Kyberkatsaus

4/2025

LOIHDE

Tiivistelmä

Huhtikuun haavoittuvuustilanne oli melko tyypillinen. Microsoftin päivitystiistaina julkaistuista haavoittuvuuksista löytyi jo aktiivista hyväksikäyttöä nähnyt haavoittuvuus Windowsissa. Lisäksi verkkolaitteista Ivantin Connect Securesta löydettiin RCE-haavoittuvuus. Etenkin reunalaitteiden haavoittuvuudet ovat korostuneet viimeisen vuoden aikana, ja ne eivät vaikuta olevan rauhoittumaan päin. Mandiantin uunituoreen M-Trends 2025 -raportin lukujen mukaan haavoittuvuuden hyväksikäyttö on viidettä vuotta putkeen kaikista yleisin saastumisvektori heidän tutkimissaan tietomurroissa (33 % kaikista poikkeamista, joissa saastumisvektori tunnistettiin). Hyväksikäytetyimmät haavoittuvuudet ovat juuri verkon reunalaitteissa.[1] Organisaatioiden on syytä ottaa tämä huomioon haavoittuvuuksien- ja muutostenhallinnassa. Suomalaisissa organisaatiossa merkittävimpiä uhkia muodostavat taloudellisesti motivoituneet toimijat, mutta myös erilaiset haktivistit ja valtiolliset toimijat.

Tunnusten kalastelua on tapahtunut aktiivisesti kevään aikana etenkin M365-tunnusten osalta. Lisäksi yksityishenkilöihin on kohdistunut mm. pankki- ja hotellihuijauksia. Maailmalla on myös havaittu hyvin edistyksellistä, kohdistettua tietojenkalastelua Ukrainaa tukevia tahoja kohtaan.

Eduskunta hyväksyi hallituksen esityksen kansallisesta kyberturvallisuuslaista 8.4.2025. Tämä tarkoittaa uusia velvoitteita ja toimenpiteitä yhteiskunnan kriittisillä toimialoilla toimiville organisaatioille.

Tietoturvahaavoittuvuuksiin käytetyn CVE-tietokannan rahoitus lakkautettiin 16.4.2025 DHS:n toimesta. Yhdysvaltain kyberturvallisuusvirasto CISA kuitenkin varmisti rahoituksen seuraavan 11 kuukauden ajaksi. Tämä on herättänyt huhtikuussa keskustelua ja mahdollisia vaihtoehtoisia ratkaisuja CVE-järjestelmälle on mietitty sen epävarman tulevaisuuden vuoksi.

Kyberkatsauksessa on lisäksi nostettu esille Loihteen CSOCin huhtikuun kolme suositusta, joita hyödyntämällä organisaatiot kykenevät havaitsemaan epäilyttävää toimintaa ympäristöissään sekä suojautumaan ja palautumaan mahdollisista tietoturvapoikkeamatilanteista merkittävästi tehokkaammin.

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.

[1] Mandiant, 24.04.2025, M-Trends 2025 Report, https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

KUUKAUSIRAPORTTI 4/2025

Tämä raportti sisältää kuvauksen huhtikuun 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 organisaatioiden 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-2025-22457: Ivanti Connect Secure Remote Code Execution

Ivanti julkaisi 3.4.2025 kriittisen haavoittuvuuden heidän Ivanti Connect Secure (ICS) VPN-tuotteessaan. Haavoittuvuus CVE-2025-22457 on puskurin ylivuotohaavoittuvuus, joka mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen etänä.[2]

Mandiant julkaisi 4.4.2025 artikkelin, jossa he kertovat yhdessä Ivantin kanssa tunnistaneensa haavoittuvuuden aktiivista hyväksikäyttöä maaliskuun puolivälistä alkaen. Mandiant on attribuoinut hyökkäyskampanjan Kiina-liitännäiseen UNC5221-ryhmään. Onnistunutta hyväksikäyttöä on seurannut ryhmän käyttämien muiden haittaohjelmien, kuten muistissa ajautuvan TRAILBLAZE-dropperin ja BRUSHFIRE-takaoven lataaminen ja suorittaminen kohdelaitteella. Tutkinnan vaikeuttamiseksi UNC5221 käyttää myös hyökkäyksissään

[2] Mandiant, 04.04.2025, Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457), https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

saastuneita verkkolaitteita, kuten QNAP NAS-laitteita ja ASUS-reitittimiä piilottaakseen todellisen lähteensä.[3]

2.2 CVE-2025-24054: Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability

Maaliskuussa julkaistu Net-NTLM-tiivisteen varastamisen mahdollistava haavoittuvuus CVE-2025-24054 on ollut aktiivisen hyökkäyskampanjan kohteena maaliskuussa ja huhtikuussa. Tietoturvayhtiö Check Point raportoi 16.4. julkaistussa artikkelissaan kampanjoista, joissa mm. Puolan ja Romanian hallintoihin sekä yksityisiin organisaatioihin on lähetetty kalasteluviestejä. Viesteissä on linkki Dropbox-palvelussa jaettuun ZIP-arkistoon, jonka lataaminen ja purkaminen suorittaa haavoittuvuuden hyväksikäytön lähettäen käyttäjän Net-NTLM-tiivisteen hyökkääjälle. Hyökkääjä voi yrittää murtaa käyttäjän selkokielisen salasanan tästä tiivisteestä.[4]

Haavoittuvuuden hyväksikäyttö tapahtuu haitallisen library-ms -tiedoston kautta, ja se on hyvin samankaltainen viime marraskuussa julkaistun haavoittuvuuden CVE-2024-43451 kanssa, joka käyttää URL-tiedostopäätteitä ja kykenee käynnistymään vain minimaalisella käyttäjän vuorovaikutuksella. Tämän ja muiden vastaavien haavoittuvuuksien estämiseksi suositellaan SMB-liikenteen estämistä internetiin päin.[4]

2.3 CVE-2025-29824: Windows Common Log File System Driver Elevation of Privilege

Huhtikuun 8. päivä Microsoft julkaisi kuukausittaisten Windows-päivitystensä ohella blogikirjoituksen, jonka mukaan tuoreeltaan korjattua 0-päivähaavoittuvuutta CVE-2025-29824 on aktiivisesti hyväksikäytetty kiristyshaittaohjelmatoimijan toimesta. Microsoft on yhdistänyt hyökkäykset Storm-2460-ryhmään tutkinnassa löytämiensä viitteiden, kuten PipeMagic-haittaohjelman, perusteella. Hyökkäysten kohteina on ollut eri toimialojen organisaatioita mm. Yhdysvalloista, Venezuelasta, Espanjasta ja Saudi-Arabiasta. Hyökkäysten yhteydessä käytetty kiristyshaittaohjelma viittaa Microsoftin tutkinnan mukaan RansomEXX-haitakeperheeseen.[5]

Hyväksikäyttö kohdistuu haavoittuvuuteen Common Log File System (CLFS) kernel-ajurissa, ja se mahdollistaa hyökkääjän korottaa oikeutensa korkeimmalle eli SYSTEM-tasolle haavoittuvalla laitteella. Haavoittuvuuden piirissä on sekä Windowsin työasema- että palvelinversioita. Korjaava päivitys suositellaan asennettavaksi pikimmiten.

[3] SOCRadar, 04.04.2025, UNC5221 Targets Critical Ivanti Flaw (CVE-2025-22457) with TRAILBLAZE & BRUSHFIRE Malware, https://socradar.io/unc5221-targets-ivanti-cve-2025-22457-trailblaze-brushfire-malware/
[4] Check Point Research, 16.04.2025, CVE-2025-24054, NTLM Exploit in the Wild, https://research.checkpoint.com/2025/cve-2025-24054-ntlm-exploit-in-the-wild/
[5] Microsoft Threat Intelligence, 08.04.2025, Exploitation of CLFS zero-day leads to ransomware activity, https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

3. Kalastelu ja huijaukset

Tietoturvayhtiö Volexity kirjoittaa blogissaan tietojenkalastelukampanjasta, jossa epäillyt venäläiset uhkatoimijat ovat pyrkineet saamaan pääsyn tiettyjen henkilöiden M365-tileihin kohdistetuilla kalasteluviesteillä. Volexityn mukaan kohteena ovat olleet erilaisissa ihmisoikeuksia tukevissa kansalaisjärjestöissä työskentelevät henkilöt. Erityisesti Ukrainan sotaan liittyvät järjestöt ja asiantuntijat ovat olleet kalasteluviestien kohteena. Henkilöitä on lähestytty Signal- tai WhatsApp-viesteillä ja heidät on kutsuttu videopuheluun keskustelemaan Ukrainan tilanteesta. Lähettäjä on esiintynyt jonkin Euroopan maan poliittisena tahona ja vastaanottajalle on ehdotettu tapaamista kyseisen maan suurlähettilään tai poliitikon kanssa.[6]

Vastaanottajan reagoidessa viestiin, on tälle lähetetty ”ohjeet” puheluun liittymiseksi erillisen dokumentin muodossa. Tämän lisäksi vastaanottajalle on lähetetty vielä erillinen linkki puhelua varten, ja sitä klikkaamalla käyttäjä on päätynyt aidolle Microsoftin kirjautumissivulle. Käyttäjän syötettyä tunnuksensa on tämä uudelleenohjattu Visual Studio Code -tekstieditorin selainversioon, jossa käyttäjälle on näytetty sisäänkirjautumiskoodi. Kyseinen koodi on OAuth 2.0:ään liittyvä valtuutuskoodi, jota voidaan käyttää sisäänkirjautumiseen 60 vuorokauden ajan. Tekaistussa ohjeessa on pyydetty syöttämään kyseinen koodi ohjeessa olevaan kenttään. Tämä koodi on samalla ns. Access token, joka mahdollistaa pääsyn käyttäjätunnukselle siinä vaiheessa, kun kohde lähettää koodin toimijalle. Toimijan saadessa koodin on tämä pystynyt käyttämään sitä sisäänkirjautumiseen käyttäjätilin M365-resursseihin.[7]

Kyberturvallisuuskeskus raportoi huhtikuussa tietojenkalasteluista, joissa on käytetty hyväksi hotellien varauspalveluita. Uhkatoimija on todennäköisesti onnistunut saamaan haltuunsa hotellin käyttäjätunnukset ja hyödyntänyt näitä huijatakseen varauksia tehneitä henkilöitä. Kalasteluyritykset ovat kohdistuneet erityisesti hiljattain varauksen tehneisiin henkilöihin lähettämällä heille vahvistusviesti tehdystä varauksesta ja tämän jälkeen on lähetetty toinen viesti, jossa on pyydetty vahvistamaan maksutiedot. Lopullisena tavoitteena ovat todennäköisesti olleet taloudelliset hyödyt ja pyrkimykset varastaa asiakkaiden maksukorttitiedot.[8]

[6] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[7] https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
[8] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-162025

4. Kiristyshaittaohjelmat ja -toimijat

RedCurl-nimellä tunnettu uhkatoimija, jonka yleensä ajatellaan olevan keskittynyt tiedon keräämiseen ja vakoiluun, on alkanut käyttää hyökkäyksissään myös uutta QWCrypt-kiristyshaittaohjelmaa. QWCrypt ei tiettävästi ole muiden ryhmien käytössä. RedCurlin toimintatapa on myös poikkeuksellinen verrattuna useisiin muihin kiristyshaittatoimijoihin. Useimmat kiristyshaittatoimijat salaavat kaikki laitteet, joille saavat pääsyn, mutta RedCurl keskittyy salaamaan hypervisoreita, kuten HyperV. RedCurlin jättämä lunnasvaatimus on tehty kopioimalla muiden kiristyshaittatoimijoiden lunnasvaatimuksia eikä RedCurlilla ole omaa vuotosivustoa, joten kiristyshaittaohjelma voi olla myös hämäysyritys.[9]

Interlock-kiristyshaittatoimija on alkanut käyttää osana hyökkäyksiään mm. ClickFix-nimellä tunnettua tekniikkaa. Interlock on rekisteröinyt itsellensä useita domaineja, jotka viittaavat tunnettuihin sovelluksiin, kuten Microsoft Teams ja Advanced IP Scanner. Sivuston avatessaan käyttäjälle esitetään väärennetty Cloudflaren CAPTCHA, jossa käyttäjää pyydetään avaamaan komentorivi ja ajamaan leikepöydällä oleva teksti päästäkseen CAPTCHA:n läpi. Sivustosta riippuen leikepöydälle kopioitunut komento asentaa joko haittaohjelmalla varustetun sovelluksen asennustiedoston tai pelkän takaoven käyttäjän laitteelle.[10]

Tom Meursin väitöskirja Twenten yliopistossa tutki yli 500:aa kiristyshaittaohjelmatapausta Alankomaissa. Tutkimuksen mukaan kybervakuutuksen omaavat yritykset saivat keskimäärin 2,8 kertaa suuremman lunnasvaatimuksen kuin ei-vakuutetut yritykset, koska kiristyshaittatoimijat etsivät yrityksen datasta viitteitä vakuutuksesta ja tietävät sen myötä kysyä korkeampaa lunnasvaatimusta. Tutkimus myös painottaa hyvien varmuuskopioiden tärkeyttä. Organisaatiot, joilla on palautettavassa kunnossa olevat varmuuskopiot, maksavat 27 kertaa harvemmin lunnaita.[11]

[9] BitDefender, 26.3.2025, RedCurl's Ransomware Debut: A Technical Deep Dive, https://www.bitdefender.com/en-us/blog/businessinsights/redcurl-qwcrypt-ransomware-technical-deep-dive
[10] Sekoia, 16.4.2025, Interlock ransomware evolving under the radar, https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/
[11] Digital Trust Center, 14.4.2025, Ransomware in het mkb: Cybercriminelen verhogen losgeld bij cyberverzekering, https://www.digitaltrustcenter.nl/nieuws/ransomware-in-het-mkb-cybercriminelen-verhogen-losgeld-bij-cyberverzekering

5. Muuta

5.1 MITRE:n CVE-ohjelman rahoitus

Huhtikuussa huolta herätti MITREn[12] 15.4. antama tieto, että CVE-haavoittuvuusohjelman tuki lakkautettaisiin Yhdysvaltain sisäisen turvallisuuden ministeriön (DHS) toimesta. Kyberturvallisuusvirasto CISA kuitenkin ilmoitti 16.4., että tämä on varmistanut CVE-ohjelman rahoituksen seuraavaksi 11 kuukaudeksi. Rahoituksen jatkuminen tämän jälkeen on kuitenkin vielä epäselvää.[13]

CVE-ohjelma on ollut toiminnassa vuodesta 1999, ja sen tarkoituksena on raportoida ja dokumentoida julkisia tietoturvahaavoittuvuuksia. CVE-ohjelman merkitys tietoturvan ja haavoittuvuuksien hallinnassa on valtava, koska se takaa yksilöidyt ja keskitetyt tunnisteet tietoturvahaavoittuvuuksille.[14]

EU:n kyberturvavirasto ENISA on julkaissut 16.4. beta-version omasta haavoittuvuustietokannastaan EUVD:stä. EUVD on osa NIS2-direktiiviä. EUVD hyödyntää CVE-tunnisteita tietokannassa, mutta käyttää myös omia tunnisteita haavoittuvuuksille. EUVD astuu oletettavasti laajemmin valokeilaan vaihtoehtona CVE-ohjelmalle tämän epävarman tilanteen vuoksi.[15]

5.2 NIS2-direktiivi astunut voimaan 8.4.2025

NIS2-direktiivi on astunut voimaan 8.4.2025, tiedottaa Kyberturvallisuuskeskus. Direktiivi tuo mukanaan velvoitteita niille toimijoille, jotka toimivat yhteiskunnan kriittisillä toimialoilla.[16] Velvoitteisiin kuuluu muun muassa ilmoittautuminen oman alan valvovalle viranomaiselle. Huomioitavaa on myös se, että mikäli organisaatio kuuluu useaan NIS2-toimialaan, on jokaisen toimialan valvovalle viranomaiselle ilmoittauduttava erikseen. Ilmoittautuminen tulee tehdä 8.5.2025 mennessä.[17] Kyberturvallisuuskeskus on julkaissut listauksen toimialoista, joita direktiivi koskettaa[18] sekä toimintaohjeita.

---

[12] MITRE, 25.4.2025, https://www.mitre.org/
[13] CISA, 16.4.2025, CISA Statement on CVE Program, https://www.cisa.gov/news-events/news/cisa-statement-cve-program
[14] The Register, 16.4.2025, Uncle Sam kills funding for CVE program. Yes, that CVE program, https://www.theregister.com/2025/04/16/homeland_security_funding_for_cve/
[15] The Register, 18.4.2025, CVE fallout: The splintering of the standard vulnerability tracking system has begun, https://www.theregister.com/2025/04/18/splintering_cve_bug_tracking/
[16] Kyberturvallisuuskeskus, 10.4.2025, Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2), https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa#67853-0
[17] Kyberturvallisuuskeskus, 8.4.2025, Kyberturvallisuuslaki on hyväksytty eduskunnassa, https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet
[18] Kyberturvallisuuskeskus, 8.4.2025, NIS2-taulukko, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_08042025.pdf

6. Suositukset

Tässä kuussa suosittelemme:

1. Etähallintaohjelmistojen (RMM) käytön rajaaminen ja valvonta
2. Sysmon-lokituslaajennuksen asentaminen
3. Varmuuskopioiden hallinnan varmistaminen ja testaaminen

Erityisesti kiristyshaittaohjelmatoimijat käyttävät toimissaan RMM-ohjelmistoja, kuten AnyDeskiä, Teamvieweriä ja ScreenConnectia. Niissä on monipuolisesti toiminnallisuuksia ja siksi ne ovatkin järjestelmien ylläpitäjien suosiossa. Tämän vuoksi uhkatoimijatkin hyödyntävät niitä. Lisäksi niiden haitallinen käyttö on vaikeasti havaittavissa, koska ne eivät ole haittaohjelmia. Esimerkiksi EDR-ratkaisut eivät automaattisesti reagoi niiden käyttöön, ellei havainnointia ole erikseen määritelty. Tämän vuoksi suosittelemme RMM-ohjelmistojen käytön rajaamista ja tarkempaa valvontaa. Tämä tarkoittaisi sitä, että ainoastaan organisaation itse määrittelemät RMM:t olisivat sallittuja ja kaikki muut olisivat kiellettyjä, ja niiden käyttöä valvottaisiin esimerkiksi EDR:llä. Esimerkiksi TeamViewer voitaisiin sallia, mutta AnyDeskin käytöstä nostettaisiin hälytys, joka olisi syytä tutkia. Havainnointikyvykkyys paranee tällöin merkittävästi, koska kielletyistä ohjelmista voidaan hälyttää suoraan.[19]

Sysmon on Microsoftin Windowsille tarjoama ilmainen lokituslaajennus.[20], joka mahdollistaa merkittävästi paremman ja selkeämmän lokituksen kuin Windowsin sisäänrakennetut lokit. Sillä voidaan valvoa esimerkiksi prosessien luonteja, verkkoyhteyksiä ja tiedostojen luonteja. Sysmon tuottaa paljon lokia, ja niitä onkin hyvä suodattaa kuorman ja kustannusten vähentämiseksi. Hyvä lähtökohta on käyttää esimerkiksi SwiftOnSecurity:n konfiguraatiopohjaa.[21] Sysmon on suositeltavaa asentaa kaikille laitteille, mutta asentaminen kannattaa aloittaa kriittisistä palvelimista ja muista laitteista, joiden lokit kerätään keskitettyyn lokienhallintaan tai SIEMiin. Tällä tavoin Sysmonin tuottamiin lokeihin voidaan kohdistaa havainnointisääntöjä.

Esimerkiksi kiristyshaittaohjelmatoimijat pyrkivät lähes jokaisessa murrossa ensin löytämään ja sitten tuhoamaan organisaation järjestelmien varmuuskopiot. Mm. viime aikoina uutisoidut haavoittuvuudet Veeam-tuotteissa ovat aktiivisesti kiristyshaittaohjelmatoimijoiden hyväksikäyttämiä.[22] Kohteen toiminnan lamauttaminen on huomattavasti tehokkaampaa ja pitkäkestoisempaa, jos palautuminen onnistutaan estämään. On äärimmäisen tärkeää harjoitella nk. Disaster recovery -tilannetta ja varmistua, että varmuuskopiot ovat ehjät ja niiden palauttaminen onnistuu halutulla tavalla. Ennen testaamista on oleellista toki varmistaa, että varmuuskopioita otetaan säännöllisesti ja 3-2-1-säännön mukaisesti: vähintään kolme kopiota datasta, kahdella eri medialla ja vähintään yhden kopion tulee olla ympäristön

[19] Intel471, 18.3.2025, Threat hunting case study: RMM software, https://intel471.com/blog/threat-hunting-case-study-rmm-software
[20] Microsoft, 23.7.2024, Sysmonv15.15, https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
[21] SwiftOnSecurity, N.d, Sysmon-config | A Sysmon configuration file for everybody to fork, https://github.com/SwiftOnSecurity/sysmon-config
[22] The Hacker News, 14.10.2024, Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware, https://thehackernews.com/2024/10/critical-veeam-vulnerability-exploited.html

ulkopuolella ja poissa verkosta. Kun varmuuskopioista palauttamista testataan säännöllisesti, on poikkeaman tapahtuessa merkittävästi helpompi palautua.

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