Mikko Tuomas Lintula

KANSALLISEN TURVALLISUUSAUDITOINTIKRITEERISTÖN ANTAMA SUOJA KOHDISTETTUJA HAITTAOHJELMAHYÖKKÄYKSIÄ VASTAAN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Lintula, Mikko Tuomas
Kansallisen turvallisuusauditointikriteeristön antama suoja kohdistettuja haittaohjelmahyökkäyksiä vastaan
Jyväskylä: Jyväskylän yliopisto, 2022, 64 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Tässä tutkimuksessa tarkastellaan tapahtuneita kohdistettuja haittaohjelmahyökkäyksiä ja ehdotetaan vastatoimia niiden torjumiseksi. Tutkimuksen teoriaosuuden tarkoituksena on taustoittaa varsinaista tutkimusta ja antaa lukijalle riittävät perustiedot tutkimusaiheesta. Tutkimuksen empiirisessä osuudessa tutkittiin tapahtuneita kohdistettuja haittaohjelmahyökkäyksiä niiden toteutuksessa käytettyjen taktiikoiden ja tekniikoiden näkökulmasta. Tutkimuksessa pyrittiin myös selvittämään, onko kansallisessa tietoturvallisuusauditointikriteeristössä puutteita kohdistetuilta haittaohjelmahyökkäyksiltä suojautumiseksi. Tutkimuksen aihe on tärkeä, sillä tutkimuksessa voidaan löytää puutteita laajasti käytössä olevasta viranomaisten turvallisuusluokitellun tiedon suojaamiseksi käytettävästä auditointikriteeristöstä. Tutkimuksen empiirinen osuus toteutettiin monitapaustutkimuksena ja aineistoa analysoitiin aineistolähtöistä sisällönanalyysiä käyttäen. Tutkimusmateriaali kerättiin julkisesti saatavissa olevista lähteistä. Tutkimuksen empiirisessä osuudessa havaittiin, että kohdistetuille haittaohjelmahyökkäyksille on tyypillistä käyttää samankaltaisia taktiikoita ja tekniikoita. Tyypillisimmiksi taktiikoiksi paljastui avointen lähteiden tiedustelu, tietojenkalastelu ja nollapäivähaavoittuvuuksien hyödyntäminen. Tutkimuksen perusteella hyökkäysten torjumiseksi henkilöstön koulutus, poikkeamien havainnointikyky ja onnistunut riskienhallinta ovat olennaisessa osassa. Kansallista turvallisuusauditointikriteeristöä noudattamalla voidaan torjua niin teollisuusympäristöön kuin salassa pidettävään tietoon kohdistettuja hyökkäyksiä. Kriteeristön heikkouksiksi havaittiin vaatimusten yleisluontoisuus, puhelinten ja IOT-laitteiden vähäinen huomiointi sekä SOC-toiminnon puuttuminen.

Asiasanat: Kohdistettu haittaohjelmahyökkäys, MITRE ATT&CK, ADDRR, Kansallinen turvallisuusauditointikriteeristö

ABSTRACT

Lintula, Mikko Tuomas
Protection against advanced persistent threat attacks provided by the National Security Auditing Criteria
Jyväskylä: University of Jyväskylä, 2022, 64 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

This study examines the advanced persistent threat attacks that have occurred and suggests countermeasures to combat them. The purpose of the theory part of the research is to provide a background to the actual research and to give the reader sufficient basic information about the research topic. In the empirical part of the study, the advanced persistent threat attacks that have occurred were investigated from the perspective of the tactics and techniques used in their implementation. The study also sought to find out whether there are any shortcomings in the national security auditing criteria for protecting against advanced persistent threat attacks. The topic of the research is important because the research can find flaws in the widely used audit criteria used to protect information classified as security by the authorities. The empirical part of the research was carried out as a multi-case study and the material was analyzed using material-based content analysis. The research material was collected from publicly available sources. In the empirical part of the study, it was found that it is typical for advanced persistent threat attacks to use similar tactics and techniques. The most typical tactics turned out to be intelligence on open sources, phishing and exploiting zero-day vulnerabilities. Based on the research, personnel training, the ability to detect deviations and successful risk management are an essential part of combating attacks. By following the national security auditing criteria, attacks targeting the industrial environment as well as confidential information can be countered. Weaknesses of the criteria were found to be the general nature of the requirements and little consideration of telephones and IOT devices.

Keywords: Advanced Persistent Threat, MITRE ATT&CK, ADDRR, National Security Auditing Criteria

KUVIOT

KUVIO 1 Katakrin osa-alueet 14
KUVIO 2 Koonti hyökkäysten kohteiden turvallisuusjohtamisen puutteista.... 54
KUVIO 3 Koonti hyökkäysten kohteiden fyysisen turvallisuuden puutteista .. 55
KUVIO 4 Koonti hyökkäysten kohteiden teknisen tietoturvallisuuden puutteista 56

TAULUKOT

TAULUKKO 1 Aineiston hakuprosessi 17
TAULUKKO 2 BlackEnergyn hyökkäystaktiikat ja -tekniikat..... 20
TAULUKKO 3 Duqun hyökkäystaktiikat ja -tekniikat..... 22
TAULUKKO 4 Flamen hyökkäystaktiikat ja -tekniikat 24
TAULUKKO 5 GhostNetin hyökkäystaktiikat ja -tekniikat..... 27
TAULUKKO 6 Havexin hyökkäystaktiikat ja -tekniikat 29
TAULUKKO 7 Industroyerin hyökkäystaktiikat ja -tekniikat..... 31
TAULUKKO 8 Pegasuksen hyökkäystaktiikat ja -tekniikat 33
TAULUKKO 9 Shamoonin hyökkäystaktiikat ja -tekniikat 35
TAULUKKO 10 Stuxnetin hyökkäystaktiikat ja -tekniikat 37
TAULUKKO 11 Tritonin hyökkäystaktiikat ja -tekniikat..... 39
TAULUKKO 12 Hyökkäysten kohteiden puutteet turvallisuusjohtamisessa.... 43
TAULUKKO 13 Hyökkäysten kohteiden puutteet fyysisessä turvallisuudessa 44
TAULUKKO 14 Hyökkäysten kohteiden puutteet teknisessä tietoturvallisuudessa 50

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 7
1.1 Tutkimuksen tavoite 8
1.2 Tutkimuskysymykset 8
1.3 Tutkimuksen keskeiset käsitteet ja rakenne 8

2 TEOREETTINEN VIITEKEHYS 9
2.1 Kohdistettu haittaohjelmahyökkäys 9
2.2 MITRE ATT&CK 10
2.3 ADDRR 12
2.4 Kansallinen turvallisuusauditointikriteeristö 13
2.4.1 Turvallisuusjohtaminen 14
2.4.2 Fyysinen turvallisuus 14
2.4.3 Tekninen tietoturvallisuus 15

3 TUTKIMUSMETODIT 16
3.1 Aineistonkeruumenetelmä 16
3.2 Aineistonanalyysimenetelmä 18
3.3 Tutkimuksen luotettavuus 18

4 TARKASTELTUJEN KOHDISTETTUJEN HAITTAOHJELMAHYÖKKÄYSTEN TOTEUTUS 19
4.1 BlackEnergy 19
4.2 Duqu 21
4.3 Flame 23
4.4 GhostNet 25
4.5 Havex 28
4.6 Industroyer 29
4.7 Pegasus 32
4.8 Shamoon 34
4.9 Stuxnet 36
4.10 Triton 38

5 HYÖKKÄYSTEN HUOMIOINTI KATAKRI-KRITEERISTÖN AVULLA 41
5.1 Turvallisuusjohtaminen 41
5.2 Fyysinen turvallisuus 43
5.3 Tekninen tietoturvallisuus 45

6 POHDINTA 51

7 YHTEENVETO 58

LÄHTEET 60

1 JOHDANTO

Yhteiskunnan digitalisaatio on tuonut mukanaan uudenlaisia uhkia niin organisaatioille kuin yksityisille ihmisille. Tiedon siirtyessä sähköiseen muotoon (Lehto, 2022) ja sen määrän massiivinen kasvu on tuonut mukanaan rikollisten ja vakoilun siirtymisen myös sähköiseen ympäristöön. Psykoterapiakeskus Vastaamon tietomurto (Poliisi, 2022) on valitettava esimerkki huonosti hoidetun tietoturvallisuuden ja kyberrikollisuuden aiheuttamasta uhkasta ihmisten yksityisyydelle. Poliisin mukaan Vastaamon tietomurrossa on tiedossa jopa noin 22 000 asianomistajaa. Ihmisten yksityisyyttä loukkaavien tietomurtojen lisäksi (Lehto, 2021, s. 68–71) erityisen haitallisia kyberhyökkäyksiä ovat olleet yhteiskunnan kriittiseen infrastruktuuriin kohdistuvat hyökkäykset ja (Lehto, 2021, s. 59–62) kybervakoilu. Yhteiskunnan kriittiseen infraan (Lehto, 2021, s. 71) kohdistuvat hyökkäykset voivat haitata merkittävästi yhteiskunnan elintärkeitä toimintoja ja aiheuttaa ihmishenkien menetystä. Esimerkkinä (Lehto, 2021, s. 70) yhteiskunnan kriittiseen infraan kohdistuneesta hyökkäyksestä on ukrainalaiseen sähköyhtiöön kohdistunut kyberhyökkäys, jonka seurauksena 225 000 ihmistä jäi ilman sähköä kuudeksi tunniksi. Kybervakoilulla (Lehto, 2021, s. 59) pyritään hankkimaan salaista tietoa kohteesta käyttäen laittomia menetelmiä. Vakoilulla on tavoitteena lisätä ymmärrystä ja vaikuttaa haitallisesti vakoilun kohteen toimintaan. Lehdon mukaan (2021, s. 60) muun muassa Suomen poliittiseen päätöksentekoon ja kansantaloudellisesti merkittäviin yrityksiin kohdistetaan edistyksellistä kybervakoilua. Samanlaisia ajatuksia (Suojelupoliisi, 2021, s. 18) kybervakoilun kohteista ja haitoista on esitetty myös Suojelupoliisin vuosikirjassa 2020. Esimerkkinä (Suojelupoliisi, 2022, s. 4–5) Suomen valtiolliseen päätöksentekoon kohdistuneesta kybervakoilusta on eduskuntaan kohdistunut APT31-kybervakoiluoperaatio. Operaatiossa (Lehto, 2021, s. 62) valtiollinen toimija yritti tunkeutua eduskunnan tietojärjestelmiin.

1.1 Tutkimuksen tavoite

Tämän tutkimuksen tavoitteena on löytää kohdistetuissa haittaohjelmahyökkäyksissä käytetyt taktiikat ja tekniikat sekä vastatoimia niitä vastaan. Lisäksi tavoitteena on löytää mahdollisia puutteita kansallisessa turvallisuusauditointikriteeristössä kohdistettuilta haittaohjelmahyökkäyksiltä suojautumisen osalta sekä ehdottaa muutoksia kriteeristöihin.

1.2 Tutkimuskysymykset

- Miten kohdistetut haittaohjelmahyökkäykset ovat tapahtuneet?
- Millaisilla vastatoimilla voidaan estää kohdistettuja haittaohjelmahyökkäyksiä?
- Onko kansallisen turvallisuusauditointikriteeristön vaatimuksissa puutteita kohdistettujen haittaohjelmahyökkäysten ehkäisemiseksi?

1.3 Tutkimuksen keskeiset käsitteet ja rakenne

Kohdistettu haittaohjelmahyökkäys (engl. advanced persistent threat, APT) on Turvallisuuskomitean (2018, s. 31) määritelmän mukaan tiettyyn rajattuun kohteeseen kohdistettu hyökkäys. Kohdistetut haittaohjelmahyökkäykset ovat yleensä luonteeltaan monivaiheisia, pitkäkestoisia ja APT-ryhmien toteuttamia.

MITRE ATT&CK (MITRE, 2022a) on kaikille avoin tietokanta kyberhyökkääjien käyttämistä taktiikoista ja tekniikoista. Tietokannan tietopohja perustuu tosielämän havaintoihin ja sitä käytetään yleisesti perustana uhkamallien ja -menetelmien kehittämiselle kyberturvallisuusalalla.

ADDRR (Henneberg, 2020) on toimintamalli, jolla pyritään oppimaan tapahtuneista kyberhyökkäyksistä turvallisuuden edistämiseksi. Tällä lähestymistavalla mahdollistetaan organisaation mukautuminen uusiin kyberuhkiin.

Kansallinen turvallisuusauditointikriteeristö (Katakri) (Turvallisuuskomitea, 2018, s. 13) on pääasiassa viranomaisten käyttöön tarkoitettu arviointityökalu. Sen avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisten turvallisuusluokiteltua tietoa.

Pro Gradu tutkielma on jaettu teoreettiseen viitekehykseen ja varsinaiseen tutkimusosaan. Luvussa kaksi keskitytään tutkimuksen teoreettiseen viitekehykseen ja avataan yksityiskohtaisemmin tutkimuksen keskeisiä käsitteitä. Luvussa kolme selitetään tutkimuksessa käytetyt tutkimusmenetelmät. Luvuissa neljä ja viisi kerrotaan tutkimuksen tulokset. Luvussa kuusi tehdään tutkimuksen johtopäätökset ja pohdinnat tutkimustuloksista. Luvussa seitsemän on lyhyt yhteenveto keskeisimmistä tutkimustuloksista.

2 TEOREETTINEN VIITEKEHYS

Tähän sisältölukuun sisältyy alakappaleet kohdistetuista haittaohjelmahyökkäyksistä, hyökkäyksissä käytetyistä taktiikoista ja tekniikoista, hyökkäysten torjuntakeinoista ja kansallisesta turvallisuusauditointikriteeristöstä. Näissä alakappaleissa avataan tutkimuksen keskeisiä käsitteitä yksityiskohtaisemmin. Tämän kappaleen tarkoituksena on antaa lukijalle riittävät lähtötiedot varsinaisen tutkimuksen aihesisällöstä.

2.1 Kohdistettu haittaohjelmahyökkäys

Kuten kappaleessa 1.3 todettiin kohdistettu haittaohjelmahyökkäys (Turvallisuuskomitea, 2018, s. 31) tarkoittaa tiettyyn rajattuun kohteeseen kohdistettua hyökkäystä. Kohdistetut haittaohjelmahyökkäykset ovat yleensä luonteeltaan monivaiheisia, pitkäkestoisia ja APT-ryhmien toteuttamia.

APT-ryhmät (Turvallisuuskomitea, 2018, s. 31) ovat itsenäisesti tai valtiollisen toiminnan tuella toimivia organisoituneita hakkeriryhmiä. APT-ryhmillä (Hutchins ym., 2011, s. 1–2) on hyvät resurssit ja koulutus toteuttaa kohdistettuja hyökkäyksiä. Usein näissä hyökkäyksissä on tavoitteena hankkia korkean profiilin kohteista kriittistä tietoa tai muuttaa hyökkäyksen kohteen toimintaa. APT-ryhmille (Mandiant, 2022a) tyypillisiä hyökkäyksen kohteita ovat valtioiden sotavoimat, kriittinen infrastruktuuri, poliittinen päätöksenteko sekä teknologiateollisuus.

Tunnettuja APT-ryhmiä on kymmenittäin (Mandiant, 2022a). Hyvänä esimerkkinä APT-ryhmien (Clayton, 2012) tekemistä kohdistetuista haittaohjelmahyökkäyksistä voidaan pitää Operaatio Auroraa. Operaatio Aurorassa Kiinaan liitetty Elderwood APT-ryhmä teki hyökkäyksiä useaa yhdysvaltalaista yritystä vastaan. Operaatiossa APT-ryhmä hankki arvokasta tietoa hyökkäysten kohteena olleista yrityksistä ja sai aikaan Googlen poistumisen Kiinan markkinoilta. Operaatiossa käytetyistä toimintatavoista on voitu päätellä, että hyökkäysten

tavoitteena on ollut nimenomaan kerätä hyökkääjälle arvokasta tietoa ei niinkään aiheuttaa välittömiä taloudellisia vahinkoja.

2.2 MITRE ATT&CK

Kuten kappaleessa 1.3 alustettiin MITRE ATT&CK (MITRE, 2022a) on kaikille avoin tietokanta kyberhyökkääjien käyttämistä taktiikoista ja tekniikoista. Tietokannan tietopohja perustuu tosielämän havaintoihin ja sitä käytetään yleisesti perustana uhkamallien ja -menetelmien kehittämiselle kyberturvallisuusalalla. The MITRE Corporation (MITRE, 2022e) kehitti MITRE ATT&CK vuonna 2013 tarpeeseen dokumentoida hyökkääjän käyttäytymistä heidän tutkimusprojektissaan nimeltä FMX.

ATT&CK (MITRE, 2022e) koostuu kahdesta osasta: ATT&CK for Enterprise ja ATT&CK for Mobile. ATT&CK for Mobile käsittää hyökkääjän toimet mobiililaitteita vastaan ja ATT&CK for Enterprise puolestaan hyökkääjän toiminnan organisaation tietoverkoissa ja pilvipalveluissa. ATT&CK for Enterprise koostuu (MITRE, 2022c) yhteensä 14 taktiikasta ja niiden alaisista tekniikoista, joilla hyökkääjä pyrkii tavoitteisiinsa:

1. **Tiedustelu** (eng. reconnaissance). Hyökkääjän (MITRE, 2020a) tavoitteena on kerätä tietoa hyökkäyksen kohteesta mahdollista hyökkäystä varten. Yleisesti käytettäviä tekniikoita tiedusteluun ovat tietojenkalastelu ja kohdeverkkojen skannaaminen.
2. **Resurssien kehittäminen** (eng. resource development). Hyökkääjän (MITRE, 2020b) tavoitteena on hankkia resursseja tukemaan varsinaista hyökkäystä. Tyypillisiä tekniikoita resurssien kehittämiseen ovat murrettujen käyttötilien ja hyökkäysinfrastruktuurin hankkiminen.
3. **Alustava sisäänpääsy** (eng. initial access). Hyökkääjän (Lehto, 2022) tavoitteena on päästä sisään hyökkäyksen kohteen verkkoon. Tyypillisiä (MITRE, 2019h) tartuntavektoreita ovat sähköpostien liitetiedostot, huijausverkkosivut ja USB-laitteet.
4. **Suoritus** (eng. execution). Hyökkääjän (Lehto, 2022) tavoitteena on pystyä ajamaan haitallista koodia hyökkäyksen kohteessa. Tyypillisiä tekniikoita (MITRE, 2019e) ovat skriptien ajaminen etäyhteyden kautta tai huijata kohdekoneen käyttäjä ajamaan haitallista koodia.
5. **Pysyvyys** (eng. persistence). Hyökkääjän (Lehto, 2022) tavoitteena on pysyä hyökkäyksen kohteessa. Tyypillisiä tekniikoita (MITRE, 2019j) ovat kohdejärjestelmän käynnistysprosessien ja autentikointiprosessien muuttaminen.
6. **Käyttöoikeuksien laajentaminen** (eng. privilege escalation). Hyökkääjän (Lehto, 2022) tavoitteena on saada korkeammat käyttöoikeudet hyökkäyksen kohteessa. Tyypillisiä tekniikoita (MITRE, 2021a) ovat käynnistysprosessien muuttaminen ja ohjelmistohaavoittuvuuksien hyödyntäminen.

7. **Puolustuksen välttely** (eng. defense evasion). Hyökkääjän (Lehto, 2022) tavoitteena on vältellä kiinnijäämistä. Tyypillisiä tekniikoita (MITRE, 2019c) ovat tietoturvallisuusohjelmistojen poistaminen käytöstä ja haitallisten tiedostojen maskeeraaminen.
8. **Valtuutettu sisäänpääsy** (eng. credential access). Hyökkääjän (Lehto, 2022) tavoitteena on varastaa tunnistetietoja. Tyypillisiä tekniikoita (MITRE, 2019b) ovat välimieshyökkäys tunnisteiden kaappaamiseksi ja näppäinnauhurien käyttö.
9. **Tutkinta** (eng. discovery). Hyökkääjän (Lehto, 2022) tavoitteena on selvittää hyökkäyksen kohteen sisäinen rakenne. Tyypillisiä tekniikoita (MITRE, 2019d) ovat tietoliikenteen ja prosessien seuraaminen.
10. **Liikkuminen** (eng. lateral movement). Hyökkääjän (Lehto, 2022) tavoitteena on pystyä liikkumaan hyökkäyksen kohteessa. Tyypillisiä tekniikoita (MITRE, 2019i) ovat kohteen sisäinen tietojenkalastelu ja etäyhteysistunnon kaappaaminen.
11. **Kerääminen** (eng. collection). Hyökkääjän (Lehto, 2022) tavoitteena on kerätä hyökkäyksen kohteessa hyökkääjälle hyödyllistä tietoa. Tyypillisiä tekniikoita (MITRE, 2022b) ovat näyttöleikkeiden ottaminen kohdekoneen näytöstä ja mikrofonin salakuuntelu.
12. **Komento & kontrolli** (eng. command and control). Hyökkääjän (Lehto, 2022) tavoitteena on saada etähallinta hyökkäyksen kohteeseen. Tyypillisiä tekniikoita (MITRE, 2019a) ovat etähallintaohjelmistojen käyttö ja tietoliikenteen tunnelointi salattuna käyttäen väylänä jotain toista tietoliikenneprotokollaa.
13. **Suodattaminen** (eng. exfiltration). Hyökkääjän (Lehto, 2022) tavoitteena on varastaa tietoa hyökkäyksen kohteesta. Mahdollisia hyökkääjien käyttämiä tekniikoita (MITRE, 2019f) ovat tiedonsiirto USB-laitteella tai verkkoyhteyttä käyttäen.
14. **Vaikutus** (eng. impact). Hyökkääjän (Lehto, 2022) tavoitteena on vaikuttaa hyökkäyksen kohteen tietoon tai järjestelmiin haitallisesti. Tyypillisiä tekniikoita (MITRE, 2019g) ovat kovalevyllä olevien tietojen tuhoaminen ja palvelunestohyökkäykset.

Muita tunnettuja (Lehto, 2022) kyberhyökkäysten toteuttamista kuvaavia viitekehyksiä/malleja ovat: Mandiant Attack Lifecycle Model, Lockheed Martin Cyber Kill Chain, Unified Kill Chain ja Hybrid Cyber Kill Chain.

- **Mandiant Attack Lifecycle Model** (Lehto, 2022) sisältää kahdeksan vaihetta ja malli kuvaa kohdistettujen haittaohjelmahyökkäysten syklisen toimintamallin. Mallia (Mandiant, 2022b) voidaan hyödyntää myös hyökkääjän hyökkäysstrategian ymmärtämisessä ja torjunnassa.
- **Lockheed Martinin Cyber Kill Chain** (Lockheed Martin, 2015, s. 3) on kyberuhkien tunnistamiseen ja ehkäisemiseen kehitetty malli, joka perustuu (Kiwia ym., 2018, s. 395) Yhdysvaltain asevoimien kehittämään kill chain-taktiikkaan (engl. find, fix, track, target, engage and assess). Malli

(Lockheed Martin, 2015, s. 3) koostuu seitsemästä vaiheesta, joista hyökkääjän tulee suorittaa jokainen onnistuneesti päästäkseen tavoitteeseensa.
- **Unified Kill Chain** (Lehto, 2022) on Lockheed Martin Cyber Kill Chainin ja MITRE ATT&CK:n yhdistelmä, jossa hyökkäys on jaettu 18 vaiheeseen.
- **Hybrid Cyber Kill Chain** (Lehto, 2022) on Lockheed Martinin Cyber Kill Chainista kehitetty viitekehys, jonka tavoitteena on vastata paremmin organisaation sisältä tuleviin uhkiin.

Tutkimuksessa päädyttiin käyttämään MITRE ATT&CK for Enterprise viitekehystä, koska siinä olevien taktiikoiden ja tekniikoiden vertaaminen Katakrin vaatimuksiin on luontevaa. MITRE ATT&CK Enterprise-viitekehys (MITRE, 2022d) sisältää myös 43 torjuntakeinoa hyökkääjien mahdollisesti käyttämiä tekniikoita vastaan.

2.3 ADDRR

Kuten kappaleessa 1.3 esiteltiin ADDRR (Henneberg, 2020) on toimintamalli, jolla pyritään oppimaan tapahtuneista kyberhyökkäyksistä turvallisuuden edistämiseksi. Tällä lähestymistavalla mahdollistetaan organisaation mukautuminen uusiin kyberuhkiin. Toimintamallin on kehittänyt digikonsultti Alex Henneberg vuonna 2019.

ADDRR-mallissa (Henneberg, 2020) on tarkoituksena ottaa kyberturvallisuuteen kokonaisvaltainen ja liiketoimintakeskeinen näkökulma. Malli on rakentunut olemassa olevien sotilas-, liiketoiminta- ja kyberturvallisuusviitekehyksien pohjalta. Malli koostuu viidestä osa-alueesta:

- **Arvioi** (eng. assess). Tässä osa-alueessa (Henneberg, 2020) muodostetaan käsitys organisaation suojattavista kohteista ja olemassa olevasta turvallisuustasosta. Organisaation suojattavien kohteiden luokittelulla pyritään kohdistamaan olemassa olevat resurssit mahdollisimman tehokkaasti suojausta tarvitsevien kohteiden suojaamiseksi. Olemassa olevaa turvallisuustasoa voidaan arvioida joko vertaamalla 45 tunnettuun hyvään toimintamalliin tai viittä erilaista uhkaa vasten: sisäinen, ulkoinen, kolmas osapuoli, lainsäädäntö ja liitetyt järjestelmät.
- **Puolusta** (eng. defend). Seuraavassa osa-alueessa (Henneberg, 2020) on tarkoituksena kohdentaa olemassa olevat resurssit organisaation suojeltavien kohteiden suojaamiseksi kyberhyökkäyksiltä.
- **Havaitse** (eng. detect). Kolmannessa osa-alueessa (Henneberg, 2020) keskitytään havaitsemaan hyökkäykset mahdollisimman nopeasti. Tämän mahdollistamiseksi organisaation tulee ymmärtää organisaation normaali toiminta, jotta haitallinen toiminta voidaan havaita.
- **Vastaa** (eng. respond). Toiseksi viimeisessä osa-alueessa (Henneberg, 2020) tavoitteena on vastata tapahtuviin hyökkäyksiin olemassa olevin resurssein ja ennalta suunnitelluin toimintatavoin.

- **Uudelleen suunnittele** (eng. redesign). Viimeisessä osa-alueessa (Henneberg, 2020) on tarkoituksena oppia tapahtuneista hyökkäyksistä, jotta niiden haitalliset vaikutukset jäisivät jatkossa mahdollisimman vähäisiksi. Tavoitteena on hyödyntää opittuja asioita, jotta olemassa olevat liiketoimintaprosessit ja järjestelmät olisivat pohjimmiltaan toteutettu mahdollisimman turvallisiksi.

Muita tunnettuja (Lehto, 2022) kyberhyökkäysten torjumiseksi tarkoitettuja malleja/viitekehyksiä ovat kappaleessa 2.2 jo aiemmin mainitut: MITRE ATT&CK, Mandiant Attack Lifecycle Model ja Lockheed Martin Cyber Kill Chain.

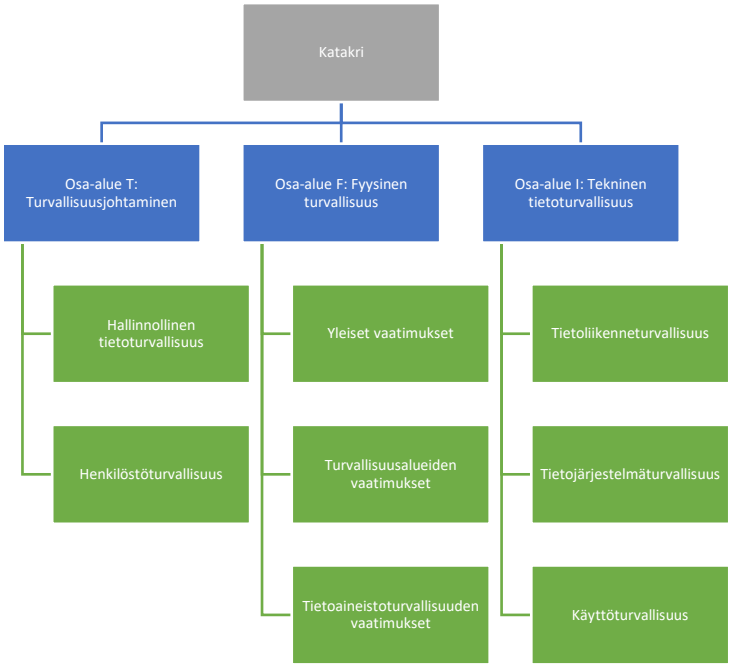
Tutkimuksessa päädyttiin käyttämään ADDRR-mallia, koska siinä on tavoitteena puuttua kyberturvallisuusongelmien juurisyihin tekemällä toimintatavoista ja järjestelmistä mahdollisimman turvallisia jo alun perin. Lisäksi ADDRR-mallin mukaista toiminnan ja järjestelmien uudelleensuunnittelua voitaneen hyödyntää Katakrin kehittämisessä.

2.4 Kansallinen turvallisuusauditointikriteeristö

Kuten kappaleessa 1.3 pohjustettiin kansallinen turvallisuusauditointikriteeristö (Turvallisuuskomitea, 2018, s. 13) on pääasiassa viranomaisten käyttöön tarkoitettu arviointityökalu. Sen avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisten turvallisuusluokiteltua tietoa. Katakri on tarkoitettu (Ulkoministeriö, 2022) käytettäväksi arvioitaessa yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Katakrin käytöllä on tavoitteena varmistaa, että kohdeorganisaatiolla on riittävät turvallisuusjärjestelyt viranomaisten salassa pidettävien tietojen suojaamiseksi niiden käsittely-ympäristöissä.

Katakrin ensimmäinen versio (Ulkoministeriö, 2020, s. 2) on valmistunut vuonna 2009 puolustusministeriön johtaman työryhmän toimesta. Ensimmäisen version jälkeen Katakrin sisältö ja sen päivitysten vetovastuu on muuttunut muutaman kerran. Tämän Pro gradututkielman kirjoittamisen aikana Katakrista on voimassa neljäs päivitysversio, ja sen on laatinut ulkoministeriössä toimiva Kansallisen turvallisuusviranomaisen (NSA) hallinnoima yhteistyöryhmä. Yhteistyöryhmä on koostunut niin viranomaisista kuin elinkeinoelämän edustajista.

Katakriin kootut vaatimukset (Ulkoministeriö, 2020, s. 5) perustuvat arviointikriteeristön uusimman version valmistuessa voimassa olleeseen lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Laki julkisen hallinnon tiedonhallinnasta (906/2019), valtioneuvosto asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) ja EU:n turvallisuussäännöt (2013/488/EU) antavat raamit Katakrissa esitetyille vaatimuksille. Katakri (Ulkoministeriö, 2020, s. 4–6) koostuu kolmesta osa-alueesta: turvallisuusjohtaminen (T), fyysinen turvallisuus (F) ja tekninen tietoturvallisuus (I). Jokainen Katakrin osa-alue koostuu useista alavaatimuksista. Seuraavalla sivulla olevassa kuviossa (kuvio 1) on esitetty Katakrin osa-alueet.



KUVIO 1 Katakrin osa-alueet

2.4.1 Turvallisuusjohtaminen

Turvallisuusjohtamisen osa-alue (Ulkoministeriö, 2020, s. 8–21) muodostuu hallinnollisen tietoturvallisuuden ja henkilöstöturvallisuuden vaatimuksista. Kaiken kaikkiaan turvallisuusjohtamisen osa-alue sisältää 13 osavaatimusta, joista 8 kpl koskee hallinnollista tietoturvallisuutta ja 5 kpl henkilöstöturvallisuutta.

Turvallisuusjohtamisen osa-alueen vaatimuksilla (Ulkoministeriö, 2020, s. 8) on tavoitteena varmistaa, että kohdeorganisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä ja sen henkilöstö käsittelee asianmukaisesti turvallisuusluokiteltuja tietoja. Kohdeorganisaation toiminta ja suojattavan tiedon suojaustarpeet vaikuttavat valittaviin tietoturvallisuuden hallintamenettelyihin.

2.4.2 Fyysinen turvallisuus

Fyysisen turvallisuuden osa-alue (Ulkoministeriö, 2020, s. 22–62) muodostuu yleisistä, turvallisuusalueiden ja tietoaineistoturvallisuuden vaatimuksista. Kaiken kaikkiaan fyysisen turvallisuuden osa-alue sisältää 8 osavaatimusta, joista 4 kpl koskee yleisiä, 3 kpl turvallisuusalueiden ja 1 kpl tietoaineistoturvallisuuden vaatimuksia. Lisäksi turvallisuusalueiden ja tietoaineistoturvallisuuden vaatimukset on jaettu useaan alavaatimuksiin.

Fyysisen turvallisuuden osa-alueen vaatimuksilla (Ulkoministeriö, 2020, s. 22–23) on tavoitteena estää luvaton pääsy turvallisuusluokiteltuihin tietoihin. Turvallisuusluokiteltujen tietojen suojaamiseksi on määritelty kolme turvallisuusaluetta: hallinnollinen alue, turva-alue ja teknisesti suojattu turva-alue. Hallinnolliset alueet (Ulkoministeriö, 2020, s. 33–41) ovat normaaliin päivittäiseen työskentelyyn käytettyjä tiloja. Kuitenkin tiloihin tulee olla pääsy vain

valtuutetuilla henkilöillä ja tilojen tulee täyttää hallinnollisille tiloille asetetut vähimmäisvaatimukset. Turva-alueet (Ulkoministeriö, 2020, s. 43–55) ovat hallinnollista aluetta paremmin suojattuja tiloja. Teknisesti suojatut turva-alueet (Ulkoministeriö, 2020, s. 56) on tarkoitettu EU:n ja Naton turvallisuusluokiteltujen tietojen suojaamiseksi. Riittävien turvatoimien (Ulkoministeriö, 2020, s. 22–23) tulee perustua aina riskiarvioon, mutta turvallisuusalueille määritetyt tavoitetasot tulee täyttyä ennen alueen hyväksyntää.

2.4.3 Tekninen tietoturvallisuus

Teknisen tietoturvallisuuden osa-alue (Ulkoministeriö, 2020, s. 63–106) muodostuu tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden vaatimuksista. Kaiken kaikkiaan teknisen tietoturvallisuuden osa-alue sisältää 21 osavaatimusta, joista 5 kpl koskee tietoliikenne-, 9 kpl tietojärjestelmä- ja 7 kpl käyttöturvallisuutta.

Teknisen tietoturvallisuuden osa-alueen vaatimuksilla (Ulkoministeriö, 2020, s. 63–64) on tavoitteena varmistaa turvallisuusluokitellun tiedon riittävä suojaus sähköisissä käyttöympäristöissä.

3 TUTKIMUSMETODIT

Tutkimuksessa hyödynnettiin kvalitatiivisia tutkimusmenetelmiä (Jyväskylän yliopisto, 2021). Kvalitatiivinen tutkimus tarkoittaa tutkimusta, jossa on tavoitteena ymmärtää tutkittavan aiheen ominaisuuksia ja merkityksiä. Tutkimus toteutettiin (IGI Global, ei pvm.) monitapaustutkimuksena. Monitapaustutkimuksella tarkoitetaan tutkimusta, jossa tutkitaan useaa tapausta niiden samankaltaisuuksien ja eroavaisuuksien havaitsemiseksi. Tutkimuksen aineistoa tarkasteltiin (Grönfors & Vilkka, 2011, s. 94) aineistolähtöisen sisällönanalyysin avulla. Aineistolähtöisen sisällönanalyysin tarkoituksena on tuottaa tietoa varsinaisia tutkijan pohdintoja varten. Tässä tutkimuksessa aineistosta pyrittiin löytämään kohdistettujen haittaohjelmahyökkäysten hyökkäysreitit, vastatoimia kohdistettuja haittaohjelmahyökkäyksiä vastaan ja ehdottamaan kehitysideoita kansalliseen turvallisuusauditointikriteeristöön.

3.1 Aineistonkeruumenetelmä

Aineiston hankinta suoritettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa tutkittiin kohdistettuja haittaohjelmahyökkäyksiä yleisellä tasolla. Hakusanoina käytettiin ”advanced persistent threat”, ”cyberattack”, ” cyber attack”, ”cyber operation” ja ”audit cyber”. Artikkeli otettiin läheisempään tarkasteluun, mikäli sen otsikossa oli jotain kohdistettuihin haittaohjelmahyökkäyksiin liittyvää. Kaiken kaikkiaan tarkasteltiin 20 artikkelia. Lähdeaineistoon perehtymisen jälkeen valittiin aineistossa usein toistuneiden kohdistettujen haittaohjelmahyökkäysten nimet. Erityisesti tutkimukseen haluttiin valita mukaan sellaisia hyökkäyksiä, joista löytyi hyvin tietoa julkisista lähteistä. Loppujen lopuksi tutkimukseen valittiin tarkasteltaviksi 10 kappaletta kohdistettuja haittaohjelmahyökkäyksiä. Valitut hyökkäykset olivat kohdistuneet erilaisiin kohteisiin ja suoritettu erilaisilla tavoitteilla. Puolessa tapauksista hyökkääjillä on ollut tavoitteena hyökkäyksen kohteen vakoilu, ja lopuissa tapauksissa tavoitteena on ollut sabotaasi.

Toisessa vaiheessa suoritettiin valittuihin kohdistettuihin haittaohjelmahyökkäyksiin liittyvä aineiston hankinta. Hakusanoina käytettiin ”blackenergy”, ”duqu”, ”flame malware”, ”GhostNet”, ”ghostnet cyber attack”, ”havex”, ”industroyer”, ”pegasus spyware”, ”pegasus malware”, ”shamoon attack”, ”stuxnet” ja ”triton cyber”. Artikkeli otettiin läheisempään tarkasteluun, mikäli sen otsikossa oli jotain hyökkäyksen puolustamiseen tai toteutukseen liittyvää. Yhteensä tarkasteltiin 26 artikkelia.

Pääasiallisina lähdeaineistoina käytettiin tieteellisiä artikkeleita. Lähdeaineistoa kerättiin julkisesti saatavilla olevista lähteistä. Aineiston etsimiseen käytettiin Web of Science -tieteellisten julkaisujen tietokantaa ja Google Scholar -tieteellisten julkaisujen hakupalvelua. Alkuperäisiä hakutuloksia Web of Science -tietokannasta suodatettiin ”Open Access”, jonka jälkeen suoritettiin varsinainen artikkelien valinta. Google Scholar -hakupalvelussa olleiden lähteiden valintaan vaikutti niihin kohdistuneiden siteerausten määrä. Alla olevassa taulukossa (taulukko 1) on eritelty aineiston hakuprosessi. Taulukossa ilmoitettu hakutulosten kappalemäärä on määrä ennen hakutulosten suodattamista. Joitain artikkeleita käytettiin lähteenä useamman hyökkäyksen osalta eikä niitä ole mainittu erikseen jokaisen hyökkäyksen valittujen artikkelien kohdalla.

TAULUKKO 1 Aineiston hakuprosessi

Tietokanta	Hakupäivämäärä	Hakusana	Hakutulokset, kpl	Valitut artikkelit, kpl
Web of Science	20.7.2022	advanced persistent threat	548	6
Google Scholar	20.7.2022	advanced persistent threat	756 000	2
Web of Science	20.7.2022	cyberattack	652	1
Google Scholar	20.7.2022	cyberattack	480 000	0
Web of Science	20.7.2022	cyber attack	9 329	2
Google Scholar	20.7.2022	cyber attack	480 000	2
Web of Science	21.7.2022	cyber operation	4 226	2
Google Scholar	21.7.2022	cyber operation	973 000	0
Web of Science	21.7.2022	audit cyber	241	4
Google Scholar	21.7.2022	audit cyber	104 000	1
Web of Science	2.8.2022	blackenergy	4	1
Google Scholar	8.8.2022	blackenergy	4 820	1
Web of Science	8.8.2022	duqu	26	0
Google Scholar	8.8.2022	duqu	5 400	4
Web of Science	8.8.2022	flame malware	9	1
Google Scholar	8.8.2022	flame malware	3 930	2
Web of Science	10.9.2022	GhostNet	44	0
Google Scholar	10.9.2022	GhostNet	3 040	1
Google Scholar	10.9.2022	ghostnet cyber attack	1 100	1
Web of Science	8.8.2022	havex	9	0
Google Scholar	8.8.2022	havex	21 000	1
Web of Science	8.8.2022	industroyer	1	1
Google Scholar	8.8.2022	industroyer	629	1

Web of Science	8.8.2022	pegasus spyware	2	0
Google Scholar	8.8.2022	pegasus spyware	5 240	3
Google Scholar	18.10.2022	pegasus malware	896	1
Web of Science	8.8.2022	shamoon attack	19	0
Google Scholar	8.8.2022	shamoon attack	8 780	3
Web of Science	8.8.2022	stuxnet	167	1
Google Scholar	8.8.2022	stuxnet	26 300	2
Web of Science	8.8.2022	triton cyber	4	0
Google Scholar	8.8.2022	triton cyber	4 390	2

Tieteellisten lähteiden lisäksi aineistona käytettiin vähäisinä määrinä tunnettujen kyberturvallisuusyritysten nettisivuja ja raportteja (Kaspersky, Mandiant, MITRE, Lookout ja Symantec) ja uutistoimistojen uutisartikkeleita.

3.2 Aineistonanalyysimenetelmä

Tutkimuksessa keskitytään löytämään tarkasteltavista kohdistetuista haittaohjelmahyökkäyksistä niiden hyökkäysreitit. Hyökkäysten torjumiseksi etsitään torjuntamenetelmät. Hyökkäysten toteuttamisesta ja torjumisesta tehtyjä havaintoja verrataan Katakrin kriteeristöihin mahdollisten puutteiden havaitsemiseksi kriteeristössä.

3.3 Tutkimuksen luotettavuus

Tutkimuksen luotettavuus perustuu käytetyn aineiston laatuun. Tutkimuksessa on käytetty pääasiassa vertaisarvioituja aineistoja ja erityisesti tieteellisiä artikkeleita. Aineistoa on analysoitu tutkimushetkellä olemassa olevan tutkimustiedon perusteella. Koska olemassa olevalla tiedolla voidaan vastata vain jo tapahtuneisiin hyökkäyksiin, on tärkeää ymmärtää tutkimuksen tulosten yleistettävyydelle tulevat rajoitukset. Uusien hyökkäysmenetelmien torjuminen vaatii jatkuvaa tutkimista, jotta myös tulevaisuuden uhat voidaan torjua.

4 TARKASTELTUJEN KOHDISTETTUJEN HAITTAOHJELMAHYÖKKÄYSTEN TOTEUTUS

Tämän kappaleen jokaisessa alakappaleessa käsitellään yhtä kohdistettua haittaohjelmahyökkäystä. Hyökkäyksistä kerrotaan ensiksi yleiset tiedot, jonka jälkeen selitetään hyökkäysten tapahtumienkulku.

4.1 BlackEnergy

BlackEnergy on Kasperskyn (2022) mukaan Troijalainen haittaohjelma, jota on käytetty hajautettuihin palvelunestohyökkäyksiin, kybervakoiluun ja tiedon tuhoamiseen. BlackEnergyn (Cherepanov & Lipovsky, 2016, s. 1) ensimmäinen versio on vuodelta 2007 ja haittaohjelma on vuosien aikana kehittynyt huomattavasti. Tässä tutkimuksessa on keskitytty vuoden 2015 hyökkäyksissä käytettyyn haittaohjelmaversioon. Kyseinen BlackEnergy (Cherepanov & Lipovsky, 2016, s. 4) on modulaarinen haittaohjelma, eli se koostuu ydinosasta ja sen toiminnallisuuksia laajentavista liitännäisistä (eng. plug-ins). BlackEnergy hyökkäysten kohteina (Kaspersky, 2022) ovat olleet teollisuuden ohjausjärjestelmät ja erityisesti energiasektorin kohteet Ukrainassa. Haittaohjelmalla tehdyt hyökkäykset aiheuttivat (Finkle, 2016) laajoja sähkökatkoja Ukrainassa joulukuussa 2015. Hyökkäys (Cherepanov & Lipovsky, 2016, s. 6) oli ensimmäinen julkisesti tiedossa oleva kyberhyökkäys, jonka kohteena oli siviiliväestö. Hyökkäysten (Finkle, 2016) takana arvellaan olleen ”Sandworm” niminen venäläinen APT-ryhmä.

BlackEnergy (Firoozjaei ym., 2022, s. 4–6) hyökkäykset ovat sisältäneet kaikki kohdistetuille haittaohjelmahyökkäyksille tyypilliset vaiheet. Tiedusteluvaiheessa (Cherepanov & Lipovsky, 2016, s. 2–3) hyökkääjät toteuttivat tietojenkalastelukampanjan, jossa oli tarkoituksena selvittää kohdeorganisaatiossa huijaussähköposteihin helposti narahtavat henkilöt. Tästä saatujen tietojen perusteella lähetettiin kohdistetulle joukolle sähköpostiviesti, jossa oli liitteenä

haitallinen Microsoft Office -tiedosto. Tiedoston avanneet ja haitalliset makrot hyväksyneet henkilöt laukaisivat BlackEnergyn lataamisen kohdekoneelle.

Asentumisen jälkeen (Cherepanov & Lipovsky, 2016, s. 4–6) kohdekoneesta on otettu yhteys hyökkääjän tietokoneelle RC4 algoritmilla salatuin viestein http-protokollaa käyttäen. Samassa verkossa olevien saastuneiden koneiden hallitsemiseen on käytetty eri hallintakoneita.

Hyökkääjien (Cherepanov & Lipovsky, 2016, s. 5) päästyä kohdeorganisaation lähiverkkoon hyökkääjät tekivät tiedustelua kohdekoneen käyttäjien käyttäytymisestä, itse tietokoneesta ja kohdeorganisaation verkosta. Hankitut tiedot välitettiin hyökkääjien hallintakoneille. Haittaohjelmassa olleiden näppäinnauhuri (eng. keylogger) ja salasanan varastustyökalu -liitännäisten avulla hankittiin tunnistetietoja, joita käytettiin siirtymisessä verkon muihin tietokoneisiin. Erityisesti hyökkääjät (Firoozjaei ym. 2022, s. 4) tavoittelivat laitteita, joista pääsi hallitsemaan energialaitosten tuotantolaitteita.

Varastettuja tunnistetietoja käyttäen hyökkääjät kirjautuivat kohteen VPN verkkoon. DSEFix -työkalua (Cherepanov & Lipovsky, 2016, s. 5) käyttäen hyökkääjät ottivat kohteen virtualisoinnissa käytetyn VirtualBox-ohjelmiston haltuunsa. Tämän jälkeen (Firoozjaei ym. 2022, s. 4) hyökkääjät virtualisoivat kohdekoneen käyttöjärjestelmän ja ohittivat laiteajurien allekirjoituksen varmistamisen haittaohjelman ajamiseksi.

Lopullisessa hyökkäysvaiheessa (Firoozjaei ym. 2022, s. 4) valvomo-ohjelmistoa hallittiin pääkäyttäjäoikeuksin ja haittaohjelma avasi SSH takaoven (eng. SSH backdoor). Lisäksi tuotantolaitteiden asetuksia muutettiin ja (Cherepanov & Lipovsky, 2016, s. 6) haittaohjelman KillDisk komponentilla tuhottiin tiedot kohdekoneiden kovalevyiltä ja lokitiedot tapahtumalokista. Alla olevaan taulukkoon (taulukko 2) on koottu BlackEnergyssa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 2 BlackEnergyn hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1566 – Tietojenkalastelu
Resurssien kehittäminen	-
Alustava sisäänpääsy	T1566.001 – Tietojenkalastelu: Kohdistetut linkit T1566.002 – Tietojenkalastelu: Kohdistetut liitetiedostot T1189 – Laiteajurien väärentäminen (eng. Drive-by Compromise)
Suoritus	T1204 – Käyttäjän suoritus T1047 – WMI-palvelun hyödyntäminen (eng. Windows Management Instrumentation)
Pysyvyys	T1137 – Office-sovelluksen käynnistys T1574 – Suoritusvirran kaappaus (eng. Hijack Execution Flow) T1543 – Järjestelmäprosessien muokkaus T1547 – Käynnistyksen aikainen suorittaminen (eng. Boot Autostart Execution)
Käyttöoikeuksien laajentaminen	T1055 – Prosessi-injektio T1548 – Käyttäjätilien hallinnan ohitus
Puolustuksen välttely	T1070 – Tapahtumatunnisteiden poistaminen (eng. Indicator Removal on Host)

Valtuutettu sisäänpääsy	T1552 – Turvattomat tunnistetiedot T1555 – Tunnistetietojen hankkiminen niiden säilytyspaikoista (eng. Credentials from Password Stores)
Tutkinta	T1083 – Tiedostojen ja hakemistojen etsintä T1046 – Verkkopalveluiden skannaus T1120 – Oheislaitteiden etsintä T1057 – Prosessien etsintä T1016 – Järjestelmän verkkoasetusten etsintä T1049 – Järjestelmän verkkoyhteyksien etsintä T1082 – Järjestelmätietojen etsintä
Liikkuminen	T1021 – Etäpalvelut
Kerääminen	T1056.001 – Syötteen kaappaaminen: Näppäinnauhuri T1113 - Näyttöleikkeiden ottaminen
Komento & kontrolli	T1008 – Varakanavat (eng. Fallback Channels) T1071 – Sovelluskerroksen protokollan käyttäminen
Suodattaminen	-
Vaikutus	T1485 – Tiedon tuhoaminen T1565 – Tiedon muokkaaminen

4.2 Duqu

Duqu on (Symantec, 2011, s. 1–3) etähallittava Troijalainen haittaohjelma (eng. remote access Trojan). Vuonna 2011 löydettyä Duqua on käytetty teollisuusvakoilussa ja sen uhriksi on joutunut ainakin (Chien ym., 2012) kuusi eri organisaatiota kahdeksassa eri maassa. Hyökkäysten kohteista (Wangen, 2015) on lähdekirjallisuudessa hyvin vähän tietoa saatavilla, eikä yhtään organisaatiota ole nimetty suoraan nimeltä Duqun uhriksi. Duqun tarkoituksena on ollut kerätä tietoa teollisuuden toimijoista, ja hyökkääjät ovat erityisesti pyrkineet hankkimaan tietoa, josta olisi hyötyä hyökkäysten valmistelussa muita kohteita vastaan. Duqun (Wangen, 2015) tekijöistä ei ole täyttä varmuutta, mutta Stuxnetin ja Duqun tekijöiksi arvellaan samaa toimijaa. Molemmissa haittaohjelmissa (Symantec, 2011, s. 1–3) on käytetty lähes samanlaista lähdekoodia ja modulaarista rakennetta, vain niiden tavoitteet ovat olleet erilaiset, Stuxnetilla teollisuussabotaasi ja Duqulla -vakoilu. Duqu koostuu laiteajuritiedostosta (eng. driver file), DLL-tiedostosta (eng. dynamic-link library), konfiguraatiotiedostosta ja asentumistiedostosta (eng. installer).

Duqu (Chien ym., 2012) on toimitettu hyökkäyksen kohteeseen käyttäen kohdistettuja huijaussähköposteja. Huijaussähköposteissa on ollut liitteenä haitallinen Microsoft Word -tiedosto, jonka avaaminen on laukaissut haittaohjelman asentumisen kohdetietokoneelle. Haittaohjelman asentumisessa on hyödynnetty Microsoft Wordin TrueType Fontin käsittelyyn liittyvää nollapäivähaavoittuvuutta.

Haittaohjelman asentuminen (Symantec, 2011, s. 1–3) tapahtuu asentumistiedoston avulla. Asennustiedosto rekisteröi laiteajuritiedoston sellaiseksi palveluksi, että se käynnistyy tietokoneen käynnistyksen yhteydessä. Seuraavaksi

laiteajuri injektoi DLL-tiedoston luotettuun prosessin. Tämän jälkeen DLL-tiedosto alkaa injektoimaan haittaohjelman komponentteja muihin prosesseihin. Em. prosessi-injektioiden avulla haittaohjelma pystyy piilottamaan haitallisen toimintansa haittaohjelmien torjuntajärjestelmiltä.

Duqu (Wangen, 2015) ei kopioi itse itseään, mutta hyökkääjät ovat voineet levittää haittaohjelmaa tietokoneesta toiseen verkon välityksellä (eng. network shares). Lisäksi hyökkääjät ovat käyttäneet kohdeorganisaation ensimmäiseksi saastunutta tietokonetta välityspalvelimena saastuneen kohdeorganisaation ja hyökkääjien komentokoneen välillä. Kohdeorganisaation sisäverkossa saastuneet tietokoneet ovat voineet keskustella välityspalvelimen kanssa peer-to-peer periaatetta noudattaen. Kommunikointi (Bencsáth ym., 2012_a) komentokoneen kanssa on toteutettu http ja https -protokollia käyttäen. Varsinainen tiedonsiirto on tehty jpeg -kuvatiedostoilla, joihin salattu tiedustelutieto on ollut upotettuna.

Duqun (Chien ym., 2012) valmistamisessa on hyödynnetty varastettua sähköistä allekirjoitussertifikaattia (eng. digital code signing certificate), jonka avulla on hämätty hyökkäysten kohteiden haittaohjelmien torjuntajärjestelmiä. Sertifikaatin avulla haittaohjelma pystyy hämäämään tuntemattomien laiteajurien (eng. driver) tunnistamista.

Hyökkäysten kohteissa (Bencsáth ym., 2012_b) hyökkääjät ovat varastaneet tunnistetietoja näppäinnauhurimoduulin avulla. Lisäksi kohteista on hankittu tiedustelutietoa muun muassa näyttöleikkein. Varastettuja tunnistetietoja on käytetty pysyvän pääsyn varmistamiseksi ja käyttöoikeuksien laajentamiseksi kohdetietokoneissa. Alla olevaan taulukkoon (taulukko 3) on koottu Duqussa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 3 Duqun hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1591 – Tiedon kerääminen uhriorganisaatiosta T1592 – Tiedon kerääminen uhrijärjestelmistä
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma T1588.004 – Hanki kyvykkyyksiä: Digitaaliset sertifikaatit T1588.006 – Hanki kyvykkyyksiä: Haavoittuvuudet
Alustava sisäänpääsy	T1566.001 – Tietojenkalastelu: Kohdistetut linkit T1078 – Pätevät tunnukset (eng. Valid Accounts)
Suoritus	T1204.002 – Käyttäjän suoritus: Haitallinen tiedosto T1053 – Aikataulutettu tehtävä
Pysyvyys	T1543 – Järjestelmäprosessien muokkaus T1053 – Aikataulutettu tehtävä T1078 – Pätevät tunnukset
Käyttöoikeuksien laajentaminen	T1134 – Käyttöoikeustunnusten manipulointi (eng. Access Token Manipulation) T1543 – Järjestelmäprosessien muokkaus T1055 – Prosessi-injektio T1055.001 – Prosessi-injektio: Dynaamisen linkkikirjaston injektio (eng. Dynamic-link Library Injection) T1053 – Aikataulutettu tehtävä T1078 – Pätevät tunnukset
Puolustuksen välttely	T1134 – Käyttöoikeustunnusten manipulointi T1055 – Prosessi-injektio T1055.001 – Prosessi-injektio: Dynaamisen linkkikirjaston injektio

	T1078 – Pätevät tunnukset
Valtuutettu sisäänpääsy	T1056.001 – Syötteen kaappaaminen: Näppäinnauhuri
Tutkinta	T1087.001 – Tilin löytäminen: Paikallinen tili (eng. Account Discovery: Local Account) T1010 – Sovellusikkunoiden etsintä (eng. Application Window Discovery) T1057 – Prosessien etsintä T1016 – Järjestelmän verkkoasetusten etsintä T1049 – Järjestelmän verkkoyhteyksien etsintä
Liikkuminen	T1021.002 – Etäpalvelut: SMB
Kerääminen	T1560.003 – Arkistoi kerätyt tiedot: Arkistoi mukautetulla menetelmällä T1074.001 – Tieto vaiheistettu: Paikallinen tiedon vaiheistus T1056.001 – Syötteen kaappaaminen: Näppäinnauhuri
Komento & kontrolli	T1071 – Sovelluskerroksen protokollan käyttäminen T1001.002 – Tiedon hämärtäminen: Steganografia (eng. Data Obfuscation: Steganography) T1572 – Protokollatunnelointi T1573.001 – Salattu kanava: Symmetrinen salaus T1090.001 – Välityspalvelin: Sisäinen välityspalvelin
Suodattaminen	T1041 – Suodatus C2-kanavan kautta (eng. Exfiltration Over C2 Channel)
Vaikutus	-

4.3 Flame

Flame (Wangen, 2015) on vakoiluun käytetty haittaohjelma, joka tunnetaan lähdekirjallisuudessa myös nimillä SKyWIper ja Flamer. Vuonna 2012 löydetty Flame on tutkijoiden mukaan yksi suurimmista (20 MB) ja kehittyneimmistä haittaohjelmista. Flamen (Fillinger & Stevens, 2015) hyökkäysten kohteet ovat sijainneet Lähi-idässä ja pääasiassa Iranissa. Hyökkäysten kohteiksi ovat joutuneet niin liike-elämän kuin julkishallinnon organisaatioita. Flamen tekijästä ei ole täyttä varmuutta, mutta tutkijoiden mukaan haittaohjelman on suurella todennäköisyydellä tehnyt valtiollinen toimija, mahdollisesti Yhdysvaltojen ja Israelin yhteistyönä.

Hyökkäyksen valmisteluvaiheessa hyökkääjät ovat hankkineet kohdeorganisaatioista tietoa haittaohjelman valmistelemiseksi ja mahdollisen tunkeutumisreitin löytämiseksi. Em. (Fillinger & Stevens, 2015) tekniikoiden käytön puolesta puhuu se, että haittaohjelma on levinnyt vain rajatulla maantieteellisellä alueella Lähi-idässä. Lisäksi hyökkääjien tavoitteena ei ole ollut levittää haittaohjelmaa mahdollisimman moneen kohteeseen, vaan vain tarkoin valittuihin kohteisiin.

Hyökkääjät ovat (Bencsáth ym., 2012_b) kehittäneet haittaohjelman, jonka tekemisessä on hyödynnetty väärennettyä allekirjoitussertifikaattia. Microsoft on käyttänyt MD5 -tiivistealgoritmia (eng. hashing algorithm) Certification Authority -palvelussaan, jota käytetään ohjelmistojen allekirjoitussertifikaattien tekemisessä. Vaikka Microsoft oli tietoinen sertifikaattiensa muodostamisessa käytettävän algoritmin heikkouksista, eivät he olleet vaihtaneet algoritmia

turvallisemmaksi. Väärennetyn sertifikaatin hankkimiseksi hyökkääjät ovat toteuttaneet valitun etuliitteen törmäyshyökkäyksen (eng. chosen prefix collision attack), jossa he ovat hyödyntäneet MD5 -tiivistealgoritmissa olevaa haavoittuvuutta. Väärennetyllä sertifikaatilla haittaohjelma on maskeerattu näyttämään luotettavalta Microsoft ohjelmistolta ja siten hämätty hyökkäysten kohteiden haittaohjelmien torjuntajärjestelmiä. Haittaohjelma onkin kohdistettu juuri Microsoft Windows-käyttöjärjestelmillä varustettuja tietokoneita vastaan.

Hyökkäysten kohteeseen tunkeutumisessa (Bencsáth ym., 2012_b) ei ole tutkijoilla täyttä varmuutta, mutta (Bermejo Higuera ym., 2020, s. 23) haittaohjelma on mahdollisesti tuotu kohteisiin USB-muistitikkua käyttäen. USB-muistitikku on voitu tuoda hyökkäyksen kohteeseen joko insiderin toimesta tai saastuneen muistitikun avulla. Insiderilla (Jääskeläinen, 2018, s. 6) tarkoitetaan organisaation työntekijää, joka tahallisesti vaarantaa organisaation tietoturvallisuutta ja hyödyntää organisaation liikesalaisuuksia omaksi tai toisen hyödyksi.

Flame (Bencsáth ym., 2012_b) leviää hyökkäysten kohteessa usealla eri tavalla. Ensinnäkin hyödyntäen kahta ohjelmistohaavoittuvuutta print spooler exploit (MS10-061) ja LNK exploit (MS10-046). Toiseksi esiintymällä välityspalvelimena Windows-käyttöjärjestelmän päivityksille, jonka ansiosta päivitysten sijaan tietokoneille onkin lähetetty haittaohjelma. Tämän (Fillinger & Stevens, 2015) välimieshyökkäyksen (eng. Man-In-The-Middle attack) suorittamisessa on hyödynnetty em. väärennettyä ohjelmakoodin allekirjoitussertifikaattia.

Haittaohjelmasuojausten hämäämiseksi (Bencsáth ym., 2012_b) Flamessa on käytetty väärennetyn sertifikaatin lisäksi ohjelmakoodin salaamista ja toimintoa, jolla haittaohjelma tarkistaa hyökkäyksen kohteessa käytössä olevat turvallisuusjärjestelmät. Pysyvän pääsyn varmistamiseksi (Bencsáth ym., 2012_b) haittaohjelma suorittaa prosessi-injektion.

Hyökkäyksen kohteeseen päästyään (Bencsáth ym., 2012_b) Flame on pystynyt hankkimaan kohteesta varsin laajasti erilaista tiedustelutietoa. Haittaohjelma on kyennyt hankkimaan tietoa näppäinnauhurein, kuuntelemalla tietokoneen mikrofonia, ottamaan näyttöleikkeitä ja varastamaan tiedostoja.

Flamella (Wangen, 2015) hankittu tiedustelutieto on ennen eteenpäin lähettämistä salattu usealla eri metodilla ja tiivistetty zlib-ohjelmakirjastoa käyttäen. Kerätty tieto on välitetty eteenpäin hyökkääjien komentopalvelimille internetin välityksellä. Alla olevaan taulukkoon (taulukko 4) on koottu Flamessa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 4 Flamen hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592 – Tiedon kerääminen uhrijärjestelmistä T1591 – Tiedon kerääminen uhriorganisaatiosta
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma T1588.003 – Hanki kyvykkyyksiä: Koodin allekirjoitussertifikaatit
Alustava sisäänpääsy	T1091 – Kopioituminen siirrettävällä tietovälineellä (eng. Replication Through Removable Media)
Suoritus	T1059 – Komento- ja komentosarjatulkki
Pysyvyys	T1136 – Luo tunnukset T1547 – Käynnistyksen aikainen suorittaminen

	T1078 – Pätevät tunnukset
Käyttöoikeuksien laajentaminen	T1547 – Käynnistyksen aikainen suorittaminen T1078 – Pätevät tunnukset
Puolustuksen välttely	T1553.002 – Kumoa luottamuksen hallinta: Koodin allekirjoitus (eng. Subvert Trust Controls: Code Signing) T1218.011 – Järjestelmän binaarivälityspalvelimen suoritus: Ryndll32 (eng. System Binary Proxy Execution: Rundll32) T1078 – Pätevät tunnukset T1518.001 – Ohjelmistojen löytäminen: Turvallisuusohjelmistot (eng. Software Discovery: Security Software Discovery)
Valtuutettu sisäänpääsy	T1056 – Syötteen kaappaaminen T1557 – Välimieshyökkäys
Tutkinta	T1046 – Verkkopalveluiden skannaus T1040 – Verkkoliikenteen seuraaminen (eng. Network Sniffing) T1120 – Oheislaitteiden etsintä
Liikkuminen	T1210 – Etäpalvelun haavoittuvuuden hyödyntäminen (eng. Exploitation of Remote Services) T1570 – Sivusuuntainen työkalujen siirto (eng. Lateral Tool Transfer) T1091 – Kopioituminen siirrettävällä tietovälineellä
Kerääminen	T1056 – Syötteen kaappaaminen T1113 – Näyttöleikkeiden ottaminen T1123 – Äänenkaappaus T1125 – Videokaappaus T1115 – Leikepöydän tiedot T1213 – Tiedot paikallisista tietovarastoista
Komento & kontrolli	T1090.001 – Välityspalvelin: Sisäinen välityspalvelin T1071 – Sovelluskerroksen protokollan käyttäminen
Suodattaminen	T1041 – Suodatus C2-kanavan kautta T1052 – Suodatus siirrettävällä välineellä (eng. Exfiltration Over Physical Medium)
Vaikutus	-

4.4 GhostNet

GhostNet (Deibert ym., 2009, s. 5–6) on Information Warfare Monitorin tutkijoiden vuonna 2009 paljastama laajamittainen kybervakoiluverkosto. Tutkijoiden mukaan verkostoon on kuulunut vähintään 1295 saastunutta tietokonetta yhteensä 103 maassa. Hyökkäysten kohteina ovat olleet eri maiden suurlähetystöt, ministeriöt, suuryritykset ja kansalaisjärjestöt. Verkoston arvellaan olevan Kiinan tekosia, sillä saastuneiden tietokoneiden ohjaamiseen käytetyt komentotietokoneet ovat sijainneet pääasiassa Kiinan maaperällä. Lisäksi hyökkäykset ovat kohdistuneet Kiinalle poliittisesti tärkeisiin kohteisiin. GhostNet (Deibert ym., 2009, s. 5–6) hyökkäykset ovat sisältäneet kohdistetuille haittaohjelmahyökkäyksille tyypillisiä taktiikoita ja tekniikoita.

Hyökkäyksen valmisteluvaiheessa (Deibert ym., 2009, s. 5–6) hyökkääjät ovat ottaneet selvää kenelle ja millaisilla sähköpostiviesteillä hyökkäyksen

kohdetta on kannattavaa lähestyä, sillä varsinainen kohteeseen tunkeutuminen on toteutettu lähettämällä hyökkäyksen kohteelle asiayhteyteen sopivia huijaussähköposteja. Sähköpostien liitteinä on käytetty yleisesti tunnettujen toimistoohjelmien tiedostoja, jotka ovat lisäksi nimetty näyttämään asiayhteyteen sopivilta (eng. Trojan horse). Liitteissä tai vaihtoehtoisesti linkeissä onkin ollut hyökkäyskoodia upotettuna. Liitetiedoston tai linkin avaaminen on laukaissut gh0st RAT-nimisen Troijalaisen haittaohjelman latautumisen kohdetietokoneelle.

gh0st RAT (Deibert ym., 2009, s. 34) on kiinalaisten kehittämä avoimen lähdekoodin Troijalainen haittaohjelma (eng. remote administration tool). Haittaohjelman voi pakata ja nimetä uudelleen hyökkäyksen kohteen hämäämiseksi ja tartuttamiseksi. Asentuessaan (Deibert ym., 2009, s. 39) kohdetietokoneeseen gh0st RAT muodostaa takaoven (eng. backdoor) pysyvän hallinnan varmistamiseksi kohteessa.

Latautumisen (Deibert ym., 2009, s. 18–25) ja asentumisen jälkeen haittaohjelma suorittaa nimipalvelukyselyn (eng. DNS look-up) yhteyden muodostamiseksi hyökkääjien hallintapalvelimeen. Haittaohjelma keskustelee hallintapalvelimen kanssa julkisen Internetin yli http-protokollaa käyttäen. http-protokollaa on käytetty, jotta tietoliikenne ei näyttäisi normaalista poikkeavalta. Hallintapalvelimia on käytetty komentojen antamisessa kohdekoneille. Hallintapalvelimilta (Deibert ym., 2009, s. 30) on annettu komentoja kohdekoneille tiedon etsimistä ja tiedostojen varastamista varten. Lisäksi hallintapalvelimilta on voitu antaa komentoja muiden haittaohjelmien lataamiseksi hyökkääjien hallinnoimilta erillisiltä komentopalvelimilta.

GhostNetin (Ghafir & Prenosil, 2014) leviämisessä on hyödynnetty saastuneista tietokoneista hankittuja yhteystietoja. Yhteystietojen avulla gh0st RAT-haittaohjelmaa on lähetetty eteenpäin sähköpostin välityksellä uusille uhreille. Uusien uhrien hämäämiseksi sähköpostit on lähetetty saastuneista tietokoneista asiayhteyteen sopivin dokumentein ja viestein.

Hyökkäysten kohteet (Deibert ym., 2009, s. 18) eivät ole olleet tietoisia laitteensa saastumisesta, sillä haitalliset liitetiedostot ovat auenneet normaalisti. Tutkijoiden mukaan vain 11/34 tutkitusta virustorjuntajärjestelmästä havaitsi haittaohjelman liitetiedostoista. Hyökkääjät olivat hyödyntäneet lähdekoodin muokkaamista (eng. code obfuscation) virustorjuntaohjelmistojen hämäämiseksi.

Hyökkäyksen kohteessa (Deibert ym., 2009, s. 5–6) hyökkääjät ovat saaneet täyden hallinnan gh0st RAT:lla saastuneesta tietokoneesta. Hyökkääjät ovat pystyneet muun muassa etsimään ja lataamaan saastuneesta tietokoneesta tiedostoja. Lisäksi (Deibert ym., 2009, s. 34) hyökkääjät ovat voineet tietokoneen käyttäjän huomaamatta avata tietokoneen mikrofonin, webbikameran, ottaa näyttöleikkeitä sekä käyttää näppäinnauhuria tietokoneen käyttäjän toiminnan seuraamiseksi. Komentorivin etäkäytöllä (eng. remote shell) hyökkääjät ovat voineet ladata ja suorittaa saastuneessa tietokoneessa myös muita haittaohjelmia. Seuraavalla sivulla olevaan taulukkoon (taulukko 5) on koottu GhostNetissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 5 GhostNetin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592 – Tiedon kerääminen uhrijärjestelmistä T1589 – Uhrin henkilöllisyystietojen kerääminen
Resurssien kehittäminen	T1583.004 – Hanki infrastruktuuria: Palvelin T1587.004 – Kehitä kyvykkyyksiä: Hyväksikäyttömenetelmät (eng. Exploits) T1588.001 – Hanki kyvykkyyksiä: Haittaohjelma
Alustava sisäänpääsy	T1566.002 – Tietojenkalastelu: Kohdistetut liitetiedostot
Suoritus	T1204.002 – Käyttäjän suoritus: Haitallinen tiedosto T1059 – Komento- ja komentosarjatulkki T1106 – Alkuperäinen ohjelmointirajapinta (eng. Native API) T1569.002 – Järjestelmäpalvelut: Palvelun toteutus T1129 – Jaetut moduulit
Pysyvyys	T1547.001 – Käynnistyksen aikainen suorittaminen: Rekisterin suoritusavaimet T1543 – Järjestelmäprosessien muokkaus T1574 – Suoritusvirran kaappaus
Käyttöoikeuksien laajentaminen	T1055 – Prosessi-injektio
Puolustuksen välttely	T1027 – Tiedostojen hämääminen (eng. Obfuscated Files) T1070.001 – Tapahtumatunnisteiden poistaminen: Windowsin lokitietojen poistaminen T1070.004 – Tapahtumatunnisteiden poistaminen: Tiedoston tuhoaminen T1112 – Rekistereiden muokkaus T1218.011 – Järjestelmän binaarivälityspalvelimen suoritus: Ryndll32
Valtuutettu sisäänpääsy	T1056 – Syötteen kaappaaminen
Tutkinta	T1087.003 – Tilin löytäminen: Verkkotunnuksen tili T1083 – Tiedostojen ja hakemistojen etsintä T1082 – Järjestelmätietojen etsintä T1012 – Rekisterikyselyt (eng. Query Registry) T1057 – Prosessien etsintä
Liikkuminen	T1534 – Sisäinen tietojenkalastelu
Kerääminen	T1123 – Äänenkaappaus T1115 – Leikepöydän tiedot T1005 – Tiedot paikallisesta järjestelmästä T1114 – Sähköpostien kokoaminen T1056.001 – Syötteen kaappaaminen: Näppäinnauhuri T1113 – Näyttöleikkeiden ottaminen T1125 – Videokaappaus
Komento & kontrolli	T1071 – Sovelluskerroksen protokollan käyttäminen T1132.001 – Tiedon salaaminen: Standardi salaus T1568.001 – Dynaaminen resoluutio: Nopea virtaus DNS (eng. Dynamic Resolution: Fast Flux DNS) T1578 – Salattu kanava T1105 – Välineiden siirto (eng. Ingress Tool Transfer)
Suodattaminen	T1020 – Automatisoitu suodatus T1041 – Suodatus C2-kanavan kautta
Vaikutus	-

4.5 Havex

Havex (Firoozjaei ym., 2022, s. 8–10) on teollisuusvakoilussa käytetty etähallittava Troijalainen haittaohjelma. Havexia käyttänyt APT-ryhmä tunnetaan usealla eri nimellä kuten Crouching Yeti, Dragonfly ja Energetic Bear. APT-ryhmä (Kaspersky, 2014, s. 2–5) on ollut aktiivinen jo vuodesta 2010 alkaen ja sen hyökkäysten pääasiallisina kohteina ovat olleet strategiset teollisuuden toimijat. Kaspersky Lab:n (Kaspersky, 2014, s. 28–29) tutkijoiden vuonna 2014 tekemässä tutkimuksessa havaittiin yhteensä 2 470 Havexilla saastunutta järjestelmää.

Hyökkäyksessä (Firoozjaei ym., 2022, s. 8–10) ei ole käytetty laajasti erilaisia taktiikoita ja tekniikoita. Hyökkäysten valmistelussa on hyödynnetty kohdeorganisaatioiden julkisesti saatavilla olevia nettisivuja, joista hankittuja tietoja on mahdollisesti käytetty haittaohjelman/haittaohjelmien kehittämisessä sekä hyökkäysvektorien valinnassa.

Hyökkäysten kohteisiin tunkeutumisessa (Kaspersky, 2014, s. 2–3) on hyödynnetty kolmea eri menetelmää: huijaussähköpostien liitetiedostot, muokattuja ohjelmistojen asentajia (eng. Trojanized software installers) ja haittaohjelmien upottaminen organisaatioiden nettivisuille (eng. watering hole attack). Pääasiallisena hyökkäysreittinä (Firoozjaei ym., 2022, s. 8–10) on käytetty haittaohjelman upottamista teollisuuden ohjausjärjestelmien valmistajien nettisivuille. Hyökkääjät ovat murtautuneet valmistajien nettisivuille ja vaihtaneet olemassa olevien asennustiedostojen tilalle haittaohjelmalla varustettuja tiedostoja. Näitä haittaohjelmalla varustettuja tiedostoja ohjausjärjestelmien asiakkaat ovat ladanneet omiin järjestelmiinsä saastuttaen samalla omat järjestelmänsä.

Havex (Firoozjaei ym., 2022, s. 8–10) on asentunut hyökkäysten kohteeseen kahdessa vaiheessa. Ensimmäisessä vaiheessa haittaohjelman asennustiedosto (eng. dropper) asentaa haittaohjelman kohdekoneeseen. Toiseksi haittaohjelma muodostaa takaoven (eng. backdoor), jonka avulla hyökkääjä voi ylläpitää hallintayhteyttä saastuneeseen järjestelmään.

Asentumisen jälkeen (Firoozjaei ym., 2022, s. 8–10) hyökkäysten kohteesta on hankittu tietoa. Tietoa on kerätty näppäinnauhuria, verkkoskannausta ja tiedostojen listaamista käyttäen. Edellä mainittuja työkaluja/menetelmiä käyttäen hyökkääjät ovat saaneet tietoonsa salaista tietoa hyökkäysten kohteiden tuotantoprosesseista. Kerätyt tiedot on pakattu, salattu epäsymmetrisellä salauksella, kirjoitettu .yls-tiedostoihin ja lähetetty eteenpäin hyökkääjien hallitsemille komentokoneille http-protokollaa käyttäen.

Havex (Firoozjaei ym., 2022, s. 8–10) on rakenteeltaan modulaarinen haittaohjelma, jonka toiminnallisuuksia on voitu muokata erilaisilla lisäosilla. Havex (Kaspersky, 2014, s. 2–3) saastuttaa Windows käyttöjärjestelmällä toimivia järjestelmiä. Havexin (Kaspersky, 2014, s. 12–15) tarkoituksena ei ole ollut aiheuttaa fyysistä tuhoa vaan kerätä hyökkääjille tietoa hyökkäysten kohteista. Tutkijoiden (Kaspersky, 2014, s. 2–3) havaintojen perusteella hyökkäyksissä ei ole käytetty yhtään nollapäivähaavoittuvuutta. Piilossa pysymiseksi (Firoozjaei ym., 2022, s. 8–10) Havexissa on moduuli jälkien peittämiseksi kohdekoneessa. Pysyvän

hallintayhteyden ylläpitämiseksi (Kaspersky, 2014, s. 12) Havex muuttaa järjestelmän käynnistymisprosesseja sekä luo automaattisen käynnistyksen rekisteriavaimen (eng. autorun registry key). Alla olevaan taulukkoon (taulukko 6) on koottu Havexissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 6 Havexin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1594 – Uhrin nettisivujen tiedustelu
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma
Alustava sisäänpääsy	T1566 – Tietojenkalastelu T1195 – Toimitusketjun vahingoittaminen (eng. Supply Chain Compromise) T1189 – Laiteajurien väärentäminen
Suoritus	-
Pysyvyys	T1547 – Käynnistyksen aikainen suorittaminen
Käyttöoikeuksien laajentaminen	T1055 – Prosessi-injektio
Puolustuksen välttely	T1547 – Käynnistyksen aikainen suorittaminen T1070 – Tapahtumatunnisteiden poistaminen T1055 – Prosessi-injektio
Valtuutettu sisäänpääsy	T1555 – Tunnistetietojen hankkiminen niiden säilytyspaikoista T1056 – Syötteen kaappaaminen
Tutkinta	T1087 – Tilin löytäminen T1083 – Tiedostojen ja hakemistojen etsintä T1057 – Prosessien etsintä T1082 – Järjestelmätietojen etsintä T1016 – Järjestelmän verkkoasetusten etsintä T1033 – Järjestelmän käyttäjän selvittäminen (eng. System Owner Discovery)
Liikkuminen	T1534 – Sisäinen tietojenkalastelu
Kerääminen	T1560 – Arkistoi kerätyt tiedot T1056 – Syötteen kaappaaminen
Komento & kontrolli	T1132 – Tiedon salaaminen T1573 – Salattu kanava T1102 – Webpalvelu
Suodattaminen	T1567 – Suodatus verkkopalvelun kautta
Vaikutus	-

4.6 Industroyer

Industroyer on (Gjesvik & Szulecki, 2022) teollisuussabotaasiin tarkoitettu haittaohjelma, jota on käytetty hyökkäyksessä Ukrainan sähköverkkoon vuonna 2016. Hyökkäys aiheutti noin tunnin ajan laajoja sähkökatkoja pääkaupunki Kiovassa. Lähdekirjallisuudessa Industroyer tunnetaan myös nimellä Crashoverride. Hyökkäyksen takana (McFail ym., 2022) arvellaan olleen Sandworm Team -

niminen APT-ryhmä, joka on yhdistetty Venäjän sotilastiedustelupalvelun GRU:n yksikköön 74455. Industroyer (Firoozjaei ym., 2022, s. 5–7) on modulaarinen haittaohjelma, joka koostuu takaportista, laukaisijasta (eng. launcher module) ja useista tukevista moduuleista.

Hyökkäyksen valmisteluun (McFail ym., 2022) on mahdollisesti hyödynnetty avointen lähteiden tiedustelua hyökkäysten kohteissa käytettyjen laitteistojen ja ohjelmistojen selvittämiseksi. Hankittujen tietojen avulla hyökkääjät ovat valmistaneet haittaohjelman, jonka valmistaminen on vaatinut erityisasiantuntemusta hyökkäysten kohteissa käytettyjen Siemensin laitteistojen ja ohjelmistojen osalta. Lisäksi hyökkäysten kohteista on hankittu käyttäjätunnuksia muun muassa Mimikatz -työkalua käyttäen.

Hyökkäyksen kohteisiin (McFail ym., 2022) on tunkeuduttu ja kohteissa on liikuttu tietokoneesta toiseen mahdollisesti käyttäen varastettuja käyttäjätunnuksia. Hyökkääjät ovat pyrkineet hankkimaan pääsyn tietokoneeseen, jolla on pystynyt olemaan yhteydessä teollisuuden ohjausjärjestelmiin (eng. industrial control system).

Pysyvän jalansijan saamiseksi ja puolustusta välttääkseen (Firoozjaei ym., 2022, s. 5–7) haittaohjelma ujuttaa itsensä järjestelmäpalveluihin, minkä ansiosta haittaohjelma käynnistyy tietokoneen uudelleen käynnistyessä. Lisäksi haittaohjelma (McFail ym., 2022) maskeeraa toimintaansa liittyvät tiedostot yleisesti käytössä olevilla nimillä ja tiedostomuodoilla.

Industroyer (McFail ym., 2022) on tiedustellut hyökkäyksen kohteessa verkkoon liitettyjä laitteita, prosessitietoja, etäkäyttöpalveluita ja järjestelmätietoja. Tiedustelutiedon ja komentojen välittämiseksi haittaohjelma (Firoozjaei ym., 2022, s. 5–7) on ollut yhteydessä hyökkääjien komentokoneisiin haittaohjelman muodostaman takaoven avulla. Lisäksi tietoliikenne haittaohjelman ja komentokoneiden välillä on reititetty Tor-verkon kautta, mikä on edesauttanut haittaohjelman piilossa pysymistä.

Lopulliset tuhot (Firoozjaei ym., 2022, s. 5–7) hyökkäysten kohteissa on aiheutettu antamalla haitallisia komentoja Siemens SIPROTEC teollisuuden ohjausjärjestelmälle. Tämä on saanut aikaan ikuisen silmukan sähkönjakeluun käytetyissä kytkimissä ja katkaisijoissa (eng. circuit breakers), minkä vuoksi sähkönjakelu on häiriintynyt. Kommunikointi ohjausjärjestelmälle on toteutettu teollisuuden ohjausjärjestelmälle ominaisia protokollia käyttäen. Haittaohjelman toiminnassa on hyödynnetty Siemens SIPROTEC:in tiedossa olleita haavoittuvuuksia (CVE-2015-5374). Lisäksi haittaohjelma on tuhonnut tuhoajamoduulilla (eng. wiper module) kovalevyiltä teollisuuden ohjausjärjestelmien asetustiedostot. Haittaohjelma tekee myös hyökkäyksestä palautumisesta vaikeaa muuttamalla palveluiden rekisteriarvoja siten, että käyttöjärjestelmästä tulee käynnistymätön. Seuraavalla sivulla olevaan taulukkoon (taulukko 7) on koottu Industroyerissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 7 Industroyerin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592.001 – Tiedon kerääminen uhrijärjestelmistä: Laitteisto T1592.002 – Tiedon kerääminen uhrijärjestelmistä: Ohjelmisto T1589.001 – Uhrin henkilöllisyystietojen kerääminen: Tunnistetiedot
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma
Alustava sisäänpääsy	T1078 – Pätevät tunnukset
Suoritus	T1106 – Alkuperäinen ohjelmointirajapinta T1059 – Komento- ja komentosarjatulkki
Pysyvyys	T1095 – Tunnusten muokkaaminen T1543 – Järjestelmäprosessien muokkaus T1133 – Ulkoiset etäpalvelut (eng. External Remote Services)
Käyttöoikeuksien laajentaminen	-
Puolustuksen välttely	T1202 – Epäsuora komennon suoritus T1078 – Pätevät tunnukset T1036 – Maskeeraus
Valtuutettu sisäänpääsy	-
Tutkinta	T1049 – Järjestelmän verkkoyhteyksien etsintä T1018 – Järjestelmän etäetsintä (eng. Remote System Discovery) T1082 – Järjestelmätietojen etsintä T1046 – Verkkopalveluiden skannaus T1135 – Verkkojaon etsiminen (eng. Network Share Discovery) T1057 – Prosessien etsintä
Liikkuminen	-
Kerääminen	T1005 – Tiedot paikallisesta järjestelmästä T1119 – Automatisoitu keräys
Komento & kontrolli	T1090 – Välityspalvelin T1572 – Protokollatunnelointi
Suodattaminen	-
Vaikutus	T1561.002 – Levyn pyyhkiminen: Levyn rakenteen pyyhkiminen (eng. Disk Wipe: Disk Structure Wipe) T1490 – Estä järjestelmän palautuminen (eng. Inhibit System Recovery) T1499 – Päätelaitteen palvelunesto T1491 – Hämääminen T1565.003 – Tiedon muokkaaminen: Ajonaikainen tiedon muokkaaminen T1489 – Palvelun pysäyttäminen (eng. Service Stop) T1498 – Verkon palvelunesto T1529 – Järjestelmän uudelleen käynnistys

4.7 Pegasus

Pegasus (Marczak ym., 2018, s. 7–10) on israelilaisen kyberturvayrityksen NSO Groupin kehittämä vakoiluhaittaohjelma. Haittaohjelma (Chawla, 2021) on tarkoitettu Android- ja iOS-käyttöjärjestelmillä varustettujen puhelimien vakoiluun. Haittaohjelma (Rudie ym., 2021) löydettiin ensimmäisen kerran vuonna 2016 Arabiemiirikuntalaisen ihmisoikeusaktivisti Ahmed Mansoorin puhelimesta. Kyseisen löydön (Marczak ym., 2018, s. 3–10) lisäksi The Citizen Labin tutkimuksissa paljastui, että haittaohjelmaa on käytetty useissa eri valtioissa niin toisinajattelijoiden kuin valtiolliseen vakoiluun. Tutkijoiden mukaan haittaohjelmaa on löytynyt ainakin 45 eri valtion alueelta ympäri maapalloa. Pegasuksesta (Chawla, 2021) on olemassa eri versiota, joita kaikkia käsitellään tässä tutkimuskappaleessa niitä erikseen erittelemättä. Pegasus (Rudie ym., 2021) on tämän tutkimuksen kirjoitushetkellä tiedossa olevista haittaohjelmista yksi kehittyneimmistä ja ensimmäinen haittaohjelma, jolla on pystytty ohittamaan (eng. Jailbreak) Apple iPhonen iOS-käyttöjärjestelmän turvallisuusjärjestelmät.

Hyökkäysten valmisteluun (Rudie ym., 2021) on käytetty paljon resursseja, sillä erityisesti haittaohjelman laatimiseen on hyödynnetty useita nollapäivähaavoittuvuuksia. Lisäksi haittaohjelmapalvelun hankkiminen NSO Groupilta on vaatinut ostajalta mittavia taloudellisia resursseja. Hyökkäysten tarkoituksena on ollut vakoilla tarkkaan valittuja henkilöitä, kuten toisinajattelijoita ja toisten valtioiden valtionjohtoa, mikä selittää saastuneiden kohteiden suhteellisen pienen lukumäärän (noin 50 000). Hyökkäysten kohteista on myös hankittu etukäteen yhteystietoja, joita on hyödynnetty haittaohjelman toimittamiseen.

Pegasus (Agrawal ym., 2022) on voitu toimittaa hyökkäysten kohteisiin kolmella eri tavalla: fyysisesti, huijauslinkkien ja ”zero-click” metodin avulla. Haittaohjelma (Rudie ym., 2021) on voitu fyysisesti toimittaa kohteeseensa, mutta hyökkäystapa on vaatinut hyökkääjältä pääsyä käsiksi saastutettavaan puhelimeen. Vaihtoehtoisesti haittaohjelma on voitu toimittaa kohteeseen tekstiviestien tai sähköpostien mukana tulevien kohdistettujen huijauslinkkien avulla. Lisäksi (Agrawal ym., 2022) Pegasuksen viimeisimmissä versioissa on hyödynnetty ns. ”zero-click” metodia, jossa haittaohjelma on toimitettu kohdepuhelimeen ilman puhelimen käyttäjän omaa toimintaa. Tässä hyökkäystavassa on hyödynnetty nollapäivähaavoittuvuuksia (CVE-2016-4655, CVE-2016-4656 ja CVE-2016-4657) toimittamalla haittaohjelma vastaamattomien WhatsApp puheluiden ja iMessage viestien avulla.

Ahmed Mansoorin (Rudie ym., 2021) tapauksessa Pegasuksen huijauslinkin avaaminen iPhone puhelimessa olisi laukaissut haittakoodin latautumisen kohdepuhelimeen. Haittakoodi on hyödyntänyt Applen WebKit verkkoselainmoottorissa (eng. the web browser engine) ja Safari -verkkoselaimessa olleita haavoittuvuuksia, jotka ovat mahdollistaneet muistiosoitteen selvittämisen iOS -käyttöjärjestelmän kernelissä. Muistiosoitteen selvittäminen on mahdollistanut koodin allekirjoittamisen (eng. code signing) poistamisen käytöstä. Koodin allekirjoittamisen käytöstä poisto on puolestaan mahdollistanut Pegasukselle

käyttöoikeuksien laajentamisen ja varsinaisen vakoilutoiminnan. Lisäksi Pegasus kykenee poistamaan itsensä hyökkäyksen kohteesta joko itsenäisesti tai NSO Groupin operaattorin toimesta. Pegasus (Agrawal ym., 2022) kykenee poistamaan myös puhelulokitietoja, jotta zero-click hyökkäyksestä ei jää jälkiä kohdepuhelimeen.

Hyökkäyksen kohteessa (Agrawal ym., 2022) Pegasus pääsee käsiksi käytännössä kaikkeen puhelimessa olevaan tietoon. Haittaohjelma kykenee kuuntelemaan mikrofonia, ottamaan videokuvaa ja hankkimaan kohdepuhelimesta paikannustietoja. Lisäksi haittaohjelma kykenee kaivamaan viestisovelluksista viestitietoja ja yhteystietoja, kohdepuhelimen järjestelmätietoja ja sovellustietoja. Haittaohjelman (Rudie ym., 2021) näppäinnauhurilla voidaan myös varastaa kohdehenkilöiden tunnistautumistietoja.

Saastuneelle puhelimelle (Marczak ym., 2018, s. 7–10) voidaan välittää komentoja hyökkääjien toimesta niin https-protokollaa kuin (Bazaliy ym., 2016, s. 17–19) SMS-viestejä käyttäen. Hankittu (Marczak ym., 2018, s. 7–10) tiedustelutieto välitetään hyökkääjien komentokoneille. Alla olevaan taulukkoon (taulukko 8) on koottu Pegasuksessa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 8 Pegasuksen hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592.002 – Tiedon kerääminen uhrijärjestelmistä: Ohjelmisto T1589 – Uhrin henkilöllisyystietojen kerääminen T1591.001 – Tiedon kerääminen uhriorganisaatiosta: Fyysisten sijaintien selvittäminen
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma T1587.004 – Kehitä kyvykkyyksiä: Hyväksikäyttömenetelmät
Alustava sisäänpääsy	T1566.001 – Tietojenkalastelu: Kohdistetut linkit T1091 – Kopioituminen siirrettävällä tietovälineellä T1189 – Laiteajurien väärentäminen
Suoritus	T1204.001 – Käyttäjän suoritus: Haitallinen linkki T1203 – Asiakkaan suorittamisen hyväksikäyttö (eng. Exploitation for Client Execution)
Pysyvyys	T1554 – Asiakasohjelmiston murtaminen (eng. Compromise Client Software Binary) T1546 – Tapahtuman käynnistämä suoritus (eng. Event Triggered Execution)
Käyttöoikeuksien laajentaminen	T1068 – Haavoittuvuuden hyödyntäminen käyttöoikeuksien laajentamiseksi (eng. Exploitation for Privilege Escalation)
Puolustuksen välttely	T1211 – Haavoittuvuuden hyödyntäminen puolustuksen välttelemiseksi (eng. Exploitation for Defense Evasion) T1070 – Tapahtumatunnisteiden poistaminen T1553.002 – Kumoa luottamuksen hallinta: Koodin allekirjoitus
Valtuutettu sisäänpääsy	T1212 – Haavoittuvuuden hyödyntäminen valtuutetun sisäänpääsyn hankkimiseksi (eng. Exploitation for Credential Access)
Tutkinta	T1614 – Sijainnin seuranta T1082 – Järjestelmätietojen etsintä T1049 – Järjestelmän verkkoyhteyksien etsintä T1518 – Ohjelmistojen etsintä

Liikkuminen	-
Kerääminen	T1123 – Äänenkaappaus T1125 – Videokaappaus T1005 – Tiedot paikallisesta järjestelmästä T1056.001 – Syötteen kaappaaminen: Näppäinnauhuri
Komento & kontrolli	T1008 – Varakanavat T1071 – Sovelluskerroksen protokollan käyttäminen
Suodattaminen	T1048 – Suodatus vaihtoehtoisen protokollan kautta (eng. Exfiltration Over Alternative Protocol) T1041 – Suodatus C2-kanavan kautta
Vaikutus	-

4.8 Shamoon

Shamoon (Hwaitat ym., 2020) on teollisuusvakoiluun ja -sabotaasiin tarkoitettu haittaohjelma. Haittaohjelmaa on käytetty hyökkäyksessä maailman suurimpaan öljy- ja energia-alan yhtiö Saudi Aramcoon. Vuonna 2012 (Bronk & Tikk-Ringas, 2013, s. 3–4) Saudi-Arabian valtion omistama Saudi Aramco joutui Shamoon haittaohjelmahyökkäyksen kohteeksi, jonka yhteydessä saastui ja tuhoutui yhtiöltä noin 30 000 Windows käyttöjärjestelmillä varustettua tietokonetta. Hyökkäyksessä Saudi Aramcolta tuhoutui tuhansien työasemien ohella myös arvokasta tuotantodataa. Lisäksi yritykseltä kului kaksi viikkoa normaalin toiminnan ja organisaation tietoverkkojen palauttamisessa. Hyökkäyksen takana (Bronk & Tikk-Ringas, 2013, s. 22) arvellaan olleen Iranilainen APT-ryhmä nimeltä ”Cutting Sword of Justice”.

Shamoon (Hwaitat ym., 2020) on tiedon tuhoamiseen tarkoitettu tuhoaja-haittaohjelma (eng. wiper). Haittaohjelma (Bronk & Tikk-Ringas, 2013, s. 17–21) koostuu asennustiedostosta (eng. dropper), tuhoamismoduulista (eng. wiper module) ja tiedotusmoduulista (eng. reporter). Asennustiedoston tarkoituksena on ollut saada haittaohjelma kohteeseen. Tiedotusmoduulin tarkoituksena on ollut ilmoittaa kohdekoneen saastumisesta hyökkääjien komentokoneelle. Tuhoamismoduulin tehtävänä on ollut tuhota tiedot kohdekoneen kovalevyltä ja tehdä kohdetietokone käyttökelvottomaksi ylikirjoittamalla kovalevyn pääkäynnistystietue (eng. master boot record).

Alkuperäisestä hyökkäysvektorista (Wangen, 2015) ei ole täyttä varmuutta, mutta (Al-Mulhim ym., 2020) tutkijoiden mukaan hyökkäyksen kohteeseen on mahdollisesti tunkeuduttu USB-muistitikkua käyttäen. Mahdollisesti käytetyn hyökkäystekniikan perusteella hyökkäyksen kohteesta on hankittu tai jo aiemmin kohdeorganisaatioon on ujutettu insider toimittamaan haittaohjelma USB-muistitikkua käyttäen.

Päästyään hyökkäyksen kohteeseen (Wangen, 2015) haittaohjelma tallentaa tiedotus- ja tuhoamismoduulit järjestelmäkansioon, luo tehtävän itsensä suorittamiseksi ja muuttaa käyttöjärjestelmän käynnistysprosesseja itsensä käynnistämiseksi tietokoneen uudelleenkäynnistyksen yhteydessä. Ennen tietojen

tuhoamista haittaohjelma muodostaa kohdetietokoneen tiedostoista listan, jonka se lähettää tiedotusmoduulilla eteenpäin hyökkääjien komentotietokoneelle.

Haittaohjelma leviää (Wangen, 2015) tietokoneesta toiseen kohdeorganisaation sisäverkossa käyttäen leviämisreittinä jaettuja resursseja (eng. network shares).

Piilossa pysymiseksi (MITRE, 2021b) haittaohjelma maskeeraa itsestään muodostamansa tehtävän muistuttamaan ”Microsoft Network Realtime Inspection Service” palvelun muodostamia ”ntssrv” -tiedostoja. Alla olevaan taulukkoon (taulukko 9) on koottu Shamoonissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 9 Shamoonin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592 – Tiedon kerääminen uhrijärjestelmistä
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma
Alustava sisäänpääsy	T1091 – Kopioituminen siirrettävällä tietovälineellä T1199 – Luotettu suhde (eng. Trusted Relationship)
Suoritus	T1053 – Aikataulutettu tehtävä
Pysyvyys	T1112 – Rekisterin muokkaaminen
Käyttöoikeuksien laajentaminen	-
Puolustuksen välttely	T1036 – Maskeeraus
Valtuutettu sisäänpääsy	-
Tutkinta	T1124 – Järjestelmän ajan selvittäminen (eng. System Time Discovery) T1016 – Järjestelmän verkkoasetusten etsintä T1082 – Järjestelmätietojen etsintä T1018 – Järjestelmän etäetsintä T1012 – Rekisterikyselyt
Liikkuminen	T1021.002 – Etäpalvelut: SMB T1570 – Sivusuuntainen työkalujen siirto
Kerääminen	-
Komento & kontrolli	T1071 – Sovelluskerroksen protokollan käyttäminen T1105 – Välineiden siirto
Suodattaminen	-
Vaikutus	T1485 – Tiedon tuhoaminen T1561.001 – Levyn pyyhkiminen: Levyn sisällön pyyhkiminen T1561.002 – Levyn pyyhkiminen: Levyn rakenteen pyyhkiminen T1490 – Estä järjestelmän palautuminen

4.9 Stuxnet

Stuxnet on (Firoozjaei ym., 2022, s. 3–5) tietokonemato, jota on käytetty hyökkäyksessä Iranin ydinlaitoksiin ja vaurioittamaan uraanin rikastamiseen käytettäviä sentrifugeja. Stuxnetin (Baezner & Robin, 2017, s. 4) kehittäjiksi on arveltu Yhdysvaltoja ja Israelia, joiden tavoitteena on ollut haitata Iranin ydinohjelmaa. Stuxnet on (Firoozjaei ym., 2022, s. 3–5) edistynyt haittaohjelma, jossa on hyödynnetty useita ennestään tuntemattomia (eng. zero-day) haavoittuvuuksia. Vuonna 2010 löydetty Stuxnet on ensimmäinen julkisesti tiedossa oleva haittaohjelma, joka on kohdistettu teollisuuden ohjausjärjestelmiä vastaan. Lisäksi voidaan todeta, että (Baezner & Robin, 2017, s. 4) Stuxnetin myötä kyberturvallisuus nousi laajemman yleisön tietoisuuteen ja yhteiskunnan kriittisen infrastruktuurin turvallisuuteen alettiin globaalisti kiinnittää enemmän huomiota.

Hyökkäyksessä (Firoozjaei ym., 2022, s. 3–5) on käytetty monipuolisesti erilaisia taktiikoita ja tekniikoita. Hyökkäystä valmisteltaessa (Chen & Abu-Nimeh, 2011) kohteesta on mahdollisesti hankittu tietoa insiderin avulla, sillä (Baezner & Robin, 2017, s. 7–8) Stuxnetin kehittäminen on vaatinut tarkkaa tietämystä kohteena olleesta Siemens Simatic WinCC/Step-7 teollisuuden ohjausjärjestelmästä. Lisäksi hyökkäys on vaatinut tietoa hyökkäyksen kohteen tiloista sekä muista käytössä olleista tietokoneohjelmista. Stuxnetin kehittämiseen on asiantuntijoiden arvioiden mukaan käytetty huomattava määrä resursseja. Stuxnetin (Chen & Abu-Nimeh, 2011) valmistamista varten on hankittu kaksi varastettua digitaalista sertifikaatti, joita on käytetty saamaan haittaohjelma näyttämään luotettavalta ohjelmalta. Lisäksi (Baezner & Robin, 2017, s. 7–8) Stuxnetin valmistamisessa on käytetty neljää nollapäivähaavoittuvuutta. Stuxnetin etukäteiseen testaamiseen on käytetty todennäköisesti vastaavanlaista laitteistoa mitä hyökkäyksen kohteessa on käytetty.

Hyökkäyksen kohteeseen (Baezner & Robin, 2017, s. 4) on mahdollisesti tunkeuduttu käyttäen USB-muistitikkua. Tätä (Baezner & Robin, 2017, s. 7) tekniikkaa on käytetty, koska hyökkäyksen kohde ei ole ollut yhteydessä Internetiin eikä muihinkaan ulkoisiin verkkoihin. Haittaohjelma (Falliere ym., 2011, s. 2) kopioi itseään hyödyntäen Microsoft Windows Shortcut 'LNK/PIF' tiedostojen suorittamiseen liittyvää haavoittuvuutta, joka oli hyökkäyksen aikana vielä nollapäivähaavoittuvuus. Haavoittuvuudella mahdollistettiin haittaohjelman automaattinen ajaminen kohdekoneessa.

Virustorjunnan ja tunkeutumisenestojärjestelmien hämäämiseksi (Falliere ym., 2011, s. 13) Stuxnetissa on käytetty menetelmää, jossa .dll -tiedostoon liittyviä latausprosesseja on muokattu antamaan hallinta hyökkääjän luomaan .dll -tiedostoon. Tässä prosessi-injektiossa (Falliere ym., 2011, s. 14–19) haittaohjelma ensin tarkistaa kohdekoneessa käytössä olevan turvallisuusohjelmiston. Lisäksi haittaohjelma tarkistaa onko sillä pääkäyttäjäoikeudet. Mikäli pääkäyttäjäoikeuksia ei vielä ole, niin niiden hankkimiseen hyödynnetään kahta käyttöoikeuksien laajentamiseen tarkoitettua nollapäivähaavoittuvuutta (joista toinen oli MS10-073 Windows Win32k.sys Local Privilege Escalation).

Turvallisuusohjelmistosta saadun tiedon ja pääkäyttöoikeuksien hankkimisen jälkeen suoritetaan kyseiselle turvallisuusohjelmistolle sopiva prosessi-injektio.

Stuxnet (Falliere ym., 2011, s. 2) on levinnyt tietokoneesta toiseen hyökkäyksen kohteen lähiverkossa. Leviämiseen (Falliere ym., 2011, s. 27–28) on hyödynnetty MS10-061 Print Spooler haavoittuvuutta, joka oli hyökkäyksen aikana vielä nollapäivähaavoittuvuus. Lisäksi haittaohjelman leviämisessä tietokoneesta toiseen oli hyödynnetty toista nollapäivähaavoittuvuutta MS08-067 Windows Server Service.

Stuxnet (Falliere ym., 2011, s. 21–23) on ollut yhteydessä hyökkääjien komentokoneisiin, joille on välitetty tietoa hyökkäyksen kohteesta http-protokollaa hyödyntäen. Stuxnet (Falliere ym., 2011, s. 25–26) on ollut yhteydessä komentokoneisiin peer-to-peer komponentilla. Komponentin avulla haittaohjelmalla saastuneet tietokoneet ovat välittäneet tietoa kohteen sisäverkosta ulkoiseen verkkoon.

Piilossa pysymiseksi Stuxnetissa (Firoozjaei ym., 2022, s. 4–5) on hyödynnetty piilohallintaohjelmistoa (eng. rootkit), jolla on piilotettu haittaohjelman haitalliset tiedostot ja prosessit virustorjunnan hämäämiseksi.

Päästyään (Firoozjaei ym., 2022, s. 4–5) käsiksi tietokoneisiin, joilla on mahdollista ohjata uraanin rikastamiseen käytettäviä sentrifugeja, Stuxnetilla aiheutettiin muutoksia sentrifugien ohjauskeskuksiin. Asetusten muuttamisella saatiin sentrifugit pyörimään liian nopeasti, jonka seurauksena laitteet hajosivat. Lisäksi käyttöliittymälle esitettiin vääriä tietoja käyttäjien hämäämiseksi ja laitteiden väärän toiminnan peittämiseksi. Alla olevaan taulukkoon (taulukko 10) on koottu Stuxnetissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 10 Stuxnetin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592.001 – Tiedon kerääminen uhrijärjestelmistä: Laitteisto T1592.002 – Tiedon kerääminen uhrijärjestelmistä: Ohjelmisto T1591.001 – Tiedon kerääminen uhriorganisaatiosta: Fyysisten sijaintien selvittäminen T1591.004 – Tiedon kerääminen uhriorganisaatiosta: Roolien tunnistaminen
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma T1588.004 – Hanki kyvykkyyksiä: Digitaaliset sertifikaatit T1588.006 – Hanki kyvykkyyksiä: Haavoittuvuudet
Alustava sisäänpääsy	T1091 – Kopioituminen siirrettävällä tietovälineellä
Suoritus	T1106 – Alkuperäinen ohjelmointirajapinta T1203 – Asiakkaan suorittamisen hyväksikäyttö T1569 – Järjestelmäpalvelut T1053 – Aikataulutettu tehtävä T1047 – WMI-palvelun hyödyntäminen T1059 – Komento- ja komentosarjatulkki
Pysyvyys	T1554 – Asiakasohjelmiston murtaminen T1547 – Käynnistyksen aikainen suorittaminen T1574 – Suoritusvirran kaappaus
Käyttöoikeuksien	T1543 – Järjestelmäprosessien muokkaus T1078 – Pätevät tunnukset

laajentaminen	
Puolustuksen välttely	T1014 – Piilohallintaohjelmisto (eng. Rootkit) T1027 – Tiedostojen hämääminen T1553 – Kumoa luottamuksen hallinta T1055 – Prosessi-injektio T1036 – Maskeeraus
Valtuutettu sisäänpääsy	T1557 – Välimieshyökkäys T1078 – Pätevät tunnukset
Tutkinta	T1018 – Järjestelmän etäetsintä T1120 – Oheislaitteiden etsintä T1082 – Järjestelmätietojen etsintä T1040 – Verkkoliikenteen seuranta
Liikkuminen	T1091 – Kopioituminen siirrettävällä tietovälineellä T1550 – Sovelluksen käyttöoikeustunnus
Kerääminen	T1005 – Tiedot paikallisesta järjestelmästä T1557 – Välimieshyökkäys T1119 – Automatisoitu keräys T1056 – Syötteen kaappaaminen
Komento & kontrolli	T1071 – Sovelluskerroksen protokollan käyttäminen
Suodattaminen	-
Vaikutus	T1565 – Tiedon muokkaaminen T1491 – Hämääminen T1495 – Laiteohjelmiston korruptoiminen (eng. Firmware Corruption) T1489 – Palvelun pysäytys

4.10 Triton

Triton (Setola ym., 2019) on teollisuuden turvallisuusjärjestelmän saastuttamiseen käytetty haittaohjelma. Haittaohjelma (Di Pinto ym., 2018, s. 2–3) on tarkoitettu vaikuttamaan Schneider Electricin kehittämään Triconex teollisuuden turvallisuusjärjestelmään. Tritonia on käytetty hyökkäyksessä Saudi-Arabialaisiin petrokemian laitoksiin joulukuussa 2017. Hyökkäyksessä Triton uudelleen ohjelmoi laitoksen Triconex turvallisuusjärjestelmää saaden aikaan teollisuuslaitoksen prosessien alasajon. Triton oli ensimmäinen julkisesti tiedossa oleva haittaohjelma, jonka kohteena on ollut teollisuuden turvallisuusjärjestelmä. Triton (Firoozjaei ym., 2022, s. 6–9) on ollut merkittävä haittaohjelma, koska Triconexin turvallisuusjärjestelmää on käytetty laajasti prosessiteollisuudessa. Kyseisten turvallisuusjärjestelmien (Di Pinto ym., 2018, s. 1) tehtävänä on estää onnettomuuksien syntyminen.

Hyökkäyksen valmistelussa (Di Pinto ym., 2018, s. 4–17) on mahdollisesti hyödynnetty avointen lähteiden tiedustelua. Julkisesti saatavilla olevista lähteistä on mahdollisesti hankittu tietoa hyökkäyksen kohteessa käytössä olevista laitteistoista ja ohjelmistoista. Tästä saaduilla tiedoilla on hankittu vastaavanlainen laitteisto kohteessa käytetyn TriStation-protokollan takaisinmallintamista ja

haittaohjelman toiminnan etukäteistä testaamista varten. TriStation-protokolla ei ole ollut julkisesti saatavilla olevaa tietoa, joten sen hyödyntäminen hyökkäyksessä on vaatinut takaisinmallintamista. TriStation-protokollaa on käytetty Triconexin turvallisuusjärjestelmässä tietoliikenteeseen ja komentojen antamiseen.

Hyökkäyksen kohteeseen tunkeutumiseen (Firoozjaei ym., 2022, s. 6–9) käytetystä tekniikasta ei ole täyttä varmuutta, mutta Triconexin kehittäneen Schneider Electricin mukaan Triton on saatu kohteen sisäiseen verkkoon mahdollisesti etäyhteyttä käyttäen.

Hyökkäyksen kohteessa (Di Pinto ym., 2018, s. 3) Triton on liikkunut kohteen sisäisestä verkosta tuotantoverkkoon hyödyntäen järjestelmiä, jotka ovat olleet saatavissa molemmissa ympäristöissä. Tuotantoverkossa Tritonilla on ollut mahdollisuus saastuttaa työasemia, joista on ollut yhteydet teollisuuden turvallisuusjärjestelmiin.

Paljastumisen estämiseksi (Firoozjaei ym., 2022, s. 6–9) Tritonin haitallinen ohjelmakoodi (eng. dropper) on maskeerattu tiedostoon trilog.exe, jotta se muistuttaisi Triconexissa käytössä ollutta Trilog-ohjelmistoa. Lisäksi Tritonin lähdekoodia on muokattu (eng. malware obfuscation) haittaohjelmien torjunnan hämäämiseksi.

Päästyään sisälle tuotantoverkkoon (Di Pinto ym., 2018, s. 3) tuotantoverkossa työskenteleviä työntekijöitä on mahdollisesti huijattu lataamaan edellä mainittu trilog.exe-tiedosto. Tiedoston lataaminen käynnisti haittaohjelman varsinaisen hyökkäyskomponentin latautumisen ja suorittamisen työntekijän päätelaitteesta Triconexin laitemuistiin.

Tritonin (Firoozjaei ym., 2022, s. 6–9) suorittamiseen hyökkäyksen kohteessa hyödynnettiin nollapäivähaavoittuvuutta. Kyseisen haavoittuvuuden ansiosta hyökkääjät saivat täyden hallinnan hyökkäyksen kohteena olleesta teollisuuden turvallisuusjärjestelmästä.

Tritonilla (Firoozjaei ym., 2022, s. 6–9) hyökkääjät onnistuivat hyökkäyksen kohteessa muokkaamaan teollisuuden turvallisuusjärjestelmiä siten, että ne mahdollistivat vaarallisten olosuhteiden muodostumisen teollisuuden prosesseissa. Alla olevaan taulukkoon (taulukko 11) on koottu Tritonissa käytetyt hyökkäystaktiikat ja -tekniikat.

TAULUKKO 11 Tritonin hyökkäystaktiikat ja -tekniikat

Tiedustelu	T1592.001 – Tiedon kerääminen uhrijärjestelmistä: Laitteisto T1592.004 – Tiedon kerääminen uhrijärjestelmistä: Asiakasmääritykset (eng. Client Configurations)
Resurssien kehittäminen	T1587.001 – Kehitä kyvykkyyksiä: Haittaohjelma
Alustava sisäänpääsy	T1195 – Toimitusketjun vahingoittaminen T1133 – Ulkoiset etäpalvelut (eng. External Remote Services)
Suoritus	T1106 – Alkuperäinen ohjelmointirajapinta
Pysyvyys	T1542.001 – Käynnistys ennen käyttöjärjestelmää: Järjestelmän laiteohjelmisto (eng. Pre-OS Boot: System Firmware)

Käyttöoikeuksien laajentaminen	-
Puolustuksen välttely	T1070 – Tapahtumatunnisteiden poistaminen T1036 – Maskeeraus T1211 – Haavoittuvuuden hyödyntäminen puolustuksen välttelemiseksi
Valtuutettu sisäänpääsy	-
Tutkinta	T1018 – Järjestelmän etäetsintä T1120 – Oheislaitteiden etsintä T1082 – Järjestelmätietojen etsintä T1057 – Prosessien etsintä
Liikkuminen	T1105 – Tiedoston etäkopiointi
Kerääminen	T1005 – Tiedot paikallisesta järjestelmästä T1119 – Automatisoitu keräys
Komento & kontrolli	T1219 – Etäkäyttöohjelmisto (eng. Remote Access Software)
Suodattaminen	T1020 – Automatisoitu suodatus
Vaikutus	T1495 – Laiteohjelmiston korruptoiminen T1485 – Tiedon tuhoaminen T1565 – Tiedon muokkaaminen T1490 – Estä järjestelmän palautuminen

5 HYÖKKÄYSTEN HUOMIOINTI KATAKRI-KRITEERISTÖN AVULLA

Tässä kappaleessa verrataan edellisessä kappaleessa kerrottujen hyökkäysten tapahtumienkulkua Katakrin vaatimuksiin. Vertailun tarkoituksena on löytää torjuntakeinoja ja puutteita Katakrin kriteeristöistä kohdistettuja haittaohjelmahyökkäyksiä vastaan.

5.1 Turvallisuusjohtaminen

Katakrin (Ulkoministeriö, 2020, s. 8–21) turvallisuusjohtamisen osa-alueen vaatimuksia noudattamalla: T-03 – Tietoturvallisuusriskien hallinta, T-04 – Turvallisuusohjeistus, T-06 – Toimintahäiriöt ja poikkeustilanteet, T-08 – Tietojen luokittelu, T-10 – Henkilöstön luotettavuuden arviointi, T-11 – Salassapito- ja vaitiolovelvollisuus sekä T-12 – Turvallisuuskoulutus, olisi voitu hyökkäykset mahdollisesti estää tai vähintään pienentää hyökkääjien mahdollisuuksia onnistua.

Kaikilla hyökkäysten kohteilla on ollut puutteita T-03 – Tietoturvallisuusriskien hallinta (Ulkoministeriö, 2020, s. 11) vaatimuksen täyttämisessä, sillä heidän arviointinsa tietoihin kohdistuneista riskeistä ei ole ollut riittävä. Riskienarvioinnin perusteella valitut tietoturvallisuustoimenpiteet ovat olleet riittämättömiä hyökkäysten torjumiseksi.

Yhdellä hyökkäyksen kohteella on ollut puutteita T-04 – Turvallisuusohjeistus (Ulkoministeriö, 2020, s. 12) vaatimuksen toteuttamisessa, sillä Shamoonin tapauksessa (Bronk & Tikk-Ringas, 2013, s. 17–21) päätelaitteiden kovalevyjen pyyhkimisen (eng. disk wipe) yhteydessä tuhoutui paljon organisaation toiminnalle arvokasta tietoa. Mikäli tietoturvaohjeistuksessa olisi ohjeistettu/vaadittu tiedostojen tallentamisesta päätelaitteiden sijasta pilvipalveluun, ei päätelaitteiden kovalevyjen pyyhkiminen olisi tuhonnut tietoja.

Kahdella hyökkäyksen kohteella on ollut puutteita T-06 – Toimintahäiriöt ja poikkeustilanteet (Ulkoministeriö, 2020, s. 14) vaatimuksen täyttämisessä. BlackEnergyn tapauksessa olemassa olleet suojaustoimenpiteet eivät riittäneet

varmistamaan tiedon eheyttä ja saatavuutta sekä järjestelmien toimintaa poikkeustilanteessa. Hyökkäysten seurauksena (Cherepanov & Lipovsky, 2016, s. 3–6) kohdekoneiden kovalevyjen tiedot tuhottiin ja aiheutettiin useiden tuntien ajan laajoja sähkökatkoja. Stuxnetin (Baezner & Robin, 2017, s. 9) kohdalla organisaatiossa ehti tuhoutua merkittävä määrä sentrifugeja haittaohjelman seurauksena, sillä laitteiden rikkoutumisen syihin alettiin pureutua tarkemmin vasta viiveellä. Organisaation olemassa olleet toimintatavat eivät olleet riittäviä laitteiston hajoamisen syiden selvittämisessä.

Kolmella hyökkäyksen kohteella on ollut puutteita T-08 – Tietojen luokittelu (Ulkoministeriö, 2020, s. 16) vaatimuksen täyttämisessä, sillä he eivät ole suojanneet riittävästi organisaationsa luottamuksellisia/salaisia tietoja. GhostNetin (Deibert ym., 2009, s. 5–6) tapauksessa hyökkäysten kohteet eivät ole mahdollisesti alkuunkaan ymmärtäneet tietojensa arvokkuutta ja ovat siten jättäneet tietonsa salaamatta. Industroyerin (McFail ym., 2022) kohdalla puutteellinen tietojenluokittelu on mahdollistanut hyökkääjille järjestelmiin liittyvien arkaluonteisten tietojen hankkimisen avointen lähteiden tiedustelulla. Tritonin (Di Pinto ym., 2018, s. 4–17) tapauksessa organisaation toimitusketjussa oleva toimija ei ole suojannut riittävästi teollisuusjärjestelmiinsä liittyviä tietoja. Schneider Electric ei ole laitetoimittajana tunnistanut ja luokitellut tietoaineistoaan arkaluonteisen tiedon paljastumisen estämiseksi. Puutteellisen tietojenluokittelun vuoksi hyökkääjät ovat mahdollisesti saaneet tietoonsa järjestelmiin liittyviä arkaluonteisia tietoja kyselemällä hyökkäyksen kohteen ja Schneider Electricin järjestelmäasiantuntijoilta. Kyseiset henkilöt eivät ole välttämättä tiedostaneet tietojen arkaluonteisuutta niiden puutteellisen luokituksen vuoksi.

Kolmella hyökkäyksen kohteella on ollut puutteita T-10 – Henkilöstön luotettavuuden arviointi (Ulkoministeriö, 2020, s. 18) vaatimuksen toteuttamisessa, koska kohteisiin on hyökätty mahdollisesti insiderin toimesta. Flamen (Bermejo Higuera ym., 2020, s. 23), Shamoonin (Al-Mulhim ym., 2020) ja Stuxnetin (Baezner & Robin, 2017, s. 4) tapauksissa hyökkäyksen kohteeseen on mahdollisesti tunkeuduttu insiderin toimittamaa USB-muistitikkua käyttäen. Henkilöstön turvallisuusselvittämisellä (Ulkoministeriö, 2020, s. 18) olisi voitu vähentää mahdollisista insidereista aiheutuvia riskejä. Henkilöstön turvallisuusselvittämisellä olisi mahdollisesti havaittu insider-tekoihin altistavia tekijöitä organisaation henkilöstössä.

Yhdellä hyökkäyksen kohteella on ollut puutteita T-11 – Salassapito- ja vaitiolovelvollisuus (Ulkoministeriö, 2020, s. 19) vaatimuksen täyttämisessä, sillä Tritonin (Di Pinto ym., 2018, s. 4–17) tapauksessa kohteen työntekijät ja laitevalmistajan asiantuntijat ovat mahdollisesti kertoneet avuliaasti järjestelmiin liittyviä tietoja hyökkääjille. Kaikkiin mahdollisiin kyselyihin tulisi aina suhtautua varauksella.

Seitsemällä hyökkäyksen kohteella on ollut puutteita T-12 – Turvallisuuskoulutus (Ulkoministeriö, 2020, s. 20) vaatimuksen toteuttamisessa. BlackEnergyn (Cherepanov & Lipovsky, 2016, s. 2–3) tapauksessa henkilöstö ei ole ymmärtänyt joutuneensa tietojenkalastelun uhriksi. Lisäksi haittaohjelman tunkeutumisreittinä käytetty Microsoft Office -tiedoston makrojen hyväksymisen

vaatiminen olisi pitänyt herättää epäilyksiä henkilöstössä. Duqun (Chien ym., 2012) kohdalla hyökkäysten kohteisiin on tunkeuduttu huijaussähköpostien liitteinä olleiden liitetiedostojen avulla. Organisaation ulkopuolelta tulleiden tiedostojen avaamisessa tulisi aina noudattaa varovaisuutta ja tätä olisi voinut korostaa henkilöstön turvallisuuskoulutuksessa. GhostNetin (Deibert ym., 2009, s. 5–6) tapauksessa hyökkäysten kohteisiin tunkeutumisessa ja eteenpäin leviämisessä on hyödynnetty huijaussähköposteja sekä haitallisia liitetiedostoja. Vaikka hyökkäyksissä käytetyt sähköpostit ja liitetiedostot ovat olleet taitavasti tehtyjä, olisi henkilöstön tietoturvakoulutuksessa voitu ottaa paremmin huomioon vastaavanlaiset hyökkäysvektorit. Havex (Kaspersky, 2014, s. 2–3) hyökkäyksissä osaan kohteista on tunkeuduttu huijaussähköpostien liitetiedostoissa olevilla haittaohjelmilla. Pegasuksen (Rudie ym., 2021) osalta onnistuneella turvallisuuskoulutuksella olisi mahdollisesti vähennetty tai estetty kokonaan haittaohjelman tarttuminen huijauslinkkien avaamisen kautta. Shamoonin (Bronk & Tikk-Ringas, 2013, s. 17–21) osalta tietoturvakoulutuksessa olisi voitu ohjeistaa tiedostojen tallentamisesta päätelaitteiden sijasta pilvipalveluun. Tällöin päätelaitteiden kovalevyjen tietojen tuhoaminen ei olisi tuhonnut organisaatiolle tärkeitä tietoja tai vähintäänkin tuhoutuneiden tietojen määrä olisi pysynyt maltillisempana. Tritonissa (Di Pinto ym., 2018, s. 4–17) haittaohjelman liikkumiseen ja asentumiseen tuotantoverkon sisällä on mahdollisesti hyödynnetty työntekijöiden huijaamista. Lisäksi työntekijät eivät ole mahdollisesti tunnistaneet heihin kohdistuneita tietojenkalasteluja. Alla olevaan taulukkoon (taulukko 12) on koottu hyökkäysten kohteiden puutteet Katakrin turvallisuusjohtamisen vaatimusten toteuttamisessa.

TAULUKKO 12 Hyökkäysten kohteiden puutteet turvallisuusjohtamisessa

Katakri kriteeri	**Hyökkäys**
T-03 – Tietoturvallisuusriskien hallinta	BlackEnergy, Duqu, Flame, GhostNet, Havex, Industroyer, Pegasus, Shamoon, Stuxnet, Triton
T-04 – Turvallisuusohjeistus	Shamoon
T-06 – Toimintahäiriöt ja poikkeustilanteet	BlackEnergy, Stuxnet
T-08 – Tietojen luokittelu	GhostNet, Industroyer, Triton
T-10 – Henkilöstön luotettavuuden arviointi	Flame, Shamoon, Stuxnet
T-11 – Salassapito- ja vaitiolovelvollisuus	Triton
T-12 - Turvallisuuskoulutus	BlackEnergy, Duqu, GhostNet, Havex, Pegasus, Shamoon, Triton

5.2 Fyysinen turvallisuus

Katakrin (Ulkoministeriö, 2020, s. 22–62) fyysisen turvallisuuden osa-alueen vaatimuksia noudattamalla: F-01 – Fyysisten turvatoimien tavoite, F-02 – Riskien arviointi ja F-03 – Fyysisten turvatoimien valinta, olisi voitu hyökkäykset mahdollisesti estää tai vähintään pienentää hyökkääjän mahdollisuuksia onnistua.

Neljällä hyökkäyksen kohteella on ollut puutteita F-01 – Fyysisten turvatoimien tavoite (Ulkoministeriö, 2020, s. 24) vaatimuksen täyttämisessä, koska kohteiden turvatoimet ovat olleet riittämättömiä hyökkäyksen torjumiseksi.

Neljällä hyökkäyksen kohteella on ollut puutteita F-02 – Riskien arviointi (Ulkoministeriö, 2020, s. 25) vaatimuksen täyttämisessä, koska puutteellisen riskien arvioinnin perusteella kohteet eivät ole toteuttaneet riittäviä turvatoimia.

Neljällä hyökkäyksen kohteella on ollut puutteita F-03 – Fyysisten turvatoimien valinta (Ulkoministeriö, 2020, s. 25–28) vaatimuksen täyttämisessä, koska valitut turvatoimet ovat olleet riittämättömiä. Flamen (Bermejo Higuera ym., 2020, s. 23), Shamoonin (Al-Mulhim ym., 2020) ja Stuxnetin (Baezner & Robin, 2017, s. 4) tapauksissa hyökkäyksen kohteeseen on tunkeuduttu insiderin toimittamaa USB-muistitikkua käyttäen. Kohteissa olisi voitu esimerkiksi käyttää kameravalvontaa valvomaan toimintaa tärkeiden työpisteiden osalta. Lisäksi koulutettua vartiointihenkilöstöä olisi voitu hyödyntää työntekijöille tehtävissä sisääntulotarkastuksissa. Sisääntulotarkastusten ja kameravalvonnan avulla olisi voitu mahdollisesti havaita luvattomien USB-välineiden tuominen kohdeorganisaation tiloihin sekä niiden luvaton käyttäminen. Pegasuksen (Rudie ym., 2021) kohdalla kohdepuhelin on voitu joissain tapauksissa saastuttaa hyökkääjän päästyä fyysisesti käsiksi puhelimeen. Omia tietoteknisiä välineitä ei tulisi jättää koskaan valvomatta.

Kahdella hyökkäyksen kohteella on ollut puutteita F-04 – Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella (Ulkoministeriö, 2020, s. 29–32) vaatimuksen toteuttamisessa. Pegasuksen (Rudie ym., 2021) kohdalla kohdepuhelin on voitu joissain tapauksissa saastuttaa hyökkääjän päästyä fyysisesti käsiksi puhelimeen. Omia tietoteknisiä välineitä ei tulisi jättää koskaan valvomatta. Stuxnetin (Baezner & Robin, 2017, s. 4) tapauksessa, mikäli kohteen henkilöstön normaalissa toiminnassa on käytetty muistitikkuja, niin onko muistitikkuja suojattu riittävästi kohdelaitoksen ulkopuolella? Jos kohteen toiminnassa on käytetty muistitikkuja, niin työntekijän USB-muistitikku on voitu joko saastuttaa tai vaihtaa saastuneeseen hyökkääjien toimesta. Alla olevaan taulukkoon (taulukko 13) on koottu hyökkäysten kohteiden puutteet Katakrin fyysisen turvallisuuden vaatimusten toteuttamisessa.

TAULUKKO 13 Hyökkäysten kohteiden puutteet fyysisessä turvallisuudessa

Katakri kriteeri	**Hyökkäys**
F-01 – Fyysisten turvatoimien tavoite	Flame, Pegasus, Shamoon, Stuxnet
F-02 – Riskien arviointi	Flame, Pegasus, Shamoon, Stuxnet
F-03 – Fyysisten turvatoimien valinta	Flame, Pegasus, Shamoon, Stuxnet
F-04 – Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella	Pegasus, Stuxnet

5.3 Tekninen tietoturvallisuus

Katakrin (Ulkoministeriö, 2020, s. 63–106) teknisen tietoturvallisuuden osa-alueen vaatimuksia noudattamalla: I-01 – Verkon rakenteellinen turvallisuus, I-02 – Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä, I-04 – Hallintayhteydet, I-06 – Pääsyoikeuksien hallinnointi, I-07 – Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä, I-08 – Järjestelmäkovennus, I-09 – Haittaohjelmasuojaus, I-10 – Turvallisuuteen liittyvien tapahtumien jäljitettävyys, I-11 – Poikkeamien havainnointikyky ja toipuminen, I-12 – Salausratkaisut, I-13 – Ohjelmistojen suojaaminen verkkohyökkäyksiltä, I-16 – Muutoshallintamenettelyt, I-18 – Etäkäyttö ja etähallinta, I-19 – Ohjelmistohaavoittuvuuksien hallinta ja I-20 – Varmuuskopiointi, olisi voitu hyökkäykset mahdollisesti havaita ja estää.

Kahdella hyökkäysten kohteella on ollut puutteita I-01 – Verkon rakenteellinen turvallisuus (Ulkoministeriö, 2020, s. 65–68) vaatimuksen täyttämisessä. BlackEnergyssa (Firoozjaei ym. 2022, s. 4) hyökkääjä on päässyt siirtymään toimistoverkossa tuotantolaitteita säätelevään tietokoneeseen. Tietojenkäsittely-ympäristöjen erottelulla toisistaan olisi voitu rajata tuotantolaitteiden säätämiseen käytettävät tietokoneet eri verkkoon kuin toimistoverkon tietokoneet. Tritonin (Firoozjaei ym., 2022, s. 6–9) osalta hyökkääjät ovat päässeet liikkumaan organisaation sisäisestä verkosta tuotantoverkkoon. Vaikka organisaation sisäinen verkko ja tuotantoverkko ovat olleet eriytettyjä toisistaan, on sisäisessä verkossa ollut laitteita ja/tai ohjelmistoja yhteydessä tuotantoverkkoon.

Kahdeksalla hyökkäyksen kohteella on ollut puutteita I-02 – Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä (Ulkoministeriö, 2020, s. 69–70) vaatimuksen toteuttamisessa. BlackEnergyn (Cherepanov & Lipovsky, 2016, s. 4), GhostNetin (Deibert ym., 2009, s. 18–30), Havexin (Firoozjaei ym., 2022, s. 8–10) ja Industroyerin (Firoozjaei ym., 2022, s. 5–7) kohdalla haittaohjelma on ollut yhteydessä organisaation sisäverkosta organisaation ulkoisessa verkossa oleviin komentokoneisiin. Organisaation sisäverkosta ulkoiseen verkkoon lähteneet yhteydet tulisi rajata vain välityspalvelimen kautta kulkevaan verkkoliikenteeseen ja vain tarpeellisiin yhteyksiin (lähde-protokolla-kohde). Duqussa (Bencsáth ym., 2012_a) hyökkääjät ovat levittäneet haittaohjelmaa tietokoneesta toiseen ja keskustelleet saastuneiden koneiden kanssa sisäverkon välityksellä. Lisäksi ensimmäiseksi saastunutta tietokonetta on käytetty välityspalvelimena ulkoiseen verkkoon. Flamessa (Bencsáth ym., 2012_b) haittaohjelma on voinut liikkua laitteesta toiseen kohteen sisäverkossa. Lisäksi haittaohjelma on ollut yhteydessä hyökkääjien komentokoneisiin kohdeorganisaatioiden sisäverkosta. Shamoonin (Wangen, 2015) osalta haittaohjelma on päässyt leviämään kohdeorganisaation sisäverkossa käyttäen leviämisreittinä jaettuja resursseja (eng. network shares). Stuxnetin (Falliere ym., 2011, s. 2) tapauksessa haittaohjelma on voinut liikkua laitteesta toiseen kohteen sisäverkossa. Vaikka hyökkäyksen kohde ei ole ollut yhteydessä ulkoisiin verkkoihin, olisi

kohteen sisäisen verkon segmentoinnilla ja niiden välisellä tietoliikenteen suodatuksella ollut haittaohjelman leviämistä ehkäisevä vaikutus.

Kahdella hyökkäyksen kohteella on ollut puutteita I-04 – Hallintayhteydet (Ulkoministeriö, 2020, s. 72–73) vaatimuksen täyttämisessä. Tritonin (Firoozjaei ym., 2022, s. 6–9) osalta turvallisuusjärjestelmien muuttamiseen ja Industroyerissa (Firoozjaei ym., 2022, s. 5–7) sähköverkon ohjauslaitteiden asetusten muuttamiseen käytetyt hallintayhteydet eivät ole kulkeneet kovennettujen hyppykoneiden kautta, joissa turvallisuusjärjestelmille ja asetuksille tehtävät muutokset olisi mahdollisesti havaittu.

Yhdellä hyökkäyksen kohteella on ollut puutteita I-06 – Pääsyoikeuksien hallinnointi (Ulkoministeriö, 2020, s. 75–77) vaatimuksen täyttämisessä, sillä BlackEnergyn (Firoozjaei ym., 2022, s. 5) tapauksessa kriittisten ylläpitotoimien tekemiseen ei ole vaadittu kahden henkilön hyväksyntää. Vaatimalla kahden henkilön hyväksyntää olisi voitu mahdollisesti estää hyökkääjien tekemän varavoiman irtikytkennän.

Yhdellä hyökkäyksen kohteella on ollut puutteita I-07 – Tietojenkäsittelyympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä (Ulkoministeriö, 2020, s. 78–79) vaatimuksen täyttämisessä, koska Tritonissa (Firoozjaei ym., 2022, s. 6–9) turvallisuusjärjestelmien asetuksia on muutettu ilman riittävää tunnistamista. Mikäli asetuksien muuttajan tunnistamiseen olisi vaadittu vahvaa käyttäjätunnistusta ja/tai kahden henkilön osallistumista, olisi turvallisuusjärjestelmän asetusten muuttaminen ollut hyökkääjille huomattavasti vaikeampaa.

Viidellä hyökkäyksen kohteella on ollut puutteita I-08 – Järjestelmäkovennus (Ulkoministeriö, 2020, s. 80–82) vaatimuksen täyttämisessä. Flamessa (Bermejo Higuera ym., 2020, s. 23), Shamoonissa (Al-Mulhim ym., 2020) ja Stuxnetissa (Baezner & Robin, 2017, s. 4) haittaohjelma on mahdollisesti toimitettu kohteeseen USB-muistitikulla. Kohteissa käytetyistä tietokoneista olisi voinut kovennetun asennuksen yhteydessä poistaa datan vienti- ja tuontiliitynnät, estää tiedon lataaminen USB-muistitikuilta, estää laitelistaan kuulumattomien laitteiden toiminta tai vähintäänkin rajoittaa ohjelmistojen suoritusoikeuksia. Havex (Firoozjaei ym., 2022, s. 8–10) hyökkäysten kohteista on hankittu arkaluonteisia tietoja. Järjestelmistä tulisi poistaa kaikki mahdolliset tarpeettomat ohjelmistot ja tiedot, jotta hyökkääjä ei voisi niissä olevia mahdollisia ohjelmistohaavoittuvuuksia hyödyntäen hyökätä syvemmälle kohteeseen tai hyödyntää tietoa jollain muulla tavalla. Tutkijoiden (Rudie ym., 2021) mukaan Pegasus hyökkäykset olisi voitu estää kernelin koventamisella.

Yhdeksällä hyökkäyksen kohteella on ollut puutteita I-09 – Haittaohjelmasuojaus (Ulkoministeriö, 2020, s. 83–84) vaatimuksen toteuttamisessa. BlackEnergyn (Cherepanov & Lipovsky, 2016, s. 2–3) tapauksessa sähköpostin liitetiedostona tullut haittaohjelman latautuminen makrojen hyväksymisen jälkeen olisi pitänyt havaita haittaohjelmasuojauksella. Duqun (Bencsáth ym., 2012_b) osalta hyökkäyksessä on käytetty nollapäivähaavoittuvuutta, mutta tutkijoiden mukaan haittaohjelma on ollut silti havaittavissa. Flamen (Bencsáth ym., 2012_b) tapauksessa haittaohjelmasuojaukset eivät ole havainneet haittaohjelman

suorittamaa prosessi-injektiota. Tutkijoiden (Deibert ym., 2009, s. 18) mukaan vain 11/34 tutkitusta virustorjuntajärjestelmästä havaitsi GhostNet hyökkäyksissä käytetyn haittaohjelman liitetiedostoista. Korkean turvallisuustason tiedon järjestelmissä voisi käyttää vähintään kahden eri toimittajan virustorjuntajärjestelmää, jotta järjestelmät paikkaisivat toistensa mahdollisia puutteita. Myöskään Havexissa (Firoozjaei ym., 2022, s. 8–10) ja Shamoonissa (Wangen, 2015) kohteiden haittaohjelmatorjunta ei ole havainnut ja torjunut hyökkäystä. Industroyerin (Firoozjaei ym., 2022, s. 5–7) osalta haittaohjelmasuojaus ei ole havainnut hyökkäystä, vaikka kohteisiin tunkeutumisessa ei ole hyödynnetty nollapäivähaavoittuvuuksia. Kappaleessa 4.7 tarkastelluissa tutkimuksissa ei löytynyt mainintoja haittaohjelmasuojauksen käyttämisestä Pegasus uhrien älypuhelimissa. Stuxnetissa (Firoozjaei ym., 2022, s. 4) on käytetty neljää nollapäivä haavoittuvuutta, joista kolmea on käytetty haitallisen koodin etäsuorittamiseen (eng. remote code execution). Lisäksi haittaohjelman itsenäiseen suorittamiseen (eng. self-launching) ja leviämiseen on hyödynnetty yhtä nollapäivä haavoittuvuutta. Haittaohjelman kohdejärjestelmälle haitallista toimintaa on piiloteltu taitavasti piilohallintaohjelmistolla, joka piilottaa haitalliset tiedostot ja prosessit haittaohjelmasuojaukselta. Näiden ennestään tuntemattomien haavoittuvuuksien torjuminen ja havaitseminen on haastavaa, mutta säännöllisellä haittaohjelmatunnisteiden päivityksellä voidaan parantaa havaitsemista.

Kahdella hyökkäyksen kohteella on ollut puutteita I-10 – Turvallisuuteen liittyvien tapahtumien jäljitettävyys (Ulkoministeriö, 2020, s. 85–86) vaatimuksen toteuttamisessa. BlackEnergy (Firoozjaei ym., 2022, s. 4–6) hyökkäyksissä hyökkääjä on onnistunut haittaohjelman KillDisk -komponentilla tuhoamaan lokitietoja. Lokitietojen turvaamiseksi olisi lokitiedot voitu ohjata vahvasti suojatulle lokipalvelimelle, jonka tiedot varmuuskopioidaan säännöllisesti. Tritonin (Di Pinto ym., 2018, s. 4–17) tapauksessa prosessiturvallisuuteen liittyvien tapahtumien tapahtumalokitus kohdeorganisaatiossa on ollut puutteellista. Turvallisuusjärjestelmien tapahtumalokien ohjaaminen keskitetylle lokipalvelimelle olisi mahdollisesti helpottanut turvallisuuteen haitallisten tapahtumien nopeammassa tunnistamisessa.

Kaikilla hyökkäysten kohteilla on ollut puutteita I-11 – Poikkeamien havainnointikyky ja toipuminen (Ulkoministeriö, 2020, s. 87–88) vaatimuksen täyttämisessä. BlackEnergyn (Firoozjaei ym., 2022, s. 4–6) hyökkäysten kohteissa ei ole ollut riittävää teknistä havainnointikykyä hyökkäyksen havaitsemiseksi. Vaikka haittaohjelman lähettämä tietoliikenne on pyritty saamaan näyttämään mahdollisimman normaalilta, tulisi tällainen normaalista poikkeavaan kohteeseen lähtevä tietoliikenne havaita tunkeutumisen havaitsemis- tai estojärjestelmin. Lisäksi hyökkäyksessä (Cherepanov & Lipovsky, 2016, s. 5) muutettiin käynnistysprosesseja, joiden muuttaminen olisi pitänyt havaita. Duqun (Bencsáth ym., 2012_b) hyökkäysten kohteet eivät ole havainneet järjestelmissään tapahtuvaa normaalista poikkeavaa toimintaa. Vaikka haittaohjelman tekijät ovat hyvin onnistuneet piilottamaan haittaohjelman toiminnasta aiheutuvia jälkiä, on Duqu kuitenkin aiheuttanut hyökkäysten kohteissa merkkejä epänormaalista toiminnasta. Tutkijoiden mukaan haittaohjelman havaitsemista varten on

nykyisin olemassa työkaluja. Flamen (Bencsáth ym., 2012_b) liikkumista ja käynnistysprosessien muuttamista järjestelmissä ei ole havaittu. GhostNet (Deibert ym., 2009, s. 18–25) hyökkäysten kohteet eivät ole havainneet järjestelmissään tapahtuvaa normaalista poikkeavaa toimintaa. Havex (Firoozjaei ym., 2022, s. 8–10) hyökkäysten kohteiden tunkeutumisenestojärjestelmät eivät ole havainneet muutoksia järjestelmien käynnistysprosesseissa. Lisäksi ohjelmistojen toimittajilta on mennyt pitkä aika havaita hyökkääjien peukaloimat ohjelmistot nettisivuillaan. Industroyerin (Firoozjaei ym., 2022, s. 5–7) tekemää tiedustelua, liikkumista laitteesta toiseen ja tiedon siirtämistä organisaation ulkopuolisille komentokoneille ei ole havaittu. Pegasuksen (Marczak ym., 2018, s. 7–10) aiheuttamaa poikkeavaa liikennettä komentokoneille ei ole havaittu. Shamoon (Wangen, 2015) on päässyt tunkeutumisenhavaitsemisjärjestelmiltä huomaamatta leviämään tuhansiin tietokoneisiin kohdeorganisaation sisällä. Leviäminen verkon välityksellä tuhansiin tietokoneisiin olisi pitänyt pystyä havaitsemaan poikkeamana. Stuxnetin (Firoozjaei ym., 2022, s. 3–5) tapauksessa haittaohjelman liikkumista ja asetusten muuttamista järjestelmissä ei ole havaittu. Lisäksi haittaohjelma on pysynyt piilossa kohdejärjestelmissä pitkän aikaa. Tritonin (Di Pinto ym., 2018, s. 4–17) aiheuttamia muutoksia turvallisuusjärjestelmissä ei ole havaittu. Tuotantoverkon tietoliikenteen normaalin tilan valvonnassa on ollut puutteita, koska järjestelmien turvallisuudelle haitallista tietoliikennettä ei ole havaittu. Muutokset järjestelmissä (Setola ym., 2019) on havaittu vasta sen jälkeen, kun hyökkääjät saivat mahdollisesti vahingossa aikaan teollisuusprosessien alasajon hyökkäyksen kohteessa.

Neljällä hyökkäyksen kohteella on ollut puutteita I-12 – Salausratkaisut (Ulkoministeriö, 2020, s. 89–90) vaatimuksen täyttämisessä. BlackEnergyssa (Firoozjaei ym., 2022, s. 5–6) hyökkääjät ovat hankkineet tunnistetietoja kohdekoneiden verkkoselaimien tiedostoista. Tunnistetietojen salaamisella olisi tunnistetietojen varastaminen ja hyödyntäminen tehty paljon vaikeammaksi hyökkääjille. GhostNet (Deibert ym., 2009, s. 18–25) ja Havex (Kaspersky, 2014, s. 2–3) hyökkäysten kohteista varastetut tiedot ja tiedostot eivät ole olleet salattuja. Kunnollisella tietojen luokittelulla ja tietojen salaaminen luokituksenmukaisella salauksella olisi varmasti haitannut tai jopa estänyt hyökkääjiä hyödyntämästä varastettua tietoa. Tritonin (Di Pinto ym., 2018, s. 4–17) tapauksessa hyökkäyksen kohteessa käytetyssä TriStation-protokollassa ei ole käytetty salausta. Mikäli protokollan tietoliikenne ja sen toimintaan liittyvät tiedostot olisivat olleet salattuja, olisi sen takaisinmallintaminen ollut hyökkääjille paljon vaikeampaa.

Neljällä hyökkäyksen kohteella on ollut puutteita I-13 – Ohjelmistojen suojaaminen verkkohyökkäyksiltä (Ulkoministeriö, 2020, s. 91–92) vaatimuksen täyttämisessä. Duqun (Symantec, 2011, s. 1–3) osalta haittaohjelman latautumista ja asentumista ei ole havaittu haitallisen sähköposti liitetiedoston avaamisen yhteydessä. GhostNetissa (Deibert ym., 2009, s. 18–25) huijaussähköpostin liitetiedoston avaaminen on saanut aikaan gh0st RAT haittaohjelman latautumisen kohdetietokoneelle. Haittaohjelman latautumisen estämiseksi tai sen toiminnan rajoittamiseksi olisi kohteessa voitu hyödyntää esimerkiksi virtualisointia. BlackEnergy (Cherepanov & Lipovsky, 2016, s. 2–3) ja Havex (Kaspersky, 2014,

s. 2–3) hyökkäyksissä sähköpostin liitteinä tulleiden tiedostojen toimintaa olisi voitu rajoittaa esimerkiksi sovelluspalomuurin käytöllä.

Kolmella hyökkäyksen kohteella on ollut puutteita I-16 – Muutoshallintamenettelyt (Ulkoministeriö, 2020, s. 96–97) vaatimuksen täyttämisessä. Säännöllisillä tietoturva-auditoinneilla ja tietojärjestelmien asetuksien muuttumisen valvonnalla BlackEnergy olisi voitu mahdollisesti havaita. Kappaleessa 4.1 tutkitussa aineistossa ei havaittu mainintoja kohteen järjestelmille tehdyistä tietoturva-auditoinneista. Vaikka Flame (Fillinger & Stevens, 2015) esiintyi Windowsin päivityspalvelimena ja sai haitalliset päivitykset siirtymään toisiin koneisiin kohdeorganisaatioissa, olisi tällainen tietokoneiden päivitysjärjestely oltava poissa käytöstä. Organisaation tietokoneiden päivityksien tulisi olla järjestetty esimerkiksi vahvasti kovennettujen keskitettyjen päivityspalvelimien kautta, jolloin saastuneen tietokoneen esiintyminen päivityspalvelimena ei olisi mahdollista. Havexilla (Firoozjaei ym., 2022, s. 8–10) saastutetut ohjelmistotuottajien nettisivuilta ladatut ohjelmistot olisi voitu ensiksi asentaa testiympäristöön niiden turvallisen toiminnan varmistamiseksi.

Kahdella hyökkäyksen kohteella on ollut puutteita I-18 – Etäkäyttö ja etähallinta (Ulkoministeriö, 2020, s. 100–101) vaatimuksen noudattamisessa. BlackEnergyn (Firoozjaei ym., 2022, s. 4–7) osalta järjestelmien etäkäytössä ei ole käytetty vahvaa tunnistautumista. Vaikka hyökkäyksissä käytetyillä näppäinnauhureilla ja näyttöleikkeiden otolla hyökkääjät saivat käsiinsä tunnistautumistietoja, olisi myös muihin tekijöihin perustuvan käyttäjätunnistautumisen käyttö (kuten mobiilivarmenne tai varmennekortti) varmasti vaikeuttanut tunkeutumista hyökkäysten kohteiden VPN-verkkoihin. Pegasuksen (Rudie ym., 2021) tapauksissa hyökkäysten kohteiden älypuhelimet on saastutettu todennäköisimmin organisaatioiden omien tilojen ulkopuolella. Älypuhelimiin pääsyä organisaation omien tilojen ulkopuolella ei ole suojattu riittävästi sivullisten peukaloinnilta eikä puhelimien sisältöä ole salattu sopivalla menetelmällä.

Kuudella hyökkäyksen kohteella on ollut puutteita I-19 – Ohjelmistohaavoittuvuuksien hallinta (Ulkoministeriö, 2020, s. 102–103) vaatimuksen täyttämisessä. BlackEnergyssa (Firoozjaei ym., 2022, s. 4) hyökkääjät ovat hyödyntäneet VirtualBox -ohjelmiston käyttöoikeuksien laajentamiseen liittyvää haavoittuvuutta CVE-2008-3431. Hyökkäyksen aikaan haavoittuvuus on ollut julkisesti tiedossa. Flamen (Bencsáth ym., 2012_b) tapauksessa haittaohjelma on levinnyt hyökkäysten kohteessa hyödyntäen kahta tiedossa ollutta ohjelmistohaavoittuvuutta print spooler exploit (MS10-061) ja LNK exploit (MS10-046). Myöskin Havexin (Kaspersky, 2014, s. 2–3) kohdalla ohjelmistohaavoittuvuuksien hallinta ohjelmistopäivityksien osalta on ollut puutteellista, koska hyökkäyksissä ei ole hyödynnetty nollapäivähaavoittuvuuksia. Industroyerissa (Firoozjaei ym., 2022, s. 5–7) ei ole käytetty nollapäivähaavoittuvuuksia. Myös teollisuuden ohjausjärjestelmien ohjelmistot tulisi päivittää säännöllisesti parhaimman mahdollisen ohjelmistohaavoittuvuussuojan takaamiseksi. Kohteiden tulisi seurata paremmin käytössä olevien ohjelmistojen haavoittuvuustiedotteita ja paikata kaikki tiedossa olevat haavoittuvuudet. Pegasus (Rudie ym., 2021) hyökkäyksissä on hyödynnetty ainakin kolmea eri nollapäivähaavoittuvuutta.

Nollapäivähaavoittuvuuksien torjuminen on vaikeaa, mutta ohjelmistojen säännöllisellä päivityksellä on mahdollista pienentää niistä aiheutuvia riskejä. Myös Tritonissa (Firoozjaei ym., 2022, s. 6–9) on käytetty nollapäivähaavoittuvuutta. Laiteohjelmistot tulisi päivittää säännöllisesti parhaimman mahdollisen ohjelmistohaavoittuvuussuojan takaamiseksi.

Kahdella hyökkäyksen kohteella on ollut puutteita I-20 – Varmuuskopiointi (Ulkoministeriö, 2020, s. 104) vaatimuksen täyttämisessä. BlackEnergyssa (Firoozjaei ym., 2022, s. 4–7) hyökkäyksen loppuvaiheessa hyökkääjät ovat onnistuneet tuhoamaan kohteessa tärkeät tiedostot. Tämä aiheutti jopa yli kuuden tunnin mittaisen sähkökatkon, jonka pituutta olisi varmasti voitu lyhentää tärkeiden tiedostojen nopeammalla palautusprosessilla. Shamoonin (Bronk & Tikk-Ringas, 2013, s. 3–4) osalta uhriorganisaatiolla on kestänyt kaksi viikkoa oman toiminnan palauttamisessa normaaliksi, jonka lisäksi hyökkäyksen seurauksena tuhoutui paljon yritykselle arvokasta tietoa. Tietojen tallentaminen keskitetylle varmuuskopiopalvelimelle olisi vähentänyt merkittävästi tuhoutuneen tiedon määrää. Lisäksi varmuuskopioiden palautusprosessin säännöllinen testaaminen olisi mahdollisesti lyhentänyt hyökkäyksestä aiheutunutta toimintakatkosta. Alla olevaan taulukkoon (taulukko 14) on koottu hyökkäysten kohteiden puutteet Katakrin teknisen tietoturvallisuuden vaatimusten toteuttamisessa.

TAULUKKO 14 Hyökkäysten kohteiden puutteet teknisessä tietoturvallisuudessa

Katakri kriteeri	**Hyökkäys**
I-01 – Verkon rakenteellinen turvallisuus	BlackEnergy, Triton
I-02 – Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusalueen sisällä	BlackEnergy, Duqu, Flame, GhostNet, Havex, Industroyer, Shamoon, Stuxnet
I-04 – Hallintayhteydet	Industroyer, Triton
I-06 – Pääsyoikeuksien hallinnointi	BlackEnergy
I-07 – Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä	Triton
I-08 – Järjestelmäkovennus	Flame, Havex, Pegasus, Shamoon, Stuxnet
I-09 – Haittaohjelmasuojaus	BlackEnergy, Duqu, Flame, GhostNet, Havex, Industroyer, Pegasus, Shamoon, Stuxnet
I-10 – Turvallisuuteen liittyvien tapahtumien jäljitettävyys	BlackEnergy, Triton
I-11 – Poikkeamien havainnointikyky ja toipuminen	BlackEnergy, Duqu, Flame, GhostNet, Havex, Industroyer, Pegasus, Shamoon, Stuxnet, Triton
I-12 – Salausratkaisut	BlackEnergy, GhostNet, Havex, Triton
I-13 – Ohjelmistojen suojaaminen verkkohyökkäyksiltä	BlackEnergy, Duqu, GhostNet, Havex
I-16 – Muutoshallintamenettelyt	BlackEnergy, Flame, Havex
I-18 – Etäkäyttö ja etähallinta	BlackEnergy, Pegasus
I-19 – Ohjelmistohaavoittuvuuksien hallinta	BlackEnergy, Flame, Havex, Industroyer, Pegasus, Triton
I-20 – Varmuuskopiointi	BlackEnergy, Shamoon

6 POHDINTA

Tässä luvussa esitetään yhteenvetona tutkimuksen tulokset ja annetaan Kansalliseen turvallisuusauditointikriteeristöön ehdotuksia kehitystoimenpiteistä.

- Miten kohdistetut haittaohjelmahyökkäykset ovat tapahtuneet?

Tiedusteluvaiheessa eniten käytetyiksi tekniikoiksi paljastui avointen lähteiden tiedustelu ja tietojenkalastelu, joilla hankittiin hyökkäyksen kohteesta tietoa varsinaisen hyökkäyksen valmistelua varten.

Resurssien kehittämisessä selvästi yleisin tekniikka oli itse kehittää haittaohjelma. Edistyneimmissä hyökkäyksissä haittaohjelman kehittämiseen on käytetty huomattavan paljon resursseja ja niiden valmistamisessa on hyödynnetty usein nollapäivähaavoittuvuuksia.

Alustavassa sisäänpääsyssä on hyödynnetty ihmisissä olevia heikkouksia, sillä tyypillisimmät hyökkäysreitit ovat olleet erilaiset tietojenkalastelut ja haittaohjelman fyysinen toimittaminen USB-muistitikun avulla.

Haittaohjelmien suorittamiseen on käytetty useita erilaisia tekniikoita. Yleisimmät tekniikat liittyvät kuitenkin uhrin huijaamiseen ja uhrin laitteessa olevien heikkouksien kuten nollapäivähaavoittuvuuksien hyödyntämiseen.

Pysyvyyden varmistamiseksi hyökkääjät ovat hyödyntäneet jo aiemmin varastettuja tunnuksia tai hyökkäyksen aikana luodaan hyökkääjälle pätevät tunnukset nollapäivähaavoittuvuutta hyödyntäen. Lisäksi tyypillisiä keinoja ovat järjestelmä- ja käynnistysprosessien muokkaaminen.

Käyttöoikeuksien laajentamiseksi hyökkääjät ovat tyypillisesti suorittaneet prosessi-injektion tai hankkineet/varastaneet pääkäyttäjätunnukset. Useissa hyökkäyksissä varsinaista käyttöoikeuksien laajentamista ei ole erikseen tehty, koska hyökkääjät ovat saaneet ennen hyökkäystä hankittua pääkäyttäjätunnukset tai niitä ei ole tarvittu ohjelmistohaavoittuvuuden hyödyntämisen takia.

Tyypillisesti hyökkääjät ovat piilossa pysyäkseen poistaneet tapahtumatunnisteita kuten lokeja, maskeeranneet tiedostoja näyttämään luotettavilta ja hyödyntäneet jotain kohdejärjestelmässä olevaa haavoittuvuutta puolustuksen välttelemiseksi.

Valtuutetun sisäänpääsyn varmistamiseksi hyökkääjät ovat pääasiassa hyödyntäneet uhrikäyttäjän syötteiden kaappaamista joko näppäinnauhurilla tai toteuttamalla välimieshyökkäyksen. Useissa hyökkäyksissä tätä taktiikkaa ei ole käytetty, koska varsinainen valtuutettu sisäänpääsy on jo hankittu muihin taktiikoihin kuuluvilla tekniikoilla kuten tiedusteluvaiheessa varastetuilla tunnistetiedoilla.

Tutkintavaiheessa hyökkääjät ovat hankkineet laajasti tietoa saastuneesta järjestelmästä. Erityisesti hyökkääjiä on kiinnostanut saastuneen järjestelmän järjestelmätiedot, tiedostot, prosessit ja oheislaitteet sekä samassa verkossa olevat muut laitteet. Hankittu tieto on myöhemmissä vaiheessa joko varastettu tai tietoa on hyödynnetty hyökkäyksen edelleen leviämiseen tahi muiden hyökkäysten valmisteluun.

Leviämisessä muihin laitteisiin hyökkäysten kohteissa ei ollut havaittavissa selkeästi esiin nousevaa trendiä. Kaikista kohdistetuimmissa hyökkäyksissä haittaohjelma ei ole liikkunut ollenkaan muihin laitteisiin kiinnijäämisen riskin minimoimiseksi. Niissä hyökkäyksissä, joissa haittaohjelma on levinnyt myös muihin laitteisiin, on leviämiseen tyypillisesti hyödynnetty organisaation sisäistä kohdistettua tietojenkalastelua, saastuttamista USB-muistilaitteiden avulla ja erilaisten etäpalveluiden kuten SSH-protokollalla avulla tapahtuvaa tiedonsiirtoa.

Erityisesti tiedustelutiedon hankkimiseksi toteutetut hyökkäykset ja niissä käytetyt haittaohjelmat ovat hyödyntäneet varsin laajasti erilaisia tekniikoita tiedonhankkimisessa. Pääasialliset tekniikat ovat liittyneet järjestelmän käyttäjän toiminnan seuraamiseen esimerkiksi näppäinnauhurein ja ottamalla näyttöleikkeitä. Lisäksi yleensä kohdejärjestelmän tietoja on kaiveltu tiedustelutiedon hankkimiseksi.

Komentoon & kontrolliin liittyvään tiedonsiirtoon hyökkääjät ovat käyttäneet sovelluskerroksen tietoliikenneprotokollia tai erilaisia kiertoreittejä kuten saastuneen kohdeorganisaation sisällä olevia välityspalvelimia. Sovelluskerroksen protokollien käytöllä tietoliikenne on saatu häivytettyä normaalin liikenteen sekaan ja kiertoreittien käytöllä on päästy käsiksi sellaisiin laitteisin, joihin ei olisi ns. normaaleja reittejä pitkin päästy.

Tiedustelutarkoituksessa tehdyt hyökkäykset ja haittaohjelmat ovat yleensä siirtäneet hankitun tiedustelutiedon aiemmin muodostettua komento & kontrolli -kanavaa käyttäen. Tuhoamistarkoitukseen käytetyt haittaohjelmat eivät ole pääasiassa siirtäneet tietoa hyökkääjien komentopalvelimille kiinnijäämisen riskin minimoimiseksi.

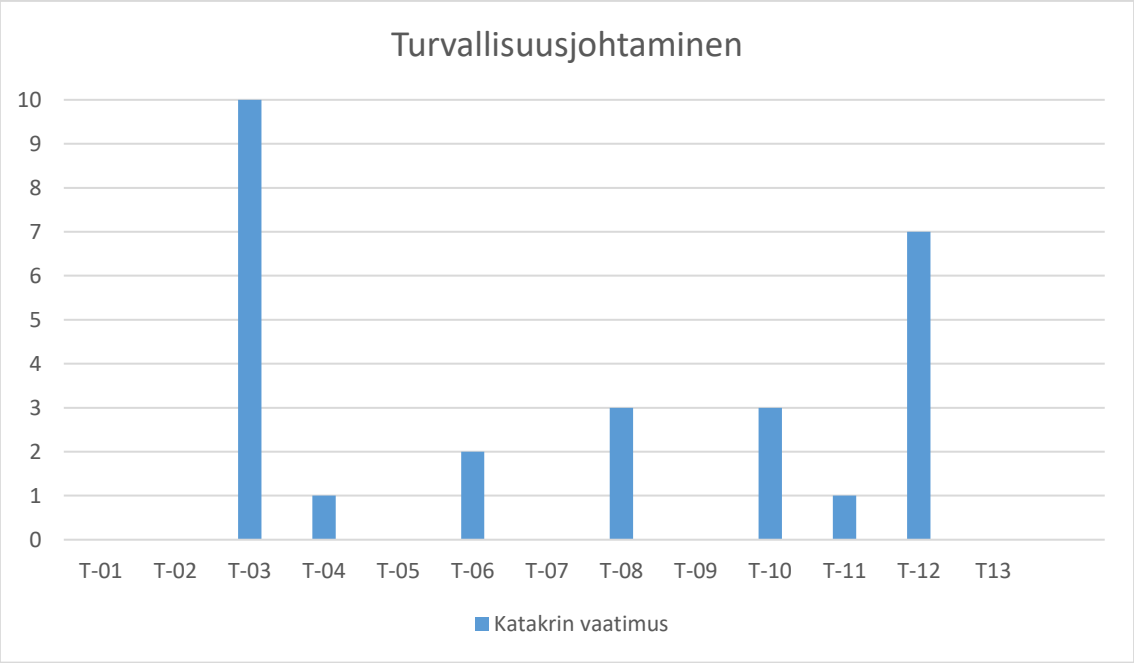
Tuhoamistarkoituksessa tehdyt hyökkäykset ja haittaohjelmat ovat pääasiassa tuhonneet saastuneessa laitteessa olevat tiedostot ja pahimmissa tapauksissa myös koko kovalevyn sisällön. Teollisuusympäristöön kohdistetut hyökkäykset ovat keskittyneet vaikuttamaan teollisuuden laiteohjelmistoihin joko aiheuttamalla niissä tuhoa tai haittaamalla teollisuuden prosessien toteutusta.

- Millaisilla vastatoimilla voidaan estää kohdistettuja haittaohjelmahyökkäyksiä?

Tutkimuksessa hyökkäysten kohteilla oli puutteita kohdistettujen haittaohjelmahyökkäysten estämisessä sekä useiden Katakrin vaatimusten noudattamisessa. Katakrin (Ulkoministeriö, 2020, s. 8–21) turvallisuusjohtamisen osa-alueen vaatimuksista eniten toistuivat: T-03 – Tietoturvallisuusriskien hallinta ja T-12 – Turvallisuuskoulutus. Hyökkäysten kohteiden turvallisuusjohtamisen vaatimusten puutteet ovat kootusti kuviossa 2.

T-03 – Tietoturvallisuusriskien hallinta (Ulkoministeriö, 2020, s. 11) vaatimuksen toteuttamisella pyritään arvioimaan organisaatioon kohdistuvat riskit ja riskiarvion perusteella valita asianmukaiset tietoturvallisuustoimenpiteet. Onnistunut tietoturvallisuusriskien hallinta (Ulkoministeriö, 2020, s. 114–115) on kustannustehokasta ja auttaa organisaatiota vähentämään tietoturvallisuuden riskit hyväksyttävälle tasolle. Hyökkäysten kohteilla on ollut puutteita erityisesti riskienhallinnassa ja riskien saattamisessa hyväksyttävälle tasolle. Avointen lähteiden tiedustelun helppous useiden hyökkäysten osalta myös osoittaa puutteellista ymmärrystä julkisesti saatavilla olevien tietojen aiheuttamasta riskistä. Erityisesti (Ghafir & Prenosil, 2014) teollisuuskohteisiin kohdistuneissa hyökkäyksissä on tyypillisesti saatu kohteesta tietoa joko käyttäen avointen lähteiden tiedustelua. Tästä saatujen tietojen perusteella on hankittu vastaavanlainen laitteisto ohjelmistoineen kuin hyökkäyksen kohteessa. Tällä kokoonpanolla on etukäteen testattu hyökkääjien kehittämän haittaohjelman toimintaa.

T-12 – Turvallisuuskoulutus (Ulkoministeriö, 2020, s. 20) vaatimuksen toteuttamisella pyritään varmistamaan, että organisaation henkilöstöllä on riittävä tuntemus keskeisistä määräyksistä, ohjeista ja tietoon liittyvistä uhkista. Onnistunut turvallisuuskoulutus on säännöllistä ja sisältää henkilön työtehtävien kannalta olennaisia käytännön asioita. Hyökkääjät ovat käyttäneet tietojenkalastelua yleisesti niin hyökkäysten valmistelussa kuin kohteisiin tunkeutumisessa. Tutkimuksen (Rudie ym., 2021) mukaan tietojenkalasteluun liittyvä turvallisuuskoulutus on parhaimpia tapoja vähentää tietojenkalastelukampanjoista aiheutuvia riskejä.

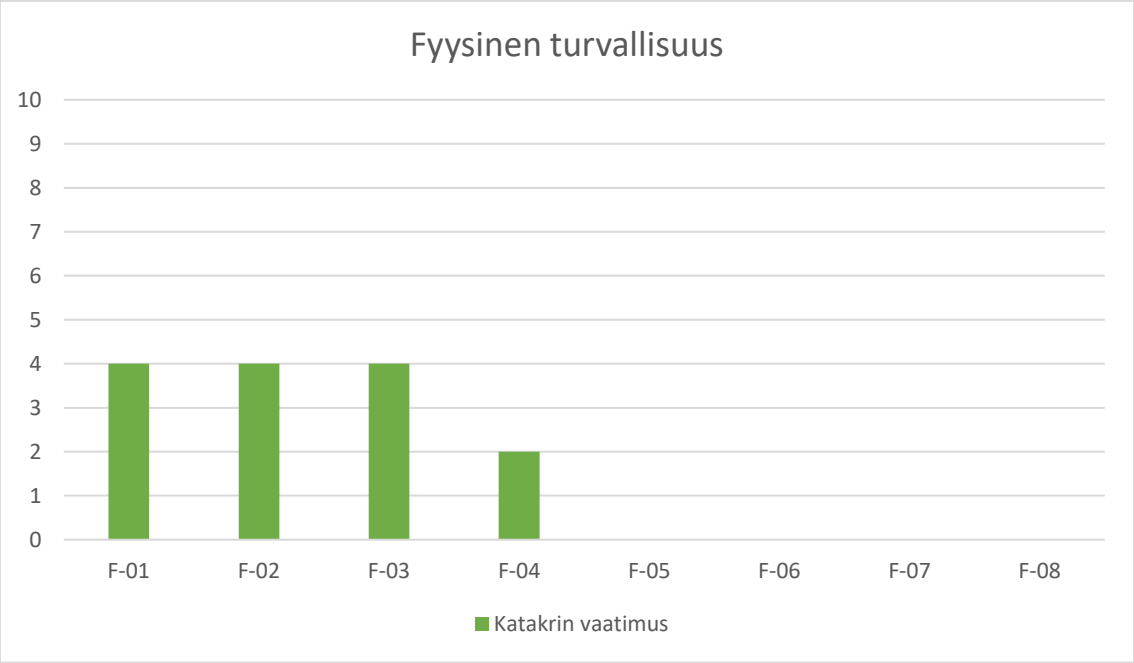


KUVIO 2 Koonti hyökkäysten kohteiden turvallisuusjohtamisen puutteista

Katakrin fyysisen turvallisuuden (Ulkoministeriö, 2020, s. 22–62) vaatimassa tasossa oli vähiten puutteita, koska suurimpaan osaan kohteista ei ollut tunkeuduttu fyysisesti. Puutteita oli eniten: F-02 – Fyysisten turvatoimien riskienarviointi ja F-3 – Fyysisten turvatoimien valinta. Hyökkäysten kohteiden fyysisen turvallisuuden vaatimusten puutteet ovat kootusti kuviossa 3.

F-02 – Fyysisten turvatoimien riskienarviointi (Ulkoministeriö, 2020, s. 25) vaatimuksen toteuttamisella pyritään, että organisaation tiloissa käsiteltävää tietoa on suojattu riittävällä tavalla ja riskien arvioinnin mukaisesti. Puutteet tässä vaatimuksessa ovat samankaltaisia kuin mitä tutkimuksessa havaittiin turvallisuusjohtamisen osalta puutteiksi organisaatioiden riskienhallinnassa.

F-3 – Fyysisten turvatoimien valinta (Ulkoministeriö, 2020, s. 26–28) vaatimuksen toteuttamisella pyritään valitsemaan riskienarvion perusteella oikeiksi mitoitetut turvatoimet. Onnistuneesti valitut turvatoimet ovat kustannustehokkaita ja laskevat riskit hyväksyttävälle tasolle. Erityisesti hyökkäysten kohteilla on ollut puutteita luvattomien tietoteknisten välineiden kuten USB-muistitikkujen valvonnan osalta. Koulutettua vartiointihenkilöstöä olisi voitu hyödyntää työntekijöille tehtävissä sisääntulotarkastuksissa. Sisääntulotarkastusten ja kameravalvonnan avulla olisi voitu mahdollisesti havaita luvattomien USB-välineiden tuominen kohdeorganisaation tiloihin sekä niiden luvaton käyttäminen.



KUVIO 3 Koonti hyökkäysten kohteiden fyysisen turvallisuuden puutteista

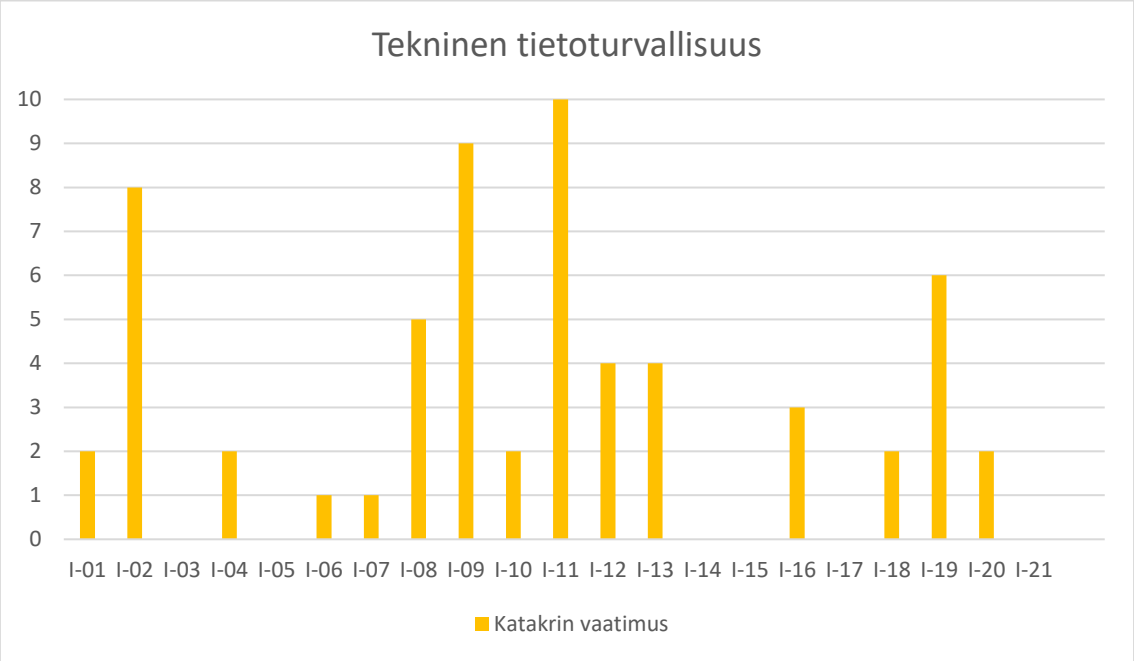
Eniten puutteita hyökkäysten kohteilla oli Katakrin teknisen tietoturvallisuuden (Ulkoministeriö, 2020, s. 63–106) vaatimusten toteuttamisen osalta. Puutteita oli erityisesti: I-02 – Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä, I-09 – Haittaohjelmasuojaus sekä I-11 – Poikkeamien havainnointikyky ja toipuminen. Hyökkäysten kohteiden teknisen tietoturvallisuuden vaatimusten puutteet ovat kootusti kuviossa 4.

I-02 – Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä (Ulkoministeriö, 2020, s. 69–70) vaatimuksella on tavoitteena estää luvaton tietoliikenne organisaation sisällä ja organisaatiosta sisään sekä ulos. Hyökkäyksissä haittaohjelmat ovat tyypillisesti vastaanottaneet komentoja ja lähettäneet tiedustelutietoa eteenpäin hyökkääjien komentokoneille, jotka ovat sijainneet organisaatioiden ulkoisessa verkossa. Tietoliikenne normaalista poikkeaviin osoitteisiin tulisi lähtökohtaisesti estää palomuurilta erityisesti turvallisuuskriittisten toimintojen osalta.

I-09 – Haittaohjelmasuojaus (Ulkoministeriö, 2020, s. 83–84) vaatimuksen tarkoituksena on torjua haittaohjelmista aiheutuvia uhkia. Tutkituissa hyökkäyksissä on usein hyödynnetty nollapäivähaavoittuvuuksia, joiden havaitsemisessa hyökkäysten kohteiden haittaohjelmasuojauksella on ollut vaikeuksia. Säännöllisten päivitys torjuntaohjelmistojen osalta on olennaista parhaan mahdollisen suojan kannalta. Perinteisillä jälkiin (eng. signature) perustuva haittaohjelmatunnistus (Mumtaz ym., 2021) on riittämätön tunnistamaan nollapäivähaavoittuvuuksia ja haittaohjelmia, joiden lähdekoodia on muokattu (eng. malware obfuscation). Lisäksi jälkiin perustuva (Bencsáth ym., 2012_b) haittaohjelmatunnistus on tehokas havaitsemaan tunnettuja haittaohjelmia. Anomalioihin perustuva haittaohjelmatunnistus kykenisi paremmin havaitsemaan tällaiset kohdistetuissa

haittaohjelmahyökkäyksissä käytetyt nollapäivähaavoittuvuuksia hyödyntävät haittaohjelmat.

I-11 – Poikkeamien havainnointikyky ja toipuminen (Ulkoministeriö, 2020, s. 87–88) vaatimuksella on tarkoituksena havaita mahdolliset poikkeamat mahdollisimman aikaisessa vaiheessa ja toipua niiden aiheuttamista haitoista. Nollapäivähaavoittuvuuksien hyödyntäminen hyökkäyksissä tekee niiden havaitsemisesta ja torjumisesta vaikeaa, mutta panostamalla anomalioiden havainnointikykyyn voidaan vähintäänkin parantaa suojaa nollapäivähaavoittuvuuksia vastaan. Lisäksi haittaohjelmien leviäminen verkkojakojen avulla ja organisaation sisäverkossa osoittaa puutteellista haitallisen tietoliikenteen havaitsemista.



KUVIO 4 Koonti hyökkäysten kohteiden teknisen tietoturvallisuuden puutteista

- Onko kansallisen turvallisuusauditointikriteeristön vaatimuksissa puutteita kohdistettujen haittaohjelmahyökkäysten ehkäisemiseksi?

Tutkimustuloksien perusteella voidaan todeta, että Katakrin kriteeristöt ottavat varsin kattavasti huomioon erilaiset kohdistetuissa haittaohjelmahyökkäyksissä käytettävät hyökkäysreitit. Katakri soveltunee paremmin arvioitaessa vakoiluun ja tiedusteluun liittyvää tiedonhankintaa kuin teollisuusjärjestelmiin kohdistettuihin hyökkäyksiin. Tutkimuksen perusteella voidaan kuitenkin havaita, että Katakrin vaatimuksien toteuttamisella on mahdollista estää tai vähintäänkin merkittävästi vähentää hyökkääjän mahdollisuuksia onnistua hyökkäyksessä myös teollisuusympäristöihin. Tämä johtunee siitä, että prosessiteollisuuden ympäristön suojaamisen perusperiaatteet ovat samankaltaisia kuin turvallisuusluokitellun tiedon turvaamisessa. Usein toistuvat hyökkäystekniikat ovat pitkälti samanlaisia niin vakoilussa kuin sabotaasissa, niiden lopulliset tavoitteet vain ovat erilaiset.

Katakrin kriteeristöissä on puutteita älypuhelinten ja IOT-laitteiden huomioimisen osalta. Lisäksi kriteeristöissä puhutaan poikkeamien havainnoinnista ja niistä toipumisesta pintapuoleisesti.

Älypuhelimet otetaan kriteeristöissä huomioon fyysisen turvallisuuden ja teknisen tietoturvallisuuden osalta. Fyysisen turvallisuuden (Ulkoministeriö, 2020, s. 22–62) vaatimuksissa puhelimiin otetaan kantaa lähinnä vain siitä näkökulmasta, että puhelimia ei saa viedä ollenkaan tietyille turvallisuusalueille. Teknisen tietoturvallisuuden (Ulkoministeriö, 2020, s. 63–106) osalta näkökulma on laajempi, mutta kantaa otetaan vain järjestelmäkovennukseen ja langattomaan tiedonsiirtoon. Järjestelmäkovennuksissa mainitaan kuitenkin, että puhelimet tulisi koventaa samoja periaatteita noudattaen kuin tietokoneet, mikäli niitä käytetään turvallisuusluokitellun tiedon käsittelyyn. Langattoman tiedonsiirron vaatimuksien osalta mainitaan vain, että puhelinta ei saa liittää tietokoneeseen akun lataamista varten, mikäli puhelin on tarkoitettu matalamman turvallisuustason laitteeksi. Puhelimiin liittyvät muut vaatimukset on ripoteltu sinne tänne kriteeristöihin ja niiden noudattaminen on juuri tämän sekavuuden vuoksi haastavaa.

IOT-laitteita ei mainita Katakrin kriteeristöissä suorasanaisesti kertaakaan. Kiertoteitse laitteet mainitaan ainoastaan fyysisen turvallisuuden vaatimuksissa laiteasennusten riskienarvioinnissa (Ulkoministeriö, 2020, s. 26–28) ja muutoshallintamenettelyissä (Ulkoministeriö, 2020, s. 96–97) todetaan tietojenkäsittely-ympäristön laitekirjanpidon yhteydessä. IOT-laitteiden määrän lisääntymisen vuoksi tulisi niihin ottaa kriteeristöissä suorasanaisemmin kantaa.

Katakrin vaatimukset eivät ota konkreettisesti kantaa SOC-toiminnon (eng. security operations center) muodostamisesta organisaatioon. Toiminnon tarkoituksena olisi vastata poikkeamiin ja hyökkäyksiin mahdollisimman aikaisessa vaiheessa. Vaikka vaatimuksessa I-11 – Poikkeamien havainnointi ja toipuminen (Ulkoministeriö, 2020, s. 87–88) otetaan kantaa poikkeamien havainnointiin, ei siinä mainita konkreettista käytännön ratkaisua poikkeamien käsittelyyn. Tutkimusten mukaan (Vielberth ym., 2020) tietoturvavalvomot (eng. security operations center) ovat kuitenkin nykyisin välttämättömiä kyberhyökkäysten torjumisessa. Tällaisesta toiminnosta tulisi olla vaatimus tai vähintäänkin maininta kriteeristöissä.

7 YHTEENVETO

Tässä kohdistettujen haittaohjelmahyökkäysten vastatoimia käsittelevässä tutkielmassa selvitettiin monitapaustutkimuksen menetelmin kohdistetuissa haittaohjelmahyökkäyksissä yleisesti käytettävät taktiikat ja tekniikat. Lähdemateriaaliksi valittiin niin tieteellisiä artikkeleita kuin kyberturvallisuusyritysten hyökkäyksistä tekemiä raportteja.

Johdantoluvussa kerrottiin tutkimuksen tausta, tavoitteet, tutkimuskysymykset ja keskeiset käsitteet sekä rakenne. Toisessa luvussa taustoitettiin varsinaista tutkimusta ja annettiin lukijalle perustiedot tutkimusaiheesta. Kolmannessa luvussa kerrottiin tutkimuksessa käytetyistä tutkimusmenetelmistä, aineistonkeruusta ja aineistonanalyysista. Neljännessä luvussa vastattiin tutkimuskysymykseen: Miten kohdistetut haittaohjelmahyökkäykset ovat tapahtuneet? Luvussa selvitettiin kymmenessä kohdistetussa haittaohjelmahyökkäyksessä käytetyt hyökkäystaktiikat ja tekniikat. Ensimmäiseen tutkimuskysymykseen voidaan vastata tiivistetysti:

- Hyökkäysten valmistelussa on hyödynnetty avointen lähteiden tiedustelua ja tietojenkalastelua.
- Hyökkäyksen kohteeseen on tunkeuduttu usein huijaussähköpostien mukana tulevilla haitallisilla linkeillä ja liitetiedostoilla tai fyysisesti USB-muistivälinettä käyttäen.
- Haittaohjelmissa on käytetty nollapäivähaavoittuvuuksia kohteen täydellisen hallinnan saavuttamiseksi ja kohteessa piilossa pysymiseksi.
- Hyökkäysten kohteista on hankittu laajasti tiedustelutietoa, jotka on lähetetty eteenpäin hyökkääjien komentokoneille normaalin tietoliikenteen seassa.
- Hyökkäysten kohteissa tapahtunut sabotaasi on tehty joko huomaamattomasti tai totaalisena laitteiden tuhoamisena.

Viidennessä luvussa vastattiin tutkimuskysymykseen: Millaisilla vastatoimilla voidaan estää kohdistettuja haittaohjelmahyökkäyksiä? Luvussa verrattiin neljännessä luvussa tutkittujen hyökkäysten toteutusta Kansalliseen

turvallisuusauditointikriteeristöön hyökkäysten vastatoimien ja kriteeristön mahdollisten puutteiden löytämiseksi. Toiseen tutkimuskysymykseen voidaan vastata lyhyesti:

- Huolellisella riskienhallinnalla valitaan organisaatiolle sopivat tietoturvallisuustoimenpiteet.
- Turvallisuuskoulutuksella voidaan merkittävästi vähentää hyökkääjien mahdollisuuksia onnistua hyökkäyksen valmistelussa ja hyökkäyksen kohteeseen tunkeutumisessa.
- Vartiointihenkilöstön tarkempi toiminta luvattomien tietoteknisten laitteiden kuten USB-muistivälineiden valvonnan osalta mahdollisesti estää haittaohjelman toimittamisen fyysisesti kohteeseen.
- Haittaohjelmasuojauksen säännöllinen päivitys on olennainen mahdollisimman kattavan ja ajantasaisen suojan ylläpitämiseksi.
- Panostamalla poikkeamien havainnointikykyyn voidaan parantaa mahdollisuuksia torjua nollapäivähaavoittuvuuksia käyttäviä hyökkäyksiä.
- SOC-toiminnolla voidaan vastata havaittuihin poikkeamiin nopeasti ja mahdollisesti estää hyökkäyksen leviäminen organisaatiossa.

Kuudennessa luvussa vastattiin tutkimuskysymykseen: Onko kansallisen turvallisuusauditointikriteeristön vaatimuksissa puutteita kohdistettujen haittaohjelmahyökkäysten ehkäisemiseksi? Kolmanteen tutkimuskysymykseen voidaan vastata seuraavasti:

- Kriteeristöt ovat hyvin yleisluonteisia, eivätkä ota riittävästi kantaa vaatimusten konkreettiseen toteuttamiseen.
- Kriteeristöt ottavat pintapuolisesti huomioon älypuhelimet ja IOT-laitteet.
- SOC-toiminnon puuttuminen kriteeristöistä.

Jatkotutkimusaiheeksi nousi tämän tutkielman myötä älypuhelinten ja IOT-laitteiden turvallisuus kohdistettujen haittaohjelmahyökkäysten osalta. Miten IOT-laitteita voidaan käyttää kohdistetuissa haittaohjelmahyökkäyksissä? Miten älypuhelinten tietoturvallisuutta voidaan edistää kohdistettuja haittaohjelmahyökkäyksiä vastaan? Lisäksi mielenkiintoinen ja konkreettinen tutkimusaihe olisi, onko SOC-toiminnolla vaikutusta organisaation puolustuskykyyn kohdistettuja haittaohjelmahyökkäyksiä vastaan?

LÄHTEET

Agrawal, M., Varshney, G., Saumya, K. P. S., & Verma, M. (2022). Pegasus: Zero-Click spyware attack–its countermeasures and challenges. ResearchGate. https://doi.org/10.13140/RG.2.2.21979.90405

Al-Mulhim, R. A., Al-Zamil, L. A., & Al-Dossary, F. M. (2020). Cyber-attacks on Saudi Arabia environment. International Journal of Computer Networks and Communications Security, 8(3), 26-31.

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

Bazaliy, M., Flossman, M., Blaich, A., Hardy, S., Edwards, K., Murray, M. (2016). Technical Analysis of Pegasus Spyware: An Investigation into Highly Sophisticated Espionage Software. Lookout.

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

Bencsáth, B., Pék, G., Buttyán, L., & Felegyhazi, M. (2012_b). The Cousins of Stuxnet: Duqu, flame, and gauss. Future Internet, 4(4), 971-1003.

Bermejo Higuera, J., Abad Aramburu, C., Bermejo Higuera, J. R., Sicilia Urban, M. A., & Sicilia Montalvo, J. A. (2020). Systematic approach to malware analysis (SAMA). Applied Sciences, 10(4), 1360.

Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? Shamoon and the Evolution of Cyber Conflict.

Chawla, A. Pegasus Spyware – 'A Privacy Killer'. (2021). SSRN. http://dx.doi.org/10.2139/ssrn.3890657

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. Computer, 44(4), 91-93.

Cherepanov, A., & Lipovsky, R. (Lokakuu 2016). Blackenergy–what we really know about the notorious cyber attacks. Virus Bull.

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

Clayton, M. (14.9.2012). Stealing US business secrets: Experts ID two huge cyber 'gangs' in China. The Christian Science Monitor. https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15(4), 277-305.

Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. M. F. (2009). Tracking ghostnet: Investigating a cyber espionage network.

Di Pinto, A., Dragoni, Y., & Carcano, A. (Elokuu 2018). TRITON: The first ICS cyber attack on safety instrument systems. In Proc. Black Hat USA (Vol. 2018, s. 1-26).

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, symantec corp., security response, 5(6), 29.

Fillinger, M., & Stevens, M. (2015). Reverse-engineering of the cryptanalytic attack used in the flame super-malware. In International Conference on the Theory and Application of Cryptology and Information Security (s. 586-611). Springer, Berlin, Heidelberg.

Finkle, J. (8.1.2016). U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage. Reuters. Luettu 2.8.2022 osoitteesta https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

Firoozjaei, M. D., Mahmoudyar, N., Baseri, Y., & Ghorbani, A. A. (2022). An evaluation framework for industrial control system cyber incidents. International Journal of Critical Infrastructure Protection, 36, 100487.

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: an overview. International Journal of Advancements in Computer Networks and Its Security, 4(4), 50-54.

Gjesvik, L., & Szulecki, K. (2022). Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. European Security, 1-21.

Grönfors, M. & Vilkka, H. (toim.). (2011). Laadullisen tutkimuksen kenttätyömenetelmät. SoFia-Sosiologi-Filosofiapu Vilkka.

Henneberg, Alex (1.3.2020). ADDRR: A counter kill chain cyber security model. In the Cyber Security: A Peer-Reviewed Journal, Volume 3, Issue 3.

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. Leading Issues in Information Warfare & Security Research, 1(1), 80.

Hwaitat, A., Manaseer, S., Al-Sayyed, R., Almaiah, A., Almomani, O. (2020). An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response. Journal of Theoretical and Applied Information Technology, 15, 98.

IGI Global. (ei pvm.). What is Multi-Case Study. Luettu 31.10.2022 osoitteesta https://www.igi-global.com/dictionary/multi-case-study/61660

Jyväskylän yliopisto. (28.10.2021). Laadullinen tutkimus. Luettu 9.8.2022 osoitteesta

https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Jääskeläinen, V. (2018). Liikesalaisuuksiin kohdistuvien insider-riskien hallinta. Suojelupoliisin julkaisusarja 1/2018.

Kaspersky. (2022). BlackEnergy APT Attacks in Ukraine. Luettu 1.8.2022 osoitteesta https://www.kaspersky.com/resource-center/threats/blackenergy

Kaspersky. (2014). Energetic bear— crouching yeti. Kaspersky Lab Global Researchand Analysis Team. Luettu 15.9.2022 osoitteesta https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. Journal of computational science, 27, 394-409.

Lehto, M. (6.4.2021). Digitaalisen kybermaailman ilmiöitä ja määrittelyjä. Versio 15.0. Jyväskylän yliopisto. Luettu 14.8.2022 osoitteesta https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kybma/kybermaailma_v15-0.pdf

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

Lockheed Martin. (2015). Gaining the Advantage Applying Cyber Kill Chain® Methodology to Network Defense. Luettu 10.7.2022 osoitteesta https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Mandiant. (2022a). Advanced Persistent Threats (APTs). Luettu 19.7.2022 osoitteesta https://www.mandiant.com/resources/apt-groups

Mandiant. (2022b). Targeted Attack Lifecycle. Luettu 14.8.2022 osoitteesta https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries. The Citizen Lab.

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

MITRE. (2022a). ATT&CK. Luettu 11.8.2022 osoitteesta https://attack.mitre.org/

MITRE. (2022b). Collection. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0009/

MITRE. (2022c). Enterprise Matrix. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/matrices/enterprise/

MITRE. (2022d). Enterprise Mitigations. Luettu 14.8.2022 osoitteesta
https://attack.mitre.org/mitigations/enterprise/

MITRE. (2022e). Frequently Asked Questions. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/resources/faq/

MITRE. (2021a). Privilege Escalation. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0002/

MITRE. (2021b). Shamoon. Luettu 28.9.2022 osoitteesta
https://attack.mitre.org/software/S0140/

MITRE. (2020a). Reconnaissance. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0043/

MITRE. (2020b). Resource Development. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0042/

MITRE. (2019a). Command and Control. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0009/

MITRE. (2019b). Credential Access. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0006/

MITRE. (2019c). Defense Evasion. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0005/

MITRE. (2019d). Discovery. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0007/

MITRE. (2019e). Execution. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0002/

MITRE. (2019f). Exfiltration. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0010/

MITRE. (2019g). Impact. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0040/

MITRE. (2019h). Initial Access. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0001/

MITRE. (2019i). Lateral Movement. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0008/

MITRE. (2019j). Persistence. Luettu 11.8.2022 osoitteesta
https://attack.mitre.org/tactics/TA0003/

Mumtaz, Z., Afzal, M., Iqbal, W., Aman, W., & Iltaf, N. (2021). Enhanced Metamorphic Techniques-A Case Study Against Havex Malware. IEEE Access, 9, 112069-112080.

Poliisi. (2022). Poliisin ohjeet Vastaamo-tietomurron uhreille. Luettu 14.8.2022 osoitteesta https://poliisi.fi/ohjeet-tietomurron-uhreille

Rudie, J. D., Katz, Z., Kuhbander, S., & Bhunia, S. (2021). Technical analysis of the nso group's pegasus spyware. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (s. 747-752). IEEE.

Setola, R., Faramondi, L., Salzano, E., & Cozzani, V. (2019). An overview of cyber attack to industrial control system. Chemical Engineering Transactions, 77, 907-912.

Suojelupoliisi. (23.3.2021). Vuosikirja 2020. Luettu 14.8.2022 osoitteesta https://supo.fi/documents/38197657/40760236/Supo+Vuosikirja+2020.pdf/70e75573-0726-f76c-846c-be661887c9db/Supo+Vuosikirja+2020.pdf?t=1646741936184

Suojelupoliisi. (29.3.2022). Vuosikirja 2021. Luettu 14.8.2022 osoitteesta https://vuosikirja.supo.fi/documents/62399122/111357887/Supo+Vuosikirja+2021.pdf/c692364f-9d7f-5e8b-e720-8763784cf27e/Supo+Vuosikirja+2021.pdf?t=1648455326088

Symantec. (23.11.2011). W32.Duqu: The precursor to the next Stuxnet. Symantec. Luettu 6.10.2022 osoitteesta https://docs.broadcom.com/doc/w32-duqu-11-en

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto. Luettu 8.7.2022 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Ulkoministeriö. (2022). Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Luettu 8.7.2022 osoitteesta https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Ulkoministeriö. (18.12.2020). Katakri 2020. Luettu 8.7.2022 osoitteesta https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. IEEE Access, 8, 227756–227779.

Wangen, G. (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. Information, 6(2), 183-211.