Cyberwatch Finland

VIIKKOKATSAUS
VIIKKO 9/2024

”KYBERTURVALLISUUS SYNTYY PIENISTÄ TEOISTA JA KOKONAISUUDEN HALLINNASTA”

Cyberwatch Finland

KEY TAKEAWAYS

1. Viranomaisten onnistuneet operaatiot aiheuttavat harmia suurille kiristyshaittaohjelmatoimijoille ja voivat vaikuttaa niiden tulevaisuuden toimintaan.

2. Google ja Meta julkistivat toimenpiteitä, joilla yhtiöt pyrkivät taistelemaan kesäkuun europarlamenttivaalien ohessa esiintyvää disinformaatiota vastaan. Osittain taustalla vaikuttaa hiljattain voimaan tullut EU:n datapalvelusäädös DSA.

3. Käyttäjän sivuhistoriatiedot kiinnostavat useita eri toimijoita. Rikollisten lisäksi myös markkinointiyritykset havittelevat dataa.

1. UUSI AIKAKAUSI KYBERRIKOLLISTEN MAAILMASSA

Viime aikoina venäläiset kyberrikollisryhmät BlackCat (ALPHV) ja LockBit ovat kokeneet suuria vaikeuksia viranomaisten onnistuneiden offensiivisten toimien takia. Joulukuussa BlackCat kärsi merkittävää vahinkoa FBI:n yhdessä eurooppalaisten kansallisten poliisiviranomaisten kanssa tehdyssä iskussa ryhmän palvelimille. Helmikuun aikana saman kohtalon koki myös LockBit Britannian kansallisen rikosvirasto NCA johtaman poliisioperaation myötä. Sekä BlackCatin että LockBitin tapauksessa viranomaiset saivat haltuunsa ryhmien verkkosivustot ja niitä ylläpitävät serverit. Molemmissa tapauksista takavarikoitiin myös muun muassa ryhmien käyttämien lunnashaittaohjelmien purkuavaimia sekä jäädytettiin rikollisiin liittyviä kryptovaluuttatilejä. Joulukuisen BlackCat ryhmän toiminnan alasajon yhteydessä LockBit- ja BlackCat-toimijat ilmoittivat aloittavansa yhteistyön lunnashaittaohjelmamarkkinoilla (Ransomware as a Service, RaaS). Nyt kuitenkin molemmat näistä suurimpina pidetyistä RaaS-toimijoista ovat joutuneet hetkellisen lamauttavan viranomaistoiminnan kohteeksi.

Molemmat rikollisryhmät ovat viime aikoina siirtyneet hyvin moraalittomaan ja kaiken hyväksyvään hyökkäystoimintaan. Aikaisemmin ryhmät ovat itse noudattaneet ja pakottaneet myös yhteistyökumppaneilleen sääntöjä, jotka ovat kieltäneet niiden kehittämän haittaohjelman käyttöä esimerkiksi sairaaloita, hätäpalveluja, koulujen tietoverkkoja tai voittoa tavoittelemattomia järjestöjä vastaan. BlackCat poisti tämän eettisyyspykälän joulukuun takaiskun jälkeen ja myös LockBit hyväksyi tammikuussa hyökkäyksen Chicagon lastensairaalaa vastaan. Huomattavaa on, että vielä vuosi sitten LockBit pyysi julkisesti anteeksi alihankkijansa suorittamaa lunnashyökkäystä Toronton lastensairaalaa vastaan, antoi lunnasohjelman purkuavaimet lastensairaalan käyttöön ja lopetti yhteistyön hyökkäyksen tehneen alihankkijan kanssa.

Kummankin rikollisryhmän toiminnan takana ovat venäläiset rikolliset, joita Venäjän viranomaiset ovat kehottaneet käymään taistelua globaalia länttä vastaan antaen samalla hyväksynnän ja suojeluksen rikollisille toimille. Tässä on eittämättä yksi juurisyy sille, miksi nyt nähdyt mittavat monikansalliset poliisioperaatiot ovat yhdistäneet viranomaistoimintaa yli valtionrajojen. Aiemmin viranomaisten tavoitteena on ollut kitkeä pois taloudellisesti motivoituneita kyberrikollisia. Nyt sen rinnalle voidaan nähdä nousseen myös painava poliittinen motiivi, koska nyt puheena olevien ja muidenkin kyberrikollisryhmien takomat hurjat lunnastulot hyödyttävät välillisesti Venäjän valtion taloutta. Länsimaisten viranomaisten ennennäkemättömän mittavat operaatiot kielivät halusta estää suurta rikollista rahaliikennettä Venäjälle lisänä talouspakotteille. Toisena tavoitteena tiivistyneeseen viranomaisyhteistyöhön voidaan olettaa olevan LockBitin jatkuvan sovelluskehityksen hidastaminen. Iskun seurauksena paljastuikin, että ryhmä oli jo valmistelemassa uutta, entistä vaarallisempaa versiota haittaohjelmastaan.

Joka tapauksessa kybermaailmassa on nähtävissä uuden aikakauden alku, jossa laajat, kansainväliset viranomaisten yhteenliittymät suorittavat onnistuneita iskuja suurimpia rikollisryhmiä vastaan. Perinteisesti on ajateltu rikollisten olevan aina askeleen edellä ja viranomaisten seuraavan perässä. Nyt nähdyissä operaatioissa poliisiviranomaiset ovat kuitenkin ottaneet proaktiivisen otteen taistelussa kyberrikollisuutta vastaan. Jokainen kyberrikollisryhmä joutuu miettimään omaa toimintaansa ja olemaan varuillaan. Jää nähtäväksi, luovatko viranomaistoimenpiteet kostokierteen, jossa rikollisryhmät kohdistavat voimiaan jatkossa enemmän nimenomaan valtiollisiin toimijoihin jättäen yritysmaailman pienemmälle roolille. On kuitenkin muistettava, että niin LockBitin kuin BlackCatinkin tapauksessa kyseessä on palveluntarjoaja, jossa iskuja suorittavat alihankkijat, jotka maksavat ryhmille niiden sovellusten käytöstä. Näin ajatellen rikolliset suuntaavat jatkossakin pääasiallisen kiinnostuksensa sinne, mistä kulloinkin saa helpoiten paljon rahaa.

2. ALUSTAJÄTIT TAISTELEVAT DISINFORMAATIOTA VASTAAN EU:SSA, MYÖS DIGIPALVELUSÄÄDÖS VELVOITTAA

Disinformaation vastainen rintama Euroopassa sai uusia vahvistuksia helmikuussa, kun Google ja Meta ilmoittivat tahoillansa aloittavansa kampanjat disinformaation torjumiseksi kesäkuisten europarlamenttivaalien kontekstissa. EU:ssa on pelätty erityisesti Venäjän propagandan määrän kasvua ja vaikutuksia tuleviin vaaleihin. Yhtiöiden ilmoitukset ajoittuivat symbolisesti sopivasti Euroopan unionin digipalvelusäädöksen DSA (Digital Services Act) kansallisten soveltamisen alkamisen, helmikuun 17. päivän, läheisyyteen. DSA:n on toivottu omalta osaltaan torjuvan disinformaatiota, sillä se asettaa verkkoalustoille velvoitteita muun muassa alustojen moderoinnin suhteen sekä velvoittaa alustoja arvioimaan ja vähentämään demokraattisiin- ja vaaliprosesseihin liittyviä riskejä. DSA:n velvoitteita on sovellettu erittäin suurten verkkoalustojen ja hakukoneiden osalta jo viime elokuun 25. päivästä alkaen.

Googlen tapauksessa yhtiö aloittaa huhti-toukokuussa mainoskampanjan, joka toteutetaan muun muassa YouTube- ja TikTok-alustoilla viidessä eri EU-maassa: Belgiassa, Ranskassa, Saksassa, Italiassa ja Puolassa. Mainokset sisältävät tietoa siitä, miten tunnistaa mis- ja disinformaatio ja minkälaista väärää tietoa pyritään levittämään. Kampanjassa hyödynnetään niin kutsuttua ”prebunking”-tekniikkaa. Tämä tarkoittaa sitä, että ilmoitus väärästä tiedosta pyritään saamaan kohteelle aiemmin kuin itse väärä tieto tavoittaa kohteen. Näin väärän tiedon saavuttaessa kohteen, osaa hän jo suhtautua siihen varauksella. Kyseisten maiden valitsemista mainosten kohteeksi perusteltiin muun muassa mahdollisuutena tavoittaa laaja määrä vaalien äänestäjiä sekä hyödyntää yhtiön omaa paikallistietoutta. Vaikka kampanjan kohteena ovat EU:n väkirikkaimmat valtiot, jää sen ulkopuolelle kuitenkin merkittävä määrä muiden jäsenmaiden äänestyskelpoisia kansalaisia, mikä osaltaan heikentää vaikuttavuutta. Toimet ovat kuitenkin eittämättä paikallaan ja oikeansuuntaisia.

Meta taas tarttuu ongelmaan avaamalla erityisen vaalikeskuksen (Elections Operation Center), joka pyrkii tunnistamaan ja torjumaan uhkia reaaliaikaisesti. Misinformaatiota torjutaan muun muassa yhteistyössä 26 kumppanin kanssa ympäri EU:ta yli 22:lla eri kielellä faktantarkastuksen avulla. Lisäksi pyrkimyksenä on taklata koordinoidut vaikuttamisoperaatiot sekä vastata tekoälyllä toteutettaviin mahdollisiin väärinkäytöksiin kuten syväväärennöksiin.

Molempien yhtiöiden päätösten taustalla vaikuttaa varmasti osittain EU:n digipalvelusäädös, vaikka ilmoituksissa ei suoraan siihen viitatakaan. Säädöksen päätavoitteena EU-komission mukaan on ”estää laitonta ja haitallista toimintaa verkossa ja torjua disinformaation leviämistä.” Digipalvelusäädös on julkisuudessa saanut tähän asti kuitenkin enemmän huomiota muun muassa sen myötä tulleesta velvollisuudesta antaa alustojen käyttäjille mahdollisuus kieltää personoitu markkinointi, velvoitteesta luoda helposti ymmärrettävät käyttöehdot sekä velvoitteesta avoimempaan sisällön moderointiin ja mahdollisuuteen valittaa moderointipäätöksestä. Lisäksi DSA kieltää yksiselitteisesti mainonnan kohdentamisen lapsille sekä mainonnan kohdistamisen aikuisille esimerkiksi etnisen taustan tai seksuaalisen suuntautumisen perusteella. Tavoitteena on siis kasvattaa käyttäjien oikeuksia ja vaikutusmahdollisuuksia.

Vaikka säädös itsessään koskee käytännössä kaikkia digitaalisia palveluita, sen keskiössä ovat erittäin suuret verkkoalustat ja hakukoneet. Tällaisiksi määritelmällisesti luetaan palvelut, joiden aktiivisten käyttäjien määrä kuukaudessa ylittää kuuden kuukauden ajanjakson keskiarvon tarkastelussa 45 miljoonaa käyttäjää EU-alueella. Näille erittäin suurille toimijoille lisävelvollisuuksina on neljän erillisen riskikategorian arviointi, joiden osalta tulisi ryhtyä myös toimiin riskien vähentämiseksi. Näitä ovat laittoman sisällön levittämiseen, kuten esimerkiksi laittoman vihapuheen leviämiseen sekä demokraattisiin prosesseihin, kansalaiskeskusteluun ja vaaliprosesseihin liittyvät riskit. Sakkojen enimmäismäärä säädöksen velvoitteiden noudattamatta jättämisestä voi olla korkeintaan 6 % yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta.

EU-sääntelyä nimitetään usein byrokraattiseksi ja sen saavutuksia epäillään. On kuitenkin selvää, että sillä on myös positiivisia vaikutuksia. DSA onkin mahdollisesti esimerkki kansalaisen näkökulmasta onnistuneesta sääntelystä, sillä se lisää palveluiden läpinäkyvyyttä ja käyttäjien valinnanmahdollisuuksia oman yksityisyytensä suhteen. Laajemmalle yhteiskunnalle hyödyt näkyvät juuri edellä kuvattujen kampanjoiden muodossa, jotka omalta osaltaan voivat vähentää vihamielisten toimijoiden EU:hun kohdistamien vaikutusyritysten tehokkuutta.

3. SELAUSHISTORIADATA ON ARVOKASTA

Viime torstaina Yhdysvaltain kauppakomissio (Federal Trade Commission, FTC) asetti tietoturvayhtiö Avastille 16,5 miljoonan dollarin sakot. Sakkojen syyksi kerrottiin, että yhtiö oli käyttäjien tietämättä sekä kerännyt että myynyt näiden dataa. Seuraamusmaksun lisäksi kauppakomissio myös kielsi käyttäjädatan myynnin jatkossa. Ironisen tilanteesta tekee se, että tuotteita, joiden kautta Avast oli dataa kerännyt, oli markkinoitu käyttäjille yksityisyydensuojaa edistävinä ja verkkoseurannan estävinä palveluina. Käytännössä kyse oli selainlaajennuksista ja antivirusohjelmistoista. Ne toki tekivät sen, mitä Avast oli asiakkailleen luvannut, mutta samalla palvelut keräsivät ja säilyttivät käyttäjien selaustietoja. Näitä tietoja Avast oli FTC:n perustelujen mukaan myynyt erilaisiin markkinointi- ja profilointitarkoituksiin ja näin rikkonut sekä lakia että itse käyttäjilleen tekemiä lupauksia.

Vaikka kyse ei ollutkaan äärimmäisen arkaluontoisesta tiedosta, voi selaus- ja hakuhistoria silti paljastaa paljon käyttäjästä. Sivustovierailut voivat esimerkiksi kertoa iästä, sukupuolesta ja kiinnostuksen kohteista, mikä tekee datasta arvokasta mainontaa kohdentaville yrityksille. Samalla sen avulla voidaan saada viitteitä esimerkiksi käyttäjien uskonnollista ja ideologista suuntautumista tai terveydentilaan liittyvistä seikoista. Näiden tietojen perusteella käyttäjiä pystytään osaltaan profiloimaan. Yksittäisen käyttäjän näkökulmasta oma selaushistoria päätyminen kolmannen osapuolen haltuun ei välttämättä tunnu uhkaavalta, mutta mieli voi muuttua, mikäli käyttäjä saisi nähtävilleen profiilin, jonka markkinointiyritykset ovat eri lähteistään saamien selaus-, haku- ja evästetietojen perusteella koonneet. Ei ole esimerkiksi harvinaista, että mainosyritykset lisäävät käyttäjistä ylläpitämiinsä profiileihin tietoja raskaudesta tai muutoksista terveydentilassa. Tämä voi tapahtua jo ennen kuin henkilö itse olisi valmis jakamaan näitä tietoja lähimmäisilleen.

Seurannan estäminen on nykypäivänä hankalaa. Verkkokäyttäytymistä seuraavat tahot, joilla siihen on perusteltu oikeus, kuten verkko-operaattorit ja vierailun kohteena olevat sivustot, mutta esimerkiksi evästeiden myötä myös ei-toivotut kolmannet osapuolet. Avastin esimerkki osoittaa, että voi olla myös vaikea löytää toimijaa, jonka lupauksiin yksityisyyttä suojaavasta palvelusta voi luottaa. Usein varsinaisesti omien tietojen salaamisen sijaan erilaisia sovellusratkaisuja käyttämällä tämä data luovutetaan tietoisesti yhdelle tietylle toimijalle, joka lupaa pitää siitä huolen. Tämä pitää paikkansa esimerkiksi VPN-palveluiden kohdalla, jotka lupauksien mukaisesti salaavat selaustiedot kolmansilta osapuolilta, mutta ovat myös ajoittain jääneet kiinni keräämänsä datan huolimattomasta käsittelystä tai pahimmillaan Avastin tavoin sen kauppaamisesta. Nämä palvelut ovat myös houkuttelevia kohteita tietomurroille, sillä vaikka yhtiö itse ei dataa myisikään, voi sen varastanut hakkeri näin tehdä. Paljon onkin kyse siitä, missä määrin ja missä muodossa nämä palvelut tietoja säilyttävät, ja kuinka paljon käyttäjä voi tai haluaa sen lupauksiin luottaa. Varmuuden saaminen tästä voi olla mahdotonta tai ainakin hyvin vaikeaa. Pienellä taustatyöllä on kuitenkin mahdollista selvittää, minkälainen maine yksityisyyttä mainostavalla palveluntarjoajalla on. Hyvänä ohjeena voi toimia myös palvelun hinta: mikäli suojausta markkinoiva tuote on selvästi kilpailijoitaan halvempi, hankkii yritys voittonsa todennäköisesti jotain muuta kautta. Ilmaisessa palvelussa käyttäjä on lähes aina itse se tuote, jota myydään.

On hyvä myös muistaa, että selausdataa keräävät myös markkinointiyritysten tai epärehellisten tietoturvatoimijoiden lisäksi huomattavasti pahantahtoisemmat tahot. Erilaiset dataa varastavat haittaohjelmat eli infostealerit ovat yleisimpien virustyyppien joukossa. Ne keräävät tartuttamiltaan laitteilta muiden arkaluontoisten tietojen lisäksi myös esimerkiksi selaus- ja hakuhistoriaa. Myös näitä tietoja myydään ja jaetaan, tosin konsulttiyritysten välisten sopimusten sijaan näissä kauppapaikkana toimivat pimeän verkon markkinafoorumit. Myös kyberrikollisia saattaa kiinnostaa käyttäjien selaushistoria, sillä sen avulla voidaan esimerkiksi päätellä, miten uhria voisi olla helpointa lähestyä sosiaalisen manipuloinnin keinoin: harrastaako tämä esimerkiksi uhkapelejä tai vieraileeko aikuisviihde- tai deittisivustoilla. Kaikkea tätä tietoa voidaan käyttää rikosten suunnitteluun ja yhdistettynä muuhun tietoon, se voi myös suoraan tarjota rikollisille painostamisen tai kiristyksen mahdollisuuksia.

Cyberwatch Finland

MITEN VÄLTTYÄ EI TOIVOTULTA SEURANNALTA:

Verkkoselaimen valinta: Eri selaimet suojaavat käyttäjien yksityisyyttä eri tavalla. Vertailuissa yleisimmät selaimet kuten Chrome ja Edge saavat usein huonoimpia arvosanoja. Parhaana vaihtoehtona tunnetuimmista selaimista pidetään Firefoxia, ja siitä muokattua suojausta pidemmälle vienyttä LibreWolfia ja tietoturvapiireissä suosittua Bravea. Usein yksityisyyttä korostavan selaimen valitsemalla käyttäjä luopuu joistakin käyttökokemusta parantavista toiminallisuuksista kuten selainlaajennuksista.

Selainten asetukset: Moni selain, myös Chrome ja Edge, tarjoavat mahdollisuuden kytkeä päälle evästeitä rajoittavia asetuksia tai muita nimellisesti yksityisyyttä lisääviä toiminnallisuuksia. Vaikkakin ne voivat olla hyödyllisiä, eivät nämä asetukset kaikissa tapauksissa välttämättä merkittävästi todellisuudessa muuta sitä, miten dataa kerätään. Esimerkiksi yleinen vaihtoehto Do Not Track (DNT) pyyntöjen lisäämisestä verkkovierailuihin on laajalti todettu täysin merkityksettömäksi seurannan kannalta. Toisaalta esimerkiksi incognito- tai yksityinen selaus- tila rajoittavat seurantaa melko hyvin.

Evästeistä kieltäytyminen: Vaikkakin työlästä, evästeistä kieltäytyminen verkkosivuja selatessa on suhteellisen toimiva keino välttyä datan päätymiseltä jatkohyödyntämiseen. Vaikeasti löydettävien kaikki evästeet estävien painikkeiden lisäksi tätä voi kuitenkin rajoittaa se, että verkkosivujen toiminnallisuus voi kärsiä evästeistä kieltäytymällä. Etenkin epäilyttävien tai ei HTTPS-sivustojen kohdalla ylimääräisten vaivan näkeminen olisi äärimmäisen tärkeää omien tietojen suojaamiseksi. Saatavilla on myös selainlaajennuksia tai sovelluksia, jotka automatisoivat tämän prosessin, mutta näitäkin käyttäessä kannattaa ensin varmistua palveluntarjoajan luotettavuudesta, ettei evästeistä kieltäytymällä tule samalla ladanneeksi piilotettua haittaohjelmaa.

Hakukoneen valinta: Kuten selaimet myös hakukoneet keräävät ja säilyttävät selaustietoja ja näissäkin vaihtelua on runsaasti. Google ja Bing ovat jälleen eniten tietoa keräävien joukossa. Hyvä ja laajasti käytetty vaihtoehto näille on esimerkiksi monessa selaimessa oletukseksikin asetettavissa oleva DuckDuckGo.

Yksityisyyttä lisäävät sovellukset: Erilaiset käyttäjätietoja suojaavat ratkaisut, kuten VPN-palvelut, ovat toimivia ratkaisua tietojenkeräykseltä välttymiseen ja oman selausdatan suojaamiseen. Näitä käyttäessä on kuitenkin hyvä varmistua palveluntarjoajan ehdoista ja luotettavuudesta, sillä samalla kun suojaa tietonsa kolmansilta osapuolilta, luovuttaa usein kaiken tämän datan VPN-palvelua tarjoavalla yritykselle.

LÄHTEET

1. Uusi aikakausi kyberrikollisten maailmassa

https://www.bleepingcomputer.com/news/security/us-offers-15-million-bounty-for-info-on-lockbit-ransomware-gang/
https://www.bleepingcomputer.com/news/security/police-arrest-lockbit-ransomware-members-release-decryptor-in-global-crackdown/
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
https://www.theregister.com/2024/02/22/lockbit_dismantled_new_variant/
https://www.theregister.com/2024/02/01/lockbit_ransomware_attack_hospital/
https://twitter.com/DailyDarkWeb/status/1609857321315835906
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/
https://cybernews.com/news/lockbit-still-showing-signs-if-life-with-new-attacks-reported-on-friday/
https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups
https://www.state.gov/first-trilateral-sanctions-against-russian-cyber-actor/
https://therecord.media/alphv-black-cat-ransomware-takedown-fbi

2. Alustajätit taistelevat disinformaatiota vastaan EU:ssa, myös digipalvelusäädös velvoittaa

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fi
https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms
https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2065#d1e2324-1-1
https://faktabaari.fi/nakokulmat/nakokulma-digipalvelusaados-lisaa-avoimuutta-ja-vahvistaa-kayttajien-oikeuksia/
https://prebunking.withgoogle.com/
https://blog.google/around-the-globe/google-europe/supporting-elections-for-european-parliament-2024/
https://about.fb.com/news/2024/02/how-meta-is-preparing-for-the-eus-2024-parliament-elections/

3. Selaushistoriadata on arvokasta

https://therecord.media/avast-fine-ftc-alleged-browser-data-sales
https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over
https://privacytests.org/
https://www.techradar.com/vpn/avoid-downloading-a-bad-vpn-these-are-the-warning-bells-to-look-out-for
https://brave.com
https://librewolf.net/

Kuvat: Pixabay, HilariousGifs.com