Kyberkatsaus

05/2026

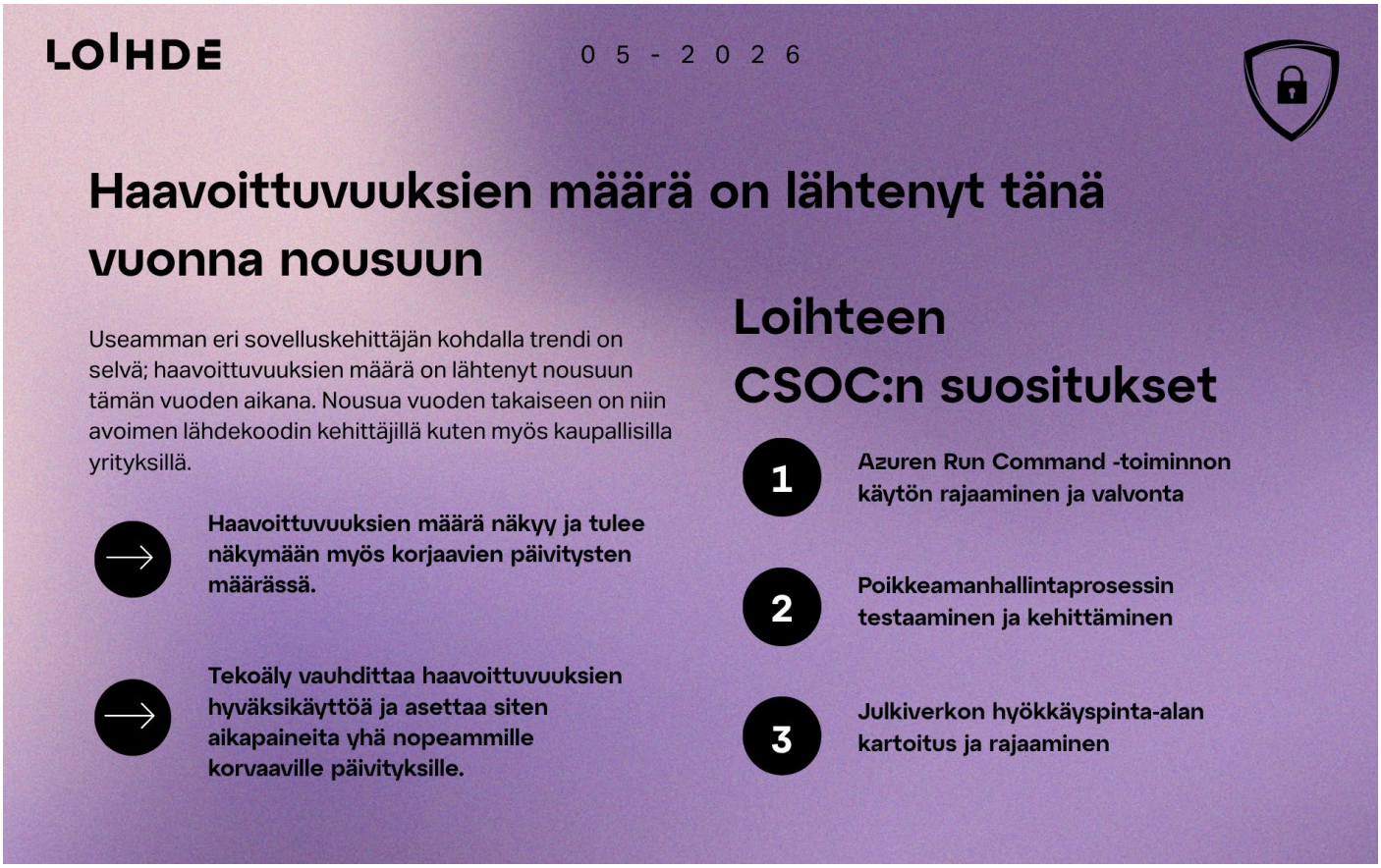
LOIHDE

Tiivistelmä

Toukokuun kyberkatsauksessa on nostettu esille kiinnostavia poimintoja ajankohtaisista tapahtumista kyberkentällä:

- TeamPCP-uhkatoimija julkaisi 12.5.2026 kehittämänsä Shai-Hulud-haittaohjelman lähdekoodin julkisesti.
- Palo Alto Networksin PAN OS -käyttöjärjestelmässä on toukokuussa todettu tietoturvahaavoittuvuus, joka on jo kohdannut aktiivista hyväksikäyttöä.
- Microsoft raportoi Storm-2949-uhkatoimijan Azureen ja M365:een suorittamasta tietoturvahyökkäyksestä, jossa yhden käyttäjätunnuksen vaarantuminen eskaloitui laajamittaiseen tietoturvapoikkeamaan.
- VulnCheck-palvelu on havainnut merkittävää nousua AI-avusteisten tietoturvahaavoittuvuuksien löytymisessä vuonna 2026.

Kyberkatsauksen toukokuun suositukset liittyvät Azuren Run Command -ominaisuuteen, poikkeamanhallintaprosessiin ja julkiverkon hyökkäyspinta-alan kartoittamiseen.



KUUKAUSIRAPORTTI 05/2026

Tämä raportti sisältää poimintoja toukokuun 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 05/2026 2
1. Poiminnat 3
1.1 CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass 3
1.2 Shai-Hulud-madon lähdekoodi julkaistu 3
1.3 Storm-2949 Cloud Compromise 3
1.4 AI:n vaikutus löydettyjen haavoittuvuuksien määrään 4
2. Suositukset 5

1. Poiminnat

1.1 CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass

Palo Alto Networks on korjannut tietoturvahaavoittuvuuden, joka vaikuttaa PAN-OS-käyttöjärjestelmään. Haavoittuvuutta hyväksikäyttämällä on mahdollista ohittaa VPN-autentikointi ja muodostaa VPN-yhteys palomuurille. Haavoittuvuus vaikuttaa Global Protect- tai Gateways-toimintoja käyttäviin palomuureihin, joihin on tehty tietyt konfiguraatiot. Haavoittuvuus ei valmistajan mukaan vaikuta Panorama-alustaan eikä pilvipohjaiseen Cloud NGFW:hen.[1]

Haavoittuvuus on jo kohdannut aktiivista hyväksikäyttöä ja valmistaja suosittelee korjaavien päivitysten asentamista ja mitigointitoimenpiteitä haavoittuvuuden paikkaamiseksi.[2]

1.2 Shai-Hulud-madon lähdekoodi julkaistu

TeamPCP-haittatoimija julkaisi 12.5. kehittämänsä Shai-Hulud-madon lähdekoodin julkisesti. TeamPCP on käyttänyt matoa useammassa eri toimitusketjuhyökkäyksessä, mm. Checkmarkx- ja LiteLLM-hyökkäyksissä. DataDog on tutkinut julkaistua lähdekoodia ja verrannut sitä aikaisemmissa toimitusketjuhyökkäyksissä käytettyihin matoihin. Lähdekoodi vastaa pitkälti aikaisemmin käytettyjä matoja, joten kyseessä on todennäköisesti sama mato kuin mitä TeamPCP on käyttänyt.[3]

On epäselvää, miksi TeamPCP päätti julkaista lähdekoodin julkisesti. Ehkä tarkoituksena on ”katsoa kun maailma palaa” tai sitten he koittavat julkaisulla tehdä hankalammaksi päätellä, onko TeamPCP tulevien toimitusketjuhyökkäysten takana. Olipa syy mikä tahansa, julkaisu tulee varmasti lisäämään toimitusketjuhyökkäysten määrää, koska lähdekoodin avulla myös vähemmän kyvykkäät toimijat kykenevät tekemään vastaavia hyökkäyksiä.

1.3 Storm-2949 Cloud Compromise

Microsoftin Threat Intelligence -tiimi raportoi Storm-2949-uhkatoimijan suorittamasta laajamittaisesta tietoturvahyökkäyksestä asiakkaan Azure- ja M365-ympäristöihin.

Toimija on epäillysti saanut jalansijan ympäristöön hyväksikäyttämällä Self-Service Password Reset -toimintoa käynnistämällä salasanan nollausprosessin ja houkuttelemalla käyttäjää hyväksymään tästä syntyvän MFA-pyynnön, esimerkiksi esiintymällä IT-osaston työntekijänä.

[1] Palo Alto Networks, 13-5-2026, CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities https://security.paloaltonetworks.com/CVE-2026-0257
[2] Rapid7, 29.5.2026, Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability (CVE-2026-0257), https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/
[3] DataDog, 13.5.2026, Shai-Hulud Goes Open Source, https://securitylabs.datadoghq.com/articles/shai-hulud-open-source-framework-static-analysis/

Tämä on mahdollistanut hyökkääjälle oikeudet poistaa olemassa olevat MFA-metodit kokonaan ja lisätä tilalle omansa. Hyökkääjä sai kaapattua kolme tiliä lisää samalla keinolla. Pääsyn saatuaan hyökkääjä varasti ison määrän dataa käyttäjien OneDrive- ja SharePoint-hakemistoista, mukaan lukien organisaation VPN-konfiguraatioita.

Osalla käyttäjistä oli myös pääsyjä Azure Subscriptioneihin ja hyökkääjä varasti dataa ja salaisuuksia mm. Azure App Service- ja Key Vault -palveluista. Hyökkääjän onnistui myös muokata Azuren palomuurisääntöjä ja kirjautua SQL-palvelimelle Key Vault:sta saamillaan tunnuksilla. Lopuksi hyökkääjä sai pääsyn Azuren virtuaalikoneille ajamalla Run Command -toiminnon kautta PowerShell-skriptin, joka poistaa Defenderin käytöstä ja joka asentaa ScreenConnect RMM:n laitteelle. Toimija yhdisti virtuaalikoneille ScreenConnect:lla ja suoritti tiedonkeruukomentoja useilla eri laitteilla ja varasti mm. sertifikaatteja.[4]

Tapaus on hyvä esimerkki siitä, että organisaatioiden tulisi käyttää FIDO2-pohjaista MFA:ta sekä vaatia luotettu laite pilvipalveluihin kirjautumiseen. Tämä voidaan toteuttaa Conditional Access Policyillä. Azuren käyttöoikeudet tulisi rajata minimiin, resursseja tulisi valvoa poikkeavien muutosten varalta sekä konfiguraatiomuutosten tekemistä pitäisi rajoittaa esimerkiksi Azure Policyllä. Run Command -toiminnon käyttöä tulisi valvoa, koska se mahdollistaa skriptien suorittamisen laitteella Azure-portaalin kautta. Ajetut skriptit suoritetaan paikallisella laitteella SYSTEM-käyttäjänä sekä Linuxin tapauksessa root-käyttäjänä.

1.4 AI:n vaikutus löydettyjen haavoittuvuuksien määrään

VulnCheck on kerännyt dataa useiden eri sovelluskehittäjien raportoimista CVE-numeroista, eli käytännössä löydetyistä haavoittuvuuksista. Useamman eri sovelluskehittäjän kohdalla trendi on selvä; haavoittuvuuksien määrä on lähtenyt nousuun tämän vuoden aikana. Nousua vuoden takaiseen on niin avoimen lähdekoodin kehittäjillä, esim. Chrome +563 %, Apache +170 % ja Mozilla +157 %, kuten myös kaupallisilla yrityksillä, esim. VMware +181 % ja F5 +114 %. Nousua selittää ainakin osittain Anthropicin Project Glasswing, jonka kautta Anthropic on jakanut pääsyä haavoittuvuuksia hyvin löytävään Mythos-kielimalliin.[5]

> ***Tekoäly vauhdittaa haavoittuvuuksien hyväksikäyttöä ja asettaa siten aikapaineita yhä nopeammille korvaaville päivityksille.***

Aika tulee näyttämään, kauanko piikki haavoittuvuuksien määrässä tulee kestämään. Haavoittuvuuksien määrä näkyy ja tulee näkymään myös korjaavien päivitysten määrässä. Haittatoimijat kykenevät myös kehittämään tekoälyn avulla nopeammin hyväksikäyttökoodia haavoittuvuuksille, mikä tekee päivitysten asennuksesta yhä kiireellisempää. Varsinkin verkon reunalaitteiden osalta organisaatioiden tulisi miettiä, kuinka päivitykset saadaan asennettua mahdollisimman

[4] Microsoft, 18.5.2026, How Storm-2949 turned a compromised identity into a cloud-wide breach, https://www.microsoft.com/en-us/security/blog/2026/05/18/storm-2949-turned-compromised-identity-into-cloud-wide-breach/
[5] Patrick Garrity, 14.5.2026, The First CVE Wave: Signs That AI-Assisted Vulnerability Discovery Is Reshaping Disclosure Volumes, https://www.vulncheck.com/blog/ai-assisted-vulnerability-discovery

nopeasti. Mahdollisuuksien mukaan ympäristöä kannattaa myös koventaa, jos julkiverkossa on palvelu, jonka ei siellä välttämättä tarvitsisi olla. Tällainen palvelu kannattaakin poistaa julkiverkosta. Haavoittuvuuksien julkaisussa ei valitettavasti oteta huomioon kesälomakautta, joten valmius asentaa päivityksiä nopealla aikataululla täytyy olla kunnossa kesälläkin.

2. Suositukset

1. Azuren Run Command -toiminnon käytön rajaaminen ja valvonta
2. Poikkeamanhallintaprosessin testaaminen ja kehittäminen
3. Julkiverkon hyökkäyspinta-alan kartoitus ja rajaaminen

Run Command-ominaisuus mahdollistaa skriptien suorittamisen Azure-portaalista Windows- ja Linux-virtuaalikoneilla sekä Arc:iin liitetyillä on-prem-koneilla.[6] Ominaisuus on hyödyllinen ylläpitotoimiin, mutta se muodostaa samalla merkittävän tietoturvauhan. Kuka tahansa riittävillä RBAC-oikeuksilla varustettu käyttäjä voi ajaa komentoja laitteille Azuren kautta. On-premises-laitteiden kohdalla ominaisuuden avulla uhkatoimijan on mahdollista pivotoida ja muodostaa jalansijamekanismeja paikalliseen ympäristöön Azuren kautta. Toimija voi esimerkiksi luoda uuden admin-tunnuksen tai asentaa RMM-työkalun, kuten aiemmin mainitussa Microsoftin artikkelissa oli tehty. Run Commandin käyttöä on syytä valvoa ja suoritusoikeuksia rajata (esimerkiksi vain ennalta sallittuihin komentoihin).[7]

Poikkeamanhallintaprosessia on syytä harjoitella ja kehittää säännöllisin väliajoin. Harjoittelun kautta voidaan todentaa suunnitelman toimivuutta ja tarkistaa esimerkiksi, onko suunnitelman eri vaiheisiin tarvetta tehdä päivityksiä ja parannuksia. Mikäli harjoittelua on jo tehty, voidaan sen painopistettä siirtää ja testata esimerkiksi vain osaan suunnitelmasta. On myös hyvä muistaa, että suunnitelmaa päästään toteuttamaan tositilanteessa harvoin samoilla, suunnitelluilla resursseilla ja yhtä rauhallisissa olosuhteissa kuin alun perin on ajateltu. Tämän vuoksi voikin olla hyvä harjoitella suunnitelmaa esimerkiksi siten, että osa henkilöstöstä puuttuu tai jokin tärkeä resurssi ei ole käytössä. Tällöin voidaan testata suunnitelman kestävyyttä myös poikkeavassa harjoitustilanteessa.

Suosittelemme organisaatioita kartoittamaan ja rajaamaan julkiverkon hyökkäyspinta-alaansa. Uhkatoimijat kartoittavat potentiaalisia kohteita jatkuvasti esimerkiksi haavoittuvuusskannereilla ja julkisesti saatavilla olevilla palveluilla. Organisaatioiden tulisi löytää puutteet ennen uhkatoimijoita, korjata ne sekä lisätä ASM (Attack Surface

[6] https://learn.microsoft.com/en-us/azure/virtual-machines/run-command-overview
[7] https://hackingthe.cloud/azure/run-command-abuse/

Management) keskeiseksi osaksi toimintojaan. Sen avulla tarpeettoman hyökkäyspinta-alan muodostumista voidaan myös ennaltaehkäistä. Esimerkkejä vaarallisista kohteista voivat olla julkiverkkoon näkyvät erinäiset hallintapaneelit, VPN:t, pilvipalveluissa sijaitsevat storaget ja tietokannat.[8]

Ilmaisista ratkaisuista Shodan on erittäin pätevä ratkaisu organisaation julkiverkkoon näkyvän rajapinnan kartoittamiseen. Sinne voi suorittaa hakuja esimerkiksi organisaation julkiverkon IP-avaruudella tai domainin nimellä, ja se palauttaa osoitteissa hostattuja palveluita. Nämä voivat olla esimerkiksi avoimia portteja, banneritietoja ja ohjelmistoja sekä niiden versionumeroita ja haavoittuvuustietoja. Shodanin avulla voi löytää esimerkiksi jonkin pitkään päivittämättömänä olleen VPN gatewayn, josta kukaan organisaatiossa ei ole ollut tietoinen.

Esimerkkikyselyitä, joilla Shodanista voi hakea tietoa omasta organisaatiosta:
net:"x.x.x.x/24"
hostname:"organisaatio.com" [9]

[8] https://www.ncsc.gov.uk/guidance/external-attack-surface-management-buyers-guide
[9] https://www.shodan.io/

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