LOIHDE

KYBERKATSAUS

9.2024

KUUKAUSIRAPORTTI 9/2024

Tämä raportti sisältää kuvauksen syyskuun 2024 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

1. Yleistilanne

Yleistilanne on pysynyt syyskuussa samalla tasolla verrattuna edellisiin kuukausiin. Kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa ja niiden vähenemisestä ei ole merkkejä. Suomalaisille yrityksille ja organisaatioille keskeisin uhka 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 kehitystyötä.

Kevään ja kesän aikana on uutisoitu erilaisista tapahtumista, jotka ovat joko suoraan tai välillisesti liittyneet Venäjän ja lännen vastakkainasetteluun. Suomen osalta keskeisimpänä ovat näkyneet esimerkiksi rajaloukkaukset merellä ja ilmassa sekä Venäjällä tapahtuva vihamielinen uutisointi Suomeen liittyen. Samoja ilmiöitä on ollut havaittavissa myös kyber- ja informaatiotilassa esimerkiksi palvelunestohyökkäysten ja informaatiovaikuttamisen muodossa. Tämä vastakkaisasettelu onkin syytä ottaa huomioon toiminnassa ja riskiarvioissa.

Suomalaisten toimijoiden on hyvä huomioida toiminnassaan, että 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.

2. Haavoittuvuudet

2.1 CVE-2024-40766 - SonicOS Improper Access Control Vulnerability

SonicWall SSLVPN -komponentissa oleva haavoittuvuus sallii hyökkääjälle koodin ajamisen palomuurilla ja VPN-tunnusten kaappaamisen. Alun perin haavoittuvuus koski vain palomuurin hallintaporttia, mutta myöhemmin SonicWall ilmoitti haavoittuvuuden koskevan myös SSLVPN-komponenttia.[1]

Haavoittuvuutta on myös mahdollisesti alettu käyttämään Akira-kiristyshaittaohjelmahyökkäyksissä. Epäillyissä tapauksissa kaapatut VPN-tunnukset ovat olleet paikallisia eikä niille ole ollut pakotettu MFA:n käyttöä.[2]

Haavoittuvuus on hyvä esimerkki SSLVPN-haavoittuvuuksien kriittisyydestä. Haavoittuvuudet tulisi korjata välittömästi haavoittuvuuden tullessa ilmi, koska haittatoimijat aloittavat haavoittuvuuden hyväksikäytön yleensä pian julkaisun jälkeen.

2.2 Veeam Backup & Replication unauth RCE CVE-2024-40711

Tieto kriittisestä haavoittuvuudesta (CVSS 9.9) Veeam Backup & Replication -ohjelmistossa julkaistiin 4.9.2024. Veeam on datan varmuuskopiointiin käytetty kaupallinen tuote, joka on käytössä laajalti eri organisaatioissa.[3]

Haavoittuvuus mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen haavoittuvalla Veeam-palvelimella ilman autentikoitumista. Haavoittuvuus koskee tuotteen versiota 12.1.2.172 sekä sitä vanhempia versioita. Veeamin aiemmat vastaavat haavoittuvuudet ovat olleet mm. kiristyshaittaohjelmatoimijoiden, kuten Akiran, aktiivisessa käytössä, joten on syytä olettaa tämänkin päätyvän heidän työkalupakkiin. Varmuuskopiot ovat luonnollisesti hyvin haluttu kohde uhkatoimijoille. Lisäksi pääsy palvelimelle mahdollistaa sivuttaisliikehdinnän kohdeverkossa.[4]

[1] SonicWall, 22.8.2024, SonicOS Improper Access Control Vulnerability, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
[2] Arctic Wolf, 6.9.2024, Arctic Wolf Observes Akira Ransomware Campaign Targeting SonicWall SSLVPN Accounts, https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/
[3] Veeam, 4.9.2024, Veeam Security Bulletin (September 2024), https://www.veeam.com/kb4649
[4] Watchtowr Labs, 9.9.2024, Veeam Backup & Response - RCE With Auth, But Mostly Without Auth (CVE-2024-40711), https://labs.watchtowr.com/veeam-backup-response-rce-with-auth-but-mostly-without-auth-cve-2024-40711-2/

Palvelimet suositellaan päivittämään tuoreimpaan versioon 12.2.0.334 pikimmiten. Syyskuun alussa internettiin avoinna olevia Veeam Backup & Replication -palvelimia oli Censysin kartoituksen mukaan 2833 kpl.[5] Haavoittuvuuteen julkaistiin esimerkkikoodi15.9.2024.[6]

2.3 GitLab Pipeline Execution CVE-2024-6678

Gitlab julkaisi 11.9.2024 päivityksen, joka korjaa kriittisen haavoittuvuuden Gitlab CE (Community Edition) ja EE (Enterprise Edition) -instansseissa. Haavoittuvat versiot ovat 8.14 - 17.1.6, 17.2 - 17.2.4, ja 17.3 - 17.3.1.[7]

Haavoittuvuus koskee Gitlabin pipelinea, jolla automatisoidaan tuotetun koodin testaamista ja käyttöönottoa osana CI/CD-ketjua. Hyväksikäyttö mahdollistaa hyökkääjän suorittavan pipelinen mielivaltaisella käyttäjällä tietyissä olosuhteissa. PoC-koodia tai tarkempaa kuvausta haavoittuvuudesta ei ole vielä julkisesti saatavilla, mutta haavoittuvuuden alhainen luokitus sen hyväksikäytön vaikeudesta nostaa haavoittuvuuden CVSS-pisteytystä.[8] [9]

3. Kalastelu ja huijaukset

Kalasteluviestit ja huijaukset ovat uhkia, jotka näkyvät yritysten ja yksilöiden arjessa. Näiden osalta tavoitteena on kohteesta riippumatta pääsääntöisesti taloudellisen hyödyn tavoittelu eri keinoin. Kuluttajiin liittyvät huijaukset pyrkivät yleensä saamaan kohteensa maksamaan tietyn summan tai luovuttamaan maksukorttinsa tiedot jollain verukkeella. Yrityspuolen kalastelussa pyritään usein saamaan käyttäjätili haltuun esimerkiksi ohjaamalla käyttäjä kirjautumaan hyökkääjän AitM-hyökkäyksen (Adversary in the Middle) avulla. Kalastelu on aktiivista ja sen vaikutukset ovat merkittävät. Esimerkiksi kuluttajapuolella vuonna 2024 on menetetty jopa 27,5 miljoonaa euroa rahallisiin huijauksiin liittyen.[10]

Yritysten tietoturvan ja talouden kannalta kalastelu on merkittävä uhka. Kalastelun kautta haltuun saadun tunnuksen avulla hyökkääjä pääsee käsiksi kohdeorganisaationsa tietoihin käyttäjätunnuksen omaamien oikeuksien puitteissa. Useissa tilanteissa tämä tarkoittaa käytännössä laajaa pääsyä erilaisiin arkaluonteisiin tietoihin. Esimerkiksi uhrin sähköposti,

[5] Censys, 6.9.2024, Unauthenticated RCE in Veeam Backup & Replication [CVE-2024-40711] , https://censys.com/cve-2024-40711/
[6] watchtowrlabs/CVE-2024-40711, 15.9.2024, Exploit for Veeam backup and Replication Pre-Auth Deserialization CVE-2024-40711, https://github.com/watchtowrlabs/CVE-2024-40711
[7] GitLab,11.9.2024, “GitLab Critical Patch Release: 17.3.2, 17.2.5, 17.1.7”, https://about.gitlab.com/releases/2024/09/11/patch-release-gitlab-17-3-2-released/
[8] Arctic Wolf, 12.9.2024, CVE-2024-6678: GitLab Fixes Critical Pipeline Execution Vulnerability https://arcticwolf.com/resources/blog/cve-2024-6678/
[9] Bleeping Computer, 12.9.2024, GitLab warns of critical pipeline execution vulnerability, https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-pipeline-execution-vulnerability/
[10] Yle, 17.9.2024, Suomalaisilta huijattu alkuvuodesta 27,5 miljoonaa euroa – tätä tahtia luku voi nousta sataan miljoonaan tänä vuonna, https://yle.fi/a/74-20112001

pilvipalvelut ja muut resurssit ovat vaarassa, mikäli kalastelu onnistuu. Viime kuun aikana Kyberturvallisuuskeskus kertoi DropBox-teemaisesta kalastelusta, jossa kohde houkuteltiin palvelun kautta kirjautumaan M365-palveluihin hyökkääjän varastaessa pääsyn tunnukselle.[11] Tämän kaltaiset kampanjat ovat yleisiä ja niiden suhteen on syytä olla valppaana. Kalasteluun liittyvät työkalut mahdollistavat erityisen vaikeasti tunnistettavien huijausten luomisen ja hyökkäysten skaalaamisen. Tähän liittyen on saatavilla useita työkaluja, jotka eivät vaadi laajaa osaamista onnistuneen kalastelukampanjan luomiseksi.[12]

Kalasteluun ja huijauksiin liittyen uutisoitiin syyskuussa myös huijaussoitoista, joiden määrä on kasvanut lähiaikoina. Puheluiden ja viestien tavoitteena on yleensä taloudellinen hyöty tai tiedon kerääminen.[13] Lisäksi kerrottiin huijauksista, joissa uhria lähestyttiin Traficomin nimissä viestillä. Viesteissä kehotetaan maksamaan linkin kautta löytyvä lasku, joka on menossa perintään. Kyseiseen huijaukseen liittyen on tullut paljon ilmoituksia Oulun poliisille.[14] Lisäksi uutisoitiin poliisin ottaneen kiinni henkilön laajaan nettihuijausjuttuun liittyen.[15]

[11] Kyberturvallisuuskeskus, 13.9.2024, Kyberturvallisuuskeskuksen viikkokatsaus - 37/2024, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-372024
[12] The Hacker News, 29.8.2024, How AitM Phishing Attacks Bypass MFA and EDR—and How to Fight Back, https://thehackernews.com/2024/08/how-to-stop-aitm-phishing-attack.html
[13] Yle, 24.9.2024, Ulkomailta tulee huijaussoittoja entistä enemmän, https://yle.fi/a/74-20113529
[14] Yle, 19.9.2024, Oulun poliisi on huolissaan huijauksista, joissa uhria on lähestetty Traficomin nimissä, https://yle.fi/a/74-20112385
[15] Yle, 6.9.2024, Poliisi otti kiinni liki sadasta nettipetoksesta epäillyn miehen – autojen varaosat eivät koskaan saapuneet, https://yle.fi/a/74-20109909

4. Venäjä ja sitä tukevat ryhmät

Venäjän ja länsimaiden välinen vastakkainasettelu jatkuu, eikä siihen liittyen ole havaittavissa lientymistä. Venäjä näkee länsimaat ja erityisesti NATO-jäsenet vastustajinaan. Länsimaat ovat pitäneet kiinni sanktioista ja pakotteista, joita Venäjää vastaan on asetettu Ukrainan sotaan liittyen. Suomen ja Venäjän välinen raja pysyy suljettuna.

Vastakkainasettelun myötä Venäjä käyttää länsimaita kohtaan erilaisia vaikuttamisen keinoja. Dis- ja misinformaation[16] lisäksi palvelunestohyökkäykset[17], välineellistetty maahantulo[18] ja esimerkiksi infrastruktuuriin vaikuttaminen[19] ovat keinoja, joita on havaittu käytettävän. Näitä toimia voivat toteuttaa niin Venäjän valtioon suoraan liittyvät tahot, kuten tiedustelupalveluiden alaiset toimijat[20] tai esimerkiksi valtiolle lojaalit rikolliset sekä haktivistit[21]. Kesän aikana Suomea kohtaan näistä on havaittu käytettävän ainakin toimia itärajalla, rajaloukkauksia,[22] sekä palvelunestohyökkäyksiä.[23]

Venäjän sisäisessä uutisoinnissa Suomea on käsitelty lähiaikoina huomattavan negatiiviseen sävyyn. Tämä on näkynyt esimerkiksi uutisoinnissa liittyen oikeudenkäyntiin, jossa käsitellään jatkosodan aikana Karjalassa tapahtuneita asioita. Venäjä nosti uudelleen esille Suomen toiminnan jatkosodan aikana ja Suomi tuomittiin kansanmurhasta tähän liittyen.[24] Suomi on myös listattu esimerkiksi maaksi, jossa Venäjän hallinnon näkökulmasta on vallalla haitallisia asenteita.[25] Lisäksi Suomen ja Venäjän rajan läheisyydessä on kerrottu partioivan äärioikeistolaisen Rusitš-palkkasotilasryhmän jäseniä. Tämän on kerrottu liittyvän

[16] Yle, 23.9.2024, Uusi tietovuoto paljasti Venäjän häikäilemättömän vaikutusoperaation, asiantuntijalta tyly huomio, https://yle.fi/a/74-20112682?origin=rss
[17] ENISA, 19.9.2024, ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[18] Rajavartiolaitos, lainattu 27.9.2024, Mitä välineellistetty maahantulo tarkoittaa?, https://raja.fi/usein-kysyttya-itarajan-esteaidasta#:~:text=Mit%C3%A4%20v%C3%A4lineellistetty%20maahantulo%20tarkoittaa%3F,tapauksessa%20hyv%C3%A4ksi%20Suomen%20poliittiseen%20painostukseen.
[19] Atlantic Council, 12.9.2024, Concerns grow over possible Russian sabotage of undersea cables, https://www.atlanticcouncil.org/blogs/ukrainealert/concerns-grow-over-possible-russian-sabotage-of-undersea-cables/
[20] CISA, 5.9.2024, Russian Military Cyber Actors Target US and Global Critical Infrastructure, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
[21] KelaCyber, 25.2.2024, Russia – Ukraine war: Pro-Russian hacktivist activity two years on, https://www.kelacyber.com/blog/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/#:~:text=DDoS%20activity%20of%205%20most,2024%20(in%20KELA's%20data%20lake)
[22] Yle, 10.6.2024, Venäläiskoneen epäillään loukanneen Suomen ilmatilaa Suomenlahdella, https://yle.fi/a/74-20093199
[23] Helsingin Sanomat, 20.7.2024, Venäjä-mielisistä kyber-hyökkäyksistä epäilty kolmikko otettiin kiinni – Ryhmä on kertonut iskeneensä myös Suomeen , https://www.hs.fi/maailma/art-2000010577171.html
[24] Tass, 1.8.2024, В Карелии признали преступления финских оккупантов геноцидом советского народа , https://tass.ru/proisshestviya/21504233
[25] Yle, 22.9.2024, Venäjä listasi ”tuhoisia asenteita” omaavia maita – joukossa myös Suomi, https://yle.fi/a/74-20113150

turvallisuuden lisäämiseen raja-alueella. Aiheesta on uutisoitu Suomessa[26] ja tähän liittyen ryhmä on myös julkaissut kuvia raja-alueelta[27]. Osa kuvista on paikannettu Saimaan kanavan alueelle ja muissa kuvissa esiintyvät samat henkilöt.

Venäjä käyttää monipuolisesti erilaisia keinoja heikentääkseen turvallisuuden tunnetta ja aiheuttaakseen polarisaatiota kohteissaan. Kyberturvallisuuteen liittyen on hyvä huomioida, että Venäjällä informaatiovaikuttaminen käsitetään toimenpiteidensä osalta laajempana ja se sisältää esimerkiksi hyökkäykselliset, puolustukselliset ja informaatiotilassa suoritettavat toimet.[28] Esimerkiksi Suomessa kyberturvallisuus ja informaatiovaikuttaminen ovat toisistaan erillisiä[29], mikä voi aiheuttaa haasteen puolustauduttaessa vaikuttamiselta.

5. Kiristyshaittaohjelmat ja -toimijat

Kiristyshyökkäykset ovat jatkuneet maailmalla aikaisempien kuukausien tavoin. Vaikka globaalisti hyökkäyksiä on julkisuuteen noussut syyskuun aikana tiuhaan tahtiin, ei Pohjoismaissa ole uutisoitu uusista hyökkäyksistä. Tähän vaikuttaa Suomen osalta varmasti sijainti ja koko sekä tunnettuus. On kuitenkin hyvä huomioida, että uhkatoimijoiden pääasiallinen motivaatio on taloudellinen hyöty ja sen suhteen uhrien sijainti ei ole karsiva tekijä.

Kyberturvallisuuskeskus julkaisi syyskuun lopussa tietoa kiristyshaittaohjelmatoimijoihin liittyen. Julkaisussa käsitellään kiristyshaittaohjelmia yleisesti sekä Akira- ja LockBit3.0-ryhmiä. Asiaa on käsitelty niin globaalista kuin kansallisesta näkökulmasta. Julkaisuun on koottu kattavasti tietoa ja aikaisempia julkaisuita aiheeseen liittyen.[30]

Syyskuun aikana nostettiin myös esille DragonForce-nimellä tunnettu kiristyshaittaohjelmatoimija. Tähän liittyen uutisoitiin siitä, että ryhmän on havaittu laajentavan RaaS-toimintaansa (Ransomware as a Service).[31] RaaS-toiminta tarkoittaa sitä, että ryhmä tarjoaa haittaohjelmaa muiden käyttöön maksua vastaan. Ryhmän työkaluihin liittyen on

[26] Yle, 13.9.2024, Suomella on Venäjällä alue, jossa nyt näyttää seisovan sotilasryhmä – haluavat pelotella, uskoo tutkija, https://yle.fi/a/74-20111102
[27] Rusitš -ryhmän Telegram kanava
[28] Juha Kukkola, 2024, Suvereenit hiekkamadot : Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla, https://urn.fi/URN:ISBN:978-951-25-3437-1
[29] Demokraatti, 6.9.2024, Janne Riiheläinen: Kuka ottaisi vastuun Suomen informaatiopuolustuksesta – ja alkaisi johtaa sitä?, https://demokraatti.fi/janne-riihelainen-kuka-ottaisi-vastuun-suomen-informaatiopuolustuksesta-ja-alkaisi-johtaa-sita
[30] Kyberturvallisuuskeskus, 27.9.2024, Akira ja Lockbit kiristyshaittaohjelmat valokeilassa, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa
[31] Hackread, 25.9.2024, DragonForce Ransomware Expands RaaS, Targets Firms Worldwide, https://hackread.com/dragonforce-ransomware-expands-raas-targets-firms/

havaittu sen käyttävän esimerkiksi LockBit-, Babuk- ja Conti-kiristyshaittaohjelmiin liittyviä variantteja. Ryhmän uhrit ovat keskittyneet Yhdysvaltoihin, Britanniaan ja Australiaan, mutta sillä on uhreja myös muista maista.[32] DragonForce on toiminut vuodesta 2023 alkaen ja sen toiminta on laajentunut nopeasti. Se on lisännyt ensimmäiset uhrit vuotosivustolleen joulukuussa 2023.[33]

Kiristyshaittaohjelmien osalta organisaatioiden on hyvä huomioida se, että uhriksi voi päätyä kuka tahansa. Usein hyväksikäyttö tapahtuu opportunistisesti esimerkiksi kaikkia niitä kohtaan, joilla on haavoittuvainen laite avoimena verkkoon. Tämän jälkeen aletaan selvittää, minkälaisia uhreja on saatu hyväksikäytön tuloksena.

6. Muuta

6.1 Chrome

Heinäkuussa Google lisäsi suojauksia Chrome-selaimeen, joiden tarkoituksena oli estää infostealer-haittaohjelmien pääsy selaimeen tallennettuihin evästeisiin. Nimensä mukaisesti infostealerit koittavat kaapata laitteelta haittatoimijalle hyödyllistä tietoa, kuten salasanoja ja evästeitä. Evästeiden kaappaaminen sallii haittatoimijan kirjautua jokaiseen palveluun, johon päätelaitteella on aktiivinen kirjautuminen selaimella.[34]

Syyskuun aikana useat infostealer-haittaohjelmien kehittäjät ilmoittivat löytäneensä tavan ohittaa Googlen uudet suojaukset ja kaapata evästeet selaimesta, usein jopa ilman admin-oikeuksia työasemalla.[35] [36] Google todennäköisesti tulee parantamaan suojauksia tulevaisuudessa, mutta organisaatioiden kannattaa ottaa infostealerien tuomat uhat tosissaan. Haittatoimijoiden yleisin tapa päästä organisaation verkkoon käsiksi on vuotaneet tunnukset. Esimerkiksi Spycloudin tutkimuksen mukaan noin kolmasosa kiristyshaittaohjelmien uhriksi joutuneista oli saanut infostrealer-tartunnan edellisen 16 viikon aikana.[37]

[32] The Record, 25.9.2024, Modified LockBit and Conti ransomware shows up in DragonForce gang's attacks, https://therecord.media/lockbit-conti-dragonforce-ransomware-cybercrime
[33] DragonForce Blog
[34] Bleeping Computer, 24.9.2024, Infostealer malware bypasses Chrome's new cookie-theft defenses, https://bleepingcomputer.com/news/security/infostealer-malware-bypasses-chromes-new-cookie-theft-defenses/
[35] X-julkaisu, 20.9.2024, @g0njxa, https://x.com/g0njxa/status/1837093565664539095
[36] X-julkaisu, 18.9.2024, @g0njxa, https://x.com/g0njxa/status/1836371924852539537
[37] SpyCloud, lainattu 26.9.2024, The 2024 Malware and Ransomware Defense report, https://spycloud.com/resource/2024-malware-ransomware-defense-report/

6.2 Pankkisektorin palvelunestohyökkäykset

Syyskuun aikana uutisoitiin Nordean palveluihin liittyvistä katkoksista, jotka aiheuttivat haasteita verkkopankin palveluiden käyttäjille. Nordea tiedotti aiheeseen liittyen toteuttaneensa ylläpitoa, minkä lisäksi sitä kohtaan oli tiedotteen mukaan toteutettu palvelunestohyökkäyksiä. Tähän liittyen tiedotteessa myös mainittiin, että hyökkäyksiä olisi Nordean tietojen mukaan toteutettu finanssisektoria kohtaan myös muissa Pohjoismaissa.[38] Muiden pankkien osalta asiasta ei ole uutisoitu.

Tapaukseen liittyen RootDoS-ryhmä on kertonut toteuttaneensa hyökkäyksiä. Ryhmä kertoo julkaisuissaan toimintansa kohdistuvan ruotsalaiseen pankkiin ja sen palveluihin. Ryhmän julkaisuiden lisäksi asiasta ei ole muuta todistusaineistoa.[39] Myös Kyberturvallisuuskeskus on nostanut palvelunestohyökkäykset esille tiedotteessaan. Tiedotteen mukaan kyseistä tekniikkaa, jossa yksittäisten palvelimien sijaan hyökätään laajasti organisaation palveluita vastaan, on havaittu myös syyskuun viimeisellä viikolla. Tiedotteen mukaan Kyberturvallisuuskeskus on saanut ilmoituksia myös muilta, mutta vaikutukset ovat olleet vähäiset.[40]

[38] Nordea, lainattu 24.9.2024, Häiriötiedotteet, https://www.nordea.fi/henkiloasiakkaat/tuki/hairiotiedotteet.html
[39] RootDoS X-tili
[40] Kyberturvallisuuskeskus, 27.9.2024, Kyberturvallisuuskeskuksen viikkokatsaus - 39/2024, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-392024

7. Suositukset

Kalastelutapauksissa toistuva ilmiö on puutteellinen pääsynhallinta organisaation pilvipalveluihin ja resursseihin. Pääsynhallintaa tulisi tiukentaa ja rajata kirjautumiset esimerkiksi Conditional Access Policyillä[41] luotettuihin (Entra ID- tai Hybrid-joined) laitteisiin. Tällöin kalastelun onnistuessa uhkatoimija ei pääse kirjautumaan käyttäjätunnukselle, vaikka salasana tai kirjautumis-token saataisiin haltuun. Toinen havaittu puute kalastelutapauksissa on liian sallivat asetukset uusien OAuth-applikaatioiden lisäämisessä pilviympäristöön. Käyttäjätunnuksen vaarantuessa uhkatoimija monesti lisää organisaation pilvipalveluun kolmannen osapuolen sähköpostisovelluksen (esim. emClient tai PERFECTDATA SOFTWARE), joka mahdollistaa toimijalle jalansijan organisaatiossa ja pitkäaikaisen sähköpostiviestien varastamisen. OAuth-applikaatioiden lisäämiseen tulisi vaatia admin-käyttäjän hyväksyntä[42].

Oletuksena skriptitiedostojen tuplaklikkaus riittää niiden ajamiseen Windowsissa. Esimerkiksi .js-tiedostot (javascript) ajetaan wscript.exe:llä. Haittatoimijat käyttävät usein skriptitiedostoja haittaohjelmien levittämiseen. Käyttäjillä on todella harvoin tarve oikeasti ajaa skriptitiedostoja tuplaklikkaamalla, joten skriptitiedostojen oletussovelluksen vaihtaminen esimerkiksi Notepadiin estää käyttäjiä vahingossa ajamasta haitallisia skriptitiedostoja. Tiedostopäätteitä, joille oletussovelluksen vaihtamista kannattaa miettiä on mm.: .js, .jse, .vbs, .vb, .vbe, .cmd, .bat, .sct, .shs, .shb, .hta, .scf, .ws, .wsf, .wsc, .wsh. Ohjeet oletussovelluksen vaihtamiseen löytyy esimerkiksi https://www.grouppolicy.biz/2011/09/how-to-use-group-policy-to-change-open-with-file-associations/

Suosittelemme myös poikkeamatilanteisiin valmistautumiseen seuraavien toimenpiteiden avulla:

1. Poikkeamanhallintaan liittyvien prosessien tarkistaminen ja päivittäminen
2. Luotetun DFIR-kumppanin valinta ja kontaktointi
3. Tällä hetkellä käytössä olevien valvonta-, reagointi- ja tietoturvakyvykkyyksien tarkistaminen

Poikkeamaan valmistauduttaessa suunnitelmien ja prosessien päivittäminen on tärkeää, sillä ne voivat vaatia muutoksia ollakseen toimivia. Samalla on hyvä pyrkiä arvioimaan, ovatko suunnitelmat edelleen sellaisia, että ne vastaavat parhaalla mahdollisella tavalla poikkeamatilanteisiin varautumiseen. Suunnitelmiin liittyen konkreettinen ja asioita helpottava

[41] Microsoft, 26.9.2024, Configure conditional access, https://learn.microsoft.com/en-us/defender-endpoint/configure-conditional-access
[42] Microsoft, 26.9.2024, Configure how users consent to applications, https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal

toimi on valita ja kontaktoida DFIR-kumppania. Tämä helpottaa siksi, että kumppanin kanssa keskustelu voi tuoda uutta näkemystä varautumiseen ja se avaa käytännön asioita, kuten avun hälyttämisen ja palvelun hinnan tietoja. Onkin hyvä käydä nämä keskustelut silloin, kun poikkeama ei ole käynnissä.

Valvonnan ja reagointikyvyn osalta on syytä suorittaa myös ajoittaista tarkastelua sen suhteen, onko näkyvyys ja kyvykkyys ajan tasalla. Esimerkiksi CSOC-valvonnan osalta tilanne voi vaatia päivitystä, koska ympäristöt ja niiden laitteet muuttuvat ja päivittyvät. Toisaalta valvontakyvykkyydet myös kehittyvät ja joissain tilanteissa valvonnan ratkaisuita voi olla hyvä päivittää.

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.

Lue lisää:
www.loihde.com/palvelut/kyberturva/

LOIHDE