Miia Pudas

TAPAUSTUTKIMUS KOLMEN APT-HYÖKKÄYKSEN MAHDOLLISTEN INDIKAATTOREIDEN HAVAITSEMISESTA KYBERUHKATIEDUSTELUN AVULLA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Pudas, Miia
Tapaustutkimus kolmen APT-hyökkäyksen mahdollisten indikaattoreiden havaitsemisesta kyberuhkatiedustelun avulla
Jyväskylä: Jyväskylän yliopisto, 2023, 66 s.
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Tapaustutkimuksena tehdyssä tutkielmassa tarkoituksena on selvittää millaisia mahdollisia indikaattoreita voitaisiin havaita kyberuhkatiedustelun avulla. Tutkimuksessa käytetään kolmen eri APT-ryhmän tekemiä APT-hyökkäyksiä esimerkkeinä ja pyritään keräämään kyberuhkatietoa näihin hyökkäyksiin liittyen. Esimerkkitapauksien osalta sekä pintanetistä että Dark webistä haetaan APT-ryhmien käyttämiä työkaluja ja pohditaan millaista kyberuhkatietoa olisi voinut olla saatavilla APT-ryhmien hyökkäyksien tapahtuessa.

Tutkimusta taustoitetaan esittelemällä keskeisiä käsitteitä, kuten TOR-verkko, mitä kyberuhkatiedustelu tarkoittaa, haittaohjelmat ja miten APT-lyhenne eroaa esimerkiksi tietokoneviruksista. Lisäksi esitellään kirjallisuudessa esiintyviä erilaisia kyberhyökkäysmalleja. Lisäksi kuvaillaan kyberhyökkäyksen havaitsemista ja sen haasteita erityisesti APT-hyökkäyksien osalta.

Tutkimuksen tuloksien osalta esiin nousee useita haasteita sekä tiedonkeruussa että erilaisten APT-esimerkkiryhmien toimintoihin liittyen. Kolmesta eri APT-ryhmistä kaksi oli ollut aktiivisessa toiminnassa ennen valittua esimerkkitapausta, mutta kolmas APT-ryhmä nousi julkisuuteen vasta APT-hyökkäyksensä paljastuttua. Tutkimuksen tarkoitukseen vastattaessa esimerkkitapauksien osalta kyberuhkatiedustelun havaittavissa olevat erilaiset indikaattorit heijastelevat myös tätä. Aktiivisessa toiminnassa olevista APT-ryhmistä löytyi indikaattoreita huomattavasti runsaammin verrattuna APT-ryhmään, jonka toiminta paljastui vasta ryhmän APT-hyökkäyksen tavoitteiden täytyttyä.

Asiasanat: APT, kyberuhkatiedustelu, Indicators of Intelligence

ABSTRACT

Pudas, Miia
Study of Three APT Attacks and the Use of Cyber Threat Intelligence to Find out Indicators of Intelligence related to Those Attacks.
Jyväskylä: University of Jyväskylä, 2023, 66 pp.
Security and Strategic Analysis, Master's Thesis.
Supervisor(s): Lehto, Martti

Three chosen APT attacks are used as examples in this master's thesis. The thesis is case study and the purpose is to study whether there are any indicators of intelligence related to example APT attacks that cyber threat intelligence could find out. Cyber threat intelligence is collected both from surface web and dark net. The main research question asks if there are any signs to be detected while the APT attack is being prepared, while attack is ongoing or only after attack has been completed.

Theoretical background is based on introducing key theoretical concepts, such as TOR network, what is cyber threat intelligence, what is malware and how APT is different from ordinary malware. Different cyber threat models are also introduced and a general cyber-attack model is also explained. IoA, IoB and IoC concepts are mentioned in addition with challenges related to detecting cyber-attacks and especially challenges related to detecting APT attacks.

Thesis had several challenges related to both collecting indicators of intelligence and how different those tactics, tools and procedures were between chosen APT groups. Some of the APT groups had been active for a long time before chosen example APT attack but one of the APT attack groups were detected only after it had completed its mission successfully. The results also indicate this and those example APT groups that had been active for a long time before chosen APT attacks had left indicators of intelligence. On the contrary was the case with the APT group that was detected only after completing its mission.

Keywords: APT, Cyber Threat Intelligence, Indicators of Intelligence

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tutkimus on tapaustutkimus, jossa keskitytään kolmeen eri APT-toimijan hyökkäykseen ja pyritään tutkimaan olisiko kyberuhkatiedustelun avulla voitu saada joitain mahdollisia indikaattoreita APT-ryhmien tulevista hyökkäyksistä. Ensimmäisessä luvussa kuvataan tutkimuksen taustaa, tutkimusongelmia sekä esitellään tutkimuskysymykset ja valittu tutkimusmenetelmä. Luvun aluksi esitellään lyhyt katsaus aikaisempaan tutkimukseen liittyvään aihepiiriin sekä tutkimusongelma tutkimuskysymyksineen ja valittu tutkimusmenetelmä. Tämän jälkeen tutkielman toisessa luvussa esitellään keskeiset käsitteet ja kolmannessa luvussa tutkimuksen kohteena olevat APT-ryhmittymät. Neljännessä luvassa esitellään tutkimuksen toteutus, tutkimustulokset sekä tutkimuksen tulosten arviointi.

1.1 Tausta

Conti, Dargahi & Deghantanha (2018, 1) huomauttavat, että yksi suurimmista haasteista on yksilöiden ja organisaatioiden turvallisuuden sekä yksityisyyden turvaaminen samalla kun erilaisten kyberhyökkäysten määrät sekä vaihtelevuudet lisääntyvät samalla vaikeuttaen tietoturva-analyytikkojen sekä forensiikka-asiantuntijoiden työtä kyberhyökkäyksien tunnistamisessa sekä puolustautumisessa. Siksi kyberuhkatiedustelun rooli on kasvanut ja kyberuhkatiedustelun tarkoituksena on tunnistaa kyberhyökkäyksien tunnusmerkkejä, kerätä tietoa hyökkäyskeinoista sekä vastata havaittuihin hyökkäyksiin (Conti ym. 2018, 2.).

Vaikka useita erilaisia hyökkäysmenetelmiä käytetään kohdennetusti, silti on löydettävissä yhteneväisyyttä siinä kuinka esimerkiksi tulevaa hyökkäystä tiedustellaan ja kuinka hyökkäystoimia toteutetaan kohteissa (Conti ym. 2018, 2). Erityisesti kohdennetut haittaohjelmat ovat nyt ja tulevaisuudessa yhä suurempi uhka, sillä niiden aikainen havaitseminen on vaikeata (Quintero-Bonilla 2020, 1). Havaitsemista vaikeuttaa erilaisten tekniikoiden käyttäminen, joiden tarkoituksena on vaikeuttaa havaitsemista sekä pysyä havaitsemattomissa mahdollisimman pitkään (Quintero-Bonilla 2020, 1). Kohdennettujen haittaohjelmien

eroavaisuudet tavallisiin kyberhyökkäyksiin ovat siis suuria ja Quintero-Bonilla (2020, 1) huomauttaa, että kohdennettujen haittaohjelmahyökkäyksien seuraukset ovat usein huomattavia.

Englanniksi kohdennetuista haittaohjelmista käytetään termiä Advanced Persistent Threat tai lyhennettä APT. Advanced-sanana viittaa hyökkääjien korkeaan osaamiseen erilaisten valittujen menetelmien sekä tekniikoiden osalta sekä kykyyn kehittää kohdetta vastaan muokattuja keinoja. Persistent-sana viittaa siihen, että toiminnalla on tarkasti mietitty tavoite sekä hyökkäystavoitteet. Threat-sana viittaa siihen, että hyökkäys on koordinoitu, motivoitunut sekä hyökkääjällä on resursseja käytettävissään (Quintero-Bonilla 2020, 2).

Shillito (2019, 186) kuvailee dark webbiä salaiseksi ja anonyymiksi paikaksi, jossa esimerkiksi rikolliset myyvät tai ostavat erilaisia laittomia tavaroita tai palveluita. Shillito (2019, 186) myös huomauttaa, että dark webbiä käytetään aika paljon erityisesti tällaisessa tarkoituksessa.

1.2 Aikaisempi tutkimus

Aikaisempia pro graduja on laadittu muutamia Jyväskylän yliopistossa mutta kyberuhkatiedustelusta on pro graduja löydettävissä vähemmän. Jyväskylän yliopiston osalta kybertiedustelusta on kirjoitettu kaksi kandidaatintutkielmaa sekä kahdet Pro gradu–tutkielmat. Lehdon (2020) kandidaatintutkielma keskittyi poliittisesti motivoituneeseen kybervakoiluun ja tiedustelutoimintaan. Katajan (2019) kandidaatintutkielma keskittyi kyberuhkatiedusteluun. Johanssonin (2021) Pro gradu–tutkielma keskittyi Venäjän ja Kiinan sotilastiedusteluorganisaatioiden kybermenetelmien kehitykseen vuosina 2004–2021. Matilainen (2021) keskittyi tutkimaan kyberuhkatiedustelun käyttöä osana organisaatioiden kyberpuolustusta.

APT osalta Jyväskylän yliopistossa on kirjoitettu seitsemän erilaista tutkimusta. Näistä kahdet ovat kandidaatin töitä, neljät pro graduja ja yksi väitöskirja. Joidenkin tutkimuksien osalta aineiston saatavuus on hyvin rajoitettua, sillä tekijät eivät ole antaneet lupaa avoimeen julkaisuun. Kuhalammen (2018) kandidaatin työssä keskitytään APT–uhkiin. Teirivaaran (2017) kandidaatintyö käsittelee tietoturvan ihmiselementtiä sosiaalisen manipuloinnin osalta. APT–uhkia Teirivaaran (2017) työssä käsitellään toteamalla, että sosiaalinen puoli on usein ensimmäinen askel laajassa tietomurtohyökkäyksessä.

Pro graduissa APTtä käsitellään sekä Siukosen (2019) että Särökaaren (2020) Pro graduissa. Siukonen (2019) tutkii miten APT-operaation eri vaiheissa tehdään päätöksiä ja mitkä tekijät vaikuttavat eri vaiheiden taustalla. Tutkimus on kvalitatiivinen tutkimus, jossa tutkimuskysymyksiin vastataan teoriasidonnaisen sisällönanalyysin avulla. Päätutkimuskysymys on kuinka OODA-loopin vaiheet toteutuvat APT-operaation eri vaiheissa ja apukysymykset kysyvät mistä vaiheista APT-operaatiot muodostuvat sekä mitkä ovat OODA-loopin vaiheet. Särökaari (2020) analysoi millaisia tekniikoita, taktiikoita sekä toimenpiteitä käytetään ja mitkä ovat APT–ryhmien osalta ryhmien prosessit kuinka

kohdennettuja hyökkäyksiä toteutetaan. Tutkimus pohjautuu Grounded Theoryyn, joka on yksi laadullisen tutkimuksen menetelmistä.

Bundan (2020) päätutkimuskysymyksenä on tutkia kuinka kohdistetut haittaohjelmahyökkäykset ovat kehittyneet vuosien 2007–2016 aikana ja apukysymyksinä on mitä kohdistetuilla haittaohjelmahyökkäyksillä tarkoitetaan ja mitkä ovat niiden rakenteita. Tutkimusmenetelmänä on tapaustutkimus ja tutkimuksen pääkohteena on APT28–niminen tutkimusryhmä.

Karsikas (2021) tutkii muutamia Kiinaan sekä Venäjään liitettyjä kyberhyökkäysryhmiä ja tutkimuskysymyksenä on tarkastella Kiinaan ja Venäjään liitettyjen kyberhyökkäysryhmien eroavaisuuksia. Lisäksi työssä pyritään selvittämään mitä yhtäläisyyksiä molempiin maihin liitetyissä ryhmissä on sekä käytetyissä työkaluissa, tekniikoissa sekä proseduureissa. Tutkimusmenetelmänä on monitapaustutkimus, joka toteutettiin laadullisena aineistolähtöisenä.

Reshin (2016) väitöskirja korostaa luotetun ja ohuen Hypervisorin osuutta, jolloin vain ennalta hyväksyttyjä komentoja voidaan suorittaa järjestelmässä. Tällainen lähestymistapa toimii myös useimpia APT-hyökkäysvektoreita sekä nollapäivähyökkäyksiä vastaan.

1.3 Tutkimusongelma ja tutkimusmenetelmät

Tutkielman päätutkimuskysymyksenä on tutkia missä vaiheessa Internetistä olisi löydettävissä havaintoja APT-hyökkäyksistä. Päätutkimuskysymyksessä keskeistä on pyrkiä vastaamaan voidaanko jotain merkkejä havaita jo kun hyökkäystä ollaan valmistelemassa, kun hyökkäys on tunkeutumassa kohteeseensa vai vasta silloin, kun hyökkäys on jo ohitse. Päätutkimuskysymystä rajataan keskittymällä kolmeen jo paljastuneeseen APT-hyökkäykseen.

Päätutkimuskysymystä täydennetään apukysymyksillä, joista ensimmäisessä apukysymyksessä pyritään tutkimaan millaisilla internet-alustoilla erilaisia havaintoja hyökkäyksistä olisi löydettävissä. Apukysymyksessä keskeisintä on selvittää voidaanko havaintoja tehdä pintawebissä vai Dark webissä ja millaisilla erilaisilla netin alustoilla, kuten sosiaalisessa mediassa vai blogeissa havaintoja voisi olla. Toisena apukysymyksenä on selvittää onko Dark webistä löydettävissä APT-hyökkäyksiin käytettäviä hyökkäystyökaluja.

Tutkimusmenetelmänä on laadullinen tapaustutkimus, jossa keskitytään valittuihin APT-hyökkäyksiin ja esitetään yleiskuvaus valituista APT-hyökkäyksistä. Lisäksi tuodaan esille millaisia erilaisia Indicators of Intelligence on löydettävissä valituista APT-hyökkäyksistä. Usein tapaustutkimuksen tarkoituksena on tehdä yleistettävissä olevia päätelmiä tai löytää jotain yleistä ihmisten toimintaan vaikuttavia säännönmukaisuuksia.

Laine, Bamberg & Jokinen (2007, 9) huomauttavat, että tapaustutkimus on tutkimustapa tai tutkimusstrategia, jossa voidaan hyödyntää useita erilaisia menetelmiä tai useita erilaisia aineistoja. Tapaustutkimuksessa tutkimukseen kohde on monesti jokin ilmiö tai tapahtumakulku. Tapaustutkimus on myös

perusteellinen ja tarkka kuvaus siitä, mitä tutkitaan ja tarkoituksena on kerätä monipuolinen aineisto ja kuvata kohdetta perusteellisesti (Laine ym. 2007, 9–10.).

Tapaustutkimuksen tehtävänä on valitun tapauksen tekeminen ymmärrettäväksi (Laine ym. 2007, 31). Tapaustutkimus myös usein kysyy mitä valitusta tapauksesta voidaan oppia, mutta tapaustutkimus sopii myös vastaamaan kysymyksiin miten ja miksi. Tapaustutkimuksessa tarkoituksena on kasvattaa ymmärrystä tutkittavasta tapauksesta tai ilmiöstä sekä olosuhteista, joiden myötä lopputulokseksi tuli sellainen kuin tuli (Laine ym. 2007, 10.). Tapaustutkimuksessa tarkoituksena on tuottaa tietoa tietyistä paikkaan tai aikaan liittyvistä ilmiöistä, prosesseista, merkityksistä ja tiedosta (Peltola 2007, 111).

Tapaustutkimuksen osalta sitä on kritisoitu paljon siitä, että voidaanko yksittäisen tapaustutkimuksen tuloksia yleistää koskemaan myös muita samankaltaisia tapahtumia ja mitä tällainen yleistäminen tarkoittaisi. Useat tapaustutkimuksen kriitikot ovat sitä mieltä, että tapaustutkimusten tulokset koskevat vain tutkittua tapahtumaa eikä niillä ole laajempaa tieteellistä arvoa. Tapaustutkimukseen liittyykin kaksi toisiinsa kytkeytyvää jännitettä eli jännite yksittäiseen tapaukseen keskittyvän näkökulman ja yleisen näkökulman välillä sekä jännite empiirisen ja teoreettisen orientaatioiden kesken. Tapaustutkimuksen tutkittava tapausta on kuvattava tarkasti mutta tapaus on myös liitettävä muuhun tutkimukseen sekä aihetta koskevaan teoreettiseen keskusteluun (Peuhkuri 2007, 130.).

Tapaustutkimuksien teoria voi olla joko yleistä teoriaa tai tutkimusteoriaa. (Peuhkuri 2007, 131). Yleisillä teorioilla voidaan tarkoittaa usean tyylisiä teorioita ja Peuhkuri (2007, 131) jatkaa toteamalla, että yleisiä teorioita voidaan jakaa joko universaaleihin tai historiallisesti ehdollisiin teorioihin. Universaalien teorioiden ilmiöiden tai lainalaisuuksien katsotaan pätevän ajasta tai paikasta riippumatta, mikäli tietyt teorian ehdot toteutuvat. Yleisiä universaaleja teorioita ovat ihmisten tai ihmisryhmien toimintaa kuvaavat teoriat. Historiallisesti ehdollisissa teorioissa sen sijaan määritellään tarkasti historialliset ajanjaksot, olosuhteet sekä paikat, joissa teorian katsotaan pätevän. Päivämäärien lisäksi keskeistä on myös kertoa teoriassa millaiset tekijät yhdistävät tällaisia olosuhteita, joissa teorian katsotaan pätevän. Yleiset teoriat ovat tutkimuksissa viitekehyksiä, joiden pohjalta valitaan sopivia käsitteitä sekä rajataan tutkimusta (Peuhkuri 2007, 131–132.).

Tapaustutkimuksen osalta ongelmana on usein tulosten huono yleistettävyys, jota valitussa aiheessa korostaa APT-hyökkäyksien luonne erittäin hyvin valmisteltuina ja kohdennettuina hyökkäyksinä (Paavilainen 2014, 49). Vaarana on erityisesti se, että valitut APT-hyökkäykset eivät olekaan edustavia esimerkkejä tai liian hatarin perustein oletetaan syy-seurausyhteyksiä. Tällöin tutkimuksen tulosten merkitys voi jäädä vähäiseksi ja hyödyntämismahdollisuudet heikoiksi.

2 KESKEISET KÄSITTEET

Luvussa taustoitetaan tutkimusaihetta aloittaen lyhyellä esittelyllä internetistä sekä määritellään Deep ja Dark web. Lisäksi luvussa kuvataan lyhyesti erilaisia haittaohjelmia sekä kuinka APT-hyökkäykset eroavat tavallisista kyberhyökkäyksistä. Lisäksi kuvataan APT-hyökkäyksien havaitsemisen vaikeutta, yleisempiä kyberuhkamalleja sekä yleistä kyberhyökkäysmallia, kybertiedustelua ja kyberuhkatiedustelun tavoitteita sekä kuinka nämä liittyvät APT-hyökkäyksiin.

2.1 Internet

Naughton (2016, 5) huomauttaa, että internet on jo yli neljäkymmentä vuotta vanha. Internetin syntyyn johtanut tutkimus alkoi jo vuonna 1973, mutta kaksi ensimmäistä vuosikymmentä internettiä käyttivät lähinnä tekninen ja akateeminen eliitti sekä huippututkijat (Naughton 2016, 5). 1990–luvun alusta lähtien internet alkoi tulla yhä laajempien käyttäjien käyttöön ja Naughton (2016, 5) jatkaa toteamalla, että internet mielletään nykyään oleelliseksi teknologiaksi, jota ilman nykyiset yhteiskunnat olisivat vaikeuksissa. Brügger, Goggin, Milligan & Schafer (2017, 1) korostavat myös internetin nopeaa kasvua neljässä kymmenessä vuodessa oleelliseksi osaksi arkista viestintää sekä mediaympäristöä ja jokapäiväistä elämää, kulttuuria sekä yhteisöä. Internet myös kehittyy ja esimerkiksi internetin käyttäminen, siihen yhdistetyt laitteet, teknologiat, protokollat sekä sosiaaliset, taloudelliset ja kulttuurilliset tavat ovat jatkuvassa kehityksessä innovaatioiden ja evoluution myötä (Brügger ym. 2017, 2).

Naughtonin (2016, 11) mukaan internetin kehitys voidaan jakaa vaiheisiin, joista ensimmäinen vaihe ajoittuu vuosiin 1983–1995. Noina vuosina internet muuttui sotilaallisesta tai tutkijoiden käytössä olleesta verkosta avoimeksi verkoksi Naughton 2016, 11). Toinen vaihe ajoittuu vuosiin 1995–2000 ja Naughton (2016, 12) kuvailee vaihetta ensimmäiseksi internet-buumiksi, jonka kupla puhkesi maaliskuussa 2000. Vaikka joidenkin mielestä internet-ilmiönä oli täysin

liioiteltua, keskeistä oli se, että asetetut odotukset voivat olla paljon teknistä ja taloudellista todellisuutta edellä ja Naughton (2016, 14–15) huomauttaa, ettei internet ollut teknisesti valmis täyttämään buumin odotuksia.

Internetin kolmatta vaihetta Naughton (2016, 16) kutsuu netti 2.0 termillä ja kolmas vaihe kattaa vuodet 2000–2003. Keskeistä oli erilaisten älykkäiden algoritmien hyödyntäminen esimerkiksi netin sivustojen arviointiin, kuten Googlen PageRank-algoritmi tai wiki-sivustojen ilmestyminen, jolloin internet muuttui yksisuuntaisesta vain luettavasta sisällöstä Tim Berners-Leen mukaan lue ja kirjoita netiksi. Myös yksittäiset ihmiset loivat yhdessä sivustoja ilmaiseksi muiden käyttöön (Naughton 2016, 16.).

Internetin neljännen vaiheen Naughton (2016, 17) kuvailee sisältävän huomattavia muutoksia siihen, kuinka ja millaisilla laitteilla internettiä käytetään. Keskeistä on mobiilien yhteyksien huomattava lisääntyminen eli internettiä käytetään paljon myös matkapuhelimilla tai tableteilla. Myös sosiaalisen median roolin keskeisyys on lisääntynyt, kuten myös erilaisten tahojen internetissä tapahtuva valvonta sekä pienten ja suurten teknologiayritysten vallan ja vaikutusvallan keskittyminen. Myös kyberrikollisuus on lisääntynyt ja mediankäyttäminen on muuttunut sekä internettiä palvelualustanaan käyttävien yrityksien syntyminen, kuten Airbnb tai Uber (Naughton 2016, 17–18.).

Naughton (2016, 18) huomauttaa, että ihmisten käyttäytymistä internetissä seurataan ja erilaisia palveluita sekä järjestelmiä on kehitetty, jotka vakoilevat ihmisiä palveluita tarjotakseen. Naughton (2016, 18) huomauttaa, että yritykset kutsuvat tätä markkinoinniksi ja internetin käyttäjät pitävät palveluista, mutta ovat haluttomia maksamaan niistä. Yritykset toisaalta haluavat kasvaa suuriksi mahdollisimman äkkiä ja tällöin nopeinta on ollut palveluiden tarjoaminen ilmaiseksi, mutta liiketoimintamalliksi muodostui tällöin mainoksien tarjoaminen. Käyttäjistä kerätään tietoa, jota hyödynnetään mainosten kohdentamisessa (Naughton 2016, 18).

Liiketoimintaan liittyvän seuraamisen lisäksi myös valtioiden internetin sekä mobiiliyhteyksien valvonta on lisääntynyt Naughtonin (2016, 19) mukaan viimeisen 15 vuoden aikana. Snowdenin paljastukset vuonna 2013 toivat seurannan laajuuden sekä kattavuuden yleiseen tietoon (Naughton 2016, 19). Myös kyberrikollisuus on lisääntynyt ja Naughton (2016, 20) huomauttaa, että kyberrikollisuus on nykyään oma teollisuuden alansa, jossa varastettua arkaluonteistakin tietoa tai esimerkiksi luottokorttitietoja vaihdetaan piilossa olevissa paikoissa.

2.2 Deep Web ja Dark Net

Internetin alkuaikoina sivustot olivat helposti indeksoitavissa ja käyttäjien oli helppoa vierailla eri sivuilla (Weimann 2016, 195). Erilaisten sivustojen lukumäärän kasvaessa hakukoneet pystyivät löytämään staattiset sivustot, mutta dynaamisten sivustojen suhteen oli vaikeuksia. Staattiset sivustot ovat toisiinsa linkitettyjä, mutta dynaamiset sivustot ovat linkitettyjä tiettyihin nettisivustoihin ja tällaiset voidaan löytää vain täsmällisten hakukysymysten tai

erityisten ohjelmistojen avulla. Vuonna 1994 esiin nousi näkymätön netti termi kuvaamaan tilannetta, jossa kaikkea internetin sisältöä ei pystynytkään saavuttamaan (Weimann 2016, 195.). Vuonna 2001 esiin nousi deep web termi kuvaamaan sisältöä, jota perinteiset hakukoneet eivät löydä tai jonne pääsee vain tiettyjen hakutermistöjen tai hakusanojen avulla tai erilaiset pääsynhallintakeinot rajoittavat sivustoille pääsyä.

Weimann (2016, 195) toteaa deep webin koon olevan lähes mahdotonta määrittää, koska suurin osa sisällöstä on joko piilotettua tai sinne pääsyä rajoitetaan. Erään arvion mukaan deep web on 400–500 kertaa tavallista internettiä suurempi. Deep webin osalta myös sisällön jatkuva dynaamisuuden muutos esimerkiksi miten sisältöä voidaan saavuttaa on muutoksessa ja kasvu on eksponentiaalista (Weimann 2016, 195–196.). Kuvaavaa on toteamus siitä, että Google indeksoi vain 16 prosenttia internetistä eikä mitään deep webistä. Myös yksittäinen haku palauttaa vain 0,03 prosenttia kaikesta internetissä olevasta tietomassasta (Weimann 2016, 196).

Deep webin osalta Bergman vuonna 2001 määritteli sen sisältävän vain organisaation omaan käyttöön tarkoitettuja tietokantoja, joita ulkopuoliset eivät voi käyttää, maksumuurien takana olevaa sisältöä, jonka sisällöstä vain osa on nähtävissä ilman korvausta tai sisältöä, joka luodaan dynaamisesti uusiksi joka kerta kun sivulla vieraillaan (Hatta 2020, 278–279). Myös sivustot, joilla voidaan vierailla vain sivuston oman hakukoneen kautta kuuluvat deep webbiin kuten myös sähköposti ja erilaiset pikaviestimien sisältävät keskustelulogit. Keskeistä deep webin sisällön osalta on se, että sisältöä ei normaalit hakukoneet, kuten Google, pysty löytämään. Bergmanin mukaan myöskään deep web ei ollut näkymätöntä (Hatta 2020, 279.).

Dark net terminä yleistyi yhtä aikaa dark webin kanssa (Hatta 2020, 280). Hattan (2020, 280) mainitsee, että on olemassa hypoteesi siitä, että termiä on käytetty jo 1970-luvulta ja jotkut yhä nykyäänkin käyttävät termiä kuvaamaan IP-osoitteita, joita esimerkiksi tietokoneille ei ole allokoitu. Toisaalta negatiivisemmassa sävyssä vertaisverkkojen tekijänoikeuksia tutkineessa tieteellisessä artikkelissa vuonna 2003 Dark net termiä käytettiin kuvaamaan laittomuuksia, joita vertaisverkoissa tehtiin (Hatta 2020, 280.). Hatta (2020, 281) viittaa Bibble ym. tutkimukseen, jossa dark net määriteltiin tavaksi jakaa digitaalista sisältöä erilaisten verkkojen sekä teknologioiden avulla, kuten CD- tai DVD-levyillä, keskitetyn palvelimen kautta tai vertaisverkkojen, kuten Napsterin tai Gnutellan kautta. Vaikka Gnutella oli täysin hajautettu, yksittäiset vertaisverkon asiakkaat eivät olleet anonyymejä, vaan IP-osoitteet olivat jäljitettävissä ja IP-osoitteiden omistajat pystyttiin saattamaan lailliseen vastuuseen laittoman sisällön jakamisesta (Hatta 2020, 281).

Dark net oli kerännyt huomiota terminä ja samaan aikaan dark net termiä alettiin käyttämään Friend-to-Friend tyylisestä teknologiasta, jonka Freenet toteutti ensimmäisenä. Friend-to-Friend on siis eräs vertaisverkkojen tyyleistä, joissa käyttäjä ottaa yhteyttä vain tuttaviin (Hatta 2020, 282). Useimmiten tuttavat ovat tavanneet fyysisesti ja ovat rakentaneet luottamusta toisiinsa verkon ulkopuolella. Autentikointiin käytetään salasanaa tai digitaalista allekirjoitusta ja

kaikki rakentuu siihen, että Friend-to-Friend on vertaisverkko, joka koostuu toisiinsa luottavista käyttäjistä (Hatta 2020, 282–283.). Hatta (2020, 285) myös korostaa, että Friend-to-Friend tyylisessä verkossa on vaikeata havainnoida koko verkon rakennetta omia tuttavuuksia lukuun ottamatta, koska verkon kokoa voidaan laajentaa ilman, että koko verkon anonymiteetti vaarantuu. Tällöin dark net terminä viittaa juuri tähän, että osa verkossa olevista tahoista jää pimeään (Hatta 2020, 285).

Dark web termin osalta sen tarkkaa alkuperää on vaikeampi tietää ja termi ilmestyi käyttöön ensimmäistä kertaa noin vuonna 2009. Hattan (2020, 285) myös jatkaa painottamalla, että dark web yhä enemmän alkoi sulautumaan deep web termistön kanssa, mutta kuitenkin viittaa eri asioihin kuin deep tai dark net. Weimann (2016, 196) määrittelee dark webin deep webin syvimmäksi kerrokseksi, jonka sisältöä tarkoituksella piilotellaan. Sekä Weimann (2016, 196) että Shillito (2019, 186) korostavat dark webin osalta sisällön laittomuutta. Shilliton (2019, 186) mukaan esimerkiksi rikolliset myyvät tai ostavat laittomia tavaroita tai palveluita ja dark webbiä käytetään erityisesti tällaisessa tarkoituksessa. Myös erilaiset alamaailman ilmiöt toimivat dark webissä, kuten sosiaalisen median rasistit, kryptoanarkistit tai transhumanistit (Weimann 2016, 196). Toisaalta Weimann (2016, 204) huomauttaa, että dark webbiä käytetään myös laillisiin tarkoituksiin. Esimerkiksi journalistit tai kansalais- tai demokratia-aktivistit kiertävät sensuuria ja esimerkiksi maissa, joissa internetiä sensuroidaan voidaan dark webin avulla kiertää sensuuria (Weimann 2016, 204). Kaur & Randhawa (2020, 2155) huomauttavatkin, että anonymiteetti on myös Dark webin suurin etu eivätkä kaikki dark webin käyttäjät ole liikkeellä pahantahtoisesti.

Kaur ym. (2020, 2140–2143) luettelevat yksityiskohtaisemmin useita dark webissä tapahtuvia rikoksia, kuten huumeiden tai ihmisten salakuljettaminen, tietojen vuotaminen, lapsipornografia, valesivustot, jotka näyttävät oikeilta sivustoilta, petokset ja virtuaalivaluuttahuijaukset, aseiden salakuljettaminen, palkkamurhat, kidutukset tai kostoporno. Dark web myös toimii tietoverkkorikoksien alustana ja Kaur ym. (2020, 2146) mainitsevat esimerkkeinä hajautetut palvelunestohyökkäykset, kalastelun, Man-in-the-middle–hyökkäykset, istunnonkaappaukset, SQL-hyökkäykset sekä salasanojen uudelleenkäyttöhyökkäykset. Dark webin osalta keskeistä on piilotettujen palveluiden hyödyntäminen, joiden avulla tällaisia resursseja voidaan käyttää ilman käyttäjän paljastumista. Myös näitä piilotettuja palveluita kohtaan voidaan kohdistaa hyökkäyksiä, joiden tarkoituksena on esimerkiksi paljastaa missä piilotetut palvelut sijaitsevat (Kaur ym. 2020, 2146).

Näiden lisäksi myös erilaisten haittaohjelmien osalta dark webissä tehdään kaupankäyntiä. Esimerkkeinä Kaur ym. (2020, 2019–2020) mainitsevat tietoa varastavat troijalaiset, kiristyshaittaohjelmat, etäkäytettävät RAT-haittaohjelmat, botnet-ohjelmistot sekä pankkiautomaattihaittaohjelmat. Myös terroristijärjestöt sekä heidän kannattajat ja mahdolliset rekrytoitavat hyödyntävät dark webbiä internetin sijasta. Dark web tarjoaa anonymiteettiä sekä piilossa olevan paikan, joka on helposti saatavilla, mutta yleensä sekä näkymätön että saavuttamattomissa (Weimann 2016, 196–197.).

Kaur ym. (2020, 2151) huomauttavat, että Dark webissä tehtävät rikokset voivat vaikuttaa tietoturvallisuuteen ja uhkia yltää sekä kansalliselle että kansainväliselle tasolle. Esimerkkeinä Kaur ym. (2020, 2152) listaavat salaisten tietojen vuotamisen, dark webin hyödyntämisen terroristien aseiden hankintaan sekä nollapäivähaavoittuvuuksien hyödyntämisen.

2.3 TOR-verkko

Bernaschi ym. (2022, 1288) mainitsevat TOR-verkon olevan tunnetuin ja laajimmin käytössä oleva protokolla dark webissä surffaamiseen. Tosin Jardine (2018, 2827) huomauttaa siitä, että vaikka TOR on suosituin, ei se ole ainoa tapa surffata dark webissä. Muita mahdollisia alustoja ovat esimerkiksi I2P, Freenet tai Zeronet (Jardine 2018, 2827). Näistä I2P on toiseksi suurin ja muut ovat huomattavasti pienempiä sekä laajuudeltaan että suosioltaan (Moore & Rid 2016, 15).

TOR on lyhenne the Onion Router sanoista ja TOR-protokollana korostaa yksityisyyttä ja anonymiteettia (Bernaschi ym. 2022, 1288). Käyttäjien osalta TOR koostuu kahdesta eri osasta, joista toinen osa on käytettävä selainohjelma ja toinen osa koostuu Dark webin sivustoista, jotka päättyvät .onion päätteeseen .com tai .fi sijasta (Jardine 2018, 2827). TOR on alkanut yhteistyöprojektina Yhdysvaltojen laivaston tutkimuslaitoksen ja voittoa tavoittelemattoman Free Haven projektin kesken. Tarkoituksena oli luoda käyttäjille hajautettu, anonyymi, helposti käytettävissä oleva ja salattu verkko ja TORia markkinoitiin erityisesti maihin, joissa verkkosensuuri on vahvaa (Moore ym. 2016, 16.).

TOR hyödyntää erilaisia solmuja tai nodeja, joiden kautta liikennettä reititetään ja liikenne reititetään vähintään kolmen tällaisen solmun tai noden kautta. (Jardine 2018, 2827). TOR verkossa jokainen lähetettävä paketti salataan usealla kerroksella, joita puretaan matkan aikana. Esimerkiksi keskimmäinen solmu kolmesta solmusta purkaa yhden kerroksen ja viimeinen solmu, jota kutsutaan poistumissolmuksi, purkaa alkuperäisen paketin ja lähettää sen kohdeosoitteeseen. Tällä tavalla toimimalla TOR-verkon liikenteen sieppaaminen ja purkaminen on huomattavasti vaikeampaa muttei täysin mahdotonta (Moore ym. 2016, 16–17.).

Owen & Savage (2016, 113) kuvaavat TOR-verkon toimintaa yksityiskohtaisesti ja vuonna 2014 TOR-verkossa oli 8000 erilaista solmua. Jokaiselle solmulle voidaan asettaa erilaisia lippuja esimerkiksi kuvaamaan niiden toimintaa. Esimerkiksi TOR-verkon ulostulosolmulle on oma lippu, joka tarkoittaa sitä, että ulostulosolmusta liikennettä ohjataan normaaliin internettiin. Mikäli solmulle on asetettu niin sanottu vartijalippu, voi solmu toimia ensimmäisenä nodena, kun liikennettä muodostetaan (Owen ym. 2016, 113.).

TOR-verkon osalta käytetään enintään kolmea solmua, joista ensimmäiseksi valitaan jokin vartijalipun sisältävistä solmuista. Owen ym. (2016, 113) kuvaavat tällaista solmujoukkoa Rguard-joukoksi. Viimeinen ulostulosolmu valitaan vastaavasti Rexit-solmuista, jotka sisältävät ulostulosolmun lipun. TOR-verkon osalta solmuja ei valita satunnaisesti, vaan jokainen solmu ilmoittaa

oman kaistansa, joita muut solmut verifioivat. Vartijasolmua käytetään pitkän aikaa, jotta todennäköisyys käyttää vihamielisen tahon hallussa olevaa solmua pienenisi. Mikäli toimittaisiin päinvastoin, vihamielisen tahon olisi mahdollista hankkia itselleen useita solmuja ja kasvattaa tällöin todennäköisyyttä sille, että hän voisi puuttua liikenteeseen (Owen ym. 2016, 113.).

TOR-verkossa useat käyttäjät myös hyödyntävät samoja solmuja, jolloin yksittäisten pakettien seuraaminen on vaikeata. Toisaalta pahimmassa tapauksessa, jossa vihamielisellä taholla on hallussaan sekä ensimmäinen että viimeinen solmu, voidaan turvautua pakettien korrelointiin ja pienentää käyttäjän anonymiteettiä. TOR-verkossa käytettävä palvelu näkee vain viimeisen solmun IP-osoitteen, joka on ulostulosolmun IP-osoite (Owen ym. 2016, 113.).

Vuonna 2016 TOR-verkolla arvioitiin olevan noin kaksi miljoonaa päivittäistä käyttäjää. Lisäksi jopa 96,6 prosenttia käyttäjistä käyttivät pintanettiä eivätkä dark webbiä. Tällaisen käytön taustalla voi olla halu suojata käyttäjiensä yksityisyyttä ja anonymiteettiä (Jardine 2018, 2828.). Tor-verkon osalta sen anonymiteettiä on ylistetty ja esimerkiksi Google ja EFF ovat edistäneet TOR-verkon käyttöä tukahduttavien hallintojen kiertämiseen (Moore ym. 2016, 17). Esimerkiksi Egyptissä vuonna 2011 TOR-verkkoa käytettiin viestintään, kun hallinto rajoitti internet-liikennettä. Toisaalta TOR-verkolla on myös pimeämpi puoli, jota kutsutaan piilotetuksi palveluksi tai englanniksi Hidden service. Piilotettu palvelu on TOR-verkkoon luotu melkeinpä jäljittämättömissä toimiva palvelin, jolla voidaan välttää rajoituksia mitä palvelimen sisältöön tulee tai valvontaan liittyen (Moore ym. 2016, 17.).

Esimerkiksi vuonna 2013 kahdeksasta tuhannesta erilaisesta .onion päätteisestä Dark webin sivustosta seitsemäntoista prosenttia näistä sisälsivät pornoa ja viisitoista prosenttia liittyivät huumeisiin. Vuonna 2016 5205 .onion päätteisen sivun osalta huumeisiin liittyi 15,5 prosenttia ja viisi prosenttia liittyviä väkivaltaiseen ekstremismiin. Kolme ja puoli prosenttia liittyvät erilaisiin hakkerointipalveluihin ja puolitoista prosenttia liittyivät aseiden hankintaan. Haittaohjelmien osalta kiristyshaittaohjelmat voivat myös hyödyntää .onion päätteisiä osoitteita maksujen saamiseen, jolloin TOR-verkkoa käytetään myös tällaiseen rikolliseen toimintaan (Jardine 2018, 2830.).

2.4 Kyberuhkatiedustelu

Luvussa kuvaillaan lyhyesti mitä kyberuhkatiedustelu tarkoittaa ja mitä haasteita kyberuhkatiedustelu kohtaa. Keskeisiä käsitteitä kyberuhkatiedustelun osalta ovat CERT- ja SOC-termit, joista ensimmäinen Computer Emergency Response Team perustettiin vuonna 1988 (Yang & Lam 2020, 145). SOC tai Security Operations Center on Yang & Lam (2020, 145) mukaan teknisemmin suuntautunut CERTiin verrattuna. SOC kerää sekä analysoi erilaista tietoturvaan liittyvää dataa verkoista, palvelimista sekä tietokannoista päivittäin, havainnoi mahdollisia poikkeamia tietojärjestelmissä sekä vastaa erilaisten suojauskeinojen tarjoamisesta (Yang ym. 2020, 145.).

Kyberuhkatiedustelun Schlette, Caselli & Pernul (2021, 1) määrittelevät tietoturvatarkoitukseen kerätyksi uhkatiedoksi, joka on tarkoituksenmukaista ja riittävää. Kyberuhkatieto on rakenteellista ja todisteisiin pohjautuvaa uhkatietoa, jota voidaan käyttää päätöksentekijöiden informoimiseen organisaation tämän hetkisestä turvallisuustasosta sekä sitä voidaan hyödyntää myös turvallisuuden parantamisessa. Tällaisen kyberuhkatiedon avulla organisaatiot voivat havainnoida kuinka ja milloin tietomurtoa yritetään, mitkä tietojärjestelmät ovat hyökkäyksen kohteena, voidaan tunnistaa mitä hyökätyille kohteille tehtiin tai millaista dataa varastettiin, eristää hyökätyt kohteet muista tietojärjestelmistä tai palautua hyökkäyksistä (Preuveneers ym. 2020, 1).

Conti ym. (2018, 1) korostavat sitä, että suurin haaste on yksilöiden ja organisaatioiden turvallisuuden sekä yksityisyyden turvaaminen samalla kun yhä erilaisten kyberhyökkäysten määrä sekä vaihtelevuus lisääntyvät vaikeuttaen tietoturva-analyytikkojen sekä forensiikka-asiantuntijoiden työtä kyberhyökkäyksien tunnistamisessa sekä puolustautumisessa. Siksi kyberuhkatiedustelun rooli on kasvanut ja kyberuhkatiedustelu voi tunnistaa kyberhyökkäyksien tunnusmerkkejä, kerätä tietoa hyökkäyskeinoista sekä vastata havaittuihin hyökkäyksiin (Conti ym. 2018, 2.). Kure & Islam (2019, 1479) korostavat kyberuhkatiedustelun roolia ja merkitystä olemassa olevien ja tuntemattomien uhkien tunnistamisessa ja kyberuhkatiedustelu tukee organisaation päätöksentekoa strategisella, taktisella sekä operationaalisella tasolla.

Kyberuhkatiedustelun roolista Oosthoek & Doerr (2021, 301) huomauttavat kyberhyökkäyksien alkamisten ja havaitsemisien välillä olevasta viiveestä, joka on keskimäärin 206 päivää hyökkäyksen alkamista. Taktisella ja operationaalisella tasolla kyberuhkatiedustelu nopeuttaa haitallisen toiminnan tunnistamista ja parhaimmillaan jo ennen kuin hyökkäys onnistuu tunkeutumaan tietojärjestelmiin. Strategisella tasolla kyberuhkatiedustelu tarjoaa päätöksentekoon tietoa vallitsevista kyberuhkista (Oosthoek ym. 2021, 301.). Oosthoek ym. (2021, 301) korostavat kyberuhkatiedustelun olevan siviilien vastine tiedustelupalveluiden puolustuksellisille vastatiedustelutoiminnoille.

Kyberuhkatiedustelusta on esitetty useita malleja, kuten Biancon Pyramid of Pain, Stillionsin DML-malli tai Chismon ja Ruksin malli (Bromander ym. 2020, 6 :1). Biancon pyramidimallissa alimmassa kerroksessa ovat haittaohjelmien tiivistearvo-tunnisteet ja vaikka näiden arvojen tunnistaminen sekä tunnisteen sisältävän datan estäminen on helppoa, voidaan näitä arvoja hyvin helposti muuttaa vaikeuttaen puolustautuvan tahon toimintaa. Seuraavissa kerroksissa tiivistearvo-tunnisteiden yläpuolella ovat IP-osoitteet sekä domain-nimet, jotka on helppoa tai yksinkertaista tunnistaa sekä estää (Bromander ym. 2020, 6:3.). Seuraavina ovat verkkoon- tai kohteeseen liittyvät artefaktit sekä hyökkäystyökalut, jotka ovat Bromanderin ym. (2020, 6:3) mukaan ärsyttäviä sekä haastavia tunnistaa sekä estää. Ylimpänä kerroksena on taktiikat, tekniikat sekä proseduurit, jotka ovat sekä hyökkääjille että puolustautujille kaikista vaikeimmin muutettavissa mutta myös vaikeimmin tunnistettavissa. TTP-käsitteellä on historiaa tiedustelussa, mutta kyberuhkatiedustelun osalta täsmällisten taktiikoiden,

tekniikoiden sekä proseduurien osalta on vaikeata tunnistaa niitä (Bromanderin ym. 2020, 6:3.).

Stillionsin DML-malli, joka on lyhenne sanoista Detection-, Maturity- ja Level-sanoista ja DML-malli kuvaa hierarkkisesti millaista dataa ja minkä tyylistä dataa milläkin mallin tasolla organisaatioiden pitäisi tunnistaa, ymmärtää sekä osata toimia oikein. Mallissa alimmalla tasolla mitään dataa ei kerätä eikä tunnisteta, mutta seuraavilla kolmella tasolla yritetään kerätä hyökkäyksiin liittyviä jälkiä. Näitä tasoja ovat atomiset indikaattorit, kohde- sekä verkkoartefaktit sekä työkalut. Seuraavalla neljällä tasolla tarkoituksena on tunnistaa kuinka hyökkäystä suunnitellaan sekä millaisia menetelmiä käytetään. Näitä menetelmiä ovat taktiikat, tekniikat, proseduurit sekä työkalut. Seuraavalla kahdella tasolla korostuu tekijöiden strategia sekä tavoitteet ja ylimpänä DML-mallissa on attribuutio eli hyökkääjien identifioiminen. Mitä alempana mallissa ollaan sitä suurempaa on tarkkuus ja päin vastoin, mutta validiteetin osalta alimmalla tasolla on päin vastoin ja korkeimmalla tasolla validiteetti on kaikista tarkinta (Bromander ym. 2020, 6:3.).

Kolmas kyberuhkatiedustelun malli, jota Bromander ym. (2022, 6:4) mainitsevat on Chismonin ja Ruksin malli. Mallissa korostuu sekä lyhytaikainen että pitkäaikainen näkökulma sekä yksityiskohtaisuus. Mallissa kyberuhkatiedustelu on jaettu strategiseen, taktiseen, teknilliseen sekä operationaalisiin osiin, joista strateginen osa ja taktinen osa keskittyvät kyberuhkatiedon osalta pitkäaikaisiin näkökulmiin. Strateginen osa ei ole näin yksityiskohtainen, vaan sisältää attribuution, tavoitteet sekä strategian. Taktinen osa korostaa yksityiskohtaisuutta ja taktiikoita, tekniikoita sekä proseduureja. Lyhyen aikavälin osalta mallissa on operationaalinen ja tekninen osa, joista operationaalinen keskittyy erilaisiin kampanjoihin ja tekninen osa keskittyy käytettyihin työkaluihin, artefakteihin sekä indikaattoreihin (Bromander ym. 2022, 6:4.). Bromander ym. (2022, 6:4) korostavat sitä, että mallissa korostuu se, että mitä yksityiskohtaisempaa tietämys on, sitä varmemmin tekijät voidaan tunnistaa. Tulevien kyberhyökkäyksien tunnistamisen ja estämisen osalta mallissa tärkeätä on taktiikan, tekniikan ja proseduurien tunnistaminen.

Perinteisesti kyberuhkien osalta korostetaan hyökkääjän sekä puolustautuvan tahon välistä epätasapainoa, jossa hyökkääjälle onnistumiseen riittää vain yhden heikon kohdan löytäminen, kun puolustautuvan tahon on huomioitava joka ikinen mahdollinen heikko kohta organisaatiossa. Kyberuhkatiedustelussa tarkoituksena on pienentää tätä hyökkääjän ja puolustautuvan välistä asymmetriaa keräämällä sekä analysoimalla kyberuhkatietoutta (Oosthoek ym. 2021, 302). Kyberuhan osalta Oosthoek ym. (2021, 302) korostavat hyökkääjän motivaatiota kohteen teknologisen infrastruktuurin haavoittuvuuksien hyödyntämisessä sopivilla tavoilla, kuten esimerkiksi haittaohjelmilla.

Vaikka kyberuhkatiedustelu tarkoituksella keskittyy puolustuksellisiin toimenpiteisiin, kuten tunkeutumisten aikaiseen havaitsemiseen ja tunnistamiseen, korostavat Oosthoek ym. (2021, 301) kyberuhkatiedustelun onnistumisten osalta sitä, että jopa 352 ainutlaatuista valtion tukemaa kyberhyökkäystä on tunnistettu vuodesta 2005 alkaen. Kyberuhkatiedustelutoteutuksia on tarjolla avoimena sekä

kaupallisina ratkaisuina ja Oosthoek ym. (2021, 302) korostavat kyberuhkatiedustelun potentiaalia kyberuhkia vastaan sekä hyödyllisyyttä kyberuhkien kissa ja hiiri pelissä.

Erilaista kyberuhkatietoa voidaan kerätä erilaisista lähteistä ja on olemassa myös avoimia kyberuhkatietolähteitä kaupallisten lisäksi. Myös erilaiset yhteisöt tai teollisuuden alat jakavat tietoa, kuten myös erilaiset muut tahot, kuten raportit tai esimerkiksi palomuuri- tai IDS-tietoturvajärjestelmät (Yang & Lam 2020, 146). Keskeistä kyberuhkatiedustelussa on siis uhkatiedon analysointi ja uhkatietoa myös jaetaan eri tahojen kesken (Oosthoek ym. 2021, 303). Yang & Lam (2020, 145) korostavat kyberuhkatiedon jakamisen tärkeyttä vastauksena sekä kyberhyökkäysten lisääntyneeseen teknisen tason parantumiseen että vahingollisuuteen. Keskeisimmät uhkatiedon osaset ovat uhka-artefaktit, jotka yleensä koostuvat taktiikoista, tekniikoista sekä proseduureista ja tunkeutumiseen liittyvistä indikaattoreista. Näitä tunkeutumiseen liittyviä indikaattoreita ovat domain nimet, IP-osoitteet sekä tiedostojen tunnisteet, jotka on yhdistetty haitalliseen toimintaan. Tunkeutumiseen liittyvät indikaattorit ovat koneellisesti käsiteltävissä ja esimerkiksi IDS-järjestelmät tai tunkeutumisen havaitsemisjärjestelmät voivat näitä hyödyntää. Tunkeutumiseen liittyvät indikaattorit myös mahdollistavat tekijän osalta laajemman toimintatavan kuvaamisen erityisesti taktiikoiden, tekniikoiden ja proseduurien osalta (Oosthoek ym. 2021, 303.).

Kyberuhkatiedustelu on tuottanut joitain analyyttisiä malleja, kuten Lockheedin Cyber Kill Chain, jota voidaan suomeksi kutsua tappoketjuksi, timanttimallin, the Pyramid of Pain ja MITRE ATT&CK-mallin. Mallien avulla on standardisoitu kyberuhkien semantiikkaa sekä kyberuhkien piirteitä (Oosthoek ym. 2021, 303.). Näitä erilaisia malleja avataan yksityiskohtaisemmin myöhemmin.

Toisaalta kyberuhkatiedustelussa on myös haasteita. Vaikka kyberuhkatiedustelusta on ollut hyötyä, Oosthoek ym. (2021, 302) mielestä kyberuhkatiedustelu on kuitenkin tuote ilman prosessia, jossa teknisiä ongelmia ratkaistaan tekniikalla. Myös kyberuhkatiedustelussa innovointi on hidastunut eikä olemassa olevia haasteita kovinkaan laajasti tunnisteta. Oosthoek ym. (2021, 302) jatkavat painottamalla sitä, että kyberuhkatiedustelun pitäisi myös ottaa opiksi tiedustelun metodologiasta sekä tiedusteluanalyysistä.

Metodologian osalta Oosthoek ym. (2021, 304) korostavat tiedustelutieteiden pohjautumista sosiaalitieteelliseen laadulliseen tutkimukseen. Tiedustelutieteiden osalta tämä pohja näkyy esimerkiksi kognitiivisten harhojen, heurististen vääristymien sekä intuitiivisten ansojen tunnistamisessa tiedusteluanalyysiin vaikuttavina tekijöinä. Vaikka Heuerin Psychology of Intelligence Analysis kirjaan usein viitataan kyberuhkatiedusteluun liittyvissä konferenssipuheissa, Oosthoek ym. (2021, 304) huomauttavat, että kyberuhkatiedustelussa jätetään huomioimatta kuinka Heuerin teos ohjaa analyysiä sekä kuinka se auttaa päivittäisessä analyytikon työssä. Myös Heuerin ja Phersonin Structured Analytic Techniques kirjan tekniikoiden osalta kyberuhkatiedustelussa ACH-tekniikka on ylikorostunut, mutta kaiken kaikkiaan kyberuhkatiedustelusta operationaalista tietoa on vähän eikä julkisuudessa esiteltyjä esimerkkejä ole myöskään montaa (Oosthoek ym. 2021, 304.).

Kyberuhkatiedustelun osalta jokapäiväisessä toiminnassa tiedustelutoiminnan hypoteesien laatimisen ja kilpailuttamisen sijasta korostuvat erilaiset hälytykset sekä raaka data. Kyberuhkien osalta sekä hyökkäyksien määrät että nopeudet korostavat metodologian puutteita ja yksittäisten tunkeutumiseen liittyvien indikaattoreiden osalta analysointi on lähes mahdotonta (Oosthoek ym. 2021, 304.). Oosthoek ym. (2021, 304) korostavat myös sitä, että vaikka esimerkiksi keinoälypohjaisia tekniikoita on otettu kyberuhkatiedustelun analysoinnin avuksi yhä enemmän, ei teknologian käyttöönottaminen ole ratkaisu, vaan tärkeätä on ottaa käyttöön toimiva prosessi.

Myös kyberuhkatiedusteluun liittyvän datan laadussa on haasteita ja esimerkiksi tunkeutumiseen liittyvien indikaattoreiden sisältävät IP-osoitteet, domainit tai tiedostojen tiivistearvot voivat olla aikaisempia tietomurroissa käytettyjä, mutta voivat olla myös vääriä esimerkiksi jos IP-osoite on otettu pois komentopalvelin käytöstä. Vaikka virustorjuntaohjelmistot ovat lopettaneet käyttämästä tiivistepohjaisia arvoja haitallisten tiedostojen tunnistamisessa, kyberuhkatiedustelussa näitä yhä käytetään. Kaiken kaikkiaan tunkeutumiseen liittyvät indikaattorit eivät sisällä tiedustelun kannalta kovinkaan paljoa arvoa, vaan niitä pitää myös verrata verkkoinfrastruktuurin havaintoihin (Oosthoek ym. 2021, 306, 308.).

Oosthoek ym. (2021, 307) nostavat haasteena myös erilaisten useiden toimijoiden kesken jaettujen kyberuhkatietojen hyödyllisyyden arvioinnin vaikeuden. Esimerkiksi jaetut kyberuhkatiedot sisälsivät tietojen kierrättämistä jopa useiden kuukausien takaa, mutta artefaktien samankaltaisuus oli vähäistä vaikka seurattiin samaa uhkaa. Oosthoek ym. (2021, 307) mukaan tällainen tarkoittaa sitä, että kenelläkään ei ole riittävää kattavuutta seurattavista uhkista. Tällöin kyberuhkatiedustelun kyky havaita erilaisia kyberuhkia ajoissa on vaikeata ja Oosthoek ym. (2021, 307) nostavat keskeisemmäksi syyksi läpinäkymättömyyden metodologioiden sekä proseduurien osalta sekä rajallisesta määrästä tiedonkeruupisteitä. Oosthoek ym. (2021, 307) korostavat kyberuhkatiedustelussa jaettujen kyberuhkatietojen osalta sitä, että tällaista tietoa jakavien tahojen on oltava vastuussa käyttämistään menetelmistä, analysointitavoistaan sekä raa'an datan laadusta.

Kybertiedustelun käyttämään dataan liittyen Oosthoek ym. (2021, 309) nostavat esille myös mahdolliset datan vinoumat. Miltä alueilta ja mistä laitteista tietoa kerätään vaikuttaa aineistoon, mutta Oosthoek ym. (2021, 309) korostavat myös sitä, että kaupallisten kyberuhkatiedustelutoimijoiden osalta houkuttavinta on keskittyä valtiotason toimijoihin sekä teknisesti edistyneisiin toimijoihin markkinointiin liittyvistä tekijöistä johtuen. Markkinoinnin kannalta keskittyminen tällaisiin toimijoihin voi johtaa siihen, että kyberrikollisuuden pikku tekijät saavat vähemmän huomiota. Oosthoek ym. (2021, 309) jatkavat myös huomauttamalla, että vähemmän tunnetut ryhmät tai esimerkiksi Turkkilaiset tai Intialaiset valtiolliset tekijät jäävät vähemmälle huomiolle. Kyberuhkatiedustelun osalta myös valtiot vaikuttavat ja Oosthoek ym. (2021, 309) mainitsevat sen, että esimerkiksi Yhdysvaltaisilla tai Venäläisillä toimijoilla on eroavaisuuksia sen suhteen millaisiin uhkiin keskitytään. Toisaalta esimerkiksi molemmilla toimijoilla on

kiinnostusta toisiinsa, mutta oman maan uhkien osalta tarjottavan tiedon osalta tasapainoillaan sen suhteen mitä kerrotaan ja milloin (Oosthoek ym. 2021, 309).

Attribuutio on myös yksi kyberuhkatiedustelun haasteista ja Oosthoek ym. (2021, 309) mainitsevat myös harhauttamisen mahdollisuuden. Attribuutiota vaikeuttaa myös se, että eri kyberuhkatiedon toimittajat nimeävät havaittuja uhkia eri nimillä, joka vaikeuttaa tekijöiden käyttämien taktiikoiden, tekniikoiden sekä proseduurien havainnointia (Oosthoek ym. 2021, 310).

Kyberuhkatiedustelun haasteina Yang & Lam (2020, 146) nostavat myös monivektoriset sekä monivaiheiset kyberhyökkäykset, joihin myös APT-hyökkäykset, polymorfiset uhat, nollapäivähaavoittuvuudet sekä komposiittiuhat kuuluvat. Nämä kaikki tavallisten kyberuhkien lisäksi haastavat puolustautuvan tahon kyvykkyyttä sekä kykyä havaita uhkia. Yang & Lam (2020, 146) jatkavat painottamalla SOC sekä muiden tietoturvaosastojen proaktiivista roolia sekä uhkatiedon jakamisen merkitystä.

Bromander ym. (2022, 6) korostavat myös automatisoinnin merkitystä yhä lisääntyvän datan myötä. Myös Preuveneers ym. (2020, 1) korostavat kyberuhkatiedon jakamisen tärkeyttä erilaisten kyberuhkien tunnistamisessa, mutta huomauttavat myös, että tällainen data voi sisältää myös dataa, joka voi olla vahingollista tietoa jakavalle taholle. Useita erilaisia tapoja kyberuhkatiedon jakamiseen on kehitetty, kuten esimerkiksi STIX tai TAXII (Haque & Krishnan 2021, 883).

2.5 Kyberuhkatiedustelu ja Dark web

Luvussa kuvaillaan lyhyesti millaista kyberuhkatiedustelu on Dark webissä ja mitä haasteita dark web nostaa esille. Kawaguchi & Ozawa (2019, 320) korostavat sitä, että dark webin louhiminen pelkästään haitallisten sivujen suhteen on hyödyllistä. Nunes, Diab, Gunn, Marin, Mishra, Paliath, Robertson, Shakarian, Thart & Shakaria (2016, 1) nostavat myös esille kyberuhkatiedustelun ja Dark webin seulomisen edut tulevien kyberuhkahyökkäyksien osalta. Numes ym. (2016, 1) kehittivät mallin, joka hyödyntää tiedonlouhintaa sekä koneoppimisen tekniikoita ja malli kerää keskimäärin 305 korkealaatuista kyberuhkavaroitusta. Nämä kyberuhkavaroitukset sisältävät vihjeitä ja tietoa uusista haittaohjelmista ja hyökkäystavoista, joita ei vielä ole käytetty kyberhyökkäyksissä (Numes ym. 2016, 1). Samtani, Li, Benjamin & Chen (2021, 27) huomauttavat kyberuhkatiedustelun reaktiivisuutta ja painottavat sitä, että kyberuhkatiedustelun kannattaisi olla proaktiivisempi ja Dark webin osalta kyberuhkatiedustelu on alkanut kiinnittää yhä enemmän huomiota siihen. Samtani ym. (2021, 27) esittelevät automatisoitua työkalua, joka kerää, analysoi sekä raportoi Dark webin lähteistä mitä hakkerit mahdollisesti tulevat tekemään ja millaisia motiiveja heillä on, jolloin kyberuhkatiedustelu parantaa tilannekuvaansa.

Alkhatib & Basheer (2019, 1) korostavat myös tiedonlouhimisen roolia tietoisuuden parantamisessa sen suhteen mitä Dark webissä tapahtuu, millaisia ovat tuotteiden ja myyjien keskinäiset suhteet sekä paljonko tuotteita myydään

Dark webissä. Tiedonlouhinnalla pystytään myös ymmärtämään haittaohjelmia tekevien yhteisöjen sosiaalisia sekä psykologisia näkemyksiä ja tällainen kerätty tieto auttaa myös rikollisuuden tutkinnassa. Haasteena on kuitenkin se, että louhittaessa tietoa Dark webistä tällaisen tiedon kyberuhkatiedoksi jalostaminen vaatii useita eri vaiheita (Alkhatib ym. 2019, 1.).

Samtani ym. (2021, 27:2) korostavat Dark webin kyberuhkatiedustelussa haasteena erilaisten myyntipaikkojen määrää sekä myös useiden sosiaalisten alustojen lukumäärää. Näitä Dark webin sosiaalisia alustoja ovat erilaiset keskustelukanavat sekä foorumit. Dark webin myyntipaikkoja ovat erilaiset markkinapaikat tai esimerkiksi varastettuja luottokorttitietoja myyvät kaupat (Samtani ym. 2021, 27:2–27:3.).

Erilaiset Dark webin lähteet tarjoavat erilaista kyberuhkatietoa ja Samtani ym. (2021, 27:4) toteavat, että kyberuhkatietoa erilaisista tekniikoista, taktiikoista sekä toimenpiteistä saadaan keskustelufoorumeilta tai keskustelukanavilta. Keskustelufoorumeilla tai keskustelukanavilla myös jaetaan hyökkäyskoodia sekä mainostetaan erilaisia kyberuhkatyökaluja muille. Erilaisista kauppapaikoista saadaan tietoa millaisilla tuotteilla on kysyntää (Samtani ym. 2021, 27:4.). Kyberuhkatiedon keräämistä voidaan vaikeuttaa erilaisilla vastatoimilla ja Samtani ym. (2021, 27:4) huomauttavat, että useat Dark webin tiedonlouhintatyökalut keskittyvät vain tiettyihin osa-alueisiin, jolloin kokonaiskuvan muodostaminen on vaikeata. Myös datan valtava määrä, monikielisyys ja oma terminologia vaikeuttavat kyberuhkatiedon keruuta (Samtani ym. 2021, 27:4).

2.6 Haittaohjelmat ja Advanced Persistent Threat

Haittaohjelmat ovat yleisnimitys ohjelmistoille, jotka toimivat vahingoittavasti tai tunkeilevasti. Haittaohjelmia kehitetään varastamistarkoituksessa, erilaisten sovelluksien suorittamiseksi esimerkiksi ylläpitäjän oikeuksilla, tietojärjestelmiin tunkeutumiseksi tai vahingoittamiseksi. Nykyään haittaohjelmien kehittäminen on hyvin tuottoisaa, jolloin haittaohjelmien määrät, erilaiset haittaohjelmatyypit sekä haittaohjelmien monimutkaisuus ovat lisääntyneet (Alenezi, Alabdulrazzaq, lshaher & Alkharang 2020, 326.).

Alenezi ym. (2020, 326) jakavat haittaohjelmat kahteen erilaiseen pääluokkaan eli ensimmäisen sukupolven tai staattisiin haittaohjelmiin sekä toisen sukupolven tai dynaamisiin haittaohjelmiin. Ensimmäisen sukupolven haittaohjelmat eivät muutu eivätkä muuta toimintatapaansa tietojärjestelmään tunkeutumisen jälkeen, mutta toisen sukupolven haittaohjelmat varioituvat jokaisen tunkeutumisen myötä muodostaen uuden variantin. Erilaisia haittaohjelmia voidaan luokitella kuten Alenezi ym. (2020, 326) luokittelevat tarttumistavan tai tarkoituksen mukaisesti. Tarttumistavan osalta haittaohjelmia voidaan luokitella viruksiin, matoihin, Troijan hevosiin, roskapostiin tai rootkitteihin**.** Tarkoituksensa mukaisesti haittaohjelmia voidaan luokitella vakoiluohjelmiin, kiristysohjelmiin, mainosohjelmiin tai näppäimistöä tarkkaileviin haittaohjelmiin (Alenezi ym. 2020, 326–327.).

Alenezi ym. (2020, 327) luokittelevat haittaohjelmat viiteen eri vaiheeseen, joista ensimmäinen vaihe oli vuosina 1949–1991, toinen vaihe vuosina 1992–1999, kolmas vaihe vuosina 2000–2008 ja neljäs vaihe vuosina 2005–2016 sekä viides vaihe vuodesta 2010 alkaen. Ensimmäisen vaiheen haittaohjelmat olivat viattomia eikä tarkoituksena ollut tietojärjestelmän vahingoittaminen. Toisen vaiheen haittaohjelmat oli kohdistettu Windows-käyttöjärjestelmään ja toisen vaiheen kehityksessä korostuvat Windowsissa toimivat haittaohjelmat, varhaiset madot sekä makrovirukset. Kolmannessa vaiheessa Internetin rooli nousi keskeiseksi ja verkkomadot sekä tietokonevirukset olivat pääosassa. Haittaohjelmat levisivät sähköpostin liitteinä, tiedostolatauksien tai verkossa jaettujen tiedostojen kautta. Neljännessä vaiheessa haittaohjelmat sekä rootkitit nousivat keskeisiksi ja yleisin leviämistapa olivat sähköpostit, RDP-ohjelmistojen kautta, erilaisten ladattujen tiedostojen kautta sekä USB-tikkujen kautta. Keskeistä oli taloudellisen hyödyn tai tietojärjestelmän hallinnan hyödyntäminen luvattomasti. Viidennessä vaiheessa korostuu erilaisten haittaohjelmien hyödyntäminen vakoiluun sekä sabotoimiseen (Alenezi ym. 2020, 327–330.).

Alenezi ym. (2020, 330) huomauttavat, että nykyään haittaohjelmien tekijöinä erottuvat myös armeijan tai poliisin yksiköt, sillä haittaohjelmat ovat myös voimakkaita aseita tietojärjestelmiä vastaan. Alenezi ym. (2020, 330) käyttävätkin kohdennetut haittaohjelmat termiä kuvaamaan tarkoin suunniteltuja kyberhyökkäyksiä tiettyjä kohteita vastaan ja mainitsevat Stuxnetin esimerkkinä.

Quintero-Bonilla ja Martín (2020, 1) huomauttavat, että kohdennetut haittaohjelmat ovat nyt ja tulevaisuudessa yhä suurempi uhka, sillä niiden varhainen havaitseminen on vaikeata. Havaitsemista vaikeuttaa erilaisten tekniikoiden käyttäminen, joiden tarkoituksena on vaikeuttaa havaitsemista sekä pysyä havaitsemattomissa mahdollisimman pitkään. Kohdennettujen haittaohjelmien eroavaisuudet tavallisiin kyberhyökkäyksiin ovat siis suuria ja Quintero-Bonilla ym. (2020, 1) huomauttavat, että kohdennettujen haittaohjelmahyökkäyksien seuraukset ovat usein huomattavia.

Englanniksi kohdennetuista haittaohjelmista käytetään termiä Advanced Persistent Threat tai APT-lyhennettä. Advanced-sana viittaa hyökkääjien korkeaan osaamiseen erilaisten valittujen menetelmien sekä tekniikoiden osalta sekä kykyyn kehittää ja hyödyntää kohdetta vastaan tarkasti valittuja yksilöllisiä keinoja. Persistent-sana viittaa siihen, että toiminnalla on tarkasti mietitty tavoite sekä hyökkäystavoitteet. Threat-sana viittaa siihen, että hyökkäys on koordinoitu, motivoitunut sekä hyökkääjällä on resursseja käytettävissään (Quintero-Bonilla ym. 2020, 2). Quintero-Bonilla ym. (2020, 2) jatkavat huomauttamalla, että kohdennetut haittaohjelmat ovat valikoituja hyökkäyksiä, joissa luvattomasti tietojärjestelmiin pääsemällä aiheutetaan vahinkoa yrityksille, toimialalle tai hallituksen organisaatiolle tai saadaan käsiin luottamuksellista tietoa. Stuxnetin jälkeen kohdennetut haittaohjelmahyökkäykset ovat yhä varovaisemmin toteutettuja mutta myös vahingoittavampia ja osoittavat kuinka helppoa on ollut tunkeutua korkean profiilin tietojärjestelmiin sekä kuinka erilaiset puolustukselliset järjestelmät on kierretty. Kohdennettujen haittaohjelmien osalta lisähaasteena on se, että useat hyökkäykset ovat vielä havaitsematta (Quintero-Bonilla ym. 2020, 2.).

Toisaalta Quintero-Bonilla ym. 2020, 2) jatkavat huomauttamalla, että usein havaitut kohdennetut haittaohjelmat ovat olleet muutoksia jo havaittuihin kohdennettuihin haittaohjelmiin ja muutoksilla on sopeuduttu muuttuneisiin tavoitteisiin.

DeVore & Lee (2017, 40) huomauttavat kohdennettujen haittaohjelmien olevan mukautettuja sekä tarkasti suunniteltuja kohdetietojärjestelmiin tunkeutumiseen sekä toimimaan halutulla tavalla kohdetietojärjestelmissä. DeVore ym. (2017, 40) jatkavat mainitsemalla, että kohdennettujen haittaohjelmien vaatimien resurssien takia vain valtioilla on resursseja sekä osaamista tällaisten kohdennettujen haittaohjelmien kehittämiseen. Kohdennettujen haittaohjelmien epäilyjen tekijöiden osalta DeVore ym. (2017, 40) huomauttavat, että sekä Kiina että Pohjois-Korea ovat aktiivisia toimijoita.

Kohdennettujen haittaohjelmien yksi hyökkäyksellisistä ominaisuuksista on se, että ne ovat erittäin kyvykkäitä yllätyksellisinä kyberaseina, mutta toisaalta ovat myös lyhytaikaisia sekä kertakäyttöisiä vaikutukseltaan. DeVore ym. (2017, 40) jatkavat toteamalla, että kohdennetut haittaohjelmat muuttavat sotilaallisten kyvykkyyksien jakautumista ennakoimattomasti ja kohdennettujen haittaohjelmien osuudet valtioiden sotilaallisessa voimankäyttöarsenaalissa ovat yhä tärkeämpiä.

Lemay, Calvet, Menet & Fernandez (2018, 26) huomauttavat, että kohdennettujen haittaohjelmien osalta tietoa on paljon saatavilla, mutta hajautetusti eri paikoissa. Eri tietolähteitä ovat haittaohjelmien torjuntaan keskittyvien yrityksien sivustot, tieteelliset julkaisut sekä erilaiset blogijulkaisut. Tällöin kokonaiskuvan saaminen vie paljon aikaa (Lemay ym. 2018, 26). Haasteena on myös akateemisten julkaisujen puute, koska haittaohjelmien torjuntaan keskittyvillä yrityksillä on monopoli keskeisiin kohdennettujen haittaohjelmien havaitsemiseen liittyvään tietoon. Erityisesti niin sanottu tapahtumiin liittyvä data, jota englanniksi kutsutaan Incident-response, ennen ja jälkeen hyökkäystä on keskeistä, jotta havaitusta kohdennetusta haittaohjelmahyökkäyksestä voidaan saada kokonaiskuva.

Kohdennetun haittaohjelman selvittämisen osalta keskeistä on myös se, että ollaan kerätty havaintoja pitkältä aikaväliltä eri kohteista. Koska kohdennetuista haittaohjelmien hyökkäyksistä havaitaan vain pieni osa, voidaan yhdenkin havaitun tapauksen osalta rakentaa kokonaiskuvaa operaatiosta, mutta tällaisia tietokantoja on yleensä vain haittaohjelmien torjuntaan keskittyvillä yrityksillä eikä akateemisilla tutkimusryhmillä (Lemay ym. 2018, 27.). Tämän takia Lemay ym. (2018, 27) korostavat haittaohjelmien torjuntaan keskittyvien yrityksien merkitystä tiedonlähteinä.

Muiden kuin akateemisten lähteiden käyttäminen tiedonlähteinä aiheuttaa kuitenkin ongelmia, kuten johtopäätösten validointia ei välttämättä olla tehty tai se on tehty puutteellisesti. Lisäksi vertaisarviointia ei yleensä olla tehty eikä lähteitä myöskään olla riippumattomasti tarkistettu, sillä lähdeaineisto on yleensä luottamuksellista. Keskeistä on myös se, että haittaohjelmien torjuntaan keskittyvien yrityksien raportit ovat myös keskeisiä markkinoinnissa. Tällöin jotkin raportit voivat teknisten yksityiskohtien sekä analyysin sijasta keskittyä lööppien

saamiseen, jotka myyvät paremmin (Lemay et a. 2018, 27.). Tämän takia Lemay ym. (2018, 27) korostavat sekä lähdekritiikkiä että attribuutioon liittyvää kriittisyyttä.

2.7 Erilaisia kyberhyökkäysmalleja sekä yleinen kyberhyökkäysmalli

Luvussa esitellään lyhyesti olemassa olevia erilaisia kyberhyökkäysmalleja sekä esitellään yleistä kyberhyökkäysmallia. Kyberuhkatiedustelu on tuottanut joitain analyyttisiä malleja, kuten Lockheed Martinin Cyber Kill Chain, Timanttimallin, Pyramid of Pain ja MITREn ATT&CK-mallin. Mallien avulla on standardisoitu kyberuhkien semantiikkaa sekä voidaan kuvata kyberuhkien ominaisuuksia (Oosthoek ym. 2021, 303.).

Hoffmann (2020, 356) huomauttaa, että kyberhyökkäyksiä ei pitäisi mieltää lyhytaikaiseksi tapahtumaksi, joka vain sattui vaan usein kyberhyökkäyksillä on tietty kaava, jossa tiettyjä toimia tehdään tiettyyn aikaan. Tällaisella kyberhyökkäyksellä on tietty kesto ja tällaista kyberhyökkäystä voidaan kutsua kyberhyökkäysmalliksi tai jopa kybertappoketjuksi (Hoffmann 2020, 356.). Tällaisen kyberuhkamallin tunteminen voi olla hyödyksi kyberhyökkäyksiltä puolustauduttaessa, sillä Hoffmannin (2020, 356) mukaan voidaan arvioida kuinka todennäköinen mahdollinen kyberhyökkäys on, kuinka kauan mahdollinen kyberhyökkäys kestäisi tai millaisia kustannuksia kyberhyökkäyksestä voisi aiheutua. Tällaisiin arvioihin vastaamalla voidaan arvioida koska mahdollinen kyberhyökkäys tapahtuisi ja missä kyberuhkamallin vaiheessa hyökkäys voisi olla (Hoffmann 2020, 356).

Kyberuhkamalleja on kuitenkin useita ja eri mallien esittäjät jakavat erilaiset vaiheet eri nimiin tai kuvaavat vaiheiden sisältöjä erilailla. Lehto (2022, 125) korostaa sitä, että eri kyberuhkamallit auttavat purkamaan kyberhyökkäyksiä erilaisiin vaiheisiin, joita voidaan hyödyntää kyberhyökkäyksen paljastuttua analyysissä sekä tulevien kyberhyökkäyksien estämiseen. Keskeistä erilaisten kyberuhkamallien osalta se, että mallien avulla voidaan pyrkiä ymmärtämään kyberhyökkääjän taktiikat, käyttämät tekniikat ja prosessit. Näiden myötä voidaan oppia kuinka erilaiset kyberhyökkääjät toimivat ja kuinka heitä vastaan voitaisiin puolustautua ja miten erilaisilla keinoilla voitaisiin pienentää kyberhyökkääjien hyödyntämiä aukkoja. (Lehto 2022, 125.).

Tatam, Shanmugam, Azam & Kannoorpatti (2021, 9) toteavat, että taktiikat kuvaavat hyökkääjän asettamia tavoitteita, joita onnistuneessa hyökkäyksessä saavutettaisiin. Käytetyt tekniikat ovat hyökkääjän valitsemia toimia, joilla hyökkääjän tavoite pyritään saavuttamaan. Jotta hyökkääjä saavuttaisi taktiikkansa asettaman tavoitteet, voidaan joutua käyttämään useita erilaisia tekniikoita. Prosessit ovat erilaisia työkaluja tai vaiheita, joita kyberhyökkääjä on hyödyntänyt tietyllä tavalla ja yleensä APT-hyökkäyksissä hyödynnetään useita taktiikoita (Tatam ym. 2021, 9.). Tatam ym. (2021, 9) huomauttavat, että yleensä

kyberhyökkääjän taktiikat, tekniikat ja prosessit säilyvät samoina pitkiäkin aikoja, jolloin jopa heikkojen erilaisten indikaattoreiden pohjalta voidaan tunnistaa kyberhyökkäys sekä tunnistaa laajempia kyberhyökkäyksiä eri kohteisiin. Erityisesti APT-hyökkäyksien osalta Hutchins, Cloppert & Amin (2011, 3) korostavat kyberhyökkäysmallin kuvaaman ketjun katkaisemista jossain vaiheessa, jolloin hyökkääjän hyökkäys pysäytetään. Lisäksi puolustajien onnistuessa vastatoimissaan hyökkääjiä nopeammin, nousevat hyökkääjiltä vaadittavat resurssivaatimukset yhä korkeammiksi, jotta hyökkäys voisi onnistua.

Hoffmann (2020, 356) esittelee Colemanin mallin, jossa erilaisia vaiheita on viidet. Mallissa ensimmäinen vaihe on tiedustelu, jonka jälkeen seuraavana on skannaus, järjestelmään tunkeutuminen, vahingollisten toimien tekeminen ja hyväksikäyttö. Hoffmann (2020, 356) jatkaa esittelemällä McAfeen, Hutchinsin ja Spring & Hatlebackin mallit, joissa erilaisia vaiheita on seitsemän erilaista. Toisaalta jo vuonna 1998 Meadows esitteli mallin, jossa kyberhyökkäys on jaettu eri vaiheisiin hyökkäyksen visuaalisen esittämisen helpottamiseksi (Haga, Meland & Sindre 2020, 112).

McAfeen, Hutchinsin ja Spring & Hatlebackin malleissa vaiheet ovat tiedustelu, aseistaminen, toimittaminen, hyväksikäyttö, asentaminen, ohjaaminen tai komentopalvelimella ohjaaminen ja viimeisenä toimiminen hyökkääjän haluamalla tavalla. Tiedusteluvaiheessa keskeistä on valita hyökkäyksen kohteet kohdeympäristöön tutustumalla esimerkiksi porttiskannauksilla, passiivisemmin erilaisia netin indeksointipalveluita hyödyntämällä, keräämällä erilaista avointen lähteiden aineistoa, kuten tutustumalla kohteen julkaisemiin aineistoihin tai julkaisuihin, keräämällä kohteen käyttämiä sähköpostiosoitteita tai tietoa kohteen sosiaalisen median käytöstä tai millaisia teknologisia ratkaisuja kohteessa käytetään (Hoffmann 2020, 357.).

Aseistaminen vaiheessa valittu tai kehitetty haittaohjelma valmistellaan kohteessa käytettäväksi. Mikäli tarvetta ei ole kehittää haittaohjelmistoa, vaiheessa keskitytään keräämään tarvittavia olemassa olevia kyberaseita. Toimittaminen vaiheessa valitut haittaohjelmistot siirretään jollain keinolla kohteeseen. Keinoina ovat esimerkiksi sähköpostiliitteet, SQL-injektiot tai muuten haitallisiksi muokatut nettisivustot tai USB-tikut (Hoffmann 2020, 357.).

Hyväksikäyttö-vaiheessa kohteessa suoritetaan haluttua haitallista koodia, jonka jälkeen seuraavassa vaiheessa voidaan asentaa muuta hyökkääjän haluamaa koodia. Esimerkkinä voidaan mainita erilaiset etäyhteyden mahdollistavat haittaohjelmat tai erilaiset takaoven avaavat ohjelmistot, joiden kautta kohteeseen voidaan viestiä ja ohjata haittaohjelmiston toimintaa. Seuraava vaihe onkin komentopalvelinvaihe, jonka kautta kohdeympäristöä hallitaan ja esimerkiksi muita tarvittavia haittaohjelmia voidaan asentaa. Lisäksi kohdeympäristön osalta voidaan muokata tai tutkia erilaisia kohteessa olevia tietoja tai tietokantoja ja esimerkiksi haittaohjelman osalta käyttöoikeuksia laajennetaan (Hoffmann 2020, 357.).

Toimiminen hyökkääjän haluamalla tavalla-vaiheessa tavoitteena on saavuttaa asetetut kyberoperaatiolle asetetut tavoitteet, kuten esimerkiksi tietojen

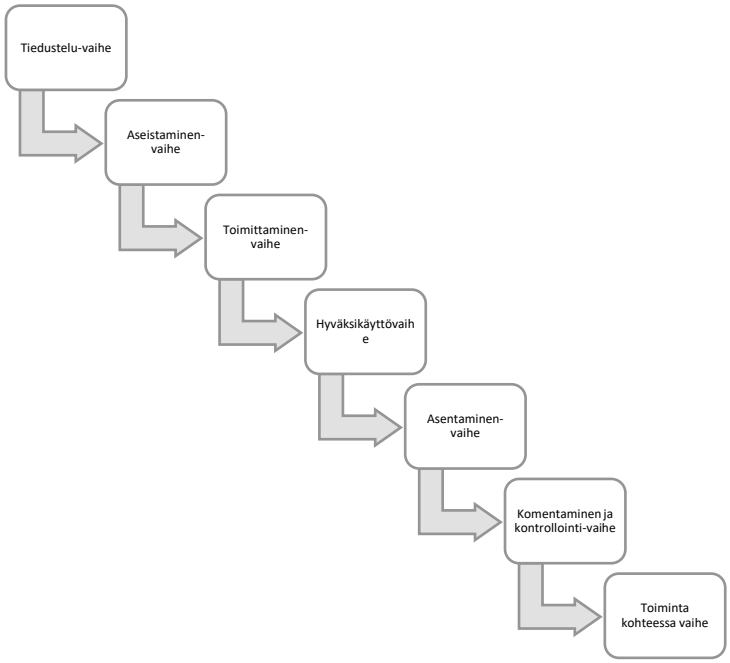
kopioiminen tai tietojärjestelmälle vahingon aiheuttaminen eikä fyysisen vahingon aiheuttaminen ole poissuljettua (Hoffmann 2020, 357.).

Kyberuhkamalleista tunnetuin on Lockheed Martinin esittelemä malli, jota kutsutaan myös kybertappoketjuksi. Lockheed Martinin malli kuvaa erilaisia vaiheita kyberhyökkäykseen liittyen. Malli on paljolti käytetty tietoturva-alalla ja se mahdollistaa tutkimisen kuinka erilaiset vaiheet vaikuttavat tietojärjestelmiin. Mallia hyödynnetään myös analysoimalla ja kehittämällä erilaisia tietoturvakontrolleja, joilla voidaan parantaa tietojärjestelmien resilienssiä erilaisia kyberhyökkäyksiä vastaan (Haga, Meland & Sindre 2020, 112–113.).

Lockheed Martin (2015, 5) esittelee mallista saatavia etuja, joita ovat muun muassa erilaisen kyberuhkatiedon priorisointi, milloin olisi syytä reagoida eri johtotasoilla, mihin investoinnit kannattaisi priorisoida, kuinka mitata kyberuhkatiedon tehokkuutta, kuinka mitata resilienssiä, kuinka mitata analyyttistä osaamista ja kuinka tunnistaa ja jäljittää erilaisia kyberuhkahyökkäyskampanjoita. Kyberuhkamallin avulla erilaisten sensorien keräämää tietoa ja hälytyksiä voidaan priorisoida, sillä mitä myöhäisemmältä kyberuhkamallin vaiheesta hälytys tulee, sitä korkeampi pitäisi tämän kyberuhkatiedon prioriteetin olla (Lockheed Martin 2015, 5.).

Lockheed Martin (2015, 5) huomauttaa, että toisinaan kyberuhkatiedon analyytikoilla on epäselvää kenelle kertoa havainnoista ja milloin hälyttää erilaisia johtotasoja. Tämän osalta kyberuhkamalli auttaa, sillä mitä myöhäisemmässä kyberuhkamallin vaiheessa havaintoja saadaan, sitä korkeammalle organisaatiossa hälytys olisi tehtävä. Pahimmillaan, mikäli kyberuhkahyökkäys on onnistunut siirtämään tietoa organisaation ulkopuolelle, on ilmoitettava johtokunnalle sekä erilaisille viranomaisille, kun taas alemmalla tasolla yksittäisen tietokoneen saastuminen voidaan hoitaa esimerkiksi tietoturvapäällikölle kertomalla (Lockheed Martin 2015, 5.).

Kyberuhkamalli auttaa myös investointien priorisoinnissa, sillä kyberuhkamallin eri vaiheiden osalta organisaatiolla olisi hyvä olla kyvykkyyttä tunnistaa, estää, häiritä, poistaa tai harhauttaa eri vaiheissa hyökkääjän toimintaa. Tällöin eri kyberuhkamallin vaiheiden osalta voidaan läpikäydä olemassa olevia kontrolleja ja miten ne auttavat esimerkiksi kyberhyökkäyksien tunnistamisessa tai estämisessä. Erityisesti täydelliset kontrollien puuttumiset tietyiltä kyberuhkamallin vaiheilta korostaisivat tärkeyttä korjata tällaiset puutteet (Lockheed Martin 2015, 6.). Alla olevaan kuvioon yksi on kuvattu Lockheed Martinin (2015, 5**)** kyberuhkamallin vaiheet, joita aikaisemmissa malleissa on jo esitelty. Lisäksi Lockheed Martinin mallissa on mukana myös tietoturvakontrollit, joilla esimerkiksi tiedustelu-vaiheen toimintaa voidaan tunnistaa kerätyn analytiikan kautta tai estää hyökkääjän tiedustelutoimintaa esimerkiksi palomuurin kautta. Virustorjuntasovellus voi myös toimia esimerkiksi asennusvaiheessa häiritsevänä kontrollina, jolloin haittaohjelman asentaminen epäonnistuu. Lisäksi toimintaa kohteessa voidaan huijata hyödyntämällä hunajapurkkeja, jolloin hyökkääjän toimista saadaan myös hälytys. Huijaamisen lisäksi myös hyökkääjän tiedonsiirtoa voidaan hidastaa rajoittamalla nettiyhteyden nopeutta (Lockheed Martin 2015, 5.).



KUVIO 1 Lockheed Martinin kybertappoketjun vaiheet.

Kyberuhkamallin avulla voidaan myös mitata kyberuhkatiedon tehokkuutta, sillä tavoitteena tulisi olla kyberuhkahyökkäysten tunnistaminen aina vain aikaisemmin. Erityisesti onnistuneiden kyberuhkahyökkäysten jälkeen tärkeätä olisi analysoida ja oppia missä vaiheessa kyberuhkahyökkäys tunnistettiin. Tämän myötä organisaatio voi parantaa kyberuhkatietonsa hyödyntämistä (Lockheed Martin 2015, 6.).

Kyberuhkamalli mahdollistaa myös organisaation resilienssin mittaamisen ymmärtämällä millaisia erilaisia kontrolleja organisaatiolla eri vaiheissa on ja missä vaiheessa aikaisemmat kyberuhkahyökkäykset on havaittu. Tämä mahdollistaa myös organisaation resilienssitason mittaamisen ja tavoitteena pitäisi olla kyberuhkahyökkäysten havaitseminen aikaisissa kyberuhkamallin vaiheissa. Lisäksi useiden kerroksellisten kontrollien hyödyntäminen korostaisi organisaation resilienssiä (Lockheed Martin 2015, 7.).

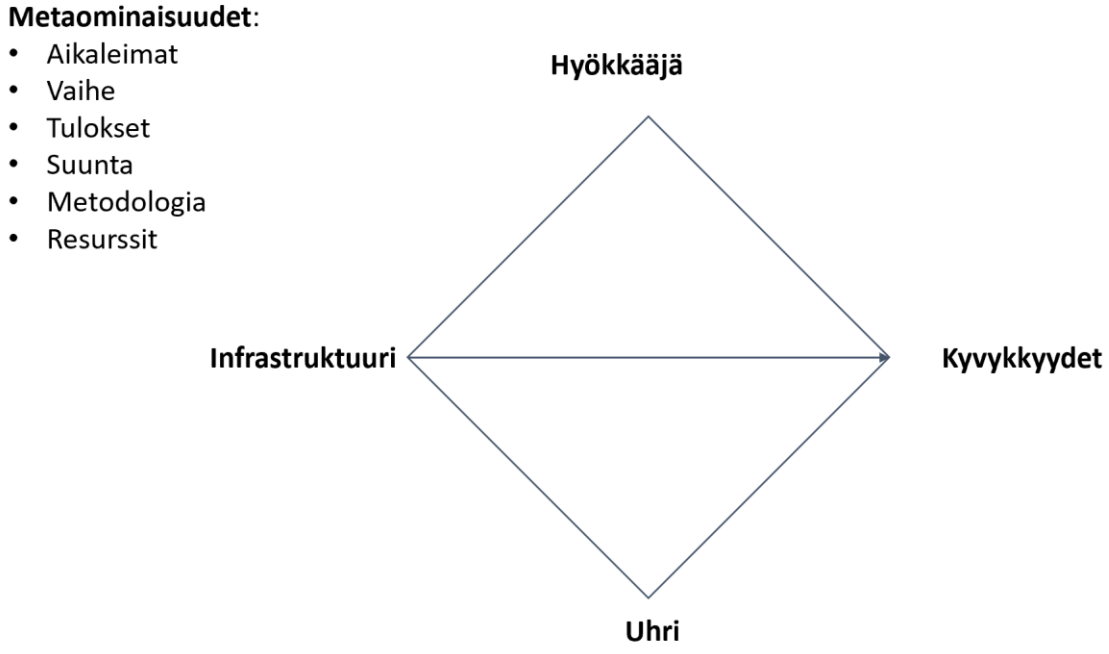
Kyberuhkamalli auttaa myös organisaation analyyttisen osaamisen mittaamisessa. Lockheed Martin (2015, 7) jatkaa korostamalla sitä, että kyberuhkahyökkäyksien osalta keskeistä on analysoida kuinka kyberuhkahyökkäys tapahtui ja syntetisoida mitä olisi voinut pahimmillaan tapahtua. Analyyttisen osaamisen osalta keskeistä on pyrkiä keräämään mahdollisimman kattava tietämys hyökkääjän osalta ja mitä hyökkääjä eri vaiheissa teki (Lockheed Martin 2015, 7).

Kyberuhkamallia voidaan hyödyntää myös eri aikaisten hyökkääjien tekniikoiden, taktiikoiden ja proseduurien tunnistamisessa ja tämän pohjalta laajempien hyökkäyskampanjoiden hahmottamisessa. Tekniikoiden, taktiikoiden ja proseduurien osalta organisaatio voi priorisoida ja mitata toimintaansa erilaisia hyökkääjien havaittuja tekniikoita, taktiikoita ja proseduureja vastaan ja parantaa erilaisia puolustuskeinoja. Tällainen aikaisempi kerätty data voi auttaa

tunnistamaan mahdollisia hyökkäyksiä, joissa samoja tekniikoita, taktiikoita ja proseduureja on käytetty sekä reagoimaan välittömästi. (Lockheed Martin 2015, 8.).

Toinen malli on Ertaul & Mouse (2018, 253) esittelemä timanttimalli, joka kuvaa erilaisia tapahtumia, joita Ertaul ym. (2018, 253) kutsuvat englanniksi eventeiksi. Mallissa hyökkääjä pyrkii kyvykkyydellään tunkeutumaan infrastruktuurin lävitse kohteeseensa. Keskeistä timanttimallissa on se, että hyökkääjä yrittää hyödyntää kyvykkyyttään kohdettaan vastaan omien asettamiensa tavoitteidensa saavuttamiseksi. Kyvykkyys kuvaa hyökkääjän käyttämiä työkaluja sekä tekniikoita. Infrastruktuuri kuvaa loogisia ja fyysisiä järjestelmiä, joita hyökkääjä käyttää hyökkäyksessään, kuten komentopalvelimet. Keskeistä on myös hyökkääjän osalta infrastruktuurin hyödyntäminen oman läsnäolonsa säilyttämiseksi kohteessa (Ertaul ym. 2018, 253.).

Timanttimallissa uhri kuvaa hyökkääjän valitsemaa kohdetta. Tällaiset kohteet voivat olla esimerkiksi erilaisia ihmisiä, organisaatioita, sähköpostiosoitteita, domaineja tai IP-osoitteita. Toisaalta malli korostaa ihmisten ja assettien erottamista analyysiä varten ja esimerkiksi ihmisen osalta tämä tarkoittaa sitä, että uhrin osalta erotetaan hyökkäyksen sosiaaliset vaikutukset teknisistä asseteista, kuten hyökkääjän hyödyntämistä haavoittuvuuksista (Ertaul ym. 2018, 254.). Alla olevassa kuviossa kaksi on Etraul ym. (2018, 253) esimerkkikuva timanttimallista, jossa on kuvattuna myös mallin metaominaisuuksia.



KUVIO 2 Ertaul ym. (2018) timanttimalli.

Yleensä timanttimallia käytetään löytämään ja tunnistamaan erilaisia tapahtumia. Mallia hyödyntämällä voidaan saada lisätietoa hyökkääjästä, hyökkääjän erilaisista operaatioista erilaisia uhreja kohtaan sekä voidaan tunnistaa erilaisia hyökkääjän kyvykkyyksiä tai uhreja. Keskeistä mallissa on se, että tapahtumat liittyvät toisiinsa muodostaen hyökkäysketjun, jota hyökkääjä toteuttaa. Mallin

metatieto auttaa kuvaamaan esimerkiksi missä vaiheessa hyökkääjä on, millaisia tuloksia hyökkääjä on voinut saavuttaa, millaista metodologiaa hyökkääjä käyttää ja millaisia resursseja hyökkääjällä on käytettävissä. Toisaalta mallissa yksittäinen timanttimalli kuvaa yksittäistä aikarajoitettua tiettyä vaihetta kyberhyökkäyksessä ja timanttimallissa yleensä suurin osa tapahtumista oletetaan sellaisiksi, ettei niitä tunneta varsinkaan ennen kuin koko kyberhyökkäys on jo ohitse (Ertaul ym. 2018, 253–254.).

MITREn ATT&CK malli on myös yksi kyberuhkamalleista, joka pohjautuu oikeisiin havaintoihin käytetyistä taktiikoista sekä tekniikoista. Malli kuvaa kyberhyökkäyksen eri vaiheita ja on lähtöisin projektista, jossa dokumentoitiin hyökkäyksen jälkeisiä havaintoja. Taulukossa yksi on kuvattuna MITREn ATT&CK-mallin vaiheita. Keskeistä oli dokumentoida hyökkääjän käyttämiä taktiikoita, tekniikoita ja proseduureja kohteena ollutta Windows-järjestelmää vastaan, jotta haitallista toimintaa voitaisiin paremmin havaita. Malli on muuttunut ja nykyään mukana on myös Linux- sekä MacOS-käyttöjärjestelmät ja malli kattaa hyökkääjän toimia myös mobiililaitteissa, pilviympäristössä tai teollisuusautomaatiossa (Blake ym. 2020, ii; 1.).

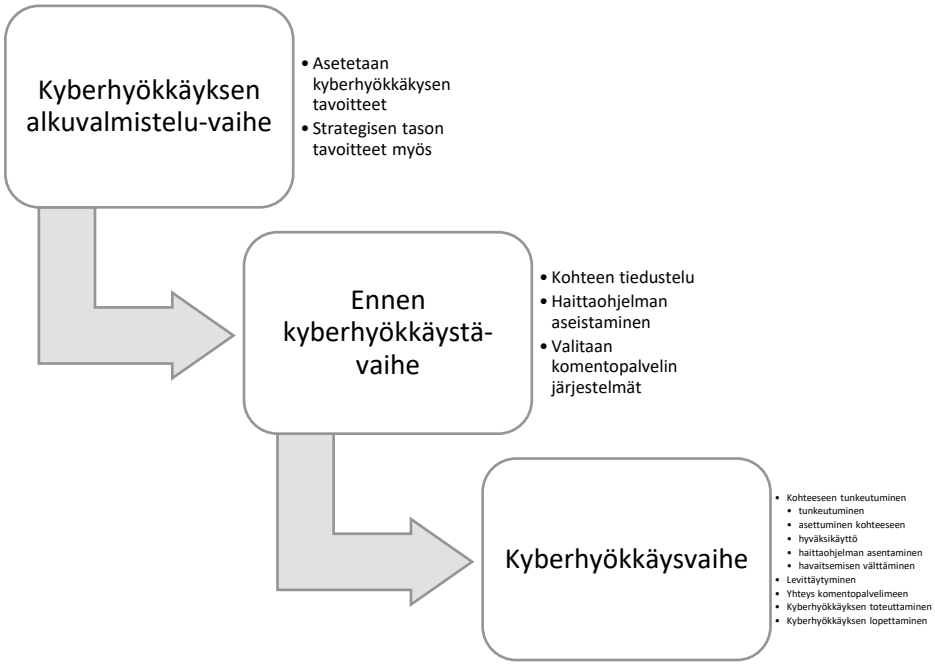
TAULUKKO 1 MITREn ATT&CK-mallin vaiheita ja vaiheiden kuvauksia.

Vaihe	**Kuvaus**
Tiedustelu	Hyökkääjä pyrkii keräämään hyödyllistä tietoa toimintansa kannalta.
Resurssien kerääminen	Hyökkääjä pyrkii hahmottamaan ja keräämään tavoitteensa mukaiset resurssit
Kohteeseen pääseminen	Hyökkääjä yrittää onnistua kohdejärjestelmään tunkeutumisessa.
Haitallisen koodin suorittaminen kohteessa	Hyökkääjä pyrkii suorittamaan haitallista ohjelmakoodiaan kohdejärjestelmässä
Pysyvyyden saavuttaminen	Hyökkääjä pyrkii ylläpitämään jalansijansa kohdejärjestelmässä.
Käyttöoikeuksien laajentaminen	Hyökkääjä pyrkii saamaan laajemmat oikeudet käyttäjäoikeudet.
Puolustuksellisten tietoturvakontrollien välttely	Hyökkääjä yrittää pysyä piilossa ilman, että puolustaja huomaa hyökkääjää järjestelmissään.
Käyttäjätunnuksien hankinta	Hyökkääjä yrittää varastaa käyttäjätunnuksia sekä salasanoja
Kohdejärjestelmän havainnointi	Hyökkääjä pyrkii määrittämään mikä on kohdejärjestelmä.
Siirtyminen kohdejärjestelmässä	Hyökkääjä pyrkii siirtymään kohdejärjestelmässä eri kohteisiin ja kohteiden välillä.
Kerääminen	Hyökkääjä kerää mielenkiintoiseksi katsomaansa dataa.
Komentaminen ja kontrollointi	Hyökkääjä yrittää luoda yhteyden asettamiinsa komentopalvelimiin, jotta voisi ohjailla toimintaansa kohteessa.
Tiedon poiskuljettaminen	Hyökkääjä yrittää siirtää keräämäänsä tietoa pois kohdejärjestelmästä
Vaikuttaminen	Hyökkääjä yrittää manipuloida tai tuhota kohdejärjestelmää tai sen dataa.

Korkealla tasolla MITREn ATT&CK-malli on behavioristinen malli, joka kuvaa hyökkääjän käyttämiä taktiikoita, tekniikoita, alitekniikoita sekä dokumentoi hyökkääjän käyttämät tekniikat, proseduurit ja muun metadatan. Taktiikat kuvaavat hyökkääjän lyhytaikaisia hyökkäyksen tavoitteita. Tekniikat kuvaavat keinoja, joilla hyökkääjä on pyrkinyt saavuttamaan tavoitteensa. Alitekniikat kuvaavat vielä tarkemmalla teknisellä tasolla keinoja, joilla hyökkääjä on pyrkinyt saavuttamaan taktiset tavoitteensa. Mallin ensimmäinen versio on vuodelta 2013 (Blake ym. 2020, 1). Lehto (2022, 122) toteaa, että mallissa on kaksi päävaihetta eli ennen hyökkäystä vaihe ja itse hyökkäysvaihe. Ennen hyökkäystä vaiheessa kuvataan sekä hyökkäyksen tiedustelu että aseistaminen. Itse hyökkäysvaiheessa kyberhyökkäys on mallinnettu ja mallissa kuvataan yksitoista erilaista taktiikkaa sekä yksi kyberhyökkäyksen päämäärä (Lehto 2022, 122.).

Lehto (2022, 122) toteaa yhteenvetona, että useita erilaisia kyberuhkamalleja APT-hyökkäyksiin liittyen on siis kehitetty. Olemassa olevilla kyberuhkamalleilla on yhteistä mutta myös eroavaisuuksia erityisesti, kuinka yksityiskohtaisesti kyberhyökkäyksen yksityiskohtia eritellään. Osa kyberuhkamalleista sisältävät yksityiskohtaisia kuvauksia hyökkäyksistä, mutta osa kyberuhkamalleista keskittyvät vain kyberhyökkäyksien pääkohtiin (Lehto 2022, 125.).

Lehto (2022, 125) esittelee yleisen kyberuhkamallin, joka pohjautuu erilaisiin jo olemassa olleisiin kyberuhkamalleihin. Tämä yleinen kyberuhkamalli on kuvattuna alla olevassa kuviossa kolme.



KUVIO 3 Yleinen kyberhyökkäysmalli (Lehto 2022).

Mallissa kyberhyökkäys on jaettu kolmeen vaiheeseen, jotka ovat kyberhyökkäyksen alkuvalmisteluvaihe, ennen kyberhyökkäystä ja itse kyberhyökkäysvaihe (Lehto 2022, 125). Alkuvalmistelussa kyberhyökkääjä asettaa hyökkäyksensä tavoitteet ja Lehto (2022, 126) korostaa myös strategisen

tason päätöksiä eli kuinka hyökkääjä tekee parhaimman mahdollisen päätöksen erilaisten kyberhyökkäykseen liittyvien tekijöiden asettaessa erilaisia rajoitteita. Keskeistä on huomioida kuinka APT-hyökkäys liittyy muihin hyökkääjän strategisiin tavoitteisiin (Lehto 2022, 126).

Ennen kyberhyökkäystä vaiheessa hyökkääjä keskittyy kohteen tiedusteluun sekä APT-hyökkäyksessä käytettävän haittaohjelman aseistamiseen. Vaiheen aluksi hyökkääjä kerää tietoa hyökkäyskohteesta ja kuinka hyökkäystavoitteet voitaisiin saavuttaa. Keskeistä on kerätä mahdollisimman paljon tietoa hyökkäyskohteesta (Lehto 2022, 126.).

Seuraavana hyökkääjä siirtyy yksityiskohtaisempaan kohteen tarkasteluun keräämällä tietoa esimerkiksi kohteen ICT-järjestelmistä ja niissä mahdollisesti olevista haavoittuvuuksista. Keskeistä tässä vaiheessa on löytää mahdollisesti hyökkääjän hyödynnettävissä oleva haavoittuvuuksia sisältävä sovellus, josta kohteeseen voitaisiin tunkeutua (Lehto 2022, 126.).

Seuraavana ennen kyberhyökkäystä vaiheessa hyökkääjä keskittyy haittaohjelman tai useiden haittaohjelmiensa aseistamiseen eli hyökkääjä valitsee mitä haavoittuvuutta hyväksikäytetään ja kehittää haittaohjelmansa. Kehitetty haittaohjelma voi olla erillinen nettisivusto, jossa kohteen halutaan vierailevan tai haittaohjelma, joka hyödyntää kohteessa olevien ICT-järjestelmien haavoittuvuuksia. Kehitetty haittaohjelma voi sisältää kohteeseen vietävän itse kehitetyn haitallisen sisällön tai haitallinen sisältö on voitu hankkia muualta, kuten Dark webistä. Haittaohjelman lisäksi hyökkääjä valitsee ja valmistelee käytettävän haittaohjelman tarvitsemat komentoyhteys- ja kontrollipalvelinjärjestelmät (Lehto 2022, 126.).

Itse kyberhyökkäysvaihe koostuu Lehdon (2022, 126) yleisessä mallissa viidestä eri vaiheesta. Ensimmäisenä kohteeseen tunkeudutaan ja Lehdon yleisessä mallissa tämä vaihe jaetaan vielä viiteen erilaiseen alivaiheeseen. Nämä alivaiheet kuvaavat hyökkääjän tunkeutumista kohteeseen, kohteeseen asettumista, hyväksikäyttöä, jossa hyökkääjä haavoittuvuuksia hyödyntämällä tavoittelee esimerkiksi ylläpito-oikeuksia. Toisaalta haavoittuvuuksia voidaan kohdentaa myös ihmisiin, teknologiaan tai kohteessa oleviin prosesseihin (Lehto 2022, 126.).

Neljäs alivaihe keskittyy haittaohjelman asentamiseen eli tavoitteena on asentaa varsinainen haittaohjelma kohteeseen ja varmistaa kohteessa pysyminen. Lisäksi hyökkääjä tavoittelee esimerkiksi etäkäyttöyhteyttä kohteeseen tai takaoven asentamista hyökkäystavoitteidensa laajentamiseksi. Viimeisenä alivaiheena on havaitsemisen välttäminen ja toisin kuin esimerkiksi kiristyshaittaohjelmien tapauksessa, hyökkääjän läsnäoloa kohteessa pyritään piilottamaan mahdollisimman pitkään (Lehto 2022, 126–127.). Lehto (2022, 127) huomauttaakin, että yleensä APT-hyökkäykset pysyvät piilossa keskimäärin viisi vuotta ennen kiinnijäämistä.

Tunkeutumisen jälkeen hyökkääjän tavoitteena yleisessä kyberhyökkäysmallissa on levittäytyminen kohteessa laajemmalle. Keskeistä hyökkääjän kannalta on hyökkäyspinta-alansa kasvattaminen sekä käyttöoikeuksiensa ja hallussaan olevien resurssien saaminen laajemmalti kohteessa. Tämän jälkeen hyökkääjän tavoitteena on varmistaa haittaohjelman yhteys komentopalvelimen

kanssa. Komentopalvelimen kautta hyökkääjä voi ohjailla haittaohjelmaansa ja säilyttää läsnäolonsa kohdejärjestelmissä (Lehto 2022, 127.).

Seuraava vaihe yleisessä kyberhyökkäysmallissa on varsinaisen hyökkääjän asettaman kyberhyökkäyksen tavoitteen toteuttaminen. Tavoite voi vaihdella eri kyberhyökkäyksien kesken ja esimerkiksi Stuxnet APT-hyökkäyksessä tavoitteena oli vahingon aiheuttaminen. Vahingon aiheuttamisen sijasta tavoitteena voi olla erilaisen kohdejärjestelmän salaisenkin tiedon kerääminen ja siirtäminen hyökkääjän haltuun tai tiedon manipulointi tai jopa tuhoaminen (Lehto 2022, 127.).

Viimeinen vaihe on kyberhyökkäyksen lopettamiseen liittyvät toimenpiteet ja hyökkääjän tavoitteena on kadota jälkiä jättämättä. Tällöin kyberhyökkääjä pyrkii peittämään ja siivoamaan kaikki kyberhyökkäyksensä jäljet tietojärjestelmistä ja erilaisista logeista. Toisaalta viimeiseen vaiheeseen voi liittyä myös siirtyminen piiloon ja kyberhyökkäys voi muuttua aktiivisemmaksi, mikäli hyökkääjä havaitsee jotain uutta ja omalta kannaltaan mielenkiintoista. Tällöin kyberhyökkääjän tavoitteena on myös sisällyttää useita erilaisia takaovia eri komentopalvelimiinsa, jolloin läsnäoloa voidaan jatkaa, vaikka jotain kyberhyökkääjän toimista paljastuisi (Lehto 2022, 127.).

2.8 Kyberhyökkäyksen havaitseminen

Luvussa kuvaillaan lyhyesti millaisia haasteita kyberhyökkäyksen havaitsemiseen liittyy erityisesti APT-haittaohjelmien osalta. Lisäksi luvussa esitellään IoC-, IoB- ja IoA-termistöt. Xing, Jiang & Jia (2021, 185) huomauttavat, että erilaisia kyberhyökkäyksiä on loputon määrä ja ne hyödyntävät useita erilaisia teknisiä keinoja. APT-haittaohjelmien osalta haasteena on erityisesti se, että ne ovat edistyneitä ja voivat hyödyntää sosiaalista manipulointia, nollapäivähaavoittuvuuksia, piilossa tapahtuvaa viestintää ja jopa koneoppimista tavoitteidensa saavuttamisessa. Usein APT-hyökkäys on myös yhdistelmä näitä eri keinoja (Xing ym. 2021, 187.).

Toinen APT-haittaohjelmiin liittyvä haaste on se, että APT-haittaohjelmien toiminta on usein pitkäkestoista. Hyökkääjä voi olla kohdejärjestelmässä jopa useita vuosia ja tarkoituksena on piilottaa oma toiminta mahdollisimman pitkään. Kolmantena APT-haittaohjelmat usein aiheuttavat suuria vahinkoja, sillä kohteet ovat yleensä valtion organisaatioita, infrastruktuuria tai suuryrityksiä (Xing ym. 2021, 188.).

Villalón-Huerta, Ripoll-Ripoll & Marco-Gisbert (2022, 1) huomauttavat, että haittaohjelmien havaitsemisessa Indicators of Compromise eli IoCt ovat kyberuhkatiedustelun osalta keskeisiä keinoja havaita haittaohjelmia. IoC mahdollistavat sekä hyökkääjän käyttämien työkalujen tai artefaktien sekä taktiikoiden, tekniikoiden ja proseduurien tunnistamisen ja hyödyntämisen. Toisaalta näiden osalta hyökkääjät usein huomioivat näiden käyttämisen kyberuhkatiedustelussa ja muokkaavat haittaohjelmiaan tarpeen mukaisesti. Tällöin IoCt ovat usein lyhytikäisiä (Villalón-Huerta ym. 2022, 1.). Villalón-Huerta ym. (2022, 1)

huomauttavatkin, että tämän johdosta kyberuhkatiedustelussa käytettävät IoC ovat kaikista helpoin tapa hyödyntää tietoa jo tunnistetuista haittaohjelmista sekä haittaohjelmien tekijöiden käyttämistä taktiikoista, tekniikoista ja proseduureista.

IoC voidaan luokitella kolmeen eri luokkaan pohjautuen kompleksisuuteen sekä niiden sisältämään dataan. Atomiset indikaattorit sisältävät esimerkiksi kyberhyökkäykseen liittyvät IP-osoitteet sekä domainnimet. Keskeistä atomisten indikaattoreiden osalta on se, ettei niitä voida pilkkoa pienemmiksi ja tällaiset indikaattorit säilyttävät merkityksensä kyberhyökkäystä analysoitaessa eli esimerkiksi tiedetään miten tietty IP-osoite kytkeytyisi kyberhyökkäystä epäiltäessä (Villalón-Huerta ym. 2022, 2.).

Laskennalliset indikaattorit kuvaavat kyberhyökkäykseen liitettyä dataa, kuten esimerkiksi hyökkääjän käyttämien haittaohjelmien tunnistearvoja. Käytökselliset indikaattorit koostuvat sekä atomisista että laskennallisista indikaattoreista ja esimerkki tällaisesta on hyökkääjien usein käyttämä kalastelusähköpostiviesti, jonka linkin avaamalla hyökkääjälle avautuisi pääsy kohdejärjestelmään (Villalón-Huerta ym. 2022, 2.). Tällaiset havaitut indikaattorit kuvailevat hyökkääjän taktiikoita, tekniikoita ja proseduureja ja Villalón-Huerta ym. (2022, 2) jatkavat huomauttamalla, että nämä kuvaavat myös hyökkääjän toimintamallia.

Kyberuhkatiedustelun osalta käytökselliset indikaattorit liittyvät operationaaliseen kyberuhkatiedusteluun ja atomiset sekä laskennalliset indikaattorit liittyvät taktiseen kyberuhkatiedusteluun. Keskeistä on kuitenkin se, että kaikki indikaattorit ovat keskeisiä kyberhyökkäyksien havaitsemisessa, mutta yleensä taktisen tason indikaattorit ovat lyhytaikaisia, kun operationaaliseen kyberuhkatiedusteluun liittyvät indikaattorit ovat pidempi-ikäisiä (Villalón-Huerta ym. 2022, 2.). Toisaalta useat organisaatiot voivat mieltää atomiset ja laskennalliset indikaattorit kyberuhkatiedustelun osalta kaikista arvokkaimpana tietona, sillä tällaista indikaattoritietoa voidaan helposti hyödyntää esimerkiksi erilaisissa IDS-tyylisissä laitteistoissa tai ohjelmistoissa. Siirryttäessä operationaaliselle tai strategiselle tasolle, korostuu ihmisten tekemä työ (Villalón-Huerta ym. 2022, 3.).

IoC osalta Villalón-Huerta ym. (2022, 6) huomauttavat, että yleisimmin erilaiset tiivistearvot, IP-osoitteet ja domainnimet ovat auttaneet tunnistamaan kyberhyökkäyksen, jossa hyökkääjä on onnistunut saamaan jalansijan. Toisaalta hyökkääjän osalta tällaisten omien jälkien muuttaminen on helppoa (Villalón-Huerta ym. 2022, 6). Villalón-Huerta ym. (2022, 6) huomauttavatkin, että mikäli hyökkääjä muuttaa näitä indikaattoreitaan, puolustajan havaitsemiskyvykkyydestä vähenee jopa 65 prosenttia. Lisäksi IoC ovat lähes hyödyttömiä APT-haittaohjelmien havaitsemisessa (Villalón-Huerta ym. 2022, 6).

APT-haittaohjelmien havaitsemisen osalta Villalón-Huerta ym. (2022, 6) korostavat käytöksellisten indikaattoreiden merkitystä ja tällaisen kyberuhkatiedon jakamista. Tällöin korostuu hyökkääjän käyttämien taktiikoiden ja tekniikoiden tunnistaminen, vaikka hyökkääjä muokkaisi tiivistearvoja, IP-osoitteita tai domainnimiä. Hankaluutena on vain se, että tällaisen kyberuhkatiedon käsitteleminen vie enemmän aikaa verrattuna esimerkiksi automatisoituun

tiivistearvojen laskentaan, IP-osoitteiden tai domainnimien tunnistamiseen (Villalón-Huerta ym. 2022, 6).

IoC:llä on kuitenkin useita heikkouksia, kuten hyökkääjän kyky muuttaa työkalujaan, erilaisten IP-osoitteiden tai domainnimien hyödyntäminen. Hyökkääjä voi myös kehittää omia työkalujaan tai muuttaa nykyisiä työkalujaan, jolloin hyökkääjän käyttämät työkalut eivät jää kiinni. Hyökkääjät voivat myös ottaa kohteeksi erilaiset kyberuhkatietoa jakavat tietokannat ja tuottaa niihin erilaista hälyä, esimerkiksi lisäämällä heidän tekemiään vääriä indikaattoreita. Tällaiset väärät indikaattorit vaativat puolustajien osalta manuaalisesti tehtävää siivoamista ja voi johtaa siihen, että erilaisten indikaattoreiden osalta niiden hyödyllisyys ja ylipäätänsä luottamus indikaattoripohjaiseen kyberuhkatietoon vähenee (Anashkin & Zhukova, 2021, 18.).

Anashkin ym. (2021, 18) huomauttavat myös, että niin sanotut tiedostomattomat hyökkäystekniikat ovat myös haaste IoC:lle. Käytettäessä tiedostotonta hyökkäystekniikkaa hyökkääjä ei lähetä haittaohjelmaa kohteeseen suoraan, vaan haittaohjelma ladataan esimerkiksi PowerShellin kautta. IoC-tyylisten indikaattoreiden osalta haaste on myös se, että niitä yleensä käytetään reaktiivisesti. Tällöin onnistunut kyberhyökkäys on paljastunut erilaisten todisteiden ja indikaattoreiden pohjalta. Erityisesti kehittyneiden haittaohjelmien osalta IoC ovat heikkoja reagoimaan proaktiivisesti ja estämään kyberhyökkäystä. Parempia IoC ovat silloin kun hyökkääjät turvautuvat jo tunnettuihin indikaattoreihin (Anashkin ym. 2021, 18.).

IoC-tyylisten indikaattoreiden puutteiden johdosta käytössä on myös IoA- ja IoB- tyyliset indikaattorit. IoA on lyhenne sanoista Indicators of Attack ja kuvaa tiettyä toimintojen joukkoa, joka on yleensä epänormaalia, harvinaista tai epäilyttävää toimintaa kohdejärjestelmässä. Esimerkiksi mikäli Windows-kohdejärjestelmässä järjestelmän tapahtumavalvonnan logien kerääminen lopetetaan ja tämän jälkeen on muokattu järjestelmän rekisteriä niin, että tietty sovellus on asetettu automaattisesti käynnistyväksi, voi tällainen toiminta viitata kohdennettuun hyökkäykseen (Anashkin ym. 2021, 18.). Crowdstrike (2021) korostaa IoAn osalta sitä, että tarkoituksena on keskittyä hyökkääjän tavoitteisiin eikä siihen millaista haittaohjelmaa hyökkääjä tällä kertaa hyödyntää. Esimerkiksi pankkiryöstäjien osalta ensimmäisenä ryöstäjät tutustuisivat valittuun kohdepankkiin ja ottaisivat selvää siitä, millaisia varashälyttimiä kohteessa olisi, millainen pankkiholvi kohteessa olisi ja miten kohteen kameravalvonta olisi toteutettu. Tällaisessa tiedusteluvaiheessa keskeistä olisi löytää heikkouksia ja tunnistettujen heikkouksien pohjalta ryöstäjät suunnittelisivat parhaan ryöstöajan ja millaisella tavalla pankkiryöstö kannattaisi toteuttaa. Tämän jälkeen ryöstäjät suuntaisivat kohdepankkiin ja vahingoittaisivat hälytinlaitteistoa ja siirtyisivät murtautumaan pankkiholviin. Pankkiholvin avauduttua, ryöstäjät ottaisivat saalinsa mukaansa ja pakenisivat mahdollisimman vähällä huomiolla ja vaihtaisivat pakoautoa jossain kohtaa. Pankkiryöstöesimerkissä IoA ovat siis joukko erilaisia tehtäviä ja tapahtumia, joiden on onnistuttava, jotta pankkiryöstö onnistui. Keskeistä on se, että yksinään tällaiset tapahtumat eivät ole epäilyttäviä, mutta peräkkäisinä askelina voivat olla epäilyttäviä eli esimerkiksi tiedusteltaessa

ulkopuoliset huomaavat, että pankin järjestelmiä kuvataan liian innokkaasti tai valvontakameroiden sijaintia selvitetään poikkeuksellisella mielenkiinnolla (Crowdstrike 2021.).

Kybermaailmassa IoA on vastaavasti joukko erilaisia askelia, joissa hyökkääjän on onnistuttava kohdejärjestelmään tunkeutumiseksi. Esimerkiksi kohdennetussa sähköpostikalastelussa hyökkääjän on saatava kohde toimimaan hyökkääjän haluamalla tavalla esimerkiksi avaamaan tietty viattoman näköinen haittaohjelman sisältävä tiedosto tai vierailemaan haittaohjelman sisältävällä sivustolla. Tämän jälkeen haittaohjelman on onnistuttava saastuttamaan kohteen tietokone ja suorittamaan hyökkääjän haluamia toimia, kuten pysymään havaitsemattomana kohteessa. Seuraavana hyökkääjän haittaohjelman on otettava jossain vaiheessa yhteyttä komentopalvelimeen ja kerrottava olevansa valmiina siirtymään seuraavaan vaiheeseen kyberuhkamallissa (Crowdstrike 2021.). Peilattaessa tällaista toimintaa Lehdon (2022) yleiseen kyberuhkamalliin hyökkääjän olisi onnistuttava viidessä erilaisessa alivaiheessa kohteeseen tunkeutumiseksi eli tunkeuduttava kohteeseen, onnistuttava asettumaan kohteeseen, hyväksikäyttämään, asentamaan varsinaisen haittaohjelman ja varmistamaan kohteessa pysyminen sekä etäkäyttöyhteyden varmistaminen tai takaportin asentaminen. Viimeiseksi näistä alivaiheista hyökkääjän tavoitteena on havaitsemisen välttäminen (Lehto 2022, 126–127.).

IoA siis kuvaavat tällaisia askelia sekä hyökkääjän asettamia tavoitteita ja mitä hyökkääjä haluaa saavuttaa. IoAt eivät siis keskity hyökkääjän osalta kuvaamaan millaisia haittaohjelmia hyökkääjä hyödyntää hyökkäyksessään. Sen sijaan IoAn osalta kannatta kiinnittää huomiota erilaisiin peräkkäisiin askeliin ja pyrkiä tunnistamaan milloin jotkin askeleet ovat epäilyttäviä ja voivat viitata haittaohjelman toimintaan. Hyökkääjän toimien tunnistamisessa IoA-tyyliset indikaattorit ovat IoCtä parempia proaktiivisuudessaan, sillä hyökkääjien osalta taktiikat, tekniikat ja proseduurit ovat yleensä samoja ja näitä on hyökkääjän vaikeampi muuttaa (Anashkin ym. (2021, 18). Kost (2022) havainnollistaa IoA ja IoC eroavaisuuksia mainitsemalla esimerkkejä. Esimerkkinä IoAsta mainitaan tietoliikenne maihin, joiden kanssa ei ole esimerkiksi asiakkuuksia tai käyttäjät kirjautuvat järjestelmään useilta eri alueilta. IoC-indikaattorit ovat vastaavasti käytettyjen haittaohjelmien tiivisteitä tai komentopalvelimen IP-osoitetietoja, jotka ovat staattisia verrattuna dynaamisiin IoA-indikaattoreihin. (Kost 2022.)

Anashkin ym. (2021, 19) mainitsevat myös Indicators of Behavior eli IoB. IoB kuvaa digitaalista käyttäytymistä, jota voidaan valvoa organisaatiossa. IoB indikaattorit koostuvat joukosta toimintaa, joka voi olla haitallista tai epäilyttävää kuten IoA. Mutta IoAn ja IoBn välillä on eroavaisuuksia. IoA keskittyy hyökkääjän taktiikoihin, tekniikoihin ja proseduureihin mutta IoB keskittyvät enemmän mahdollisesti haitallisiin toimiin. Tällaisia mahdollisesti haitallisia toimia ovat esimerkiksi ulkoisen massamuistin hyödyntäminen ja tietojen siirtäminen sinne, käyttäjän sisäänkirjautuminen useisiin erilaisiin työpisteisiin, etäyhteyksien luomiset tai erilaisten ylläpitosovellusten käyttäminen. Tällaiset mahdollisesti haitalliset toimet ovat siis laajempia kuin IoA ja voivat viitata esimerkiksi

sisäpiiriläiseen, piittaamattomuuteen organisaation tietoturvasäännöksistä tai esimerkiksi luottamuksellisen tiedon vuotamiseen (Anashkin ym. 2021, 19.).

Anashkin ym. (2021, 21) mainitsevat UBEA–järjestelmän, joka on lyhenne sanoista User Behavior and Entity Analytics. UBEA-järjestelmällä voidaan tunnistaa erilaisia tietoturvauhkia pohjautuen käyttäjän toimien analysointiin tai laitteen taikka sovelluksen toimintaan. Järjestelmä seuraa erilaisia IoB-indikaattoreita ja havaitsee esimerkiksi käyttäjän kirjautumisen järjestelmään esimerkiksi työkaverinsa tunnuksella tai käyttöoikeuksilla. Tällainen IoB indikaatio liittyen esimerkiksi työasemaan, jota käyttäjä ei ole koskaan aikaisemmin käyttänyt, voi aiheuttaa hälytyksen epäilyttävästä toiminnasta. Tällainen UBEA–järjestelmä voi auttaa myös sisäpiiriläisen epäilyttävän käytöksen havaitsemisessa (Anashkin ym. 2021, 21.).

3 TUTKIMUKSEN KOHTEENA OLEVAT APT-RYHMITTYMÄT

Luvussa kuvataan erilaiset APT-ryhmät, joiden avulla pyritään vastaamaan tutkimuskysymyksiin. Kuvauksissa keskiössä on yksittäinen hyökkäys, jonka osalta esimerkiksi taktiikat, tekniikat, proseduurit sekä työkalut pyritään kuvailemaan. Aineistoksi valikoitui paljolti tietoturvayhtiöiden tekemiä analyysejä erilaisista APT-ryhmien haittaohjelmahyökkäyksistä ja heidän käyttämistä työkaluistaan.

3.1 Advanced Persistent Threat APT1

Luvussa kuvaillaan aluksi APT1-ryhmittymää ja siihen liitettyjä APT-hyökkäyksiä. APT1-ryhmittymän hyökkäyksistä tarkempaan analyysiin otetaan yksi, jonka osalta pyritään vastaamaan tutkimuskysymyksiin. Oosthoek ym. (2021, 302) kuvailevat APT1-ryhmän liittyvän Kiinan armeijan yksikköön 61398. APT1-ryhmän osalta Oosthoek ym. (2021, 302) jatkavat toteamalla, että APT1-ryhmä on liitetty erilaisiin hyökkäyksiin ainakin 150 organisaatioon ja erilaiset hyökkäyskampanjat ovat olleet pitkäkestoisia. Oosthoek ym. (2021, 303) jatkavat APT1-ryhmän olleen myös ensimmäisiä julkisesti paljastettuja APT-toimijoita ja APT1-ryhmän osalta heidän käyttämänsä domain- sekä IP-osoitteet julkistettiin yhdessä tiedostojen tiivistearvojen kanssa, jolloin esimerkiksi kyberuhkatiedustelut voivat helpommin havaita APT1-ryhmän jälkiä.

Mandiant (2014, 20) huomauttaa, että APT1-ryhmä on ollut toiminnassa vähintään vuodesta 2006 alkaen. APT1-ryhmän osalta merkittävää on ollut se, että kohteena on ollut useita organisaatioita yhtä aikaa ja kohdejärjestelmissä ollaan oltu pitkiäkin aikoja. Keskeistä on ollut erilaisten immateriaalinalaisten aineistojen varastaminen kohdeorganisaatioista. Lisäksi kohdeorganisaatiot ovat suurimmaksi osaksi olleet englantia puhuvista maista. (Mandiant 2014, 20–21.) Mandiant (2014, 22) huomauttaa, että APT1-ryhmän hyökkäyksien kohteena on ollut 150 organisaatiota, jolloin APT1-ryhmä ei keskity tiettyihin yritysaloihin. Lisäksi

näin suuri määrä organisaatioita ja useat yhtä aikaiset operaatiot viittaavat siihen, että APT1-ryhmällä on huomattavat resurssit käytössään (Mandiant 2014, 22).

APT1-ryhmän osalta Mandiant (2014, 27) on laatinut oman hyökkäysmallin ryhmän toimista. APT1-ryhmän osalta ensimmäisenä kohteen valinnan jälkeen on Spearphising tekniikan käyttäminen. Tällöin sähköpostissa voi olla haitallinen liitetiedosto tai linkki haitalliseen nettisivustoon. APT1-ryhmä myös huomioi kohdeorganisaation ja on luonut ilmaisiin sähköpostipalveluihin sähköpostitilejä henkilöille, jotka kohdehenkilö mieltää tuttuina. Nämä sähköpostitilit ovat yleensä työkavereiden, yrityksen johdon tai alihankkijoiden nimissä. Mandiant (2014, 28;30) huomauttaa, että kohdehenkilön järjestelmään yritetään ujuttaa haitallinen takaovi, jotka ovat yleensä räätälöityjä, mutta APT1-ryhmä on myös käyttänyt Poison Ivy tai Gh0st RAT-takaoviohjelmistoja. Karkeana jakona Mandiant (2014, 30) on tehnyt APT1-ryhmän takaovien osalta jaon keihäänkärkija normaaleihin takaoviohjelmistoihin. Näistä keihäänkärkitakaoviohjelmistot sisältävät mahdollisimman vähän toiminnallisuutta ja tarkoituksena on saada pieni jalansija kohdeorganisaatiosta. Keihäänkärkitakaoviohjelmistojen tavoitteena on tiedonkerääminen ja monimutkaisempien takaoviohjelmistojen lataaminen (Mandiant 2014, 31.).

APT1-ryhmän normaalit takaoviohjelmistot sisältävät enemmän toiminnallisuutta ja hyökkääjä voi tiedonkeräämisen ja tiedostojen lataamisen lisäksi ottaa etäyhteyksiä, kerätä salasanoja, muokata sekä järjestelmän rekisteriä että erilaisia prosesseja. Useat tällaiset takaoviohjelmistot salaavat liikenteensä havaitsemisen vaikeuttamiseksi ja käyttävät normaaleja nettiliikenteen protokollia (Mandiant 2014, 32–33.).

Käyttöoikeuksien laajentaminen ei APT1-ryhmän osalta eroa huomattavasti muista APT-ryhmistä, vaan käyttää yleisesti käytettäviä ohjelmia esimerkiksi salasanojen tiivisteiden hankkimiseen. Näitä ohjelmia ovat esimerkiksi cachedump, fgdump, gsecdump, lslsass, mimikatz, pass-the-hash-toolkit, pwdump7 tai pwdumpX-ohjelmat. Cachedump on saatavilla Githubista ja on osa Metasploit-ohjelmistoa. Ohjelmalla voidaan ottaa talteen kymmenen viimeksi välimuistiin laitettua salasanojen hash-arvoa (Mandiant 2014, 36).

fgdumpin viimeisin versio on vuodelta 2008 ja tarkoitettu tietoturvan auditointiin. Ohjelmalla voidaan saada Windowsin salasanojen hash-arvoja, joita voidaan yrittää brute force eli kokeilemalla kaikkia vaihtoehtoja-taktiikalla murtaa. gsecdump on myös erilaisten salasanojen hash-arvojen kaiveluun tarkoitettu sovellus. lslsass vuorostaan palauttaa aktiivisen session salasanan hash-arvon Windowsin lsass-prosessilta. Mimikatz on avoimen lähdekoodin ohjelmisto, jota yleensä käytetään käyttäjän salasanan ohittamiseen. Esimerkiksi Mimikatzilla annetaan jonkin käyttäjän käyttämän salasanan hash-arvo, jolloin Windowsiin voidaan kirjautua sisään. Tosin enää salasanojen hash-arvoja ei tallenneta NTLM:nä. (Mandiant 2014, 36.)

Pass-the-hash-toolkitin avulla on myös mahdollista kirjautua tietokonejärjestelmään vaikkei tietäisi käyttäjän selväsanaista salasanaa. pwdump7 ja pwdumpX ovat myös salasanojen hash-arvojen saamiseen tarkoitettuja ohjelmistoja. pwdump7 keskittyy SAM ja SYSTEM tiedostoihin ja kaivaa näistä

salasanojen hash-arvoja. pwdumpX mahdollistaa salasanojen hash-arvojen saamisen muilta kuin paikallisesta tietokoneesta. (Mandiant 2014, 36.)

Sisäisessä tiedusteluvaiheessa APT1-ryhmä hyödyntää pääsääntöisesti käyttöjärjestelmän omia ohjelmistoja (Mandiant 2014, 35). Mandiant (2014, 35) huomauttaa, että APT1-ryhmä ei tämän suhteen eroa muista APT-ryhmistä. Siirtyminen kohteessa vaiheessa APT1-ryhmä hyödyntää käyttöjärjestelmän tarjoamia komentoja, joiden avulla verkkoasemia voidaan tutkia. Myös käyttöjärjestelmän omia ohjelmistoja voidaan hyödyntää, kuten ”Tehtävien ajoitusta” tai Microsoftin psexec-ohjelmistoa, jolla voidaan suorittaa komentoja etänä. (Mandiant 2014, 36.) Mandiant (2014, 36) huomauttaa, että APT1-ryhmän suorittamana tällaista toimintaa on vaikeata erottaa normaaleista järjestelmän ylläpitäjien toimista.

Läsnäolon osalta APT1-ryhmittymä on hyödyntänyt erilaisia takaovia, jolloin yhden paljastuminen ei keskeytä toimintaa. APT1-ryhmittymä on myös hyödyntänyt vuotaneita tai muulla keinoin hankittuja käyttäjätunnuksia ja esimerkiksi kirjautunut intraverkon sivustoille tai kohteen sähköpostijärjestelmään.

Viimeisenä asetettujen tavoitteiden vaiheessa APT-ryhmittymä on pyrkinyt pakkaamaan haluamiaan tiedostoja Rar-pakkausmuotoon. Salasanalla suojattuina tällaisia on ollut helpompaa siirtää APT1-ryhmittymän hallitsemille palvelimille. (Mandiant 2014, 36–37.)

3.2 Advanced Persistent Threat Stuxnet

Luvussa tarkoituksena on kuvailla Stuxnet APT-haittaohjelmaa. Stuxnetistä DeVore ym. (2017, 40) toteavat sen olleen APTnä hienostunut muoto kyberaseesta. Stuxnetin osalta DeVore ym. (2017, 40) nimeävät tekijöiksi Yhdysvallat sekä Israelin, mutta Alenezi ym. (2020, 330) ovat varovaisempia ja uskovat Yhdysvaltojen sekä Israelin olleen todennäköiset Stuxnetin kehittäjät. Stuxnet oli haittaohjelmista mato, jonka tarkoituksena oli vaikuttaa uraanin rikastamisessa käytettäviin sentrifugeihin. Sentrifugeja ohjataan SCADA-järjestelmän kautta, jotka ovat tietokoneella ohjattuja valvonta- ja ohjausjärjestelmiä fyysisiin toimintoihin. SCADA-järjestelmässä on siis erilaisia sensoreita, ohjaimia tai viestintälaitteita. Keskeistä on myös keskitetty tiedonkerääminen ja -hallinta ja esimerkkejä SCADA-järjestelmistä ovat esimerkiksi sähköverkkojen valvontajärjestelmät, vedenjakelu- ja vedenpuhdistusjärjestelmät tai öljy- sekä kaasuputkien valvonta. Stuxnetin osalta Iranin uraaninrikastamisen osalta kohteena olivat SCADA-järjestelmän ohjelmoitavat logiikkapiirit. Ohjelmoitavat logiikkapiirit ovat pieniä tietokoneita, jotka ohjaavat esimerkiksi erilaisten kytkimien, releiden tai ajastimien toimintoja. Stuxnetin tapauksessa keskeistä oli päästä vaikuttamaan uraaninrikastamista ohjaavien ohjelmoitavien logiikkapiirien toimintaan (Collins & McCombie 2012, 84.).

Stuxnetin osalta Alenezi ym. (2020, 330) käyttävät superhaittaohjelma termiä kuvaamaan sitä ja Stuxnet havaittiin vasta sen saavutettua tavoitteensa.

Tavoitteena oli tuhota tai hidastaa iranilaisten ydinaseohjelmaa. Stuxnet levisi USB-tikkujen kautta ja piilotti itsensä rootkitin avulla (Alenezi ym. 2020, 330.). Collins ym. (2012, 85) korostavat Stuxnetin superhaittaohjelmamaisuuttaan korostamalla sitä, että Stuxnet hyödynsi neljää erilaista nollapäivähaavoittuvuutta, vaikeutti virustorjuntaohjelmistojen toimintaa ja toimintansa tutkimista, sisälsi Windows-rootkitin, komentopalvelimen sekä ensimmäisenä myös PLC-rootkitin. Stuxnet hyödynsi myös varastettuja sertifikaatteja, jotka olivat Realtekin sekä JMicron allekirjoittamia (Collins ym. 2012, 86).

Stuxnetin leviämisen osalta useimmat ovat sitä mieltä, että leviäminen tapahtui USB-tikkujen kautta. Stuxnet myös oli varovainen saastuttaessaan kohteitaan, jottei se paljastuisi. Tämä korostaa myös tekijöidensä maltillisuutta, sillä tällainen toiminta on ihan erilaista kuin mitä tavalliset haittaohjelmat tekevät (Collins ym. 2012, 85.). Stuxnetin eroavaisuutta korostaa myös se, että Stuxnetin kehittämiseen on kulutettu vähintään 10 000 henkilötyötuntia sekä tekijät ovat olleet asiantuntijoita sekä Microsoftin käyttöjärjestelmissä että sulautetuissa käyttöjärjestelmissä (Collins ym. 2012, 86).

Stuxnetin osalta keskeistä oli myös se, että kyberrikollisuuden ja valtion välinen toiminta yhdistyivät poliittisessa ja strategisessa kontekstissa. Stuxnetin osalta valtio hyödynsi kyberrikollisten kehittämiä tekniikoita hidastaakseen Iranin ydinaseohjelmaa. Kineettisen iskun sijasta Stuxnet nähtiin paremmaksi tavaksi Iranin ydinaseohjelman hidastamiseksi (Collins ym. 2012, 88.). Toisaalta Stuxnetin osalta attribuutiossa korostuu se, ettei mikään taho ole virallisesti ilmoittanut olevansa Stuxnetin tekijä. (Rollins ym. 2010, 2). Tosin Stuxnetin osalta useat tekijät, kuten tekninen monimutkaisuus ja kohteen ainutkertaisuus, korostavat tekijöidensä resursseja. Lisäksi tekijöillä oli huomattavat taloudelliset resurssit, osaamista useilla teknisillä osa-alueilla, tiedustelutietoa Stuxnetin kohteesta ja kuinka kohteeseen voitaisiin tunkeutua. Lisäksi tekijöiden attribuution osalta korostuu valtioiden motiivit Stuxnetin käytössä. Stuxnetin osalta keskeistä oli se, että tarkoituksena oli häiritä ja vahingoittaa kohteena olevan uraanin rikastamiseen käytettävän ohjausjärjestelmän toimintaa (Rollins ym. 2010, 2.). Rollins ym. (2010, 2) luettelee muutamia valtioita, joilla on ollut sekä osaamista että motivaatiota Stuxnetin kehittämiseen ja näitä valtioita ovat muun muassa Yhdysvallat, Israel, Iso-Britannia, Venäjä, Kiina tai Ranska.

Stuxnetin osalta Yhdysvaltojen ja Israelin osalta Rollins ym. (2010, 5) huomauttavat, että on ollut aikaisempia yrityksiä sabotoida Iranin uraanin rikastamisessa käytettäviä sentrifugeja. Tammikuussa 2009 New York Times kirjoitti, että sabotaasin osalta keskeistä oli ollut keskittyminen sähköntuotossa ja sähkönjakelemisessa käytettäviin järjestelmiin, tietojärjestelmiin tai muihin Iranin kannalta kriittisten verkkojen sabotoimiseen. Uraanin rikastamisen osalta keskityttiin yksittäisten virtayksikköjen sabotoimiseen, joita Iran osti Turkista. Tällaisen sabotaasin myötä useat sentrifugit hajosivat (Rollins ym. 2010, 5.).

Bencsáth, Pék, Buttyán ja Félegyházi (2012, 987) huomauttavat, että Stuxnet onnistui tarttumaan useisiin tuhansiin tietokoneisiin, mutta sitä ei havaittu muutamaan vuoteen. Stuxnetin osalta todetaan, ettei Stuxnetin havaitseminen manuaalisesti olisi ollut vaikeata osaaville järjestelmänylläpitäjille.

Järjestelmänylläpitäjä olisi voinut havaita Stuxnetin joko rootkitin havaitsemiseen tarkoitetuilla sovelluksilla tai analysoimalla järjestelmää manuaalisesti. (Bencsáth ym. 2012, 987.) Toisaalta Stevens (2020, 144) huomauttaa, että Stuxnetin osalta paljastuminen johtui osin sattumasta. Pieni Valko-Venäläinen VirusAdBloka havaitsi yhdellä asiakkaallaan tietokoneessa epätavallista toimintaa ja tieto alkoi levitä virustorjuntayhteisössä (Stevens 2020, 143). Lisäksi jälkikäteen on havaittu, että Stuxnetista on ollut useita versioita ja 0.500 versiota on alettu kehittämään marraskuussa 2005 (McDonald, Murchu, Doherty & Chie 2013, 2). Marraskuussa 2007 Stuxnetin 0.5000 versio lähetettiin yleisesti käytössä olevaan haittaohjelmien tarkastamissivustolle, mutta Stuxnettiä ei havaittu näytteestä eikä siihen kiinnitetty suurempaa huomiota (McDonald ym. 2013, 2).

3.3 Advanced Persistent Threat APT28

Jensen, Valeriano & Maness (2019, 218) huomauttavat, että APT28-ryhmä tai Fancy Beariksikin kutsuttu APT-toimija on käyttänyt haittaohjelmia tiettyjen kiinnostavien kohteiden kybervakoiluun. Näitä kiinnostavia kohteita ovat olleet useiden maiden turvallisuus- tai sisäministeriöt, journalistit, Puolan tai Unkarin hallitukset, NATO sekä eurooppalainen OSCE-virasto. (Jensen ym. 2019, 218.) Zsolt & Tamas (2020, 53) huomauttavat, että APT28-ryhmästä on käytetty myös muita nimityksiä kuten Swallowtail, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, Strontium tai Tsar Team. APT28-ryhmän tiedetään olleen toiminnassa ainakin vuodesta 2007 alkaen ja APT28-ryhmä yhdistetään vahvasti Venäjään. Venäjään liittyviä tekijöitä ovat ainakin venäjänkielen käyttäminen sekä haittaohjelmien käännösajat vastaavat Moskovan työaikoja (Zsolt ym. 2020, 53.).

APT28-ryhmän ensimmäinen APT-ohjelma havaittiin ensimmäistä kertaa vuonna 2011 ja APT28-ryhmä hyödyntää yleisiä haittaohjelmia tietojärjestelmiin tunkeutumisessa (Jensen ym. 2019, 218). APT28-ryhmän keskeisiä mielenkiinnon kohteita ovat olleet erityisesti itä-Euroopan hallitukset tai armeijat, Nato sekä muut eurooppalaiset turvallisuusjärjestöt. Myös Baltian maat, Puolat sekä Unkari ovat olleet erityisesti mielenkiinnon kohteina (Zsolt ym. 2020, 53.).

Jensen ym. (2019, 218–219) jatkavat toteamalla, että APT28-ryhmä on yhdistetty erilaisiin digitaalisiin sekä fyysisiin toimiin, jotka palvelevat joko poliittisia tai sotilaallisia tavoitteita. Esimerkiksi vuonna 2015 alkoi operaatio, jonka tarkoituksena oli saada kohteet klikkaamaan sähköpostiviestin linkkejä. Demokraattien kansalliseen komiteaan tapahtunut onnistunut tunkeutuminen huomattiin kesällä 2016 ja tavoitteena oli ollut seurata DNCn viestintää. APT28 oli saanut käsiinsä myös erilaista informaatiota, jota pystyttäisiin hyödyntämään laajemmissa informaatio-operaatioissa tai kiristämiseen (Jensen ym. 2019, 220.).

Lee, Harbinson & Falcone (2018) huomauttavat, että esimerkkitapauksissa APT28-ryhmittymä käytti erilaisia työkaluja eri kohteisiinsa. Hyökkäykset alkoivat kalastelusähköpostilla, jossa oli viittaus Outlookin kalenteritapaamiseen tiedostoliitteenä. Todellisuudessa tiedostoliite oli Excelin tiedosto, jossa oli haitallinen makroskripti. Jotta tiedostoliitteen saanut sallisi makrot, on tiedostossa

peitetty kaikki tekstit ja pyritään houkuttelemaan käyttäjää sallimaan makrojen suorittaminen. (Lee ym. 2018.)

Mikäli käyttäjä sallii makrojen suorittamisen, APT28-ryhmittymä on hyödyntänyt makroja, jotka kirjoittavat satunnaisen tiedoston .txt-tiedostopäätteellä C:\Programdata-kansioon. Tämän jälkeen Windowsissa olevaa Certutil-komentoriviohjelmaa käytetään purkamaan .txt-tiedostopäätteisen tiedoston sisältöä ja purettu sisältö kirjoitetaan vuorostaan .exe-tiedostopäätteellä C:\Programdata-kansioon. Makro pitää pienen tauon, jonka jälkeen .exe-tiedosto ajetaan. (Lee ym. 2018.)

Exe-tiedosto on troijalainen, jonka tarkoituksena on asentaa varsinainen taistelukärki. Taistelukärki on .dll-tiedostossa salattuna omalla algoritmillaan, joka suoritetaan start–komennolla antamalla .dll-tiedosto parametrina rundll32.exe-ohjelmalle. Tämän myötä Windowsin rekisteriin lisätään arvo, joka suoritetaan joka käynnistyksessä. (Lee ym. 2018.) Lee ym. (2018) toteavat, että taistelukärki on APT28-ryhmän yleisesti käyttämä SofaceCarberp, joka aluksi kerää lisää tietoa järjestelmästä sekä aloittaa viestinnän komentopalvelimen kanssa. IoCn osalta Lee ym. (2018) huomauttavat, että analysoitu SofaceCarberp sisälsi yhtenäisyyksiä, mutta käytti erilaista hashing algoritmia sekä kommunikointitapaa aikaisempiin analysoituihin versioihin verrattuna.

Avoimen lähdekoodin Luckystrike-ohjelmistoa oli käytetty kalastelusähköpostin tiedostoliitteen luomiseen. Kyseessä on Microsoftin PowerShell-pohjainen työkalu, jolla voidaan luoda haitallista koodia sisältäviä Excel- tai Word-tiedostoja. Haitallinen koodi on makrossa, joka suoritetaan käyttäjän salliessa makrojen suorittamisen. (Lee ym. 2018.)

Luckystrike-ohjelmisto on tarkoitettu penetraatiotestaukseen tai koulutuskäyttöön ja on saatavilla Githubista. Esimerkiksi ”The Hacker Playbook 3” esittelee Luckystriken käyttämistä osana kalastelua. FireEye (2014, 5) korostaa myös sitä, että APT28-ryhmän osalta keskeistä on huomioida kohteen toimintaympäristö ja räätälöidä käytettävät komponentit näitä hyödyntämään. APT28-ryhmän attribuution osalta attribuutio-ongelma on yhä olemassa, mutta APT28-ryhmän analysoiduista APT-hyökkäyksien näytteistä suurin osa ovat sisältäneet vihjeitä venäjäksi eivätkä englanniksi, jolloin kehitysympäristöissä on todennäköisesti ollut käytössä venäjän kielen asetukset. Toinen vahva attribuutiotekijä on se, että yli 89 prosenttia näytteistä oli käännetty arkipäivinä aamukahdeksan ja iltakuuden välillä ja aikavyöhyke oli merkitty UTC+4 aikaan. UTC+4 aika sopii hyvin kuvaamaan työskentelyaikoja esimerkiksi Pietarissa tai Moskovassa. (FireEye 2014, 5.)

IoI osalta Benchea, Vatamanu, Maximciuc & Luncasu (2015, 11) nostavat esille nmapin käyttämisen kohdejärjestelmässä siirtymisen osalta. nmapin osalta keskeistä oli -T5 parametrin ja 15 erilaisen, mutta hyvin yleisen portin skannaus. Lisäksi skannauksessa painottuu kohteen otsikko- eli header-tietojen hankinta –script=http-headers valinnalla. Benchea ym. (2015, 12) huomauttavat, että eri kerroilla kohdealueena olevia IP-osoitteita oli eri määriä, jolloin voidaan olettaa kyseessä olleen hyvinkin kohdennetun hyökkäyksen. nmapin käyttämisen jälkeen

Benchea ym. (2015, 12) toteavat, että näiden automatisoitujen hyökkäystyökalujen sijasta ihmiset ovat alkaneet tarkemmin tutkia skannauksen tuloksia.

4 TULOKSET JA ARVIOINTI

Luvussa vastataan valittujen APT-ryhmien osalta tutkimuskysymyksiin. Lisäksi kuvataan käytetyt tiedonkeruumenetelmät eli miten tutkimusta tehtiin. Lopuksi luvussa esitellään tutkielman tulokset ja niiden arviointi.

4.1 Tutkimusmenetelmät

Tutkimusmenetelmänä on tapaustutkimus, jossa julkisesti saatavilla olevista lähteistä kerätään tietoa valituista APT-ryhmistä. Tietoa kerättiin myös Dark webistä kahdella eri hakukoneella eli Ahmia ja Torch. Hakusivustot valittiin Georgievin (2022) listauksen pohjalta. Ahmia on pintanetin hakusivusto, joka voi etsiä myös Dark webistä. Toisaalta Ahmia-sivustossa on suodatus päällä, jolloin haitallista sisältöä sisältävät hakutulokset jätetään näyttämättä. Torch on yksi vanhimmista ja suosituimmista Dark webin hakukoneista ja on perustettu jo vuonna 1996. Torch ei myöskään suodata hakutuloksia mitenkään. (Georgiev 2022.)

Tutkimuskysymykseen millaisilla alustoilla havaintoja on löydettävissä käytettiin ilmaisia ja ilman tiliä käytettäviä alustoja. Keskeisin oli Google, mutta myös Social-searcher sivustoa käytettiin sivuston puutteista huolimatta. Social-Searcher on ilmainen työkalu, jolla voidaan useiden sosiaalisen median sivustoja seurata ja havaita miten esimerkiksi tietty aihe leviää. Social-Searcher seuraa Facebookia, Twitteriä, YouTubea, Instagrammia, Tumblria, Reddittiä, Flickriä, Dailymotionia, Vimeota sekä VKontaktea. (Social-Searcher 2023.). Viimeiseen apukysymyksen osalta tarkoituksena oli keskittyä Dark Webin kauppapaikkoihin. Dark Webin kauppapaikkojen suhteen Shibi (2022) luettelee viisi yleisintä ja näistä Exploit.in sekä Dread olivat tutkimushetkellä alhaalla. Tästä johtuen toisen apukysymyksen osalta tiedonkeruu muutettiin painottamaan Torch- ja Ahmia-hakukoneiden tuloksia.

Tiedonkeräämisessä keskityttiin erityisesti Indicators of Intelligenceen eli IoA, IoC ja IoB liittyvää tietoa kerättiin. APT-ryhmien raporteissa painottui IoC

tiedonosuus ja vähemmän oli IoB tai IoA tyylistä tietoa. Tämä myös vaikeutti tutkimuskysymyksiin vastaamista erityisesti Cyber Kill Chainin alkuvaiheiden osalta, kun ei ollut pääsyä esimerkiksi NIDSin logeihin. Yhteistä IoIn osalta se, että avointen lähteiden käyttäminen APT-ryhmien osalta oli tärkeätä, jota on toisaalta vaikeata havaita.

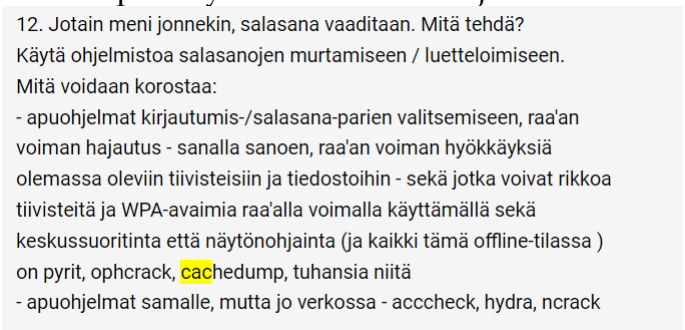
4.2 APT1

APT1 osalta tiedonhaussa käytettiin taulukko kahdessa kuvattuja hakusanoja.

TAULUKKO 2 Dark Webin Torch- ja Ahmia-hakukoneiden tuloksia APT1-ryhmän osalta.

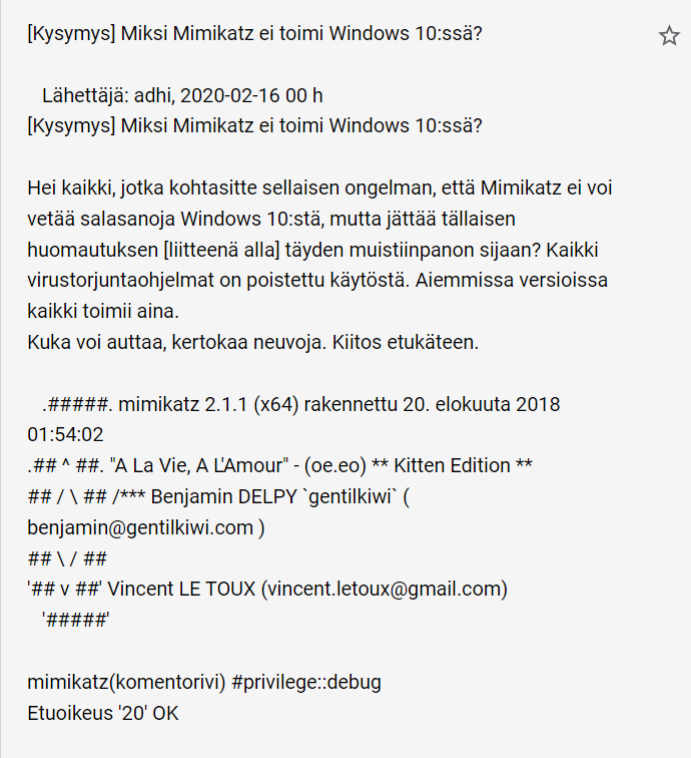
Hakusana	**Tuloksia Torch**	**Tuloksia Ahmia**
cachedump	1 tulos	1 tulos
fgdump	0 tulosta	0 tulosta
gsecdump	0 tulosta	0 tulosta
lslsass	0 tulosta	0 tulosta
mimikatz	1 tulos	1 tulos
pass-the-hash-toolkit	70 tulosta	70 tulosta
pwdump7	0 tulosta	0 tulosta
pwdumpX	0 tulosta	0 tulosta

Toiseen apututkimuskysymykseen hakusanat on valittu Mandiantin (2014) raportista ja verrattaessa taulukko kahdessa olevia Torchin tuloksia Ahmian tuloksiin, huomataan, että hakutulokset ovat samanlaiset. cachedump palautti kuvion neljän mukaisen venäjästä suomeksi käännetyn tuloksen, jossa keskeistä oli cachedumpin käyttäminen salasanojen murtamiseen.


12. Jotain meni jonnekin, salasana vaaditaan. Mitä tehdä?
Käytä ohjelmistoa salasanojen murtamiseen / luetteloimiseen.
Mitä voidaan korostaa:
- apuohjelmat kirjautumis-/salasana-parien valitsemiseen, raa'an voiman hajautus - sanalla sanoen, raa'an voiman hyökkäyksiä olemassa oleviin tiivisteisiin ja tiedostoihin - sekä jotka voivat rikkoa tiivisteitä ja WPA-avaimia raa'alla voimalla käyttämällä sekä keskussuoritinta että näytönohjainta (ja kaikki tämä offline-tilassa) on pyrit, ophcrack, cachedump, tuhansia niitä
- apuohjelmat samalle, mutta jo verkossa - acccheck, hydra, ncrack

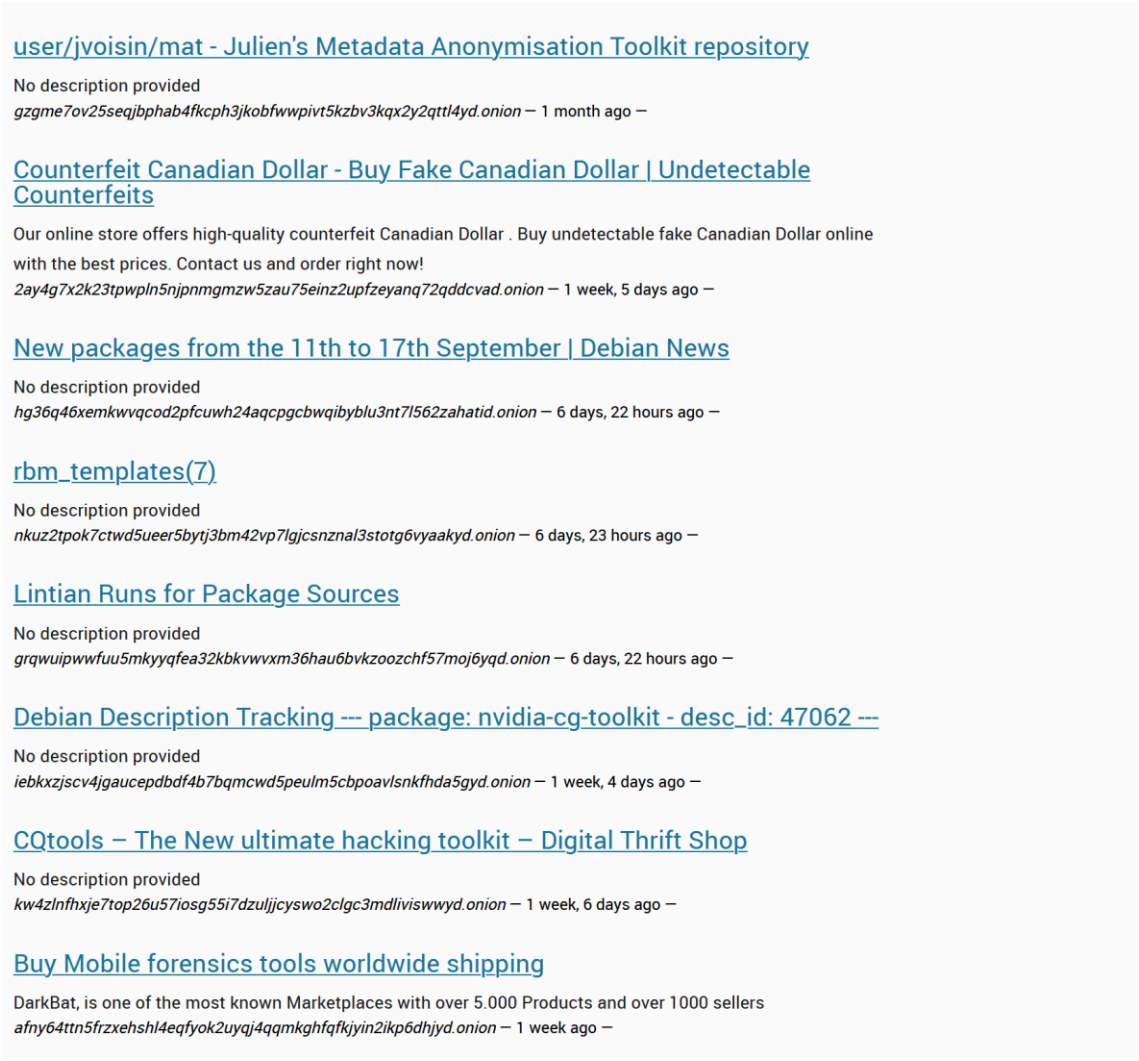
KUVIO 4 APT1-ryhmän cachedump-hakusanan tulos.

Mimikatz palautti cachedump hakusanan tyylisen tuloksen eli venäjäksi on kysytty ohjeita Mimikatziin liittyen. Mimikatz-hakusanan tulos on suomeksi käännettynä kuviossa viisi.



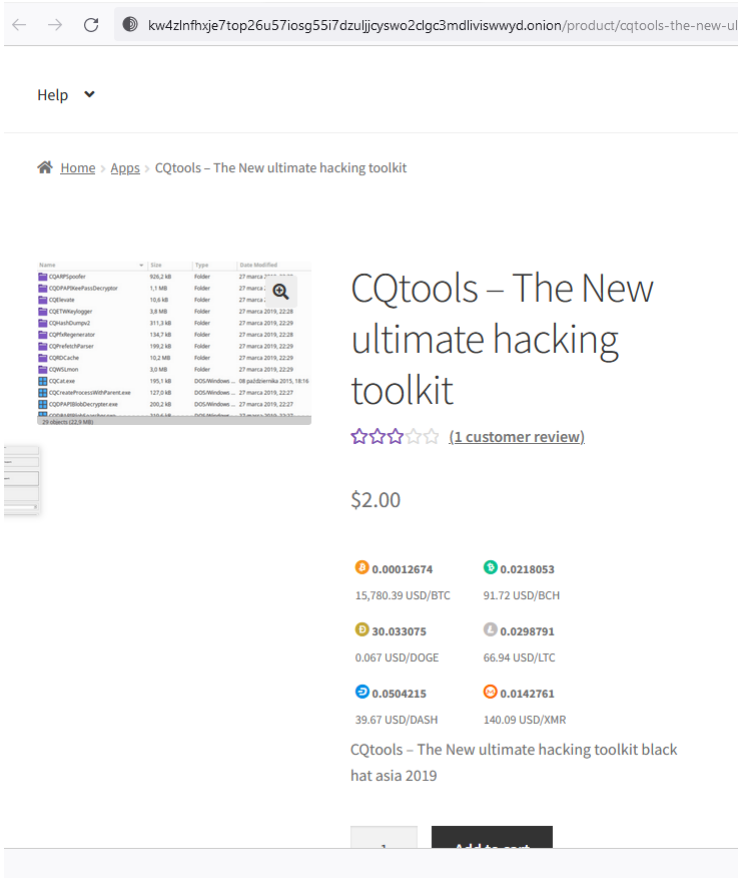
KUVIO 5 APT1-ryhmän Mimikatz-hakusanan hakutulos.

Pass-the-hash-toolkit hakusanaa käytettäessä tuloksia oli 70 erilaista ja hakutulosjoukko oli todella laidasta laitaan. Hakutuloksissa oli kaikkea väärennetyistä Kanadan dollareista Debianiin liittyviin uutisiin ja näitä on kuvattu kuviossa kuusi.



KUVIO 6 Pass-the-hash-toolkitin Torch-hakukoneen tuloksia.

Näistä tuloksista esimerkiksi CQtools markkinoi kahden dollarin työkalua hakkerointiin. Tosin alla olevassa kuviossa seitsemän on kuvattu, että arviointeja on vain yksi kappale ja sekin kolmen tähden.



KUVIO 7 Hakutuloksista on valittu CQtools tarkempaan tarkasteluun.

Yhteenvetona ja vastauksena toiseen apututkimuskysymykseen voidaan todeta, että APT1-ryhmän osalta Dark Webistä valittujen hakusanojen osalta tuloksia löytyi aika vähän ja nekin hyvin yleisistä ohjelmista. Tämä ilmeni erityisesti pass-the-hash-toolkitin osalta. Lisäksi löydetyt tulokset olivat lähinnä apupyyntöjä tai esimerkiksi hakkerointityökalujen tai väärennettyjen dollareiden markkinointia eikä liittynyt APT1-ryhmään mitenkään.

Ensimmäiseen apututkimuskysymykseen APT1-ryhmään liittyen havaintoja haettiin Mandiantin (2014) raportin pohjalta. Mandiantin (2014) raportista otettiin aikajana, jolloin havaintoja haettiin erityisesti vuoden 2014 osalta, mutta myös ennen ja jälkeen vuoden 2014. Tällöin hakuaikajana oli tutkia, millaista tietoa APT1-ryhmästä olisi ollut saatavilla vuosina 2013–2015. Havaintoja kerättiin social-searcher.com sivuston avulla. Hakusanana oli APT1-sana ja havaintoja oli saatavilla 421 kappaletta 211 eri käyttäjältä. Työkalusta sai tiedot ulos myös .csv-muodossa ja sieltä Excelin suodatustoiminnolla oli helppoa tutkia aineistoa. Kuitenkin 421 havainnosta vain kahdet olivat vuodelta 2014 ja neljät vuodelta 2013. Vuodelta 2015 havaintoja oli myös neljät. Nämä havainnot on kuvattu taulukossa kolme.

TAULUKKO 3 Social-searcher.comin hakutuloksia APT1-ryhmästä.

Päiväys	Teksti	Lähde

2013-02-21 00:41:11 GMT	Mandiant Exposes APT1 â€" One of Chinaâ€s Cyber Espionage Units & Releases 3000 Indicators Iâ€™ve been so engrossed by this that I almost forgot to repost it.This is by far the most significant security research released this year and the included video is icing on top.Now to put those IOCs to ...	tumblr
2013-02-21 22:06:13 GMT	The Shanghai Army Unit That Hacked 115 U.S. Targets Likely Wasn't Even China's 'A-Team' In just the last week the abbreviation APT1 has come to represent the bogeyman of digital espionage nightmares. On Monday security response firm Mandiant released a report profiling a hacker group of that nameaâ€" ...	tumblr
2013-08-08T13:42:18.000Z	OHRID APARTMENTS - WWW.PLANET4RENT.COM http://www.planet4rent.com/ohrid-gjole-apartments-1/243/en/ Three bedroom apartment (55m2) for four guests. Located on 7th km south of Ohrid in the district Lagadin on a shore of Ohrid Lake. Luxury equipment with TV kitchen bathroom air-conditio ...	dailymotion
2013-08-19 10:40:45 GMT	Chinese Military Tied to Cyber-Attacks on US China Hacking the U.S. - 2013 (by epsil2)	tumblr
2014-01-28T07:35:21.000Z	19 â€" Paul RascagnA¨res - APT1: Technical Backstage	dailymotion
2014-09-04 07:19:17 GMT	Hakkerit tarkistavat tiedostot VirusTotalilla haitallisten koodiaukkojen etsimiseen Hakkerit tarkistavat tiedostot VirusTotalilla haitallisten koodiaukkojen etsimiseen Virus Writers Google Inc. Yksityinen virustorjuntasivusto VirusTotal tarjoaa oman haittaohjelmansa...	tumblr
2015-01-23 02:25:27 GMT	amaradonis called cinnamon pita chips cinnamon doritosâ and i just want everyone to be alerted to that	tumblr
2015-07-18T13:51:31.000Z	SecureNinjaTV RSA 2013 Mandiant APT1 China Hackers Report	dailymotion
2015-07-22T11:04:52.000Z	APT1: Exposing One of China's Cyber Espionage Units	dailymotion
2015-11-14 21:19:36 GMT	Live from #APT1 // #WeWorkin #WeMixin #WithOURNewSkills #OSOVIViD #OSOVIViDRecords #TaurusLife,	tumblr

Koska tuloksia oli aika vähän, kerättiin lisää tietoa myös googlettamalla. Hakusanana oli APT1 ja aikajanana 1.1.2013–31.12.2014. Tämän haun tuloksia on kuvattu alla olevassa taulukossa neljä.

TAULUKKO 4 Googlen hakutuloksia APT1-ryhmästä.

Päiväys	Teksti	Lähde
2013-02-19	Mandiant Exposes APT1 – One of China's Cyber Espionage — Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators · Digital delivery of over 3,000 APT1 indicators, such as domain names, ...	https://www.mandiant.com/resources/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units
2013-02-19	APT1: Exposing One of China's Cyber Espionage Units — APT1: Exposing One of China's Cyber Espionage Units ... This group is identified "as a Chinese military unit within the 2nd Bureau of the People's Liberation Army ...	https://www.hsdl.org/c/apt1-exposing-one-of-chinas-cyber-espionage-units/
2013-02-19	Mandiant revealed Chinese APT1 Cyber Espionage campaign – During the attacks the attackers have took over APT1 malware families and has revealed by the report APT1's modus operandi (tools, tactics, procedures) ...	https://thehackernews.com/2013/02/mandiant-revealed-chinese-apt1-cyber.html
2013-02-19	Chinese Military Group Linked to Hacks of More Than 100 ... — "We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398." Trending Now.	https://www.wired.com/2013/02/chinese-army-linked-to-hacks/
2013-02-20	Mandiant Report on "APT1" - Lawfare Blog— APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our ...	https://www.lawfareblog.com/mandiant-report-apt1
2013-02-28	Mandiant on Twitter: "Mandiant's Marshall Heilman presenting ...— Mandiant's Marshall Heilman presenting on #cybersecurity & #APT1 @ M's booth 2439 #RSAC. Image. 1:42 AM · Feb 28, 2013.	https://twitter.com/mandiant/status/306942342907183104?lang=fi

2013-03-26	Unit 61398: Chinese Cyber-Espionage and the Advanced ... — APT1 controls thousands of systems in support of their computer intrusion activities. In the last two years Mandiant has observed APT1 establishing a minimum of ...	https://resources.infosecinstitute.com/topic/unit-61398-chinese-cyber-espionage-and-the-advanced-persistent-threat/
2014-04-03	APT1: Exposing One of China's Cyber Espionage Units — APT1: Exposing One of China's Cyber Espionage Units. Download. Mandiant, an American cybersecurity firm, released this report to address the growing thread ...	https://www.nationalcyberwatch.org/resource/apt1-exposing-one-of-chinas-cyber-espionage-units-2/
2014-04-08	One Year Later: The APT1 Report - Dark Reading — One of the most positive impacts of APT1 is the undeniable rise in the stature of the threat intelligence industry. "Threat Intelligence" is the SIEM, ...	https://www.darkreading.com/vulnerabilities---threats/advanced-threats/one-year-later-the-apt1-report/d/d-id/1127681?

Verrattaessa yllä olevaa taulukko neljän havaintoja Social-Searcherin havaintoihin, oli esimerkiksi vuodelta 2013 paljon enemmän havaintoja ja erityisesti vuoden 2013 osalta havaintoja on aika paljon. Lisäksi vuoden 2013 havainnoissa tuodaan esille APT1-ryhmän toiminnan laajuutta. Vuoden 2014 osalta tuloksissa korostuu jo edellisen vuoden havaintoihin peilaaminen. Pohdittaessa yllä olevien taulukkojen havaintoja korostuu tuloksissa se, että APT1-ryhmän toimista on löydettävissä havaintoja valitulla aikajanalla. Tosin havainnot painottuvat Mandiantin (2014) raportin aikajanalla niin, että kolme havaintoa on vuodelta 2013, yksi havainto vuodelta 2014 ja kaksi havaintoa vuodelta 2015**.** Tosin yleisempi taulukko neljässä kuvattu googlaus korostaa APT1-ryhmän toimintaa ja kiinnijäämistä jo vuoden 2013 osalta.

Pohdittaessa APT1-ryhmän toimintaa tutkimuskysymyksiin on päätutkimuskysymyksen osalta vastaus selvähkö. APT1-ryhmän osalta hyökkäyksiä on läpikäytyjen raporttien osalta havaittu vasta myöhemmissä toimittaminen-, hyväksikäyttö- tai asentaminen vaiheissa. Toisaalta IoCn osalta ryhmän toimista on runsaasti tietoa ja esimerkiksi CircleID (2020) korostaa APT1-ryhmän osalta domainnimien osalta oman ug-tyylisen puumerkin käyttämistä. CircleID (2020) toteaa myös, että tuollaiset domainnimet merkitään haitallisiksi.

Peilattaessa APT1-ryhmää ensimmäiseen apukysymykseen keskeistä on pohtia olisiko internet-alustoilla voinut tehdä havaintoja ryhmän toimista? Bahrami, Dehghantanha, Dargahi, Parizi, Choo & Javadi (2019, 866) korostavat APT1-ryhmän osalta heidän keskittymistä kohteisiin, joista on tehty kattava tiedustelu ja tavoitteet ovat olleet selkeitä. Lisäksi APT1-ryhmä on käyttänyt edistyneitä työkaluja sekä tekniikoita hyväksikäyttövaiheessa mutta myös nollapäivähaavoittuvuuksia. Lisäksi APT1-ryhmän osalta hyökkäysoperaatiot ovat olleet

hyvin resursoituja. (Mandiant 2014, 22.) Cyware (2019) jatkaa myös korostamalla APT1-ryhmän kohdeorganisaatioiden osalta Kiinan valtion asettamien tavoitteiden merkitystä ja kohteiden valintaa näihin pohjautuen. APT1-ryhmän osalta Cyware (2019) toteaa sen myös toimineen joko Kiinan armeijan PLA 61398 yksikön puolesta tai yhteistyössä ja PLA 61398 keskittyy poliittiseen, taloudelliseen ja sotilaalliseen tiedusteluun, josta Kiinalle olisi hyötyä. Toisaalta APT1-ryhmän toimintaa on analysoitu paljon ja useita erilaisia raportteja on saatavissa. Lisäksi julkisuudessa esimerkiksi Suojelupoliisi tai Kyberturvakeskus ovat varoittaneet valtioista, joilla on kiinnostusta tiettyjen alojen toimintaan. Pohdittaessa vastausta ensimmäiseen apukysymykseen siitä millaisilla internet-alustoilla erilaisia havaintoja APT1-ryhmän toimista olisi ollut löydettävissä, esiin nousee Internetin rooli ja erityisesti pintanetin rooli. APT1-ryhmän toiminta oli jo ennen Mandiantin (2014) raporttia noussut esiin julkisuuteen erityisesti vuoden 2013 osalta. Toiseen apututkimuskysymykseen vastattaessa APT1-ryhmän toimista ei löytynyt laisinkaan havaintoja Dark webistä.

4.3 Stuxnet

Stuxnetin osalta taulukko viidessä kuvattuja hakusanoja käytettiin tiedonhaussa toiseen apututkimuskysymykseen vastattaessa. Hakusanat on valittu Stuxnetin hyödyntämien neljän eri Windowsin nollapäivähaavoittuvuuden tunnisteista (Sood & Enbod 2014, 44).

TAULUKKO 5 Dark Webin Torch- ja Ahmia-hakukoneiden tuloksia Stuxnetin osalta.

Hakusana	**Tuloksia Torch**	**Tuloksia Ahmia**
CVE-2008-4250	75 tulosta	75 tulosta
CVE-2010-2568	244 tulosta	244 tulosta
CVE-2010-2729	70 tulosta	70 tulosta
CVE-2010-2743	70 tulosta	70 tulosta

Taulukko viiden hakusanat on valittu Stuxnetin käyttämistä nollapäivähaavoittuvuuksista ja verrattaessa Torchin tuloksia Ahmian tuloksiin, huomataan, että hakutulokset ovat samanlaiset. Ihmetystä herätti myös se, että hakutulokset olivat myös hyvin samankaltaisia. Esimerkiksi alla kuviossa kahdeksan on vierekkäin hakusanojen CVE-2010-2568 ja CVE-2010-2729 tulokset Torch-selaimella.

KUVIO 8 CVE-2010-2568 ja CVE-2010-2729 tulokset Torch-hakukoneella.

CVE-2010-2568 tuloksista kuudet ovat myös CVE-2010-2729 tuloksissa. CVE-2010-2729 tuloksissa eroavaisuutta CVE-2010-2568 tuloksiin on kolmantena oleva « Browse WNPP bugs based on debtags »-tulos mutta muuten tulokset ovat lähes identtisiä. Yhteenvetona ja vastauksena toiseen apututkimuskysymykseen voidaan todeta, että Stuxnetin osalta Dark Webistä valittujen hakusanojen osalta tuloksia löytyi lukumääräisesti paljon, mutta varsinaisiin haavoittuvuuksiin liittyen todella vähän. Lisäksi suurin osa tuloksista ei liittynyt Stuxnettiin mitenkään.

Ensimmäiseen apututkimuskysymykseen Stuxnettiin liittyen havaintoja haettiin keskittyen vuoteen 2010. Havaintoja oli tarkoitus kerätä myös socialsearcher.com sivuston avulla ja Stuxnetin osalta aikajanana oli erityisesti vuosi 2010, mutta myös ennen ja jälkeen vuoden 2010 haettiin havaintoja. Tällöin hakuaikajanaksi oli tarkoitus asettaa vuodet 2009–2011. Havaintoja kerättiin socialsearcher.com sivuston avulla. Hakusanana oli Stuxnet-sana ja havaintoja oli saatavilla 575 kappaletta 395 eri käyttäjältä. Työkalusta sai tiedot ulos myös .csv-muodossa ja sieltä Excelin suodatustoiminnolla olisi ollut helppoa tutkia aineistoa. Tämän jälkeen tuloksissa paljastui yllätys eli aikaisimmat havainnot ovat vasta vuodelta 2012. Tämän takia työkalun käyttäminen hylättiin Stuxnetin osalta ja siirryttiin Googlen käyttöön painottaen vuosia 2009–2011.

Tämän takia Stuxnetin havaintoja internetistä haettiin googlettamalla ja googlessa hakukoneeseen laitettiin #Stuxnet inurl :twitter hakusanat sekä aikajanaksi vuosi 2010 sekä 1.1.2009 alkaen. Lisäksi hakutuloksia haettiin myös pelkällä stuxnet sanalla sekä vuosi 2010 aikajanana. Nämä havainnot on kuvattu taulukossa kuusi.

TAULUKKO 6 Googlen hakutuloksia Stuxnetistä.

Päiväys	Teksti	Lähde
2010-06-15	How Stuxnet Worked Usb Stick, Siemens, Deployment, Infrastructure, Spectrum,	pinterest

	Microsoft,. https://www.pinterest.com/pin/326018460520568409/	
2010-06-15	What is Stuxnet? 5 Fast Facts | Security Encyclopedia A key uranium-enrichment facility in Natanz was crippled when a malware worm — called Stuxnet — infected Windows computers, resulting in the self-destruction of ...	https://www.hypr.com › stuxnet
2010-07-15	Stuxnet | CFR Interactives Stuxnet was the first publicly known instance in which a cyber operation caused physical damage outside of a controlled testing environment. It demonstrated the	https://www.cfr.org › cyber-operations
2010-07-19	Worm:Win32/Stuxnet.A - Microsoft Security Intelligence— Worm:Win32/Stuxnet.A is the detection for a worm that spreads to all removable drives. It does this by dropping shortcut files (.LNK) that automatically run ...	https://www.microsoft.com › threats
2010-07-19	Malware Affecting Siemens WinCC and PCS7 Products ... — Just got this from some of the process control security group within Dow Chemical...Some of you may have already seen information about this “Stuxnet” ...	https://support.industry.siemens.com › ...
2010-09-14	'Stuxnet' Worm Far More Sophisticated Than Previously Thought — Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically ...	https://krebsonsecurity.com
2010-09-18	Stuxnet analysis by Langner - OT-BASE In the summer of 2010, a malware of unprecedented complexity made the news. It used multiple zero-day exploits, and was dubbed “Stuxnet” by anti-virus ...	https://www.langner.com › stuxnet
2010-09-21	Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr ... Once a system is infected, Stuxnet simply sits and waits – checking every five seconds to see if its exact parameters are met on the system. When they are, ...	https://www.csmonitor.com › USA › S...
2010-09-25	Iran's nuclear agency trying to stop computer worm...— The semi-official ISNA news agency says Iranian nuclear experts met this week to discuss how to remove the malicious computer code, dubbed Stuxnet, ...	https://iranfocus.com › nuclear › 218
2010-09-27	Why the Stuxnet worm is like nothing seen before | New Scientist — Why the fuss over Stuxnet? Computer viruses, worms and trojans have until now	https://www.newscientist.com › article

	mainly infected PCs or the servers that keep e-businesses running. They may delete ...	
2010-09-29	Primary Stuxnet Advisory - US-CERT – CISA — ICS Advisory (ICSA-10-272-01). Primary Stuxnet Advisory. Original release date: September 29, 2010	https://us-cert.cisa.gov › ics › advisories
2010-09-30	W32.Stuxnet Dossier — Once Stuxnet had infected a computer within the organization it began to spread in search of Field PGs, which are typical Windows computers but used to program ...	https://docs.broadcom.com › doc › security-respo...
2010-09-30	El código del virus Stuxnet alberga una cita bíblica del Antiguo Testamento http://nyti.ms/bWMd5V #myrtus #nytimes	twitter
2010-10-01	STUXNET Malware Targets SCADA Systems - Trend Micro – What is STUXNET? STUXNET is a worm that initially made news in July due to its use of certain vulnerabilities to propagate and execute its routines.	https://www.trendmicro.com › vinfo
2010-10-01	#stuxnet #netmem – Hidden backwards message in Stuxnet code: ”I am the eggman. I am the walrus”	twitter
2010-10-01	Stuxnet analysis supports Iran as target, Israel as source – but is it all too neat? htto://bit.ly/aVZNgv #vb2010	twitter
2010-10-07	7.10.2010 — Stuxnet is a specialised malware targeting SCADA systems running Siemens SIMATIC® WinCC or SIMATIC® Siemens STEP 7 software for process visualisation and	https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis
2010-10-07	The Story Behind The Stuxnet Virus - Forbes As the story goes, the Stuxnet worm was designed and released by a government--the U.S. and Israel are the most common suspects--specifically to attack the	https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

Pohdittaessa miten vastattaisiin Stuxnetin osalta tutkimuskysymyksiin, on päätutkimuskysymyksen osalta vastaus selvä. Stuxnetin havaitseminen tapahtui vasta jälkikäteen ja osittain sattumalta. Toisaalta Iran oli tietoinen uraanin rikastamiseen liittyvän ydinohjelmansa riskeistä ja siksi uraania rikastava laitos oli erillään internetistä sekä sijoitettuna maan alle, jolloin suojauduttiin myös esimerkiksi lentokoneilta tehtäviltä pommituksilta. Tietoa siitä kuka kuljetti USB-tikun ja miten Stuxnet löysi tiensä uraania rikastavaan laitokseen ei ole, mutta mahdollisuutena pidetään USB-tikkua, joka kytkettiin johonkin laitoksen verkotetuista tietokoneista. Jälkiviisaana mediassa oli useita kirjoituksia pyrkimyksistä sabotoida sentrifugeja, joihin olisi kannattanut kiinnittää huomiota. Lisäksi Stuxnetin 0.5000 versiota olisi kannattanut analysoida paremmin, mutta haittaohjelmiston kehittäjät olivat kiinnittäneet huomiota sekä haittaohjelmansa leviämiseen että aktivoitumiseen vain oikeassa kohteessa. Tämän osalta esimerkiksi mediaa seuraamalla olisi ollut joitain havaintoja mahdollista tehdä, mutta haasteena olisi ollut oikean informaation havaitseminen valtavasta kohinasta. Lehto (2022) myös huomauttaa, että

Stuxnetin osalta vihjeitä oli saatavilla mahdollisesta hyökkäyksestä. Toisaalta jo Marsh (1997, 31) luettelee useita mahdollisia haittaohjelmalla tehtäviä kyberhyökkäyksiä alkaen tietokantahyökkäyksestä, vakoiluun tai toiminnan sammuttamiseen tai tuhoamiseen haitallisilla komennoilla. Stuxnetin osalta korostui myös oletussalasanojen merkitys, sillä Farwell & Rogozinski (2011, 24) huomauttavat Stuxnetin käyttäneen Siemensin oletussalasanaa. Stuxnetin osalta korostui muutenkin avointen lähteiden käyttäminen tiedustelussa, kuten Moinescu & Glävan (2018, 100) toteavat. Stuxnetin osalta sekä Iranin presidentin sivustolla ja televisiossa julkaistiin paljastavia valokuvia ja videoita Nantzissa, joita on hyödynnetty Stuxnetissa. (Moinescu ym. 2018, 100).

Peilattassa Stuxnettia ensimmäiseen apukysymykseen keskeistä on pohtia olisiko internet-alustoilla voinut tehdä havaintoja Stuxnetistä? Ennen Stuxnetin paljastumista tietoa ei ollut Internetistä saatavilla ja Virustotalin havaintoon vuoden 2007 lopussa ei kiinnitetty huomiota. Toisaalta muualta mediasta oli saatavilla vihjeitä ja esimerkiksi Rollins ym. (2010, 5) nostavat esille aikaisemman sabotaasin Iranin sentrifugeja kohtaan. Toisaalta Iran oli myös varautunut esimerkiksi pommituksiin huomioimalla tämän uraaninrikastamon sijoittamisessa maan alle mutta myös eristämällä laitoksen internetistä. Toiseen apututkimuskysymykseen vastattaessa Stuxnetistä ei löytynyt laisinkaan havaintoja Dark webistä.

4.4 APT28

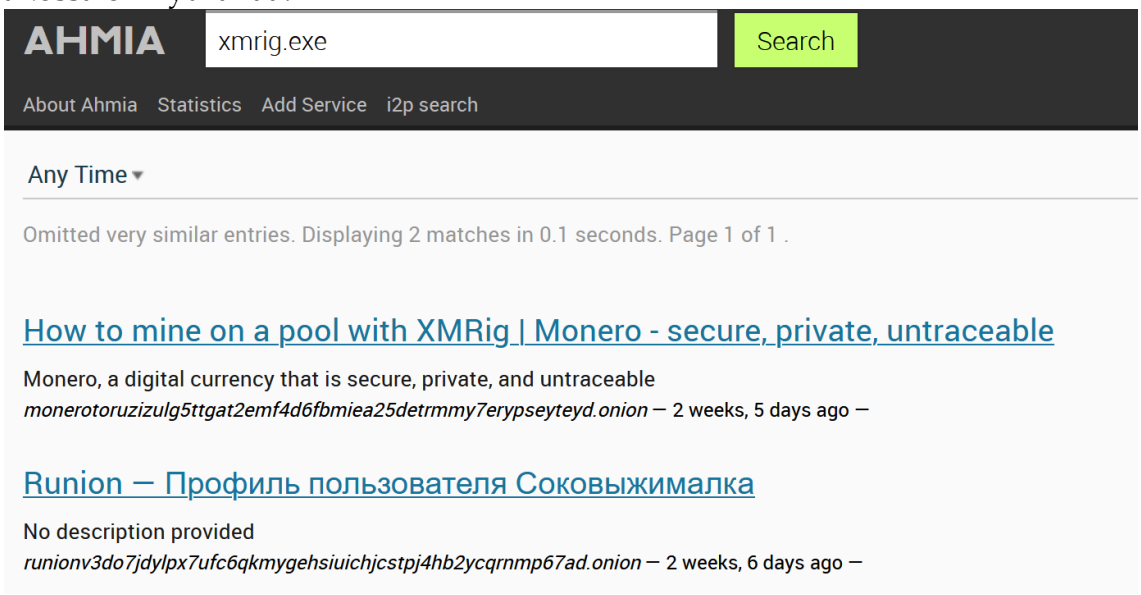
APT28 osalta taulukko seitsemässä kuvattuja hakusanoja käytettiin toiseen apututkimuskysymykseen liittyvässä tiedonhaussa. Hakusanat on valittu Benchea ym. (2015, 19) liitteestä mutta täydennetty myös RedDrip7 (2023) APT28-ryhmän havainnoilla.

TAULUKKO 7 Dark Webin Torch- ja Ahmia-hakukoneiden tuloksia APT28-ryhmän osalta.

Hakusana	**Tuloksia Torch**	**Tuloksia Ahmia**
certserv.exe	0 tulosta	0 tulosta
xmrig.exe	2 tulosta	2 tulosta
myfile.exe	0 tulosta	0 tulosta
RPCNETP.EXE	0 tulosta	0 tulosta
wg.exe	0 tulosta	0 tulosta
xp.exe	0 tulosta	0 tulosta
run.exe	0 tulosta	0 tulosta
svehost.exe	0 tulosta	0 tulosta

Yhteenvetona ja vastauksena toiseen apututkimuskysymykseen voidaan todeta, että APT28-ryhmän osalta Dark Webistä valittujen hakusanojen osalta tuloksia löytyi aika vähän sekä Torchilla että Ahmialla. xmrig.exe-hakusanalla löytyi kaksi tulosta, jotka on kuvattu kuviossa yhdeksän. Toisessa hakutuloksessa

kysytään kuinka xmrigiä voidaan käyttää bittirahan louhintaan ja toisessa hakutuloksessa kiitetään avusta bittirahan louhintaan liittyen, sillä louhijan lompakossa on nyt rahaa.



KUVIO 9 APT28-hakutuloksia xmrig.exe-hakusanalla

Ensimmäiseen apututkimuskysymykseen APT28-ryhmään liittyen havaintoja haettiin Lee ym. (2018) raportin pohjalta. Lee ym. (2018) raportista otettiin aikajana, jolloin havaintoja haettiin erityisesti vuoden 2018 osalta, mutta myös ennen ja jälkeen vuoden 2018. Tällöin hakuaikajana oli tutkia, millaista tietoa APT28-ryhmästä olisi ollut saatavilla vuosina 2017–2019. Havaintoja kerättiin social-searcher.com sivuston avulla. Hakusanana oli APT28-sana ja havaintoja oli saatavilla 265 kappaletta 86 eri käyttäjältä. Työkalusta sai tiedot ulos myös .csv-muodossa ja sieltä Excelin suodatustoiminnolla oli helppoa tutkia aineistoa. Ensimmäisiä tuloksia oli jopa vuosilta 2006 ja 2007, mutta molemmissa kyseessä oli asuntoon liittyviä vuokrausilmoituksia eli asunnon numerona oli 28. Ensimmäinen varsinainen havainto on lokakuulta 2014 Flickr-palvelusta Humansdevelin tekemänä ja siinä on viittaus Valkoisen talon hakkerointiin. Vuoden 2017 osalta 265 havainnosta havaintoja oli vain kolmet ja kahdet vuodelta 2018. Vuodelta 2019 havaintoja oli huomattavasti enemmän eli 23 kappaletta. Nämä havainnot on kuvattu taulukossa kahdeksan.

TAULUKKO 8 Social-searcher.comin hakutuloksia APT28-ryhmästä.

Päiväys	Teksti	Lähde
2017-05-04T20:42:43.000Z	Advanced Google Docs Phishing Attack Se naamioituu näyttämällä aidolta Advanced Google Docsin tietojenkalasteluhyökkäys, joka naamioituu näyttäytymällä laillisena APT28 #Gmail #Google #GoogleDocuments #İinternetVirus #IdentityAvi #Pishing	flickr
2017-07-04T22:56:23.000Z	APT 28 Databending with Audacity Applied compressor phaser and low pass filter	flickr

2017-10-06T04:02:25.000Z	CSE CybSec ZLAB Malware Analysis Report: APT28 Hospitality malware https://t.co/N4XJfMiG8r CSE CybSec ZLAB Malware Analysis Report APT28 Hospitality malware tcoN4XJfMiG8r via Twitter twittercomLifeGenstatus916150203299663873	flickr
2018-07-16T19:29:13.000Z	Kyberturvallisuus, virhe Italian verkoissa. Venäläinen ryhmä APT28 toiminnassa	flickr
2018-08-04T18:46:32.000Z	Italia kyberhyökkäyksen alla, "#MattarellaResign", APT28:n venäläiset kulissien takana?	flickr
2019-02-20T09:41:14.000Z	@htbridge : #Microsoft reveals new APT28 #cyberattacks against European political entities: https://t.co/aTJQN7rkJT #cybercrime @htbridge Microsoft reveals new APT28 #cyberattacks against European political entities tcoaTJQN7rkJT #cybercrime via Twitter twittercomhtbridgestatus109815508759835852 ...	flickr
2019-02-20T09:43:26.000Z	@htbridge: #Microsoft reveals new APT28 #cyberattacks against European political entities: https://t.co/aTJQN7rkJT #cybercrime	reddit
2019-02-20T22:59:07.000Z	Microsoft says Russian APT28 espionage group hit Democratic Institutions in Europe	reddit
2019-02-21T11:31:14.000Z	Microsoft says Russian APT28 espionage group hit Democratic Institutions in Europe	reddit
2019-03-30T18:28:19.000Z	How To Locate Domains Spoofing Campaigns (Using Google Dorks) #Midterms2018 How To Locate Domains Spoofing Campaigns (Using Google Dorks) #Midterms2018 How To Locate Domains Spoofing Campaigns (Using Google Dorks) #Midterms2018 The government accounts of US Senator Claire McCaskill (and her staff) w ...	reddit
2019-04-12T15:21:34.000Z	APT28 and Upcoming Elections: evidence of possible interference	reddit
2019-04-18T20:06:15.000Z	APT28 and Upcoming Elections: evidence of possible interference (Part II)	reddit
2019-04-18T14:48:30.000Z	Who are Earworm and APT28? https://t.co/pKGHMHoiMw https://t.co/Rs3xzfA7sM Who are Earworm and APT28? https://t.co/pKGHMHoiMw[pic.twitter.com/Rs3xzfA7sM](https://t.co/Rs3xzfA7sM) â€" DigitalMunition (@maher275) [April 18 2019](https://twitter.com/maher275/status/111888875 ...	reddit
2019-04-18T13:07:10.000Z	APT28 and Upcoming Elections: evidence of possible interference (Part II)	reddit
2019-05-26T11:33:45.000Z	[netsec] 05/31/18 - "APT28 Rollercoaster: The Lowdown on Hijacked LoJack" by /u/teksquisite	reddit
2019-06-16T18:01:32.000Z	Are you aware of advanced persistent threats? There's quite a few of them and plenty to learn from each intrusion.APT10 - China attacking and stealing intellectual property from corporations	reddit

	around America.APT28/APT29 - Russia inference with the US 2016 elections.APT38 - North Korea hacking b ...	
2019-07-12T22:01:22.000Z	Important Essay by Cyberanalyst Jeffrey Carr Pertinent to the "Hack" of the DNC Also Scrubbed from Medium's Site Here's the essay by Carr that was posted at Medium.com in December of 2016. Fortunately he also posted it at LinkedIn.https://www.linkedin.com/pulse/fbidhs-joint-analysis-report-fat ...	reddit
2019-07-12T22:13:36.000Z	The â€œHackâ€ of the DNC â€“ What I Think REALLY Happened My contention is that US intelligence tipped off the DNC that one of their employees was planning to leak their emails to Wikileaks and that the DNC then brought in their computer consultants Crowdstrike to manage the situation. They then hit on ...	reddit
2019-07-13T02:21:40.000Z	The â€œHackâ€ of the DNC â€“ What I Think REALLY Happened My contention is that US intelligence tipped off the DNC that one of their employees was planning to leak their emails to Wikileaks and that the DNC then brought in their computer consultants Crowdstrike to manage the situation. They then hit on ...	reddit
2019-07-18T02:03:33.000Z	Microsoft warns 10000 customers theyâ€™re targeted by nation-sponsored hackers This is the best tl;dr I could make [original](https://arstechnica.com/tech-policy/2019/07/microsoft-warns-10000-customers-theyre-targeted-by-nation-sponsored-hackers/) reduced by 69%. (I'm a bot)*****> Microsoft sai ...	reddit
2019-08-05T15:19:00.000Z	Using TweetDeck For Defensive Monitoring & Threat Intelligence Twitter's great right?There are approximately 500 million tweets a day. That's a lot of information to get through but TweetDeck makes it a lot easier to monitor trends follow hashtags and perform live searches. This is a usefu ...	reddit
2019-08-22T09:00:14.000Z	Hackers attack Indian healthcare website steal 6.8 million records. | A US-based cyber security firm said cyber criminals - mostly China-based are directly selling data stolen from healthcare organisations and web portals globally including in India in the underground markets. This is the best tl;d ...	reddit
2019-10-28T22:01:50.000Z	Microsoft announced Monday that it had found evidence of a Russian hacking group targeting more than a dozen national and international sporting and anti-doping groups with â€œsignificant cyberattacksâ€ This is the best tl;dr I could make [original](https://thehill.com/policy/cybersecurity/467792-micr ...	reddit
2019-10-29T00:01:25.000Z	Microsoft says Russia-linked hackers target sports organizations This is the best tl;dr I could make [original](https://www.reuters.com/article/us-microsoft-cyber/microsoft-says-russia-linked-hackers-target-sports-organizations-idUSKBN1X724L) reduced by 51%. (I'm a bot)*****> Microsoft Corp sa ...	reddit
2019-10-30T15:15:18.000Z	New cyberattacks from APT28 FancyBear targeting sporting and anti-doping organizations in lead-up to Tokyo Summer Games in 2020	reddit
2019-11-21T16:07:03.000Z	Russia's â€˜Sandwormâ€™ Hackers Also Targeted Android Phones This is the best tl;dr I could make [original](https://www.wired.com/story/sandworm-android-malware/) reduced by 55%. (I'm a bot)*****> The Russian state-	reddit

	sponsored hackers known as Sandworm have launched some of the most aggressive and d ...	
2019-12-05T10:36:11.000Z	The evolutions of APT28 attacks	reddit
2019-12-07T13:50:50.000Z	Double blow to GRU ahead of Normandy Summit Just a couple of days ago in my piece "GRU spy fails level Russian lobbyism in EU" I noted that more extraordinary revelations are ahead regarding GRU following a plethora of their major failures abroad of which we learned from the media and which affect ...	reddit

Koska tuloksia oli aika vähän, kerättiin lisää tietoa myös googlettamalla. Hakusanana oli APT28 ja aikajanana 1.1.2017–31.12.2018. Tämän haun tuloksia on kuvattu alla olevassa taulukossa yhdeksän.

TAULUKKO 9 Googlen hakutuloksia APT1-ryhmästä.

Päiväys	**Teksti**	**Lähde**
2017-01-11	The malware, zero-day exploits, and phishing scams used by Russian hackers APT28, known as Fancy Bear.	https://www.wired.co.uk/article/how-russian-hackers-work
2017-02-16	The report published by FireEye revealed that the APT28 is behind long-running cyber espionage campaigns that targeted also US defense contractors and European	https://securityaffairs.co/56336/apt/apt28-leaked-report.html
2017-03-24	Germany blocked Russian hacking attacks in 2016 - Reuters — Germany last year warded off two cyber attacks by APT28, a top official said Friday, referring to a Russian hacking group also dubbed "Fancy Bear" that	https://www.reuters.com/article/us-germany-elections-russia-idUSKBN16V2FW
2017-05-22	Sofacy Advisory— Sofacy (also known as APT28, Pawn Storm, Tsar Team, Fancy Bear, Sednit and Strontium) is a cyber espionage group. Its behaviour has been classified as an ...	https://nfr.indianrailways.gov.in/nciipc.htm
2017-05-27	Intro to APT28 & APT30 | Azeria — APT28 is an adversary group which has been active since at least 2007. This group was identified to be targeting mostly military or government entities and ...	https://azeria-labs.com/intro-to-apt28-apt30/
2017-08-11	APT28 hackers are leveraging NSA Hacking tool to spy on – According to FireEye, the notorious Russia-linked APT28 group is behind an ongoing	https://securityaffairs.co/61924/apt/apt28-hotels-guests.html

	campaign targeting hotels in several European countries.	
2017-08-14	Alleged Russian APT28 Used Spy Tools to Hack Hotels and ... — Alleged Russian APT28, also known as Fancy Bear, Sofacy, and Pawn Storm among others, exploited EternalBlue to hack into hotel Wifi networks and steal inf	https://edgy.app/spy-tools-used-by-hackers-to-pry-on-hotels-and-steal-information
2017-09-07	Russian APT Groups Continue Their Stealthy Operations — The APT 28 group (aka Pawn Storm, Sednit, Sofacy, Fancy Bear and Tsar Team) is a ... The Russian cyber espionage APT28 group launched spear phishing attacks ...	https://resources.infosecinstitute.com/topic/russian-apt-groups-continue-stealthy-operations/
2017-10-19	APT28 racing to exploit CVE-2017-11292 Flash vulnerability ... Käännä tämä sivu — APT28 is a sophisticated state-sponsored group that is using the vulnerability to attack potentially high-value targets but it is likely that other threat ...	https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed
2017-11-07	Threat Group APT28 Slips Office Malware into Doc Citing NYC ... – APT28 is a resourceful threat actor that not only capitalizes on recent events to trick potential victims into infections, but can also rapidly incorporate new ...	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/
2018-02-22	APT28 is probably best known for its attacks on the Democratic National Committee (DNC) and other political targets in 2016. The group has a reputation for ...	https://www.anomali.com/blog/a-timeline-of-apt28-activity
2018-04-10	Advanced Persistent Threat group, APT28 (also known as Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy), is a highly skilled threat actor, best known for its.	https://www.ncsc.gov.uk/files/NCSC_APT28.pdf
2018-09-21	Fancy Bear & Cozy Bear, APT28 & APT29, targeting 2018 US — APT28 is traditionally associated with the Russian military intelligence agency GRU. It has been active since at least 2007. Initially Fancy Bear just stole ...	https://www.thesslstore.com/blog/apt28-apt29/

Vaikka ihan kaikki havainnot yllä olevassa taulukko yhdeksässä eivät ole APT28-ryhmästä, voi taulukkoja tutkimalla tehdä sen johtopäätöksen, että APT28-ryhmän toimista löytyy havaintoja aikajanalla. Tosin havainnot painottuvat Leen

ym. (2018) raportin aikajanan loppupäähän eli vuoteen 2019. Tosin vuoden 2017 Cmyhsi Flickrissä heinäkuussa tekemä postaus on suosituimmuudeltaan kaikista korkein eli arvoltaan 555. Tosin vuodelta 2014 on yksi havainto APT28-ryhmään liittyen, mutta sitten vuodet 2015 ja 2016 eivät Social-Searcherissä palauta yhtään ainutta havaintoa. Yhteenvetona pohdittaessa APT28-ryhmän toiminnasta kertovia havaintoja tutkimuskysymykseen liittyen havaintoja oli Social-Searcherissä paljon. Sama korostui myös taulukko yhdeksän tuloksissa eli APT28-ryhmä oli otsikoissa valittuna aikana. Erityisesti vuoden 2017 osalta APT28-ryhmän toiminnan laajuudesta uutisoitiin paljon. Siksi pohdittaessa yllä olevien taulukkojen havaintoja korostuu tuloksissa se, että APT28-ryhmän toimista on löydettävissä havaintoja valitulla aikajanalla.

Pohdittaessa APT28-ryhmää tutkimuskysymyksiin on erityisesti päätutkimuskysymyksen osalta vastaus selvä. Läpikäydyissä raporteissa IoC-tietoa oli runsaasti, mutta painottui toimittaminen-, hyväksikäyttö- ja asentaminen vaiheisiin. Toisaalta raporteissa nousi esille myös nmapin käyttäminen, jolloin NDIS olisi saattanut jotain ilmoittaa, mutta yleensä tuollainen muutamien porttien skannaus hukkuu internetin kohinaan ja muidenkin tahojen tekemiin porttiskannauksiin. Tosin käytettävissä ei ollut yhtäkään APT28-ryhmään liittyvää NDIS-logia tai muitakaan IDS-/IPS-laitteiden logeja.

Mwiki, Dargahi, Dehghantanha &Choo (2019, 231) korostavat APT28-ryhmän osalta avointen lähteiden käyttämistä tiedusteluvaiheessa. APT28-ryhmä on hyödyntänyt erilaisia ohjelmia esimerkiksi nettisovelluksien haavoittuvuuksien havaitsemiseen tai etsinyt XSS- tai SQL-haavoittuvuuksia nettisovelluksista. APT28-ryhmä on myös käyttänyt erilaisia haavoittuvuuksia, kuten CVE-2014-4114 eli Sandworm-haavoittuvuutta toimissaan. (Mwiki ym. 2019, 231.) Näiden osalta ennakkovaroituksen saamisessa keskeisessä roolissa olisivat esimerkiksi käytettävissä olevat NDIS-logit, joita ei nyt ollut käytössä. Siksi pohdittaessa APT28-ryhmää ensimmäiseen apukysymykseen keskeistä on pohtia olisiko internet-alustoilla voinut tehdä havaintoja ryhmän toimista? Vastauksessa millaisilla internet-alustoilla erilaisia havaintoja APT28-ryhmän toimista olisi ollut löydettävissä, esiin nousee kuten APT1-ryhmän osalta Internetin rooli ja erityisesti pintanetin rooli. Kuten APT1-ryhmän osalta, oli APT28-ryhmän toiminnasta useita havaintoja erityisesti vuosien 2017–2018 osalta, jolloin tarkasteltu APT-hyökkäys tapahtui. Toiseen apututkimuskysymykseen vastattaessa APT28-ryhmän toimista ei löytynyt laisinkaan havaintoja Dark webistä.

4.5 Yhteenveto

Päätutkimuskysymyksenä on pohtia missä vaiheessa Internetistä olisi löydettävissä havaintoja APT-hyökkäyksistä. Pohdittaessa vastausta päätutkimuskysymykseen valitun kolmen esimerkkitapauksen osalta, esiin nousee tapauksien eroavaisuudet. Sekä APT1- ja APT28-ryhmät olivat olleet aktiivisessa toiminnassa eri kohteisiin ennen valittuja esimerkkitapauksia, mutta Stuxnet keskittyi yhteen kohteeseen. Tällöin Stuxnetin osalta havaintoja APT-hyökkäyksestä oli

saatavilla vasta kun hyökkäystä oltiin lopettamassa ja asetetut tavoitteet oli saavutettu. Toisaalta Stuxnetin osalta Bencsáth ym. (2012, 972) nostavat esille sen, ettei Stuxnet ollut mikään yksittäinen APT-ohjelma, vaan osa APT-ohjelmaperhettä. APT-ohjelmaperheeseen kuuluvat ainakin Flame, Duqu sekä Gauss, joista viimeiseksi mainittu havaittiin vuonna 2012 Stuxnetin lopetettua toimintansa. Toisaalta Gaussin osalta sen sisältämän salatun ohjelmamoduulin sisältöä eikä tavoitetta ei edelleenkään tiedetä, sillä Gauss purkaa ohjelmamoduulin salauksen vasta oikeassa kohteessa. (Bencsáth ym. 2012, 972.) Vaikka Stuxnet on lopettanut toimintansa, on saman APT-haittaohjelma perheen osalta siis vielä paljon epäselvyyttä.

APT1- ja APT28-ryhmien osalta esimerkkitapauksissa Internetin havaintojen osalta korostui se, että molemmat APT-ryhmät olivat saaneet huomattavaa mediahuomiota pitkäaikaisesti jatkuneille toimilleen ennen valittuja esimerkkitapauksia, kuten sekä Oosthoek ym. (2021, 302) sekä Jensen ym. (2019, 218) toteavat. Siksi APT1- ja APT28-ryhmien osalta Internetistä oli löydettävissä havaintoja ennen esimerkkitapauksia. Toisaalta APT-ryhmien tekemää tiedustelu-vaihetta on vaikeata havaita ja esimerkkitapauksien raporteissa kummankin APT-ryhmän osalta hyökkäykset etenivät tiedustelu- ja aseistamisvaiheista toimittaminen-, hyväksikäyttö- ja asentaminen vaiheisiin.

Ensimmäinen apututkimuskysymys kysyy millaisilla internet-alustoilla havaintoja olisi löydettävissä ja keskeisintä on tutkia onko havaintoja löydettävissä pintawebissä vai Dark webissä sekä millaisilla alustoilla. Toinen apututkimuskysymys kysyy onko Dark webistä löydettävissä APT-hyökkäyksiin käytettäviä hyökkäystyökaluja. Molempien apututkimuskysymyksien osalta haasteena oli niin sanottujen oikeiden kyberuhkatiedustelutyökalujen puuttuminen, jolloin apututkimuskysymyksiin vastauksia haettiin saatavilla olevilla työkaluilla, kuten Social-Searcher tai Ahmia-, Torch- tai Google-hakutyökaluilla.

Vastattaessa ensimmäiseen apukysymykseen esiin nousee uudestaan esimerkkitapauksien erilaisuudet. Sekä APT1- että APT28-ryhmät olivat olleet aktiivisia sekä mediassa esillä ennen esimerkkitapauksia, jonka johdosta Internetistä oli löydettävissä havaintoja sekä uutisia ryhmien toimista. Havaintojen osalta esiin nousee Internetin rooli ja käytössä olevilla tiedonhakukeinoilla Internetistä löytyi havaintoja sekä uutisina että sosiaalisen median puolelta.

Peilattassa Stuxnettia ensimmäiseen apukysymykseen tilanne on ihan erilainen. Vasta Stuxnetin paljastuttua oli tietoa löydettävissä, vaikka Stuxnetin aikainen versio oli ladattu Virustotaliin. Toisaalta muualta mediasta oli saatavilla vihjeitä ja esimerkiksi Rollins ym. (2010, 5) nostavat esille aikaisemman sabotaasin Iranin sentrifugeja kohtaan. Lisäksi Iran oli myös huomioinut 1980–luvulla tapahtuneet ydinaseiden valmistamisiin liittyvät kineettiset iskut Irakissa sijoittamalla uraaninrikastamon maan alle mutta myös eristämällä laitoksen internetistä.

Toisena apukysymyksenä on selvittää onko Dark webistä löydettävissä APT-hyökkäyksiin käytettäviä hyökkäystyökaluja. Kyberuhkatiedustelutyökalujen puuttuminen korostui erityisesti toisen apukysymyksen osalta. Dark webistä löytyi esimerkkitapauksien raporteista valittujen hakusanojen osalta

tuloksia todella vähän ja nämäkin tulokset liittyivät hyvin yleisiin ohjelmiin. Lisäksi löydetyt tulokset olivat lähinnä apupyyntöjä tai esimerkiksi hakkerointityökalujen tai väärennettyjen dollareiden markkinointia eikä liittynyt APT-ryhmiin tai heidän työkaluihin tai ohjelmistoihin mitenkään.

4.6 Arviointi

Gradun tiedonhankintaa vaikeutti huomattavasti se, ettei tiedonhakuun ollut käytössä niin sanotusti oikean elämän työkaluja, vaan tiedonhaku painottui vahvasti Googleen ja muihin vapaasti sekä ilmaiseksi käytettäviin työkaluihin. Toisaalta myös opiskelijabudjetti rajoitti eikä ollut mahdollista sijoittaa rahaa esimerkiksi erilaisiin sosiaalisen median analysointityökaluihin, joilla olisi mahdollisesti saanut huomattavasti enemmän tietoa. Yllätys oli myös Social-Searcher työkalun rajoittuminen vuoteen 2012, jolloin sen hyödyllisyys Stuxnetin osalta oli olematonta. Lisäksi työkalussa hakutuloksissa oli hyvin vähän esimerkiksi Twitterin tuloksia, joka epäilytti ja jonka takia käyttöön otettiin laajempaan rooliin myös googlettaminen.

Tiedonhaussa näkyy myös se, ettei käytössä ollut esimerkiksi esimerkkitapauksien yrityksien omia logitietoja, jolloin esimerkiksi APT28-ryhmän nmap-ajoja ei voinut millään tutkia olisiko niitä ollut havaittavissa ja milloin porttiskannauksia tehtiin. Toisaalta APT28-ryhmän nmapin skannaamat portit olivat aika yleisesti käytössä olevia, mutta lähteissä korostettiin APT28-ryhmän osalta tapaa tehdä esimerkiksi tiettyjen maiden osalta laajamittaista porttiskannausta ja olisiko tällainen maanlaajuinen porttiskannaus noussut laajasti kerätyssä uhka-aineistossa esille poikkeamana. Tästä johtuen APT-ryhmien toimintaa kuvaavat raportit olivat aika korkean tason raportteja, joka vaikeutti ryhmien toiminnan arviointia kyberuhkaketjun vaiheisiin peilattaessa.

Lisäksi aineistona käytetyt APT-raportit eivät käsittele APT-ryhmien havaintoja peilaten Cyber Kill Chainin vaiheita vastaan. Tällöin on lähes mahdotonta pohtia sitä oliko ja olisiko jonkin käytetyn tietyn haittaohjelman tunnistavan ohjelmiston tai muun tietoturvakontrollin pitänyt havaita APT-ryhmän toimintaa vai ei. Toisaalta paljastamalla tällaista tietoa voi olla riski siitä, että kontrollia vastaan kehitetään vastatoimia, jolloin käytetyn haittaohjelman tunnistavan kontrollin hyödyllisyys alkaisi vähenemään.

Dark Webin osalta aikaisemmin mainitut tiedonhaun ongelmat korostuivat myös, mutta uutena haasteena oli useiden Top5- tai Top10 Dark web kauppapaikkoja esittelevien sivustojen sulkeutuminen. Esimerkiksi Shibi (2022) luettelee viisi yleisintä ja näistä Exploit.in sekä Dread olivat tutkimushetkellä alhaalla. Toisaalta tiedonhaussa korostui ongelmana myös se, että esimerkiksi Benchea (2015, 19) raportissa on listattu vain kolmet erilaiset APT28-ryhmän käyttämät työkalut, jolloin tiedonhaku kohdistui paljolti vain julkaistujen raporttien nimeämiin työkaluihin.

Tiedonhaun osalta korostui myös se, että esimerkiksi APT28-ryhmään liitetään Mitren Att&ck-sivustolla useita eri nimiä, kuten Swallowtail, Group 74,

Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM tai Tsar Team. Toisaalta APT28 on pääasiallisesti Mitren käyttämä nimi APT28-ryhmään attribuoiduille teoille. Siksi arvioinnissa keskeistä on pohtia sitä, että onko ryhmän toimintaan tutustuttu riittävällä kattavuudella vai ei. Toisaalta APT-ryhmien toimia käsiteltäessä virustorjuntayritykset joutuvat huomioimaan sitä, mitä ja millaisella tarkkuudella tietoa tapahtumista kerrotaan. Tällöin keskeistä on pohtia sitä, että ovatko valitut tapaukset edustavia APT-ryhmän toimintaan liittyen vai ei.

Keskeisiä tekijöitä arvioitaessa tehtyä tutkimusta on myös huomioida esimerkiksi jälkiviisausharha tai vahvistusharha. Valitut APT-tapaukset ovat aika vanhoja ja Stuxnet havaittiin jo vuonna 2010. Valitut APT1- ja APT28-tapaukset ovat vuosilta 2014 ja 2018 eli myös useita vuosia vanhoja. Tällöin keskeistä on pohtia esimerkiksi jälkiviisausharhan vaikutusta kerättäessä tietoa APT-ryhmien toimintaan liittyen. Roese & Vohs (2012, 411) toteavat jälkiviisausharhan olevan yksi yleisimmistä päätökseen liittyvistä ansoista, joka vaikuttaa yleisesti ihmisten päätöksiin. Jälkiviisausharhassa keskeistä on se, että tapahtuma mielletään jälkikäteen paljon ennakoitavammaksi kuin mitä tapahtuma oli tilanteen kehittyessä eikä tapahtumakulun lopputulosta tiedetty (Roese ym. 2012, 411). Keskeistä on siksi pohtia voidaanko kerättyjen havaintojen pohjalta todellakin todeta, että APT-hyökkäykset olisivat olleet havaittavissa jokaisen valitun APT-ryhmän hyökkäysvuosina. Esimerkiksi havaintojen vähyys korostuu jälkiviisausharhan osalta APT1-ryhmän tapauksessa, jolloin havaintoja oli kolme edelliseltä vuodelta APT1-ryhmään liittyen mutta vain yksi havainto vuodelta 2014, jolloin raportin yritys joutui APT-ryhmän hyökkäyksen kohteeksi. Miten helppoa olisi oikeasti ollut vuosina 2013–2014 tehdä nämä neljä havaintoa?

Jälkiviisausharhaan liittyy vahvasti myös vahvistusharha ja Lehner ym. (2008, 584) huomauttavat vahvistusharhan liittyvän ihmisten taipumukseen tehdä johtopäätöksiä pahimmillaan vain muutamien todisteiden pohjalta, jotka liittyvät ihmisten aikaisempiin asiaan liittyviin hypoteeseihin tai uskomuksiin. Lisäksi vahvistusharhaan liittyy se, että ihmisten pitää tietoisesti hankkia vallitsevia uskomuksia kyseenalaistavia todisteita (Lehner ym. 2008, 584). Keskeistä on pohtia miten vahvistusharha voisi ilmetä ja esiin nousee ainakin yleisesti vallitseva uskomus APT-ryhmien toiminnasta ja resurssoinnista. Tällöin keskeistä on pohtia miten uskomus siitä, että APT-ryhmien toiminnan havaitseminen on yleensä vaikeata ja APT-ryhmät toimivat piilossa useita vuosia voisi ilmetä tutkimuksen tuloksissa.

Vahvistusharhaan liittyen Lehner ym. (2008, 584) korostavat sitä, että monimutkaisemmissa analyyseissä ACH-menetelmän käyttö vähensi vahvistusharhan roolia mutta vahvistusharha ilmeni painotusharhana eikä väärien tulkintojen tekemisenä. Tällöin yhtä mieltä oltiin todisteiden tulkinnasta, mutta todisteiden tärkeydessä korostui niiden todisteiden painottaminen, jotka tukivat uskottuja hypoteeseja. Vastaavasti vähemmän painotettiin todisteita, jotka olivat hypoteeseja vastaan (Lehner ym. 2008, 584.). Tässä työssä ACH-menetelmää ei käytetty ja ainoastaan yhdessä APT-ryhmän havainnossa esiin nostettiin sosiaalisen median havainnon huomattava suosio.

Keskeinen tekijä arvioitaessa tutkimuksen tuloksia on siis se, että voidaanko kerätystä aineistosta tehdä tieteellistä tutkimusta. Haasteena on huomioida kerätyn aineiston vähäinen määrä sekä APT-ryhmien oman toiminnan turvaamiseen liittyvät käytännöt sekä tutkimuksen tiedonhakuun liittyvät haasteet. Toisaalta tähän liittyy myös attribuutio-ongelma eli kuinka esimerkiksi sosiaalisesta mediasta kerätyt havainnot on attribuoitu verrattuna esimerkiksi virustorjuntayrityksien raportteihin verrattuna. Edwards, Furnas, Forrest & Axelrod (2017, 2825) huomauttavat kyberympäristön osalta vaikeuksista osoittaa varmasti kuka teon takana oli. Tällaista vaikeutta korostaa sekä tekniset tekijät että määrittelyihin liittyvät ongelmat, kuten mitä määritellään esimerkiksi kyberhyökkäykseksi. Lisäksi tekijöinä voi olla eri tahoja, kuten valtio tai valtio voi hyödyntää muita tekijöitä toimintansa piilottamiseksi. Lisäksi digitaalisia todisteita voidaan väärentää, muokata tai tekoa voidaan naamioida näyttämään enemmän vahingolta kuin tahalliselta teolta. (Edwards ym. 2017, 2825.)

Tutkimuksen validiteetin osalta keskeistä on tarkastella sisäistä validiteettia eli onko tutkimuksen johtopäätös oikea vai onko johtopäätöksiin vaikuttaneet erilaiset häiriötekijät. Ulkoisen validiteetin osalta keskeinen ongelma liittyy tulosten yleistettävyyteen ja erityisesti tapaustutkimuksien osalta yleistettävyys on yleensä huonoa. Konstruktiovaliditeetin osalta keskeistä on tarkastella mitataanko sitä mitä oli tarkoitus mitata. Lisäksi kannattaa huomioida reliabiliteetti eli kuinka toistettavissa tutkimus olisi.

Keskeisenä haasteena tutkimuksessa korostuu sekä Dark webin että pintanetin tiedonhakeminen. Keskeistä on pohtia oliko tiedonhaku tehty oikein, sopivilla työkaluohjelmistoilla ja oikeilla hakusanoilla vai tehtiinkö näissä virheitä. Tiedonhaun osalta korostui sopivien työkalujen puute, jolloin tiedonhakua tehtiin yleisillä hakukoneilla sekä pintanetin että Dark webin osalta. Hakusanojen osalta hakusanat poimittiin esimerkkiraporteista ja peilattaessa näitä hakusanoja esimerkiksi APT1- tai APT28-ryhmän Mitren ATT&CK sivustoihin, on havaittavissa samoja hakusanoja. Lisäksi Mitren ATT&CK sivustolla korostuu sekä APT1- että APT28-ryhmien osalta kalastelu sekä erityisesti kohdistettujen tietojenkalasteluviestien hyödyntäminen. (Mitre ATT&CK APT1 2022; APT28 2021.) Tällöin valitut esimerkkitapaukset erityisesti APT1- ja APT28-ryhmien osalta ovat ainakin osittain edustavia mitä tulee APT1- ja APT28-ryhmien taktiikoihin, tekniikoihin sekä tunnettuihin työkaluihin.

Reliabiliteetin eli tutkimuksen toistettavuuden osalta haasteena on erityisesti Dark netin osalta tiedonhakemisen ongelmat, mutta myös esimerkiksi suosittujen kauppapaikkojen sulkeutumiset. Esimerkiksi tiedonhaku muutamista TOP5 Dark webin kauppapaikoista epäonnistui, koska tällaisia kauppapaikkoja oli suljettu. Tämän takia toista apututkimuskysymystä muutettiin. Jatkotutkimuksena olisi mielenkiintoista tehdä vastaavaa kyberuhkatiedustelua ihan oikeilla yrityksissä käytettävillä työkaluilla oikeassa yritysympäristössä.

LÄHTEET

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. *International Journal of Communication Networks and Information Security, 12(3), 326-337*. Verkkojulkaisu 20.11.2021. https://www.proquest.com/scholarly-journals/evolution-malware-threats-techniques-review/docview/2483989571/se-2?accountid=11774.

Alkhatib, B. & S. Basheer, R. (2019). Mining the Dark Web: A Novel Approach for Placing a Dark Website under Investigation. *International Journal of Modern Education and Computer Science, 11(10), 1–13*. Verkkojulkaisu 20.11.2021. https://doi.org/10.5815/ijmecs.2019.10.01.

Anashkin, Y. & Zhukova, M. (2021). Implementation of Behavioral Indicators in Threat Detection and User Behavior Analysis. Verkkojulkaisu 21.8.2022. http://ceur-ws.org/Vol-3094/paper_1.pdf.

Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K–K. R. & Javad, H. H. S. (2019). Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. *Journal of Information Processing Systems, 15(4).* Verkkojulkaisu 13.11.2022. https://doi.org/10.3745/JIPS.03.0126.

Benchea, R., Vatamanu, C., Maximciuc, A. & Luncasu, V. (2015). Bitdefender APT28 Under the Scope. A Journey into Exfiltrating Intelligence and Government Information. Verkkojulkaisu 12.11.2022. https://cdn2.hubspot.net/hubfs/341979/PDFs/Bitdefender_In-depth_analysis_of_APT28The_Political_Cyber-Espionage_Mal....pdf.

Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet 2012, 4, 971–1003*. Verkkojulkaisu 16.10.2022. https://doi.org/10.3390/fi4040971.

Bernaschi, M., Celestini, A., Cianfriglia, M., Guarino, S., Lombardi, F. & Mastrostefano, E. (2022). Onion under Microscope: An in-depth analysis of the Tor Web. *World wide web (Bussum), 25(3), 1287–1313*. Verkkojulkaisu 9.6.2022. https://doi.org/10.1007/s11280-022-01044-z.

Blake E., Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and Philosophy. Verkkojulkaisu 13.8.2022. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

Bromander, S., Swimmer, M., Muller, L. P., Jøsang, A., Eian, M., Skjøtskift, G. & Borg, F. (2022). Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge

Representation and Exchange. *Digital threats (Print), 3(1), 1–22*. Verkkojulkaisu 12.11.2021. https://doi.org/10.1145/3458027.

Brügger, N., Goggin, G., Milligan, I. & Schafer, V. (2017). Introduction: Internet Histories. *Digital Technology, Culture and Society, Volume 1, 2017, Issue 1–2, s. 1–7.* Verkkojulkaisu 6.11.2021. https://doi.org/10.1080/24701475.2017.1317128.

Bunda, J. (2020). APT28: tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007–2016. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/67845. 30.1.2023.

Collins, S. & McCombie, S. (2012). Stuxnet: The Emergence of a New Cyber Weapon and its Implications. *Journal of Policing, Intelligence and Counter Terrorism, 7(1), 80–91*. Verkkojulkaisu 1.9.2022. https://doi.org/10.1080/18335330.2012.653198.

Conti, M., Dargahi, T. & Deghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. Teoksessa Dehghantanha, A., Conti, M. & Dargahi, T. (toim.): *Cyber Threat Intelligence 2018*. Springer International Publishing AG.

Crowdstrike. (2021). IoA vs. IoC. Verkkojulkaisu 21.8.2022. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/.

CircleID. (2020). Revisiting APT1 IoCs with DNS and Subdomain Intelligence. Verkkojulkaisu 13.11.2022. https://circleid.com/posts/20201215-revisiting-apt1-iocs-with-dns-and-subdomain-intelligence/.

Cyware (2019). APT1: A Nation-State Adversary Attacking a Broad Range of Corporations and Government Entities Around the World. Verkkojulkaisu 13.11.2022. https://cyware.com/blog/apt1-a-nation-state-adversary-attacking-a-broad-range-of-corporations-and-government-entities-around-the-world-3041.

DeVore, M. R., & Lee, S. (2017). Apt(Advanced Persistent Threat)S and Influence: Cyber Weapons And The Changing Calculus Of Conflict. *The Journal of East Asian Affairs, 31(1), 39–64*. Verkkojulkaisu 21.11.2021. https://www.proquest.com/scholarly-journals/apt-advanced-persistent-threat-s-influence-cyber/docview/1994247718/se-2?accountid=11774.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic Aspects of Cyberattack, Attribution, and Blame. *Proceedings of the National Academy of Sciences - PNAS, 114(11), 2825–2830*. Verkkojulkaisu 15.1.2023. https://doi.org/10.1073/pnas.1700442114.

Ertaul, L. & Mouse, M. (2018). Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics. Verkkojulkaisu 13.8.2022. http://mcs.csueastbay.edu/~lertaul/SAM9723.pdf.

Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the Future of CyberWar. *Survival, Global Politics and Strategy, Volume 53:1, 23–40*. Verkkojulkaisu 30.10.2022. https://doi.org/10.1080/00396338.2011.555586.

FireEye (2019). APT41 – Double Dragon. APT41, a Dual Espionage and Cyber Crime Operation. Verkkojulkaisu 27.8.2022. https://content.fireeye.com/apt-41/rpt-apt41.

FireEye. (2014). APT28: A Window into Russia's Cyber Espionage Operations? Verkkojulkaisu 12.11.2022. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

Georgiev, D. (2022). Most Popular Search Engines for Dark Web. Verkkojulkaisu 18.12.2022. https://techjury.net/blog/most-popular-search-engines-for-dark-web/.

Haque, M. F. & Krishnan, R. (2021). Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence. *Information Systems Frontiers, 23(4), 883–896*. Verkkojulkaisu 13.11.2021. https://doi.org/10.1007/s10796-020-10103-7.

Hatta, M. (2020). Deep web, dark web, dark net: A taxonomy of "hidden" internet. *Annals of Business Administrative Science, Volume 19, 2020. Issue 6. s 277–292*. Verkkojulkaisu 6.11.2021. https://dx.doi.org/10.7880/abas.0200908a.

Haga, K., Meland, P.H., Sindre, G. (2020). Breaking the Cyber Kill Chain by Modelling Resource Costs. Teoksessa Eades III, H., Gadyatskaya, O. (toim.), *Graphical Models for Security. GraMSec 2020*. Lecture Notes in Computer Science(), vol 12419, s. 111–126. Springer, Cham. Verkkojulkaisu 1.8.2022. https://doi-org.ezproxy.jyu.fi/10.1007/978-3-030-62230-5_6.

Hoffmann, R. (2020). Stochastic Model of the Simple Cyber Kill Chain: Cyber Attack Process as a Regenerative Process. Teoksessa Saeed, K., Dvorský, J. (eds) *Computer Information Systems and Industrial Management. CISIM 2020*. Lecture Notes in Computer Science(), vol 12133, s. 355–365. Springer, Cham. Verkkojulkaisu 31.7.2022. https://doi.org/10.1007/978-3-030-47679-3_30.

Hutchins, E. M., Cloppert, M. J. & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Verkkojulkaisu 7.8.2022. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Jardine, E. (2018). Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society*, 20(8), 2824–2843. Verkkojulkaisu 5.7.2022. https://doi.org/10.1177/1461444817733134.

Jensen, B., Valeriano, B., & Maness, R. (2019) Fancy bears and digital trolls: Cyber strategy with a Russian twist, *Journal of Strategic Studies*, 42:2, 212–234, Verkkojulkaisu 21.11.2021. https://doi.org/10.1080/01402390.2018.1559152.

Johansson, M. (2021). Venäjän ja Kiinan sotilastiedusteluorganisaatioiden kybermenetelmien kehitys vuosina 2004–2021. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/75923.

Karsikas, J. (2021). Monitapaustutkimus valikoiduista Kiinaan ja Venäjään liitetyistä kyberhyökkäysryhmistä: kohdennetut haittaohjelmahyökkäykset. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/75892.

Kataja, M. (2019). Cyber Threat Intelligence. Verkkojulkaisu 5.2.2023. https://jyx.jyu.fi/handle/123456789/66566

Kaur, S. & Randhawa, S. (2020) Dark Web: A Web of Crimes. *Wireless Personal Communications* 112, 2131–2158 (2020). Verkkojulkaisu 7.11.2021. https://doi-org.ezproxy.jyu.fi/10.1007/s11277-020-07143-2.

Kawaguchi Y., Ozawa S. (2019) Exploring and Identifying Malicious Sites in Dark Web Using Machine Learning. Teoksessa Gedeon T., Wong K., Lee M. (toim.), *Neural Information Processing. ICONIP 2019*. Lecture Notes in Computer Science, vol 11955, s 319–327. Springer, Cham. Verkkojulkaisu 15.11.2021. https://doi.org/10.1007/978-3-030-36718-3_27.

Kianpour, M. (2021). Socio-Technical Root Cause Analysis of Cyber-enabled Theft of the U.S. Intellectual Property – The Case of APT41. Verkkojulkaisu 24.8.2022. https://www.researchgate.net/publication/349914331_Socio-Technical_Root_Cause_Analysis_of_Cyber-enabled_Theft_of_the_US_Intellectual_Property_--_The_Case_of_APT41.

Kost, E. (2022). What are Indicators of Attack (IOAs)? How they Differ from IOCs. Verkkojulkaisu 28.1.2023. https://www.upguard.com/blog/what-are-indicators-of-attack.

Kuhalampi, M. (2018). APT–kohdistettu hyökkäys. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/58026.

Kure, H. I. & Islam, S. (2019). Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. *Journal of Universal Computer Science*, 25(11), 1478–1502. Verkkojulkaisu 8.11.2021. https://doi.org/10.3217/jucs-025-11-1478.

Laine, M., Bamberg, J., & Jokinen, P. (2007). Tapaustutkimuksen käytäntö ja teoria. Teoksessa Laine, M., Bamberg, J., & Jokinen P. (toim.): *Tapaustutkimuksen taito*. Gaudeamus Helsinki University Press.

Lee, B., Harbinson, M. & Falcone, R: (2018). Sofacy Attacks Multiple Government Entities. Verkkojulkaisu 5.11.2022.

https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/.

Lehner, P. E., Adelman, L., Cheikes, B. A. & Brown, M. J. (2008). Confirmation Bias in Complex Analyses. *IEEE Transactions on Systems, Man, and Cybernetics* – Part A: Systems and Humans, vol. 38, no. 3, pp. 584–592, May 2008. Verkkojulkaisu 14.1.2023. https://doi.org/10.1109/TSMCA.2008.918634.

Lehto, I. (2020). Poliittisesti motivoitunut kybervakoilu ja tiedustelutoiminta. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/73423.

Lehto, M. (2022). APT Cyber-attack Modelling: Building a General Model. Teoksessa R. P. Griffin, U.Tatarand, & B. Yankson (toim.), *ICCWS 2022: Proceedings of the 17th International Conferenceon Cyber Warfare and Security*, 17, s. 121–129). Academic Conferences International Ltd. The proceedings of the 17th international conference on cyber warfare and security. Verkkojulkaisu 10.8.2022. https://doi.org/10.34190/iccws.17.1.36.

Lemay, A., Calvet, J., Menet, F. & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, 72, 26–59. Verkkojulkaisu24.11.2021. https://doi.org/10.1016/j.cose.2017.08.005.

Lockheed Martin. (2015). Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Verkkojulkaisu 14.8.2022. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf.

Mandiant (2014). APT1 – Exposing One of China's Cyber Espionage Units. Verkkojulkaisu 21.11.2021. https://www.mandiant.com/media/9941/download.

Marsh, R. T. (1997). Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Verkkojulkaisu 5.11.2022. https://sgp.fas.org/library/pccip.pdf.

Matilainen, J. (2021). Using Cyber Threat Intelligence as a Part of Organizational Cybersecurity. Verkkojulkaisu 5.2.2023. https://jyx.jyu.fi/handle/123456789/76092

McDonald, G., Murchu, L. O., Doherty, S. & Chie, E. (2013). Stuxnet 0.5: The Missing Link. Verkkojulkaisu 17.10.2022. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en,.

Mitre ATT&CK (2022). APT1. Verkkojulkaisu 28.1.2023. https://attack.mitre.org/groups/G0006/.

Mitre ATT&CK (2021). APT28. Verkkojulkaisu 28.1.2023. https://attack.mitre.org/groups/G0007/.

Moinescu, R. & Glävan, D. (2018). Frequently Used Methods in the Preparation of the Informational Attack. *Scientific Bulletin ("Mircea cel Bătrân" Naval Academy), XIX(1), 97–102*. Verkkojulkaisu 14.1.2023. https://doi.org/10.21279/1454-864X-18-I1-014.

Moore, D. & Rid, T. (2016) Cryptopolitik and the Darknet. *Survival, Global Politics and Strategy*, 58:1, 7–38. Verkkojulkaisu 10.7.2022. https://doi.org/10.1080/00396338.2016.1142085.

Mwiki, H., Dargahi, T., Dehghantanha, A. & Choo, K–K. R. (2019). Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. Teoksessa Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (toim.), *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*, s. 221–244. Springer, Cham. Verkkojulkaisu 13.11.2022. https://doi.org/10.1007/978-3-030-00024-0_12.

Naughton, J. (2016). The Evolution of the internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, Volume 1, 2016, Issue 1. s. 5–28. Verkkojulkaisu 6.11.2021. https://doi.org/10.1080/23738871.2016.1157619.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., & Shakaria P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. *IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 7–12. Verkkojulkaisu 15.11.2021. https://doi.org/10.1109/ISI.2016.7745435.

Oosthoek, K. & Doerr, C. (2021). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and Counterintelligence*, 34(2), 300-315. Verkkojulkaisu 9.11.2021. https://doi.org/10.1080/08850607.2020.1780062.

Owen, G. & Savage, N. (2016). Empirical analysis of Tor Hidden Services. *IET Information Security*, 10(3), 113–118. Verkkojulkaisu 10.7.2022. https://doi.org/10.1049/iet-ifs.2015.0121.

Paavilainen, P. (2014). *Psykologian tutkimustyöopas*. Otavan kirjapaino.

Peltola, T. (2007). Empirian ja teorian vuoropuhelu. Teoksessa Laine, M., Bamberg, J., & Jokinen P. (toim.): *Tapaustutkimuksen taito*. Gaudeamus Helsinki University Press.

Peuhkuri, T. (2007). Teoria ja yleistämisen kriteerit. Teoksessa Laine, M., Bamberg, J., & Jokinen P. (toim.): *Tapaustutkimuksen taito.* Gaudeamus Helsinki University Press.

Preuveneers, D., Joosen, W., Bernal Bernabe, J. & Skarmta, A. (2020). Distributed Security Framework for Reliable Threat Intelligence Sharing. *Security and Communication Networks*, 2020, 1–15. Verkkojulkaisu 13.11.2021. https://doi.org/10.1155/2020/8833765.

Quintero-Bonilla, S., & Angel Martín, d. R. (2020). A new proposal on the advanced persistent threat: A survey. *Applied Sciences*, 10(11), 3874. Verkkojulkaisu 20.11.2021. http://dx.doi.org/10.3390/app10113874.

RedDrip7. APT_Digital_Weapon. Verkkojulkaisu 14.1.2023. https://github.com/RedDrip7/APT_Digital_Weapon.

Resh, A. (2016). Enforcing trust for execution-protection in modern environments. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/52371.

Rollins, J., Name Redacted, & Name Redacted. (2010). The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. *CRS Report for Congress Prepared for Members and Committees of Congress*. Verkkojulkaisu 5.9.2022. https://www.everycrsreport.com/files/20101209_R41524_baf11ede95c2db6d49b908a0ca783653a7668527.pdf.

Roese, N. J., & Vohs, K. D. (2012). Hindsight Bias. *Perspectives on Psychological Science, 7(5), 411–426*. Verkkojulkaisu 14.1.2023. https://doi-org.ezproxy.jyu.fi/10.1177/1745691612454303.

Samtani, S., Li, W., Benjamin, V. & Chen, H. (2021). Informing Cyber Threat Intelligence through Dark Web Situational Awareness: The AZSecure Hacker Assets Portal. *Digital Threats: Research and Practice*, 2(4), 1–10. Verkkojulkaisu 20.11.2021. https://doi.org/10.1145/3450972.

Schlette, D., Caselli, M., & Pernul, G. (2021). "A comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective,". *IEEE Communications Surveys & Tutorials,* 23:4, 2525–2556. Verkkojulkaisu 8.11.2021. https://doi.org/10.1109/COMST.2021.3117338.

Shibi, Y. (2022). Top 5 Hacker Forums on the Deep and Dark Web in 2022. Verkkojulkaisu 1.1.2023. https://webz.io/dwp/top-5-hacker-forums-on-the-deep-and-dark-web-in-2022/.

Shillito, M. R. (2019). Untangling the 'Dark Web' : an emerging technological challenge for the criminal law. *Information & Communications Technology Law*, 28(2), 186-207. Verkkojulkaisu 19.9.2021. https://doi.org/10.1080/13600834.2019.1623449

Siukonen, V. (2019). APT-operaation inhimilliset tekijät: operaation tarkastelu päätöksenteon näkökulmasta. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/64330.

Social-Searcher. Free Social Media Search Engine. Verkkojulkaisu 5.1.2023. https://www.social-searcher.com/pricing/.

Sood, A. K. & Enbod, R. (2014). *Targeted Cyber Attacks – Multi-staged Attacks Driven by Exploits and Malware*. Syngress publications.

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality oftechnical malware reports and the case of Stuxnet. *Contemporary Security*

Policy, 41:1, 129–152. Verkkojulkaisu 17.10.2022. https://doi.org/10.1080/13523260.2019.1675258.

Särökaari, N. (2020). Phishing attacks and mitigation tactics. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/72569.

Tatam, M., Shanmugam, B., Azam, S. & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, Volume 7, Issue 1, 2021, e05969, ISSN 2405-8440. Verkkojulkaisu 7.8.2022. https://doi.org/10.1016/j.heliyon.2021.e05969.

Teirivaara, T. (2017). Tietoturvan ihmiselementti: sosiaalinen manipulointi. Verkkojulkaisu 30.1.2023. https://jyx.jyu.fi/handle/123456789/55852.

Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2022). Key requirements for the detection and sharing of behavioral indicators of compromise. *Electronics*, 11(3), 416. Verkkojulkaisu 20.8.2022. https://doi.org/10.3390/electronics11030416.

Yang W., Lam KY. (2020) Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC. Teoksessa: Zhou J., Luo X., Shen Q., Xu Z. (toim.*) Information and Communications Security. ICICS 2019*. Lecture Notes in Computer Science, vol 11999, 145–164. Springer, Cham. Verkkojulkaisu 8.11.2021. https://doi.org/10.1007/978-3-030-41579-2_9.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, Volume 39, 2016. Issue 3. Journal of Cyber Policy, Volume 1, 2016, Issue 1. s. 195–206. Verkkojulkaisu 6.11.2021. https://doi.org/10.1080/1057610X.2015.1119546.

Xing, K., Li, A., Jiang, R., Jia, Y. (2021). Detection and Defense Methods of Cyber Attacks. Teoksessa: Jia, Y., Gu, Z., Li, A. (toim.) *MDATA: A New Knowledge Representation Model.* Lecture Notes in Computer Science, vol 12647, 185–198. Springer, Cham. Verkkojulkaisu 14.8.2022. https://doi-org.ezproxy.jyu.fi/10.1007/978-3-030-71590-8_11.

Zsolt, B., & Tamas, S. (2020). Cyber espionage through botnets. *Security Journal*, 33(1), 43–62. Verkkojulkaisu 27.8.2022. https://doi.org/10.1057/s41284-019-00194-6.