LOIHDE

KYBERKATSAUS

3.2025

Tiivistelmä

Maaliskuussa kybermaailmassa on jälleen julkaistu vakavia haavoittuvuuksia monissa yleisesti käytetyissä ohjelmistoissa. Suomalaisissa organisaatiossa merkittävimpänä uhkana ovat pääsääntöisesti taloudellisesti motivoituneet toimijat, mutta myös erilaiset haktivistit ja valtiolliset toimijat muodostavat uhkia. Merkittävien tietoturvahaavoittuvuuksien ja muiden uhkien vuoksi organisaatioiden on pysyttävä ajan hermolla pitääkseen ympäristönsä suojattuina.

Tunnusten kalastelu ja huijausyritykset ovat olleet maaliskuun aikana nosteessa. Etenkin vaarantuneiden tunnusten käyttö kalastelukampanjoiden jatkamiseksi on korostunut. Tunnusten kalastelun ensisijainen tavoite on taloudellinen hyöty esimerkiksi laskuhuijausten muodossa ja jalansijan pitäminen organisaatioiden pilvipalveluissa.

Kiristyshaittaohjelmia on esiintynyt myös suomalaisissa organisaatiossa maaliskuun aikana. Kohteeksi voi joutua mikä tahansa organisaatio, josta uhkatoimijat kokevat voivansa hyötyä taloudellisesti. Tietoturvan jatkuva kehittäminen on ensisijaisen tärkeää, jotta riski onnistuneen kiristyshaittaohjelman toteutumiseksi pystytään minimoimaan. Tämän lisäksi yritysten on syytä tarkistaa varautumissuunnitelmansa ja varautua esimerkiksi tietoliikenteen ja sähkönjakelun katkoksiin.

Suojelupoliisi julkaisi maaliskuun alussa kansallisen turvallisuuden katsauksen, jossa se kertoi Suomeen kohdistuvista kyberuhkista. Erityisesti Venäjän ja Kiinan tuomia kyberuhkia on painotettu tämän vuoden katsauksessa ja niihin liittyen Supo julkaisikin myös analyysiä edellä mainittujen kybervaikuttamisen infrastruktuurista.

Maaliskuun loppupuolella laajaa keskustelua on herättänyt Oracle Cloudiin kohdistunut mahdollinen tietomurto. Uhkatoimija väittää saaneensa haltuunsa yli 140 000:n Oracle Cloud -asiakkaan asiakastietoja. Lisäksi ulkoasiainhallinto ilmoitti tutkivansa keskusrikospoliisin kanssa epäiltyä tietomurtoa etäyhteyspalvelimessa.

Alkuvuoden perusteella voidaan kyberturvallisuuteen liittyvien uhkien osalta odottaa aktiivista loppukevättä. Rikollisten toiminta on aktiivista ja tähän trendiin ei näytä tulevan muutosta. Geopoliittinen tilanne aktivoi valtiollisia toimijoita, mutta mahdollistaa myös rikollisille erilaisia keinoja käyttää kyvykkyyksiään omien päämääriensä ajamiseksi. Suomalaisten yritysten on myös syytä tunnistaa oma potentiaalinsa hyökkäyksen mahdollistavana kohteena; yrityksen kautta vaikuttamalla hyökkääjä voi päästä käsiksi esimerkiksi kriittisen infrastruktuurin tai huoltovarmuuden kannalta tärkeisiin toimijoihin.

KUUKAUSIRAPORTTI 3/2025

Tämä raportti sisältää kuvauksen maaliskuun 2025 kybertapahtumista. Raportin sisältö pohjautuu avoimiin lähteisiin, joita ovat esimerkiksi uutiset, sosiaalisen median palvelut ja muut aiheeseen liittyvät verkkolähteet. Raportti tuo esille kyberturvallisuuteen liittyviä merkittäviä tapahtumia ja trendejä, jotka vaikuttavat meidän ja asiakkaidemme toimintaan.

Sisällys

1. Yleistilanne

Suomalaisissa yrityksissä kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa eikä niiden vähenemisestä ole merkkejä. Suomalaisille yrityksille ja organisaatioille keskeisin kyberuhka ovat taloudellisesti motivoituneet rikolliset toimijat. Näiden lisäksi tietyille tahoille uhkaa muodostavat myös haktivistit ja valtiolliset toimijat. Edellä mainittuihin uhkiin vastaaminen vaatii organisaatioilta aktiivisia toimia ja jatkuvaa kyberturvallisuuden kehitystyötä.

Tilanne Suomen lähialueella on ollut jännitteinen jo muutamien vuosien ajan. Itämeren valtiot ovat joutuneet toistuvasti Venäjän aggressiivisen retoriikan ja toiminnan kohteeksi. Harjoitustoiminnan häiritseminen, alueloukkaukset, mahdollisesti vaurioitettu infrastruktuuri ja negatiivinen retoriikka ovat vakiintuneet osaksi Suomen lähialueen arkipäivää. Lisäksi Itämeren vedenalaista infrastruktuuria on vahingoitettu toistuvasti Suomen lähialueella. Suomalaisten yritysten on syytä ottaa tämä huomioon omassa toiminnassaan ja riskiarvioissaan.

Tietoturvaan liittyvät uhat voivat olla sekä paikallisia että kansainvälisiä. Paikallisiin uhkiin vaikuttaa Suomen geopoliittinen asema ja kohdennetut kampanjat rikollisten taholta. Kansainvälistä uhkaa edustavat esimerkiksi globaalisti hyväksikäytettävät verkon reunalaitteiden haavoittuvuudet. Näihin uhkiin varautuminen edellyttää jatkuvaa työskentelyä ja kehittämistä tietoturvaan liittyen. Valvonta, reagointikyky ja poikkeamiin valmistautuminen ovat keskeinen osa jatkuvuuden varmistamista.

2. Haavoittuvuudet

2.1 CVE-2025-23120: Veeam Backup & Replication authenticated RCE

Varmuuskopioratkaisuja tarjoava Veeam julkaisi maaliskuussa tiedotteen kriittisestä haavoittuvuudesta sen Backup & Replication -ohjelmistossa.[1] CVE-2025-23120:n hyväksikäyttö mahdollistaa mielivaltaisen koodin suorittamisen kenen tahansa Veeam-palvelimen Builtin Users -ryhmään kuuluvan käyttäjän toimesta. Oletuksena tämä kattaa jokaisen domainin käyttäjän, mikäli Veeam-palvelin on liitetty Active Directory -domainiin.[2]

WatchTowr Labs:n analyysin mukaan haavoittuvuus on hyvin samankaltainen kuin viime syksyllä samasta tuotteesta julkaistu haavoittuvuus CVE-2024-40711. Veeamin haavoittuvuudet, kuten CVE-2024-40711, ovat laajalti kiristyshaittaohjelmatoimijoiden suosiossa ja heidän on havaittu aktiivisesti hyväksikäyttävän näitä. Korjaava päivitys on

[1] Arctic Wolf, 21.03.2025, CVE-2025-23120: Critical Remote Code Execution Vulnerability in Veeam Backup & Replication, https://arcticwolf.com/resources/blog/cve-2025-23120/
[2] watchTowr Labs, 20.03.2025, By Executive Order, We Are Banning Blacklists - Domain-Level RCE in Veeam Backup & Replication (CVE-2025-23120), https://labs.watchtowr.com/by-executive-order-we-are-banning-blacklists-domain-level-rce-in-veeam-backup-replication-cve-2025-23120/

julkaistu ja haavoittuvat versiot (12.3.0.310 ja vanhemmat) suositellaan päivitettäväksi pikimmiten.[3]

2.2 CVE-2025-29927: Next.js Authorization bypass

Maaliskuussa löydettiin kriittinen haavoittuvuus CVE-2025-29927 avoimen lähdekoodin Next.js frameworkista, joka mahdollistaa hyökkääjien ohittavan käyttöoikeuksien tarkastuksia. Next.js on web-sovellusten rakentamiseen hyvin laajalti käytetty Reactin framework ja sillä on viikoittain yli 9 miljoonaa latausta npm-paketinhallinnasta.

Haavoittuvuutta hyväksikäyttämällä on mahdollista ohittaa Next.js:n middleware-komponentin tekemät tarkistukset, joita tyypillisesti käytetään tunnistautumiseen ja valtuutuksiin. Hyväksikäyttö on yksinkertainen ja tapahtuu ”x-middleware-subrequest” -HTTP headeria käyttämällä. Next.js-versiot ennen 15.2.3, 14.2.25, 13.5.9 ja 12.3.5 ovat haavoittuvia.[4]

2.3 ”IngressNightmare”: Unauthenticated RCE Vulnerabilities in Ingress NGINX

Maaliskuun lopulla julkaistiin Wiz:n tutkijoiden Kubernetesin Ingress NGINXControllerista löytämä kokoelma haavoittuvuuksia (CVE-2025-1097, CVE-2025-1098, CVE-2025-24514 ja CVE-2025-1974), joita ketjuttamalla tunnistautumattoman hyökkääjän on mahdollista suorittaa mielivaltaista koodia etänä. Ingress NGINX:ää käytetään ohjaamaan julkiverkosta tulevia pyyntöjä Kubernetes-palveluille toimien käänteisenä välityspalvelimena.[5]

Hyväksikäyttämällä haavoittuvuuksia ketjutetusti hyökkääjän on mahdollista syöttää NGINX:lle haitallinen konfiguraatio ja suorittaa haitallinen binääri. Korjaus haavoittuvuuteen on julkaistu Ingress NGINX Controllerin versioissa 1.12.1 ja 1.11.5, ja se suositellaan asentamaan kiireellä. Mikäli päivitys ei ole mahdollista, suositellaan harkitsemaan Wiz:n mainitsemia workaroundeja.[5]

[3] Veeam, 19.03.2025, CVE-2025-23120, https://www.veeam.com/kb4724
[4] Bleeping Computer, 24.03.2025, Critical flaw in Next.js lets hackers bypass authorization, https://www.bleepingcomputer.com/news/security/critical-flaw-in-nextjs-lets-hackers-bypass-authorization/
[5] Wiz, 24.03.2025, IngressNightmare: 9.8 Critical Unauthenticated Remote Code Execution Vulnerabilities in Ingress NGINX, https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities

3. Kalastelu ja huijaukset

Microsoft 365 -tunnusten kalastelu on jälleen ollut nosteessa maaliskuun aikana. Erityisesti ovat korostuneet vaarantuneilla tunnuksilla lähetetyt kalasteluviestit. Vastaanottajan voi olla haastavaa tunnistaa viesti kalasteluksi, koska se tulee tutulta lähettäjältä eikä välttämättä sisällä mitään suoraan haitallisia viitteitä. Seurauksena vaarantuneiden tunnusten määrä kasvaa helposti moninkertaisesti, koska viestejä lähetetään laajasti eri organisaatioiden välillä, eivätkä monissa tapauksissa organisaatiot itse tiedä tunnustensa vaarantuneen ennen kuin ulkopuolinen taho siitä ilmoittaa. Tunnusten vaarantuessa Azure- ja M365-ympäristöihin olisi syytä suorittaa perusteellinen tutkinta, jotta uhkatoimijan tekemät toimet saadaan selville ja mahdolliset lisäjalansijat pystytään poistamaan ympäristöstä.

Loihteen CSOC on havainnut tunnusten kalastelua, joissa kalasteluviesti on sisältänyt useamman vaiheen. Vastaanottajalle on saapunut kalasteluviesti yleensä tutulta lähettäjältä, mutta tunnukset ovat olleet vaarantuneena. Viesti on sisältänyt linkin, joka on vienyt Microsoftin Forms-lomakkeeseen. Lomakkeessa on ollut linkki seuraavalle sivustolle, joka on sisältänyt CloudFlaren Turnstile:n.[6] Tämän jälkeen linkkiketju on vienyt väärennetylle Microsoft 365 -kirjautumissivulle. Tunnusten syöttäminen tälle sivustolle johtaa lopulta Adversary-in-the-Middle[7] -tyyppiseen tunnusten kalasteluun, jolla uhkatoimija saa anastettua tunnukset monivaiheisesta tunnistautumisesta huolimatta.

Mainittu tapahtumaketju kuvastaa sitä, miten uhkatoimijat yrittävät ohittaa sähköpostisuojaukset käyttämällä CAPTCHA:a ja esimerkiksi Microsoftin omia palveluita ja domaineja haitallisten tavoitteidensa saavuttamiseksi. Näihin liittyy kuitenkin aina lopulta yritys kalastella käyttäjän tunnukset, useimmiten juuri väärennetyn Microsoft 365 -kirjautumissivun avulla. Organisaatioiden olisi tärkeää miettiä Conditional Access Policyjen käyttöönottoa Microsoftin palveluihin. Suositeltavaa olisi rajata kirjautumiset organisaation resursseihin ainoastaan luotetuista IP-osoitteista tai laitteista.[8] AiTM-kalastelu on tullut jäädäkseen ainakin niin pitkään kuin valtaosa edelleen käyttää perinteisiä sisäänkirjautumismenetelmiä ilman riittäviä rajoituksia.

[6] https://www.cloudflare.com/application-services/products/turnstile/
[7] https://techcommunity.microsoft.com/blog/microsoftsentinelblog/identifying-adversary-in-the-middle-aitm-phishing-attacks-through-3rd-party-netw/3991358
[8] https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-alt-all-users-compliant-hybrid-or-mfa

4. Kiristyshaittaohjelmat ja -toimijat

Yhdysvalloissa BianLian-kiristyshaittaohjelmatoimijan nimissä on lähetetty useita lunnasvaatimuksia fyysisen kirjeen muodossa. Kirjeissä on väitetty BianLianin saaneen organisaation tiedot käsiinsä ja että ne uhataan vuotaa BianLianin TOR-sivustolla. Lunnasvaatimukset vaikuttavat olevan huijausta, koska yksikään kirjeen saanut organisaatio ei ole löytänyt viitteitä datan vuotamisesta verkostaan. [9]

S-RM uutisoi kiristyshaittaohjelmatapauksesta, jossa Akira-toimija on ajanut kiristyshaittaohjelmaa hieman poikkeuksellisella tavalla. Päätelaitesuojauksen (EDR) estäessä kiristyshaittaohjelman ajon Windows-laitteilla, Akira löysi samasta verkosta suojaamattoman web-kameran ja onnistui pääsemään sen sisälle tunnetun haavoittuvuuden avulla. Web-kameran kautta Akira onnistui yhdistämään Windows-laitteille SMB:llä ja salaamaan tiedostot sitä kautta, käytännössä ohittaen EDR:n. [10]

Viime kuussa Black Basta -haittaohjelmatoimijan keskustelulokit vuotivat ja useampi taho on ehtinyt käymään niitä läpi. EclecticIQ on löytänyt lokien avulla aikaisemmin tuntemattoman BRUTED-työkalun, jota Black Basta on käyttänyt. Käytännössä BRUTED automatisoi brute force -hyökkäyksiä eri julkiverkon palveluihin, kuten Citrix Gateway:hin ja palomuurien SSL VPN:ään kierrättäen liikenteen proxy-verkon kautta. Vastaavia työkaluja on muitakin, mutta BRUTED on hyvä esimerkki, miksi julkiverkon palveluiden koventaminen on tärkeää. [11]

[9] Arctic Wolf, 4.3.2025, Self-Proclaimed “BianLian Group” Uses Physical Mail to Extort Organizations, https://arcticwolf.com/resources/blog/self-proclaimed-bianlian-group-uses-physical-mail-to-extort-organizations/
[10] S-RM, 5.3.2025, Camera off: Akira deploys ransomware via webcam, https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam
[11] EclecticIQ, 13.3.2025, Inside BRUTED: Black Basta (RaaS) Members Used Automated Brute Forcing Framework to Target Edge Network Devices, https://blog.eclecticiq.com/inside-bruted-black-basta-raas-members-used-automated-brute-forcing-framework-to-target-edge-network-devices

5. Muuta

5.1 Oracle Cloudin mahdollinen tietomurto

Nimeä ”rose87168” kantava uhkatoimija väittää saaneensa haltuun yli 140 000:n Oracle Cloud -asiakkaan asiakastietoja. Toimijan mukaan tiedot sisältävät mm. kryptattuja SSO-salasanoja, salaisuuksia (kuten JKS-tiedostoja) ja muita salaisuuksiin sekä salasanoihin liittyviä tietoja. Uhkatoimija on tarjoutunut jakamaan tietoja sille taholle, joka auttaa tätä avaamaan kryptattuja tietoja.[12]

BleepingComputerin mukaan Oracle itse kieltää tietomurron tapahtuneen ja että asiakastietoja ei olisi vaarantunut.[13] Tapaus on kuitenkin herättänyt laajalti keskustelua ja huolta. CloudSEK on analysoinut artikkelissaan vuoden 2021 Oracle Access Managerin haavoittuvuutta CVE-2021-35587, joka saattaisi liittyä tapaukseen. Raportin kirjoitushetkellä tapauksesta on kuitenkin vielä suhteellisen niukasti tietoa saatavilla.

5.2 Supo: Kansallisen turvallisuuden katsaus 2025

Suojelupoliisi kertoo kansallisen turvallisuuden katsauksessaan, että Venäjä ja Kiina muodostavat merkittävän kyberuhkan Suomelle. Tämä poikkeaa aiempien vuosien katsauksista niin, että esimerkiksi molempien valtioiden kyberekosysteemejä on esitelty tarkemmin.[14] Venäjän lähentyminen Kiinan kanssa, geopoliittinen tilanne, lännen kasvava Kiina-vastaisuus ja Suomen Nato-jäsenyys ovat lisänneet Suomeen kohdistuvaa kiinnostusta kyberuhkien näkökulmasta.[15]

Supon mukaan kiinalaiset kybertoimijat hyödyntävät toiminnassaan suomalaista tietoverkkoinfrastruktuuria, jota he käyttävät muihin maihin kohdistuvissa kyberoperaatioissa. Lisäksi kuluttajille suunnatut verkkolaitteet korostuvat kyberoperaatioissa. Erityisesti kotireitittimet ovat alttiita tietoturvauhkille, koska ne ovat monesti päivittämättömiä ja puutteellisesti suojattuja. Kotireitittimien suuren määrän vuoksi hyökkäyspinta-ala on merkittävä.[16]

[12] https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants
[13] https://www.bleepingcomputer.com/news/security/oracle-denies-data-breach-after-hacker-claims-theft-of-6-million-data-records/
[14] https://katsaus.supo.fi/autoritaaristen-valtioiden-kyberekosysteemit
[15] https://katsaus.supo.fi/vakoilun-ja-vaikuttamisen-tilannekatsaus
[16] https://katsaus.supo.fi/vakoilun-ja-vaikuttamisen-tilannekatsaus

6. Suositukset

Tässä kuussa suosittelemme:

1. Sähköpostisuojauksen asetusten katselmointi
2. Merkittävän tietoturvapoikkeaman viestinnän suunnitelmien tarkastaminen ja harjoittelu
3. Luotetun DFIR-kumppanin valinta ja kontaktointi

Kalasteluviestit ovat edelleen yleisin hyökkäysvektori organisaatioiden järjestelmiin. Tämän vuoksi suosittelemme käytössä olevan sähköpostisuojauksen asetusten läpikäyntiä. Monissa tapauksissa käytössä on palveluntarjoajan oletusasetukset, jotka olisivat suositeltavaa konfiguroida organisaation tarpeita paremmin vastaaviksi. Esimerkiksi Microsoftilla on Defender for Office 365 -tuotteeseensa konfigurointiohje[17], jota voi käyttää pohjana kyseisen tuotteen konfiguroinnille. On kuitenkin syytä huomioida, että jokaisella organisaatiolla on erilaiset tarpeet, joten asetukset on räätälöitävä organisaation tarpeiden mukaiseksi, jotta päivittäistä toimintaa haittaavilta ongelmilta vältyttäisiin. Lisäksi suosittelemme SPF:n, DKIM:n ja DMARC:in konfiguroimista päälle sähköpostiliikenteen suojaamiseksi.[18]

Merkittävän poikkeaman sattuessa viestintä on merkittävässä roolissa sekä sisäisesti että yhteistyökumppaneiden ja asiakkaiden suuntaan. Poikkeaman aikana tilannekuva päivittyy jatkuvasti ja viestinnän tarve voi muuttua nopeasti. Viestintään liittyen on syytä suunnitella ja varautua erilaisiin skenaarioihin, jotta tositilanteessa valmiita suunnitelmia voidaan käyttää mahdollisimman helposti hyödyksi. Suosittelemme käymään läpi viestintään liittyvät suunnitelmat ja tarkastamaan, ovatko ne ajan tasalla. Suunnitelmaa tarkastaessa on hyvä miettiä, onko niissä huomioitu esimerkiksi tarve asiantuntijoiden tietotaidolle tai yrityksen johdon linjaukselle. Kriisitilanteessa viestintää ei voida toteuttaa erillisessä kuplassa, vaan se voi vaatia esimerkiksi teknisen asiantuntijan, yrityksen johdon ja viestintätiimin tiivistä yhteistyötä onnistuakseen.

Poikkeamaan valmistauduttaessa suunnitelmien ja prosessien päivittäminen on tärkeää, sillä ne voivat vaatia muutoksia ollakseen toimivia. Samalla on hyvä pyrkiä arvioimaan, ovatko suunnitelmat edelleen sellaisia, että ne vastaavat parhaalla mahdollisella tavalla poikkeamatilanteisiin varautumiseen. Suunnitelmiin liittyen konkreettinen ja asioita helpottava toimi on valita DFIR-kumppani tai kontaktoida jo olemassa olevaa kumppania. Tämä helpottaa siksi, että kumppanin kanssa keskustelu voi tuoda uutta näkemystä varautumiseen ja se avaa käytännön asioita, kuten avun hälyttämisen ja palvelun hinnan tietoja. Onkin hyvä käydä nämä keskustelut silloin, kun poikkeama ei ole käynnissä.

[17] https://learn.microsoft.com/en-us/defender-office-365/recommended-settings-for-eop-and-office365
[18] https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

Tämän raportin koostaa
Loihteen asiakkaille
kuukausittain
Loihteen CSOC:n eli
kyberturvakeskuksen
asiantuntijat hyödyntäen sekä
avoimia lähteitä että omaa
tietämystään.

Kellon ympäri miehitetty
kyberturvakeskuksemme valvoo
ja reagoi tietoturvatapahtumiin
pitäen huolen siitä, että
asiakkaamme voivat rauhassa
keskittyä liiketoimintaansa.

Lue lisää:
www.loihde.com/palvelut/kyberturva/

LOIHDE