TLP:CLEAR

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

警察庁
National Police Agency

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Kyberuhkien lieventäminen rajallisilla resursseilla: Ohje kansalaisyhteiskunnalle

Julkaisuajankohta: Toukokuu 2024

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), Estonian Computer Response Team (CERT-EE), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), National Center of Incident Readiness and Strategy for Cybersecurity (NISC) Japan, Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (NCSC-FI), National Police Agency (NPA) Japan, United Kingdom National Cyber Security Centre (NCSC-UK)

TIIVISTELMÄ

Yhdysvaltain kyberturvallisuusvirasto CISA ja seuraavat organisaatiot (jäljempänä “ohjeen laatineet virastot”) ovat luoneet tämän ohjeistuksen yhteistyössä keskeisten valtiollisten, valtiosta riippumattomien, yritysmaailman ja kansalaisyhteiskunnan kumppaneiden kanssa. Ohjeen laatineet virastot julkaisevat tämän yhteisen kyberturvallisuuden ohjeistuksen erityisen riskialttiille yhteisötoimijoille, kuten kansalaisyhteiskunnan järjestöille ja yksilöille:

- Federal Bureau of Investigation (FBI)
- Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- Estonian Computer Emergency Response Team (CERT-EE)
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- National Center of Incident Readiness and Strategy for Cybersecurity (NISC) Japan
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (NCSC-FI)
- National Police Agency (NPA) Japan
- United Kingdom National Cyber Security Centre (NCSC-UK)

Kansalaisyhteiskunnan toimijoiden (ihmisoikeuksia ja demokratiaa edistävät järjestöt, yhteisöt ja yksilöt, kuten voittoa tavoittelemattomat, etuja valvovat, kulttuuriset, uskonnolliset ja akateemiset järjestöt, ajatushautomot, toimittajat, toisinajattelijat ja siirtolaisjärjestöt) katsotaan olevan erityisen riskialttiita yhteisöjä. Nämä järjestöt ja niiden työntekijät ovat yleisiä kohteita valtioiden tukemille uhkatoimijoille, joiden tavoitteena on heikentää demokraattisia arvoja ja etuja. Uhkatoimijat hyödyntävät digitaalista rajat ylittävää painostusta, jonka avulla he pyrkivät saamaan haltuunsa järjestöjen ja yksilöiden laitteita ja tietoverkkoja pelotellakseen, hiljentääkseen, painostaakseen, häiritäkseen tai vahingoittaakseen kansalaisyhteiskunnan järjestöjä ja yksilöitä.

Toimialan raportoinnin perusteella valtioiden tukemia toimia kohdennetaan riskialttiisiin yhteisöihin pääasiassa Venäjän, Kiinan, Iranin ja Pohjois-Korean hallintojen taholta. Toimijat tekevät yleensä laaja-alaista tutkimusta ennen hyökkäystään löytääkseen mahdollisia uhreja, kerätäkseen tietoa käyttäjän manipuloinnin tueksi tai päästäkseen käsiksi kirjautumistietoihin. Tavoitteena on valvoa ja seurata järjestöjen tietoverkkoja, henkilökohtaisia tilejä (esim. sähköposti) ja yksilöiden laitteita esimerkiksi vakoiluohjelmien eli vaarantuneista laitteista tietoja keräävien haittaohjelmien avulla.

Tämä ohje antaa suosituksia kansalaisyhteiskunnan järjestöille ja yksilöille valtioiden tukemien kybertoimien uhkien lieventämiseksi havaitun haitallisen toiminnan perusteella. Lisäksi se sisältää suosituksia ohjelmistovalmistajille asiakkaiden turvallisuusaseman parantamiseksi.

Sisällysluettelo

JOHDANTO

Kansalaisyhteiskuntaan kohdistuvien kyberuhkien yleisyys ja globaali luonne korostuvat toimialan raportoinnissa, minkä vuoksi toimijoiden onkin tärkeää varautua erilaisten poliittisesti ja ideologisesti motivoituneiden uhkatoimijoiden varalta. Kansalaisyhteiskunnan järjestöjä pidetään erityisen riskialttiina yhteisöinä niiden korkean uhkatason ja matalan puolustusvalmiuden vuoksi. Erityisesti:

- Kansalaisyhteiskunnan järjestöjen ja niiden henkilökunnan jäsenten **uhka** joutua haitallisten kybertoimijoiden kohteeksi on **korkea**. Toimialan raportoinnin perusteella nämä järjestöt ja niiden henkilökunta ovat mahdollisia kohteita demokraattisia arvoja heikentämään pyrkiville valtioiden tukemille toimijoille.
- Kansalaisyhteiskunnan järjestöillä on usein **matala puolustusvalmius**. Niillä ei ole käytössään sisäistä IT-tukea ja olennaista kyberhygieniaa, joilla estää haitallista toimintaa (esim. elinkaaren hallintaa, korjaustiedostojen hallintaa, monivaiheista tunnistautumista, salasanojen hallintaa). Kansalaisyhteiskunnan alalla toimivat yksilöt käyttävät usein turvaamattomia viestintäkanavia ja hallinnoivat julkisia profiileja työnsä edistämiseksi. Puolustusvalmiudeltaan heikot organisaatiot ovat alttiita yleisille kyberuhkille, kuten käyttäjän manipulointiyrityksille.

Useimmissa tapauksissa tilannetta pahentaa vielä se, että tuotteet ja palvelut on suunniteltu tavalla, joka jättää kyberuhkien vähentämisen asiakkaan tai loppukäyttäjän tehtäväksi. Asiakkaan tai loppukäyttäjän on esimerkiksi tehtävä tiettyjä ja toisinaan työläitä toimia parantaakseen kyberturvallisuusasemaansa.

Tämä yhteinen ohje on kehitetty osana CISA:n High-Risk Community Protection (HRCP) -hanketta* ja NCSC-UK:n Defending Democracy -kampanjaa†, ja siinä tarjotaan kansalaisyhteiskunnan järjestöille toimenpiteitä, joilla lieventää yleisten kyberuhkien aiheuttamaa riskiä. Ohjeen laatineet virastot rohkaisevat kansalaisyhteiskunnan järjestöjä ja niihin liittyviä yksilöitä käyttämään tämän ohjeen sisältämiä lieventäviä toimenpiteitä. Ohjeen laatineet virastot rohkaisevat vahvasti myös ohjelmistovalmistajia ottamaan vastuuta asiakkaidensa turvallisuudesta soveltamalla tämän ohjeen lieventäviä toimenpiteitä ja suunnittelemalla tuotteita, jotka estävät haitallisten toimijoiden yleisimmät hyökkäykset.‡

---

* Vuonna 2023 käynnistyneessä HRCP-hankkeessaan CISA tunnistaa erityisen riskialttiita yhteisöjä ja tekee yhteistyötä niiden kanssa ymmärtääkseen yhteisöihin kohdistuvia uhkia, tunnistaakseen puolustusta vahvistavia resursseja ja täydentääkseen tarjolla olevaa tukea. Lisätietoa CISA:n HRCP-hankkeesta löytyy Yhdysvaltain kotimaan turvallisuusviraston tiedotteesta (englanniksi): Secretary Mayorkas Discusses New U.S. Efforts to Counter Spread of Digital Authoritarianism at Summit for Democracy.

† NCSC-UK noudattaa kyberpuolustuksessa koko yhteiskunnan kattavaa lähestymistapaa ja pitää kansalaisyhteiskuntaa yhtenä kolmesta painopistealueestaan. Defending Democracy -projektissaan NCSC-UK pyrkii yhteistyöhön erityisen riskialttiiden julkisten ja vaaleilla valittujen viranhaltijoiden kanssa edistääkseen ymmärrystä henkilökohtaisten ja yrityksille kuuluvien laitteiden kautta yksilöihin kohdistuvista kehittyneistä uhkista. Lisätietoa NCSC-UK:n verkkosivuilla (englanniksi): Defending Democracy.

‡ Tuotteet, joiden suunnittelussa turvallisuus on keskiössä, noudattavat turvallisen suunnittelun periaatteita (Secure by Design). Olennaista on, että ohjelmistovalmistajat ottavat vastuun asiakkaidensa turvallisuudesta rakentamalla kyberturvallisuuden osaksi suunnittelua ja kehittämistä. Lisätietoa turvallisen suunnittelun periaatteista (englanniksi) osoitteessa cisa.gov/securebydesign ja oppaassa Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.

KANSALAISYHTEISKUNNAN KYBERUHKAT

Uhkien telemetria- ja tiedustelutietojen raportoinnin puute sekä erityisen riskialttiiden yhteisöjen rajalliset yritystason ratkaisut estävät kaupallisia ja julkisia organisaatioita mittaamasta tarkasti näihin yhteisöihin kohdistuvia uhkia. Toimialan raportoinnista käy kuitenkin ilmi, että tietyt kansalaisyhteiskunnan osat ovat johdonmukaisesti valtioiden tukemien kybertoimijoiden kohteena. Etenkin kansalaisjärjestöt, ajatushautomot, ihmisoikeusaktivistit ja toimittajat ovat toistuvasti näiden toimijoiden kohteena:

- Microsoftin mukaan kansalaisjärjestöt ja ajatushautomot olivat vuonna 2023 toiseksi yleisin kohde valtioiden tukemille toimijoille (heti IT-sektorin jälkeen).[1]
- CrowdStriken raportointi paljasti marraskuussa 2023, että valtioiden tukemista ryhmistä viisi pitää kohteenaan ajatushautomoita,[2] 11 ryhmää muodostaa mahdollisesti uhkia kansalaisjärjestöille,[3] kahden ryhmän kohteena ovat toisinajattelijat[4] ja yhden ryhmän tiedetään uhkaavan voittoa tavoittelemattomia järjestöjä.[5]
- Cloudflare on havainnut haitallisen kybertoiminnan kansalaisyhteiskunnan järjestöjä kohtaan lisääntyneen yleisesti.[6] Vuoden 2023 toisella neljänneksellä voittoa tavoittelemattomat järjestöt olivat toiminnan kohteena enemmän kuin mikään muu toimiala, kun tarkastellaan haitallista liikennettä järjestöjen verkkosivuille suhteessa niiden kokonaisliikenteeseen.[7] Vuoden 2023 kolmannella neljänneksellä voittoa tavoittelemattomat ja riippumattomat mediajärjestöt olivat toisella sijalla metalli- ja kaivosteollisuuden jälkeen, sillä 17,14 % niiden kokonaisliikenteestä tuli hajautetuista palvelunestohyökkäyksistä (DDoS).[8] Vastaavasti Euroopan unionin kyberturvallisuusvirasto (ENISA) havaitsi, että kohteeksi valitut kansalaisyhteiskunnan yksilöt olivat maailmanlaajuisesti toiseksi suosituin kohde kybertoimille heinäkuun 2022 ja kesäkuun 2023 välillä.[9]

Valtioiden tukemat toimijat kohdistavat tekojaan kansalaisyhteiskunnan järjestöihin ja niiden työntekijöihin osana demokraattisia arvoja heikentäviä työkalujaan. Ne ottavat kohteekseen järjestöjä ja yksilöitä etenkin verkossa tavoitteenaan pelottelu, häirintä,§ painostaminen ja tarkkailu. Tämä on niin sanottua digitaalista rajat ylittävää painostusta.

Digitaalista rajat ylittävää painostusta edeltää usein verkossa tapahtuva kattava kaupallisten verkkosivustojen, sosiaalisen median sivujen, geopoliittisten julkaisujen ja tiedotteiden tutkimus, jonka avulla toimijat keräävät tietoa kohdeorganisaatioista ja -yksilöistä. Tämän tutkimustyön jälkeen valtioiden tukemat toimijat pääsevät usein käsiksi järjestön tietoverkkoihin tai henkilökohtaisiin laitteisiin (a) hyödyntämällä käyttäjän manipulointia, joka houkuttelee uhrin paljastamaan kirjautumistietoja tai lataamaan haittaohjelmia, tai (b) saamalla käyttäjän lataamaan näennäisesti aidon sovelluksen, joka sisältää haittaohjelman. Päästyään sisälle laitteisiin toimijat asentavat niille usein vakoiluohjelmia. Vakoiluohjelma on kaupallinen työkalu, joka mahdollistaa kattavan valvonnan, kuten sijainnin seurannan, kuvien ja äänen kaappauksen sekä pääsyn henkilökohtaisiin tiedostoihin ja viesteihin.

§ Valtiot käyttävät häirintää itsenäisenä työkaluna hiljentämään, hallitsemaan tai tukahduttamaan toisinajattelijoita. Kun tämä tapahtuu verkossa, kyseessä on digitaalinen häirintä, joka voi esimerkiksi tarkoittaa sosiaalisen median tilien aktivoimista toimimaan tiettyjä yksilöitä vastaan.

Lue lisätietoa valtioiden tukemista ryhmistä, joiden tiedetään kohdistavan toimiaan kansalaisyhteiskunnan järjestöihin: Liite A: Valtioiden tukemat toimijat. Lue teknistä tietoa kybertoimista, joiden avulla toimijat pääsevät käsiksi tietoverkkoihin ja laitteisiin yksilöiden valvomiseksi: Liite B: Valtioiden tukemien toimijoiden taktiikat ja tekniikat.

LIEVENTÄVÄT TOIMENPITEET

Kansalaisyhteiskunnan järjestöt

Ohjeen laatineet virastot rohkaisevat kansalaisyhteiskunnan järjestöjä noudattamaan CISA:n määrittelemiä kyberturvallisuuden parhaita käytäntöjä (Cross-Sector Cybersecurity Performance Goals (CPG)). Näissä kyberturvallisuuden ohjeissa määritellään vähimmäiskäytännöt ja -suojaukset, jotka perustuvat yleisimpiin ja vaikuttavimpiin uhkiin ja toimiin. Valtioiden tukemien toimijoiden suorittamaa taktista tiedustelua ja tunkeutumista yrityksen tietoverkkoihin tietojenkalastelun ja vaarantuneiden kirjautumistietojen avulla voi estää seuraavasti:

CISA:N PARHAAT KÄYTÄNNÖT:

- Etusijalle asetetut kyberturvallisuuskäytännöt.
- Tavoitteena riskien vähentäminen.
- Perustuvat CISA:n ja sen julkisten ja yksityisten kumppaneiden havaitsemiin uhkiin.
- Tavoitteena merkittävästi vähentää kriittiseen infrastruktuuriin ja kansalaisiin kohdistuvia riskejä.

- **Ota käyttöön tietojenkalastelun estävä monivaiheinen tunnistautuminen (MFA)** [CPG 2.H]. Monivaiheinen tunnistautuminen on yksi parhaita keinoja vähentää yleisiä kirjautumistietoihin perustuvia hyökkäyksiä. Lisätietoa CISA:n monivaiheisen tunnistautumisen oppaasta Phishing-Resistant Multifactor Authentication (englanniksi).
- **Tarkasta tilit ja poista käyttämättömät tilit käytöstä.**
- **Vähemmän oikeuden periaate.** Älä käytä päivittäisten tehtävien suorittamiseen käyttäjätilejä, joilla on laajat oikeudet (pääkäyttäjän oikeudet) [CPG 2.E]. Myönnä kullekin käyttäjälle vain heille määrätyissä tehtävissä tarvittavat oikeudet. Näiden tilien käyttöä tulee valvoa säännöllisesti.
- **Poista käyttäjätilit ja pääsy organisaation resursseihin entisiltä työntekijöiltä** [CPG 2.D].
- **Noudata huolellisuutta palveluntarjoajien kuten pilvipalvelujen (CSP) ja hallinnoitujen palveluiden (MSP) tarjoajien valinnassa** pienentääksesi toimitusketjun riskejä. Käytä vain hyvämaineisia palveluntarjoajia.
  - **Tarkista sopimussuhteet** kaikkien palveluntarjoajien kanssa. Varmista, että sopimuksiin sisältyy:
    - asiakkaan asianmukaisiksi katsomat turvallisuustoimet
    - palveluntarjoajan hallinnoimien asiakasjärjestelmien asianmukainen valvonta ja lokitus
    - palveluntarjoajan läsnäolon, toiminnan ja asiakasverkkoyhteyksien asianmukainen valvonta ja
    - ilmoitukset palveluntarjoajan infrastruktuurissa ja hallinnollisessa tietoverkossa tapahtuvista vahvistetuista tai epäillyistä turvallisuustapahtumista ja -poikkeamista.
  - **Hallitse arkkitehtuurin riskejä**:
    - Tarkasta ja varmista kaikki asiakkaan järjestelmien, palveluntarjoajan järjestelmien ja asiakkaan muiden irrallisten järjestelmien väliset yhteydet.

        - Ota yhteys MSP-palveluntarjoajan infrastruktuuriin virtuaalisen erillisverkon (VPN) avulla. Kaiken verkkoliikenteen palveluntarjoajan suunnasta tulisi käyttää vain tähän tarkoitukseen varattua turvattua yhteyttä.
    - **Suosi palveluntarjoajia, jotka noudattavat turvallisen suunnittelun periaatteita.**
- **Tarjoa kyberturvallisuuden peruskoulutusta,** jossa käsitellään esimerkiksi tietojenkalastelua ja salasanaturvallisuutta [CPG 2.I]. Varmista, että koulutus käsittelee valtioiden tukemien kybertoimijoiden henkilökohtaisiin sähköposteihin ja laitteisiin kohdistuvaa toimintaa ja ohjeistaa henkilökuntaa suojaamaan henkilökohtaiset sähköpostitilinsä ja mobiililaitteensa noudattamalla seuraavassa luvussa yksilöille annettavia suosituksia.
- **Kehitä poikkeamien tutkinta- ja palautumissuunnitelmia ja noudata niitä** [CPG 2.S]**.** Varmista, että suunnitelmissa kerrotaan yhteystiedot avun saamiseksi ja poikkeaman raportoimiseksi. (Tämän ohjeen kohdassa Yhteystiedot annetaan kunkin ohjeen laatineen viraston raportointitiedot. Kohdassa Tietoja annetaan ohjeita poikkeamien tutkinta- ja palautumissuunnitelmien laatimiseen.)

Kansalaisyhteiskunnan yksilöt

Ohjeen laatineet virastot rohkaisevat kansalaisyhteiskunnan yksilöitä noudattamaan seuraavia suosituksia, joilla lievennetään riskejä valtioiden tukemien toimijoiden pääsystä yritysten tietoverkkoihin ja mobiililaitteisiin valvontaa ja seurantaa varten. Nämä riskejä lieventävät toimenpiteet perustuvat CISA:n Project Upskill -projektiin. CISA:n kyberpuolustuksen yhteistyöelimen (JCDC) projektissa kehitetyt ohjeet auttavat ei-teknisiä käyttäjiä parantamaan digitaalista turvallisuuttaan. Yksityiskohtaista ohjeistusta seuraavien suositusten noudattamiseen (englanniksi): Project Upskill.

- **Rajoita julkisesti saatavilla olevan tiedon näkyvyyttä.**
    - **Noudata varovaisuutta sosiaalisessa mediassa** ja verkossa. Harkitse, mitä tietoja lisäät julkisille alustoille.
    - **Kannusta rajoittamaan ystävien ja perheen kesken jaettavia tietoja** suojauksena mahdollista väärinkäyttöä vastaan.
- **Varmista yhteystiedot ja tiedosta käyttäjän manipulointi.** Ymmärrys oman toimialasi ja itsesi kannalta relevanteista uhkista ja toimista on olennaista henkilökohtaisen ja organisaation kyberturvallisuuden lisäämiseksi. Luo mahdollisten uhkien tarkistuslista, jossa huomioidaan työhösi, kiinnostuksen kohteisiisi ja organisaatioihisi liittyvät uniikit riskit. Tämä voi sisältää toimialakohtaisia kyberuhkia, sääntelykysymyksiä ja toteutuneita hyökkäyksiä.
    - **Varmista sosiaalisen median kontaktien henkilöllisyys** lieventääksesi väärennettyjen profiilien ja käyttäjän manipuloinnin riskejä.
    - **Varo yrityksiä esiintyä vääränä henkilönä**, etenkin henkilöiltä, jotka väittävät olevansa toimittajia tai vastaavia.
    - **Ole varovainen kun napsautat linkkejä tai liitetiedostoja** sähköposteissa, tekstiviesteissä tai muilla viestintäalustoilla.
    - **Noudata varovaisuutta, kun avaat tuntemattomasta lähteestä tulevia linkkejä tai liitetiedostoja.**
- **Suojaa kaikki viestintä verkkopalveluiden kanssa salausmenetelmien avulla** [Project Upskill, Module 4, Topic 4.0]. Salaus on ensisijaisen tärkeää kaikessa viestinnässä verkkopalveluiden kanssa. Ilman salausta uhkatoimijat voivat hyväksikäyttää salaamattomia

tai epävirallisia kanavia ja asentaa käyttäjälaitteisiin haittaohjelmia, jotka ovat merkittävä riski yksityisyydelle ja turvallisuudelle. Näiden riskien lieventämiseksi käyttäjien tulee suosia verkkosivuilla ja palveluissa HTTPS-yhteyttä, joka salaa käyttäjän laitteen ja verkkosivun palvelimen välillä vaihdettavan tiedon ja siten suojaa sen vihamielisten toimijoiden salakuuntelulta ja muokkaamiselta. Myös salattujen viestisovellusten käyttö lisää turvallisuutta, sillä niiden avulla viestit ja puhelut säilyvät koskemattomina, salaisina ja suojassa luvattomalta käytöltä.

- **Käytä tileillä vahvoja salasanoja ja monivaiheista tunnistautumista** [Project Upskill, Module 2, Topic 2.0, Topic 2.2]
  - **Käytä vahvoja monivaiheisen tunnistautumisen ratkaisuja,** kuten digitaalisia tai laitteistoon perustuvia välineitä tilien turvaamiseen.
- **Valitse sovellukset huolellisesti.**
  - **Käytä luotettavia sovelluskauppoja** välttääksesi haitallisten kolmannen osapuolen sovellusten aiheuttamat uhkat.
  - **Tarkista sovelluksen ja sen kehittäjän tiedot huolellisesti** ennen lataamista. Näin lievennät mahdollisia riskejä jo niiden alkulähteellä.
  - **Tarkasta kolmannen osapuolen sovellukset** ja varmista, että ne vastaavat kyberturvallisuusstandardeja [Project Upskill, Module 1, Topic 1.4].
- **Tarkastele ja rajoita sovellusten oikeuksia säännöllisesti.** Tämä tietojen altistumisen minimoiminen lisää kokonaisturvallisuutta [Project Upskill, Module 1, Topic 1.3].
- **Pidä sovellukset ja käyttöjärjestelmä päivitettynä** [Project Upskill, Module 1, Topic 1.1].
  - **Asenna päivitykset viipymättä** estääksesi uhkatoimijoita hyväksikäyttämästä haavoittuvuuksia.
  - **Salli käyttöjärjestelmän ja sovellusten automaattiset päivitykset** osana ennakoivaa turvallisuuden hallintaa.
- **Harkitse mobiililaitteesi viikoittaista uudelleenkäynnistystä,** joka voi poistaa mahdolliset vakoiluohjelmat. Tietyt mobiililaitteet mahdollistavat ajastetun uudelleenkäynnistyksen, jolloin voit määrätä ajankohdan esimerkiksi päivittäiselle tai viikoittaiselle uudelleenkäynnistykselle.
- **Turvaa selaustavat ja digitaalisen jalanjäljen hallinta.**
  - Käytä iPhone/iPad -laitteilla **yksityisiä Wi-Fi-osoitteita**. Harkitse korkean riskitason ympäristöissä **Sulkutilaa**. (Lisätietoa Sulkutilasta Apple Support - Tietoja Sulkutilasta -verkkosivuilta).
  - **Harkitse selaimen eristämisratkaisuja,** kun teet arkaluontoista tutkimusta verkossa.
  - **Käytä tavanomaista käyttäjätiliä selailuun ja muihin säännöllisiin tehtäviin** [Project Upskill, Module 1, Topic 1.0].

Ohjelmistovalmistajat

CISA kehottaa ohjelmistovalmistajia noudattamaan turvallisen suunnittelun periaatteita: (1) ottamaan vastuun asiakkaan turvallisuudesta, (2) noudattamaan täyttä läpinäkyvyyttä ja vastuullisuutta sekä (3) johtamaan ylhäältä ja tekemään turvallisuuden vaatimat muutokset. Asiakkaiden turvallisuusasemaa voidaan parantaa esimerkiksi seuraavilla toimenpiteillä:

- **Velvoita kaikki salasanoja käyttävät tilit** (esim. palvelu-, pääkäyttäjä- ja verkkotunnustilit) **noudattamaan** NIST:n standardeja. Edellytä työntekijöiltä pitkiä salasanoja. Harkitse myös

edellytätkö säännöllisiä salasanan vaihtoja tai oletussalasanoja, sillä ne voivat heikentää turvallisuutta.

- **Aseta monivaiheinen tunnistus oletukseksi kaikissa tuotteissa**.
- **Tarjoa lokitus ilman lisäkustannusta ja ilmoita asiakkaille** epäilyttävästä tai poikkeavasta käytöksestä heidän tietoverkoissaan.
- **Ota käyttöön huomiota herättävät ilmoitukset, jotta asiakkaat havaitsevat turvattomat konfiguraatiot**, epäilyttävän käytöksen ja haittaohjelmien lataamisen.
- **Edellytä HTTPS-yhteyttä** verkkosivuille.
- **Lisää tiedot turvallisen suunnittelun noudattamisesta yrityksesi taloudellisiin raportteihin.**

Yhteystiedot

Yhdysvallat: Raportoi tämän oppaan tietoihin liittyvästä epäilyttävästä tai rikollisesta toiminnasta:

- CISA:n 24/7-keskukseen sähköpostitse Report@cisa.gov tai puhelimitse (888) 282-0870 tai paikalliseen FBI:n toimipisteeseen. Jos mahdollista, lisää ilmoitukseen seuraavat tiedot: tapahtuman päivämäärä, aika ja sijainti; toiminnan tyyppi; kohteena olleiden henkilöiden lukumäärä; toiminnassa käytetyt laitteet; raportoivan yrityksen tai organisaation nimi; nimetty yhteyspiste.

Australia: Raportoi kyberturvallisuuspoikkeamista ja tarkastele hälytyksiä ja ohjeita osoitteessa cyber.gov.au tai soittamalla 1300 292 371 (1300 CYBER 1).

Kanada: Raportoi poikkeamista sähköpostitse osoitteeseen contact@cyber.gc.ca.

Viro: Raportoi poikkeamista sähköpostitse osoitteeseen cert@cert.ee tai soita numeroon +372 663 0299

Suomi: Ota yhteyttä Kyberturvallisuuskeskukseen sähköpostitse ncsc@ncsc.fi tai raportoi poikkeamasta osoitteessa https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Japani: Raportoi tähän ohjeeseen liittyvistä poikkeamista osoitteessa https://www.kantei.go.jp/jp/forms/nisc_opinion.html (NISC) tai lähetä sähköpostia osoitteeseen info@jpcert.or.jp (JPCERT/CC). Rikollisesta toiminnasta raportoidaan osoitteessa https://www.npa.go.jp/bureau/cyber/soudan.html (NPA).

Yhdistynyt kuningaskunta: Raportoi merkittävästä kyberturvallisuuspoikkeamasta: ncsc.gov.uk/report-an-incident (24/7). Kiireellisessä avuntarpeessa soita numeroon 03000 200 973.

Lisätietoja

CISA:n Project Upskill -verkkosivusto tarjoaa yksityiskohtaisia ohjeita kyberturvallisuusaseman parantamiseen ja uhkatoimijalta vaadittavan ajan ja resurssien kasvattamiseen.

CISA:n Cybersecurity Training & Exercises -verkkosivu sisältää julkisesti saatavilla olevaa kyberturvallisuuskoulutusta.

Lisätietoja poikkeamien tutkinta- ja palautumissuunnitelmista (englanniksi):

- ASD:n ACSC: Preparing for and Responding to Cyber Incidents, Cyber Incident Response Plan - Guidance ja Cyber Incident Response Readiness Checklist
- CISA: Incident Response Plan Basics ja Federal Government Cybersecurity Incident and Vulnerability Response Playbook. (Vaikka ohjeet on suunnattu yhdysvaltalaisille virastoille (FCEB), ne tarjoavat toimintamenettelyjä ja yksityiskohtaisia ohjeita kyberturvallisuuspoikkeamiin ja haavoittuvuuksiin vastaamiseksi.)

Access Now -järjestön Digital Security Helpline ja Amnesty Internationalin Security Lab tarjoavat käytännöllistä tukea ihmisoikeuksien puolustajille ja kansalaisyhteiskunnan jäsenille. Cisco tarjoaa apua sähköpostitse osoitteessa no-spyware@external.cisco.com.

Digitaalisissa hätätapauksissa Access Now -järjestön Digital Security Helpline ja Amnesty Internationalin Security Lab tarjoavat käytännöllistä tukea ihmisoikeuksien puolustajille ja kansalaisyhteiskunnan jäsenille.

Jos uskot joutuneesi haittaohjelman kohteeksi, voit lähettää sähköpostia Ciscolle osoitteeseen no-spyware@external.cisco.com.

Vastuuvapauslauseke

Tämän raportin sisältö esitetään sellaisenaan ainoastaan tiedoksi. Ohjeen laatineet virastot eivät suosi mitään kaupallista tahoa, tuotetta, yritystä tai palvelua, mukaan lukien tässä asiakirjassa mainitut tahot, tuotteet tai palvelut. Mikään viittaus tietyn kaupallisen tahon, tuotteen, prosessin tai palvelun merkkiin, tavaramerkkiin, valmistajaan tai vastaavaan ei merkitse ohjeen laatimien virastojen suosimista tai suositusta.

Kiitokset

Atlantic Council, Authentic8, Cisco, Cloudflare, CrowdStrike, IBM ja Meta osallistuivat oppaan laatimiseen.

LIITE A: VALTIOIDEN TUKEMAT TOIMIJAT

Toimialan raportoinnin perusteella valtioiden tukemia toimia kohdennetaan riskialttiisiin yhteisöihin pääasiassa Venäjän, Kiinan, Iranin ja Pohjois-Korean hallintojen taholta. ** Ajatushautomoiden tutkimuksissa on kuitenkin havaittu, että myös lukuisat muut maat käyttävät digitaalisen rajat ylittävän painostuksen taktiikoita toisinajattelijoiden rankaisemiseen ja hiljentämiseen.

Kansalaisyhteiskunnan järjestöihin toimia kohdistavia ryhmiä ovat muun muassa seuraavat:

- **Velvet Chollima**: Korean demokraattiseen kansantasavaltaan (Pohjois-Korea) yhdistetty ryhmä, joka harjoittaa kybervakoilua. Velvet Cholliman pääasiallisia kohteita ovat Korean niemimaan asioista raportoivat toimittajat ja Itä-Aasian politiikkaan keskittyvät tutkijat kansalaisjärjestöissä, ajatushautomoissa ja akateemisissa laitoksissa.[10]
- **Mustang Panda**: Kiinan kansantasavaltaan yhteydessä oleva ryhmä, joka keskittyy poliittiseen vakoiluun. Ryhmän kohteina ovat kansalaisjärjestöt, uskonnolliset instituutiot, ajatushautomot ja aktivistiryhmät maantieteellisesti laajalla alueella esimerkiksi Yhdysvalloissa, Euroopassa, Taiwanissa, Hongkongissa, Tiibetissä, Myanmarissa, Mongoliassa, Vietnamissa, Afganistanissa, Pakistanissa, Intiassa ja muualla. Ryhmän pääasiallisena tavoitteena on tarkkailla uhrien toimintaa yksityiskohtaisesti ja tarkoituksella tahrata ja loukata uhrien mainetta. [11] Mustang Pandan käyttämät taktiikat korostavat sen kykyä suorittaa kohdistettuja pitkäkestoisia poliittisia vakoilukampanjoita.
- **Charming Kitten**: Iranin hallintoon liitetty ryhmä, jonka erityiskohteena ovat poliittiset toisinajattelijat, ihmisoikeusjärjestöt, mediatoimijat ja Iranin tutkimukseen keskittyvät tutkijat, joista kerätään tietoa kybervakoilun avulla. Iranilaisten kyberuhkatoimijoiden seurantaan erikoistuneen CERFTA:n (Computer Emergency Response Team) mukaan Charming Kittenin on havaittu kohdistaneen toimiaan yksilöihin, tutkijoihin, toimittajiin, aktivisteihin ja ajatushautomoihin sekä sotilaalliseen ja julkiseen sektoriin Yhdysvalloissa, Euroopassa ja Lähi-Idässä jopa vuodesta 2014 alkaen.[12] IBM X-Force dokumentoi Charming Kittenin päässeen käsiksi lukuisiin uhreihin Iranin uudistusmielisessä liikkeessä elokuun 2020 ja toukokuun 2021 välisenä aikana. Kampanjan strategisena tavoitteena oli soluttautua henkilökohtaisille sähköpostitileille ja sosiaalisen media tileille osana valvontatavoitteita ennen Iranin presidentinvaaleja kesäkuussa 2021.[13]
- **Earth Empusa**: Kiinan kansantasavallan tukema ryhmä, joka keskittyy tarkkailemaan aktivisteja, toimittajia ja toisinajattelijoita etenkin ulkomailla asuvien uiguurien keskuudessa esimerkiksi Turkissa, Kazakstanissa, Yhdysvalloissa, Syyriassa ja Australiassa. [14]
- **Syrian Electronic Army (SEA) tai APT-C-27**: Ryhmä, joka kohdistaa toimiaan humanitaarisiin järjestöihin, toimittajiin ja toisinajattelijoihin, etenkin oppositiota tukevaan Syyrian vapautusarmeijaan liittyen.[15]

** Toimiala ja viranomaiset seuraavat toiminnan esiintymistä erilaisin analyyttisin metodein. Tietystä toimijoiden ryhmästä tuleva toiminta tunnistetaan nimeämällä kyseinen ryhmä. Joillain ryhmillä on useita nimiä tai ne ovat osittain päällekkäisiä, koska eri järjestöt seuraavat niiden toimintaa itsenäisesti. Kehittynyt jatkuva uhka (APT) viittaa usein hyvin resursoituihin valtioiden tukemiin ryhmiin. Ne harjoittavat edistynyttä toimintaa, jonka tavoitteena on usein pitkäkestoinen tietoverkkoon/järjestelmään tunkeutuminen. Lisätietoa CISA:n verkkosivuilla valtiollisista kybertoimijoista ja osoitteessa attack.mitre.org/groups (englanniksi).

LIITE B: VALTIOIDEN TUKEMIEN TOIMIJOIDEN TAKTIIKAT JA TEKNIIKAT

Ohjeen laatineiden virastojen mielestä haitallisten kybertoimijoiden käytöksen ymmärtäminen on usein ensimmäinen askel tietoverkkojen ja tietojen turvaamiseen. Hyvin resursoiduissa organisaatioissa tämä ymmärrys määrittää sen, miten hyvin tietoverkkojen suojaajat onnistuvat haitallisten kybertoimintojen havaitsemisessa ja estämisessä. Vaikka kansalaisyhteiskunnan järjestöiltä voi puuttua sisäinen tietoverkkoa puolustava henkilöstö, haitallisten toimijoiden ymmärtäminen mahdollistaa tietoon perustuvat kyberturvallisuustoimien resursointipäätökset valtioiden tukemaa toimintaa vastaan.

Tässä liitteessä luodaan yleiskatsaus kybertoimintaan, jonka avulla toimijat keräävät tietoa tulevien toimien tukemiseksi ja pääsevät sisälle yritysten tietoverkkoihin tai mobiililaitteisiin valvontaa ja seurantaa varten tai oppimaan lisää kohteen tavoitteista, kiinnostuksen kohteista ja yhteystiedoista. Toimintaa kartoitetaan maailmanlaajuiseen haitallisen kybertoiminnan tietokantaan eli MITRE ATT&CK -viitekehykseen, jossa toiminta luokitellaan taktiikoihin ja tekniikoihin††:

- **Taktiikat** vastaa kysymyksen ”miksi”, eli kuvaa haitallisen kybertoimijan tekojen tavoitteet, päämäärät ja motiivit.
- **Tekniikat** vastaa kysymykseen ”miten”, eli millä keinoin vihollinen saavuttaa taktisen tavoitteensa.

MITRE ATT&CK on jaettu kolmeen teknologia-alueeseen eli ekosysteemiin, jossa toimijat toimivat: Yritysorganisaatiot (Enterprise), Mobiili Mobile ja Yritysorganisaatiot ja Teollisuusautomaatiojärjestelmät Industrial Control Systems.‡‡ Tässä liitteessä luodaan yleiskatsaus kansalaisyhteiskunnan järjestöjä kohtaan käytettävistä taktiikoista ja tekniikoista viitekehyksissä Enterprise ja Mobile, versio 14.

Yritysorganisaatiot (Enterprise)

Taktiikka: Tiedustelu (Reconnaissance) [TA0043]

Määritelmä: Kybertoimijat keräävät tietoa tulevia operaatioita varten.

Tunnettujen tiedustelutekniikoiden kuvaus: Valtioiden tukemat toimijat keräävät usein tietoa avoimen lähdekoodin tutkimuksen avulla, ja monien kansalaisyhteiskunnan järjestöjen ja henkilökunnan luonnostaan julkinen luonne altistaa ne suuremmille riskeille. Kansalaisyhteiskunnan järjestöt ja yksilöt ovat usein hyvin näkyvillä verkossa yritysten verkkosivujen, sosiaalisen median vaikuttamistyön, geopoliittisten julkaisujen ja tiedotteiden kautta. Tämän tiedon avulla valtioiden tukemat toimijat:

- arvioivat tietojen vaarantumisen jälkeisten tavoitteiden laajuutta ja priorisointia
- tunnistavat kohteita, myös yksilöitä, mahdollisille tietojenkalastelukampanjoille ja
- keräävät laite- ja tietoverkkotietoa (kuten IP-osoitteita ja käyttöjärjestelmiä).

Uhkatoimijat käyttävät myös tietojenkalastelua, eräänlaista käyttäjän manipulointia, varastaakseen kirjautumistietoja tietoverkkoon tunkeutumiseksi. Uhkatoimijat esittävät näissä tapauksissa

†† Haitalliseen käytökseen viitataan kyberyhteisössä yleisesti termeillä taktiikat, tekniikat ja menetelmät (TTP).

‡‡ Lisätietoja osoitteesta attack.mitre.org ja oppaasta Best Practices for MITRE ATT&CK Mapping (englanniksi).

luotettavia lähteitä (esim. kollegoja, tuttavia tai organisaatioita) ja houkuttelevat uhreja luovuttamaan kirjautumistietonsa. Tämä tapahtuu usein uhkatoimijan hallussa olevilla sivuilla.

Valtioiden tukemat toimijat käyttävät huomattavasti aikaa ja resursseja identiteettien luomiseen tietojenkalastelua varten, ja yritykset ovat huolellisesti räätälöityjä (kohdennettu verkkourkinta tai ”spearphishing”). Vaikka sähköposti on yleisin menetelmä, uhkatoimijat muokkaavat taktiikoitaan erityisen riskialttiiden yhteisöjen suosimien viestintätapojen perusteella ja hyödyntävät tekstiviestejä, sosiaalisen median alustoja ja erilaisia tutkimukseen ja vaikuttamistyöhön käytettäviä digitaalisia kanavia.

Esimerkki – Velvet Chollima: Velvet Chollima suorittaa tiedustelua kerätäkseen tietoa kohteen tavoitteista, kiinnostuksen kohteista ja ammatillisista yhteyksistä. Osana tiedusteluaan Velvet Chollima on huijannut käyttäjiä antamaan kirjautumistietonsa valesivustolla, joka muistuttaa Googlen kirjautumissivua. Ryhmä sai uhrin kirjautumistiedot, joiden avulla se saattoi tehdä jatkotoimenpiteitä.

MITRE ATT&CK -kartoitus: Taulukko 1 sisältää MITRE ATT&CK Enterprise -viitekehyksen tunnettuja tiedustelutekniikoita.

Taulukko 1: MITRE ATT&CK -tiedustelutekniikoita

Tekniikan nimitys	Tunniste	Kuvaus
Tietojen kerääminen kohdeorganisaatiosta	T1591	Haitalliset toimijat keräävät tietoa kohdeorganisaatiosta (tai kohdeyksilön organisaatiosta) tulevia operaatioita varten.
Julkisten verkkosivujen/verkkotunnusten tutkiminen	T1593	Haitalliset toimijat etsivät verkkosivuilta ja/tai verkkotunnuksilta tietoja kohteesta tulevia operaatioita varten.
Julkisten verkkosivujen/verkkotunnusten tutkiminen: Sosiaalinen media	T1593.001	Haitalliset toimijat etsivät sosiaalisesta mediasta tietoja kohteesta tulevia operaatioita varten.
Tietojen kerääminen kohdeyksilöstä	T1589	Haitalliset toimijat keräävät tietoa kohdeyksilöstä tai kohdeorganisaation henkilöstöstä tulevia operaatioita varten. Henkilöllisyyttä koskevat tiedot voivat sisältää erilaisia tietoja, kuten henkilötietoja (esim. työntekijän nimet, sähköpostiosoitteet) sekä arkaluontoisia tietoja, kuten kirjautumistietoja.
Tietojen kerääminen kohdeisännästä	T1592	Haitalliset toimijat keräävät tietoa kohteen isännistä (laitteet, tietokoneet, palvelimet) tulevaa kohdennusta varten. Isäntätieto voi sisältää erilaisia tietoja, kuten hallinnollisia tietoja (esim. määrätyt IP-osoitteet) sekä konfiguraation yksityiskohtia (käyttöjärjestelmä).

Tekniikan nimitys	Tunniste	Kuvaus
Tietojen kerääminen kohdetietoverkosta	T1590	Haitalliset toimijat keräävät tietoa uhrin tietoverkoista tulevaa kohdennusta varten. Tietoverkkotieto voi sisältää erilaisia tietoja, kuten hallinnollisia tietoja (esim. IP-osoitteet, verkkotunnisteet) sekä topologian ja toiminnan yksityiskohtia.
Tietojenkalastelu	T1598	Haitalliset toimijat lähettävät tietojenkalasteluviestejä saadakseen arkaluontoista tietoa (esim. kirjautumistietoja) tulevia operaatioita varten.

Taktiikka: Jalansijan saavuttaminen (Initial Access) [TA0001]

Määritelmä: Jalansijan saavuttaminen viittaa haitallisten kybertoimijoiden yrityksiin tunkeutua kohdeverkkoon.

Tunnettujen jalansijan saavuttamisen tekniikoiden kuvaus: APT-toimijat käyttävät tietojenkalastelun avulla saatuja kirjautumistietoja (katso kohta Tiedustelu) päästäkseen sisälle tietoverkkoihin.

APT-toimijat hyödyntävät jalansijan saavuttamisessa myös haittaohjelmiin perustuvaa tietojenkalastelua. Haittaohjelmin perustuvassa tietojenkalastelussa haitalliset toimijat esiintyvät luotettavina lähteinä ja houkuttelevat uhrin avaamaan haitallisen hyperlinkin tai sähköpostin liitetiedoston, joka suorittaa haittaohjelmaa isäntäjärjestelmissä. Käynnistetty haittaohjelma mahdollistaa tietovarkauden, tarkkailun tai kehittyneen kybertunkeutumisen. **Huomautus:** Tietojenkalastelua helpottavat usein ohjelmistojen tunnetut heikkoudet, joita toimijat käyttävät hyväkseen haittaohjelmien hyötykuormien siirtämisessä.

Esimerkkejä: Iraniin, Kiinaan, Pohjois-Koreaan ja Venäjään yhdistetyt APT-ryhmät käyttävät kohdennettuja verkkourkintasähköposteja osana laajempia riskialttiisiin yhteisöihin kohdistuvia kampanjoita. Ryhmät hyödyntävät räätälöityjä ja hyvin vakuuttavia viestejä, joilla käyttäjiä houkutellaan avaamaan linkkejä tai liitetiedostoja.

Velvet Chollima: Velvet Cholliman uhkatoimijoiden on havaittu esiintyvän haastattelua pyytävänä toimittajana tai kyselytutkimukseen osallistujia hakevana tutkijana. Velvet Chollima rakentaa ensin luottamusta alustavien sähköpostien avulla ja lisää taktisesti haitallisia elementtejä myöhempiin viesteihin, yleensä petollisten linkkien tai liitetiedostojen muodossa. Näiden linkkien takana on usein haittaohjelmia, jotka tarjoavat Velvet Chollimalle luvattoman pääsyn uhrin tietokoneelle ja mahdollistavat uhrin viestinnän tarkkailun.

Velvet Chollima on lisäksi onnistunut säätämään automaattisen edelleenlähetyksen uhrin sähköpostitilille, millä se varmistaa viestinnän tarkkailun jatkuvuuden, vaikka suora pääsy tilille katoaisi.

Velvet Cholliman kohdennettu verkkourkinta on osa hyvin hienostunutta ja kohdennettua kybervakoilustrategiaa, jossa hyödynnetään käyttäjän

manipulointia ja haitallisia hyötykuormia arvokkaisiin kohteisiin tunkeutumiseksi ja niiden viestinnän valvomiseksi.

Mustang Panda: Ryhmä suosii tunkeutumisen vektorina kohdennettuja verkkourkintasähköposteja, joiden kautta se levittää troijalaisia. Ne mahdollistavat kohteen tietokoneen etähallinnan ja tämän toiminnan kattavan tarkkailun. Mustang Panda käyttää strategisia taktiikoita houkutellakseen kohteita napsauttamaan linkkejä tai liitetiedostoja, jotka usein viittaavat ajankohtaisiin tapahtumiin ja sisältävät haitallisia versioita aidoista tai varastetuista asiakirjoista. Esimerkiksi tammikuussa 2022 eurooppalaisille kohteille lähetyt sähköpostit sisälsivät valheellisena liitteenä ihmisoikeuksia käsittelevän Euroopan komission raportin ja linkin Euroopan unionin tiedotteeseen.

Jalansijan saavutettuaan Mustang Panda suorittaa pitkäkestoista salaista tarkkailua kehittyneiden tekniikoiden avulla. Ryhmä osoitti useissa tapauksissa kykynsä valvoa ja varastaa tietoa pitkän ajan kuluessa sekä toimia huomaamatta organisaation tietoverkossa.

Charming Kitten: Charming Kitten toteuttaa kehittyneitä käyttäjän manipulointitoimia erilaisilla verkkoviestintäalustoilla. Tämän APT-ryhmän strategiana on omaksua esimerkiksi toimittajan tai kansalaisjärjestötoimijan rooli ja hankkia kohteiden luottamus petollisten keskusteluiden avulla ennen haitallisten tiedostojen tai linkkien käyttöönottoa. Toukokuussa 2020 IBM X-Force löysi 40 gigatavua Charming Kittenin koulutusvideoita, jotka paljastivat tietoja ryhmän menetelmistä varastaa tietoa suosituilta sähköpostialustoilta.

MITRE ATT&CK Enterprise -kartoitus: Taulukko 2 sisältää MITRE ATT&CK -viitekehyksen jalansijan saavuttamisen tekniikoita.

Taulukko 2: MITRE ATT&CK Enterprise: Jalansijan saavuttamisen tekniikat

Tekniikan nimitys	Tunniste	Käyttötarkoitus
Tietojenkalastelu	T1566	Haitalliset toimijat lähettävät tietojenkalasteluviestejä päästäkseen sisälle uhrin järjestelmiin. Viestien tuloksena ajetaan koodia tai ladataan haittaohjelmia uhrin järjestelmiin.
Tietojenkalastelu: Kohdennettu verkkourkintaliite	T1566.001	Haitalliset toimijat lähettävät haitallisen liitetiedoston sisältäviä kohdennettuja verkkourkintaviestejä päästäkseen sisälle uhrin järjestelmiin.
Tietojenkalastelu: Kohdennettu verkkourkintalinkki	T1566.002	Haitalliset toimijat lähettävät haitallisen linkin sisältäviä kohdennettuja verkkourkintaviestejä päästäkseen sisälle uhrin järjestelmiin. Linkit johtavat haittaohjelman lataamiseen uhrin järjestelmään yleensä hyödyntäen käyttäjän

		manipulointia, joka rohkaisee vastaanottajia napsauttamaan tai kopioimaan URL:n (tämä edellyttää tekniikkaa käyttäjän ohjelmakoodin suorittaminen (User Execution) [T1204]).

Mobiili (Mobile)

Taktiikka: jalansijan saavuttaminen (Initial Access) [TA0027], sisäinen kartoitus (Discovery) [TA0032], tiedon keruu (Collection) [TA0035] komentokanava (Command and Control) [TA0037]

Määritelmät: Jalansijan saavuttaminen viittaa haitallisten kybertoimijoiden yrityksiin tunkeutua kohteena olevaan mobiililaitteeseen. Sisäinen kartoitus tapahtuu, kun toimijat pyrkivät saamaan laitetta koskevia tietoja toimiensa tueksi. Tiedon keruu tapahtuu, kun toimijat pyrkivät keräämään laitteen sisältämiä tietoja. Komentokanava tarkoittaa toimijoiden viestintää vaarantuneiden laitteiden kanssa niiden hallitsemiseksi.

Tunnettujen tekniikoiden kuvaus: Toimijat pyrkivät tunkeutumaan laitteille tietojenkalastelun avulla, usein tekstiviestien välityksellä. Ne käyttävät myös troijalaisia sovelluksia. Käyttäjät lataavat näennäisesti aitoja sovelluksia, jotka kuitenkin sisältävät haitallisia ohjelmistoja, joiden avulla toimijat pääsevät käsiksi arkaluontoisiin tietoihin, kuten puhelulokeihin ja paikannustietoihin, ja voivat hallita käyttäjän laitetta.

Päästyään sisälle laitteisiin toimijat asentavat niille usein vakoiluohjelmia, kuten Pegasus ja Intellexa. Vakoiluohjelma on työkalu, joka mahdollistaa kattavan valvonnan, kuten sijainnin seurannan, kuvien ja äänen kaappauksen sekä pääsyn henkilökohtaisiin tiedostoihin ja viesteihin.

Esimerkkejä: Seuraavissa esimerkeissä esitetään, miten valtioiden tukemat toimijat käyttävät troijalaisia ja vakoiluohjelmia kampanjoissaan.

Earth Empusa: Meta raportoi vuonna 2021, että Earth Empusa loi huijaussivustoja, jotka muistuttivat kolmannen osapuolen Android-sovelluskauppoja. Näillä valealustoilla tarjottiin uiguureille (turkkilaissukuinen etninen ryhmä, joka on lähtöisin ja kulttuurisesti keskisen ja itäisen Kiinan alueelta) suunnattuja sovelluksia, kuten näppäimistö-, rukous ja sanakirjasovellus.

TrendMicron analyysissa paljastui, että näiden sovellusten lataaminen saastutti käyttäjän laitteen haittaohjelmilla. Earth Empusan järjestämän haittaohjelmiston tavoitteena oli kerätä erilaista arkaluontoista tietoa, kuten paikannustietoa, soittolokeja ja tekstiviestejä. Haittaohjelma tarjosi lisäksi luvattoman pääsyn laitteen kameraan, mikrofoniin ja kuvankaappauksiin, mikä on todiste ryhmän kehittyneistä ja perusteellisista valvontatekniikoista.

APT-C-27: Yksilöiden suojauksen murtamiseksi APT-C-27 loi kekseliäitä haittasovelluksia, mukaan lukien sovelluksen nimeltä VPN Secure, sekä valeversioita suosituista viestintäalustoista, kuten Telegramista ja syyrialaisesta uutissovelluksesta. Näennäisesti vaarattomien sovellusten

strateginen käyttö heijastelee APT-C-27:n kehittynyttä lähestymistapaa kohdeyksilöiden turvallisuuden ja yksityisyyden heikentämiseen.

APT-C-27 suoritti myös toisen kampanjan, jonka kohteena olivat Syyrian vapautusarmeijan liittolaiset ja entinen sotilashenkilöstö. Käyttäjän manipuloinnin avulla ryhmä huijasi yksilöitä avaamaan linkkejä, jotka johtivat suosittuja palveluita, kuten Telegramia ja Facebookia, matkiville petollisille verkkosivuille.

MITRE ATT&CK Mobile -kartoitus: Taulukko 3– 6 sisältää MITRE ATT&CK Mobile -viitekehyksen tekniikoita.

Taulukko 3: MITRE ATT&CK Mobile: Jalansijan saavuttamisen tekniikat

Tekniikan nimitys	Tunniste	Kuvaus
Tietojenkalastelu	T1660	Haitalliset toimijat lähettävät haitallista sisältöä päästäkseen sisälle uhrin laitteisiin.

Taulukko 4: MITRE ATT&CK Mobile: Sisäisen kartoituksen tekniikat

Tekniikan nimitys	Tunniste	Kuvaus
Sijainnin seuranta	T1430	Haitalliset toimijat seuraavat laitteen fyysistä sijaintia.

Taulukko 5: MITRE ATT&CK Mobile: Tiedon keruun tekniikat

Tekniikan nimitys	Tunniste	Kuvaus
Suojatut käyttäjätiedot: Puheluloki	T1636.002	Haitalliset toimijat keräävät puhelulokitietoja.
Suojatut käyttäjätiedot: Tekstiviestit	T1636.004	Haitalliset toimijat keräävät tekstiviestejä.
Videon kaappaus	T1512	Haitalliset toimijat käyttävät laitteen kameroita tiedon keräämiseen kaappaamalla videotallenteita. Haitalliset toimijat voivat myös kaapata kuvia säännöllisin väliajoin videotiedostojen sijasta.
Äänen kaappaus	T1429	Haitalliset käyttäjät kaappaavat ääntä, kuten käyttäjän keskusteluja, äänimaisemaa ja puhelinsoittoja.
Ruutukaappaus	T1513	Haitalliset toimijat käyttävät ruutukaappausta kerätäkseen tietoa kohdelaitteesta, kuten käynnissä olevista sovelluksista, käyttäjätiedoista ja kirjautumistiedoista.

Taulukko 6: MITRE ATT&CK Mobile: Komentokanavatekniikat

Tekniikan nimitys	Tunniste	Käyttötarkoitus

Tunkeutumistyökalujen siirto	T1544	Haitalliset toimijat siirtävät työkaluja, tiedostoja ja haittaohjelmia uhrin laitteeseen ulkoisesta järjestelmästä.

Viitteet

[1] "Microsoft Digital Defense Report 2023", lokakuu 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023. Microsoftin *Digital Defense Report 2023* -raportti kuvaa kehittynyttä jatkuvaa uhkaa (APT) ajatushautomoita, kansalaisjärjestöjä, mediaa ja ihmisoikeusaktivisteja kohtaan Venäjältä (Nobelium, Strontium, Seaborgium), Kiinasta (Nickel, Gadolinium), Pohjois-Koreasta (Osmium) ja Iranista (Phosphorus).
[2]"CrowdStrike Threat Landscape: APTs & Adversary Groups", CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. CrowdStriken Global Threat Landscape -raportin mukaan APT-toimijat Iranista (Charming Kitten), Kiinasta (Phantom Panda, Aquatic Panda) ja Pohjois-Koreasta (Velvet Chollima, Ricochet Chollima) olivat mahdollisia uhkia ajatushautomoille ajanjaksolla 18.8.–16.11.2023.
[3]"CrowdStrike Threat Landscape: APTs & Adversary Groups", CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. CrowdStriken Global Threat Landscape -raportin mukaan APT-toimijat Iranista (Static Kitten, Haywire Kitten, Charming Kitten), Kiinasta (Cascade Panda, Overcast Panda, Aquatic Panda, Emissary Panda), Venäjän federaatiosta (Fancy Bear, Gossamer Bear) ja Pohjois-Koreasta (Velvet Chollima, Ricochet Chollima) olivat mahdollisia uhkia kansalaisjärjestöille ajanjaksolla 18.8.–16.11.2023.
[4]"CrowdStrike Threat Landscape: APTs & Adversary Groups", CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. CrowdStriken Global Threat Landscape -raportin mukaan APT-toimijat Pohjois-Koreasta (Ricochet Chollima) ja Iranista (Charming Kitten) olivat mahdollinen uhka toisinajattelijoille ajanjaksolla 18.8.–16.11.2023.
[5]"CrowdStrike Threat Landscape: APTs & Adversary Groups", CrowdStrike, n.d, https://www.crowdstrike.com/adversaries/. CrowdStriken Global Threat Landscape -raportin mukaan venäläinen APT-toimija (Fancy Bear) oli mahdollinen uhka voittoa tavoittelemattomille järjestöille ajanjaksolla 18.8.–16.11.2023.
[6] "Project Galileo 9th Anniversary", (Cloudflare Radar, 5.6.2023), https://radar.cloudflare.com/reports/project-galileo-9th-anniv.
[7] Cloudflare Radar, "DDoS Attack Trends for 2023 Q2" (Cloudflare Radar, 18.7.2023), https://radar.cloudflare.com/reports/ddos-2023-q2.
[8] Cloudflare Radar, "DDoS Attack Trends for 2023 Q3" (Cloudflare Radar, 26.10.2023), https://radar.cloudflare.com/reports/ddos-2023-q3.
[9] "ENISA Threat Landscape 2023", ENISA, 19.10.2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
[10] CrowdStrike, "Velvet Chollima", crowdstrike.com, 25.2.2023, https://www.crowdstrike.com/adversaries/velvet-chollima/.
[11] "BRONZE PRESIDENT Targets NGOs", Secureworks, n.d., https://www.secureworks.com/research/bronze-president-targets-ngos.
[12] Certfa Lab, "Charming Kitten: 'Can We Have a Meeting?'" Certfa, n.d., https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/.
[13] "ITG18: Operational Security Errors Continue to Plague Sizable Iranian Threat Group", Security Intelligence, 23.8.2023, https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/.
[14] Mike Dvilyanski ja Nathaniel Gleicher, "Taking Action Against Hackers in China", *Meta*, 20.4.2021, https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.
[15] Mike Dvilyanski ja David Agranovich, "Taking Action Against Hackers in Pakistan and Syria", *Meta*, 16.11.2021, https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/amp/.