



Kyberkatsaus

8/2025

LOIHDE



Tiivistelmä

Elokuun kyberkatsauksessa on nostettu esille kriittisiä ja jo aktiivista hyväksikäyttöä kohdanneita haavoittuvuuksia. Elokuun haavoittuvuuksiin on nostettu Citrix-tuotteita, paikallinen SharePoint ja N-Able. Mikäli haavoittuvuuksissa mainittuja tuotteita on organisaatioilla käytössä, tulisi päivitykset tehdä välittömästi.

Traficom ja suojelupoliisi kertovat, että Suomen kyberturvallisuuden uhkataso on pysynyt koholla koko kuluneen vuoden. Vakavien tietomurtojen ja niiden yritysten määrä on jatkanut kasvuaan, ja Kyberturvallisuuskeskuksen selvittämien vakavien tapausten määrä on yli kaksinkertaistunut viime vuoteen verrattuna. Myös ohjelmistojen haavoittuvuuksiin liittyvien havaintojen määrä on kasvanut, mikä lisää merkittävästi yleistä kyberuhkaa suomalaisessa yhteiskunnassa.

Tunnusten kalastelu on lisääntynyt merkittävästi loppukesästä, etenkin M365-tunnusten osalta. Uhkatoimijat käyttävät yhä enemmän jo vaarantamiaan tunnuksia lähettämään uusia kalastelusähköposteja. Lisäksi viesteihin sisällytetään mm. OneDrive- tai SharePoint-jakoja hämäämään vastaanottajaa ja vastaanottavan organisaation sähköpostisuojaus. Kompensoivia kontroleja, kuten Conditional Access Policyt, on syytä harkita vakavasti otettavaksi käyttöön, jotta onnistuneista tunnusten kalasteluista syntyneet vahingot saadaan minimoitua tai estettyä kokonaan.

Microsoftin tuore uhkaraportti varoittaa Storm-0501-uhkatoimijan muuttuneista toimintatavoista. Ryhmä on siirtynyt perinteisestä paikallisista päätelaitteiden kiristyshaittaohjelmien käytöstä pilvipohjaisiin hyökkäyksiin. Kyseinen toimintamalli korostaa pilviympäristöjen suojauksen merkitystä ja sitä, että hyökkäykset kohdistuvat yhä enemmän pilviresurssien hallintaan ja varmuuskopiointiin.

Kyberkatsauksessa on lisäksi nostettu esille Loihteen CSOC:n elokuun kolme suositusta, joita hyödyntämällä organisaatiot kykenevät havaitsemaan epäilyttävää toimintaa ja suojautumaan ympäristöissään tapahtuvilta tietoturvapoikkeamilta. Riittävä näkyvyys ympäristöihin on perusedellytys tietoturvapoikkeamien ennaltaehkäisemiseen, havaitsemiseen ja niistä palautumiseen.

KUUKAUSIRAPORTTI 8/2025

Tämä raportti sisältää kuvauksen elokuun 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

Tiivistelmä	1
KUUKAUSIRAPORTTI 8/2025	2
1. Yleistilanne	3
2. Haavoittuvuudet	4
2.1 CVE-2025-7775: Critical Citrix NetScaler RCE vulnerability	4
2.2 "ToolShell": SharePoint RCE exploit chain	4
2.3 CVE-2025-8875 & CVE-2025-8876: N-able N-central vulnerabilities	5
3. Kalastelu ja huijaukset	6
4. Kiristyshaittaohjelmat ja -toimijat	7
4.1 Pilvipalvelupainotteinen kiristyshaittaohjelmahyökkäys	7
4.2 Tekoälyä käyttävä kiristyshaittaohjelma	7
5. Muuta	8
5.1 PDF Editor -haittaohjelmaa levitetään Euroopassa aktiivisesti	8
5.2 CrowdStrike Threat Hunting -raportti 2025	8
6. Suositukset	10

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.

Vakavien tietoturvapoikkeamien määrät suomalaisissa organisaatioissa ovat olleet kasvussa vuonna 2025. Kyberturvallisuuskeskuksen selvittämät vakavat tapaukset ovat kaksinkertaistuneet vuodesta 2024. Lisäksi vakavien tietoturvaahaavoittuvuuksien määrä, sekä niiden nopea hyväksikäyttö aiheuttavat huolta. Lisäksi tietojen- ja tunnustenkalastelutapaukset ovat selvässä kasvussa.¹ Tämä on laitettu merkille myös Loihteen CSOC:ssa.

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.

¹Traficom ja supo, 29.8.2025, <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-ja-supo-kyberturvallisuuden-uhkataso-pysynyt-koholla-vakavien-tapausten>

2. Haavoittuvuudet

2.1 CVE-2025-7775: Critical Citrix NetScaler RCE vulnerability

Citrix julkaisi 26.08.2025 tämän kesän jo kolmannen vakavuudeltaan kriittisen tiedotteen haavoittuvuudesta koskien Citrix NetScaler ADC- ja NetScaler Gateway -tuotteita. CVE-2025-7775 on muistin ylivuotohaavoittuvuus, joka mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen etänä. Haavoittuvuutta hyväksikäyttämällä hyökkääjä kykenee saamaan siis laitteen haltuunsa. Citrixin mukaan haavoittuvuuden hyväksikäyttöä on jo havaittu maailmalla. Samassa tiedotteessa kerrottiin myös kahdesta muusta NetScaleria koskevasta haavoittuvuudesta: CVE-2025-7776 ja CVE-2025-8424.²

Korjaavat päivitykset haavoittuvuuksiin on julkaistu ja ne suositellaan asennettavaksi välittömästi. NetScalerin aiemmat vastaavat haavoittuvuudet, kuten CVE-2023-4966 (nk. CitrixBleed), ovat olleet hyvin aktiivisen hyväksikäytön kohteita ja uhkatoimijoiden tehokkaassa käytössä.³ On odotettavaa, että myös tämä haavoittuvuus päättyy etenkin kiristyshaittaohjelmatoimijoiden kohteeksi.

2.2 “ToolShell”: SharePoint RCE exploit chain

Heinäkuussa julkaistiin päivitykset kriittiseen ja aktiivisen hyväksikäytön kohteena olevaan haavoittuvuusketjuun, joka kohdistuu paikallisiin (on-premises) Microsoft SharePoint -palvelimiin. Microsoft julkaisi 08.07.2025 korjauspäivitykset haavoittuvuuksiin CVE-2025-49704 ja CVE-2025-49706, jotka tietoturvatutkija Khoa Dinh löysi jo toukokuussa.⁶ Haavoittuvuudet mahdollistavat autentikoinnin ohittamisen sekä mielivaltaisen tiedoston kirjoittamisen, jotka yhdessä johtavat mielivaltaisen koodin suorittamiseen palvelimella ilman, että hyökkääjä tarvitsee valideja käyttäjätunnuksia. Näistä kahdesta haavoittuvuudesta julkaistiin 19.07. uudet variantit CVE-2025-53770 ja CVE-2025-53771.⁴

Kesällä havaitut haavoittuvuuksien hyväksikäytöt ovat Microsoftin mukaan liitettävissä kiinalaisiin valtiollisiin toimijoihin, kuten Linen Typhoon, Violet Typhoon ja Storm-2603:een⁵. Heinäkuussa raportoiduissa hyökkäyksissä hyväksikäyttö on johtanut lähes aina webshell-takaoven asentamiseen SharePoint-palvelimille sekä palvelimien ASP.net-salausavainten vuotamiseen. Myös 4L4MD4R-kiristyshaittaohjelman asentamista haavoittuvuuden kautta on nähty.⁶

² Citrix, 26.08.2025, NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-7775, CVE-2025-7776 and CVE-2025-8424, <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938>

³ CISA, 21.11.2023, #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a>

⁴ Varonis, 23.07.2025, ToolShell: A SharePoint RCE chain actively exploited, <https://www.varonis.com/blog/toolshell-sharepoint-rce>

⁵ Microsoft, 22.07.2025, Disrupting active exploitation of on-premises SharePoint vulnerabilities, <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>

⁶ Unit 42, 31.07.2025, Active Exploitation of Microsoft SharePoint Vulnerabilities: Threat Brief (Updated August 12), https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/#post-147463-_50343o6a6han

2.3 CVE-2025-8875 & CVE-2025-8876: N-able N-central vulnerabilities

N-ablen etämonitorointi ja -hallintatuotteesta N-Centralista on löydetty kaksi haavoittuvuutta: CVE-2025-8875 ja CVE-2025-8876. Yhdysvaltain Cybersecurity and Infrastructure Security Agency (CISA) -virasto on lisännyt haavoittuvuudet tunnettujen hyväksikäytettyjen haavoittuvuuksien listalle ja ohjeistanut korjaavat päivitykset asennettavaksi pikaisesti. CVE-2025-8875 on insecure deserialization -haavoittuvuus ja CVE-2025-8876 komentoinjektiohaavoittuvuus.⁷

N-able on kertonut havainneensa hyväksikäyttöä paikallisissa ympäristöissä, muttei pilvessä ylläpidetyssä N-Centralissa. Haavoittuvuuksien hyväksikäyttö edellyttää hyökkääjältä autentikoitumista, eli hyökkääjällä täytyy olla hallussaan toimivat käyttäjätunnukset. Haavoittuvat N-Central-palvelimet suositellaan päivittämään korjattuun versioon mahdollisimman pian.⁷

⁷ Help Net Security, 14.08.2025, Vulnerabilities in MSP-friendly RMM solution exploited in the wild (CVE-2025-8875, CVE-2025-8876), <https://www.helpnetsecurity.com/2025/08/14/vulnerabilities-in-msp-friendly-rmm-solution-exploited-in-the-wild-cve-2025-8875-cve-2025-8876/>

3. Kalastelu ja huijaukset

Loihteen CSOC on havainnut merkittävää kasvua M365-tunnusten kalasteluissa ja murroissa loppukesän 2025 aikana. Tähän vaikuttanee osaltaan se, että työntekijät käyvät läpi lukemattomia sähköpostejaan palatessaan töihin kesälomien jälkeen ja näiden seassa on kalasteluviestejä. Saapuvien kalasteluviestien määrä on myös yleisesti ollut kasvussa.

Kalasteluissa käytetyt tekniikat ja uhkatoimijoiden lopulliset tavoitteet eivät kuitenkaan vaikuta muuttuneen. Tapahtumaketju etenee yksinkertaistetusti seuraavasti: Käyttäjä saa näennäisesti aidolta vaikuttavan sähköpostiviestin joko ennestään tutulta tai tuntemattomalta lähettäjältä. Useimmiten viesti liittyy asiakirjan jakamiseen esimerkiksi Sharepointista, OneDrivesta tai Docusign:sta. Viestissä oleva linkki johtaa lopulta hyökkääjän hallinnoimalle verkkosivulle, joka on aidonnäköinen, mutta väärennetty M365-kirjautumisnäkyvä, johon käyttäjä syöttää tunnuksensa sekä hyväksyy kaksivaiheisen tunnistautumisen (MFA) mobiililaitteensa Authenticator-sovelluksesta. Uhkatoimija varastaa välistä ns. session tokenin, jonka avulla voi kirjautua käyttäjätunnuksella tämän M365-resursseihin.

Tästä seuraa yleensä se, että sisäänkirjautumisen jälkeen hyökkääjä lisää käyttäjätunnukselle oman laitteensa MFA-metodiksi, luo sähköpostilaatikkoon uudelleenohjaussääntöjä mielenkiintoisilta lähettäjiltä sekä lisää OAuth-sovelluksia Azureen ja M365:een saaden pysyvämmän jalansijan käyttäjätunnukselle. Useimmin esiintyvät sovellukset ovat mm. eM Client ja PERFECTDATA SOFTWARE, jotka ovat kolmannen osapuolen sähköpostisovelluksia. Suosittelemmekin lukijoita tarkistamaan, löytyykö organisaation OAuth-applikaatiolistauksesta näitä kahta sovellusta ja mikäli niitä löytyy, selvittämään niiden alkuperän. Lähes poikkeuksetta mainittujen sovellusten löytyminen applikaatiolistauksesta on liittynyt käyttäjätunnuksen vaarantumiseen.

Uhkatoimija tavoittelee näissä tapauksissa useimmiten taloudellista hyötyä. Kun käyttäjätunnukselle on saatu pääsy ja pysyvä jalansija on muodostettu, uhkatoimija alkaa käymään läpi kiinnostavia sähköposteja ja asiakirjoja. Uhkatoimijat pyrkivät etsimään ensisijaisesti maksuliikenteeseen ja laskuihin liittyviä dokumentteja. Toimija alkaa matkimaan käyttäjän tyyliä kirjoittaa sähköposteja ja lähetellä viestejä. Tutustuttuaan käyttäjätunnukseen riittävästi toimija yleensä pyrkii lähettämään omalle organisaatiolle tai asiakasorganisaatiolle väärennettyjä laskuja, jotka voivat johtaa merkittäviin taloudellisiin tappioihin ja mainehaittoihin. Lisäksi käyttäjätunnuksen vaarantuminen ja sähköpostien urkinta on jo itsessään tietosuojaloukkaus, jolloin organisaatio on velvollinen tekemään ilmoituksen tietosuojavaltuutetulle.

Pankkihuijausten rintamalla kesä on ollut aktiivinen. OP:n nimissä on kesän aikana tehty suuri määrä huijauspuheluita. Puheluissa hyvää suomen kieltä puhuva soittaja on esiintynyt mm. pankin työntekijänä ja uskotellut uhrille, että hänen pankkitilitään ollaan tekemässä maksua ulkomaille ja tämä voidaan estää siirtämällä varat ”turvatilille”. Huijari yrittää tällä uskotella uhrin luovuttamaan pankkitunnuksensa taikka hyväksymään rikollisen tekemän maksun.⁸

⁸ OP, 11.07.2025, Juuri nyt: Varo huijauspuheluita OP:n nimissä, <https://www.op.fi/-/juuri-nyt-varo-huijauspuheluita-0625>

4. Kiristyshaittaohjelmat ja -toimijat

4.1 Pilvipalvelupainotteinen kiristyshaittaohjelmahyökkäys

Microsoft varoittaa tuoreessa uhkaraportissaan uhkatoimija Storm-0501:n muuttuneista toimintatavoista heidän viimeisimmissä kampanjoissaan, joissa he ovat siirtyneet suorittamaan kiristyshaittaohjelman pilvessä paikallisen (on-premises) ympäristön päätelaitteiden salaamisen sijaan. Tyypillisestä kiristyshaittaohjelmahyökkäyksestä poiketen Microsoftin analysoimassa hyökkäyksessä Storm-0501 on suorittanut kiristämisen puhtaasti pilvessä. Saavutettuaan täyden hallinnan paikallisessa Active Directory -ympäristössä uhkatoimija on pivotoinut Microsoft Entraan ja sitä kautta Azuren resursseihin tyypillisesti Entra Connect -palvelimen kautta.

Saatuaan Global Administrator -tason tunnukset ja täten täyden hallinnan myös Azuressa, uhkatoimija nopeasti ryhtyi varastamaan dataa Azure Storage -tunnuksilta käyttäen Azuren omia työkaluja. Kun uhrin arkaluontoinen data oli imuroitu, käynnisti uhkatoimija Azure resurssien massapoiston yrittäen estää tiedon palauttamisen snapshotista, palautuspisteistä ja muista varmuuskopioresursseista. Resurssit, joiden poisto ei onnistunut, uhkatoimija salasi käyttäen Azure Key Vaultia ja sitä kautta luotua salausavainta. Resurssien salaamiseen käytetyn avaimen poisto ei kuitenkaan onnistunut oletuksena 90 vuorokautta kestävä avaimen ja Key Vaultin palauttamisen vuoksi.⁹

4.2 Tekoälyä käyttävä kiristyshaittaohjelma

Kyberturvallisuusyhtiö ESET on kertonut löytäneensä tekoälyä hyödyntävän kiristyshaittaohjelman. PromptLockiksi nimetty Go:lla kirjoitettu haittaohjelma käyttää OpenAI:n elokuun alussa julkaisemaa gpt-oss:20b -kielimallia luomaan haitallisia Lua-skriptejä ajon aikana. Skriptit luodaan käyttäen haittaohjelmaan kovakoodattua kehotetta ja niillä ohjelma mm. etsii tiedostojärjestelmästä määritettyjä kohdetiedostoja, tarkastelee niiden sisältöä, varastaa datan ja salaa tiedostot. Myös kiristysviestin kirjoittamiseen se käyttää tekoälyä. Tämä luo haasteita havainnointiin, koska haittaohjelman tunnistamiseen käytetyt indikaattorit (IoC) muuttuvat haittaohjelman suoritusten välillä, kun tekoäly tuottaa aina hieman erilaista haittakoodia.¹⁰

ESETin mukaan kyseinen haittaohjelmanäyte vaikuttaa olevan keskeneräinen tai nk. proof-of-concept, eikä sitä ole nähty käytettävän hyökkäyksissä.¹⁰ On kuitenkin vain ajan kysymys, milloin tekoälytyökaluja aletaan käyttää kiristyshaittaohjelmahyökkäyksissä laajemmin sekä uusin tavoin.

⁹ Microsoft, 27.08.2025, Storm-0501's evolving techniques lead to cloud-based ransomware, <https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/>

¹⁰ The Hacker News, 27.08.2025, Someone Created the First AI-Powered Ransomware Using OpenAI's gpt-oss:20b Model, <https://thehackernews.com/2025/08/someone-created-first-ai-powered.html>

5. Muuta

5.1 PDF Editor -haittaohjelmaa levitetään Euroopassa aktiivisesti

Euroopassa on havaittu loppukesän 2025 aikana PDF Editor -nimeä kantavaa troijalaista haittaohjelmaa. Haittaohjelmaa on havaittu levitetävän verkossa esiintyvillä mainoksilla.¹¹ PDF Editoriin liittyvät mainokset, joiden kautta ohjelmisto ladataan, on onnistuttu saamaan näkyville hakukoneissa esiintyville suosituille sivustoille ja näin ollen se on onnistunut leviämään laajamittaisesti.¹² Haittaohjelma on naamioitu PDF-tiedostojen muokkaustyökaluksi, mutta todellisuudessa se on haittaohjelma, jolla on kyvykkyyksiä varastaa käyttäjän kirjautumistietoja selaimesta sekä liittää saastunut laite osaksi bottiverkkoa. Tällöin toimija voi hyödyntää sitä esimerkiksi palvelunestohyökkäyksissä. Haittaohjelma pyrkii lisäksi muodostamaan pysyvämmän jalansijan laitteelle melko perinteisillä mekanismeilla, kuten Windowsin rekisterin, scheduled taskien tai servicejen avulla.¹³

PDF Editorin kaltaisten troijalaisten käyttö ja kehittäminen kielii uhkatoimijoiden vaivannäöstä ja tekoälyavusteisesta haittaohjelmakampanjoiden luomisesta. Todennäköisesti vastaavanlaisia ohjelmistoja, jotka naamioidaan legitiimeiksi sovelluksiksi, mutta ovat todellisuudessa haittaohjelmia, tullaan näkemään tulevaisuudessa entistä enemmän. Tämän vuoksi käyttäjiä tulisi ohjeistaa lataamis- ja asentamiskäytänteistä ja ennalta sallimattomien ohjelmistojen asentaminen tulisi estää.

5.2 CrowdStrike Threat Hunting -raportti 2025

Tietoturvayhtiö CrowdStrike on julkaissut vuoden 2025 Threat Hunting -raportin 4.8.2025.¹⁴ Raportin mukaan uhkatoimijat ovat lisänneet tekoälyn käyttöä merkittävästi vuosina 2024 ja 2025. CrowdStrike on havainnut uhkatoimijoiden hyödyntävän tekoälyä uskottavampien kalastelukampanjoiden toteuttamiseen, sosiaalisen median profiilien ja verkostojen luontiin, haittaohjelmien kehittämiseen ja parantamiseen sekä disinformaation levittämiseen.

Raportissa mainitaan myös puhelinsoittojen kautta tapahtuvan kalastelun, eli vishingin, ohittaneen vuoden 2024 lukumäärän jo vuoden 2025 ensimmäisellä puoliskolla. Puhelinkalastelulla pyritään mm. pääsemään sisään organisaatioon huijaamalla esimerkiksi soittamalla asiakaspalveluun ja pyytämällä käyttäjätunnuksen salasanan tai monivaiheisen tunnistautumisen nollaamista.

Raportissa korostetaan myös verkon reunalaitteiden hyväksikäyttöä. CrowdStriken mukaan 52 % julki tulleista haavoittuvuuksista liittyivät ensimmäisen jalansijan saamiseen ja julkiverkkoon näkyvillä oleviin palveluihin. Organisaatioiden tulisi tarkastella sekä rajata

¹¹Traficom, 22.8.2025, <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelmia-levitetaan-aktiivisesti-pdf-editoriohjelmiksi-naamioituina>

¹² AppSuite PDF Editor Backdoor: A Detailed Technical Analysis, 28.8.2025. <https://www.gdatasoftware.com/blog/2025/08/38257-appsuite-pdf-editor-backdoor-analysis>

¹³ Under Code Testing, 20.8.2025. <https://undercodetesting.com/the-tamperedchef-trojan-how-a-simple-pdf-editor-can-pwn-your-entire-network/>

¹⁴ CrowdStrike 2025 Threat Hunting Report, 4.8.2025. https://www.crowdstrike.com/explore/2025-threat-hunt-report?utm_medium=org

hyökkäysrajapintaansa. Tarpeettomat julkiverkkoon avoinna olevat palvelut tulisi sulkea, koska ne voivat toimia pääsynä organisaation verkkoon.

6. Suositukset

Tässä kuussa suosittelemme:

- Sähköpostisuojausten asetusten katselmointi
- Paikallisten järjestelmänvalvojatunnusten käytön rajaaminen
- Siivoamaan vanhat ja tarpeettomat AD-käyttäjät säännöllisesti

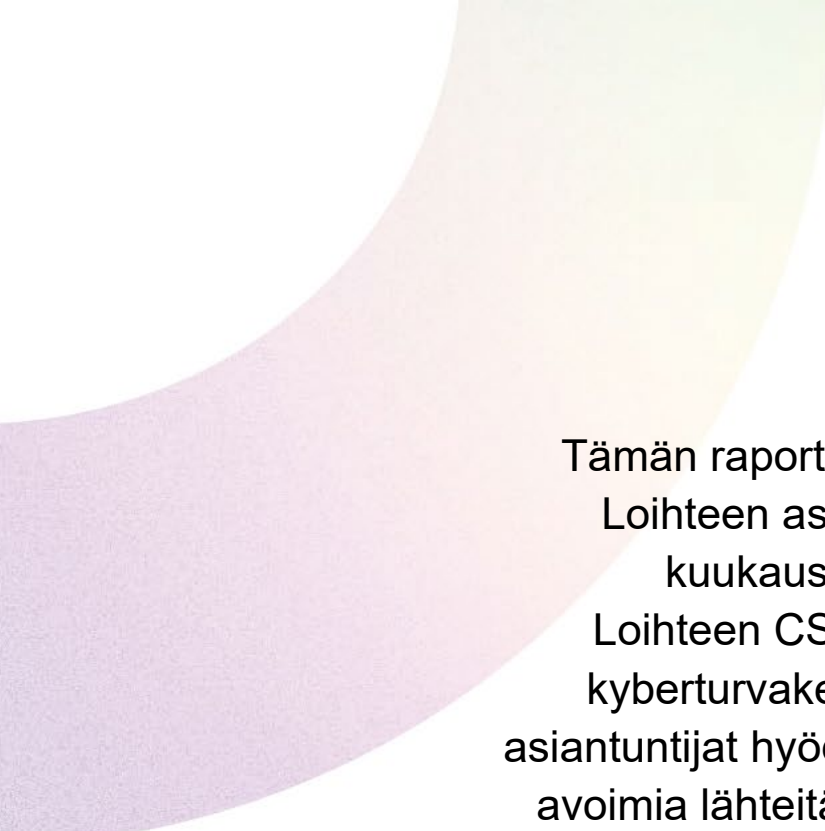
Kalasteluviestit ovat edelleen yleisin hyökkäysvektori organisaatioiden järjestelmiin. Tämän vuoksi suosittelemme käytössä olevan sähköpostisuojausten asetusten läpikäyntiä. Monissa tapauksissa käytössä on tuotteen oletusasetukset, jotka olisivat suositeltavaa konfiguroida organisaation tarpeita paremmin vastaaviksi. Esimerkiksi Microsoftin Defender for Office 365 -tuotteessa on oletuksena perustason Built-in Protection, joka ei takaa riittävää suojaa kalasteluviesteiltä. Samassa tuotteessa ovat myös Microsoftin määrittelemät, erikseen päälle kytkettävät Standard- ja Strict-esiasetukset, jotka kiristävät asetuksia, mutta eivät kuitenkaan ole täydellisiä ratkaisuja vaan asetukset pitää räätälöidä organisaatiokohtaisesti. Esiasetusten hyödyntäminen on kuitenkin hyvä lähtökohta turvallisemmalle sähköpostiliikenteelle.

Liian laajat paikalliset järjestelmänvalvojan oikeudet ympäristöissä ovat toistuva ja merkittävä haitallisen toiminnan mahdollistaja etenkin kiristyshaittaohjelmahyökkäyksissä. Valitettavan usein kaikilta käyttäjiltä löytyvät paikalliset järjestelmänvalvojaoikeudet työasemilleen ja tunnusten vaarantuessa hyökkääjällä on vapaat kädet toimia kyseisellä käyttäjätunnuksella. Lähes poikkeuksetta jokaisen verkkoon päässeän hyökkääjän täytyy korottaa oikeuksiaan jossain vaiheessa saavuttaakseen tavoitteensa, ja murretun laitteen pääkäyttäjätunnukset ovat yksi ensimmäisistä kandidaateista. Jos päätelaitteen paikallisen järjestelmänvalvojatunnuksen saa haltuunsa, riittää oikeudet varastaa laitteen muistista mahdolliset muut sinne tallentuneet tunnukset ja salasana käyttäen esimerkiksi Mimikatz-työkalua. Lisäksi esimerkiksi järjestelmien ylläpitäjien yleisesti käyttämän PsExec-työkalun käyttö vaatii paikalliset järjestelmänvalvojatunnukset toimiakseen. Kyseinen työkalu on myös hyvin suosittu kiristyshaittaohjelmatoimijoiden keskuudessa ja sitä käytetäänkin paljon sivuttaisliikkeitään ja kiristyshaittaohjelman levittämiseen ympäristöissä. Käyttäjäkohtaisten paikallisten järjestelmänvalvojatunnusten poistaminen käytöstä on suositeltavaa ja vähintäänkin järjestelmänvalvojaoikeuksien käytössä tier-mallin noudattaminen suositeltavaa. Erilaisilla Privileged Access Management (PAM) -ratkaisulla voidaan tämän jälkeen hallitusti myöntää järjestelmänvalvojatunnuksia käyttäjille tilapäisesti, kun niitä tarvitaan esimerkiksi sovelluksen asentamiseen. Järjestelmänvalvojatunnusten rajaaminen voi aiheuttaa vastustusta käyttäjissä, mutta se hankaloittaa uhkatoimijoiden kyvykkyksiä toimia ympäristössä merkittävästi.

Active Directory -ympäristöön voi herkästi unohtua vanhoja käyttämättömiä käyttäjätunnuksia ja ryhmiä, kun henkilöstö vaihtuu ja palveluita uusitaan. Ajan saatossa ympäristöön saattaa jäädä lojumaan käytöstä poistamattomia entisten työntekijöiden tai kumppaneiden tunnuksia, joilla on pahimmillaan tarpeettoman korkeat oikeudet ympäristöön. Juuri tällaiset käyttäjät kiinnostavat hyökkääjiä, koska niiden käyttöä monesti ei huomata ja ne voivat olla oikotie domainin haltuun saamiseksi. Sama koskee palvelukäyttäjiä, joita ei enää käytetä. Hyökkäysvektorin lisäksi sotkuinen AD myös monimutkaistaa ylläpitoa ja poikkeaman

sattuessa tutkintaa. AD:n käyttäjät ja ryhmät suositellaan tarkastelemaan ja siivoamaan säännöllisesti.¹⁵

¹⁵Microsoft, 30.6.2025, <https://learn.microsoft.com/en-us/services-hub/unified/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory>



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.

