Kyberkatsaus

5/2025

LOIHDE

Tiivistelmä

Toukokuun raportissa on jälleen tuotu esille tietoturvahaavoittuvuuksia, joiden aktiivista hyväksikäyttöä on myös raportoitu maailmalla.[1] Toukokuussa haavoittuvuuksia edustavat Microsoft Windows, Ivanti EPMM ja SAP Netweaver.

Tunnusten kalastelua on tapahtunut aktiivisesti kevään aikana etenkin M365-tunnusten osalta. Uhkatoimijat käyttävät yhä enemmän jo vaarantamiaan tunnuksia lähettämään uusia kalastelusähköposteja. Lisäksi viesteihin sisällytetään mm. OneDrive-jakoja hämäämään vastaanottajaa ja vastaanottavan organisaation sähköpostisuojauksia. Kompensoivia kontrolleja, kuten Conditional Access Policyt, on syytä harkita otettavaksi käyttöön, jotta onnistuneista tunnusten kalasteluista syntyneet vahingot saadaan minimoitua tai estettyä kokonaan.

Microsoft esti pääsyn Kansainvälisen rikostuomioistuimen (ICC) pääsyyttäjältä tämän sähköpostiin sen jälkeen, kun Yhdysvaltain hallinto asetti ICC:tä kohtaan pakotteita. Tapaus on herättänyt keskustelua ja huolta, sillä hyvin monet eurooppalaiset organisaatiot nojaavat laajasti Microsoftin palveluihin.

Microsoft ja Europol suorittivat mittavan operaation Lumma Stealer-haittaohjelman toimintojen heikentämiseksi ja katkaisemiseksi. Tämä on johtanut siihen, että yli 2300 Lummaan liittyvää domainia on estetty, ajettu alas tai otettu haltuun Microsoftin toimesta.

Kyberkatsauksessa on lisäksi nostettu esille Loihteen CSOCin toukokuun 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.

Alkuvuoden perusteella voidaan kyberturvallisuuteen liittyvien uhkien osalta odottaa aktiivista kesää. 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] EclecticIQ, 21.5.2025, https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability

KUUKAUSIRAPORTTI 5/2025

Tämä raportti sisältää kuvauksen toukokuun 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

..... 0
Tiivistelmä 1
KUUKAUSIRAPORTTI 5/2025 2
1. Yleistilanne 3
2. Haavoittuvuudet 3
2.1 Active Directory dMSA Privilege Escalation: "BadSuccessor" 3
2.2 CVE-2025-4427 & CVE-2025-4428: Ivanti Endpoint Manager Mobile (EPMM) Remote Code Execution 4
2.3 CVE-2025-31324: Critical SAP NetWeaver Vulnerability 4
3. Kalastelu ja huijaukset 6
4. Kiristyshaittaohjelmat ja -toimijat 7
5. Muuta 8
5.1 Microsoft estänyt ICC:n pääsyyttäjältä pääsyn sähköpostiin 8
5.2 Microsoft ja Europol keskeyttäneet Lumma Stealer -haittaohjelman toimintoja 8
6. Suositukset 9

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 Active Directory dMSA Privilege Escalation: "BadSuccessor"

Toukokuun 21. päivänä Akamai julkaisi blogissaan artikkelin uudesta hyökkäystekniikasta, jossa Delegated Managed Service Account (dMSA) -palvelutunnuksia hyväksikäyttämällä on mahdollista ottaa haltuun mikä tahansa domainin käyttäjä. Haavoittuvuus koskee Active Directory -metsiä, joissa on vähintään yksi Windows Server 2025 -version AD-palvelin, jossa dMSA-käyttäjät lisättiin uutena ominaisuutena.[2]

Osana dMSA:ta on toiminnallisuus muuttaa perinteinen palvelutunnus hallituksi dMSA-tunnukseksi. Tässä muunnosprosessissa on haavoittuvuus, joka tyypillisillä oletusasetuksilla mahdollistaa hyökkääjän hallitsemalle tai luomalle dMSA-tunnukselle mielivaltaisen käyttäjän oikeudet Kerberos-tikettiin. Hyväksikäyttö mahdollistaa täten koko domainin murtamisen esim. Domain Admin -tason oikeuksiin korottamalla. Uuden dMSA-käyttäjän luomiseen riittää CreateChild-oikeudet vähintään yhteen Organizational Unitiin (OU).[2]

[2] Akamai, 21.05.2025, BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory, https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory7

Toistaiseksi Microsoft ei ole vielä julkaissut haavoittuvuuteen korjausta. Hyökkäyspinta-alan rajoittamiseksi on suositeltavaa tunnistaa sekä rajata käyttäjät, ryhmät ja konetilit, joilla on oikeus luoda dMSA-käyttäjiä domainissa. SpecterOps julkaisi blogissaan kattavan analyysin lisäksi PowerShell-skriptin, jolla mitigoida BadSuccessor-hyökkäyksen mahdollistavat skenaariot Access Control Entryillä (ACE).[3]

2.2 CVE-2025-4427 & CVE-2025-4428: Ivanti Endpoint Manager Mobile (EPMM) Remote Code Execution

Ivanti julkaisi 13.5.2025 tiedotteen kahdesta haavoittuvuudesta Endpoint Manager Mobile (EPMM) -tuotteessaan. Ivantin mobiililaitteiden hallintaratkaisusta löytyneet kaksi haavoittuvuutta, autentikoinnin ohittava CVE-2025-4427 ja mielivaltaisen koodin suorittamisen mahdollistava CVE-2025-4428 yhdessä mahdollistavat autentikoimattoman hyökkääjän suorittaa koodia laitteella verkon yli[4] käyttäen yksinkertaista hyväksikäyttökoodia. Haavoittuvuuden aktiivista hyväksikäyttöä on jo nähty ainakin kiinalaisen UNC5221-ryhmän toimesta, jonka tekemiksi EclecticIQ attribuoi toukokuussa havaitsemiaan hyökkäyksiä, joissa tätä kriittistä haavoittuvuusparia on hyväksikäytetty. Hyökkäyskampanjan kohteena ovat olleet organisaatiot monesta eri sektorista niin Euroopasta, Pohjois-Amerikasta kuin Aasiastakin.[5]

Koodin suorittamisen salliva haavoittuvuus piilee tuotteen API:ssa, jonka */api/v2/featureusage* -päätepisteen ”format”-parametri mahdollistaa Expression Language -injektion. Tätä API-päätepistettä on mahdollista kutsua myös ilman kirjautumista ja täten EPMM:n web-hallintaan ja sen API-rajapintaan yhteyden saava hyökkääjä voi ottaa laitteen haltuunsa käyttöjärjestelmätason komentoja suorittamalla ilman mitään käyttäjätunnuksia palveluun.[6]

Haavoittuvuudet on korjattu Ivanti EPMM:n versioissa 11.12.0.5, 12.3.0.2, 12.4.0.2 ja 12.5.0.1. Korjaavat päivitykset suositellaan asennettavaksi pikimmiten.[4] Päivitysten lisäksi oleellista on myös varmistaa, että pääsy palvelun hallintaportaaliin on sallittu vain tarvittavista lähteistä.

2.3 CVE-2025-31324: Critical SAP NetWeaver Vulnerability

Aivan huhtikuun lopussa 24.04.2025 SAP julkaisi tiedon kriittisestä haavoittuvuudesta (CVSS 10.0) heidän SPA NetWeaver Visual Composer Framework -ratkaisustaan. CVE-2025-31324 hyväksikäyttäen autentikoimaton hyökkääjä voi ladata mielivaltaisen tiedoston NetWeaver-sovelluspalvelimelle. Tämä johtaa mielivaltaisen koodin suorittamiseen ja mahdollistaa

[3] SpecterOps, 27.05.2025, Understanding & Mitigating BadSuccessor, https://specterops.io/blog/2025/05/27/understanding-mitigating-badsuccessor/
[4] Ivanti, 13.05.2025, Security Advisory Ivanti Endpoint Manager Mobile (EPMM) May 2025 (CVE-2025-4427 and CVE-2025-4428), https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US
[5] EclecticIQ, 21.05.2025, China-Nexus Threat Actor Actively Exploiting Ivanti Endpoint Manager Mobile (CVE-2025-4428) Vulnerability, https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability
[6] watchTowr Labs, 15.05.2025, Expression Payloads Meet Mayhem - Ivanti EPMM Unauth RCE Chain (CVE-2025-4427 and CVE-2025-4428), https://labs.watchtowr.com/expression-payloads-meet-mayhem-cve-2025-4427-and-cve-2025-4428/

palvelimen täyden haltuunoton lataamalla palvelimelle esimerkiksi webshellin komentojen suorittamista varten.[7]

Onapsiksen havaintojen mukaan haavoittuvuutta on käytetty aktiivisesti hyväksi maaliskuun alusta alkaen. Hyökkäyskampanjoissa uhkatoimija on ladannut palvelimelle Java server page (JSP) -webshellin, jonka kautta suoritetuilla komennoilla hyökkääjä on suorittanut jatkotoimenpiteitä kuten lisähaittaohjelmien asentamista. Onapsis on havainnut hyökkäysten aiheutuneen kahdessa aallossa, kun huhtikuun lopun jälkeen toiset opportunistiset hyökkääjät ovat pyrkineet hyödyntämään alkuperäisten hyökkääjien asentamia webshellejä.[7]

SAP on julkaissut korjauspäivityksen sekä tiedotteita haavoittuvuuden lieventämiseksi ja näiden implementointi on suositeltavaa tehdä välittömästi. Mikäli SAP NetWeaverin haavoittuva versio on auki julkiverkkoon, on sen saastuminen syytä varmistaa forensisella tutkinnalla.[7]

[7] Onapsis, 13.05.2025, SAP NetWeaver Flaw Lets Threat Actors Take Full Control: CVE-2025-31324 and CVE-2025-42999 Explained, https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/

3. Kalastelu ja huijaukset

M365-käyttäjätunnusten kalastelu on ollut aktiivista koko kevään 2025 ajan, eikä ilmiö näytä hiipumisen merkkejä. Perinteisen kaksivaiheisen tunnistautumisen ohittaminen AiTM:n[8] avulla on arkipäivää, eikä se tarjoa riittävää suojaa kalastelua vastaan. Kalasteluissa käytetään yhä enemmän aiemmin kaapattuja tunnuksia, joilta lähetetään kalasteluviestejä muihin suomalaisiin organisaatioihin. Lisäksi viesteissä hyödynnetään laajasti Microsoftin palveluita, kuten PowerBI ja Microsoft Forms, haitallisten linkkien toimittamiseen. Näiden avulla monet kalasteluviestit läpäisevät sähköpostisuojauksen helpommin, eivätkä viestien vastaanottajat välttämättä osaa epäillä luotetulta lähettäjältä tulevaa viestiä kalasteluviestiksi.

Onnistuneen kalastelun tapahtuessa uhkatoimijat kirjautuvat lähes reaaliajassa käyttäjän tunnuksilla Microsoft 365 -palveluun ja suuntaavat etsimään mielenkiintoisia asiakirjoja ja sähköposteja OneDriveen, SharePointiin ja Outlookiin. Arkaluontoisia tietoja voi näin ollen vaarantua minuuttien sisään ensimmäisestä haitallisesta kirjautumisista. Uhkatoimijat pyrkivät myös useimmiten lisäämään käyttäjälle uuden MFA:n, sähköpostiin uudelleenohjaussääntöjä tai lisäämään Azure/M365-ympäristöön haitallisia OAuth-sovelluksia, joilla he pystyvät pitämään jalansijan käyttäjätunnuksella. Tällaisissa tapauksissa on syytä suorittaa perusteellinen tutkinta käyttäjällä tehtyihin toimiin, jotta mahdolliset jalansijat pystytään poistamaan. Pelkkä istuntojen katkaisu tai salasanan vaihtaminen ei poista jälkikäteen lisättyä MFA:ta tai OAuth-sovelluksia.

Tämä alleviivaa kerroksittaisen suojauksen tärkeyttä. Kaikkia kalasteluviestejä ei pystytä estämään, joten on tärkeää kyetä minimoimaan vahingot onnistuneen kalastelun tapahtuessa. M365-tunnusten tapauksessa olennaisessa roolissa ovat Conditional Access -policyt ja kalastelun kestävä MFA (FIDO2). Kirjautumisten rajaaminen ainoastaan luotettuihin laitteisiin estää kirjautumisen onnistuneen kalastelun tapahtuessa. Tässä on kuitenkin syytä huomioida se, että salasana vaarantuu joka tapauksessa ja se on syytä vaihtaa. FIDO2 vähentää käyttäjän virheestä syntyneen kalastelun riskiä merkittävästi, koska onnistuneeseen kirjautumiseen vaaditaan MFA-mekanismin fyysinen läsnäolo eli fyysinen turva-avain, joka on kiinni työasemassa (esim. Yubikey) tai Bluetooth-yhteys matkapuhelimen ja työaseman välillä (Passkeys).

[8] Kyberturvallisuuskeskus. 27.5.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille/aitm-adversary-middle

4. Kiristyshaittaohjelmat ja -toimijat

SentinelOne EDR-agentin paikallisesta päivitysominaisuudesta on löytynyt haavoittuvuus, jonka avulla agentti on voitu poistaa käytöstä. Haittatoimijan saadessa paikallisen ylläpitäjän oikeudet laitteelle, on agentin päivityksen voinut käynnistää manuaalisesti paikallisesti, normaalin etäpäivityksen sijaan. Haittatoimija on voinut tappaa päivitysprosessin kesken päivityksen, jolloin agentti jää vikatilaan eikä enää suojaa laitetta. Haavoittuvuutta on käytetty ainakin Babuk-kiristyshaittatoimijan toimesta. SentinelOne on muuttanut oletusasetuksia haavoittuvuuden löytämisen jälkeen eikä paikallinen agentin päivitys ole enää mahdollista, ellei sitä erikseen sallita.[9]

UK:ssa on käynnissä kohdistettu hyökkäyksien sarja kaupan alaa vastaan. Tähän mennessä hyökkäysten kohteena on ollut Marks & Spencer[10], Co-op[11] ja Harrods[12]. Hyökkäysten uskotaan olevan Scattered Spider -haittatoimijan tekemiä, koska hyökkäyksissä käytetyt toimintatavat vastaavat ryhmän toimintatapoja, kuten soittaminen kohdeorganisaation help deskiin ja sosiaalisen manipuloinnin avulla saada pääsy organisaation dataan.[13] BBC:n tietojen mukaan intialainen palveluntarjoaja Tata Consultancy Services (TCS) on käynnistänyt selvityksen, onko Scattered Spider päässyt TCS:n kautta sisälle ainakin Mark & Spencerin ympäristöön.[14]

Sophos raportoi tapauksesta, jossa kiristyshaittatoimija DragonForce onnistui hyväksikäyttämään haavoittuvuutta palveluntarjoaja SimpleHelpin etähallintasovelluksessa. Haavoittuvuuksien avulla DragonForce sai pääsyn palveluntarjoajan SimpleHelpin hallintaan ja pystyi sitä kautta ajamaan erinäisiä komentoja ja sovelluksia, mukaan lukien kiristyshaittaohjelman, palveluntarjoajan asiakkaiden palvelimilla.[15]

[9] AON, 5.5.2025, Bring Your Own Installer: Bypassing EDR Through Agent Version Change Interruption, https://www.aon.com/en/insights/cyber-labs/bring-your-own-installer-bypassing-sentinelone
[10] Lawrence Abrams, 28.4.2025, Marks & Spencer breach linked to Scattered Spider ransomware attack, https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/
[11] BBC, 3.5.2025, Co-op cyber attack affects customer data, firm admits, after hackers contact BBC, https://www.bbc.com/news/articles/crkx3vy54nzo
[12] BBC, 1.5.2025, Harrods latest retailer to be hit by cyber attack, https://www.bbc.com/news/articles/c62x4zxe418o
[13] BBC, 21.5.2025, Retail hackers believed to be young and from US and UK, detectives say, https://www.bbc.com/news/articles/ckgnndrgxv3o
[14] BBC, 23.5.2025, Indian IT giant investigates link to M&S cyber-attack. https://www.bbc.com/news/articles/c989le2p3lno
[15] Sophos, 27.5.2025, DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers, https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/

5. Muuta

5.1 Microsoft estänyt ICC:n pääsyyttäjältä pääsyn sähköpostiin

NL Times raportoi Microsoftin estäneen Kansainvälisen rikostuomioistuimen ICC:n pääsyyttäjän Karim Khanin pääsyn sähköpostiinsa sen jälkeen, kun Yhdysvaltion hallinto asetti ICC:tä kohtaan pakotteita helmikuussa 2025. Pakotteet pitävät sisällään mm. talouspakotteita ja viisumirajoitteita. ICC teki marraskuussa 2024 pidätysmääräyksen Israelin pääministeristä Benjamin Netanjahusta ja entisestä puolustusministeristä Yoav Gallantista.[16]

Tämä on herättänyt keskustelua ja huolta siitä, miten riippuvaisia eurooppalaiset organisaatiot ovat yhdysvaltalaisista yrityksistä ja pilvipalveluteknologioista ja miten kyseiset yritykset voivat mahdollisesti estää pääsyn järjestelmiin. Myös europarlamentaarikko Aura Salla on ottanut asiaan julkisesti kantaa ja on esittänyt asiasta huolen, sillä suomalaiset julkishallinnolliset toimijat ja yksityiset yritykset nojaavat myös vahvasti Microsoftin teknologioihin.[17]

5.2 Microsoft ja Europol keskeyttäneet Lumma Stealer -haittaohjelman toimintoja

Microsoft ja Europol ovat yhteistyössä tehneet mittavan operaation Lumma Stealer -haittaohjelman infrastruktuuria vastaan. Maaliskuun 16:n ja toukokuun 16:n välisenä aikana Microsoft on havainnut yli 394000 Lumma Stealerin saastuttamaa päätelaitetta.[18] Lumma kerää päätelaitteilta tietoja esimerkiksi käyttäjätunnuksiin, salasanoihin, maksukorttitietoihin ja kryptovaluuttoihin liittyen, sekä lähettää ne eteenpäin uhkatoimijan komentopalvelimille.[19] Microsoft on toimittanut Europolille tiedustelutietoa liittyen Lummaan ja tahot ovat tehneet yhteistyötä komentoyhteyksien katkaisemiseksi Lumman ja saastuneiden laitteiden väliltä. Tämä on johtanut yli 2300 domainin haltuunottoon ja estämiseen Microsoftin toimesta.[20]

[16] NL Times, 20.5.2025, https://nltimes.nl/2025/05/20/microsofts-icc-email-block-triggers-dutch-concerns-dependence-us-tech
[17] Verkkouutiset, 28.5.2025, https://www.verkkouutiset.fi/a/eu-parlamentaarikko-varoittaa-suomi-liian-haavoittuva-microsoft-riippuvuudessa/#d93d500d
[18] Europol, 21.5.2025, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
[19] Forcepoint, 7.5.2025, https://www.forcepoint.com/blog/x-labs/unmasking-lumma-stealer-campaign
[20] Microsoft, 21.5.2025, https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

6. Suositukset

Tässä kuussa suosittelemme:

1. Sähköpostilokien auditoinnin tarkistus
2. Salasanojen ja korttitietojen säilyttämistä selaimissa on syytä välttää
3. Microsoft Graph API-lokituksen käyttöönotto

Vaarantuneita M365-käyttäjätunnuksia tutkittaessa on erityisen tärkeää selvittää, mitä asiakirjoja ja sähköposteja on mahdollisesti tarkasteltu ja anastettu uhkatoimijan toimesta. Ne saattavat sisältää arkaluontoisia ja GDPR:n alaisia tietoja, joten vaarantuneet tiedot pitäisi saada selville mahdollisimman tarkasti. Microsoftin dokumentaation perusteella sähköpostien käsittelyyn liittyvät lokit, kuten MailItemsAccessed ja Send, ovat oletuksena päällä.[21] On kuitenkin mahdollista, että organisaatioissa lokit ovat kytketty pois päältä osalta käyttäjistä tai jopa koko organisaationlaajuisesti. Tietoturva-asiantuntija Nathan McNulty kirjoittaa blogissaan, että on mahdollista, etteivät kyseiset lokitapahtumat välttämättä lokitu automaattisesti riittävästä lisenssitasosta huolimatta, jos käyttäjätunnus on useamman vuoden vanha.[22] Lokituspolitiikka olisi syytä tarkistaa, että sähköpostien ja asiakirjojen käsittelytapahtumat varmasti lokittuvat koko organisaatiossa.

Infostealer-tyyppisten haittaohjelmien määrä on ollut kovassa kasvussa koko vuoden ajan. Esimerkiksi Lumma Stealer ja ViperSoftX ovat hyvin yleisesti käytössä olevia infostealer-haittaohjelmia. Nämä leviävät päätelaitteille pääasiassa kalasteluviestien, saastuneiden verkkosivujen tai ClickFix[23]-huijauksen kautta. Nämä haittaohjelmat pyrkivät anastamaan laitteilta tietoa liittyen mm. käyttäjätunnuksiin, salasanoihin, kryptovaluuttalompakoihin ja maksukorttitietoihin. Selaimiin tallennetut tiedot muodostuvat ongelmaksi, sillä haittaohjelmat löytävät niissä sijaitsevat tiedot helposti. Ilmiö on erityisen vaarallinen henkilökohtaisten tietokoneiden tapauksessa. Näillä laitteilla ei välttämättä ole riittävää päätelaitesuojausta tai valvontaa ja niille saatetaan silti tallentaa työpaikan käyttäjätietoja. Näin ollen organisaation tiedot voivat vaarantua käyttäjien henkilökohtaisten laitteiden kautta. Selaimeen tallentamisen sijaan olisi suositeltavaa käyttää esimerkiksi salasanojen hallintaohjelmistoa käyttäjätietojen säilyttämiseksi.

Microsoftin Azuren näkyvyyden ja havainnointikyvykkyyden parantamiseksi suosittelemme ottamaan käyttöön Microsoft Graph API -lokituksen. Kyseiset lokit antavat näkyvyyden Azuressa tapahtuviin HTTP- ja API-kyselyihin. Monien Azuressa käytettävien hyökkäystyökalujen, kuten AzureHound[24] ja GraphRunner[25], jäljet ovat pääasiassa havaittavissa ainoastaan näiden lokien avulla. Graph API -lokit ovat siis erittäin hyödyllisiä poikkeavan toiminnan havaitsemiseksi Azuressa, ja ne olisivat suositeltavaa olla kytkettynä

[21] Microsoft, 27.5.205, https://learn.microsoft.com/en-us/purview/audit-mailboxes
[22] Nathan McNulty, 27.5.2025, https://nathanmcnulty.com/blog/2023/01/azure-automation-advanced-auditing/
[23] Group-IB, 28.5.2025, https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims/
[24] SpecterOps, 28.5.2025, https://github.com/SpecterOps/AzureHound
[25] Dafthack, 28.5.2025, https://github.com/dafthack/GraphRunner

päälle ympäristöissä. Tietoturva-asiantuntija Eric M. on myös tuonut LinkedIn:ssä esille uuden tavan ladata sähköposteja käyttäjien sähköpostilaatikoista uuden Graph Export-Import APIn[26] avulla. Eric M:n mukaan kyseisen APIn kautta tehdyt toimet eivät synnytä ollenkaan lokitapahtumia perinteisiin M365-lokeihin, kuten Unified Audit Log:iin tai OfficeActivity-tauluun.[27] Tämän APIn kautta tehdyt sähköpostien tarkasteluun liittyvät toimet näkyvät kuitenkin Graph APIn lokeissa. Sähköpostia tarkastelevalla entiteetillä on lisäksi oltava MailboxItem.ImportExport.All-käyttöoikeus. Graph API-lokien kerääminen SIEMiin voi aiheuttaa merkittäviä lisäkustannuksia organisaation lokimäärästä riippuen ja niiden osalta voi olla tarpeen tehdä suodatusta kustannusten hillitsemiseksi.

[26] Microsoft, 28.5.2025, https://learn.microsoft.com/en-us/graph/mailbox-import-export-concept-overview
[27] Eric M, 27.5.2025, https://www.linkedin.com/posts/emannon_exfilling-m365-mailboxes-the-sneaky-activity-7332951156064690176-NTCf?utm_source=share&utm_medium=member_desktop&rcm=ACoAACGhYXoBUmguM2xVfFkiB10gzN9EpEUBSwQ

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