Tampereen yliopisto

Akseli Piilola

KYBERASEIDEN OMINAISUUKSIA JA KYVYKKYYKSIÄ

Kirjallisuuskatsaus ja luokittelu

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Kesäkuu 2023

TIIVISTELMÄ

Akseli Piilola: Kyberaseiden ominaisuuksia ja kyvykkyyksiä
Pro gradu -tutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Kesäkuu 2023

Kybersodankäynti ja kyberaseet ovat viime aikoina olleet paljon esillä mediassa. Kyberhyökkäyksiä pidetään yleisesti yhtenä suurimmista valtioihin kohdistuvista uhista, minkä lisäksi sekä läntisten että itäisten valtioiden suorittamia kyberoperaatioita on vuosien saatossa saatu enenevissä määrin paljastettua ja niissä käytettyjä ohjelmistoja tutkittua. Viimeisimpänä vain muutama viikko ennen tämän työn valmistumista paljastunut venäläinen haittaohjelma Snake, jonka epäillään vakoilleen läntisen liittouman valtioita jo lähes 20 vuotta.

Tässä tutkielmassa perehdytään valikoituun joukkoon kyberaseita ja vertaillaan niiden kyvykkyyksiä neljässä eri kategoriassa: tyyppi ja alkuperä, aika ensimmäisestä tartunnasta havaitsemiseen, leviämistapa, sekä havaitsemisen ja analysoinnin estäminen. Pohjatietona lukija perehdytetään kyberaseiden historiaan ja määritelmään. Tavoitteena on muodostaa tutkielman lukijalle kuva siitä mitä kyberaseet ovat, miten ne toimivat, mitä niiden avulla yritetään saavuttaa ja miten ne ovat muuttuneet vuosien varrella. Lisäksi tutkielmassa pohditaan eroavaisuuksia eri toimijoiden käyttämien ja kehittämien kyberaseiden välillä. Loppuyhteenvedossa pohditaan kyberaseiden tulevaisuuden näkymiä sekä hyökkäyksen että puolustautumisen näkökulmasta.

Tutkielman lopputuloksena havaittiin selkeitä trendejä kaikkien neljän käsiteltävän osa-alueen suhteen. Huomionarvoista on kuitenkin se, että käytössä oli vain hyvin pieni otanta jo tunnettuja ja analysoituja kyberaseita. On mahdollista ja erittäin todennäköistä, että isoilla toimijoilla on laaja valikoima myös sellaisia aseita, joita ei ole vielä havaittu ja joita ei ole päästy analysoimaan. Tämä täytyy ottaa huomioon tutkielman lopputuloksia käsiteltäessä. Lisäksi osa aseista on paljastunut maailmanpoliittisten tilanteiden kuten sotien ansiosta – ja näihin sotiin on tosiasiallisesti ollut osallisena vain hyvin rajallinen määrä vahvoja kyberkyvykkyyksiä omaavista valtioista. Mikäli esimerkiksi USA, Israel, tai Kiina ajautuisivat osaksi isompia konflikteja, saattaisimme nähdä täysin uudenlaisia kyberoperaatioita ja -aseita.

Avainsanat: Kyberaseet, Kybersodankäynti, Kyberoperaatiot, Haittaohjelmat, Duqu, Duqu 2.0, Flame, NotPetya, Pegasus, HermeticWiper, CaddyWiper, IsaacWiper, Snake, Sutxnet, WannaCry

1 Johdanto

Vuonna 2013 Yhdysvaltain kansalliselle turvallisuusvirastolle työskennellyt Edward Snowden järisytti maailmaa vuotamalla suuren määrän huippusalaiseksi luokiteltuja dokumentteja, jotka käsittelivät pitkälti kyseisen viraston verkossa harjoittamaa tiedustelutoimintaa. Vuodetuista asiakirjoista paljastui mm. viraston alaisuudessa toimivan *Tailored Access Operations* -yksikön kyvykkyys murtautua useimpiin yleisesti käytettyihin atk-laitteisiin ja ohjelmistoihin. Lisäksi dokumenttien mukana vuodettiin listaus yksikön kehittämistä työkaluista ja niiden kyvykkyyksistä. Vuonna 2014 italialainen valtiollisille toimijoille kybertiedusteluun tarkoitettuja työkaluja kehittävä yritys *Gamma Group* joutui tietomurron uhriksi. Vuodon seurauksena julkisessa internetissä julkaistiin paitsi lähdekoodia myös suuri määrä dokumentteja, joissa kuvattiin yksityiskohtaisesti yrityksen kehittämien työkalujen toimintamallia ja kyvykkyyksiä. Vuonna 2015 oli niin ikään italialaisen viranomaisille kybertiedusteluun ja tietomurtojen suorittamiseen tarkoitettuja työkaluja kehittävän ja myyvän Hacking Teamin vuoro tulla hakkeroiduksi. Tämän seurauksena internetissä julkaistiin jälleen kerran joukko työkalujen lähdekoodia, sekä suuri määrä yrityksen sisäisiä dokumentteja. Vuonna 2016 oli NSA:n vuoro tulla hakkeroiduksi. Tällä kertaa internetissä julkaistiin lukuisia tiedustelupalvelun kehittämiä työkaluja sekä useita entuudestaan tuntemattomia haavoittuvuuksia. Esimerkiksi huomattavan paljon julkisuutta saanut EternalBlue on peräisin kyseisestä tietomurrosta. Näiden tapahtumien jälkeen tuskin kenellekään oli epäselvää, että kybersodankäynnin kyvykkyyttä kehitetään aktiivisesti ympäri maailman sekä valtiollisten toimijoiden että yksityisten yritysten toimesta. Edellä mainitut 2010-luvun tietomurrot yhdistettynä viimeaikaisiin maailmanpoliittisiin tapahtumiin ovat antaneet aiheen tutkia tarkemmin kybersodankäyntiä sekä sen mahdollisia vaikutuksia.

Tutkielman aiheen merkityksellisyyteen ja ajankohtaisuuteen vaikuttaa lisäksi se, että myös perinteistä sotaa käydään etenevissä määrin kyberavaruudessa. Jo nyt on olemassa esimerkkejä, viimeisimpänä meneillään olevasta Venäjän ja Ukrainan välisestä sodasta, joissa kyberoperaation onnistuminen johtaa suoraan henkilötappioihin – ja vastaavasti sen torjunnan nopeus ja tehokkuus korreloi suoraan säästettyjen ihmishenkien määrään. Kyberoperaatioilla osana sodankäyntiä on siis kiistatta olemassa oleva merkitys, jota ei ainakaan tarkemmin tutkimatta voida vähätellä.

Tämän tutkielman tavoitteena on selvittää ja vertailla jo tunnettujen ja hyvin tutkittujen aikaisemmissakin esimerkeissä mainittujen kyberaseiden ominaisuuksia ja kyvykkyyksiä, sekä muodostaa lukijalle kattava kuva siitä miltä moderni kybersodankäynnin taistelukenttä näyttää.

1.1 Aikaisempi tutkimus

Kybersodankäyntiä on aiheena tutkittu paljon, joskin julkaistu aineisto on osin myös hyvin ristiriitaista. Osa tutkijoista on sitä mieltä, että kyseessä on oikean sodankäynnin rinnalla lähes merkityksetön nörtti-ilmiö. Toiset taas ovat sitä mieltä, että kyseessä on yksi suurimpia tulevaisuuden uhkakuvia maailmanrauhalle ja yleiselle turvallisuudelle. Aiheesta on myös kirjoitettu useita kirjoja, joiden avulla lukija saa hyvän kokonaiskuvan kybersodankäynnistä ja sen mahdollisista vaikutuksista maailmalle. Näistä mainittakoon esimerkiksi Fred Kaplanin [2017] kirjoittama *Dark Territory: The Secret History of Cyber War*, joka kertoo tiivistää hyvin kybersodankäynnin tähänastista historiaa.

Useat tutkijat ovat myös huomioineet kybersodankäyntiin liittyvän lainsäädännöllisen tyhjiön ja sen aiheuttamat ongelmat. Näistä mainittakoon esimerkiksi Kerttunen [2018] ja Stevens [2017]. Osittain tämän takia jo pelkkä kybersodankäynnin ja kyberaseen määritelmä on hyvin ongelmallinen. Tässä tutkielmassa perehdytään tarkemmin kyberaseiden määritelmään luvussa 4.

Kyberaseista itsestään sen sijaan on tehty lukuisia tutkimuksia ja teknisiä analyysejä. Ohjelmistoja on takaisinmallinnettu, niiden salauksia on purettu sekä toimintaa selvitetty. Komentopalvelinten sijainteja ja omistavien yritysten nimiä on saatu selville. Digitaalisen forensiikan tutkimusalalla on onnistuttu jälkeenpäin selvittämään kokonaisia hyökkäysketjuja. Myös ohjelmistojen kehityksen takana olleita tahoja on pystytty lähes varmuudella tunnistamaan. Näihin talkoisiin ovat kantaneet kortensa kekoon niin yliopistojen tiedekunnat ja tutkijat kuin monikansallisten pörssiyritysten alaisuudessa toimivat yksityiset laboratoriot.

Tutkielman lähdemateriaali nojaa pitkälti näihin teknisiin raportteihin ja analyyseihin, mutta mukaan on mahdollisuuksien mukaan otettu myös yliopistojen tuottamia akateemisia vertaisarvioituja tutkimuksia. Käytetty lähdemateriaali poikkeaa luonteeltaan ehkä hieman perinteisesti opinnäytetöissä käytetyistä materiaaleista. Suurin osa haittaohjelmien teknisistä analyyseista tuotetaan yleisesti ottaen yksityisten yritysten alaisuudessa toimivien laboratorioiden tai tutkimusyksiköiden toimesta, eikä näitä tuotoksia läheskään aina julkaista alan tunnetuissa akateemisissa julkaisuissa. Yritykset julkaisevat pääsääntöisesti näitä tutkimuksia ja niistä johdettuja reportaaseja omien verkkosivujensa, blogiensa, tai asiakaskanaviensa kautta. Tämä johtaa usein siihen, että ko. tutkimukset eivät ole samalla tavalla vertaisarvioituja, kuin monet muut akateemiset tekstit. Lisäksi osassa tutkimusyksiköitä vallitseva käytäntö on tuottaa julkaisuja yrityksen nimellä ja jättää varsinaisten tutkijoiden nimet pois julkaisusta. Edellä mainittujen seikkojen johdosta tutkimuksen lähteenä käytettyä materiaalia tuottaneet tahot on erikseen esitelty luvussa 4 ja niistä jokaisen kohdalla on erikseen esitetty perustelut siitä, miksi kyseisen laitoksen tuottamia tekstejä on hyväksytty lähdemateriaaliksi. Luonnollisestikin vähänkään tuntemattomampien, tai muuten sellaisten tahojen, joiden laadusta ei voida riittävällä varmuudella

mennä takuuseen, tuottamaa materiaalia ei ole käytetty tutkimuksen lähteenä. Tämä on myös johtanut siihen, että kaikkia haluttuja kyberaseita ei voitu ottaa mukaan tutkielmaan, sillä osasta ei löytynyt riittävän laadukkaan ja luotettavan tahon tuottamaa teknistä analyysiä.

1.2 Tutkimusongelma ja -kysymykset

Aikaisempi tutkimus aiheesta on perehtynyt lähinnä kybersodankäyntiin käsitteenä, ja on muutenkin ollut hyvin pohdiskelevaa. Konkreettista vertailututkimusta kyberoperaatioista ja niiden vaikutuksista on kovin vähän saatavilla. Tämän tutkielman tavoitteena on muodostaa kelvollinen kehikko kyberaseiden vertailuun sekä tarjota muuten hankalasti saatavilla olevaa pohjatietoa mahdollisia tulevia tarkempia tutkimuksia varten. Vertailukohteet on tässä tutkielmassa rajattu puhtaasti kyberaseisiin ja siten käytännössä haittaohjelmiin. Yhteenveto tehdään kokoamalla jo selvitetyt asiat yhteen sellaisessa muodossa, että se on myös vähemmän aiheeseen perehtyneen lukijan ymmärrettävissä. Lisäksi koostettua tietoa analysoidaan ja sen perusteella pyritään muodostamaan järkeviä ja luotettavia johtopäätelmiä, joita voidaan mahdollisesti hyväksikäyttää tulevan tutkimuksen pohjana. Esimerkiksi tutkielmassa pohditaan jo tunnistettujen kyberaseiden alkuperän ja tyypin välistä korrelaatiota, sekä sen merkitystä tulevaisuutta ajatellen. Tulevaisuutta ajatellen myös muunlaiselle tutkimukselle olisi varmasti käyttöä – esimerkiksi kyberoperaatioita suorittavista yksiköistä (tiedustelupalvelut, yksityiset yritykset, sotilasorganisaatiot, yms.) voisi tuottaa vastaavanlaista vertailua, sillä esimerkiksi tietoa tässäkin tutkielmassa käsiteltävien kyberaseiden kehittäjistä on kyllä saatavilla.

1.3 Tutkielman eteneminen

Tutkielmassa käsitellään ensin luvussa 2 kybersodankäynnin ja kyberaseiden historiaa, minkä jälkeen luvussa 3 esitellään lukijalle pohjatiedoksi tarkemmin kolme paljon julkisuutta saanutta ja hyvin tunnettua valtiollista kyberoperaatiota. Luvussa 4 tutkielma johdattaa lukijan kybersodankäynnin ja kyberaseiden määritelmiin, joiden osalta pohditaan mm. tämänhetkiseen määritelmään liittyvää problematiikkaa ja esimerkiksi siitä johtuvia juridisia seurauksia. Myöhemmin samassa luvussa esitellään valikoitu joukko tunnettuja ja hyvin tutkittuja kyberaseita. Luvussa 5 kyberaseita analysoidaan osatekijöistään lähtien ja niiden ominaisuuksia ja kyvykkyyksiä vertaillaan neljässä eri kategoriassa: 1) tyyppi ja alkuperä, 2) aika ensimmäisestä tartunnasta havaitsemiseen, 3) leviämistapa, sekä 4) havaitsemisen ja analysoinnin esto. Luvussa 6 on yhteenveto ja pohdinta, minkä jälkeen luvussa 7 esitetään loppupäätelmät tutkielman tekijän näkökulmasta.

2 Kybersodankäynnin historiaa

Kesällä 1983 julkaistu Sotaleikit (*Wargames*) -elokuva esitti aikoinaan suurille massoille skenaarion, jossa nuori hakkeri pelaa peliä ydinaseita hallitsevan supertietokoneen kanssa

ja on lähellä aloittaa ydinsodan USA:n ja Neuvostoliiton välillä. Sotaleikit oli aikoinaan ensimmäinen suurille massoille esitetty elokuva, jonka teemana oli kybermaailman yhdistäminen sodankäyntiin. Elokuva aiheutti valtavan mediaspektaakkelin aiheen ympärille. Tiedostusvälineet ympäri maailman haastattelivat asiantuntijoita ja pohtivat, voisiko elokuvassa kuvattu skenaario toteutua oikeassa elämässä. Aiheeseen kerrotaan havahtuneen muiden joukossa myös USA:n silloisen presidentin Ronald Reaganin, joka määräsi välittömästi korkea-arvoisen kenraalinsa selvittämään asiaa. Viikkoa myöhemmin presidentin kerrotaan saaneen huolestuttavan vastauksen: ”Herra presidentti. Ongelma on paljon pahempi, kuin mitä pelkäsitte.” [Kaplan 2017]

Kybersodankäynnillä tarkoitetaan yleisesti sodankäynnin muotoa, jossa sotatoimiin verrattavia operaatioita suoritetaan kyberavaruudessa, eli tuttavallisemmin internetissä tai muulla tavoin tietokoneiden välityksellä. Lähteestä riippuen kybersodankäynniksi on määritelty kaikkea mahdollista informaatiovaikuttamisesta toisen valtion alueella tapahtuviin tietomurtoihin. Tässä tutkielmassa emme tarkemmin ota kantaa kybersodankäynnin määritelmään, sillä tutkielman aiheena ovat kyberaseet. Kyberaseiden määritelmästä taas puhutaan enemmän luvussa 4. Todetkaamme kuitenkin kybersodankäynnin olevan määritelmästä riippumatta todellinen ja varmasti tulevaisuudessa myös kasvava, sekä koko ajan enemmän vaikuttava ilmiö. Tämä on luonnollista, sillä perinteisetkin sodankäynnin operaatiot ja niissä käytettävä laitteisto nojaa yhä enemmän kybermaailmaan – kentältä saatetaan esimerkiksi siirtää tilannekuvaa johtokeskukseen internetin yli, ohjusjärjestelmät nojaavat tietoliikennetekniikkaan etsiessään kohdettaan, ja pommeja tiputetaan vihollisen niskaan kauko-ohjattavilla tai ennalta ohjelmoitavilla drooneilla.

Yksi huomionarvoinen seikka kybersodankäynnistä on kuitenkin todettava. Toistaiseksi kansainväliset sodankäynnin säännöt eivät juurikaan ota kantaa kybersodankäyntiin, eikä kybersodankäyntiä ole em. säännöksissä oikeastaan edes määritelty. Tämän takia esimerkiksi rajanveto valtiollisen kiusanteon ja kybersodankäynnin välillä saattaa olla hyvin hankalaa, ja eri lähteet saattavatkin käsitellä samoja asioita eri nimillä. Esimerkkinä voisi olla valtiollismielisen hakkeriryhmän suorittama tietomurto, jota voidaan toisessa lähteessä käsitellä kybersodankäyntinä ja toisessa taas terroristitekona. Vastaava ongelma on luonnollisesti myös kyberaseissa. Siinä missä toinen lähde voi puhua vahingossa leviävästä haittaohjelmasta, saatetaan toisessa lähteessä puhua valtion kehittämästä kyberaseesta. Tämä epäselvyys mahdollistaa myös täysimittaisten valtiollisten kyberoperaatioiden suorittamisen vihollisen maaperällä ilman, että tekoa voidaan tuomita esimerkiksi sotatoimena tai sodan aloittamisena. Voinemme kuitenkin olettaa kyberoperaatioiden yleistyessä osana sodankäyntiä myös näihin sääntöihin tulevan odotettavissa olevia muutoksia. [Robinson ja muut 2015]

3 Esimerkkejä valtiollisista kyberoperaatioista

Tässä luvussa esitellään lukijalle pohjatiedoksi joukko suurvaltojen suorittamia ja hyvin tunnettuja kyberoperaatioita. Tarkoitus on muodostaa lukijalle korkean tason kuva jo tapahtuneista ja varmennetuista kyberoperaatiosta, sekä niiden aiheuttamista vaikutuksista.

Luvussa 3.1 esitellään operaatio Infektio, jonka avulla Neuvostoliitto sai viime vuosituhannen loppupuolella levitettyä valeuutisia USA:n valtion osallisuudesta HIV:n alkuperään uutislehtiin ympäri maailman. Aiheesta kirjoitettiin lopulta myös suomalaisessa sanomalehdessä. Luvussa 3.2 on toisena vuorossa operaatio Olympic Games, jonka varjolla USA harjoitti tarkoin kohdennettua vakoilua Euroopassa ja Lähi-Idässä vuosikausia. Operaatio Olympic Gamesin tuotoksia on mm. aikoinaan ansaitusti paljon palstatilaa saanut mato nimeltä Stuxnet. Lopuksi luvussa 3.3 tutustutaan tämän opinnäytetyön kirjoitushetkellä vielä meneillään olevaan Venäjän ja Ukrainan väliseen sotaan ja siihen, miten kyberoperaatiota on käytetty hyväksi puolin ja toisin sekä konfliktin aikana että sitä ennen. Mainittavia tapahtumia ovat mm. satelliittien tilaaminen Elon Muskilta Twitterin välityksellä, sekä innokkaiden IT-asiantuntijoiden rekrytointi viestintäpalvelu Telegrammissa johdettuun Ukrainan IT-armeijaan. Sivutaanpa luvussa myös presidentinvaaleissa käytettyyn ääntenlaskentajärjestelmään murtautumista ja sen manipuloimista.

3.1 Operaatio ”INFEKTIO” – lyhyt historia harhaanjohtamisesta

”Sodan ensimmäinen uhri on totuus”
-Hiram W. Johnson, 1917

Disinformaation levittäminen konfliktien yhteydessä ei ole mikään uusi ilmiö. Todennäköisesti jokainen sotaa käynyt tai käymätön valtio on enemmän tai vähemmän syyllinen väärän, tai ainakin puolueellisen informaation levittämiseen. Disinformaatio on kuitenkin vaarallinen ja petollisen toimiva ase, jonka käytössä on kunnostautunut etenkin Neuvostoliitto ja sittemmin Venäjä. Näistä jälkimmäisen väitetään esimerkiksi UK:n parlamentin tiedustelu- ja turvallisuusvaliokunnan (*Intelligence and Security Committee of Parliament, ISC*) vuonna [2020] julkaiseman ”The Russia Reportin” mukaan olleen vahvasti mukana masinoimassa Brexitiä disinformaatiota ja muita siihen liittyviä työkaluja hyväksikäyttäen – todennäköisesti aiheuttaakseen eripuraa ja vähentääkseen Euroopan Unionin koheesiota, sekä eurooppalaisten yhtenäisyyden tunnetta. Väitetäänpä samaisessa lähteessä venäläisten olleen vaikuttamassa myös Skotlannin itsenäistymisyrityksessä ja monessa muussakin poliittisessa tapahtumassa.

Edellä mainituille lähteille ei kuitenkaan koskaan löytynyt vedenpitäviä todisteita, joten jätetään ne omaan arvoonsa, ja keskustellaan hetki hyvin dokumentoidusta ja jälkikäteen varmennetusta, oikeasta disinformaatiokampanjasta, eli operaatio Infektiosta. Vaikka kyseisen operaation suorittamiseen ei varsinaisesti sana ”kyber” juurikaan liittynyt, niin voidaan sitä silti hyvästä syystä pitää osana kybersodankäyntiä, sillä kyseinen

operaatio on ollut isossa osassa vaikuttamassa nykyiseen puhtaasti kybermaailmassa käytävään disinformaatiosotaan osana muuta kybersodankäyntiä. Oikeastaan voidaan todeta operaatio Infektion olleen oman aikansa kybersodankäyntiä – kyseisellä ajanjaksolla ”kyber” ei vain sanan varsinaisessa merkityksessä vielä juurikaan sisältänyt internettiä, tietokoneita, tai muita nykyisen kybersodankäynnin elementtejä.

Operaatio Infektion, alkuperäiseltä nimeltään operaatio Denver, on hyvin dokumentoitu ja sen kulku vahvistettu useista lähteistä Neuvostoliiton hajoamisen jälkeen. Operaatiosta on kirjoitettu paljon tiivistelmiä, ja siihen liittyvää materiaalia voi kukin käydä tutkailemassa esimerkiksi Stasin arkistoista. Esimerkiksi Jeppsson [2017] on tiivistänyt operaation Neuvostoliiton disinformaatiokampanjaksi, jonka tarkoituksena oli saada muu maailma uskomaan, että HIV oli kehitetty USA:n armeijan tutkimuslaitoksessa, josta se oli joko vahingossa tai tarkoituksella päässyt karkuun ja aiheuttanut maailmanlaajuisen epidemian. Hän ei ota kantaa operaation syntyyn johtaneisiin syihin tai sen poliittisiin motiiveihin, mutta kirjoittaa yksityiskohtaisesti sen suorittamisesta. Tämä antaa hyvän kuvan operaation vaatimista resursseista, sekä sen taustalla olevien motivaattoreiden vahvuudesta, jotta kyseinen määrä resursseja on haluttu tai ylipäätään voitu operaation suorittamiseksi käyttää.

Jeppsson kertoo julkaisussaan onnistuneeseen operaatioon tarvitun ensinnäkin joukon aitoja tutkijoita, jotka eivät olleet perillä siitä, että koko operaation pohjalla oleva väite oli huijaus. Tähän tarkoitukseen löytyikin jo eläköitynyt tutkijapariskunta, biologian tohtori Jakob Segal ja hänen vaimonsa Lilly Itä-Saksasta. Tutkijapariskunta saatiin vakuutettua väitteen aitoudesta mm. tekaistujen lehtiartikkeleiden ja tutkimustulosten avulla. Pariskunta alkoi pian tämän jälkeen levittää väitettä omatoimisesti eteenpäin, esimerkiksi julkaisemalla aiheesta lehtiartikkeleita sekä puhumalla erilaisissa konferenssseissa. He väittivät mm. osoitetun, että koko HIV epidemia alkoi USA:ssa jo kauan ennen Afrikkaa. Lisäksi he väittivät saaneensa salaista tietoa lähteeltään USA:n armeijan sisällä, jonka henkilöllisyyttä he eivät tietenkään voineet paljastaa. Tämä lähde oli tietenkin kaikella todennäköisyydellä neuvostoliittolainen agentti, joka oli puheillaan saanut tutkijapariskunnan vakuutettua siitä, että hän todellisuudessa työskenteli USA:n armeijalle ja että hänellä oli hallussaan salassapidettävää tietoa HIV:n kehityksestä.

Jeppson jatkaa kertomalla väitteen lopulta päätyneen itäsaksalaisen toisinajattelijan Stefan Heymin korviin. Tämä innostui kovasti ajatuksesta ja omasi lisäksi suhteita länsimaisiin sanomalehtiin. Hänen avullaan alkuperäinen väite saatiin lopulta istutettua laajalti myös länsimaiseen mediaan. Kampanjan onnistumiseen vaikutti suuresti myös samaan aikaan kiertävä huhu Yhdysvaltojen yleisesti harjoittamista ihmiskokeista. Lisäksi biologiset aseet olivat samoihin aikoihin päätyneet käsitteenä suuren yleisön tietoon, ja niiden käyttöä ja kehitystä pelättiin laajalti.

Joka tapauksessa onnistuneesti masinoitunut kampanja johti lopulta, vuosien työn jälkeen siihen, että myös suomalaisessa sanomalehdessä kerrottiin näistä vakavista epäilyistä. Se, mitä operaatiolla lopulta saavutettiin, jäi oikeastaan hämärän peittoon. Ehkä tarkoituksena oli testata vastaavan operaation toimivuutta myöhempiä, huomattavasti tärkeämpiä tavoitteita ajatellen.

APN syytti USA:n armeijaa AIDS:in kehittämisestä

(KU) Neuvostoliittolainen professori Pjotr Nikolajev syyttää Yhdysvaltojen armeijaa AIDS-viruksen kehittämisestä.

Uutistoimisto APN:n sotilaspoliittisessa tiedotteessa julkaistussa artikkelissa professori väittää viruksen vuotaneen USA:n sotilaallisesta laboratoriosta Fort Detrickistä, jossa 70-luvun alussa toimi bakteeriaseiden kehittämisen pääkeskus ja jossa hänen mukaansa on tehty myös ihta, että myös HIV-virusta on kokeiltu ihmisiin. Sen piilevä vaikutusaika on pitkä. Aidsin tartunnankantajia pidettiin diagnostiikan silloisella tasolla itse asiassa terveinä, Nikolajev päättelee.

Hänen mukaansa ensimmäiset Aids-tapaukset kirjattiin New Yorkissa vuonna 1979 minkä jälkeen tauti levisi kaikkialle Yhdysvaltoihin.

Professori arvelee, että HIV-viruksella pyritiin li-

Kuva 1: Lehtileike Kansan Uutiset -sanomalehdestä

Miksi disinformaatio sitten toimii niin tehokkaasti? Tätä aihetta on käsitellyt mm. Henry Tikkanen [2020] operaatio Infektiosta kertovassa podcastin jaksossaan. Tiivistettynä uutiset ja juorut ovat historiallisesti olleet ihmisen selviytymisen kannalta erittäin tärkeässä roolissa. Esimerkiksi luolamiesaikaan naapuriheimosta saapuvat uutiset ovat olleet elintärkeitä ja parhaassa tapauksessa saattaneet vaikkapa pelastaa koko yhteisön uhkaavalta vaaralta. Vääriä uutisiakin on toki voitu yrittää levittää harhautusmielessä, mutta tuohon aikaan viholliset ja erityisesti ystävät ovat varmasti olleet helppoja erottaa toisistaan. Joka tapauksessa ihmisellä on siis geneettisesti taipumus paitsi kuunnella, myös uskoa uutisia. Modernissa yhteiskunnassa ennen sosiaalista mediaa uutisten levittämisestä ovat pitkälti olleet vastuussa viralliset uutistoimitukset, jotka sitten ovat levittäneet uutisiansa esimerkiksi tv-kanavien ja sanomalehtien välityksellä. Uutistoimitusten keskittyminen yrityksille ja valtion toimijoille on mahdollistanut järjestelmällisen väärän tiedon ja propagandan levittämisen.

3.2 Operaatio ”Olympic Games” – joukkotuhoaseet kyberavaruudessa

Kamiński [2020] on kirjoittanut tiivistelmän operaatio Olympic Gamesista, sen taustoista sekä seurauksista. Kaikki alkaa siitä, kuinka Yhdysvaltojen ja oikeastaan koko läntisen maailman turvallisuuspolitiikka on jo pitkään perustunut erilaisiin sopimuksiin ja muihin keinoihin joukkotuhoaseiden määrien rajoittamisesta. Näin ylläpidetään ns. ”kauhun tasapainoa” eli tilannetta, jossa kaikilla on riittävästi aseita siihen, että niiden käyttö ei ole kenellekään kannattavaa. Kauhun tasapainossa on myös tärkeässä roolissa se, että kaikki

edellä mainittuja joukkotuhoaseita omaavat valtiot ovat yhdessä sopineet pelisäännöt niiden käyttöä koskien. Mikäli esimerkiksi yhteisiä sääntöjä noudattamaton terroristivaltio saisi käsiinsä ydinaseen, voisi tämä johtaa globaaliin ydinsotaan. Erityisen huolissaan Yhdysvallat oli Iranin ydinohjelmasta ja siitä, että Iran onnistuisi tämän avulla hankkimaan käsiinsä ydinaseita. Olihan Yhdysvallat jo 2000-luvun alussa silloisen presidenttinsä George W. Bushin johdolla julistanut Iranin terroristivaltioksi. Tästä uhkakuvasta syntyi vuonna 2006 operaatio Olympic Games. Vuosia kestänyt Iraniin ja sen liittolaisiin kohdistunut kyberoperaatio, jonka aikana nähtiin ja käytettiin useita täysin aikaansa edellä olevia kyberaseita.

Kamiński kertoo artikkelissaan, kuinka operaatio alkoi pikkuhiljaa paljastua maailmalle, kun kesäkuussa 2010 valkovenäläinen turvallisuusyritys VirusBlokAda raportoi uudesta, entuudestaan tuntemattomasta tietokoneviruksesta, joka näytti levinneen laajalle, mutta aiheuttaneen ihmeen vähän vahinkoa. Nopeasti selvitettiin viruksen kohteena olevan teollisuudessa käytettävät taajuusmuuntimet. Virus kykeni ensimmäisten tietojen mukaan ottamaan haltuunsa tietyn valmistajan tietyn mallisen taajuusmuuntimen – todettakoon vielä, että varsinainen tartunta tapahtui taajuusmuuntimia ohjelmoiviin laitteisiin. Pian kyseiset laitteet yhdistettiin Iranin ydinvoimaloihin ja meneillään olevaan ydinhankkeeseen. Koska taajuusmuuntimilla kontrolloidaan esimerkiksi sähkömoottorien nopeutta, voisi haltuun otetulla muuntimella ainakin teoriassa aiheuttaa fyysisiä vahinkoja – ja näin siinä kävikin. Iranissa viruksen leviäminen huomattiin mystisesti hajonneina sentrifugeina, joiden korvaaminen oli paitsi hidasta myös erittäin kallista.

Stuxnetiksi nimettyä matoa pidetään useissa lähteissä ensimmäisenä oikeana kyberaseena. Tässä tapauksessa valtiollisen tahon kehittämänä haittaohjelmana, joka iskee täsmällisesti ennalta valittuihin kohteisiin ja jonka tarkoitus on aiheuttaa haittaa toiselle valtiolle. Vaikka täyttä varmuutta tuskin koskaan saadaan, oli Stuxnet erittäin todennäköisesti USA:n ja Israelin yhteinen hanke ja sen tarkoituksena oli hidastaa Iranin ydinaseohjelman valmistumista. Tämän väitteen vahvisti myöhemmin mm. Edward Snowden. Joka tapauksessa ohjelman kehittäjät varmasti tiesivät, ettei Iran tule perumaan ydinaseohjelmaansa pienten vastoinkäymisten takia ja että kyberhyökkäystä ei olla jatkamassa fyysisellä sodankäynnillä. Täten koko operaation tarkoituksena oli todennäköisesti paitsi testata tällaisen kyberaseen toimivuutta ja analysoida sen vaikutuksia, niin myös näyttää Iranille, että edes heidän turvallisimmat laitoksensa eivät ole vihollisen ulottumattomissa.

Toimintaperiaatteiltaan Stuxnet oli vähintäänkin nerokas. Se levisi puhtaasti USB-tikkujen välityksellä ja käytti kohteen tartuttamiseen useampaa ennalta tuntematonta, niin kutsuttua nollapäivähaavoittuvuutta *(eng. zero-day)*. Nollapäivähaavoittuvuudella tarkoitetaan sellaista tietoturvahaavoittuvuutta, joka on olemassa ja hyödynnettävissä ennen kuin sen kohteena olevan ohjelmiston tai järjestelmän kehittäjät ovat tietoisia siitä tai ehtineet korjata sen. Käytännössä nollapäivähaavoittuvuudella tarkoitetaan siis sellaista

haavoittuvuutta, johon ei ole vielä olemassa korjausta. Erityisen vaarallisia nollapäivähaavoittuvuudet ovat mm. siksi, että niiltä ei voi suojautua perinteisin keinoin pitämällä järjestelmä ja ohjelmistot päivitettyinä. Stuxnetin tapauksessa saastunut USB-tikku saattoi tartuttaa useita laitteita, jotka puolestaan saastuttivat uusia USB-tikkuja. Koska Stuxnet ei aiheuttanut minkäänlaista haittaa saastuttamilleen laitteille, kesti sen havaitseminen poikkeuksellisen pitkään. Tänä aikana Stuxnet ehti USB-tikkujen välityksellä levitä myös sellaisille laitteille, joita ei ollut koskaan edes kytketty internettiin – kuten tässä tapauksessa Iranin ydinvoimalat. Lopulta tartutettuaan miljoonia ja miljoonia laitteita, sekä levittyään läpi maapallon, virus löysi kohteensa – Natanzin ydinvoimalaitoksen. Siellä virus otti aikaisemmin mainitut taajuusmuuntimet hallintaansa, sekoitti sähkömoottorien pyörimisnopeudet, ja alkoi hitaasti, mutta varmasti rikkoa kallista laitteistoa.

Lopulta operaatio kuitenkin viivytti Kamińskin mukaan Iranin ydinohjelmaa vain noin vuodella, mikä kuulostaa kohtuullisen vähäiseltä ottaen huomioon sen, että operaatio itsessään kesti useita vuosia, ja sen aikana "poltettiin" useita huippumoderneja vakoilu- ja haittaohjelmia. Polttamisella tarkoitetaan haittaohjelman paljastumista, eli sen vuotamista yleiseen tietoon ja siten sen päätymistä paitsi vastapuolen tietoon, niin myös esimerkiksi antivirussovellusten ja laitevalmistajien torjuntalistalle. Toisaalta Kamiński toteaa operaation olleen kuitenkin ennen kaikkea myös voimannäyttö itäisille terroristivaltioille – osoitus siitä, että Yhdysvallat liittolaisineen ovat kykeneviä suorittamaan kyberoperaatioita missä tahansa päin maailmaa ja vaikkapa tunkeutumaan USB-tikulla vihollisen alueella sijaitsevaan ulkopuolisilta suljettuun ydinvoimalaan.

Operaatiossa käytettyjen kyberaseiden arsenaaliin palaamme tarkemmin vielä myöhemmin tässä tutkielmassa.

3.3 Sodankäyntiä Twitterissä – Ukrainan ja Venäjän välinen sota

Ducheine ja muut [2022] kirjoittavat kattavasti Ukrainan ja Venäjän välisestä konfliktista ja siihen liittyvistä kyberoperaatioista. Oikeastaan nykyinen kriisi ja siihen liittyvä kybersodankäynti juontavat juurensa jo vuoden 2004 Ukrainan presidentinvaaleihin ja niihin kohdistuneeseen Venäjän informaatiovaikuttamiseen suotuisan lopputuloksen aikaansaamiseksi. Tilanne pysyi vakaana aina vuoteen 2014, jolloin nähtiin ensimmäinen todellinen invasiivinen operaatio vieraalla maaperällä, kun vahvasti Venäjän hallitukseen liitoksissa ollut hakkeriryhmittymä onnistui murtautumaan Ukrainan vaalien ääntenlaskentajärjestelmään ja muokkaamaan sitä siten, että vaalien voittajaksi olisi voitu valita haluttu edustaja todellisista äänistä huolimatta. Tietomurto kuitenkin havaittiin juuri ennen varsinaista ääntenlaskua eikä siitä ehtinyt koitumaan todellista harmia.

Samojen tutkijoiden mukaan vakavampia kyberoperaatioita alettiin nähdä vasta vuoden 2014 vaalien ja Krimin niemimaan miehityksen jälkeen. Nämä kohdistuivat mm. Ukrainan energiainfrastruktuuriin, aiheuttaen esimerkiksi sähkökatkoksia ympäri maata. Konkreettiset haitat jäivät kuitenkin lähinnä kiusanteon tasolle, eikä hyökkäyksissä

tuntunut olevan juurikaan koordinaatiota tai minkäänlaista suurempaa kuvaa. Jälkikäteen ajateltuna Ukraina on saattanut toimia eräänlaisena ”vapaana riistana” ja harjoituskohteena Venäjän kyberoperaatioiden ja kyberaseiden kyvykkyyksien kehittämiseksi.

Vaikka muutama kuukausi ennen helmikuussa 2022 alkanutta täysimittaista sotaa nähtiin selkeää kasvua Ukrainaan Venäjältä kohdistetuissa kyberhyökkäyksissä, ei suoritetuilla operaatiolla kuitenkaan ollut kovin mainittavia vaikutuksia. Kyseessä oli lähinnä kiusanteoksi määriteltäviä palvelunestohyökkäyksiä, sekä esimerkiksi verkkosivustoille murtautumista ja niiden sisällön vaihtamista venäjämyönteiseksi propagandaksi. Huomionarvoista on kuitenkin se, että myös Ukrainan ja sen liittolaisten puolelta alettiin käyttää kyberoperaatiota Venäjää vastaan. Em. tutkijat sivuavat ainakin yhtä mainitsemisen arvoista tapausta, jossa valkovenäläiset hakkerit onnistuivat murtautumaan oman maansa rautatiejärjestelmiin ja siten vaikeuttamaan venäläisten sotilaiden liikkumista Valko-Venäjän alueella.

Raportin mukaan vain hieman ennen sotaa, tammikuun 2022 puolessa välissä nähtiin taas uusi kyberhyökkäys, kun Microsoftin järjestelmät löysivät useisiin ukrainalaisiin laitteisiin pesiytyneen haittaohjelman nimeltä ”WhisperGate”. Haittaohjelma esitti tavallista kiristysohjelmaa, vaikka sen tosiasialliseksi tarkoitukseksi selvitettiin tiedon pysyvä tuhoaminen. Haittaohjelman alkuperäksi epäiltiin Venäjän tiedustelupalvelu GRU:ta, joskaan tästä ei koskaan saatu täyttä vahvistusta. On yleisesti epäilty, että haittaohjelman tarkoitus oli selvittää Ukrainan kyberpuolustuksen kyvykkyyttä ja kartoittaa siellä mahdollisesti olevia puutteita.

Vain päivää ennen Venäjän armeijan hyökkäystä löydettiin useista ukrainalaisista järjestelmistä taas uusi haittaohjelma, tällä kertaa nimeltään ”HermeticWiper”. Haittaohjelma oli hyvin samankaltainen aikaisemmin löydetyn WhisperGaten kanssa, mutta kuitenkin huomattavasti kehittyneempi.

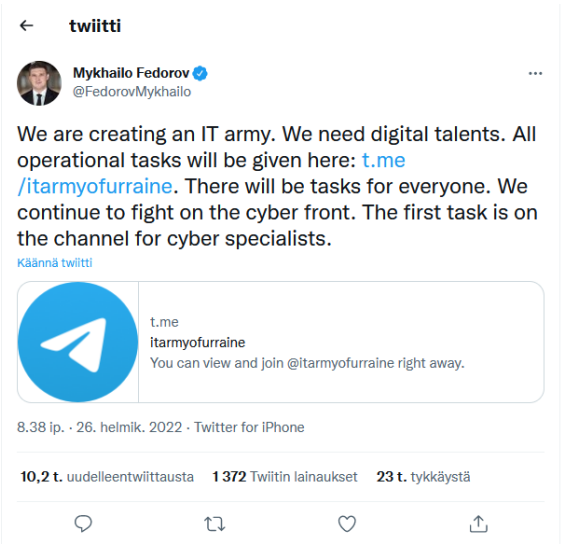
Edelleen Ducheine ja muut [2022] analysoivat kyberoperaatiota konfliktin muututtua täysimittaiseksi sodaksi helmikuun 24. päivä 2022. Hyökkäyshetkellä venäläiset hakkerit onnistuivat kyberhyökkäyksessään yhtä Ukrainan suurinta satelliittipalveluita tarjoavaa organisaatiota, Viasatia, vastaan. Venäjän hyökkäys oli tuolloin jo täysimittaisesti käynnissä ja Ukrainan infrastruktuuria oli merkittävästi heikennetty erilaisilla ohjushyökkäyksillä. Satelliittiyhteyksien menetys vaikutti merkittävästi Ukrainan armeijan mahdollisuuksiin reaaliaikaiseen kommunikaatioon ja tilannekuvan muodostamiseen, mikä luonnollisesti on sodankäynnissä äärimmäisen tärkeää. Käytännössä hyökkäys teki Ukrainasta hetkeksi kokonaan sokean vihollisen liikkeille ja aiheutti osaltaan varmasti myös kuolonuhreja.

Kyseisen tapauksen jälkipyykkinä maailma sai mielenkiintoisen esimerkin informaatioyhteiskunnan vaikuttavuudesta, kun Ukrainan digitaalisen muutoksen ministeri Mykhailo Fedorov lähetti Twitterissä Elon Muskille avunpyynnön. Elon vastasi

avunpyyntöön, niin ikään Twitterissä, ja muutamassa tunnissa Starlink satelliittijärjestelmä oli siirretty Ukrainan ylle. Näin Ukraina käytännössä Twiittasi armeijalleen toimivat satelliittiyhteydet. Vaikka hyökkäyksen alkuperää ei pystyttykään varmuudella todentamaan, voidaan sen takana lähes varmasti todeta olleen suoraan valtioon liitoksissa olevan toimijan, etenkin kun mietitään sen ajoitusta suhteessa varsinaiseen hyökkäykseen.

Kuva 2: Twitter-keskustelu Mykhailo Fodorovin ja Elon Muskin välillä

Starlink ei ollut ainoa esimerkki Twitterin käytöstä osana sodankäyntiä. Ukrainan hallitus perusti nimittäin myös virallisen vapaaehtoisarmeijan – niin ikään Twitterissä. Heti sodan ensimmäisinä päivinä Mykhailo Fedorov Twiittasi Ukrainan perustaneen uuden vapaaehtoisyksikön nimeltään IT-armeija. Yksikössä oli hänen mukaansa ”tehtäviä kaikille” ja ensimmäiset tehtävät olivat jo julkisesti jaossa viestintäpalvelu Telegramiin perustetussa ryhmässä, johon oli kutsulinkki samassa Twiitissä.



Kuva 3: Ukrainan ilmoitus IT-armeijan perustamisesta Twitterissä

On vaikea arvioida, että kuinka paljon kyseinen ryhmä on oikeasti päässyt vaikuttamaan sodan kulkuun, mutta kirjoitushetkellä siellä on kuitenkin satoja tuhansia jäseniä ja erilaisia tehtäviä jaetaan jatkuvalla syötöllä. Tehtävät koostuvat lähinnä eri typpisistä

palvelunestohyökkäyksistä venäläisiä organisaatioita vastaan ja todennäköisesti koko ryhmän toiminta onkin jäänyt lähinnä haitanteon asteelle. Ei kuitenkaan voida sulkea pois vaihtoehtoa, missä em. avoimen ryhmän kautta olisi vaikkapa muodostettu myös oikeista ammattilaisista koostuvia suljettuja ryhmiä, jotka puolestaan olisivat voineet osallistua huomattavasti vaikutusvaltaisempiin operaatioihin. Tällaisesta ei kuitenkaan toistaiseksi ole minkäänlaisia viitteitä. Totuutta joudumme todennäköisesti odottamaan vähintään sodan päättymiseen saakka. Joka tapauksessa konfliktin jälkipyykkiä perataan varmasti vielä vuosia ja todennäköisesti myös kyberrintamalta tulee paljastumaan paljon sellaisia asioita, joista emme vielä ole tietoisia. Tätä jäämme mielenkiinnolla odottamaan.

4 Kyberaseet

Tässä luvussa lukijalle selvitetään mitä kyberaseella tarkoitetaan ja miten erilaisia haittaohjelmia voidaan luokitella kyberaseeksi. Lisäksi lukijalle esitellään tämän tutkielman piiriin valikoidut kyberaseet sekä niiden tutkimiseen käytetty lähdemateriaali.

Luvussa 4.1 esitellään kyberaseen määritelmä. Määritelmän lisäksi selvitetään kriteeristö, jonka mukaan tässä tutkielmassa esiintyvät kyberaseet on valittu mukaan. Luvussa sivutaan myös kyberaseiden ja kybersodankäynnin lainsäädännöllisiä ongelmia. Tämän jälkeen luvussa 4.2 siirrytään esittelemään myöhemmin tutkielmassa käsiteltävien kyberaseiden ja suurelta osin tämän tutkielman lähdemateriaalina käytettyjä teknisiä analyyseja tuottaneet laboratoriot ja yritykset, sekä perustellaan niiden käyttö lähteenä. Lopulta luvussa 4.3 esitellään yksityiskohtaisesti tutkielman piiriin valikoidut kyberaseet. Aseista käydään läpi yleisellä tasolla esimerkiksi niiden käyttötarkoituksia ja kyvykkyyksiä.

4.1 Kyberaseen määritelmä

Kyberaseen määritteleminen terminä on hankalaa, ja kyberaseeksi onkin kutsuttu lähteestä riippuen kaikkea mahdollista aina yksinkertaisista haittaohjelmista digitaalisiin joukkotuhoaseisiin. Termi on myös kovin mediaseksikäs, mikä varmasti osaltaan edesauttaa myös perinteisten laajoja vahinkoja aiheuttaneiden haittaohjelmien määrittelemisen kyberaseiksi etenkin iltapäivälehtien sivuilla. Osa aikaisemmista määrittelyistä on ollut vähintäänkin vähätteleviä. Esimerkiksi Valeriano ja muut [2016] toteavat artikkelissaan ”Dropping the cyber bomb”, että yksikään kyberase ei vedä vertoja ISIS:in aiheuttamalle uhalle ja että on hölmöä ajatella kyberaseiden olevan mitään muuta kuin ”rivien muuttamista taulukoissa, sähköpostin kaappaamista, yhteyksien häiritsemistä sekä vihollisen harhauttamista”. Toisaalta Rid ja McBurney määrittelevät omassa tekstissään [2012] kyberaseen työkaluksi ”jota käytetään, tai joka on suunniteltu käytettäväksi aiheuttamaan tai uhkaamaan aiheuttaa fyysistä, henkistä tai toiminnallista vahinkoa järjestelmille, rakennuksille tai eläville olennoille.” Maathuis ja muut [2016] taas määrittelevät kyberaseen pitkälti sille asetettujen tavoitteiden kautta ”Tietokoneohjelmaksi, joka on tehty tai jota käytetään muokkaamaan tai tuhoamaan järjestelmiä (sotilaallisen) tavoitteen

saavuttamiseksi kyberavaruuden sisä- ja/tai ulkopuolella". Mikään edellä mainituista, sen enempää kuin mistään muistakaan määritelmistä, ei kuitenkaan ole juridisesti pätevä tai millään muullakaan tavalla valtioita tai muita toimijoita sitova, sillä esimerkiksi kansainvälisessä laissa ei kyberasetta ole määritelty, eikä sen käyttöä siten myöskään säädelty [Stevens 2017].

Tämän tutkielman kontekstissa määrittelemme itse kyberaseen seuraavasti:

- Edistynyt haitallinen ohjelmakoodi, sovellus tai muu ohjelmisto,
- jonka kehittämisen takana, tai kohteena on joko suoraan tai välillisesti valtiollinen, tai valtioon rinnastettava toimija,
- ja jolla on selkeä, ennalta määritelty tavoite, jonka saavuttaminen perinteisin konstein vaatisi joko tiedustelupalvelun käyttöä, sotilaallisen operaation aloittamista, tai muiden vastaavien resurssien hyödyntämistä.

Lisäksi, jotta kyseinen ohjelmisto voidaan ottaa mukaan tähän tutkimukseen:

- Tulee em. kriteerit täyttävästä ohjelmistosta olla tuotettu julkisesti saatavilla oleva, korkealaatuinen ja luotettavan tahon teettämä tekninen analyysi, tai muu vastaava tutkimus.

Vaikka ylivoimaisesti suurin osa kyberaseista onkin valtiollisten tahojen kehittämiä, on kuitenkin hyvä ottaa huomioon, että myös ei-valtiolliset toimijat, kuten terroristit tai aktivistit, voivat kehittää ja käyttää kyberaseita siinä missä muutkin, joten valtioriippumattouus ei voi olla automaattisesti poissulkeva peruste. Lisäksi myös yksityisten yritysten toimesta kehitetään kyberaseita kaupallisille viranomaismarkkinoille. Tämän takia kriteeristö voi täyttyä myös sellaisten haittaohjelmien osalta, joiden ensisijaisena kohteena on valtio, mutta jotka on kehitetty esimerkiksi yksityisten yritysten tai aktivistiryhmittymien toimesta.

Kriteeristön myötä myös joitain ehkä useimpien mielestä kyberaseeksi määriteltäviä ohjelmistoja on jätetty pois. Tästä esimerkkinä vaikkapa erittäin tehokas EternalBlue, joka mahdollisti aikanaan lähes minkä tahansa julkiseen verkkoon näkyvän Microsoft Windows -järjestelmän haltuun ottamisen, mutta joka ei kuitenkaan täytä em. määrittelyn kolmatta kohtaa liittyen ohjelmiston selkeään ja ennalta määritettyyn tavoitteeseen. Sen sijaan EternalBlueta on sen paljastumisen jälkeen käytetty komponenttina useissa muissa kyberaseissa ja haittaohjelmissa. Samasta syystä myös useita muita NSA:lta vuonna 2016 varastettuja työkaluja, jotka saattaisivat muuten täyttää kyberaseen määritelmän, on jouduttu jättämään pois tämän tutkielman piiristä, sillä ne ovat käyttötarkoitukseltaan työkaluja, eivätkä aseita. Esimerkkinä EternalBlueta voidaan verrata ohjuksen ohjausjärjestelmään. Ohjus itse on varsinainen ase, mutta siihen on kytketty erillinen järjestelmä, joka ohjaa sen kohteeseensa – eräänlainen mahdollistaja, enabloija. Samanlaisen roolin

EternalBlue on saanut useissa haittaohjelmissa. Lisäksi pois on jäänyt selkeästi kyberaseeksi luokiteltavia haittaohjelmia, joita ei ole vielä ehditty tutkia tarpeeksi, tai joita ei oltu tutkittu riittävän luotettavien ja akateemisesti kelvollisten lähteiden toimesta, tai joista tuotettuja tuloksia ei ole kyetty varmentamaan useammasta eri lähteestä.

Tutkielman ulkopuolelle on niin ikään jätetty esimerkiksi kiinalainen Great Cannon sekä USA:n XKeyScore, joita molempia on mediassa kutsuttu kyberaseiksi. Vaikka kyseiset järjestelmät ansaitsisivat jo pelkästään kokonsa ja kyvykkyyksiensä puolesta kokonaan omat tutkielmansa, ei kumpikaan kuitenkaan istu tämän tutkielman määritelmään kyberaseesta. Todellisuudessa molemmat ovat laajempia järjestelmäkokonaisuuksia, jotka ennemminkin mahdollistavat yksittäisten kyberaseiden kohdistamista ja käyttöä. Hyvänä esimerkkinä molemmista järjestelmistä löytyy moduuli, jonka avulla suojaamatonta verkkoliikennettä voidaan kaapata, ja sen sekaan voidaan lisätä esimerkiksi haitallista koodia. Tämä mahdollistaa mm. haittaohjelmien suorittamisen kohteeksi valikoidulla päätelaitteella. Aikaisemman kyberaseen määritelmän mukaisesti sekä Great Cannon että XKeyScore eivät siis täytä kyberaseelle asettamiamme vaatimuksia, mutta em. moduulin avulla ajettava haittakoodi sen sijaan saattaisi. Järjestelmiä voidaan siis ajatella eräänlaisina alustoina varsinaisille kyberaseille, eikä niitä sen takia tässä tutkielmassa ole tämän enempää käsitelty.

Luotettaviksi tahoiksi haittaohjelmien analysoinnin suhteen on tässä tutkielmassa arvioitu yleisesti tunnettujen ja korkealaatuisten yrityslaboratorioiden tuottamat artikkelit ja raportit (esim. Symantec ja F-Secure), akateemisten tutkimuslaboratorioiden tekemät tutkimukset (esim. CrySyS), sekä toki myös muu perinteisesti vertaisarvioitu ja julkaistu akateeminen materiaali.

4.2 Analyyseja tuottaneet laboratoriot

Työn lähdekäytäntö eroaa ehkä hieman perinteisistä akateemisista lopputöistä sen osalta, että suuri osa käytetyitä lähteistä on yksityisten laboratorioiden tai tutkimusyskiköiden tuottamia raportteja, joita kovin harvoin on julkisesti vertaisarvioitu. Edellä mainituitten seikkojen takia tässä luvussa esitellään lähteenä käytetyn materiaalin tuottaneet toimijat, sekä perustellaan niiden käyttö lähteenä. Erityisesti kaupallisten toimijoiden osalta tietojen lähteenä on käytetty yritysten omien verkkosivujen lisäksi myös julkisista lähteistä saatavilla olevia tietoja esimerkiksi yritysten liikevaihdosta tai työntekijöiden määrästä.

4.2.1 CrySyS

CrySyS Lab on osa Budapestin teknillisen ja taloustieteellisen yliopiston tietoliikenneviestinnän laitosta. Sen nimi on johdettu sanoista ”Laboratory of Cryptography and System Security”, eli suomeksi ”kryptografian ja tietojärjestelmäturvallisuuden laboratorio”. Laboratorio on arvostettu ja se tuottaa laadukasta tutkimusta erityisesti tietoturvasta ja siihen liittyvistä aihealueista. Laitoksen julkaisuja on julkaistu hyvällä tahdilla

esimerkiksi paljon siteeratuissa lehdissä, kuten IEEE Transactions on Dependable and Secure Systems ja IEEE Transactions on Mobile Computing. Laboratorio on ollut mukana useissa korkean profiilin haittaohjelma-analyyseissa, minkä lisäksi se sai julkisuutta erittäin kehittyneen Duqu -nimisen haittaohjelman löytämisestä vuonna 2011 (Duqu esitellään tarkemmin luvussa 4.3.1). Laitoksen tuottamat julkaisut ovat ammattilaisten mielestä yleisesti laadukkaita, minkä lisäksi kyseessä on tunnetun yliopiston tutkimuslaitos, joka antaa sen tuottamille raporteille tietynlaisen laatutakuun. [”CrySyS Lab” 2022; CrySyS Lab Homepage 2023]

4.2.2 CyberArk

CyberArk on USA:ssa vuonna 1999 perustettu, erilaisiin tunnistamisen ja pääsynhallinnan ratkaisuihin erikoistunut kansainvälinen tietoturvayritys. Yrityksellä on kiinteä toimipiste yli 16:ssa ja asiakkuuksia yli 110:ssa maassa, yli 2400 työntekijää ja yli 400 miljoonan dollarin vuotuinen liikevaihto. Yritys ylläpitää omaa laboratoriotaan, joka tuottaa jatkuvalla tahdilla laadukasta tutkimusta erityisesti haittaohjelmien toiminnasta ja niiden havaitsemisesta. CyberArk ei ole tutkimusmaailmassa ehkä vielä yhtä tunnettu kuin monet muut tässä tutkielmassa käsiteltävät laitokset, mutta tutkimukset ovat silti nauttineet ammattipiireissä laadukkaan tuotoksen mainetta. Lisäksi kyseessä on hyvin pitkään toiminnassa ollut ja pörssinoteerattu yritys, jonka on luonnollisesti ylläpidettävä myös omaa mainettaan ja siten varmistuttava siitä, että tuotettu tutkimustyö on laadukasta. [”CyberArk” 2023; CyberArk Labs Homepage 2023]

4.2.3 Kaspersky Lab

Kaspersky Lab ZAO on venäläinen tietoturvayhtiö. Yhtiö työllistää yli 3000 työntekijää, ja sillä on toimipisteitä yli 30:ssa maassa. Yhtiö on toiminut vuodesta 1997, ja sen pääasiallisena tuotteena ovat erilaiset yksityisille ja yrityksille suunnatut antivirus ja verkkoturvallisuustuotteet. Yritys on vuosien varrella julkaissut lukuisia laadukkaita tutkimuksia ja analyyseja haittaohjelmista, sekä niiden toiminnasta ja torjunnasta. Yritys tunnetaan myös siitä, että sen työntekijät löysivät Duqu 2.0:n. Ehkä hieman ironisesti, haittaohjelma ehti kuitenkin saastuttaa yrityksen laitteita ja sen verkkoa kuukausia ennen löytöä. Vaikka monet ovat viimeaikaisten maailmanpoliittisten tapahtumien takia kyseenalaistaneet yhtiön luotettavuutta, on se silti kiistatta yksi maailman tunnetuimmista ja arvostetuimmista tietoturvatutkimusta tekevistä yksityisistä yrityksistä. [”Kaspersky Lab” 2023; Kaspersky Lab Homepage 2023]

4.2.4 Malwarebytes

Malwarebytes on vuonna 2004 perustettu amerikkalainen tietoturvaratkaisuja tarjoava yritys, jolla on pitkä historia haittaohjelmien tai tietokonevirusten analysoinnissa, sekä niiden torjuntaan perustuvien ratkaisujen kehittämisessä. Yrityksen tuotevalikoimaan kuuluu erilaisia haittaohjelmien tunnistus- ja poistamistyökaluja. Yritys on tullut

maailmalla tunnetuksi tuottamistaan haittaohjelmiin liittyvistä reportaaseista ja muista ajankohtaisista julkaisuistaan. Yritys on yli 200 miljoonan dollarin liikevaihdollaan esimerkiksi suomalaista F-Securea kookkaampi. Yrityksen tunnettuja julkaisuja ovat mm. ”State of malware 2021”, sekä raportti yritykseen kohdistuneesta hyökkäyksestä ja sen omasta taistelusta osana SolarWinds-hyökkäysketjua. Yrityksen tuottamat raportit ovat olleet suosittuja, ja niitä ovat lukeneet ja referoineet tutkijat ympäri maailman. Mikäli raportit sisältäisivät virheellistä tietoa, tai niiden laadussa olisi puutteita, tämä todennäköisesti selviäisi hyvin nopeasti. [”Malwarebytes” 2023; Malwarebytes Homepage 2023]

4.2.5 ESET Research

Kansainvälinen yritys, joka palvelee miljoonia asiakkaita ympäri maailman. Yritys aloitti toimintansa vuonna 1987 omalla antivirus-tuotteellaan. Yrityksellä on myös maineikas ja laadukas tutkimusosasto, joka työllistää nykyisellään lähes 200 asiantuntijaa. Tutkimuksia tuotetaan yli 13:ssa tutkimuskeskuksessa eri puolilla maailmaa. ESET Researchin tapauksessa kyseessä on pitkään alalla toiminut ja paljon tutkimusta tuottava laitos. Vaikka laitos on ehkä tässä tutkielmassa käsiteltävistä laitoksista vähiten tunnettu, on kyseessä silti hyvin pitkään toiminnassa ollut yritys, jolla on vankka jalansija markkinoilla ja joka on yleisesti tunnettu ja arvostettu. Tämä antaa omalta osaltaan tietynlaisen laatulupauksen myös yrityksen tuottamille raporteille. [”ESET” 2023; ESET Homepage 2023]

4.3 Tutkittavien kyberaseiden esittely

Tähän tutkielmaan on pyritty valitsemaan kaikki aikaisemmin mainitut kriteerit täyttävät haittaohjelmat, joiden toiminnasta löytyy riittävän korkealaatuinen ja julkisesti saatavilla oleva tekninen analyysi. Luonnollisesti vaihtelevien määrittelyjen ja erilaisten kriteeristöjen takia joukosta saattaa puuttua sellaisia ohjelmistoja, joita esimerkiksi mediassa on tituleerattu kyberaseiksi. Monesti tällaisissa tilanteissa kyse on nimenomaan kyberaseen ongelmallisesta määritelmästä. Iso osa mainituista kyberaseista on todellisuudessa kaikkien saatavilla olevia avoimen lähdekoodin ohjelmistoja, jotka on vain onnistuttu ujuttamaan kohteeseensa tavalla tai toisella. Tällaisissa tapauksissa emme tämän tutkielman määritelmän perusteella voi puhua kyberaseesta, vaikka itse hyökkäys olisikin valtiollisen tahon toteuttama. Esimerkkinä voidaan käyttää vaikkapa hyökkäystä, jossa sisäpiirin toimija asentaa julkisesti saatavilla olevan takaoven organisaation verkkoon. Vaikka kyse saattaakin olla valtiollisesti kyberoperaatiosta tai kybersodankäynnistä, ei kyseessä kuitenkaan ole kyberase tai sen käyttäminen.

4.3.1 Duqu

Kyseessä on vuonna 2011 levinnyt vakoiluun tarkoitettu haittaohjelma, jota pidettiin aikanaan erityisen kehittyneenä ja kaikin puolin aikaansa edellä olevana. Useimmat Duqua tutkineet lähteet, kuten Chien ja muut [2012] ovat tulleet siihen lopputulokseen, että Duqu on lähtöisin samoilta kehittäjiltä kuin hieman aiemmin levinnyt Stuxnet, tai vähintäänkin

Duqun kehittäjillä on ollut pääsy Stuxnetin lähdekoodiin, sekä motivaatio tai muu halu kohdistaa hyökkäyksiä samoihin kohteisiin. Yhteneväisyyksien takia voidaan päätellä, että Duqu on Stuxnetin lailla todennäköisesti kehitetty USA:n ja Israelin yhteystyönä, mutta täyttä varmuutta tästä on tietenkin vaikea saada.

Chien ja muut [2012] havaitsivat Duqun kartoittaneen tietojärjestelmiä ja niiden ominaisuuksia todennäköisesti mahdollisia tulevia hyökkäyksiä varten. Mikäli Duqua ei olisi pysäytetty, olisimme saattaneet vielä nähdä uuden, mahdollisesti Stuxnetiäkin tuhoisamman, fyysiseen infrastruktuuriin kohdistetun, samasta haittaohjelmaperheestä lähtöisin olevan hyökkäyksen. Duqulla on kyvykkyys ainakin seuraavien tietojen keräämiseen saastuttamaltaan laitteelta: näppäinpainallukset, laitteen perustiedot (käyttöjärjestelmäversio, päivitykset, laitteen nimi, lista käyttäjistä, jne.), lista laitteella ajossa olevista prosesseista, tiedot laitteen käytössä olevista verkoista, tiedot verkkojen välityksellä jaetuista resursseista, listaus muista ko. verkoissa olevista laitteista, sekä saastutetun laitteen näytön etäkatselu ruudunkaappausten avulla [Szor 2011].

Duqu on valikoitu mukaan tähän tutkielmaan, sillä se on valtiollisen toimijan kehittämä haittaohjelma, jonka toiminnan kohteena ovat olleet toiset valtiot.

4.3.2 Duqu 2.0

Duqu 2.0 on vuonna 2015 havaittu ja Euroopassa sekä Lähi-idässä levinnyt haittaohjelma. Kaspersky Labin [2015] tutkijat toteavat Duqu2.0:n kuuluvan samaan haittaohjelmaperheeseen Stuxnetin ja Duqun kanssa, ja sen olevan todennäköisesti osa samaa Lähi-Itään kohdistuvaa operaatiota, jonka kohteena oli erityisesti Iranin ydinohjelma ja siihen liittyvä tiedustelu sekä haitanteko. He kertovat Duqu 2.0:n tartuttamia laitteita löytyneen mm. hotelleista ja muista relevanteista paikoista, joissa on käyty neuvotteluja liittyen Iranin ydinohjelmaan.

Edelleen he toteavat analyysissaan Duqu 2.0:n käytäneen leviämisessään hyväkseen jopa kolmea eri nollapäivähaavoittuvuutta ja sen olevan “sukupolven verran edellä mitään, mitä olemme koskaan nähneet”. Täyttä varmuutta Duqu 2.0:n kehittäjistä ei ole, mutta erittäin suurella todennäköisyydellä heillä on ollut vähintäänkin pääsy sekä Stuxnetin että alkuperäisen Duqun lähdekoodeihin. Kyseessä saattaa olla konkreettisesti sama kehittäjätiimi, mutta joka tapauksessa samaan operaatioon osallistuva ryhmittymä.

Duqu 2.0 on valittu mukaan tähän tutkielmaan luonnollisena jatkumona ja osana samaa operaatiota alkuperäisen Duqun ja Stuxnetin kanssa.

4.3.3 Flame (a.k.a Flamer a.k.a sKyWIper a.k.a Skywiper)

Flame on vuonna 2012 havaittu Euroopan kautta Lähi-Itään levinnyt ja pääasiassa vakoiluun käytetty haittaohjelma. Bencsáth ja muut [2012b] totesivat ohjelman ehtineen toimia todennäköisesti useita vuosia ennen sen havaitsemista. Ohjelman kautta onkin saatettu vakoilla huomattavan suurta kohderyhmää ja huomattavan pitkään. Samassa analyysissa todettiin suurimman osan ohjelman todennetuista kohteista olleen Iranissa. Ohjelma

tuhosi itse itsensä hyvin pian löydöksen julkistamisen jälkeen, mikä osoittaa sen olleen aktiivisessa käytössä aina löytämiseensä saakka. Vaikka ohjelman tekijöistä tai sen operoijista ei koskaan saatu täyttä varmuutta, epäillään sen yleisesti olleen osa samaa operaatiokokonaisuutta Duqun ja Stuxnetin kanssa.

Bencsáth ja muut [2012b] totesivat Flamen olleen löydettäessään yksi aikansa kehittyneimmistä haittaohjelmista. Lisäksi he totesivat tutkimuksessaan Duqun ja Flamen kyvykkyyksiltään hyvin samankaltaisiksi, molempien ollessa vakoiluun ja tiedonkeruuseen tarkoitettuja haittaohjelmia, mutta kuitenkin eroavan oleellisesti teknisen toteutuksen yksityiskohtien osalta. Ensinnäkin Flame oli massiivisesti kookkaampi kuin Duqu tai mitkään haittaohjelmat yleensä. Flame myös tallensi keräämänsä tiedot täysin eri tavalla Duquun verrattuna, käyttäen hyväkseen mm. SQLite tietokantoja. Lisäksi komentopalvelinten arkkitehtuuri oli erilainen: Duqun komentopalvelimia ajetaan CentOS-käyttöjärjestelmällä, kun taas Flamen Ubuntulla/Debianilla. Varsinaisen haittakoodin osalta molemmat ohjelmistot käyttävät myös täysin erilaista injektiotekniikkaa. Edellä mainittujen eroavaisuuksien takia pidetään todennäköisenä, että molemmat haittaohjelmat on kehitetty eri tahojen toimesta.

Vaikka Flame löydettiin vasta Duqun jälkeen, on Flame kuitenkin ollut toiminnassa todennäköisesti huomattavan pitkän ajan, ja siten kehitetty kauan ennen Duqua. On siis perusteltua pitää Duqua eräänlaisena Flamen seuraajana.

Flame on valikoitu mukaan tähän tutkielmaan, sillä se on käytännössä varmasti valtiollisen toimijan kehittämä ja erittäin kehittynyt haittaohjelma, jonka toiminnan kohteena ovat olleet toiset valtiot.

4.3.4 NotPetya

NotPetya on vuonna 2017 levinneestä Petya -nimisestä haittaohjelmasta kehitetty kiristyshaittaohjelma, joka saastutti valtavan määrän laitteita erityisesti Ukrainassa ja jonka epäillään aiheuttaneen satojen miljoonien dollarien edestä vahinkoja. NotPetyan uhriksi joutui myös joukko suuria kansainvälisiä yrityksiä, esimerkiksi FedEx ja Saint-Gobain. Yleisesti on todettu Venäjän tai siihen tiukasti kytköksissä olevan ryhmittymän olleen NotPetyan takana. NotPetyasta poiketen Petyan takana ei epäillä olleen valtiollista tahoa.

Sai ja Kumar [2019] tuottivat kattavan teknisen analyysin NotPetyasta ja kertovat yksityiskohtaisesti sen leviämisestä ja toiminnasta. NotPetyaa levitettiin alun perin lähinnä tilitoimistojen ja taloushallintoyksiköiden käytössä olevan, täysin legitiimin kolmannen osapuolen sovelluksen, M.E.Doc:n välityksellä. Päästyään kohdelaitteeseen M.E.Doc:n päivityksen mukana, levisi NotPetya edelleen verkossa käyttämällä jo aiemmin NSA:n tietomurron seurauksena julkistettuja Windows-käyttöjärjestelmän EternalBlue ja EternalRomance -haavoittuvuuksia. Mielenkiintoisen asiasta tekee se, että haavoittuvuuksiin oli julkaistu korjaukset jo kuukausia aiemmin, mutta NotPetya:n leviämisen mahdollisti se, että järjestelmien ylläpitäjät eivät yksinkertaisesti olleet päivittäneet

laitteitaan. NotPetya osasi edellä mainitun ei-nollapäivähaavoittuvuuden lisäksi levittää itseään myös hyödyntämällä Mimikaz -nimistä ohjelmistoa käyttäjätunnusten ja salasanojen keräämiseksi jo saastutetuilta laitteilta, ja käyttäen sitten näitä kerättyjä käyttäjätunnuksia levittääkseen itseään verkon sisällä myös sellaisille laitteille, jotka oli jo suojattu EternalBluea ja EternalRomancea vastaan.

NotPetya toimii hieman poikkeavasti verrattuna useimpiin kiristyshaittaohjelmiin, sillä varsinaisten tiedostojen sijasta se salaa saastuttamiensa laitteiden pääkäynnistyslohkot (*Master Boot Record*) sekä tiedostojärjestelmien päätiedostotaulukot (*Master File Table*). Vaikka varsinaisia tiedostoja ei missään vaiheessa salata, on tämä kuitenkin täysin riittävä toimenpide siihen, että tietoja ei levyltä saa palautettua ilman salauksen purkamista. Tietojen salaamisen jälkeen haittaohjelma pakottaa saastuttamansa laitteen uudelleenkäynnistymään ja esittää lunnasvaatimuksensa. Tutkimukset, mm. aiemmin mainittu Sai ja Kumar [2019] osoittivat myöhemmin, että ohjelman salaamia tietoja ei ollut edes teoriassa mahdollista palauttaa, vaikka lunnaat olisikin maksettu. Tästä voidaan päätellä ohjelman tosiasiallisena tarkoituksena olleen tiedon tuhoaminen.

NotPetya on otettu mukaan tähän tutkielmaan, sillä se on lähes varmasti Venäjän valtion tai Venäjän valtioon tiiviisti kytköksissä olevan ryhmittymän kehittämä haittaohjelma, jonka ainoana tavoitteena epäillään olleen tietojen tuhoaminen ja siten Ukrainan taloussektorin hetkellinen lamauttaminen.

4.3.5 Pegasus

Pegasus on israelilaisen NSO-Groupin valmistama matkapuhelinten vakoiluun tarkoitettu ohjelmisto, jonka tarkoituksena on antaa käyttäjälleen lähes täysi pääsy saastuttamaansa laitteeseen ja sen sisältämiin tietoihin. Ohjelmistosta on saatavilla suhteellisen paljon tietoa, sillä se on yksityisen yrityksen valmistama kaupallinen tuote. Ainakin alun perin ohjelmisto on tarkoitettu myyntiin vain valtiollisille toimijoille ja se onkin vuosien saatossa ollut käytössä useiden eri maiden viranomaisilla. Pegasusta levitettiin alun perin haitallisen linkin avulla ja se tulikin suuren yleisön tietoon vuonna 2016 arabialaisen ihmisoikeusaktivistin lähetettyä saamansa linkin tutkittavaksi Toronton Yliopistolle. [”Pegasus (spyware)” 2023].

Agrawal ja muut [2022] ovat avanneet Pegasuksen toimintaa tuoreessa artikkelissaan. Pegasus hyväksikäyttää ns. zero-click haavoittuvuuksia, mikä esimerkiksi haitallisen linkin tapauksessa tarkoittaa sitä, että pelkkä linkin klikkaaminen riittää laitteen saastuttamiseksi. Pegasusta ja sen leviämistapoja on myös jatkuvasti kehitetty ja sitä on levitetty esimerkiksi iPhoneissa olleen nollapäivähaavoittuvuuden avulla, jonka hyväksikäyttöön riitti pelkkä viestin lähettäminen kohdelaitteeseen. Toisessa tapauksessa haittaohjelman levittämiseen WhatsAppin kautta riitti pelkkä soitettu puhelu – riippumatta siitä, että vastasiko kohdehenkilö puhelimeensa vai ei. Saastutettuaan kohdelaitteensa tarjoaa Pegasus hyökkääjälle mahdollisuuden mm. puhelujen, pikaviestimien sekä laitteen sijainnin

reaaliaikaiseen seurantaan. Hyökkääjän on mahdollista seurata myös salattujen pikaviestimien, kuten Signalin ja WhatsAppin viestiliikennettä reaaliaikaisesti. Pegasus yrittää myös rootata kohdelaitteensa (prosessi, jossa matkapuhelimen käyttöjärjestelmään pyritään samaan root -tason käyttäjäoikeudet) ja siinä onnistuessaan luonnollisesti pystyy tarjoamaan lähes rajoittamattoman pääsyn saastuneelle laitteelle. Koska Pegasus tarjoaa pääsyn laitteeseen sovellustasolla, ei sen käyttämiseksi myöskään tarvita minkäänlaista yhteistyötä esimerkiksi puhelinoperaattorien kanssa. Teknisesti ottaen Pegasuksella voi siis saastuttaa laitteita missä päin maailma tahansa ilman paikallisten viranomaisten tai muiden toimijoiden yhteistyötä tai hyväksyntää.

Pegasusta pidetään yleisesti ottaen yhtenä kehittyneimmistä ja vaarallisimmista haittaohjelmista. Osa Pegasuksen vaarallisuudesta tulee siitä, että sen kehittäjänä ja ylläpitäjänä on yksityinen yritys, jolla on luonnollisesti taloudellinen motiivi ohjelman myymiseksi mahdollisimman laajalle. Vaikka Israelin puolustusministeriö väitetysti kontrolloikin ohjelmiston myyntiä tarkasti, lienee kuitenkin jossain määrin perusteltua pelätä ohjelman joutuvan riittävällä rahasummalla myös kontrolloimattomien tahojen käsiin.

4.3.6 Russian Wipers: HermeticWiper, CaddyWiper, IsaacWiper ja FoxBlade

Tämä on kokoelma haittaohjelmia, joita on käytetty mm. Venäjän ja Ukrainan välisessä sodassa vuonna 2022. Samankaltaisista nimistä huolimatta ohjelmilla on kovin vähän yhteistä keskenään, mikä onkin johtanut epäilyksiin siitä, että Kremlin palkkalistoilla on useita toisistaan erillisiä hakkeriryhmittymiä. Yleisesti ohjelmistojen laatu on ollut hieman kyseenalainen verrattuna esimerkiksi amerikkalaisiin kilpailijoihinsa, mikä kieliikin siitä, että Venäjän kyky toteuttaa edistyneitä kyberhyökkäyksiä on luultua heikompi.

Nämä kolme haittaohjelmaa toimivat myös hyvänä esimerkkinä modernista valtioiden välisessä laajamittaisessa konfliktissa käytetyistä kybersodankäynnin välineistä, eikä vastaavaa tilaisuutta tarkastella tämän typpistä kyberhyökkäystä ole aiemmin ollut. Vaikka NotPetya oli toiminnaltaan hyvin samankaltainen, ei pelissä silloin ollut fyysistä sotilasoperaatiota tai tuhansien sotilaiden henkeä. Voidaan siis kohtuudella olettaa, että näiden kolmen haittaohjelman osalta niiden kehittäjä/tilaaja on käyttänyt parasta osaamistaan.

Malwarebytes Laboratorion [2022b] työntekijät totesivat analyysissaan HermeticWiperin olevan näistä kolmesta selvästi kehittynein, monimutkaisin sekä kyvykkäin. Nimensä HermeticWiper sai sen käyttämistä digitaalisista sertifikaateista, jotka oli myönnetty yritykselle Hermetic Digital Ltd. Tiettävästi kyseisillä sertifikaateilla ei ole allekirjoitettu ollenkaan ei-haitallisia tiedostoja ja koko sertifikaatti tuntuukin olevan hankittu vain haittaohjelman käyttöön – mahdollisesti esimerkiksi ostamalla kokonainen yritys, tai rakentamalla laillinen liiketoiminta, jonka varjolla sertifikaatit on hankittu.

Raportin mukaan haittaohjelmasta tekee erityisen vaarallisen sen kyky ohittaa käyttöjärjestelmän perinteisiä suojauksia, sekä kyky tuhota laitteen tiedot siten, että niiden palauttaminen on erittäin vaikeaa. Haittaohjelma osaa myös mukautua kohdejärjestelmän arkkitehtuurin mukaisesti ja se toimii hyvin sekä 32- että 64-bitin Windows käyttöjärjestelmissä. Sovellus kuljettaa mukanaan joukon legitiimejä laiteajureita, joiden avulla se pääsee suoraan käsiksi levytoimintoihin, kuten ositusten hallintaan. Legitiimien ajureiden käyttäminen mahdollistaa samalla tiettyjen käyttöjärjestelmän suojausten ohittamisen liittyen esimerkiksi levysektorien manipulointiin käyttäjämoodissa (*user-mode*).

Raportissa esitellään myös haittaohjelman varsinainen toiminta tartunnan jälkeen. Ensimmäiseksi HermeticWiper asentaa levyasemien manipulointia varten mukana kantamansa laitteistoajurit järjestelmään. Ajureista on mukana useita versioita ja käytettävä versio valikoituu laitteistoarkkitehtuurin mukaan. Haittaohjelma ottaa tässä vaiheessa myös järjestelmän kaatumisvedokset (*crash dump*) pois käytöstä. Tämän tehdään luultavasti vaikeuttamaan haittaohjelman löytämistä tilanteessa, jossa kohdejärjestelmä kaatuu ennenaikaisesti haittaohjelman toiminnan seurauksena. Asennettu ajuri ladataan muistiin ja käynnistetään käyttöjärjestelmän palveluna. Tästä syystä esimerkiksi ajurin poistaminen levyltä ei tässä vaiheessa enää vaikuta ohjelman toimintaan. Ajurin muistiin lataamisen jälkeen haittaohjelma käy myös ottamassa ”Shadow Copy” -toiminnallisuuden pois päältä. Tämä vaikeuttaa joissain tilanteissa tiedon palauttamista varmuuskopioista. Seuraavaksi haittaohjelma muuttaa tiedostojen näyttämiseen liittyviä asetuksia, luultavasti estääkseen tietyt tapaukset, joissa käyttäjä voisi saada vihiä tiedostojen muokkaamisesta. Tämän jälkeen haittaohjelma alkaa pirstaloida (*fragment, eheyttämisen vastakohta*) levyllä sijaitsevia tiedostoja. Tämä luonnollisesti sen takia, että tiedostojen palauttaminen useassa eri sijainnissa sijaitsevista palasista on huomattavasti vaikeampaa, ellei jopa mahdotonta, verrattuna kokonaisena levyltä ylikirjoitettuun tiedostoon. Käyttöjärjestelmän tiedostot säästetään tältä toimenpiteeltä, luultavasti sekä ajan säästämiseksi että järjestelmän kaatumisen tai muiden epäilyksiä herättävien tapahtumien välttämiseksi. Lopulta haittaohjelma iteroi tiedostorakenteiden läpi ja ylikirjoittaa levyasemalla sijaitsevat tiedostot kryptografisesti luodulla satunnaisella datalla. Haittaohjelma ylikirjoittaa samalla tavalla myös levyasemien pääkäynnistyslohkot sekä tiedostojärjestelmien päätiedostotaulukon. Tehdäkseen tietojen palauttamisesta mahdollisimman hankalaa, ohjelma ylikirjoittaa levyltä myös muita rajoitetun pääsyn alueita, kuten MFTMirrorin, joka toimii päätiedostotaulukon varmuuskopiona.

Sekä Mike Bosland [2022] että Malwarebytes Laboratorion tiimi [2022a] tutkivat tuoreeltaan omilla tahoillaan löydetyn CaddyWiperin. Tutkimusten perusteella CaddyWiper on mainituista kolmesta haittaohjelmasta toimintaperiaatteiltaan selvästi yksinkertaisin. Se käy läpi laitteen levyasemat yksi kerrallaan ylikirjoittaen niillä olevat tiedostot nollatavuilla. Lopuksi se käy fyysiset levyt läpi yksi kerrallaan ja ylikirjoittaa levyjen

ositustaulukot (*partition table)*. Tämä vaikeuttaa tietojen palauttamista ja estää mm. laitteen käynnistämisen. Mielenkiintoisena yksityiskohtana CaddyWiper yrittää myös tarkastaa levyaseman ”]:\\” olemassaolon. Tämä on kaikella todennäköisyydellä vain näppäilyvirhe ohjelman koodissa, tarkemmin sanottuna levyasemat yksi kerrallaan läpi iteroivan silmukan yläehdossa, sillä ASCII-taulukossa ”]” on seuraava kirjain heti Z:n jälkeen. Se, että näinkin tärkeään tehtävään kehitetyn ja suhteellisen yksinkertaisen sovelluksen tuotantoversion koodiin on päätynyt näppäilyvirhe, kertonee siitä että kehityksellä on ollut kiire.

Malwarebytes Laboratorion [2022a] tuottaman analyysin mukaan IsaacWiper on myös huomattavasti HermeticWiperia yksinkertaisempi ja toimii lähes identtisesti CaddyWiperin kanssa iteroiden läpi sekä loogiset että fyysiset levyasemat, ja tuhoten niillä sijaitsevat tiedot. Analyysistä selviää, että IsaacWiperissa on CaddyWiperin tapaan merkkejä huolimattomuudesta tai kiireestä. Sovelluksen tuotantoversioon on jäänyt joukko tavallisesti virheenselvityksessä ja testauksessa käytettäviä merkkijonoja, jotka selostavat sovelluksen toimintaa varsin mallikelpoisesti. Esimerkkinä ”getting drives…” ja ”start erasing system physical drive…”.

Kaikki kolme edellä mainittua venäläistä tuhoajaa on valikoitu mukaan tähän tutkielmaan, sillä ne ovat olleet suorassa kytköksessä Venäjän ja Ukrainan väliseen konfliktiin, ja niiden kehittäjä on vähintään tehnyt tiivistä yhteistyötä Venäjän valtion instanssien kanssa.

4.3.7 Snake

Snake on Venäjän ja sen kansallisen turvallisuuspalvelu FSB:n vastine läntisen rintaman vakoojille Duquille ja Flamelle. Vaikka Snaken olemassaolosta on tiedetty ja sen Venäjäkytköksiä epäilty jo useita vuosia, ilmestyi siitä tarpeeksi kattava analyysi julkisuuteen vasta keväällä 2023. Analyysissä on selostettu Snaken toimintaa kattavasti ja hyvin teknisellä tasolla, mutta muutamia avainasioita jää silti selvittämättä erityisesti haittaohjelman historiasta sekä siitä, että miten ja kenen toimesta se on alun perin havaittu.

Edellä mainittu tekijänimellä ”CISA and Partners” [2023] julkaistu lähes 50-sivuinen usean eri maan ja viranomaisen yhteistyönä tuotettu tekninen raportti haittaohjelmasta valottaa sen toimintaa hyvin tarkalla tasolla. Raportin mukaan esimerkiksi Snaken kehitys ja käyttö on alun perin aloitettu jo vuonna 2003 nimellä ”Uroburos”, ja vaikka ohjelmiston olemassaolosta on tasaisin väliajoin saatu viitteitä ja muutaman kerran jopa julkistakin huomiota, on FSB kuitenkin koko ajan jatkanut sen kehittämistä. Vaikka Snake onkin koko ajan ollut yksi ja sama haittaohjelma ei se silti ole kovin kaukana Duqusta, Duqu 2:0:sta ja Flamesta, jotka ovat jokainen vuorollaan korvanneet edeltäjänsä, mutta jatkaneet silti selkeästi samaa operaatiota ja ajaneet samoja tavoitteita. Periaatteessa Snakenkin voitaisiin ajatella koostuvan vuosien varrella kehitetyistä useammista eri versiosta,

vaikka niitä ei olekaan lähdetty erikseen nimeämään. Snake on siis kehityshistorialtaan hyvin saman kaltainen edellä mainittujen läntisten kyberaseiden kanssa.

Raportissa todetaan myös Snaken olevan ylivoimaisesti kehittynein Venäjän tuottama haittaohjelma, minkä lisäksi sen epäillään toimineen poikkeuksellisen pitkän aikaa lähes huomaamatta. Varsinaiselta toiminnallisuudeltaan Snake ei juuri eroa muista kehittyneistä vakoojista – se tarjoaa hyökkääjälle lähes rajattoman pääsyn saastuttamaansa laitteeseen ja pyrkii piilottamaan oman toimintansa, sekä estämään oman havaitsemisensa. Lisäksi muiden vakoojien tavoin sitä käytetään vain tarkoin valikoitua ja suhteellisen pientä kohdejoukkoa vastaan. Snaken tavoitteena on tutkimusten mukaan ollut tarjota pitkäaikainen pääsy sen saastuttamien järjestelmien sisältämään tietoon, ja se vaikuttaakin onnistuneen siinä poikkeuksellisen hyvin. Mielenkiintoisesti Snakea tutkineet tahot ovat myös väittäneet tutkineensa Snaken toimintaa koko sen lähes 20-vuotisen elinkaaren ajan. He eivät kuitenkaan erittele esimerkiksi sitä, että ovatko he kyenneet estämään Snaken toimintaa tai esimerkiksi syöttämään tarkoituksella valheellista tietoa Snaken saastuttamille laitteille, vai onko kyseessä ollut vain poikkeuksellisen pitkäkestoinen vastatiedusteluoperaatio, jossa on toimittu koko ajan muutama askel hyökkääjän jäljessä. Sinänsä olisi outoa, jos asiaan olisi ollut mahdollista vaikuttaa, ja Snaken on silti annettu rauhassa vakoilla yli vuosikymmenen ajan läntisen liittouman valtioita ja Naton jäseniä.

Niin ikään raportissa mainitaan Snaken kehittäjien vuosien varrella tekemiä virheitä, jotka lopulta edesauttoivat ohjelmiston takaisinmallinnusta ja sen toiminnan ja alkuperän selvittämistä. Kehittäjät ovat esimerkiksi jättäneet ohjelmiston koodiin humoristisia lausahduksia vastaukseksi tunnetuille analysointiyrityksille. Ainakin kerran kehittäjät ovat myös unohtaneet siistiä valmiin haittaohjelman ajettavan ohjelmatiedoston ylimääräisistä tiedoista, minkä seurauksena tutkijat saivat selville esimerkiksi käytettyjen funktioiden nimiä. Lisäksi Snakessa on käytetty tunnettuja kryptografisia algoritmeja väärin sellaisella tavalla, joka ei selity laiskuudella, vaan ainoastaan osaamisen puutteella.

Virheistään huolimatta Snake on Venäjältä käyttökelpoinen vastine USA:n Duquille ja Flamelle, ja vaikka sen kehityksessä käytettävät resurssit ja osaaminen vaikuttavatkin olevan jäljessä vastapuoleen nähden, on kyseessä kuitenkin erittäin kehittynyt ja vaarallinen haittaohjelma.

4.3.8 Stuxnet

Kuten jo luvussa 3.2 kerrottiin, on Stuxnet vuonna 2010 levinnyt haittaohjelma, jonka tarkoituksena oli aiheuttaa haittaa Iranin ydinohjelmalle sotkemalla sentrifugien toimintaa laitoksissa. Stuxnet suoritti tehtävänsä uudelleenohjelmoimalla sentrifugien moottoreita hallitsevia logiikkatietokoneita siten, että pyörintäliikkeeseen aiheutettiin ”häiriöitä”, jotka lopulta johtivat sentrifugien sattumanvaraiseen, mutta säännölliseen hajoamiseen.

Falliere ja muut [2011] tuottivat Stuxnetin toiminnasta aikoinaan hyvin kattavan analyysin. Analyysissä silmiinpistävää on koko hyökkäysketjun monimutkaisuus. Kohdentaakseen hyökkäyksen toisella puolella maapalloa korkean turvaluokituksen laitoksessa sijaitsevaan, täysin julkisesta internetistä erotettuun paikallisverkkoon kytkettyyn ohjelmoitavaan logiikkaan (*programmable logic controller, PLC*), tulee hyökkääjän tehdä aivan valtava määrä pohjatyötä.

Ensinnäkin tulee selvittää, että miten haittaohjelma ylipäätään on mahdollista saada näin suljettuun ympäristöön. Stuxnetin kohdalla tämä ratkaistiin omintakeisella lähestymistavalla, ohjelmoimalla haittaohjelma leviämään ei verkon, vaan USB-massamuistilaitteiden välityksellä. Näin ohjelmisto levisi tehokkaasti läpi maailman, kunnes lopulta löysi kohteeseensa. Analyysissa todetaan Stuxnetiin tehdyn jopa sisäänrakennetun ”rajoittimen” tartuntamäärien hillitsemiseksi – yhden muistitikun tartutettua kolme uutta laitetta, tuhosi Stuxnet itsensä kyseiseltä tikulta. Tällainen on todennäköisesti tehty tartuntamäärien hallitsemiseksi ja siten ohjelmiston ennenaikaisen havaitsemisen välttämiseksi.

Levittämisen jälkeen seuraavaksi kynnyskysymykseksi muodostuu kohdelaitteiden tarkka malli ja versio, sekä esimerkiksi niissä käytetty konfiguraatio. Näin tarkkoja tietoja ei luonnollisesti julkisteta verkossa tai muuallakaan julkisissa lähteissä. Analyysin mukaan Stuxnetin kohdalla em. tietojen hankinta on todennäköisesti tehty aikaisempien haittaohjelmien (Flame ja/tai Duqu) toimesta. Tätä on kuitenkin vaikea tyhjentävästi osoittaa.

Kolmas haaste liittyy siihen, kuinka tartuntakohteessa toimitaan huomaamatta siihen asti, että ohjelmiston alkuperäinen tehtävä on suoritettu onnistuneesti. Analyysin mukaan Stuxnet käytti tähän sekä nollapäivähaavoittuvuuksia että luotetulla digitaalisella avaimella allekirjoitettuja ajureita. Näin mahdolliset torjuntaohjelmistot eivät osanneet epäillä haittaohjelmaa, eikä esimerkiksi käyttöjärjestelmän ja ohjelmiston päivittämisellä ajantasaiseen versioon ollut merkitystä havaitsemisen kannalta.

Analyysissa mainitaan vielä yksi mielenkiintoinen ja hieman poikkeuksellinen seikka Stuxnetistä. Vaikka Stuxnetillä oli perinteinen komentopalvelininfrastruktuuri, jonka kautta haittaohjelman oli mm. mahdollista päivittää itseään ja jonka kautta haittaohjelman tekijät pystyivät todennäköisesti seuraamaan ohjelman levittämistä, ei ohjelman toimintaa voitu kuitenkaan laskea komentopalvelininfrastruktuurin varaan. Koska Stuxnetin lopullisesta toimintaympäristöstä oli erittäin epätodennäköistä saada internetyhteyttä ulospäin, tuli kaikki mahdollisesti tarvittava toiminnallisuus joka tapauksessa paketoida jo alkuperäiseen haittaohjelmaan. Perinteinen malli, jossa varsinainen haittaohjelma on mahdollisimman kevyt, ja jossa vasta tartunnan jälkeen ladataan lisämoduulit ei siis tullut kysymykseen Stuxnetin kohdalla. Tämä on varmuudella monimutkaistanut Stuxnetin kehitystä ja vaatinut todennäköisesti aivan valtavan määrän testaamista. Käytännössä hyökkääjällä on täytynyt olla lähes identtinen kohdeympäristö harjoittelua ja testaamista varten.

Kokonaisuutenaan Stuxnetiä pidetään onnistuneena operaationa ja yleisesti ollaan sitä mieltä, että haittaohjelma ehti saavuttaa tavoitteensa ennen sen havaitsemista. Vaikka Stuxnetin kehittäjästä ei koskaan saatu täyttä varmuutta, ovat useimmat asiaa tutkineet tahot päätyneet siihen lopputulokseen, että Stuxnet oli USA:n ja Israelin yhteinen kyberoperaatio Iranin ydinohjelmaa vastaan [Baezner ja Robin 2017].

Stuxnet on valikoitu mukaan tähän tutkielmaan siksi, että se on valtiolähtöinen haittaohjelma, jonka tarkoitus on ollut aiheuttaa fyysistä tuhoa toisen valtion alueella.

4.3.9 WannaCry

WannaCry oli hyvin tehokkaasti ja täysin autonomisesti leviävä haittaohjelma, joka saastutti vuonna 2017 yli 200000 tietokonetta yli 150:ssa maassa. Tyypiltään WannaCry oli niin kutsuttu kiristyshaittaohjelma. Ohjelma salasi saastuttamastansa järjestelmästä tietoja ja pyysi tämän jälkeen bitcoineja ”lunnaina” salauksen purkamisesta tietojen takaisin hankkimiseksi. WannaCry:ta on tutkittu paljon ja näihin perustietoihin ovat päätyneet mm. Akbanov ja muut [2018] sekä Trautman ja Ormerod [2019]. Molemmat toteavat niin ikään hyökkäyksen levinneen laajalti mm. kriittisen infrastruktuurin toimijoihin, kuten sairaaloihin ja lainvalvontayksiköihin. Trautman ja Ormerod [2019] toteavat myös tiedusteluviranomaisten selvittäneen hyvin nopeasti Pohjois-Korean olleen hyökkäyksen takana ja hyökkäyksen kriittisenä komponenttina käytetyn pari kuukautta aiemmin NSA:n tietomurrossa ”karannutta” Eternal Blue -nimistä Microsoft Windowsin haavoittuvuutta. Mielenkiintoista WannaCry:n leviämisessä on se, että kyseinen haavoittuvuus oli korjattu jo useampi kuukausi ennen WannaCry:n leviämistä. NotPetyan tavoin Wannacry toimii hyvänä esimerkkinä siitä, kuinka organisaatiot ja käyttäjät eivät ylläpidä laitteistoaan riittävän tehokkaasti. Samalla se osoittaa myös sen, että vakavan ja erittäin laajalle leviävän haittaohjelman voi tuottaa myös ilman nollapäivähaavoittuvuuksia.

Teknisen analyysin WannaCry:sta tuottaneet Akbanov ja muut [2018] tutkailivat haittaohjelman toimintaa tarkemmin ja totesivat sen käyttäneen Eternal Bluen lisäksi myös toista aikaisemmassa NSA:n tietomurrossa julkaistua työkalua, DoublePulsaria. Kyseessä on eräänlainen takaovikomponentti, jolla varmistetaan saastuneen laitteen etähallinta myös varsinaisen saastumisen jälkeen.

Samassa analyysissa jatketaan ohjelman toiminnan selvittämistä varsinaisen saastuttamisen jälkeen. Ensinnäkin ohjelma salaa suuren osan levyjärjestelmän tiedoista kryptografisesti turvallisilla menetelmillä, tehden tiedoista käytännössä käyttökelvottomia. Tämän jälkeen sovellus tarjoaa mahdollisuutta purkaa salaus maksamalla n. 300 €:n lunnaat. Toimintansa jatkuvuuden varmistamiseksi ohjelma huolehtii useammalla eri tavalla siitä, että se ajetaan automaattisesti järjestelmän uudelleenkäynnistyksen yhteydessä. Tämän lisäksi ohjelma ottaa Windowsin varmuuskopiointiin liittyvää toiminnallisuutta pois käytöstä, sekä yrittää katkaista mahdolliset aktiiviset tietokantayhteydet, todennäköisesti estääkseen tiedon varmuuskopioinnin tätä kautta. Näiden alkutoimintojen jälkeen ohjelma

yrittää levittää itseänsä jokaiseen mahdolliseen IP-osoitteeseen paikallisessa verkossa. Analyysissa todetaan myös alun perin Marcus Hutchinin löytämän ”tappokytkimen” olemassaolo. Kyseessä on verkko-osoite, johon WannaCry yrittää heti toimintansa alkuvaiheessa ottaa yhteyttä ja mikäli verkko-osoitteesta ei saada vastausta, jatkaa haittaohjelma toimintaansa. Haittaohjelman leviämisen pystyi siis käytännössä keskeyttämään kuka tahansa rekisteröimällä tuon verkko-osoitteen itselleen.

Todennäköisesti WannaCry:n oli tarkoituskin levitä mahdollisimman nopeasti ja mahdollisimman laajalle, sillä kyseisen tappokytkimen löytäminen ei ollut teknisesti kovin haastava toimenpide, ja sen olisikin todennäköisesti löytänyt hyvin nopeasti kuka tahansa vähänkään kokenut haittaohjelmien analysoinnin ammattilainen. Ohjelman elinikä ja sen mahdollisuudet pitkäaikaiseen leviämiseen olivat siis jo alusta pitäen kovin heikot.

Waleed ja Harshini [2018] pohtivat mm. haittaohjelman mahdollisia rahallisia ja poliittisia motiiveja. Rahallisesti he totesivat haittaohjelman olleen massiivinen epäonnistuminen, sillä lunnaita saatiin kerätyksi yhteensä vain noin 140000 dollaria. Rahallista motiivia ei kuitenkaan voi sulkea pois, sillä pohjoiskorealaisten hakkeriryhmien tiedetään tehneen aikaisemmin kyberhyökkäyksiä puhtaasti rahaa kerätäkseen. Motiivin suhteen he päätyvät kuitenkin johtopäätökseen, että WannaCry on Pohjois-Korean kehittämä kyberase, jonka oikeana tarkoituksena oli aiheuttaa tuhoa ja joka oli vain naamioitu kiristysohjelmaksi.

WannaCry on otettu mukaan tähän tutkielmaan, sillä se on lähes varmasti valtiolähtöinen haittaohjelma, ja vaikka sillä ei välttämättä ole ollut tarkkaa ja ennalta määriteltyä toisen valtion alueella sijaitsevaa kohdetta, on se kuitenkin aiheuttanut huomattavan määrän tuhoa ympäri maailman.

5 Analyysi

Tässä luvussa tutkitaan ja vertaillaan aiemmin esiteltyjä kyberaseita neljässä eri kategoriassa: *tyyppi ja alkuperä*, *aika ensimmäisestä tartunnasta haittaohjelman havaitsemiseen*, *leviämistapa* sekä *havaitsemisen ja analysoinnin esto*. Tuloksista muodostetaan taulukot, joiden perusteella ohjelmien ja niiden kyvykkyyksien vertailu on helppoa. Taulukot toimivat myös pohjustuksena yhteenvetoon ja pohdintaan luvussa 6.

5.1 Tyyppi ja alkuperä

Tämän tutkielman kohteena olevat kyberaseet on kategorisoitu kolmeen eri luokkaan niiden pääasiallisen tehtävän mukaan. Luokat ovat vakooja, tuhoaja sekä sabotoija. Vakoojan tehtävä on kerätä informaatiota tai mahdollistaa vaikkapa etäkäyttöyhteys saastuneeseen laitteeseen tai järjestelmään. Tuhoajan tehtävä on tuhota tietoa tai muulla tavoin tehdä tiedosta pysyvästi käyttökelvotonta esimerkiksi salaamalla laitteen kovalevy satunnaisesti generoidulla avaimella. Sabotoijan tehtävä on aiheuttaa fyysistä tuhoa esimerkiksi hajottamalla laitteita tai niiden komponentteja. Sabotoijan ja tuhoajan konkreettinen

ero on siinä, että tuhoajan kohteena on tieto ja sabotoijan kohteena fyysinen infrastruktuuri tai laitteisto. On hyvä kuitenkin ottaa huomioon, että esimerkiksi jotkut vakoojat saattavat myös mahdollistaa tietojen pysyvän tuhoamisen ja jotkut tuhoajat saattavat myös sivutoimisesti vakoilla. Vastaavasti tiedon tuhoaminen tai vakoilu voi kumpikin välillisesti aiheuttaa vahinkoa myös fyysiselle infrastruktuurille. Jaottelu on siis tehty ohjelmiston pääasiallisen tavoitteen mukaan, eikä se ole missään nimessä eksplisiittinen.

Vaikka haittaohjelman alkuperää on usein vaikea todistaa aukottomasti, on tutkimuksissa silti pystytty useimpien ohjelmien kohdalla päätymään vähintäänkin todennäköiseen lähteeseen. Monesti alkuperää voidaan tutkailla esimerkiksi haittaohjelman tavoitteiden tai sen leviämisreitin kautta. Tunnetaan myös tapauksia, jossa haittaohjelman toimintaa analysoimalla saatiin selville yksityiskohtia sitä operoineen tahon työajoista ja esimerkiksi siitä, että milloin ko. taho vietti viikonloppua. Tämä luonnollisesti antaa jo hyvää osviittaa ohjelman taustalla mahdollisesti olevista tahoista ja lähes varmasti ainakin sulkee pois paljon vaihtoehtoja. Tiedot sekä haittaohjelmien alkuperästä että tyypistä on koostettu taulukkoon 1. Mielenkiintoisesti esimerkiksi Kiinalta ei ole saatu kriteeristöä täyttäviä haittaohjelmia mukaan tutkielmaan.

	Vakooja	**Tuhoaja**	**Sabotoija**	**Alkuperä**
CaddyWiper		x		Venäjä
Duqu	x			USA & Israel
Duqu 2.0	x			USA & Israel
Flame/Skywiper	x			USA & Israel
HermeticWiper		x		Venäjä
IsaacWiper		x		Venäjä
NotPetya		x		Venäjä
Pegasus	x			Israel
Snake	x			Venäjä
Stuxnet			x	USA & Israel
WannaCry		x		Pohjois-Korea

Taulukko 1: Tyyppi ja alkuperä

CaddyWiper, HermeticWiper ja IsaacWiper ovat kaikki Ukrainan ja Venäjän välisessä sodassa heti alkumetreillä fyysisen hyökkäyksen kanssa synkronoituun kyberhyökkäykseen käytettyjä tuhoajia [ESET Research 2022a]. Kaikkien kolmen kohdalla alkuperä osoittaa selkeästi Venäjälle, sillä haittaohjelmia käytettiin nimenomaan tukemaan

Venäjän hyökkäystä ja lamauttamaan Ukrainan puolustusta. Tämän lisäksi etenkin HermeticWiperin ja IsaacWiperin käyttö oli aikataulutettu niin tiukasti varsinaisen sotilasoperaation kanssa, ettei sijaa epäilyksille valtiolähtöisyydestä juuri voi jäädä [ESET Research 2022a].

Huolimatta yhdenkaltaisuudestaan Stuxnetin kanssa, on Duqu puhdas vakooja [Chien ja muut 2012]. Sama pätee myös Duqu 2.0:aan, joka on tosin alkuperäiseen Duquun verrattuna vielä huomattavasti kehittyneempi ja kyvykkäämpi [Bencsáth ja muut 2015]. Vakoojaksi paljastui myös vuonna 2012 havaittu Flame, joka tarjoaa operoijalleen käytännössä täyden näkyvyyden kohdelaitteen toimintaan [Bencsáth ja muut 2012b].

Kuten mainittu, on tutkimuksissa Duqun havaittu jakavan hämmentävän paljon komponentteja Stuxnetin kanssa, ja sen perusteella Duqun onkin yleisesti epäilty olevan lähtöisin samasta organisaatiosta - eli niin ikään USA:n ja Israelin yhteisestä hankkeesta Iranin ydinohjelmaa vastaan [Bencsáth ja muut 2012a]. Myös Chien ja muut [2012] päätyivät tutkimuksissaan täysin samaan loppupäätelmään.

Flamen osalta Bencsáth ja muut [2012b] taas totesivat tuhansista sen saastuttamista laitteista suurimman osan sijaitsevan niin ikään Lähi-Idässä ja vähemmän yllättävästi Iranissa. He epäilivät Flamen kohteena olleen pääasiallisesti Iranin ja Libanonin hallitukset. Lisäksi tutkimuksessa todettiin Duqun ja Flamen jakavan hyvin paljon yhtäläisyyksiä esimerkiksi korkean tason toimintamallissa, kohteiden valinnassa sekä kehityksen aikatauluissa. Tämä todetaan antavan aiheen epäillä molempien haittaohjelmien kehityksen tapahtuneen vähintäänkin samaa operaatiota varten ja siten todennäköisesti saman tahon koordinoimana. Avoinna on pidettävä esimerkiksi mahdollisuus, jossa alkuperäinen hyökkääjä on halunnut varmistaa operaation onnistumisen tilaamalla samaan päämäärään tähtääviä haittaohjelmia useammalta eri toimittajalta. Teoriassa kehittäjinä voisivat varmaan toimia myös saman viraston eri osastot.

Bencsáth ja muut [2015] myös totesivat Duqu 2.0:n kehittäjillä olleen lähes varmasti pääsyn myös alkuperäisen Duqun lähdekoodeihin. Kaspersky Lab:n työntekijät [2015] puolestaan havaitsivat ohjelman toimintaa analysoimalla, että Duqu 2.0:n kehittäjät ovat erittäin todennäköisesti työskennelleet sunnuntaista torstaihin, perjantain ollessa huomattavasti kevyempi päivä ja lauantain käytännössä vapaapäivä. Tämä sopisi esimerkiksi Israeliin, mutta ei USA:an. Lisäksi havaittiin, että ainakin yksi kohde oli saastutettu sekä Duqu 2.0:n, että NSA:n oman yksikön, Equation Groupin, toimesta. Tämä viittaa siihen, että Duqu 2.0:n kehittänyt organisaatio ja Equation Group ovat osittain myös keskenään kilpailevia sekä vahvistaa entisestään olettamaa, että Duqu 2.0 ei ole yksin USA:n oma hanke, vaan mitä todennäköisemmin sama jo Duqun, Flamen ja Stuxnetin kohdalla tutuksi tullut USA:n ja Israelin yhteinen hanke [Kaspersky Lab 2015].

Hieman muusta joukosta poikkeava vakooja on vuonna 2016 suurten massojen tietoisuuteen tiensä löytänyt Pegasus, jonka kohteena ovat erityisesti matkapuhelimet.

Useimmista muista tämän tutkielman kyberaseista poiketen Pegasus on myös yksityisen yrityksen kehittämä ja ylläpitämä, joskin vain valtiolliseen käyttöön myytävissä oleva ratkaisu. Pegasusta kehittävä ja myyvä yritys on kotoisin Israelista, ja sen myyntiä ja levitystä kontrolloidaan Israelin puolustusministeriön toimesta. [Agrawal ja muut 2022]

Kiristyshaittaohjelmaksi on WannaCryn lisäksi naamioitunut myös tartuntojen perusteella Ukrainaa vastaan kohdistettu NotPetya, jonka kehittäjillä (tai levittäjillä) ei todellisuudessa ollut mitään mahdollisuutta palauttaa uhriensa tietoja, vaikka nämä olisivatkin maksaneet vaaditut lunnaat [Sai ja Kumar 2019]. Ohjelman todellisen motiivin epäillään-kin olleen haitan aiheuttaminen mm. Ukrainan finanssisektorille. Yleisesti myös NotPetyaa pidetään osana Ukrainan ja Venäjän välistä konfliktia, ja mm. Yhdysvaltojen keskustiedustelupalvelu (*Central Intelligence Agency, CIA*) sekä kansallinen kyberturvakeskus (*National Cyber Security Centre, NCSC)* ovat todenneet Venäjän hallituksen olevan ”lähes varmasti” haittaohjelman taustalla. Tämän ovat todenneet mm. Greenberg [2018] ja Krasznay [2020].

Viimeisimpänä vahvistuksena tähän tutkielmaan mukaan saatu Snake on Venäjältä peräisin oleva vakooja, joka toiminnaltaan muistuttaa paljon läntisen liittoumaan ykkösvakoojia Duquja sekä Flamea. Erityisesti USA on yhdessä muiden Five Eyes -maiden kanssa tutkinut ja seurannut Snakea jo vuosien ajan, eikä sen alkuperästä ole seurannan perusteella jäänyt epäselvyyttä. Snaken päivittäistä operointia ja kehitystyötä on suoritettu FSB:n yksiköstä Ratsan kaupungista Venäjältä, minkä lisäksi sen avulla on suoritettu operaatioita myös Moskovasta. Vaikka Snake ottaakin kohdelaitteensa lähes täydellisesti haltuunsa, on sen käyttötarkoitukseksi kuitenkin osoittautunut Duqun ja Flamen tavoin ennen kaikkea vakoileminen. Snaken avulla Venäjän tiedustelun tiedetään päässeen käsiksi arkaluontoiseen materiaaliin mm. valtioiden verkoissa ja tutkimuslaitoksissa. [CISA and Partners 2023]

Stuxnet, jonka ainoa tunnistettu tehtävä oli hidastaa Iranin ydinohjelmaa aiheuttamalla fyysistä tuhoa, on tyypiltään selkeä sabotoija [Falliere ja muut 2011]. Taulukosta 1 nähdään Stuxnetin myös olevan tämän tutkielman ainoa sabotoija. Kuten luvussa 3.2 jo todettiin, ei Stuxnetin kehittäjästä koskaan saatu täyttä varmuutta. Esimerkiksi Baezner ja Robin [2017] totesivat kuitenkin useimpien tutkijoiden hyväksyneen sen lopputuloksen, että haittaohjelma oli USA:n ja Israelin yhteinen hanke. Tähän on päädytty mm. molempien maiden motivaatiolla vahingoittaa Stuxnetin kohteena ollutta Iranin ydinohjelmaa, sekä Stuxnetin kehityksen vaatineiden valtavien resurssien ja asiantuntemuksen takia.

Tuhoajaksi lasketaan myös WannaCry. Waleedin ja Harshinin [2018] loppupäätelmää WannaCryn roolista tuhoajana kiristysohjelman sijaan tukee mm. ohjelman aiheuttamien tuhojen laajuus suhteessa sen avulla kerättyjen rahojen määrään. Lisäksi ohjelman kehittäjien on myös täytynyt tietää, että ohjelma tulee joka tapauksessa aiheuttamaan

fyysistä tuhoa mm. sairaaloissa. WannaCryn suhteen useat tutkijat, mm. Trautman ja Ormerod [2019], ovat todenneet sen olevan lähtöisin LazaruGroupilta, joka taas on yhdistetty Pohjois-Korean valtioon. WannaCry esimerkiksi jakaa moduuleja aikaisempien saman ryhmän kehittämien haittaohjelmien kanssa, minkä lisäksi mm. NSA:n tutkijat selvittivät haittaohjelman alkuperän murtautumalla sen komentopalvelimille. Joulukuussa 2017 Yhdysvaltain hallitus syytti julkisesti Pohjois-Koreaa haittaohjelman kehittämisestä [Waleed ja Harshini 2018].

5.2 Aika ensimmäisestä tartunnasta haittaohjelman havaitsemiseen

Vaikka haittaohjelmien tarkkoja kehitysajankohtia pyritäänkin peittelemään esimerkiksi väärentämällä tiedostojen ja kääntäjien aikaleimoja, on niiden leviämisestä yleensä saatavilla luotettavaa ja hyvinkin tarkkaa tietoa. Tällaista tietoa tuottavat esimerkiksi antivirusohjelmistojen valmistajat, jotka pystyvät reaaliaikaisesti seuraamaan haittaohjelman liikkumista internetissä uusien tartuntahavaintojen avulla. Tieto on yleensä saatavilla myös jälkikäteen digitaalisen forensiikan keinoin tutkimalla esimerkiksi tartunnan jo saaneita laitteita haittaohjelman jättämien jälkien varalta. Taulukoon 2 on koostettu jokaisen haittaohjelman osalta ajankohta ensimmäisestä havaitusta tartunnasta ja haittaohjelman löytämisestä, sekä laskettu näiden välillä kulunut aika.

	Ensimmäinen todennettu tartunta	**Haittaohjelma löydetty / julkistettu**	**Aika tartunnasta havaitsemiseen**
CaddyWiper	Maaliskuu 2023	Maaliskuu 2023	Välitön
Duqu	Maaliskuu 2010 - Huhtikuu 2011	Lokakuu 2011	n. 6kk-18kk
Duqu 2.0	2014	2015	n. 12kk
Flame/Skywiper	Joulukuu 2007	Toukokuu 2012	> 5v
HermeticWiper	Helmikuu 2023	Helmikuu 2023	Välitön
IsaacWiper	Helmikuu 2023	Helmikuu 2023	Välitön
NotPetya	27.6.2017	27.6.2017	Välitön
Pegasus*	2011	2016	> 5v
Snake**	n. 2004	2023	19v
Stuxnet	Marraskuu 2008	Kesäkuu 2010	n. 18kk
WannaCry	12.5.2017	12.5.2017	Välitön

Taulukko 2: Aika ensimmäisestä tartunnasta haittaohjelman havaitsemiseen

**Kyseessä on kaupallinen sovellus, jolla on ollut sekä käyttäjiä että kohteita ympäri maailman. Vaikka ohjelma onnistuikin välttelemään suuren yleisön tietoisuutta, on sen olemassaolo tuskin ollut kovin suuri salaisuus valtioiden tasolla.*

*** Snaken olemassaolosta on tiedetty julkisuudessa jo useita vuosia, mutta tarkkaa ja luotettavaa tietoa sen toiminnasta, laajuudesta ja alkuperästä ei ole ollut aiemmin saatavilla. Teknisesti ottaen haittaohjelma on siis havaittu jo aiemmin, mutta löytöpäiväksi on tässä tutkielmassa merkitty vuosi 2023, jolloin haittaohjelman olemassaolo julkistettiin koko maailmalle.*

Venäläisten Wiperien kohdalla haittaohjelmat ovat mitä ilmeisimmin kehitetty vain joitakin kuukausia ennen niiden löytämistä. HermeticWiperin kohdalla haittaohjelman valmistuminen voidaan kohdentaa loppusyksyyn vuonna 2021. Tämä voidaan todeta paitsi ajettavien tiedostojen, myös käytetyn sertifikaatin sisältämistä aikaleimoista [Guerrero-Saade 2022]. ESET Research Laboration työntekijät [2022a] päätyivät samaan aikajanaan myös IsaacWiperin osalta. Bosland [2022] taas osoitti CaddyWiperin käännöspäivän ollen maaliskuussa 2023, eli vain joitakin viikkoja ennen sen löytymistä. Kaikissa kolmessa tapauksessa em. tutkimukset totesivat kuitenkin varsinaisten tartuntojen tapahtuneen lähes välittömästi ennen haittaohjelmien aktivoitumista ja niiden havaitsemista.

Duqu ”löydettiin” tai sen löytyminen tehtiin julkiseksi lokakuussa 2011, kun CrySyS laboratorion työntekijät julkistivat kirjoittamansa 60-sivuisen analyysin löytämästään uudesta haittaohjelmasta. Chien ja muut [2012] kertovat, että ensimmäiset varmistetut havainnot Duqun tartuttamista laitteista ovat huhtikuulta vuodelta 2011. Samassa tutkimuksessa todetaan kuitenkin myös, että todellisuudessa ensimmäiset hyökkäykset olivat mahdollisesti tapahtuneet jo vuoden 2010 maaliskuussa.

Duqu 2.0:n kohdalla ensimmäinen varmennettu tartunta löydettiin vasta vuonna 2015, mutta Kaspersky Lab:n työryhmä [2015] epäili ohjelmiston olleen toiminnassa ainakin vuoden ennen tätä.

Flamen tapauksessa aika haittaohjelman havaitsemiseen oli poikkeuksellisen pitkä, jopa viidestä kahdeksaan vuotta. Vaikka Flame löydettiinkin virallisesti vasta toukokuussa 2012, on ensimmäisten tartuntojen ajankohta jälkikäteen saatu pääteltyä siitä, että Flamen hyvin omintakeisesti nimeämää tiedostoa ”wavesup3.drv” on raportoitu löytyneen eurooppalaisista järjestelmistä ensimmäisen kerran jo 5.12.2007, Arabiemiraateista noin puoli vuotta myöhemmin 28.4.2008 sekä Iranista (todennäköinen oikea kohdemaa) vajaa kaksi vuotta myöhemmin 1.3.2010 [Bencsáth ja muut 2012b].

NotPetya havaittiin käytännössä heti ensimmäisten tartuntojen jälkeen, sillä se esitti lunnasvaatimuksensa pakottamalla saastuttamansa laitteet käynnistymään uudelleen lähes välittömästi salattuaan laitteelta haluamansa tiedot [Krasznay 2020].

Pegasus on mielenkiintoinen ja hieman poikkeava tapaus, sillä sen ensimmäiset versiot ovat olleet olemassa jo 2010-luvun alkupuolella, mutta ensimmäiset konkreettiset havainnot sen käytöstä tulivat julkisuuteen vasta vuonna 2016. Koska kyseessä on kuitenkin kaupallinen sovellus, on sitä mitä suuremmalla todennäköisyydellä esitelty ja markkinoitu ainakin jonkinlaiselle kohderyhmälle. Toki tämä joukko on voinut olla hyvinkin rajattu, esimerkiksi vain Yhdysvaltalaisten ja Israelilaisten toimijoiden

keskuuteen. Joka tapauksessa tietoja haittaohjelman olemassaolosta ei juuri liikkunut julkisuuteen. Kokonaisuutena ohjelma ehti toimia 5 vuotta ennen sen havaitsemista. [Bazaliy ja muut 2016]

Snakea ja sen eri versioita on tutkittu Five Eyes -maiden toimesta väitetysti jo lähes 20 vuotta, mikä tekee siitä tässä tutkielmassa mukana olevien haittaohjelmien keskuudessa kaikkein pitkäikäisimmän. Myös julkisuuteen on säännöllisen epäsäännöllisesti päätynyt tietoja tai tiedon palasia kyseisestä haittaohjelmasta, mutta suurempi julkistus sen olemassaolosta sekä analyysi sen toiminnasta julkistettiin vasta vuonna 2023, mikä on myös tässä tutkielmassa merkitty haittaohjelman havaitsemisajankohdaksi. Vaikka tiedustelupalveluissa ohjelman olemassaolosta onkin tiedetty jo huomattavasti pidempään, on mysteeriksi jäänyt se, että millä tasolla tiedustelupalvelut ovat kyenneet Snaken toimintaa seuraamaan. Onko sen toimintaa esimerkiksi kyetty estämään, vai onko vain ollut tiedossa, että tällainen ohjelma vakoilee tiettyjä kohteita. [CISA and Partners Advisory 2023]

Falliere ja muut [2011] totesivat Stuxnetin levinneen n. 1v - 1,5v ennen sen havaitsemista kesäkuussa 2010. Ko. tutkimuksen mukaan ensimmäiset vahvistetut löydökset haittaohjelmasta ovat todennäköisesti jo loppuvuodesta 2008, mutta viimeistään huhtikuulta 2009.

WannaCry:n tapauksessa sen erittäin nopean leviämisen ja siitä seuranneen tuhoisan luonteen takia se havaittiin myös lähes välittömästi leviämisen alettua. Leviäminen alkoi 12. toukokuuta 2017, ja loppui myöhemmin samana päivänä ohjelman sisäänrakennetun tappokytkimen löydyttyä [Akbanov ja muut 2017; Waleed ja Arshini 2018].

5.3 Leviämistapa

Useiden haittaohjelmien tavoitteena on levitä autonomisesti laitteelta toiselle viimeistään sen jälkeen, kun se on löytänyt tiensä kohdeorganisaation sisäiseen verkkoon. Tehokkaimmat keinot leviämiseen ovat yleensä nollapäivähaavoittuvuudet, sillä nimensä mukaisesti niihin ei ole olemassa korjaavia päivityksiä. Näin varmistetaan se, että edes täysin päivitetyt ja hyvin ylläpidetyt laitteet eivät ole haittaohjelmalta turvassa. Nollapäivähaavoittuvuuksien käyttöön liittyy kuitenkin iso ongelma – kun haavoittuvuutta käytetään laajalti hyväksi, tulee se nopeasti yleiseen tietoon, minkä jälkeen sen kohteena oleva ohjelmiston valmistaja yleensä korjaa haavoittuvuuden hyvin nopealla aikataululla. Korjaavan päivityksen julkaisemisen jälkeen nollapäivähaavoittuvuuden tehokkuus heikkenee oleellisesti, eikä sitä enää voi onnistuneesti käyttää aktiivisesti ylläpidettyjä järjestelmiä vastaan. On hyvä myös huomioida, että vakavat nollapäivähaavoittuvuudet suosittuihin ohjelmiin ovat suhteellisen harvinaisia, ja niiden löytämisestä sekä omistamisesta käydään jatkuvaa kilpailua. Nollapäivähaavoittuvuudet eivät myöskään ole ainoa tapa levittää haittaohjelmaa, sillä historiassa on nähty myös monia erittäin onnistuneita haittaohjelma-aaltoja, joissa ei ole ollenkaan käytetty hyväksi nollapäivähaavoittuvuuksia.

Tarkempia tietoja haittaohjelmien käyttämistä leviämistavoista sekä mahdollisten nollapäivähaavoittuvuuksien hyväksikäytöstä on koostettu taulukkoon 3.

	Nollapäivähaavoittuvuuksien hyväksikäyttö	**Tartuntatapa**
CaddyWiper	Ei tiedossa	Tartutetaan manuaalisesti, todennäköisesti muun tietomurron yhteydessä
Duqu	Kyllä	Kohdennettu, keihäskalastus
Duqu 2.0	Kyllä	Kohdennettu, todennäköisesti keihäskalastus
Flame/Skywiper	Kyllä	Kohdennettu, todennäköisesti keihäskalastus
HermeticWiper	Ei tiedossa	Tartutetaan manuaalisesti, todennäköisesti muun tietomurron yhteydessä
IsaacWiper	Ei tiedossa	Tartutetaan manuaalisesti, todennäköisesti muun tietomurron yhteydessä
NotPetya	Ei	Lievästi kohdennettu ns. ”Watering hole” -hyökkäys
Pegasus	Kyllä	Kohdennettu, useita eri tapoja
Snake	Ei tiedossa	Kohdennettu, tarkka tapa ei tiedossa
Stuxnet	Kyllä	Leviää automaattisesti
WannaCry	Ei	Leviää automaattisesti

Taulukko 3: Leviämistapa

HermeticWiperin, IsaacWiperin ja CaddyWiperin osalta leviämistavasta ei ole vielä saatu täyttä varmuutta, mutta suurella todennäköisyydellä haittaohjelmat istutettiin kohdeverkkoon aluksi manuaalisesti, minkä jälkeen ne alkoivat levitä autonomisesti verkon sisällä tähän tarkoitukseen varta vasten kehitetyn komponentin avulla [ESET Research 2022]. Kohteiden tarkan valikoinnin ja manuaalisen tartuttamisen puolesta puhuu mm. tartuntojen suhteellisen vähäinen määrä, mikä ei olisi mahdollinen hallitsemattomasti leviävän haittaohjelman tapauksessa. Saman suuntaisiin johtopäätöksiin ovat päätyneet ESET Researchin lisäksi myös mm. CyberArk Laboratorion [2022] tutkijat.

Duqu ei leviä itsestään tai edes monista itse itseään, vaan sitä levitettiin kohteisiinsa kohdistetuin hyökkäyksin nollapäivähaavoittuvuuden sisältävän MS Office tiedoston välityksellä [Bencsáth ja muut 2012a]. Tämä tarkoittanee sitä, että haittaohjelma on todennäköisesti useimmissa tapauksissa välitetty valikoiduille kohteilleen sähköpostin liitetiedostona tai muulla vastaavalla tavalla, Spear Phishing -metodia käyttäen. Spear Phishing eroaa tavallisesta Phishingistä, eli tietojen kalastelusta, sillä että kalasteluyritykset on

kehitetty tarkkaan valikoidulle joukolle ja ne ovat pääsääntöisesti huomattavasti laadukkaampia, ja siten myös vaarallisempia perinteisiin kalasteluyrityksiin verrattuna. Aikoinaan Duqun levitessä ei sähköpostien liitetiedostoihin vielä yleisestikään suhtauduttu läheskään niin vainoharhaisesti kuin nykyään, minkä lisäksi onnistunut hyökkäys vaati vain sen, että edes yksi henkilö kohdeorganisaatiossa avaa lähetetyn liitteen. Tämä on tehnyt Duqusta erittäin tehokkaasti levitettävän ja vaikeasti torjuttavan uhan.

Sama kaava pätee myös Duqu 2.0:aan, jonka tapauksessa tartunnat tapahtuivat Kaspersky Lab:n tutkimustiimin [2015] mukaan todennäköisesti niin ikään Spear Phishingillä nollapäivähaavoittuvuutta (CVE-2014-4148) hyväksikäyttäen. Varsinaisen tartunnan jälkeen he totesivat Duqu 2.0:n liikkuvan verkossa lateraalisesti hyväksikäyttäen toista nollapäivähaavoittuvuutta (CVE-2014-6324), joka mahdollisti tavalliselle käyttäjälle käyttöoikeuksien nostattamisen domain-pääkäyttäjän (*domain administrator*) tasolle.

Flamen kohdalla alkuperäistä tartuntavektoria ei koskaan pystytty luotettavasti selvittämään, mutta saastutettuaan ensimmäisen laitteen verkossa Bencásath ja muut [2012c] osoittivat sen leviävän eteenpäin kuten monet muutkin edistyneet haittaohjelmat nollapäivähaavoittuvuuksia hyväksikäyttäen. He totesivat myös Flamen jopa jakavan kaksi näistä nollapäivähaavoittuvuuksista Stuxnetin kanssa. Flamella oli nollapäivähaavoittuvuuksien lisäksi omintakeinen keino leviämiseen verkon sisällä: Se kykeni esiintymään verkon muille laitteille Microsoft Windowsin päivityksiä jakavana palvelimena, jolta muut laitteet sitten kävivät näitä päivityksiä lataamassa – saaden luonnollisesti päivityksen asemasta tartunnan Flamesta. Haittaohjelman tekijät onnistuivat tässä hyväksikäyttämällä MD5-tiivistealgoritmin heikkouksia ja väärentämällä allekirjoitusavaimen tiivisteen käyttäen tarkoin valikoitua törmäyshyökkäystä. Tiivisteellä taas onnistuttiin huijaamaan Microsoftin automaattisesta prosessista sovelluspäivitysten allekirjoittamiseen vaadittava avain [Bencásath ja muut 2012c].

NotPetya on poikkeus useisiin muihin kyberaseisiin verrattuna siksi, että se ei hyödyntänyt leviämisessään nollapäivähaavoittuvuuksia, vaan onnistui sen sijaan saamaan jalansijan organisaatioissa saastuneen kolmannen osapuolen sovelluksen toimittamien ohjelmistopäivitysten avulla. Organisaation sisällä se levisi tehokkaasti laitteelta laitteelle hyväksikäyttäen paitsi NSA:lta julkiseen verkkoon karannutta EternalBlueta ja EternalRomancea, myös keräämällä jo saastuneilta laitteilta käyttäjätunnuksia ja salasanoja Mimikaz-ohjelmiston avulla. Näillä kerätyillä kirjautumistiedoilla ohjelma kykeni leviämään myös sellaisille laitteille, jotka eivät olleet haavoittuvaisia aiemmin mainituille tietoturva-aukolle. [Sai ja Kumar 2019; Krasznay 2020]

Kaupallista Pegasusta levitettiin alun perin haitallisten linkkien välityksellä. Sovellusta kehittävä yritys on kuitenkin aktiivisesti päivittänyt sovelluksen levittämistapoja aina kulloinkin saatavilla olevien haavoittuvuuksien avulla. Vuosien varrella sovellus on hyväksikäyttänyt mm. iPhoneissa ollutta haavoittuvuutta, mikä mahdollisti

kohdepuhelimen haltuun saamisen pelkän viestin lähettämisellä. Vastaavasti sovellus on myös käyttänyt WhatsAppissa ollutta haavoittuvuutta, jolla hyökkääjä sai kohdelaitteen haltuunsa soittamalla uhrilleen puhelun. Joka tapauksessa sovellusta on koko sen elinkaaren ajan tartutettu vain yksittäin ja tarkoin valikoituihin kohteisiin. Minkäänlaisesta automatisoidusta leviämisestä edes organisaatioiden sisällä ei ole viitteitä. [Agrawal ja muut 2022]

Snaken osalta tarkkaa leviämistapaa ei ole vielä tätä tekstiä kirjoittaessa julkaistu. Joka tapauksessa saastutettuaan ensimmäisen laitteen verkossa, kykenee Snake levittämään itse itseään verkon sisällä. Tähän Snake käyttää ainakin yleisesti tiedossa olevia menetelmiä, kuten vakiosalasanojen arvaamista tai heikkojen salasanojen murtamista. Snaken tartuttamat kohteet on joka tapauksessa valikoitu tarkkaan, eikä se leviä autonomisesti kohdeverkkojen ulkopuolelle. Nollapäivähaavoittuvuuksien osalta Snakesta ei ole luotettavaa tietoa saatavilla, joten taulukkoon merkitään ”ei tietoa”. Lienee kuitenkin kohtuullista olettaa, että myös nollapäivähaavoittuvuuksia on Snaken 20-vuotisen elinkaaren aikana ainakin jossain määrin käytetty hyväksi. Jäämme mielenkiinnolla odottamaan tästä mahdollisesti saatavia lisätietoja, jotta pääsemme vertaamaan Snaken kyvykkyyksiä Duquun ja Flameen myös nollapäivähaavoittuvuuksien osalta. [CISA and Partners 2023]

Stuxnetin leviämistapa oli aikaansa nähden omintakeinen, sillä se käytti liikkumiseensa verkkojen välillä muistitikkuja. Leviämistavan lisäksi Falliere ja muut [2011] havaitsivat Stuxnetissä olevan sisäänrakennetun ”rajoittimen”, jonka tehtävänä oli varmistaa se, että yksi muistitikku tartuttaa maksimissaan kolme uutta laitetta. Käytännössä kolmen tartunnan jälkeen mato poisti itsensä muistitikulta. Tästä rajoittimesta huolimatta Stuxnet levisi valtavalla vauhdilla ympäri maapallon. Vastaavia innovatiivisia leviämistapoja on tavattu mm. Stuxnetia ajallisesti edeltäneen Flamen tapauksessa.

WannaCry ei myöskään NotPetyan tavoin hyödyntänyt leviämisessään nollapäivähaavoittuvuuksia [Akbanov ja muut 2017]. Se levisi silti tehokkaasti ja itsenäisesti jo aiemmin julkistetun EternalBluen avulla, sillä organisaatiot ja järjestelmien ylläpitäjät eivät olleet asentaneet Microsoftin uusimpia tietoturvapäivityksiä. WannaCry:n leviämistä voidaan pitää jopa poikkeuksellisen aggressiivisena, eikä siinä ollut minkäänlaista mekanismia, jolla olisi edes yritetty rajoittaa leviämisnopeutta tai tartutettujen laitteiden määrää.

5.4 Havaitsemisen ja analysoinnin esto

Suurin osa haittaohjelmista pyrkii jollain tavalla hankaloittamaan itsensä havaitsemista ja analysointia. Yleisesti käytettyjä teknologioita on mm. haitallisen tiedoston salaaminen kryptografisin menetelmin, jolloin esimerkiksi antivirusohjelmisto ei pysty suoraan analysoimaan tiedoston sisältöä. Lisäksi haittaohjelma voidaan esimerkiksi pakata erilaisilla polymorfisilla algoritmeilla, joka tekee jokaisesta haittaohjelman instanssista tietyllä tapaa yksilöllisen. Tämä käytännössä estää esimerkiksi tiedoston sormenjäljen vertaamisen

tietokantaan. Haittaohjelman liikennettä voidaan niin ikään koittaa häivyttää esimerkiksi steganografisin menetelmin, piilottamalla komentoliikennettä vaikkapa verkon yli lähetettäviin kuvatiedostoihin. Monet näistä keinoista kuitenkin tekevät haittaohjelman havaitsemisesta vain hankalampaa ja hitaampaa ja kyseessä onkin jatkuva kissa-hiirileikki haittaohjelmien ja niiden havaitsemiseen tarkoitettujen ohjelmien kehittäjien välillä.

Taulukkoon 4 on koottu tietoa haittaohjelmien käyttämistä mekanismeista havaitsemisen ja analysoinnin vaikeuttamiseksi tai estämiseksi. Taulukossa on tietoa esimerkiksi koodin allekirjoituksesta, salausmekanismien käytöstä, sekä mahdollisen itsetuhomekanismin olemassaolosta.

	Koodin allekirjoitus legitiimillä sertifikaatilla	**Viestiliikenteen tai ohjelmiston salaaminen**	**Itsetuhomekanismi tai tappokytkin**
CaddyWiper			
Duqu	x	x	
Duqu 2	x	x	
Flame/Skywiper	x	x	x
HermeticWiper	x		
IsaacWiper			
NotPetya			
Pegasus		x	x
Snake		x	
Stuxnet	x	x	
WannaCry			x

Taulukko 4: Havaitsemisen ja analysoinnin esto

HermeticWiper oli digitaalisesti allekirjoitettu, mutta CaddyWiperin ja IsaacWiperin osalta vastaavasta ei ainakaan toistaiseksi ole löytynyt viitteitä [ESET Research 2022a]. Myös kryptografiaa on todennäköisesti käytetty, mutta tästä ei vielä ole saatavilla luotettavaa ja yksityiskohtaista analyysiä. Näiden ohjelmien osalta tarkempia analyysejä tullaan kuitenkin varmasti vielä tekemään ja tämänhetkiset tiedot voivat vielä muuttua.

Bencsáth ja muut [2012a] tekivät kattavan teknisen analyysin Duqusta. Duqu on levyllä ollessaan lähes kokonaan salattu ja se purkaa itse oman salauksensa ajonaikaisesti siten, että sen moduulit ovat salaamattomina vain kohdelaitteen muistissa. Varsinainen salauksen purku tapahtuu täsmälleen samalla tavalla, kuin Stuxnetinkin tapauksessa. Duqu käyttää myös hyväkseen alkeellista steganografiaa komento ja hallinta (*eng. command & control, tai c&c*) -viestiliikenteessään, jossa varsinainen data on lisätty verkossa

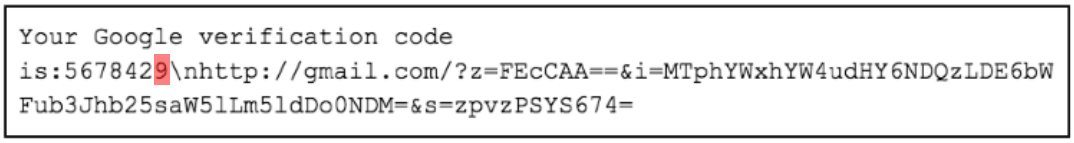
lähetettävän kuvatiedoston perään. Tämän lisäksi tutkijat ovat havainneet yksilöllisiä eroavaisuuksia eri tartuntakohteista saatujen näytteiden välillä. Tämä viittaa siihen, että Duqu on polymorfinen haittaohjelma, jonka havaitsemista on pyritty vaikeuttamaan yksilöimällä kulloisessakin hyökkäyksessä käytettävää haittaohjelmaa. Se, että tekeekö Duqu tämän muokkauksen automaattisesti, ei ole tiedossa. Ottaen kuitenkin huomioon Duqun korkeasti kohdennetun luonteen, voitaneen todennäköisenä vaihtoehtona kuitenkin pitää sitä, että toisistaan eriävät versiot ovat manuaalisesti käännetty ja eroavaisuudet liittyvät joko siihen, että haittaohjelmaa on pyritty kohdentamaan entistä paremmin tiettyyn organisaatioon, tai tietyn tyyppisiin laitteisiin, tai sitten siihen, että itse haittaohjelmaa on välissä kehitetty eteenpäin. Lisäksi osa Duqun kernel-tason ajureista oli allekirjoitettu luotetulta taiwanilaiselta C-Media -nimiseltä yritykseltä varastetulla, tai muutoin haltuun saadulla allekirjoitusavaimella, mikä johti siihen, että käyttöjärjestelmät pitivät kyseistä koodia lähtökohtaisesti luotettavana, mikä taas vaikeutti havaitsemisen mahdollisuuksia entisestään. Kyseinen sertifikaatti mitätöitiin vasta kuukausia myöhemmin CrySyS laboratorion työntekijöiden jaettua kirjoittamansa raportin.

Duqu 2.0 käytti digitaalisesti allekirjoitetun koodin sijasta nollapäivähaavoittuvuutta, saadakseen kernel-tason oikeudet koodin suorittamiseen. Haittaohjelman havaitsemisen aikoihin sen käyttämä haavoittuvuus toimi lähes kaikissa sen aikaisissa Windows-käyttöjärjestelmän versioissa. Edeltäjänsä tavoin Duqu 2.0 on levyllä salatussa muodossa, ja hyväksikäyttää kuvasteganografiaa kommunikoidessaan komentopalvelintensa kanssa. [Kaspersky Lab 2015]

Flame on niin ikään salattu usealla eri metodilla, joista tosin osa on hyvin yksinkertaisia. Esimerkkinä tästä yksinkertainen xor-operaatio avaimella 0xFF, eli tavulla, jossa kaikki bitit ovat ykkösiä. Vaikka tämän tyyppinen koodin ”sekoittaminen” on saattanut aikoinaan toimia esimerkiksi antivirusohjelmistojen ohittamiseksi, ei se ole tehnyt sitä enää pitkään aikaan. Lisäksi tällaiset hyvin yksinkertaiset tavat salata tietoa ovat helposti havaittavissa, ja salaus purettavissa. Steganografiaa ei Flamen tapauksessa ole havaittu. Kuten suurin osa muistakin haittaohjelmista, oli myös Flamen käyttämä ajurikoodi allekirjoitettu digitaalisesti siten, että käyttöjärjestelmä ei ymmärtänyt estää sen ajoa. [Bencásath ja muut 2012c]

NotPetyassa ei ollut varsinaista itsetuhomekanismia, mutta haittaohjelmaa vastaan oli mahdollista luoda eräänlainen ”rokotus”. NotPetya tarkistaa ennen tietojen salaamista kohdelaitteelta tiedostosijainnin ”c:\windows\perfc”, ja mikäli kyseinen tiedosto löytyy, lopettaa haittaohjelma toimintansa [Kumar ja Sai 2019]. Tämä ei kuitenkaan poistanut haittaohjelman jälkiä laitteista tai verkosta, eikä sitä siten voida pitää yrityksenä estää ohjelman havaitsemista tai analysointia. Kyseinen tapa ei myöskään sopinut käytettäväksi etänä, eikä siten mahdollistanut esimerkiksi haittaohjelman kehittäjille sen leviämisen pysäyttämistä.

Pegasus toimii mobiilisovelluksena hieman poikkeavalla tavalla useimpiin muihin tämän tutkielman kyberaseisiin verrattuna. Ensinnäkin se pyrkii turvaamaan olemassaolonsa roottaamalla kohdelaitteensa ja ottamalla sen täysin haltuunsa. Kun root-tason käyttöoikeudet on saatu, on haittaohjelman mahdollista ohittaa matkapuhelinten perinteisesti tehokkaat virtualisointiin ja hiekkalaatikoihin perustuvat sovellusten väliset suojaukset. Pegasus ei yleensä myöskään lataa kohdelaitteelle varsinaista haittakoodia, vaan hyväksikäyttää laitteelta jo löytyviä sovelluksia. Se esimerkiksi naamioi viestintäänsä komentopalvelinten kanssa siten, että viestintä vaikuttaa täysin tavalliselta monivaiheiseen tunnistautumiseen liittyvältä sms-viestiketjulta. Tosiasiassa lähetetyt sms-viestit sisältävät komentoja haittaohjelmaa varten. Kuvassa 4 näkyy komentopalvelimelta Pegasuksen sisältämään laitteeseen lähetetty viesti, joka on täysin identtinen Googlen monivaiheiseen tunnistukseen liittyvän viestinvaihdon kanssa, mutta tosiasiassa vahvistuskoodin viimeiset numerot antavat Pegasukselle käskyn suorittaa jokin toiminto - kuvan esimerkissä toiminnon numero yhdeksän. Pegasus on myös tehokas poistamaan omat jälkensä, esimerkiksi poistamalla alkuperäisen tartunnan aiheuttaneen tekstiviestin tai puhelun laitteen lokeista ennen kuin laitteen omistaja ehtii edes nähdä mitään tapahtumineen. Pegasus sisältää myös itsetuhotoiminnon, joka pyrkii poistamaan kohdelaitteesta sekä itse haittaohjelman että kaikki sen käytöstä jääneet jäljet. Tämän takia Pegasuksen havaitseminen laitteesta jälkikäteen saattaa olla todella vaikeaa. [Bazaliy ja muut 2016; Agrawal ja muut 2022]



Kuva 4: Komentopalvelimen viesti Pegasus -haittaohjelmalle [Bazaliy ja muut 2016]

Snake käyttää monimuotoista ja kerroksittaista salausta sekä viestiliikenteen salaamiseen, että oman olemassaolonsa peittämiseksi kohdelaitteessa. Snake sisältää myös monikäyttöisen kernel-moduulin, jonka avulla se välttelee esimerkiksi kiinnijäämistä. Vaikka raportissa ei tätä erikseen tarkemmin avata, täytyy moduulin kaikella todennäköisyydellä käyttää näennäisesti vaarattomia ja luotetuilla avaimilla allekirjoitettuja ajureita, sillä omalla allekirjoituksella varustettuja ajureita ei ole enää aikoihin voinut käyttää vähänkään modernimmissa ympäristöissä. Varsinaista tappokytkintä tai itsetuhomekanismia ei Snaken osalta ole raportoitu. [CISA and Partners 2023]

Stuxnet käytti kryptografiaa hyväkseen sekä salatakseen osia itsestään, että kommunikoidessaan komentopalvelinten kanssa. Se, että Stuxnet onnistui pysymään piilossa hyvin pitkän ajan, oli kuitenkin enimmäkseen kiinni siitä, että se ei aiheuttanut saastuttamilleen kohteille minkäänlaista haittaa. Täten kukaan ei osannut epäillä minkään olevan vialla. Ohjelmiston paljastumisella myöhemmin taas ei ollut juurikaan väliä – se oli jo

suorittanut tehtävänsä, eikä sille ollut enää käyttöä. Lisäksi ohjelman kehittäjien on täytynyt olla tietoisia siitä, että ydinvoimaloiden sabotointi aiheuttaa kansainvälisen tutkinnan, mikä kaikella todennäköisyydellä johtaa haittaohjelman löytymiseen ja mm. sen sisältämien nollapäivähaavoittuvuuksien palamiseen. Luonnollisesti myös ajurikoodin allekirjoittamiseen käytetyt sertifikaatit palavat ohjelman löytämisen yhteydessä. [Baezner ja Robin 2017]

WannaCry sisälsi salatun zip-tiedoston, joka puolestaan sisälsi suuren osan ohjelman tarvitsemista resursseista, kuten osoitteet sen hallintapalvelimille. Tiedoston salasana saatiin kuitenkin nopeasti selvitettyä ja sen sisältö tutkittua takaisinmallintamalla haittaohjelman salauksen purusta vastaava osio. Muita havaitsemisen ja analysoinnin estoon käytettäviä menetelmiä ei WannaCrysta löydetty, ja se luottikin leviämisessään puhtaasti nopeuteen ja siihen, että päivittämättömiä kohdejärjestelmiä on riittävästi. Oikeastaan voidaan todeta, että WannaCry:n ei edes tarvinnut yrittää piilottaa itseään tehtävänsä suorittamiseksi. [Akbanov ja muut 2017]

Kunnollinen tappokytkin löytyi vain WannaCrysta ja Flamesta. WannaCry sisälsi etäkäyttöisen tappokytkimen, joka pysäytti sen toiminnan käytännössä välittömästi, mutta ei kuitenkaan saanut haittaohjelmaa tuhoamaan itseänsä eikä siten auttanut sen uhreiksi jo joutuneiden laitteiden salauksen purkamisessa [Akbanov ja muut 2017]. Flamen sisältämä itsetuhokomento sen sijaan pyrki poistamaan koko sovelluksen ja kaikki sen jättämät jäljet järjestelmästä [Bencsáth ja muut 2012b]. Flamen tapauksessa komennon tarkoituksena olikin todennäköisesti tartunnan havaitsemisen vaikeuttaminen, kun taas WannaCryn tapauksessa on selkeästi haluttu tapa pysäyttää ohjelman eteneminen syystä tai toisesta, esimerkiksi sen karatessa käsistä ja uhatessa sen kehittänyttä valtiota.

6 Tulokset ja pohdinta

Tutkielmassa havaittiin selvä yhteys esimerkiksi kyberaseiden tyypin ja alkuperän osalta: tuhoajat tulivat idästä ja vakoojat lännestä. Tätä pohditaan lisää luvussa 6.1. Tutkittaessa aikaa tartunnasta haittaohjelman havaitsemiseen on havaittavissa huolestuttavaa dataa siitä, että tehokkaimmat haittaohjelmat näyttävät suorittavan tehtäväänsä jopa vuosia ilman minkäänlaista havaitsemista. Tätä pohditaan tarkemmin luvussa 6.2. Leviämismallin suhteen havaittiin niin ikään selkeä trendi: lähes kaikki kyberaseet ovat kohdistettuja ja niitä käytetään vain hyvin tarkkaan joukkoon ennalta määriteltyjä kohteita. Riskiä aseen ”karkaamisesta” voitaisiin muuten pitää vähäisenä, mutta WannaCry osoitti räjähdysmäisen leviämisen ja massiivisten vahinkojen syntymisen jo korjattuja tietoturva-aukkoja hyväksikäyttäen olevan kuitenkin täysin mahdollista. Leviämismallia pohditaan tarkemmin luvussa 6.3. Havaitsemisen ja havaitsemisen eston osalta tämän tutkielman anti jää hieman laihaksi, sillä lähes kaikki tutkitut ohjelmistot käyttivät hyvin samankaltaisia keinoja havaitsemisen estämiseksi. Tieto siitä, että ohjelman toimintaa pyritään piilottamaan

esimerkiksi liikennettä salaamalla tuskin yllättää ketään. Tätä käsitellään tarkemmin luvussa 6.4.

6.1 Tyyppi ja alkuperä

Heti alkuun havaittavissa oleva mielenkiintoinen seikka liittyy haittaohjelmien alkuperään ja niiden tyyppiin. On selkeästi havaittavissa trendi, jossa länsi tuottaa vakoojia ja itä tuhoajia. Lisäksi edellä mainitut lännen tuottamat vakoojat ovat olleet poikkeuksetta erittäin laadukkaita tuotoksia. Uusimpana tulokkaana myös Venäjältä on saatu kiinni laadukas ja hienostunut vakooja, muta syystä tai toisesta emme kuitenkaan ole nähneet vastaavanlaisia operaatioita esimerkiksi Kiinalta, jossa ainakin perinteisen käsityksen mukaan pitäisi olla myös hyvin kyvykkäitä toimijoita. Syynä tähän voi olla esimerkiksi se, että Kiinalla ei ole ollut intressejä kohdistaa vastaavanlaista tiedustelua länsimaihin, joilla taas olisi kyvykkyys se havaita. Toisaalta Kiinan voisi myös kuvitella omaavan halukkuutta läntisen maailman tiedusteluun esimerkiksi Taiwanin osalta, ja mikäli tällaisiin operaatioihin olisi ryhdytty, tarkoittaisi se sitä, että kyseisiä ohjelmia ei ole vielä saatu kiinni, tai ainakaan tietoa niistä ei ole vuotanut julkisuuteen. Yhtenä vallitsevana teoriana alalla pidetään myös Kiinan huomattavasti hienostuneempaa ja vähemmän tungettelevaa tapaa vakoilla muuta maailmaa suosittujen applikaatioiden ja laajalti käytettyjen kiinalaisvalmisteisten laitteiden avulla. Näistä mainittakoon esimerkiksi viimeisten vuosien aikana massiiviseen suosioon noussut TikTok, jonka on sitä takaisinmallinnettaessa havaittu käyttävän erittäin hienostuneita tekniikoita sen tarkan toiminnan selvittämisen estämiseksi. Numeroiden valossa TikTokia käyttää yli miljardi ihmistä ympäri maapallon ja arviolta noin puolet koko maailman elektroniikasta on valmistettu joko Kiinassa tai kiinalaisten toimesta.

On toki myös mahdollista, että suurimmalla osalla muista toimijoista ei ole vastaavaa kyvykkyyttä riittävän kehittyneiden vakoojien valmistamiseen. Kiinan osalta tämä on ehkä hieman epätodennäköistä, mutta monen muun toimijan kohdalla täysin mahdollinen vaihtoehto. Onnistuneen vakoojan kehittäminen on kuitenkin kaikin puolin erittäin monimutkainen, kallis sekä laajaa ammattitaitoa vaativa prosessi. Tuhoajien osalta vastaus lienee siinä mielessä selkeä, että niiden käyttöön ei liene ollut juurikaan syytä valtioiden välisten konfliktien ulkopuolella, joten tutkittavaksi saadut tapaukset liittyvät lähes yksinomaan Venäjän ja Ukrainan väliseen konfliktiin. Mielenkiintoisena yksityiskohtana emme ole konfliktin aikana vielä nähneet Venäjään kohdistettuja tuhoaja, vaikka Ukrainalla ja sen liittolaisilla varmasti olisi kyvykkyyttä tällaisia valmistaa. Onko niin, että sotaan ei varauduttu ja nyt tuhoajia ei olekaan hyllyssä valmiina, koska kaikki kehitysresurssit on käytetty vakoojiin ja tiedusteluun?

6.2 Aika tartunnasta havaitsemiseen

Haittaohjelmien havaitsemisen suhteen mielenkiintoa herättää erityisesti USA:n ja Israelin yhteisoperaation tuotoksien Duqun, Duqu 2.0:n, Flamen ja Stuxnetin toiminta. Flamen on vahvistettu olleen toiminnassa yli viisi vuotta ennen havaitsemistaan ja ottaen huomioon Duqun ja erityisesti Duqu 2.0:n kehittyneisyyden, on helppo uskoa näidenkin olleen käytössä huomattavasti pidempään, kuin mitä on saatu todennettua. On hyvin mahdollista, että kyseessä on yhdestä ja samasta koodipohjasta rakennettu haittaohjelmaperhe, josta julkistetaan säännölliseen tahtiin uusia versioita jatkamaan aikaisempien versioiden tehtävää. On myös oletettavaa, että vastaavia operaatioita on kohdennettu myös muihin kyseisen liittouman vihollisiin – esimerkiksi Venäjälle. Tätä päätelmää tukee myös tuoreeltaan havaittu Snake, jolla Venäjä on vuorostaan vakoillut läntisen liittouman jäseniä jo lähes 20 vuotta. Vaikka Snaken tapauksessa kyse on selkeästi yhdestä ja samasta jatkuvan kehityksen alaisesta ohjelmistosta on trendi silti sama, eli erittäin pitkäkestoinen tiedusteluoperaatio tarkoin valikoituihin kohteisiin. Kun mietitään esimerkiksi tässä tutkielmassa esiteltyjen toimijoiden haittaohjelmien kehitykseen käytettävissä olevia resursseja ja asiantuntemuksen määrää, tai yksinkertaisesti niiden jo paljastuneiden haittaohjelmien hyväksikäyttämien nollapäivähaavoittuvuuksien lukumäärää, tulee väkisinkin mieleen ajatus siitä, että kuinka paljon vastaavia ohjelmistoja on tälläkin hetkellä liikkeessä ilman, että niitä on havaittu? On hyvin mahdollista ja ehkä jopa todennäköistä, että vastaavilla kyvykkyyksillä varustettuja haittaohjelmia on tälläkin hetkellä vakoilemassa vähintään Venäjällä ja Kiinassa. Ja kuka tietää, että millainen kompetenssi esimerkiksi Kiinalla on. Nyt olemme saaneet analysoitavaksemme vasta USA:n ja Venäjän tuottamia ohjelmistoja.

6.3 Leviämismalli

Leviämismallin osalta selkeä trendi on havaittavissa: Lähes kaikki tutkimuksessa mukana olleet kyberaseet toimitetaan kohteeseensa manuaalisesti, jonka jälkeen ne leviävät autonomisesti kohdeverkon sisällä yleensä nollapäivähaavoittuvuuksien avulla. Todennäköinen syy manuaaliselle tartuttamiselle löytynee tarpeesta pysytellä piilossa mahdollisimman pitkään. Stuxnetin tavoin läpi maailman kohteeseensa matkaava haittaohjelma olisi todennäköisesti helppo havaita jo hyvissä ajoin nykyisten tietoturvaratkaisujen ansioista, ja vähänkään heikommilla resursseilla valmisteltu haittaohjelma tuskin pääsisi edes niinkään pitkälle. Tämän lisäksi haittaohjelman havaitseminen lähtökohtaisesti myös ”polttaa” sen hyväksikäyttämät nollapäivähaavoittuvuudet, mikä tekee haittaohjelman löytämisestä erittäin vahingollisen sitä operoineelle taholle, sillä nollapäivähaavoittuvuudet laajalti käytössä oleviin järjestelmiin ovat pääsääntöisesti paitsi harvinaisia myös erittäin arvokkaita. Kohdennetuilla hyökkäyksillä ja manuaalisella tartuttamisella saadaan todennäköisesti useissa tapauksissa annettua haittaohjelmalle huomattavasti enemmän elinikää ja aikaa suorittaa tehtävänsä. Automaattinen leviäminen tartutetun verkon sisällä taas

kuulostaa hyvinkin järkeenkäyvältä, sillä esimerkiksi keihäskalastamalla perille toimitettua haittaohjelmaa tuskin avataan sen lopullisella kohdelaitteella. Ohjelman on siis erittäin tärkeää kyetä suorittamaan lateraalista liikettä verkon sisällä mahdollisimman tehokkaasti. Ajatus siitä, että aseiden käyttäjät haluaisivat jotenkin vähentää sivullisille aiheutuvaa haittaa ei vaikuta todennäköiseltä skenaariolta, kun ajatellaan esimerkiksi Venäjän Ukrainaa vastaan käyttämien tuhoajien tilannetta. Koska vieläkin isommista vahingoista olisi ollut vain ja ainoastaan hyötyä hyökkääjälle, jää haittaohjelman leviämisen rajoittamiselle käytännössä ainoana kelvollisena vaihtoehtona edellä mainittu havaitsemisen hankaloittaminen.

6.4 Havaitseminen ja analysoinnin esto

Vähemmän yllättäen iso osa tutkituista ohjelmistoista käytti kryptografiaa hyväkseen toimintansa piilottamisessa salaamalla joko viestiliikennettä ja/tai osia itsestään. Ehkä hieman yllättävänä voidaan todeta heikkojen algoritmien, kuten rc4:n käyttö. Toisaalta voidaan myös ajatella kryptografian olevan tarkoitettu lähinnä automaattisia analysointityökaluja vastaan, jolloin manuaalinen takaisinmallinnus kuukausia tai vuosia myöhemmin ei enää vaikuta ohjelman alkuperäisten tavoitteiden saavuttamiseen.

Vastaavasti varastetulla sertifikaatilla allekirjoitettujen ajureiden käyttö laitteiden ja käyttöjärjestelmien sisäisten suojausten ohittamiseksi on myös hyvin yleinen ja yleisesti tiedossa oleva toimenpide, joskin sen hyväksikäyttö näyttää liittyvän vahvasti haittaohjelmalla tavoiteltuun vaikutukseen. Osassa esimerkkejä haittaohjelma olisi myös selvästi tällaisesta hyötynyt, mutta syystä tai toisesta sertifikaatteja ei kuitenkaan ollut käytössä. Syynä saattaa olla esimerkiksi se, että luotetun sertifikaatin hankkiminen on pitkäkestoinen ja kallis prosessi, jota ei yksinkertaisesti ole aikaa odotella esimerkiksi sodan ollessa käynnissä.

Huomionarvoista, joskin myös järkeenkäypää lienee se, että vakoojien kohdalla on nähty huomattavasti enemmän vaivaa havaitsemisen hankaloittamiseen, kun taas tuhoajien kohdalla ei tosiaan aina ole vaivauduttu edes hankkimaan koodin allekirjoittamiseen soveltuvaa sertifikaattia. Luonnollisesti tämä johtunee siitä, että tuhoaja suorittaa tehtävänsä nopeasti, kun taas vakoojan on tarkoitus lymyillä kohdelaitteessa mahdollisimman pitkään.

7 Loppupäätelmät

Pelkästään jo tässä tutkielmassa esitettyjen seikkojen perusteella voidaan todeta suurilla valtiollisilla toimijoilla olevan sellaiset resurssit, että pienempien tai kehittymättömämpien kohteiden on hyvin vaikeaa, ellei jopa mahdotonta puolustautua tällaisten toimijoiden suorittamia kyberoperaatiota vastaan. Oman osansa yhtälöön tuovat myös kaupalliset toimijat, kuten aikaisemmin mainittu NSO-Group, jotka tuottavat parhaimmillaan hyvinkin laajalle joukolle saatavissa olevia kaupallisia kyberaseita, jotka eivät juuri

tiedustelupalveluiden itse kehittämille haittaohjelmille kalpene. Yksityiset yritykset muuttavat kenttää siten, että käsiksi huipputeknologiaan pääsevät myös sellaiset toimijat, joilla ei omasta takaa ole riittävästi resursseja tai asiantuntevuutta tehokkaiden kyberaseiden kehittämiseen. Mielenkiintoista on myös esimerkiksi aiemmin kybersodankäynnin suurvaltana pidetyn Venäjän selkeä alisuoriutuminen kyberrintamalla Ukrainaa vastaan. Esimerkiksi Cederberg [2023] toteaa Venäjän kybermiekan olevan tylsä. Toisaalta Maschmeyer [2022] toteaa kyberoperaatioiden ylipäätään olevan vielä kaukana oikeasta sodankäynnistä. Oli miten oli, Venäjä ei ole saavuttanut mittavia voittoja kyberrintamalla, eikä myöskään tämän tutkielman piirissä ole päästy tutkimaan kovinkaan kehittyneitä itäisen liittouman kehittämiä haittaohjelmia – Snake pois lukien. On myös mahdollista, että itäisten valtioiden kompetenssi kybersodankäynnin suhteen on ollut liioiteltua, ja että ne eivät pääse käsiksi kaikkein kehittyneimpiin ohjelmistoihin edes kaupallisten toimijoiden avulla.

Ainakin sekä Duqun että Flamen osalta todettiin, että molemmat haittaohjelmat jättivät laitteistoon sellaisia jälkiä, jotka olisi myös manuaalisesti voitu havaita ammattitaitoisen järjestelmäasiantuntijan toimesta, ja että nykyaikaisilla tietoturvaratkaisuilla haittaohjelmat olisivat todennäköisesti löytyneet nollapäivähaavoittuvuuksista huolimatta. Kenties paras mahdollisuus puolustautumiseen onkin käyttää monikansallisten tietoturvayhtiöiden palveluita, sillä ainakaan toistaiseksi ei ole viitteitä siitä, että yritykset tai niiden tuotteet esimerkiksi jättäisivät tarkoituksella tiettyjen toimijoiden haittaohjelmat havaitsematta. Oikeastaan päinvastoin, sillä esimerkiksi Microsoftin Defender Security Research Team on julkaissut hyvin yksityiskohtaisen teknisen artikkelin FinFisher -nimisen, Pegasuksen tapaisen valtiollisten toimijoiden käyttämän kaupallisen vakoiluohjelman havaitsemisesta ja analysoinnista [Microsoft Defender Security Research Team & Office 365 Threat Research Team 2018]. Lisäksi esimerkiksi USA:n valtio on joutunut käymään oikeutta teknologiayrityksiä vastaan yrittäessään saada auki matkapuhelinten salauksia [”FBI – Apple encryption dispute” 2023]. Tällaisten takaovien luominen järjestelmiin olisi käytännössä myös hyvin vaikeaa, sillä tuotekehityksessä asian havaitsevien henkilöiden lukumäärä olisi todennäköisesti kovin suuri, mikä vaikeuttaisi asian pitämistä salaisuutena. Todennäköisesti ennemmin tai myöhemmin tällainen toiminta paljastuisi esimerkiksi huonoissa väleissä irtisanotun työntekijän tai tavallisen tietomurron seurauksena. Lisäksi on olemassa lukuisia esimerkkejä ja tutkimuksia esimerkiksi koneoppimisen ja muiden modernien teknologioiden käytöstä entuudestaan tuntemattomien ja muuten edistyneiden haittaohjelmien toiminnan havaitsemisessa jo hyvin varhaisessa vaiheessa [Kumar ja muut 2022; Carrier ja muut 2022]. Vaikka se ehkä hieman ristiriitaiselta kuulostaakin, niin monikansallisten yritysten tarjoamat modernit tietoturvaratkaisut ovat kaikella todennäköisyydellä paras puolustus ennalta tuntemattomien haittaohjelmien torjunnassa.

Vielä lopuksi on todettava, että moni tavalliselle käyttäjälle kaikkein haitallisimmista ja vakavimmista haittaohjelma-aalloista olisi voitu estää sillä, että organisaatiot ja niiden tietojärjestelmistä vastuussa olevat tahot asentaisivat järjestelmä- ja sovellustoimittajien julkaisemat tietoturvapäivitykset välittömästi niiden julkaisun jälkeen. Tätä voidaan perustella esimerkiksi sillä, että nollapäivähaavoittuvuuksia hyväksikäyttävät haittaohjelmat havaitaan nopeasti niiden levitessä suuren yleisön keskuuteen ja yleisesti ottaen korjaavat päivitykset julkaistaan hyvin nopealla tahdilla. Käytännössä siis maailmanlaajuisen katastrofin aiheuttavan haittaohjelman tulee vähintään osittain nojata siihen tosiasiaan, että kaikki eivät näitä päivityksiä ajallansa asenna. Erityisen tärkeää tämä on organisaatioille ja kriittiselle infrastruktuurille, joiden järjestelmien saastuminen aiheuttaa pahimmillaan fyysisiä vaaratilanteita ja kuolonuhreja. Samaan hengenvetoon täytyy myös muistaa, että ainakin läntisellä rintamalla tuntuu olevan käytössään myös sellaisia nollapäivähaavoittuvuuksia sisältäviä kohdennettuun hyökkäykseen tarkoitettuja haittaohjelmia, joilta suojautuminen perinteisin keinoin on lähes mahdotonta. Tämän tiedon valossa korkean riskin ympäristöjen ainoa täysin toimiva suojakeino on fyysinen eristys julkisesta internetistä. Sekään ei tosin Stuxnetin tapauksessa riittänyt, ja siitäkin on jo yli vuosikymmen aikaa.

Kerrotaan, että USA:n asevoimilla oli internetin alkuaikoihin nappula, jonka painaminen räjäytti kaapelin, joka yhdisti armeijan sen aikaisen verkon julkiseen internettiin. Aikoinaan asialle naurettiin, mutta nykytiedon valossa kyseinen ratkaisu ei ehkä sittenkään ollut liioittelua.

Lähdeluettelo

Agrawal, M., Varshney, G., Saumya, K. P. S., & Verma, M. 2022. Pegasus: Zero-Click spyware attack–its countermeasures and challenges.

Akbanov, M., Vassilakis, V. G., Moscholios, I. D., & Logothetis, M. D. 2018. Static and dynamic analysis of WannaCry ransomware. *In Proc. IEICE Inform. and Commun*. Technol. Forum ICTF 2018.

Baezner, M., & Robin, P. 2017. Stuxnet (No. 4). ETH Zurich.

Bazaliy, M., Hardy, S., Flossman, M., Edwards, K., Blaich, A., & Murray, M. 2016. Technical Analysis of Pegasus Spyware. *An Investigation Into Highly Sophisticated Espionage Software.* Viitattu: 02.04.2023. *https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf*

Bencsáth, B., Ács-Kurucz, G., Molnár, G., Vaspöri, G., Buttyán, L., & Kamarás, R. 2015. *Duqu 2.0: A comparison to Duqu*. CrySyS Lab Technical Report, Budapest University of Technology and Economics, Department of Telecommunications.

Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M. 2011. *Duqu: A Stuxnet-like malware found in the wild*. CrySyS Lab Technical Report, Budapest University of Technology and Economics, Department of Telecommunications.

Bencsáth, B., Pék, G., Buttyán, L. & Felegyhazi, M. 2012a. Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*.

Bencsáth, B., Pék, G., Buttyán, L. & Felegyhazi, M. 2012b. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. CrySyS Lab Technical Report, Budapest University of Technology and Economics, Department of Telecommunications.

Bencásath, B., Pék, G., Buttyán. L. & Félegyházi, M. 2012c. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet,* 4(4), 971-1003.

Bosland, M. 2022. Technical Analysis of New CaddyWiper Malware discovered in Ukraine. Mike Bosland's Blog. Viitattu 30.1.2023. *https://mikebosland.com/technical-analysis-of-new-caddywiper-malware/*

Carrier, T., Victor, P., Tekeoglu, A., & Lashkari, A. H. 2022. Detecting Obfuscated Malware using Memory Feature Engineering. In *ICISSP*, p. 177-188.

Cederberg, A. 2023. The Cyber War in Ukraine. In *Cyberwatch Finland magazine,* 1/23, p. 3-5.

Chien, E., OMurchu, L. & Falliere, N. 2012. W32.Duqu: The Precursor to the Next Stuxnet. In: *5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 12)*.

CISA and Partners. 2023. *Joint Cybersecurity Advisory: Hunting Russia Intelligence "Snake" Malware.* Product ID: AA23-129A.

CrySyS Lab. 2022. In *Wikipedia*. Viitattu 29.03.2023. *https://en.wikipedia.org/wiki/CrySyS_Lab*

CrySyS Lab Homepage. 2023. *CrySyS Lab Homepage*. Viitattu 29.03.2023. *https://crysys.hu/*

CyberArk. 2023. In Wikipedia. Viitattu 29.03.2023. *https://en.wikipedia.org/wiki/CyberArk*

CyberArk Labs. 2022. HermeticWiper: What We Know About New Malware Targeting Ukrainian Infrastructure (Thus Far). Viitattu 5.1.2023. *https://www.cyberark.com/resources/blog/hermeticwiper-what-we-know-about-new-malware-targeting-ukrainian-infrastructure-thus-far*

CyberArk Labs Homepage. 2023. *CyberArk Labs Homepage.* Viitattu: 29.03.2023. *https://labs.cyberark.com/*

De León, R. 2020. 50% of U.S. tech execs say state-sponsored cyber warfare their biggest threat: CNBC survey. *CNBC*. Viitattu: 02.04.2023. *https://www.cnbc.com/2020*

/12/17/50percent-of-tech-execs-say-cyber-warfare-biggest-threat-cnbc-survey.html

Ducheine, P. A., Pijpers, P. B., & Arnold, K. L. 2022. The 'Next' War Should Have Been Fought in Cyberspace, Right? An Analysis of Cyber-Activities in the 2022 Russo-Ukraine War. Amsterdam Law School Research Paper, (47).

ESET Research. 2022a. Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper. Viitattu 23.01.2023. *https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/*

ESET Research. 2022b. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. Viitattu 10.2.2023. *https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/*

ESET. 2023. In *Wikipedia*. Viitattu 29.03.2023. *https://en.wikipedia.org/wiki/ESET*

ESET Homepage. 2023. *Threat and Software Vulnerabilities Research*. Viitattu 29.03.2023. *https://www.eset.com/uk/research/*

Falliere, N., Murchu, L. & Chien, E. 2011. W32.Stuxnet Dossier. White paper, Symantec corp., security response, version 1.4.

FBI – Apple encryption dispute. 2023. In *Wikipedia*. Viitattu. 01.04.2023. *https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute*

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

Guerrero-Saade, J. A. 2022. Sentinel Labs: HermeticWiper New Destructive Malware Used In Cyber Attacks on Ukraine. Viitattu 1.2.2023. *https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/*

Intelligence and Security Committee of Parliament. 2020. *Russia.* ISBN 978-1-5286-1686-7.

Jeppsson, A. 2017. How East Germany fabricated the myth of HIV being man-made. *Journal of the International Association of Providers of AIDS Care (JIAPAC),* 16(6), p. 519-522.

Kamiński, M. A. 2020. Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. Security and Defence Quarterly, 29(2), p. 63-71.

Kaplan, Fred. 2017. *Dark Territory: The Secret History of Cyber War.* Simon & Schuster.

Kaspersky Lab. 2023. In *Wikipedia*. Viitattu 29.03.2023. *https://en.wikipedia.org/wiki/Kaspersky_Lab*

Kaspersky Lab. 2015. *The Duqu 2.0: Technical Details.*

Kaspersky Lab Homepage. 2023. Caspersky Cyber Security Solutions for Home and Business. Viitattu 29.03.2023. https://www.kaspersky.com/

Kerttunen, M. 2018. Cyber warfare–from science fiction to reality. *Sicherheit und Frieden (S+ F) / Security and Peace*, *36*(1), p. 27-33.

Kumar, S., Mishra, D., Panda, B., & Shukla, S. K. 2021. DeepDetect: A Practical On-device Android Malware Detector. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*, p. 40-51). IEEE.

Krasznay, C. 2020. Case study: The NotPetya campaign. Információés kiberbiztonság, 485-499.

Maathuis, C., Pieters, W. & Van Den Berg, J. Cyber weapons: a profiling framework. *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 2016, p. 1-8, doi: 10.1109/CYCONUS.2016.7836621.

Malwarebytes Labs. 2022a. Double Header: IsaacWiper and CaddyWiper. Malwarebytes Labs Blog. Viitattu 30.1.2023. *https://www.malwarebytes.com/blog/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper*

Malwarebytes Labs. 2022b. HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine. Viitattu 30.1.2023. *https://www.malwarebytes.com/blog/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine*

MalwareBytes. 2023. In *Wikipedia*. Viitattu 29.03.2023. *https://en.wikipedia.org/wiki/Malwarebytes*

Malwarebytes Homepage. 2023. *Malwarebytes Cyber Security for Home & Business*. Viitattu 29.03.2023. *https://www.malwarebytes.com/*

Maschmeyer, L., & Dunn Cavelty, M. 2022. Goodbye Cyberwar: Ukraine as Reality Check. *CSS Policy Perspectives*, *10*(3).

Microsoft Defender Security Research Team & Office 365 Threat Research Team. 2018. *FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines.* Viitattu: 02.04.2023. *https://www.microsoft.com/en-us/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/*

Pegasus (spyware). 2023. In *Wikipedia.* Viitattu: 01.04.2023. *https://en.wikipedia.org/wiki/Pegasus_(spyware)*

Rid, Thomas & McBurney, Peter. 2012. Cyber-Weapons. *The RUSI Journal* 157:1, 6-13, DOI: 10.1080/03071847.2012.664354.

Robinson, M., Jones, K., & Janicke, H. 2015. Cyber warfare: Issues and challenges. *Computers & security*, 49, p. 70-94.

Sai, L. P, & Kumar, P. T. 2019. Reverse Engineering the Behaviour of NotPetya Ransomware. *International Journal of Recent Technology and Engineering (IJRTE).* ISSN: 2277-3878, Volume-7, Issue-6S, March 2019

Stevens, T. 2017. Cyberweapons: an emerging global governance architecture. *Palgrave Communications* 3, 16102.

Szor, P. 2011. Duqu – threat research and analysis. *McAfee Labs.*

Tikkanen, H. 2020. Operaatio infektio - Miten uutisvirus tartutetaan aivoihisi. In: *Tiedetrippi*. Yleisradio. *https://areena.yle.fi/podcastit/1-50471117*

Trautman, L. J., & Ormerod, P. C. 2018. Wannacry, ransomware, and the emerging threat to corporations. Tenn. L. Rev., 86, 503.

Valeriano, B., Roff, H. & Lawson, S. 2016. Dropping the Cyber Bomb? Spectacular Claims and Unremarkable Effects. Council on Foreign Relations. Viitattu 18.10.2022. *http://web.archive.org/web/20210918071758/https://www.cfr.org/blog/dropping-cyber-bomb-spectacular-claims-and-unremarkable-effects*

Waleed A., & Harshini S. 2018. Comprehensive Analysis of WannaCry: Technical Analysis, Reverse Engineering, and Motivation.