Kyberkatsaus

03/2026

LOIHDE

Tiivistelmä

Maaliskuun kyberkatsauksessa haavoittuvuuksissa esille on nostettu Citrix Netscaleriin ja Cisco Secure Firewall Management Centeriin liittyvät kriittiset haavoittuvuudet sekä Axios JavaScript -kirjastoon kohdistunut toimitusketjuhyökkäys.

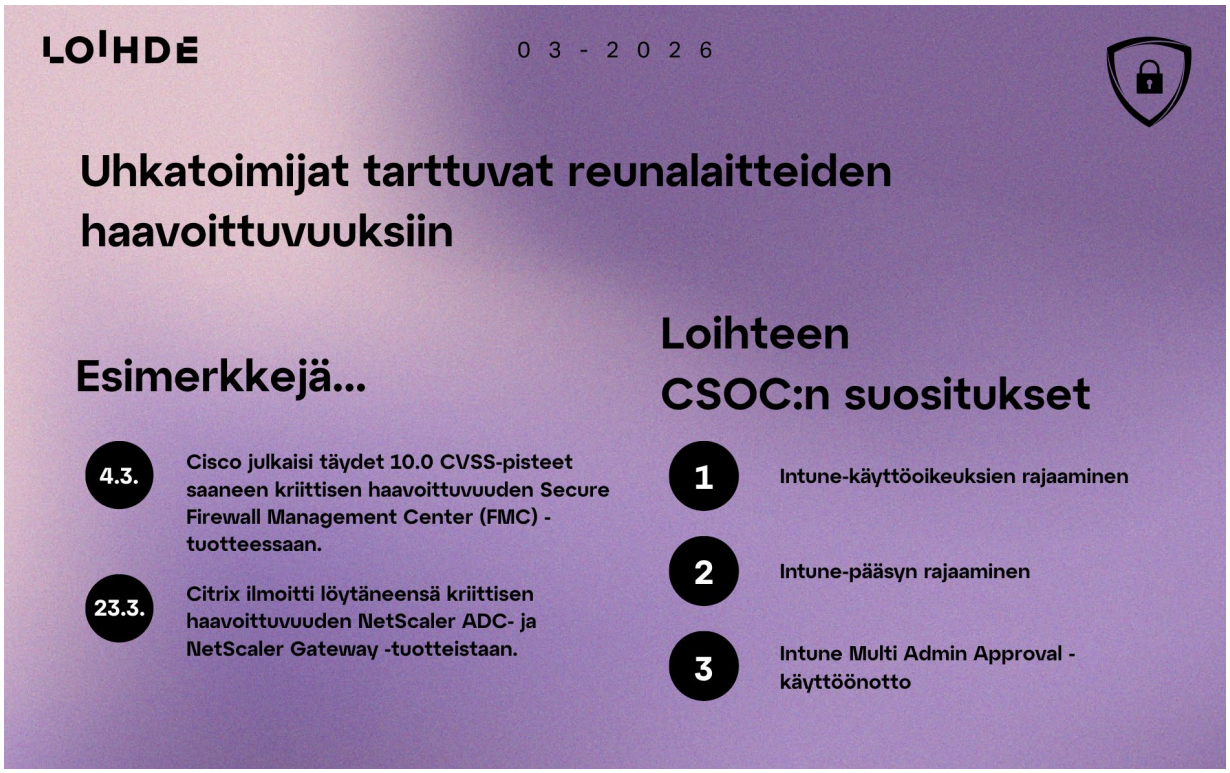
Uhkatoimijat ovat alkaneet käyttää kalasteluviesteissään OAuth-protokollan toimintaa hyväkseen. Muokkaamalla OAuth-kirjautumislinkkiä uhkatoimijat onnistuvat käyttämään mm. Microsoftin omaa domainia hyökkäyksissä. Microsoftin johtamassa operaatiossa Tycoon 2FA -kalastelupalvelu on saatu ainakin osittain ajettua alas.

Pimeässä verkossa on avautunut uusi Leak Bazaar -palvelu, joka koittaa tehdä kiristyshaittatoimijoiden elämästä helpompaa prosessoimalla uhreilta kaapattua dataa. LeakNet-kiristyshaittatoimijan uudessa kampanjassa käytetään hieman poikkeuksellista Deno-työkalua. Mahdollisesti tarkoituksena on tehdä päätelaitesuojauksella toimien havainnoinnista hankalampaa.

Yhdysvaltojen oikeusministeriö ilmoitti ajaneensa alas neljän suuren bottiverkon hallintainfrastruktuurin. Bottiverkoissa oli yli 3 miljoonaa saastunutta laitetta, joilla on tehty pahimmillaan yli 30 Tbps:n kokoisia palvelunestohyökkäyksiä.

Yhdysvaltojen ja Iranin sota on eskaloitunut myös kyberpuolelle. Handala-haittatoimija on käyttänyt Intunea hyväkseen tyhjentämään ainakin yhden suuren organisaation laitteet.

Kyberkatsauksessa on lisäksi mukana Loihteen CSOC:n maaliskuun suositus Intunen tietoturvaan.



KUUKAUSIRAPORTTI 03/2026

Tämä raportti sisältää kuvauksen maaliskuun 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 03/2026 2
1. Haavoittuvuudet 3
1.1 CVE-2026-3055: Citrix NetScaler - Insufficient input validation leading to memory overread 3
1.2 CVE-2026-20131: Cisco Secure Firewall Management Center RCE 3
1.3 Axios NPM -paketin toimitusketjuhyökkäys 4
2. Kalastelu ja huijaukset 5
2.1 OAuth-sovelluksen uudelleenohjaus 5
2.2 Tycoon 2FA -kalastelutyökalun alasajo 5
3. Kiristyshaittaohjelmat ja -toimijat 6
3.1 LeakNet ja Deno 6
3.2 Uusi kiristyspalvelu Leak Bazaar 6
4. Muuta 7
4.1 IoT-bottiverkkojen hallintainfrastruktuurin alasajo 7
4.2 Handala-haittatoimijan Intune-hyökkäykset 7
5. Suositukset 8

1. Haavoittuvuudet

1.1 CVE-2026-3055: Citrix NetScaler - Insufficient input validation leading to memory overread

Citrix ilmoitti 23.3. löytäneensä kriittisen haavoittuvuuden NetScaler ADC- ja NetScaler Gateway -tuotteistaan. Haavoittuvuuden hyväksikäyttö vaatii, että NetScaler on konfiguroitu SAML Identity Provideriksi. Haavoittuvuus löydettiin Citrixin toimesta ja Citrix ei ole tietoinen, että haavoittuvuutta olisi käytetty hyväksi ennen sen julkaisua.[1]

Haavoittuvuus muistuttaa paljon ”CitrixBleed”- ja ”CitrixBleed2”-nimellä tunnettuja haavoittuvuuksia, jotka myös sallivat NetScalereiden muistin lukemisen ja sitä kautta mm. kirjautumissessioiden kaappaamisen[2]. NetScalerit ovat verkon reunalaitteita ja haittatoimijoiden suosiossa, joten suosittelemme päivittämään haavoittuvaiset NetScalerit mahdollisimman pian.

1.2 CVE-2026-20131: Cisco Secure Firewall Management Center RCE

Maaliskuun 4. päivä Cisco julkaisi täydet 10.0 CVSS-pisteet saaneen kriittisen haavoittuvuuden Secure Firewall Management Center (FMC) -tuotteessaan. Haavoittuvuus mahdollistaa autentikoimattomalle hyökkääjälle mielivaltaisen koodin suorittamisen laitteella root-oikeuksin.[3]

Amazonin Threat Intelligence -tiimi on kertonut havainneensa viitteitä haavoittuvuuden CVE-2026-20131 potentiaalisesta hyväksikäytöstä jo tammikuun lopulta Interlock-kiristyshaittaohjelmatoimijan toimesta. Ryhmällä on siis ollut tuolloin hallussaan nollapäivähaavoittuvuus. Kampanjan tutkinnan yhteydessä Amazon löysi Interlockin käyttämän ja huonosti suojatun palvelimen, joka mahdollisti tutkijoille hyvän näkymän ryhmittymän käyttämiin työkaluihin ja haittaohjelmiin.[4]

Hyväksikäyttö vaatii hyökkääjän pääsyn FMC:n hallintarajapintaan, joten hyökkäyspinta-alan vähentämiseksi yhteys siihen tulisi olla rajattu vain luotettuihin lähteisiin koko internetin sijaan. Korjaavat päivitykset on syytä asentaa välittömästi.[3]

---

[1] Citrix, 23.3.2026, NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-3055 and CVE-2026-4368, https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300
[2] Kevin Beaumont, 24.6.2025, CitrixBleed 2: Electric Boogaloo — CVE-2025–5777, https://doublepulsar.com/citrixbleed-2-electric-boogaloo-cve-2025-5777-c7f5e349d206
[3] Cisco, 4.3.2026, Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
[4] AWS Security Blog, 18.3.2026, Amazon threat intelligence teams identify Interlock ransomware campaign targeting enterprise firewalls, https://aws.amazon.com/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/

1.3 Axios NPM -paketin toimitusketjuhyökkäys

Maaliskuun lopulla havaittiin sofistikoitunut toimitusketjuhyökkäys, joka kohdistui hyvin laajalti käytettyyn Axios JavaScript -kirjastoon. Axios on HTTP client -kirjastoista kaikkein suosituin ja sen NPM-paketilla on yli 100M viikoittaista latausta.[5] Pohjois-Koreaan liitetty uhkatoimija onnistui 31.3. julkaisemaan haittaohjelmalla saastutetun version Axios-paketista. Saastunut paketti on asennuttuaan suorittanut RAT-tyyppisen haittaohjelman, joka välittömästi ottaa yhteyttä komentopalvelimeen.[6]

Haitallinen versio kirjastosta poistettiin jakelusta noin kolmessa tunnissa, mutta kirjaston laajan käytön vuoksi vaikutus on merkittävä. Laitteet, joista löytyy viitteitä hyökkääjän lisäämään plain-crypto-js-moduuliin, on syytä käsitellä vaarantuneina ja kaikki järjestelmässä olleet tunnukset, avaimet ja salaisuudet on syytä vaihtaa. Hyökkäyksen kautta varastetut salaisuudet ja tunnukset mahdollistavat uusia hyökkäyksiä ja lisäävät niiden riskiä etenkin lähitulevaisuudessa.[6]

[5] StepSecurity, 30.3.2026, axios Compromised on npm - Malicious Versions Drop Remote Access Trojan, https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious-versions-drop-remote-access-trojan
[6] Google Threat Intelligence Group, 1.4.2026, North Korea-Nexus Threat Actor Compromises Widely Used Axios NPM Package in Supply Chain Attack, https://cloud.google.com/blog/topics/threat-intelligence/north-korea-threat-actor-targets-axios-npm-package

2. Kalastelu ja huijaukset

2.1 OAuth-sovelluksen uudelleenohjaus

Microsoft varoittaa uudenlaisesta kalastelukampanjasta, jossa käytetään hyväksi OAuth-protokollan uudelleenohjausominaisuutta. Microsoftin havaitsemassa kampanjassa haittatoimijat ovat ensin rekisteröineet uuden OAuth-sovelluksen omassa Azure/M365-ympäristössään ja konfiguroineet sille uudelleenohjausosoitteen. Haittatoimijan OAuth-sovelluksen kirjautumislinkkiä on sitten tarkoituksella muokattu palauttamaan virheen ja automaattisesti ohjaamaan käyttäjä aikaisemmin konfiguroituun uudelleenohjausosoitteeseen. Tätä muokattua kirjautumislinkkiä on sitten käytetty kalasteluviesteissä. Koska OAuth-kirjautumislinkki käyttää Microsoftin omaa login.microsoftonline.com-domainia, menee se todennäköisesti helposti läpi sähköpostisuodattimista ja loppukäyttäjät saattavat herkemmin uskoa linkin olevan aito. Klikkauksen jälkeen käyttäjä ohjautuu suoraan haittatoimijan sivustolle, jossa on tarjottu haittaohjelmaa ladattavaksi. Samaa mekanismia voidaan hyödyntää myös tunnustenkalasteluun uudelleenohjaamalla käyttäjä väärennetylle M365-kirjautumissivustolle.[7]

2.2 Tycoon 2FA -kalastelutyökalun alasajo

Microsoft, Europol[8] ja muut tahot raportoivat ottaneensa haltuunsa 330 domainia, jotka kuuluvat Tycoon 2FA -kalastelutyökalulle, aiheuttaen ainakin jonkinlaisen katkoksen sen toimintaan. Tycoon 2FA on ollut aktiivisessa käytössä ainakin vuodesta 2023 alkaen, ja sitä on myyty SaaS-palvelun kaltaisena pakkauksena haittatoimijoille. Tycoon 2FA:n avulla haittatoimijat ovat saaneet rahaa vastaan yhden portaalin, josta ovat voineet tehdä kaiken kalasteluun liittyen. Microsoftin mukaan pahimmillaan 62 % kaikista sen estämistä kalasteluviesteistä on ollut Tycoon 2FA:n kautta lähetettyjä, mikä kertoo palvelun saavuttamasta suosiosta haittatoimijoiden keskuudessa.[9]

[7] Microsoft, 2.3.2026, OAuth redirection abuse enables phishing and malware delivery, https://www.microsoft.com/en-us/security/blog/2026/03/02/oauth-redirection-abuse-enables-phishing-malware-delivery/
[8] Europol, 4.3.2026, Global phishing-as-a-service platform taken down in coordinated public-private action, https://www.europol.europa.eu/media-press/newsroom/news/global-phishing-service-platform-taken-down-in-coordinated-public-private-action
[9] Microsoft, 4.3.2026, Defending the gates: How a global coalition disrupted Tycoon 2FA, a major driver of initial access and large-scale online impersonation, https://blogs.microsoft.com/on-the-issues/2026/03/04/how-a-global-coalition-disrupted-tycoon/

3. Kiristyshaittaohjelmat ja -toimijat

3.1 LeakNet ja Deno

ReliaQuest kirjoittaa LeakNet-kiristyshaittatoimijasta ja heidän uudesta Deno-pohjaisesta haittaohjelmasta. LeakNet käyttää yleensä ClickFix-tyyppisiä taktiikoita saadakseen käyttäjän ajamaan komennon laitteellansa. ClickFixin kautta laitteella ajetaan hieman harvinaisempi Deno-pohjainen haittaohjelma. Deno on node.js:n kaltainen JavaScript-ohjelmistokehys, joka on suosittu kehittäjien keskuudessa, eikä ole itsessään millään tapaa haitallinen. On mahdotonta sanoa, onko Deno valittu mahdollisesti hankalamman AV/EDR-havainnoinnin vuoksi vai onko se vain ollut haittaohjelman kehittäjälle mieluinen ohjelmistokieli. LeakNet jatkaa yleensä hyökkäystä liikkumalla lateraalisesti verkossa PsExec:llä. Lopuksi verkosta löydetty data pusketaan AWS S3 -ämpäreihin.[10]

3.2 Uusi kiristyspalvelu Leak Bazaar

Pimeän verkon foorumeilla on maaliskuussa alkanut liikkumaan mainoksia uudesta kyberrikollisille tarkoitetusta palvelusta nimeltään Leak Bazaar. Palvelun ideana on prosessoida kiristyshyökkäyksissä varastettua suurta määrää dataa ja auttaa uhkatoimijoita löytämään datasta esim. arkaluontoiset ja kiristystarkoituksessa hyödyllisen tiedon. Leak Bazaarin tarkoituksena ei ole olla alusta datan vuotamiselle, vaan enemminkin uusi prosessointikerros tuolle datalle jalostaen siitä jäsenneltyä ja haettavissa olevaa.[11]

[10] ReliaQuest, 17.3.2026, Casting a Wider Net: ClickFix, Deno, and LeakNet's Scaling Threat, https://reliaquest.com/blog/threat-spotlight-casting-a-wider-net-clickfix-deno-and-leaknets-scaling-threat
[11] Flare, 25.3.2026, Leak Bazaar: Inside the New Criminal Platform Turning Stolen Data Into a Structured Marketplace, https://flare.io/learn/resources/blog/leak-bazaar-inside-new-criminal-platform

4. Muuta

4.1 IoT-bottiverkkojen hallintainfrastruktuurin alasajo

Yhdysvaltojen oikeusministeriö on yhteistyössä FBI:n kanssa onnistunut ajamaan alas neljän suuren IoT-bottiverkon hallintainfrastruktuurin. Toimet kohdistuivat Aisuru-, KimWolf-, JackSkid- ja Mossad-bottiverkkoihin. Bottiverkoissa oli yli 3 miljoonaa laitetta, pääasiassa erilaisia IoT-laitteita sekä muita verkon reunalaitteita. Bottiverkkoja on käytetty mm. palvelunestohyökkäyksiin, joiden koko on ollut pahimmillaan yli 30 Tbps.[12]

4.2 Handala-haittatoimijan Intune-hyökkäykset

Iranin ja Yhdysvaltojen sota on näkynyt kyberpuolella ainakin Handala-haittatoimijan hyökkäyksissä. Hyökkäyksistä tekee poikkeuksellisen niissä käytetyt työkalut. Handala ei yrittänyt ajaa kiristyshaittaohjelmaa tai mitään haittaohjelmaa laitteille, vaan käytti laitteiden nollaukseen Intunen natiiveja työkaluja. Hyökkäyksiä on kohdistunut ainakin yhdysvaltalaiseen Stryker-yritykseen.[13] Hyökkäyksiä on kohdistunut myös ainakin israelilaisiin yrityksiin, mutta näissä käytetyistä työkaluista tai haittaohjelmista ei ole vielä tarkempaa tietoa.[14]

Microsoft on julkaissut hyökkäyksen jälkeen ohjeistuksia Intunen koventamiseen. Microsoft ohjeistaa mm. minimoimaan Intune-ylläpitotunnusten määrää, rajaamaan pääsyä Intune-hallintaportaaliin Conditional Accessilla sekä aktivoimaan ”Multi Admin Approval” -ominaisuuden kriittisille asetuksille.[15]

[12] U.S. Attorney's Office, District of Alaska, 19.3.2026, Authorities disrupt world’s largest IoT DDoS botnets responsible for record breaking attacks targeting victims worldwide, https://www.justice.gov/usao-ak/pr/authorities-disrupt-worlds-largest-iot-ddos-botnets-responsible-record-breaking-attacks
[13] Stryker, 11.3.2026, Customer Updates: Stryker Network Disruption, https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html
[14] Unit42, 12.3.2026, Insights: Increased Risk of Wiper Attacks, https://unit42.paloaltonetworks.com/handala-hack-wiper-attacks/
[15] Microsoft, 14.3.2026, Best practices for securing Microsoft Intune, https://techcommunity.microsoft.com/blog/intunecustomersuccess/best-practices-for-securing-microsoft-intune/4502117

5. Suositukset

1. Intune-käyttöoikeuksien rajaaminen
2. Intune-pääsyn rajaaminen
3. Intune Multi Admin Approval -käyttöönotto

Handalan tekemien Intune-hyökkäysten vuoksi suosittelemme tässä kuussa tarkistamaan Intunen asetukset ja tarvittaessa koventamaan niitä. Vaikka ohjeistukset ovat Intunelle, niitä voi osittain myös soveltaa muille vastaaville tuotteille.

Microsoft julkaisi tässä kuussa listan kolmesta tavasta, jolla Intunen tietoturvaa voi parantaa. Suositukset jakautuvat kolmeen eri kategoriaan: 1) käyttäjien oikeuksien rajaaminen, 2) käyttäjien pääsyn rajaaminen ja 3) Multi Admin Approval -ominaisuuden käyttöönotto kriittisille asetuksille.

> ***Anna admin-oikeuksia vain niille, jotka oikeasti niitä tarvitsevat.***

Mieti kuka tarvitsee pääsyn Intuneen ja mitä toimia heidän tarvitsee pystyä tekemään. Anna admin-oikeuksia vain niille, jotka oikeasti niitä tarvitsevat. Useat toimet onnistuvat myös alemman tason oikeuksilla. Jos ylläpitäjän ei tarvitse hallinnoida kuin tiettyjä laitteita, voi oikeuksia rajata myös scope-tageilla. Varsinkin kaikki admin-roolit kannattaa laittaa PIM:n taakse, jolloin niiden aktivointiin voidaan vaatia esimerkiksi vahvempi MFA.

Mistä ja miltä laitteilta ylläpitäjien tarvitsee päästä Intuneen käsiksi? Conditional Accessilla voidaan vaatia Intune-pääsyyn (ja muihin admin-portaaleihin) esimerkiksi fyysinen FIDO2-avain, luotettu laite tai tietty julkinen IP kirjautumiselle. Optimaalisessa tilanteessa kaikki ylläpitotoimet tapahtuvat erilliseltä työasemalta, joka on dedikoitu vain ja ainoastaan ylläpitotoimiin (Privilege Admin Workstation).

Intunessa on myös mahdollista vaatia useamman ylläpitäjän hyväksyntä kriittisille muutoksille Multi Admin Approvalin avulla. Ominaisuuden käyttöönotto vaatii mietintää jokaiselta organisaatiolta ja tarkoituksena on löytää sopiva kompromissi käytettävyyden ja turvallisuuden välillä. Mietittäviä asioita ovat esimerkiksi, mitkä toimet vaativat useamman henkilön hyväksyntää, ketkä nämä hyväksynnät tekevät ja miten hätämuutokset hoidetaan.

Listatuilla kovennuksilla on mahdollista myös lukita itsensä täysin pois Intunesta. Tätä varten on suositeltavaa olla yksi tai useampi ”breakglass”-tunnus, jotka eivät ole kovennusten

piirissä. Tunnuksille on suositeltavaa laittaa vahva MFA, esimerkiksi fyysinen FIDO2-avain, ja tunnuksen käytöstä pitäisi aina tulla hälytys.

Nämä kovennukset eivät kuitenkaan tee Intunen vaarantamisesta mahdotonta. Ideana on tehdä siitä mahdollisimman vaikeaa ja aikaa vievää, jolloin mahdolliset hyökkäysyritykset voidaan todennäköisemmin huomata ja estää.

Microsoftin ohjeistukset voit lukea kokonaisuudessaan Microsoftin blogista https://techcommunity.microsoft.com/blog/intunecustomersuccess/best-practices-for-securing-microsoft-intune/4502117

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