Kyberkatsaus

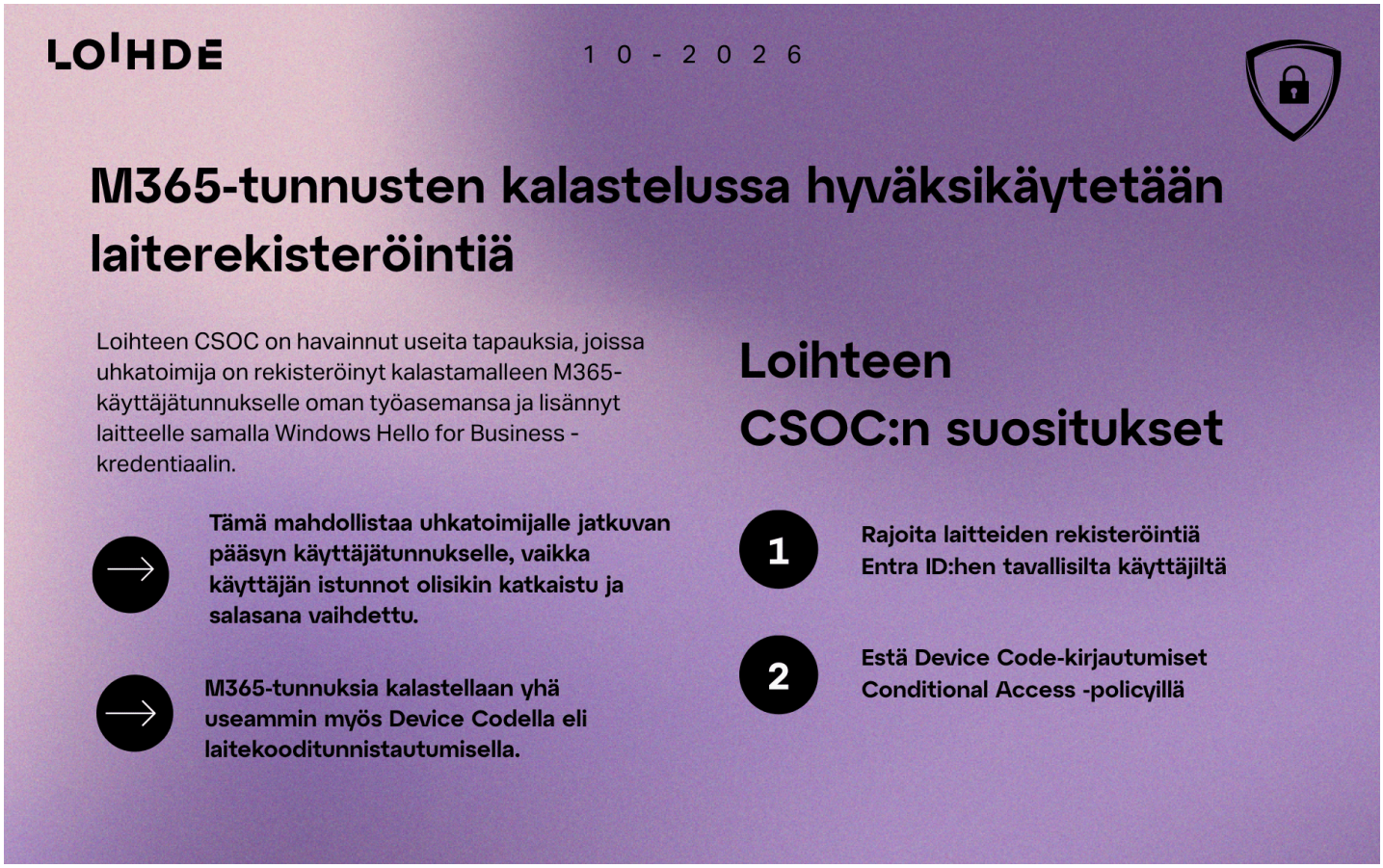
10/2026

LOIHDE

Tiivistelmä

Lokakuun kyberkatsauksessa on nostettu esille kiinnostavia poimintoja ajankohtaisista tapahtumista kyberkentällä:

- ConnectWise Cloud Backup joutui kohteeksi toimitusketjuhyökkäykselle, joka on voinut altistaa kaikki sitä käyttävät M365-ympäristöt.
- Citrix NetScaler -haavoittuvuuksia on hyväksikäytetty laajasti, myös Suomessa.
- PHP:hen julkistettiin kaksi kriittistä tietoturvahaavoittuvuutta, joka ovat saaneet runsaasti julkisuutta.
- eMudhra Certificate Authorityn kahdeksan yksityistä avainta vaarantui heikon luontimenetelmän vuoksi.
- Lokakuun suositukset koskettavat Entra ID:n koventamiseen liittyviä asioita. Suosittelemme rajoittamaan laitteiden rekisteröintiä ja Device Code Flow -kirjautumisia.



KUUKAUSIRAPORTTI 10/2026

Tämä raportti sisältää poimintoja lokakuun 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 10/2026 2
1. Poiminnat 3
ConnectWise Cloud Backup toimitusketjuhyökkäys 3
Citrix NetScaler -haavoittuvuuksia hyväksikäytetty Suomessa 4
PHP2shell 4
eMudhra CA:n heikot private keyt 5
2. Suositukset 6

1. Poiminnat

ConnectWise Cloud Backup -toimitusketjuhyökkäys

M365-palveluiden varmuuskopiointiin käytetty ohjelmisto ConnectWise Cloud Backup (ent. Skykick) joutui lokakuussa toimitusketjuhyökkäyksen kohteeksi. Ohjelmiston käyttämä API-avain vaarantui, mikä antoi uhkatoimijalle pääsyn kaikkiin Cloud Backupia käyttäviin M365-tenanteihin. Kyseessä on Entra ID:hen rekisteröitävä multi-tenant-applikaatio, jonka API-avaimen ylläpidosta vastaa ConnectWise. Cloud Backup tarvitsee varmuuskopiointitoimenpiteitä varten korkeat käyttöoikeudet M365-ympäristöön, ja applikaation vaarantuessa myös uhkatoimija voi niitä hyödyntää. Uhkatoimijan on ollut mahdollista kirjautua applikaatiota käyttävälle palvelutunnukselle ja kartoittaa sekä varastaa ympäristöstä dataa. Tietoturvayhtiö Huntress raportoi havainneensa onnistuneita kirjautumisia yli 300 M365-tenantissa lyhyen ajan sisään, mikä viittaisi automatisoituihin toimiin.[1]

Muutamissa ympäristöissä Huntress raportoi havainneensa uhkatoimijan tekemää pivotointia syvemmälle ympäristöön. Toimijan on havaittu korottaneen Global Administrator -oikeudet ConnectWise Teams -applikaatiolle ja lisänneensä client secrettejä muutamille muille applikaatioille. Nämä ovat mahdollistaneet toimijalle jatkossakin korkeat käyttöoikeudet sekä jalansijan pitämisen ympäristössä, vaikka alkuperäisen vaarantuneen ConnectWise-sovelluksen secretit vaihdettaisiin.[2]

Microsoft on myös tutkinut asiaa ja epäilee hyökkäyksen takana olevan kiinalainen valtiollinen toimija Storm-0940. Microsoftin mukaan Storm-0940 käyttää toiminnoissaan ARTEX open source -tietoturvatestausviitekehystä, joka on mahdollistanut erittäin nopeat, autonomiset kartoitustoimenpiteet vaarannetuissa M365-ympäristöissä.[3]

[1]Semon. J, 16.10.2026, ConnectWise (SkyKick) Vendor Credentials Abused in M365 Attacks, https://www.huntress.com/blog/vendor-credential-enables-unauthorized-access
[2] Semon. J, 16.10.2026, ConnectWise (SkyKick) Vendor Credentials Abused in M365 Attacks, https://www.huntress.com/blog/vendor-credential-enables-unauthorized-access
[3]Microsoft, 21.10.2026, AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise, https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/

Citrix NetScaler -haavoittuvuuksia hyväksikäytetty Suomessa

Citrix julkaisi 27. syyskuuta korjaukset kahdeksaan NetScaler ADC- ja NetScaler Gateway -tuotteiden haavoittuvuuteen. Vakavin niistä, CVE-2026-88771, voi mahdollistaa komentojen suorittamisen laitteella ilman tunnistautumista. Kyberturvallisuuskeskus varoitti 1. lokakuuta, että haavoittuvuuksia oli käytetty tietomurtoihin Suomessa jo ennen korjausten julkaisua. He kartoittivat Suomesta satoja NetScaler-instansseja.[4]

Kyberturvallisuuskeskus päivitti varoitustaan 3. lokakuuta uudella SAML-todennusta koskevalla haavoittuvuudella, CVE-2026-88779:llä, joka altistaa jo korjatut laitteet, jos SAML-todennusta käytetään.[4] Lisäksi 9. lokakuuta KTK tiedotti kolmannesta kriittisestä haavoittuvuudesta, CVE-2026-107406:sta, joka koskee SAML-palveluntarjoajaksi tai identiteetintarjoajaksi konfiguroituja laitteita.[5] Rapid7:n tutkimassa tapauksessa hyökkääjä ketjutti CVE-2026-88771:n ja CVE-2026-88779:n niin, että haitallinen komento suoritettiin laitteen uudelleenkäynnistyksen jälkeen pääkäyttäjän oikeuksilla. Hyökkääjä asensi laitteelle PHP-web shellejä, kartoitti sisäverkon DNS-, LDAP- ja Active Directory -palveluita sekä VMware vCenteriä ja vei laitteen konfiguraatiotietoja ja avainmateriaalia.[6] Reunalaite, joka näkyy internetiin ja kantaa avaimia sisäverkkoon, on hyökkääjälle erityisen houkutteleva kohde.

Organisaatioiden tulee olettaa, että julkiverkkoon näkyvät NetScaler-järjestelmät ovat voineet altistua, ja tutkinta on suositeltavaa myös nopeasti asennettujen päivitysten jälkeen.[4] Suosittelemme päivittämään laitteet uusimpiin korjattuihin versioihin ja tarkistamaan laitteen lokit, uudet käyttäjätunnukset ja ajastetut tehtävät. Ylläpitäjien salasanat sekä laitteelle tallennetut tunnukset ja avaimet on syytä vaihtaa. NetScalerin paikallisten lokien oletusasetukset ovat hyvin niukat ja päälokitiedosto *ns.log* kierrätetään, kun se on kasvanut noin 100 kilotavun kokoiseksi, ja vanhoja pakattuja arkistoja säilytetään 25. Suosittelemme keräämään NetSclareiden lokit keskitettyyn lokienhallintaan kuten SIEMiin sekä kasvattamaan lokitiedoston maksimikokoa oletuskoosta.

PHP2shell

Lokakuun 21. päivänä PHP Foundation ilmoitti kahdesta kriittisestä haavoittuvuudesta (CVE-2026-109618 & CVE-2026-109619) PHP-ohjelmointikielessä, joita sittemmin kutsuttiin yhdessä PHP2Shelliksi. Haavoittuvuudet mahdollistavat etäkoodin suorittamisen ilman tunnistautumista pelkillä HTTP-pyynnöillä. Korjatut versiot ovat 8.5.12, 8.4.27, 8.3.36 ja 8.2.35. PHP 8.1 ja sitä vanhemmat versiot eivät saa PHP-projektilta korjauksia lainkaan.

[4] Kyberturvallisuuskeskus, 1.10.2026, Citrix NetScaler ADC- ja Gateway-tuotteissa kriittisiä haavoittuvuuksia, useita tietomurtoja Suomessa, https://www.kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa

[5] Kyberturvallisuuskeskus, 9.10.2026, Citrix Netscaler ADC ja Gateway -tuotteessa kriittinen haavoittuvuus, https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-34

[6] Rapid7, 19.10.2026, Rapid7 Analysis: NetScaler intrusions chaining CVE-2026-88771 and CVE-2026-88779, https://www.rapid7.com/blog/post/ra-netscaler-intrusions-chaining-cve-2026-88771-and-cve-2026-88779

Apache mod_php on suurimmassa riskissä, koska hyökkäys voi onnistua ennen kuin sovelluskoodia on edes ajettu.[7]

Haavoittuvuuksien hyväksikäyttö alkoi jo ennen korjausta. Sekoian mukaan ensimmäinen hyökkäys havaittiin 17. lokakuuta, koska julkaisun salaus vuoti usean kanavan kautta.[8] CISA lisäsi molemmat haavoittuvuudet aktiivisesti hyväksikäytettyjen haavoittuvuuksien KEV-luetteloonsa 26. lokakuuta.[9] Paria päivää myöhemmin 28. lokakuuta CISA varoitti, että hyökkääjät ketjuttavat PHP2Shellin Linux-ytimen Fragnesia-haavoittuvuuden (CVE-2026-46300) saavuttaen root-oikeudet.[10]

Haavoittuvuuksista pian julkaistuista julkisista hyväksikäyttökoodeista suurin osa oli toimimattomia, mikä edes hieman helpotti ylläpitäjien tuskaa. Organisaatioita suositellaan kartoittamaan, missä heillä käytettään PHP:tä, myös toimittajien sovelluksissa ja laitteissa, ja asentamaan päivitykset viipymättä internetiin näkyvistä järjestelmistä alkaen. Jos päivitystä ei voi asentaa, sovellus tulee eristää julkisesta verkosta.

eMudhra CA:n heikot private keyt

Kahdeksan eMudhra CA:n private key:tä vaarantui, minkä syynä oli sertifikaatin luontiprosessissa oleva vakava puute. Sertifikaattien private keyt luotiin riittämättömällä satunnaisuudella (entropy), jonka vuoksi ne ovat olleet helposti selvitettävissä julkisesta sertifikaatista. eMudhran mukaan avaintenluontiseremonian paketointi- ja purkuvaihe tuotti vahvojen avainten rinnalle toisen, heikon avainsarjan, ja juuri heikot avaimet päätyivät sertifikaatteihin.[11] Google ja Mozilla estivät sertifikaatit nopeasti tapauksen tullessa julki ja Apple, Microsoft sekä Android seurasivat perässä muutaman päivän sisällä tapahtuneesta.

Sertifikaattien revokointi ei kuitenkaan valu automaattisesti kaikkialle, vaan vaatii esimerkiksi ohjelmistojen päivittämistä. Tämä mahdollistaa sertifikaattien väärinkäytön mm. MITM:n ja väärennettyjen sertifikaattien muodossa niin kauan, kunnes vaarantuneet sertifikaatit ovat revokoitu kaikkialta.

Tapahtuman seurauksena eMudhra ilmoitti luopuvansa TLS-sertifikaattiliiketoiminnasta.[12]

[7] PHP, 21.10.2026, October 2026 Security Releases, https://www.php.net/archive/2026.php#2026-10-21-5
[8] Sekoia, 27.10.2026, PHP2Shell Was Exploited Before the Patch, https://www.sekoia.com/blog/php2shell-was-exploited-before-the-patch-expect-more-of-it
[9] CISA, 26.10.2026, CVE-2026-109618: PHP Group PHP — PHP Memory Corruption Vulnerability, https://nvd.nist.gov/vuln/detail/CVE-2026-109618
[10] BleepingComputer, 29.10.2026, CISA warns of Fragnesia Linux flaw chained in PHP2Shell attacks, https://www.bleepingcomputer.com/news/security/cisa-warns-of-fragnesia-linux-flaw-chained-in-php2shell-attacks/
[11] Google Security, 20.10.2026, Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates, https://blog.google/security/protecting-chrome-and-android-users-from-compromised-emudhra-intermediate-ca-certificates/
[12] Khandelwal. S, 22.10.2026, eMudhra to Exit Global SSL/TLS Business After 8 Intermediate CA Keys Found Easily Guessable https://thehackernews.com/2026/10/emudhra-to-exit-global-ssltls-business.html

2. Suositukset

1. Rajoita laitteiden rekisteröintiä Entra ID:hen tavallisilta käyttäjiltä
2. Estä Device Code-kirjautumiset Conditional Access -policyillä

Suosittelemme estämään käyttäjien omatoimisen laitteiden rekisteröinnin Entra ID:hen. Uhkatoimijat rekisteröivät omia laitteitaan vaarantamilleen käyttäjätunnuksille. Tämä antaa toimijalle jalansijan ympäristöön ja mahdollisuuden toimia huomaamattomammin.

Laitteiden rekisteröintiä voidaan rajoittaa esimerkiksi estämällä se Entra ID:stä kokonaan ja luomalla poikkeukset tarpeellisille tunnuksille, vaatimalla tietyn tasoinen MFA (esim. FIDO2) tai TAP laitteen rekisteröimiseksi. Suosittelemme organisaatioita myös auditoimaan Entra ID:n laitetietokannan organisaation nimeämiskäytäntöä noudattamattomien laitteiden varalta. Erityisesti geneerisesti nimetyt Windows-laitteet (WIN- ja DESKTOP-) on syytä tarkistaa tarkemmin.

Loihteen CSOC on havainnut useita tapauksia, joissa M365-käyttäjätunnuksen kalastelun yhteydessä uhkatoimija on rekisteröinyt käyttäjälle oman työasemansa ja lisännyt laitteelle samalla Windows Hello for Business -kredentiaalin. Tämä mahdollistaa uhkatoimijalle jatkuvan pääsyn käyttäjätunnukselle, vaikka käyttäjän istunnot olisikin katkaistu ja salasana vaihdettu. Nämä toimet ovat pääasiallisesti tehty suomalaisista residential proxy IP-osoitteista, jotka hankaloittavat toimien havaitsemista.

M365-käyttäjätunnuksia kalastellaan yhä useammin Device Codella eli laitekooditunnistautumisella. Kalasteluketju hyödyntää Microsoftin legitiimejä domaineja, jolloin esimerkiksi sähköpostisuodattimet päästävät kalasteluviestejä helposti läpi. Suosittelemme poistamaan Device Coden käytöstä Conditional Access -policyllä. Tämä estää sen hyväksikäytön tunnusten kalasteluissa kokonaan. Mikäli Device Code -kirjautumista tarvitaan organisaatiossa, voidaan policyyn luoda poikkeuksia esim. ylläpitäjille tai videoneuvottelulaitteille. Valtaosa käyttäjistä ei kuitenkaan sitä koskaan tarvitse, joten se kannattaa lähtökohtaisesti estää.[13] [14]

[13] Microsoft, n.d, Block authentication flows with Conditional Access policy, https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows#device-code-flow-policies

[14] Kyberturvallisuuskeskus, 21.5.2026. Uusi aalto M365-tietojenkalastelussa – AI-avusteinen laitekoodin kalastelukampanja, https://kyberturvallisuuskeskus.fi/fi/uutiset/uusi-aalto-m365-tietojenkalastelussa-ai-avusteinen-laitekoodin-kalastelukampanja

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