Kyberkatsaus

11/2025

LOIHDE

Tiivistelmä

Tietojenkalastelussa ei ole tapahtunut merkittäviä muutoksia lokakuuhun verrattuna. Kyberturvallisuuskeskus poisti syyskuussa antamansa vakavan varoituksen M365-tunnusten kalasteluun liittyen, mutta niitä tapahtuu silti merkittävissä määrin eikä muutosta ole näköpiirissä. Marraskuun kyberkatsauksessa tietoturvahaavoittuvuuksia edustavat Fortinetin FortiWeb ja Microsoft Windows.

Maailmalla sattuneista kyberturvatapahtumista nostamme esiin pari mielenkiintoista tapausta. Japanilaiseen panimo Asahiin kohdistui merkittävä kiristyshaittaohjelmahyökkäys, joka lamaannutti mm. heidän oluttuotantoaan. Palautumistoimenpiteet kestävät näillä näkymin helmikuuhun 2026 saakka. Yhdysvalloissa puolestaan kolme entistä tietoturva-asiantuntijaa on tuomittu kiristyshaittaohjelmahyökkäyksistä. He ovat suorittaneet viiteen yritykseen kiristyshaittaohjelmahyökkäyksiä BlackCat-haittaohjelmalla.

Microsoftin Ignite 2025 -tapahtumassa julkistettiin lukuisia uusia ominaisuuksia ja parannuksia Microsoftin ekosysteemiin. Näihin liittyen raportille on nostettu Sysmon-lokituslaajennuksen laajeneminen natiiviksi lisäkomponentiksi Windows Server 2025:lle ja Windows 11:lle, mikä on otettu tietoturvapiireissä ilolla vastaan.

Marraskuussa keskustelua on herättänyt Shai-Hulud 2.0 -haittaohjelmakampanja, joka on npm-pakettien kautta leviävä haittaohjelma. Se asentuu huomaamatta kehitysympäristöihin, varastaa tunnisteita ja muuta arkaluonteista dataa sekä pyrkii peittämään toimintansa. Koska monet kehittäjät ja CI/CD-ympäristöt luottavat laajalti npm-ekosysteemiin, tällaiset toimitusketjuhyökkäykset muodostavat merkittävän riskin ja vastaavia uhkia voidaan odottaa tulevaisuudessa lisää.

Kyberkatsauksessa on lisäksi mukana Loihteen CSOC:n marraskuun 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.

Kyberkatsaus viettää joululomaa kuukauden ajan. Seuraava kyberkatsaus julkaistaan näin ollen helmikuun alussa.

KUUKAUSIRAPORTTI 11/2025

Tämä raportti sisältää kuvauksen marraskuun 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 11/2025 2
1. Yleistilanne 3
2. Haavoittuvuudet 4
2.1 CVE-2025-64446: Critical Vulnerability in Fortinet FortiWeb 4
2.2 CVE-2025-62215: Windows Kernel Zero-Day Vulnerability 4
3. Kalastelu ja huijaukset 5
4. Kiristyshaittaohjelmat ja -toimijat 6
4.1 Asahiin kohdistunut kiristyshaittaohjelmahyökkäys 6
4.2 Entiset tietoturva-asiantuntijat kiristyshaittaohjelmatoimijoina 6
5. Muuta 7
5.1 Sysmon-lokituslaajennus tulossa natiivina laajennuksena Windows 11:lle ja Windows Server 2025:lle 7
5.2 Shai-Hulud-mato saastuttaa npm-paketteja 7
6. Suositukset 8

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. Myös vakavien tietoturvahaavoittuvuuksien 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.

[1] Traficom 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-2025-64446: Critical Vulnerability in Fortinet FortiWeb

Fortinetin FortiWeb-tuotteesta on löydetty kriittinen haavoittuvuus, jonka hyväksikäyttöä on havaittu maailmalla mahdollisesti jo lokakuussa. Perjantaina 14.11. Fortinet julkaisi tiedotteen haavoittuvuudesta CVE-2025-64446, joka mahdollistaa autentikoimattoman hyökkääjän saada pääkäyttäjäoikeuden pääsy FortiWeb Manager -paneeliin.[2]

Haavoittuvuutta hyväksikäyttääkseen hyökkääjä voi lähettää FortiWeb-tuotteen webhallintaan http-kutsun, joka yhdistää path traversal -haavoittuvuuden ja autentikoinnin ohituksen haavoittuvuuden.[3] Haavoittuvuutta hyväksikäyttämällä voi mm. luoda laitteelle uuden, hyökkääjän hallitseman järjestelmänvalvojatason käyttäjän. Hyväksikäytön yksinkertaisuus ja haavoittuvuuden laajuus tekevät siitä kriittisen.

Korjaavat päivitykset suositellaan asennettavan välittömästi. Fortinet suosittelee myös tarkistamaan laitteen konfiguraatiot ja lokit epäilyttävien muutosten, kuten sinne kuulumattomien admin-käyttäjien, varalta. Haavoittuvuuden hyväksikäyttö vaatii hyökkääjän pääsyn laitteen webhallintaan, jonka ei tulisi olla auki internetiin samoin kuin ei muidenkaan verkon reunalaitteiden hallintarajapintojen.[4]

2.2 CVE-2025-62215: Windows Kernel Zero-Day Vulnerability

Osana marraskuun päivityksiä Microsoft julkaisi 11.11. korjauksen lokaaliin käyttöoikeuksien korottamisen mahdollistavaan haavoittuvuuteen CVE-2025-62215. Haavoittuvuus istuu Windowsin kernelissä, ja se koskettaa päivittämättömiä Windows 10- ja 11 -versioita sekä palvelinversioita Windows Server 2019–2025.[5]

Haavoittuvuus juontuu kilpailutilanteesta (race condition) Windowsin kernelissä liittyen jaettujen resurssien samanaikaiseen käsittelyyn. Onnistunut hyväksikäyttö voi mahdollistaa paikallisen pääsyn omaavalle hyökkääjälle korkeimman eli SYSTEM-tason oikeudet laitteelle. Microsoft on vahvistanut havainneensa haavoittuvuuden aktiivista hyväksikäyttöä.[6] Korjaavien päivitysten asentaminen pikimmiten on suositeltavaa, kuten Windows-päivitysten säännöllinen ja automaattinen asentaminen muutenkin, jonka osana tämä ja myös liuta muita haavoittuvuuksia on korjattu.

---

[2] Rapid7, 19.11.2025, CVE-2025-64446: Critical Vulnerability in Fortinet FortiWeb Exploited in the Wild, https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/
[3] WatchTowr Labs, 14.11.2025, When The Impersonation Function Gets Used To Impersonate Users (Fortinet FortiWeb Auth. Bypass CVE-2025-64446), https://labs.watchtowr.com/when-the-impersonation-function-gets-used-to-impersonate-users-fortinet-fortiweb-auth-bypass/
[4] Fortinet, 14.11.2025, Path confusion vulnerability in GUI, https://fortiguard.fortinet.com/psirt/FG-IR-25-910
[5] Microsoft, 11.11.2025, Windows Kernel Elevation of Privilege Vulnerability, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215
[6] SOCRadar, 12.11.2025, November 2025 Patch Tuesday: Microsoft Fixes 63 Vulnerabilities, Including Windows Kernel Zero-Day (CVE-2025-62215), https://socradar.io/november-2025-patch-tuesday-microsoft-cve-2025-62215/

3. Kalastelu ja huijaukset

Kyberturvallisuuskeskus on poistanut syyskuussa julkaisemansa vakavan varoituksen liittyen Microsoft 365 -tilimurtoihin. Tilimurtojen tasoittumisesta huolimatta uhka on edelleen olemassa, ja Loihteen CSOC havaitsee murrettuja M365-tilejä edelleen lähes päivittäin. Alkava joululomakausi myös ruokkii uhkatoimijoita suorittamaan tietojenkalastelua, koska käyttäjät pyrkivät kiireessä saamaan tehtäviään valmiiksi ennen lomia, jolloin virheiden riski kasvaa.[7] Kyberturvallisuuskeskuksella on kattava lista toimintaohjeita mm. Microsoft 365-tunnusten kalasteluilta suojautumiseen.[8]

Sneaky 2FA -kalastelutyökalun kehittäjät ovat lisänneet uusia toiminnallisuuksia työkaluunsa. Kalastelutyökalun kehittäjät ovat lisänneet ns. Browser-in-the-Browser (BitB) -toiminnallisuuden työkaluun. BitB mahdollistaa väärennettyjen selainikkunoiden luomisen CSS:n ja HTML:n avulla, ja nämä ikkunat pystyvät matkimaan oikeita kirjautumissivustoja. Sneaky 2FA osaa tehdä ehdollista tarkastelua, mikä tarkoittaa sitä, että ainoastaan kalasteluviestin kohde voi avata lopullisen kalastelusivun ja muille näytetään tavallisia sivustoja, kuten Google tai YouTube. Tässäkin tarkoituksena on lopulta kalastella käyttäjän Microsoft 365 -tunnukset.[9]

[7] https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/microsoft-365-tilimurroista-kertova-varoitus-poistettu
[8] https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille
[9] https://www.reddit.com/r/msp/comments/1lowust/really_poor_experience_with_barracuda_xdr/

4. Kiristyshaittaohjelmat ja -toimijat

4.1 Asahiin kohdistunut kiristyshaittaohjelmahyökkäys

Qilin-kiristyshaittatoimijan uhriksi joutunut japanilainen panimoyhtiö Asahi Group on kertonut tavoittelevansa toimintansa palauttamista normaaliksi helmikuuhun mennessä. Syyskuun lopulta asti kiristyshaittaohjelmahyökkäyksen aiheuttamista tuotannon katkoksista kärsinyt Asahi ilmoitti myös, että Qilinin varastaman datan joukossa on jopa 1,5 miljoonan heidän asiakkaansa henkilötietoja. Poikkeama on aiheuttanut oluen saatavuusongelmia kaupoissa ja ravintoloissa ympäri Japanin.[10]

BBC:n mukaan Asahi kattaa 40 % Japanin olutmarkkinasta ja kiristyshaittaohjelmahyökkäys on näkynyt oluen puutteena kauppojen hyllyissä. Asahi pyrkii palauttamaan toiminnot normaaliksi helmikuuhun 2026 mennessä.[11]

4.2 Entiset tietoturva-asiantuntijat kiristyshaittaohjelmatoimijoina

Kolmeen tietoturva-alalla työskennelleeseen mieheen on kohdistettu syytteitä, koska he ovat yrittäneet kiristää viittä yhdysvaltalaista yritystä BlackCat-kiristyshaittaohjelmalla vuonna 2023. Viidestä uhrista yksi päätyi maksamaan lunnasvaatimukset. Miehet kiristivät lääkinnällisiä laitteita valmistavalta yritykseltä 10 miljoonaa dollaria ja yritys päätyi lopulta maksamaan 1,27 miljoonan dollarin arvoista kryptovaluuttaa. Muut kiristyksen kohteena olleet yritykset eivät maksaneet lunnasvaatimuksia. Yksi syytetyistä on ilmoittanut motiivikseen henkilökohtaisen velan. Kun yksi miehistä oli joutunut FBI:n ratsaamaksi, toinen oli paennut vaimonsa kanssa Pariisiin. Heidät oli kuitenkin sittemmin saatu kiinni.[12]

[10] https://www.reuters.com/world/asia-pacific/personal-details-15-million-asahi-group-customers-may-have-been-leaked-2025-11-27/
[11] https://www.bbc.com/news/articles/ce86n44178no
[12] https://securityaffairs.com/184240/cyber-crime/former-cybersecurity-employees-attempted-to-extort-five-u-s-companies-in-2023-using-blackcat-ransomware-attacks.html

5. Muuta

5.1 Sysmon-lokituslaajennus tulossa natiivina laajennuksena Windows 11:lle ja Windows Server 2025:lle

Sysmon-lokituslaajennus on tulossa saataville Windows Server 2025- ja Windows 11 -käyttöjärjestelmille natiivina ominaisuutena vuoden 2026 aikana. Tämä on merkittävä parannus, jota on odotettu pitkään. Sysmon mahdollistaa laajemman ja selkeämmän lokituksen kuin esimerkiksi Windowsin natiivit Security-lokit. Haitallisen toiminnan havaitseminen sekä tutkinta ovat huomattavasti helpompaa laitteilla, joilta Sysmon löytyy. Tähän asti Sysmon on ollut käsin asennettava ohjelmisto, jota on pitänyt päivittää manuaalisesti.[13]

Sysmon ei kuitenkaan ole oletuksena päällä, ja se pitää ottaa käyttöön Windowsin Add Features -toiminnon kautta. Lisäksi sitä ei viimeisimmän tiedon mukaan voida ottaa käyttöön kuin Windows 11- ja Server 2025 -käyttöjärjestelmillä. Vanhemmissa käyttöjärjestelmissä asennus pitää edelleen tehdä manuaalisesti. Käyttöönotto ja ylläpitäminen kuitenkin helpottuvat merkittävästi, koska sen voi tehdä suoraan Windowsista ja päivitykset tulevat automaattisesti Windows Update:n mukana.[14]

5.2 Shai-Hulud-mato saastuttaa npm-paketteja

Shai-Hulud 2.0 -nimeä kantavaa haittaohjelmaa on havaittu levitettävän suosittujen npm-pakettien kautta. Tietoturvayhtiö Wiz raportoi, että esimerkiksi Zapier, Posthog ja Postman ovat olleet saastuneiden pakettien joukossa. Haittaohjelma varastaa kehitysympäristöistä mm. GitHub-access tokeneita, pilvipalvelutunnuksia ja API-avaimia ja lähettää ne edelleen hyökkääjälle. Haittaohjelma asentuu samalla, kun saastunut paketti asennetaan ohjelmistokehitysympäristöön. Tällöin se monesti päätyy myös käyttäjän päätelaitteelle. Sillä on myös kyvykkyyksiä piilottaa toimiaan, esimerkiksi poistamalla automaattisesti workflow-tiedoston ja versionhallintaan luomansa branchin.[15]

Koska monet kehitysympäristöt luottavat npm-paketteihin, haittaohjelma aiheuttaa merkittävän uhan mm. lähdekoodille, tunnuksille ja CI/CD-ympäristöille. Koska tällainen toimitusketjutyyppinen haittaohjelmahyökkäys on tehokas, vastaavanlaisia haittaohjelmia on varmasti odotettavissa tulevaisuudessa lisää.[16]

Kyberturvallisuuskeskus on julkaissut tapauksesta listauksen suositeltavista toimenpiteistä.[17]

[13] https://techcommunity.microsoft.com/blog/windows-itpro-blog/native-sysmon-functionality-coming-to-windows/4468112
[14] https://learn.microsoft.com/fi-fi/windows/client-management/client-tools/add-remove-hide-features?tabs=gpo&pivots=windows-11
[15] https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack
[16] https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack
[17] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/shai-hulud-hyokkayksen-toinen-aalto-toimenpidesuositukset-organisaatioille

6. Suositukset

Tässä kuussa suosittelemme:

- Käyttäjien ohjeistaminen kalasteluviesteistä joululomakaudella
- Digipoolin DFIR-jaoksen tietoturvapoikkeamaohjeistuksen läpikäynti
- Pilviympäristöjen käyttöoikeuksien säännöllinen tarkistus

Juhlapyhät ovat otollista aikaa tietojenkalastelulle. Käyttäjät ovat kiireisiä ennen joululomille siirtymistään, koska keskeneräiset työtehtävät pyritään saamaan mahdollisimman valmiiksi ennen lomille siirtymistä. Kiireessä toimiminen altistaa käyttäjät virheille. Uhkatoimijat tiedostavat tämän ja pyrkivät käyttämään tilanteen hyväkseen. Käyttäjiin kohdistetaan kalasteluviestejä juuri ennen lomien ja juhlapyhien alkamista, jolloin riski joutua tietojenkalastelun uhriksi kasvaa merkittävästi. Kalasteluviesti voi tulla tutultakin lähettäjältä, jonka tunnukset ovat vaarantuneet aiemmin. Suosittelemme organisaatioita tiedottamaan loppukäyttäjiä tästä uhasta ja kiinnittämään erityistä huomioita etenkin niihin viesteihin, joissa pyydetään suorittamaan kiireellisesti jokin toimenpide, esimerkiksi laskun maksaminen.

Digipoolin tietoturvapoikkeamajaos (DFIR) on tuottanut ohjeen, jonka tarkoituksena on auttaa varsinkin huoltovarmuuskriittisiä organisaatioita valmistautumaan tietomurron varalle sekä helpottaa tutkintaa ja poikkeamista palautumista. Ohjeistusta voi kuitenkin hyödyntää mikä tahansa organisaatio. Ohjeistukseen on koottu suosituksia tietoturvapoikkeaman eri vaiheisiin ja niitä on priorisoitu tärkeysjärjestyksessä. Ohjeessa on suosituksia liittyen esimerkiksi Windows-laitteiden lokituspolitiikkaan, päätelaitesuojauksen käyttöönottoon ja sopimusteknisiin asioihin sekä tutkintojen suorittamiseen. Suosittelemme organisaatioita käymään ohjeistuksen läpi ja ottamaan suositukset käyttöön organisaatiossa.[18]

Pilvipalveluympäristöihin 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 ei monesti huomata ja ne voivat olla oikotie tenantin haltuun saamiseksi. Suosittelemme organisaatioita auditoimaan käyttöoikeuksia säännöllisesti. Esimerkiksi Entra ID:ssä tämän voi toteuttaa Access Reviews -toiminnolla esimerkiksi tiettyihin ryhmiin tai rooleihin kohdistettuna ja poistamaan niitä esimerkiksi kirjautumishistoriaan perustuen.[19]

[18] https://teknologiateollisuus.fi/digipooli/varautuminen-tietomurtoon/
[19] https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

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.

LOIHDE