Rebekka Ritokallio

UKRAINAN JA VENÄJÄN VÄLISEN SODAN KYBER-TAPAHTUMIA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Ritokallio, Rebekka
Ukrainan ja Venäjän välisen sodan kybertapahtumia
Jyväskylä: Jyväskylän yliopisto, 2024, 64 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Venäjä aloitti aseellisen hyökkäyksensä Ukrainaan 24. helmikuuta 2022, minkä jälkeen se on pyrkinyt vaikuttamaan Ukrainaan aseellisten iskujen lisäksi myös kyberhyökkäyksillä. Tässä tutkielmassa käsitellään Ukrainassa havaittuja kybertapahtumia. Päätutkimuskysymyksenä oli selvittää, millaisia kyberhyökkäyksiä havaittiin ennen Ukrainan ja Venäjän välisen sodan alkamista ja sodan ensimmäisinä kuukausina. Toisena tutkimuskysymyksenä oli tunnistaa Venäjän kyberoperaatioissa tapahtuneita muutoksia sodan edetessä. Tutkimus toteutettiin laadullisella sisällönanalyysilla. Ennen aseellista hyökkäystä Venäjä keskittyi tietojenkalasteluun, joka kohdistui Ukrainan lisäksi myös muihin maihin, erityisesti Nato-maihin. Noin vuoden kestäneen tehostetun tietojenkalastelun tarkoituksena oli todennäköisesti valmistella myöhempiä kyberhyökkäyksiä ja kerätä tietoa siitä, miten muut maat reagoisivat Venäjän aseelliseen hyökkäykseen. Noin kuukausi ennen aseellista hyökkäystä Ukrainassa havaittiin tietojenkalastelun lisäksi palvelunestohyökkäyksiä, verkkosivustojen tuhrimishyökkäyksiä ja tietoa tuhoavia haittaohjelmia. Sodan ensimmäisten kuukausien aikana Venäjän kyberoperaatioiden pääpaino oli tietoa tuhoavissa haittaohjelmissa, joita havaittiin Ukrainassa poikkeuksellisen suuri määrä. Tietoa tuhoavien haittaohjelmien kohteena olivat erityisesti Ukrainan valtionhallinto ja kriittinen infrastruktuuri. Sodan ensimmäisten kuukausien jälkeen tietoa tuhoavien haittaohjelmien määrä väheni, mikä todennäköisesti kertoi Venäjän käyttäneen sotaa varten tietojärjestelmiin valmistellut jalansijansa. Sodan alkuhetkistä alkaen Ukrainassa ja Ukrainaa tukevissa maissa on havaittu jatkuvasti palvelunestohyökkäyksiä, joille on annettu poliittisia motiiveja. Hyökkäysten taustalla ovat olleet haktivistiryhmät, joista ainakin osa on todennäköisesti Venäjän valtionhallinnon ohjauksessa. Palvelunestohyökkäykset ovat yksi esimerkki kyber- ja informaatio-operaatioiden yhdistämisestä, jota Venäjä on toteuttanut sodan aikana runsaasti. Sodan edetessä Venäjä on jatkanut tietojenkalastelua Ukrainassa ja Ukrainaa tukevissa maissa. Tiedonhankintaan on kehitetty uusia menetelmiä ja sitä on kohdistettu ajankohtaisten teemojen mukaan. Sodan aikana Venäjä on kehittänyt jatkuvasti uusia hyökkäysmenetelmiä ja -työkaluja, mutta operaatioista voidaan tunnistaa myös historiasta tuttuja piirteitä, kun niitä verrataan Venäjän aikaisempiin kyberoperaatioihin.

Asiasanat: kyberoperaatiot, sodankäynti, Venäjä

ABSTRACT

Ritokallio, Rebekka
Cyber Activity in the Russia-Ukraine War
Jyväskylä: University of Jyväskylä, 2024, 64 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

On 24 February 2022, Russia launched its invasion of Ukraine. After the invasion, it has tried to devastate Ukraine not only with missiles and other physical weapons but also with cyber attacks. This master's thesis describes the most significant cyber attacks observed before the start of the invasion and during the first months of the war. The study also identifies changes in Russia's cyber operations as the war continued. The research was carried out with qualitative content analysis. For about a year before the invasion, Russia focused on phishing attacks targeting Ukraine and other countries, especially Nato countries. The purpose of the intensified intelligence gathering was likely to prepare for future cyber operations and to gather information on how other countries would react to the war between Russia and Ukraine. About a month before the invasion, Ukraine was also targeted with denial-of-service attacks, website defacements, and wiper malware attacks. During the first months of the war, Russia's main focus was on destructive cyber attacks. The targets of the destructive attacks included but were not limited to Ukrainian government and critical infrastructure. After the first months of the war, the number of destructive attacks decreased, indicating that Russian threat actors had used the prepared footholds on targeted systems. Since the beginning of the war, denial-of-service attacks have been targeting Ukraine and countries supporting Ukraine. Hacktivists have taken credit on most of the denial-of-service attacks, but at least some of the hacktivist groups are likely to be supported by the Russian government. Denial-of-service attacks are an example of the combination of cyber and information operations, which Russia has carried out continuously during the war. Until today, Russia has continued spear phishing attacks targeting Ukraine and countries supporting Ukraine. Russia has developed new intelligence gathering methods during the war and its targets have varied based on the relevant information needed at the time. During the war, Russia has developed new attack methods and tools, but it is also possible to recognize old methods from the Russian cyber operations history.

Keywords: cyber operations, warfare, Russia

KUVIOT

SISÄLLYS

1 JOHDANTO

Venäjä aloitti aseellisen hyökkäyksensä Ukrainaan 24. helmikuuta 2022, minkä jälkeen se on suoran aseellisen vaikuttamisen lisäksi pyrkinyt vaikuttamaan Ukrainaan myös kyberhyökkäyksillä. Tässä pro gradu -tutkielmassa käsitellään Ukrainan ja Venäjän välisen sodan kybertapahtumia ja arvioidaan niiden tavoitteita ja vaikutuksia. Tutkielmassa keskitytään kyberoperaatioihin, joiden taustalla uskotaan olevan Venäjän valtionhallinto.

Toistaiseksi kybertapahtumien aktiivisin ajanjakso on ollut juuri ennen Venäjän aseellista hyökkäystä ja välittömästi sen jälkeen. Vaikka aktiivisuus oli korkeimmillaan aseellisen hyökkäyksen alkaessa, Ukraina on ollut jatkuvien kyberhyökkäysten kohteena läpi sodan. Tutkielmassa keskitytään erityisesti aseellisen hyökkäyksen alkamispäivän läheisiin kybertapahtumiin.

Tässä tutkielmassa ei käsitellä kaikkia Ukrainan ja Venäjän välisen sodan kybertapahtumia niiden suuren määrän vuoksi. Ukrainan CERT (CERT-UA) havaitsi vuonna 2022 yhteensä lähes 2200 kybertapahtumaa, joista noin 1100 oli kriittisiä tai korkean prioriteetin tapahtumia (SSSCIP, 2023a). Kybertapahtumien suuren määrän vuoksi tutkielmassa keskitytään vain merkittävimpiin havaintoihin.

Vaikka valtiolliset uhkatoimijat ovat suorittaneet kyberoperaatioita jo pitkään, Ukrainan ja Venäjän välinen sota on ollut ensimmäinen kerta, kun kyberhyökkäykset ovat selkeästi osana sodankäyntiä. Tämän vuoksi Ukrainan ja Venäjän välisen sodan kybertapahtumien tutkiminen ja ymmärtäminen on tärkeää.

Kyseessä ei ole ensimmäinen kerta, kun Venäjä käyttää kyberhyökkäyksiä edistämään valtionhallinnon tavoitteita. Venäjä on toteuttanut laaja-alaisesti erilaisia valtionhallinnon tukemia kyberoperaatioita jo pitkään. Myös Ukraina on ollut jo vuosia Venäjän jatkuvien kyberhyökkäysten kohteena, ja sitä on kutsuttu Venäjän kyberhyökkäysten koelaboratorioksi. Venäjän valtiollisia uhkatoimijoita ja niiden aikaisemmin suorittamia kyberoperaatioita kuvataan tarkemmin tämän työn teoriaosuuksissa.

Tutkimuksella oli yksi päätutkimuskysymys ja yksi täydentävä tutkimuskysymys. Tutkimuksen päätutkimuskysymyksenä oli selvittää, millaisia

kyberhyökkäyksiä havaittiin ennen Ukrainan ja Venäjän välisen sodan alkamista ja sodan ensimmäisinä kuukausina. Toisena tutkimuskysymyksenä oli analysoida, miten kyberoperaatiot ovat muuttuneet sodan aikana. Tutkimuskysymyksiin vastattiin laadullisella sisällönanalyysilla.

Laadullinen sisällönanalyysi toteutettiin kolmessa vaiheessa, jotka olivat valmistelu, analyysi ja raportointi. Valmisteluvaiheessa etsittiin ajankohtaista tutkimusmateriaalia, jota kerättiin pääasiassa tietoturvatalojen ja eri viranomaisten julkaisuista. Analyysivaiheessa kerättyä materiaalia analysoitiin ja ryhmiteltiin siten, että aineistosta löydettiin tutkimuskysymysten kannalta oleellinen tieto. Raportointivaiheessa löydökset kirjoitettiin raporttimuotoon ja kirjallisen analyysin tueksi luotiin kuvioita. Sisällönanalyysin raportointivaiheessa painotettiin päätutkimuskysymystä, eli sotaa ennen ja sen aikana havaittuja kyberhyökkäyksiä.

Pohdinta-osuudessa analysoidaan sodan aikana tapahtuneita muutoksia kyberoperaatioissa. Pohdinta perustuu ensimmäisinä kuukausina havaittuihin kyberhyökkäyksiin ja sisällönanalyysissa löydettyihin muutoksiin toiminnassa.

Tutkielman tuloksena luotiin kokonaisuus, jossa Ukrainan ja Venäjän välisen sodan ensimmäisten kuukausien kybertapahtumia kuvattiin hyökkäystyyppien mukaan ryhmiteltynä. Lisäksi tunnistettiin eri hyökkäystyypeissä tapahtuneita muutoksia sodan aikana.

2 TUTKIMUSKYSYMYKSET, TUTKIMUSMENETELMÄ JA TEOREETTINEN VIITEKEHYS

Tässä luvussa kuvataan tutkielman tutkimuskysymykset, käytetty tutkimusmenetelmä ja tutkimuksen teoreettinen viitekehys. Ensimmäisessä alaluvussa käsitellään tutkimuskysymykset, joihin tutkielmassa vastataan. Toisessa alaluvussa esitellään käytetty tutkimusmenetelmä, joka on laadullinen sisällönanalyysi. Kolmannessa alaluvussa kuvataan kyberuhkatiedustelussa käytetty timanttimalli, joka toimi tutkimuksen teoreettisena viitekehyksenä.

2.1 Tutkimuskysymykset

Tämän tutkielman tavoitteena on kuvata Ukrainan ja Venäjän välisen sodan merkittävimpiä kybertapahtumia, analysoida niiden muodostamia kokonaisuuksia ja tunnistaa kybertapahtumien muutoksia sodan aikana. Tutkielman tutkimuskysymykset ovat:

1) Millaisia kyberhyökkäyksiä havaittiin ennen Ukrainan ja Venäjän välisen sodan alkamista ja sodan ensimmäisinä kuukausina?

2) Miten kyberoperaatiot ovat muuttuneet sodan aikana?

Ensimmäiseen tutkimuskysymys on tutkielman päätutkimuskysymys. Siihen vastatessa luodaan kokonaiskuva Ukrainan ja Venäjän välisen sodan merkittävimmistä kybertapahtumista. Tutkielmassa ei käsitellä jokaista havaittua ja raportoitua kybertapahtumaa, vaan luodaan kokonaiskuva merkittävimmistä hyökkäyksistä.

Toisena tutkimuskysymyksenä on selvittää, miten Ukrainan ja Venäjän välisen sodan kyberoperaatiot ovat muuttuneet sodan aikana. Tavoitteena on tunnistaa, ovatko esimerkiksi kohteet tai hyökkäystavat muuttuneet sodan edetessä.

2.2 Tutkimusmenetelmä

Tutkielmassa käytetty tutkimusmenetelmä on laadullinen sisällönanalyysi. Kyseessä on laadullinen tutkimusmenetelmä, jota tyypillisesti käytetään kuvaamaan tai selittämään tutkittua ilmiöitä (Elo, 2022, s. 216). Kyseinen menetelmä valittiin, koska se soveltui laajan tietoaineiston analysoimiseen, tutkitun ilmiön kuvaamiseen ja tulosten raportointiin. Laadullinen sisällönanalyysi koostuu tyypillisesti seuraavista kokonaisuuksista: valmistelu, analysointi ja raportointi (Elo, 2022, s. 215). Tässä luvussa kuvataan tutkielman näkökulmasta oleelliset sisällönanalyysin vaiheet ja niihin liittyvät kokonaisuudet.

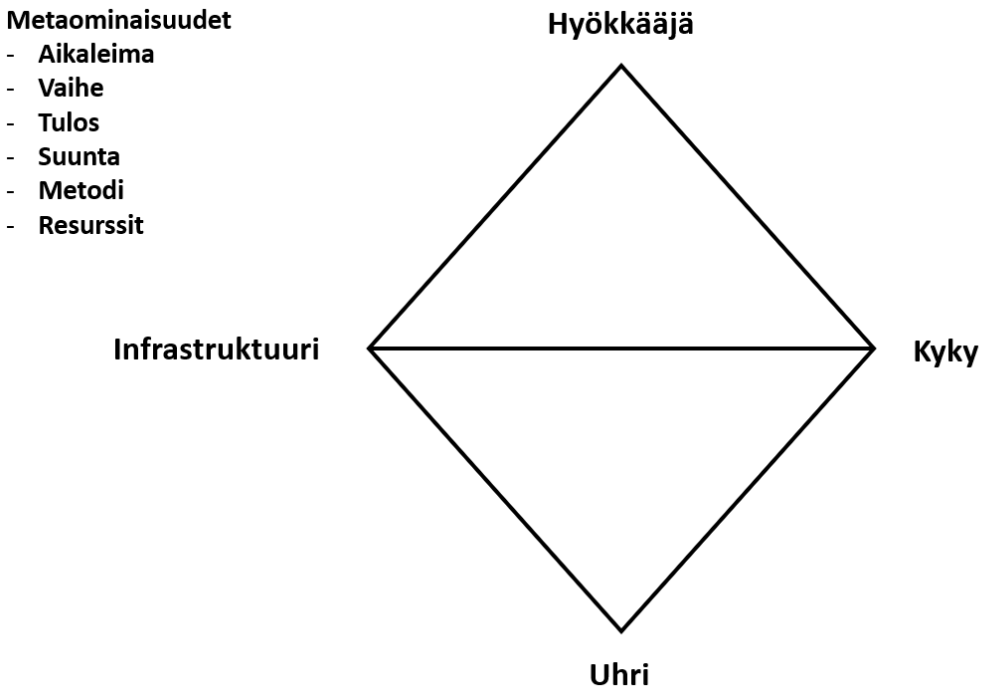
Laadullisen sisällönanalyysin valmisteluvaiheeseen kuului tässä tutkielmassa olennaisten avainsanojen tunnistaminen, mahdollisimman ajankohtaisen tutkimusaineiston kerääminen ja tutkimuskysymysten tarkentaminen. Kaikki edellä mainitut ovat yleisiä toimenpiteitä laadullisen sisällönanalyysin valmisteluvaiheessa (Elo, 2022, s. 219). Ukrainan ja Venäjän sodan aikaisista kybertapahtumista etsittiin tietoa ensisijaisesti tietoturvatalojen ja viranomaisten julkaisemilta raporteilta. Teoriatietoa kybersodankäynnistä ja Venäjän aikaisemmista kyberoperaatioista haettiin edellä mainittujen lisäksi tieteellisistä julkaisuista. Valmisteluvaiheessa tarkennettiin tutkimuskysymyksen ajallista rajausta.

Analyysivaiheessa kerätystä aineistosta etsittiin vastauksia tutkimuskysymyksiin. Samalla aloitettiin myös aineiston ryhmittely ja luokittelu suurempien kokonaisuuksien alle. Suuremmat kokonaisuudet olivat tässä tutkimuksessa kyberhyökkäyksen tyyppi, taustalla oleva uhkatoimija ja kyberhyökkäyksen ajankohta. Kyseessä on aineistolähtöinen analyysi, jonka tavoitteena on oleellisten kokonaisuuksien tunnistaminen ja aineiston tiivistäminen (Elo, 2022, s. 219-220).

Raportointivaiheessa tulokset raportoitiin analysointivaiheessa tunnistettujen kokonaisuuksien mukaan. Koska käsitelty kokonaisuus oli laaja ja sisälsi paljon yksityiskohtia, kirjallisen raportoinnin tukena käytettiin kuvioita selventämään erilaisia asiakokonaisuuksia.

2.3 Teoreettinen viitekehys

Tässä luvussa kuvataan tutkielman teoreettinen viitekehys, joka on kyberuhkatiedustelussa käytetty timanttimalli (engl. Diamond model in Cyber Threat Intelligence). Timanttimalli koostuu neljästä peruselementistä, joita ovat hyökkääjä, kyky, infrastruktuuri ja uhri. Timanttimallin perusideana on, että *hyökkääjä* käyttää sen *kykyjä* käytössään olevan *infrastruktuurin* kautta hyökätäkseen *uhria* vastaan (Caltagirone ym., 2013, s. 11-13). Timanttimallin peruselementit ja metaominaisuudet esitetään kuviossa 1.



KUVIO 1 Timanttimallin neljä peruselementtiä ja metaominaisuudet. Kuvio mukailee Caltagirone ym. (2013, s. 9) luomaa mallia.

Caltagirone ym. (2013, s. 11-13) kuvaavat neljää peruselementtiä seuraavalla tavalla:

1) Hyökkääjä (engl. adversary) – Hyökkääjä on hyökkäyksen takana oleva henkilö tai organisaatio. Hyökkääjä voidaan ymmärtää kahdella tavalla: hyökkääjä voi olla joko hyökkäyksen toteuttaja tai sen tuloksista hyötyvä toimija, joka esimerkiksi ostaa hyökkäyksen teknisesti taitavammalta toimijalta.
2) Kyky (engl. capabilities) – Kyky kuvaa hyökkääjän käyttämiä tekniikoita ja/tai työkaluja. Kyky voi olla esimerkiksi käytetty haittaohjelma (työkalu) tai salasanan murtaminen (tekniikka).
3) Infrastruktuuri (engl. infrastructure) – Infrastruktuuri tarkoittaa hyökkääjän käyttämiä resursseja tai rakenteita, jotka mahdollistavat hyökkäyksen toteuttamisen. Infrastruktuuriin kuuluvat muun muassa hyökkääjän hallussa olevat IP-osoitteet, verkkotunnukset (engl. domains), sähköpostiosoitteet ja laitteet.
4) Uhri (engl. victim) – Uhri on hyökkäyksen kohde, jota vastaan hyökkääjä käyttää kykyjään. Uhri voi olla esimerkiksi henkilö tai organisaatio.

Timanttimallissa on olemassa myös metaominaisuuksia, jotka täydentävät peruselementeistä saatua tietoa. Metaominaisuuksia ovat Caltagirone ym. (2013, s. 15-17) mukaan:

- Aikaleima – Aikaleimat hyökkäyksen alku- ja loppuhetkille. Aikaleimat sisältävät päivämäärän ja kellonajan.
- Vaihe – Hyökkäyksen vaihe. Määritellään, onko kyseessä esimerkiksi kohteen tiedustelu, jalansijan rakentaminen kohdejärjestelmään tai aktiivinen hyökkäystoiminta.
- Tulos – Kuvaillaan hyökkäyksen tuloksia. Voidaan esimerkiksi määritellä, oliko hyökkäys onnistunut tai epäonnistunut. Lisäksi voidaan kuvailla vaikutuksia datan luottamuksellisuuteen, eheyteen ja saatavuuteen.
- Suunta – Hyökkäyksen suunnan määrittäminen. Kuvaillaan, miten hyökkäys on liikkunut kohdejärjestelmässä.
- Metodi – Hyökkäyksessä käytetty menetelmä, esimerkiksi sähköpostilla toteutettu tietojenkalastelu.
- Resurssit – Resurssit, joita hyökkääjä tarvitsee hyökkäyksen toteuttamiseen. Resursseihin kuuluvat muun muassa ohjelmistot, hyökkäyksen toteuttamiseen tarvittavat tiedot ja taidot, informaatio, laitteistot ja taloudellinen pääoma.

Tässä tutkielmassa timanttimallia käytetään teoreettisena viitekehyksenä Ukrainan ja Venäjän välisen sodan kybertapahtumien analysoinnissa. Kybertapahtumista on pyritty löytämään mahdollisimman monta timanttimallissa kuvattua peruselementtiä ja metaominaisuutta, jotta analyysista on saatu mahdollisimman kattava. Kaikkia ominaisuuksia ei voida käsitellä jokaisen tapahtuman kohdalla, koska julkisten tietolähteiden perusteella kaikkien ominaisuuksien tunnistaminen on usein mahdotonta.

3 KESKEISIÄ KÄSITTEITÄ

Tässä luvussa määritellään kybertapahtuman, -hyökkäyksen, -operaation ja -sodankäynnin käsitteet. Luvun tavoitteena on esitellä edellä mainitut käsitteet ja tarkastella niiden yhteyksiä toisiinsa.

3.1 Kybertapahtuma

Kybertapahtumalla (engl. cyber security incident) tarkoitetaan tässä tutkielmassa yleiskäsitettä, joka kattaa sekä kyberhyökkäykset että kyberoperaatiot. Kybertapahtuma kuvaa tilannetta, jossa tiedon luottamuksellisuus (engl. confidentiality), eheys (engl. integrity) tai saatavuus (engl. availability) on uhattuna (NIST, 2020, s. 28). Kybertapahtuma voi vaikuttaa joko yhteen tai useampaan edellä mainittuun osa-alueeseen. Määritelmä pohjautuu CIA-malliin, jota käytetään usein kuvaamaan kyberturvallisuuden uhkia.

Tiedon luottamuksellisuus on vaarantunut, jos tietoon pääsee käsiksi joku, jolla ei pitäisi olla oikeutta tarkastella tietoja. Tiedon saatavuus on uhattuna, jos tietoon ei pääse käsiksi, vaikka sen kuuluisi olla saatavilla. Tiedon eheys on uhattuna, jos tietoa pääsee muokkaamaan ilman asianmukaisia oikeuksia. (ISO/IEC 27000:2018, 2018.)

3.2 Kyberhyökkäys

Laarin ym. (2019, s. 37) määritelmän mukaan kyberhyökkäys on kybertoimintaympäristössä tai sen avulla toteutettu tapahtuma, jossa uhkatoimija pyrkii vahingoittamaan tai käyttämään oikeudettomasti tietoverkkoa, tietojärjestelmää, laitetta tai dataa. Kyberhyökkäykset voivat vaikuttaa kaikkiin kybertoimintaympäristön kerroksiin (Lehto, 2014, s. 171).

Kyberhyökkäys voi alkaa hyvin erilaisin keinoin. Hyökkäys voi saada alkunsa esimerkiksi saastuneesta USB-muistilaitteesta (fyysinen kerros),

haitallisesta sähköpostiviestistä ja käyttäjän manipuloimisesta (käyttäjäkerros) tai suoraan haavoittuvien ohjelmistojen hyväksikäytöstä (looginen kerros) (Laari ym., 2019, s. 12-13).

Kyberhyökkäyksillä voi olla erilaisia vaikutuksia kohteeseen. Kyberhyökkäysten vaikutukset voivat olla häiritseviä, heikentäviä tai tuhoavia, mutta joskus hyökkäykset pyrkivät aiheuttamaan mahdollisimman huomaamattomia muutoksia kohteen toimintaan (Lobel, 2011). Huomaamattomat muutokset järjestelmän toimintaan ovat hyökkääjän kannalta toivottuja esimerkiksi kybervakoilussa, sillä hyökkäyksen paljastuminen voisi keskeyttää tiedonhankinnan kohdejärjestelmästä (Laari ym., 2019, s. 33).

Kyberhyökkäys ei aina ole yksittäinen tapahtuma, vaan se voi olla osana laajempaa kokonaisuutta. Tällaista laajempaa kybertoimintaympäristössä tapahtuvaa toimintojen kokonaisuutta kutsutaan kyberoperaatioksi (Laari ym., 2019, s. 37).

3.3 Kyberoperaatio

Kyberoperaatiolla tarkoitetaan suunnitelmallista toimintojen kokonaisuutta, joka tapahtuu pääosin kybertoimintaympäristössä (Sanastokeskus TSK, 2018, s. 33). Kyberoperaation vaikutukset eivät välttämättä rajoitu kyberympäristöön, vaan toiminnoilla voidaan pyrkiä vaikuttamaan myös fyysiseen maailmaan (Laari ym., 2019, s. 37). Toiminnoilla pyritään joko vaikuttamaan kohteena olevan järjestelmän toimintaan tai keräämään informaatiota (Sanastokeskus TSK, 2018, s. 33).

Kyberoperaatioilla voi olla erilaisia tavoitteita. Kyberoperaatio voi olla puolustuksellinen (kybersuojautumista), hyökkäyksellinen (kybervaikuttamista) tai sillä voidaan pyrkiä tiedusteluun kybertoimintaympäristössä (kybertiedustelua) (Lehto, 2014, s. 170).

Puolustuksellinen kyberoperaatio pyrkii suojaamaan omia tietojärjestelmiä ja laitteita vastustajan vaikuttamiselta. Puolustuksellisessa kyberoperaatiossa voidaan etsiä uhkatoimijaa omista tietojärjestelmistä, rajoittaa sen toimintamahdollisuuksia ja tavoitetilassa poistaa se omasta järjestelmästä (Laari ym., 2019, s. 58). Operaatioon voi kuulua järjestelmien valvontaa, datan analysointia, suojaamismenetelmien kehittämistä ja vastatoimenpiteiden toteuttamista (Lehto, 2014, s. 170).

Hyökkäyksellisessä operaatiossa puolestaan pyritään vaikuttamaan kohdejärjestelmiin, laitteisiin tai niiden kautta fyysiseen maailmaan (Laari ym., 2019, s. 61). Hyökkäyksellisillä operaatioilla voidaan pyrkiä häiritsemään, rajoittamaan tai heikentämään järjestelmien toimintaa tai niiden sisältämän informaation käyttöä (Lehto, 2014, s. 170).

Kybertoimintaympäristöä voidaan käyttää myös tiedusteluun. Valtiolliset toimijat ovat kehittäneet edistyksellisiä ja vaikeasti havaittavia keinoja, joiden avulla ne voivat kerätä informaatiota kohdejärjestelmistä (Laari ym., 2019, s. 33). Tiedustelun kohteena voivat olla itse järjestelmät tai niiden sisältämä informaatio.

Uhkatoimijoita voivat kiinnostaa esimerkiksi järjestelmän sisältämät palvelut, niiden haavoittuvuudet sekä järjestelmien ja verkkojen muodostamat kokonaisuudet (Lehto, 2014, s. 171). Toisaalta tavoitteena voi olla kerätä järjestelmistä sensitiivistä tietoa kuten asiakirjoja, sähköpostiviestejä tai käyttäjätietoja (Laari ym., 2019, s. 33).

Tässä tutkielmassa keskitytään Venäjän valtiollisten uhkatoimijoiden suorittamiin hyökkäyksellisiin kyberoperaatioihin ja tiedusteluun kybertoimintaympäristössä. Tutkielmassa pyritään tunnistamaan kyberoperaatioiden muodostamat kokonaisuudet, jotka lopulta muodostavat kybersodankäynnin.

3.4 Kybersodankäynti

Kybersodankäynnille ei ole olemassa yhtä selkeää määritelmää. Kyseessä on kiistanalainen käsite, sillä se rajaa sodankäynnin ainoastaan yhteen toimintaympäristöön (Sanastokeskus TSK, 2018, s. 30). Perinteisesti sodan katsotaan tapahtuvan kaikissa toimintaympäristöissä: maa-, meri-, ilma-, avaruus-, ja kybertoimintaympäristöissä (Laari ym., 2019, s. 16).

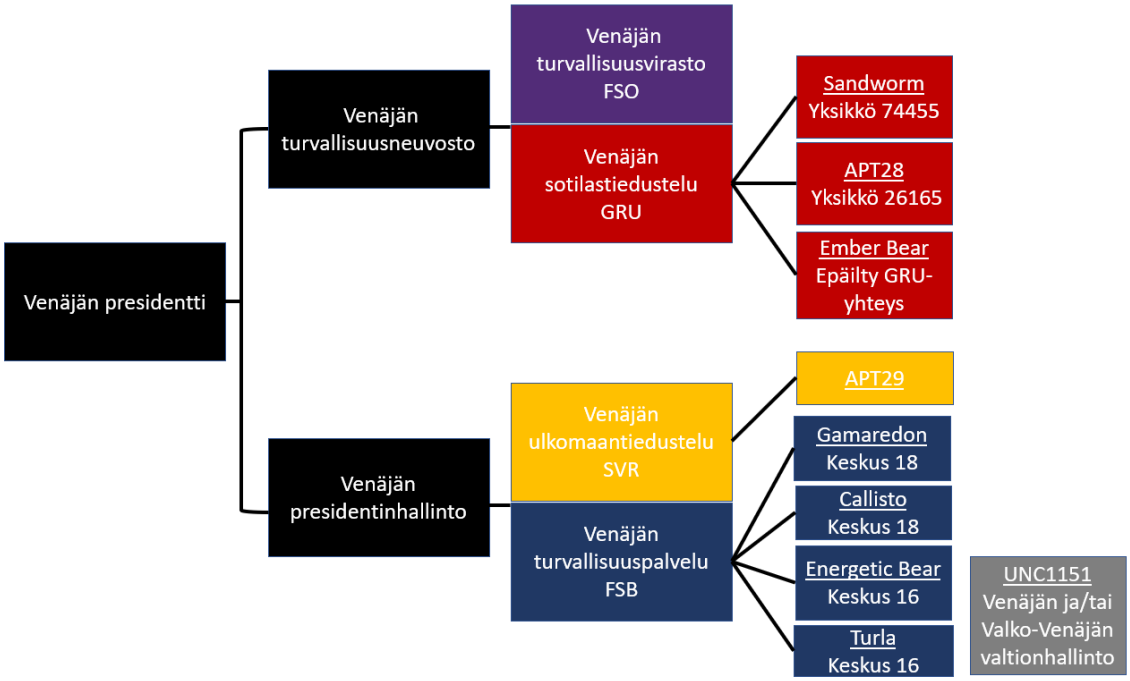
Sanastokeskus TSK:n määritelmän mukaan kybersodankäynti on valtioiden välistä vihamielistä toimintaa, joka tapahtuu tietoverkkojen välityksellä (Sanastokeskus TSK, 2018, s. 30). Kybersodankäynnissä kyberoperaatiot tukevat kokonaisoperaatiota, jonka toteuttamiseen voidaan käyttää eri toimintaympäristöjen keinoja (Lehto, 2014, s. 170).

Tässä tutkielmassa tarkastellaan kybersodankäyntiä osana Ukrainan ja Venäjän välistä sotaa. Tapahtumia tarkastellaan erityisesti siitä näkökulmasta, miten kybersodankäynti on tukenut Venäjän kokonaistavoitteita sodankäynnissä.

4 VENÄJÄN VALTIOLLISIA UHKATOIMIJOITA

Venäjän valtionhallintoon on liitetty useita uhkatoimijoita, jotka ovat suorittaneet kehittyneitä kyberoperaatioita jo pitkään. Tässä luvussa annetaan yleiskuvaus tunnetuimmista uhkatoimijoista ja niiden kohteista, toimintahistoriasta ja tavoitteista.

Ensimmäisenä kuvataan Venäjän sotilastiedustelu GRU:hun liitetyt uhkatoimijat, toisena Venäjän ulkomaantiedustelu SVR:ään yhdistetyt uhkatoimijat ja kolmantena Venäjän turvallisuuspalvelu FSB:hen liitetyt uhkatoimijat. Viimeisenä käsitellään uhkatoimija, jonka takana oleva organisaatio on toistaiseksi epäselvä. Yhteenveto käsiteltävistä uhkatoimijoista esitetään kuviossa 2.



KUVIO 2 Yhteenveto Venäjän valtiollisista uhkatoimijoista.

Kuvioon on koottu tietoa useista eri lähteistä. Lähteet attribuutioihin kuvataan myöhemmin tekstissä. Organisaatiorakenne on luotu mukaillen Euroopan

ulkosuhteiden neuvoston (engl. European Council on Foreign Relations, ECFR) julkaisemaa kaaviota (Galeotti, 2016, s. 9).

4.1 Sandworm

Sandworm tunnetaan myös nimillä UAC-0082 (SSSCIP, 2023a), ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh ja Voodoo Bear (MITRE, 2022). Sandworm on Venäjän sotilastiedustelu GRU:hun liitetty valtiollinen uhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2009 alkaen (CISA ym., 2022, s. 5). Yhdysvaltain oikeusministeriö (Department of Justice, DOJ) on yhdistänyt Sandwormin GRU:n sotilasyksikköön 74455 (DOJ, 2020). Vaikka Sandwormilla uskottiin olevan kytköksiä Venäjän valtionhallintoon jo aiemmin (Holt, 2022), se yhdistettiin julkisesti GRU:hun vasta vuonna 2020 (DOJ, 2020).

Sandwormin käyttämät tekniikat ovat kehittyneitä. Sandworm on tunnettu tuhoavista kyberhyökkäyksistään kriittistä infrastruktuuria ja teollisuuden ohjausjärjestelmiä kohtaan (Microsoft, 2022a, s. 34). Tuhoavien ja häiritsevien kyberhyökkäysten lisäksi uhkatoimija on suorittanut myös vakoilua (CISA ym., 2022, s. 5) ja informaatio-operaatioita (Microsoft, 2022b) kybertoimintaympäristössä. Sandworm on kohdistanut hyökkäyksiään erityisesti kriittisen infrastruktuuriin, valtionhallintoihin ja asevoimiin (CISA ym., 2022, s. 6).

Sandworm on yhdistetty lukuisiin kyberhyökkäyksiin, joiden avulla se on tukenut Venäjän valtionhallinnon tavoitteita yli kymmenen vuoden ajan. Tunnetuimmat Sandwormin suorittamat kyberhyökkäykset ovat kohdistuneet Ukrainan sähkönjakeluun vuosina 2015 ja 2016, joiden seurauksena Ukrainan sähkönjakelussa havaittiin väliaikaisia häiriöitä (CISA ym., 2022, s. 6). Lisäksi Sandworm on tunnettu muun muassa vaalivaikuttamisesta ja laajalle levinneestä NotPetya-hyökkäyksestä (Holt, 2022).

4.2 APT28

APT28 tunnetaan myös nimillä FANCY BEAR, Group 74, IRON TWILIGHT, PawnStorm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, Swallowtail, TG-4127, Threat Group-4127 ja Tsar Team (MITRE, 2022). APT28 on Venäjän sotilastiedustelu GRU:n sotilasyksikköön 26165 liitetty uhkatoimija (NSA ja FBI, 2020, s. 2).

Uhkatoimijan aktiivisuuden alkamisajankohdasta on julkisuudessa vaihtelevia arvioita. Yhdysvaltain kyberturvallisuusviraston (CISA:n) mukaan APT28 on ollut aktiivinen ainakin vuodesta 2004 (CISA ym., 2022, s. 5), mutta esimerkiksi tietoturvayhtiö CrowdStrike arvioi aktiivisuuden alkaneen viimeistään vuonna 2008 (CrowdStrike, 2019). Arviot aktiivisuuden alkamisesta vaihtelevat edellä mainitulla välillä, vuodesta 2004 vuoteen 2008.

APT28:n tyypillisimmät operaatiot kyberympäristössä ovat vakoiluoperaatioita (CISA ym., 2022, s. 5), joissa keräämiään tietoja uhkatoimija voi jatkohyödyntää esimerkiksi informaatiovaikuttamiseen (FireEye, 2017, s. 5). APT28 kohdistaa operaatioitaan erityisesti Yhdysvaltoihin, Eurooppaan ja entisiin Neuvostoliiton maihin (FireEye, 2017, s. 2). Aktiivisuus ei rajoitu ainoastaan näille maantieteellisille alueille, vaan uhkatoimijan on havaittu kohdistavan hyökkäyksiään eri maihin ympäri maapalloa (CISA ym., 2022, s. 5).

APT28 on kohdistanut kyberhyökkäyksiä laajasti eri sektoreille. Microsoft (2022, s. 34) on nimennyt uhkatoimijan ensisijaisiksi kohteiksi eri maiden valtionhallinnot, asevoimat, ajatushautomot ja korkeakoulut. CISA ym. (2022, s. 5) puolestaan ovat maininneet APT28:n ensisijaisiksi kohteiksi eri maiden valtionhallinnot, matkailu- ja majoitussektorin, tutkimuslaitokset, kansalaisjärjestöt ja kriittisen infrastruktuurin.

APT28:n tiedetään tehneen yhteistyötä myös Sandwormin kanssa. APT28 on esimerkiksi hyödyntänyt Sandwormin infrastruktuuria omissa kyberoperaatioissaan (Brady, 2018, s. 5).

Yksi APT28:n tunnetuimmista kyberoperaatioista on vuoden 2016 olympialaisiin ja paralympialaisiin kohdistunut kyberhyökkäys. Syyskuussa 2016 APT28 julkaisi Maailman antidopingtoimiston (Word Anti-Doping Agency WADA:n) tietojärjestelmistä varastamiaan tietoja ja väitti niiden olevan todiste siitä, että yhdysvaltalaiset urheilijat käyttivät dopingia vuoden 2016 olympialaisissa (FireEye, 2017, s. 2). WADA:n (2016) mukaan kaikki APT28:n julkaisemat tiedot eivät vastanneet heidän järjestelmissään olleita tietoja, vaan niitä oli muokattu ennen julkaisua.

4.3 Ember Bear

Ember Bear tunnetaan myös nimillä Saint Bear, UNC2589, UAC-0056, Lorec53, Lorec Bear, Bleeding Bear (MITRE, 2022) ja FROZENVISTA (Google, 2023, s. 23). Ember Bear on Venäjän valtionhallintoon yhdistetty uhkatoimija (Sadowski & Hall, 2022), jonka aktiivisuuden on arvioitu alkaneen vuoden 2021 maaliskuussa (CrowdStrike, 2022). Kyseessä on suhteellisen uusi uhkatoimija, joka aktivoitui näkyvästi Ukrainan ja Venäjän välisen sodan alkuaikoina.

Ember Bearin tavoitteet sopivat GRU:n yleisiin toimintamalleihin, mutta täysin varmaa attribuutiota Venäjän sotilastiedusteluun ei ole tehty (CrowdStrike, 2022). Tietoturvayhtiö CrowdStriken (2022) mukaan uhkatoimijan tekniikat, taktiikat ja proseduurit ovat yhdenmukaisia muiden GRU:n kyberoperaatioiden kanssa, minkä lisäksi hyökkäysten kohteet ja tavoitteet tukevat yhteyttä GRU:hun.

Ember Bear on suorittanut kybervakoilua, informaatio-operaatioita ja tietoa tuhoavia kyberhyökkäyksiä (Sadowski & Hall, 2022; CrowdStrike, 2022). Uhkatoimija on kohdistanut hyökkäyksiään ensisijaisesti Ukrainaan, mutta Ember Bearin suorittamia kyberhyökkäyksiä on havaittu myös Länsi-Euroopassa ja Pohjois-Amerikassa (Sadowski & Hall, 2022).

Kyberhyökkäysten ensisijaisia kohteita ovat olleet valtionhallinnot ja asevoimat (CrowdStrike, 2022). Muita Ember Bearin kohteita ovat olleet lääkeyhtiöt ja finanssialan organisaatiot (Sadowski & Hall, 2022).

Ember Bearin tunnetuimmat operaatiot ovat kohdistuneet Ukrainaan vuoden 2022 alussa. Ember Bear on yhdistetty tietoa tuhoavaan WhisperGate-haittaohjelmaan, verkkosivustojen tuhrimishyökkäyksiin (engl. website defacement) ja kybervakoiluoperaatioihin (CrowdStrike, 2022).

4.4 APT29

APT29 tunnetaan myös nimillä IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear ja CozyDuke (MITRE, 2022). APT29 on Venäjän ulkomaantiedustelu SVR:ään yhdistetty uhkatoimija. Yhdysvaltain, Kanadan ja Yhdistyneen kuningaskunnan valtionhallinnot ovat yhdistäneet APT29:n julkisesti SVR:ään vuonna 2021 (Valkoinen talo, 2021; Global Affairs Canada, 2021; GOV.UK, 2021).

APT29 on ollut aktiivinen uhkatoimija ainakin vuodesta 2008 alkaen (CISA ym., 2022, s. 4). Uhkatoimija on suorittanut aktiivisesti kybervakoilua, jonka kohteena ovat olleet erityisesti Euroopan ja Nato-maiden valtionhallinnot, tutkimuslaitokset ja ajatushautomot (MITRE, 2022). Uhkatoimijan käyttämät tekniikat ovat usein hyvin kehittyneitä, minkä takia uhkatoimijan kybervakoiluoperaatiot voivat pysyä piilossa pitkään (CISA ym., 2022, s. 4).

SolarWinds on yksi tunnetuimmista APT29:n kyberhyökkäyksistä. Kyseessä on erityisen laaja toimitusketjuhyökkäys, joka levisi SolarWinds Orion -ohjelmiston kautta organisaatioihin ympäri maailmaa vuonna 2020 (Valkoinen talo, 2021). Hyökkäyksen yhteydessä APT29 pääsi sisälle muun muassa Yhdysvaltain valtionhallinnon, kriittisen infrastruktuurin ja yksityisen sektorin tietojärjestelmiin (CISA ym., 2022, s. 4). Hyökkäys havaittiin loppuvuodesta 2020, mutta uhkatoimija oli ollut järjestelmässä sisällä jo vuoden 2019 syyskuusta alkaen (Oladimeji & Kerner, 2023).

4.5 Gamaredon

Gamaredon tunnetaan myös nimillä UAC-0010 (SSSCIP, 2023a), IRON TILDEN, Primitive Bear, ACTINIUM, Armageddon, Shuckworm ja DEV-0157 (MITRE, 2022). Gamaredon on Venäjän valtionhallintoon liitetty uhkatoimija, joka on yhdistetty Venäjän turvallisuuspalvelu FSB:n 18. keskukseen (SSU, 2021). Uhkatoimijan aktiivisuuden arvioidaan alkaneen viimeistään vuonna 2013 (Boutin, 2020). Kyseessä on erittäin aktiivinen uhkatoimija, jolla on käytössään poikkeuksellisen laaja infrastruktuuri (Ventura, 2021).

Vaikka Gamaredon on kehittynyt uhkatoimija, se ei käytä toiminnassaan yhtä kehittyneitä tekniikoita kuin useat muut Venäjän valtionhallintoon

yhdistetyt uhkatoimijat (Ventura, 2021). Gamaredonin käyttämät tekniikat ovat usein melko yksinkertaisia, eikä uhkatoimija tyypillisesti pyri pitämään toimintaansa piilossa pitkiä aikoja (SSU, 2021). Uhkatoimijan toimintatapoja on verrattu rikollisryhmän toimintaan (Ventura, 2021).

Gamaredonin käyttämät tekniikat voivat olla yksinkertaisia, mutta uhkatoimijan suorittamien hyökkäysten havaitseminen voi silti olla vaikeaa. Uhkatoimija kehittää toimintamallejaan jatkuvasti tekemällä pieniä muutoksia työkaluihinsa (Boutin, 2020). Jatkuvan kehityksen lisäksi Gamaredonin käytössä oleva laaja infrastruktuuri mahdollistaa nopeat muutokset toimintaan, mikä vaikeuttaa hyökkäysten automaattista tunnistamista esimerkiksi virustorjuntaohjelmistoilla (Ventura, 2021).

Gamaredonin toiminta on kohdistunut erityisesti Ukrainaan jo usean vuoden ajan (Boutin, 2020; Microsoft, 2022a, s. 34). Vaikka aktiivisuutta on havaittu eniten Ukrainassa, Gamaredonin kampanjat eivät rajoitu ainoastaan yhteen maahan. Gamaredonin toteuttamia kyberhyökkäyksiä on havaittu ympäri maailmaa useilla eri sektoreilla, ja uhkatoimijan kohteina ovat olleet muun muassa valtionhallinnot, asevoimat ja lainvalvonta (Microsoft, 2022a, s. 34).

Tyypillinen Gamaredonin suorittama kyberoperaatio on laaja tietojenkalastelukampanja, jonka levitys tapahtuu sähköpostin välityksellä (Boutin, 2020). Usein sähköposti sisältää haitallisen liitetiedoston, jonka avaaminen aiheuttaa haittaohjelman aktivoitumisen (Ventura, 2021).

4.6 Callisto

Callisto tunnetaan myös nimillä COLDRIVER, SEABORGIUM ja TA446 (Malpedia, 2022). Callisto on kehittynyt uhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2015 alkaen (F-Secure, 2017, s. 3). Callisto on yhdistetty FSB:n 18. keskukseen (DOJ, 2023).

Uhkatoimijan päätavoitteena on kybervakoilu (F-Secure, 2017, s. 5; MSTIC, 2022). Aikaisemmin Callisto on kohdistanut tiedonhankintaansa erityisesti Euroopan ja Etelä-Kaukasian maiden ulko- ja turvallisuuspoliittisiin päätöksiin (F-Secure, 2017, s. 5), mutta viime aikoina uhkatoimijan ensisijaisiksi kohteiksi on tunnistettu Nato-maat. Calliston toimintaa on havaittu vuonna 2022 erityisesti Yhdysvalloissa ja Yhdistyneessä kuningaskunnassa, mutta myös Baltiassa, Pohjoismaissa ja Itä-Euroopassa (MSTIC, 2022).

Callisto on kohdistanut hyökkäyksiään erityisesti tiedusteluorganisaatioiden ja asevoimien henkilöstöön sekä ajatushautomoihin (Microsoft, 2022a, s. 34). Kohteiksi on valikoitunut muun muassa entisiä tiedusteluviranomaisia, Venäjäpolitiikan asiantuntijoita sekä ulkomailla asuvia Venäjän kansalaisia (MSTIC, 2022).

Callisto kykenee toteuttamaan uskottavia ja vaikeasti havaittavia tietojenkalasteluoperaatioita (F-Secure, 2017, s. 2). Calliston tyypillinen tietojenkalasteluoperaatio alkaa avointen lähteiden tiedustelulla, jonka aikana keräämiään tietoja uhkatoimia hyödyntää luodessaan uskottavia tietojenkalasteluviestejä.

Uhkatoimija voi esimerkiksi kartoittaa kohteen sosiaalisia verkostoja, mielenkiinnon kohteita ja työhön liittyviä asioita (MSTIC, 2022).

4.7 Energetic Bear

Energetic Bear tunnetaan myös nimillä Dragonfly, TEMP.Isotope, DYMALLOY, Berserk Bear, TG-4192, Crouching Yeti ja IRON LIBERTY (MITRE, 2022). Energetic Bear on Venäjän turvallisuuspalvelu FSB:hen yhdistetty uhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2010 alkaen (MITRE, 2022). Uhkatoimija on liitetty FSB:n 16. keskukseen (CISA ym., 2022, s. 4).

Uhkatoimijan aktiivisuutta on havaittu Euroopassa, Yhdysvalloissa ja Aasiassa (CISA ym., 2022, s. 4). Energetic Bear on kohdistanut hyökkäyksiään erityisesti energiasektoriin, ilmailuun ja puolustusteollisuuteen (Microsoft, 2022a, s. 34). Lisäksi sen kohteena ovat olleet esimerkiksi vesi- ja jätevesijärjestelmät sekä muut kriittisen infrastruktuurin tietojärjestelmät (CISA ym., 2022, s. 4).

Uhkatoimija on ollut erityisen kiinnostunut energiasektorin organisaatioiden toimintatavoista ja toiminnanohjausjärjestelmistä (Secureworks, 2019). Energetic Bear on kerännyt energiasektorin järjestelmistä informaatiota kybervakoilun menetelmillä, minkä lisäksi se on pyrkinyt saamaan pääsyn toiminnanohjausjärjestelmiin (Symantec, 2017). Uhkatoimijalla on todennäköisesti kyky hallita ja sabotoida energiasektorin toiminnanohjausjärjestelmiä (CISA ym., 2022, s. 4).

Energetic Bear on tullut tunnetuksi useista energiasektoriin kohdistuneista kyberhyökkäyksistään. Uhkatoimijan suorittaman kybervakoilun kohteina ovat olleet muun muassa norjalaiset öljy- ja kaasuyhtiöt, minkä lisäksi vastaavia energiasektoriin kohdistettuja hyökkäyksiä on havaittu ainakin Yhdysvalloissa, Kanadassa ja Yhdistyneissä kuningaskunnissa (Secureworks, 2019).

4.8 Turla

Turla tunnetaan myös nimillä IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton ja Venomous Bear (MITRE, 2022). Turla on kehittynyt uhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2014 alkaen (Toulas, 2022). Turla on mahdollisesti aloittanut toimintansa jo vuonna 2004, mutta sen aktiivisuus ainakin kasvoi merkittävästi vuoden 2014 aikoihin (MITRE, 2022). Toukokuussa 2023 Yhdysvaltojen kyber- ja infrastruktuuriturvallisuusvirasto (CISA) attribuoi Turlan julkisesti FSB:n 16. keskukseen (CISA, 2023).

Turla on kohdistanut hyökkäyksiään erityisesti Nato-maihin (CISA ym., 2022, s. 7), mutta uhkatoimijan aktiivisuutta on havaittu myös useissa muissa maissa (MITRE, 2022). Turlan kohteet vaihtelevat, ja sen toteuttamia kyberhyökkäyksiä on havaittu useilla eri sektoreilla (Toulas, 2022). Uhkatoimijan kohteena

ovat olleet ainakin valtionhallinnot, asevoimat, suurlähetystöt sekä koulutus- ja tutkimussektori (MITRE, 2022).

Uhkatoimijalla on käytössään kehittyneitä ja poikkeuksellisia keinoja toteuttaa kyberhyökkäyksiä. Turla on tunnettu kyvystään hyödyntää satelliittiyhteyksiä, joiden avulla se on ylläpitänyt hyökkäystensä komentokanavia (CISA ym., 2022, s. 7). Turla on myös esimerkiksi kaapannut käyttöönsä muiden kehittyneiden uhkatoimijoiden infrastruktuuria, jonka avulla se on toteuttanut kybervakoiluoperaatioita Lähi-idässä (Toulas, 2022). Uhkatoimija hyödyntää operaatioissaan monipuolisesti kehittyneitä haittaohjelmia (CISA ym., 2022, s. 7).

4.9 UNC1151

UNC1151 tunnetaan myös nimellä PUSHCHA (Google, 2023, s. 25). UNC1151 on uhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2016 alkaen (Cardiffin yliopisto, 2023). Uhkatoimija on suorittanut kybertoimintaympäristössä vakoilua (Google, 2023, s. 25) ja lukuisia informaatio-operaatioita (Cardiffin yliopisto, 2023). UNC1151 on kohdistanut operaatioitaan erityisesti Euroopan maihin, muun muassa Ukrainaan, Liettuaan, Latviaan, Puolaan ja Saksaan (Google, 2023, s. 25). Operaatioilla on pyritty ajamaan Venäjän ja Valko-Venäjän valtionhallintojen etuja (Roncone ym., 2021). Toiminnan taustalla uskotaan olevan venäläisiä ja/tai valkovenäläisiä valtionhallinnon tukemia toimijoita (Cardiffin yliopisto, 2023).

Uhkatoimija on keskittynyt erityisesti informaatio-operaatioihin kybertoimintaympäristössä. Toiminta on kehittynyttä, sillä valheellista informaatiota levitetään ensisijaisesti aitojen sivustojen ja käyttäjien kautta. UNC1151 on käyttänyt valheellisen tiedon levittämiseen muun muassa kaapattuja sähköpostitilejä, murrettuja sosiaalisen median käyttäjätunnuksia ja aitoja verkkosivustoja (Cardiffin yliopisto, 2023). Informaatio-operaatioita on suoritettu useilla eri kielillä, ainakin englanniksi, liettuaksi, puolaksi, latviaksi, ukrainaksi, venäjäksi ja saksaksi (Roncone ym., 2021).

UNC1151 on suorittanut kybertoimintaympäristössä myös vakoilua, jonka yhtenä tavoitteena on ollut valmistella edellä mainittuja informaatio-operaatiota (Roncone ym., 2021). Ensisijaisina kohteina ovat olleet puolustussektorin ja ministeriöiden työntekijät (Roncone ym., 2021), joiden kirjautumistunnuksia on pyritty kalastelemaan kohdennetuilla tietojenkalasteluoperaatioilla (Cardiffin yliopisto, 2023). Käyttäjätunnusten avulla uhkatoimija on todennäköisesti saanut haltuunsa arkaluontoista tietoa kohdeorganisaatioista.

UNC1151 tunnetaan parhaiten Ghostwriter-nimisestä informaatiokampanjastaan, jonka on arvioitu alkaneen vuonna 2016 (Cardiffin yliopisto, 2023). Ennen vuoden 2020 elokuuta Ghostwriter-kampanja kohdistui erityisesti Liettuaan, Latviaan ja Puolaan, ja sen keskeisin tavoite oli luoda negatiivista kuvaa Natosta (Roncone ym., 2021). Negatiivista mielikuvaa pyrittiin levittämään julkaisemalla valheellista tietoa muun muassa Naton luomasta sotilaallisesta uhasta ja Natomaiden sotilaiden käytöksestä (Cardiffin yliopisto, 2023). Vuoden 2020

ensimmäisellä vuosipuoliskolla Ghostwriter-kampanjan keskeisenä teemana oli levittää tietoa siitä, miten COVID-19-tauti levisi Nato-maiden sotilaiden kautta (Roncone ym., 2021).

Vuoden 2020 ensimmäisen vuosipuoliskon jälkeen informaatiokampanjan toiminnassa havaittiin selkeä muutos. Elokuussa 2020 Valko-Venäjällä järjestettiin kiistanalaiset vaalit, joiden jälkeen Ghostwriter-kampanja on keskittynyt luomaan negatiivista mielikuvaa Valko-Venäjän oppositiosta (Roncone ym., 2021) sekä Puolan ja Liettuan valtionhallinnoista (Cardiffin yliopisto, 2023). Tavoitteena on ollut todennäköisesti luoda jännitteitä Puolan ja Liettuan välille sekä vastata voimakkaaseen kritiikkiin Valko-Venäjän vaaleja kohtaan (Roncone ym., 2021).

5 VENÄJÄN TOIMINTAHISTORIAA KYBERTOIMINTAYMPÄRISTÖSSÄ

Tässä luvussa kuvataan Venäjän toimintahistoriaa kybertoimintaympäristössä. Luvussa ei kuvata jokaista havaittua kyberhyökkäystä, vaan pyritään antamaan yleiskuva Venäjän valtiollisten uhkatoimijoiden kyvykkyyksistä.

Venäjällä kyberoperaatioita ei nähdä erillisenä sodankäynnin kokonaisuutena, vaan ne ovat yksi osa informaatiosodankäyntiä. Kyberoperaatioiden lisäksi Venäjän informaatiosodankäyntiin kuuluvat elektroninen sodankäynti, informaatio-operaatiot ja psykologiset operaatiot, joiden keinoilla Venäjä pyrkii saamaan hallinnan informaatioympäristöstä (Sadowski & Hall, 2022). Tämän kokonaisuuden ymmärtäminen on tärkeää, jotta voidaan arvioida paremmin Venäjän suorittamien kyberoperaatioiden tavoitteita.

5.1 Viron pronssisoturikiista, 2007

Viron pronssisoturikiista sai alkunsa, kun Virossa päätettiin siirtää Neuvostoaikainen patsas, pronssisoturi, ja sen läheisyyteen haudattuja vainajia pois Tallinnan keskustasta vuonna 2007 (Ruus, 2008). Tapahtumat johtivat siihen, että Venäjä kohdisti Viroon yhteiskunnan toimintaa häiritseviä kyberhyökkäyksiä 22 päivän ajan (Ottis, 2008). Kyseessä oli ensimmäinen kerta, kun toinen valtio kohdisti laajoja, yhteiskunnan toimintaa häiritseviä ja poliittisesti motivoituneita kyberhyökkäyksiä toista maata kohtaan (Ruus, 2008).

Pronssisoturi oli pystytetty Tallinnan keskustaan kuolleiden neuvostosotilaiden hautauspaikalle vuonna 1947 (Ottis, 2008). Muistomerkin läheisyyteen haudatut sotilaat olivat kuolleet toisen maailmansodan aikana, kun he olivat taistelleet valloittaessaan Tallinnaa (Ruus, 2008). Virossa asuville venäläisille patsas symboloi vapauttajaa, kun taas virolaisille patsas edusti sortajaa (Ottis, 2008).

Koska pronssisoturi oli aiheuttanut jännitteitä virolaisten ja Virossa asuvien venäläisten välille edellisten vuosien aikana, patsas päätettiin pitkän julkisen keskustelun jälkeen siirtää pois Tallinnan keskustasta (Ottis, 2008).

Pronssisoturin siirto Tallinnan keskustasta muutaman kilometrin päässä sijaitsevalle sotilaalliselle hautausmaalle toteutettiin 27. huhtikuuta 2007 (Ruus, 2008).

Kyberhyökkäykset alkoivat 27. huhtikuuta 2007, kun Viron tietojärjestelmiin kohdistuneet palvelunestohyökkäykset alkoivat (Ottis, 2008). Palvelunestohyökkäyksiä kohdistettiin ministeriöiden verkkosivustoille, kahteen suureen pankkiin ja useiden poliittisten puolueiden verkkosivustoille (Herzog, 2011). Kohteina olivat myös verkon uutispalvelut, Viron parlamentin käytössä ollut sähköpostipalvelu (Ruus, 2008), poliisin verkkopalvelut ja useiden pienien yritysten verkkosivustot (Ottis, 2008).

Palvelunestohyökkäysten toteutustapa vaihteli merkittävästi. Venäjänkielisillä keskustelupalstoilla kannustettiin yksityishenkilöitä toteuttamaan palvelunestohyökkäyksiä Viroa vastaan, ja niiden toteuttamiseen annettiin tarkkoja ohjeita (Ottis, 2008). Samalla Virosta pyrittiin luomaan negatiivista kuvaa venäläisten keskuudessa. Myöhemmin palvelunestohyökkäyksiä toteutettiin kehittyneemmillä tavoilla, kun hyökkääjät siirtyivät käyttämään laajoja bottiverkkoja (Ruus, 2008).

Palvelunestonhyökkäysten lisäksi hyökkääjät onnistuivat saamaan haltuunsa yhden poliittisen puolueen verkkosivuston, jolle he julkaisivat valheellista informaatiota. Hyökkääjät julkaisivat verkkosivustolle Viron pääministerin nimissä anteeksipyyntökirjeen, jossa pahoiteltiin patsaan siirtämistä (Ruus, 2008).

Hyökkäyksillä oli häiritseviä vaikutuksia Viron yhteiskuntaan. Esimerkiksi osa palvelunestohyökkäysten kohteena olleista pankeista (Ottis, 2008) ja uutispalveluista (Ruus, 2008) joutuivat estämään väliaikaisesti palveluihinsa kaiken verkkoliikenteen Viron ulkopuolelta. Tämän seurauksena Viron ulkopuolella asuvat asiakkaat eivät päässeet käyttämään kyseisiä palveluita. Vaikutuksia oli myös valtionhallintoon, sillä Viron parlamentin sähköpostipalvelu oli poissa käytöstä neljän päivän ajan (Ruus, 2008).

Venäjän valtionhallinto on toistuvasti kieltänyt osallisuutensa kevään 2007 kyberhyökkäyksiin, mutta hyökkäysten aikana Venäjä ei pyrkinyt pysäyttämään tai estämään hyökkäyksiä millään tavalla (Ottis, 2008). Venäjä ei myöskään suostunut tekemään yhteistyötä Viron kanssa kyberhyökkäysten tutkimisessa (Ruus, 2008). Hyökkäyksen taustalla uskotaan olevan venäläisiä toimijoita, mutta julkisissa lähteissä hyökkäyksiä ei ole yhdistetty mihinkään tiettyyn uhkatoimijaan.

Kyberhyökkäykset saivat Viron kehittämään aktiivisesti omaa kyberpuolustustaan. Lisäksi hyökkäykset herättivät laajaa kansainvälistä keskustelua kybertoimintaympäristöön kohdistuvasta vaikuttamisesta (Laari ym., 2019, s. 24).

5.2 Georgian ja Venäjän välinen sota, 2008

Venäjä hyökkäsi aseellisesti Georgiaan 7. elokuuta 2008, mikä aloitti viisi päivää kestäneen sodan maiden välillä. Myös hyökkäystä edeltävä aika oli merkityksellistä, sillä noin kolme viikkoa ennen aseellista hyökkäystä Venäjä aloitti kyberhyökkäysten kohdistamisen Georgian tietojärjestelmiin (Hollis, 2011, s. 2). Kyberhyökkäykset Georgian tietojärjestelmiä kohtaan jatkuivat myös silloin, kun

Venäjä hyökkäsi aseellisesti Etelä-Ossetiaan ja aloitti pommitukset Georgiassa (Recorded Future, 2022, s. 2).

Noin kolme viikkoa ennen Venäjän aseellista hyökkäystä, 19. heinäkuuta 2008, Georgiassa havaittiin useita palvelunestohyökkäyksiä (Kozlowski, 2014, s. 238). Palvelunestohyökkäykset oli toteutettu bottiverkkojen avulla, ja ne onnistuivat häiritsemään Georgian verkkosivujen toimintaa (Hollis, 2011, s. 2). Vastaavia hyökkäyksiä havaittiin myös aseellisen hyökkäyksen alkamisen jälkeen, mutta suuremmassa mittakaavassa (Kozlowski, 2014, s. 238).

Venäjän aseellisen hyökkäyksen alkamisen jälkeen, 8. elokuuta 2008, palvelunestohyökkäyksiä kohdistettiin laaja-alaisesti eri tietojärjestelmiin Georgiassa (Kozlowski, 2014, s. 238). Hyökkäysten kohteena olivat muun muassa uutissivustot, pankit ja valtionhallinnon verkkosivustot (Recorded Future, 2022, s. 2). Verkkosivustojen lisäksi hyökkäykset häiritsivät pankkien ja puhelimien toimintaa (Kozlowski, 2014, s. 239).

Georgiassa havaittiin myös verkkosivustojen tuhrimishyökkäyksiä, kun Georgian parlamentin verkkosivustolle lisättiin kuvia silloisesta Georgian presidentistä Saakashvilistä ja Hitleristä (Kozlowski, 2014, s. 239). Kuvissa he elehtivät samoilla tavoilla, minkä oli tarkoitus luoda mielikuva siitä, että he olivat samanlaisia johtajia.

Kyberhyökkäysten tavoitteena oli edistää Venäjän valtionhallinnon tavoitteita ja tukea Venäjän sotilaallisia operaatioita (Recorded Future, 2022, s. 2). Verkkosivustojen sisällön muuttamisella pyrittiin luomaan väestöön kauhua ja epävarmuutta, kun taas palvelunestohyökkäykset vaikuttivat Georgian valtionhallinnon mahdollisuuksiin kommunikoida sodan tilanteesta maan kansalaisille ja muulle maailmalle (Kozlowski, 2014, s. 239).

Georgiassa ei havaittu kriittisen infrastruktuuriin, esimerkiksi sähkönjakeluun, kohdistuneita kyberhyökkäyksiä. Arvioiden mukaan uhkatoimijoilla olisi ollut kyky häiritä kriittisen infrastruktuurin toimintaa, mutta vaikuttamista ei julkisten lähteiden mukaan havaittu (Kozlowski, 2014, s. 239).

5.3 Ukrainan sähkönjakelu, 2015

Ukrainan sähkönjakelussa havaittiin 23.12.2015 häiriöitä, jotka aiheuttivat katkoksia 225 000 asiakkaan sähkönsaantiin noin kolmen tunnin ajan (Lee, Assante & Conway, 2016). Havaitut sähkökatkot olivat poikkeuksellisia, sillä niiden syynä oli SCADA-toiminnanohjausjärjestelmään (engl. Supervisory Control and Data Acquisition System) kohdistunut kyberhyökkäys (Liang ym., 2016). Kyseessä oli ensimmäinen kerta, kun kyberhyökkäys aiheutti häiriöitä sähkönjakeluun (Lee, Assante & Conway, 2016). Kyberhyökkäys on yhdistetty uhkatoimija Sandwormiin (DOJ, 2020).

Ukrainan sähkönjakelua häirinnyt kyberhyökkäys oli kehittynyt, monivaiheinen ja huolellisesti valmisteltu. Hyökkäys alkoi sähköyhtiöihin kohdistetulla tietojenkalastelulla, mikä mahdollisti haittaohjelmien (BlackEnergy 3 ja KillDisk) levittämisen, käyttäjätunnusten varastamisen ja pääsyn yhtiöiden sisäisiin

verkkoihin (Liang ym., 2016). Tätä seurasi SCADA-järjestelmien etäkäyttö ja tietoa tuhoavien haittaohjelmien aktivointi kohdejärjestelmissä (Lee, Assante & Conway, 2016). Hyökkäyksiä kohdistettiin myös sähköyhtiöiden puhelinpalveluihin, kun niitä häirittiin palvelunestohyökkäyksillä (Liang ym., 2016).

Varsinainen sähkönjakelun katkaiseminen toteutettiin SCADA-järjestelmien etäohjauksella. Hyökkääjä oli saanut kohteena olleisiin SCADA-järjestelmiin etähallinnan, minkä avulla se kykeni ohjaamaan sähköasemien fyysisiä laitteita (Liang ym., 2016). Hyökkääjä häiritsi sähköasemien normaalia toimintaa avaamalla katkaisijat (engl. circuit breakers), mikä katkaisi sähkönjakelun (Lee, Assante & Conway, 2016). Tämän jälkeen tietoa tuhoavat haittaohjelmat aktivoituivat, mikä hidasti tapahtumien selvitystä ja palautumista hyökkäyksestä (Liang ym., 2016).

Kyberhyökkäyksellä oli vaikutuksia kolmen sähköyhtiön toimintaan (Liang ym., 2016). Hyökkääjä pääsi etäkäyttämään ja ohjaamaan manuaalisesti SCADA-toiminnanohjausjärjestelmiä, minkä seurauksena yhteensä 30 sähköasemaa irtosi sähkönjakeluverkosta kolmen tunnin ajaksi (Lee, Assante & Conway, 2016). Puhelinpalveluihin kohdistetut palvelunestohyökkäykset estivät sähköyhtiöiden asiakkaita tekemästä häiriöilmoituksia, mikä vaikeutti tilannekuvan muodostamista (Liang ym., 2016).

Ukrainan valtionhallinto yhdisti hyökkäyksen nopeasti Venäjään (Lee, Assante & Conway, 2016). Hyökkäyksen takana uskotaan olevan Sandworm (Holt, 2022), joka toteutti vastaavaan sähkönjakelua häirinneeseen kyberhyökkäyksen myös noin vuotta myöhemmin, joulukuussa 2016.

5.4 Industroyer, 2016

Noin vuosi edellisen sähkönjakelua häirinneen kyberhyökkäyksen jälkeen Ukrainassa havaittiin jälleen poikkeuksellisia sähkökatkoksia. Osa Kiovan sähköverkosta pimeni noin tunnin ajaksi 17. ja 18.12.2016 välisenä yönä, kun haittaohjelman aktivoitumisen seurauksena alueen sähkönjakelu häiriintyi (Cherepanov & Lipovsky, 2017). Myös tämä sähköverkkoihin kohdistunut kyberoperaatio on yhdistetty uhkatoimija Sandwormiiin (DOJ, 2020).

Hyökkäyksessä käytetty haittaohjelma tunnetaan parhaiten nimellä Industroyer. Haittaohjelma on poikkeuksellinen, sillä kyseessä on ensimmäinen haittaohjelma, joka oli suunniteltu vaikuttamaan suoraan sähköntuotannon toiminnanohjausjärjestelmiin (Lee, Assante & Conway, 2017, s. 4). Vuoden 2015 kyberhyökkäyksessä sähkönjakelua oli häiritty manuaalisesti etäyhteydellä, mutta nyt sähköverkon toimintaa onnistuttiin häiritsemään suoraan haittaohjelmalla.

Sähkökatkoksen aiheutti yhden sähköaseman katkaisijoiden (engl. circuit breakers) avaaminen haittaohjelmalla (Slowik, 2019, s. 3). Katkaisijoiden avaamisen seurauksena sähköasema irtosi sähköverkosta, mikä aiheutti sähköjen katkeamisen osassa Kiovan kaupunkia (Cherepanov & Lipovsky, 2017). Sähköntuotannon häiritsemisen jälkeen aktivoitui tietoa tuhoava haittaohjelma, jonka

tarkoituksena oli poistaa dataa kohdejärjestelmistä ja hidastaa hyökkäyksestä toipumista (Slowik, 2019, s. 3).

Haittaohjelma koostui useista kokonaisuuksista, joista neljä oli rakennettu hyökkäämään tiettyjä tietoliikenneprotokollia (määritelty standardeissa IEC 60870-5-101, IEC 60870-5-104, IEC 61850 ja OPC DA) vastaan (Lee, Assante & Conway, 2017, s. 13–22). Kyseessä ovat pitkään käytössä olleet protokollat, joiden käyttö on alun perin suunniteltu siten, että teollisuuden toiminnanohjausjärjestelmät pysyvät omissa eristetyissä ympäristöissään. Haittaohjelmaa analysoitaessa todettiin, että käytetyillä tekniikoilla voitaisiin häiritä sähkönjakelun lisäksi muita teollisuuden toiminnanohjausjärjestelmiä, esimerkiksi vedenjakelua tai kaasuntuotantoa (Cherepanov & Lipovsky, 2017).

Verrattuna edellisen vuoden sähkökatkoksiin hyökkäys oli toteutettu kehittyneemmillä työkaluilla, mutta sen vaikutukset jäivät merkittävästi pienemmiksi (Slowik, 2019, s. 3). Sähköaseman sähköntuotanto saatiin palautettua normaaliksi noin tunti hyökkäyksen alkamisen jälkeen (Cherepanov & Lipovsky, 2017), kun edellisenä vuonna katkos kesti noin kolme tuntia (Lee, Assante & Conway, 2016). Vuonna 2015 kyberhyökkäys vaikutti noin 225 000 asiakkaan sähkönsaantiin (Lee, Assante & Conway, 2016), mutta vuonna 2016 määrä oli huomattavasti pienempi (Slowik, 2019, s. 3). Huolimatta suhteellisen pienistä vaikutuksista, kyberhyökkäys herätti keskustelua kriittiseen infrastruktuuriin kohdistetuista kyberhyökkäyksistä ja niiden mahdollisista tuhoisista vaikutuksista.

5.5 NotPetya, 2017

Kesäkuun 27. päivänä vuonna 2017 tietoja tuhoava haittaohjelma nimeltä NotPetya alkoi leviämään maailmanlaajuisesti eri organisaatioiden tietojärjestelmissä (Greenberg, 2018). Haittaohjelma oli kohdistettu erityisesti ukrainalaisiin organisaatioihin, mutta se levisi organisaatioiden välisten toimitusketjujen kautta ympäri maapalloa (Crosignani, Macchiavelli & Silva, 2021). Harvinaisen laajalle levinnyt ja vaikutuksiltaan suuri NotPetya on yhdistetty uhkatoimija Sandwormiin (DOJ, 2020).

NotPetya sai nimensä Petya-nimisen kiristyshaittaohjelman mukaan, sillä se muistutti kyseistä haittaohjelmaa huomattavan paljon (Greenberg, 2018). Petya oli kiristyshaittaohjelma, joka oli ollut rikollisten aktiivisessa käytössä vuonna 2016 (Crosignani, Macchiavelli & Silva, 2021). Aluksi vaikutti, että vuoden 2017 hyökkäyksessä oli käytetty Petya-kiristyshaittaohjelman uutta versiota, mutta todellisuudessa NotPetya naamioitiin muistuttamaan kyseistä kiristyshaittaohjelmaa.

Vaikka NotPetya näyttäytyi kiristyshaittaohjelmana, sen motiivina ei ollut taloudellisen hyödyn saaminen. NotPetyan lunnasvaatimukset olivat ainoastaan hämäystä, eikä salausta voinut todellisuudessa purkaa hyökkääjän esittämillä keinoilla (Greenberg, 2018). Haittaohjelman todellisena tarkoituksena oli aiheuttaa mahdollisimman laajaa tuhoa erityisesti ukrainalaisiin organisaatioihin (Crosignani, Macchiavelli & Silva, 2021).

NotPetya päätyi organisaatioiden sisäisiin tietojärjestelmiin toimitusketjuhyökkäyksen kautta. NotPetya lähti leviämään ohjelmistopäivityksen yhteydessä, kun M.E.Doc veronhallintaohjelmiston päivitys oli saastutettu haittaohjelmalla (Greenberg, 2018). Ukrainan verohallinto vaati verotietojen ilmoittamiseen kyseisen ohjelmiston käyttöä, minkä vuoksi se oli Ukrainassa hyvin laajassa käytössä (Crosignani, Macchiavelli & Silva, 2021). Saastuneista laitteista NotPetya levisi automaattisesti verkon muihin laitteisiin (Greenberg, 2018).

NotPetyaa on kuvailtu historian tuhoisammaksi haittaohjelmaksi (Crosignani, Macchiavelli & Silva, 2021). NotPetya aiheutti merkittäviä ongelmia organisaatioiden toimintaan, ja sen aiheuttamien kustannusten on arvioitu olleen yhteensä yli kymmenen miljardia dollaria (Greenberg, 2018). Vaikutukset näkyivät useissa kriittisissä tietojärjestelmissä, muun muassa sairaaloiden tietojärjestelmissä, kuljetusalalla ja lääkeyhtiöiden tuotannossa (Crosignani, Macchiavelli & Silva, 2021).

5.6 SolarWinds, 2019–2020

SolarWinds oli pitkäkestoinen kybervakoiluoperaatio, josta raportoitiin julkisuuteen joulukuussa 2020 (Willett, 2021, s. 7). Vakoiluoperaatio toteutettiin toimitusketjuhyökkäyksenä, jonka kohteena olivat erityisesti Yhdysvaltain valtionhallinto sekä yhdysvaltalaiset yksityiset organisaatiot. Vaikka havaintoja tehtiin eniten Yhdysvalloissa, hyökkäyksellä oli vaikutuksia tuhansiin organisaatioihin ympäri maailmaa (Oladimeji & Kerner, 2023). Operaation takana uskotaan olevan APT29 (Mandiant, 2022b).

SolarWinds-toimitusketjuhyökkäys sai nimensä hyökkäyksen kohdejärjestelmän mukaan. Kohteena oli SolarWinds Orion niminen IT-infrastruktuurin hallinta- ja valvontatyökalu, jonka haavoittuva versio oli vuonna 2020 käytössä noin 18 000 organisaatiossa (Oladimeji & Kerner, 2023). Haavoittuvaa versiota ohjelmistosta käyttivät muun muassa FireEye, Cisco, Intel, Nvidia, Microsoft ja Yhdysvaltain valtionhallinnon organisaatiot (Willett, 2021, s. 8).

Uhkatoimija oli luonut jalansijan SolarWindsin ympäristöön jo syyskuussa 2019 (Oladimeji & Kerner, 2023). Jalansija mahdollisti uhkatoimijalle SolarWinds Orion -hallintatyökalun päivitysten muokkaamisen siten, että päivitykset olivat allekirjoitettu SolarWindsin allekirjoitusvarmenteella. Ensimmäinen muokkaus päivityksiin tehtiin lokakuussa 2019, mutta muutoksilla ei ollut vielä merkittäviä vaikutuksia ohjelmiston toimintaan (Willett, 2021, s. 8). Uhkatoimija pyrki tällä todennäköisesti varmistamaan, että valmisteltu jalansija ja valittu hyökkäystapa toimivat.

Helmikuussa 2020 uhkatoimija lisäsi haitallista koodia Orion-päivityksiin (Oladimeji & Kerner, 2023), joiden jakelu asiakkaille aloitettiin maaliskuussa 2020 (Willett, 2021, s. 8). Päivitysten yhteydessä kohdeohjelmistoon asennettiin takaovi, joka mahdollisti informaation keräämisen kohdejärjestelmästä (Oladimeji & Kerner, 2023). Tieto toimitusketjuhyökkäyksestä julkaistiin joulukuussa 2020, joten uhkatoimijalla oli todennäköisesti pääsy kohdejärjestelmiin useiden

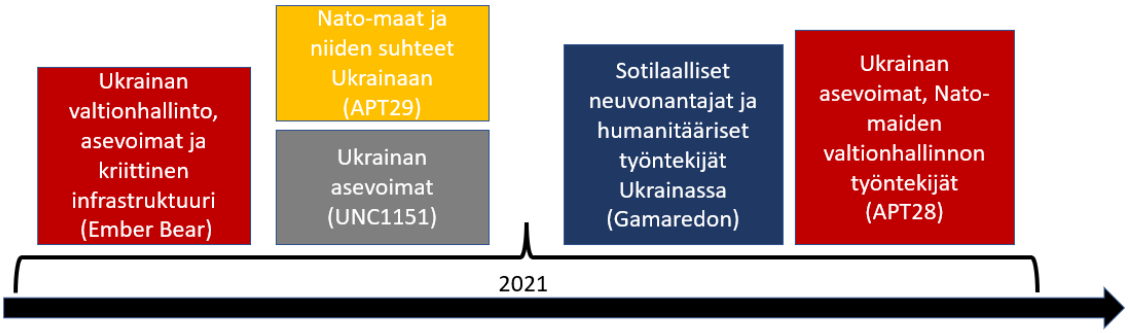
kuukausien ajan (Willett, 2021, s. 7). Vaikka operaation tavoitteena oli selvästi laaja tiedonhankinta, hyökkäyksen tarkka motiivi on epäselvä (Oladimeji & Kerner, 2023). Hyökkäykseen liittyen ei havaittu esimerkiksi tietojärjestelmien toiminnan häiritsemistä tai tiedon tuhoamista (Willett, 2021, s. 9).

6 TIETOJENKALASTELUOPERAATIOITA VUONNA 2021

Venäjä kohdisti kyberoperaatioita Ukrainaan pitkään ennen aseellisen hyökkäyksen aloittamista. Venäjä on kohdistanut aktiivisesti kyberoperaatioita Ukrainaan vuodesta 2014 alkaen, mutta operaatioiden määrän havaittiin kasvaneen merkittävästi vuoden 2021 alussa (Google, 2023, s. 7). Tämä lisääntynyt aktiivisuus näkyi erityisesti lisääntyneinä tietojenkalasteluoperaatioina. Koska Venäjä on kohdistanut kyberoperaatioitaan Ukrainaan jo vuosia, on vaikea määritellä tarkasti, milloin operaatioiden tavoitteeksi muuttui hyökkäyssodan valmistelu (Microsoft, 2022b).

Venäjän valtiolliset uhkatoimijat kohdistivat tietojenkalasteluoperaatioita Ukrainan lisäksi myös useisiin muihin maihin, erityisesti Nato-maihin. Tietojenkeräämisen tavoitteena oli todennäköisesti kerätä Venäjän valtionhallinnolle sellaista tietoa, josta voitaisiin päätellä maiden reagointia Venäjän aseelliseen voimankäyttöön (Microsoft, 2022b). Nato-maissa lisääntynyttä tietojenkalastelua havaittiin useilla sektoreilla, muun muassa valtionhallinnon, asevoimien, kriittisen infrastruktuurin ja median organisaatioissa (Google, 2023, s. 7).

Tässä luvussa keskitytään Venäjän valtionhallintoon liitettyjen uhkatoimijoiden suorittamiin tietojenkalasteluoperaatioihin vuonna 2021. Yhteenveto käsiteltävistä tietojenkalasteluoperaatioista esitetään kuviossa 3.



KUVIO 3 Havaittuja tietojenkalasteluoperaatioita ja niiden kohteita vuonna 2021.

Kuvion tarkastelujakso on vuosi 2021. Kuviossa on esitetty punaisella GRU:n, keltaisella SVR:n ja sinisellä FSB:n uhkatoimijat. Harmaalla uhkatoimija, jonka taustaorganisaatio on tuntematon. Vuoden 2021 tapahtumia ei ole sijoitettu aikajanalle tarkasti, koska niiden tarkat ajankohdat ovat osin epäselviä. Kuviossa ei ole esitetty jokaista havaittua tietojenkalastelukampanjaa, vaan keskitytään Ukrainan sodan kannalta keskeisiin teemoihin.

6.1 Ember Bear – Ukrainan valtionhallinto, asevoimat ja kriittinen infrastruktuuri

Ember Bearin tietojenkalasteluoperaatiot alkoivat alkuvuodesta 2021 ja ne jatkuivat aktiivisena hyökkäyssodan alkamiseen asti (Google, 2023, s. 23; CrowdStrike, 2022). Vuonna 2021 havaittiin kaksi suurempaa uhkatoimijaan liitettyjä kampanjaa, jotka ajoittuivat helmi- ja huhtikuulle (Google, 2023, s. 23).

Helmikuun kampanjassa käytettiin COVID-19-teemaisia tietojenkalastelusähköposteja, joita lähetettiin lääkeyhtiöille ja valtionhallinnon organisaatioille ympäri maailmaa (Google, 2023, s. 23). Kyseinen kampanja ei ollut kohdistettu erityisesti Ukrainaan.

Huhtikuun laaja tietojenkalastelukampanja puolestaan kohdistui selvästi Ukrainaan. Kampanja toteutettiin sähköpostiviesteillä, joiden vastaanottajia oli Ukrainassa noin 2000. Yli 80 % kaikista vastaanottajista oli Ukrainan asevoimien tai valtionhallinnon työntekijöitä, mutta joukossa oli myös kriittisen infrastruktuurin toimijoita, kuten veden, kaasun ja öljyn jakeluun liittyviä organisaatioita (Google, 2023, s. 23). Tietojenkalastelun tarkoituksena oli todennäköisesti kerätä tietoa kohdeorganisaatioiden henkilöstöstä, rakenteesta ja toiminnasta (CrowdStrike, 2022). Kerättyjä tietoja voitiin myöhemmin hyödyntää myös uusien kyberoperaatioiden valmisteluun (Google, 2023, s. 23).

6.2 APT29 – Nato-maat ja niiden suhteet Ukrainaan

APT29 toteutti laajaa tietojenkalastelua vuonna 2021 (Microsoft, 2022b). Uhkatoimijan tietojenkalastelu kohdistui erityisesti Nato-maihin, (Microsoft, 2022b), mutta kampanjoiden kohteena oli myös muita maita ympäri maailmaa (Mandiant, 2022b). Kohteena olivat valtionhallinnon organisaatiot, erityisesti maiden ulkopoliittisista suhteista vastaavat toimijat (Mandiant, 2022b).

Alkuvuodesta 2021 APT29 kohdisti operaatioitaan IT-alan organisaatioihin, jotka tarjosivat palvelujaan valtionhallinnon asiakkaille (Microsoft, 2022b). Palveluntarjoajien kautta APT29 pyrki saamaan pääsyn valtionhallinnon organisaatioiden tietoihin. Tavoitteena oli todennäköisesti kerätä tietoa siitä, miten Venäjän aseelliseen hyökkäykseen reagoitaisiin ja millaista tukea Ukraina saisi aseellisen konfliktin aikana (Microsoft, 2022b).

6.3 UNC1151 – Ukrainan asevoimat

UNC1151 aloitti alkuvuodesta 2021 useita tietojenkalastelukampanjoita, jotka kohdistuivat Ukrainan asevoimiin. Tietojenkalastelun tavoitteena oli päästä käsiksi Ukrainan asevoimien sähköpostitileihin ja verkkoihin (Microsoft, 2022b). Kyseisten kampanjoiden lukumäärästä, laajuudesta tai vaikutuksista ei ole tarkempaa tietoa julkisuudessa.

6.4 Gamaredon – Sotilaalliset neuvonantajat ja humanitääriset työntekijät Ukrainassa

Vuoden 2021 elokuussa Gamaredon kohdisti Ukrainaan laajan tietojenkalastelukampanjan, jonka kohteena olivat Ukrainassa työskentelevät ulkomaiset sotilaalliset neuvonantajat ja humanitaariset työntekijät (Microsoft, 2022b). Kampanjasta on saatavilla hyvin vähän tietoa julkisissa lähteissä. Gamaredon on hyvin aktiivinen uhkatoimija, joten todennäköisesti kyseinen kampanja ei ollut uhkatoimijan ainut tietojenkalasteluoperaatio vuonna 2021.

6.5 APT28 - Ukrainan asevoimat ja Nato-maat

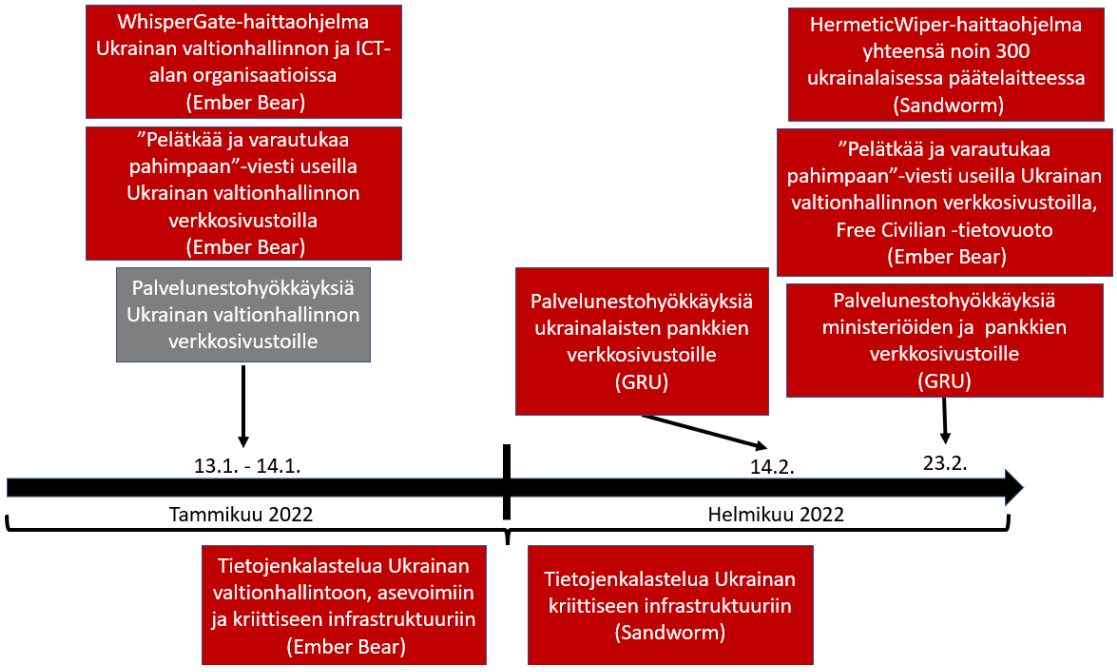
APT28 suoritti aktiivista tietojenkalastelua Ukrainassa vuonna 2021. APT28 on aikaisemminkin kohdistanut operaatioitaan Ukrainaan, mutta aktiivisuuden havaittiin kasvaneen vuonna 2021 (Google, 2023, s. 11). Vuonna 2021 APT28 pyrki saamaan haltuunsa tietoja organisaatioista, jotka liittyivät Ukrainan asevoimien toimintaan (Microsoft, 2022b).

Ukrainan lisäksi APT28 on ollut kiinnostunut Nato-maista. Uhkatoimija suoritti Nato-maita kohtaan eniten tietojenkalasteluoperaatioita kaikista Venäjän valtionhallintoon liitetyistä uhkatoimijoista vuodesta 2021 vuoteen 2022 (Google, 2023, s. 12).

APT28 suoritti laajan tietojenkalastelukampanjan syys-lokakuussa 2021. Kampanjan aktiivisin vaihe kesti 11 päivää, joiden aikana tietojenkalastelusähköposteja lähetettiin yli 14 000 vastaanottajalle ympäri maailmaa (Google, 2023, s. 11). Laajan kampanjan tarkat kohteet, motiivit tai vaikutukset eivät ole tiedossa.

7 KYBERTAPAHTUMIA ENNEN VENÄJÄN ASEELLISTA HYÖKKÄYSTÄ VUONNA 2022

Tässä luvussa keskitytään kybertapahtumiin, joita Venäjän valtionhallintoon yhdistetyt uhkatoimijat kohdistivat Ukrainaan ennen Venäjän aseellista hyökkäystä vuonna 2022. Vaikka useiden Venäjän valtionhallintoon liitettyjen uhkatoimijoiden aktiivisuus Ukrainaa kohtaan oli noussut jo vuoden 2021 alussa, kybertapahtumia havaittiin erityisen paljon vuoden 2022 tammikuun puolesta välistä alkaen (Microsoft, 2022b). Yhteenveto havaituista kybertapahtumista ennen Venäjän aseellista hyökkäystä vuonna 2022 esitetään kuviossa 4.



KUVIO 4 Ukrainassa havaittuja kybertapahtumia alkuvuonna 2022.

Kuvassa punaisella GRU:hun yhdistetyt kybertapahtumat. Harmaalla tapahtumat, joita ei ole yhdistetty mihinkään tiettyyn uhkatoimijaan tai organisaatioon.

7.1 Tietoa tuhoavat haittaohjelmat

Ukrainassa havaittiin uusia tietoa tuhoavia haittaohjelmia (engl. wipers) alkuvuodesta 2022. Haittaohjelmien toiminta perustuu siihen, että ne tuhoavat tietokoneesta kaiken tiedon tavalla, joka on peruuttamaton. Tuhoutuneet tiedot voidaan palauttaa ainoastaan varmuuskopioista. Tietoa tuhoavia haittaohjelmia havaittiin ennen hyökkäyssodan alkamista sadoissa ukrainalaisissa päätelaitteissa (Microsoft, 2022b).

Tietoa tuhoavia haittaohjelmia oli havaittu Ukrainassa myös aikaisemmin. Ukrainan tietojärjestelmiin oli kohdistettu tietoa tuhoavia haittaohjelmia vuosina 2015, 2016 ja 2017, minkä vuoksi vastaavia hyökkäyksiä osattiin odottaa myös Ukrainan ja Venäjän välisen sodan aikana (Google, 2023, s. 15).

7.1.1 WhisperGate-haittaohjelma Ukrainan valtionhallinnon ja ICT-alan organisaatioissa

13. ja 14. tammikuuta 2022 tietoa tuhoava haittaohjelma nimeltä WhisperGate levisi Ukrainan valtionhallinnon ja ICT-alan organisaatioissa (Microsoft, 2022b; Mandiant, 2022a). Haittaohjelma oli naamioitu kiristyshaittaohjelmaksi kiristysviestin avulla, mutta todellisuudessa datan palauttamiseen ei ollut olemassa toimivaa mekanismia (CERT-EU, 2023). WhisperGate on yhdistetty uhkatoimija Ember Beariin (CrowdStrike, 2022).

WhisperGaten vaikutukset jäivät todennäköisesti odotettua pienemmiksi. Haittaohjelma levisi vain muutamaan organisaatioon Ukrainassa (Microsoft, 2022b), eikä hyökkäyksellä raportoitu olleen merkittäviä vaikutuksia organisaatioiden toimintaan. Huomionarvoista on, että WhisperGaten kanssa samanaikaisesti Ukrainassa havaittiin palvelunestohyökkäyksiä ja laaja verkkosivustojen tuhrimiskampanja (CERT-EU, 2023).

7.1.2 HermeticWiper- ja HermeticRansom-haittaohjelmat useissa ukrainalaisissa organisaatioissa

23. helmikuuta tietoa tuhoava haittaohjelma nimeltä HermeticWiper levisi noin 300 päätelaitteeseen ukrainalaisissa organisaatioissa (Microsoft, 2022b). HermeticWiperin aktivoituminen havaittiin vain tunteja ennen Venäjän aseellista hyökkäystä, 23. helmikuuta kello 17:00 Ukrainan paikallista aikaa (ESET, 2023). Kyberhyökkäyksen kohteena oli valtionhallinnon, ICT-organisaatioiden, energiantuotannon ja talouden tietojärjestelmiä (Microsoft, 2022b). Kohdeorganisaatioiden lukumäärä vaihtelee julkisissa lähteissä viidestä (ESET, 2023) yli 12 organisaatioon (Microsoft, 2022b). HermeticWiper on yhdistetty uhkatoimija Sandwormiin (Microsoft, 2022b).

Samoin kuin aikaisemmin mainittu WhisperGate, myös HermeticWiper oli naamioitu kiristyshaittaohjelmaksi päätelaitteen näytölle ilmestyneellä kiristysviestillä. Tässä tapauksessa naamiointia ei tehty pelkällä viestillä, vaan erillisellä

haittaohjelmalla nimeltä HermeticRansom, joka myös salasi kohdejärjestelmän tiedostoja (Microsoft, 2022b).

Vaikka haittaohjelmien naamioitumisessa oli samankaltaisia piirteitä, WhisperGateen verrattuna HermeticWiper oli selvästi kehittyneempi haittaohjelma (Sadowski & Hall, 2022). HermeticWiper oli suunniteltu leviämään automaattisesti kohdeverkon muihin laitteisiin, joten se levisi organisaatioiden tietojärjestelmissä nopeasti ja tehokkaasti (Microsoft, 2022b). Hyökkäyksen vaikutuksista kohdeorganisaatioiden toimintaan on saatavilla hyvin vähän tietoa julkisissa lähteissä.

7.2 Tietojenkalastelu

Noin kuukausi ennen Venäjän aseellista hyökkäystä tietojenkalasteluoperaatioiden määrässä havaittiin kasvua. Tietojenkalastelu oli aktiivista jo vuonna 2021, mutta uusia kampanjoita havaittiin vuoden 2022 tammi-helmikuussa.

7.2.1 Ember Bear – Ukrainan valtionhallinto, asevoimat ja kriittinen infrastruktuuri

Ember Bearin tietojenkalastelua havaittiin useissa aalloissa ukrainalaisissa organisaatioissa 5. tammikuuta – 2. helmikuuta 2022. Kohteet olivat osittain samoja kuin vuoden 2021 huhtikuun tietojenkalastelukampanjassa, mutta mukana oli myös uusia kohteita. Myös tässä tapauksessa kohteena olivat Ukrainan asevoimat, valtionhallinto ja kriittinen infrastruktuuri (Google, 2023, s. 23).

7.2.2 Sandworm - Ukrainan kriittinen infrastruktuuri

Sandworm on kohdistanut Ukrainaan ainakin tammikuusta 2022 alkaen jatkuvaa tietojenkalastelua, jonka tavoitteena on ollut saada kirjautumistietoja eri kohdejärjestelmiin (Google, 2023, s. 17). Tammikuun 2022 kohteita ei ole avattu julkisilla raporteilla tarkasti. Koska Sandwormin on raportoitu suorittaneen useita kriittiseen infrastruktuuriin kohdistuneita tietojenkalasteluoperaatioita vuonna 2022 (Google, 2023, s. 17), myös tammikuun 2022 tietojenkalastelu kohdistui todennäköisesti Ukrainan kriittiseen infrastruktuuriin

7.3 Verkkosivustojen tuhriminen

Verkkosivustojen tuhrimisella (engl. defacement) tarkoitetaan hyökkäystä, jossa verkkosivuston sisältö korvataan uudella, mahdollisesti haitallisella tai provosoivalla sisällöllä. Alkuvuonna 2022 ukrainalaisille verkkosivustoille lisättiin uhkaavia viestejä, joilla pyrittiin todennäköisesti luomaan epäluottamusta Ukrainan valtionhallintoon ja aiheuttamaan pelkoa ukrainalaisissa.

7.3.1 Valtionhallinnon julkisten verkkosivustojen tuhriminen tammikuussa 2022

Samaan aikaan kun tietoa tuhoava WhisperGate-haittaohjelma levisi ukrainalaisissa valtionhallinnon ja ICT-alan organisaatioissa, useat Ukrainan valtionhallinnon verkkosivustot olivat verkkosivustojen tuhrimishyökkäyksen kohteena (Microsoft, 2022b). Hyökkäysten seurauksena 14. tammikuuta verkkosivustojen tavanomainen sisältö oli korvattu uhkaavalla viestillä, joka oli osoitettu ukrainalaisille (CERT-EU, 2023). Hyökkäys on yhdistetty samaan uhkatoimijaan kuin WhisperGate-haittaohjelma, ja molempien hyökkäysten takana uskotaan olevan uhkatoimija Ember Bear (Microsoft, 2022b).

Hyökkäys yritettiin kohdistaa yhteensä 70 verkkosivustoon, mutta hyökkääjä onnistui muokkaamaan lopulta vain 10 sivuston sisältöä (Cimpanu, 2022). Onnistuneiden kohteiden joukossa oli ainakin Ukrainan eri ministeriöiden verkkosivustoja (CERT-EU, 2023). Verkkosivustoille lisätyssä viestissä väitettiin, että ukrainalaisten henkilökohtaisia tietoja on varastettu ja vuodettu verkkoon. Lisäksi viestissä sanottiin, että ukrainalaisten tulisi pelätä tulevaa ja varautua pahimpaan (Cimpanu, 2022).

7.3.2 Valtionhallinnon julkisten verkkosivustojen tuhriminen helmikuussa 2022 ja FreeCivilian-tietovuoto

Helmikuun 23. päivänä, päivää ennen Venäjän aseellista hyökkäystä, havaittiin jälleen verkkosivustojen tuhrimishyökkäyksiä. Hyökkäysten kohteena oli yhteensä 13 Ukrainan valtionhallinnon verkkosivustoa, joille lisätiin uhkaava viesti. Uhkausviesti oli näkyvissä noin vuorokauden ajan. Hyökkäystä seuraavana päivänä viesti oli näkyvissä enää yhdellä verkkosivustolla (Secureworks, 2022). Hyökkäysten takana uskotaan olevan uhkatoimija Ember Bear, joka oli myös tammikuun hyökkäysten takana (CrowdStrike, 2022).

Hyökkäyksissä käytetty uhkausviesti oli lähes identtinen kuin tammikuussa käytetty viesti. Verkkosivustoille lisätty viesti oli ulkoasultaan samanlainen kuin aikaisemmin ja sisälsi samat uhkaukset. Eroavaisuutensa edelliseen hyökkäykseen uhkausviestin alle oli lisätty kaksi linkkiä, jotka johtivat Tor-verkkosivustolle (Secureworks, 2022).

Viestiin lisätyt linkit johtivat sivustolle, joka sisälsi väitetysti ukrainalaisten kaapattuja henkilötietoja. Sivustoa ylläpiti Free Civilian -niminen käyttäjä, joka väitti henkilötietojen olevan peräisin Ukrainan valtionhallinnon verkkopalveluista. Free Civilian oli listannut 50 ukrainalaista verkkosivustoa, joilta tiedot oli väitetysti saatu. Vuodettujen henkilötietojen todellinen lähde on epäselvä, minkä lisäksi tietojen aitoutta on kyseenalaistettu. On mahdollista, että kyseessä oli informaatio-operaatio, jossa tekaistuilla henkilötiedoilla pyrittiin pelottelemaan ukrainalaisia ja luomaan epäluottamusta Ukrainan valtionhallinnon palveluihin (Secureworks, 2022).

7.4 Palvelunestohyökkäykset

Noin kuukausi ennen hyökkäyssodan alkamista, vuoden 2022 tammikuun puolesta välistä alkaen, Ukrainaan kohdistettujen palvelunestohyökkäysten määrä nousi merkittävästi (CERT-EU, 2023). Palvelunestohyökkäysten kohteina olivat muun muassa Ukrainan valtionhallinnon, asevoimien ja Ukrainassa toimivien pankkien verkkosivustot (Antoniuk, 2022). Palvelunestohyökkäysten seurauksena niiden kohteena olleet verkkosivustot olivat hetkellisesti saavuttamattomissa.

Palvelunestohyökkäykset ovat tyypillisesti lyhytkestoisia ja vaikutuksiltaan pieniä, mutta ne saavat runsaasti näkyvyyttä esimerkiksi mediassa. Palvelunestohyökkäyksillä on otettu usein kantaa kohdeorganisaation tai valtion poliittisiin tai poliittisiksi tulkittaviin päätöksiin. Hyökkääjät ovat tyypillisesti julkaisseet uhreistaan tietoja esimerkiksi Telegram-kanavalle ja perustelleet hyökkäyksensä motiiveja julkaisuissaan, mikä on auttanut motiivien tunnistamisessa. Palvelunestohyökkäykset voidaan katsoa osaksi informaatiovaikuttamista, jota toteutetaan kybertoimintaympäristön kautta.

7.4.1 Palvelunestohyökkäyksiä Ukrainan valtionhallinnon verkkosivustoille tammikuussa 2022

14. tammikuuta Ukrainan valtionhallinnon verkkosivustoille kohdistui useita palvelunestohyökkäyksiä (Microsoft, 2022b). Verkkosivustojen toiminta häiriintyi hetkellisesti, mutta hyökkäyksellä ei ollut pitkäaikaisia vaikutuksia niiden toimintaan. Palvelunestohyökkäykset ajoittuivat samoihin aikoihin kuin edellä mainitut verkkosivustojen tuhrimishyökkäykset ja tietoa tuhoava WhisperGate-haittaohjelma. Palvelunestohyökkäyksiä ei ole yhdistetty tiettyyn uhkatoimijaan, mutta ne ajoittuivat samaan aikaan kuin muut Ember Beariin liitetyt kyberhyökkäykset (Microsoft, 2022b).

7.4.2 Palvelunestohyökkäyksiä Ukrainan asevoimien, valtionhallinnon ja pankkien verkkosivustoille helmikuussa 2022

15. helmikuuta Ukrainassa havaittiin jälleen uusia palvelunestohyökkäyksiä (Microsoft, 2022b), joiden kohteena olivat useat verkkosivustot, muun muassa Ukrainan asevoimien, puolustusministeriön ja kahden Ukrainan suurimman pankin verkkosivustot (Antoniuk, 2022). Palvelunestohyökkäykset vaikuttivat verkkosivustojen lisäksi myös kahden pankin, Privatbank ja Oschadbank, mobiilisovelluksiin ja verkkomaksuihin (Antoniuk, 2022). Palvelunestohyökkäysten takana uskotaan olevan Venäjän sotilastiedustelu, mutta niitä ei ole liitetty tarkemmin mihinkään GRU:n alaiseen uhkatoimijaan (Microsoft, 2022b).

Venäjän aseellista hyökkäystä edeltävänä päivänä, 23.2.2022, palvelunestohyökkäyksiä havaittiin samojen pankkien ja ministeriöiden verkkosivustoilla, jotka olivat olleet kohteina tammikuussa ja aikaisemmin helmikuussa. Palvelunestohyökkäysten kohteina olivat muun muassa ulkoministeriön,

puolustusministeriön, sisäministeriön ja kahden pankin (Privatbank ja Oschadbank) verkkosivustot (Secureworks, 2022).

8 KYBERTAPAHTUMIA 24.–25. HELMIKUUTA 2022

Tässä luvussa käsitellään Venäjän ja Ukrainan välisen sodan kahden ensimmäisen päivän kybertapahtumia. Kahden ensimmäisen päivän aikana Ukrainaa vastaan käytettiin useita tietoa tuhoavia haittaohjelmia, joilla pyrittiin vaikuttamaan Ukrainan valtionhallinnon ja asevoimien kommunikaatio- ja johtamisyhteyksiin. Lisäksi Euroopan maihin kohdistettiin tietojenkalastelua, jolla pyrittiin saamaan tietoa pakolaisten liikkeistä Euroopassa. Muut hyökkäystyypit olivat sodan ensimmäisinä päivinä pienemmässä roolissa, tai ainakaan niistä ei ole raportoitu julkisuuteen.

8.1 Tietoa tuhoavat haittaohjelmat

Sodan kahtena ensimmäisenä päivänä tietoa tuhoavia haittaohjelmia havaittiin useissa ukrainalaisissa kohteissa. Tässä luvussa on kuvattu sodan ensimmäisinä päivinä havaittuja tietoa tuhoavia haittaohjelmia.

8.1.1 AcidRain-haittaohjelma Viasatin KA-SAT-satelliittiverkossa

Helmikuun 24. päivänä, vain tuntia ennen Venäjän aseellista hyökkäystä, havaittiin yksi merkittävimmistä kyberhyökkäyksistä Ukrainan ja Venäjän välisen sodan aikana (ESPI, 2022). Kohteena oli Viasatin KA-SAT-satelliittiverkko, jonka toiminnassa havaittiin hyökkäyksen seurauksena häiriöitä Ukrainassa ja muualla Euroopassa (Guerrero-Saade & van Amerongen, 2022). Euroopan laajuisesti hyökkäys vaikutti kymmeniin tuhansiin asiakkaisiin, kun taas Ukrainassa vaikutuksia oli tuhansien käyttäjien palveluihin (Viasat, 2022). KA-SAT-satelliittiverkko tarjosi hyökkäyshetkellä palvelujaan muun muassa Ukrainan valtionhallinnolle, asevoimille ja turvallisuuspalveluille (ESPI, 2022).

Hyökkäyksestä voidaan erottaa kaksi eri vaihetta. Ensimmäisessä vaiheessa hyökkääjä levitti tietoa tuhoavaa haittaohjelmaa nimeltä AcidRain KA-SAT-verkon hallintapalvelimen kautta, mikä sai kymmenet tuhannet modeemit irtoamaan verkosta (Guerrero-Saade & van Amerongen, 2022). Toinen vaihe

toteutettiin palvelunestohyökkäyksenä, jonka aikana verkkolaitteille lähetettiin suuri määrä haitallista liikennettä, mikä vaikeutti verkosta irronneiden modeemien saamista takaisin verkkoon (Greig, 2023). Toisen vaiheen palvelunestohyökkäyksellä pyrittiin hidastamaan ensimmäisen vaiheen haittaohjelmasta toipumista.

On epäselvää, miten hyökkääjä oli ensimmäisessä vaiheessa päässyt käsiksi verkon hallintapalvelimeen. Vuonna 2022 Viasat raportoi hyökkääjän hyväksikäyttäneen VPN-yhteyden konfiguraatiovirheitä (Viasat, 2022), mutta vuonna 2023 Viasatin edustaja sanoi tapahtumaketjun olevan edelleen epäselvä (Greig, 2023). On mahdollista, että hyökkääjä oli saanut haltuunsa VPN-kirjautumistunnuksia esimerkiksi aikaisempien tietovuotojen yhteydessä (ESPI, 2022), minkä lisäksi on tutkittu sisäpiiriuhkan mahdollisuutta (Greig, 2023).

Hyökkäyksen yksityiskohtaisista vaikutuksista Ukrainan tietojärjestelmiin ei ole raportoitu julkisuuteen. KA-SAT-verkko oli hyökkäyshetkellä käytössä muun muassa Ukrainan asevoimilla, valtionhallinnolla ja turvallisuuspalveluilla (ESPI, 2022), joten hyökkäys on mahdollisesti vaikuttanut Ukrainan johtamis- ja kommunikaatioyhteyksiin merkittävästi sodan ensimmäisillä hetkillä.

Kyberhyökkäyksen vaikutukset näkyivät myös Ukrainan ulkopuolella. Yhteysongelmia havaittiin ympäri Eurooppaa, muun muassa Saksassa, Ranskassa, Unkarissa, Kreikassa, Italiassa ja Puolassa (ESPI, 2022). Suurimmat häiriöt raportoitiin Saksassa, jossa 5800:n tuuliturbiinin etävalvonta ja -ohjaus katkesivat hyökkäyksen seurauksena (Guerrero-Saade & van Amerongen, 2022). Vaikka hyökkäys oli kohdistettu erityisesti Ukrainaan, sen vaikutukset levisivät myös muualle.

Muun muassa Yhdysvallat ja Euroopan Union ovat yhdistäneet kyberhyökkäyksen Venäjän sotilastiedusteluun (ESPI, 2022). Hyökkäyksen taustalla oli todennäköisesti Sandworm (Guerrero-Saade & van Amerongen, 2022). Hyökkäyksessä käytetyssä AcidRain-haittaohjemassa on tunnistettu samanlaisia ominaisuuksia kuin Sandwormin aikaisemmin käyttämässä VPNFilter-haittaohjelmassa, minkä lisäksi Sandworm on käyttänyt Ukrainassa useita muita tietoa tuhoavia haittaohjelmia kriittisiä kohteita vastaan (Guerrero-Saade & van Amerongen, 2022).

8.1.2 IsaacWiper-haittaohjelma valtionhallinnon organisaatioissa

Hyökkäyspäivänä havaittiin myös toinen tietoa tuhoava haittaohjelma, jolle on annettu nimi IsaacWiper. Haittaohjelma levisi Ukrainan valtionhallinnon organisaatioissa 24. helmikuuta 2022, mutta sen vaikutuksista ei ole tarkkaa tietoa julkisuudessa (ESET, 2022a). Myöskään kohdeorganisaatioita ei ole eritelty tarkemmin.

IsaacWiper ei todennäköisesti toiminut suunnitellusti. Haittaohjelman toimintaan lisättiin seuraavana päivänä (25.2.) muutoksia, joiden avulla pyrittiin todennäköisesti kartoittamaan ongelmia haittaohjelman toiminnassa. Hyökkääjät lisäsivät haittaohjelmaan sen lokitietojen keräämisen, mikä auttoi tunnistamaan mahdollisia haittaohjelman toimintavirheitä (ESET, 2022a). IsaacWiper-haittaohjelmaa ei ole yhdistetty mihinkään tiettyyn uhkatoimijaan.

8.1.3 Tietoa tuhoava haittaohjelma Ukrainan rajavalvonnassa

Hyökkäystä seuraavana päivänä, 25. helmikuuta, uutisoitiin uudesta tietoa tuhoavasta haittaohjelmasta. Haittaohjelmalla oli väitetysti isketty Ukrainan rajavalvontaan ja hidastettu sotaa pakenevien ihmisten poistumista Ukrainasta (Berger, 2022). Haittaohjelmasta on hyvin vähän tietoa julkisissa lähteissä, eivätkä esimerkiksi tietoturvatalot ole julkaisseet haittaohjelmasta omaa analyysiaan tai teknisiä uhkatunnisteita.

Uutisessa väitettiin, että haittaohjelma hidasti merkittävästi Ukrainasta pakenevien ihmisten rajanylitystä Romaniaan. Haittaohjelma esti rajavalvonnan tietojärjestelmien käytön, minkä vuoksi ihmisten tietoja jouduttiin kirjaamaan kynällä ja paperilla (Berger, 2022). Tietoa haittaohjelmasta tai sen vaikutuksista ei ole voitu vahvistaa muista läheistä.

8.2 Tietojenkalastelu

Hyökkäyspäivänä 24. helmikuuta havaittiin laaja tietojenkalastelukampanja, joka kohdistui useisiin eri Euroopan maihin. Tietojenkalastelun kohteena olivat henkilöt, jotka liittyivät ukrainalaisten pakolaisten kuljetusten järjestelyihin. Tavoitteena oli todennäköisesti kerätä tietoa pakolaisten liikkeistä ja niihin liittyvistä päätöksistä Euroopassa. Tietojenkalastelu on yhdistetty uhkatoimijaan UNC1151 (Raggi & Cass, 2022).

Tietojenkalastelussa käytetty sähköpostiviesti oli hyvin ajankohtainen ja uskottava. Viesti oli lähetetty Ukrainan asevoimissa työskentelevän henkilön nimissä, todennäköisesti murretulta sähköpostitililtä. Viestin sisältämän liitetiedoston uskoteltiin liittyvän edellisenä päivänä järjestettyyn Naton hätäkokoukseen, mikä houkutteli vastaanottajia avaamaan viestin liitteen. Todellisuudessa tiedosto oli haitallinen ja latasi järjestelmään haittaohjelman nimeltä SunSeed, joka mahdollisti tietojen viemisen kohdejärjestelmästä (Raggi & Cass, 2022).

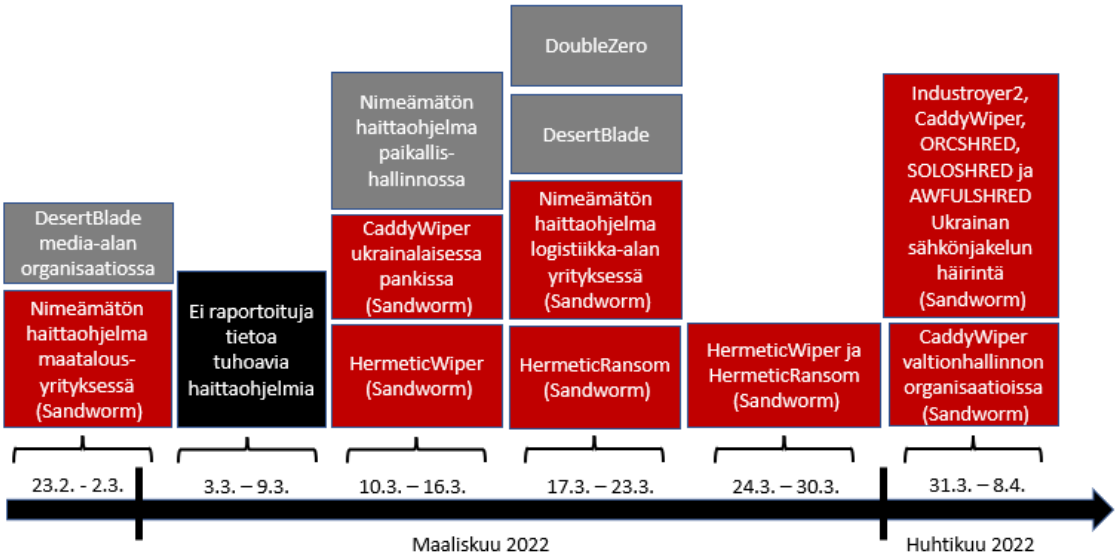
9 KYBERTAPAHTUMIA HUHTIKUUHUN 2022 MENNESSÄ

Keväällä 2022 Venäjä keskittyi kybertoimintaympäristössä tuhoaviin ja häiritseviin operaatioihin. Kevään aikana havaittiin useita tietoa tuhoavia haittaohjelmia, joiden kohteina olivat muun muassa Ukrainan valtionhallinto, media-alan organisaatiot ja kriittinen infrastruktuuri.

Erityisesti maaliskuu oli tietoa tuhoavien haittaohjelmien osalta aktiivista aikaa. Maaliskuun aikana havaittiin useita uusia tietoa tuhoavia haittaohjelmia, minkä lisäksi joitain aikaisemmin havaittuja haittaohjelmia käytettiin uudelleen. Microsoftin vuonna 2023 tekemän arvion mukaan noin puolet kaikista tietoa tuhoavista hyökkäyksistä tehtiin sodan kuuden ensimmäisen viikon aikana (Microsoft, 2023, s. 48).

9.1 Tietoa tuhoavat haittaohjelmat

Ukrainassa havaittiin useita erilaisia tietoa tuhoavia haittaohjelmia keväällä 2022. Pelkästään maaliskuun aikana havaittiin viisi erilaista tietoa tuhoavaa haittaohjelmaa, joille on annettu nimet DesertBlade, HermeticWiper, HermeticRansom, DoubleZero ja CaddyWiper (ESET, 2023). DesertBlade, HermeticWiper, DoubleZero ja CaddyWiper ovat haittaohjelmia, joiden toiminta perustuu datan tuhoamiseen ylikirjoittamalla tiedostoja. HermeticRansom puolestaan salaa tiedostoja kiristyshaittaohjelman tapaan, ja sitä on joissain kampanjoissa käytetty yhdessä HermeticWiperin kanssa (Microsoft, 2022b). Kuviossa 5 esitetään yhteenveto havaituista haittaohjelmista.



KUVIO 5 Ukrainassa havaittuja tietoa tuhoavia haittaohjelmia huhtikuun 8. päivään mennessä.

Kuviosta on jätetty pois kyberhyökkäykset, jotka ovat selkeästi sijoitettavissa sodan kahdelle ensimmäiselle päivälle. Kuvassa punaisella GRU:hun yhdistetyt kybertapahtumat ja harmaalla tapahtumat, joita ei ole yhdistetty mihinkään tiettyyn uhkatoimijaan tai organisaatioon.

9.1.1 DesertBlade-haittaohjelma media-alan organisaatiossa

Maaliskuun 1. päivänä ukrainalaiseen media-alan organisaatioon kohdistettiin kyberhyökkäys, jossa käytettiin DesertBlade-haittaohjelmaa. Samana päivänä Venäjän asevoimat iskivät Kiovan TV-torniin ohjuksilla ja ilmoittivat, että heidän tavoitteenaan on tuhota valheellista informaatiota levittäviä kohteita Ukrainassa. Haittaohjelma on yhdistetty Venäjään, mutta ei tarkemmin mihinkään tiettyyn uhkatoimijaan (Microsoft, 2022b). DesertBlade-haittaohjelma oli todennäköisesti osa laajempaa Venäjän asevoimien kampanjaa, jossa sitä käytettiin pohjustamaan tai täydentämään ohjushyökkäystä ja sen vaikutuksia.

Toinen hyökkäys DesertBlade-haittaohjelmalla tehtiin sodan neljännellä viikolla 17.–23. maaliskuuta (Microsoft, 2022b). Tästä hyökkäyksestä ei ole julkaistu tarkempia yksityiskohtia.

9.1.2 HermeticWiper- ja HermeticRansom-haittaohjelmien useat aallot

HermeticWiper ja HermeticRansom ovat haittaohjelmia, jotka havaittiin ensimmäisen kerran ennen Venäjän aseellista hyökkäystä 23. helmikuuta 2022. Myöhemmin vuoden 2022 keväällä haittaohjelmia havaittiin käytettävän sekä yhdessä että erikseen. Haittaohjelmat on yhdistetty uhkatoimija Sandwormiin (Microsoft, 2022b).

Kolmannella viikolla sodan alkamisen jälkeen, 10.–16. maaliskuuta, havaittiin hyökkäyksiä, joissa käytettiin ainoastaan HermeticWiper-haittaohjelmaa (ESET, 2023). Sodan neljännen viikon aikana, 17.–23. maaliskuuta, puolestaan havaittiin hyökkäys, jossa käytettiin ainoastaan HermeticRansom-haittaohjelmaa (Microsoft, 2022b). Sodan viidennellä viikolla 24.–30. maaliskuuta havaittiin hyökkäyksiä, joissa käytettiin molempia edellä mainittuja haittaohjelmia (Microsoft, 2022b). Edellä mainittujen hyökkäysten kohteista tai vaikutuksista ei ole saatavilla tarkempaa tietoa julkisissa lähteissä.

HermeticWiper- ja HermeticRansom-haittaohjelmien käyttö oli aktiivista kevään 2022 aikana. Samoja haittaohjelmia käytettiin Ukrainassa useampaan otteeseen, mutta julkisten lähteiden raporteissa ei kerrota, tehtiinkö haittaohjelmiin muutoksia hyökkäysten välillä. On mahdollista, että haittaohjelmien toimintaa tai rakennetta on muutettu hyökkäysten välissä, jotta niiden havaitseminen ja tunnistaminen olisi vaikeampaa.

9.1.3 DoubleZero-haittaohjelma

DoubleZero-haittaohjelmalla hyökättiin useisiin ukrainalaisiin organisaatioihin 17. maaliskuuta 2022. Haittaohjelman tavoitteena oli häiritä ukrainalaisten yritysten tietojärjestelmien toimintaa (CERT-UA, 2022), mutta hyökkäyksen laajuudesta tai vaikutuksesta ei ole julkaistu tarkempia yksityiskohtia. CERT-UA on julkaissut haittaohjelman toiminnasta tarkempaa teknistä analyysia, mutta muilta osin kampanjasta on saatavilla hyvin vähän tietoa. Haittaohjelmaa ei ole yhdistetty mihinkään tiettyyn uhkatoimijaan.

9.1.4 CaddyWiper-haittaohjelma ukrainalaisessa pankissa ja valtionhallinnon organisaatioissa

CaddyWiper-haittaohjelmaa havaittiin Ukrainassa useissa aalloissa kevään 2022 aikana. Myös CaddyWiper on yhdistetty Sandworm-uhkatoimijaan (Microsoft 2022b), aivan kuten monet muut tietoa tuhoavat haittaohjelmat, joita havaittiin Ukrainassa vuonna 2022.

Ensimmäisen kerran CaddyWiper-haittaohjelmaa käytettiin maaliskuun 14. päivänä, jolloin sen kohteena oli ukrainalainen pankki (ESET, 2023). Seuraavan kerran havaintoja CaddyWiperista tehtiin huhtikuun 1. päivänä, kun haittaohjelmalla tehtiin hyökkäyksiä valtionhallinnon organisaatioihin (ESET, 2023).

Huhtikuun 8. päivänä CaddyWiper oli osaa laajempaa kokonaisuutta, kun Ukrainan sähkönjakelua yritettiin häiritä käyttämällä useita erilaisia haittaohjelmia. Kyseinen kokonaisuus tunnetaan parhaiten nimellä Industroyer2. Industroyer2-kampanjaa käsitellään tarkemmin seuraavassa luvussa.

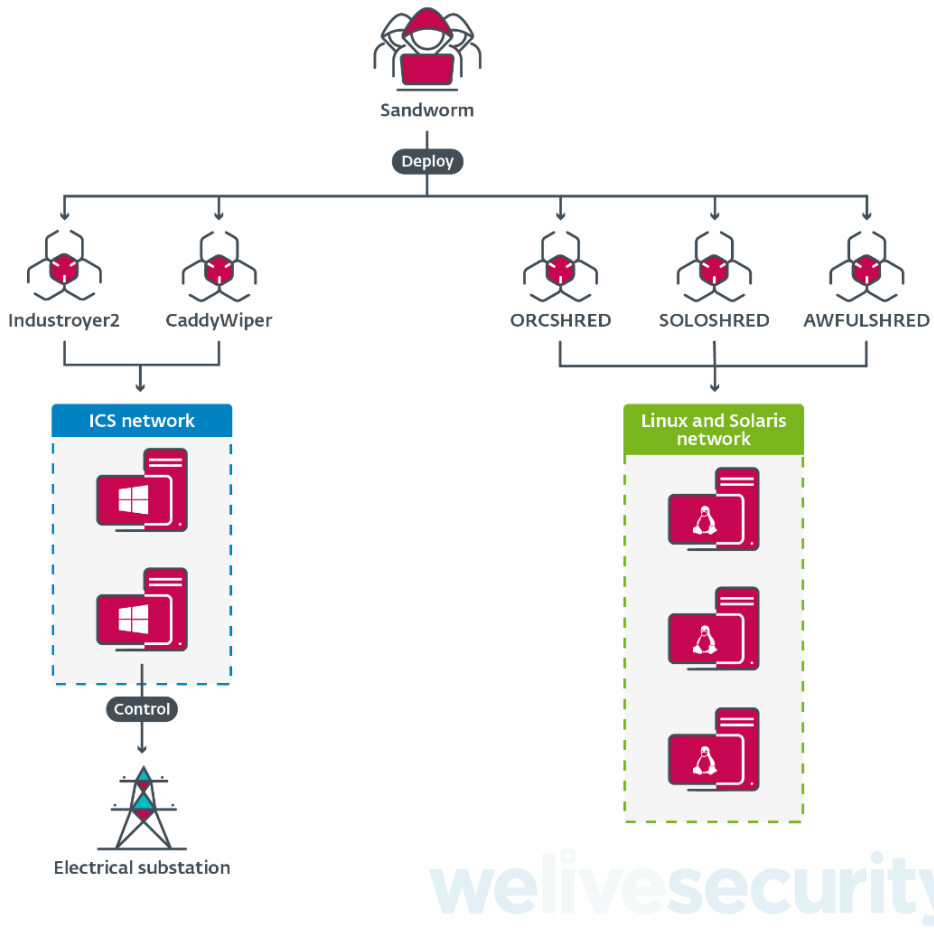
9.1.5 Industroyer2-hyökkäys Ukrainan sähkönjakeluun

Huhtikuussa 2022 Ukrainan sähkönjakelua yritettiin häiritä kyberhyökkäyksellä. Onnistuessaan hyökkäys olisi katkaissut sähköt noin 2 miljoonalta

ukrainalaiselta, mutta hyökkäys onnistuttiin estämään ennen haittaohjelmien aktivoitumista kohdejärjestelmissä (Tidy, 2022). Hyökkäyksessä oli samoja piirteitä kuin vuoden 2016 kyberhyökkäyksessä, joka häiritsi Ukrainan sähkönjakelua noin tunnin ajan (ESET, 2022b).

Sähkönjakelua pyrittiin häiritsemään haittaohjelmalla, jolle on annettu nimi Industroyer2. Nimensä haittaohjelma sai siitä, että se oli erittäin todennäköisesti uusi versio Industroyer-haittaohjelmasta, jota uhkatoimija Sandworm käytti Ukrainassa vuonna 2016 häiritäkseen Ukrainan sähkönjakelua (ESET, 2022b). Industroyer2 oli suunniteltu ohjaamaan sähköntuotannon toiminnanohjausjärjestelmiä, joiden kautta pyrittiin katkaisemaan alueen sähkönjakelu. Tuhoava hyökkäys oli ajastettu alkamaan perjantai-iltana 8.4.2022, mutta hyökkäys saatiin estettyä ennen haittaohjelmien aktivoitumista (Tidy, 2022).

Industroyer2-haittaohjelman lisäksi hyökkäyksessä käytettiin useita tietoa tuhoavia haittaohjelmia. Tietoa tuhoavat haittaohjelmat olivat nimeltään CaddyWiper, ORCSHRED, SOLOSHRED ja AWFULSHRED (ESET, 2022b). Aktivoituessaan haittaohjelmat olisivat tuhonneet tietoa Windows-, Linux- ja Solaris-käyttöjärjestelmistä, mikä olisi todennäköisesti hidastanut hyökkäyksestä palautumista. Kuviossa 6 esitetään hyökkäyksessä käytetyt haittaohjelmat ja niiden kohdejärjestelmät.



KUVIO 6 Sandwormin käyttämät haittaohjelmat ja niiden kohdejärjestelmät Industroyer2-kampanjassa (ESET, 2022b).

9.1.6 Nimeämättömät haittaohjelmat

Microsoftin (2022b) julkaisemassa raportissa on käsitelty myös sellaisia tietoa tuhoavia haittaohjelmia, joita ei ole erikseen nimetty. Tässä luvussa käsitellään sellaisia hyökkäyksiä, joita ei voida suodaan yhdistää mihinkään edellä mainittuun haittaohjelmaan. On todennäköistä, että kaikki tai suurin osa käsiteltävistä haittaohjelmista on kuvattu edeltävissä kappaleissa, mutta saatavilla olevan tiedon perusteella tapahtumia ei voida yhdistää.

Sodan ensimmäisellä viikolla Sandworm suoritti kyberhyökkäyksen ukrainalaiseen maatalousyritykseen. Tarkkaa ajankohtaa ei ole kerrottu julkisuuteen, mutta hyökkäys ajoittui aikavälille 23. helmikuuta - 2. maaliskuuta. Hyökkäyksessä käytettiin haittaohjelmaa, joka salasi kohdejärjestelmän tiedostot, mutta niitä ei ainakaan tässä vaiheessa tuhottu. Hyökkäyksen tavoitteena oli todennäköisesti häiritä Ukrainan viljantuotantoa ja vaikuttaa negatiivisesti Ukrainan talouteen (Microsoft, 2022b). Julkisen kuvauksen perusteella kyseessä voisi olla Sandwormiin yhdistetty tietoja salaava HermeticRansom-haittaohjelma, mutta tästä ei ole vahvistettua tietoa.

Sodan kolmannella viikolla tuntematon, todennäköisesti venäläinen, uhkatoimija tuhosi dataa paikallishallinnon organisaatiosta Ukrainan itäosassa. Kyberhyökkäyksellä oli häiritseviä vaikutuksia paikallishallinnon toimintaan alueella (Microsoft, 2022b).

Sodan neljännellä viikolla Sandworm kohdisti tietoja tuhoavan kyberhyökkäyksen ukrainalaiseen kuljetus- ja logistiikka-alan organisaatioon. Kyseinen organisaatio oli sellainen, että se olisi voinut osallistua Ukrainan joukkojen huoltamiseen konfliktialueilla (Microsoft, 2022b). Hyökkäyksen tavoitteena oli todennäköisesti häiritä Ukrainan asevoimien ja/tai siviilien huollon onnistumista.

9.2 Tietojenkalastelu ja muu tiedonhankinta

Kevään 2022 aikana tietojenkalastelu jatkui aktiivisena, kun useat Venäjän valtiolliset uhkatoimijat kohdistivat operaatioitaan Ukrainaan. Lisäksi tietoja varastettiin kohdejärjestelmistä myös muilla keinoilla, kun venäläiset uhkatoimijat suorittivat tiedonhankintaoperaatioitaan. Toiminta oli jatkuvaa ja laaja-alaista.

9.2.1 Sandworm

Maaliskuussa 2022 Sandworm varasti tietoja ukrainalaisen tutkimuslaitoksen tietojärjestelmistä. Hyökkäyksen tavoitteena oli todennäköisesti tukea varastetulla tiedolla Venäjän informaatio-operaatioita, joissa levitettiin valheellista tietoa Ukrainan käyttämistä biologisista ja kemiallisista aseista. Sandworm on aikaisemminkin käyttänyt operaatioidensa aikana varastettua tietoa tukemaan

informaatio-operaatioita, mikä todennäköisesti motivoi myös tähän hyökkäykseen (Microsoft, 2022b).

9.2.2 APT28

Maaliskuussa 2022 APT28 toteutti useita tietojenkalastelukampanjoita Ukrainassa. APT28 kohdisti tietojenkalastelua Ukrainan asevoimiin, paikallishallintoon (Microsoft, 2022b) sekä media-alan organisaatioihin (Google 2023, s. 19). Uhkatoimija ei ollut aikaisemmin kohdistanut operaatioitaan maiden paikallishallintoon, joten kohde oli uhkatoimijalle epätavallinen (Microsoft, 2022b).

9.2.3 Callisto

Sodan alkuvaiheessa Callisto suoritti laajoja tietojenkalasteluoperaatioita. Maaliskuussa Calliston kohteena olivat ainakin asevoimat useissa Euroopan maissa, Ukrainan puolustusteollisuuden ja valtionhallinnon organisaatiot sekä kansalaisjärjestöt, ajatushautomot, virkamiehet, poliitikot ja toimittajat Yhdysvalloissa (Google, 2023, s. 21). Callisto kohdisti tietojenkalastelua tyypillisiin kohteisiinsa, mutta keskittyi aikaisempaa enemmän Ukrainaan.

9.2.4 UNC1151

Pian sodan alkamisen jälkeen UNC1151 kohdisti tietojenkalastelua Ukrainan asevoimiin, paikallishallintoon (Microsoft, 2022b) ja valtionhallintoon (Google, 2023, s. 25). Uhkatoimijaan liitettyä tietojenkalastelua havaittiin myös muun muassa Puolassa, jossa kohteena olivat valtionhallinnon ja asevoimien organisaatiot (Google, 2023, s. 25).

9.2.5 Nimeämättömät uhkatoimijat

Maaliskuun 13. päivänä tuntematon, todennäköisesti Venäjän valtiollinen uhkatoimija, varasti tietoa Ukrainan ydinturvallisuuteen liittyvästä organisaatiosta. Sama organisaatio oli ollut aikaisemmin Energetic Bear -uhkatoimijan kohteena, mutta kyseistä operaatiota ei ole julkisissa lähteissä liitetty Energetic Beariin. Tietojen varastaminen sijoittui ajankohtaan, jossa venäläiset sotilaat olivat valloittaneet ydinvoimaloita. Samaan aikaan Venäjä myös levitti valheellista tietoa Ukrainan kehittämistä kemiallisista ja biologisista aseista (Microsoft, 2022b). Tietojen varastaminen liittyi todennäköisesti laajempaan kampanjaan, jolla pyrittiin mustamaalaamaan Ukrainaa ja levittämään valheellista informaatiota sen asekehityksestä.

9.3 Palvelunestohyökkäykset ja haktivismi

Palvelunestohyökkäykset alkoivat ennen Venäjän aseellista hyökkäystä ja jatkuivat aktiivisina myös sen jälkeen. Suurin osa palvelunestohyökkäyksistä on ollut yhdistettävissä haktivistiryhmiin, jotka aktivoituivat keväällä 2022.

Haktivistiryhmät väittävät olevansa itsenäisiä ryhmittymiä, jotka tekevät kyberhyökkäyksiä Venäjän puolesta. Haktivistiryhmät ottavat usein kantaa poliittiseen päätöksentekoon esimerkiksi julkaisemalla Telegram-kanavalleen palvelunestohyökkäyksensä kohdelistan ja perustelemalla hyökkäyksensä motiiveja. Motiivit ovat olleet usein poliittisia, esimerkiksi Ukrainalle annettaviin tukipaketteihin liittyviä.

Vaikka haktivistiryhmät toisin väittävät, ainakin osa niistä liittyy todennäköisesti Venäjän valtionhallintoon. Mandiant on yhdistänyt osan haktivistiryhmistä Sandworm-uhkatoimijaan. Sandwormiin yhdistetyt haktivistiryhmät ovat XakNet Team, Infoccentr ja CyberArmyofRussia_Reborn (Mandiant, 2022c). Attribuutio on tehty analysoimalla Sandwormin ja haktivistiryhmien kyberhyökkäyksiä ja niiden yhtymäkohtia.

9.4 Esimerkki informaatio-operaatiosta kybertoimintaympäristössä

Kyberoperaatioiden lisäksi Venäjä suoritti jatkuvasti myös informaatio-operaatioita keväällä 2022. Vaikka informaatio-operaatiot eivät liity suoraan kyberoperaatioihin, suuri osa informaatio-operaatioista toteutettiin kybertoimintaympäristössä. Tässä luvussa annetaan esimerkki informaatio-operaatioista, joka on toteutettu kybertoimintaympäristössä.

Maalis-huhtikuun vaihteessa ukrainalaisille lähetettiin sähköposteja, joissa mustamaalattiin Ukrainan valtionhallintoa. Sähköposteissa esiinnyttiin Mariupolin asukkaana ja väitettiin Ukrainan valtionhallinnon hylänneen Mariupolin asukkaat täysin. Viestissä kehotettiin muun muassa vastustamaan valtionhallinnon levittämiä valheita ja puolustamaan ukrainalaisten oikeuksia (Microsoft, 2022b).

Sähköpostiviestin yksityiskohdat vahvistivat viitteitä informaatio-operaatiosta. Viesti ei sisältänyt esimerkiksi haitallisia linkkejä tai liitetiedostoja, joten sillä ei todennäköisesti pyritty levittämään haittaohjelmaa tai tekemään tietojenkalastelua. Sähköpostit olivat osoitettu suoraan vastaanottajille mainitsemalla heidän nimensä viestissä, millä pyrittiin todennäköisesti herättämään lukijan mielenkiintoa viestiä kohtaan (Microsoft, 2022b). Tapaus on hyvä esimerkki siitä, miten kybertoimintaympäristöä voidaan käyttää informaatiovaikuttamisen välineenä.

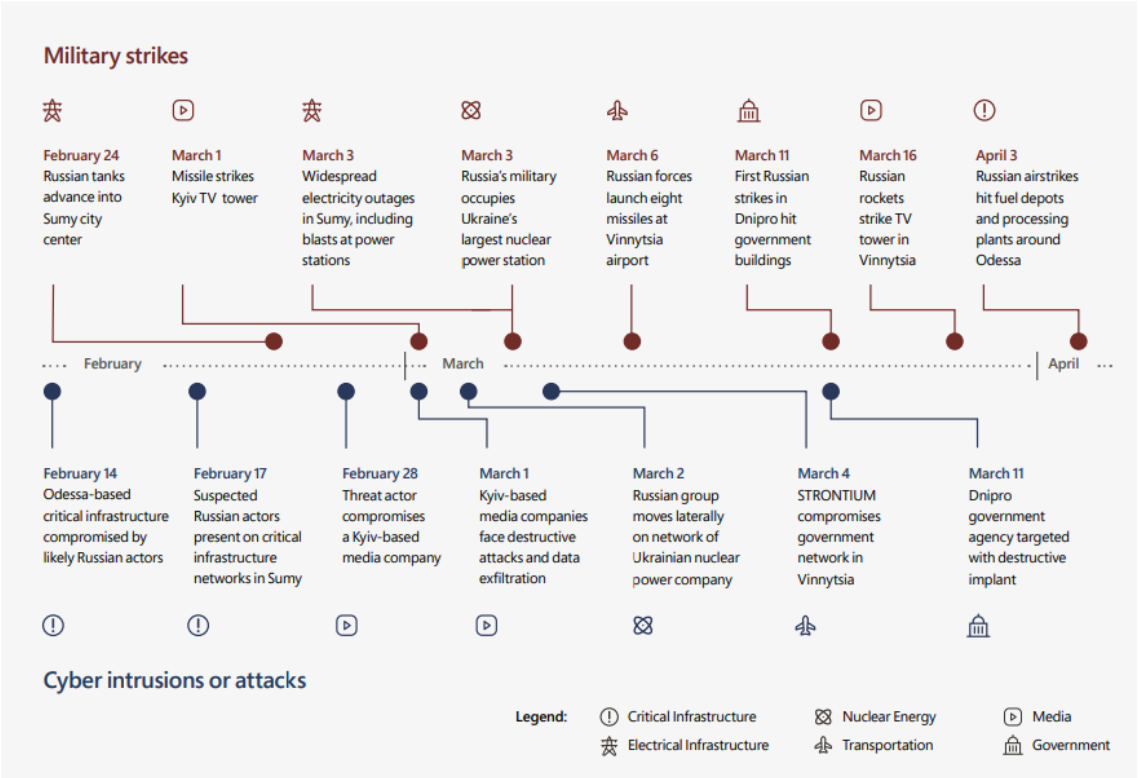
Sähköpostikampanja on yhdistetty uhkatoimija Ember Beariin, joka oli aikaisemmin kohdistanut tietojenkalasteluoperaatioita Ukrainan valtionhallintoon.

Microsoftin (2022b) mukaan informaatiokampanjan kohteiden henkilötiedot olivat todennäköisesti peräisin aikaisemmista tietojenkalastelukampanjoista.

9.5 Kybertoimintaympäristössä tehtyjä havaintoja liitettynä fyysisen maailman tapahtumiin

Sodan ensimmäisten kuukausien aikana kybertoimintaympäristössä tehtiin useita havaintoja, jotka olivat yhdistettävissä niitä seuraaviin tai edeltäviin fyysisen maailman tapahtumiin. Useimmiten kybertoimintaympäristön tapahtumat ajoittuivat siten, että niitä seurasi myöhemmin fyysisen maailman vaikuttamista (Microsoft, 2022b).

Microsoftin tekemä yhteenveto ensimmäisten kuukausien havainnoista esitetään kuviossa 7. Kybertoimintaympäristön havainnoista ei useimmissa tapauksissa ole saatavilla enempää informaatiota, minkä vuoksi niitä ei ole käsitelty tarkemmin. Fyysisten iskujen ja kybertoimintaympäristön havaintojen välistä yhteyttä on haastava todistaa, mutta on todennäköistä, että ainakin osa kuvassa esitetyistä kybertapahtumista oli koordinoitu fyysisen maailman iskujen kanssa.



KUVIO 7 Fyysisen maailman tapahtumiin liitettyjä havaintoja kybertoimintaympäristössä sodan ensimmäisten kuukausien ajalta (Microsoft, 2022b).

10 JOHTOPÄÄTÖKSET

GRU, SVR ja FSB ovat kaikki toimineet aktiivisesti Ukrainassa ennen sodan alkamista ja sen aikana. Kaikki tiedustelupalvelut ovat suorittaneet tietojenkalastelua, mutta GRU on ollut päävastuussa tietoa tuhoavista operaatioista Ukrainassa. GRU:hun liitettyjä uhkatoimijoita on myös yhdistetty haktivistiryhmien toiminnan ohjaamiseen, verkkosivustojen tuhrimishyökkäyksiin ja lukuisiin informaatio-operaatioihin.

Venäjä tehosti tietojenkalasteluaan noin vuosi ennen hyökkäyssodan aloittamista. Venäjän tavoitteena oli todennäköisesti kerätä tietoa Ukrainan valtionhallinnosta, asevoimista, kriittisestä infrastruktuurista ja edellä mainittujen tietojärjestelmistä. Lisäksi Venäjä oli kiinnostunut Ukrainaa tukevien maiden poliittisesta päätöksenteosta ja maiden suhteista Ukrainaan. Tiedon kerääminen tietojenkalasteluoperaatioilla oli todennäköisesti yksi Venäjän tavoista valmistautua aseelliseen hyökkäykseen, valmistella kyberoperaatioita ja ennakoida Ukrainalle annettavaa tukea.

Sodan ensimmäisinä kuukausina Venäjän painopiste kybertoimintaympäristössä oli tietoa tuhoavissa haittaohjelmissa. Tuhoavien haittaohjelmien käyttö väheni selvästi sodan ensimmäisten kuukausien jälkeen, mikä todennäköisesti kertoi Venäjän käyttäneen sotaa varten tietojärjestelmiin valmistellut jalansijat.

Ukrainan ulkopuolella Venäjä on keskittynyt tietojenkalasteluun. Vaikka juuri ennen sotaa ja sodan alkuvaiheessa suurin osa Venäjän kyberoperaatioista kohdistui Ukrainaan, Venäjän mielenkiinto on säilynyt myös muuhun maailmaan, erityisesti Nato-maihin.

Haktivistit ovat olleet näkyvässä roolissa Venäjän ja Ukrainan välisen sodan aikana. Erityisen äänekkäitä ovat olleet venäjämieliset haktivistiryhmät, joiden aktiivisuus on näkynyt paljon Ukrainassa ja sen ulkopuolella. Ryhmät ovat kohdistaneet myös Suomeen palvelunestohyökkäyksiä, joiden motiiveina ovat olleet esimerkiksi Suomen lähettämä aseapu Ukrainaan ja muut Suomen poliittiset päätökset. Ainakin osa haktivistiryhmistä toimii todennäköisesti Venäjän valtionhallinnon ohjauksessa.

Venäjän toteuttamat informaatio- ja kyberoperaatiot ovat liittyneet tiiviisti toisiinsa läpi sodan. Esimerkiksi ukrainalaisten henkilötietoja on vuodettu osana

informaatio-operaatiota, palvelunestohyökkäyksille on annettu avoimesti poliittisia motiiveja ja tietojärjestelmistä vuotaneita sähköpostiosoitteita on käytetty informaatio-operaatioiden kohdelistoina. Tämä ei ole yllättävää, sillä Venäjällä kyberoperaatiot nähdään osana informaatiosodankäyntiä.

Venäjän toteuttamat kyberoperaatiot ovat sisältäneet paljon tuttuja elementtejä menneisyydestä. Esimerkiksi verkkosivustojen tuhrimishyökkäykset ja palvelunestohyökkäykset ovat tuttuja muun muassa Viron pronssisoturikiistasta ja Georgian ja Venäjän välisestä sodasta. Ukrainan sähkönjakeluun kohdistetun Industroyer2-hyökkäyksen puolestaan oli tarkoitus olla kehittyneempi versio vuoden 2016 Industroyer-hyökkäyksestä, jolla saatiin häirittyä Kiovan sähkönjakelua. Tietojenkalastelua Venäjän valtiolliset uhkatoimijat ovat suorittaneet jo pitkään, joten sen näkyminen myös Ukrainassa ja sitä tukevissa maissa ei ole ollut yllättävää. Tietoa tuhoavia haittaohjelmia havaittiin poikkeuksellisen suuri määrä sodan ensimmäisten kuukausien aikana, mutta vastaavia haittaohjelmia on havaittu myös aikaisemmin historiassa, esimerkiksi Industroyer-hyökkäyksessä. Myös tietoa tuhoavien haittaohjelmien naamioiminen kiristyshaittaohjelmaksi on tuttua esimerkiksi NotPetya-hyökkäyksestä. Venäjä kehittää jatkuvasti uusia hyökkäysmenetelmiä ja -työkaluja, mutta operaatioista voidaan tunnistaa myös historiasta tuttuja toimintatapoja.

11 POHDINTA

Ukrainan ja Venäjän välisen sodan ensimmäisten kuukausien kybertapahtumista on saatavilla runsaasti tietoa julkisuudessa, samoin kuin sotaa edeltävien kuukausien kybertapahtumista. Yksityiskohtainen raportointi vähentyi merkittävästi ensimmäisten kuukausien jälkeen, mikä johtuu ainakin osittain kaikista intensiivisimmän kybervaikuttamisen vaiheen päättymisestä. Toinen syy aktiivisen raportoinnin vähentymiselle voi olla se, että yleisesti sotaa edeltäviä ja sodan alkuhetken kybertapahtumia on pidetty kaikista mielenkiintoisimpina. Tässä luvussa pohditaan kybertapahtumien muutoksia ensimmäisten kuukausien jälkeen.

Kevään 2022 jälkeen tietoa tuhoavien haittaohjelmien määrä pieneni, mutta ne eivät loppuneet kokonaan. Vaikka tuhoavat hyökkäykset painottuivat sodan ensimmäiseen vuoteen, vastaavia hyökkäyksiä havaitaan edelleen. Esimerkiksi vuoden 2023 joulukuussa yksi Ukrainan suurimmista teleoperaattoreista, Kyivstar, oli tuhoavan kyberhyökkäyksen kohteena. Hyökkäyksessä tuhottiin suuri määrä tietoa muun muassa työasemilta ja palvelimilta, mikä vaikutti merkittävästi Kyivstarin toimintaan (Balmforth, 2024). Tietoa tuhoavat haittaohjelmat ovat edelleen ajankohtainen uhka, vaikka niiden aktiivisin vaihe oli sodan alussa.

Venäjä on kehittänyt sodan aikana uusia tietoa tuhoavia haittaohjelmia, joista osa on pohjautunut aikaisemmin käytettyihin haittaohjelmiin. Esimerkiksi AcidRain-haittaohjelmasta löydettiin maaliskuussa 2024 kehittyneempi uusi versio, jolle on annettu nimi AcidPour. AcidPour oli todennäköisesti suunniteltu häiritsemään ukrainalaisten teleoperaattoreiden toimintaa, mutta kohteita ei ole vahvistettu julkisuuteen (Guerrero-Saade & Hegel, 2024). Uusien versioiden kehittäminen vanhoista haittaohjelmista ei ole poikkeuksellista.

Tuhoavia kyberhyökkäyksiä on havaittu Ukrainan ulkopuolella todella vähän. Marraskuussa 2022 tehtiin havaintoja tietoa tuhoavasta kiristyshaittaohjelmasta nimeltä Prestige, jolla toteutettiin kyberhyökkäys kuljetus- ja logistiikka-alan organisaatioihin Ukrainassa ja Puolassa (Microsoft, 2023, s. 86). Kyseessä oli ensimmäinen kerta, kun tietoa tuhoava haittaohjelma havaittiin Ukrainan

ulkopuolella sodan alkamisen jälkeen. Muista vastaavista, vahvistetuista tapauksista ei ole ainakaan raportoitu julkisuuteen.

Venäjän tietojenkalasteluoperaatiot ovat kohdistuneet Ukrainaan ja sitä tukeviin maihin ennen sotaa ja sen alkamisen jälkeen. Venäjä pyrki jo vuonna 2021 selvittämään, miten eri maat reagoisivat Venäjän aseelliseen hyökkäykseen ja millaista tukea Ukraina tulisi saamaan. Tietojenkalastelu on jatkunut aktiivisena läpi sodan. Esimerkiksi maaliskuussa 2024 Venäjä kohdisti tietojenkalastelua Saksan puolueisiin, todennäköisesti kerätäkseen tietoa maan poliittisesta päätöksenteosta (Jenkins & Black, 2024). Mielenkiinto Saksaa kohtaan voi selittyä esimerkiksi EU-vaaleilla tai sillä, että Saksa oli vasta päättänyt antavansa Ukrainalle lisää sotilaallista tukea. Vastaavaa toimintaa tullaan lähes varmasti havaitsemaan myös tulevaisuudessa.

Tietojenkalasteluoperaatioiden kohteet ovat muuttuneet ajankohtaisten ilmiöiden mukaan. Vuonna 2023 Venäjän havaittiin kohdistaneen tiedonhankintaa aikaisempaa enemmän Ukrainan lainvalvontaan. Uhkatoimijoita kiinnostivat erityisesti viranomaisten keräämät todisteet Venäjän tekemistä sotarikoksista sekä tiedot oikeudenkäynneistä ja pidätysmääräyksistä (SSSCIP, 2023b).

Tiedonhankintaan on kehitetty sodan aikana myös uusia menetelmiä. Sähköpostikalastelujen lisäksi Venäjä on pyrkinyt saamaan entistä enemmän tietoa myös pikaviestisovellusten, erityisesti Signalin ja Telegramin, kautta (CERT-UA, 2023). Kyseiset pikaviestimet ovat ukrainalaisilla aktiivisessa käytössä, minkä vuoksi niihin on kohdistunut entistä enemmän venäläisten mielenkiintoa.

Toinen uusi tiedonhankintamenetelmä tuli julkisuuteen elokuussa 2023, kun Ukraina kertoi Venäjän hyödyntäneen operaatioissaan taistelukentältä kaapattuja Android-laitteita. Laitteisiin oli asennettu lukuisia haittaohjelmia, joiden avulla pyrittiin saamaan tietoa muun muassa taistelujen suunnittelusta ja johtamisesta (SSU, 2023). Vastaavasta toiminnasta ei ollut aikaisemmin raportoitu julkisuuteen.

Venäläisten haktivistiryhmien tekemät palvelunestohyökkäykset ovat olleet vaikutuksiltaan pieniä, mutta ne ovat saaneet runsaasti medianäkyvyyttä sodan alusta asti. Ryhmien tekemät hyökkäykset ovat kohdistuneet Ukrainaan ja sitä tukeviin maihin, myös Suomeen. Esimerkiksi helmikuussa 2024 haktivistiryhmä NoName057(16) otti kantaa Suomen lakkoihin ja ilmoitti tekevänsä suomalaisille verkkosivustoille palvelunestohyökkäyksiä ”tyytymättömien suomalaisten puolesta” (Palvaila, 2024). Ryhmät ovat usein ottaneet kantaa maiden ulko- ja sisäpoliittisiin päätöksiin. On todennäköistä, että ainakin osa haktivistiryhmistä toimii Venäjän valtionhallinnon ohjauksessa (Mandiant, 2022c). Haktivistiryhmien kytköksiä Venäjän valtionhallintoon on haastava todistaa.

Venäjä on kohdistanut sodan aikana jatkuvasti erilaisia kyberhyökkäyksiä Ukrainaan. Vaikka kyberoperaatioita on kohdistettu myös Ukrainan kriittiseen infrastruktuuriin, niiden kokonaisvaikutukset ovat jääneet julkisten raporttien perusteella odotettua pienemmiksi. Kyberoperaatioilla on todennäköisesti pyritty tukemaan fyysisen maailman tapahtumia, missä on todennäköisesti ainakin osittain onnistuttu. Ukrainassa havaittiin eniten Venäjän suorittamia

kyberoperaatioita sodan ensimmäisten kuukausien aikana, mutta Venäjä on jatkanut operaatioitaan läpi sodan.

Kyberoperaatioiden todellisten vaikutusten arviointi on haastavaa. Vaikka Ukraina on julkaissut tietoa kybertapahtumista melko avoimesti, tarkat kohdeorganisaatiot ja kybertapahtumien vaikutukset eivät usein päädy julkisuuteen. Tämä vaikeuttaa todellisten vaikutusten ja kyberoperaatioiden onnistumisen arviointia.

Kyberoperaatioiden todellisten vaikutusten arviointia vaikeuttaa myös se, että operaatiot voivat paljastua jopa vuosien viiveellä. Haittaohjelmat voidaan pyrkiä pitämään salassa, jotta uhkatoimija säilyttää jalansijansa kohdejärjestelmässä mahdollisimman pitkään. Esimerkiksi huhtikuussa 2024 julkaistiin tietoa Kapeka-haittaohjelmasta, jota on käytetty Keski- ja Itä-Euroopan maissa, todennäköisesti myös Ukrainassa, jo vuonna 2022 (Nejad, 2024). On tyypillistä, että kyberoperaatioiden yksityiskohtien selvittäminen ja julkaiseminen voivat viedä jopa vuosia.

LÄHTEET

Antoniuk, D. (15.2.2022). DDoS attacks hit Ukrainian government websites. *The Record from Recorded Future News.* https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces

Balmforth, T. (5.1.2024). Exclusive: Russian hackers were inside Ukraine telecoms giant for months. *Reuters*. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

Berger, M. (26.2.2022). 400,000 Ukrainians flee to European countries, including some that previously spurned refugees. *The Washington Post*. https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/

Boutin, J-I. (11.6.2020). Gamaredon group grows its game. *WeLiveSecurity.* https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

Brady, S. (3.10.2018). *Indictment – United States of America v. ALEKSEI SERGEYEVICH MORENETS, et al.* https://www.justice.gov/opa/page/file/1098481/download

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center For Cyber Intelligence Analysis and Threat Research Hanover Md.

Cardiffin yliopisto. (2023). *The Ghostwriter campaign as a multi-vector information operation.* https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf

Cimpanu, C. (14.1.2022). Hackers deface Ukrainian government websites. *The Record from Recorded Future News.* https://therecord.media/hackers-deface-ukrainian-government-websites

CERT-EU. (2023). *Russia's war on Ukraine: one year of cyber operations.* https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

CERT-UA. (22.3.2022). Cyber attack on Ukrainian enterprises using the DoubleZero destructor program (CERT-UA#4243). https://cert.gov.ua/article/38088

CERT-UA. (13.7.2023). Summary information on the activities of the UAC-0010 group as of July 2023. https://cert.gov.ua/article/5160737

Cherepanov, A. & Lipovsky, R. (12.6.2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. *WeLiveSecurity*.

https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

CISA. (9.5.2023). Hunting Russian Intelligence "Snake" Malware. *Cybersecurity Advisory*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

CISA, FBI, National Security Agency (United States), Australian Cyber Security Centre, Canadian Centre for Cyber Security, National Cyber Security Centre (New Zealand), National Cyber Security Centre (United Kingdom), National Crime Agency (United Kingdom). (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.* https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/0/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2021). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448.

CrowdStrike. (12.2.2019). Who is FANCY BEAR (APT28)?. *CrowdStrike Blog.* https://www.crowdstrike.com/blog/who-is-fancy-bear/

CrowdStrike. (30.3.2022). Who is EMBER BEAR?. *CrowdStrike Blog.* https://www.crowdstrike.com/blog/who-is-ember-bear/

DOJ. (19.10.2020). Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. *Office of Public Affairs, Department of Justice.* https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

DOJ. (7.12.2023). Two Russian Nationals Working with Russia's Federal Security Service Charged with Global Computer Intrusion Campaign. *Office of Public Affairs, Department of Justice.* https://www.justice.gov/opa/pr/two-russian-nationals-working-russias-federal-security-service-charged-global-computer

Galeotti, M. (2016). *Putin's hydra: inside Russia's intelligence services*. London: European Council on Foreign Relations.

Elo, S., Kajula, O., Tohmola, A. & Kääriäinen, M. 2022. Laadullisen sisällönanalyysin vaiheet ja eteneminen. Hoitotiede. 34 (4), 215-225.

ESET. (1.3.2022a). IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. *WeLiveSecurity*. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

ESET. (12.4.2022b). Industroyer2: Industroyer reloaded. *WeLiveSecurity.* https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

ESET. (24.2.2023). A year of wiper attacks in Ukraine. *WeLiveSecurity.* https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/

European Space Policy Institute (ESPI). (2022). *The War in Ukraine from a Space Cybersecurity Perspective.* https://www.espi.or.at/reports/new-espi-short-report%E2%80%95the-war-in-ukraine-from-a-space-cybersecurity-perspective/

FireEye. (2017). *APT28: At the centre of the storm.* https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

F-Secure. (2017). *Callisto Group.* https://www.f-secure.com/content/dam/f-secure/en/labs/whitepapers/Callisto_Group.pdf

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired, August*, *22*.

Global Affairs Canada. (2021). *Statement on SolarWinds Cyber Compromise.* https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html

Google. (2023). *Fog of War - How the Ukraine Conflict Transformed the Cyber Threat Landscape.* https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

GOV.UK. (2021). *Russia: UK exposes Russian involvement in SolarWinds cyber compromise.* https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise

Greig, J. (11.8.2023). NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation. *The Record. Recorded Future News.* https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions

Guerrero-Saade, J., & Hegel, T. (21.3.2024). AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine. *SentinelLabs.* https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/

Guerrero-Saade, J., & van Amerongen M. (31.3.2022). AcidRain | A Modem Wiper Rains Down on Europe. *SentinelLabs.* https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Harbison, M., & Renals, P. (19.7.2022). Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive. *Unit 42 Blog.*

https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49-60.

Holt, R. (21.3.2022). *Sandworm: A tale of disruption told anew.* https://www.welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/

ISO/IEC 27005: 2018. (2018). *Information Technology. Security Techniques. Information Security Risk Management: ISO/IEC 27005: 2018*. International Organization for Standardization.

Jenkins, L., & Black, D. (22.3.2024). APT29 Uses WINELOADER to Target German Political Parties. *Mandiant Threat Intelligence*. https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, *3*(4), 237-245.

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). # kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. *Julkaisusarja 3: Työpapereita nro 12*.

Lee, R., Assante, M., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, *388*, 1-29.

Lee, R. M., Assante, M. J., & Conway, T. (2017). Crashoverride: Analysis of the threat to electric grid operations. *Dragos Inc., March*.

Lehto, M. (2014). Kybertaistelu ilmavoimaympäristössä. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 157–177). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317-3318.

Lobel, H. (2011). Cyber war inc.: The law of war implications of the private sector's role in cyber conflict. *Tex. Int'l LJ*, *47*, 617.

Malpedia. (2022). *Callisto*. https://malpedia.caad.fkie.fraunhofer.de/actor/callisto

Mandiant. (20.7.2022a). Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities. *Mandiant Threat Intelligence*. https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities

Mandiant. (27.4.2022b). Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. *Mandiant Threat Intelligence*. https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

Mandiant. (23.9.2022c). Hacktivists Collaborate with GRU-sponsored APT28. *Mandiant Threat Intelligence*. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

McFail, M., Hanna, J., & Rebori-Carretero, D. (2022). *Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study*. MITRE CORP MCLEAN VA.

Microsoft. (2022a). *Microsoft Digital Defense Report 2022.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Microsoft. (2022b). *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Microsoft. (2023). *Microsoft Digital Defense Report 2023.* https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

MITRE. (2022). *Groups*. https://attack.mitre.org/groups/

MSTIC. (2022). Disrupting SEABORGIUM's ongoing phishing operations. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/

Nejad, M. (2024). Kapeka: A novel backdoor spotted in Eastern Europe. *WithSecure Intelligence*. https://labs.withsecure.com/publications/kapeka

NIST. (2020). NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0.

Oladimeji, S., & Kerner, M. S. (3.11.2023). SolarWinds hack explained: Everything you need to know. *TechTarget*. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Teoksessa *Proceedings of the 7th European Conference on Information Warfare* (s. 163). Reading, MA: Academic Publishing Limited.

Palvaila, J. (2.2.2024). Kysyimme, miksi hakkeri haluaa kaataa suomalaisen pikkukaupungin kotisivun – tutkija: Venäjän informaatiosotaa. *Yle*. https://yle.fi/a/74-20072707

Raggi, M., & Cass, Z. (1.3.2022). Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement. *Proofpoint*. https://www.proofpoint.com/au/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

Recorded Future. (2022). *Overview of the 9 Distinct Data Wipers Used in the Ukraine War.* https://go.recordedfuture.com/hubfs/reports/mtp-2022-0512.pdf

Roncone, G., Wahlstrom, A., Revelli, A., Mainor, D., Riddell, S., & Read, B. (16.11.2021). UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests. *Mandiant's Cyber Security Blog*. https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government

Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia. *European Affairs, 9*(1–2).

Sadowski, J. & Hall, R. (4.3.2022). Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation. *Mandiant's Cyber Security Blog.* https://www.mandiant.com/resources/blog/russia-invasion-ukraine-retaliation

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Secureworks. (24.7.2019). Resurgent Iron Liberty Targeting Energy Sector. *Threat Intelligence Research.* https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector

Secureworks. (25.2.2022). Disruptive HermeticWiper attacks targeting Ukrainian organizations. *Cybersecurity threat intelligence blogs*. https://www.secureworks.com/blog/disruptive-hermeticwiper-attacks-targeting-ukrainian-organizations

Slowik, J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. *Dragos, Inc*.

SSSCIP. (2023a). *Russia's Cyber Tactics: Lessons Learned 2022.* https://cip.gov.ua/services/cm/api/attachment/download?id=53466

SSSCIP. (2023b). *Russia's Cyber Tactics H1 2023*. https://cip.gov.ua/services/cm/api/attachment/download?id=60068

SSU. (2021). *Gamaredon/Armageddon Group. FSB RF cyber attacks against Ukraine.* https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armageddon.pdf

SSU. (2023). *Cyber operation of russian intelligence services as a component of confrontation on the battlefield.* https://ssu.gov.ua/uploads/files/DKIB/technical-report.pdf

Symantec. (20.10.2017). Dragonfly: Western energy sector targeted by sophisticated attack group. *Symantec Enterprise Blogs - Threat Intelligence.* https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Tidy, J. (12.4.2022). Ukrainian power grid 'lucky' to withstand Russian cyber-attack. *BBC News*. https://www.bbc.com/news/technology-61085480

Toulas, B. (2022). *Russian hackers perform reconnaissance against Austria, Estonia.* https://www.bleepingcomputer.com/news/security/russian-hackers-perform-reconnaissance-against-austria-estonia/

Valkoinen talo. (15.4.2021). FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government. *Statements and releases.* https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Ventura, V. (23.2.2021). Gamaredon - When nation states don't pay all the bills. *Cisco Talos Intelligence Blog.* https://blog.talosintelligence.com/gamaredonactivities/

Viasat. (30.3.2022). KA-SAT Network cyber attack overview. *Corporate News.* https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

WADA. (5.10.2016). Cyber Security Update: WADA's Incident Response. https://www.wada-ama.org/en/news/cyber-security-update-wadas-incident-response

Willett, M. (2021). Lessons of the SolarWinds hack. *Survival*, *63*(2), 7-26.