



Kyberkatsaus

08/2026

LOIHDE



Tiivistelmä

Elokuun kyberkatsauksessa on nostettu esille kiinnostavia poimintoja ajankohtaisista tapahtumista kyberkentällä:

- EU:n kyberkestävyyslainsäädännön (CRA, Cyber Resilience Act) ilmoittamisvelvollisuus astuu voimaan 11.9.2026
- ClickFix-tyyppiset hyökkäykset ovat nousseet merkittävästi vuonna 2026
- Microsoft Teamsin kautta tapahtuu enenevässä määrin tunnusten- ja tietojenkalastelua
- NSA on yhteistyössä mm. suojelupoliisin kanssa julkaissut varoituksen Venäjän kybertiedustelusta, joka kohdistuu länsimaiseen kriittiseen infrastruktuuriin



Teamsin kautta enenevässä määrin tunnusten- ja tietojenkalastelua

Loihteen CSOC:lla on tiedossa tietojenkalastelutapauksia, joissa organisaatioiden loppukäyttäjiä on kontaktoitu suoraan Microsoft Teamsin kautta.

Näissä tapauksissa on tyypillisesti...



...esiinnytty organisaation johtoryhmän jäsenenä tai IT-tukena ja lähettävän henkilön nimi on vastannut oikeaa henkilöä.



...käytetty sujuvaa suomen kieltä todennäköisesti tekoälyavusteisesti ja pyydetty ratkaisemaan jokin ongelma esim. laskun maksaminen nopealla aikataululla.

Loihteen CSOC:n suositukset

1

Estä Teams-keskustelut hallinnoimattomista organisaatioista

2

Säännöllinen Active Directoryn tietoturvakartoitus

3

Digipoolin DFIR-jaoksen tietoturva-poikkeamaohjeistuksen läpikäynti

KUUKAUSIRAPORTTI 08/2026

Tämä raportti sisältää poimintoja elokuun 2026 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 08/2026	2
1. Poiminnat	3
1.1 EU:n kyberkestävyysäädöksen (CRA) ilmoittamisvelvollisuus astuu voimaan 11.9.2026 ..	3
1.2 ClickFix-hyökkäyksissä tapahtunut merkittävää kasvua	3
1.3 Microsoft Teamsin kautta tapahtuva kalastelu	3
1.4 Venäjän FSB:n verkkovakoilusta julkaistu varoitus	4
2. Suositukset	5

1. Poiminnat

1.1 EU:n kyberkestävyysäädöksen (CRA) ilmoittamisvelvollisuus astuu voimaan 11.9.2026

EU:n kyberkestävyysäädöksen ilmoittamisvelvollisuus astuu voimaan 11.9.2026. Tämä tarkoittaa sitä, että digitaalisia tuotteita valmistavien tahojen on ilmoitettava viranomaisille heidän tuotteissaan esiintyvistä aktiivista hyväksikäyttöä kohtaavista tietoturvaavaoittuvuuksista tai tietoturvapoikkeamista. CRA koskettaa laajemmin valmistajien lisäksi myös tuotteiden maahantuoja ja jakelijoita. Kyberturvallisuuskeskus on julkaissut kattavan tietopaketin ja ohjeistuksen aiheeseen liittyen.¹

1.2 ClickFix-hyökkäyksissä tapahtunut merkittävää kasvua

Loihteen CSOC on havainnut merkittävää kasvua ClickFix-hyökkäyksissä vuoden 2026 aikana. Useimmat hyökkäykset vaikuttavat saaneen alkunsa murretuilta legitiimeiltä verkkosivuilta, jonne ClickFixiä tarjoileva haitake on saatu ladattua. Käyttäjän vieraillessa murretulla sivulla on tälle ilmestynyt CAPTCHAa muistuttava ponnahdusikkuna, jossa on pyydetty tekemään ”korjaustoimenpiteitä” työasemallaan. Tämä lisää itsessään hyökkäyksen uskottavuutta, koska käyttäjät saavat normaalistikin Internetissä vastaansa CAPTCHA-verifiointeja. Hyökkäysten tarkoituksena on harhauttaa käyttäjää suorittamaan haitallisia PowerShell- tai curl-komentoja työasemallaan. Komennon suorittaminen aiheuttaa haittaohjelman latautumisen laitteelle. Tyypillisesti haittaohjelmat ovat joko infostealereita tai etäkomentoja mahdollistavia troijalaisia. ClickFix-hyökkäykset ovat vaarallisia ja haastavia estää, koska käyttäjä saadaan huijattua tekemään itse pyydetty toimenpiteet esimerkiksi haittaohjelman toimittamisen sijaan.²

Tehokas keino torjua ClickFix-hyökkäykset Windows-laitteilla on estää PowerShellin käyttö tavallisilta käyttäjiltä, jolloin haitallista Powershell-komentoa ei pystytä laitteella suorittamaan.

1.3 Microsoft Teamsin kautta tapahtuva kalastelu

Loihteen CSOC:lla on tiedossa tietojenkalastelutapauksia, jossa organisaatioiden loppukäyttäjää on kontaktoitu suoraan Microsoft Teamsin kautta. Poikkeavaa näissä on ollut se, että viestin lähettäjän sähköpostiosoitetta ei ole näkynyt käyttäjän Teams-profiilissa eikä myöskään M365:n lokeissa. Tutkinnan perusteella vaikuttaisi siltä, että mikäli Teams-viestejä lähetetään kuluttajatileiltä käyttäen Teamsin ilmaisversiota, ei lähettäjän sähköpostiosoite

¹ Kyberturvallisuuskeskus, 31.8.2026, Kyberkestävyysäädös (Cyber Resilience Act, CRA), <https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyysaadoss-cyber-resilience-act-cra>

² Microsoft, 21.8.2025, Think before you Click(Fix): Analyzing the ClickFix social engineering technique, <https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/>

näissä tapauksissa lokitu. Tapauksissa on tyypillisesti esiinnytty organisaation johtoryhmän jäsenenä tai IT-tukena ja lähettävän henkilön nimi on vastannut oikeita henkilöitä.

Push Securityn kirjoittamassa artikkelissa on raportoitu vastaavasta toiminnasta. Keskustelut ovat tyypillisesti johtaneet esimerkiksi haitallisen etähallintatyökalun jakamiseen käyttäjälle tai laskutuspetosyritykseen.³

Hyökkäysvektori on siinä mielessä vaarallinen, että uhkatoimija pääsee suoraan keskusteluyhteyteen käyttäjän kanssa ohittaen esimerkiksi sähköpostisuodattimet. Teams kuitenkin varoittaa ennen ensimmäistä keskustelun avaamista, että organisaation ulkopuolelta yritetään avata keskustelua. Käyttäjän täytyy tämä pyyntö erikseen hyväksyä.

1.4 Venäjän FSB:n verkkovakoilusta julkaistu varoitus

NSA julkaisi 13.7.2026 varoituksen yhteistyössä länsimaisten tiedustelupalvelujen kanssa Venäjän tiedustelupalvelu FSB:n kybervakoilusta. Raportin mukaan FSB hyödyntää vakoilussaan heikosti suojattuja julkiverkkoon näkyviä verkkolaitteita. Raportissa on avattu 16:n FSB:n alaisuudessa toimivan organisaation tapoja murtautua organisaatioihin. Toiminta kohdistuu erityisesti kriittiseen infrastruktuuriin, mutta toiminta on myös opportunistista riippuen siitä, mihin järjestelmiin onnistutaan tunkeutumaan.

Raportissa on listattu suosituksia haavoittuvien verkkolaitteiden havaitsemiseksi ja suojaamiseksi haitalliselta toiminnalta. Esimerkkisuosituksina on mainittu SNMPv1- ja v2-versioiden korvaaminen v3:lla ja heikkojen salasanojen välttäminen verkkolaitteiden paikallisilla käyttäjillä.^{4 5}

³ <https://pushsecurity.com/blog/phishing-microsoft-teams-for-initial-access>

⁴ SUPO, 13.7.2026, Suojelupoliisi ja sotilastiedustelu varoittavat yrityksiä Venäjän FSB:n verkkovakoilusta, <https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venajan-fsb-n-verkkovakoilusta>

⁵ NSA, 13.7.2026, Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting, https://media.defense.gov/2026/Jul/09/2003959498/-1/-1/0/CSA_IMPROVE_ROUTER_HYGIENE.PDF

2. Suositukset

- 1 Estä Teams-keskustelut hallinnoimattomista organisaatioista
- 2 Säännöllinen Active Directoryn tietoturvakartoitus
- 3 Digipoolin DFIR-jaoksen tietoturvapoikkeamaohjeistuksen läpikäynti

Teamsin kautta tapahtuvat kuluttajatileiltä (=Unmanaged Organizations) tulevat yhteydenotot on suositeltavaa estää Teams Admin centeristä. Oletusasetukset vaikuttaisivat sallivan yhteydenotot eli asetus pitää erikseen kytkeä pois päältä. Kyseessä on eri toiminnallisuus, kuin ulkopuolisista hallinnoiduista organisaatioista tulevat Teams-yhteydenotot. Microsoftin dokumentaatioissa on ohjeistettu hallinnoimattomista organisaatioista tulevien keskusteluiden estäminen.⁶

Active Directory -ympäristöt ovat suuria ja monimutkaisia kokonaisuuksia, joihin kertyy vuosien saatossa erinäisiä konfiguraatioita. Tämän takia AD:ssa on lukematon määrä vaarallisia hyökkäyspolkuja, joista monet ovat kuitenkin hyvin dokumentoituja ja paikattavissa. Ympäristöjen eläessä jatkuvasti suosittelemme Active Directoryn säännöllistä tietoturvakartoitusta. Hyvä lähtökohta on tehdä kartoitus PingCastle-työkalulla. Työkalu suorittaa ympäristöön "terveystarkastuksen" havaitsemalla mm. konfiguraatiovirheitä, liiallisia admin-oikeuksia, ADCS-riskejä ja potentiaalisia hyökkäyspolkuja. PingCastle luo havainnoistaan selkokiehisen raportin ja priorisoi löydökset pisteyttämällä ne. Raportin avulla voi lähteä priorisoimaan korjaustoimenpiteitä. Organisaation sisäiseen käyttöön työkalu on ilmainen.⁷

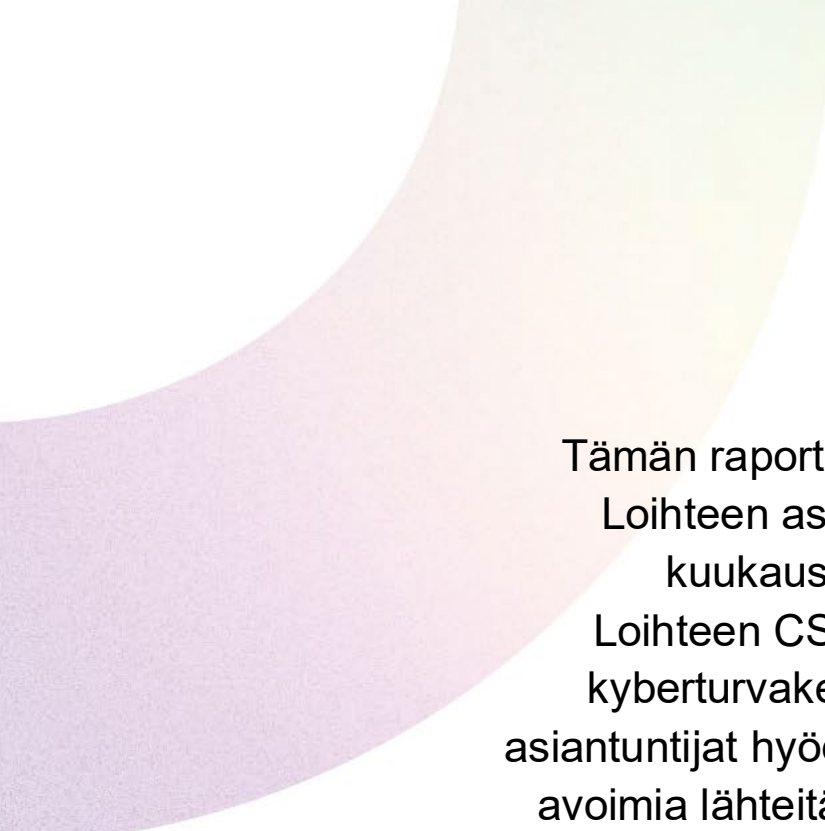
Digipoolin tietoturvapoikkeamajaos (DFIR) on tuottanut ohjeen, jonka tarkoituksena on auttaa varsinkin huoltovarmuuskriittisiä organisaatioita valmistautumaan tietomurron varalle sekä helpottaa tutkintaa ja poikkeamista palautumista. Ohjeistusta voi kuitenkin hyödyntää mikä tahansa organisaatio. Ohjeistukseen on koottu suosituksia tietoturvapoikkeaman eri vaiheisiin ja niitä on priorisoitu tärkeysjärjestyksessä. Ohjeessa on suosituksia liittyen esimerkiksi Windows-laitteiden lokituspolitiikkaan, päätelaitesuojauksen käyttöönottoon ja

⁶ Microsoft, 26.8.2026, Manage chats and meetings with external Teams users not managed by an organization, <https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings#manage-chats-and-meetings-with-external-teams-users-not-managed-by-an-organization>

⁷ <https://www.pingcastle.com/>

sopimusteknisiin asioihin sekä tutkintojen suorittamiseen. Suosittelemme organisaatioita käymään ohjeistuksen läpi ja ottamaan suositukset käyttöön organisaatiossa.⁸

⁸ Teknologiateollisuus, 28.8.2026, Varautuminen tietomurtoon, <https://teknologiateollisuus.fi/digipooli/varautuminen-tietomurtoon/>



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.

