LOIHDE

KYBERKATSAUS

2.2025

Tiivistelmä

Helmikuussa verkon reunalaitteista julkaistiin jälleen merkittäviä haavoittuvuuksia ja myös niiden aktiivista hyväksikäyttöä on raportoitu osassa haavoittuvuuksista.

Pohjoismaisessa mediassa keskustelua on helmikuussa herättänyt Nordnetilla tapahtunut tekninen ongelma, jonka seurauksena palvelussa on ollut mahdollista päästä käsiksi muiden käyttäjien tilitietoihin. Helmikuussa uutisotsikoihin nousi myös Black Basta -kiristyshaittaohjelmatoimijan vuodetut sisäiset keskustelut. Keskustelut ovat sisältäneet kiinnostavaa tietoa ryhmittymän toimiin liittyen.

Suomen lähialueella tilanne on edelleen Venäjän ja länsimaiden välillä kireä. Helmikuun loppupuoliskolla Gotlannin edustalla vaurioitui jälleen merikaapeli. Kyseinen kaapeli vahingoittui edellisen kerran joulupäivänä 2024. Itämeren tilanne ja esimerkiksi Venäjän retoriikka länsimaita kohtaan ei ole vuoden alussa näyttänyt lieventymisen merkkejä.

Suomalaisten yritysten näkökulmasta helmikuun tapahtumat alleviivaavat proaktiivisen ja jatkuvasti kehitettävän tietoturvan merkitystä. Tämän lisäksi yritysten on syytä tarkistaa varautumissuunnitelmansa ja varautua esimerkiksi tietoliikenteen ja sähkönjakelun katkoksiin.

KUUKAUSIRAPORTTI 2/2025

Tämä raportti sisältää kuvauksen helmikuun 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 2/2025 2
1. Yleistilanne 3
2. Haavoittuvuudet 3
2.1 CVE-2025-0108 PAN-OS: Authentication Bypass in the Management Web Interface 3
2.2 CVE-2025-21589: Juniper Networks Session Smart Router Authentication Vulnerability 4
2.3 CVE-2025-22467: Stack-based buffer overflow in Ivanti Connect Secure 4
3. Kalastelu ja huijaukset 5
4. Kiristyshaittaohjelmat ja -toimijat 5
5. Muuta 6
5.1 Nordnet 6
5.2 Kaapelikatkos Itämerellä 6
6. Suositukset 7

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 kehitystyötä kyberturvallisuuden kehittämiseksi.

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.

Suomalaisten yritysten on hyvä huomioida toiminnassaan, että 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

Helmikuussa julkaistiin jälleen merkittäviä haavoittuvuuksia. Verkon reunalaitteista löytyvät haavoittuvuudet ovat korostuneet viime aikoina, eivätkä helmikuussa julkaistut haavoittuvuudet olleet poikkeus näiden osalta.

2.1 CVE-2025-0108 PAN-OS: Authentication Bypass in the Management Web Interface

Palo Alto Networks julkisti 12.2.2025 kriittisen haavoittuvuuden, joka koskettaa heidän PAN-OS-käyttöjärjestelmäänsä. Kyseistä käyttöjärjestelmää käyttävät mm. yhtiön valmistamat palomuurituotteet. Kyseinen haavoittuvuus mahdollistaa autentikoinnin ohittamisen hallintapaneeliin. Haavoittuvuuden hyväksikäyttö kuitenkin edellyttää, että hallintapaneeliin on rajoittamaton pääsy Internetistä. Näin ollen valmistaja suosittelee rajapinnan rajaamista ainoastaan luotettuihin IP-osoitteisiin.

Tietoturvayhtiö Arctic Wolf raportoi, että maailmalla on havaittu haavoittuvuuden hyväksikäyttöä ketjutettuna yhdessä CVE-2024-9474:n kanssa mahdollistaen koodin suorittamisen root-oikeuksin.[1] Palo Alto Networks on myös julkaissut haavoittuvuuden korjaavan päivityksen ja organisaatioita suositellaankin päivittämään ohjelmistoversio pikimmiten.[2]

2.2 CVE-2025-21589: Juniper Networks Session Smart Router Authentication Vulnerability

Juniper Networks tiedotti 11.2.2025 haavoittuvuudesta, joka vaikuttaa valmistajan Session Smart Router SD-WAN-ratkaisuun.[3] Haavoittuvuutta hyväksikäyttämällä on mahdollista ohittaa autentikointi kokonaan ja saada pääkäyttäjäoikeudet järjestelmään. Juniper ei itse ole tiedotteen mukaan toistaiseksi havainnut haavoittuvuuden hyväksikäyttöä, mutta sen saadessa enemmän julkisuutta on hyväksikäyttö todennäköistä. Hacker Newsin julkaiseman artikkelin perusteella Juniper olisi itse löytänyt haavoittuvuuden sisäisen tietoturvatestauksen seurauksena.[4] Juniper on julkaissut haavoittuvuudelle korjaavan päivityksen, joka onkin valmistajan mukaan ainut tapa korjata haavoittuvuus.

2.3 CVE-2025-22467: Stack-based buffer overflow in Ivanti Connect Secure

Ivantin Connect Secure VPN:ään julkaistiin 11.2.2025 kriittinen muistin ylivuotohaavoittuvuus, joka mahdollistaa koodin suorittamisen etänä VPN-laitteella. Hyväksikäyttö voi johtaa arkaluontoisen tiedon varastamiseen ja uhkatoimijan laajempaan pääsyyn organisaation ympäristöön.

Haavoittuvuuden CVSS-luokitus on 9.9, joka tekee siitä erityisen kriittisen. Tämänkin haavoittuvuuden kohdalla korostuu hallintarajapinnan pääsyn rajaaminen luotettuihin verkkoihin, mikä vähentää hyökkäyspinta-alaa merkittävästi.[5] Ivantin mukaan haavoittuvuuden hyväksikäyttöä ei olla vielä havaittu[6], mutta päivityksen ja Proof of Concept -koodin julkaisemisen jälkeen haavoittuvuutta tullaan mitä todennäköisimmin hyväksikäyttämään.

[1] https://arcticwolf.com/resources/blog/cve-2025-0108/
[2] https://security.paloaltonetworks.com/CVE-2025-0108
[3] https://supportportal.juniper.net/s/article/2025-02-Out-of-Cycle-Security-Bulletin-Session-Smart-Router-Session-Smart-Conductor-WAN-Assurance-Router-API-Authentication-Bypass-Vulnerability-CVE-2025-21589?language=en_US
[4] https://thehackernews.com/2025/02/juniper-session-smart-routers.html
[5] https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US
[6] https://www.ivanti.com/blog/february-security-update

3. Kalastelu ja huijaukset

Microsoft Threat Intelligence[7] raportoi helmikuussa tietojenkalastelukampanjasta, jonka Microsoft on havainnut uhkatoimijan nimeltä Storm-2372 toimesta. Microsoftin mukaan kampanjaa on toteutettu jo elokuusta 2024 lähtien, ja se on kohdistunut laaja-alaisesti niin hallituksiin, kansalaisjärjestöihin kuin eri toimialoihin. Mikä tekee tästä poikkeuksellista, on se, että toimija on käyttänyt kalastelutekniikkana laitekoodia (Device Code). Laitekoodi on kirjautumiskeino, jota käytetään monesti silloin, kun halutaan kirjautua palveluun laitteella, jossa ei ole näppäimistöä. Tällaisia voivat olla esimerkiksi älytelevisio tai videoneuvottelulaite. Kalastelussa vastaanottajalle on lähetetty valheellinen Microsoft Teams -palaverikutsu.

Kalasteluun on käytetty mm. WhatsAppia, Signalia ja Teamsia. Vastaanottajan kanssa on aluksi keskusteltu pikaviestisovelluksessa luottamussuhteen muodostamiseksi ja tämän jälkeen on lähetetty kalastelusähköposti. Viestissä on annettu hyökkääjän generoima laitekoodi, jolla vastaanottajaa pyydetään kirjautumaan viestissä olevan linkin kautta, joka on aito Microsoftin sivusto. Vastaanottaja syöttää saamansa laitekoodin sivustolle, ja hyökkääjä saa tässä vaiheessa pääsyn vastaanottajan käyttäjätunnukselle. Sisäänkirjautumisprosessi tapahtuu kokonaisuudessaan Microsoftin osoitteissa, joten mitään haitallisia sivustoja tai URLeja ei kirjautumiseen liity. Havainnointikeinoina ovat tässä tapauksessa vastaanottajan valppaus kalasteluviestien suhteen ja laitekoodikirjautumisten valvonta.

Mikäli laitekoodia ei käytetä kirjautumiseen organisaatiossa, on se suositeltavaa ottaa pois päältä kokonaan. Esimerkiksi Microsoftin Entra ID:stä laitekoodikirjautumiset voidaan estää Conditional Access Policyin.[8]

4. Kiristyshaittaohjelmat ja -toimijat

Psykoterapiakeskus Vastaamon tietomurtoon liittyen on otettu kiinni toinen epäilty Virossa tammikuussa. Kiinniotetun epäillään olevan Vastaamon toimitusjohtajalle ja muille vastuuhenkilöille lähetettyjen lunnasvaatimusten takana.[9]

Yhdysvallat lisäsi Zservers-nimisen ”bulletproof hosting” -palveluntarjoajan pakotelistalleen. Pian tämän jälkeen Alankomaiden poliisi takavarikoi 127 Zserversin käyttämää palvelinta, jotka sijaitsivat alankomaisessa konesalissa. LockBit- ja Conti-kiristyshaittatoimijoiden uskotaan käyttäneen Zserversin palveluita hyökkäyksissään.[10]

[7] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/#Update-February-14
[8] https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows
[9] HS, 21.2.2025, Verkko-uutiset: Toinen Vastaamon tietomurrosta epäilty otettu kiinni Virossa, https://www.hs.fi/suomi/art-2000011048938.html
[10] The Record, 13.2.2025, Dutch police say they took down 127 servers used by sanctioned hosting service, https://therecord.media/dutch-police-take-down-127-servers-sanctioned-host

Symantec raportoi poikkeuksellisesta RA World -kiristyshaittaohjelmatapauksesta, jossa haittatoimija on käyttänyt hyökkäyksessä työkaluja, jotka on aikaisemmin linkitetty kiinalaiseen tiedustelutoimintaa tehneeseen Mustang Panda -haittatoimijaan. On epäselvää, miksi työkalut ovat päätyneet kiristyshaittatoimijalle. Kyseessä voi olla tiedustelutoiminnan peittely kiristyshaittaohjelmalla tai sitten Mustang Pandan jäsen saattaa kerätä lisätienestejä kiristyshaittaohjelmilla.[11]

Helmikuussa Black Basta -kiristyshaittaohjelmaryhmän sisäiset Matrix-palvelun chat-keskustelut vuodettiin MEGA-tiedostonjakopalveluun, josta poistuttuaan ne jaettiin eräälle Telegram-kanavalle. Toistaiseksi tuntematon henkilö jakoi arkiston, joka sisältää mm. ryhmän käyttämiä kalasteluviestien pohjia, kryptovaluuttaosoitteita sekä uhrien käyttäjätunnuksia ajalta 18.9.2023–28.9.2024.[12]

5. Muuta

5.1 Nordnet

Verkkopankki Nordnetilla sattui 11.2. laaja ja erittäin vakava tekninen ongelma, jonka takia Nordnetin asiakkaiden oli hetkellisesti mahdollista päästä käsiksi muiden palvelun asiakkaiden tileihin. Varotoimenpiteenä Nordnet sulki tiistaina verkko- ja mobiilipalvelunsa havaittuaan ongelman. Ongelman syynä oli Nordnetin mukaan ”kirjautumiseen liittyvä ohjelmistokomponentti”, jonka tekninen ongelma mahdollisti. Tiistaina 11.2. palveluun kirjautuessaan osa asiakkaista sai eteensä jonkun muun kuin oman tilinsä näkymän omistuksineen kaikkineen. Palvelu palautui toimintaan muutaman tunnin katkon jälkeen.[13]

Ongelman aikana oli Nordnetin mukaan tapahtunut vain yksi virheellinen transaktio, jossa palvelun ruotsalainen asiakas oli myynyt erään suomalaisen asiakkaan sijoituksia n. 7000 eurolla.[14]

5.2 Kaapelirikko Itämerellä

21.2.2025 tiedotettiin jälleen uudesta kaapelirikosta Itämerellä. Epäilty vaurio todettiin Suomen ja Saksan välisessä Cinian omistamassa C-Lion1-kaapelissa, ja se on tapahtunut Ruotsin talousvyöhykkeellä Gotlannin edustalla. Samassa kaapelissa havaittiin vaurio vasta paria kuukautta aikaisemmin, kun Eagle S -alus vaurioitti kaapelia joulupäivänä.

[11] Symantec, 13.2.2025, China-linked Espionage Tools Used in Ransomware Attacks, https://www.security.com/threat-intelligence/chinese-espionage-ransomware
[12] Bleeping Computer, 20.2.2025, Black Basta ransomware gang's internal chat logs leak online, https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/
[13] X, 11.2.2025, Nordnetin postaus X-tilillään, https://x.com/nordnetFI/status/1889327238845280563
[14] HS, 12.2.2025, Nordnetin ruotsalais-asiakas myi 7 000 eurolla suomalaisen asiakkaan osakkeita, https://www.hs.fi/talous/art-2000011029048.html

Keskusrikospoliisi on käynnistänyt tapauksesta esiselvityksen. Traficomin mukaan vaurio ei vaikuta suomalaisiin.[15]

6. Suositukset

Tässä kuussa suosittelemme:

1. Conditional Access Policyjen tiukentaminen
2. Paikallisten järjestelmänvalvojatunnusten käytön rajaaminen
3. Audit Policy -lokitusten parantaminen

M365-käyttäjätilien kalastelut ja murrot ovat olleet jälleen nosteessa suomalaisissa organisaatioissa alkuvuodesta 2025. Perinteiset kaksivaiheiset tunnistautumiset (MFA), kuten tekstiviesti tai puhelinsovellus, on todettu riittämättömiksi suojaamaan käyttäjätunnuksia Adversary in the Middle (AiTM)-kalasteluilta. MFA:n käytön lisäksi pääsynhallintaa organisaation pilvipalveluihin tulisi tiukentaa ja rajata kirjautumiset esimerkiksi Conditional Access Policyillä[16] luotettuihin (Entra ID- tai Hybrid-liitettyihin) laitteisiin tai IP-osoitteisiin. Tällöin kalastelun onnistuessa uhkatoimija ei pääse kirjautumaan käyttäjätunnukselle, vaikka salasana tai kirjautumis-token saataisiin haltuun, koska kirjautuminen ei ole tullut luotetulta laitteelta tai luotetusta sijainnista. Tämäkään ei takaa täyttä suojaa, mutta vähentää kirjautumispinta-alaa merkittävästi.

Uhkatoimijoiden käyttämät kalastelumekanismit kehittyvät jatkuvasti ja organisaatioiden on pysyttävä niistä ajan tasalla. Kaikkia kalasteluviestejä ei pystytä pysäyttämään, joten kompensoivia kontrolleja, kuten Conditional Access Policyt, on oltava olemassa siinä vaiheessa, kun estävät kontrollit epäonnistuvat. Policyjen käyttöönotto voi olla organisaatiosta riippuen haastavaa, mutta AiTM-kalastelu on tullut jäädäkseen, eivätkä perinteiset kontrollit riitä niistä syntyvien tietomurtojen pysäyttämiseksi.

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. Esimerkiksi järjestelmien ylläpitäjien yleisesti käyttämän PsExec-työkalun[17] käyttö vaatii paikalliset järjestelmänvalvojatunnukset toimiakseen. Kyseinen työkalu on myös hyvin suosittu kiristyshaittaohjelmatoimijoiden keskuudessa ja sitä käytetäänkin paljon sivuttaisliikehdintään ja kiristyshaittaohjelman levittämiseen ympäristöissä. Toinen kiristyshaittaohjelmatoimijoiden suosima haittaohjelma on Mimikatz[18], jota käytetään mm. salasanojen keräämiseen (Credential dumping). Mimikatzin käyttö vaatii myös vähintään

[15] HS, 21.2.2025, Tämä viimeisimmästä kaapeli-vauriosta tiedetään nyt, https://www.hs.fi/suomi/art-2000011049753.html
[16] https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-alt-all-users-compliant-hybrid-or-mfa
[17] https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
[18] https://github.com/ParrotSec/mimikatz

paikalliset järjestelmänvalvojatunnukset laitteelle. Käyttäjäkohtaisten paikallisten järjestelmänvalvojatunnusten poistaminen käytöstä on suositeltavaa. Erilaisilla Privileged Access Management (PAM) -ratkaisuilla voidaan tämän jälkeen hallitusti myöntää järjestelmänvalvojatunnuksia käyttäjille tilapäisesti, kun niitä tarvitaan esimerkiksi sovelluksen asentamiseen. Järjestelmänvalvojatunnusten rajaaminen voi aiheuttaa vastustusta käyttäjissä, mutta se hankaloittaa uhkatoimijoiden kyvykkyyksiä toimia ympäristössä merkittävästi.

Hyödyllisen lokin ja telemetrian kerääminen ja valvominen ympäristön laitteilta vaatii sen, että laitteet on konfiguroitu ylipäätään lokittamaan halutut tapahtumat. Etenkin Windows-ympäristössä lokitusasetukset eivät oletuksena tue poikkeamien havaitsemista ja tutkintaa parhaalla mahdollisella tavalla. Microsoft on tuottanut suositukset eri audit policy -asetuksista[19], jotka toimivat hyvänä pohjana ja jotka suosittelemme konfiguroimaan päälle. audit policy -asetusten lisäksi suosittelemme erittäin vahvasti konfiguroimaan päälle myös:

- Komentorivien lokituksen prosessien luonti -tapahtumissa (Command line auditing)[20]
- PowerShell Script Block Logging

Näiden lisäksi suosittelemme kasvattamaan ainakin Windowsin Security-lokin maksimikoon vähintään yhteen gigatavuun. Jo näillä parannuksilla tietomurtotukinta helpottuu merkittävästi poikkeaman sattuessa.

[19] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
[20] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

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