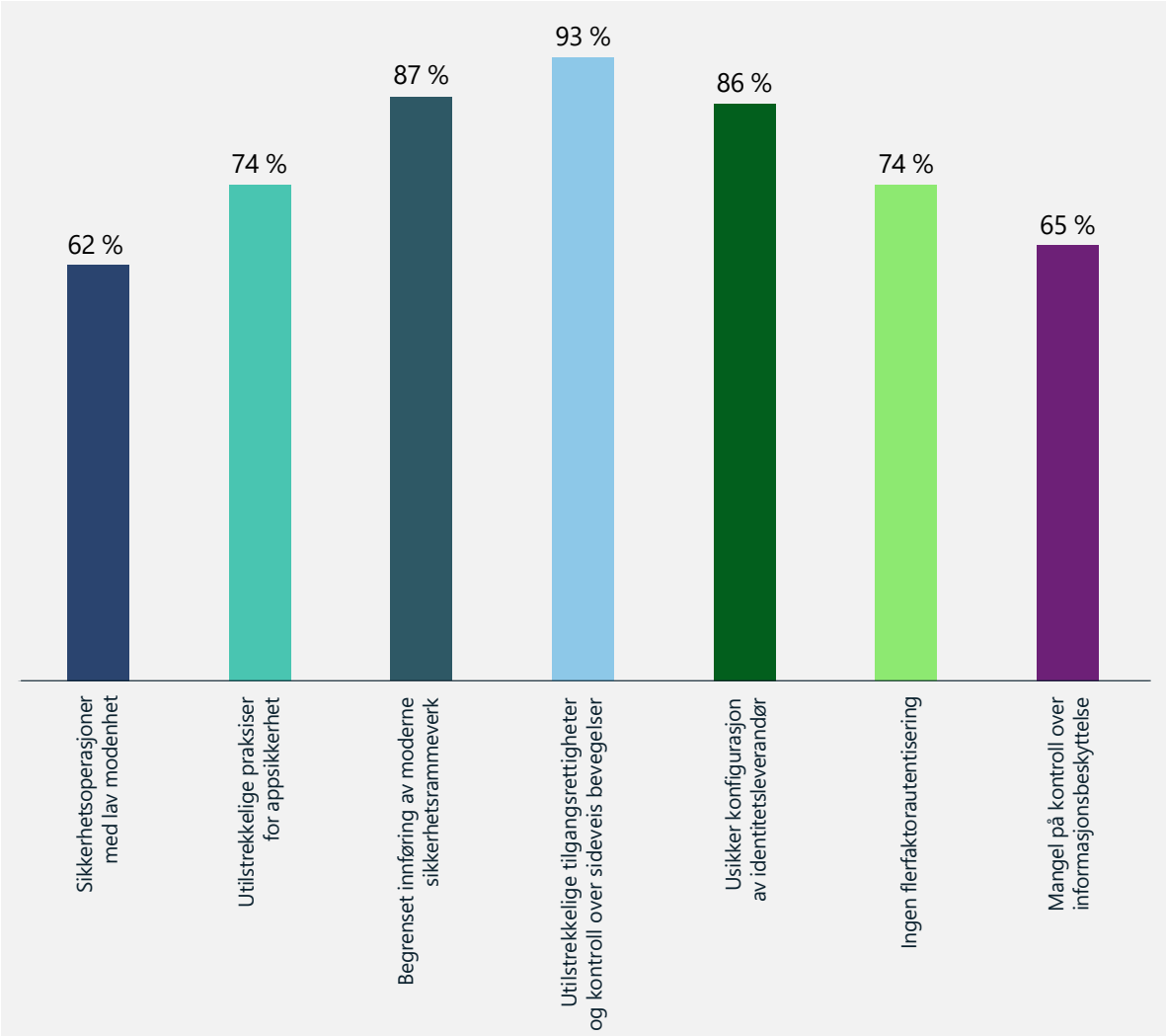


Etter hvert som nye små grupper og trusler dukker opp, må forsvarende arbeidsgrupper være oppmerksomme på nye løsepengevirustrusler, samtidig som de beskytter mot tidligere ukjente serier av med skadelig programvare med løsepengevirus. Den raske utviklingstilnærmingen som brukes av kriminelle grupper, har ført til etableringen av intelligente løsepengevirus pakket i brukervennlige sett. Dette gir større fleksibilitet til å gjennomføre spredte angrep på et høyere antall mål.

Følgende sider gir et dypere innblikk i de mest observerte medvirkende faktorene til svak beskyttelse mot løsepengevirus, gruppert i tre kategorier av funn:

1. Svake identitetskontroller
2. Ineffektive sikkerhetsoperasjoner
3. Begrenset databeskyttelse

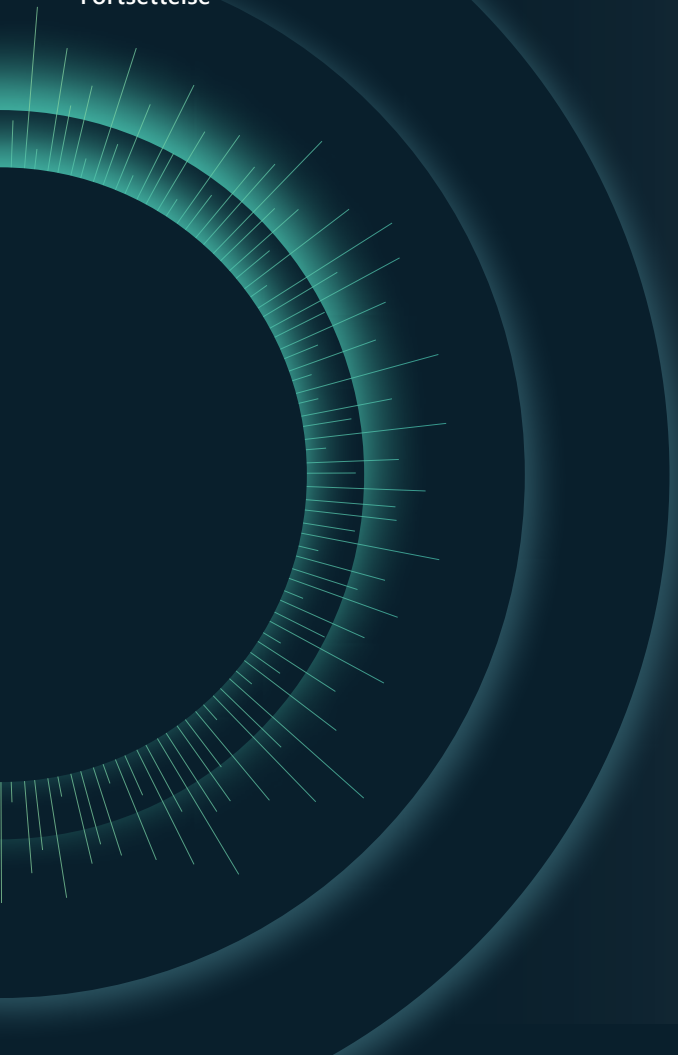
Sammendrag av de vanligste funnene i engasjementer for respons på løsepengevirus



Det vanligste funnet blant engasjementer for respons på løsepengevirushendelser var utilstrekkelig kontroll av rettighetstilgang og sideveis bevegelse.

Innsikt i løsepengevirus fra frontlinjepersonalet

Fortsettelse



De tre viktigste medvirkende faktorene sett i våre responsoppdrag på stedet:

① **Svake identitetskontroller:** Legitimasjonstyveriangrep er fortsatt en av de viktigste faktorene

② **Ineffektive sikkerhetsprosesser** utgjør ikke bare et åpent vindu av muligheter for angripere, men har også en betydelig negativ innvirking på tiden som brukes på gjenoppretting

③ Til syvende og sist handler det om data – organisasjoner sliter med å implementere en effektiv **databeskyttelsesstrategi** som samsvarer med forretningsbehovene deres

① Svake identitetskontroller

Menneskeopererte løsepengevirus fortsetter å utvikle seg og tar i bruk legitimasjonstyveri og metoder for sideveis bevegelse som tradisjonelt er forbundet med målrettede angrep. Vellykkede angrep er ofte et resultat av langvarige kampanjer som involverer kompromittering av identitetssystemer, for eksempel Active Directory (AD), som gjør det mulig for menneskelige operatører å stjele legitimasjon, få tilgang til systemer og forbli i nettverket.

Active Directory (AD) og Azure AD-sikkerhet

88 %

av berørte kunder tok ikke i bruk anbefalte fremgangsmåter for AD- og Azure AD-sikkerhet. Dette har blitt en vanlig angrepsvektor når angripere utnytter feilkonfigurasjoner og svakere sikkerhetsholdninger i kritiske identitetssystemer for å få bredere tilgang og innvirkning på bedrifter.

Tilgang med minste privilegium og bruk av arbeidsstasjoner med privilegert tilgang (PAW)

Ingen av de berørte organisasjonene implementerte tilstrekkelig administrativt skille av legitimasjon og prinsipper for tilgang med minste privilegium via dedikerte arbeidsstasjoner under administrasjonen av kritiske identitets- og høyverdiressurser, for eksempel proprietære systemer og forretningskritiske apper.

Sikkerhet for privilegerte kontoer

88 %

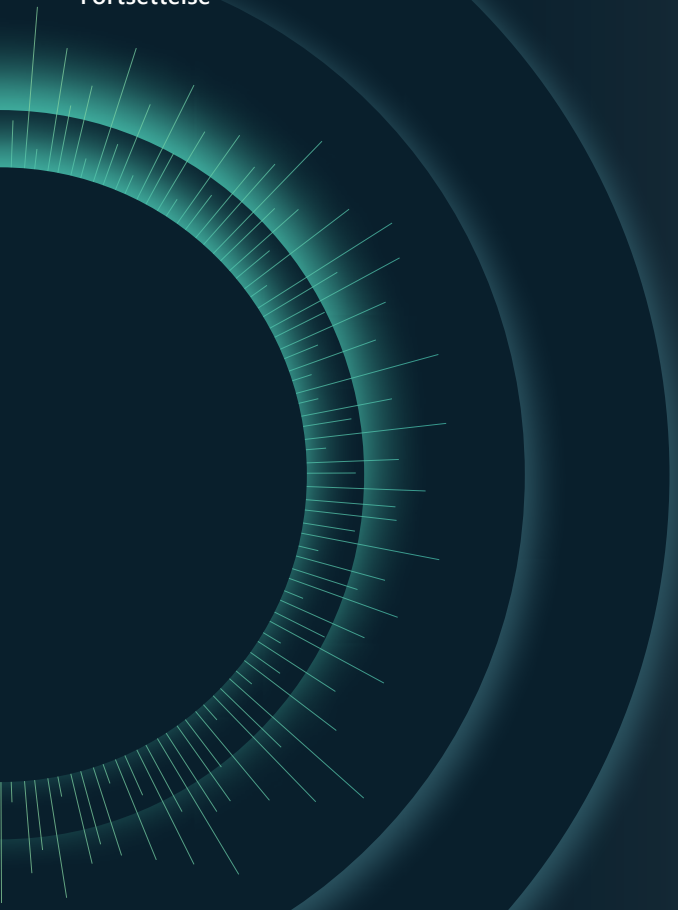
av engasjementer ble MFA ikke implementert for sensitive og høyt privilegerte kontoer, noe som etterlot et sikkerhetsgap, der angripere kunne kompromittere legitimasjon og innrette videre angrep ved hjelp av legitim legitimasjon.

84 %

Administratorer i 84 prosent av organisasjonene brukte ikke ID-kontroller for rettigheter, for eksempel JIT-tilgang (just-in-time), for å hindre ytterligere ondsinnet bruk av kompromittert privilegert legitimasjon.

Innsikt i løsepengevirus fra frontlinjepersonalet

Fortsettelse



② Ineffektive sikkerhetsoperasjoner

Dataene våre viser at organisasjoner som ble rammet av løsepengevirusangrep, har betydelige hull i livssyklusadministrasjonen av sikkerhetsoperasjoner, verktøy og informasjonsteknologiressurser. Følgende hull ble oftest observert basert på de tilgjengelige dataene:

Oppdatering:

68 %

av berørte organisasjoner hadde ikke en effektiv prosess for administrasjon av sårbarheter og oppdateringer, og en høy avhengighet av manuelle prosesser kontra automatisert oppdatering førte til kritiske åpninger. Produksjon og kritisk infrastruktur fortsetter å slite med vedlikehold og oppdatering av eldre driftsteknologisystemer (OT).

Mangel på verktøy for sikkerhetsoperasjoner:

De fleste organisasjoner rapporterte en mangel på ende-til-ende-sikkerhetssynlighet på grunn av mangel på eller feilkonfigurasjon av sikkerhetsverktøy, noe som fører til redusert effektivitet for oppdagelse og respons.

60 %

av organisasjoner rapporterte ingen bruk av et EDR-verktøy[6], en grunnleggende teknologi for deteksjon og respons.

60 %

investerte ikke i SIEM-teknologi (administrasjon av sikkerhetsinformasjon og -hendelser), noe som fører til overvåking av siloer, begrenset evne til å oppdage ende-til-ende-trusler og ineffektive sikkerhetsoperasjoner. Automatisering er fortsatt et viktig gap i SOC-verktøy og -prosesser, noe som tvinger SOC-personell til å bruke utallige timer på å forstå sikkerhetstelemetri.

84 %

av berørte organisasjoner hadde ikke muliggjort integrasjon av miljøer med flere skyer i sine verktøy for sikkerhetsoperasjoner.

Respons- og gjenopprettingsprosesser:

76 %

Mangel på en effektiv responsplan var et kritisk område som ble observert i 76 prosent av berørte organisasjoner, og dette forhindret riktig organisatorisk kriseberedskap og hadde negativ innvirkning på reaksjons- og gjenopprettingstiden.

③ Begrenset databeskyttelse

Mange kompromitterte organisasjoner manglet tilstrekkelige databeskyttelses-prosesser, noe som førte til en alvorlig innvirkning på gjenopprettingstider og muligheten til å returnere til forretnings-driften. De vanligste hullene som ble oppdaget, inkluderer følgende:

Uforanderlig sikkerhetskopi:

44 %

av organisasjoner hadde ikke uforanderlige sikkerhetskopier for de berørte systemene. Data viser også at administratorer ikke har sikkerhetskopierings- og gjenopprettingsplaner for kritiske ressurser, for eksempel AD.

Forebygging av datatap:

Angripere finner vanligvis sin måte å kompromittere systemer på ved å utnytte sårbarheter i organisasjonen, og de henter ut kritiske data for utpressing, tyveri av immaterielle rettigheter eller inntektsgenerering.

92 %

av berørte organisasjoner implementerte ikke effektive kontroller for hindring av datatap for å redusere disse risikoene, noe som fører til kritisk tap av data.

Løsepengevirus gikk tilbake i enkelte regioner og frem i andre

I år observerte vi en nedgang i det totale antallet saker om løsepengevirus rapportert til våre responsgrupper i Nord-Amerika og Europa sammenlignet med året før. Samtidig økte antallet rapporterte saker i Latin-Amerika.

En tolkning av denne observasjonen er at kriminelle vendte seg bort fra områder som ble oppfattet å ha en høyere risiko for å utløse politimyndigheters gransking til fordel for mykere mål. Siden Microsoft ikke observerte en betydelig forbedring i sikkerheten for bedriftsnettverk over hele verden for å forklare nedgangen i støttesamtaler relatert til løsepengevirus, tror vi den mest sannsynlige årsaken er en kombinasjon av politimyndigheters aktiviteter i 2021 og 2022, noe som økte kostnadene for kriminell aktivitet, sammen med enkelte geopolitiske hendelser i 2022.

En av de mest utbredte RaaS-operasjonene tilhører en russisktalende kriminalgruppe kjent som REvil (også kjent som Sodinokibi) som har vært aktiv siden 2019. I oktober 2021 ble REvils servere frakoblet som en del av den internasjonale politimyndighetsoperasjonen GoldDust.[7] I januar 2022 pågrep Russland 14 påståtte REvil-medlemmer og ransaket 25 steder tilknyttet dem.[8] Dette var første gang Russland handlet mot løsepengevirusoperatører i sitt land.

Selv om politimyndigheters aktiviteter sannsynligvis forsinket hyppigheten av angrep i 2022, kan trusselaktører fint utvikle nye strategier for å unngå å bli oppdaget i fremtiden. I tillegg ser det ut til at spenningen mellom Russland og USA over Russlands invasjon av Ukraina har satt en stopper for Russlands nye samarbeid i den globale kampen mot løsepengevirus. Etter en kort periode med usikkerhet etter REvil-pågripelsene stanset USA og Russland samarbeidet i jakten på løsepengevirusaktører, noe som betyr at nettkriminelle kan se på Russland som en trygg havn igjen.

Når vi ser fremover, spår vi at tempoet på løsepengevirusaktiviteter vil avhenge av utfallet av noen viktige spørsmål:

1. Vil regjeringer iverksette tiltak for å hindre at løsepengeviruskriminelle opererer innenfor sine grenser, eller vil de prøve å forstyrre aktører som opererer fra utlandet?
2. Vil løsepengevirusgrupper endre taktikken for å fjerne behovet for løsepengevirus og ty til utpressingsangrep?
3. Vil organisasjoner kunne modernisere og transformere IT-driften raskere enn kriminelle kan utnytte sårbarheter?
4. Vil fremskritt innen sporing av betalinger av løsepenger tvinge mottakere av løsepenger til å endre taktikk og forhandlinger?

Selv om politimyndigheters aktiviteter sannsynligvis forsinket hyppigheten av angrep i 2022, kan trusselaktører fint utvikle nye strategier for å unngå å bli oppdaget i fremtiden.

Fordo-bling

Løsepengevirusangrep gikk ned i enkelte regioner, men løsepengekravene er mer enn fordoblet.

Handlingsrettet innsikt

1. Fokuser på helhetlige sikkerhetsstrategier, da alle løsepengevirusfamiliene utnytter de samme sikkerhetssvakhetene for å påvirke et nettverk.
2. Oppdater og opprettholde grunnleggende sikkerhet for å øke det dyptgående beskyttelsesnivået og modernisere sikkerhetsoperasjoner. Ved å flytte til skyen kan du oppdage trusler raskere og reagere raskere.

Koblinger til mer informasjon

- Beskytt organisasjonen din mot løsepengevirus | Microsoft Security
- 7 måter å forsterke miljøet ditt på mot kompromittering | Microsoft Security Blog
- Forbedring av AI-basert forsvar for å forstyrre menneskeoperert løsepengevirus | Microsoft 365 Defender Research Team
- Security Insider: Utforsk den nyeste innsikten og oppdateringer om cybersikkerhet | Microsoft Security

Nettkriminalitet som tjeneste

Nettkriminalitet som tjeneste (CaaS) er en voksende trussel mot kunder over hele verden. Microsoft Digital Crimes Unit (DCU) observerte fortsatt vekst i CaaS-økosystemet med et økende antall tjenester på nettet som tilrettelegger for ulike former av nettkriminalitet, inkludert BEC og menneskeoperert løsepengevirus. Phishing fortsetter å være en foretrukket angrepsmetode ettersom nettkriminelle kan tilegne seg betydelig verdi fra å stjele kontoer og selge tilgang til stjålne kontoer.

Som en respons på det voksende CaaS-markedet forbedret DCU lyttersystemene for å oppdage og identifisere CaaS-tilbud i hele økosystemet, bestående av Internett, det dype nettet, granskede fora,[9] dedikerte nettsteder, diskusjonsfora på nettet og meldingsplattformer.

Nettkriminelle samarbeider nå på tvers av tidssoner og språk for å levere spesifikke resultater. Et CaaS-nettsted som administreres av en person i Asia, kan for eksempel ha operasjoner i Europa og opprette ondsinnede kontoer i Afrika. Disse operasjonene på tvers av flere jurisdiksjoner utgjør komplekse utfordringer knyttet til lovverk og håndhevelse. Som en respons fokuserer DCU innsatsen på å ta ned ondsinnet kriminell infrastruktur som brukes til å tilrettelegge for CaaS-angrep, og de samarbeider med politimyndigheter over hele verden for å holde kriminelle ansvarlige.

Nettkriminelle bruker i økende grad analyse for å maksimere rekkevidde, omfang og gevinst. I likhet med legitime bedrifter må CaaS-nettsteder sikre gyldigheten av produkter og tjenester for å opprettholde et solid omdømme. CaaS-nettsteder automatiserer for eksempel rutinemessig tilgang til kompromitterte kontoer for å sikre gyldigheten av kompromittert legitimasjon. Nettkriminelle vil avslutte salget av bestemte kontoer når passord tilbakestilles eller sårbarheter blir oppdatert. Vi har i økende grad oppdaget CaaS-nettsteder som gir kjøpere verifisering etter behov som en kvalitetskontrollprosess. Som et resultat kan kjøperne føle seg trygge på at CaaS-nettstedet selger aktive kontoer og passord, samtidig som de reduserer de potensielle kostnadene til CaaS-forhandleren hvis den stjålne legitimasjonen utbedres før salget.

DCU observerte også CaaS-nettsteder som tilbyr kjøpere muligheten til å kjøpe kompromitterte kontoer fra bestemte geografiske steder, utpekte tjenesteleverandører på nettet og spesielt målrettede enkeltpersoner, yrker og bransjer. Kontoer som bestilles ofte, fokuserer på fagfolk eller avdelinger som behandler fakturering, for eksempel finansdirektører eller «kundefordringer». På samme måte blir bransjer som er med på offentlige anbud, ofte målrettet på grunn av mengden informasjon som blir gjort tilgjengelig gjennom den offentlige anbudsprosessen.

DCU-undersøkelser av CaaS avdekket en rekke viktige trender:

Antallet tjenester øker, og de blir stadig mer avanserte.

Et eksempel på dette er utviklingen av nettskall som vanligvis består av kompromitterte nettservere som brukes til å automatisere phishing-angrep. DCU observerte at CaaS-forhandlere forenkler opplastingen av phishing-sett eller skadelig programvare gjennom spesialiserte dashbord på nettet. CaaS-selgere forsøker ofte å selge tilleggstjenester til trusselaktøren via dashbordet, for eksempel tjenester for søppelpostmeldinger og spesialiserte lister over søppelpostmottakere basert på definerte attributter, inkludert geografisk sted eller yrke. I enkelte tilfeller observerte vi at ett enkelt nettskall ble brukt i flere angrepskampanjer, noe som tyder på at trusselaktører kan opprettholde vedvarende tilgang til den kompromitterte serveren. Vi observerte også en økning i anonymiseringstjenester som er tilgjengelige som en del av CaaS-økosystemet, samt tilbud for VPN-kontoer (virtuelle private nettverk) og VPS-kontoer (virtuell privat server). I de fleste tilfeller ble VPN-ene/VPS-ene som tilbys, innledningsvis anskaffet via stjålne kredittkort. CaaS-nettsteder tilbød også et større antall RDP (Remote Desktop Protocol), SSH (Secure Shell) og cPanels for bruk som en plattform for å organisere nettkriminelle angrep. CaaS-forhandlere konfigurerer RDP, SSH og cPanels med egnede verktøy og skript for å tilrettelegge for ulike typer nettangrep.

Tjenester for oppretting av plagierte domener krever i økende grad betaling i kryptovaluta.

Plagierte domener utgir seg for å være legitime domenenavn ved å bruke tegn som er identiske eller nesten identiske i utseende til et annet tegn. Målet er å lure personen til å tro at det plagierte domenet er det ekte domenet. Disse domenene er en allestedsnærværende trussel og en inngangsport til en betydelig mengde nettkriminalitet. CaaS-nettsteder selger nå egendefinerte navn på plagierte domener, slik at kjøpere kan be om etterligninger av bestemte firma- og domenenavn. Etter at betalingen er mottatt, bruker CaaS-forhandlerne et verktøy for å generere plagiater for å velge domenenavnet og deretter registrere det ondsinnede plagiatet. Betaling for denne tjenesten foregår nær sagt utelukkende i kryptovaluta.

2 750 000

nettstedsregistreringer blokkert av DCU i år for å komme i forkant av kriminelle aktører som planla å bruke dem til å engasjere seg i global nettkriminalitet.

Nettkriminalitet som tjeneste

Fortsettelse

CaaS-selgere tilbyr i økende grad kompromittert legitimasjon for kjøp.

Kompromittert legitimasjon gir uautorisert tilgang til brukerkontoer, inkludert e-posttjeneste, bedriftens ressurser for fildeling og OneDrive for Business. Hvis administratorlegitimasjon blir kompromittert, kan uautoriserte brukere få tilgang til konfidensielle filer, Azure-ressurser og firmabrukerkontoer. I mange tilfeller avdekket DCU-undersøkelser uautorisert bruk av den samme legitimasjonen på flere servere som et middel til å automatisere verifisering av legitimasjon. Dette mønsteret antyder at den kompromitterte brukeren kan være offer for flere phishing-angrep eller ha ondsinnet programvare på enheten som tillater botnet-nøkkelloggere å samle inn legitimasjon.

Det kommer stadig nye CaaS-tjenester og -produkter med forbedrede funksjoner for å unngå deteksjon.

Én CaaS-selger tilbyr phishing-sett med økt kompleksitet og anonymiseringsfunksjoner utformet for å omgå oppdagelses- og forebyggingssystemer for så lite som 6 USD per dag. Tjenesten tilbyr en rekke omdirigeringer som utfører kontroller før trafikk tillates til neste lag eller nettsted. Én av disse kjører over 90 sjekker for fingeravtrykk på enheten, inkludert om det er en virtuell maskin, innsamling av detaljer om nettleseren og maskinvaren som brukes, og mer. Hvis alle sjekker er bestått, sendes trafikk til en landingsside som brukes for phishing.

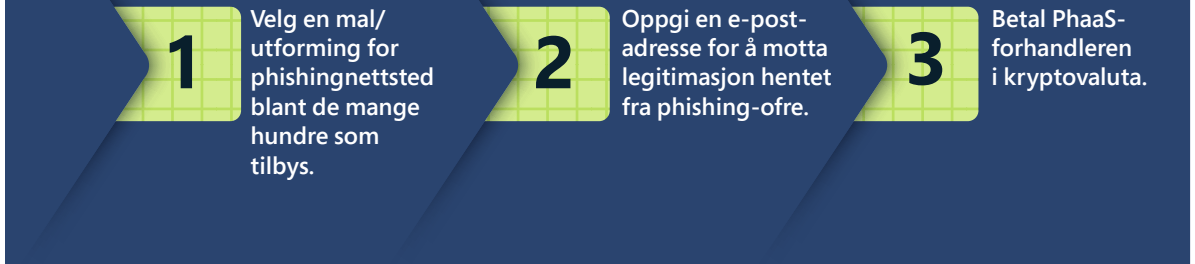
Ende-til-ende-tjenester for nettkriminalitet selger abonnementer på administrerte tjenester.

Vanligvis kan hvert trinn i iverksettelsen av nettkriminalitet eksponere trusselaktører hvis driftssikkerheten er dårlig. Risikoen for eksponering og identifikasjon øker hvis tjenester kjøpes fra flere CaaS-nettsteder. DCU observerte en bekymringsverdig trend i det mørke nettet, der det er en økning i tjenester som tilbyr å anonymisere programvarekode og komponere generell nettstedstekst for å redusere eksponeringen. Leverandører av ende-til-ende-abonnementstjenester for nettkriminalitet administrerer alle tjenester og garanterer resultater som ytterligere reduserer eksponeringsrisikoen for den abonnerende OCN-en. Den reduserte risikoen har økt populariteten til disse ende-til-ende-tjenestene.

Phishing som tjeneste (PhaaS) er ett eksempel på en ende-til-ende-tjeneste for nettkriminalitet. PhaaS er en utvikling av tidligere tjenester kjent som fullstendig uoppdagbare tjenester (FUD), og tilbys på abonnementsbasis. Vanlige PhaaS-vilkår inkluderer å holde phishing-nettsteder aktive i en måned.

DCU identifiserte også en CaaS-forhandler som tilbyr DDoS (distribuert tjenestenekt) i en abonnementsmodell. Denne modellen utkontraherer opprettingen og vedlikeholdet av botnettet som er nødvendig for å utføre angrep, for CaaS-forhandleren. Hver kunde med DDoS-abonnement mottar en kryptert tjeneste for å forbedre driftssikkerheten og ett år med døgnåpen kundestøtte. DDoS-abonnementstjenesten tilbyr ulike arkitekturer og angrepsmetoder, så en kjøper velger ganske enkelt en ressurs å angripe, og selgeren gir tilgang til en rekke kompromitterte enheter på sitt botnet for å gjennomføre angrepet. Kostnaden for DDoS-abonnementet er kun på 500 USD.

PhaaS-nettkriminelle tilbyr flere tjenester i ett enkelt abonnement. Generelt trenger en kjøper kun å utføre tre handlinger:



Når disse trinnene er fullført, oppretter PhaaS-forhandleren tjenester med tre eller fire lag med omdirigering og drifting av ressurser for å målrette mot bestemte brukere. Deretter lanseres kampanjen, og offerlegitimasjon høstes, verifiseres og sendes til e-postadressen oppgitt av kjøperen. For et påslag i prisen tilbyr mange PhaaS-forhandlere å drifte phishingnettsteder i den offentlige blokkjeden, slik at de kan nås av alle nettlesere, og slik at omdirigeringer kan peke brukere til en ressurs i den distribuerte hovedboken.

DCUs arbeid med å utvikle verktøy og teknikker som identifiserer og forstyrrer CaaS-nettkriminelle, pågår stadig. Utviklingen av CaaS-tjenester byr på betydelige utfordringer, spesielt når det gjelder å forstyrre betalinger i kryptovaluta.

Kriminell bruk av kryptovaluta

Etter hvert som bruken av kryptovaluta blir vanlig, bruker kriminelle i økende grad det til å unngå politimyndigheter og tiltak mot hvitvasking av penger (AML). Dette øker utfordringen for politimyndighetene når de skal spore utbetalinger i kryptovaluta til nettkriminelle.

Forbruket til blokkjedeløsninger har økt med omtrent 340 prosent de siste fire årene på verdensbasis, mens nye lommebøker for kryptovaluta har økt med rundt 270 prosent. Det finnes flere enn 83 millioner unike lommebøker globalt, og den totale markedsverdien av alle kryptovalutaer var på omtrent 1,1 billioner USD per 28. juli 2022.[10]

Kilde: Twitter.com—@PeckShieldAlert (PeckShield er et blokkjedesikkerhetsselskap basert i Kina).

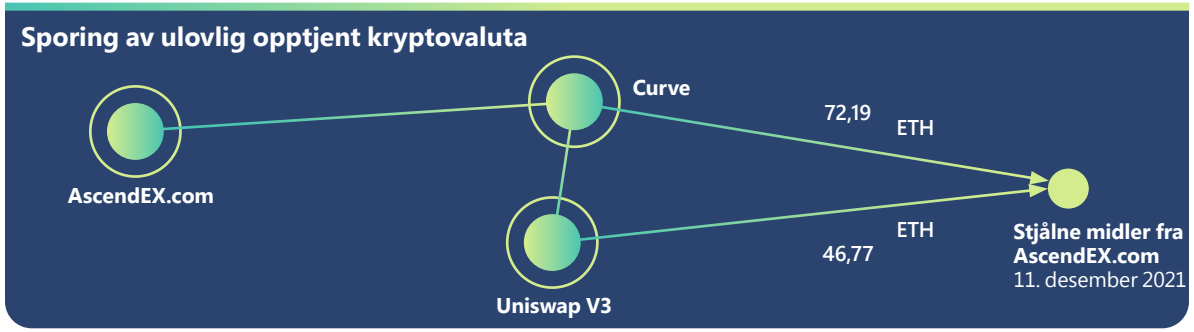
Sporing av utbetalinger for løsepengevirus

Løsepengevirus er en av de største kildene til ulovlig opptjent kryptovaluta. I et forsøk på å ta ned ondsinnet teknisk infrastruktur som brukes i løsepengevirusangrep – for eksempel Zloader i april 2022[11] – sporer Microsofts DCU kriminelle lommebøker for å muliggjøre sporing av kryptovaluta og gjenoppretting.

DCU-etterforskere har observert at løsepengevirusaktører utvikler kommunikasjonstaktikken med ofrene for å skjule pengesporet. Opprinnelig inkluderte nettkriminelle Bitcoin-adresser i kravene om løsepenger. Dette gjorde det imidlertid enkelt å følge betalingstransaksjoner på blokkjeden, så løsepengevirusaktørene sluttet å inkludere adresser til lommebøker og tilføyde i stedet e-postadresser eller koblinger til chatnettsteder for å formidle adresser til betaling av løsepenger til ofrene. Enkelte aktører har til og med opprettet unike nettsider og påloggінger for hvert offer for å hindre at sikkerhetsforskere og politimyndigheter får tak i de kriminelles adresser til lommebøker ved å utgi seg for å være ofre. Til tross for de kriminelles innsats for å skjule sporene sine, kan enkelte betalinger av løsepenger fortsatt gjenopprettes ved å samarbeide med politimyndigheter og kryptoanalyseselskaper som kan spore bevegelse på blokkjeden.

Populært: DEX-hvitvasking av ulovlige inntekter

En viktig sak for nettkriminelle er konverteringen av kryptovaluta til fiatpenger. Nettkriminelle har flere potensielle muligheter for konvertering, der hver av dem har en egen risikograd. En metode som brukes til å redusere risikoen, er å hvitvaske inntektene gjennom en desentralisert veksling (DEX) før utbetaling via tilgjengelige alternativer, for eksempel sentraliserte vekslinger (CEX), node-til-node (P2P) og veksling over disk (OTC). DEX-er er et attraktivt alternativ for hvitvasking fordi de ofte ikke følger AML-tiltak.



Ved å bruke verktøyet Chainalysis for undersøkelse av kryptovaluta oppdaget Microsofts enhet for digital kriminalitet at AcendEX-hackerne byttet sine stjålne midler hos en mindre DEX kalt Curve, i tillegg til Uniswap. Dette diagrammet illustrerer hvitvaskingsrutene gruppen avdekket. Hver sirkel representerer en klynge av lommebøker, og tallene på hver linje representerer det totale Ethereum-beløpet som ble overført for hvitvaskingsformål.

I desember 2021 angrep hackere den globale handelsplattformen for kryptovaluta, AscendEx, og stjal omtrent 77,7 millioner USD i kryptovaluta som tilhørte kundene.[12] AscendEx hyret blokkjedeanalysefirmaer og kontaktet andre CEX-er, slik at lommebøkene som mottok stjålne midler, kunne svartelistes. I tillegg ble adresser som valutaen ble sendt til, merket som svartelistet i Ethereum-blokkjedeutforskeren Etherscan.[13] For å omgå varslingen og svartelistingen sendte hackerne 1,5 millioner USD i Ethereum til Uniswap, en av verdens største DEX-er, 18. februar 2022.[14]

Innføringen av sterkere AML-tiltak hos DEX-er kan dempe hvitvaskingsaktiviteten på plattformene og tvinge kriminelle til å bruke andre tilsløringsmetoder, for eksempel myntblanding eller ulisensiert veksling. Som et eksempel kunngjorde Uniswap nylig at de vil begynne å bruke svartelister for å blokkere lommebøker som er kjent for å være involvert i ulovlige aktiviteter, fra å gjennomføre transaksjoner på børsen.[15]

Handlingsrettet innsikt

1. Hvis du er utsatt for nettkriminalitet og har betalt kriminelle i kryptovaluta, kan du kontakte lokale politimyndigheter som kan hjelpe til med å spore og gjenopprette tapte midler.
2. Bli kjent med ALM-tiltakene som er iverksatt, når du velger en DEX.

Koblinger til mer informasjon

- Maskinvarebasert trusselforsvar mot stadig mer komplekse kryptojackere | Microsoft 365 Defender Research Team

Det utviklende landskapet for phishing-trusler

Strategier for phishing etter legitimasjon er i økning og utgjør fortsatt en betydelig trussel mot brukere over hele verden fordi de ukritisk målretter mot alle innbokser. Blant truslene forskerne våre sporer og beskytter mot, er volumet av phishing-angrep større enn alle andre trusler.

Ved å bruke data fra Defender for Office oppdager vi ondsinnet e-post og kompromittert identitetsaktivitet. Azure Active Directory Identity Protection har enda mer informasjon gjennom varsler om hendelser angående kompromittert identitet. Ved hjelp av Defender for Cloud Apps oppdager vi hendelser med tilgang til kompromitterte identitetsdata, og Microsoft 365 Defender (M365D) gir korrelasjon på tvers av produkter. Måleverdien for sideveis bevegelse kommer fra Defender for Endpoint (varsler om angrepsatferd og hendelser), Defender for Office (ondsinnet e-post) og M365D for korrelasjon på tvers av produkter.

710 millioner

phishing-e-poster blokkert per uke.

1 time og 12 minutter

Mediantiden det tar for en angriper å få tilgang til de private dataene dine hvis du blir utsatt for en phishing-e-post.[16]

1 time og 42 minutter

Mediantiden det tar for en angriper å komme i gang med sideveis bevegelse på bedriftsnettverket ditt når en enhet er kompromittert.[17]

Microsoft 365-legitimasjon er fortsatt en av de mest ettertraktede kontotypene for angripere. Når påloggingslegitimasjon er kompromittert, kan angripere blant annet logge seg på datasystemer som er knyttet til en bedrift, for å tilrettelegge for infeksjoner med skadelig programvare og løsepengevirus, stjele konfidensielle bedriftsdata og informasjon ved å få tilgang til SharePoint-filer og fortsette spredningen av phishing ved å sende flere ondsinnede e-poster via Outlook.

I tillegg til kampanjer med bredere mål, phishing etter legitimasjon, donasjoner og personlig informasjon målretter angripere mot selektive bedrifter for større utbetalinger. Phishing-angrep via e-post mot bedrifter for økonomisk gevinst kalles samlet sett BEC-angrep.

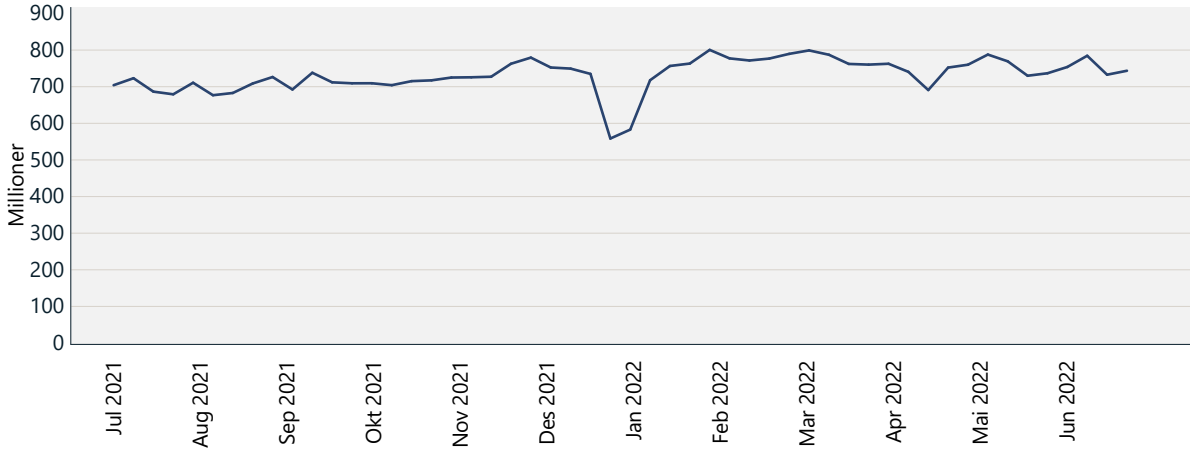
Microsoft oppdager millioner av BEC-e-poster hver måned, tilsvarende 0,6 prosent av alle phishing-e-poster som er observert. En rapport fra IC3[18] publisert i mai 2022 indikerer en oppadgående trend i eksponerte tap på grunn av BEC-angrep.

Teknikkene som brukes i phishing-angrep, blir stadig mer avanserte. Som et svar på mottiltakene tilpasser angripere seg og finner nye måter å implementere teknikkene sine på, noe som øker kompleksiteten i hvordan og hvor de drifter infrastruktur for kampanjeoperasjoner. Dette betyr at organisasjoner regelmessig må revurdere strategien sin for å implementere sikkerhetsløsninger for å blokkere ondsinnede e-poster og styrke tilgangskontrollen for individuelle brukerkontoer.

531 000

I tillegg til nettadressene som blokkeres av Defender for Office, overså avdelingen vår for digital kriminalitet nedstengingen av 531 000 unike phishing-adresser driftet utenfor Microsoft.

Oppdagede phishing-e-poster



Antallet phishing-oppdagelser per uke fortsetter å øke. Nedgangen i desember–januar er et forventet sesongfall, som også ble rapportert i fjorårets rapport. Kilde: Exchange Online Protection-signaler.

Det utviklende landskapet for phishing-trusler

Fortsettelse

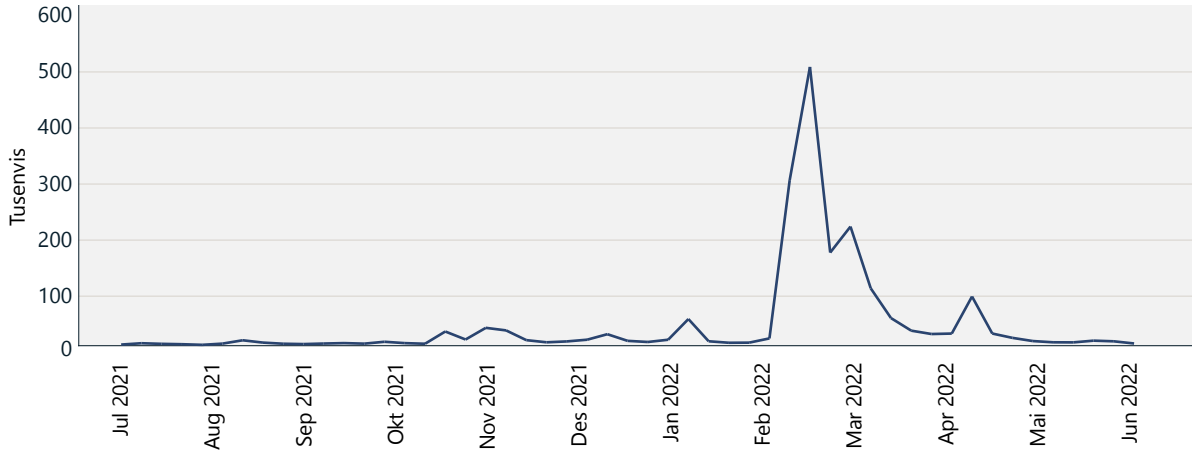
Vi fortsetter å observere en jevn årlig økning i phishing-e-poster. Overgangen til eksternt arbeid i 2020 og 2021 medførte en betydelig økning i phishing-angrep med sikte på å utnytte det skiftende arbeidsmiljøet. Phishing-operatører er raske til å ta i bruk nye e-postmaler ved hjelp av lokkemidler som er rettet inn mot viktige hendelser i verden, for eksempel COVID-19 pandemien og temaer knyttet til samarbeids- og produktivitetsverktøy som Google Drive eller OneDrive-fildeling. Mens det har vært en nedgang i COVID-19 temaer, ble krigen i Ukraina et nytt lokkemiddel fra begynnelsen av mars 2022. Forskerne våre observerte en svimlende økning av e-poster som utgir seg for å være fra legitime organisasjoner, som ber om donasjoner i kryptovaluta i Bitcoin og Ethereum, angivelig for å hjelpe innbyggere i Ukraina.

Bare noen få dager etter starten på krigen i Ukraina sent i februar 2022 økte antallet oppdagede phishing-e-poster med Ethereum-adresser fra bedriftskunder dramatisk. Det totale antallet nådde en topp den første uken i mars, da en halv million phishing-e-poster inneholdt en adresse til en Ethereum-lommebok. Før starten av krigen var antallet adresser til Ethereum-lommebøker på tvers av andre e-poster oppdaget som phishing betydelig lavere, og i snitt var det noen få tusen e-poster per dag.

Phishing-angripere er mer enn noensinne avhengig av legitim infrastruktur for å operere, noe som fører til en økning i phishing-kampanjer med sikte på å kompromittere ulike aspekter av en operasjon, slik at de ikke trenger å kjøpe, drifte eller drive sin egen. Ondsinnede e-poster kan for eksempel komme fra kompromitterte avsenderkontoer. Angripere drar nytte av å bruke disse e-postadressene som har et bedre omdømme, og som blir sett på som mer pålitelige enn nyopprettede kontoer og domener. I enkelte mer avanserte phishing-kampanjer observerte vi at angripere foretrakk å sende og etterligne fra domener som har DMARC[19] feilaktig konfigurert med policyen «ingen handling», noe som åpner døren for etterligning av e-post.

Store phishing-operasjoner har en tendens til å bruke skytjenester og virtuelle maskiner i skyen (VM-er) for å operasjonalisere angrep i stor skala. Angriperne kan fullt ut automatisere prosessen med å distribuere og levere e-poster fra VM-er ved å bruke omdirigeringer av SMTP-e-post eller skybasert e-postinfrastruktur og dra nytte av de høye leveringsratene og det positive omdømmet til disse legitime tjenestene. Hvis ondsinnet e-post kan sendes via disse skytjenestene, må forsvarerne basere seg på sterke funksjoner for e-postfiltrering for å blokkere e-poster fra å trenge inn i miljøet.

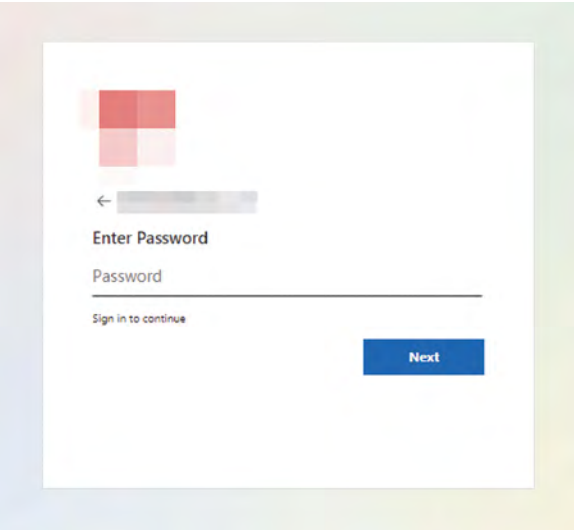
Phishing-e-poster med adresser til Ethereum-lommebøker



Det totale antallet e-poster oppdaget som phishing og med adresser til Ethereum-lommebøker økte i starten av konflikten mellom Russland og Ukraina og avtok siden etter den første kraftige økningen.

Microsoft kontoer er fortsatt et populært mål for phishing-operatører, noe som er dokumentert av de mange phishing-landingssidene som utgir seg for å være Microsoft 365-påloggingssiden. Phishing-angripere forsøker for eksempel å etterligne Microsoft-påloggingsopplevelsen i phishing-pakkene ved å generere en unik nettadresse som er tilpasset mottakeren. Denne nettadressen peker til en ondsinnet nettside utviklet for å høste legitimasjon, men en parameter i nettadressen inneholder den spesifikke mottakerens e-postadresse. Når målet navigerer til siden, vil phishing-pakken forhåndsutfylle brukerinnloggingsdata og en bedriftslogo tilpasset til e-postmottakeren, der den gjenspeiler utseendet til det målrettede selskapets egendefinerte Microsoft 365-påloggingsside.

Phishing-side som etterligner en Microsoft-pålogging med dynamisk innhold

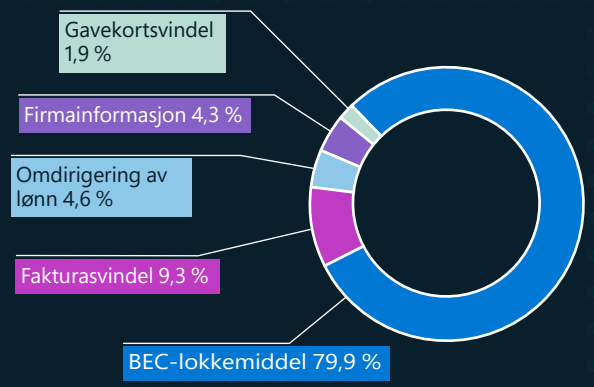


Søkelys på kompromittering av bedrifts-e-post

Nettkriminelle utvikler stadig mer komplekse ordninger og teknikker for å bekjempe sikkerhetsinnstillinger og målrette mot enkeltpersoner, bedrifter og organisasjoner. Vi investerer betydelige ressurser for å forbedre BEC-håndhevelsesprogrammet vårt ytterligere som en respons på dette.

BEC er den dyreste typen økonomisk nettkriminalitet, med anslagsvis 2,4 milliarder USD i justerte tap i 2021, noe som representerer mer enn 59 prosent av de fem største tapene fra kriminalitet på Internett globalt.[20] For å forstå omfanget av problemet og hvordan man best kan beskytte brukere mot BEC, har Microsofts sikkerhetsforskere sporet de vanligste temaene som brukes i angrep.

BEC-temaer (januar–juni 2022)



BEC-temaer etter prosentandel av forekomst

BEC-trender

Som et inngangspunkt forsøker BEC-angripere vanligvis å starte en samtale med potensielle ofre for å etablere tillit. Ved å utgi seg som en kollega eller en bekjent i bedriften kan angriperen gradvis lede samtalen i retning av en pengeoverføring. Introduksjons-e-posten, som vi sporer som et BEC-lokkemiddel, representerer nær 80 prosent av oppdagede BEC-e-poster. Andre trender identifisert Microsofts sikkerhetsforskere det siste året inkluderer følgende:

- De mest brukte teknikkene i BEC-angrep som ble observert i 2022, var forfalskning[21] og etterligning.[22]
- BEC-undertypen som forårsaket mest økonomisk skade på ofrene, var fakturasvindel (basert på volum og forespurte dollarbeløp som ble oppdaget i BEC-kampanjeundersøkelsene).
- Tyveri av forretningsinformasjon, for eksempel leverandørrapporter og kundekontakter, gjør det mulig for angripere å skape en overbevisende fakturasvindel.
- De fleste forespørsler om omdirigering av lønninger ble sendt fra kostnadsfrie e-posttjenester og sjelden fra kompromitterte kontoer. E-postvolumet fra disse kildene økte rundt den første og den femtende i hver måned, de vanligste betalingsdatoene.
- Til tross for å være velkjente muligheter for svindel utgjorde svindel med gavekort bare 1,9 prosent av BEC-angrepene som ble oppdaget.

Handlingsrettet innsikt

Forsvar mot phishing

For å redusere organisasjonens eksponering for phishing oppfordres IT-administratorer til å implementere følgende retningslinjer og funksjoner:

1. Krev bruk av MFA for alle kontoer for å begrense uautorisert tilgang.
2. Aktiver funksjoner for betinget tilgang for høyt privilegerte kontoer for å blokkere tilgang fra land, regioner og IP-adresser som vanligvis ikke genererer trafikk i organisasjonen.
3. Vurder bruk av fysiske sikkerhetsnøkler for ledere, ansatte som er involvert i betalings- eller kjøpsaktiviteter, og andre privilegerte kontoer.
4. Gjør det obligatorisk å bruke nettlesere som støtter tjenester, for eksempel Microsoft SmartScreen, for å analysere nettadresser for mistenkelig atferd, og som blokkerer tilgang til kjente ondsinnede nettsteder.[23]
5. Bruk en maskinlæringsbasert sikkerhetsløsning som setter adresser som høyst sannsynlig er phishing, i karantene, og som plasserer nettadresser og vedlegg i en sandkasse før e-posten når innboksen, for eksempel Microsoft Defender for Office 365.[24]
6. Muliggjør funksjoner for beskyttelse mot etterligning og forfalskning i hele organisasjonen.
7. Konfigurer retningslinjer for DKIM- (DomainKeys Identified Mail) og DMARC-handlinger (Domain-based Message Authentication Reporting & Conformance) for å forhindre levering av ikke-godkjente e-poster som kan etterligne pålitelige avsendere.
8. Overvåk tillatelsesregler opprettet av leiere og brukeren og fjerne brede domene- og IP-baserte unntak. Disse reglene har ofte forrang og kan tillate kjente ondsinnede e-poster via e-postfiltrering.
9. Kjør phishing-simulatorer regelmessig for å måle den potensielle risikoen i hele organisasjonen og identifisere og lære opp sårbare brukere.

Koblinger til mer informasjon

- Fra tyveri av informasjonskapsler til BEC: Angripere bruker AiTM-phishing-nettsteder som inngangspunkt til videre økonomisk svindel | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Plagieringsbedrag

BEC og phishing er vanlige taktikker innen sosial manipulering. Sosial manipulsering spiller en betydelig rolle innen kriminalitet. Prinsippet går ut på å overtale et mål om å samhandle med den kriminelle ved å få tillit.

I fysisk handel brukes varemerker til å sikre tillit til opprinnelsen til et produkt eller en tjeneste, og forfalskede produkter er et misbruk av varemerket. På samme måte utgjør nettkriminelle seg for å være en kontakt som er kjent for målet under et phishing-angrep, ved hjelp av plagiater for å bedra potensielle ofre.

Et plagiat er et domenenavn som brukes til e-postkommunikasjon i BEC, der et tegn erstattes av et som er identisk eller nesten identisk i utseende, for å lure målet.

Plagieringsteknikker som brukes i BEC-forsøk

BEC har vanligvis to faser, der den første innebærer kompromittering av legitimasjon. Disse typene legitimasjonslekkasjer kan være et resultat av phishing-angrep eller store databrudd. Legitimasjonen blir deretter solgt eller forhandlet på det mørke nettet.

Den andre fasen er svindelfasen, der angripere bruker kompromittert legitimasjon til å engasjere seg i sofistikert sosial manipulering ved hjelp av plagierte e-postdomener.

Fremdriften til et BEC-angrep

Teknikk	Prosent av domener som viser plagiering-steknikk
bytt ut l med I	25 %
bytt ut i med l	12 %
bytt ut q med g	7 %
bytt ut rn med m	6 %
bytt ut .cam med .com	6 %
bytt ut 0 mot o	5 %
bytt ut ll med l	3 %
bytt ut ii med i	2 %
bytt ut vv med w	2 %
bytt ut l med ll	2 %
bytt ut e med a	2 %
bytt ut nn med m	1 %
bytt ut ll med I, bytt ut l med i	1 %
bytt ut o med u	1 %

Analyse av over 1700 plagierte domener mellom januar og juli 2022. Mens 170 plagieringsteknikker ble brukt, brukte 75 % av domenene kun 14 teknikker.

En plagiering i aksjon

Et plagiert domene som ser identisk ut som et e-postdomene offeret gjenkjenner, er registrert på en e-postleverandør med et identisk brukernavn. En kapret e-post blir deretter sendt fra det kaprede domenet med nye betalingsinstruksjoner.

Ved å utnytte intelligens med åpen kildekode og tilgang til e-posttråder identifiserer den kriminelle personer som har ansvar for fakturering og betalinger. Deretter oppretter de en etterligning av en e-postadresse til personen som sender fakturaer. Denne etterligningen består av et identisk brukernavn og e-postdomene som er en plagiering av den ekte avsenderen.

Angriperen kopierer en e-postkjede som inneholder en legitim faktura, og endrer deretter fakturaen slik at den inneholder angriperens egne bankopplysninger. Denne nye, endrede fakturaen sendes deretter på nytt fra e-postmeldingen med den plagierte etterligningen til målet. Fordi konteksten er fornuftig og e-posten ser ekte ut, følger ofte målet de falske instruksjonene.

Handlingsrettet innsikt

1. Gjør det obligatorisk å bruke nettlesere som støtter tjenester for å analysere nettadresser for mistenkelig atferd, og som blokkerer tilgang til kjente ondsinnede nettsteder, for eksempel Safe Links og SmartScreen.[25]
2. Bruk en maskinlæringsbasert sikkerhetsløsning som setter adresser som høyst sannsynlig er phishing, i karantene, og som plasserer nettadresser og vedlegg i en sandkasse før e-posten når innboksen.

Koblinger til mer informasjon

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Falsk analyseinnsikt – Office 365 | Microsoft Docs
- Innsikt om etterligninger – Office 365 | Microsoft Docs

En tidslinje med botnet-forstyrrelser fra Microsofts tidlige samarbeidsdager

I over ti år har DCU jobbet for proaktivt å stoppe nettkriminalitet som resulterer i 26 forstyrrelser fra skadelig programvare og statlige aktører. Siden DCU-teamet bruker mer avanserte taktikker og verktøy for å ta ned disse ulovlige operasjonene, ser vi at nettkriminelle også utvikler tilnærmingene sine i et forsøk på å holde seg ett skritt foran. Her er en tidslinje som viser et eksempel på botnettene som ble forstyrret av DCU, og strategiene som Microsoft tok i bruk for å stenge dem ned.

2008

Conficker-botnet

Beskrivelse: En orm som sprer seg raskt, målrettet mot Windows OS, infiserer millioner av datamaskiner og enheter i et felles nettverk, forårsaket nettverksbrudd over hele verden.

Samarbeid: Dannelsen av Conficker Working Group, det første konsortiet i sitt slag. Microsoft samarbeider med 16 organisasjoner over hele verden for å bekjempe botnettet.

Respons fra Microsoft: Gruppen samarbeidet på tvers av mange internasjonale jurisdiksjoner og lyktes med å ta ned Conficker.

2009

Waledac-botnet

Beskrivelse: Et komplekst søppelpost-botnet med amerikanske domener som samlet inn e-postadresser og distribuerte søppelpost som infiserte opptil 90 000 datamaskiner over hele verden.[26]

Samarbeid: Oppretting av nok et konsortium, Microsoft Malware Protection Center (MMPC), med fokus på nært samarbeid med akademikere.[27]

Respons fra Microsoft: Microsoft brukte nivåbasert tilnærming til forstyrrelser mot C2 og overrasket ondsinnede aktører ved å ta ned domener basert i USA uten forvarsel.[28] Microsoft ble gitt midlertidig eierskap av nesten 280 domener som brukes av Waledacs servere.

2011

Microsoft Digital Crimes Unit dannes

Samarbeid: Utviklet for å stanse nettkriminalitet som påvirker Microsoft-økosystemet, gjennom tett integrasjon med en gruppe av etterforskere, advokater og ingeniører.

Microsoft-tilnærming: Målet er å bedre forstå de tekniske aspektene ved ulike typer skadelig programvare og gi denne innsikten til Microsofts juridiske avdeling for å utvikle en effektiv forstyrrelsesstrategi.

2013

Rustock-botnet

Beskrivelse: En trojansk spam-robot for e-post via bakdøren som brukte Internett-leverandører som primære C2-er, designet for å selge farmasøytiske produkter.

Samarbeid: Microsoft dannet et samarbeid med Pfizer Pharmaceuticals for å forstå medisinene som selges av Rustock, og samarbeidet tett med nederlandske politimyndigheter.[29]

Respons fra Microsoft: Microsoft jobbet med US Marshalls og politimyndigheter i Nederland for å ta ned C2-serverne i landet. Registrerte og blokkerte alle fremtidige domenegeneratoralgoritmer (DGA-er).

Sirefef/Zero Access-botnet

Beskrivelse: Et botnet for reklame utviklet for å sende folk til farlige nettsteder som installerer skadelig programvare eller stjeler personlig informasjon. Infiserte over to millioner datamaskiner og kostet annonsører over 2,7 millioner USD per måned, hovedsakelig i USA og Vest-Europa.

Samarbeid: Samarbeidet tett med FBI og Europols senter for nettkriminalitet for å ta ned node-til-node-infrastrukturen.

Respons fra Microsoft: Ble med i Zero Access-nettverket, erstattet de kriminelle C2-serverne og beslagla serverdomener.

2019

Trickbot-botnet

Beskrivelse: Et sofistikert botnet med fragmentert infrastruktur over hele verden som målrettet seg mot finansnæringen, kompromitterte IoT-enheter.

Samarbeid: Microsoft inngikk samarbeid med Financial Services Information Sharing and Analysis Center (FS-ISAC) for å ta ned Trickbot.[30]

Respons fra Microsoft: DCU bygde et system for å identifisere og spore robotinfrastruktur og genererte varslinger for aktive Internett-leverandører, der de tok hensyn til spesifikke lover i diverse land.

Kontinuerlig fokus på forstyrrelser

Beskrivelse: Microsoft forstyrret infrastrukturen til sju trusselaktører det siste året og hindret dem i å distribuere ytterligere skadelig programvare, kontrollere ofrenes datamaskiner og målrette mot flere ofre.

Samarbeid: I partnerskap med Internett-leverandører, regjeringer, politimyndigheter og privat industri delte Microsoft informasjon for å løse problemer for over 17 millioner ofre for skadelig programvare over hele verden.

2022

Med blikket fremover

DCU fortsetter å innovere og er ute etter å bruke sin erfaring i botnet-forstyrrelser for å gjennomføre koordinerte operasjoner for mer enn kun skadelig programvare. Vår fortsatte suksess krever kreativt ingeniørarbeid, deling av informasjon, innovative juridiske teorier og offentlige og private partnerskap.

Nettkriminelles misbruk av infrastruktur

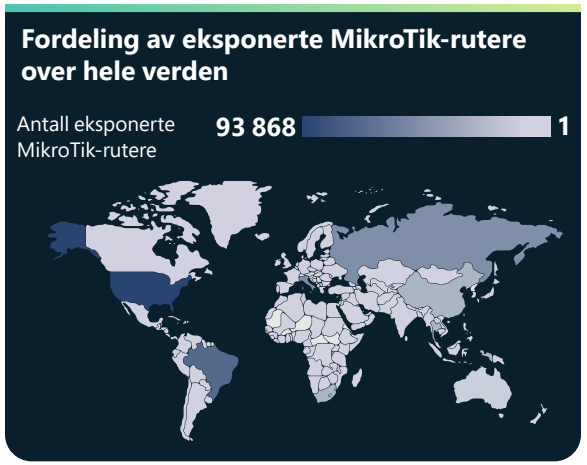
Internett-gatewayer som infrastruktur for kriminelles kommandoer og kontroll

IoT-enheter blir et stadig mer populært mål for nettkriminelle som bruker utbredte botnet. Når rutere ikke er oppdatert og blir eksponert direkte for Internett, kan trusselaktører misbruke dem og få tilgang til nettverk, utføre ondsinnede angrep og til og med støtte sine egne operasjoner.

Microsoft Defender for IoT-teamet forsker på utstyr som spenner fra eldre kontrollere for industrikontrollsystemer til banebrytende IoT-sensorer. Teamet undersøker IoT- og OT-spesifikk skadelig programvare for å bidra til den delte listen over indikatorer for kompromittering.

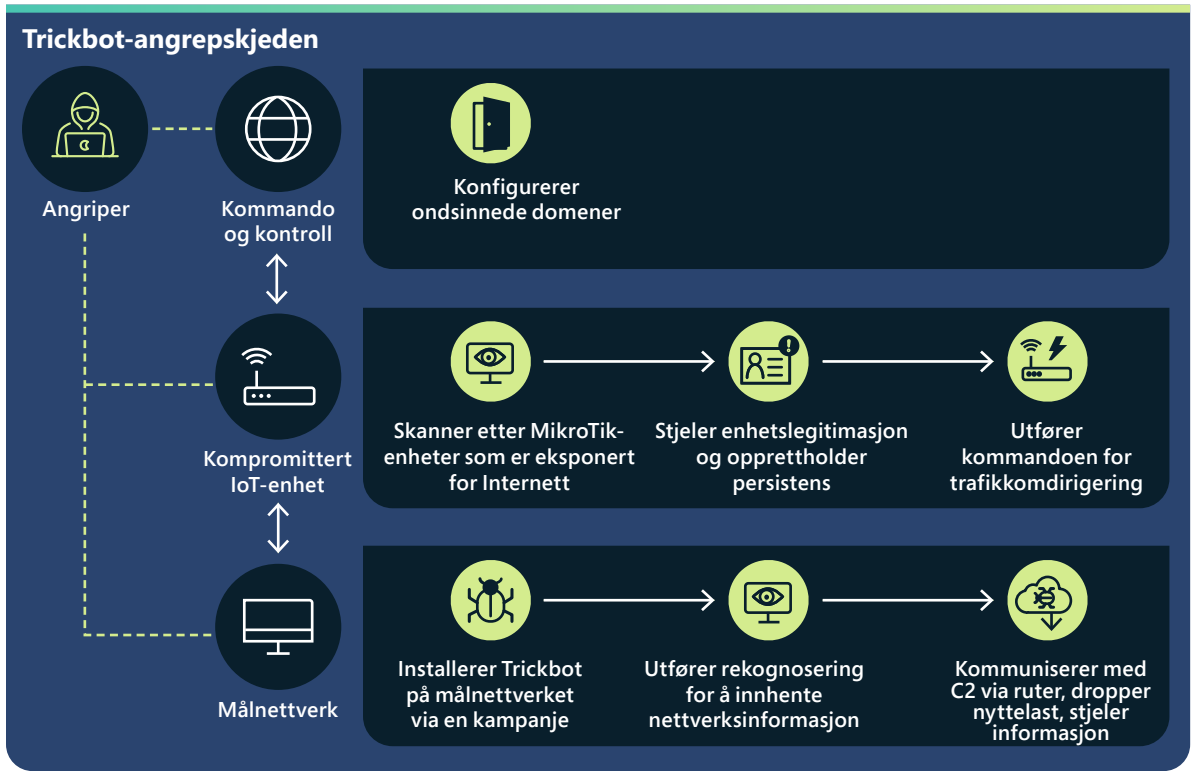
Rutere er spesielt sårbare angrepsvektorer fordi de er allestedsnærværende på tvers av Internett-tilkoblede hjem og organisasjoner. Vi har sporet aktiviteten til MikroTik-rutere, en populær ruter i hele verden, både privat og kommersielt, og identifisert hvordan de brukes til kommando- og kontrollangrep (C2), DNS-angrep (domenenavnsystem) og kapring av kryptoutvinning.

Nærmere bestemt identifiserte vi hvordan Trickbot-operatører bruker kompromitterte MikroTik-rutere og omkonfigurerer dem til å fungere som en del av C2-infrastrukturen. Populariteten til disse enhetene øker alvorlighetsgraden av misbruket av Trickbot, og deres unike maskinvare og programvare gjør det mulig for trusselaktører å unngå tradisjonelle sikkerhetstiltak, utvide infrastrukturen og kompromittere flere enheter og nettverk.



Eksponerte rutere risikerer at potensielle sårbarheter blir utnyttet.

Ved å spore og analysere trafikk som inneholder SSH-kommandoer (Secure Shell), observerte vi angripere som brukte MikroTik-rutere til å kommunisere med Trickbot-infrastrukturen etter å ha innhentet legitim legitimasjon til enheter. Denne legitimasjonen kan innhentes gjennom angrep med rå kraft, utnyttelse av kjente sårbarheter med lett tilgjengelige oppdateringer og bruk av standardpassord. Når angriperen har fått tilgang til en enhet, utsteder angriperen



Trickbot-angrepskjede som viser bruk av MikroTik IoT-enheter som proxyservere for C2.

en unik kommando som omdirigerer trafikk mellom to porter i ruteren, og etablerer kommunikasjonslinjen mellom Trickbot-berørte enheter og C2.

Vi har samlet vår kunnskap om de ulike metodene for å angripe MikroTik-enheter, utover kun Trickbot, samt kjente vanlige sårbarheter og eksponeringer (CVE-er) i et verktøy med åpen kildekode for MikroTik-enheter, som kan trekke ut artefaktene som skal granskes, knyttet til angrep på disse enhetene.[31]

Enheter som fungerer som omvendte proxyer for skadelig programvare fra C2, er ikke unike kun for Trickbot- og MikroTik-rutere. I samarbeid med Microsoft RiskIQ-teamet sporet vi tilbake til den involverte C2-enheten, og ved å observere SSL-sertifikater identifiserte vi Ubiquiti- og LigoWave-enheter som også er påvirket.[32] Dette er en sterk indikasjon på at IoT-enheter blir aktive komponenter i koordinerte angrep fra nasjonalstater og et populært mål for nettkriminelle ved hjelp av utbredte botnet.

Kriminelle på nettet misbruker IoT-enheter

Gateway-enheter er et stadig mer verdifullt mål for trusselaktører, ettersom antallet kjente sårbarheter har vokst konsekvent fra år til år. De brukes til utvinning av krypto og andre typer skadelig aktivitet.

Etter hvert som kryptovaluta har blitt mer populært, har mange enkeltpersoner og organisasjoner investert datakraft og nettverksressurser fra enheter som rutere for å utvinne mynter på blokkjeden. Utvinning av kryptovaluta er imidlertid en tids- og ressursintensiv prosess med lav sannsynlighet for suksess. For å øke sannsynligheten for å utvinne en mynt samles utvinnere i distribuerte, samarbeidende nettverk og mottar hasher i forhold til prosentandelen av mynten de lyktes i å utvinne med sine tilkoblede ressurser.

I løpet av det siste året har Microsoft observert et økende antall angrep som misbruker rutere for å omdirigere innsats for utvinning av kryptovaluta. Nettkriminelle kompromitterer rutere som er koblet til utvinningsutvalg, og omdirigerer utvinningstrafikk til sine tilknyttede IP-adresser med DNS-forgiftningsangrep, som endrer DNS-innstillingene for målrettede enheter. Berørte rutere registrerer feil IP-adresse til et gitt domenenavn og sender utvinningsressursene – eller hashene – til utvalg som brukes av trusse-laktører. Disse utvalgene kan utvinne anonyme mynter knyttet til kriminelle aktiviteter eller bruke legitime hasher generert av datautvinnere for å anskaffe en prosentandel av mynten som de utvinner, og dermed høste belønningen.

Mer enn halvparten av kjente sårbarheter som ble funnet i 2021, mangler en oppdatering, og oppdatering og sikring av rutere på bedriftsnettverk og private nettverk er fortsatt en betydelig utfordring for enhetseiere og administratorer.

Kompromittering av enheter for ulovlig utvinning av krypto.

En del av hash-ene fra det opprinnelige utvalget blir stjålet av trusselaktører, eller ressurser blir overført til utvalget, eller rutere har skadelig programvare som stjeler ressurser for utvinning.

DNS-forgiftning av gateway-enheter kompromitterer legitime utvinningsaktiviteter og omdirigerer ressurser til kriminelle utvinningsaktiviteter.

Virtuelle maskiner som kriminell infrastruktur

Den utbredte overgangen til skyen inkluderer nettkriminelle som utnytter private ressurser som uforvarende ofre innhentet gjennom phishing eller distribusjon av skadelig programvare som stjeler legitimasjon. Mange nettkriminelle velger å konfigurere ondsinnede infrastrukturer på skybaserte virtuelle maskiner (VM-er), containere og mikrotjenester.

Når nettkriminelle har tilgang, kan det oppstå en hendelsessekvens for å konfigurere infrastruktur – for eksempel en serie med virtuelle maskiner gjennom skripting og automatiserte prosesser. Disse skriptede, automatiserte prosessene brukes til å starte ondsinnet aktivitet, inkludert e-postangrep i stor skala, phishing-angrep og nettsider som er verter for ondsinnet innhold. Det kan til og med omfatte å sette opp et skalert virtuelt miljø som utvinner kryptovaluta, noe som gjør at sluttofferet får en regning på hundretusenvis av kroner ved slutten av måneden.

Nettkriminelle forstår at den ondsinnede aktiviteten har en begrenset levetid før den oppdages og stenges ned. Som et resultat har de skalert opp og opererer nå proaktivt med fokus på alle eventualiteter. De har blitt observert under klargjøring av kompromitterte kontoer på forhånd og overvåking av miljøene sine. Så snart en konto (konfigurert ved hjelp av hundretusenvis av virtuelle maskiner) er oppdaget, går de til neste konto – allerede klargjort av skript som aktiveres umiddelbart – og den ondsinnede aktiviteten fortsetter med få eller ingen avbrudd.

I likhet med skyinfrastruktur kan lokal infrastruktur brukes i angrep med virtuelle lokale miljøer som er ukjente for den lokale brukeren. Dette krever at det første tilgangspunktet forblir åpent og tilgjengelig. Lokale private ressurser har også blitt misbrukt av nettkriminelle for å starte en pågående kjede med skyinfrastruktur, konfigurert for å tilsløre opprinnelsen for å unngå oppdagelse av mistenkelig infrastruktur.

Handlingsrettet innsikt

1. Implementer god netthygiene og gi opplæring i nettsikkerhet for ansatte med veiledning for å unngå å bli sosialt manipulert.
2. Utfør regelmessige automatiserte avvikssjekker av brukeraktivitet gjennom gjenkjenninger i stor skala for å redusere disse angrepstypene.
3. Oppdater og sikre rutere på bedriftsnettverk og private nettverk.

Er hacktivisme kommet for å bli?

Selv om hacktivisme ikke er et nytt fenomen, har vi sett en økning av frivillige hackere etter krigsutbruddet i Ukraina, inkludert enkelte ledet av regjeringer, som tar i bruk nettverktøy for å skade omdømmet eller ressursene til politiske motstandere, organisasjoner og til og med nasjonalstater.

I februar 2022 oppfordret myndighetene i Ukraina private sivile rundt om i verden til å utføre nettangrep på Russland som en del av «IT-hæren» på 300 000 «soldater».[33] Samtidig begynte etablerte hacktivistgrupper som Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans og RaidForum2 å gjennomføre angrep til støtte for Ukraina. Andre grupper, inkludert noen av Conti-løsepengevirusgjengen, tok parti med Russland.[34]

I de påfølgende månedene var aktivitetene til Anonymous svært synlige. Hackere som agerte i gruppens navn – eller i et av dets tilknyttede selskaper – deaktiverte midlertidig tusenvis av russiske og hviterussiske nettsteder, lekket hundrevis av GB med stjålne data, hacket russiske TV-kanaler for å spille av pro-ukrainsk innhold og tilbød seg til og med å betale i bitcoin for russiske stridsvogner som overgav seg.

Fremveksten av selvlærte hackere

Sosiale medieplattformer muliggjorde rask organisasjon og mobilisering av tusenvis av selvlærte hackere, som ble gitt retningslinjer for å gjennomføre enkle kjørbare angrep, for eksempel DDoS-angrep. Arrangørene utnyttet Twitter, Telegram og private fora for å samle hackere, organisere operasjoner og spre instruksjoner for hacking.

De fleste av disse hackerne har imidlertid sannsynligvis begrensede ferdigheter, selv etter å ha fått instruksjoner. Dette antyder to potensielle muligheter for fremtiden: én der hundrevis eller tusenvis av personer med kun grunnleggende tekniske evner bruker angrepsmaler til å gjennomføre fremtidige koordinerte eller individuelle hacktivistiske angrep mot mål, eller en annen mulighet der den endelige slutten på krigshandlinger i Ukraina gjør at de legger hacktivismen bak seg, i hvert fall frem til neste politiske eller sosiale problem inspirerer dem til handling.

Politisering av hackere

Den største risikoen som denne politiske mobiliseringen utgjør, er distribusjonen av teknologisk kunnskapsrike hackere som kan fortsette å utføre nettangrep mot utenlandske regjeringer for å understøtte sine egne nasjonale prioriteringer, enten på eget initiativ eller på vegne av myndighetene.

Iran, Kina og Russland bruker allerede hacktivisme som et utgangspunkt for rekruttering i sine statlige hackingsgrupper. I april 2022 lanserte for eksempel den pro-russiske hackinggruppen Killnet DDoS-angrep mot tsjekkiske jernbaner, regionale flyplasser og Tsjekkias sivile tjenesteserver, selv om Tsjekkia ikke er direkte involvert i krigen.[35] Samtidig kan enkelte regjeringer bruke hacktivisme som et dekke for tradisjonell nettspionasje eller sabotasjeoperasjoner – for eksempel iranske aktiviteter mot Israel.

I et miljø med økte DDoS-angrep knyttet til hacktivisme blir teknologibransjen utfordret til raskt å dechiffrere forskjellen mellom normal og unormal trafikkflyt til et nettsted. Microsoft og dets partnere har utviklet en samling av verktøy som skiller ut ondsinnet DDoS-trafikk og sporer den tilbake til sin opprinnelse. I tillegg kan Microsoft Azure-plattformen identifisere maskiner på plattformen som produserer ekstraordinært høye nivåer av utgående trafikk, og stenge dem av.

Fremvekst av protestvare

Protestvare har dukket opp som et direkte resultat av emosjonelle reaksjoner på krigen mellom Russland og Ukraina. Enkelte utviklere av programvare med åpen kildekode brukte populariteten til programvaren som et middel til å sette fokus på eller iverksette tiltak mot den geopolitiske situasjonen i utfoldning. Dette inkluderte harmløse tekstfiler som ble åpnet på et skrivebord eller i en nettleser for å spre fredsmeldinger, men inkluderte også målrettede angrep basert på geolokasjon for IP-adresser og destruktive handlinger, som sletting av harddisker. Etter hvert som andre globale hendelser utfolder seg, kan vi forvente å se protestvare igjen i fremtiden. Siden dette generelt sett er tilfeller der velrespekterte vedlikeholdere av åpen kildekode bestemmer seg for å komme med personlige ytringer via sine egne komponenter med åpen kildekode, er det for øyeblikket ingen beskyttelse på plass for å hindre at disse typene endringer oppstår i kildefilpakkene, og brukerne bør fortsatt være bevisste på potensiell påvirkning.

Sosiale medieplattformer muliggjorde organisasjon og mobilisering av tusenvis av selvlærte hackere, som ble gitt retningslinjer for å gjennomføre enkle kjørbare angrep, for eksempel DDoS-angrep.

Handlingsrettet innsikt

1. Teknologibransjen må komme sammen for å utforme en omfattende respons på denne nye trusselen.
2. Ledende teknologiselskaper, deriblant Microsoft, har verktøy for å identifisere ondsinnet trafikk knyttet til DDoS-angrep og deaktivere de ansvarlige maskinene.
3. Brukere av åpen kildekode bør være mer på vakt i tider med geopolitiske stridigheter.

Sluttnoter

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. Endepunktsoppdagelse og -respons. 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 gransket forum er et diskusjonsforum på nettet som krever at et eksisterende medlem går god for å legge til et nytt medlem.
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 (ondsinnet e-post / kompromittert identitet), Azure Active Directory Identity Protection (kompromitterte identitetshendelser/-varsler), Defender for Cloud Apps (hendelser med kompromittert tilgang til identitetsdata) og M365D (kryssproduktkorrelasjon).
17. Datakilde: Defender for Endpoint (varsler om / hendelser med angrepsatferd), Defender for Office (ondsinnet e-post) og M365D (kryssproduktkorrelasjon).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Domenebasert meldingsgodkjenning, rapportering og samsvar: e-postgodkjenning, retningslinjer og rapporteringsprotokoll utformet for å gi eiere av e-postdomener muligheten til å beskytte domenet mot uautorisert bruk.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va. 22. februar 2010).
27. Se Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27. september 2011.
28. Nærmere bestemt tillater regel 65 i Federal Rules of Civil Procedure en part å søke en slik løsning hvis: 1) parten vil lide umiddelbar og uopprettelig skade hvis hjelp ikke blir gitt, og 2) parten forsøker å varsle den andre parten i tide. Videre krever loven at en balanseringstest brukes, en test som balanserer den tiltaltes rett til innsigelser mot skadeomfanget for offentligheten.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9. februar 2011).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12. august 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

Statlige trusler

Statlige aktører lanserer stadig mer sofistikerte nettangrep for å unngå deteksjon og fremme sine strategiske prioriteringer.

En oversikt over
statlige trusler

Statlige aktører lanserer stadig mer sofistikerte nettangrep for å unngå deteksjon og fremme sine strategiske prioriteringer. Distribusjonen av cybervåpen under hybridkrigen i Ukraina utgjør starten på en ny tidsalder med konflikt.

Russland har også understøttet krigen med informasjonspåvirkningsoperasjoner, ved å bruke propaganda for å påvirke meninger i Russland, i Ukraina og globalt. Denne første hybride konflikten i full skala har gitt oss andre viktige lærdommer. For det første kan sikkerheten til digitale operasjoner og data beskyttes best – både på nettet og rent fysisk – ved å flytte til skyen. Innledende angrep fra Russland målrettet mot lokale tjenester med ondsinnet slettingsprogramvare, og fysiske datasentre var målene til et av de første rakettangrepene.

Ukraina responderte ved å flytte arbeidsbelastninger og data til skyer i hyperskala som driftes i datasentre utenfor Ukraina. For det andre har fremskritt innen etterretning om nettrusler og endepunktsbeskyttelse drevet av data og avanserte AI- og ML-tjenester i skyen hjulpet Ukraina med å forsvare seg mot russiske nettangrep.

Ellers har statlige aktører økt aktiviteten og benytter seg av fremskritt innen automatisering, skyinfrastruktur og teknologi for ekstern tilgang til å angripe et bredere sett med mål. IT-forsyningskjeder i bedrifter som gir tilgang til endelige mål, har ofte blitt angrepet. Det har blitt enda viktigere med nettsikkerhetshygiene etter hvert som aktører raskt utnytter ikke-oppdaterte sårbarheter, bruker både sofistikerte teknikker og rå kraft-teknikker til å stjele legitimasjon og tilslører operasjonene ved hjelp av åpen kildekode eller legitim programvare. Iran har i tillegg slått seg sammen med Russland i bruk av destruktive cybertrusler, inkludert løsepengevirus, som et fast innslag i angrepene.

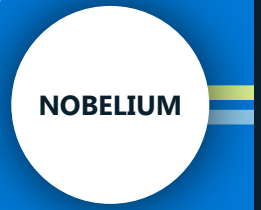
Denne utviklingen krever presserende implementering av et konsistent, globalt rammeverk som prioriterer menneskerettigheter og beskytter mennesker mot hensynsløs statlig atferd på nettet. Alle nasjoner må arbeide for å implementere vedtatte normer og regler for ansvarlig statlig atferd.

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

Økt målretting mot kritisk infrastruktur, spesielt IT-sektoren, finanstjenester, transportsystemer og kommunikasjonsinfrastruktur.

Finn ut mer på side 35

IT-forsyningskjeden brukes som en gateway for å få tilgang til mål.



Finn ut mer på side 36

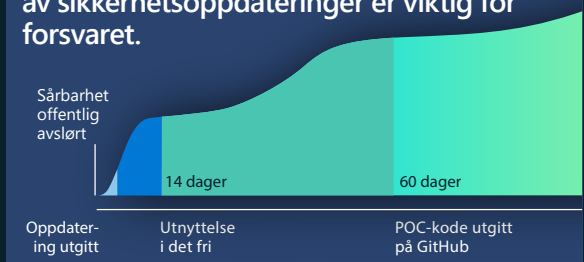
Kina utvider global målretting, spesielt mot mindre nasjoner i Sørøst-Asia, for å samle etterretning og oppnå konkurransefortrinn.

Finn ut mer på side 44

Iran har blitt stadig mer aggressive etter maktovergangen. De har utvidet angrep fra løsepengevirus utover regionale motstandere til ofre i USA og EU og målrettet mot høyprofilert kritisk infrastruktur i USA.

Finn ut mer på side 46

Identifisering og rask utnyttelse av ikke-oppdaterte sårbarheter har blitt en viktig taktikk. Rask implementering av sikkerhetsoppdateringer er viktig for forsvaret.



Finn ut mer på side 39

Nord-Korea målrettet mot forsvars- og luftfartsselskaper, kryptovaluta, nyhetsutsalg, avhoppere og hjelpeorganisasjoner for å nå regimets mål: utvikle forsvaret, styrke økonomien og sikre innenlandsk stabilitet.

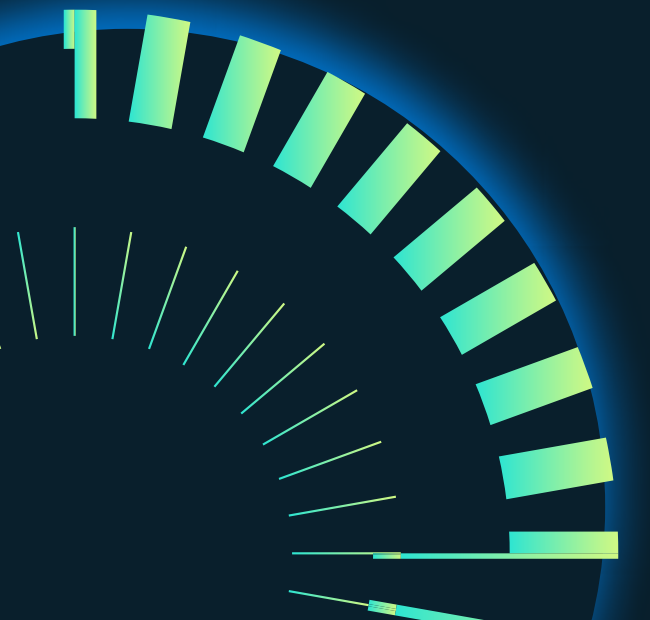
Finn ut mer på side 49

Nettselgere truer stabiliteten på nettet ettersom denne voksende bransjen av private selskaper utvikler og selger avanserte verktøy, teknikker og tjenester for å gjøre det mulig for kundene sine (ofte regjeringer) å bryte seg inn på nettverk og enheter.

Finn ut mer på side 52

Innledning

Etter høyprofilerte angrep i 2020 og 2021 brukte statlige trusselaktører betydelige ressurser til å tilpasse seg nye typer sikkerhetsbeskyttelse implementert av organisasjoner for å forsvare seg mot sofistikerte trusler.



Mye på samme måte som selskapsorganisasjoner begynte angripere å benytte seg av fremskritt innen automatisering, skyinfrastruktur og teknologier for ekstern tilgang for å utvide angrepene mot et bredere sett med mål. Disse taktiske justeringene resulterte i nye tilnærminger og angrep i stor skala mot selskapers forsyningskjeder. IT-sikkerhetshygiene ble enda viktigere etter hvert som aktører utviklet nye måter for rask utnyttelse av ikke-oppdaterte sårbarheter, utvidet teknikker for å kompromittere bedriftsnettverk og tilslørte operasjonene sine ved hjelp av programvare med åpen kildekode eller legitim programvare. Nye angrepsteknikker ga nye vektorer som er vanskeligere å oppdage, for å få tilgang til nettverket til et mål. Til slutt, etter hvert som fysiske angrep i krigen har eskalert, har vi sett at nettangrep spiller en fremtredende rolle i militær aktivitet.

Konflikten i Ukraina har gitt oss et meget og altfor håndgripelig eksempel på hvordan nettangrep utvikler seg for å påvirke verden, parallelt med militær konflikt på bakken. Kraftsystemer, telekommunikasjonssystemer, medier og annen kritisk infrastruktur har blitt mål både for fysiske angrep og nettangrep. Forsøk på nettverkskompromittering som vanligvis ble observert som en del av spionasje og informasjonseksfiltrasjonskampanjer, har blitt fokusert i hybrid krig mot destruktive angrep fra slettingsprogramvare mot kritiske infrastruktursystemer. Tilknytning av sikkerheten til disse systemene til skyen resulterte i tidlig oppdagelse og avbrudd av potensielt ødeleggende angrep.[1]

For første gang i en stor cyberhendelse brukte atferdsoppdagelse som utnytter maskinlæring, kjente angrepsmønstre for å kunne identifisere og stoppe videre angrep uten forkunnskaper om den underliggende ondsinnede programvaren – selv før mennesker var klar over truslene. Vi bekreftet også verdien av å dele trusseletterretning i sanntid med forsvarere som beskytter disse systemene, noe som gir dem viktig informasjon de kan bruke til å forutse og forsvare seg mot aktive angrep.

Statlige trusselaktører over hele verden fortsetter å utvide operasjonene sine på nye og gamle måter. Kina, Nord-Korea, Iran og Russland har utført angrep på Microsoft-kunder. Forsyningskjeden for IT-tjenester ble et vanlig mål da aktører flyttet fokuset til tjenester oppstrøms som kan fungere som tilgangspunkter til flere organisasjoner. Vi forventer at aktører fortsetter å utnytte pålitelige relasjoner i forsyningskjeder for bedrifter, og vi understreker viktigheten av omfattende håndheving av godkjenningsregler, hyppig oppdatering og kontokonfigurasjon for infrastruktur for ekstern tilgang og hyppige revisjoner av partnerrelasjoner for å verifisere autentisitet.

Statlige aktører, har mye på samme måte som løsepengevirus og kriminelle operatører, reagert på økt eksponering ved å bevege seg mot målretting mot dårlig konfigurerte eller ikke-oppdaterte bedriftssystemer (VPN/VPS-infrastruktur, lokale servere og tredjepartsprogramvare) for å utføre fysiske angrep. Mange har økt bruken av ondsinnet programvare som en handelsvare og «red team»-verktøy med åpen kildekode for å tilsløre sin ondsinnede aktivitet.

Som et resultat av dette har det å opprettholde streng IT-sikkerhetshygiene gjennom prioritert oppdatering, aktivere antimanipuleringsfunksjoner, bruke administrasjonsverktøy for angrepsoverflate som RiskIQ for å få et utenforstående syn på et angrepsoverflate og aktivere flerfaktorautentisering i hele bedriften blitt grunnleggende tiltak for å proaktivt forsvare seg mot mange sofistikerte aktører.

Statlige aktører har også økt bruken av løsepengevirus som en taktikk i angrepene sine, og de gjenbruker ofte ondsinnet programvare for løsepengevirus skapt av dette kriminelle økosystemet i angrepene sine. Vi har sett aktører basert både i Iran og Nord-Korea utnytte verktøy for løsepengevirus for å skade målrettede systemer, ofte kritisk infrastruktur, hos rivaler i regionen. Til slutt har vi sett den økende trusselen fra leiesoldater på nettet som utvikler og selger verktøy, teknikker og tjenester for å utvide truslene mot sårbare tredjepartsløsninger. De sofistikerte og smidige angrepene fra statlige aktører vil fortsette å utvikle seg år for år. Organisasjoner må reagere ved å bli informert om disse aktørendringene og utvikle forsvaret parallelt.

John Lambert
Viseadministrerende direktør og anerkjent ingeniør, Microsoft Threat Intelligence Center

Bakgrunn om nasjonsdata

Statlige trusler er trusselaktiviteter på nettet som kommer fra et bestemt land, med en åpenbar hensikt om å fremme nasjonale interesser. Statlige aktører utgjør noen av de mest avanserte og vedvarende truslene kundene våre står overfor, inkludert tyveri av immaterielle rettigheter, spionasje, overvåking, legitimasjonstyveri, destruktive angrep og mer.

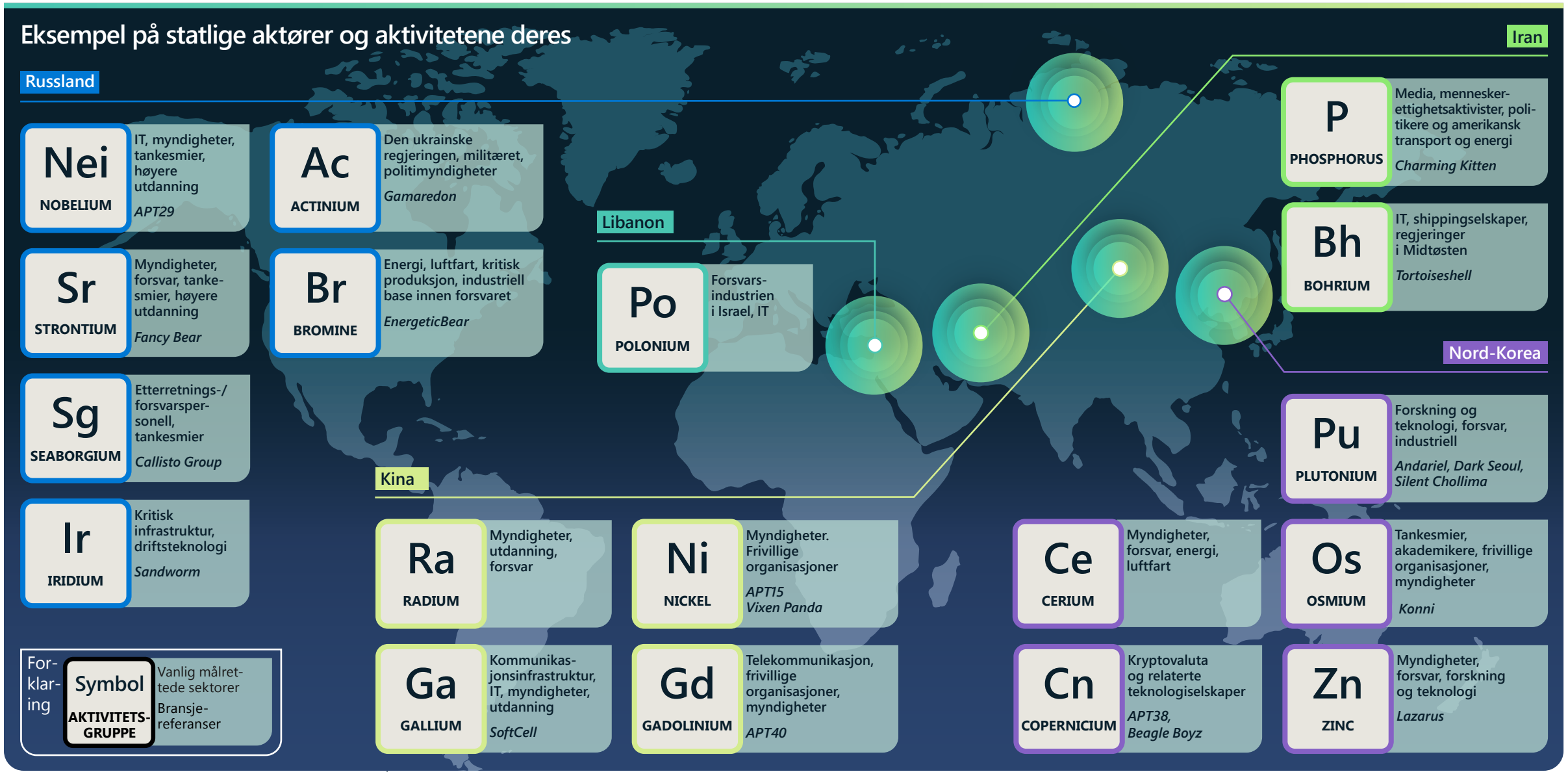
Vi investerer betydelige ressurser i å oppdage, forstå og motvirke disse truslene. Når en organisasjon eller individuell kontoinnehaver er målrettet eller kompromittert av observerte statlige aktiviteter, leverer Microsoft et varsel i form av et NSN (nasjonalt varsel) direkte til kunden, inkludert informasjonen de trenger for å undersøke aktiviteten. Per juni 2022 hadde vi levert over 67 000 NSN-er siden vi begynte i 2018.

Microsoft NSN-varslingsdata presenteres i dette kapittelet for å gi en oversikt over målbar aktivitet. Nivået av aktivitet fra nasjonale aktører som vises i diagrammene, er basert på antallet NSN-er Microsoft utstedte til kunder som respons på oppdagelsen av statlige aktører som målretter mot eller som kompromitterer minst én konto i kundeorganisasjonen.

De fire primære nasjonalstatene som har trusselgrupper vi inkluderer i denne rapporten, er Russland, Kina, Iran og Nord-Korea. Disse representerer opprinnelseslandene for de mest vanlige observerte aktørene som har målrettet mot Microsoft-kunder i løpet av det siste året. Rapporten inneholder også observasjonene våre om trusselgrupper fra Libanon og fra leiesoldater på nettet, eller angrepsaktører i privat sektor som er til leie.

Microsoft identifiserer statlige grupper etter navn på kjemiske grunnstoffer (for eksempel NOBELIUM), hvorav kun noen få vises på følgende side. Vi bruker DEV-#####-betegnelser som et midlertidig navn gitt til et ukjent, fremvoksende eller utviklende klynge av trusselaktivitet, slik at vi kan spore den som et unikt sett med informasjon til vi når en høy grad av tillit til opprinnelsen eller identiteten til aktøren bak aktiviteten.

Når den oppfyller kriteriene, konverteres en DEV til en navngitt aktør eller slås sammen med eksisterende aktører. Gjennom dette kapittelet siterer vi eksempler på nasjonale grupper og DEV-grupper for å gi et dypere innblikk i angrepsmål, teknikker og analyse av motivasjoner. Selv om mange av disse gruppene bruker de samme verktøyene som nettkriminelle, utgjør de unike trusler i form av skreddersydd ondsinnet programvare, muligheten til å oppdage og utnytte nulldagssårbarheter og straffefrihet.


Eksempel på statlige aktører og aktivitetene deres
Russland
Nei
NOBELIUM
IT, myndigheter, tankesmier, høyere utdanning
APT29
Ac
ACTINIUM
Den ukrainske regjeringen, militæret, politimyndigheter
Gamaredon
Sr
STRONTIUM
Myndigheter, forsvar, tanke-smier, høyere utdanning
Fancy Bear
Br
BROMINE
Energi, luftfart, kritisk produksjon, industriell base innen forsvaret
EnergeticBear
Sg
SEABORGIUM
Etterretnings-/ forsvarsper-sonell, tankesmier
Callisto Group
Ir
IRIDIUM
Kritisk infrastruktur, driftsteknologi
Sandworm
Libanon
Po
POLONIUM
Forsvars-industrien i Israel, IT
Iran
P
PHOSPHORUS
Media, mennesker-ettighetsaktivister, poli-tikere og amerikansk transport og energi
Charming Kitten
Bh
BOHRIUM
IT, shippingselskaper, regjeringer i Midtøsten
Tortoiseshell
Nord-Korea
Pu
PLUTONIUM
Forskning og teknologi, forsvar, industriell
Andariel, Dark Seoul, Silent Chollima
Kina
Ra
RADIUM
Myndigheter, utdanning, forsvar
Ni
NICKEL
Myndigheter. Frivillige organisasjoner
APT15
Vixen Panda
Ce
CERIUM
Myndigheter, forsvar, energi, luftfart
Os
OSMIUM
Tankesmier, akademikere, frivillige organisasjoner, myndigheter
Konni
Ga
GALLIUM
Kommunikas-jonsinfrastruktur, IT, myndigheter, utdanning
SoftCell
Gd
GADOLINIUM
Telekommunikasjon, frivillige organisasjoner, myndigheter
APT40
Cn
COPERNICIUM
Kryptovaluta og relaterte teknologiselskaper
APT38,
Beagle Boyz
Zn
ZINC
Myndigheter, forsvar, forskning og teknologi
Lazarus
For-klar-ing
Symbol
AKTIVITETS-GRUPPE
Vanlig målret-tede sektorer
Bransje-referanser

Det utviklende trussellandskapet

Microsofts mål om å spore statlig aktøraktivitet og varsle kunder når vi ser at de blir målrettet eller kompromittert, er forankret i vår misjon om å beskytte kundene våre mot angrep.

Denne varslingen er en viktig del av vår forpliktelse til å informere kunder om observerte angrep er avverget av sikkerhetsproduktet vårt, eller om angrepene er effektive på grunn av ukjente sikkerhetssvakheter. Sporing av varslinger over tid hjelper Microsoft å identifisere nye trusseltrender fra aktører, og vi kan fokusere produktbeskyttelsen på proaktiv begrensning av trusler mot kunder i alle skytjenestene våre.

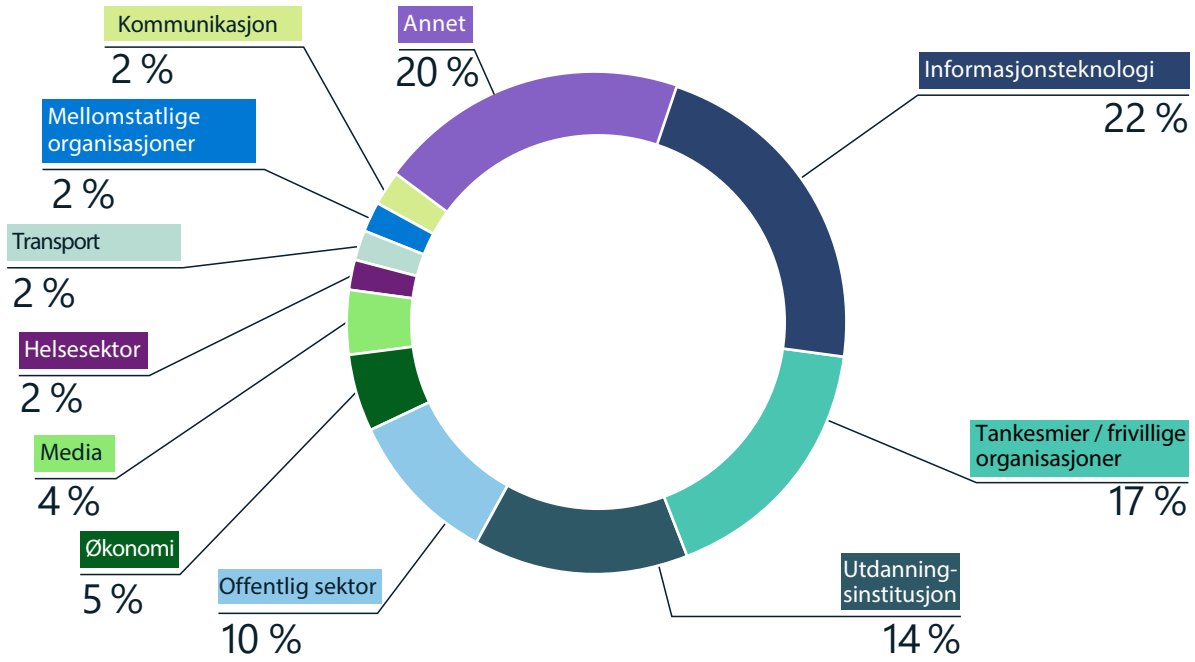
Med denne sporingen kan vi også dele data og innsikt om det vi ser. Analytikerne som sporer disse aktørene og følger angrepene, baserer seg på en kombinasjon av tekniske indikatorer og geopolitisk ekspertise for å forstå motivasjonen til aktørene, og de kombinerer teknisk og global kontekst i ny innsikt. Denne kurateringen gir et unikt innblikk i prioriteringene til statlige aktører på nettet og hvordan motivasjonene deres kan gjenspeile de politiske, militære og økonomiske prioriteringene i nasjonalstatene som hyrer dem.

Den politiske utviklingen det siste året har formet prioriteringene og risikotoleransen til trusselgrupper sponset av nasjonalstater over hele verden. Etter hvert som geopolitiske relasjoner har brutt sammen og haukiske elementer har fått mer kontroll i enkelte nasjoner, har nettaktører blitt mer frekke og aggressive. Eksempler:

- Russland har nådeløst målrettet seg mot myndighetene i Ukraina og landets kritiske infrastruktur for å komplementere den militære aksjonen på bakken.[2]
- Iran har aggressivt forsøkt å trenge inn i den kritiske infrastrukturen i USA, for eksempel havnemyndigheter.
- Nord-Korea har fortsatt sin kampanje for å stjele kryptovaluta fra finans- og teknologiselskaper.
- Kina har utvidet sine globale nettspionasjeoperasjoner.

Selv om statlige aktører kan være teknisk sofistikerte og anvende en rekke taktikker, kan angrepene ofte begrenses av god netthygiene. Mange av disse aktørene er avhengige av relativt lavteknologiske virkemidler, for eksempel målrettede phishing-e-poster, for å levere sofistikert ondsinnet programvare i stedet for å investere i utvikling av tilpassede trusler eller bruk av målrettet sosial manipulering for å nå sine mål.

Bransjesektorer målrettet av statlige aktører



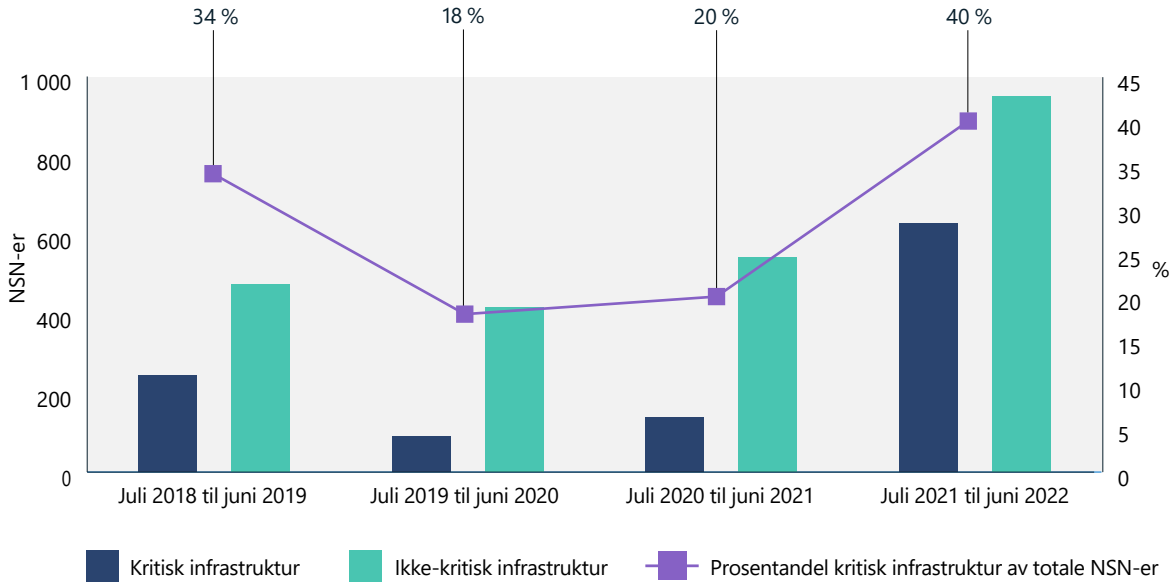
Statlige grupper målrettet mot en rekke sektorer. Statlige aktører i Russland og Iran målrettet mot IT-bransjen som et middel for å få tilgang til IT-firmaenes kunder. Tankesmier, ikke-statlige organisasjoner (NGO-er), universiteter og offentlige etater er fortsatt andre vanlige mål for statlige aktører.

Statlige aktører har en rekke mål som kan resultere i målretting mot bestemte grupper av organisasjoner eller enkeltpersoner. I løpet av det siste året har angrep på forsyningskjeden økt, med et spesielt fokus på IT-selskaper. Ved å kompromittere IT-tjenesteleverandører er trusselaktører ofte i stand til å nå sitt opprinnelige mål gjennom en pålitelig relasjon til selskapet som administrerer tilkoblede systemer, eller potensielt utføre angrep i mye større skala ved å kompromittere hundrevis av kunder nedstrøms i ett angrep. Etter IT-sektoren var de mest målrettede enhetene tankesmier, akademikere knyttet til universiteter og offentlige tjenestepersoner. Dette er ønskelige «myke mål» for spionasje, for innsamling av etterretning om geopolitiske spørsmål.

Det utviklende trussellandskapet

Fortsettelse

Trender innen kritisk infrastruktur

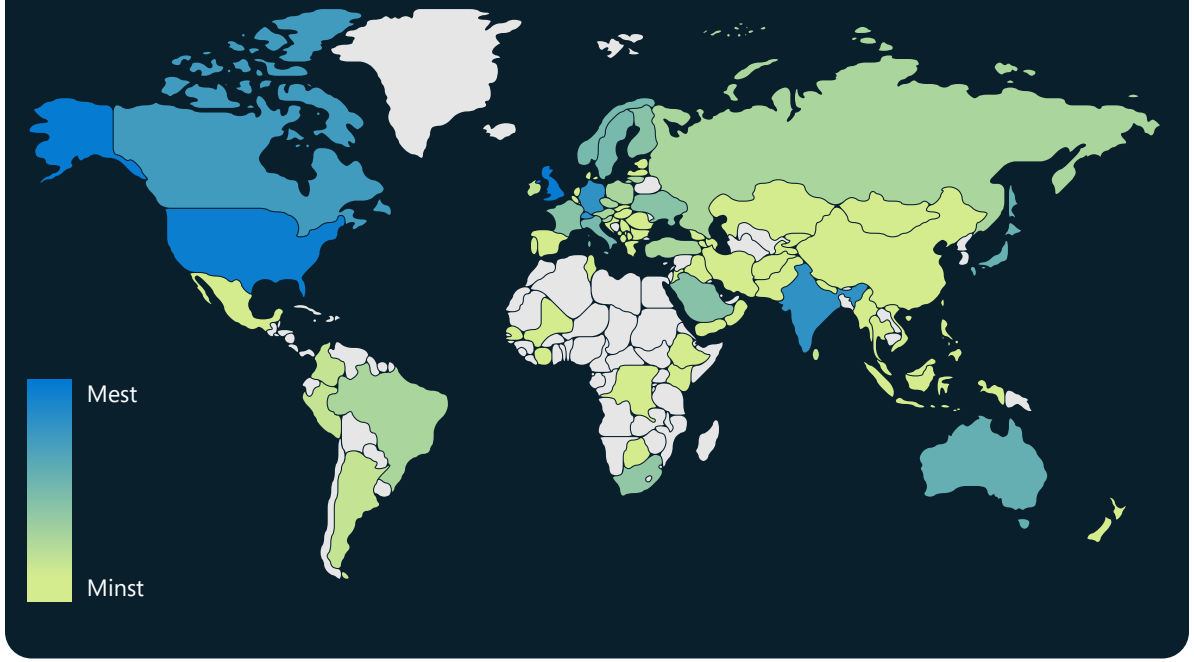


Statlige gruppers målretting mot kritisk infrastruktur[3] økte det siste året, med aktørers fokus på selskaper i IT-sektoren, finansielle tjenester, transportsystemer og kommunikasjonsinfrastruktur.

«Før invasjonen av Ukraina trodde myndighetene at data måtte beholdes internt i en nasjon for å være sikre. Etter invasjonen er overføring av data til skyen og flytting utenfor territorielle grenser nå en del av robusthetsplanlegging og god styring.»

Cristin Flynn Goodwin,
Assisterende rådgiver, kundesikkerhet og -tillit

Statlige aktørers geografiske målretting



Målrettingen på nettet til statlige grupper har spredt seg over hele verden det siste året, med et spesielt tungt fokus på amerikanske og britiske bedrifter. Organisasjoner i Israel, De forente arabiske emirater, Canada, Tyskland, India, Sveits og Japan var også blant de mest målrettede, i henhold til NSN-dataene våre.

Handlingsrettet innsikt

1. Identifiser og beskytt dine potensielle datamål av høy verdi, teknologi i risikogruppen, informasjon og bedriftsoperasjoner som kan sammenfalle med de strategiske prioriteringene til statlige grupper.
2. Aktiver skybeskyttelse for å sørge for identifisering og avverging av kjente og nye trusler mot nettverket ditt i stor skala.

IT-forsyningskjeden som en gateway til det digitale økosystemet

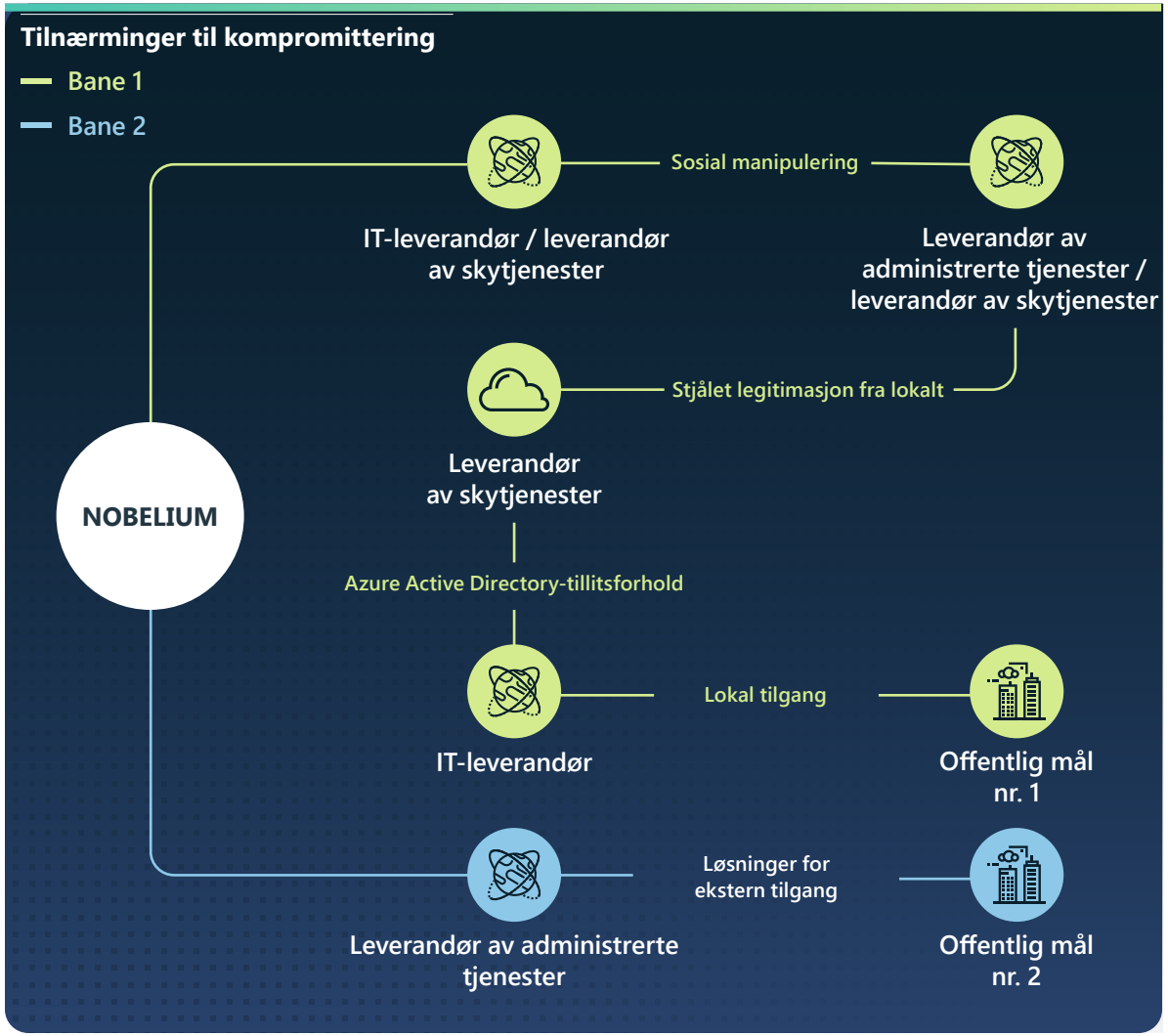
Nasjonalstaters målretting av IT-tjenesteleverandører kan gjøre det mulig for trusselaktører å utnytte andre organisasjoner av interesse ved å dra nytte av tillit og tilgang gitt til disse leverandørene av forsyningskjeden. I det siste året målrettet statlige cybertrusselgrupper leverandører av IT-tjenester for å angripe tredjepartsmål og få tilgang til klienter nedstrøms i offentlig sektor, politikk og kritisk infrastruktur.

IT-tjenesteleverandører er attraktive mellommål siden de betjener hundrevis av direkte og tusenvis av indirekte kunder av interesse for utenlandske etterretningstjenester. Hvis disse utnyttes, kan rutinemessige forretningspraksiser og de delegerte administrative privilegiene som disse bedriftene nyter godt av, gi ondsinnede aktører tilgang til og muligheten til å manipulere klientnettverk for IT-tjenesteleverandører uten umiddelbart å utløse varsler.

I løpet av det siste året forsøkte NOBELIUM å kompromittere og utnytte privilegerte kontoer hos skyløsninger og andre leverandører av administrerte tjenester for å forsøke målrettet tilgang nedstrøms, primært mot amerikanske og europeiske myndigheter og politiske kunder.

NOBELIUM demonstrerte hvordan en «kompromitter én for å kompromittere mange»-tilnærming kan rettes inn mot en oppfattet geopolitisk motstander. Det siste året har trusselaktører brukt både tredjepartsinntrenging og direkte inntrenging i sensitive organisasjoner basert i medlemslandene i NATO, , som den russiske regjeringen oppfatter som en eksistensiell trussel. Mellom juli 2021 og begynnelsen av juni 2022 gikk 48 prosent av Microsofts kundevarsler om russisk trusselaktivitet mot kunder på nettet til IT-bedrifter basert i medlemsland i NATO, sannsynligvis som tilgangspunkter i form av mellomledd. Samlet sett gikk 90 prosent av varslene om russiske trusselaktiviteter i løpet av samme periode til kunder basert i medlemsland i NATO, primært innen IT, tankesmier og ikke-statlige organisasjoner (NGO-er) og offentlig sektor, noe som antyder en strategi der de tar i bruk flere metoder for å oppnå innledende tilgang til disse målene.

Det har vært et skifte fra å utnytte programvareforsyningskjeden til å utnytte forsyningskjeden for IT-tjenester, målrette mot skyløsninger og leverandører av administrerte tjenester for å nå kunder nedstrøms.



Dette diagrammet viser NOBELIUMs multivektorbaserte tilnærming for å kompromittere sine endelige mål og følgeskadene for andre ofre underveis. I tillegg til handlingene vist ovenfor iverksatte NOBELIUM passordspray og phishing-angrep mot de involverte enhetene, og målrettet til og med den personlige kontoen til minst én offentlig ansatt som en annen potensiell vei mot kompromittering.

IT-forsyningskjeden som en gateway til det digitale økosystemet

Fortsettelse

Gjennom hele året oppdaget Microsoft Threat Intelligence Center (MSTIC) et økende antall statlige aktører fra Iran og aktører tilknyttet Iran som kompromitterte IT-selskaper. I mange tilfeller ble aktørene oppdaget under stjeling av påloggingslegitimasjon for å få tilgang til klienter nedstrøms for en rekke formål, fra innhenting av etterretning til destruktive gjengjeldelsesangrep.

- I juli og august 2021 kompromitterte DEV-0228 en israelsk leverandør av forretningsprogramvare for senere å kompromittere kunder nedstrøms i det israelske forsvaret, energisektoren og juridisk sektor.[4]
- Fra august til september 2021 oppdaget Microsoft en topp i statlige aktører fra Iran som målrettet mot IT-selskaper basert i India. Mangelen på presserende geopolitiske problemer som ville ha medført et slikt skifte, antyder at denne målrettingen er for indirekte tilgang til datterselskaper og klienter utenfor India.
- I januar 2022, kompromitterte DEV-0198, en gruppe som vi vurderer er tilknyttet regjeringen i Iran, en israelsk skyløsning-sleverandør. Microsoft vurderer at aktøren sannsynligvis brukte kompromittert legitimasjon fra leverandøren for å logge seg inn på et israelsk logistikkselskap. MSTIC observerte at den samme aktøren forsøkte å gjennomføre et destruktivt nettangrep mot logistikkselskapet senere samme måned.
- I april 2022 kompromitterte POLONIUM, en gruppe basert i Libanon som vi vurderer samarbeidet med statlige grupper i Iran om teknikker for IT-forsyningskjede, et annet israelsk IT-selskap for å få tilgang til det israelske forsvaret og juridiske organisasjoner.[5]

Aktiviteten i løpet av det siste året viser at trusselaktører som NOBELIUM og DEV-0228 gjør seg kjent med organisasjoners pålitelige relasjoner bedre enn organisasjonene selv. Denne økte trusselen understreker behovet for at organisasjoner må forstå og styrke grensene og inngangspunktene til sine digitale ressurser. Det understreker også viktigheten av at IT-tjenesteleverandører strengt overvåker sin egen nettsikkerhetstilstand. Organisasjoner bør for eksempel implementere retningslinjer for flerfaktorautentisering og betinget tilgang, noe som gjør det vanskeligere for ondsinnede aktører å ta over privilegerte kontoer eller spre seg på et nettverk.

Grundig gjennomgang og revisjon av partnerrelasjoner bidrar til å minimere eventuelle unødvendige tillatelser mellom organisasjonen og leverandører oppstrøms og umiddelbar fjerning av tilgang for eventuelle relasjoner som ser ukjente ut. Økt kjennskap til aktivitetslogger og gjennomgang av tilgjengelig aktivitet gjør det enklere å oppdage avvik, noe som kan sette i gang ytterligere undersøkelser.

Statlig målretting av tredjeparter gjør det mulig for dem å utnytte sensitive organisasjoner ved å dra nytte av tillit og tilgang i en forsyningskjede.

Handlingsrettet innsikt

1. Gå gjennom og overvåk relasjoner til tjenesteleverandører oppstrøms og nedstrøms og delegert tilgang til rettigheter for å minimere unødvendige tillatelser. Fjern tilgangen for eventuelle partnerrelasjoner som ser ukjente ut, eller som ennå ikke er revidert.[6]
2. Aktiver logging og gå gjennom all autentiseringsaktivitet for infrastruktur for ekstern tilgang og virtuelle private nettverk (VPN-er), med fokus på kontoer som er konfigurert med godkjenning med én faktor, for å bekrefte ekthet og undersøke avvikende aktivitet.
3. Aktiver flerfaktorautentisering for alle kontoer (inkludert tjenestekontoer) og sørg for at dette håndheves for all ekstern tilkobling.
4. Bruk passordløse løsninger for å sikre kontoer.[7]

Koblinger til mer informasjon

- NOBELIUM målretter mot delegerte administrative privilegier for å tilrettelegge for bredere angrep | Microsoft Threat Intelligence Center (MSTIC)
- Iransk målretting mot IT-sektoren på vei opp | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Eksponering av POLONIUM-aktivitet og infrastruktur målrettet mot israelske organisasjoner | Microsoft Threat Intelligence Center (MSTIC)

Rask sårbarhetsutnyttelse

Når organisasjoner styrker sine holdninger til nettsikkerhet, svarer statlige aktører med å ta i bruk nye og unike taktikker for å levere angrep og unngå oppdagelse. Identifikasjon og utnyttelse av tidligere ukjente sårbarheter – kjent som nulldagssårbarheter – er en viktig taktikk i dette arbeidet.

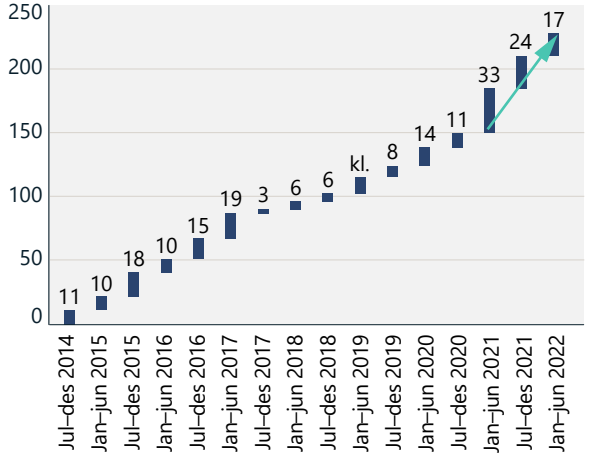
Nulldagssårbarheter er et spesielt effektivt middel for innledende utnyttelse, og når offentlig eksponert, kan sårbarheter raskt gjenbrukes av andre statlige og kriminelle aktører. Antallet offentlig avslørte nulldagssårbarheter det siste året er på høyde med året før, som var det høyeste som noen gang har vært registrert.

Etter hvert som trusselaktører på nettet – både statlige og kriminelle – blir flinkere til å utnytte disse sårbarhetene, har vi observert en reduksjon i tiden mellom kunngjøringen av en sårbarhet og kommodifiseringen av denne sårbarheten. Dette gjør det viktig for organisasjoner å oppdatere umiddelbart, for å forebygge mot trusler. På samme måte er det viktig at organisasjoner eller enkeltpersoner som avdekker nye sårbarheter, på en ansvarlig måte avslører eller rapporterer dem til berørte leverandører så snart som mulig, i tråd med koordinerte prosedyrer for avsløring av sårbarheter.

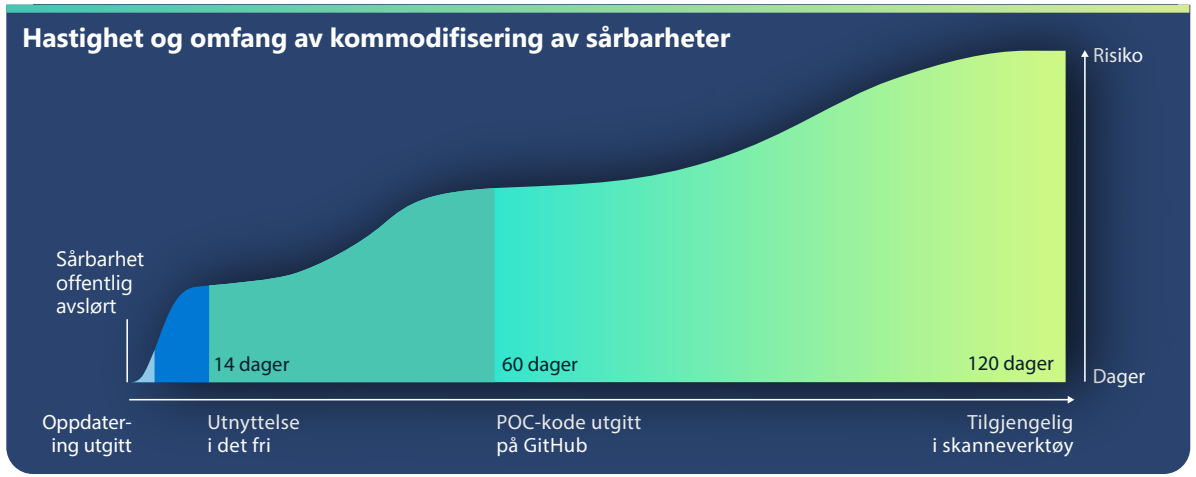
Dette sikrer at sårbarheter identifiseres, og at oppdateringer utvikles i tide for å beskytte kunder mot tidligere ukjente trusler.

Mange organisasjoner antar at det er mindre sannsynlig at de blir utsatt for nulldagsangrep hvis administrasjonen av sårbarheter er integrert i nettverkssikkerheten. Kommodifiseringen av trusler gjør imidlertid at angrepene blir mer hyppige. Nulldagstrusler oppdages ofte av andre aktører og gjenbrukes bredt i en kort tidsperiode, noe som gjør at ikke-oppdaterte systemer er i fare. Selv om nulldagstrusler kan være vanskelige å oppdage, er aktørenes handlinger etter utnyttelsen ofte enklere å oppdage, og hvis dette kommer fra fullstendig oppdatert programvare, kan det fungere som et fareskilt for kompromittering.

Oppdateringer utgitt for nulldags-sårbarheter



Antall offentlig avslørte nulldagstrusler fra listen over vanlige sårbarheter og avsløringer (CVE-er).



I gjennomsnitt tar det bare 14 dager før en utnyttelse er tilgjengelig etter at en sårbarhet er offentlig avslørt. Denne visningen gir en analyse av tidslinjene for utnyttelse av nulldagssårbarheter, sammen med antall systemer som er sårbare for den gitte utnyttelsen, og som er aktive på Internett fra tidspunktet for første offentlige avsløring.

Selv om nulldagsangrep på sårbarheter i utgangspunktet har en tendens til å målrette seg mot et begrenset sett med organisasjoner, blir de raskt tatt i bruk i det større økosystemet for trusselaktører. Dette starter et kappløp for trusselaktører om å utnytte sårbarheten så mye som mulig før de potensielle målene installerer oppdateringer.

Selv om vi observerer mange statlige aktører som utvikler utnyttelser fra ukjente sårbarheter, er statlige trusselaktører basert i Kina spesielt dyktige til å oppdage og utvikle nulldagstrusler. Kinas forskrifter for sårbarhetsrapportering trådte i kraft september 2021. Dette er første gang i verden en regjering krever rapportering av sårbarheter til en offentlig myndighet for gjennomgang før sårbarheten deles med produkt- eller tjenesteeieren. Denne nye forskriften kan gjøre det mulig for elementer i den kinesiske regjeringen å lagre rapporterte sårbarheter for deretter å bruke dem som et våpen. Den økte bruken av nulldagsangrep det siste året fra aktører basert i Kina gjenspeiler trolig det første hele året av Kinas krav til avsløring av sårbarheter for det kinesiske sikkerhetsfellesskapet og et stort skritt i bruken av nulldagstrusler som en statlig prioritet. Sårbarhetene som er beskrevet nedenfor, ble først utviklet og tatt i bruk av statlige aktører i Kina under angrep, før de ble oppdaget og spredt blant andre aktører i det bredere trusseløkosystemet.

Rask sårbarhetsutnyttelse

Fortsettelse

Selv organisasjoner som ikke er et mål for statlige angrep, har en begrenset periode på å oppdatere nulldagssårbarheter i berørte systemer før de utnyttes av det bredere aktørøkosystemet.

Disse eksemplene på nylig identifiserte sårbarheter viser at organisasjoner i gjennomsnitt har 60 dager fra tidspunktet en sårbarhet blir oppdatert og en konseptutprøvingskode (POC) gjøres tilgjengelig på nettet, og dette plukkes ofte opp av andre aktører for gjenbruk. På samme måte har organisasjoner i gjennomsnitt 120 dager før en sårbarhet er tilgjengelig i automatiserte verktøy for sårbarhetsskanning og utnyttelse, som Metasploit – noe som ofte fører til at utnyttelsen brukes i stor skala. Dette fremhever at selv organisasjoner som ikke er et mål for statlige trusselaktører, har en begrenset periode på å oppdatere nulldagssårbarheter i berørte systemer før sårbarhetene utnyttes av det bredere aktørøkosystemet.

CVE-2021-35211 SolarWinds Serv-U

I juli 2021 utstedte SolarWinds et sikkerhetsråd for CVE-2021-35211, der Microsoft ble kreditert varslingen.[8] På dette tidspunktet oppdaget vi at en statlig trusselaktør, DEV-0322, aktivt utnyttet SolarWinds Serv-U-sårbarheten. RiskIQ-teamet vårt observerte 12 646 IP-adresser som driftet Internett-tilkoblede versjoner av de berørte enhetene mellom 15. juni og 9. juli.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

I september 2021 observerte forskerne våre at aktører knyttet til Kina utnytter Zoho ManageEngine i flere enheter basert i USA. Sårbarheten ble offentlig rapportert 6. september som CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, som organisasjoner vanligvis bruker til å håndtere tilbakestilling av passord.[9] DEV-0322 utnyttet sårbarheten senere i september, ved å bruke den som en innledende vektor for å få et fotfeste i nettverk og utføre flere handlinger, inkludert legitimasjonsdumping, installering av egendefinerte binærfiler og dumping av ondsinnet programvare for å opprettholde persistens. På tidspunktet for avsløringen observerte RiskIQ 4011 forekomster av disse systemene aktive og på Internett.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Sent i oktober 2021 observerte vi at DEV-0322 utnyttet en sårbarhet (CVE-2021-44077) i et annet Zoho ManageEngine-produkt, ServiceDesk Plus, programvare for IT-brukerstøtte med ressursstyring. DEV-0322 brukte denne sårbarheten for å målrette mot og kompromittere enheter i helsevesenet, informasjonsteknologi, høyere utdanning og kritiske produksjonssektorer. 2. desember utstedte Federal Bureau of Investigation (FBI) og Cybersecurity and Infrastructure Security Agency (CISA) en felles rådgivende advarsel til publikum om statlige trusselaktører som utnytter sårbarheten. På tidspunktet for avsløringen observerte RiskIQ 7956 forekomster av disse systemene aktive og på Internett.

CVE-2021-42321 Microsoft Exchange

En nulldagsutnyttelse for en Exchange-sårbarhet, CVE-2021-42321, ble avslørt under Tianfu Cup, et internasjonalt toppmøte om nettsikkerhet og en hacking-konkurranse som avholdes 16. oktober og 17. oktober 2021 i Chengdu i Kina. Sikkerhetsforskere hos Microsoft observerte utnyttelsen av Exchange-sårbarheten i fri bruk 21. oktober, kun tre dager etter at sårbarheten ble avslørt. På tidspunktet for avsløringen observerte RiskIQ 61 559 forekomster av disse systemene aktive og på Internett. Vi fortsatte å observere utnyttelsesaktivitet inn i november 2021.

CVE-2022-26134 Confluence

En aktør knyttet til Kina hadde sannsynligvis nulldagskoden for Confluence-sårbarheten (CVE-2022-26134) fire dager før sårbarheten ble offentlig avslørt 2. juni, og utnyttet den sannsynligvis mot en enhet basert i USA. På tidspunktet for avsløringen observerte RiskIQ 53 621 forekomster av sårbare Confluence-systemer på Internett.

Sårbarheter blir plukket opp og utnyttet i stor skala, og i stadig kortere tidsrammer.

Handlingsrettet innsikt

1. Prioriter oppdatering av nulldagssårbarheter så snart de utgis. Ikke vent på implementering av behandlingssyklusen for oppdateringer.
2. Dokumenter og lag beholdning av alle maskinvare- og programvareressurser for bedrifter for å fastslå risiko og raskt fastslå når det skal ageres på oppdateringer.

Russiske statlige aktørers taktikk på nettet i krigstid er en trussel både for Ukraina og resten av verden

I år har russiske statlige aktører lansert cyberoperasjoner for å komplementere militære handlinger under Russlands invasjon av Ukraina, ofte ved hjelp av de samme taktikkene og teknikkene som har blitt tatt i bruk mot mål utenfor Ukraina. Det er avgjørende at organisasjoner over hele verden iverksetter tiltak for å skjerpe nettsikkerheten mot digitale trusler som stammer fra trusselaktører samordnet fra Russland.

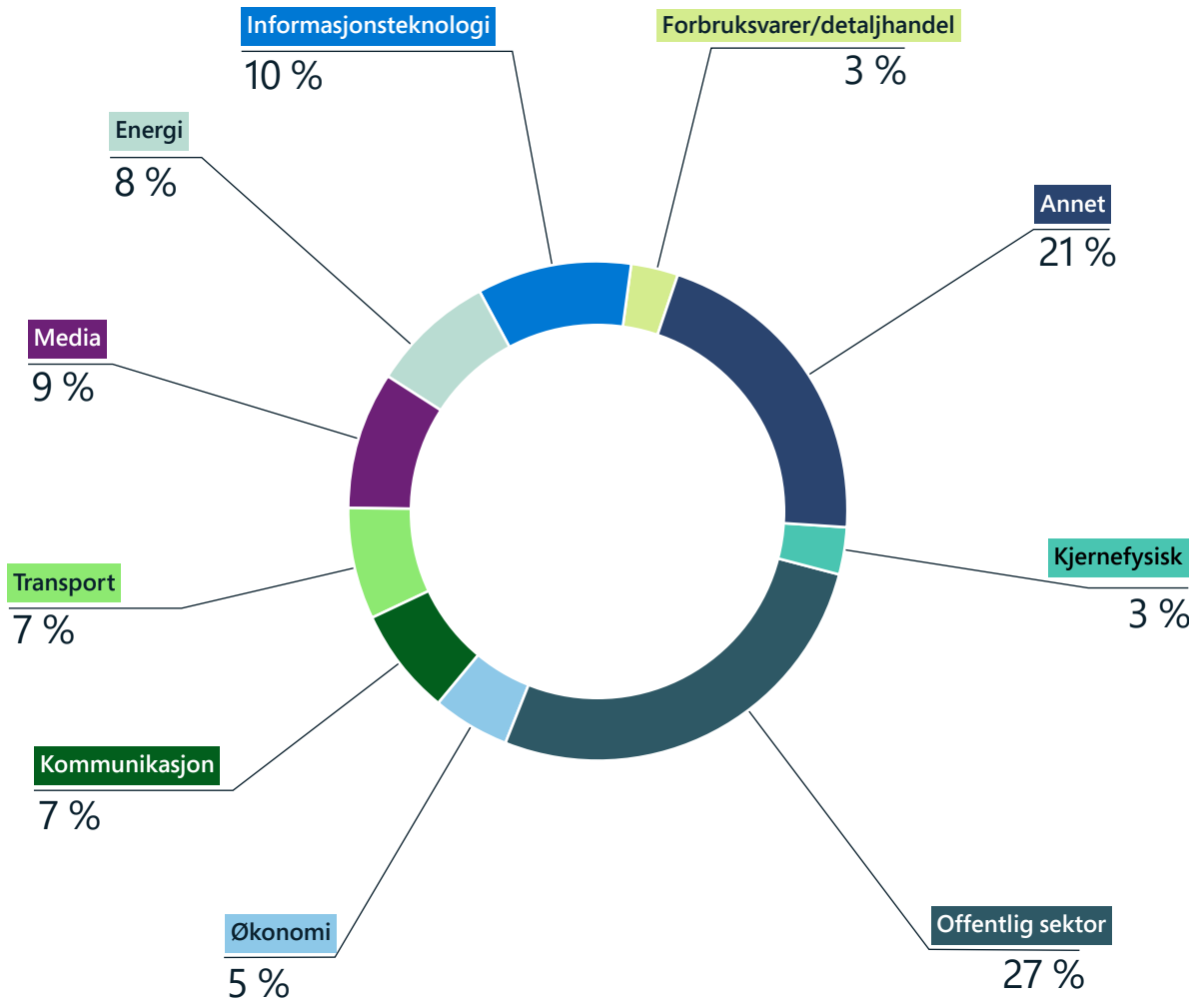
Situasjonen på bakken fortsetter å variere etter hvert som den militære konflikten vedvarer, og Ukraina og landets allierte må være forberedt på å forsvare seg hvis statlige nettoperatører i Russland øker hyppigheten eller intensiteten av inntrenging i tråd med militære mål. I løpet av de første fire månedene av krigen observerte Microsoft at trusselaktører knyttet til det russiske militæret lanserte en rekke bølger av destruktive nettangrep mot nesten 50 forskjellige instanser og bedrifter, og spionasjefokusert inntrenging mot mange andre. Hvis vi ekskluderer operasjoner mot kunder hos nettjenester, var 64 prosent av den russiske trusselaktiviteten mot kjente mål rettet mot organisasjoner basert i Ukraina mellom slutten av februar og juni.

I hver operasjon benyttet russiske trusselaktører mange av taktikkene, teknikkene og prosedyrene (TTP-er) som vi har observert i bruk før invasjonen, mot mål både i og utenfor Ukraina. Disse aktørene hadde til hensikt å ødelegge data og sette offentlige etater i Ukraina ute av spill i den innledende perioden i konflikten. Siden har de forsøkt å forpurre transporten av militær og humanitær assistanse til Ukraina, forstyrre publikums tilgang til tjenester og medier og stjele informasjon om langsiktig intelligens eller av økonomisk verdi til Russland.

Målretting mot transport truer et område av kritisk viktighet for innbyggere i Ukraina som prøver å overleve under krigen. Ifølge en undersøkelse sponset av UNICEF i mai var respondentene i konfliktberørte urbane områder mest bekymret for transport og drivstoff, forsyningsforstyrrelser, sikkerhet og begrenset tilgang til mat, medisinske tjenester og finansielle tjenester.[10] I juni sa FNs krisekoordinator for Ukraina at minst 15,7 millioner mennesker i landet hadde et presserende behov for humanitær assistanse, og at antallet ville vokse etter hvert som krigen fortsetter.[11]

Utenfor Ukraina har Microsoft oppdaget russiske forsøk på nettverksinntrenging mot 128 organisasjoner i 42 land mellom slutten av februar og juni. USA var Russlands primære mål. Polen, som har vært et transittland for mye av den internasjonale militære og humanitære hjelpen til Ukraina, var også et betydelig mål i denne perioden. Trusselaktører tilknyttet Russland angrep også organisasjoner i de baltiske landene og datanettverk i Danmark, Norge, Finland og Sverige i april og mai.

Mest målrettede bransjesektorer i Ukraina siden invasjonen



Føderale, statlige og lokale myndighetsorganisasjoner i Ukraina har forblitt prioriterte mål for russiske trusselgrupper og statlig tilknyttede trusselgrupper gjennom hele konflikten. Fokuset på organisasjoner innen transport-, energi-, finans- og mediesektoren fremhever risikoen som disse nettoperasjonene utgjør for tjenester som innbyggerne i Ukraina er avhengige av.

Russiske statlige aktørers taktikk på nettet i krigstid er en trussel både for Ukraina og resten av verden

Fortsettelse

Vi har sett en økning i lignende aktivitet rettet mot utenriksdepartementene i NATO-land.

Russiske statlige trusselgrupper har forblitt interessert i å kompromittere kritisk infrastruktur både i og utenfor Ukraina det siste året. IRIDIUM distribuerte den skadelige programvaren Industroyer2 i et mislykket forsøk på å koble ut strømmen for millioner av mennesker i Ukraina. Utenfor Ukraina utførte BROMINE inntrenginger mot organisasjoner som er involvert i produksjon, og mot industrikontrollsystemer tidlig i 2022.

Statlige aktører i Russland og aktører tilknyttet staten rettet nettoperasjoner mot Ukraina, landets allierte og andre mål av etterretningsverdi i år ved hjelp av mange av følgende TTP-er:

Målrettet phishing med ondsinnede vedlegg eller koblinger

Russiske statlige grupper og grupper tilknyttet den russiske staten, som ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM og IRIDIUM, brukte phishing-kampanjer for å få innledende tilgang til ønskede kontoer og nettverk i organisasjoner i og utenfor Ukraina.

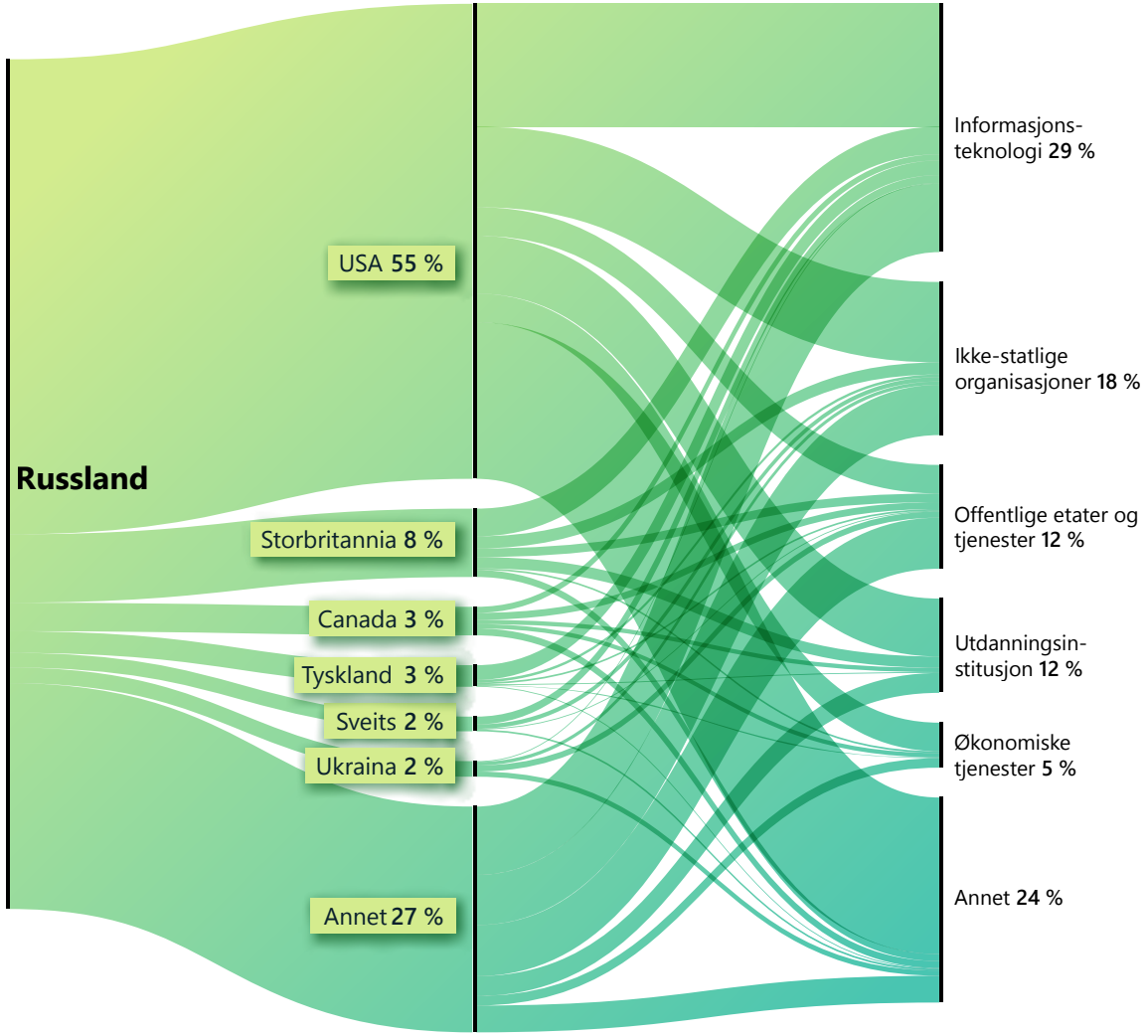
Mange kampanjer benyttet kompromitterte eller forfalskede kontoer i målrettede organisasjoner eller innen samme bransje og overbevisende temaer for å lokke ofre. NOBELIUM brukte kompromitterte, diplomatiske kontoer til å sende phishing--post forkledd som diplomatisk kommunikasjon til ansatte i utenriksdepartementer over hele verden. STRONTIUM opprettet falske kontoer basert på offentlig tilgjengelige navn på kontoinnehavere i tankesmier i USA og sendte phishing-meldinger for å få tilgang til kontoer i disse tankesmiene. SEABORGIUM iverksatte phishing-angrep ved hjelp av lokkemidler knyttet til rapportering om konflikten i Ukraina for å få innledende tilgang til kontoer hos internasjonale tankesmier i de nordiske landene.

Utnyttelse av forsyningskjeden for IT-tjenester for å påvirke kunder nedstrøms

Sent i 2021 kompromitterte russiske statlige aktører IT-tjenesteleverandører og brukte tilgangen til å legge til rette for defacing av nettsteder og implementering av Whispergates destruktive ondsinnede programvare DEV-0586 i januar.[12] DEV-0586 kompromitterte også nettverket til et IT-firma som bygde ressursstyringssystemer for det ukraniske forsvarsdepartementet og andre organisasjoner i kommunikasjons- og transportsektoren, noe som indikerte at gruppen utforsket angrepsalternativer fra tredjeparter i disse sektorene også.

Over hele verden, men spesielt i USA og Vest-Europa, målrettet NOBELIUM seg mot leverandører av IT-tjenester for å få tilgang til offentlige og andre sensitive nettverk i hele 2021 og 2022 (se diskusjonen om sårbarheter i forsyningskjeden tidligere i dette kapittelet).

Russland: topp målrettede land og bransjesektorer



Til tross for et intensivert fokus på organisasjoner basert i Ukraina siden tidlig i 2022, var bedrifter basert i Nord-Amerika og Vest-Europa fortsatt nettjenestekundene som russiske aktører målrettet seg mest mot. NOBELIUMs kampanje mot IT-sektoren gjorde den til den mest målrettede sektoren det siste året.

Russiske statlige aktørers taktikk på nettet i krigstid er en trussel både for Ukraina og resten av verden

Fortsettelse

Utnyttelse av apper vendt mot offentligheten for å få innledende tilgang til nettverk

Siden minst fra slutten av 2021 har STRONTIUM jobbet med å utvikle og forbedre sine muligheter til å utnytte offentlige tjenester, for eksempel Microsoft Exchange-servere, for å stjele informasjon. STRONTIUM utnyttet ikke-oppdaterte Exchange-servere for å få tilgang til kontoer hos regjeringen i Ukraina, i tillegg til organisasjoner relatert til militæret og forsvaret i USA, Libanon, Peru og Romania, og andre offentlige etater basert i Armenia, Bosnia og Malaysia. DEV-0586, som også er tilknyttet det russiske militæret, utnyttet Confluence-serversårbarheter for å få innledende tilgang til organisasjoner i offentlig sektor og IT-sektoren i Ukraina og andre østeuropeiske land.

Statlige russiske aktører og tilknyttede trusselaktører bruker mange av de samme TTP-ene til å kompromittere organisasjoner av interesse, både i krig og i fredstid.

Bruk av administrative kontoer og protokoller og innebygde verktøy for nettverksoppdagelse og sideveis bevegelse

Etter å ha fått innledende tilgang til et nettverk, observerte Microsoft at russiske statlige aktører utnytter legitime kontoer og programvareverktøy som brukes til å utføre grunnleggende vedlikeholdsoppgaver, for å unngå oppdaging så lenge som mulig. De baserte seg på kompromitterte identiteter med administrative funksjoner og gyldige administrasjonsprotokoller, verktøy og metoder for å bevege seg sideveis i nettverk uten umiddelbart å tiltrekke seg oppmerksomheten til automatiserte skjermer og nettverksforsvarere.

Grunnleggende netthygiene og implementering av verktøy for endepunktsoppdagelse og respons kan bidra til å redusere den negative innvirkningen av disse typene operasjoner i fredstid og i krig.

Uforutsigbarheten i den pågående konflikten krever at organisasjoner over hele verden iverksetter tiltak for å skjerpe nettsikkerheten mot digitale trusler som stammer fra statlige aktører i Russland og tilknyttede trusselaktører.

Handlingsrettet innsikt

1. Minimer legitimasjonstyveri og kontomisbruk ved å beskytte identitetene til brukerne ved å implementere verktøy for flerfaktorgodkjenning for identitetsbeskyttelse, og ved å håndheve minste privilegium for tilgang for å sikre de mest sensitive og privilegerte kontoene og systemene.
2. Bruk oppdateringer for å sikre at alle systemene dine får høyest mulig beskyttelsesnivå så snart som mulig, og at de holdes oppdatert.
3. Ta i bruk løsninger for beskyttelse mot ondsinnet programvare, endepunktsoppdagelse og identitetsbeskyttelse i hele organisasjonen. En kombinasjon av dyptgående sikkerhetsløsninger, sammen med opplært og dyktig personell, kan gi organisasjonen din muligheten til å identifisere, oppdage og forhindre at inntrenginger påvirker virksomheten din.
4. Aktiver undersøkelser og gjenoppretting i tilfelle du oppdager eller mottar et varsel om en trussel mot miljøet ditt ved å sikkerhetskopiere kritiske systemer og aktivere logging. Det anbefales på det sterkeste at du etablerer en hendelsesresponsplan.

Koblinger til mer informasjon

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

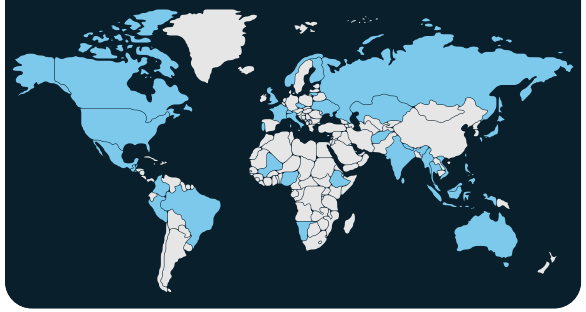
Kina utvider global målretting for å oppnå konkurransemessige fordeler

I dagens komplekse geopolitiske klima gjennomfører statlige aktører i Kina og tilknyttede trusselaktører ofte cyberoperasjoner for å fremme landets strategiske mål for militæret, økonomien og utenlandske relasjoner som en del av Kinas mål om å oppnå konkurransefortrinn. I det siste året har Microsoft observert utbredt kinesisk trusselaktivitet rettet mot land over hele verden.

Siden midten av 2021 har Kina manøvrert for å sikre økonomisk og finansiell stabilitet i den verste COVID-19-bølgen på to år.[13] Kina fortsatte å sjonglere sin posisjon på geopolitiske hendelser, for eksempel kampen for å balansere sitt «grenseløse» partnerskap med Russland,[14] og opprettholde sin posisjon på verdensscenen.[15] I tillegg fortsatte Kinas holdning mot USA og dets allierte overfor Taiwan[16] og Sør-Kina-havet å belaste relasjonene med mange land.[17]

Statlige aktører i Kina og tilknyttede trusselgrupper økte målrettingen mot mindre nasjoner over hele verden med fokus på Sørøst-Asia for å få konkurransefortrinn på alle fronter.

Land målrettet av statlige aktører i Kina og tilknyttede grupper

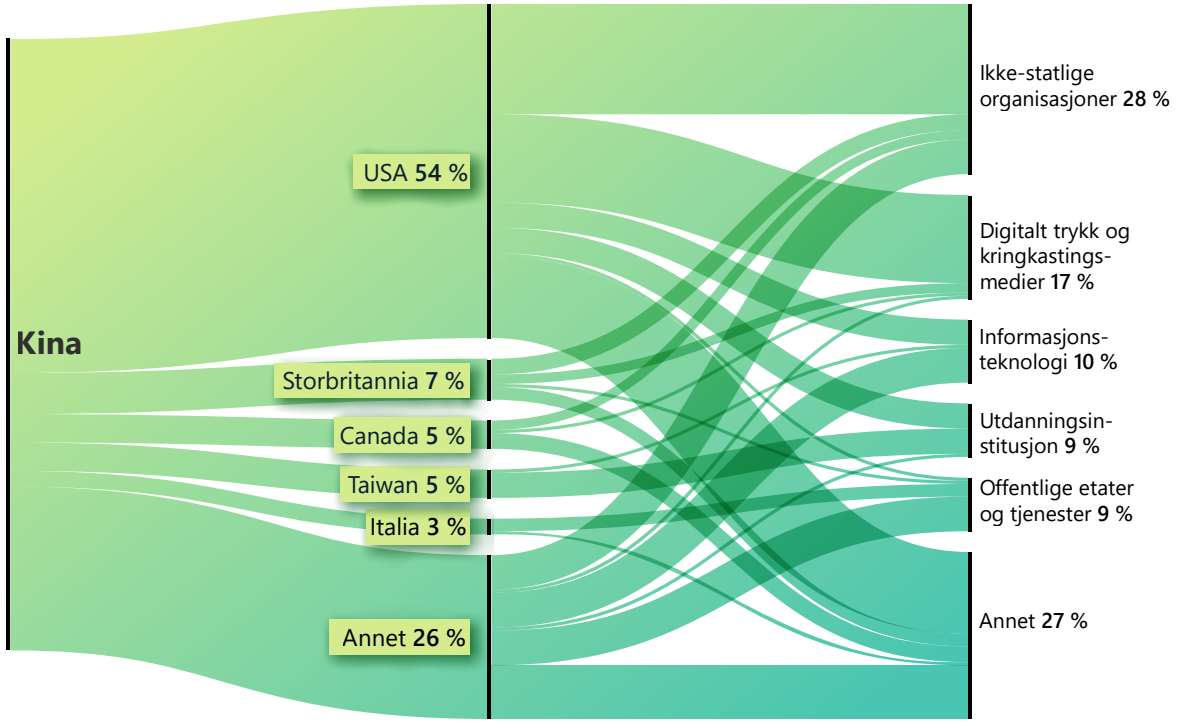


Kina fortsatte også å utvide sin økonomiske innflytelse globalt gjennom tidligere etablerte Belt and Road Initiatives (BRI), som forsøkte å gjenopplive et omfattende investeringsrammeverk med EU,[18] og forhandle frem en ny regional handelsavtale med 15 land i Det fjerne Østen, kjent som det regionale omfattende økonomiske partnerskapet.[19] Microsoft vurderer at Kina vil fortsette å bruke innsamling på nettet som et verktøy for å fremme sine strategiske politiske, militære og økonomiske mål, grunnet observerte nettoperasjoner og bredden av enheter som er målrettet.

Målretting på nettet som sannsynligvis fremmer økonomiske og militære interesser.

Microsoft har observert utstrakt målretting mot mindre nasjoner rundt om i verden av statlige aktører i Kina og tilknyttede trusselgrupper, noe som antyder at Kina sannsynligvis bruker cyberspionasje som en del av sin globale økonomiske og militære innflytelse.

Kina: topp målrettede land og bransjesektorer



Tankesmier / frivillige organisasjoner, medier, IT, myndigheter og utdanningssektoren var blant de mest målrettede sektorene for trusselgrupper basert i Kina, sannsynligvis for vedvarende innsamling av etterretning og rekognosering.

Spennvidden av mål omfattet, men var ikke begrenset til, land i Afrika, Karibia, Midtøsten, Oseania og Sør-Asia, med spesielt fokus på land i Sørøst-Asia og Stillehavsøyene.

I tråd med Kinas BRI-strategi målrettet trusselgrupper basert i Kina mot enheter i Afghanistan, Kasakhstan, Mauritius, Namibia og Trinidad og Tobago.[20] Trinidad og Tobago var for eksempel det første karibiske landet som anbefalte Kinas BRI-strategi i 2018, og Kina anser landet som en viktig partner i regionen. NICKEL har hatt vedvarende nettverksoperasjoner rettet mot Trinidad og Tobago siden 2021. I mars 2022 gjennomførte NICKEL for eksempel rekognoseringsaktiviteter rettet mot en offentlig etat, sannsynlig for innsamling av etterretning.

Kina utvider global målretting for å oppnå konkurransemessige fordeler

Fortsettelse

I mellomtiden observerte Microsoft statlige aktører i Kina og tilknyttede trusselgrupper som fokuserte sine nettverksoperasjoner mot enheter i Sørøst-Asia og ekspanderte til Stillehavsøyene, etter hvert som Kina skiftet sine militære og økonomiske prioriteringer for å takle utfordringene med USAs fornyede interesse i regionen. I januar 2022 observerte Microsoft at RADIUM målrettet mot et energiselskap og en offentlig etat tilknyttet energi i Vietnam, og en offentlig etat i Indonesia. RADIUMs aktiviteter vil trolig samsvare med Kinas strategiske mål i Sør-Kinahavet.[21] Sent i februar og tidlig i mars kompromitterte GALLIUM over 100 kontoer tilknyttet en fremtredende, mellomstatlig offentlig organisasjon i Sørøst-Asia. Tidspunktet for GALLIUMs målretting av IGO i regionen sammenfalt med kunngjøringen av et planlagt møte mellom USA og regionale ledere. GALLIUM-aktører hadde sannsynligvis til oppgave å overvåke kommunikasjon og samle inn etterretning før hendelsen.

Etter hvert som Kina utvidet sin innflytelse på Stillehavsøyene, ble aktivitetene til kinesiske trusselgrupper fulgt. I april signerte Kina og Salomonøyene en sikkerhetsavtale som var ment å «fremme fred og sikkerhet». Avtalen gjør potensielt at Kina kan deployere væpnet politi og militære på Salomonøyene.[22] I mai var Kina vert for det andre møtet mellom utenriksministere i Kina og Stillehavsøyene på Fiji og foreslo å inngå et «omfattende strategisk partnerskap» for å fremme politiske, kulturelle, sosiale og sikkerhetsmessige interesser, fokus på klimaendringer og også bekjemping av pandemien.[23] Omtrent på samme tid i mai identifiserte Microsoft GADCYIUMs ondsinnede programvare på systemene til regjeringen på Salomonøyene. RADIUM kjørte også ondsinnet kode på systemer i et telekommunikasjonsselskap i Papua New Guinea. Vi vurderer at disse aktivitetene sannsynligvis var for innsamling av etterretning for å understøtte Kinas generelle regionale strategi.

Microsoft forstyrrer operasjoner hos NICKEL, men trusselgruppen viser at den vedvarer.

I desember 2021 leverte Microsoft Digital Crimes Unit (DCU) innlegg hos US District Court for the Eastern District of Virginia, der de søkte om myndighet til å beslaglegge 42 kommando- og kontrolldomener (C2) kontrollert av NICKEL. Disse C2-domenene har blitt brukt i operasjoner mot regjeringer, diplomatiske enheter og frivillige organisasjoner i Mellom-Amerika, Sør-Amerika, Karibien, Europa og Nord-Amerika siden september 2019.[24] Gjennom disse operasjonene oppnådde NICKEL langsiktig tilgang til flere enheter og kunne konsekvent eksfiltrere data fra ofre siden slutten av 2019.

Etter hvert som Kina fortsetter å etablere bilaterale økonomiske relasjoner med flere land – ofte i avtaler knyttet til BRI – vil Kinas globale innflytelse fortsette å vokse. Vi vurderer at statlige aktører i Kina og tilknyttede trusselaktører vil forfølge mål i sektorer som myndigheter, diplomati og ikke-statlige organisasjoner for å få ny innsikt, sannsynligvis i form av økonomisk spionasje eller tradisjonelle mål for etterretningsinnsamling. Siden forstyrrelsen fra Microsoft har NICKEL målrettet mot flere offentlige etater, og de forsøker sannsynligvis å vinne tilbake tapt tilgang. Mellom slutten av mars og mai 2022 kompromitterte NICKEL minst fem offentlige etater over hele verden på nytt. Dette tyder på at gruppen hadde flere inngangspunkter til disse enhetene eller fikk tilgang via nye C2-domener. NICKELs persistens ved at de gjentatte ganger kompromitterer de samme offentlige etatene globalt, indikerer viktigheten av oppgaven på et høyt nivå.

Kina er mer selvsikre med sin holdning til utenrikspolitikk. Vi vurderer at økonomisk spionasje aktivert på nettet og innsamling av etterretning sannsynligvis vil fortsette.

Handlingsrettet innsikt

1. Øk cyberforsvaret for å redusere trusler på nettet proaktivt. Persistensen til kinesiske trusselaktører krever at organisasjoner identifiserer, beskytter, oppdager og reagerer på mulig inntrenging i tide.
2. Trusselaktører misbruker planlagte oppgaver[25] som en vanlig metode for persistens og unnvikelse av forsvaret. Sørg for at miljøet ditt bruker flere sikkerhetsretningslinjer for å beskytte mot denne ofte brukte teknikken.[26]
3. Vi fortsetter å observere bruk av webskall som en innledende vektor i målrettede nettverk.[27] Organisasjoner bør herde systemene sine mot webskallangrep som kan gi angripere tilgang til å kjøre eksterne kommandoer.[28]

Koblinger til mer informasjon

- NICKEL målretter seg mot offentlige organisasjoner over hele Latin-Amerika og Europa | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Beskytt folk mot nylige nettangrep | Microsoft On the Issues

Iran blir stadig mer aggressive etter maktovertagelse

Microsoft har observert at statlige grupper i Iran og tilknyttede aktører øker tempoet og omfanget av cyberangrep mot Israel, utvider angrep fra løsepengevirus utover regionale fiender til ofre i USA og EU og målretter seg mot høyprofilert kritisk infrastruktur i USA for å i det minste posisjonere seg for potensielle destruktive cyberangrep.

Den voksende aggresjonen på nettet fra statlige aktører i Iran har fulgt en overgang av presidentmakten. Sommeren 2021 erstattet den totalitære presidenten Ibrahim Raisi den moderate presidenten Hassan Rouhani. I skarp kontrast til Raisi, som er en protégé av den ypperste lederen og en nær alliert av Islamic Revolutionary Guard Corps (IRGC), brakte tidligere president Rouhanis tilbøyelighet til diplomati ham ofte på kant med den ypperste lederen og topplederne i IRGC.[29] De haukiske synspunktene til Raisi-administrasjonen ser ut til å ha økt villigheten til iranske aktører til å iverksette dristige handlinger mot Israel og Vesten, spesielt USA, til tross for gjenopptakelsen av diplomatisk engasjement for å gjenopplive atomavtalen med Iran.

Økt tempo og omfang av iranske cyberangrep mot Israel

Innen uker etter at Raisi hadde satt sammen utenriksteamet sitt,[30] gjenopptok statlige aktører i Iran destruktive cyberangrep mot Israel i et raskere tempo enn året før. Disse løsepengevirusangrepene og hacking-og-lekkasje-angrepene ble gjennomført med bare noen ukers mellomrom fra september og involverte minst tre aktører knyttet til Iran, noe som antyder at angrepene kan ha vært en del av en landsdekkende kampanje for gjengjeldelse mot Israel. I minst ett tilfelle vurderte Microsoft at et løsepengevirusangrep mot en israelsk organisasjon sent i 2021 var ment å skjule et underliggende dataslettingsangrep. Microsofts analyse av ondsinnet programvare fant ut at løsepengeviruset som ble levert til offeret, var programmert til å kjøre ondsinnet slettingsprogramvare etter kryptering.

I 2022 eskalerte iranske cyberangrep i målvalg og angrepsform. I februar forsøkte DEV-0198 å gjennomføre et destruktivt angrep mot kritisk infrastruktur i Israel. Microsoft vurderer også at en aktør tilknyttet Iran sannsynligvis var ansvarlig for et sofistikert cyberangrep som satte ut nødrakettsirener i Israel i juni, trolig ved å bruke programvare som justerer lyd over IP-nettverk.

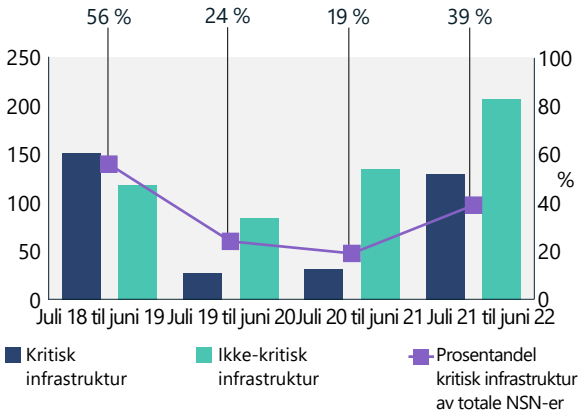
Iransk trussel mot kritisk infrastruktur i USA og Israel gjennom hele året

Microsoft vurderer at statlige aktører i Iran er tilknyttet IRGC (PHOSPHORUS og DEV-0198), målrettet mot høyprofilert kritisk infrastruktur i USA og Israel fra slutten av 2021 til midten av 2022. Det sannsynlige målet var å gi Teheran alternativer for gjengjeldelse mot de samme sektorene som overordnede IRGC-tjenestemenn beskyldte USA og Israel for å ha forstyrret i Iran.[31] Vi vurderer at denne aktiviteten er knyttet til påstander sent i oktober 2021 av IRGC-general Gholamreza Jalali, leder av Irans passive forsvarsorganisasjon, som gjenspeilte anklager fra andre innflytelsesrike personer i regimet om at USA og Israel gjennomførte cyberangrep på Irans havner, jernbaner og drivstoffstasjoner.[32] Jalali fremsatte denne anklagen for andre gang i forberedte bemerkninger i en tale under fredagsbønnen på et podium med et bilde av en rakett som treffer et mål, med ordet «USA», noe som antyder at de overordnede tjenestemennene hadde samme syn.[33]

PHOSPHORUS begynte omfattende skanning av amerikanske organisasjoner i oktober 2021 for ikke-oppdaterte Fortinet- og ProxyShell-sårbarheter. Når disse ikke-oppdaterte systemene først var kompromittert, ble de brukt til å gjennomføre løsepengevirusangrep, i flere tilfeller mot kritisk infrastruktur i USA og andre vestlige nasjoner. Disse markerte de første bekreftede tilfellene av løsepengevirusangrep fra angripere knyttet til Iran utenfor Midtøsten. Etter cyberangrepet mot bensinstasjonene i Iran i slutten av oktober observerte Microsoft en topp i iranske løsepengevirusangrep mot amerikanske selskaper, noe som tyder på en mulig sammenheng.

Samtidig beveget PHOSPHORUS seg mot dirigert målretting, ofte via målrettet phishing, av høyt profilerte kritiske infrastrukturselskaper i USA, inkludert store havner og lufthavner, transportsystemer, kraftselskaper og olje- og gasselskaper. Denne målrettingen, som ofte gjennomføres via målrettet phishing, varte til midten av 2022. Målene innrettet seg direkte etter sektorene Teheran har beskyldt USA og Israel for å ha angrepet i Iran, og vil trolig gi Iran alternativer for gjengjeldelse. Kompromitteringen av nær identiske mål ville gi en mulighet til å avskrekke slike fremtidige angrep, samtidig som de søker å unngå eskalering ved å signalisere årsaken til angrep uten å innrømme skyld.

Gjenoppbygging av iransk infrastrukturmålretting



Den iranske målrettingen mot kritisk infrastruktur økte til de høyeste nivåene som er observert siden slutten av 2018 til tidlig i 2019. Vi brukte US Presidential Policy Directive 21 (PPD-21) for å avgjøre om et selskap passer til kriteriene for kritisk infrastruktur. (Juli 2021 – juni 2022).

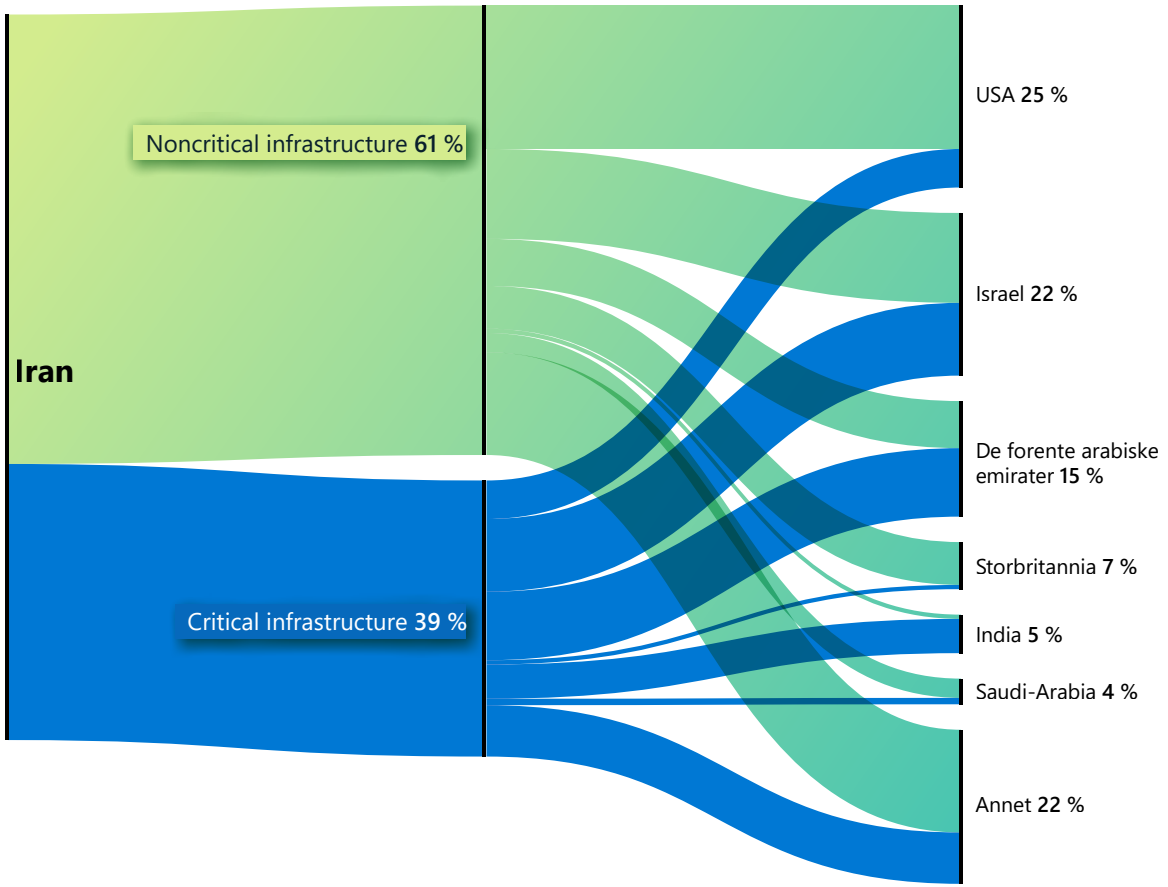
Iran blir stadig mer aggressive etter maktovertagelse

Fortsettelse

I Israel målrettet DEV-0198 mot israelske jernbaner, logistikkselskaper, programvare-leverandører til logistikkselskaper og drivstoffselskaper, med fokus på bensinstasjoner. Tidlig i 2022 gjennomførte gruppen et alvorlig angrep på nettverket til et stort israelsk logistikkselskap, noe som tvang selskapet til å stenge ned datamaskinene og noen av operasjonene for å holde angrepet i sjakk. I et annet tilfelle observerte vi at gruppen forsøkte å få tilgang til nettverket til en stor israelsk transportleverandør via stjålet eller gjenbrukt legitimasjon. I mellomtiden er det mye som tyder på at en annen iransk aktør, DEV-0343 – hvis målretting av selskaper innen forsvar, sjøfart og satellittbilder, har koblinger til IRGC – kompromitterte kontoer hos israelske transport- og havnerelaterte enheter i begynnelsen av 2021.

Det er sannsynlig at iranske trusselgrupper vil forbli en trussel mot amerikanske og israelske transport- og energiselskaper, spesielt fordi den diplomatiske innsatsen for å gjenopplive den iranske atomavtalen vil avta, mens Washington, Tel Aviv og Teheran søker alternative midler for å utnytte konsesjoner.

Iransk målretting mot kritisk infrastruktur per land



Den iranske målrettingen av kritisk infrastruktur var mest fremtredende mot organisasjoner i Israel, Emiratene og USA.

Iranske aktører vil trolig forbli en trussel mot amerikanske og israelske transport- og energiselskaper i løpet av det neste året.

Iranske grupper har utvidet løsepenge-virusangrep utover regionale motstandere og sikter seg inn på høyprofilerte amerikanske og israelske kritiske infrastrukturmål.

Handlingsrettet innsikt

1. Forbedre organisasjonens generelle netthygiene ved å aktivere passordløse løsninger, for eksempel flerfaktor-autentisering, og håndhev bruken av dette for all ekstern tilkobling for å redusere potensielt kompromittert legitimasjon.
2. Evaluer autentisiteten til all innkommende e-posttrafikk for å sikre at avsenderadressen er legitim.
3. Oppdater tidlig og ofte.[34]
4. Se gjennom og revider hver av partner-forholdene med tjenesteleverandører for å minimere unødvendige tillatelser mellom organisasjonen din og leverandører oppstrøms. Microsoft anbefaler umiddelbar fjerning av tilgangen for eventuelle partnerrelasjoner som ser ukjente ut, eller som ennå ikke er revidert.[35]

Koblinger til mer informasjon

- Iransk målretting mot IT-sektoren på vei opp | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- DEV-0343, knyttet til Iran, målretter mot forsvarssektoren, GIS og maritim sektor | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Libanon-basert gruppe med koblinger til Iran som målretter mot Israel

Microsoft overvåker cybertrusselaktiviteter uavhengig av plattform, målrettede ofre eller geografiske områder. Vi opprettholder synlighet og aktiv trusseljakt over hele verden for å skrive bedre gjenkjenninger for kundene våre.

Selv om trusler fra Russland, Kina, Iran og Nord-Korea utgjør flertallet av vår observerte statlige aktøraktivitet, sporer vi også og kommuniserer om trusler fra NATO-medlemsland og demokratiske nasjoner. I fjor omtalte vi aktiviteten til en aktør basert i Tyrkia (SILICON) og en aktør basert i Vietnam (BISMUTH). I år har vi flere detaljer om en Libanon-basert gruppe som vi tidligere har avslørt offentlig.[36]

Microsoft avdekket en tidligere udokumentert Libanon-basert gruppe som vi vurderer, med moderat tillit, har operert i koordinering med aktører tilknyttet Irans Ministry of Intelligence and Security (MOIS). Et slikt samarbeid eller en slik retning fra Teheran vil samsvare med avsløringer siden slutten av 2020 om at regjeringen i Iran bruker tredjeparter til å utføre nettoperasjoner, noe som sannsynligvis vil gjøre at Iran kan benekte aktiviteten med økt troverdighet.

I den observerte aktiviteten målrettet eller kompromitterte POLONIUM to dusin organisasjoner basert i Israel og én IGO med operasjoner i Libanon mellom februar og mai 2022, før Microsoft forstyrret og avslørte aktiviteten offentlig. Nesten halvparten av de israelske organisasjonene var en del av Israels forsvarsindustri eller hadde koblinger til israelske forsvarsselskaper, noe som indikerer at gruppen har hatt samme type interesse som Iran for å samle inn etterretning om og/eller direkte arbeide mot Israel.[37]

POLONIUMs vurderte koblinger til MOIS-grupper er basert på observerte overlappinger av ofre og felles verktøy og teknikker.

- Overlapping av ofre: En statlig gruppe i Iran knyttet til Irans MOIS, som Microsoft sporer som MERCURY, kompromittert tidligere flere ofre av POLONIUM, noe som indikerer et sammenfall av oppdragskrav eller en mulig «overlevering» av ofrene mellom grupper.
- Felles verktøy og teknikker: I likhet med POLONIUM observerte MSTIC at DEV-0588 (også kjent som CopyKittens) ofte bruker AirVPN for operasjoner, og DEV-0133 (også kjent som Lyceum[38]) bruker OneDrive for C2 og eksfiltrasjon. I likhet med statlige aktører i Iran brukte POLONIUM en skytjenesteleverandør til å kompromittere et israelsk luftfartsselskap og advokatfirma.[39]

POLONIUM distribuerte en rekke tilpassede implantater ved hjelp av skytjenester for C2 og dataeksfiltrasjon – spesielt OneDrive og DropBox. POLONIUM opprettet ofte unike OneDrive-apper for mål, sannsynligvis for å unngå deteksjon.

Per juni 2022 suspenderte Microsoft over 20 OneDrive-apper opprettet av POLONIUM, varslet berørte organisasjoner og distribuerte en rekke oppdateringer av sikkerhetsetterretning for å sette verktøy utviklet av POLONIUM i karantene.

Microsoft oppdaget og deaktiverte POLONIUMs misbruk av OneDrive som C2.

Handlingsrettet innsikt

1. Oppdater antivirusverktøy[40] og sørg for at skybeskyttelse[41] er aktivert for å oppdage relaterte indikatorer.
2. For kunder med relasjoner til tjenesteleverandører må du sørge for gjennomgang og revisjon av alle partnerrelasjoner for å minimere unødvendige tillatelser mellom organisasjonen og leverandører oppstrøms.[42] Fjern tilgang umiddelbart for alle partnerrelasjoner som virker ukjente, eller som ikke har vært revidert.

Koblinger til mer informasjon

- Eksponering av POLONIUM-aktivitet og infrastruktur målrettet mot israelske organisasjoner | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY utnytter Log4j 2-sårbarheter i systemer som ikke er oppdatert, for å målrette mot israelske organisasjoner | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Nordkoreanske nettegenskaper utnyttes for å oppnå de tre hovedmålene til regimet

Nord-Koreas cyberprioriteringer det siste året reflekterte regjeringens oppgitte globale prioriteringer. Kim Jong Un understreket de tre prioriteringene ved å bygge opp forsvarskapasitet, styrke landets vaklende økonomi og sikre innenlandsk stabilitet på flere viktige områder.[43] Handlingene som utføres av statlige aktører i Nord-Korea, viser tydelig at nettet brukes til å nå disse tre målene.

Statlige aktører i Nord-Korea brukte en rekke taktikker for å forsøke å trenge inn i luftfartsselskaper over hele verden.

Statlige trusselgrupper i Nord-Korea, primært CERIUM og ZINC, brukte en rekke taktikker for å forsøke å trenge inn i nettverk hos forsvars- og luftfartsselskaper over hele verden. Da Nord-Korea gikk inn i sin mest aggressive periode med testing av raketter i første halvdel av 2022, brukte de cyberspionasje for å hjelpe nordkoreanske forskere med å få et fortrinn i utviklingen av egenutviklede forsvarssystemer og mottiltak for fremskrittene som fiendene gjorde.

Vi observerte at COPERNICIUM målrettet mot en rekke kryptovalutarelaterte selskaper over hele verden, ofte med suksess, for å bidra til å understøtte Nord-Koreas svake økonomi. Selv om vi ikke kan bekrefte om gruppen var i stand til å eksfiltrere penger etter en kompromittering, observerte vi at COPERNICIUM infiserer dusinvis av maskiner ved å sende ondsinnede dokumenter maskerte som forslag fra andre kryptovalutaselskaper.

Til slutt jobbet en gruppe som Microsoft sporer som DEV-0215, med å opprettholde stabilitet og lojalitet i Nord-Korea ved å målrette mot nyhetsorganisasjoner som rapporterer om nordkoreanske saker. Disse kanalene har kilder både i Nord-Korea og innenfor fellesskap av avhoppere, som Pyongyang ser på som en eksistensiell trussel. I tillegg jobbet gruppen for å få tilgang til nettverk av kristne grupper som snakker koreansk, som har en tendens til å uttale seg fritt mot Nord-Korea og arbeide aktivt med nordkoreanske avhoppere.

Målretting mot forsvars- og luftfartsselskaper

Statlige aktører i Nord-Korea, ledet av CERIUM og ZINC, har lagt ned betydelig innsats i å utvikle taktikker rettet mot inntrenging av forsvars- og luftfartsselskaper. CERIUM undersøkte gjentatte ganger virtuelle private nettverk (VPN-er) i Sør-Korea ved å laste ned klienter og se etter svakheter. De lastet også ned vanlige apper som brukes av militæret og offentlige klienter i Sør-Korea, sannsynligvis på jakt etter sårbarheter. Gruppen fulgte nøye med på aktuelle hendelser og skrev nye lokkedokumenter som brukte høyprofilerte emner som agn for å oppmuntre mål til å klikke på kjørbare filer og koblinger til ondsinnet programvare.

Både ZINC og CERIUM brukte sosiale medier og sosial manipulering i kampanjer. ZINC var spesielt gode til å opprette falske profiler på LinkedIn og andre profesjonelle nettsteder for sosiale medier, der operatørene fremstod som rekrutterere for store forsvars- og luftfartsselskaper. Ved hjelp av disse profilene sendte de koblinger eller ondsinnede filvedlegg til potensielle ofre ved hjelp av direktemeldinger på sosiale medier eller e-post.

I tillegg til ansatte i selskaper målrettet CERIUM også bredt mot medlemmer i det sørkoreanske militæret, med spesiell interesse for både sørkoreanske militære akademier og militære medlemmer som arbeider i akademiene.

Målretting mot kryptovaluta for å balansere tap

Siden FN-sanksjonene ble skjerpet i 2016, har Nord-Koreas økonomi fortsatt å krympe, forsterket av naturkatastrofer, blant annet oversvømmelser[44] og tørke[45], i tillegg til en nær sagt total stengning av grensene for importeringer siden starten av COVID-19-pandemien tidlig i 2020.[46] Selv om Nord-Korea åpnet grensene for handel med Kina i en kort periode tidlig i 2022, ble de snart stengt igjen.[47] I midten av mai rapporterte Nord-Korea om sitt første innenlandske tilfelle av COVID-19.[48] Landet har siden innført en «null COVID»-strategi, lik Kinas strategi, med massenedstengninger for å bekjempe viruset,m noe som har virket negativt inn på Nord-Koreas allerede skjøre økonomi.

Den statlige nordkoreanske gruppen COPERNICIUM prøvde å kompensere for litt av de tapte inntektene ved å stjele penger – vanligvis i form av kryptovaluta – fra alle selskaper der de kunne trenge inn i nettverket. Vi har sett dusinvis av maskiner som har blitt kompromittert, som tilhører selskaper relatert til kryptovaluta i USA, Canada, Europa og i hele Asia. COPERNICIUM har til og med kompromittert maskiner som tilhører selskaper relatert til kryptovaluta i Nord-Koreas nærmeste allierte, Kina, både i selve Kina og i Hongkong. Gruppen har basert seg tungt på sosiale medier for tidlig rekognosering og tilnærminger til mål. Aktører bygger profiler som utgir seg for å være utviklere eller toppsjefer i bedrifter knyttet til kryptovaluta. De etablerte deretter relasjoner med personer i bransjen ved å sende ondsinnede koblinger eller filer når de hadde nok informasjon.

Nordkoreanske nettegenskaper utnyttes for å oppnå de tre hovedmålene til regimet

Fortsettelse

En gruppe relatert til PLUTONIUM utvikler og distribuerer løsepengevirus

En gruppe aktører som kommer fra Nord-Korea, som Microsoft sporer som DEV-0530, begynte å utvikle og bruke løsepengevirus i angrep i juni 2021. Denne gruppen, som kalte seg selv for H0lyGh0st, benyttet en nyttelast for løsepengevirus med samme navn for kampanjene sine og kompromitterte småbedrifter i flere land så tidlig som i september 2021.

Microsoft vurderte at DEV-0530 hadde forbindelser med en annen gruppe basert i Nord-Korea, sporet som PLUTONIUM (også kjent som DarkSeoul eller Andariel). Mens bruken av H0lyGh0st-løsepengevirus i kampanjer er unik for DEV-0530, observerte MSTIC kommunikasjon mellom de to gruppene, samt DEV-0530, ved hjelp av verktøy opprettet utelukkende av PLUTONIUM.

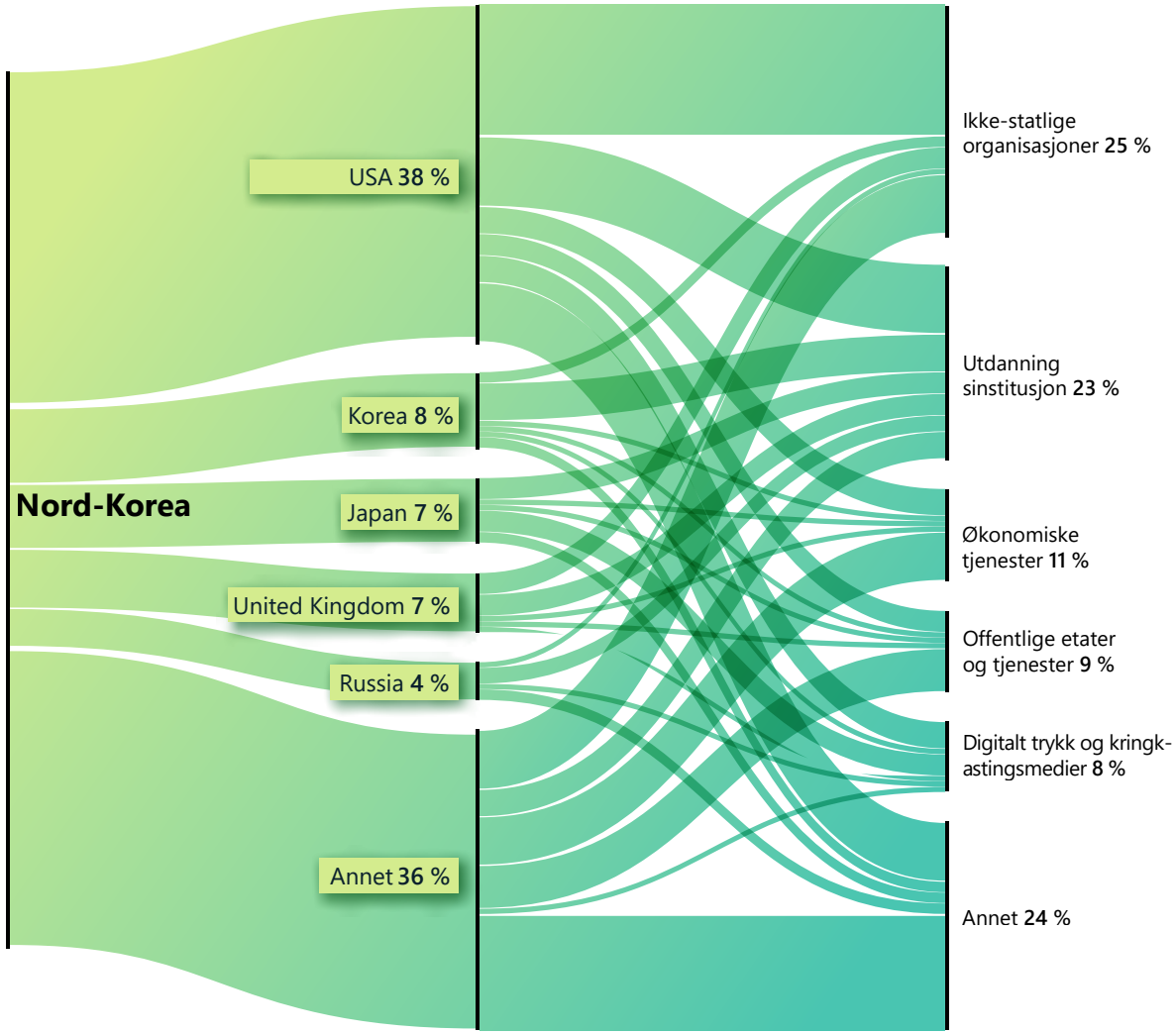
Det er ikke sikkert at aktiviteten til DEV-0530 var statlig sponset. Selv om løsepengevirusangrep kunne ha blitt bestilt av myndighetene av samme grunn som de sponser tyveri fra kryptovalutaselskaper, er det også mulig at aktørene bak DEV-0530 handlet uavhengig for å tjene penger for seg selv. Hvis det var nordkoreanske hackere som opererte uavhengig, ville det forklart hvorfor aktiviteten ikke var utbredt sammenlignet med statlig sponsede tyverioperasjoner mot kryptovalutaselskaper.

Målretting mot nordkoreanske aviskiosker, avhoppere, religiøse grupper og hjelpeorganisasjoner

I løpet av det siste året har den øverste lederen, Kim Jong Un, offentlig vært mer fokusert på intern sikkerhet og lojalitet enn på raketter og atomvåpen. Minst to statlige grupper i Nord-Korea fokuserte på aspekter som regimet ville sett på som innenlandske trusler, for å gjenspeile dette.

Den første var en gruppe som Microsoft sporer som DEV-0215, som sikter seg inn på medieorganisasjoner som følger nordkoreanske nyheter tett. En sannsynlig grunn til denne målrettingen er at disse mediene får nyheter fra nordkoreanske avhoppere, kinesiske borgere som jobber tett med Nord-Korea, og til og med enkelte nordkoreanske innbyggere som er basert i landet, som bruker en rekke metoder for å kommunisere med omverdenen. Den nordkoreanske regjeringen ser på disse gruppene som en eksistensiell trussel mot statens overlevelse, og spesielt innbyggere i Nord-Korea vil bli sett på som forrædere og spioner. DEV-0215 forsøkte sannsynligvis å identifisere kildene til disse utsalgsstedene, slik at de kunne nøytralisere potensielle informasjonslekkasjer.

Nord-Korea: Topp målrettede land og bransjesektorer



Nord-Korea ser på USA, Sør-Korea og Japan som sine hovedfiender. Selv om Russland har vært en alliert i lang tid, sikter nordkoreanske trusselaktører seg mot russiske tankesmier, akademikere og diplomatiske tjenestemenn for å innhente etterretning om russiske synspunkter om globale anliggender.

Nordkoreanske nettegenskaper utnyttes for å oppnå de tre hovedmålene til regimet

Fortsettelse

Microsoft også bevis på at DEV-0215 målrettet mot koreansktalende kristelige samfunn. Evangelisk-kristne kirker i Sør-Korea har en tendens til å være kritiske både mot de nordkoreanske og sørkoreanske regjeringene, som favoriserer engasjement med Nord-Korea. Disse menighetene vil sannsynligvis oppsøke avhoppere, og enkelte engasjerer seg i humanitært arbeid med Nord-Korea. Nord-Korea ser på dem som en trussel fordi, selv om strømmen av avhoppere fra Nord-Korea nesten tørket opp under pandemien,[49] spiller disse kristne gruppene ofte en avgjørende rolle i å hjelpe avhoppere med å slippe unna. DEV-0215 har generert falske dokumenter om kristne konferanser for koreanske foredragsholdere som lokkemiddel for å målrette mot gruppen og oppdage hvem som bidrar til å organisere avhoppere.

Til slutt viste den statlige gruppen OSMIUM stabil interesse for internasjonale hjelpeorganisasjoner gjennom hele året, inkludert organisasjoner som har hjulpet Nord-Korea tidligere. Mens Nord-Korea generelt bryskt har avslått tilbud om hjelp fra utlandet, spesielt etter utbruddet av COVID-19,[50] er det mulig at Nord-Korea vurderer å si ja til tilbud om hjelp, men de er skeptiske til sikkerhetskonsekvensene av å tillate utenlandske hjelpearbeidere adgang til landet. Nord-Korea kan trenge inn i nettverkene til hjelpeorganisasjoner over hele verden for å avgjøre om slik hjelp skal tillates inn i eget land.

Handlingsrettet innsikt

1. Statlige aktører i Nord-Korea er dyktige, standhaftige og kreative, men organisasjoner kan forsvare seg mot dem.
2. De fleste vellykkede angrep kan stoppes med grunnleggende netthygiene, for eksempel tofaktorautentisering eller ved å ikke åpne vedlegg fra ukjente personer i et virtuelt miljø.

Koblinger til mer informasjon

- Nordkoreanske trusselaktører sikter seg inn på små og mellomstore bedrifter med H0lyGh0st-løsepengevirus | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Blant eksperter på Nord-Korea har det lenge vært debatt om hvorvidt den nordkoreanske regjeringen mener alvor med sine offentlige uttalelser eller om det er skremselspropaganda. Samkjøringen av cyberangrep med Nord-Koreas annonserte prioriteringer sementerer troen på at Nord-Korea mener det de sier, når de uttaler seg offentlig om sine mål.

Leiesoldater truer stabiliteten på nettet

Det er en voksende bransje av private selskaper som utvikler og selger verktøy, teknikker og tjenester som gjør det mulig for kundene, ofte regjeringer, å bryte seg inn i nettverk, datamaskiner, telefoner og Internett-tilkoblede enheter. Disse enhetene er et aktivum for statlige aktører, og de truer ofte dissidenter, forsvarere av menneskerettigheter, journalister, talsmenn for det sivile samfunnet og andre private innbyggere. Vi refererer til disse som leiesoldater på nettet eller offensiv aktører i privat sektor.

En verden der bedrifter i privat sektor skaper og selger nettangrep er farligere for forbrukere, bedrifter av alle størrelser og regjeringer. Disse offensive verktøyene kan brukes på måter som er inkonsekvente med normene og verdiene til god styring og et sunt demokrati. Microsoft mener at beskyttelse av menneskerettigheter er en grunnleggende forpliktelse, og vi tar dette på alvor ved å begrense «overvåking som en tjeneste» over hele verden.

Microsoft har vurdert visse statlige aktører både hos demokratiske og autoritære regimer som outsourcer utviklingen eller bruken av teknologi for «overvåking som en tjeneste». Slik unngår de ansvarlighet og tilsyn, i tillegg til at de skaffer seg funksjoner som det er vanskelig å utvikle internt.

> Disse cybervåpnene gir nasjonalstater overvåkingsfunksjoner de ikke ville ha kunnet utvikle alene.

Markedet der leiesoldater på nettet opererer, er ugjennomsiktig. Likevel fortsetter vi å observere disse gruppene ved hjelp av nulldagsutnyttelser og nullklikksutnyttelser som ikke krever samhandling med offeret i det hele tatt, noe som muliggjør overvåking som en tjeneste.

Microsoft kunngjorde nylig en offensiv aktør i europeisk privat sektor som vi kaller KNOTWEED, en PSOA basert i Østerrike, kalt for DSIRF. Flere nyhetsrapporter har knyttet selskapet til utvikling og forsøk på salg av et verktøysett for ondsinnet programvare, kalt for Subzero.[51] Ofrene inkluderer advokatfirmaer, banker og byråer for strategisk konsultasjon i land som Østerrike, Storbritannia og Panama.[52]

Fordi disse offensive overvåkingsfunksjonene ikke lenger er strengt hemmelige funksjoner opprettet av forsvars- og etterretningsbyråer, men i stedet kommersielle produkter som nå tilbys til selskaper og enkeltpersoner, må ethvert regulatorisk regime for cybervåpen gå lengre enn kun eksportkontroll. Virkningen av disse cybervåpnene kan være ødeleggende.

Når en leiesoldat på nettet utnytter en sårbarhet i et produkt eller en tjeneste, setter de hele databehandlingsøkosystemet i fare. Når sårbarheter identifiseres offentlig, er selskaper i et kappløp med tiden for å lansere beskyttelse før omfattende angrep iverksettes (se vår tidligere diskusjon om sårbarhetsut-nyttelser). Dette er en farlig og vanskelig syklus både for programvareleverandører (som må utvikle oppdateringer på en hensiktsmessig måte) og forbrukere av produkter (som må implementere oppdateringene umiddelbart).

Som grunnlegger av Cybersecurity Tech Accord[53] – en ledende allianse som sammenfatter over 150 teknologiselskaper – har Microsoft inngått en forpliktelse om ikke å engasjere seg i offensiv drift på nettet. Vi står ved denne forpliktelsen og ved vårt ansvar for menneskerettigheter på dette området. Vi har engasjert oss i tekniske forstyrrelser og juridiske utfordringer for å fremheve de negative virkningene forårsaket av tjenestene som tilbys av leiesoldater på nettet, og vi vil fortsette å beskytte kundene våre når vi oppdager misbruk.

> Leiesoldater på nettet oppretter og leverer funksjoner for «overvåking som en tjeneste» som er teknologisk sofistikerte og bredt tilgjengelige, inkludert avansert ondsinnet programvare og en rekke teknikker.

Handlingsrettet innsikt for regjeringer

1. Implementer krav til åpenhet og tilsyn for overvåking som en tjeneste, spesielt innen innkjøp, inkludert forbud mot disse offensive aktørene, som USA har gjort med handelsdepartementets liste over selskaper på enhetslisten.
2. Etabler restriksjoner etter ansettelse for tidligere ansatte i denne sektoren.
3. Ha som mål å implementere «kjenn din kunde»-forpliktelser, og oppmuntre bedrifter til å opprettholde sine forpliktelser om menneskerettigheter.

Koblinger til mer informasjon

- Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Fortsettelse av kampen mot cybertrusler i privat sektor | Microsoft On the Issues

Operasjonalisering av nettsikkerhetsnormer for fred og sikkerhet på nettet

Vi trenger et konsistent, globalt rammeverk som prioriterer menneskerettigheter og beskytter mennesker mot hensynsløs statlig atferd på nettet. Ingen steder er dette tydeligere demonstrert enn under den pågående krigen i Ukraina. I tillegg til en global strategisk innsats kan regjeringer handle nå for å få en umiddelbar positiv innvirkning.

For fem år siden oppmuntret Microsoft til en «digital Genève-konvensjon» for å fremme ansvar og forpliktelser på tvers av sektorer for å forsvare fred og sikkerhet på nettet. Nettet dukket opp som et distinkt og flyktig domene med konflikt og konkurranse mellom stater, og angrep ble stadig vanligere, selv i tider med fred.

I dag er det fortsatt et tydelig behov for et slikt rammeverk – dokumentert av russiske cyberangrep mot Ukraina som en del av Russlands invasjon. Denne krigen har skapt en ny frontlinje som er dramatisk forskjellig fra alt vi har kjent før.

Å bringe stabilitet til nettet vil kreve styrking og omdefinering av globale styringsinstitusjoner, slik at de er egnet til formålet. Nettet er fundamentalt forskjellig fra andre domener – det er grenseløst, syntetisk og vedlikeholdes i stor grad av privat industri. Dette betyr at vi må be teknologibransjen om å ta større ansvar både for sikkerheten til produkter og tjenester og det bredere digitale økosystemet. Selv om det har vært merkbar fremgang på alle fronter, har utfordringene vokst dramatisk.

Vi må fordoble den kollektive innsatsen for å forsvare sikkerheten på nettet. Vi kan ikke ta rettighetene og frihetene vi har forventer på nettet, for gitt. Mens vi sliter med å løse utfordringene, planlegger ondsinnede aktører hvordan og hvor de skal slå til neste gang, ved å bruke kunstig intelligens, utnytte desinformasjon og finne måter å undergrave det ferske metaverset. Menneskerettighetsforsvarere, teknologibransjen og regjeringer som respekterer rettigheter, må arbeide sammen mot en overordnet visjon for en trygg og sikker nettverden. Veien fremover er lang, men det er ting regjeringer kan gjøre nå for å umiddelbart forbedre økosystemet for nettsikkerhet:

- Siter normer, lover og konsekvenser i tilskrivelser. En stor forbedring i løpet av de siste fem årene har vært hastigheten og koordineringen av offentlige tilskrivelser av nettangrep. Utover kun å offentliggjøre navn og plassere skyld må disse påstandene fremheve hvilke internasjonale lover eller normer som blir krenket, og hvilke konsekvenser som vil bli pålagt, for å bidra til å styrke anerkjennelse av internasjonale forventninger.
- Klargjør tolkning av internasjonal lov på nettet. Selv om regjeringer er enige om at internasjonal lov gjelder på nettet, gjenstår spørsmål om hvordan den gjelder i bestemte tilfeller. Dette er spesielt relevant i kjølvannet av invasjonen av Ukraina. Regjeringer kan langt på vei definere forventninger, unngå misforståelser og bygge tillit ved å erklære hvordan de forstår sine forpliktelser i henhold til internasjonal lov.
- Rådfør med andre interessenter. Etter hvert som internasjonale fora fortsetter å oppdage de beste måtene for å tilrettelegge for inkludering av robuste interessenter, kan regjeringer støtte informert dialog ved å konsultere med fellesskap med flere interessenter, spesielt teknologibransjen, for å oppnå fordeler via dialog med personer med uunnværlig ekspertise.
- Etabler et stående organ for å støtte ansvarlig atferd fra nasjonalstater på nettet. Arbeidet med internasjonale diplomatiske fora for å fremme ansvarlig statlig atferd på nettet har aldri vært viktigere. Det er et tydelig behov for en permanent FN-mekanisme som kan håndtere nettet som et konfliktområde.
- Definer nye normer for trusler i utvikling. Trusler på nettet er i stadig utvikling sammen med innovasjon innen teknologi. Internasjonale normer bør være teknologinøytrale, men de må oppdateres og utvannes basert på endringer i trussellandskapet og hvordan vi bruker teknologi. Selv i dag ser vi hull i det eksisterende internasjonale rammeverket som misbrukes. Stater bør forplikte seg til å eksplisitt beskytte kjerneprosesser som underbygger det digitale økosystemet som for øyeblikket ikke er beskyttet, for eksempel oppdatering av programvare. I tillegg fortjener bestemte områder ekstra beskyttelse. Som vi for eksempel har lært under pandemien, er normer for beskyttelse av helsetjenester avgjørende.

Statlige aktører og angrep fra disse øker i volum og raffinement, noe som skaper en uholdbar situasjon.

Umiddelbar handling er avgjørende – det er ting regjeringer kan gjøre nå for å umiddelbart forbedre økosystemet for cybersikkerhet, inkludert implementering av vedtatte normer og regler for statlig atferd i cyberområdet, og arbeide med det bredere fellesskapet for interessenter for å håndtere nye mangler.

En må se nytt på multilaterale institusjoner for å håndtere den presserende utfordringen med cyberangrep fra nasjonalstater.

Koblinger til mer informasjon

- Et erkjennelsens øyeblikk: behovet for en sterk og global cybersikkerhetsrespons | Microsoft On the Issues
- Nettangrep rettet mot helsevesenet må stoppe | Microsoft On the Issues
- Det neste kapittelet i cyberdiplomati i FN er like rundt hjørnet | Microsoft On the Issues

Sluttnoter

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 kapittelet er definert av 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

Sluttnoter, fortsettelse

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. Spesielt oppdatering av Exchange-server for ProxyShell-sårbarheter (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 og CVE-2021-27065, CVE-2021-34473). Sørg også for å oppdatere Fortinet FortiOS SSL VPN-apparater for sårbarheter.
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 notert i den tekniske bloggen vår betyr identifisering av mål i et land ikke nødvendigvis at en DSIRF-kunde befinner seg i samme land, ettersom internasjonal målretting er vanlig.
53. Home | Cybersecurity Tech Accord (cybertechaccord.org)

Enheter og infrastruktur

Med stadig raskere digital transformasjon er sikkerheten til digital infrastruktur viktigere enn noensinne.

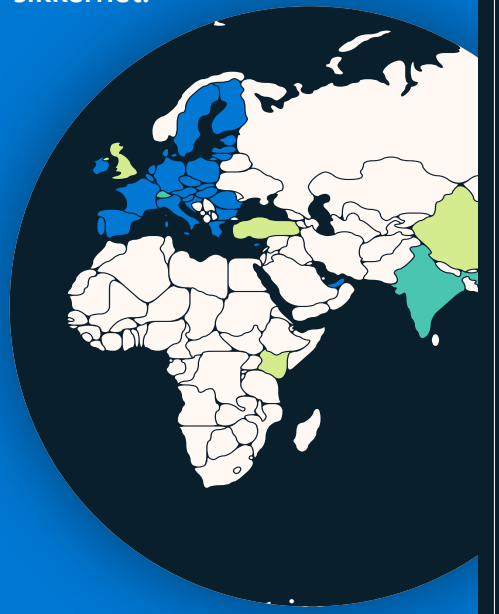
En oversikt over

enheter og infrastruktur

Pandemien, kombinert med rask innføring av alle typer enheter rettet mot Internett som en komponent i den digitale transformasjonen, har i stor grad økt angrepsoverflaten i den digitale verden.

Nettkriminelle og nasjonalstater drar raskt nytte av det. Sikkerheten til IT-maskinvare og -programvare har styrket seg de siste årene, men sikkerheten til IoT-enheter (Internet of Things) og OT-enheter (driftsteknologi) har ikke holdt tritt. Trusselaktører utnytter disse enhetene til å etablere tilgang på nettverk og muliggjøre sideveis bevegelse, for å etablere et fotfeste i en forsyningskjede eller for å forstyrre målorganisasjonens OT-operasjoner.

Regjeringer over hele verden iverksetter tiltak for å beskytte kritisk infrastruktur ved å forbedre IoT- og OT-sikkerhet.

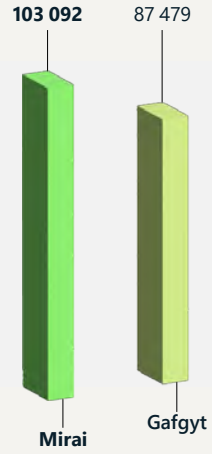


Finn ut mer på side 59

Globalt konsekvente og interoperable sikkerhetsretningslinjer er nødvendig for å sikre bred innføring.

Finn ut mer på side 59

Ondsinnet programvare som en tjeneste har begynt med storskalaoperasjoner mot eksponert IoT og OT i infrastruktur og det offentlige strømnettet samt bedriftsnettverk.



Finn ut mer på side 63

Angrep mot eksterne administrasjonsenheter er på vei opp, og mer enn 100 millioner angrep ble observert i mai 2022 – en femdobbel økning det siste året.

Finn ut mer på side 62

Angripere utnytter i økende grad sårbarheter i fastvaren for IoT-enheter for å infiltrere bedriftsnettverk og iverksette ødeleggende angrep.

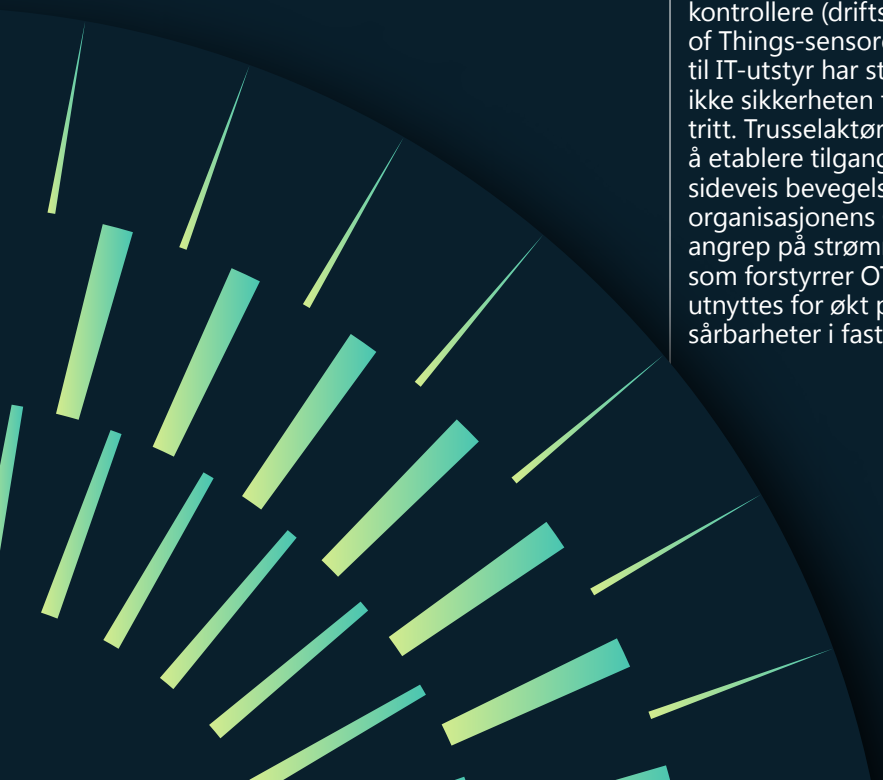
Finn ut mer på side 65

32 % av de analyserte fastvareavbildningene inneholdt minst 10 kjente kritiske sårbarheter.

Finn ut mer på side 66

Innledning

Fremskynding av digital transformasjon har økt nettsikkerhetsrisikoen for kritisk infrastruktur og fysiske nettsystemer.



I løpet av de siste årene har vi sett en enestående endring i den digitale verden. Organisasjoner utvikler seg for å utnytte fremskritt innen databehandlingsfunksjonalitet både fra den intelligente skyen og Intelligent Edge. Som et resultat av pandemien som tvinger enheter til å digitalisere seg for å overleve, og hastigheten som bransjer over hele verden tar i bruk Internett-aktiverte enheter på, øker angrepsoverflaten i den digitale verden eksponentielt.

Denne raske migrasjonen har overskredet sikkerhetsfellesskapets evne til å holde tritt. I løpet av det siste året har vi observert trusler som utnytter enheter i alle deler av en organisasjon, fra tradisjonelt IT-utstyr til OT-kontrollere (driftsteknologi) eller enkle Internet of Things-sensorer (IoT). Selv om sikkerheten til IT-utstyr har styrket seg de siste årene, har ikke sikkerheten til IoT- og OT-enheter holdt tritt. Trusselaktører utnytter disse enhetene til å etablere tilgang på nettverk og muliggjøre sideveis bevegelse eller for å forstyrre organisasjonens OT-operasjoner. Vi har sett angrep på strømnett, løsepengevirusangrep som forstyrrer OT-operasjoner, IoT-rutere som utnyttes for økt persistens, og angrep rettet mot sårbarheter i fastvare.

Selv om utbredelsen av IoT- og OT-sårbarheter er en utfordring for alle organisasjoner, er det økt risiko for kritisk infrastruktur fordi trusselaktører har lært at å ta ut kritiske tjenester er et kraftig middel. Løsepengevirusangrepet mot Colonial Pipeline Company i 2021 demonstrerte hvordan kriminelle kan forstyrre en kritisk tjeneste for å øke sannsynligheten for løsepengebetaling. Og Russlands cyberangrep mot Ukraina viser at enkelte nasjonalstater ser på cyberangrep mot kritisk infrastruktur som akseptabel sabotasje for å oppnå sine militære mål.

Det er imidlertid håp i sikte. Politikere og nettverksforsvarere agerer for å forbedre cybersikkerheten til kritisk infrastruktur, inkludert IoT- og OT-enhetene de er avhengige av. Politikerne fremskynder utviklingen av lover og forskrifter for å bygge offentlig tillit til cybersikkerheten til kritisk infrastruktur og enheter.

Microsoft samarbeider med regjeringer over hele verden for å gripe denne muligheten til å forbedre nettsikkerheten, og vi ønsker ekstra engasjement velkommen. Vi er imidlertid bekymret for at inkonsekvente, skreddersydde eller komplekse krav kan ha utilsiktede effekter, inkludert reduksjon av sikkerheten i enkelte tilfeller, ved å avlede knappe sikkerhetsressurser mot samsvar med flere dupliserte sertifiseringer.

Fra et sikkerhetsoperasjonsståsted bruker nettverksforsvarere flere tilnærminger til å forbedre organisasjonens holdning til IoT-/OT-sikkerhet. Én tilnærming er å implementere kontinuerlig overvåking av IoT- og OT-enheter. En annen er «shift-left» – noe som betyr å kreve og implementere bedre nettsikkerhetspraksis for selve IoT- og OT-enhetene. En tredje tilnærming er å implementere en sikkerhetsovervåkingsløsning som spenner over både IT- og OT-nettverk. Denne helhetlige tilnærmingen har en betydelig ekstra fordel, nemlig å bidra til kritiske organisatoriske prosesser, for eksempel «bryte ned siloene» mellom OT og IT, som i sin tur gjør det mulig for organisasjonen å oppnå en forbedret sikkerhetsholdning mens forretningsmålene oppfylles.

Michal Braverman, Blumenstyk
Viseadministrerende direktør, teknologisjef, sky- og KI-sikkerhet

Myndigheter tar grep for å forbedre sikkerhet og robusthet for kritisk infrastruktur

Myndigheter over hele verden utvikler retningslinjer for å håndtere kritisk cybersikkerhetsrisiko for infrastrukturen. Mange innfører også retningslinjer for å forbedre sikkerheten for IoT- og OT-enheter. Den økende globale bølgen av politiske initiativer skaper enorme muligheter til å forbedre nettsikkerheten, men utgjør også utfordringer for interessenter i hele økosystemet.

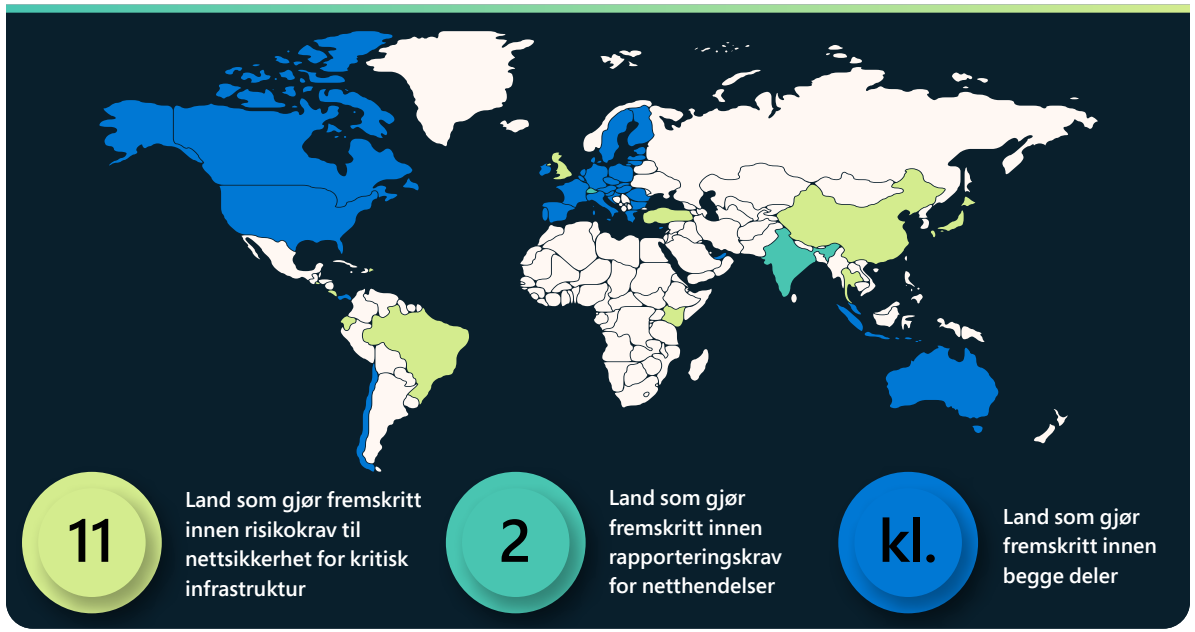
Utvikling av en helhetlig visjon for håndtering av nettrisiko for kritisk infrastruktur er avgjørende, men spesielt med tanke på graden av sammenkobling på tvers av flere typer teknologi og globale leverandører, omfanget av teknologibruk og tilknyttede risikoer, og behovet for å investere i både kortsiktige og langsiktige strategier. Retningslinjer med effektivt omfang som legger til rette for gjentakende læring og forbedringer, og som støtter global interoperabilitet på tvers av sektorer, kan bidra til å håndtere kompleksitet og muliggjøre en digital transformasjon med mer fokus på sikkerhet. En fragmentert tilnærming til lovgivning kan imidlertid føre til overlappende og inkonsekvente forskriftsmessige krav. Dette kan påvirke ressurser og til syvende og sist undergrave sikkerhetsmålene. Organisasjoner kan for eksempel avlede ressurser fra innovasjon og sikkerhet til formalistiske samsvarsformål.

Microsoft ønsker å samarbeide med regjeringer over hele verden for å forfølge effektive retningslinjer for sikkerhet på nettet for kritisk infrastruktur, øke forståelsen av utfordringer og muligheter og støtte innsatsen for å øke den kollektive risikoholdningen.

Politiske utviklinger innen risikostyring av nettsikkerhet for kritisk infrastruktur

I løpet av det siste året har flere jurisdiksjoner, inkludert Australia, Chile, EU, Japan, Singapore, Storbritannia og USA, utviklet, oppdatert eller implementert krav til nettsikkerhet på tvers av sektorer eller sektorspesifikke krav til nettsikkerhet.[1] Mange av disse regjeringene – og andre, for eksempel India[2] og Sveits[3] – har allerede utstedt eller utvikler krav til rapportering av nettsikkerhetshendelser for kritisk infrastruktur og viktige tjenesteleverandører.[4]

Noen bemerkelsesverdige politiske utviklinger fant sted i Australia, EU, Indonesia og USA i løpet av det siste året. Australia vedtok to lover for hjelpe til å håndtere risiko på nettet for kritisk infrastruktur på tvers av sektorer. Lovene utpeker blant annet nye kritiske infrastruktursektorer, krever utvikling av risikostyringsplaner, gir mandat til rapportering av nettsikkerhetshendelser og gjør det mulig for regjeringen å gripe inn hvis den fastslår at en kritisk infrastrukturoperatør er uvillig eller ute av stand til å respondere på en hendelse på en tilstrekkelig måte.



EU jobbet for å oppdatere NIS-direktivet av 2016, som gir et rammeverk for EUs medlemsland for regulering av teknologitjenester og produkter som anses som avgjørende for økonomien og samfunnets funksjon. Den foreslåtte NIS 2 inkluderer revisjoner som vil skape en ny kategori av kritisk digital infrastruktur, øke krav til rapportering av cyberhendelser og innføre ytterligere krav til risikostyring for nettsikkerhet, har EU også utviklet en foreslått oppdatering av sin Digital Operational Resilience Act (DORA), og skaper nye krav til informasjonskommunikasjonsteknologi som brukes i finanssektoren.

I mai utstedte Indonesia en presidentforskrift om beskyttelse av vital informasjonsinfrastruktur («IIV»), som trer i kraft i mai 2024, og dekker blant annet sektorer som energi, transport, finans og helse. Indonesias formål med forskriften er å beskytte kontinuiteten til implementeringen av IIV, forhindre nettangrep og øke beredskapen for håndtering av netthendelser. IIV-leverandører vil være ansvarlige for å gjennomføre sikker og pålitelig beskyttelse, implementere effektiv nettrisikostyring og rapportere nettrisikoresultater til tilsvarende offentlige etater. Forskriften inkluderer et krav om å rapportere netthendelser innen 24 timer.

Myndigheter tar grep for å forbedre sikkerhet og robusthet for kritisk infrastruktur

Fortsettelse

Den amerikanske kongressen vedtok en lov som autoriserte Cybersecurity and Infrastructure Security Agency (CISA) å utstede forskrifter for å kreve rapportering av netthendelser fra operatører av kritisk infrastruktur, og US Transportation Security Administration (TSA) utstedte nye sektorspesifikke krav til nettsikkerhet i transportsektoren. I 2021 utstedte TSA to sikkerhetsdirektiver til operatører av rørledninger for farlige væsker og naturgass som svar på løsepengevirusangrepet på Colonial Pipeline Company:

- Det første direktivet krever at operatørene utpeker en koordinator for nettsikkerhet, rapporterer om netthendelser innen 12 timer og gjennomfører en sårbarhetsvurdering av systemene sine.
- Det andre direktivet, som TSA revidert i 2022, krever at de implementerer spesifikke tiltak for å beskytte mot løsepengevirusangrep og andre kjente trusler mot IT- og OT-systemer, utvikler og implementerer en beredskaps- og responsplan for nettsikkerhet innen 30 dager og foretar en årlig gjennomgang av utformingen av nettsikkerhetsarkitekturen.

Ved å bygge på forskriftene for rørledninger utstedte TSA ytterligere to sikkerhetsdirektiver senere i 2021 som kunngjorde krav til nettsikkerhet for godsvogner, jernbaneoperatører eller jernbanetransportsystemer. Direktivene krever at dekkede operatører utnevner en koordinator for nettsikkerhet, rapporterer om nettsikkerhetshendelser innen 24 timer, utvikler og implementerer en responsplan for nettsikkerhet og gjennomfører en vurdering av sikkerhetssårbarheter. TSA kunngjorde samtidig at de også oppdaterer sine sikkerhetsprogrammer for luftfart for å kreve at operatører på flyplassen og flyselskaper implementerer de to første bestemmelsene, utpeker en koordinator og rapporterer om hendelser innen 24 timer.

Politiske utviklinger innen sikkerhet for IoT- og OT-enheter

I en rekke land arbeider regjeringene aktivt med å utvikle krav for å fremme nettsikkerheten til ICT-produkter og -tjenester (informasjons- og kommunikasjonsteknologi), inkludert IoT- og OT-enheter. Når det gjelder ICT-produkter og -tjenester, er de største bekymringene sikkerhet for programvareforsyningskjeden og IoT-sikkerhet.

- Europakommisjonen foreslo loven om robusthet på nettet, som ville etablere krav til nettsikkerhet for frittstående programvare, tilkoblede enheter og tilleggstjenester.[5] Relevante fremgangsmåter for programvareleverandører inkluderer å utnytte en sikker livssyklus for programvareutvikling[6] og tilby en materialliste for programvare.[7] Nye sikkerhetskrav vil gjelde for tilkoblede enheter, og alle produsenter må håndtere koordinert avsløring av sårbarheter[8] for utgitte produkter.

Politikerne har også fokusert oppmerksomheten sin på den kontinuerlige spredningen av IoT-enheter og OT-enheter på nettverk.

- I Storbritannia vil utkastet til Product Security and Telecommunications Infrastructure Bill kreve at produsenter av tilkoblede produkter for forbrukere, for eksempel smarte TV-er, slutter å bruke standardpassord, som er et enkelt mål for nettkriminelle, etablerer retningslinjer for avsløring av sårbarheter (for eksempel en måte å motta varsel om sikkerhetsfeil på) og sørger for åpenhet om minimumstiden de vil tilby sikkerhetsoppdateringer.[9]
- I EU implementeres nye sikkerhetsstandarder eller -krav via flere lovgivende instrumenter, inkludert en delegert lov i direktivet for radioutstyr som gjelder for trådløse enheter, og søker å forbedre nettverkssikkerheten, beskytte forbrukernes personvern og redusere risikoen for pengesvindel.[10] I tillegg kan bruk av en skysertifiseringsordning,[11] for tiden under utvikling som følge av 2019 EU Cybersecurity Act,[12] være nødvendig.

Behovet for konsistens

I mange tilfeller blir omfanget av aktiviteter på tvers av regioner, sektorer, teknologi og driftsrisikostyring iverksatt samtidig, noe som resulterer i potensiell overlapping eller inkonsekvens i omfang, krav og kompleksitet for organisasjoner som ønsker å utnytte veiledning eller demonstrere samsvar. Uten en universelt akseptert definisjon av IoT er omfanget spesielt utfordrende for regulering av IoT- og OT-enheter. Eksemplene ovenfor gjelder potensielt for «tilkoblede produkter og tilleggstjenester», «forbrukertilkoblede produkter» og «trådløse enheter». Samtidig har mange regjeringer som mål å implementere mer robuste vurderingsregimer for bedre å forstå om og hvordan organisasjoner og produkter oppfyller gjeldende, fremvoksende og utviklende krav. Etter hvert som disse trendene slås sammen, vil kompleksiteten øke. Spørsmål stilt under konsultasjonen om EUs lov om robusthet utforsket oppmuntrende nok hvordan nye forskrifter potensielt kan samhandle med eksisterende nettsikkerhetsforordninger, og indikerte en hensikt om å unngå motstridende krav til nettsikkerhet.

Gjentagende tilnærminger som er risikobaserte og resultat- eller prosessorienterte (i motsetning til implementeringsspesifikke), kan fremme forbedret nettsikkerhet og kontinuerlig forbedring. På samme måte kan et fokus på å muliggjøre interoperabilitet på tvers av sektorer, regioner og politikk konsekvent øke nettsikkerheten på tvers av sammenkoblede globale forsyningskjeder.

Myndigheter tar grep for å forbedre sikkerhet og robusthet for kritisk infrastruktur

Fortsettelse

Stadig mer komplekse retningslinjer for nettsikkerhet for kritisk infrastruktur er i utvikling på tvers av regioner, sektorer og emner. Denne aktiviteten gir store muligheter og medfører betydelige utfordringer. Hvordan regjeringer fortsetter, vil være avgjørende for fremtiden til digital transformasjon og sikkerhet over hele økosystemet.

Fremskyndelse av investeringer i sikkerhet for programvareforsyningskjede og nulltillitsarkitektur over hele økosystemet

Us Executive Order (EO) 14028 om å forbedre nettsikkerheten har vært en katalysator for å fremskynde Microsofts pågående initiativer for å investere i sikkerheten til vår egen forsyningskjede og over hele økosystemet og gjøre det mulig for kundene våre å oppfylle nulltillitsmål.

Vi har lenge ment at forbedring av programvareforsyningskjeden krever deling av erfaringer og anbefalte fremgangsmåter, fra og med vår offentlige utgivelse av Microsofts livssyklus for sikkerhetsutvikling for omtrent 15 år siden.

I tillegg samarbeider vi tett med National Cybersecurity Center of Excellence for å demonstrere tilnærminger til nulltillitsarkitektur som brukes på både lokal og skybasert teknologi og etablering av nye produktfunksjoner, inkludert muligheten til å håndheve phishing-motstandsdyktig godkjenning for hybride miljøer og miljøer med flere skyer.

I dag går vi utover EOs krav for å demonstrere samsvar med sikkerhetskravene til programvareforsyningskjeden, og vi tilbyr SBOM-informasjon (Software Bill of Materials) på to måter:

1. Først deler vi en åpen kildekode-versjon av SBOM-generatorverktøyet vårt, som vi utviklet for enkel integrering med CI/CD-forløp som støtter builder i Windows, Linux, Mac, iOS og Android.[13]
2. For det andre bidrar vi til utviklingen av bransjestandarder for forsyningskjedeintegritet, åpenhet og tillit (SCITT). Dette muliggjør automatisert utveksling av verifiserbar forsyningskjedeinformasjon, inkludert artefakter som demonstrerer samsvar med krav, for eksempel krav som følge av EOs veiledning for programvareforsyningskjeden.

Handlingsrettet innsikt

1. En må se nytt på multilaterale institusjoner for å håndtere den presserende utfordringen med cyberangrep fra nasjonalstater.
2. Utvikle retningslinjer for nettsikkerhet som er konsekvente og interoperable på tvers av regioner, sektorer og emner.

Koblinger til mer informasjon

- Fortsatte investeringer i forsyningskjedesikkerhet for å støtte Cybersecurity Executive Order | Microsoft Tech Community
- Amerikanske myndigheter lanserer strategi og krav til arkitektur for nulltillitssikkerhet | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Forsyningskjedeintegritet, åpenhet og tillit | github.com
- Implementering av en nulltillitsarkitektur | NCCoE (nist.gov)

IoT og OT eksponert: Trender og angrep

Den stadig mer tilkoblede digitale verdenen betyr at enheter kommer raskt på nettet, kommuniserer med større systemer, samler inn data og skaper synlighet på tvers av tidligere uklare områder. Dette gir muligheter både for organisasjoner og trusselaktører, der nettkriminalitet er i ferd med å bli både en industri og risiko verdt flere milliarder dollar.

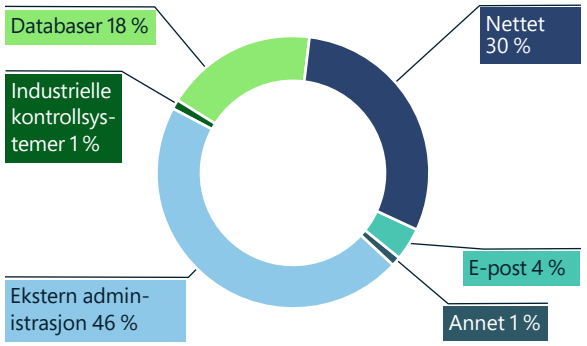
IoT-enheter – inkludert alt fra skrivere til nettkameraer, klimakontrollenheter og tilgangskontroller for bygninger – utgjør en unik sikkerhetsrisiko for enkeltpersoner, organisasjoner og nettverk. Selv om de er avgjørende for driften til mange organisasjoner, kan de raskt utgjøre en belastning og sikkerhetsrisiko. Den raske implementeringen av IoT-løsninger i nær sagt alle bransjer har økt antallet angrepsvektorer og eksponeringsrisikoen for organisasjoner.

Ondsinnet programvare som en tjeneste har blitt vanlig i storskalaoperasjoner både mot sivil og offentlig infrastruktur (inkludert sykehus, olje og gass, el-nett, transporttjenester og annen kritisk infrastruktur) samt bedriftsnettverk. Betydelig forskningsinnsats kreves av trusselaktører for å avdekke og utnytte konfigurasjonen av driftsmiljøer og innebygde IoT- og OT-enheter.

IoT-enheter utgjør unike sikkerhetsrisikoer som inngangs- og dreiepunkter i nettverket. Millioner av IoT-enheter er ikke oppdatert eller eksponert.

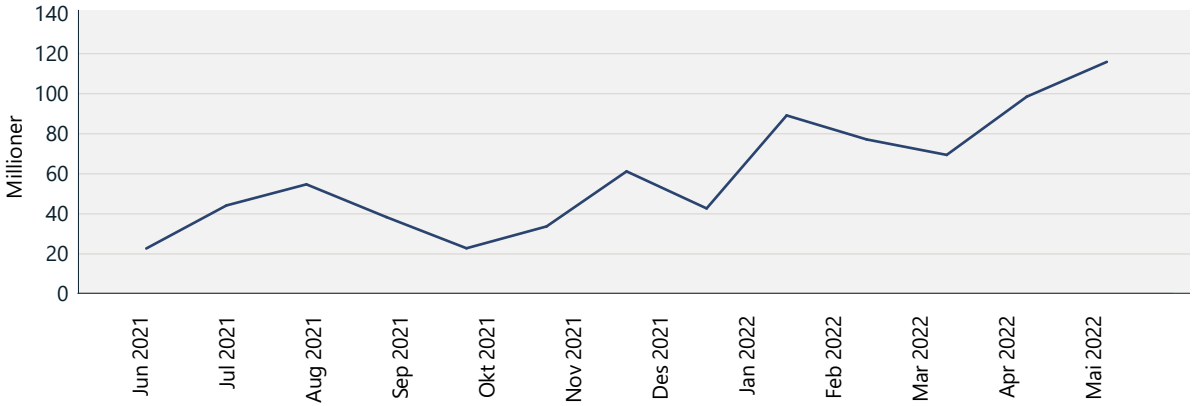
Eksponerte enheter kan oppdages via søkeverktøy på Internett ved å identifisere tjenester som lytter på åpne nettverksporter. Disse portene brukes ofte til ekstern administrasjon av enheter. Hvis den ikke er sikret riktig, kan en eksponert IoT-enhet brukes som et dreiepunkt i et annet lag av bedriftsnettverket, ettersom uautoriserte brukere kan få ekstern tilgang til portene. Vi har observert en rekke trusselaktører som forsøker å utnytte sårbarheter i enheter eksponert for Internett, både kameraer, rutere og termostater. Men til tross for risikoen forblir millioner av enheter ikke oppdatert, eller de blir eksponert.

Sammendrag av angrepstyper på IoT/OT



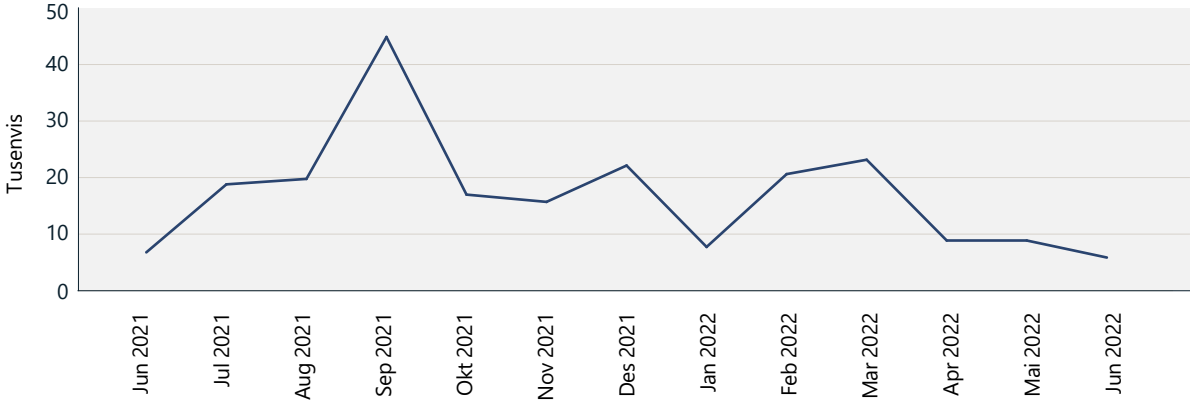
Angrepstyper observert gjennom MSTIC-sensornettverk. De mest utbredte angrepene var angrep mot eksterne administrasjonsenheter, angrep via nettet og angrep på databaser (rå kraft eller utnyttelse).

Angrep mot eksterne administrasjonsenheter



Økning i angrep på eksterne administrasjonsporter over tid, som sett gjennom MSTIC-sensornettverket.

Nettangrep mot IoT og OT



Volumet av nettangrep over tid, som sett gjennom MSTIC-sensornettverket. Etter hvert som antallet enheter som er direkte koblet til nettet, fortsetter å synke, kan det være mindre sannsynlig at angripere sonderer etter dem.

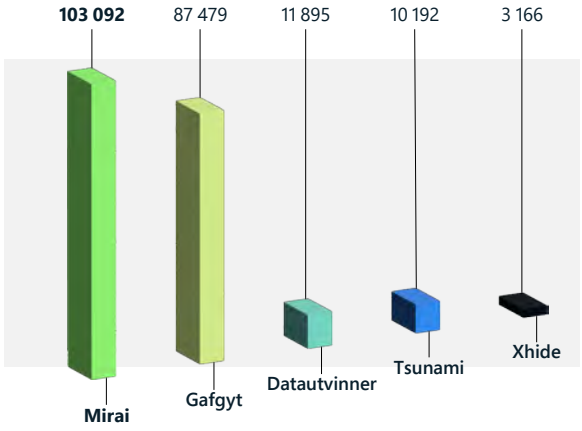
IoT og OT eksponert: Trender og angrep

Fortsettelse

Fornyet verktøy for ondsinnet programvare

Nettkriminalitetsgrupper har utviklet seg, og dette gjelder også implementeringen av ondsinnet programvare og valg av mål. I løpet av det siste året har vi observert at angrep mot vanlige IoT-protokoller – for eksempel Telnet – har blitt betydelig redusert, i enkelte tilfeller med så mye som 60 prosent. Samtidig økte bruken av botnett igjen blant nettkriminelle grupper og statlige aktører. Persistensen til ondsinnet programvare, for eksempel Mirai, fremhever modulariteten til disse angrepene og tilpasningsdyktigheten til eksisterende trusler.

Mest brukt skadelig IoT-programvare oppdaget i fritt omløp



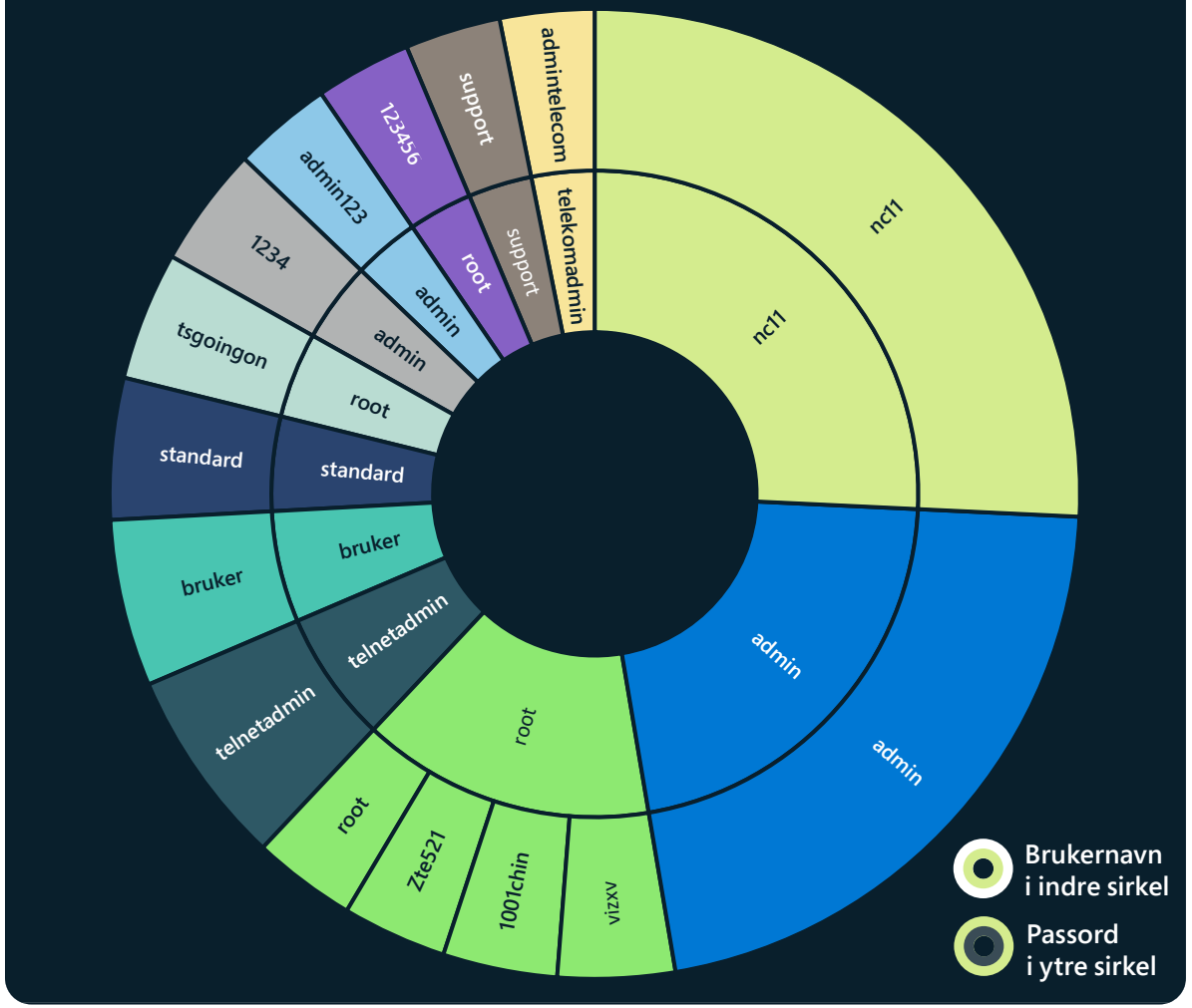
Mirai har blitt utviklet for å infisere et bredt spekter av IoT-enheter, inkludert Internett-protokollkameraer, digitale videoopptakere i sikkerhetskameraer og rutere. Angrepsvektoren omgikk eldre sikkerhetskontroller og utgjør en risiko for endepunkter i nettverket ved å utnytte flere sårbarheter og bevege seg sideveis. Mirai har blitt utformet på nytt flere ganger, med varianter som tilpasser seg ulike arkitekturer og utnytter både kjente sårbarheter og nulldagssårbarheter for å kompromittere nye angrepsvektorer.

Bruken av Mirai vokste blant både 32- og 64-biters x86 CPU-arkitekturer i løpet av det siste året, og ondsinnet programvare fikk nye funksjoner som raskt ble tatt i bruk av statlige og kriminelle grupper. Statlige angrep utnytter nå nye varianter av eksisterende botnett i DDoS-angrep (distribuert tjenestenekt) mot utenlandske fiender.

Etter hvert som inntektene fra angrep mot IoT-enheter ble redusert i 2022, observerte vi flere trusselaktørgrupper som misbrukte sårbarheter – for eksempel Log4j og Spring4Shell – for å levere en ondsinnet nyttelast til enheter, for eksempel servere, infisere dem og rekruttere dem til store botnett som utfører DDoS-angrep. Den fornyede benyttelsen av ondsinnet programvare utformet for å målrette mot sårbare IoT-enheter medfører alvorlige implikasjoner både for organisasjoner og nasjoner, ettersom sideveis lateral bevegelse kan utsette bakdører for ekstra nyttelast og andre enheter på nettverk.

Mange industrielle kontrollsystemprotokoller er uovervåket og derfor sårbare for OT-spesifikke angrep. Dette kan bety økt risiko for kritisk infrastruktur.

Relativ utbredelse av par med brukernavn og passord sett blant IoT/OT-enheter i løpet av 45 dager med sensorsignaler.



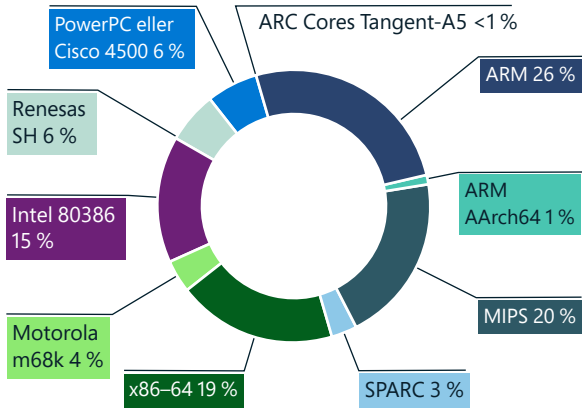
Bruk av par med vanlige brukernavn og passord øker risikoen for kompromittering. Basert på en utvalgsstørrelse på over 39 millioner IoT- og OT-enheter representerte de som brukte identiske brukernavn og passord, rundt 20 prosent.

IoT og OT eksponert: Trender og angrep

Fortsettelse

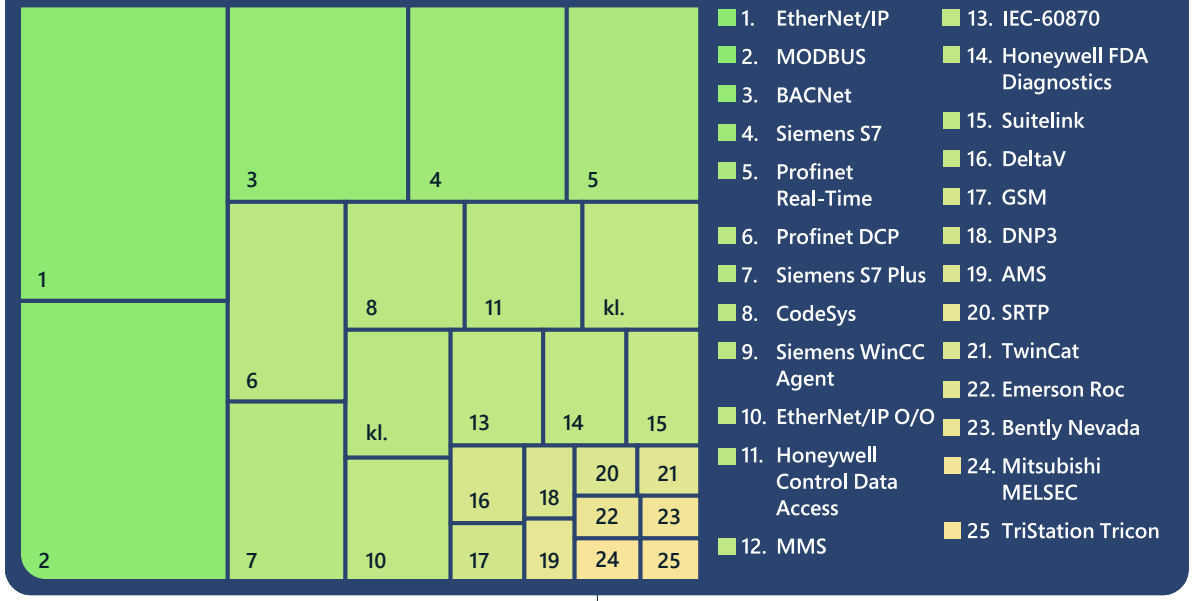
Selv om svake konfigurasjoner og standardlegitimasjon fortsatt utgjør en risiko for nettverk, har Microsoft observert mange nettbaserte utnyttelser ved hjelp av HTTP. Vi observerte denne økningen i angrep på nettbaserte tjenester ved hjelp av eldre botnett. Samtidig var det en nedgang i antall åpne Telnet-porter på Internett, et positivt tegn for nettverkssikkerhet siden botnett, som har utgjort en historisk risiko for enheter, mister relevans. Til tross for denne nedgangen i åpne Telnet-porter, observerte vi fortsatt persistente botnett i sensornettverk.

Fordeling av ondsinnet IoT-programvare per CPU-arkitektur



Microsoft observerte at IoT-enheter som kjører på ARM, er mest målrettet av ondsinnet programvare, etterfulgt av MIPS, X86-64 og Intel 80386 CPU.

Utbredelse av industrielle kontrollsystemprotokoller



Sårbarheter for industrielle kontrollsystemprotokoller

Vi så på OT-data fra de skytilkoblede sensorene våre og avdekket de vanligste ICS-protokollene (industrielt kontrollsystem). Disse protokollene gir innsikt i hvilken type disse enhetene er, og angrepsoverflaten. Dette er spesielt relevant for sikkerheten til kritisk infrastruktur. Noen viktige erfaringer er følgende:

1. De fleste protokollene som representeres, er proprietære, så standard IT-overvåkingsverktøy vil ikke ha tilstrekkelig sikkerhetssynlighet for alle disse enhetene og protokollene. Som et resultat blir nettverk uovervåkede og derfor mer sårbare for OT-spesifikke angrep.
2. Det finnes et stort utvalg av leverandørspesifikke protokoller. Dette betyr at leverandørspesifikke sikkerhetsløsninger ikke vil kunne dekke hele nettverket tilstrekkelig. Microsoft prioriterer en leverandøragnostisk tilnærming, for å gi sikkerhetsdekning for det brede utvalget av ulike enheter.
3. Organisasjoner må sørge for at disse protokollene ikke eksponeres direkte for Internett fra nettverkene sine. En slik eksponering kan utgjøre en stor sikkerhetsrisiko på grunn av sårbarheter og fordi protokollene er usikre.

Ondsinnet programvare som Mirai vedvarer ved å utvikle nye funksjoner. Det blir tatt i bruk av grupper med nettkriminelle og statlige aktører som utnytter nye varianter av eksisterende botnett i DDoS-angrep på utenlandske fiender.

Handlingsrettet innsikt

1. Sørg for at enhetene er robuste ved å bruke oppdateringer, endre standardpassord og standard SSH-porter.
2. Reduser angrepsoverflaten ved å eliminere unødvendige Internett-tilkoblinger og åpne porter, noe som begrenser ekstern tilgang ved å blokkere porter, nekte ekstern tilgang og bruke VPN-tjenester.
3. Bruk en IoT/OT-bevisst løsning for nettverksgjenkjenning og -respons (NDR) og en SIEM-løsning (sikkerhetsinformasjon og hendelsesstyring) eller en SOAR-løsning (sikkerhetsorkestrering og respons) for å overvåke enheter for avvikende eller uautorisert atferd, for eksempel kommunikasjon med ukjente verter.
4. Segmenter nettverk for å begrense angriperens evne til å bevege seg sideveis og kompromittere ressurser etter første inntrenging. IoT-enheter og OT-nettverk må isoleres fra bedriftens IT-nettverk via brannmurer.
5. Sørg for at ICS-protokoller ikke er eksponert direkte for Internett.

Hacking av forsyningskjede og fastvare

Nesten alle Internett-tilkoblede enheter har fastvare, som er programvare innebygd i enhetens maskinvare eller kretskort. I løpet av de siste årene har vi sett økt målretting av fastvare for å starte ødeleggende angrep. Ettersom fastvare sannsynligvis vil fortsette å være et verdifullt mål for trusselaktører, må organisasjoner beskytte mot hacking av fastvare.

Fastvare er ansvarlig for enhetens primære funksjoner, for eksempel tilkobling til et nettverk eller lagring av data. Fastvare finnes i rutere, kameraer, TV-er og andre enheter som brukes i bedrifter (IoT), sammen med industrielt kontrollutstyr (OT) som brukes i kritisk infrastruktur. Historisk sett har fastvare blitt skrevet med usikret kode, noe som skaper betydelige sårbarheter som kan utnyttes til å ta over enheten eller injisere skadelig kode i fastvaren.

Denne risikoen blir forverret når det gjelder forsyningskjeden. De fleste enheter er bygd ved å bruke programvare- og maskinvare-komponenter fra mange produsenter samt biblioteker med åpen kildekode. I mange tilfeller har ikke enhetsoperatører innsyn i stykklisten for maskinvaren og programvaren (H/SBOM) for å evaluere forsyningskjedens risiko for enheter på nettverket. I juni 2020 ble sårbarheter avdekket i en nettverksstakk som ble brukt av mange forskjellige produsenter, noe som påvirket mange hundre millioner IoT-enheter i forbruker- og industriutstyrssektoren.[14] I enkelte tilfeller ble nettverksstakken omprofilert av andre leverandører, og det var ingen indikasjon på at en enhet var sårbar. Vi ser en økende trussel fra ondsinnede aktører som målretter mot denne programvare- og maskinvareforsyningskjeden til IoT/OT-enheter for å kompromittere organisasjoner.

Oppdateringsprosessen for fastvare varierer mye fra enhet til enhet, og kompleksiteten og den logistiske utfordringen med å utføre den påvirker oppdateringshyppigheten. Det er ikke alltid mulig å finne ut om en enhet kjører den nyeste fastvaren, noe som gjør det vanskelig for sikkerhetsteknikere å overvåke og sørge for god sikkerhetsholdning i IoT- og OT-enhetene. I tillegg har enkelte enheter fastvare som ikke er kryptografisk signert, slik at de kan oppdateres uten bekreftelse fra brukeren. Disse svakhetene øker sjansene ytterligere for angrep fra forsyningskjeden gjennom hele produksjons- og distribusjonskjeden.

For å håndtere disse truslene investerer Microsoft betydelig i å sørge for sikkerheten og integriteten til fastvaren når den beveger seg gjennom ulike faser av forsyningskjeden, og ved når som helst å attestere at den ikke har blitt tuklet med under inntak eller underveis. Dette gjør at vi kan validere tillit mellom hvert segment i forløpet og gi en sertifisert og beviselig fullstendig forvaringskjede for hver komponent vi sender til kundene. Vi samarbeider med partnerne våre for å sørge for at alle enheter på bedriftsnettverket og OT-nettverket har denne brikke-til-sky-sikkerheten.

«Leverandører av IKT-infrastruktur utgjør stadig mer utsatte mål ved at de muliggjør utbredt replikering av ett enkelt angrep. Samtidig øker globale forskrifter, regulering og kundenes krav til sikkerhet og robusthet i forsyningskjeden, noe som ofte kommer i konflikt med kravene deres.

Løsningen er partnerskap. Sammen med leverandører og regjeringer globalt er Microsoft innstilt på å håndtere sikkerhet i hele forsyningskjedeøkosystemet vårt og overgå kravene både fra kunder og tilsynsmyndigheter. For å gjøre dette legger vi til rette for en omfattende tilnærming til sikkerhet og operasjonell elastisitet som er fleksibelt distribuert i hele forsyningskjeden.

Nøkkelen til vår kollektive tilnærming er å legge til rette for fastvareintegritet fra design til enhetsoperasjon. Eksempler på hvordan vi kan «bygge inn» forsyningsk-jedeintegritet, omfatter å sikre leverandørers SDL-prosesser og innovasjon for å distribuere maskinvarebasert rotsertifikat.

Samfunnet vårt utnytter kollektiv forskning og utvikling som spenner over nye anti-manipuleringsteknikker og kryptografiske mekanismer, kombinert med kontinuerlig overvåking og oppdagelse av avvik. Sammen utvikler vi oss med å minimere tilførselskjeden som en angrepsoverflate.»

Edna Conway,
Viseadministrerende direktør, sikkerhets- og risikoansvarlig, skyinfrastruktur

Søkelyset på fastvaresårbarheter

Angripere utnytter i økende grad sårbarheter i fastvaren for IoT-enheter for å infiltrere bedriftsnettverk. I motsetning til tradisjonelle IT-endepunkter som bruker XDR-agenter til å identifisere svakheter, er sårbarhetsidentifikasjon i IoT/OT-enheter mye mer unnvikende.

En fersk undersøkelse utført av Microsoft og Ponemon Institute fremhever både muligheten og sikkerhetsutfordringen til IoT/OT-enheter i en bedrift.[15] Mens 68 prosent av de spurte mener innføringen av IoT/OT er avgjørende for den strategiske digitale transformasjonen, erkjenner 60 prosent at IoT/OT-sikkerhet er et av de minst sikrede aspektene ved IT/OT-infrastrukturen.

Et eksempel på angripere som bruker sårbarheter i fastvare for IoT-enheter til å infiltrere et nettverk, er Trickbot-trojaneren som utnyttet standardpassord og sårbarheter i Mikrotik-rutere[16] for å omgå forsvarssystemer til bedrifter. Den fundamentale utfordringen med fastvare for IoT-enheter er mangelen på innsyn i sikkerhetsnivået og sårbarhetene til enheter.

Selv om det finnes løsninger for å bygge sikre enheter, finnes det milliarder av enheter som allerede er på markedet og tatt i bruk i bedrifter. Disse er kjent som «brownfield»-enheter. I 2021 kjøpte Microsoft ReFirm Labs for å belyse over sikkerheten til «brownfield»-enheter og gjøre det mulig for enhetsbyggere å forbedre sikkerheten til produktene sine. ReFirm Labs analyserer den binære fastvareavbildningen av en enhet og produserer en detaljert rapport om potensielle sikkerhetssvakheter.[17] Denne teknologien blir innlemmet i en fremtidig utgivelse av Microsoft Defender for IoT.

I løpet av det siste året har vi undersøkt aggregerte resultater av den unike fastvaren som ble skannet av kundene våre. Selv om ikke alle svakheter som oppdages, kan utnyttes, understreker de den fundamentale utfordringen med fastvaresikkerhet for enheter.

Vær oppmerksom på at svakhetstypene som finnes i IoT/OT-enheter, aldri ville være akseptabelt på tradisjonelle Windows- eller Linux-endepunkter.

- Svake passord: 27 prosent av fastvareavbildningene som ble skannet, inneholdt kontoer med passord kodet med svake algoritmer (MD5/DES), som enkelt kan brytes av angripere.

Sikkerhetssvakheter i analyserte fastvareavbildninger

- Kjente sårbarheter: Som i andre systemer brukte IoT/OT-enhetsfastvaren i utstrakt grad biblioteker med åpen kildekode. Enheter leveres imidlertid ofte med utdaterte versjoner av disse komponentene. I analysen vår inneholdt 32 prosent av avbildningene minst 10 kjente sårbarheter (CVE-er) vurdert som kritiske (9,0 eller høyere). Fire prosent inneholdt minst 10 kritiske sårbarheter som var over seks år gamle.
- Utløpte sertifikater: Sertifikater brukes til å godkjenne tilkoblinger og identiteter, i tillegg til å beskytte sensitive data, men 13 prosent av avbildningene som ble analysert, inneholdt minst 10 sertifikater som hadde utløpt for over tre år siden.
- Programvarekomponenter: 36 prosent av avbildningene inneholder programvare-komponenter Microsoft anbefaler å ekskludere i IoT-enheter, for eksempel pakkelagringsverktøy (tcpdump, libpcap), som kan utnyttes for nettverksrekognosering som en del av en angrepskjede.

Fastvareangrep i fritt omløp

Viasat: Bruk av en fastvaresårbarhet for å målrette mot satellittkommunikasjon

I februar 2022 gjorde en hendelse i et satellittnettverk at et strategisk kommunikasjonsnettverk ble frakoblet, med innvirkninger over hele Europa. Viasats KA-SAT-system mottok en stor mengde trafikk som koblet fra mange modemer, og et tjenestenektangrep ble iverksatt mot nettverket. Etter hvert som det faste bredbåndet ble forstyrret, ble tusenvis av vindmøller utilgjengelige for operatører, og ondsinnet slettingsprogramvare ble implementert på berørte modemer. Forstyrrelsen påvirket over 30 000 satellitterminaler som brukes av selskaper og organisasjoner for kommunikasjon.

Cyclops Blink: Bruk av et fastvareforsynings-kjedeangrep for å målrette mot brannmurgatewayer

For trusselaktører er utvikling og utvidelse av kommando- og kontrollinfrastruktur (C2) og angrepsinfrastruktur en avgjørende del av suksessen. Etter hvert som behovet for en stabil C2-infrastruktur har vokst, har rutere blitt en ønskelig angrepsvektor på grunn av at de oppdateres sjelden og mangler omfattende sikkerhetsløsninger.

Microsoft samarbeider med myndighetene og industrien om fastvareanalyseteknologi for å få dypere innsyn i enhetssikkerhet og tilby full livssyklussikkerhet for enhetsbyggere og operatører.

Siden juni 2019 har en statlig tilknyttet avansert trusselgruppe (APT) brukt den modulære ondsinnede programvaren Cyclops Blink til å målrette mot sårbare WatchGuard-brannmurenheter og ASUS-rutere ved å utføre ondsinnede fastvareoppdateringer og rekruttere dem til et stort botnet. Den ondsinnede programvaren infiserer enheter ved å utnytte en kjent sårbarhet som muliggjør eskalering av rettigheter, slik at trusselaktørene kan administrere enheten. Når den er infisert, tillater den ondsinnede programvaren at flere moduler installeres og unngår fastvareoppdateringer. Kompromitterte enheter har blitt observert ved tilkobling til C2-servere som driftes på andre WatchGuard-enheter. Cyclops Blink-operatørene har utstedt mange SSL-sertifikater for C2 på ulike TCP-porter, og de har fått privilegert ekstern tilgang til nettverk ved å kjøre ondsinnede fastvareoppdateringer og ved å unngå tradisjonelle sikkerhetsmetoder som skanning.

Hvordan Microsoft forbedrer sikkerhet i forsyningskjeden

Microsoft samarbeider med myndighetene og industrien for å løse disse sikkerhetsutfordringene for IoT- og OT-enheter (se diskusjonen på side 66). Bidraget vårt vil omfatte bruk av fastvareanalyseteknologi for å gi enhetsoperatører innsyn i sikkerhetsholdningen til enhetene på nettverket. Dette vil gjøre det mulig for kunder å identifisere og prioritere enheter med behov for ekstra beskyttelse, oppgraderinger eller erstatning – og øke behovet for enhetsbyggere å investere i enhetssikkerhet. Samtidig støtter vi utbyggere med omfattende løsninger for å konstruere sikre enheter og ta i bruk sikre utviklingslivssykluser.

En annen viktig komponent er å gi utbyggere og operatører en robust infrastruktur som gjør det mulig å oppdatere fastvaren for enheter så snart sikkerhetsproblemer oppdages og løses. Microsoft kombinerer fastvareanalyse og Defender for IoT med Device Update for IoT Hub for å tilby en løsning som håndterer IoT- og OT-enhetssikkerhet gjennom hele livssyklusen. Dette er viktige brikker for å realisere visjonen om å gi kundene mulighet til å sikre infrastrukturen ved å ta i bruk enheter som støtter en nulltillit-tilnærming til IoT- og OT-løsningene sine.[18]

Angripere målretter i økende grad sårbarheter i fastvaren til IoT-enheten for å infiltrere bedriftsnettverkene.

Handlingsrettet innsikt

1. Få dypere innsikt i IoT/OT-enheter på nettverket, og prioriter enhetene etter risiko for bedriften hvis de blir kompromittert.
2. Bruk skanneverktøy for fastvare for å forstå potensielle sikkerhetssvakheter, og samarbeid med leverandører for å finne ut hvordan du kan redusere risikoen for høyrisikoenheter.
3. Påvirk sikkerheten til IoT/OT-enheter positivt ved å kreve at leverandørene dine tar i bruk anbefalte fremgangsmåter for sikker utviklingslivssyklus.

Koblinger til mer informasjon

- Vurdering av de kritiske forsyningskjedene som støtter informasjons- og kommunikasjonsteknologibransjen i USA

Rekognoseringsbaserte OT-angrep

Komplekse forsyningskjeder bruker spesifikk designinformasjon for å planlegge det faktiske systemet. Prosjektfilen, som definerer miljøet og ressursene i det, er den mest sensitive av de utallige ressursene som utgjør denne designinformasjonen. Denne filen er et avgjørende strategisk mål for trusselaktører som ønsker å få tilgang til og distribuere et vellykket angrep helt skreddersydd til miljøet.

Å målrette angrep mot industrisystemer for å forstyrre driftsprosesser innebærer to trinn.

1. Først må angriperen få tilgang til OT-nettverket. Dette kan gjøres via IoT-enheter på bedriftssiden av nettverket (Purdue-modellnivå 4) og krysse IT-OT-grensen, som tradisjonelt er atskilt med brannmurer og nettverksutstyr, til drifts- og kontrollnivåene.
2. For det andre må nettverksenhetene identifiseres. Industrielle systemer bruker standardenheter og komponenter i tilpassede arkitekturer som er spesielt utformet for sine miljøer. Én av disse standardenhetene er den programmerbare logiske kontrolleren (PLC). Hver produsent utvikler unike grensesnitt og funksjoner for sine PLC-er, som er en avgjørende komponent i industrielle systemer, og disse enhetene blir ytterligere konfigurert med tilpassede skjemaer spesielt utformet for kundens miljøer.

Den unike konfigurasjonen av hver PLC er beskrevet i prosjektfilen, som inneholder definisjonen av miljøet og dets eiendeler, stigelogikken med mer.

I de fleste miljøer som beviselig er angrepet, viser analyser at tidslinjen før angrepet langt overskrider lengden på selve angrepet. Trusselaktører investerer ofte måneder i å simulere miljøet og dets ressurser eksternt, gjør mange forsøk på å konstruere en modell og forbereder det målrettede angrepet. Etter hvert som miljøer kontinuerlig endres og integrerer nye enheter, opprettes sårbarheter spesifikt rundt dataene i prosjekt- og konfigurasjonsfilene. Tyveri av en prosjektfil kan forserer et angrep med uker eller måneder og gjøre det mulig for angripere å modellere målmiljøet raskt og nøyaktig, noe som gjør det vanskeligere å oppdage skadelig aktivitet.

Industroyer og Incontroller

Vi har observert et økende antall angrep på organisasjoner, kritisk infrastruktur og offentlige mål av statlig sponsede aktører som bruker modulære rammeverk for skadelig programvare og angrep. Nye forsøk på å forstyrre kritiske operasjoner i Ukraina understreker den økende trusselen om rekognoseringsbaserte OT-angrep som er svært skreddersydd til sine målmiljøer. De utvidede rekognoserings- og researchfasene utført av statlige cyberaktører peker mot en strategi der cyberkrigføring brukes for å lamme infrastrukturen eksternt for å nå spesifikke strategiske eller operative mål i en blanding av cyberkinetiske operasjoner og politisk strategi.

Vi har observert en økende trussel om rekognoseringsbaserte OT-angrep som er svært skreddersydd til miljøene de angriper.

Rekognoseringsbaserte OT-angrep

Fortsettelse

Tidlig i 2022 ble to tilpasningsdyktige kritiske OT-angrep identifisert. Et cyber-fysisk angrep på elektriske transformatorstasjoner og beskyttelsesreléer i Ukraina ble utført med tilpasset skadelig programvare, inkludert en variant av Industroyer, en skadelig programvare kjent for å ha forårsaket strømbrudd i Ukraina etter at den ble utplassert i 2016.

Industroyer2 er den første kjente redistribusjonen av skadelig OT-angrepsprogramvare på et nytt mål. Den benyttet programtillegget til IEC104-protokollen (standardprotokollen for overvåking og styring av kraftsystemer) utviklet for Industroyer og målrettet for det meste PLC-lignende eksterne terminalenheter med modellnummer ABB RTU540/560. Forfatteren av denne skadelige programvaren brukte kunnskap om offerets miljø til å sende kommandoer gjentatte ganger til forhåndsbestemte utganger, slik at de ikke kunne aktiveres manuelt. Dette sikret langvarige strømbrudd og en mer ødeleggende effekt.

Incontroller, et modulært angrepsrammeverk som ble identifiseres i løpet av samme periode, er et modulært verktøysett som i betydelig grad reduserer ledetiden til å trenge inn og angripe OT-enheter og omgå eldre sikkerhetsløsninger. Det generelle verktøysettet har funksjoner for datainnsamling, rekognosering og angrep som er svært tilpassbare til ulike miljøer, og som i stor grad kan påvirke researchfasen for et OT-angrep. Dette reduserer tiden det tar å utføre rekognosering og støtter simulering av miljøer ved å trekke ut informasjon om enheter og deres konfigurasjoner.

Incontroller-rammeverket støtter protokoller for Schneider Electric og Omron PLC-er og samler inn informasjon, for eksempel fastvareversjon, modelltype og tilkoblede enheter. Verktøysettet kan utstede kommandoer for å endre konfigurasjoner og slå utdata av og på. Når det er skaffet tilgang til et miljø, støtter rammeverket implantering av bakdører i enheter for levering av flere nyttelaster, utstedelse av sårbarheter for å øke antall tilgangspunkter, opplasting av stigelogikk og muligheten til å sette i gang DoS-angrep. Den generiske naturen til verktøysettet gjør det mulig for en trusselaktør å angripe et miljø raskt uten å måtte skrive nye angrep for hver PLC eller plassering. Dette gjør at aktøren enkelt kan samhandle med ulike typer maskiner i mange bransjer.

Handlingsrettet innsikt

1. Unngå å overføre filer som inneholder systemdefinisjoner gjennom usikre kanaler, eller til ikke-essensielt personell.
2. Når overføring av slike filer er uunngåelig, må du sørge for å overvåke aktiviteten på nettverket og sørge for at ressursene er sikre.
3. Beskytt engineeringstasjoner ved å overvåke dem med EDR-løsninger.
4. Utfør hendelsesrespons proaktivt for OT-nettverk.
5. Ta i bruk kontinuerlig overvåking, for eksempel Defender for IoT.

Sluttnoter

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. uten navn (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Se for eksempel Microsoft Security Development Lifecycle
7. Se f.eks. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft, se også f.eks. 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—product security factsheet—GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)
12. Certification — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool» GitHub - Microsoft/sbom-tool: SBOM-verktøyet er et svært skalerbart og bedriftsklart verktøy for å opprette SPDX 2.2-kompatible SBOM-er for alle typer 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 (des. 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 (mai 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 (mai 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Cyberpåvirknings-operasjoner

Dagens påvirkningsoperasjoner fra utlandet bruker nye metoder og teknologier, noe som gjør kampanjene som er utformet for å svekke tillit, mer effektive.

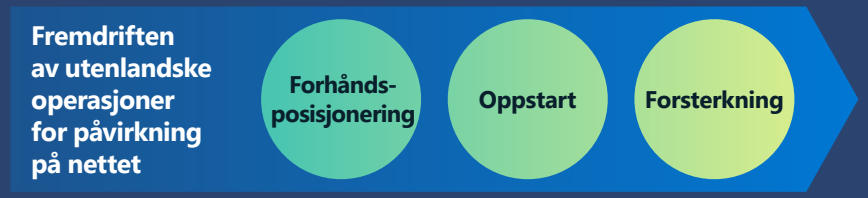
En oversikt over

cyberpåvirknings-operasjoner

Dagens påvirkningsoperasjoner fra utlandet bruker nye metoder og teknologier, noe som gjør kampanjene som er utformet for å svekke tillit, mer effektive.

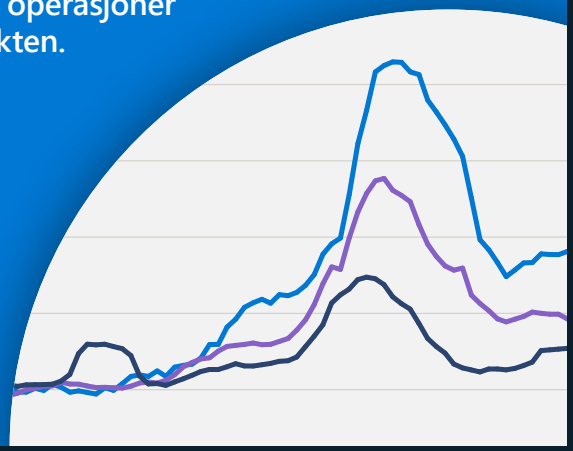
Nasjonalstater bruker i økende grad sofistikerte påvirkningsoperasjoner til å distribuere propaganda og påvirke opinionen i befolkningen både innenlands og internasjonalt. Disse kampanjene svekker tilliten, øker polariseringen og truer demokratiske prosesser. Dyktige, avanserte og vedvarende manipulatorer bruker tradisjonelle medier sammen med Internett og sosiale medier for å øke omfanget av, skalaen og effektiviteten til kampanjene vesentlig, og de har en enorm innvirkning i det globale informasjonsøkosystemet. I løpet av det siste året har vi sett disse operasjonene brukt som en del av Russlands hybride krig i Ukraina, men vi har også sett Russland og andre nasjoner, inkludert Kina og Iran, i økende grad tar i bruk propaganda i sosiale medier for å utvide sin globale innflytelse i en rekke saker.

Cyberpåvirkningsoperasjoner blir stadig mer sofistikerte etter hvert som flere regjeringer og nasjonalstater bruker disse operasjonene til å påvirke meninger, diskreditere motstandere og fremme misnøye.



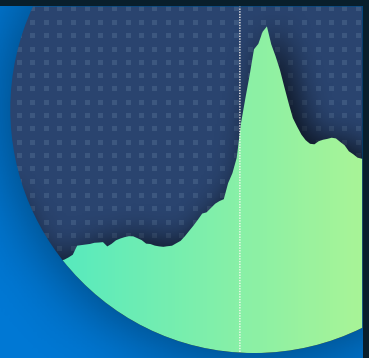
Finn ut mer på side 74

Under Russlands invasjon av Ukraina ble cyberpåvirkningsoperasjoner integrert med mer tradisjonelle cyberangrep og kinetiske militære operasjoner for å maksimere effekten.



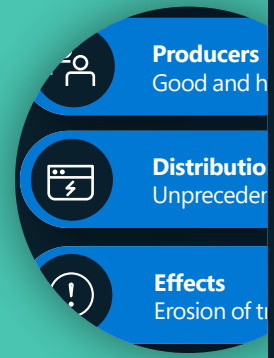
Finn ut mer på side 76

Russland, Iran og Kina brukte propaganda- og påvirkningskampanjer gjennom COVID-19-pandemien, ofte som et strategisk redskap, for å oppnå bredere politiske mål.



Finn ut mer på side 76

Syntetiske medier er blitt mer utbredt på grunn av spredningen av verktøy som enkelt lager og sprer svært realistiske kunstige bilder, videoer og lyd. Digital opphavsteknologi som sertifiserer opprinnelsen til medieressurser, er lovende med tanke på å bekjempe misbruk.



Finn ut mer på side 80

En helhetlig tilnærming for å beskytte mot cyberpåvirkningsoperasjoner

Microsoft bygger på den allerede modne infrastrukturen for cybertrusseletterretning for å bekjempe operasjoner med cyberpåvirkning. Strategien vår er å oppdage, forstyrre, bekjempe og avskrekke propagandakampanjer fra utenlandske aggressorer.

Finn ut mer på side 83

Innledning

Demokratiet trenger pålitelig informasjon for å blomstre. Et sentralt fokusområde for Microsoft er påvirkningsoperasjonene som utvikles og gjenno-mføres av nasjonalstater. Disse kampanjene svekker tilliten, øker polariseringen og truer demokratiske prosesser.

Påvirkningsoperasjoner fra utlandet har alltid vært en trussel mot informasjonsøkosystemet. Det som imidlertid er forskjellig i en tidsalder med internett og sosiale medier, er det enormt økte omfanget og effektiviteten til kampanjene, og den enorme innvirkningen de kan ha på helsen til det globale informasjonsøkosystemet.

Det gamle ordtaket om at «en løgn kommer halvveis rundt jorden før sannheten har en sjanse til å ta på seg skoene», blir nå bekreftet med data. En undersøkelse utført av Massachusetts Institute of Technology (MIT)[1] viste at det er 70 prosent mer sannsynlig at usannheter blir retweetet enn sannheten, og at de når de første 1500 personene seks ganger raskere. Informasjonsøkosystemet har blitt stadig mer uklart etter hvert som kampanjene på internett og i sosiale medier har blomstret og undergravd tilliten til tradisjonelle nyheter. I en studie fra 2021[2] svarte bare syv prosent av amerikanske voksne at de har «mye» tillit til avis-, TV- og radionyheter, mens 34 prosent svarte «ingen i det hele tatt».

Microsoft har jobbet med å identifisere de viktigste aktørene, truslene og taktikkene innen utenlands cyberpåvirkning og for å dele erfaringer. I juni i år publiserte vi en omfattende rapport om erfaringene fra Ukraina, som inneholdt en detaljert vurdering av Russlands cyberpåvirkningsoperasjoner.[3]

Vi studerer også hvordan avansert teknologi som dype forfalskninger kan brukes som våpen og undergrave troverdigheten til journalister. Og vi samarbeider med industri, myndigheter og akademia for å utvikle bedre måter å oppdage syntetiske medier på og gjenopprette tillit – for eksempel systemer med kunstig intelligens (AI) som kan oppdage forfalskninger.

Den raskt skiftende naturen til informasjonsøkosystemet og nasjonals-tatbasert nettpropaganda, inkludert sammensmeltingen av tradisjonelle nettangrep med påvirkningsoperasjoner og innblanding i demokratiske valg, krever en helhetlig tilnærming for å demme opp mot både nettbaserte og fakoblede trusler mot demokratiet.

Microsoft er dedikert til å støtte et sunt informasjonsøkosystem der pålitelige nyheter og informasjon trives. Vi utvikler verktøy og trusseldeteksjonsevner for å bekjempe den økende risikoen for nasjonalstatsdrevne påvirkningsoperasjoner. For å muliggjøre dette arbeidet erververt vi nylig Miburo Solutions, vi samarbeider med tredjepartsvalidatorer som Global Disinformation Index og NewsGuard, og vi deltar og leder til tider multipartnerskap, inkludert Coalition for Content Provenance and Authenticity (C2PA). Bare ved å samarbeide kan vi lykkes i å bekjempe de som søker å undergrave demokratiske prosesser og institusjoner.

Teresa Hutson

Vice President, Technology and Corporate Responsibility

Trender i cyberpå-virkningsoperasjoner

Cyberpåvirkningsoperasjonene blir stadig mer sofistikerte i takt med at teknologien utvikler seg. Vi ser en overlapping og utvidelse ved at verktøyene som brukes i tradisjonelle cyberangrep også brukes i cyberpåvirkningsoperasjoner. I tillegg ser vi en økt koordinering og forsterket samarbeid mellom nasjonalstatene.

Microsoft investerte i å bekjempe utenlandske påvirkningsoperasjoner foregående år ved oppkjøpet av Miburo Solutions, et selskap som spesialiserer seg på analyse av utenlandske påvirkningsoperasjoner. Ved å kombinere disse analytikerne med Microsofts egne trusselkon-tekstanalytikere, dannet vi Microsoft Digital Threat Analysis Center (DTAC). DTAC analyserer og rapporterer om nasjonalstatstrusler, inkludert både cyberangrep og påvirkningsoperasjoner, og kombinerer informasjon og trusseletterretning med geopolitisk analyse for å gi innsikt og informere om effektiv respons og beskyttelse.

Mer enn tre fjerdedeler av mennesker som ble spurt over hele verden, svarte at de bekymrer seg for informasjon brukt som våpen,[4] og dataene våre støtter disse bekymringene. Microsoft og partnerne våre har avdekket hvordan nasjonalstatsaktører bruker påvirkningsoperasjoner for å nå strategiske og politiske mål. I tillegg til destruktive cyberangrep og cyberspionasje, bruker autoritære regimer i økende grad cyberpåvirkningsoperasjoner til å forme meninger, diskreditere motstandere, mane frem frykt, fremme splid og forvrenge virkeligheten.

Disse cyberpåvirkningsoperasjonene fra utlandet har vanligvis tre stadier:

Forhåndsposisjonering

I likhet med forhåndsposisjonering av skadelig programvare i en organisasjons datanettverk, forhåndsposisjonerer utenlandske cyberoper-asjoner falske narrativer i det offentlig rom på internett. Forhåndsposisjoneringstaktikken har lenge bistått mer tradisjonelle cyberaktiviteter, spesielt hvis IT-administratorer skanner sin siste nettverksaktivitet. Skadelig programvare som ligger i dvale i lengre tid på et nettverk, kan gjøre den etterfølgende bruken mer effektiv. Falske fortellinger som ligger ubemerket på internett, kan få påfølgende referanser til å virke mer troverdige.

Lansering

Ofte på det tidspunktet som er mest fordelaktig for å nå aktørens mål, lanseres en koordinert kampanje for å formidle fortellinger gjennom statlig støttede og påvirkede medier og sosiale medier-kanaler.

Forsterkning

Til slutt forsterker nasjonalstatskontrollerte medier og representanter fortellinger overfor utpekte målgrupper. Ofte utvider uvitende teknologiske muliggjørere rekkevidden til fortellingene. Nettannonsering kan for eksempel bidra til å finansiere aktiviteter, og koordinerte systemer for innholdslevering kan oversvømme søkemotorer.

Denne tre-trinns tilnærmingen ble brukt på slutten av 2021 for å støtte de falske russiske fortellingene om påståtte biovåpen og biolaboratorier i Ukraina. Denne historien ble først lastet opp til YouTube 29. november 2021 som en del av et vanlig engelskspråklig program, av en Moskva-basert amerikansk utflytter som hevdet at USA-finansierte biolaboratorier i Ukraina var koblet til biovåpen. Historien gikk stort sett ubemerket hen i flere måneder. Den 24. februar 2022, samtidig som russiske stridsvogner krysset grensen, ble fortellingen sendt inn i kamp. Et dataanalyseteam hos Microsoft identifiserte ti russiskkontrollerte eller russiskpåvirkede nyhetssteder som 24. februar publiserte rapporter som alle pekte tilbake til «rapporten fra i fjor» for å gi den troverdighet. I tillegg holdt tjenestemenn i det russiske utenriksdepartementet pressekonferanser som ytterligere sådde falske påstander om amerikanske biolaboratorier, i informasjonsmiljøet. Russiskstøttede team jobbet deretter for å ytterligere forsterke fortellingen på sosiale medier og internettsider.

Vi ser autoritære regimer rundt om i verden som jobber sammen for å forurense informasjonsøkosystemet til gjensidig fordel. Gjennom hele COVID-19-pandemien gjennomførte for eksempel Russland, Iran og Kina propaganda- og påvirkningsoperasjoner ved å bruke en blanding av åpenlyse, halvskjulte og skjulte spredningsmetoder for å målrette mot demokratier og ytterligere geopolitiske mål (drøftet nærmere på side 76). De tre regimene spilte på hverandres meldings- og informasjonsøkosystemer for å fremme foretrukne narrativer. Mye av denne dekningen besto av kritikk eller konspirasjonsteorier om USA og deres allierte, drevet av offisielle uttalelser fra myndighetspersoner, samtidig som de promoterte sine egne vaksiner og svar på COVID-19 som overlegne i forhold til USA og andre demokratier. Ved å forsterke hverandre skapte statlige medier et økosystem der negativ dekning av demokratier – eller positiv dekning av Russland, Iran og Kina – produsert av ett statlig medium som ble forsterket av andre.

Illustrasjon av hvordan narrativer om amerikanske biolaboratorier og biologiske våpen spredte seg via de tre brede fasene med mange utenlandsk påvirkningsoperasjoner – forhåndsposisjonering, lansering og forsterkning.

Trender i cyber-påvirkningsoperasjoner

Fortsettelse

En ting som gjør det hele mer utfordrende, er at teknologienheter i privat sektor ubevisst kan legge til rette for disse kampanjene. Aktiverere kan inkludere selskaper som registrerer internettdomener, driver nettsteder, promoterer materiale på sosiale medier og søkesider, kanaliserer trafikk og hjelper til med å betale for disse øvelsene gjennom digital annonsering. Organisasjoner må være klar over verktøyene og metodene som brukes av autoritære regimer for cyberpåvirkningsoperasjoner, slik at de kan oppdage og deretter forhindre spredning av kampanjer. Det er også et økende behov for å hjelpe forbrukere med å utvikle en mer sofistikert evne til å identifisere utenlandske påvirkningsoperasjoner og begrense engasjementet sitt med deres fortellinger eller innhold.

Cyberpåvirkningsoperasjoner, inkludert autoritær propaganda, er en trussel mot demokratier over hele verden ettersom de eroderer tilliten, øker polariseringen og truer demokratiske prosesser.

Økt koordinering og informasjonsdeling på tvers av myndigheter, privat sektor og sivilsamfunn er nødvendig for å øke åpenheten og for å avsløre og forstyrre disse påvirkningskampanjene.

Globalt bekymrer tre fjerdedeler av de spurte seg for hvordan informasjon brukes som våpen.

Søkelys på påvirkningso-perasjoner under COVID-19 og Russlands invasjon av Ukraina

Nasjonalstater som søker å kontrollere informasjonsmiljøet gjennom hele pandemien og under den russiske invasjonen av Ukraina, gir sterke eksempler på hvordan autoritære regimer blander cyber- og informasjonsoperasjoner.

COVID-19-propaganda

Russland, Iran og Kina brukte propaganda- og påvirkningskampanjer gjennom hele COVID-19-pandemien. COVID-19 hadde en fremtredende plass i disse kampanjene på to sentrale måter:

1. Representasjoner av selve pandemien.
2. Kampanjer som brukte COVID-19 som et strategisk verktøy for å oppnå bredere politiske mål.

Det brede målet med denne typen kampanjer er todelt: for det første å undergrave demokratier, demokratiske institusjoner og bildet av USA og dets allierte på den globale scenen, og for det andre å styrke sin egen anseelse nasjonalt og internasjonalt.

Et eksempel på dette kan sees i meldingene fra kjente russiske kontoer og medieorganisasjoner rettet mot engelskspråklige lesere versus hvordan den russiske regjeringen kommuniserte med sine egne innbyggere angående vaksinen og alvorlighetsgraden av COVID-19.

Emner dekket av de 10 mest sette koronavirushistoriene på RT.com
(oktober 2021–april 2022)

Antivaksinepropaganda retter seg mot ikke-russiske lesere

Russisk (oversatt nedenfor til norsk)	Engelsk
«Lockdown og boostere forhindrer overføring»	«Vaksinasjoner klarer ikke å dempe smitte og er ineffektive mot nye stammer»
«Russiske myndighetspersoner tester positivt»	«Pfizer-vaksinen har farlige bivirkninger»
«Antall tilfeller og dødsfall øker i Russland»	«Massevaksinasjon er politisk motivert»
«Sputnik V-vaksinen er svært effektiv»	«Pfizer og Moderna gjennomfører ukontrollerte forsøk»
«Det kreves vaksinebevis på offentlig transport»	

Russiske COVID-19-meldinger varierer fra språk til språk.

Kampanjer som forsøkte å skjule opprinnelsen til COVID-19-viruset er et annet eksempel. Siden starten av pandemien har russisk, iransk og kinesisk COVID-19-propaganda økt dekningen fra de andre for å forsterke disse sentrale temaene. Mye av denne dekningen besto av å fremme kritikk eller konspirasjonsteorier om USA. Ved å jevnlig forsterke hverandre utviklet statlige medier et økosystem der negativ dekning av demokratier eller positiv dekning av Russland, Iran og Kina fra ett statlig medium ble forsterket av de andre gang på gang.

Ett slikt eksempel er det tidlige forslaget fra russiske og iranske statlige medier om at COVID-19 kan være et biovåpen laget av USA. Denne påstanden kom på nettsteder med løse konspirasjoner tidlig i pandemien etter et intervju med en jussprofessor som hevdet at COVID-19 ble laget som et våpen.[6] Etter at intervjuet ble publisert på noen nettsteder med begrenset rekkevidde, ble historien hentet frem av statlig eide medier. PressTV, en iransk engelsk- og franskspråklig nyhetsformidler, sponset av den iranske regjeringen,[7] publiserte en engelskspråklig artikkel i februar 2020 med tittelen «Er coronavirus et amerikansk biokrigføringsvåpen slik Francis Boyle tror?». Artikkelen antydet at USA sto bak COVID-19-utbruddet, og skrev: i alle amerikanske kriger brukes radiologiske, kjemiske, biologiske og andre forbudte våpen, noe som påfører mennesker i målrettede områder en ødeleggende lidelse.[8] Russiske statlige medier og kinesiske regjeringskontoer gjentok påstanden. Russia Today (RT) – en statseid nyhetsformidler kjent for sin rolle i å spre Kreml-propaganda[9] – publiserte minst én historie som fremmet uttalelser fra iranske tjenestemenn som hevdet at COVID-19 kan være et «produkt av USAs biologisk angrep rettet mot Iran og Kina»[10] og sendte ut innlegg på sosiale medier som antydet det samme. En RT-tweet fra 27. februar 2020 lød for eksempel: «Håndsopprekning, hvem bli ikke overrasket om det noen gang blir avslørt at #coronavirus er et biovåpen?»[11]

Krigen i Ukraina – propaganda som krigsvåpen

Russlands invasjon av Ukraina gir et tydelig eksempel på hvordan cyberpåvirkning-soperasjoner kan smeltes sammen med mer tradisjonelle cyberangrep og militære operasjoner på bakken for å maksimere effekten av dem.

I forkant av invasjonen av Ukraina så Microsofts trusseletterretningsanalytikere minst seks separate Russland-vennlige aktører starte mer enn 237 cyberangrep mot Ukraina. Disse kampanjene forsøkte å forringe tjenester og institusjoner, forstyrre ukrainernes tilgang til pålitelig informasjon og så tvil om landets lederskap.

Søkelys på påvirkningsoperasjoner under COVID-19 og Russlands invasjon av Ukraina

Fortsettelse

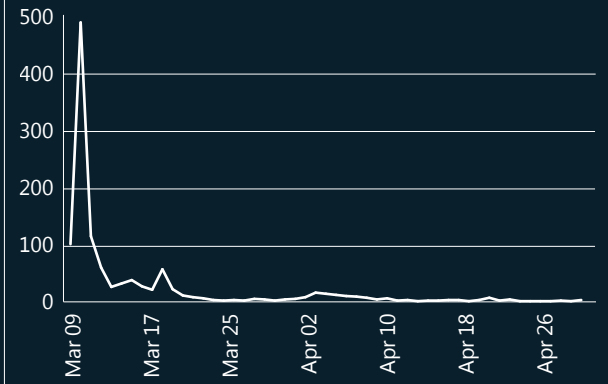
I en Microsoft-rapport utgitt i april 2022 viste vi hvordan Russland i et tilsynelatende forsøk på å kontrollere informasjonsmiljøet i Kiev satte i gang et missilangrep mot et TV-tårn i Kiev samme dag som det lanserte en destruktiv skadevare mot et stort ukrainsk mediaselskap.[12]

I et annet eksempel på hvordan cyberangrep og påvirkningsoperasjoner løper sammen, sendte en russisk trusselaktør e-poster som ble påstått å være fra innbyggere i Mariupol, til ukrainske borgere, og ga den ukrainske regjeringen skylden for eskalering av krigen og oppfordret sine landsmenn til å slå tilbake mot regjeringen. Disse e-postene ble spesifikt adressert (med navn) til de som mottok e-posten, noe som indikerer at personopplysningene deres kan ha blitt stjålet i et tidligere spionasjerelatert cyberangrep. Ingen ondsinnede lenker ble inkludert, noe som tyder på at hensikten var rene påvirkningsoperasjoner.

Å vise til påstått hacket, lekket eller på annen måte sensitivt materiale er en vanlig taktikk brukt av russiske aktører i påvirkningsoperasjoner. Gjennom krigen i Ukraina har prorussiske sosiale medier-kanaler promotert det de hevder er lekket eller på annen måte sensitivt materiale fra ukrainske kilder. Lekket eller sensitivt materiale brukes av prorussiske sosiale medier-kanaler og publiseringskanaler som en del av en bredere påvirkningsstrategi for å svekke tilliten til institusjoner og så tvil om tradisjonelle fortolkninger. Denne informasjonen kan manipuleres for å lage propaganda rettet mot Ukraina og Vesten, redusere tilliten til digital sikkerhet og redusere støtten til vestlig bistand til Ukraina.

Russland brukte andre informasjonsangrep for å forme opinionen etter hendelser på bakken for å skjule eller undergrave fakta. 7. mars forhåndsposisjonerte Russland en fortelling gjennom en sak om FN og at et fødesykehus i Mariupol i Ukraina var blitt tømt og brukt som et militært kvarter. 9. mars bombet Russland sykehuset. Etter at nyheten om bombingen ble spredt, tvitret Russlands FN-representant Dmitry Polyanskiy at dekningen av bombingen var «falske nyheter» og siterte Russlands tidligere påstander om den påståtte militære bruken av sykehuset. Russland dekket deretter denne fortellingen bredt på russiskkontrollerte nettsteder i to uker etter angrepet på sykehuset.

Domener med trafikk
(9. mars 2022–30. april 2022)



Propagandanettsteder publiserte historier om fødesykehuset i omtrent to uker etterfulgt av en kort gjenopplivningsperiode som startet 1. april 2022. Kilde: Microsoft AI for Good Lab.

Satellittbilder av et fødesykehus i Mariupol i februar og mars 2022

Microsofts egen satellittbildeanalyse viste at fødselssykehuset ble bombet. Det første bildet er fra 24. februar 2022 og det andre er fra 24. mars 2022. Fotokilde: Planet Labs.

Russlands hvitvasking av grusomheter har fortsatt etter hvert som krigen har utviklet seg. I slutten av juni 2022 fremstilte for eksempel russiske medier og influencere bombingen av et kjøpesenter som berettiget og nødvendig, og hevdet feilaktig at det ikke var i bruk som et kjøpesenter, men snarere var i bruk som et våpenlager for ukrainske territorielle forsvarsstyrker. [13] Flere pro-Kreml-bloggere på Telegram la ut innhold som forsterket «falsk flagg»-fortellingen, med bloggere som pekte på påståtte indikatorer på fabrikasjon, inkludert tilstedeværelsen av mennesker i militæruniform i opptak fra åstedet[14] og fraværet av kvinner i opptakene.[15] Russland lanserte kampanjer ved å stole på et innebygd system av propagandabudbringere og medier. Forsterkningen av disse historiene på nettet gir Russland muligheten til å avlede skyld på den internasjonale scenen og unngå å bli stilt til ansvar.

Nasjonalstater som Russland, forstår verdien av å bruke informasjon hentet fra lukkede kilder for å påvirke offentlige oppfatninger gjennom «hack og lekk»-kampanjer for å spre motfortellinger og så mistillit.

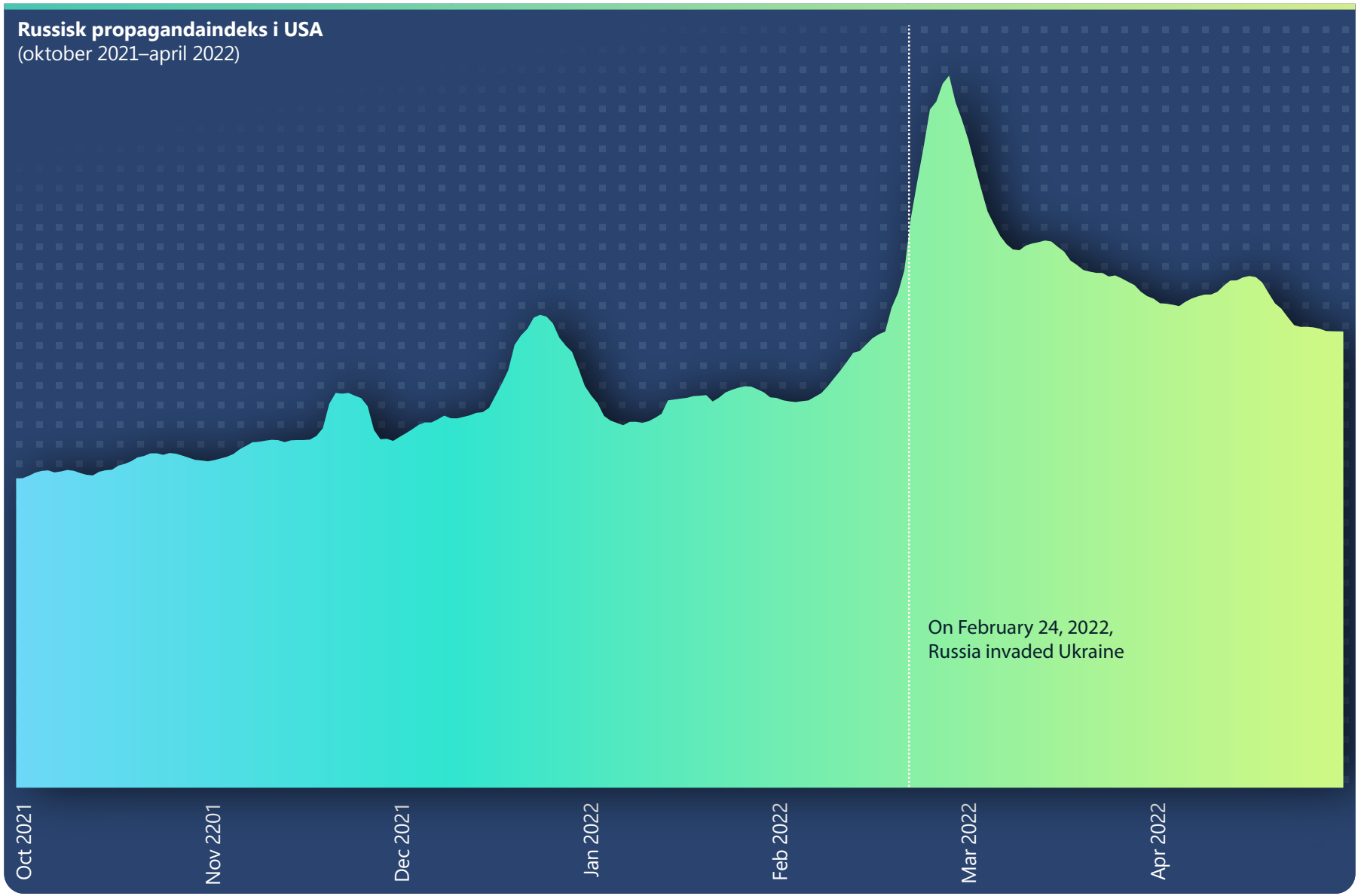
Koblinger til mer informasjon

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- En oversikt over Russlands cyberangrepsaktivitet i Ukraina | Microsoft Special Report
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues

Sporing av den russiske propagandaindeksen

I januar 2022 henviste nesten tusen amerikanske nettsteder trafikk til russiske propagandanettsteder. De vanligste temaene for russiske propagandanettsteder rettet mot et amerikansk publikum var krigen i Ukraina, amerikansk innenrikspolitikk (enten pro-Trump eller pro-Biden) og covid-19 og vaksinerelaterte fortellinger.

Den russiske propagandaindeksen (RPI) overvåker strømmen av nyheter fra russiske statskontrollerte og statsstøttede nyhetskanaler og forsterkere som en andel av den totale nyhetstrafikken på internett. RPI-en kan brukes til å kartlegge forbruket av russisk propaganda over internett og i forskjellige geografiske områder på en presis tidslinje. Microsoft bemerker imidlertid at vi bare kan observere den russiske propagandaen som er lagt ut på allerede identifiserte nettsteder. Vi har ikke innsikt i propaganda på andre typer nettsteder, inkludert autoritative nyhetsnettsteder, uidentifiserte nettsteder og sosiale nettverksgrupper.



Sporing av den russiske propagandaindeksen

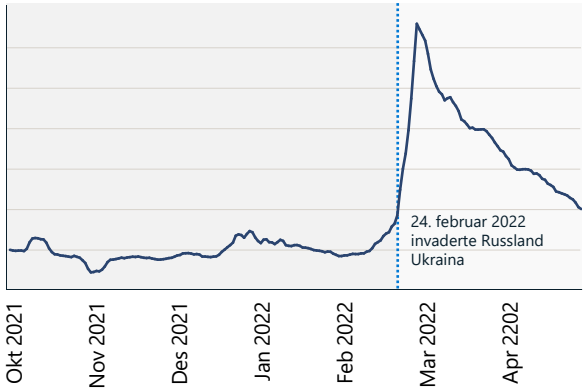
Fortsettelse

Russisk propagandaindeks: Ukraina

Da Ukraina-krigen begynte, så vi en økning på 216 prosent i russisk propaganda, med en topp 2. mars. Diagrammet nedenfor viser hvordan denne plutselige økningen falt sammen med invasjonen. De to grafene viser hvordan russisk propaganda økte like etter at invasjonen begynte.

RPI, Ukraina

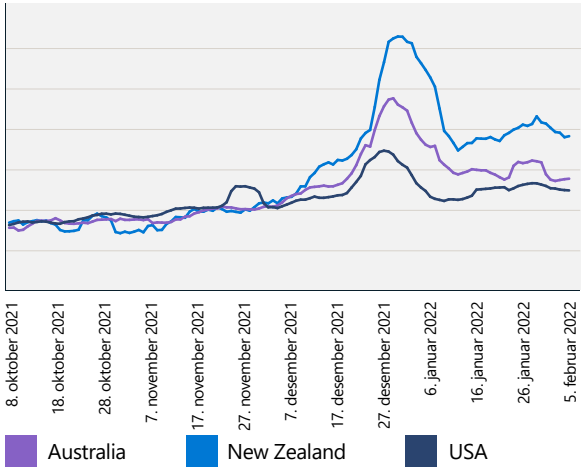
(7. oktober 2021–30. april 2022)



Russisk propagandaindeks: New Zealand vs. Australia og USA

En vurdering av RPI i New Zealand viste en topp mot slutten av 2021 som var relatert til COVID-19-propaganda. Denne økningen i russisk propagandaforbruk i New Zealand gikk forut for en økning i offentlige protester tidlig i 2022 i Wellington. En annen topp var tydelig relatert til den russiske invasjonen av Ukraina og overgikk RPI-ene til Australia og USA.

RPI, New Zealand vs. Australia og USA



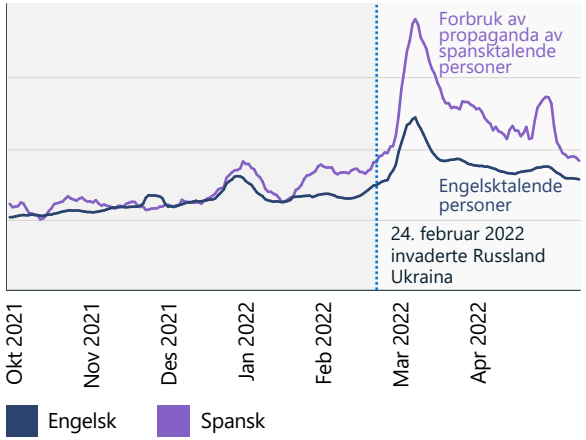
Russisk propagandaforbruk i New Zealand ligner på Australia frem til den første uken i desember 2021. Etter desember økte det russiske propagandaforbruket i New Zealand med over 30 prosent i forhold til forbruket i Australia og USA.

Russisk propagandaindeks i USA: engelsk og spansk

RPI sporer også propaganda på tvers av språk. Flere publiseringskanaler, inkludert RT og Sputnik News, er tilgjengelig på over 20 språk. Disse inkluderer engelsk, spansk, tysk, fransk, gresk, italiensk, tsjekkisk, polsk, serbisk, latvisk, litauisk, moldavisk, hviterussisk, armensk, ossetisk, georgisk, aserbajdsjansk, arabisk, tyrkisk, persisk og dari.

Følgende graf viser at RPI for spanskspråklige nyheter i USA er mye høyere enn for engelskspråklige nyheter.

Russisk propagandaforbruk er to ganger høyere blant spansktalende



Russisk propagandaforbruk i USA er to ganger høyere blant spansktalende.

Russisk propaganda er omfattende i Latin-Amerika

RT på spansk er det internasjonale nyhetsmediet med flest sidevisninger og Facebook-følgere.

Kilde: Microsoft AI for Good Research Lab

Syntetiske medier

Vi går inn i en gyllen æra for AI-aktivert medieskaping og manipulasjon. Microsoft-analytikere bemerker at dette er drevet av to hovedtrender: spredningen av brukervennlige verktøy og tjenester for kunstig å lage svært realistiske syntetiske bilder, videoer, lyd og tekst, og muligheten til raskt å spre innhold optimalisert for spesifikke målgrupper.

Ingen av disse utviklingene er iboende problematiske i seg selv. AI-basert teknologi kan brukes til å lage morsomt og spennende digitalt innhold, enten det er laget rent syntetisk eller er en forbedring av eksisterende materiale. Disse verktøyene blir mye brukt av bedrifter i reklame og kommunikasjon, og av enkeltpersoner for å lage engasjerende innhold for følgerne sine. Når syntetiske medier opprettes og distribueres med den hensikt å skade, har de imidlertid potensial til å gjøre alvorlig skade på enkeltpersoner, selskaper, institusjoner og samfunnet. Microsoft har vært en pådriver for å utvikle teknologier og retningslinjer, både internt og på tvers av det bredere medieøkosystemet, for å begrense denne skaden.

Denne delen utforsker innsikt fra Microsoft-analyser om den nåværende toppmoderne teknologien for å lage skadelig syntetisk innhold, skadene som kan oppstå hvis dette innholdet spres bredt, og tekniske avbøtende tiltak som kan være et forsvar mot cybertrusler basert på syntetiske media.

Skaping av syntetiske medier

Feltet for syntetisk tekst og medier utvikler seg utrolig raskt ettersom teknikker som en gang bare var mulig med de enorme dataressursene til store filmstudioer, nå er integrert i telefonapper. Samtidig blir verktøy enklere å bruke og kan generere innhold med et nivå av realisme som kan lure selv tekniske mediespesialister. Vi er svært nær punktet der hvem som helst kan lage en syntetisk video av hvem som helst, som sier eller gjør hva som helst. Det er ikke urimelig å tro at vi går inn i en tidsalder der en betydelig mengde av innholdet vi ser på nettet er helt eller delvis syntetisk laget ved bruk av AI-teknikker.

> Med tilgjengeligheten av mer sofistikerte, brukervennlige og allment tilgjengelige verktøy, øker produksjonen av syntetisk innhold og det vil snart være umulig å skille det fra virkeligheten.

Det finnes mange fritt tilgjengelige og kommersielle bilde-, video- og lydredigeringsverktøy av høy kvalitet. Disse verktøyene kan brukes til å gjøre enkle, men potensielt skadelige endringer i digitalt innhold, som å legge til villedende tekst, bytte ansikter og fjerne eller endre kontekst. Slike "billige forfalskninger" er mye brukt for å spre ondsinnet innhold, fremme politiske ideologier og skade omdømmer. Et velkjent eksempel er videoen fra 2019[16] der talen til Nancy Pelosi, speakeren i Representantenes hus, ble gjort grøtete slik at hun fremsto som beruset. Selv om det raskt ble avslørt at videoen ble spilt på lav hastighet for å skape effekten, spredte den «billige forfalskningen» seg vidt før den originale videoen og konteksten dukket opp.

Mer sofistikerte tilnærminger for å endre medieinnhold inkluderer bruk av avanserte AI-teknikker for å (a) lage rent syntetiske medier og (b) gjøre mer sofistikerte redigeringer av eksisterende medier. Begrepet deepfake brukes ofte om syntetiske medier som er laget ved hjelp av banebrytende AI-teknikker (navnet kommer fra de dype nevrale nettverkene som noen ganger brukes). Disse teknologiene blir utviklet som frittstående apper, verktøy og tjenester og integrert i etablerte kommersielle redigeringsverktøy basert på åpen kildekode.

Slike teknologier gjøres til våpen av uhederlige aktører som håper å skade enkeltpersoner og institusjoner. Eksempler på deepfake-teknikker inkluderer:

- **Ansiktsbytte (video, bilder)** – å erstatte et ansikt i en video med et annet. Denne teknikken kan brukes til å forsøke utpressing av en person, bedrift eller institusjon, eller for å plassere enkeltpersoner på pinlige steder eller i pinlige situasjoner.
- **Dukkespill (video, bilder)** – bruk av en video for å animere et stillbilde eller en annen video. Dette kan få det til å virke som en person sa noe pinlig eller misvisende.
- **Generative motstridende nettverk (video, bilder)** – en familie av teknikker for å generere fotorealistiske bilder.
- **Transformasjonsmodeller (video, bilder, tekst)** – skaping av rike bilder fra tekstbeskrivelser.

Slike avanserte AI-baserte teknikker er ennå ikke mye brukt i cyberpåvirkningskampanjer, men vi forventer at problemet kommer til å vokse etter hvert som verktøyene blir enklere å bruke og mer tilgjengelig.

Virkningen av manipulasjon av syntetiske medier

Bruken av informasjonsoperasjoner for å forårsake skade eller utvide innflytelse er ikke ny. Men hastigheten som informasjon kan spre seg med, og den manglende evnen vår til raskt å sortere fakta fra fiksjon, betyr at virkningen og skaden forårsaket av forfalskninger og andre syntetisk genererte ondsinnede medier kan bli mye større, som vist med Pelosi-eksemplet.

Det er flere kategorier av skader som vi vurderer: markedsmanipulasjon, betalingssvindel, vishing, etterligning, merkevareskade, omdømmeskade og botnett. Mange av disse kategoriene har mange eksempler fra den virkelige verden, noe som kan undergrave evnen vår til å skille fakta fra fiksjon.

En langsiktig og mer lumsk trussel er rettet mot forståelsen vår av hva som er sant hvis vi ikke lenger kan stole på det vi ser og hører. På grunn av dette kan ethvert kompromitterende bilde, lyd eller video av en offentlig eller privat person avvises som falske – et utfall kjent som «Løgnerens utbytte».[17] Nylig forskning[18] viser at dette misbruket av teknologi allerede brukes til å angripe finansielle systemer, selv om mange andre misbruksscenarioer er sannsynlig.

Syntetiske medier

Fortsettelse

Oppdagelse av syntetiske medier

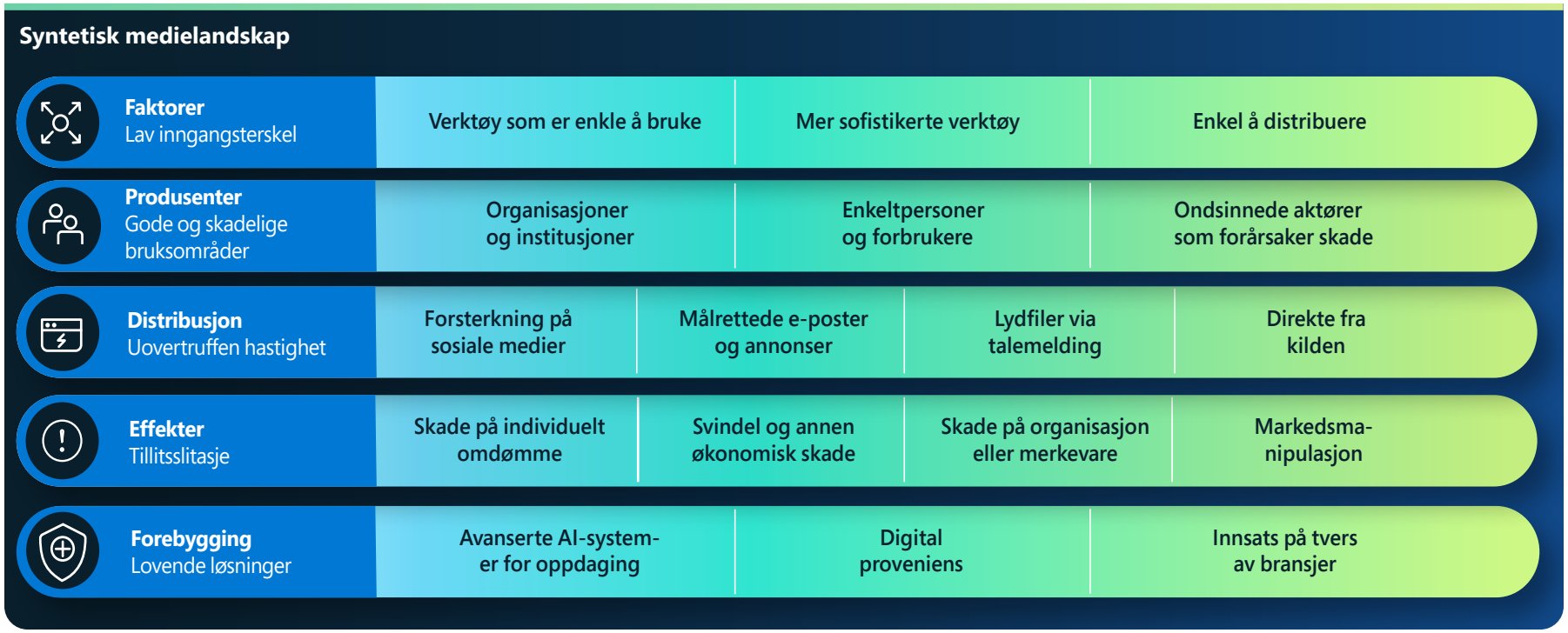
Arbeid er i gang på tvers av industri, myndigheter og akademia for å utvikle bedre måter å oppdage og redusere syntetiske medier på og gjenopprette tillit. Det er flere lovende veier fremover, samt barrierer som krever vurdering.

En tilnærming er å bygge AI-baserte systemer som kan oppdage forfalskninger – i hovedsak «defensive» AI-systemer for å motvirke de offensive AI-systemene. Dette er et område med aktiv forskning der gjeldende systemer for å lage syntetisk lyd og video etterlater avslørende artefakter som kan oppdages av trente tekniske medieanalytikere og automatiserte verktøy.

Dessverre, mens gjeldende forfalskninger har avslørende feil, har de nøyaktige artefaktene en tendens til å være spesifikke for et bestemt verktøy eller algoritme. Dette betyr at trening på kjente forfalskninger vanligvis ikke generaliserer til andre algoritmer, slik det ble demonstrert i en åpen konkurranse i 2020 for å bygge deepfake-bildedetektorer.[19] Det er fristende å øke investeringene i å utvikle mer avanserte detektorer, men Microsoft er svært skeptisk til at dette vil resultere i meningsfulle forbedringer av to grunner:

For det første har vi utmerkede fysiske modeller som gjenspeiler den virkelige verden. Nåværende falske skapere kutter hjørner, noe som resulterer i artefakter som kan oppdages, men nyere modeller blir stadig mer realistiske. Det er ikke noe spesielt med en virkelig scene tatt av et kamera som ikke kan modelleres av en datamaskin.

For det andre bruker avanserte falske opprettingsalgoritmer en teknikk kalt Generative Adversarial Networks (GANs) som en del av opprettelsesprosessen. En GAN spiller to AI-systemer mot hverandre ved å bruke en generator for å lage det falske og en diskriminator for å oppdage falske bilder og trene generatoren. Enhver investering i å utvikle en bedre detektor vil bare gjøre det mulig for generatoren å forbedre kvaliteten på forfalskningene.



Syntetiske medier

Fortsettelse

Opprinnelse for digitale aktiva

Hvis det er vanskelig å oppdage forfalskninger, hva kan gjøres for å beskytte mot skadelig bruk av syntetiske medier? En viktig fremvoksende teknologi er digital proveniens – en mekanisme som gjør det mulig for digitale medieskapere å sertifisere en eiendel og hjelper forbrukere å identifisere hvorvidt den digitale eiendelen har blitt tuklet med eller ikke. Digital proveniens er spesielt viktig i sammenheng med dagens sosiale medier-nettverk gitt hastigheten som innhold kan spres på via internett og muligheten for uhederlige aktører til enkelt å manipulere innhold.

900 %

år-over-år-økning i spredning av deepfake siden 2019.[20]

Digital Provenance Technology er en moderne versjon av kryptografisk dokumentsignering, designet for å fange opp kilden, redigere historie og metadata til objekter mens de flyter gjennom dagens internett. Visjonen og de tekniske metodene for å muliggjøre denne typen ende-til-ende-manipulasjonssikker sertifisering av medier ble utviklet av et tverrfaglig team av forskere og vitenskapsfolk hos Microsoft. Vi er en av lederne i et tverrindustrielt partnerskap som tar sikte på å bringe medieprovenienssteknologi til live i Project Origin (grunnlagt av Microsoft, BBC, CBC/Radio-Canada og New York Times) og engasjerer oss i Content Authenticity Initiative (grunnlagt av Adobe). Microsoft jobbet også med partnere innen teknologi og medietjenester for å etablere Coalition for Content Provenance and Authenticity (C2PA). C2PA er en standardorganisasjon som nylig publiserte den mest avanserte digitale provenienssspesifikasjonen for bruk med medieressurser, inkludert bilder, videoer, lyd og tekst.

Et C2PA-aktivert objekt har et manifest som beskytter objektet og metadataene mot tukling, og det medfølgende sertifikatet identifiserer utgiveren.

Syntetiske medier ble opprinnelig ikke laget for å forårsake skade, men de blir gjort om til våpen av uhederlige aktører for å undergrave tilliten til enkeltpersoner og institusjoner.

Digital proveniens er en lovende fremvoksende teknologi som har potensial til å bidra til å gjenopprette folks tillit til nettbasert medieinnhold ved å bekrefte opprinnelsen til et medium.

Offentlig tilgjengelige løsninger basert på C2PA-spesifikasjonen dukker opp enten som en ny funksjon i eksisterende produkter eller nye frittstående apper og tjenester. Vi forventer at de fleste av de mest brukte opptaks-, redigerings- og autoriseringsverktøyene kommer til å være C2PA-aktivert om få år. Dette gir en mulighet for bedrifter til å bestemme sitt behov og bruk for digital proveniens i dag, og å kreve dette ekstra beskyttelseslaget i verktøyene de bruker i eksisterende arbeidsflyter.

Handlingsbar innsikt

1. Ta proaktive skritt for å beskytte organisasjonen din mot trusler mot feilinformasjon gjennom proaktiv vurdering av PR- og kommunikasjonssvar.
2. Bruk provenienssteknologi for å beskytte offisiell kommunikasjon.

Koblinger til mer informasjon

- Et lovende skritt fremover for å hindre desinformasjon | Microsoft On the Issues
- En milepæl er nådd, 31. januar 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Utforsk tekniske detaljer om systemet Project Origin bruker for mediegodkjenning | Microsoft ALT Innovation

En helhetlig tilnærming for å beskytte mot cyberpåvirknings-operasjoner

Microsoft bygger på sin allerede modne infrastruktur for cybertrusseletterretning for å utvikle et bredere, mer inkluderende syn på cyberpåvirkningsoperasjoner.

Vi bruker et rammeverk for foreslått respons og avbøtende strategier for å bekjempe trusselen fra operasjoner, som kan deles inn i fire hovedpilarer: oppdage, forstyrre, forsvare og avskrekke.

I tillegg har Microsoft tatt i bruk fire prinsipper for å forankre arbeidet vårt på dette området. Det første er en forpliktelse til å respektere ytringsfriheten og opprettholde kundenes evne til å opprette, publisere og søke etter informasjon via plattformene, produktene og tjenestene våre. For det andre jobber vi proaktivt for å forhindre at plattformene og produktene våre brukes til å forsterke utenlandske nettsteder og innhold som har til hensikt å drive cyberpåvirkning. For det tredje vil vi ikke med vilje tjene på utenlandsk cyberpåvirkningsinnhold eller aktører. Til slutt prioriterer vi å vise frem innhold for å motvirke utenlandske cyberpåvirkningsoperasjoner ved å bruke interne og pålitelige tredjepartsdata på produktene våre.

Oppdage

Som med cyberforsvar, er det første trinnet i å motvirke utenlandsk cyberpåvirkningsoperasjoner å utvikle kapasiteten til å oppdage dem. Ingen enkelt bedrift eller organisasjon kan håpe på å oppnå den fremgangen som er nødvendig individuelt. Nytt, bredere samarbeid på tvers av teknologisektoren kommer til å være avgjørende, med fremgang i å analysere og rapportere cyberpåvirkningsoperasjoner som i stor grad er avhengige av sivilsamfunnets rolle, inkludert akademiske institusjoner og ideelle organisasjoner.

Ved å anerkjenne denne rollen har forskerne Jake Shapiro og Alicia Wanless ved henholdsvis Princeton University og Carnegie Endowment for International Peace kartlagt planene for å lansere det nye "Institute for Research on the Information Environment" (IRIE). Med støtte fra Microsoft, Knight Foundation og Craig Newmark Philanthropies skal IRIE opprette en inkluderende forskningsinstitusjon med flere interessenter etter modell av European Organization for Nuclear Research (CERN). Den kommer til å kombinere ekspertise innen databehandling og analyse for å fremskynde og skalere nye funn innen dette området. Funnene blir delt for å informere beslutningstakere, teknologiselskaper og forbrukere mer bredt.

Forsvare

Den andre strategiske pilaren er å styrke demokratiske forsvar, en langvarig prioritet med behov for investeringer og innovasjon. Den bør ta hensyn til utfordringene teknologien har skapt for demokratiet, og mulighetene teknologien har skapt for å forsvare demokratiske samfunn mer effektivt.

Microsofts strategirammeverk er rettet mot å hjelpe tverrsektorielle interessenter med å oppdage, forstyrre, forsvare og avskrekke mot propaganda – spesielt kampanjer fra utenlandske aggressorer.

Det er passende å starte med en av de store teknologiske utfordringene i vår tidsalder – virkningen av internett og digital reklame på tradisjonell journalistikk. Siden 1700-tallet har en fri og uavhengig presse spilt en spesiell rolle i å støtte ethvert demokrati på planeten – avdekke korrupsjon, dokumentere kriger og belyse de største samfunnsutfordringene i denne og i enhver annen tid. Internett har imidlertid ødelagt for lokale nyheter ved å sluke annonseinntekter og lokke bort betalte abonnenter. Mange lokalaviser er nedlagt. En av de mange innsiktene fra det siste arbeid vårt er byer som mangler en avis, ubevisst og uunngåelig utsatt for et større volum av utenlandsk propaganda enn gjennomsnittet. Av disse grunnene må en av demokratiets kritiske defensive spydspisser styrke tradisjonell journalistikk og en fri presse, spesielt på lokalt nivå. Dette krever kontinuerlige investeringer og innovasjon som må reflektere de lokale behovene til ulike land og kontinenter. Disse utfordringene er ikke enkle å løse, og de krever tilnærminger fra mange interessenter, som Microsoft og andre teknologiselskaper i økende grad støtter.

Vi trenger også nye innovasjoner innen offentlig policyer, som må være en offentlig prioritet. Dette kan inkludere lover som gjør det mulig for utgivere å forhandle om annonseinntekter kollektivt med teknologiselskaper, og lovgivning som gir skattefradrag for å frita lokale redaksjoner for en del av lønnsskatten for journalister de ansetter. Journalister trenger mange andre verktøy for håndverket sitt, inkludert muligheten til å skille innhold fra legitime og uredelige kilder.

Det er også et raskt voksende behov for å hjelpe forbrukere med å utvikle en mer sofistikert evne til å identifisere nasjonalstatsdrevne informasjonsoperasjoner. Selv om dette kan virke skremmende, ligner det arbeidet teknologisektoren lenge har utført for å bekjempe andre cybertrusler. Vurder opplæring av forbrukere til å se mer nøye på en e-postadresse for å hjelpe dem med å oppdage søppelpost eller annen uredelig kommunikasjon. Initiativer i USA – som for eksempel News Literacy Project og Trusted Journalism.

En langsiktig og mer lumsk trussel er rettet mot forståelsen vår av hva som er sant hvis vi ikke lenger kan stole på det vi ser og hører.

En helhetlig tilnærming for å beskytte mot cyberpåvirknings-operasjoner

Fortsettelse

Program – bidrar å utvikle bedre informerte forbrukere av nyheter og informasjon. Globalt kan ny teknologi som nettlesertilleggs-programmet fra NewsGuard bidra til å flytte denne innsatsen mye raskere fremover.

Dette bør også minne oss om at en del av grunnlaget for demokrati er en utdanning i samfunnskunnskap. Som alltid må denne innsatsen starte i skolen. Men vi lever i en verden som krever at vi får kontinuerlig samfunnsopplæring gjennom hele livet. Det nye Civics at Work-løftet, ledet av Center for Strategic and International Studies, som Microsoft var en av de første underskriverne og partnerne av, søker å gi nytt liv til samfunnskunnskap i bedriftssamfunn. Det er et godt eksempel på bredden av muligheter til å styrke vårt demokratiske forsvar.

Forstyrre

De siste årene har Microsofts Digital Crimes Unit (DCU) foredlet taktikk og utviklet verktøy for å avbryte cybertrusler – alt fra løsepengeprogramvare til botnett og nasjonalstatsangrep. Vi har tilegnet oss mange viktige lærdommer, og starter med rollen som aktiv avbryter i å motvirke et bredt spekter av nettangrep.

Når vi tenker på å motvirke cyberpåvirkningsoperasjoner, kan avbrudd spille en enda viktigere rolle, og den beste tilnærmingen til avbrudd blir tydeligere. Den mest effektive motgiften mot omfattende bedrag er åpenhet. Det er grunnen til at Microsoft økte kapasiteten til å oppdage og forstyrre påvirkningsoperasjoner fra nasjonalstater ved å kjøpe opp Miburo Solutions, et ledende cybertrusselsanalyse- og forskningsselskap som spesialiserer seg på oppdagelse av og respons på utenlandske cyberpåvirkningsoperasjoner.

Vår erfaring har vist at myndigheter, teknologiselskaper og frivillige organisasjoner bør gjenkjenne cyberangrep nøye og med rikelig bevis. Å forstå virkningen av slike forstyrrelser er avgjørende og kan være enda mer nyttig for å forstyrre cyberpåvirkning. Studer den amerikanske regjeringens informasjonsdeling i forkant av Russlands invasjon av Ukraina, som satte åpenhet inn i effektive handlinger – for eksempel å avsløre russiske planer inkludert spesifikke kampanjer som et komplott om å bruke en falsk grafisk video.

Som vist i forrige sommers publikasjon fra CyberPeace Institute i Genève om pågående cyberangrep i og utenfor Ukraina, er det en mulighet for et bredt spekter av sivilsamfunn og private organisasjoner til å fremme åpenhet knyttet til cyberpåvirkningsoperasjoner. Pålitelige rapporter om nylig oppdagede og godt dokumenterte operasjoner kan hjelpe publikum til å bedre vurdere hva de leser, ser og hører, spesielt på internett. For dette formålet vil Microsoft bygge på og utvide sine eksisterende cyberrapporter og vil gi ut nye rapporter, data og oppdateringer knyttet til det vi oppdager om cyberpåvirkningsoperasjoner, inkludert attribusjonserklæringer når det er aktuelt. Vi kommer til å publisere en årsrapport som bruker en datadrevet tilnærming for å se på tvers av selskapet på utbredelsen av utenlandske informasjonsvirksomheter og neste trinn for å sikre inkrementell forbedring. Vi vurderer også ytterligere tiltak som bygger på denne typen åpenhet.

Rollen til digital reklame er spesielt viktig, blant annet fordi reklame kan bidra til å finansiere utenlandske virksomheter og samtidig skape et utseende av legitimitet for utenlandskstøttede propagandanettsteder. Ny innsats er nødvendig for å forstyrre disse finansstrømmene.

Avskrekke

Til slutt kan vi ikke forvente at nasjoner skal endre atferd hvis ingen blir stilt til ansvar for brudd på internasjonale regler. Å håndheve slik ansvarlighet er unikt et statlig ansvar. Likevel spiller handling fra en rekke interessenter i økende grad en viktig rolle i å styrke og utvide internasjonale normer. Mer enn 30 nettbaserte plattformer, annonsører og utgivere – inkludert Microsoft – signerte EU-kommisjonens nylig oppdaterte retningslinjer for desinformasjon, og gikk med på styrkede forpliktelser for å takle denne økende utfordringen. I likhet med den nylige Paris Call, Christchurch Call og Declaration on the Future of the Internet, kan multilaterale og samarbeidende interessenter bringe sammen regjeringer og offentligheten blant demokratiske nasjoner. Regjeringer kan deretter bygge på disse normene og lovene for å fremme ansvarligheten verdens demokratier trenger og fortjener.

Gjennom rask radikal åpenhet kan demokratiske regjeringer og samfunn effektivt redusere effekten av påvirkningskampanjer ved å tilskrive kilden til nasjonalstatsangrep, informere offentligheten og bygge tillit til institusjoner.

> Vi har økt teknisk kapasitet til å oppdage og forstyrre utenlandske påvirkningsoperasjoner og er forpliktet til å rapportere transparent om disse operasjonene, som vår rapportering om cyberangrep.

Handlingsrettet innsikt

1. Implementer sterke digitale hygienepraksiser på tvers av organisasjonen.
2. Vurder måter å redusere utilsiktet aktivering av cyberpåvirkningskampanjer av dine ansatte eller forretningspraksis. Dette inkluderer å redusere henvisninger til kjente utenlandske propagandasider.
3. Støtt kampanjer for informasjonskunnskap og samfunnsengasjement som en nøkkelkomponent for å hjelpe samfunn med å forsvare seg mot propaganda og utenlandsk påvirkning.
4. Engasjer deg direkte med grupper som er relevante for din bransje som jobber med å påvirke driften.

Sluttnoter

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. Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Talskvinne for russiske UD, 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. Russia's Kremenchuk Claims Versus the Evidence—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas og Kristjan Peterson, oktober 2020

Cybersikkerhet

Å forstå risikoene og belønningene ved modernisering blir avgjørende for en helhetlig tilnærming til robusthet.

En oversikt over

cybersikkerhet

Cybersikkerhet er en viktig faktor for teknologisk suksess. Innovasjon og forbedret produktivitet kan bare oppnås ved å innføre sikkerhetstiltak som gjør organisasjoner så resiliente som mulig mot moderne angrep.

Pandemien har utfordret oss til å justere sikkerhetspraksisene og teknologiene våre for å beskytte Microsofts ansatte uansett hvor de jobber. Det siste året har trusselaktører fortsatt å dra nytte av sårbarheter eksponert under pandemien og overgangen til et hybrid arbeidsmiljø. Siden den gang har hovedutfordringen vår vært å håndtere utbredelsen og kompleksiteten til ulike angrepsmetoder og økt statlig aktivitet.

Effektiv cybersikkerhet krever en helhetlig, adaptiv tilnærming for å stå imot nye trusler mot kjernetjenester og infrastruktur.

Finn ut mer på side 89

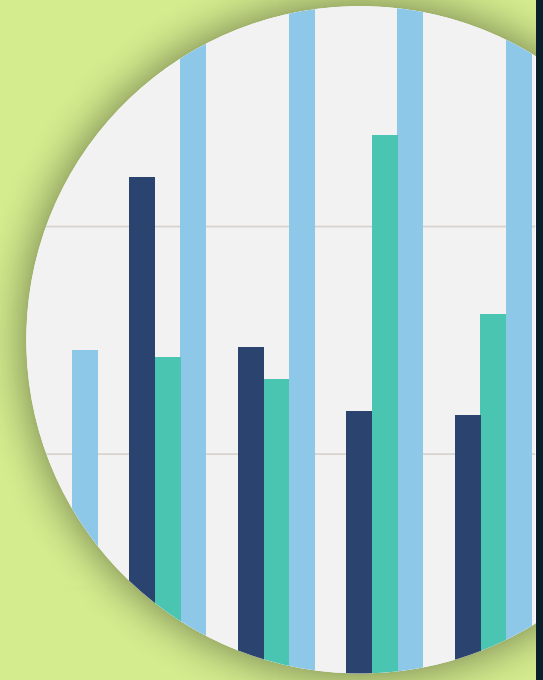
Moderniserte systemer og arkitektur er viktig for å håndtere trusler i en hyperkoblet verden.

Finn ut mer på side 90

Grunnleggende holdning til sikkerhet er en avgjørende faktor i avansert løsningseffektivitet.

Finn ut mer på side 92

Samtidig som passordbaserte angrep fortsatt er hovedkilden til kompromittering av identiteter, dukker det opp andre typer angrep.



Finn ut mer på side 93

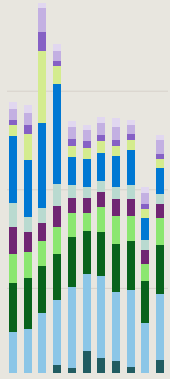
Den menneskelige dimensjonen av robusthet mot cyberpåvirkning er evnen vår til å samarbeide.

Finn ut mer på side 102

De aller fleste vellykkede cyberangrep kunne vært forhindret med grunnleggende sikkerhetshygiene.

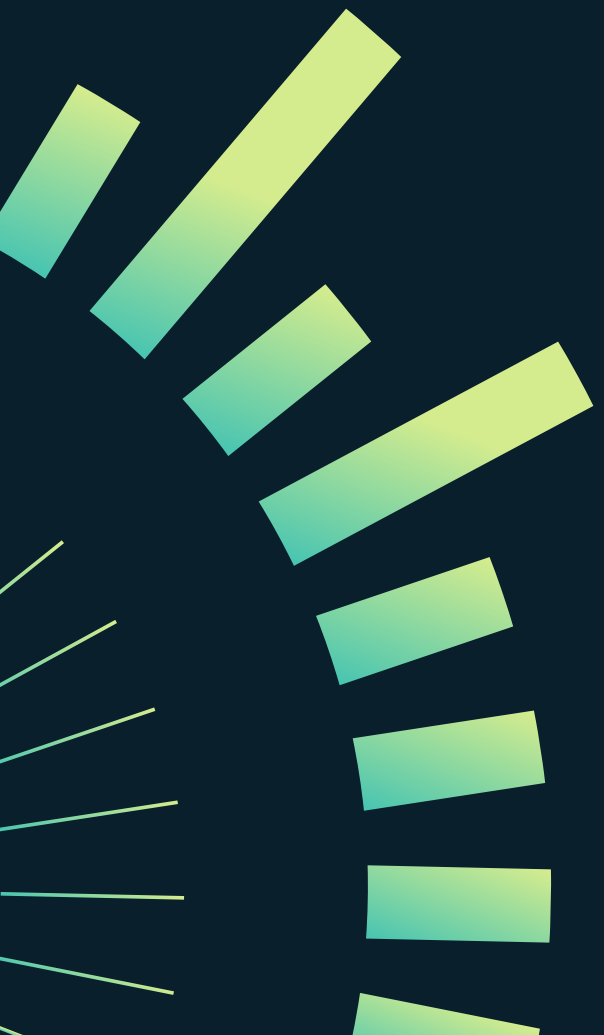
Finn ut mer på side 108

I løpet av det siste året har verden opplevd en DDoS-aktivitet som er enestående i volum, kompleksitet og frekvens.



Finn ut mer på side 98

Innledning



Pandemien utfordret oss til å justere sikkerhetspraksisene og teknologiene våre for å beskytte Microsofts ansatte uansett hvor de jobber. Det siste året har trusselaktører fortsatt å dra nytte av sårbarheter eksponert under pandemien og overgangen til et hybrid arbeidsmiljø. Siden den gang har hovedutfordringen vår vært å håndtere utbredelsen og kompleksiteten til ulike angrepsmetoder og økt statlig aktivitet.

Digital trusselaktivitet og nivået av sofistikerte cyberangrep øker hver dag. Mange av dagens komplekse angrep fokuserer på å kompromittere identitetsarkitekturer, forsyningskjeder og tredjeparter med ulik grad av sikkerhetskontroll. Spesielt har vi observert at identitetsphishing-angrep er en tydelig og tilstedeværende trussel. Denne typen angrep mislykkes imidlertid ofte hvis de møter god identitetsadministrasjon, phishing-kontroll og endepunktadministrasjonspraksis.

Som et resultat, må vi huske det grunnleggende: Nittiåtte prosent av angrepene kan stoppes med grunnleggende hygienetiltak på plass. Hos Microsoft administrerer vi identiteter og enheter som en del av vår nulltillittilnærming, som inkluderer minimale rettigheter og phishingresistente legitimasjoner for effektivt å stoppe trusselaktører og holde dataene våre beskyttet.

I dag kan selv trusselaktører som mangler sofistikerte tekniske ferdigheter sette i gang svært destruktive angrep, ettersom tilgang til avanserte taktikker, teknikker og prosedyrer blir allment tilgjengelig i nettkriminalitetøkonomien. Krigen i Ukraina demonstrerte hvordan nasjonalstatsaktører har eskalert de offensive cyberoperasjonene sine gjennom økt bruk av løsepengevirus. Løsepengevirus er nå en sofistikert bransje med trusselaktører som bruker dobbel eller trippel utpressingstaktikk for å fremtvinge utbetaling, og utviklere som tilbyr løsepengevirus som en tjeneste (RaaS). Med RaaS bruker trusselaktører et tilknyttet nettverk for å utføre angrep, noe som senker adgangsterskelen for mindre dyktige nettkriminelle og til slutt utvider angriperpoolen.

Som et resultat utviklet Microsoft et program for eliminering av løsepengevirus. Målet med programmet er å utbedre hull i kontroller og dekning, bidra til funksjonsforbedringer for tjenester og utvikle gjenopprettingshåndbøker for sikkerhetsoperasjonssenteret og ingeniørteamet vårt i tilfelle løsepengevirusangrep.

Nylige angrep på forsyningskjeden og tredjepartsleverandører indikerer et stort vendepunkt i bransjen. Forstyrrelsene disse angrepene forårsaker for kundene våre, partnere, myndigheter og Microsoft fortsetter å øke, noe som illustrerer viktigheten av fokusert oppmerksomhet på cyberresiliens og samarbeid på tvers av sikkerhetsinteressenter. Motstandere retter seg også mot lokale systemer, noe som forsterker behovet for at organisasjoner håndterer sårbarheter knyttet til eldre systemer ved å modernisere og flytte infrastruktur til skyen hvor sikkerheten er mer robust.

Vi lever i en tid der sikkerhet er en nøkkelfaktor for teknologisk suksess. Innovasjon og forbedret produktivitet kan bare oppnås ved å innføre sikkerhetstiltak som gjør organisasjoner så robuste som mulig mot moderne angrep. Etter hvert som digitale trusler øker og utvikler seg, er det avgjørende å bygge cyberresiliens inn i strukturen til hver organisasjon.

Bret Arsenault
Sjef for informasjonssikkerhet

Cybersikkerhet: Et avgjørende fundament for et tilkoblet samfunn

Revolusjonen innen digital teknologi har bidratt til at organisasjoner transformeres til å bli stadig mer tilkoblet både i måten de opererer på og i tjenestene de tilbyr. Etter hvert som truslene i cyberlandskapet øker, er det like viktig å bygge cyberresiliens inn i organisasjonens struktur som finansiell og operasjonell motstandskraft.

Digital transformasjon har for alltid endret måten organisasjoner samhandler med kunder, partnere, ansatte og andre interessenter på. Ny teknologi gir enorme muligheter til å engasjere seg med mennesker, transformere produkter og optimalisere driften. Pandemien akselererte den digitale transformasjonen ved å drive frem innovative teknologier som lar folk samarbeide på nye måter og fra hvor som helst.

Etter hvert som cybertrusler blir endemiske, blir det vanskeligere å hindre dem i å kompromittere en organisasjon i vår «alltid tilkoblede» verden. Cyberresiliens representerer en organisasjons evne til å fortsette driften og opprettholde veksten til tross for bombardementet av angrep. Forebygging må balanseres med overlevelses- og gjenopprettingsevner, og myndigheter og virksomheter utvikler omfattende modeller som strekker seg utover sikkerhet og personvern for å beskytte eiendeler, data og andre ressurser som en del av cyberresiliensen.

Utvikle en helhetlig tilnærming til cybersikkerhet

Cyberresiliens krever en helhetlig, adaptiv og global tilnærming som kan motstå stadige trusler mot kjernetjenester og infrastruktur, inkludert:

- Grunnleggende cyberhygiene som beskrevet i normalkurven vår for cybersikkerhet.
- Forstå og håndter avveiningen mellom risiko/belønning i den digital transformasjon.
- Sanntidsresponsfunksjoner som muliggjør proaktiv oppdagelse av trusler og sårbarheter.
- Beskyttelse mot kjente angrep og forebyggende aktivitet mot nye og forventede angrepsvektorer, inkludert mulighet til å utbedre automatisk.
- Redusert påvirkning av angrep og katastrofer gjennom feilisolering og segmentering.
- Automatisert gjenoppretting og redundans i tilfelle avbrudd.
- Prioritering av operasjonell testing for å finne hull og forstå delt ansvar og avhengigheter av eksterne ressurser som skybaserte sikkerhetsløsninger.

Et effektivt cyberresiliensprogram begynner med ressursgrunnlag som å forstå tilgjengelige tjenester og ha en pålitelig katalog over ressurser som kan benyttes i tilfelle avbrudd. På grunnlag av dette må programmet være i stand til å vurdere sin egen effektivitet, måle ytelsen til kritiske tjenester og deres avhengigheter, teste og validere evner på tvers av lokale tjenester og skytjenester, og levere kontinuerlig forbedring gjennom organisasjonens digitale livssyklus.

For å levere en helhetlig tilnærming samarbeider vi med organisasjoner for å identifisere deres mest kritiske lokale og nettbaserte tjenester, forretningsprosesser, avhengigheter, personell og leverandører. Vi søker også å identifisere aktiva og ressurser knyttet til kunde- og markeds-forventninger, regulatoriske og kontraktsmessige forpliktelser og interne operasjoner. Etter hvert som disse kritiske ressursene identifiseres, bør parallelle anstrengelser oppdage og overvåke trusler, forstyrrelser, potensielle angrepsvektorer og system- og prosessårbarheter. Evnen til å gjøre dette under den nåværende kompetansemangelen krever streng prioritering basert på den samlede risikoen for organisasjonen.

Denne typen helhetlig tilnærming må være tilpasningsdyktig mot et bakteppe av et trussellandskap i stadig utvikling, med et mål om å drive målbar ytelsesforbedring, redusert tid til å oppdage, reagere og gjenopprette, og redusert innvirkningsradius i tilfelle avbrudd. Tilnærmingen må også anerkjenne truslenes økende sammenheng. En sikkerhetshendelse kan for eksempel resultere i et datainnbrudd med personvernimplikasjoner, som krever at mange interne og eksterne team jobber sammen for å reagere raskt og minimere innvirkningen.

> Cybersikkerhet er en bedrifts evne til å fortsette driften og opprettholde vekstakselerasjon til tross for forstyrrelser, inkludert cyberangrep.

Handlingsrettet innsikt

1. Bygg og administrer teknologisystemer som begrenser virkningen av et innbrudd, og gjør det mulig for dem å fortsette å operere sikkert og effektivt, selv om et innbrudd lykkes. Fokuser på vanlige kritiske ressurser, støtte for smidighet og konstruer for tilpasningsevne (for eksempel hybrid og multisky, multiplattform), reduser angrepsflatene (fjern f.eks. ubrukte apper og overdrevne tilgangsrettigheter), anta at ressursene blir kompromittert og forvent at motstanderne utvikler seg.
2. Når du planlegger digitale prosjekter, bør du vurdere potensielle trusler ved siden av muligheter, og delt ansvar for resiliens på tvers av den digitale teknologiens forsyningskjede, inkludert skybaserte sikkerhetsløsninger.
3. Bygg systemer for å bygge inn sikkerhet ved design og ta skritt for å forutse, oppdage, motstå, tilpasse og svare på fremtidige trusler.
4. Sørg for at forretningsansvarlige ledere rådfører seg med sikkerhetsteam etter behov for å forstå risikoene forbundet med nye utviklinger. På samme måte bør sikkerhetsteamene vurdere forretningsmål og gi råd til lederne om hvordan de kan prøve å nå dem på en sikker måte.
5. Sørg for at klare operasjonelle fremgangsmåter og prosedyrer for organisasjonsmessig resiliens er på plass for cyberhendelser.

Viktigheten av å modernisere systemer og arkitektur

Samtidig som vi utvikler nye muligheter for en hyperkoblet verden, må vi håndtere truslene fra eldre systemer og programvare.

Eldre systemer – de som ble utviklet før moderne tilkoblingsverktøy som smarttelefoner, nettbrett og skytjenester ble normen – representerer en risiko for en organisasjon som fortsatt bruker dem. Denne risikoeksponeringen forsterkes av funnene til Microsoft Security Services for Incident Response-teamet, en gruppe sikkerhetseksperter som hjelper kunder med å svare på angrep og gjenopprette etter et angrep.

I løpet av det siste året var utfordringene hos kunder som gjenopprettet systemene etter angrep relatert til seks kategorier som vist i diagrammet på denne siden. Den følgende siden skisserer handlingsrettede tiltak for å forbedre resiliensen.

Over 80 prosent av sikkerhetshendelsene kan spores til noen få manglende elementer som kan løses gjennom moderne sikkerhetstilnærminger.

Sentrale utfordringer som påvirker cyberresiliensen

Dette diagrammet viser prosentandelen av berørte kunder som mangler grunnleggende sikkerhetskontroller som er avgjørende for å øke organisasjonens cyberresiliens. Funnene er basert på Microsoft-engasjementer det siste året.

«Ledere bør tenke på cybersikkerhet som en kritisk fasett av forretningsrobustheten. De bør planlegge for cyberforstyrrelser på samme måte som de planlegger for naturkatastrofer eller andre uforutsette hendelser og bringe sammen interne interessenter som drift, kommunikasjon, juridisk og andre, for å utforme strategier. Ved å gjøre dette bidrar de til å sikre at organisasjoner kan bringe de kritiske forretningssystemene tilbake på nettet så raskt som mulig for å gjenoppta normal forretningsdrift.

Men det stopper ikke der. Siden mange organisasjoner er avhengige av tredjepart-sleverandører og tjenesteleverandører, bør ledere utvide planleggingen av cybersikkerheten til sin ende-til-ende-verdikjede for ytterligere å sikre forretningskontinuitet og robusthet.»

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

Viktigheten av å modernisere systemer og arkitektur

Fortsettelse

Det er klare områder som organisasjoner kan adressere for å modernisere tilnærmingen sin og beskytte mot trusler:

Problem	Handlingstrinn
Usikker konfigurasjon av identitetsleverandør Feilkonfigurering og eksponering av identitetsplattformer og disses komponenter er en vanlig vektor for å få uautorisert tilgang med høye privilegier.	Følg grunnleggende sikkerhetskonfigurasjon og anbefalte fremgangsmåter når du distribuerer og vedlikeholder identitetssystemer som AD og Azure AD-infrastruktur. Implementer tilgangsbegrensninger ved å håndheve segregering av privilegier, minimale rettigheter og bruk Privileged Access Workstations (PAW) for å administrere identitetssystemer.
Utilstrekkelige tilgangsrettigheter og kontroll over sideveis bevegelser Administratorer har overdrevne tillatelser på tvers av det digitale miljøet og avslører ofte administrative legitimasjoner på arbeidsstasjoner som er utsatt for internett- og produktivitetsrisiko.	Sikre og begrense administrativ tilgang for å gjøre miljøet mer motstandsdyktig og begrense omfanget av et angrep. Bruk Privilege Access Management-kontroller, for eksempel just-in-time-tilgang og akkurat nok administrasjonsrettigheter.
Ingen flerfaktorautentisering (MFA) Dagens angripere bryter seg ikke inn, de logger seg på.	MFA er en kritisk og grunnleggende brukertilgangskontroll som alle organisasjoner bør aktivere. Hvis den kombineres med betinget tilgang, kan MFA være uvurderlig i bekjempelsen av cybertrusler.
Sikkerhetsoperasjoner med lav modenhet De mest berørte organisasjonene brukte tradisjonelle verktøy for trusseloppdagelse og hadde ikke relevant innsikt for rettidig respons og utbedring.	En omfattende strategi for trusseloppdagelse krever investeringer i utvidet oppdaging og respons (XDR) og moderne skybaserte verktøy som bruker maskinlæring, for å skille støy fra signaler. Moderniser verktøyene for sikkerhetsoperasjoner ved å innlemme XDR. Det kan gi dyp sikkerhetsinnsikt i hele det digitale landskapet.
Mangel på styring av informasjonsbeskyttelsen Mange organisasjoner strever fortsatt med å sette sammen en helhetlig styring av informasjonsbeskyttelsen som har full dekning av alle dataplasseringer, forblir effektiv gjennom hele informasjonslivssyklusen og tar hensyn til forretningskritiske data.	Identifiser de kritiske forretningsdataene og hvor de befinner seg. Gjennomgå livssyklusprosessene for informasjonen, og håndhev databeskyttelse samtidig som forretningskontinuiteten opprettholdes.
Begrenset innføring av moderne sikkerhetsrammeverk Identitet er det nye sikkerhetsperimeteret, som gir tilgang til ulike digitale tjenester og datamiljøer. Å integrere prinsipper for nulltillit, appsikkerhet og andre moderne cyberrammeverk gjør det mulig for organisasjoner å håndtere risikoer proaktivt, noe som de ellers sliter med å oppnå.	Nulltillitsrammeverk håndhever konsepter med minimale rettigheter, eksplisitt verifisering av all tilgang og antar alltid kompromittering. Organisasjonene bør også implementere sikkerhetskontroller og praksiser i DevOps og prosesser for applivssykluser for høyere sikkerhetsnivåer i forretningssystemene sine.

Grunnleggende holdning til sikkerhet er en avgjørende faktor i avansert løsningseffektivitet

I analysen vår oppdaget vi en utbredelse av vanlige blindsoner i organisatoriske forsvar som gjør det mulig for angripere å få innledende tilgang, etablere et springbrett og implementere et angrep, selv i nærvær av avanserte sikkerhetsløsninger.

I mange tilfeller fastslås utfallet av et cyberangrep lenge før angrepet begynner. Angripere utnytter sårbare miljøer for å få innledende tilgang, gjennomføre overvåking og skape kaos via sideveis bevegelse og kryptering eller eksfiltrasjon. Hvis en angriper blir stoppet på et tidlig stadium, øker muligheten til å redusere den totale effekten av angrepet vesentlig.

Microsoft undersøkte bestemte konfigurasjoner i sikkerhetsstatusene for å identifisere de vanligste manglene ved den faktiske praksisen i disse miljøene. Dette gjorde det mulig for oss å se de vanligste sårbarhetene som ble utnyttet under menneskelig ledede angrep med løsepengevirus, som gjorde at trusselaktørene kunne få tilgang til og ta seg gjennom et nettverk uoppdaget.

Grunnleggende sikkerhetskonfigurasjoner må være aktivert

Hvis enhetene til en organisasjons ikke er sikret eller er utdatert (når det gjelder sårbarheter og sikkerhetsagentstatus), fungerer de som potensielle inngangspunkter og tilgangsetableringsruter for angripere. Vi fant at selv om det er viktig å sikre at organisatoriske enheter er inkludert i en oppdatert løsning for endepunktsoppdagelse og svar[1] (EDR) og en plattform for endepunktsbeskyttelse[2] (EPP), så er dette ingen garanti for å stoppe løsepengevirus.

Avanserte løsninger som EDR og EPP er avgjørende for å oppdage en angriper tidlig i angrepsflyten og muliggjør automatisk utbedring og beskyttelse. Siden disse avanserte løsningene er avhengige av en grunnleggende evne til å oppdage et angrep, krever de likevel at grunnleggende sikkerhetskonfigurasjoner er aktivert. Vi observerte flere scenarioer hvor avanserte løsninger var på plass, men hvor løsningene ble underminert på grunn av fraværet av grunnleggende sikkerhetskonfigurasjoner.

Gode fremgangsmåter når det gjelder sikkerhetskonfigurasjoner er en viktigere indikator på resiliensen enn responstiden til analytikerne i sikkerhetsoperasjonssenteret (SOC).

Blant kundene og partnerne våre observerte vi over en seks måneders periode 70 prosent reduksjon i tiden det tar en SOC-analytiker å se og handle på et relevant varsel. Denne økte bevissthetenen er et godt tegn. Selv om synligheten av sikkerhetskonfigurasjonen forbedret SOC-analytikerens ytelse, var det å muliggjøre produktsynlighet ved å integrere og oppdatere organisasjonens enheter, en viktigere variabel for vellykket forebygging.

Risiko fra ukjente enheter

I motsetning til skynettverk, der kundene vet hvilke ressurser som kjører på hvilke operativsystemer, kan lokale nettverk inneholde en lang rekke enheter som IoT, skrivebordsmaskiner, servere og nettverksenheter som ikke overvåkes eller administreres av organisasjonen.

Et gjennomsnittlig bedriftsnettverk har over 3500 tilkoblede enheter som ikke er beskyttet av en EDR-agent, og som kan ha tilgang til bedriftsressurser eller til og med verdifulle ressurser. Microsoft Defender for endepunkt (MDE) bruker nettverksinspeksjon for å oppdage enheter og gi informasjon om enhetsklassifiseringer for de som er koblet til nettverket, for eksempel enhetsnavn, operativsystemdistribusjon og enhetstype.

3500

er det gjennomsnittlige antallet tilkoblede enheter i en bedrift som ikke er beskyttet aven endepunktdeteksjon og responsagent.

For enheter som ikke støttes av en EDR-agent, er det viktig i det minste å være klar over deres eksistens og handle for å beskytte dem ved å vurdere sårbarheter, samt begrense nettverkstilgangen.

Handlingsrettet innsikt

1. Selv avanserte løsninger kan undergraves av fravær av grunnleggende sikkerhetskonfigurasjoner.
2. Invester i anbefalte fremgangsmåter ved konfigurasjon av sikkerhetsstatus for å beskytte mot fremtidige angrep. Disse grunnleggende innstillingene gir en solid gevinst når det gjelder organisasjonens evne til å forsvare seg mot angrep.
3. Inkluder alle aktuelle enheter i en EDR-løsning.
4. Sørg for å oppdatere sikkerhetsagenter, og sikre beskyttelse mot manipulering for å muliggjøre større synlighet og bedre beskyttelsesutbytte av produkter.

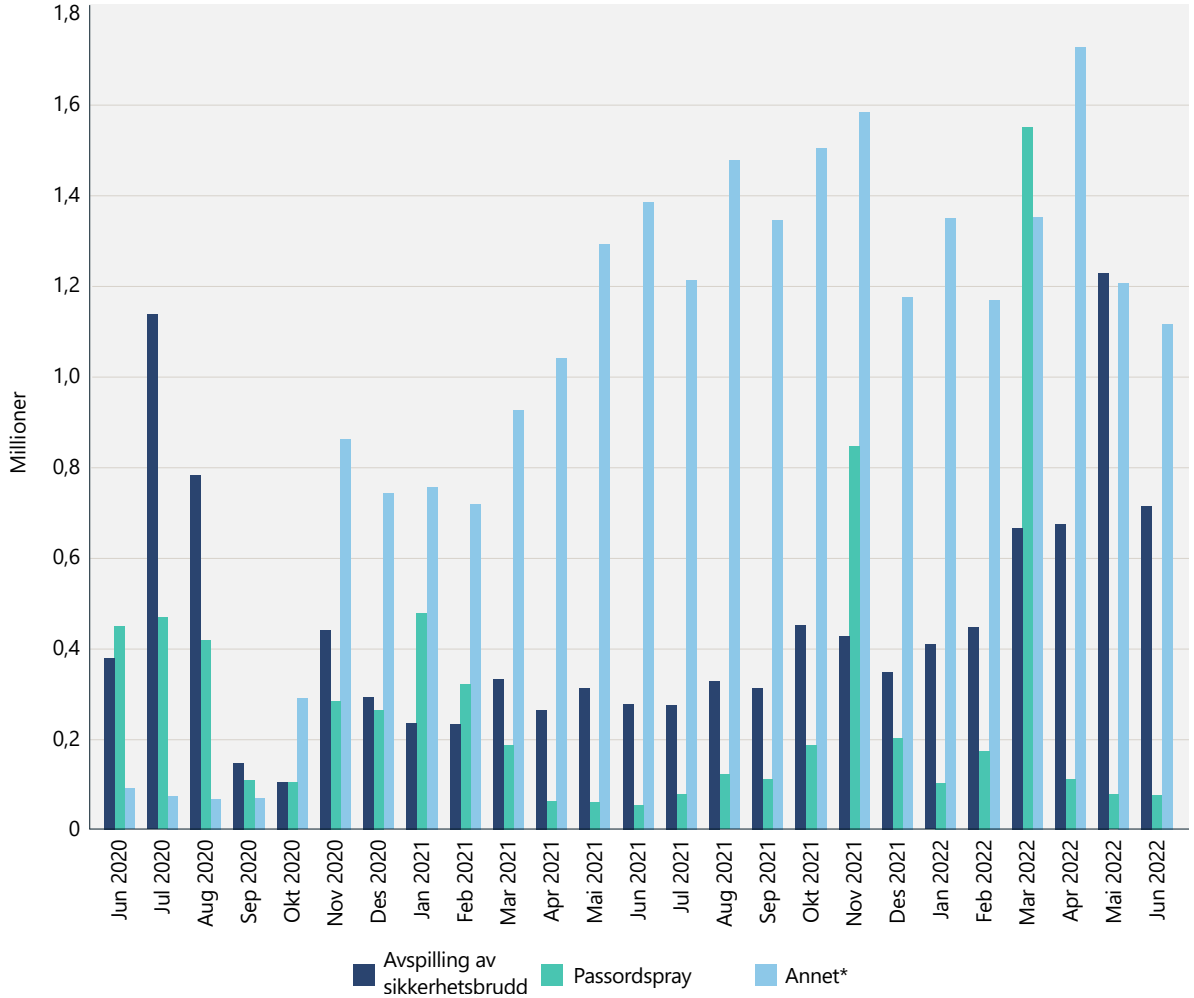
Å opprettholde god identitetshelse er helt grunnleggende for organisasjonens vel

Å ivareta identitet er viktigere enn noen gang. Samtidig som passordbaserte angrep fortsatt er hovedkilden til kompromittering av identiteter, dukker det opp andre typer angrep. Volumet av sofistikerte angrep fortsetter å øke sammenlignet med sprayangrep med passord og gjentakende brudd, som var den tidligere normen.

Passordbaserte angrep er fortsatt vanlige, og over 90 prosent av kontoene som er kompromittert via disse metodene, er ikke beskyttet med sterk autentisering. Sterk autentisering bruker mer enn én autentiseringsfaktor, for eksempel passord + SMS og FIDO2-sikkerhetsnøkler.

Vi har sett en økning i målrettede sprayangrep med passord, med svært store volum av angripertrafikk spredt over tusenvis av IP-adresser.

Brukere kompromittert etter angrepskategori



Brukere kompromittert per måned etter angrepskategori. Volumene i sprayangrepene med passord har vært svært variable, med topper i november 2021 og mars 2022. Disse toppene representerer tusenvis av brukere og tusenvis av IP-adresser som ble berørt. *«Annet» indikerer angrep som er forskjellige fra sprayangrep med passord og gjentakende brudd, inkludert phishing, skadelig programvare, mellommannbaserte angrep, kompromittering av lokal tokenutsteder med mer. Kilde: Azure AD Identity Protection.

4500

I løpet av tiden det tar å lese denne uttalelsen, har vi forsvart oss mot 4500 passordangrep.

Å opprettholde god identitetshelse er helt grunnleggende for organisasjonens vel

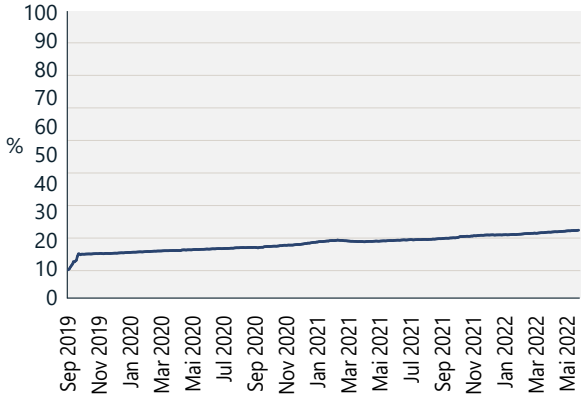
Fortsettelse

Innføring av sterk godkjenning

På en positiv måte ser vi en jevn vekst i bruk av sterk autentisering blant bedriftskundene på Azure Active Directory (Azure AD). For Azure AD vokste månedlig aktive brukere med sterk autentisering (MAU) fra 19 prosent til 26 prosent det siste året, mens sterk autentisering MAU for administrative kontoer vokste fra 30 til omtrent 33 prosent.

Denne trenden er positiv, men det er fortsatt nødvendig med betydelig vekst for å nå en majoritetsdekning av sterk autentisering. Kunder som ikke allerede bruker sterk autentisering i sine miljøer, bør starte planleggingen og distribusjonen av sterk autentisering for å beskytte brukerne sine.[3] Samtidig som det planlegges implementering av sterk autentisering, bør passordløs autentisering vurderes, siden dette gir den sikreste brukeropplevelsen ved at det eliminerer risikoen for passordangrep.

Bruk av sterk autentisering
(september 2019–mai 2022)

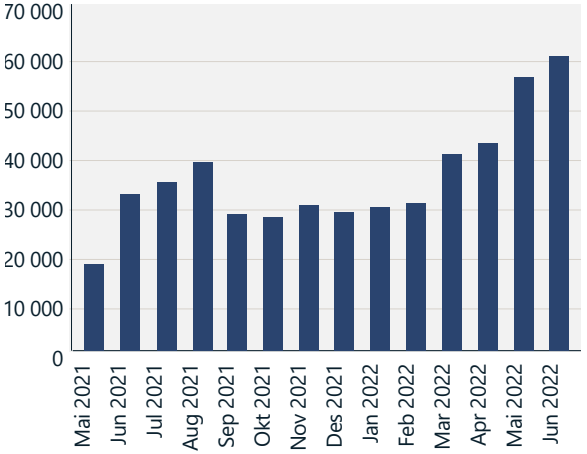


Selv om bruken av sterk autentisering har doblet seg siden 2019, bruker bare 26 prosent av brukerne og 33 prosent av administratorene sterk autentisering. Kilde: Azure Active Directory.

Jevn økning i token-svar-angrep

Andelen andre former for angrep økte i 2022. Vi så en økning i målrettede angrep som spesifikt unngår passordbasert autentisering, for å redusere sjansen for å bli oppdaget. Disse angrepene utnytter informasjonskapsler for enkel pålogging i nettleseren (SSO) eller oppdateringstokener innhentet via skadelig programvare, phishing og andre metoder. I noen tilfeller velger angripere infrastrukturer på steder nær den geografiske plasseringen til brukeren angrepet rettes mot for ytterligere å redusere sjansene for å bli oppdaget. Vi har sett en jevn økning i token-svar-angrep, med over 40 000 deteksjoner per måned i Azure AD Identity Protection. Token-svar er bruken av tokener som er utstedt til en legitim bruker, av en angriper som har skaffet seg disse tokenene. Tokener innhentes vanligvis via skadelig programvare, for eksempel ved å eksfiltrere informasjonskapslene fra brukerens nettleser eller gjennom avanserte phishing-metoder.

Volumet av oppdagede token-svar-angrep



Oppdagede token-svar-angrep per måned. Kilde: Azure AD Identity Protection, unike økter flagget på grunn av deteksjon av unormale token.

Å opprettholde god identitetshelse er helt grunnleggende for organisasjonens vel

Fortsettelse

Ekstrahering av tokener

Mer enn skadelig programvare, trenger angripere legitimasjon for å nå målene sine. Faktisk inkluderer 100 prosent av alle menneskelig opererte løsepengeangrep stjålet legitimasjon. Mange sofistikerte inntrengninger inkluderer legitimasjon kjøpt fra det mørke nettet, opprinnelig stjålet fra usofistikert og bredt distribuert skadelig programvare for legitimasjonstyveri. Denne klassen av skadelig programvare har utviklet seg til å stjele tokener, inkludert øktinformasjon og MFA-krav. Dette betyr at infeksjoner på hjemmesystemer, der brukere logger inn på bedriftsressurser, kan føre til alvorlige hendelser på bedriftsnettverkene.

Angripere kan også trekke ut tokener fra ofrenes enheter gjennom mellommannbasert angrep, der offeret klikker på en ondsinnet lenke i en phishing-e-post eller direktemelding og blir dirigert til et nettsted som ser ut som den legitime påloggingssiden til identitetsleverandøren. I virkeligheten er det en nettjeneste satt opp av angriperen, som videresender og avskjærer all trafikk mellom brukeren og identitetsleverandøren. Angriperen er i stand til å avskjære brukernavnet og passordet og også videresende MFA-utfordringer. Dette resulterer i at tokener som utstedes av identitetsleverandøren og fanges opp av angriperen, kan inneholde MFA-krav som kan brukes av angriperen for å tilfredsstille MFA-kravene.

Microsoft Defender for Cloud Apps har oppdaget et gjennomsnitt på 895 slike angrep per måned siden begynnelsen av 2022. Denne formen for angrep kan forhindres ved å bruke phishing-resistente faktorer av MFA, som sertifikatbasert autentisering, Windows Hello for Business eller FIDO2-sikkerhetsnøkler.

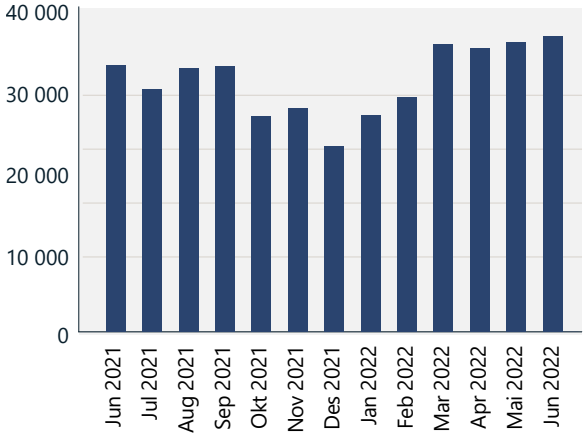
Passordbaserte angrep er den primære metoden for kompromittering av kontoer.

MFA-tretthet

Ved å bruke konseptet «MFA-tretthet» genererer angripere flere forespørsler om MFA til offerets enhet, i håp om at offeret aksepterer forespørselen enten utilsiktet eller som et resultat av tretthet. Dette angrepet kan forhindres ved å bruke moderne autentiseringsapper som Microsoft Authenticator kombinert med funksjoner som nummersamsvar[4] og aktivering av ytterligere kontekst.[5] Azure AD Identity Protection anslår at det er 30 000 MFA-tretthetsangrep per måned.

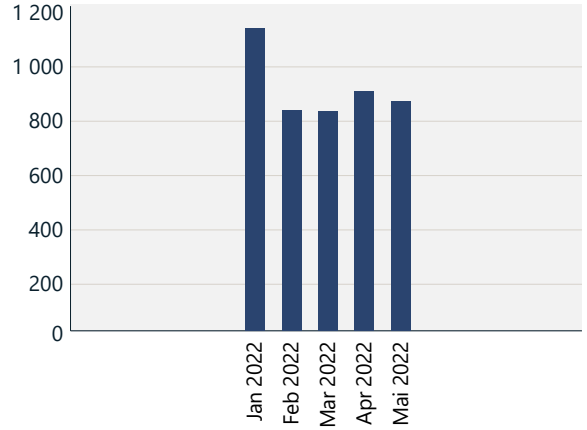
Andelen sofistikerte angrep fortsetter å øke, noe som understreker behovet for phishing-resistente faktorer for flerfaktorautentisering.

Anslåtte tilfeller av MFA-tretthetsangrep



Kilde: Azure AD Identity Protection.

Oppdagede tilfeller av phishing etterfulgt av mellommannbaserte angrep



Kilde: Microsoft Defender for Cloud Apps.

Handlingsbar innsikt

1. Sørg for at alle kontoer i hele organisasjonen er beskyttet av tiltak for sterk autentisering.
2. Passordløs autentisering gir den sikreste og mest brukervennlige opplevelsen, og eliminerer risikoen for passordangrep.
3. Deaktiver eldre autentisering i hele organisasjonen.
4. Beskytt høyverdikontoer og administrative kontoer med phishing-resistente former for sterk autentisering.
5. Moderniser ved å bytte fra en lokal identitetsleverandør til en skyidentitetsleverandør, og koble alle appene dine til den skybaserte identitetsleverandøren for konsistent brukeropplevelse og sikkerhet.

Koblinger til mer informasjon

› Denne verdenspassorddagen vurderer å droppe passord helt | Microsoft Security

Standard sikkerhetsinnstillinger for operativsystemet

Med et landskap for sikkerhetstrusler som er i stadig utvikling, ser vi et økende behov for datasikkerhet konfigurert som standard for å forbedre cyberrobustheten. Selv om sikkerhet for operativsystemet er mer presserende, komplekst og forretningskritisk enn noen gang før, kan det være utfordrende å gjøre og administrere dette riktig.

Tidligere inkluderte datamaskin- og enhetssikkerhet innebygde sikkerhetsfunksjoner som kunden eller IT-eksperten ble forventet å konfigurere til sitt eget ønskede nivå. Denne tilnærmingen er ikke lenger tilstrekkelig, ettersom angripere bruker mer avanserte verktøy innen automatisering, skyinfrastruktur og fjerntilgangsteknologier for å nå målene sine. Det er blitt kritisk nødvendig at alle lag med sikkerhet, fra databrikken til skyen, er konfigurert som standard. Microsoft er videreutviklet til å konfigurere Windows-operativsystemsikkerhet som standard.[6]

Kunder som tar forsvaret på alvor og går i dybden, inkludert en lagdelt sikkerhetsstatus, nye sikkerhetsfunksjoner, regelmessige og konsistente oppdateringer, samt sikkerhetsopplæring og er bevisst på å rapportere phishing og annen svindel – kan forvente mindre skadelig programvare.

For å forenkle forsvaret i dybden, har Windows 11 tett integrert maskinvare- og programvarebeskyttelse slått på som standard, inkludert minneintegritet, sikker oppstart og en Trusted Platform Module 2.0. Windows 10-brukere på egnet maskinvare kan også slå på disse funksjonene i Windows-innstillinger-appen eller i BIOS-menyen.

Eldre enheter har ofte ikke like sterk tilpasning mellom maskinvaresikkerhet og programvaresikkerhetsteknikker. Enheter hvor sikkerhet ikke er aktivert som standard, bør konfigureres manuelt i innstillingene der det er mulig.[7]

For enheter der sikkerhet ikke er aktivert som standard, anbefaler Microsoft å konfigurere dem manuelt i innstillingene, der det er mulig.

Vær proaktiv når det gjelder å bruke kontinuerlige operativsystemoppdateringer og sikkerhetsoppdateringer som bidrar til å gi beskyttelse gjennom hele maskinvare- og programvarelivssyklusen.

Handlingsbar innsikt

1. Bruk en passordløs løsning som binder påloggingsinformasjonen i Trusted Platform Module, se spesifikt etter en passordløs løsning som oppfyller bransjestandarden Faster Identity Online (FIDO) Alliance[8].
2. Utfør rettidig opprydding av alle ubrukte og foreldede kjørbare filer på organisasjonens enheter.
3. Beskytt mot avanserte fastvareangrep ved å aktivere minneintegritet, sikker oppstart og Trusted Platform Module 2.0, hvis dette ikke er aktivert som standard, noe som gjør oppstarten fastere ved å bruke funksjoner innebygd i moderne prosessorer.
4. Slå på datakryptering og legitimasjonsbeskyttelse.
5. Aktiver app- og nettleserkontroller for forbedret beskyttelse mot ikke klarerte apper og andre innebygde utnyttelsesbeskyttelser.
6. Aktiver beskyttelse mot minnetilgang for å beskytte mot tilfeldige fysiske angrep, for eksempel at noen kobler en ondsinnet enhet til eksternt tilgjengelige porter.

Koblinger til mer informasjon

- Windows Security Book | Commercial
- Nye sikkerhetsfunksjoner for Windows 11 bidrar til beskyttelse av hybridarbeid | Microsoft Security Blog

Sentralitet i program-varefor syningskjeden

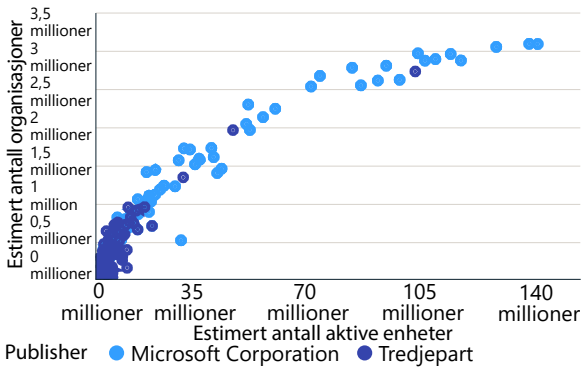
Angrep på tredjepartsapper, plugin-moduler og utvidelser kan redusere kundenes tillit til leverandører som spiller en sentral rolle i forsyningsøkosystemet. Bruk av nettverksteori for å se på programvaresentraliteten bidrar til å belyse det kritiske ved oppdatering, spesielt for sentrale apper.

Windows App Network som har 18 millioner kjørbare programmer installert og er brukt i fem millioner organisasjoner, gir et toppnivåbilde av programvareøkosystemet vårt. Av de 100 000 mest brukte appene er 97 prosent produsert av tredjepartsorganisasjoner hvor oppdateringer og sikkerhetspatcher vedlikeholdes av dem. Dette illustrerer to viktige trekk ved det kommersielle appøkosystemet vårt.

For det første er det en sentralitet i det kommersielle Windows-appøkosystemet. Bare de 100 000 mest brukte appene (av de 18 millionene) brukes på 1000 eller flere enheter. Med andre ord har bare litt over halvparten av 1 prosent av disse appene denne typen vidtrekkende effekt i enhetsøkosystemet.

For det andre er det et mangfold i administrer-barheten til disse appene, der de 10 000 ledende appleverandørene administrerer oppdateringene og sikkerhetsoppdateringene til disse mest brukte kommersielle appene. Dette viser den gjensidige avhengigheten et selskap har til et mangfoldig sett av programvareleverandørers sikkerhet, regeloverholdelse og administrasjonskontroller.

Kommersiell spredning av de mest brukte appene



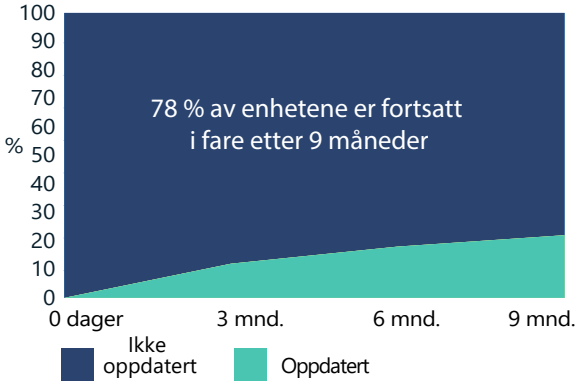
De mest populære appene brukes av millioner av organisasjoner og titalls millioner enheter. Siden de er nær sagt allestedsnærværende, er motstandere på konstant utkikk etter å utnytte sårbarheter i disse toppappene, som kan påvirke millioner av enheter i brukerbasen.

Vi observerer at millioner av kommersielle enheter fortsatt bruker sårbare appversjoner mange måneder etter utgivelsen av oppdateringer eller til og med år etter at produktstøtten har opphørt. For eksempel er det mer enn én million aktive kommersielle Windows-enheter som kjører en versjon av en PDF-leser som ikke er støttet siden 2017.

Gamle versjoner av apper som ikke støttes, forblir i aktiv bruk på millioner av kommersielle enheter. Som et resultat av dette risikerer organisasjoner å opprettholde sårbarheter som ikke blir rettet.

For appversjoner med innebygd støtte ser vi en utflating av nivået på foretatte oppdateringer, noe som er den motsatte trenden av den vi trenger for å drive frem resiliens. Kurven burde i stedet ha vært eksponentiell oppadgående når det gjelder gjennomførte oppdateringer måned for måned – for å oppnå den resiliensen som er nødvendig.

Distribusjonshastigheten til kritiske oppdateringer



Etter å ha undersøkt en kritisk sårbarhet som berørte 134 versjoner av et sett med nettlesere, fant vi ut at 78 prosent, eller millioner av enheter, fortsatt brukte en av de berørte versjonene ni måneder etter at oppdateringen ble utgitt.

Vi brukte InterpretML[9]-verktøysettet for å identifisere egenskaper som er korrelert med organisasjoner som er mer sannsynlig å ha enheter med eldre appversjoner. De viktigste av disse prediktorene inkluderte: få timer med engasjement på enhetene, geografiske områder som Asia-Stillehavsregionen og Latin-Amerika og bransjer som bilindustri, kjemikalier, telekommunikasjon, transport og logistikk, helseutbetalere (kravbehandlere) og forsikring.

Vedlikehold av programvarerobusthet bør omfatte regelmessig deaktivering eller avinstallering av ubrukte apper.

Sikkerheten og regeloverholdelsen til en organisasjon avhenger av dens egen innsats og innsatsen til programvareleverandørene.

Handlingsbar innsikt

1. Utfør rettidig oppdatering av alle apper og endepunkter i hele organisasjonen.
2. Utfør rettidig opprydding av alle ubrukte og foreldede kjørbare filer på organisasjonens enheter.

Koblinger til mer informasjon

- Microsoft Intune-dokumentasjon | Microsoft Docs
- Administrering av apper | Microsoft Docs
- Microsoft Defender for endepunkt | Microsoft Security
- OSS Secure Supply Chain Framework | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

Bygg elastisitet mot nye DDoS-angrep og nettapp- og nettverksangrep

En tiltagende digital transformasjon har gjort slutt på den tradisjonelle nettverks- og sikkerhetsperimetermodellen. Å flytte til skyen betyr at bedrifter må ta i bruk skybasert nettverkssikkerhet for å beskytte de digitale ressursene.

Angrepskompleksitet, -frekvens og -volum fortsetter å vokse og er ikke lenger begrenset til høytider, noe som indikerer et skifte mot angrep året rundt. Dette fremhever viktigheten av kontinuerlig beskyttelse utover de tradisjonelle høytrafikksesongene.

Distribuerte tjenestenektangrep (DDoS)

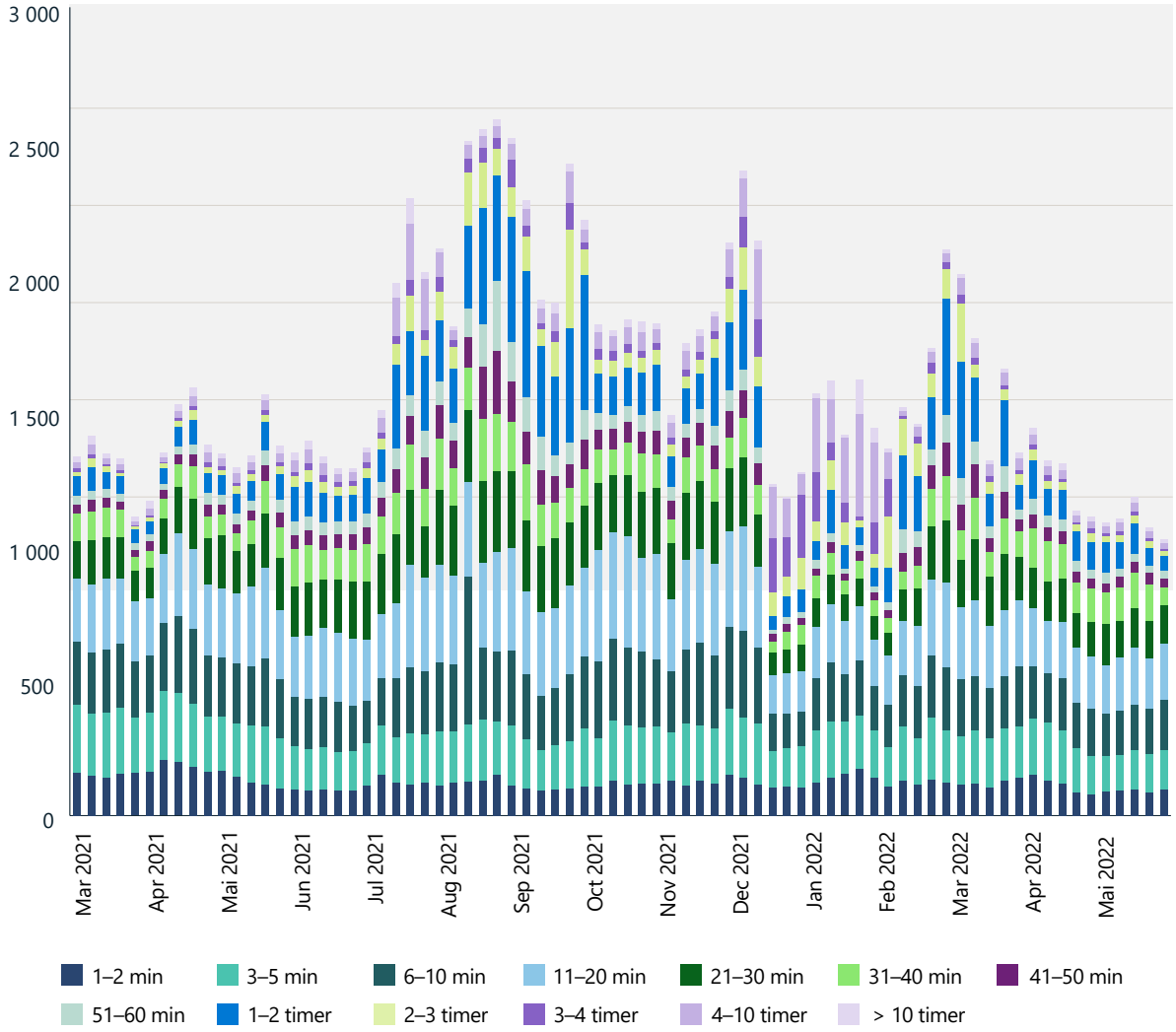
I løpet av det siste året har verden opplevd en DDoS-aktivitet som er enestående i volum, kompleksitet og frekvens. Denne DDoS-eksplosjonen ble drevet av en betydelig økning i angrep fra nasjonalstater og fortsatt spredning av rimelige DDoS-til-leie-tjenester. Microsoft begrenset i gjennomsnitt 1955 angrep per dag, en økning på 40 prosent fra året før. Tidligere skjedde det høyeste antallet angrep normalt i høytidssesongen mot slutten av året. I 2021 ble det imidlertid registrert flest angrep 10. august. Dette kan tyde på et skifte mot angrep året rundt og understreker viktigheten av kontinuerlig beskyttelse utover de tradisjonelle høytrafikksesongene.

I november 2021 hindret Microsoft et volumetrisk DDoS-angrep med en gjennomstrømning på 3,4 terabiter per sekund (Tbps) fra omtrent 10 000 kilder i flere land. Lignende høyvolumetriske angrep over 2+ Tbps ble begrenset i 2022 og fremhevet at det ikke bare er kompleksiteten og frekvensen av angrepene som øker, men også angrepsvolumet (båndbredden).

Angrepsvarighet

De fleste angrepene observert det siste året var kortvarige. Omtrent 28 prosent av angrepene varte i mindre enn 10 minutter, 26 prosent varte i 10–30 minutter og 14 prosent varte i 31–60 minutter. 32 prosent av angrepene varte i mer enn en time.

Antall DDoS-angrep og fordeling på varighet
(mars 2021–mai 2022)



De fleste angrepene det siste året var kortvarige. Omtrent 28 prosent av angrepene varte mindre enn 10 minutter.

Bygg elastisitet mot nye DDoS-angrep og nettapp- og nettverksangrep

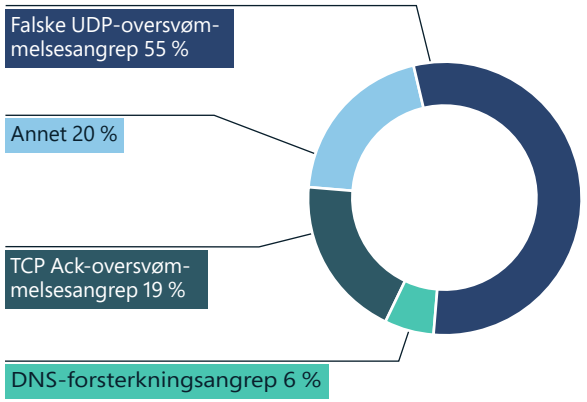
ortsettelse

DDoS-angrepsvektorer

Angrepsvektorene som vanligvis ble brukt det siste året var UDP (User Datagram Protocol)-refleksjon på port 80 ved hjelp av SSDP (Simple Service Discovery Protocol), CLDAP (Connectionless Lightweight Directory Access Protocol), DNS (Domain Name System) og NTP (Network Time Protocol) bestående av én enkelt topp. Vi så også en økning i DDoS-angrep i programlaget målrettet mot nettsteder, med 16,3 millioner topp RPS (forespørsler per sekund) og 9,89 Tbps topptrafikk.

I 2022 begrenset Microsoft nesten 2000 DDoS-angrep daglig og hindret det største DDoS-angrepet som er rapportert i historien.

DDoS-angrepsvektorer



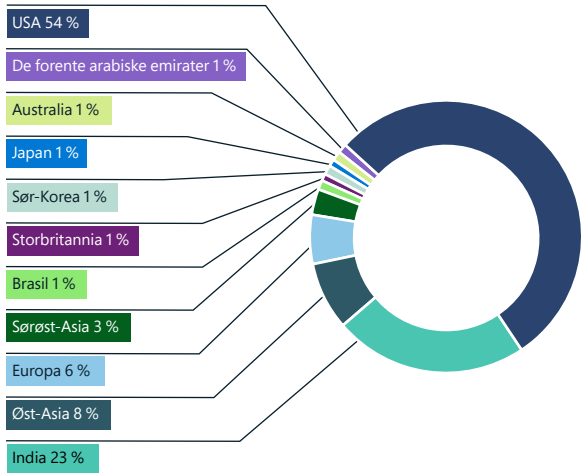
UDP Spoof Flood-angrep steg til toppvektoren i første halvdel av 2022, fra 16 prosent til 55 prosent. TCP Ack Flood-angrep sank fra 54 prosent til 19 prosent.

Spillindustrien fortsetter å være det fremste målet for DDoS-angrep, hovedsakelig fra mutasjoner av Mirai-botnet og UDP-protokolla-ngrep med lavt volum. Siden UDP vanligvis brukes i spill- og strømmingsapper, var et overveldende flertall av angrepsvektorene UDP Spoof Floods, mens en liten del var UDP-refleksjon og forsterkningsangrep.

Geografiske målområder

Av DDoS-angrepene som ble oppdaget det siste året, ble 54 prosent utført mot mål i USA, en trend som delvis kan forklares av det faktum at de fleste Azure- og Microsoft-kunder er i USA. Vi så også en kraftig økning i angrep mot India, fra bare 2 prosent av alle angrep i andre halvdel av 2021 til 23 prosent i første halvdel av 2022. Øst-Asia, og særlig Hongkong, er fortsatt et populært mål med 8 prosent. I Europa så vi konsentrasjoner av angrep mot områdene Amsterdam, Wien, Paris og Frankfurt.

DDoS-angrepsmål

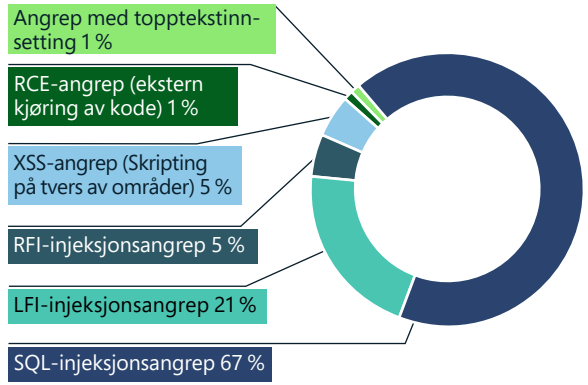


Vi tilskriver det høye volumet av angrep i Asia til områdets enorme spill-fotavtrykk, spesielt i Kina, Japan, Sør-Korea og India. Dette fotavtrykket fortsetter å øke etter hvert som veksten i smarttelefoner øker populariteten til mobilspilling, noe som tyder på at dette geografiske målet bare kommer til å fortsette å vokse.

Utnytting av nettapper

Brannmur for nettapper (WAF), i kombinasjon med DDoS-beskyttelse, utgjør en integrert del av den dyptgående forsvarsstrategien for å beskytte API-ressurser (nett- og programmeringsgrensesnitt). Microsoft observerte i overkant av 300 milliarder WAF-regler utløst per måned via Azure WAF-er.

Distribusjon mest utbredte angrepstyper



Azure WAF oppdager milliarder av OWASP (Open Web Application Security Project) topp 10^{10}-angrep daglig. Ifølge signalene våre har angriperne flest forsøk på SQL-injeksjonsangrep etterfulgt av lokale filinnsettingsangrep og eksterne filinjeksjonsangrep. Dette er i tråd med OWASP-topp-10-listen som viser injeksjonsangrep som den tredje vanligste typen nettangrep.

Det har også vært en økning i robotangrep mot Azure-nettapper, med et gjennomsnitt på 1,7 milliarder robotforespørsler per måned, og 4,6 prosent av den trafikken kommer fra skadelige roboter.

Bygg elastisitet mot nye DDoS-angrep og nettapp- og nettverksangrep

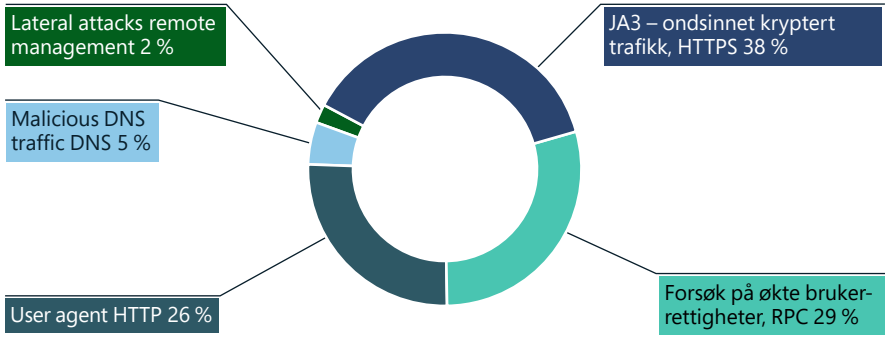
Fortsettelse

På grunn av et økende antall roboter som utfører legitimasjonsangrep, kredittkortsvindel, cyberpåvirknings-kampanjer og forsyningskjedeangrep, forventer vi en jevn økning i robotangrep mot nettapper.

Nettverksinntrenging: oppdaging og forhindring

I 2022 observerte vi en betydelig økning i nettverkslagutnyttelser, spesielt med skadelig programvare. Azure Firewall gjenkjennings- og forebyggingssystem (IDPS) blokkerte mer enn 150 millioner tilkoblinger bare i juni.

IDPS-trafikkavvisningsårsak



Årsaker til IDPS-trafikkvarsler

Analyser av IDPS-varsler og -trafikkavvisninger viser følgende tilnærminger som brukes av angripere. I «Avvis trafikk» ser vi at angripere som bruker SSL til å skjule aktivitetene sine og angrep med ekstern kjøring, blir stadig vanligere. I «Varsle trafikk» ser vi SMB-/SMB2-protokoller som brukes til å utføre angrep med ekstern kjøring.

Handlingsbar innsikt

1. Inspiser all trafikk mellom systemer i et datasenter eller en skytjeneste, og trafikk som søker å få tilgang til dem.
2. Utvikle en robust året-rundt-responsstrategi for nettverkssikkerhet.
3. Bruk skybaserte sikkerhetstjenester til å implementere en robust nulltillit-nettverkssikkerhetsstatus.

Koblinger til mer informasjon

- Forbedre sikkerhetsforsvaret mot angrep fra løsepengevirus med Azure Firewall | Azure-bloggen og oppdateringer | Microsoft Azure
- Anatomi av et DDoS-forsterkningsangrep | Microsoft Security Blog
- Intelligent appbeskyttelse fra kant til sky med Azure Web Application Firewall | Azure-bloggen og oppdateringer | Microsoft Azure

Utvikle en balansert tilnærming til datasikkerhet og cybersikkerhet

Den digitale transformasjonen har bidratt til en enorm utvidelse av dataressurser og en økning i sikkerhets-, samsvars- og personvernrisikoer. Organisasjoner som er cyberresiliente, må balansere investeringer i funksjoner for databeskyttelse, samsvar og gjenoppretting, og integrere disse med spesialiserte prosesser for forskriftsmessig respons for å håndtere ulike typer innbrudd.

Datainnbrudd er ikke et spørsmål om hvis, men om når. IBM og Ponemon Institutes studie «Cost of a Data Breach, 2021» rapporterer en global gjennomsnittlig kostnad for datainnbrudd på 4,24 millioner USD (en økning på 10 prosent fra året før) og 9,05 millioner USD i USA. Samsvarsfeil var den største kostnadsforsterkende faktoren. Når det gjelder de kostnadsreduserende tiltakene var disse knyttet til anbefalte fremgangsmåter som planlegging av hendelsesrespons (IR), distribusjonsmodenhet for nulltillit, AI-sikkerhet og -automatisering samt bruk av kryptering.

Datainnbrudd er uunngåelige. Organisasjoner som har en balansert og resilient tilnærming, reduserer hyppigheten, virkningen og kostnaden av innbrudd.

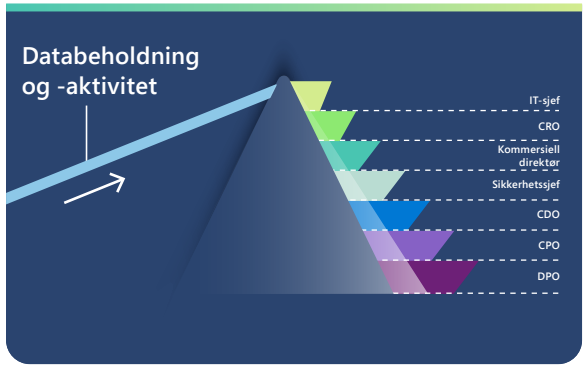
Datastyring, sikkerhet, samsvar og personvern er gjensidig avhengig av hverandre

Vi har de siste årene sett at dataene øker i viktighet, noe som er en avgjørende motor for verdiskaping i organisasjonene. Samtidig har fremveksten av personvernregler som krever både datastyring og -sikkerhet, visket ut skillet mellom risikoroller. Nyere roller på C-nivå, som for eksempel Chief Data Officer (CDO) eller Chief Privacy Officer (CPO), har en iboende interesse for sikkerhet og samsvar, men implementeringen og operasjonaliseringen av personvernet påhviler ofte team som er ledet av Chief Information Officer (CIO) og/eller Chief Information Security Officer (CISO). At flere er involvert kan være positivt, ettersom datastyringsinitiativer ledet av CDO-er også har sikkerhetsfordeler. Som et resultat av denne sammenkoblingen må IT-, datastyrings-, sikkerhets-, samsvars- og personvernteamene arbeide stadig tettere for å oppnå effektivitet og håndtere risiko.

Fremtiden ligger i plattformer for enhetlig risikostyring av hele databeholdningen til organisasjonen

Innretting av IT, datastyring, sikkerhet, samsvar og personvernadministrasjon er utfordrende i miljøer med skreddersydde apper for hver disiplin og en ikke enhetlig dekning på tvers av organisasjonens hybride data spredt på flere skyer. Vi mener at organisasjonene trenger en enkeltvisning for å finne og kjenne dataene sine, beskytte dataene, styre tilgangen, bruken og livssyklusen til dataene, og forhindre tap av data på tvers av databeholdningen.

Å arbeid fra samme databeholdning og ha den samme aktivitetsinformasjonen forenkler prosessene på tvers av teamene, gir et mer omfattende risikobilde og gjør det mulig for organisasjonene å forberede og strømlinjeforme responsen på et innbrudd på en bedre måte.



«Enkeltvisningen» bør fungere som et prisme. Teamene som har en eierandel i datasikkerhet, samsvar og personvern, trenger ulike, men konsistente visninger av den samme databeholdningen og -aktiviteten for å samspille og samarbeide. Dataaktivitet inkluderer datatilgang, modifisering og bevegelseshendelser, som er en verdifull del av den totale datasikkerheten.

Effektiv datastyring, sikkerhet, samsvar og personvern er gjensidig avhengig av hverandre og krever samarbeid på tvers av teamene.

Handlingsbar innsikt

1. Balanser forsvaret med gjenoppretting, og minimer virkningen av datainnbrudd ved å investere i samsvar, databeskyttelse og evnen til å respondere.
2. Utvikle og ta i bruk prosesser og verktøy som går på tvers av datarisikosiloer og dekker hele databeholdningen.

Koblinger til mer informasjon

- Microsoft Purview – løsninger for databeskyttelse | Microsoft Security
- Fremtiden for samsvar og datastyring er her: Vi presenterer Microsoft Purview | Microsoft Security Blog

Resiliensen til cyberpåvirknings-operasjoner: den menneskelige dimensjonen

De siste fem årene har utviklingen innen grafikk og maskinlæring bidratt til brukervennlige verktøy som raskt kan generere realistisk innhold av høy kvalitet som kan spres bredt over internett på bare noen sekunder.

Når det gjelder hendelser rapportert via tekst, lyd og visuelt innhold, har vi nådd et punkt der verken mennesker eller algoritmer kan skille fakta fra fiksjon på en pålitelig måte. Spredningen av disse verktøyene og resultatene av dem, reiser tvil om påliteligheten til alle digitale medier, noe som reduserer forståelsen vår av både lokale hendelser og hendelser rundt om i verden. Nye former for innflytelse som er gjort mulig av teknologiske fremskritt, har alvorlige implikasjoner for de demokratiske prosessene.[11]

Spørsmålet er hva vi kan gjøre for å forberede oss på en mer robust fremtid hvor vi kan stå imot disse cyberpåvirkningsoperasjonene. Teknologien er bare én bit av puslespillet. Det kreves flere tiltak, inkludert utdanning om mediekunnskap, bevissthet og årvåkenhet, investeringer i kvalitetsjournalistikk – med pålitelige reportere på stedet, lokalt, nasjonalt og internasjonalt – nettverk for deling og varsling om påvirkningsoperasjoner, og nye typer reguleringer som straffer ondsinnede aktører som genererer eller manipulerer digitale medier med sikte på å bedra.

Vi erkjenner også at å gjenopprette tilliten til digitalt innhold er et ambisiøst mål som kommer til å kreve ulike perspektiver og deltakelse. Det finnes ikke én bedrift, institusjon eller myndigheter som kan løse disse truslene på egen hånd. Superkraften vår som mennesker, er evnen vår til å samarbeide. Dette er spesielt viktig nå fordi det kommer til å kreve at alle – globale myndigheter, bransjer, akademia og spesielt organisasjoner for nyheter, media og sosiale medier – arbeider sammen for samfunnets beste.

Koblinger til mer informasjon

- Apper for kunstig intelligens brukt i cyberforsvaret til Department of Defense | Microsoft On the Issues
- Kunstig intelligens og cybersikkerhet: økte utfordringer og lovende retninger. Høring om anvendelser av kunstig intelligens til operasjoner i cyberspace for underutvalget for cybersikkerhet i senatets Armed Services Committee, 117. kongress (3. mai 2022, uttalelser fra Eric Horvitz)

Forsterkning av den menneskelige faktoren med kompetanse

Å ta tak i den menneskelige faktoren er en viktig komponent i enhver strategi for å øke cybersikkerheten. Ifølge studien Human Factor in IT Security,[12] utført av Kaspersky, involverer 46 prosent av hendelsene innen cybersikkerhet uforsiktig eller uniformert personell som utilsiktet forenkler angrepet.

Teamet for utdanning og bevissthet i Digital Security and Resilience-organisasjonen i Microsoft er ansvarlig for å styrke den menneskelige faktoren i cybersikkerheten ved å gjøre de ansatte bedre i stand til å sikre både våre egne og kundenes systemer og data. Målene våre er å

- redusere risikoen for Microsoft og kundene våre ved å bygge en sentralisert kjerneferdighet for hele bedriften på tvers av alle ansatte
- forsterke de ansattes sikkerhetskunnskap gjennom en opplæring i flere faser for å støtte ønsket atferd
- fremme kulturendringer ved å gjøre et sikkerhetstankesett til en iboende del av Microsoft gjennom årlige nødvendig sikkerhetsopplæringer og -arrangementer
- fremme en sentralisert nettressurs, på ett sted, med anbefalte fremgangsmåter, informasjon om bedriftens retningslinjer og hendelsesrapportering for alt som er relatert til nettsikkerhet

Et målrettet, sentralisert kompetanseprogram for cybersikkerhet når hver eneste Microsoft-ansatt minst én gang i året. Opplæringstilbud er optimalisert for å støtte nåværende cybersikkerhetsinitiativer og levere målbare atferdsresultater. Microsoft Information Risk Management Council (IRMC) spiller en nøkkelrolle i å identifisere viktige endringsresultater for cybersikkerhetsatferd som skal håndteres ved hjelp av opplæring.

Med alle ferdighetsprogrammene våre for nettsikkerhet måler vi løsningens effektivitet, virkningsgrad og resultater der dette er mulig. Tilbudet vårt om ferdigheter om innsidetrusler har for eksempel 95 prosent opplæringssamsvar, eksepsjonelt gode tilbakemeldinger på opplæringen og har resultert i en betydelig økning i ledernes rapportering av mulige innsidetrusseltilfeller via selskapets Report It Now-verktøy. Programmet inkluderer:

Sikkerhetsfundament: Sentralisert, virksomhetsomspennende cybersikkerhets-bevissthet og samsvarsopplæring som tar for seg viktige sikkerhets- og personvernspraksiser. Denne svært etterlengtede opplæringsserien bruker en edutainmentmodell for å gjøre læring om cybersikkerhet engasjerende og interessant.

STRIKE: Microsofts obligatoriske tekniske opplæring for teknikere som utvikler og vedlikeholder bransjeløsninger. Denne opplæringen som er kun for inviterte, tar for seg aktuelle og kritiske områder innen cybersikkerhetshygiene, og bruker en modell for direktesendt hybrid levering som er skreddersydd til målgruppens behov.

Programspesifikt: Målrettede opplæringsprogrammer støtter spesifikke cybersikkerhetsinitiativer, inkludert Shadow IT, Insider Threat og Microsoft Federal. Disse tilbudene er tett integrert i den samlede engasjementsstrategien for de respektive cybersikkerhetsinitiativene gjennom støtte fra ledere og målstyringsrapportering for å hindre en «kryss av i boksen»-opplæring.

MSProtect: Microsofts sentraliserte nettressurs inneholder anbefalte fremgangsmåter, informasjon om bedriftens retningslinjer og hendelsesrapportering for alt som er relatert til cybersikkerhet. Denne behovsbasert ressursen er det viktigste stedet å hente informasjon fra for ansatte uten formelle opplæringstilbud.

Sikkerhetsferdigheter må ikke sees på som en samsvarshandling a la «kryss av i boksen». Fokuser i stedet på atferdsendringer for å gjøre det mulig å overvåke utfall på tvers av identifisert målatferd, og etabler lyttesystemer for å fastslå virkningen av tilbudene.

Handlingsbar innsikt

1. Gi ansatte sikkerhetsopplæring og -ressurser når og der de trenger den.
2. Utvikle en sentralisert kompetansestrategi bygget på informasjon fra interessenter i hele virksomheten.
3. Sørg for at virkningen av opplæring spores og analyseres for effektivitet (kvantitet), virksomhetsgrad (kvalitet) og resultater (forretningspåvirkning).

Koblinger til mer informasjon

- Microsoft lanserer neste trinn i kompetanseinitiativet etter å ha bistått 30 millioner mennesker

Innsikt fra programmet vårt for eliminering av løsepengevirus

Microsoft har gjennomført en egen nulltillitsreise[13] de siste fem årene for å sikre at identiteter og enheter er robust administrert og sunne. I takt med at risikoen for løsepengevirus har vokst, har vi utviklet et dypt syn for å støtte tilnærming vår til å beskytte oss selv og kundene våre.

Etter en grundig intern evaluering bygget vi et elimineringsprogram for løsepengevirus for å utbedre mangler i kontroller og dekning, bidra til funksjonsforbedringer for tjenester som Defender for Endpoint, Azure og M365, og for å utvikle håndbøker for sikkerhets- og ingeniørteamene våre om hvordan tjenestene kan gjenopprettes i tilfelle et angrep med løsepengevirus.

Det første steget var å forstå omfanget av beskyttelsen vår mot løsepengevirusangrep rettet mot Microsoft. Innsatsen var allerede godt i gang ved å ta i bruk Defender for Endpoint, og sikre at alle enheter administreres og overholder retningslinjene for nulltillit, men vi måtte finne en måte å forstå alle fasetter av det større spørsmålet om vi effektivt kunne gjenopprette systemene fra et angrep. For å få innsikt evaluerte vi NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile,[14] som samsvarer med våre generelle bedriftsretningslinjer når det gjelder den kjente listen vår over kontroller. Denne analysen identifiserte raskt mangler i dekningen.

Deretter prioriterte vi hull på tvers av funksjonene Identifiser, Oppdag, Beskytt, Responder og Gjenopprett i CSF. Vi fant strategisk tilpasning til nulltillit og andre programmer, og oppdaget også hull som ikke hadde noen eksisterende arbeidsstrøm. Etter å ha vurdert hvor mye arbeid og innsats som trengs for å utbedre disse hullene, delte vi dem inn i to søyler:

- **Beskytte bedriften (PtE):** Definerer arbeidselementer som vi må gjøre som en bedrift, for å beskytte oss selv og være i stand til å gjenopprette fra et angrep, hvis angrepet skulle lykkes.
- **Beskytte kunden (PtC):** Bygge inn funksjoner i tilbudene våre for å beskytte både kundene våre og virksomheten vår.

Innbygging av svar på funnene i vår egen bedrift

For å rette opp topprisikoene og beskytte de kritiske tjenestene våre mot løsepengevi-rusangrep planlegger vi å fokusere investeringene de neste 6 til 12 månedene for å oppnå de fem scenarioene nedenfor som en del av et dedikert løsepengevirusprogram. Når vi har lykkes i hvert av scenarioene, utvider vi gradvis omfanget av programmet for å nå alle deler av virksomheten.

Scenario 1: Medlemmene av sikkerhetsteamene forstår den generelle risikoen forbundet med løsepengevirusangrep, og har en prosess etablert for å styrke bevisstheten til lederne om kontrollhull og risikostatus.

Scenario 2: Medlemmer av sikkerhetsteamene har tilgang til planer utarbeidet for å hjelpe dem og andre team i Microsoft til å svare på og gjenopprette kritiske tjenester fra et angrep med løsepengevirus.

Scenario 3: Medlemmene i Enterprise Resilience-teamet har en standard de følger for sikkerhetskopiering av kritiske systemer. Det finnes håndbøker og det gjennomføres regelmessige øvelser med sikkerhetskopiering og gjenoppretting for å sikre at data kan gjenopprettes i tilfelle et angrep med løsepengevirus.

Scenario 4: Tjenesteeiere forstår og implementerer de nødvendige sikkerhets- og driftskontrollene og retningslinjene for å beskytte sine tjenester, kundedata, endepunkter og nettverksressurser mot angrep fra løsepengevirus – med spesielt fokus på tjenester prioritert som Microsoft-kritiske tjenester.

Scenario 5: Alle ansatte kan få tilgang til utdannings- og opplæringsressurser som beskriver hvordan de kan gjenkjenne et angrep med løsepengevirus, og hvordan de kan varsle sikkerhetsteamet og starte responsen.

Handlingsrettet innsikt

1. Dokumenter og valider ende-til-ende-gjenoppretting og utbedringsaktiviteter knyttet til angrep fra løsepengevirus mot kritiske tjenester.
2. Involver interessenter i å oppdatere krisehåndteringsplanene til å inkludere spesifikke aktiviteter for løsepengevirus og en beslutningsprosess og veiledning for å avgjøre om/når det skal betales for løsepengevirus.
3. Forbedre gjenkjenning og beskyttelse ved å aktivere funksjoner som er tilgjengelige i de distribuerte sikkerhetsproduktene (f.eks. Defender for Endpoint Attack Surface Reduction-regler).
4. Samarbeid med teamet for sikkerhetsstandarder for å definere en grunnlinje for beskyttelse mot løsepengevirusangrep, og gi opplæring og dokumentasjon til teknikere om hvordan de kan beskytte mot angrep fra løsepengevirus.
5. Få automatisering på plass for å gjøre distribusjonen av retningslinjer for sikkerhet og drift enklere på DevOps-teamene, og sørg for at hvis et system avviker fra samsvar, flagges og utbedres det raskt.

Koblinger til mer informasjon

- Deling av hvordan Microsoft beskytter mot løsepengevirus | Microsoft Inside Track

Handle nå basert på Quantum Security-implikasjoner

Den store utfordringen er å håndtere trusselen kvantedatabehandling utgjør for dagens kryptografi og alt den beskytter. Det nylig utstedte Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] bygget på US Executive Order 10428[16] om forbedring av nasjonens nettsikkerhet, fremhever sikkerhet i programvareforsyningskjeden som avgjørende for å håndtere fremtidige nasjonalstatangrep.

Hva er kvantedatamaskiner?

Kvantedatamaskiner er maskiner som bruker kvantefysikkegenskaper til å lagre data og utføre beregninger. Dette kan være svært fordelaktig for visse oppgaver der de i vesentlig grad kan overgå selv de beste superdatamaskinene våre. Kvantedatabehandling åpner allerede nye horisonter for datakryptering og -behandling. Studier spår at kvantedatabehandling blir en kvanteindustri verdt flere milliarder dollar så tidlig som i 2030.[17] Faktisk ser kvantedatabehandling og kvantekommunikasjon ut til å ha en transformerende effekt i en rekke bransjer, i alt fra helse og energi til økonomi og sikkerhet.

Kvantedatabehandling er en trussel mot dagens kryptografi og alt den beskytter.

Trusselen mot dagens kryptografi

Med Shors 1994-algoritme og en kvantedatamaskin i industriell skala på mer enn noen få millioner fysiske kvantebiter, kan alle våre nåværende, allment distribuerte kryptografiske fellesnøkkelalgoritmer effektivt løses. Det er viktig å vurdere, evaluere og standardisere «kvantesikre» krypteringssystemer som er effektive, smidige og trygge mot et kvantebasert angrep som er i gang. Programvaremigrering fra de eksisterende klassiske algoritmene og protokollene til kvantesikre kryptografiløsninger som er robuste mot kvanteangrep, kommer til å ta flere år – om ikke et tiår eller enda lenger.[18]

Dette betyr at det allerede i dag er et økt press på å håndtere trusselen mot dagens kryptografi og alt den beskytter. Angripere kan registrere krypterte data nå og utnytte dem senere når en kvantedatamaskin er tilgjengelig. Det er med andre ord for sent å vente på at kvantedatabehandling blir tilgjengelig før vi adresserer de kryptografiske implikasjonene av den.

Ettersom kryptografi brukes i hele cyberøkosystemet, betyr dette at de kryptografibaserte sikkerhetstjenestene våre kan bli kompromittert. Dette inkluderer for eksempel tjenester for kommunikasjon (TLS, IPSec), meldinger (e-post, nettkonferanser), identitets- og tilgangsadministrasjon, nettlesing, kodesignering, betalingstransaksjoner og andre tjenester som er avhengige av kryptografi for beskyttelse.

I takt med at kvantedatamaskiner blir en realitet, vil tredjeparts programvarekomponenter som inneholder implementeringer av kryptografiske algoritmer og funksjoner, også kreve ytterligere granskning. Dette krever at alle organisasjoner langs verdikjeden gjør sitt for å sikre at kjeden forblir sikker. Bransjeorganer og myndigheter øker innsatsen for å definere sikkerhetskravene til programvareforsyningskjeden, og i noen tilfeller innføres det nye mandater for å sikre kjeden. National Security Memorandum NSM-8[19] skisserer krav og tidslinjer for implementering av kvantesikker kryptografi i nasjonale sikkerhetssystemer (NSS). Der forventes det at det innen 180 dager ses på «moderniseringsplanlegging, bruken av ustøttet kryptering, godkjente unike oppdragsprotokoller, kvantebestandige protokoller og planlegging for bruk av kvantemotstandig kryptografi der det er nødvendig.»

Standardisering er en tidskrevende aktivitet i overgangen til kvantesikker kryptografi. Standardiseringsorganer som arbeider med standarder for fellesnøkkelkryptografi, må begynne å eksperimentere med og tilpasse seg kvantesikre algoritmer nå.

Nye algoritmer for kvantesikker kryptografi (PQC) – klassiske algoritmer som er antatt å være robuste for kvanteangrep – gjennomgås nå gjennom NISTs Post-Quantum Standardization Project.[20] Dette arbeidet kommer til å påvirke den globale innsatsen innenfor standardiseringsorganene. Selv om det kan være noe overlapping med valg av algoritmer fra amerikanske myndigheter, kan ulike nasjonale organers/myndigheters valg av samsvarende algoritmer by på internasjonale utfordringer. Denne fragmenteringen kommer i sin tur til å komplisere produkt- og tjenesteutviklingen.

Nye kvantesikre kryptografialgoritmer gjennomgås gjennom NISTs Post-Quantum Cryptography Standardization-program. Dette arbeidet kommer til å påvirke den globale innsatsen innenfor standardiseringsorganene.

Handlingsbar innsikt

I tillegg til SAFECode og samarbeidsmed-lemmene, bør bransjen ta umiddelbare kortsiktige grep for å forberede seg på PQC-overgangen.[21] Disse inkluderer:

1. Lag en oversikt over produktene/kodene som bruker kryptografi.
2. Implementer en strategi for kryptografi på tvers av organisasjonen som inkluderer minimering av kodefrafallet som kreves når kryptografien endres.
3. Test bruken av kandidater til kvantesikre algoritmer i produktene eller tjenestene som bruker kryptografi.
4. Vær forberedt på å bruke ulike fellesnøkkelalgoritmer for kryptering, nøkkelutveksling og signaturer.
5. Test appene dine for virkningen av svært store nøkkelstørrelser, chiffreringer og signaturer.

Koblinger til mer informasjon

› Microsoft har demonstrert den underliggende fysikken som kreves for å skape en ny type kvantebit | Microsoft Research

Integrering av forretninger, sikkerhet og IT for økt robusthet

Robust cybersikkerhet er avhengig av at bedriftslederne samarbeider med sikkerhetsteamene for å implementere sikkerhet. Microsofts erfaring er at sikkerhetslederskap er en utfordrende disiplin som krever støtte fra organisatoriske ledere for å beskytte organisasjonen på en mest mulig effektiv måte.

Sikkerhetsledere navigerer blant en rekke dynamiske utfordringer som spenner over emner knyttet til risiko, teknologi, økonomi, organisasjonsprosesser, forretningsmodeller, kulturtransformasjon, geopolitiske interesser, spionasje og internasjonalt sanksjonssamsvar. Hver av disse har nyanser som må forstås og nøye administreres.

Sikkerhetslederne må også hindre både intelligente, velfinansierte og svært motiverte menneskelige angripere, og mindre kunnskapsrike, men effektive, nettkriminelle. Teamene deres må forsvare komplekse tekniske ressurser som ofte er bygget opp trinnvis over 30 eller enda flere år – fra en tid da sikkerheten hadde lav eller ikke-eksisterende prioritet. Beslutninger tatt for mange år siden kan utgjøre en risiko i dag frem til vi betaler av den tekniske gjelden og håndterer hullene i sikkerheten.

Organisatoriske ledere og policybesluttere kan ha en betydelig positiv innvirkning på sikkerheten ved aktivt å støtte sikkerhetsledere og bidra til å bygge en bro mellom integrert sikkerhet og resten av organisasjonen. Når Microsoft arbeider med kunder som har denne tilpasningen, ser vi at de bygger en mer robust organisasjon og også forbedrer fleksibiliteten for å tilpasse seg og innovere.

Organisatorisk lederskap kan støtte sikkerhetsledere ved å fokusere på tre viktige områder:

1. Bygg sikkerhet med design

Sikkerhet blir noen ganger sett på som et hinder eller noe man legger til etterpå i forretningsprosesser og blir ofte vurdert i beslutninger bare når det er for sent å unngå en risiko eller fikse på en rimelig og enkel måte.

Organisatoriske ledere og policyutformere bør sørge for at

det inkluderes sikkerhet tidlig i nye initiativer nye digitale initiativer og bruken av skyen prioriterer sikkerhet for å bidra til at organisatorisk risiko ikke øker med hver nye app eller digitale funksjon Når sikkerheten er pålitelig inkludert, kan du bruke disse prosessene til å modernisere eldre systemer for å få sikkerhets- og produktivitetsfordeler samtidig.

Normaliser forebyggende vedlikehold av sikkerhet. Sørg for at grunnleggende sikkerhetsvedlikehold (for eksempel ved å bruke sikkerhetsoppdateringer og sikre konfigurasjoner) har full organisasjonsstøtte tildelt (inkludert budsjetter, planlagt nedetid, anskaffelseskrav for leverandørproduktstøtte o.l).

Dessverre forsinker eller utsetter mange organisasjoner disse vanlige fremgangsmåtene, eller de bruker dem bare delvis. Dette gir omfattende muligheter som angriperne kan utnytte. Behovet for normalisering av sikkerhet er fanget opp i US NIST 800-40.[22]

2. Engasjer deg i sikkerheten

Organisatoriske ledere bør aktivt delta i og støtte viktige sikkerhetsprosesser for å sikre prioritering av ressurser og beredskap ved sikkerhetskatastrofer. Dette inkluderer å engasjere seg i:

Identifisere kritiske forretningsressurser. Sikkerhetsledere og -team må vite hvilke ressurser som er forretningskritiske for å kunne fokusere på de sikkerhetsressursene som betyr mest. Dette er ofte en ny øvelse som inkluderer å stille og svare på spørsmål som ikke har vært behandlet tidligere.

Øvelser for forretningskontinuitet og Disaster Recovery av cybersikkerhet. Cyberangrep kan bli store hendelser som forstyrrer eller stopper de fleste eller alle forretningsoperasjoner. Å sikre at team i hele organisasjonen er forberedt på å håndtere disse situasjonene, reduserer tiden det tar å gjenopprette driften, begrenser skade på organisasjonen og bidrar til å opprettholde tilliten fra kundene og befolkningen. Dette bør integreres i en eksisterende forretningskontinuitets- og Disaster Recovery-prosess.

Beslutninger om sikkerhetsrisikoer tas best av bedrifts- eller oppdragseiere som har full oversikt over alle risikoer og muligheter.

Integrering av forretninger, sikkerhet og IT for økt robusthet

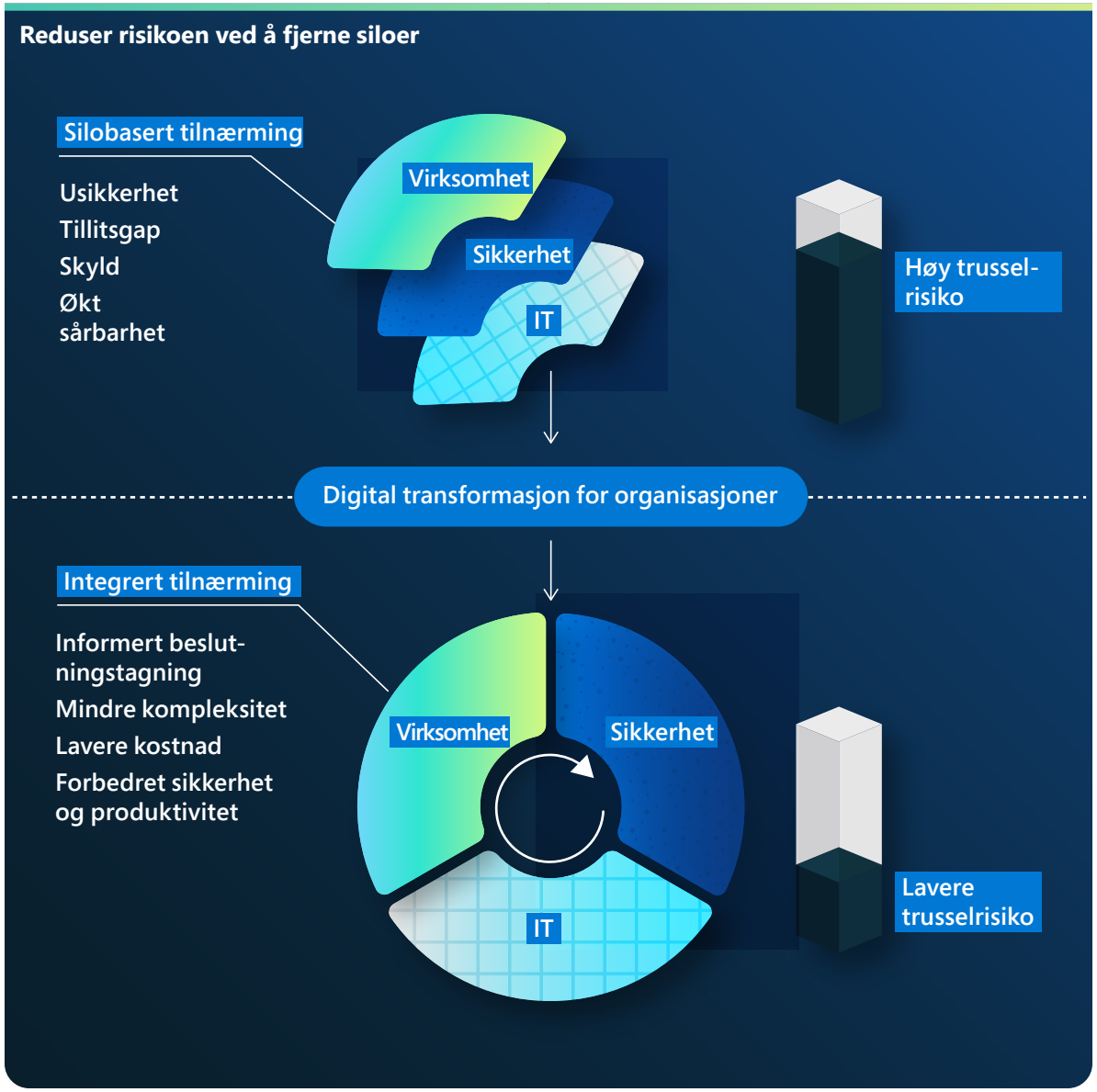
Fortsettelse

3. Plasser sikkerheten riktig

Måten organisasjonens strukturerer ansvaret for sikkerhetsrisikoene på, utsetter dem ofte for dårlig beslutningstaking vedrørende sikkerhetsrisikoer. Risikobeslutninger tas best av bedrifts- eller oppdragseiere som har full oversikt på tvers av alle risikoer og muligheter, men ofte tilordner organisasjonene (implisitt eller eksplisitt) sikkerhetsrisikoansvaret til fageksperter i sikkerhetsteamene i stedet. Å plassere denne byrden på sikkerhetsteamet er uheldig, da det ofte fratar bedriftseierne oversikten og kontrollen over en viktig risiko for virksomheten. Organisasjoner kan korrigere dette ved å

Forberede bedriftseierne: Lær opp bedriftseiere om sikkerhetsrisikoer generelt, og hvordan disse truslene kan og vil påvirke virksomheten. Å engasjere sikkerhetsteam direkte i dette arbeidet gir også et bedre samarbeid mellom sikkerhet og generell forretningsmessig smidighet.

Tilordning av sikkerhetsrisiko til bedriftseiere: Etter hvert som ledere med forretningsansvar blir informerte nok til å forstå og akseptere sikkerhetsrisiko, bør organisasjonen eksplisitt flytte ansvaret for sikkerhetsrisikoene til dem, samtidig som sikkerhetsteamene er ansvarlige for å håndtere denne risikoen og gi informert ekspertise og veiledning til forretningslederen.



«Cybersikkerheten ligger på en skyveskala fra klassisk forretningskontinuitet og Disaster Recovery og starter med god datasikkerhetskopiering, går videre til gjenopprettingsfunksjoner for prosesser, teknologier og deres avhengigheter (inkludert personer og tredjeparter) og deretter over til selvreparasjonstjenester, robusthet for kritiske roller og failovers for kritiske tredjeparter. De mest resiliente organisasjonene fremmer integrasjon mellom IT, bedriftsledere og sikkerhetspersonell. Stor resiliens inkluderer utforming for resiliens fra starten, sikker endringsadministrasjon og detaljert feilisolasjon. Cybersikkerhet er bare ett scenario i et godt planleggingsprogram for alle farer. Etter hvert som nettrisikoene øker og skjæringspunktet mellom cybersikkerhet og resiliens blir viktigere, blir forbindelsen mellom Chief Information Security Officer (CISO) og bedriftens resiliensprogram sterkere. Hvert år tar flere CISO-er eierskap til robustheten til hele selskapet.»

Lisa Reshaur
General Manager, Risk Management, Microsoft

Koblinger til mer informasjon

- Fra robusthet til digital utholdenhet: Hvordan organisasjoner bruker digital teknologi til å forbedre seg i usikre tider | Official Microsoft Blog
- Hvordan IT- og sikkerhetsteam kan arbeide sammen for å forbedre endepunktsikkerheten | Microsoft Security

Normalfordelingen av cybersikkerhet

Suksessfaktorer for resiliens som enhver organisasjon bør ta i bruk

Som vi har sett, lykkes mange cyberangrep ganske enkelt fordi grunnleggende sikkerhetshygiene ikke er fulgt. Minimumsstandardene enhver organisasjon bør innføre, er:

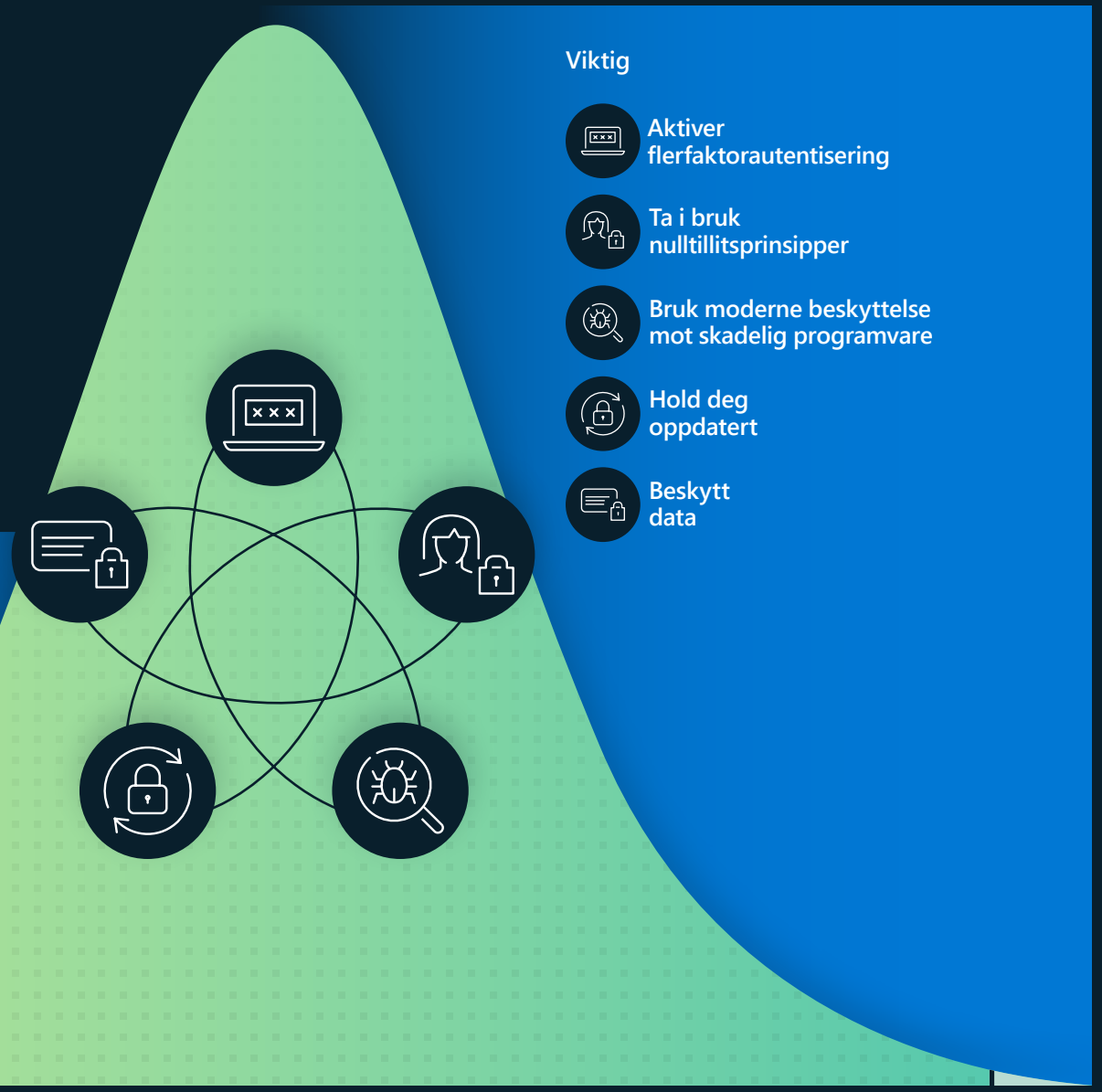
- **Aktiver flerfaktorautentisering (MFA):** For å beskytte mot kompromitterte brukerpassord og bidra til å gi ekstra robusthet for identiteter.
- **Bruk prinsipper for nulltillit:** Hjørnesteinen i en robusthetsplan som begrenser innvirkningen på en organisasjon. Disse prinsippene er:

1. – Verifiser eksplisitt – sørg for at brukere og enheter er i en god tilstand før du gir tilgang til ressurser.
2. – Bruk tilgang med minimale rettigheter – tillat bare de nødvendige privilegiene for tilgang til en ressurs og ikke mer.
3. – Anta innbrudd – anta at systemforsvaret har blitt brutt og at systemer kan bli kompromittert. Dette betyr kontinuerlig overvåking av miljøet for mulige angrep.

- **Bruk utvidet oppdagelse og svar mot skadelig programvare:** Implementer programvare for å oppdage og automatisk blokkere angrep og gi innsikt til sikkerhetsoperasjonene. Overvåking av innsikt fra systemer for trusseloppdagelse er avgjørende for å kunne svare på trusler i tide.
- **Hold deg oppdatert:** Systemer som er utdaterte og ikke oppdaterte, er en viktig grunn til at mange organisasjoner blir offer for et angrep. Sørg for at alle systemer holdes oppdatert, inkludert fastvare, operativsystem og apper.
- **Beskytt data:** Kjennskap til viktige data, hvor de er plassert og om de riktige systemene er implementert, er avgjørende for å implementere riktig beskyttelse.

98 %

Grunnleggende sikkerhetshygiene beskytter fortsatt mot 98 % av angrepene



Sluttnoter

1. Endpoint Detection and Response (EDR) er en plattform for endepunktsikkerhet som hjelper bedriftsnettverk med å forebygge, oppdage, undersøke og reagere på avanserte trusler. Funksjoner for endepunktsoppdagelse og -respons gir avanserte angrepsoppdaginger som er i nær sanntid og er handlingsbare. Sikkerhetsanalytikere kan prioritere varsler effektivt, få innsyn i hele omfanget av et innbrudd og iverksette tiltak for å utbedre trusler.
2. En Endpoint Protection Platform (EPP) er en løsning som distribueres på endepunktsenheter for å forhindre filbasert skadelig programvare, oppdage og blokkere skadelig aktivitet fra klarerte og ikke-klarerte apper, og for å levere undersøkelses- og utbedringsfunksjonene som trengs for å dynamisk reagere på sikkerhetshendelser og -varsler.
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 sikkerhetsfunksjoner for Windows 11 bidrar til beskyttelse av hybridarbeid | Microsoft Security Blog
8. FIDO Alliance: Åpne godkjenningsstandarder sikrere enn passord
9. https://interpret.ml/
10. OWASP topp ti | 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 Forbedring av nasjonens cybersikkerhet
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

Arbeidsgrupper som har bidratt

Arbeidsgrupper som har bidratt

Dataene og innsikten i denne rapporten ble levert av en mangfoldig gruppe sikkerhetsfokuserte fagfolk, som arbeider på tvers av mange Microsoft-team. Samlet sett er målet deres å beskytte Microsoft, selskapets kunder og verden generelt mot trusler fra nettangrep. Vi er stolte av å dele denne innsikten åpent, med et felles mål om å gjøre den digitale verden til et tryggere sted for alle.

AI for Good Research Lab: Utnytter kraften i data og AI for å håndtere mange av verdens utfordringer. Laboratoriet samarbeider med organisasjoner utenfor Microsoft og bruker AI til å forbedre næringsveier og miljøer. Fokusområder inkluderer nettsikkerhet (desinformasjon, cybersikkerhet, sikkerhet for barn), katastroferespons, bærekraft og AI for helse.

Azure Edge & Platform, Enterprise & OS Security: Ansvarlig for kjerneoperativsystemet og plattformsikkerheten på tvers av Windows, Azure og andre Microsoft-produkter. Teamet bygger bransjeledende sikkerhets- og maskinvareløsninger inn Microsoft-plattformene for å redusere utnyttelsen, identiteten og skadelig programvare fra brikken til skyen. Skaperne av Microsoft Secured-core-plattform på tvers av pc, kanten og server, den beste Microsoft Pluton-sikkerhetsprosessoren og mer.

Azure Networking, Core: Et skynettverksteam som fokuserer på Microsoft WAN, datasenternettverk og programvaredefinert nettverksinfrastruktur i Azure, inkludert DDoS-plattformen, nettverkskantplattformen og nettverkssikkerhetsprodukter som Azure WAF, Azure Firewall og Azure DDoS Protection Standard.

Cloud Security Research-teamet: Ved å sikre Microsoft-skyen bygger de innovative sikkerhetsfunksjoner og produkter og gjennomfører forskning, beskytter og styrker dette teamet Microsoft-kundene med å transformere organisasjonene sine på en sikker måte.

Customer Security and Trust (CST): En tverrfaglig gruppe som driver kontinuerlig forbedring av kundesikkerheten i Microsoft-produktene og nettjenestene våre. Ved å arbeide med ingeniør- og sikkerhetsteam over hele selskapet sikrer CST samsvar, forbedrer sikkerheten og sørger for gjennomsiktighet for å beskytte kundene og fremme global tillit til Microsoft.

Customer Success: Sikkerhetsteam i Customer Success samarbeider direkte med kunder for å dele anbefalte fremgangsmåter, erfaringer og veiledninger for å akselerere sikkerhetstransformasjon og -modernisering. Dette teamet samler og organiserer anbefalte fremgangsmåter og erfaringer fra Microsofts egen utvikling – så vel som erfaringer fra kundene våre – og gjør dem om til referansestrategier, referansearkitekturer, referanseplaner og mer.

Cyber Defense Operations Center (CDOC): Microsofts cybersikkerhets- og forsvarsanlegg er en smeltedigel som samler sikkerhets-personell fra hele selskapet for å beskytte bedriftsinfrastrukturen og skyinfrastrukturen vår som kundene har tilgang til. Ansvarlige for hendelsesrespons jobber sammen med dataforskere og sikkerhetspersonell fra alle Microsofts tjeneste-, produkt- og enhetsgrupper for å bidra til å beskytte, oppdage og svare på trusler hele døgnet.

Democracy Forward Initiative: Dette er et Microsoft-team som arbeider for å bevare, beskytte og fremme det grunnleggende ved demokratiet ved å fremme et sunt informasjonsøkosystem, sikre åpne og trygge demokratiske prosesser og fremme bedriftenes samfunnsansvar.

Digital Crimes Unit (DCU): En gruppe advokater, etterforskere, dataforskere, ingeniører, analytikere og forretningspersoner som er dedikert til å bekjempe cyberkriminalitet på globalt nivå ved hjelp av teknologi, etterretning, sivile søksmål, anmeldelse av kriminalitet og både offentlige og private partnerskap.

Digital Diplomacy: Et internasjonalt team av tidligere diplomater, politikere og juridiske eksperter som arbeider for å fremme et fredelig, stabilt og sikkert cyberspace i møte med økende nasjonsstatskonflikter.

Digital Security & Resilience (DSR): En organisasjon dedikert til å gjøre det mulig for Microsoft å bygge de mest pålitelige enhetene og tjenestene, samtidig som selskapet vårt er trygt, og både selskapets og kundedataene våre beskyttes.

Digital Security Unit (DSU): Et team av cybersikkerhetsadvokater og analytikere som tilbyr juridisk, geopolitisk og teknisk ekspertise for å beskytte Microsoft og kundene våre. DSU bygger tillit til Microsofts sikkerhetsforsvar mot avanserte cybermotstandere over hele verden.

Digital Threat Analysis Center (DTAC): Et team av eksperter som analyserer og rapporterer om nasjonalstatstrusler, inkludert cyberangrep og påvirkningsoperasjoner. Teamet kombinerer informasjon og cybertrusseletterretning med geopolitisk analyse for å gi innsikt til kundene våre og til Microsoft for å informere om effektiv respons og beskyttelse.

Enterprise and Security: Et team som tilbyr en moderne, sikker og håndterlig plattform for den intelligente skyen og den intelligente kanten.

Enterprise Mobility: Et team som bidrar til å levere moderne arbeidsplasser og moderne administrasjon for å holde data sikre – i skyen og lokalt. Endpoint Manager inkluderer tjenestene og verktøyene som Microsoft og kundene bruker til å administrere og overvåke mobilenheter, stasjonære datamaskiner, virtuelle maskiner, innebygde enheter og servere.

Arbeidsgrupper som bidrar

Fortsettelse

Enterprise Risk Management: Et team som arbeider på tvers av forretningsenheter for å prioritere risikodiskusjoner med toppledelsen i Microsoft. ERM kobler sammen flere driftsrisikoteam, administrerer Microsoft virksomhetsrisikorammeverk og forenkler selskapets interne sikkerhetsvurderinger ved hjelp av NIST Cybersecurity Framework.

Global Cybersecurity Policy: Et team som arbeider med myndigheter, frivillige organisasjoner og bransjepartnere for å fremme offentlige retningslinjer for cybersikkerhet som gjør at kundene kan forsterke sikkerheten og robustheten når de implementerer og bruker Microsoft-teknologi.

Identity and Network Access (IDNA) Security: Et team som arbeider for å beskytte Microsoft mot uautorisert tilgang og svindel. IDNA Security er et tverrfaglig team av teknikere, produktledere, dataforskere og sikkerhetsforskere.

M365 Security: En organisasjon som utvikler sikkerhetsløsninger, inkludert Microsoft Defender for endepunkt (MDE), Microsoft Defender for identitet (MDI) og andre, for å sikre bedriftskunder.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Et rådgivende styre i Microsoft som har som mål å sikre at ny teknologi utvikles og utplasseres på en ansvarlig måte.

Microsoft Bing Search and Distribution: Et team som er dedikert til å tilby en internettsøkemotor i verdensklasse, slik at brukere over hele verden kan finne pålitelige søkeresultater og informasjon raskt, inkludert sporing av emner og populære historier som er viktige for dem, samtidig som de gir brukerne kontroll over personvernet.

Microsoft Customer and Partner Solutions: Microsofts enhetlige kommersielle markedsverdiorganisasjon som er ansvarlig for feltroller som sikkerhet, tekniske salgsspesialister og rådgivere.

Microsoft Defender Experts: Microsofts største globale organisasjon av produktfokuserte sikkerhetsanalytikere, forskere og trusseletterretningsanalytikere. Defender-ekspertene leverer innovative oppdagelses- og responsfunksjoner i Microsoft 365-sikkerhetsprodukter og til Microsoft Defender Experts administrerte tjenester.

Microsoft Defender for IoT: Et team bestående av domeneekspertforskere som spesialiserer seg på omvendt utvikling av skadelig IoT/OT-programvare, protokoller og fastvare. Teamet jakter på IoT/OT-trusler for å avdekke skadelige trender og kampanjer.

Microsoft Defender Threat Intelligence (RiskIQ): Et team som produserer taktisk etterretning gjennom analyse av Microsofts omfattende eksterne telemetrisamling, kartlegger trussellandskapet etter hvert som det utvikler seg for å oppdage tidligere ukjent trusselinfrastruktur og legger til kontekst til trusselaktører og -kampanjer. Teamet publiserer regelmessig tidsaktuell og målrettet forskning for å levere avgjørende taktisk intelligens til forsvarere.

Microsoft Security Business Development Team: Et team som leder Microsoft strategi for cybersikkerhetsvekst, partnerskap og strategiske investeringer.

Microsoft Security Response Center (MSRC): Et team med sikkerhetsforskere som jobber for å beskytte økosystemet til Microsofts kunder og partnere. MSRC er en integrert del av Microsofts Cyber Defense Operations Center (CDOC) og samler sikkerhetsresponseksperter for å oppdage og svare på trusler i sanntid.

Microsoft Security Services for Incident Response: Et team av cybersikkerhetseksperter som hjelper kunder gjennom hele cyberangrepet fra etterretning til vellykkede begrensnings- og gjenopprettingsrelaterte aktiviteter. Tjenester tilbys via to svært integrerte team, Detection and Response Team (DART) med fokus på undersøkelse og grunnlag for gjenoppretting, og Compromise Recovery Security Practice (CRSP), som fokuserer på begrensning og gjenoppretting.

Microsoft Threat Intelligence Center (MSTIC): Et team som har fokus på å identifisere, spore og samle inn informasjon relatert til de mest sofistikerte og avanserte motpartene som påvirker Microsoft-kundene, inkludert statlige trusler, skadelig programvare og phishing.

One Engineering System (1ES): Et team som har som mål å levere verktøy i verdensklasse for å hjelpe Microsoft-utviklere å være så produktive og sikre som mulig. Teamet leder den sentrale strategien for å sikre Microsofts ende-til-ende-programvareforsyningskjede.

Operational Threat Intelligence Center (OpTIC): Teamet som er ansvarlige for å administrere og spre cybertrusselinformasjon som støtter Microsoft Cyber Defense Operation Centers (CDOC) oppdrag med å beskytte Microsoft og kundene våre.

Microsoft

Fremhev trussellandskapet og styrk et digitalt forsvar

- Finn ut mer: **https://microsoft.com/mddr**
- Dykk dypere: **https://blogs.microsoft.com/on-the-issues/**
- Hold kontakten: **@msftissues og @msftsecurity**