jamk

Kiristyshaittaohjelma kasvavana uhkana - kasvun syyt sekä reagointi SOC-tiimissä

Arttu Aarnio

Opinnäytetyö, AMK
Huhtikuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Aarnio, Arttu

Kiristyshaittaohjelma kasvavana uhkana - kasvun syyt sekä reagointi SOC-tiimissä

Jyväskylä: Jyväskylän ammattikorkeakoulu. Huhtikuu 2022, 85 sivua

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Kiristyshaittaohjelmien aiheuttamien hyökkäysten uutisointi mediassa on arkipäivää ja ilmiö vaikuttaa tällä hetkellä kyberturvallisuuden tilanteeseen kansainvälisesti. Monet asiantuntijalausunnot sekä tietoturvallisuudessa vaikuttavat tekijät ovat tuoneet esille kiristyshaittaohjelmien muodostaman todellisen uhan jopa yhteiskunnan toimivuuteen kannalta. SOC-toiminnalla on yhä jokapäiväisempi sekä entistä vastuullisempi rooli kasvavassa kiristyshaittaohjelmauhan hallinnassa.

Opinnäytetyön toimeksiantajana toimi Telia Cygate Oy. Opinnäytetyön toimeksiantona oli selvittää kiristyshaittaohjelmien aiheuttamien hyökkäyksien ajankohtaista kehityssuuntaa maailmalla sekä miten SOC-toimintaa voisi kehittää vastaavien kyberhyökkäyksien varalle ja onko SOC-toiminnalla merkitystä kiristyshaittaohjelmahyökkäysten estämiseen ja reagointiin. Työn tavoitteena oli muodostaa kehitysnäkymä kiristyshaittaohjelmien havaintojen määrästä sekä niiden muutoksesta viimeisen 5 vuoden aikana. Lisäksi SOC-toiminnan osalta oli tavoitteena koostaa havaittujen yhteisten piirteiden avulla selkeitä käytänteitä sekä suosituksia kiristyshaittaohjelmien aiheuttamien kriisitilanteiden välttämiseksi.

Opinnäytetyössä hyödynnettiin soveltavaa monimenetelmällistä tutkimusta, jossa on myös piirteitä tutkivasta kehittämistoiminnasta. Työn alussa kattavalla tietoperustalla tarkasteltiin yleisesti ajankohtaista kyberturvallisuustilannetta, kiristyshaittaohjelmaa sekä SOC-toimintaa. Tietoperustan jälkeen selvitettiin viimeaikaisen esimerkkitapauksen avulla kiristyshaittaohjelman vaikutusta organisaation ja kansallisen tason näkökulmasta. Myös kiristyshaittaohjelmien tulevaisuuden kehityskulkua arvioitiin julkisten lähteiden avulla. Arvioinnin jälkeen tarkasteltiin kerätyn tutkimusmateriaalin avulla toimeksiannossa esille tuotuja selvitettäviä kehityskulkuja sekä muutoksia.

Lopputuloksena opinnäytetyössä saatiin kuvattua tarkasti useisiin eri lähteisiin sekä tutkimusmateriaaleihin vedoten kiristyshaittaohjelmien muutokset työn tavoitteiden mukaisesti. Kiristyshaittaohjelmien hyökkäyksissä havaittujen yhteisten piirteiden selvitys saatiin toteutettua hyökkääjän sekä puolustajan näkökulmat huomioiden. Lisäksi SOC-toiminnan kehityskohteita ja reagoinnin parantamista kiristyshaittaohjelmia vastaan tuotiin esille eri toimijoiden yksityiskohtainen tilanne huomioiden. Tuloksista pystyttiin päättelemään kiristyshaittaohjelmien kasvumuutos sekä ajankohtaiset piirteet hyökkäyksissä. Myös SOC-toiminnassa tarvitaan jatkuvaa kehittämistä kyberturvallisuustilanteen nopeissa muutoksissa tehokkuuden ylläpitämiseksi.

Avainsanat (asiasanat)

Kiristyshaittaohjelma, SOC, kyberturvallisuustilanne, kyberhyökkäys, kehittäminen, reagointi, kasvu

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Aarnio, Arttu

Ransomware as a growing threat - the causes of growth and the response in SOC

Jyväskylä: JAMK University of Applied Sciences, April 2022, 85 pages

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Media coverage of attacks caused by ransomware is commonplace and the phenomenon is currently affecting the state of cyber security internationally. Expert opinions and factors affecting information security have highlighted the real threat posed by ransomware even to the functioning of society. Security Operation Center actors are playing increasingly more responsible and everyday role in the growing management of ransomware attacks.

The thesis was commissioned by Telia Cygate Oy. The assignment of the thesis was to find out the current trend of ransomware attacks in the world and how Security Operation Center could be developed for similar cyber attacks and whether SOC play a role in preventing and responding to ransomware attacks. The aim of the work was to make a perspective on the number of findings of ransomwares and their changes during the last 5 years. Regarding to SOC actions, the aim was also to compile clear practices and recommendations with using the common features identified to avoid crisis situations caused by ransomware attacks.

The thesis was carried out as an applied multi-method research, which also has features of exploratory development activities. At the beginning of the work, a comprehensive knowledge base was used to examine the current cybersecurity situation, the ransomware attacks, and the SOC-actions. Following the knowledge base, a recent case study was used to investigate the impact of a ransomwares from an organizational and national perspective. The future development of ransomware was also assessed using public sources. After the assessed, the developments and changes presented in the assignment were examined with the help of the collected research material.

As a result, the changes in the ransomware attacks were described with several different sources and research materials. The analysis of the common features detected in the ransomware attacks was carried out considering the views of the attacker's side and the defender's side. In addition, the detailed situation of SOC-actors was highlighted. From the results, it was possible to deduce the change in the growth of ransomware attacks and the current features of the attacks. SOC also need continuous development in the face of rapid changes in the cyber security situation to maintain level.

Keywords/tags (subjects)

Ransomware, SOC, cyber security situation, cyber attack, development, response, growth

Miscellaneous (Confidential information)

Sisältö

1 Johdanto 7
1.1 Toimeksiantaja sekä tausta 8
1.2 Tehtävä ja tavoitteet 8
2 Tutkimusideologia 8
2.1 Tutkimuskysymys 9
2.2 Tutkimusmenetelmä 10
3 Teoreettis-käsitteelliset lähtökohdat 10
3.1 Kyberturvallisuuden tilanne 10
3.1.1 Kyberturvallisuuden nykytila maailmalla 11
3.1.2 Kyberturvallisuuden nykytila Suomessa 13
3.2 Kiristyshaittaohjelma 14
3.2.1 Kiristyshaittaohjelman historia 16
3.2.2 Kiristyshaittaohjelman tekninen toimintatapa 18
3.2.3 Kristyshaittaohjelman vaikutus 24
3.3 SOC – Security Operation Center 27
3.3.1 SOC:in toimintatavat 28
3.3.2 SOC:in työkalut 31
3.3.3 SOC-toimijat 34
3.3.4 SOC-toiminnan haasteet 36
4 Kiristyshaittaohjelma – isku yhteiskuntaa vastaan 37
4.1 Kiristyshaittaohjelmahyökkäykset viime aikoina – Case Colonial Pipeline 38
4.1.1 Syitä hyökkäyksen onnistumiseen 40
4.2 Aktiiviset hyökkäykset ja nykytila 40
4.3 Kiristyshaittaohjelma hyökkäykset tulevaisuudessa 44
5 Kiristyshaittaohjelmien havainnot ja torjuntamahdollisuudet SOC-toiminnassa 45
5.1 Telia Cygate SOC 46
5.2 Kyberturvallisuuskeskus 52
5.3 Poliisin näkökulma ja rikostilastot 55
5.4 SOC-toiminnan rooli 61
5.5 Kysely SOC-toimijoille 63
6 Tulokset 64
6.1 Kiristyshaittaohjelmien trendi 65
6.2 Hyökkäysten kohteet ja yhteiset piirteet 67

6.3 SOC-toimijat 68
6.3.1 SOC-toimijoiden yhteistyö 68
6.3.2 Reagoinnin parantaminen 69
6.3.3 Kehittäminen tulevaisuudessa 70
7 Pohdinta 71
Lähteet 74
Liitteet 83
Liite 1. Kysely SOC-toimijoille 83

Kuviot

Kuvio 1. FireEye yrityksen kyberuhkakartta 11
Kuvio 2. Kiristyshaittaohjelmien luokittelu 15
Kuvio 3. Kiristyshaittaohjelmien aikajana 18
Kuvio 4. Kiristyshaittaohjelman tyypillinen elinkaari 20
Kuvio 5. CryptoLocker-kiristyshaittaohjelman esittämä ilmoitus 23
Kuvio 6. Kiristyshaittaohjelmahyökkäysten uhrien toimialat Q4-kvartaalilla vuonna 2020 25
Kuvio 7. DART-tiimin kiristyshaittaohjelmahavainnot toimialoittain 26
Kuvio 8. Tietoturvapoikkeaman eskalointi 29
Kuvio 9. Esimerkki keskikokoisesta SOC-toiminnasta 30
Kuvio 10. SIEM-järjestelmän merkitys tiedon yhdistämisessä 32
Kuvio 11. Security Operations Center-toiminnan kehitys 35
Kuvio 12. Security Operations Centerin haasteet 37
Kuvio 13. Colonial Pipeline hyökkäyksen aikajana 39
Kuvio 14. Aktiivisia viimeaikaisia kiristyshaittaohjelmahyökkäyksiä 41
Kuvio 15. Aktiivisia kiristyshaittaohjelma toimijoita 42
Kuvio 16. Kiristyshaittaohjelmien kohtaamisprosentti yritysasiakkailla 43
Kuvio 17. ENISA:n esittämät keskimääräiset lunnaat perustuen Coveware:n tietoihin 43
Kuvio 18. Telia Cygaten SOC-herätteiden määrä 2 vuoden ajalla sanasta "Ransomware" 47
Kuvio 19. Telia Cygate SOC-herätteiden määrä 2 vuoden ajalla sanasta "Wannacry" 47
Kuvio 20. Telia Cygaten SOC-herätteiden määrä 1 vuoden ajalla sanasta "Ransomware" 48
Kuvio 21. Telia Cygate SOC-herätteiden määrä 1 vuoden ajalla sanasta "Wannacry" 48
Kuvio 22. Tietoturvapoikkeamatikettien lukumäärä graafisessa muodossa 51
Kuvio 23. Autoreporter raportoitujen kiristyshaittaohjelmien kehitys 53
Kuvio 24. Kyberturvallisuuskeskukselle ilmoitettujen kiristyshaittaohjelmatapauksien määrä 55

Kuvio 25. Rikosluokitukset vuositasolla ICCS-muuttujina 59
Kuvio 26. Rikosluokitukset neljännesvuositasoin ICCS-muuttujina 60

Taulukot

Taulukko 1. Avattujen tietoturvapoikkeamatikettin lukumäärä vuositasolla 50
Taulukko 2. Autoreporter ilmoitusten lukumäärä kiristyshaittaohjelmista 28.10.2021 53
Taulukko 3. Kyberturvallisuuskeskukselle ilmoitettujen kiristyshaittaohjelmatapauksien määrä 1.1.2016-30.11.2021 54
Taulukko 4. Poliisille ilmoitetut rikokset koko maassa 57

Lyhenteet

AES Advanced Encryption Standard

APT Advanced Persistent Threat

CERT Computer Emergency Response Team

CISA Cybersecurity and Infrastructure Security Agency

DART Detection and Response Team

DES Data Encryption Standard

DFIR Digital Forensics & Incident Response

ECDH Elliptic-curve Diffie–Hellman

ENISA European Union Agency for Cybersecurity

EPP Endpoint Protection Platform

ETL ENISA Threat Landscape

FMCSA Federal Motor Carrier Safety Administration

GDPR General Data Protection Regulation

ICT Information and Communication Technology

ICCS International Classification of Crimes

IDS	Intrusion Detection System
IoC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
MFA	Multi-Factor Authentication
MISP	Malware Information Sharing Platform
MSSP	Managed Security Service Provider
NTA	Network Traffic Analysis
RaaS	Ramsomware as a Service
RDP	Remote Desktop Protocol
RSA	Rivest–Shamir–Adleman
SIEM	Security Information & Event Management
SIRT	Security Incident Response Team
SLA	Service Level Agreement

SMB	Server Message Block
SOC	Security Operation Center
TDK	Trojan Development Kit
VPN	Virtual Private Network
WAN	Wide Area Network

1 Johdanto

Kiristyshaittaohjelmien aiheuttamia kyberhyökkäyksiä maailmalla on uutisoitu mediassa viime vuosien aikana paljon, ja niiden aiheuttamat seuraukset ovat entistä suurempia sekä vaikuttavampia jokapäiväiseen arkeen. Hyökkäysten tavoitteet ja syyt voivat olla monitahoisia, mutta hyökkäyksiä toteuttavat organisaatiot ovat kasvaneet sekä muuttuneet lisääntyvän digitalisaation yhteiskunnassa. Asiaan perehtymättömän henkilön tai hyökkäyksen uhriksi joutuneen onkin vaikea ymmärtää, missä hyökkäyksen juuret sijaitsevat. (History Of Ransomware 2021.)

Tarkoituksena opinnäytetyössä oli tutkia maailmalla olleita viimeisimpiä kiristyshaittaohjelmien hyökkäyksiä. Työssä pyrittiin selvittämään syyt toteutettuihin kiristyshaittaohjelmahyökkäyksiin, kuka ne on toteuttanut, mihin hyökkäys on kohdistettu sekä niiden aiheuttamat seuraukset. Lisäksi tarkoituksena oli tutkia SOC:in näkökulmasta, olisiko kyseisiä hyökkäyksiä voitu estää ja mitä toimenpiteitä se olisi mahdollisesti vaatinut.

Opinnäytetyössä hyökkäysten kasvun kehitystä pyrittiin tarkastelemaan viiden vuoden aikavälillä. Tästä syntyi ajankohtainen selvitys mihin kiristyshaittaohjelmien kyberhyökkäykset erityisesti kohdistuvat sekä mitkä nykypäivänä olisivat potentiaalisimpia kohteita kyberrikollisille. Näiden alojen yritysten tulisi ottaa kiristyshaittaohjelmien iskut todellisina uhkina ja laatia yrityskohtaisia suunnitelmia niiden varalle jo ennakkoon.

Näkökulmana työssä esitetään myös Security Operation Center (SOC) toiminnan merkitystä ja havainnointia kyseisten hyökkäysten kannalta. Tästä pyrittiin selvittämään, onko SOC-toiminnalla merkitystä hyökkäysten estämiseen ja reagointiin. Saaduilla johtopäätöksillä ja havainnoilla pyrittiin lisäksi ohjeistamaan SOC-toimintaa kiristyshaittaohjelmien varalle. Lisäksi hyötynä SOC-toiminnalle työstä saadaan ajankohtaista tietoa tämänhetkisten kiristyshaittaohjelmien toiminnasta.

Opinnäytetyössä esitellään SOC-toimintaa rakenteellisesti sekä toiminnallisesti. Kiristyshaittaohjelmasta kerrotaan sen toimintaperiaate, miksi sitä käytetään ja mihin sen hyökkäykset erityisesti kohdistetaan. Lisäksi vertaillaan SOC-toimijoiden kokemuksia hyökkäysten kasvuun liittyen ja pohditaan yhteistyön kasvattamisen mahdollisuutta toimijoiden välillä.

1.1 Toimeksiantaja sekä tausta

Opinnäytetyön toimeksiantajana toimi Telia Cygate Oy, joka on osa monikansallista Telia Company teleoperaattorikonsernia. Telia Cygate on ICT-ratkaisuihin keskittyvä yritys, joka tarjoaa kaikki liiketoiminnan kannalta oleellisimmat palvelut yhteen hallintamalliin perustuen korkean tietoturvan ehdoilla. Yrityksellä työskenteli vuonna 2021 yli 400 henkilöä ja toimipisteitä oli yhteensä 9 eri paikkakunnalla. (Telia Cygate 2021.)

Telia Cygate tarjoaa SOC-palvelua yrityksille ja yhteisöille. Toiminta perustuu yleiseen SOC- eli tietoturvahallintakeskuksen toimintamalliin, jossa tarkoituksena on analysoida ja korjata tietoturvapoikkeamia. Näitä koostetaan tietoturva-analysoijien sekä automatiikan avulla tietoturvahavainnoiksi eri lähteiden kautta. Telia Cygate toteuttaa analysointia muun muassa SIEM-palveluiden kautta, joiden avulla pystytään taltioimaan ja käsittelemään ICT-laitteiden lokitietoja paremman tietoturvatilannekuvan aikaansaamiseksi. Lisäksi haavoittuvuuksien hallinnan avulla havainnoidaan ja tunnistetaan erilaisia uhkia sekä haavoittuvuuksia suojattavasta ympäristöstä. Kirjoittaja työskentelee toimeksiantajan tietoturvahallintakeskuksessa. (SOC as a service 2021.)

1.2 Tehtävä ja tavoitteet

Opinnäytetyön toimeksiantona oli selvittää kiristyshaittaohjelmien aiheuttamien hyökkäyksien nykytilannetta maailmalla ja mikä on niiden kehityssuunta. Lisäksi toimeksiannossa pyydettiin selvittämään miten SOC-toimintaa voisi kehittää vastaavien kyberhyökkäyksien varalle ja onko SOC-toiminnalla merkitystä kiristyshaittaohjelmahyökkäysten estämiseen ja reagointiin. Tämän pohjalta sekä kiristyshaittaohjelmissa havaittujen yhteisten piirteiden avulla SOC-toimintaan olisi mahdollista luoda yhteisiä selkeitä käytänteitä sekä suosituksia kiristyshaittaohjelmien aiheuttamien kriisitilanteiden varalle tai välttämiseksi.

2 Tutkimusideologia

Tutkimusideologiassa tuodaan esille mitkä ovat opinnäytetyön tutkimuskysymykset ja millä menetelmillä näihin saadaan vastauksia. Lisäksi tutkimusmenetelmissä tuodaan esille, millä tutkimustavalla opinnäytetyö on toteutettu.

2.1 Tutkimuskysymys

Teknisen alan opinnäytetyössä yksi tärkeimpänä asiana on saada vastaukset tutkimuskysymyksiin. Nämä määrittävät mitä kyseisellä tutkimuksella halutaan selvittää ja mihin lopullisen työn pitäisi vastata. Nämä myös ohjaavat opinnäytetyön kirjoittajaa tutkimusmenetelmän sekä koko opinnäytetyön toteuttamisessa. (Tutkimusasetelma n.d.)

Opinnäytetyössä nousi esiin kolme selkeää tutkimuskysymystä. Ensimmäisenä selvitettävänä tutkimuskysymyksenä on mikä on ajankohtainen kehityssuunta kiristyshaittaohjelmahyökkäyksillä. Maailmalla kehityssuunnat kyberturvallisuudessa voivat vaihdella hyvin nopealla aikataululla, jolloin esimerkiksi muutaman vuoden takaiset uhkakuvat eivät välttämättä vastaa enää todellisuutta. Kyseinen tutkimuskysymys on myös hyvin ajankohtainen, sillä kyseisistä hyökkäyksistä uutisoidaan mediassa paljon niiden aiheuttamien seurauksien vuoksi.

Toisena tutkimuskysymyksenä nousi esille, mitkä syyt ovat mahdollistaneet maailmalla tapahtuneita isoja kiristyshaittaohjelmahyökkäyksiä. Tutkimuskysymyksessä korostuu, onko maailmalla uutisoiduissa hyökkäyksissä löydettävissä yhteisiä piirteitä. Lisäksi tarkasteltiin, miten kiristyshaittaohjelmien kehitys on vaikuttanut hyökkäysten kehityssuuntaan.

SOC-toiminnan kehittäminen on myös tärkeä tavoite jokaisella toimijalla. Tämän vuoksi opinnäytetyössä kolmantena tutkimuskysymyksenä tarkastellaan SOC-toiminnan kehittämistä sekä reagoinnin parantamista kiristyshaittaohjelmahyökkäyksien osalta. SOC:in toimet kyseisten hyökkäysten tullessa kohdalle voivat olla hyvin yritys- tai toimijakohtaisia. SOC-toimijoilla saattaa olla pitkälle ja tarkasti suunniteltu malli, miten kiristyshaittaohjelmahyökkäyksen alkumetreiltä toimitaan aina tilanteen jälkiselvittelyyn asti, kun taas pahimmassa tapauksessa SOC-toimijan havainnointikyky tai toimintasuunnitelma voivat olla heikkoja sekä puutteellisia. Tämän tutkimuskysymyksen kohdalla selvitetään, onko kiristyshaittaohjelmahyökkäyksissä ollut yhteisiä tekijöitä, joita jokaisen SOC-toimijan olisi syytä huomioida omassa reagoinnissaan hyökkäyksiä vastaan. Lisäksi jos mahdolliset kiristyshaittaohjelmahyökkäykset Suomessa tapahtuvat isossa mittakaavassa, voivat aktiiviset hyökkäykset levitä useiden eri SOC-toimijoiden selvitettäviksi, jolloin myös SOC-toimijoiden tiedonvaihto sekä yhteistyö keskenään korostuu. SOC-toimijoiden yhteistyön kehittämistä on myös järkevää ottaa huomioon tämän osalta.

2.2 Tutkimusmenetelmä

Opinnäytetyössä pyritään lähtökohtaisesti aluksi selvittämään realiteetteja tutkimuskysymyksiin tutkimalla nykytilannetta ja viime vuosien tapahtumia. Tämän pohjalta on tarkoituksena vastata tutkimuskysymyksiin ja lopulta kehittää niiden pohjalta ratkaisuja toimeksiantajan kysymyksiin. Rakenteen vuoksi opinnäytetyö vastaa soveltavaa monimenetelmällistä tutkimusta, jossa on myös piirteitä tutkivasta kehittämistoiminnasta. Kyseisen tutkimusmenetelmän avulla saadaan paitsi kattava selvitys kiristyshaittaohjelmien nykytilanteesta, myös selvitys useiden SOC-toimijoiden yhteistyön tilanteesta ja kehityssuunasta. SOC-toimijoiden käytännön ongelmia yhteistyön osalta pyritään selvittämään, jossa apuna toimivat kiristyshaittaohjelmien aiheuttamien hyökkäysten kasvun trendi ja syyt (Työelämän tutkiva kehittämistoiminta n.d.)

3 Teoreettis-käsitteelliset lähtökohdat

Tässä osiossa esitellään opinnäytetyön kolme merkittävää tekijää: Kyberturvallisuuden tilanne, kiristyshaittaohjelma sekä SOC. Kyberturvallisuustilanteessa avataan Suomen kyberturvallisuustilannetta ja muun maailman tilannetta sekä selvitetään, onko niissä merkittäviä eroavaisuuksia. Selvityksessä tulee myös ilmi mikä on kiristyshaittaohjelmien ja SOC:in rooli kyberhyökkäyksen aikana ja mitkä tavoitteet molemmilla tekijöillä on. Lisäksi osiossa ilmenee myös kiristyshaittaohjelman tekninen rakenne sekä SOC:in taktinen toimintamalli operatiivisessa toiminnassa. Myös molempien tekijöiden historia tuodaan esille keskeisten piirteiden esittelyllä.

3.1 Kyberturvallisuuden tilanne

Kyberturvallisuuden tilanteella kuvataan tietoverkkojen sekä IT-infrastruktuurien turvallisuuden tilaa. Tilanteen kuvauksessa otetaan huomioon verkotettujen järjestelmien potentiaalisten uhkien sekä todellisuudessa koettujen häiriöiden vaikutuksia yhteiskunnan sekä yritysten kriittisiin toimintoihin. Ajankohtaisen kyberturvallisuuden tilannekuvan avulla voidaan puolustaa tietojärjestelmiä muuttuvien uhkakuvien varalta tehokkaammin. Lisäksi kyberturvallisuuden tilannekuvan avulla saadaan luotua yhteinen kattava kokonaiskuva kyberturvallisuuskentän tapahtumista. (Kybersää 2022; What is cybersecurity? n.d.)

3.1.1 Kyberturvallisuuden nykytila maailmalla

Kyberturvallisuuden tilanne maailmalla tarkasteltuna antaa ajankohtaisen kokonaiskuvan kaikista uhista mitä eri toimijat ja valtiot kokevat kyberturvallisuuden osalta. Uhat eivät ole keskenään samanlaisia ja niissä voi olla suuriakin eroja esimerkiksi maanosien ja yksittäisien valtioiden osalta. Pääosin kyberhyökkäyksistä kärsivät lukumäärällisesti tarkasteltuna kuitenkin suuret ja varakkaat valtiot, joissa sijaitsee myös enemmän uhan alaista tietoa, jota kyberhyökkäysten avulla muun muassa halutaan saada haltuun tai vahingoittaa. Esimerkiksi Yhdysvallat on ollut Angin kirjoittaman artikkelin mukaan kyberhyökkäyksen kohdemaiden kärkeä vuosien ajan, mutta toisaalta myös merkittävä tekijä hyökkäysten toteuttajien osalta useamman vuoden aikana Knellin kirjoittaman artikkelin mukaan (Ang 2021; Knell 2013). Yhdysvaltalaistoimija Microsoftin digitaalisessa puolustusraportissa tuodaan myös esille Yhdysvaltoihin kohdistuvan peräti 46 prosenttia kyberhyökkäyksistä, mutta raportin väitteen mukaan Venäjältä, Pohjois-Koreasta sekä Iranista tehtäisiin eniten kyberhyökkäyksiä ottamatta kantaa ovatko hyökkäykset valtiollisia vai yksittäisten toimijoiden tuottamia (Microsoft Digital Defense Report 2021, 53-55). Vastaavia raportteja tarkastellessa lukijan täytyy huomioida lähteiden kirjoittajien eri sidonnaisuudet tiedon tarkastelussa.

Myös useat kyberturvallisuusalan yritykset ylläpitävät verkossa julkisesti reaaliaikaista kyberuhkien uhkakarttaa, jotka keräävät muun muassa yrityksen omia työkaluja hyödyntäen tilannetietoa maailmanlaajuisesti. Esimerkkinä voidaan mainita FireEye yrityksen pitämä uhkakartta (ks. kuvio 1), jossa havainnollistetaan valtiotasollisesti reaaliaikaista uhkakuvaa (FireEye cyber threat map n.d.).

Kuvio 1. FireEye yrityksen kyberuhkakartta (FireEye cyber threat map n.d.)

Euroopan unionin verkko- ja tietoturvavirasto (ENISA) julkaisee myös Euroopan tasolla säännöllisesti raportteja, joissa tuodaan esille myös yleiskatsaus kyberturvallisuuden uhkamaailmaan Euroopassa. ENISA Threat Landscape (ETL) -raportin yhdeksännessä painoksessa vuoden 2021 osalta tuodaan esille yleiskatsauksen kyberturvallisuusuhkien maisemaan. ETL-raportti on osittain strateginen ja osittain tekninen, kun se sisältää sekä teknis- että yleistietoa. (Enisa Threat Landscape 2021, 7.)

ENISA:n raportissa tuodaan esille kyberturvallisuushyökkäysten jatkuvaa lisääntymistä vuosien 2020 ja 2021 aikana, ei vain pelkästään vektorien ja lukujen, mutta myös niiden vaikutuksen kannalta. COVID-19-pandemia on myös vaikuttanut kyberturvallisuusuhkakuvaan. Yksi suurimmista COVID-19-pandemian seurauksista on kestävä muutos hybriditoimistomalliin, jonka seurauksena muun muassa pandemiaan liittyvät kyberturvallisuusuhat ja sen hyödyntäminen kyberhyökkäyksissä on raportin mukaan kasvussa. Kyseinen ETL-raportti on tunnistanut vuosien 2020 ja 2021 aikana 8 ensisijaista kyberturvallisuuden uhkaryhmää, joissa kiristyshaittaohjelma on listattuna yhtenä näistä. (Enisa Threat Landscape 2021, 7–8.)

EU:n yleinen tietosuoja-asetus (GDPR), joka julkaistiin vuonna 2016, on tuonut kiristyshaittaohjelmien avulla tehtävien hyökkäysten osalta myös huomioon otettavia asioita varsinkin yritysten ja organisaatioiden osalta. F-Secure:n artikkelin mukaan GDPR huomioiden organisaatioiden saattaa olla tarpeen paljastaa kiristyshaittaohjelmatartunnat viranomaisille ja asiakkaille, joita tämä koskee. GDPR artikloissa 33 ja 34 annetaankin GDPR:n ohjeita yhteydenotosta viranomaisiin ja henkilöihin, joita asia koskee. Artikkelin mukaan se on kuitenkin tarpeen vain silloin, kun henkilötietojen tietoturvaloukkaus on riski luonnollisten henkilöiden oikeuksille. Kiristyshaittaohjelmatartunnassa hyökkääjällä on usein teoriassa pääsy materiaaliin, joka voi vaarantaa näitä oikeuksia. Kiristyshaittaohjelman uhkakuvan ollessa suuri, yritysten on suositeltavaa kehittää toimintamalli tämän osalta täyttääkseen GDPR:än vaatimukset. (Pilkey 2017.)

Ajankohtaisia aiheita huomioiden joulukuussa 2021 havaittiin vakava nollapäivähaavoittuvuus, joka sai laajaa kansainvälistä huomiota ja vaikutti globaalisti kyberturvallisuudessa. Kyseinen haavoittuvuus koski Apache:n ohjelmistokirjasto *Log4j*, joka on rakennettu suositulle koodauskielelle Javalle, jota käytetään laajasti muissa maailmanlaajuisesti käytetyissä ohjelmistoissa ja sovelluksissa. Log4j:n virheen arvioitiin esiintyvän yli 100 miljoonassa tapauksessa maailmanlaajuisesti.

Tätä haavoittuvuutta ja siihen liittyviä hyökkäyksiä kyberturvallisuusyhteisössä on luonnehdittu *Log4Shell* haavoittuvuudeksi. Haavoittuvuuden vaikutuksia ja kestoa luonnehdittiin aluksi vakavaksi sekä pitkäaikaiseksi, mutta maaliskuussa 2022 kyseiset väitteet eivät vaikuta toteutuneen niin kriittisinä kuin eri tahot aluksi epäilivät. (Log4j Zero-Day Vulnerability Response 2022.)

Myös helmikuussa 2022 alkanut Ukrainan kriisi näkyy vahvasti myös kybermaailmassa. Ukrainassa onkin havaittu vuoden 2022 aikana useita kyberhyökkäyksiä ja hyökkäyksiin kuuluivat hallinnon verkkosivuihin kohdistuvia palvelunestohyökkäyksiä, järjestelmien tietoja tuhoava haittaohjelmia ja erilaisia tietojenkalasteluyrityksiä. Kyseiset käytetyt menetelmät eivät ole uusia tai poikkeuksellisia toimenpiteitä, mutta kriisin aikana on nähty aluksi tunnistamattomia muun muassa HermeticWiper- sekä WhisperGate-haittaohjelmia. WhisperGate-haittaohjelman seurantatutkimuksessa tietoturvayhtiö CrowdStrike ilmoitti, että haittaohjelman tarkoituksena on tuhota peruuttamattomasti tartunnan saaneiden järjestelmien tiedot ja yrittää naamioitua aidoksi nykyaikaiseksi kiristysohjelmatoiminnaksi. (Greig 2022; Karlamaa 2022.) Massiivisten kohdistettujen kyberhyökkäysten osalta ilmenee ongelmana hyökkäysten rajaamisen vaikeus. Tietoturvayhtiö Symantec oli raportoinut omaan uhkatietoon perustuen Ukrainaan kohdistettujen kyberhyökkäysten vaikuttaneen lisäksi Latviassa ja Liettuassa toimivissa organisaatioissa, jotka eivät välttämättä ole olleet alkuperäisinä suunniteltuina kohteina. (Abrams 2022.)

3.1.2 Kyberturvallisuuden nykytila Suomessa

Suomessa kyberturvallisuuden nykytilan raportointi toteutetaan Kyberturvallisuuskeskuksen toimesta myös ajankohtaisin tiedottein sekä määräajoin tehtävin raportein. Kyberturvallisuuskeskus tuottaa kuukausittain kattavan kybersää-raportin, joka kertoo kuluneen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Raportti on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille, mutta se sisältää neuvoja myös tavalliselle kansalaiselle. Raportin avulla lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. (Kybersää 2022.)

Tammikuun 2022 kybertilanteesta kertova kybersää-raportti julkaistiin helmikuun 2022 aikana. Raportissa tuodaan esille uhkakuvia kuudesta isommasta näkökulmasta: Tietomurrot ja -vuodot, huijaukset ja kalastelut, haittaohjelmat ja haavoittuvuudet, automaatio, verkkojen toimivuus sekä vakoilu. Raportin mukaan muun muassa tammikuussa on raportoitu Facebook Messengerin kautta

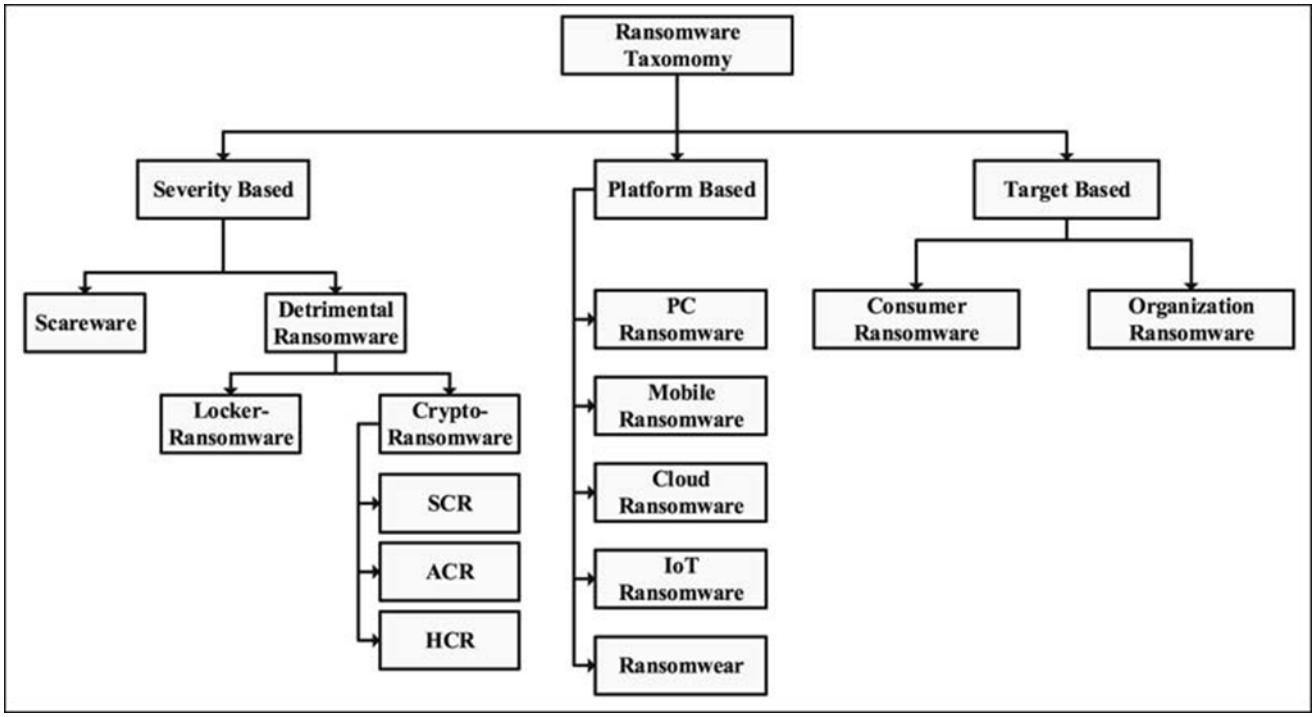
tehtävää aktiivisia tunnustenkalastelua, mutta muutoin kyseessä oli rauhallinen kuukausi tietomurtoilmoitusten suhteen. Kyberturvallisuuskeskus on lisäksi poistanut Log4shell-haavoittuvuudesta annettu kriittinen varoituksen kahden kuukauden voimassaolon jälkeen sekä myös FluBot-varoitus on poistettu, koska operaattoreiden suodatustoimenpiteet ovat todettu toimineen ongelmaan. Vakoilun osalta merkittävänä nostona on suomalaisdiplomaatteihin kohdistunut mobiililaitteiden vakoilu Pegasus-haittaohjelmalla. (Kybersää Tammikuu 2022.)

Kyberturvallisuustilanteeseen Suomessa vaikuttaa vahvasti maailman tilanne ja myös Suomen kyberturvallisuustilanne elää jatkuvassa muutoksessa. Globaalit uhat koetaan myös Suomessa vakavina uhkina ja nopea sekä kattava reagointi uhkien torjuntaan on syytä säilyttää kehityksen kohteena sekä valtio-, että organisaatiotasollisesti.

3.2 Kiristyshaittaohjelma

Viime vuosien aikana erilaiset haittaohjelmat ovat yleistyneet tietotekniikassa. Niiden avulla yritetään saada hyötyä hyökkääjän toimesta tai aiheuttaa vaikeuksia haittaohjelman kohteelle. Kiristyshaittaohjelma (engl. ransomware) on yksi haittaohjelmien muodoista, joka on suunniteltu salaamaan laitteessa olevia tiedostoja, jolloin kaikki tiedostot ja niihin perustuvat järjestelmät muuttuvat käyttökelvottomiksi. Hyökkäyksen uhrilta vaaditaan usein rahallista korvausta, jotta tiedostot voitaisiin palauttaa käyttäjälle. (Ransomware Guide 2020, 2; Schofield 2016)

Kiristyshaittaohjelmalle tuottavana kohderyhmänä toimii suurimmaksi osaksi yritykset tai vaikutusvaltaiset sekä varakkaat henkilöt, joita vastaan hyökkäyksiä voidaan helposti toteuttaa. Niiden aiheuttamat tapahtumat vaikuttavat usein vakavasti yrityksen liiketoimintaan ja hyökkäysten avulla pyritään jättämään yritykset ilman kriittisiä tietoja ja palveluja, joita he tarvitsevat toimiakseen päivittäisesti. (Ransomware Guide 2020, 2.) Al-rimyn, Maarofin ja Shaidin (2018) julkaiseman tutkimukseen perustuen kiristyshaittaohjelmia voidaan luokitella laajan levinneisyyden vuoksi myös kohdejärjestelmätyyppisesti sekä vakavuusasteen määrittelemällä. Kuviossa 2 on selitetty kiristyshaittaohjelmien luokittelu tarkemmin.



Kuvio 2. Kiristyshaittaohjelmien luokittelu (Al-rimy, Maarof & Shaid 2018)

Kiristyshaittaohjelmat voidaan luokitella myös hyökkääjän motiivien ja toimintamallien mukaan. Niin sanottu kryptomato (engl. cryptoworm) on yksinkertaisesti suunniteltu vain itsenäiseksi kiristysohjelmaksi, joka pyrkii replikoimaan itsensä muihin tietokoneisiin mahdollisimman nopeasti ja laajasti verkkojen sisällä. Kiristyshaittaohjelmien kehittäjät ovat jalostaneet tätä hyödyntäen myyntitarkoituksessaan kiristyshaittaohjelmia ja ovat luoneet liiketoimintamallin *Ransomware-as-a-Service* (RaaS). Tässä toimintamallissa kiristyshaittaohjelma myydään niin sanotussa pimeässä verkossa palveluna. RaaS-paketit tarvitsevat varsinaiselta hyökkääjältä vain vähän teknisitä ymmärrystä ja sen avulla on kyky hyökätä helposti haluttua kohdetta vastaan. Tämän tyyliset hyökkäykset toteutetaan yleensä haitallisten roskapostisähköpostien kautta tai erillisenä latauksena huijaussivustojen kautta. (Loman 2019, 4.)

Aktiiviset automatisoidut hyökkääjät voidaan luokitella myös omaksi kategoriaksi motiivin ja toiminnan perusteella. Siinä niin sanottuja skannausohjelmia käyttävät hyökkääjät etsivät automaattisesti internetistä heikosti suojattuja IT-järjestelmiä. Kun tällaisia järjestelmiä löydetään, hyökkääjät suunnittelevat ja tiedustelevat huolellisesti kiristysohjelmahyökkäyksen mahdollisimman suuren vahingon saamiseksi. Palvelut, jotka ovat avoimesti alttiina Internetiin, kuten esimerkiksi Remote Desktop Protokollaa (RDP) hyödyntävät ohjelmat, ovat haluttuja sisääntulokohtia niiden

ollessa alttiita niin sanotulle väsytyshyökkäykselle (engl. Brute Force Attack) laitteen käyttäjätunnusten arvaamiseksi. Tämän tyylisessä hyökkäyksessä on tyypillistä, että uhrit saattavat kokea olevansa erityisenä kohteena, vaikka hyökkäys on yleensä opportunistinen. (Loman 2019, 4.)

Hyökkäysten tehostamisiksi haitalliset toimijat ovat luoneet ja kehittäneet omia kiristyshaittaohjelmataktiikoita. Näihin sisältyy muun muassa uhrien painostaminen maksamaan uhkaamalla luovuttaa varastettuja tietoja ulkopuolisille tahoille, jos he kieltäytyvät maksamasta, sekä uhrien julkisesti nimeäminen ja häpeäminen toissijaisina kiristyksen muotoina. (Ransomware Guide 2020, 2.) Kansainväliset kyberturvallisuudesta vastaavat tahot eivät suosittele kuitenkaan maksamaan toimijoille, sillä ei ole takeita, että lunnaiden maksaminen korjaisi tilanteen. Se voi myös tehdä uhrista uudelleen haavoittuvan tuleville vastaaville hyökkäyksille (Microsoft Digital Defense Report 2021, 14-15; Ransomware n.d.).

Kiristyshaittaohjelmien sekä niiden ryhmittymien kokemia muutoksia tarkastellaan tarkemmin luvussa 3.2.1. Kiristyshaittaohjelmien teknistä näkökulmaa esitellään omassa alaluvussa 3.2.2 ja kiristyshaittaohjelmien vaikutusta maailmalla analysoidaan tarkemmin luvussa 3.2.3.

3.2.1 Kiristyshaittaohjelman historia

Kiristyshaittaohjelmat kuten myös monet muutkin tietotekniikan haittaohjelmat linkittyvät toisiinsa muun muassa teknisten tapojen sekä toimintamalliensa kautta. Kiristyshaittaohjelmat ovat ajan kuluessa kehittyneet edistyneimmiksi ja ensimmäiset kiristyshaittaohjelmiksi luokitellut tapaukset näyttävät melko alkeellisilta tänä päivänä tarkastelussa. Kiristyshaittaohjelmien historia voidaankin jakaa kahteen osaan: ennen salausta ja sen jälkeen. (Drozhzhin 2016; Palozza 2018.)

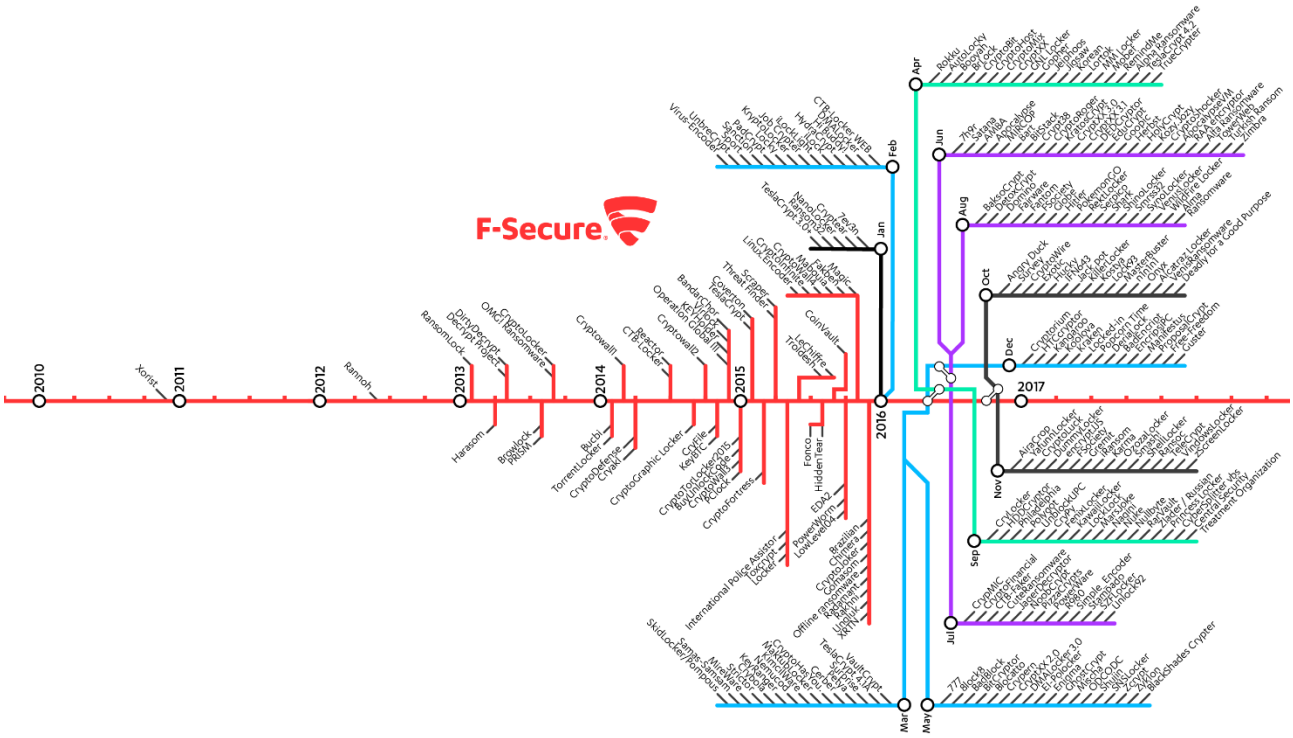
Palozzan artikkelin mukaan kiristyshaittaohjelman ensimmäinen malli esiteltiin niin sanottuna AIDS-troijalaisena vuonna 1989, kun Harvardissa koulutettu biologi Joseph L. Popp lähetti 20 000 vaarantunutta levykettä nimeltä maailman terveysjärjestön järjestämän sisäisen AIDS-konferenssin osallistujille. Kyseinen troijalainen toimi salaamalla tiedostojen nimet asiakkaiden tietokoneella ja piilottamalla hakemistoja. Uhreja pyydettiin maksamaan fyysisesti 189 dollaria postilaatikossa Panamassa. (Palozza 2018.)

Myös niin kutsutut blokkaajat toimivat nykyisten kiristyshaittaohjelmien esikuvina. Blokkaaja haittaohjelmana esti pääsyn käyttäjän käyttöjärjestelmään tai selaimeen, kunnes uhri maksoi vaadittavat lunnaat. Maksaminen vaati tyypillisesti tekstiviestin lähettämistä lyhytkoodiin tai rahan siirtämistä sähköiseen lompakkoon. Kun sähköisen maksamisen säännökset muuttuivat, kyberrikolliset eivät enää kyennyt hyödyntämään näitä tekniikoita, jolloin nämä muuttuivat vähemmän kannattavaksi ja riskialttiimmaksi rikollisten näkökulmasta. (Drozhzhin 2016.)

Salaustekniikkaa hyödyntäviä kiristyshaittaohjelmia alkoi esiintyä myöhemmin 2000-luvun puolella ja vuodesta 2006 lähtien kyberrikolliset ovat aktivoituneet näiden osalta ja alkaneet käyttää epäsymmetristä RSA-salausta. Lisäksi kyberrikolliset siirtyivät samalla uuteen lähestymistapaan, kun he alkoivat salata uhrien kiintolevyille tallennettuja tiedostoja, toisin kuin olisi estetty pääsy vain kiristyshaittaohjelman uhrin selaimiin ja käyttöjärjestelmiin (Drozhzhin 2016). Ensimmäisissä versioissa hyödynnettiin niin sanottua Archiveus-troijalaista, joka salasi tietokoneen *Tiedostot*-hakemiston sisältämät tiedostot. Uhreille luvattiin pääsy takaisin näihin vain, jos he päättivät ostaa erilliseltä verkkosivulta 30-numeroiseen salasanaan. (Palozza 2018.)

Vuoden 2012 jälkeen kiristysohjelmat alkoivat levitä maailmanlaajuisesti tartuttaen järjestelmiä ja muuttumaan kehittyneemmiksi muodoiksi helpottaakseen hyökkäysten toimittamista vuosien kuluessa. Kiristyshaittaohjelmien iskut maailmalla moninkertaistuivat ja löytöjä näistä tehtiin yli 200 000:een vuoden 2012 kolmannella neljänneksellä. Yksi ensimmäisistä maailmalla laajasti huomiota herättäneistä kiristyshaittaohjelmista nimeltään CryptoLocker ilmestyi ensimmäisenä versiona syyskuussa 2013 ja ensimmäinen kopiointiohjelmisto nimeltä Locker esiteltiin saman vuoden joulukuussa. (Palozza 2018.)

Kiristyshaittaohjelmien kasvu lähti lopulta kiihtyvään jyrkkään nousuun muun muassa virtuaalivaluutta bitcoinin käytön kasvun seurauksena, josta tuli laajalle levinnyt ja melko suosittu kyberrikollisten keskuudessa. Tällä kryptovaluutalla on samanaikaisesti digitaalinen omaisuus ja maksujärjestelmä, jota on haastava jäljittää tai valvoa. Muutamien vuosien aikana maailmalla levisi useita eri nimisiä kiristyshaittaohjelmia, joiden takana oli osittain myös suurempia ryhmittymiä. (Drozhzhin 2016.) Kasvun kehitystä vuoteen 2017 asti havainnollistaa tietoturvayhtiö F-Securen tuottama aikajana eri kiristyshaittaohjelmista (ks. kuvio 3).



Kuvio 3. Kiristyshaittaohjelmien aikajana (Hyvärinen 2017)

3.2.2 Kiristyshaittaohjelman tekninen toimintatapa

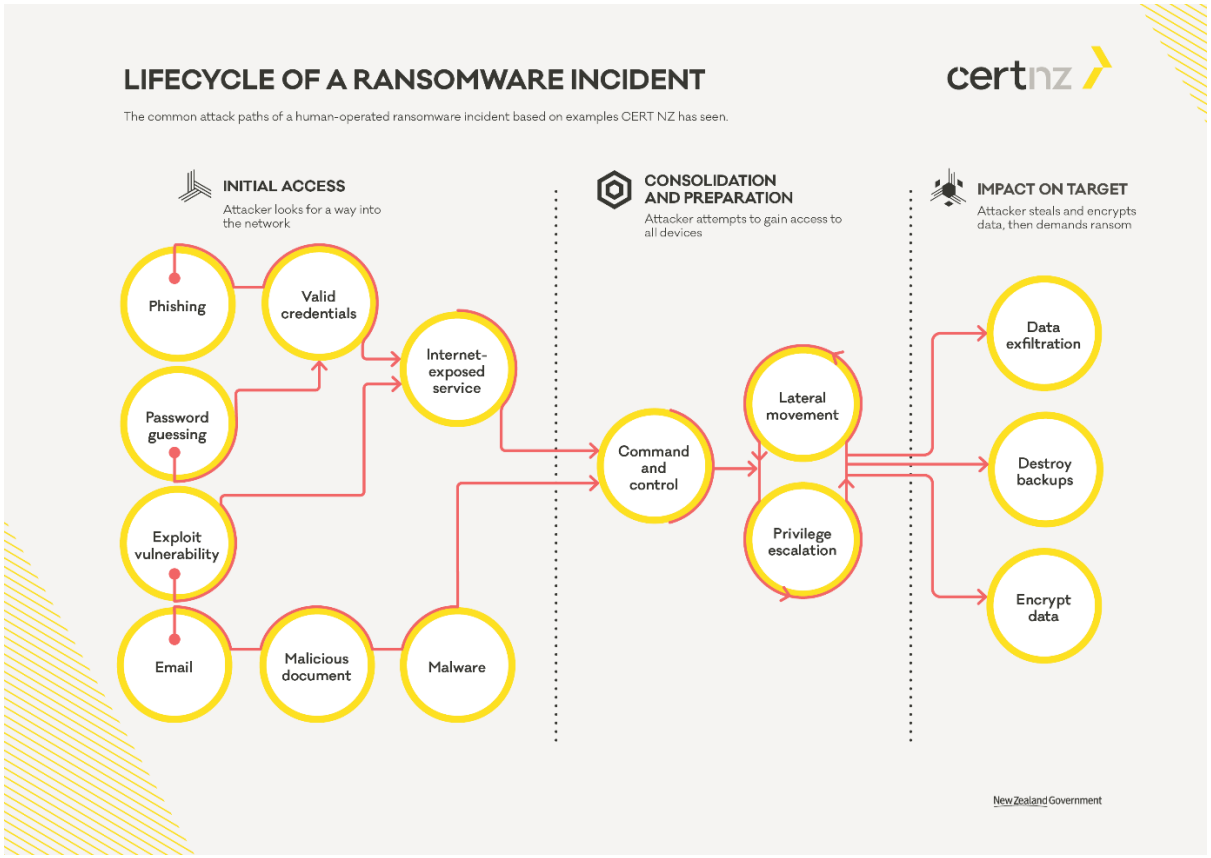
Yksittäisen toimijan itsenäisesti kehittämä kiristyshaittaohjelmanhyökkäys on monivaiheinen prosessi ja sen toteuttaminen vaatii hyökkääjältä riittävää teknistä ymmärrystä muun muassa salausmenetelmistä, tietoliikenteestä, ohjelmoinnista sekä tietoa haavoittuvuuksista eri järjestelmissä. Erityisesti hakkerointiin keskittyneillä keskustelupalstoilla on kuitenkin viime vuosien aikana ilmestynyt helppoja ohjeita sekä työkaluja, joilla kiristyshaittaohjelman luontia on helpotettu. Tällaisia palveluja ovat muun muassa BluEnt yrityksen How to Create Your Own Ransomware (2017) blogikirjoituksen mukaan Android-älypuhelimille suunnattu Trojan Development Kit (TDK), jonka avulla kuka tahansa voi luoda mukautetun kiristysohjelman ja se voidaan rakentaa kokonaisuudessaan älypuhelimella itsenäisesti ilman että käyttäjän tarvitsee kirjoittaa yhtään koodiriviä. (Ransomware Guide 2020, 4.)

Kun kiristyshaittaohjelma on luotu, tarvitsee se saada sisälle sille tarkoitettuun kohdejärjestelmään. Tähän on olemassa useita tapoja ja ne vaihtelevat hyökkääjien mukaan, vaikkakin hyökkääjät usein suosivat muutamia tapoja. Yksi yleisistä tavoista on hyödyntää uhrille tarkoitettua kohdennettua haitallista sähköpostia. Kyseinen sähköposti sisältää haitallisen liitetiedoston, jonka

avatessaan se suorittaa haitallisen ohjelman, joka on usein naamioitu luotettavaksi käyttötarkoitukselliseksi ohjelmaksi uhrin huijaamiseksi. Myös tietojenkalastelusähköpostit ovat yleisiä, joissa uhria pyydetään syöttämään käyttäjätunnukset ulkoiseen palveluun. Näiden avulla hyökkääjä pyrkii kirjautumaan haluttuun kohdejärjestelmään ja lataamaan sekä suorittamaan kiristyshaittaohjelman. Edistyneemmät ja aggressiiviset kiristyshaittaohjelmahyökkäykset voivat hyödyntää myös eri tietoturva-aukkoja, joita ilmenee sovelluksissa sekä käyttöjärjestelmissä. (Fruhlinger 2020; Ransomware Attack – What is it and How Does it Work n.d.; Ransomware Guide 2020, 5.)

Haittaohjelma voi toteuttaa uhrin tietokoneella useita prosesseja eikä se rajoitu pelkästään tietojen salaamiseen. Kyseinen toimenpide on hyvin riippuvainen kiristyshaittaohjelman tyypistä, joista edistyneemmät voivat lähettää tietokoneen tiedostoja sekä tietoja eteenpäin ulkoisille hyökkääjien hallussa oleville verkkopalvelimille tai yrittää skannata samassa verkossa olevia toisia haavoittuvia laitteita ja levittää kiristyshaittaohjelmatartuntaa myös näihin. Esimerkki tämän tyylisestä kiristyshaittaohjelmasta on nimeltään WannaCry, joka on itsenäisesti leviävä kiristysohjelma hyödyntäen haavoittuvuuksia Microsoftin Server Message Block (SMB) -protokollassa LAN- ja WAN-verkon kautta (Lu, Liu, Chen, Zhang, Gao & Zhong 2020). (Ransomware Attack – What is it and How Does it Work n.d.; What Ransomware Allows Hackers to Do Once Infected n.d.)

Kun kiristyshaittaohjelmat ovat päässeet uhrin tietojärjestelmään, seuraa usein toinen laajempi vaihe prosessissa. Perustuen Checkpoint yrityksen kirjoituksiin (n.d.) sekä Fruhlingerin (2020) julkaisemaan artikkeliin, aloittavat kiristyshaittaohjelmat seuraavaksi uhrin tiedostojen salaamisen. Salaus voidaan toteuttaa monella eri salausalgoritimilla, mutta niissä hyödynnetään hyökkääjän luomaa matemaattista avainta. Riippuen valitusta salausalgoritmista sekä kiristyshaittaohjelman teknisestä toteutuksesta, prosessin kesto voi vaihdella suurella aikaikkunalla. Uhrin kovalevyltä pyritään salaamaan mahdollisimman paljon tiedostoja sekä mahdollisesti tärkeimmiksi luokitellut tiedostot kiristyshaittaohjelma pyrkii priorisoimaan. (Pompon 2020.) Jos salaus on tehty riittävän tehokkaalla algoritmilla sekä tiedoston salauksen onnistuessa niitä ei voida purkaa ilman hyökkääjän tuntemaa salausavainta, ja tällöin uhrin tiedostot muuttuvat käyttökelvottomiksi (Fruhlinger 2020). Ihmisjohteisesti ohjatun kiristyshaittaohjelmatapauksen elinkaari esitellään kuviossa 4, joka on Uuden-Seelannin valtiollisen CERT-toimijan laatima kuvaus.



Kuvio 4. Kiristyshaittaohjelman tyypillinen elinkaari (Lifecycle of a ransomware incident n.d.)

Hyökkääjän näkökulmasta salausalgoritmin tarvitsee olla riittävän tehokas, jotta haluttuun lopputulokseen päästään onnistuneesti ja uhrin huomaamatta. Se vaatii huolellista suunnittelua sekä toteutusta, sillä itse salausprosessi sisältää useita erillisiä vaiheita perustuen kuitenkin kahteen pääosaan: algoritmeihin ja avaimiin. Tietokonejärjestelmissä käytettävät algoritmit ovat monimutkaisia matemaattisia kaavoja, jotka sanelevat säännöt, kuinka selväteksti muutetaan salatekstiksi. Avain on taas satunnaisten bittien merkkijono, jota itse algoritmi käyttää lisäämään salausprosessin satunnaisuutta. (Pompon 2020; Harris 2010, luku 8.)

Salausalgoritmit ovat joko symmetrisiä tai asymmetrisiä. Symmetriset algoritmit hyödyntävät symmetrisiä avaimia eli niin sanottuja salaisia avaimia, kun taas asymmetrinen algoritmi käyttää epäsymmetrisiä avaimia, joita voidaan kutsua myös julkisiksi ja yksityisiksi avaimiksi. (Harris 2010, luku 8.)

Symmetristä kryptografiaa käyttävässä salausjärjestelmässä lähettäjä ja vastaanottaja käyttävät kahta saman avaimen esiintymää salaukseen ja salauksen purkamiseen. Avaimella on siis täten kaksi toimintoa, sillä se voi suorittaa sekä salauksen että salauksen purkamisenprosessit. Salauksen hyödyntämiseksi symmetrisessä salauksessa avain on näin ollen syytä pitää asianmukaisesti suojattuna sillä se myös mahdollistaa salauksen purun. Symmetrisiä salausalgoritmeja ovat esimerkiksi Data Encryption Standard (DES) sekä Advanced Encryption Standard (AES). (Harris 2010, luku 8.)

Asymmetrisessä eli epäsymmetrisessä salausjärjestelmässä erona symmetriseen salausjärjestelmään on useamman avaimen hyödyntäminen. Asymmetrisessä salausjärjestelmässä jokaisella objektilla on eri avaimet ja julkinen ja yksityinen epäsymmetriset avaimet liittyvät matemaattisesti toisiinsa. Jos viesti on salattu yhdellä avaimella, toinen avain tarvitaan viestin salauksen purkamiseen. Näin ollen yhden käyttäjän avainpari koostuu yhdestä julkisesta avaimesta ja yhdestä yksityisestä avaimesta. Normaalitilanteessa salausta hyödyntäessä julkinen avain voidaan jakaa yleisesti muiden tietoisuuteen ja yksityinen avain on henkilökohtainen ja kenelläkään muulla kuin omistajalla ei pitäisi olla pääsyä yksityiseen avaimeen. Asymmetrinen salausalgoritmi toimii myös paljon hitaammin kuin vastaava symmetrinen salausalgoritmi sen suorittaessa salattaville biteille suhteellisen yksinkertaisia matemaattisia toimintoja salaus- ja salauksenpurkuprosessien aikana, kun taas asymmetrinen salaus käyttää paljon monimutkaisempaa matematiikkaa toimintojensa suorittamiseen, mikä vaatii enemmän käsittelyaikaa. Esimerkkeinä asymmetristä salausalgoritmeja hyödyntävistä salauksista on Rivest-Shamir-Adleman (RSA) sekä Elliptisen käyrän salausjärjestelmä (ECC). (Harris 2010, luku 8.)

Niin sanotun hybridisalausmenetelmän avulla voidaan hyödyntää sekä symmetrisen että asymmetrisen salauksen tekniikoita. Hybridisalausprosessissa symmetrisen algoritmin avulla luodaan avaimia, joita käytetään yleisen tiedon salaamiseen, ja epäsymmetrinen algoritmin avulla luodaan avaimia, joita voidaan käyttää aikaisemmin luotujen symmetristen avainten jakeluun ja pitää ne näin ollen suojattuna koko ajan (Harris 2010, luku 8). Nykyään myös edistyneet kiristyshaittaohjelmat osaavat hyödyntää hybridisalausmenetelmää. Sen etuna on myös, että kiristys-haittaohjelman salausprosessi ei välttämättä tarvitse aktiivisesti Internet-yhteyttä prosessin aikana. Harriksen (2010) oppaan lisäksi hybridisalausmenetelmää esitellään Marinhon (2018) artikkelissa. Salattavalle kohteelle kiristyshaittaohjelma luo aluksi epäsymmetrisellä tavalla asiakaspuolen julkisen

sekä yksityisen avaimen. Lisäksi kiristyshaittaohjelman koodiin on sisällytetty sen tarvitsema serveripuolen julkinen avain. Toisessa vaiheessa kiristyshaittaohjelma salaa symmetrisellä AES-salausalgoritmilla sekä omaa toimintaperiaatteettaan noudattaen kohdejärjestelmän tiedostot. Tämän valmistuttua, kolmannessa vaiheessa salataan AES-salausmenetelmän tuottamat avaimet aluksi luodulla epäsymmetrisen salausalgoritmin julkisella avaimella. (Marinho 2018; Harris 2010, luku 8.)

Kiristyshaittaohjelman uhri ei kykene kyseistä hybridisalausmenetelmää hyödyntävältä kiristyshaittaohjelmalta palauttamaan salattuja tiedostojaan, sillä sen tarvittavat avaimet on salattu kahden eri menetelmän avulla. Tarvittavat AES-avaimet on nimittäin salattu asiakaspuolen julkisella avaimella ja näiden AES-avainten salauksen purkamiseen tarvitaan asiakaspuolen yksityinen avain. Vastaavasti asiakaspuolen yksityinen avain on salattu serveripuolen julkisella avaimella. Asiakaspuolen yksityisen avaimen salauksen purkamiseen tarvittaisiin serveripuolen yksityinen avain, ja kiristyshaittaohjelman palvelin on ainoa, jolla on kyseinen avain hallussa. (Marinho 2018.)

Koska erilaisia salausmenetelmiä on useita, voidaan kiristyshaittaohjelma luoda vastaavasti lukuisia eri rakenteita ja protokollia hyödyntäen. Yhdistävänä tekijänä kiristyshaittaohjelmilla on kuitenkin, että suurimmassa osassa niistä tavallista tunnettua salausalgoritmia. Hu:n kirjoittaman artikkelin (2017) mukaan tavallisista salausalgoritmeista korkeimman käyttöasteen kiristyshaittaohjelmissa on saavuttanut AES-algoritmi, jota seuraa RSA-algoritmi, mutta jotkut kiristysohjelmat käyttävät myös ECDH-algoritmia. Koska kaikkia näitä tavallisia salausalgoritmeja voidaan pitää kirjoitushetkellä purkamattomina, syy siihen, jos kiristyshaittaohjelmat voidaan murtaa, johtuu täysin tavallisten salausalgoritmien virheellisestä käytöstä kiristyshaittaohjelmissa. (Hu 2017; Ransomware Guide 2020, 12.)

Kiristyshaittaohjelma hyökkäyksen viimeinen vaihe on usein käyttäjälle ilmoittaminen kiristyshaittaohjelman tekemistä toimenpiteistä. Tämän tarkoituksena on aiheuttaa pelkoa ja hämmennystä hyökkäyksen uhrissa. Ilmoituksessa ilmoitetaan selkeällä tekstillä, että tiedostot on salattu ja toimenpiteet, jotka käyttäjän on suoritettava, että hän voisi saada tiedostot purettua. Varmistaakseen, että uhrit ymmärtävät välittömästi mitä on tapahtunut, esittää esimerkiksi CryptoLocker-kiristyshaittaohjelma käyttäjälle ponnahdusikkunan, kun taas WannaCry- ja Sodinokibi-

kiristyshaittaohjelmat, korvaavat Windowsin työpöydän taustakuvan viestillään. Uhrin suoritettavat toimenpide pohjautuvat maksuihin, joita heidän on maksettava hyökkääjille. Usein maksu halutaan krypto- tai virtuaalivaluutassa, sillä niiden lopullinen jäljittäminen on vaativampaa kuin suora rahallinen maksu (Martin 2021). Ilmoitukseen on myös usein lisätty myös aikamääre, joka lähtee liikkumaan kohti nollaa, jonka kuluessa maksu pitää suorittaa tai tiedostot tuhotaan lopullisesti. Esimerkkinä kuviossa 5 CryptoLocker-kiristyshaittaohjelman ilmoitus. (Goodin 2013; Loman 2019, 4.)

Kuvio 5. CryptoLocker-kiristyshaittaohjelman esittämä ilmoitus (Goodin 2013)

Jos lunnaat maksetaan, hyökkääjä usein toimittaa joko kopion yksityisestä avaimesta, jota käytetään symmetrisen salausavaimen purkamiseen, tai kopion itse symmetrisestä salausavaimesta. Nämä tiedot voidaan syöttää salauksenpurkuohjelmaan (myös kyberrikollisen tarjoamaan), joka

voi käyttää niitä salauksen kumoamiseen ja pääsyn palauttamiseen käyttäjän tiedostoihin. Maksaminen hyökkääjille ei kuitenkaan takaa, että uhri saa tiedostot takaisin, sillä kyberrikolliset voivat uhrin kannalta pahimmassa tapauksessa vain ottaa rahat ja kadota, eivätkä he ole edes rakentaneet salauksen purkutoimintoa kiristyshaittaohjelmiin. Hyökkääjä voi jossain tapauksessa tarjota tai esittää ohjelmaa, jonka avulla uhri voi ilmaiseksi purkaa muutaman valitsemaansa tiedostoa todisteeksi siitä, että purkuohjelma on olemassa. (Ransomware Attack – What is it and How Does it Work, n.d.; Fruhlinger 2020; Webb 2021.)

Maailmalla on ollut liikkeellä useita eri nimisiä sekä tyylisiä kiristyshaittaohjelmia, joiden hahmottaminen ilman niihin perehtymistä on erittäin haastavaa. Osa kiristyshaittaohjelmien iskuista on edennyt vuosi- ja kuukausitasolla tarkasteltuna aaltomaisesti eri kampanjoissa. Monet toimijat myös vaihtavat kiristyshaittaohjelmien sekä omien organisaatioiden nimiään aktiivisesti eri vaiheissa, vaikka kyseessä voi olla teknisesti ottaen olla samasta tai samantyyppisestä kiristyshaittaohjelmasta (Schwartz 2021).

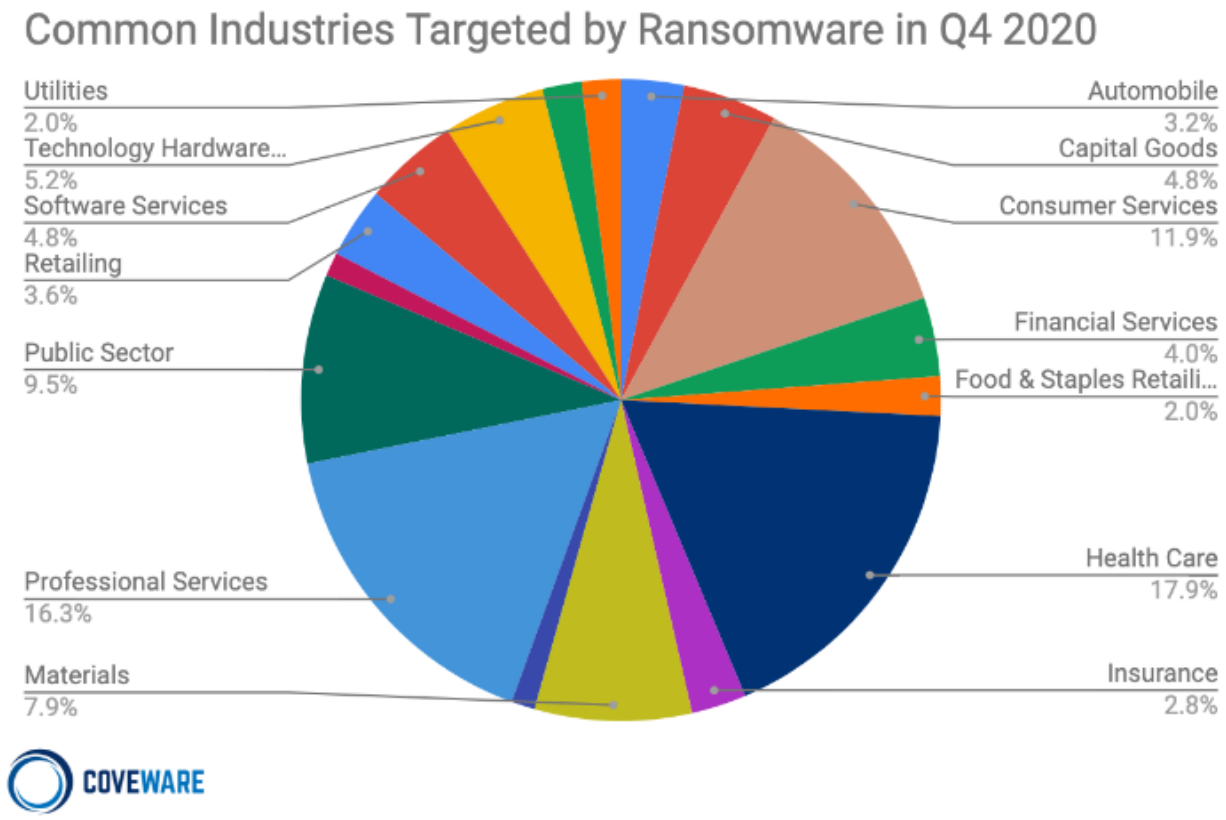
3.2.3 Kristyshaittaohjelman vaikutus

Kiristyshaittaohjelmien vaikutukset hyökkäyksen uhrille ovat riippuvaisia hyökkääjän motiiveista sekä kiristyshaittaohjelman tyypistä. Hyökkääjä saattaa olla erityisesti tiettyä uhria vastaan motivoitunut toteuttamaan hyökkäyksen, jolloin tarkoituksena on aiheuttaa uhrille myös muitakin kuin rahallista tappiota. Maailmalla yleisten poliittisten tilanteiden muutoksissa kansainvälisten jännitteiden lisääntyminen on johtanut entistä enemmän poliittisesti motivoituneisiin hyökkäyksiin. Toisaalta myös lisääntynyt digitalisaatio arkaluonteista dataa käsittelevissä yrityksissä, kuten esimerkiksi terveydenhuollon organisaatioissa, antaa kyberrikollisille lisää taloudellista motivaatiota toteuttaa kohdennettuja hyökkäyksiä. Kiristyshaittaohjelmien kehitys RaaS-palveluksi mahdollistavat vastaavasti varsinaisten haittaohjelmien laajempaa sekä tehokkaampaa kehitystä. (Partida 2021.)

Kiristyshaittaohjelman uhrille hyökkäyksessä menetetty data sekä mahdollisesti maksettava rahallinen lunnasvaatimus eivät ole ainoita ongelmia uhrille. Yrityksen täytyy ottaa huomioon vioittuneiden tietojärjestelmien korjaustoimiin liittyvät taloudelliset tappiot sekä tuloja tuottavien toimintojen pysäyttämisestä aiheutuvat kustannukset.

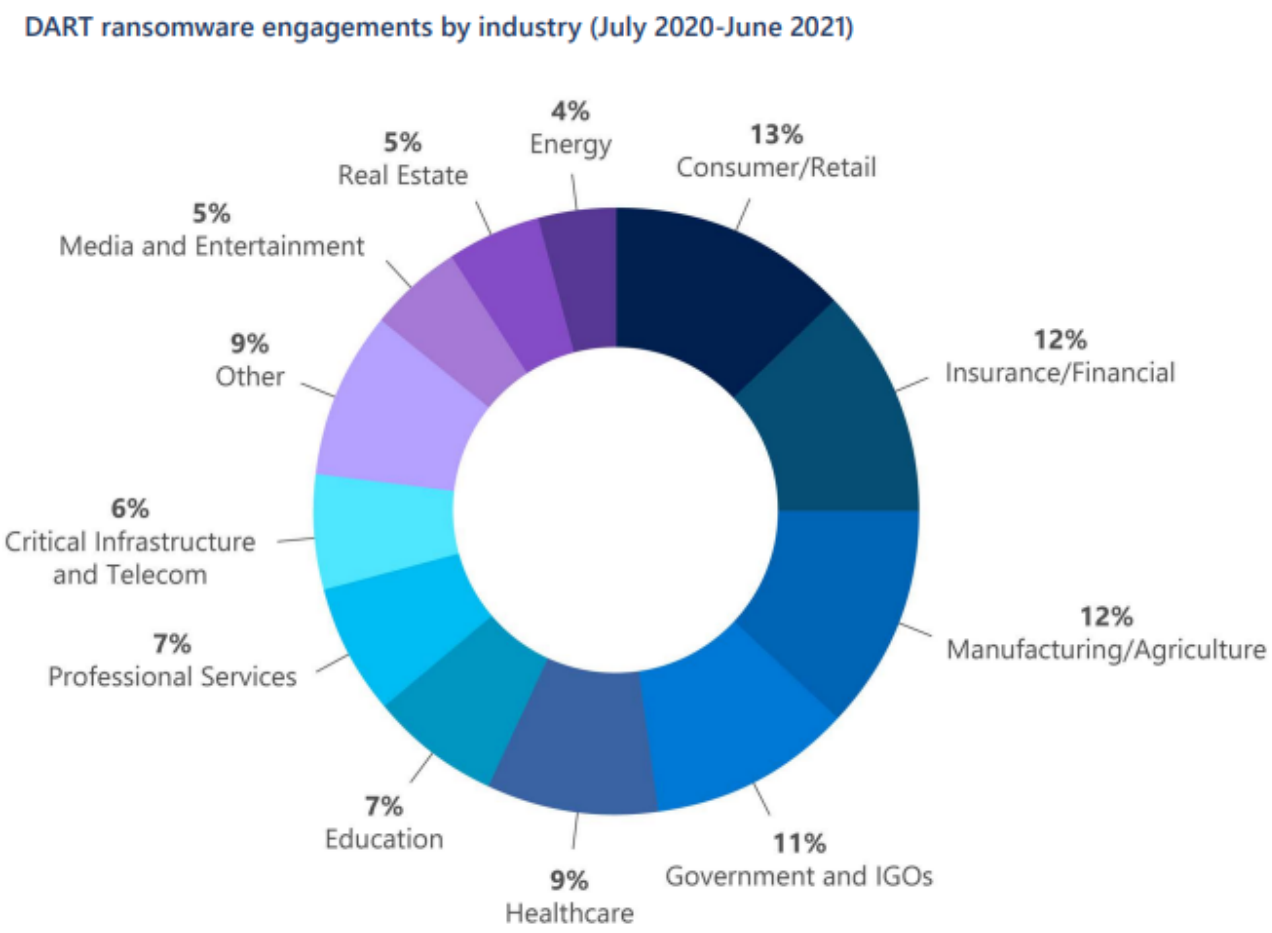
Lisäksi erityisesti suuryritykset voivat kärsiä oman maineen vahingoittumisesta uutisoinnin sekä tiedottamisen johdosta. (The Impact of Ransomware n.d.)

Toimialakohtaisesti tarkasteltuna kiristyshaittaohjelmat vaikuttavat kaikkiin toimialoihin. Maailmanlaajuisen koronapandemian aikana, vuoden 2020 viimeisellä neljänneksellä, terveydenhuolto oli Coveware yrityksen tuottaman raportin mukaan suurin kiristysohjelmien kohteena oleva toimiala, jonka jälkeen seurasivat asiantuntija- ja kuluttajapalvelut. Koronapandemian aikana kiristyshaittaohjelmahyökkäykset kohdistuivat myös koulutussektorin toimijoihin, jotka koettiin helpoiksi uhreiksi muun muassa vanhentuneiden IT-laitteiden sekä arkaluonteisen tiedon ansiosta. (Singh 2021.) Kiristyshaittaohjelmahyökkäysten kohteiksi joutuneiden yritysten määriä vuoden 2020 viimeisellä neljänneksellä toimialakohtaisesti esitellään tarkemmin kuviossa 6.



Kuvio 6. Kiristyshaittaohjelmahyökkäysten uhrien toimialat Q4-kvartaalilla vuonna 2020 (Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands 2021)

Microsoftin digitaalista puolustusraporttia (2021) tarkasteltaessa, joka tutki havaintoja pideämmällä aikavälillä vuoden 2020 ja 2021 aikana, havaitaan myös samantapaista kehitystä muutamilla eroavaisuuksilla toimialakohtaisesti. Microsoftin DART-tiimin (Detection and Response Team) havainnoimat kiristyshaittaohjelmatapaukset osoittavat, että kolme eniten kohdistettua alaa olivat kuluttaja-, rahoitus- ja tuotantosektori. Myös terveydenhuoltosektori pysyi viiden suurimman toimialan kärjessä Microsoftin raportissa. (Microsoft Digital Defense Report 2021, 18.) Kuviossa 7 on nähtävissä myös muiden toimialojen muutokset. Kuviota 6 ja 7 tarkasteltaessa on kuitenkin hyvä ymmärtää, että Covewaren ja Microsoftin ilmoittamat toimialaluokat eivät ole täysin samoja, joka vaikuttaa osittain tuloksiin. Lyhyellä tarkastelujaksolla muutokset tapausten määrissä kuitenkin voivat olla suuria yksittäisten toimialojen kohdalla, mutta pidemmästä tarkastelujaksosta on havaittavissa selkeät eroavaisuudet kohteiden välillä.



Kuvio 7. DART-tiimin kiristyshaittaohjelmahavainnot toimialoittain (Microsoft Digital Defense Report 2021, 18)

3.3 SOC – Security Operation Center

Security Operation Center (SOC) tarkoittaa tietoturvahallintakeskusta, joka on erillinen tietoturvaan keskittyvä yksikkö. Kyseinen tiimi koostuu useista ihmisistä sekä toimintatavoista, joiden pääasiallisena tehtävänä on havaita, analysoida, torjua sekä korjata suojattavaan kohteeseen kohdistuvia kyberturvallisuusuhkia. Tähän tavoitteeseen päästään analysoimalla esimerkiksi verkkoliikennettä tai tietoteknisten laitteiden sekä järjestelmien lokitietoja. SOC voi olla yrityksen sisällä toimiva yksikkö tai se voi olla ulkopuolisena palveluna ostettu toiminta sitä tarjoavalta yritykseltä. Ulkopuolisen yrityksen tarjoamaa SOC-palvelua kutustaan Managed Security Service Provider (MSSP) palveluksi, joka sisältää erikseen ostetut palvelut, kuten esimerkiksi haittaohjelmien torjuntapalvelut, palomuuripalvelun tai Virtual Private Network (VPN) palvelun (Smith 2021). (de Groot 2020.)

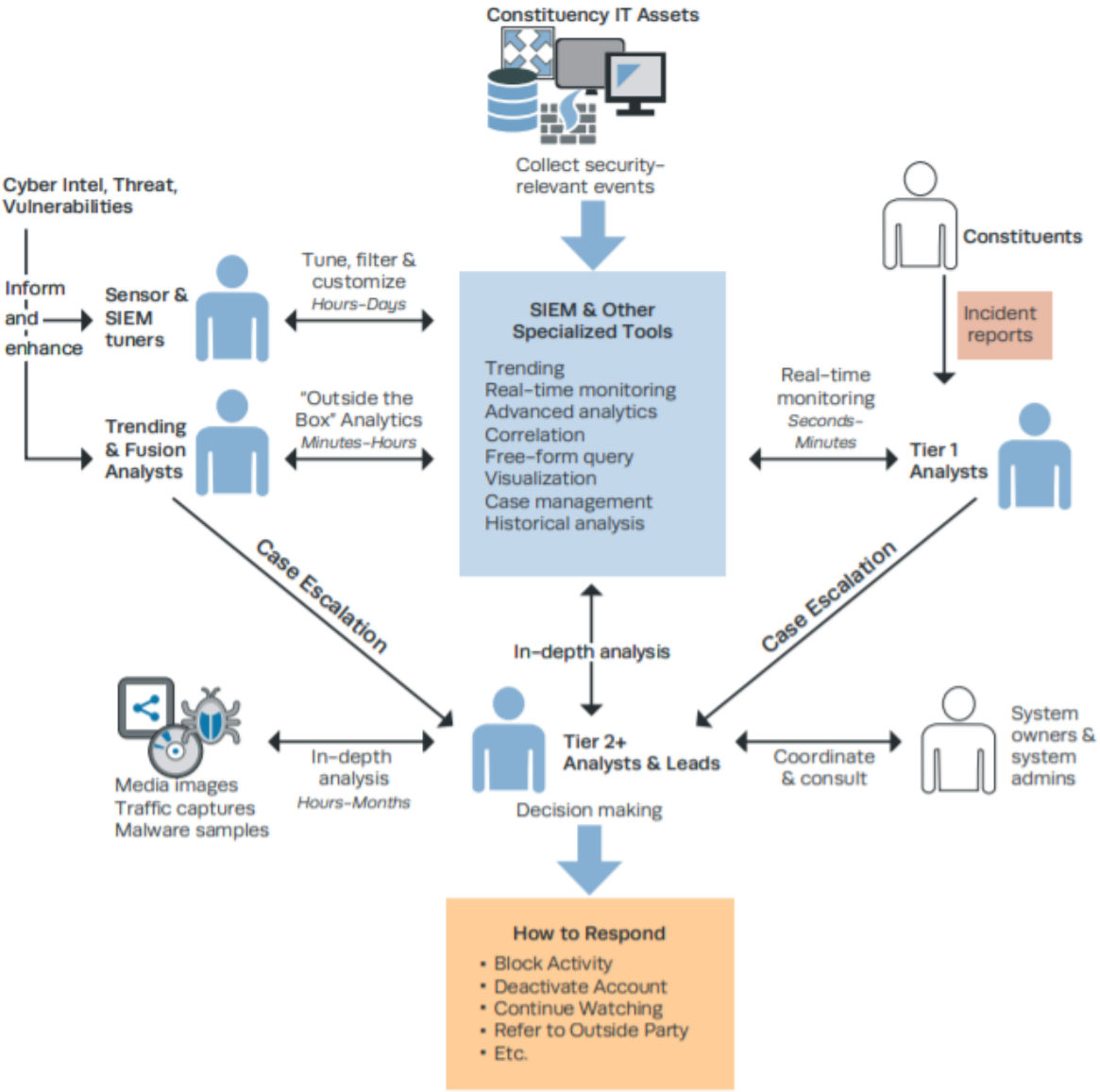
Nykypäivänä tietoturvauhat kehittyvät kovaa vauhtia ja maailmalla tähän on reagoitu panostamalla kyberturvallisuuteen yrityksissä ja yhteisöissä. Nopeimmillaan hyökkääjät voivat päästä yritysten järjestelmiin käsiksi vain tunneissa hyödyntämällä haavoittuvuuksia. Vastaavasti suurissa ja kasvavissa yrityksissä haavoittuvuuksien korjaamiseen tarvittavien päivitysten asentaminen voi kestää jopa vuorokausia, jolloin haavoittuvuudet ovat hyökkääjien käytettävissä (Yoo 2021). Ennen korjaavien päivityksien asentamista SOC voi kuitenkin havaita kyseisiä haavoittuvuuksien käyttöjä jo alkuvaiheessa ja estää haitallisten toimijoiden pääsyn suojattavaan verkkoon.

Ilman SOC-palvelua kyberrikollisten toteuttamat hyökkäykset voivat pysyä piilossa pitkään, koska yrityksillä ei tällöin ole kykyä ja resursseja havaita uhkia ja reagoida niihin ajoissa (Why is a soc (Security Operations Center) essential today? 2020). Esimerkkinä pitkään tapahtuneesta kyberhyökkäyksestä on verkkopalvelu *Yahoo* vastaan toteutettu isku vuonna 2014 jossa varastettiin noin 500 miljoonan käyttäjän tietoja. Vaikka Yahoo tietojen mukaan tiesi hyökkäyksestä, ei se kuitenkaan alkuvaiheessa ymmärtänyt hyökkäyksen laajuutta ja ensimmäiset tiedot tapahtuneesta kyberhyökkäyksestä tuotiin julkisuuteen vasta vuonna 2016. Tapahtuneesta on epäilty muun muassa, että yrityksellä kesti yli kaksi vuotta huomata tietomurron laajuus. (Redfren 2021 & Volz 2016.)

3.3.1 SOC:in toimintatavat

Security Operation Center toimii aina tiiminä ja se vaatii useamman henkilön toimiakseen riittävän tehokkaasti. Tyypillinen SOC on jaettu henkilöstön osalta 4 eri osaan, joita usein kutsutaan tasoiksi. Tasot on numeroitu välillä 1–4 ja jokaisella tasolla on oma tehtävänsä SOC-toiminnassa. Tämä ei kuitenkaan ole ainoa mahdollinen toimintamalli, vaan henkilöstön ja valvottavien ympäristöjen lukumäärä vaikuttaa oleellisesti toimivaan malliin (Zimmerman 2014, 53-57.). Oikeanlaisella rakenteella saadaan toiminta tehokkaaksi ja tietoturvapoikkeamat pystytään tunnistamaan ja niihin voidaan reagoida tarvittavilla toimenpiteillä oikeassa vaiheessa. (Torres 2015, 4.)

Tietoturvauhat havaitaan SOC:issa usein tietoturvaherätteistä, jotka ovat tietoteknisten automaatioprosessien tuottamia havaintoja epäilyttävistä toimista IT-infrastruktuurissa. Näitä tietoturvaherätteitä valvotaan ja kategorisoidaan SOC:issa tasolla 1 toimivien tietoturva-analyytikkojen toimesta. Kattavasta tietoturvaherätteestä analyytikolle selviää mitä epäilyttävää toimintaa se on havainnut ja tarvittavat tunnistetiedot, kuten esimerkiksi IP-osoitteet, on järkevää ilmoittaa jo tässä yhteydessä. Tämän perusteella analyytikko kykenee tiedostamaan miten ja mistä tapahtumaa voi tutkia tarkemmin ja sulkea pois mahdollisen väärän hälytyksen. Havaituista tietoturvatapahtumista on syytä myös kirjata tarvittavat tiedot talteen, jonka tason 1 analyytikko voi tehdä esimerkiksi tikettityökalua hyödyntäen. Tiketille voidaan kirjata mikä tietoturvapoikkeama on havaittu, mihin aikaan se on havaittu sekä tarvittavat tunnistetiedot mitkä herätteestä ja SIEM-järjestelmien kautta on saatu selville. Kuvion 8 avulla selitetään prosessin kulkua myös tasolla 2 toimivalle kokeneemmalle analyytikolle. (Torres 2015, 4.)

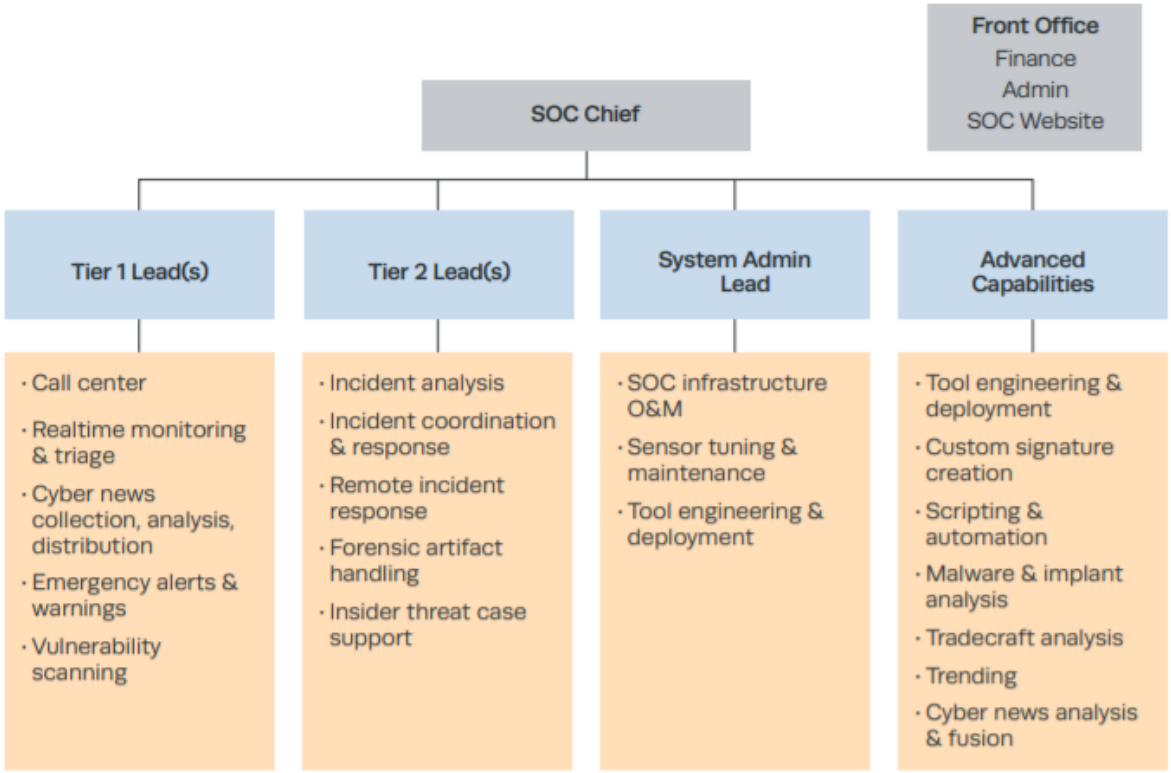


Kuvio 8. Tietoturvapoikkeaman eskalointi (Zimmerman 2014, 25)

Tietoturvapoikkeamaa analysoidaan tarkemmin tasolla 2 toimivan analyytikon toimesta. Hänellä on usein laajempi kokemus tietoturvatehtävissä toimimisesta. Analyytikko määrittelee kuinka suurelle osalle järjestelmästä tai sen sisältävästä datasta poikkeama on vaikuttanut. Tarvittavat korjaustoimenpiteet uusien ongelmien estämiseksi tehdään tai ohjeistukset niiden suorittamiseen annetaan tason 2 analyytikon toimesta. Tarvittaessa analyytikko myös konsultoi järjestelmän omistajaa tai hallinnoijaa kuvion 8 mukaisesti, erityisesti jos kyseessä on MSSP palvelulla tuotettu SOC. (Torres 2015, 4.)

Tasolla 3 toimivat teknisesti usein kaikkein kokeneimmat henkilöt, jotka ovat usein mukana isoissa yrityksen tai yhteisön liiketoimintaa vaarantavissa tapauksissa. Analyytikot voivat myös ennakoivasti suorittavat ja valvovat penetraatiotestausta, jonka avulla pyritään tunnistamaan ennen hyväksikäyttöä tietoturvaongelmat sekä haavoittuvuudet. Tällä tasolla analyytikot tutkivat myös jo tapahtuneita tietoturvaloukkauksia ja haavoittuvuuksien hyväksikäyttöjä. Sen tutkimiseen tarvitaan osaamista muun muassa digitaalisesta forensiikasta sekä haittaohjelmien analysointityökaluista ja tekniikoista. (Vielberth, Böhm, Fichtinger & Pernul 2020; Torres 2015, 4.)

Kaikkien tasojen valvonnasta ja päivittäisestä ohjauksesta SOC-tiimissä vastaa tiiminvetäjä, joka toimii tasolla 4. Tiiminvetäjä vastaa SOC-toiminnassa henkilöstöresursseista ja strategiasta, jotta SOC kykenee pääsemään tavoitteisiinsa ja suuntautumaan oikein. Tiiminvetäjä myös kommunikoi ylemmän johdon kanssa ja välittää tilannetietoa tarvittaessa SOC:in sidosryhmille. SOC-managerin tehtävänkuvaan sisältyy myös prosessien arvioiminen ja kehittäminen sekä samalla tiimin taloudellisien näkökulmien huomioiminen. (Vielberth, Böhm, Fichtinger & Pernul 2020; Torres 2015, 4.) Tarkemmin SOC-toimintaa kuvataan kuviossa 9, joka on esimerkki keskitason SOC-toiminnasta.



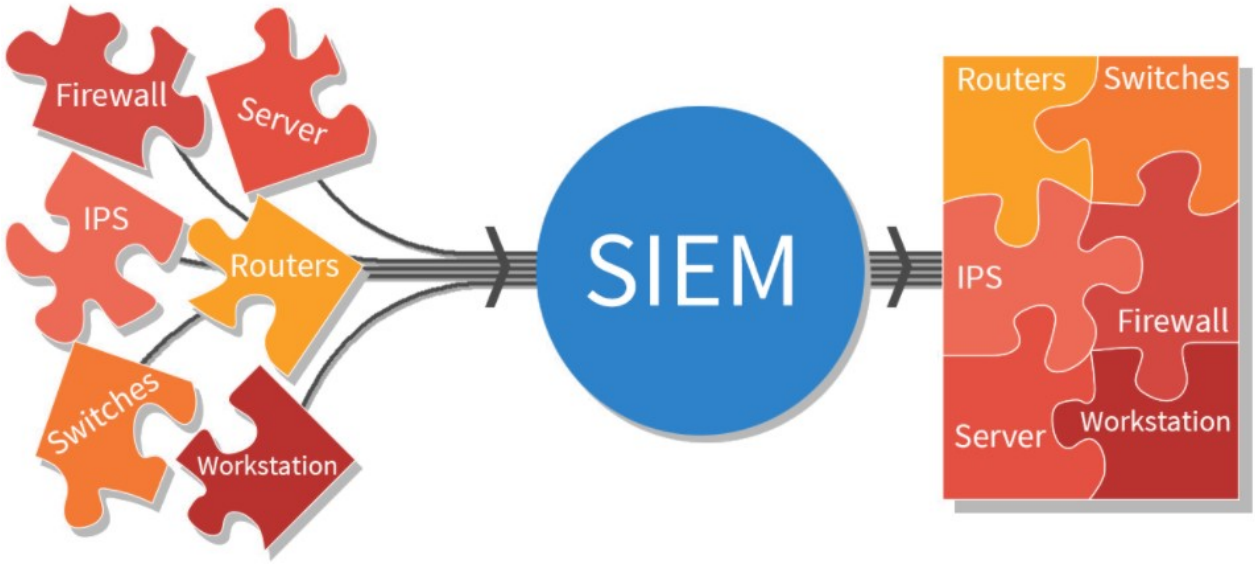
Kuvio 9. Esimerkki keskikokoisesta SOC-toiminnasta (Zimmerman 2014, 55)

Kaupallinen SOC-toiminta perustuu pääosin palvelutasosopimukseen eli SLA-sopimukseen (engl. Service Level Agreement). Sopimuksessa määritetään asiakkaan sekä palvelutuottajan välillä kaikki tarvittavat näkökohdat palvelun toimintaan, joita ovat esimerkiksi palvelun laatu, saatavuus sekä vastuut molemmilla osapuolilla. Palvelutasosopimuksessa määritellään usein myös vasteajat, jonka kuluessa SOC reagoi tietoturvapoikkeamiin sekä minkä kuluessa SOC:in on tuotettava asiakkaalle selvitys mahdollisesta tietoturvaloukkauksesta. Sopimuksen perusteella määritetään myös palveluajat, jonka perusteella SOC-toimintaa tuotetaan. Palveluajat voivat olla esimerkiksi viikkomallien (tunnit *x* vuorokaudet) 8x5, 12x5, 12x5 lisättynä 8x2 tai 24x7 mukaisia. Usein pienemmissä SOC-toimintaa tuottavissa organisaatioissa ei ympärivuorokautinen toiminta ole mahdollista ja toimenpiteitä suoritetaan 8x5 mallin mukaisesti. Tämä vaarantaa yrityksen toimintaa erityisesti viikonloppujen aikana, kun vasteajat kasvavat muutamien vuorokausien pituisiksi, kun taas parhaimmillaan hyökkääjille riittää muutama tunti aikaa suorittaa tarvittavat toimenpiteet. 24x7, eli keskeytymättömällä ympärivuorokautisella valvonnalla kyseinen uhkatekijä voidaan poistaa, kun vasteajat ovat pieniä, mutta vastaavasti 24x7 toimintaan siirtyminen on vastaavasti kalliimpaa organisaatiolle. 12x5 malli toimii arkipäiväisen ja ympärivuorokautisen mallin välimuotona, jolloin valvontaa jatketaan ilta-aikaan ja mahdollisesti osittain viikonloppuisin, mutta keskeytetään kokonaan yön ajaksi. Kyseinen toimintatapa säästää organisaation kustannuksissa, kun työntekijöiden ei tarvitse olla yöllä töissä, joka on organisaatiolle hinnakkaampaa. (Hiles, FBCI & EloSCM 2016; Zimmerman 2014, 291-294.)

3.3.2 SOC:in työkalut

Security Operation Center toiminnassa työkaluilla on merkittävä rooli, jotta toimintaa voidaan toteuttaa tehokkaasti. Työkaluina SOC-ympäristössä käytetään verkkolaitteiden valvontaan ja hallintaan tarkoitettuja ohjelmia, joilla jokaisella on pääkäyttötarkoitus. Esimerkiksi palomuurilla voidaan tallettaa ja tarkastella raakamuodossa yksittäisiä paketteja mitkä kulkevat sen läpi, kun taas edistyneemmät automaatiotyökalut, kuten esimerkiksi Network Traffic Analysis (NTA) -työkalut, analysoivat läpi kulkevaa verkkoliikennettä ja yhdistävät raakalokin tiedonpalasia yhteen muodostaen yhtenäisen poikkeamahavainnon. Analysoitava datan määrä riippuu verkkoinfrastruktuurin koosta ja voivat sen perusteella vaihdella todella suuresti, jolloin automaatiotyökalut ovat välttämätön apu analyytikon työskentelyssä. (Zimmerman 2014, 32-35.; The Modern Security Operations Center, SecOps and SIEM: How They Work Together n.d.)

SOC:in yksi tärkeimmistä työkaluista on kuitenkin nimeltään SIEM (Security Information and Event Management). Sen toiminta perustuu datavirtojen yhtenäistämiseen, kun kaikista ulkoisista lähteistä tuleva erimuotoinen data kerätään, suodatetaan, tallennetaan, lajitellaan sekä korreloidaan näyttäen tietoturvan kannalta merkityksellisiä tiedot sekä reaaliajassa että historiallisessa muodossa tarvittavaa tarkastelua ja analysointia varten. SIEM:in lisätoimintojen avulla voidaan rikastaa kerättyä dataa ja muuttaa se SOC:in tason 2 analyytikolle raportoinnin kannalta tarvittavaan muotoon ja tason 1 analyytikolle hälytyksen tutkimiseen ja eskalointiin tarvittavaan muotoon. SIEM:in lokilähteisiin on analyytikon kannalta optimaalisinta liittää kaikki tarvittavat järjestelmät, jolloin ne ovat tiedon hakemisen kannalta yhdessä keskitetyssä paikassa. Tätä kuvataan kuvion 10 avulla. (Zimmerman 2014, 154.; Vielberth, Böhm, Fichtinger & Pernul 2020.)



Kuvio 10. SIEM-järjestelmän merkitys tiedon yhdistämisessä (Security Information and Event Management system. N.d.)

SIEM-järjestelmiä tuottaa useita eri kaupallisia yrityksiä, mutta niiden toiminta perustuu poikkeuksetta samanlaiseen ideologiaan: Ne ovat ohjelmistopohjaisesti rakennettuja työkaluja, jotka päätarkoituksellisesti tuottavat käyttökelpoisia verkkoliikenteen ja IT-infrastruktuurin näkymiä turvallisuustiimeille. Valvontaa voidaan toteuttaa esimerkiksi erilaisten koostettujen hallintanäkymien (engl. dashboard) kautta, jolloin lokitapahtumien kokonaiskuvaa voidaan pitää keskitetysti yllä. SIEM-järjestelmät voidaan toteuttaa paikallisesti omalla palvelimella tai pilvipalveluratkaisulla. (Gast 2021; Zimmerman 2014, 154-156; SIEM Architecture: Technology, Process and Data n.d.)

Ensimmäiset SIEM-järjestelmät ovat tulleet markkinoille 2000-luvun alkuvaiheessa, ja ne ovat kehittyneet ajan kuluessa uusien sukupolvien järjestelmiksi (Gast 2021). Nykypäivän SIEM-ratkaisut ovat kehittyneet erityisesti kasvavan datamäärän käsittelyssä sekä uhkakuvien monimutkaisuuden hallinnassa. Pilvikäyttöönoton, mobiiliteknologioiden, hybridipalvelinkeskusten ja etätyöskentelyn lisääntyessä seuraavan sukupolven SIEM-järjestelmät tulevat tarjoamaan uusia ominaisuuksia turvallisuuden näkyvyyden ja uhkien havaitsemisen parantamiseen ja samalla virtaviivaistavat tietoturvatiimien prosessia työtaakan hallintaan automatisoinnin avulla. (Gast 2021; SIEM Architecture: Technology, Process and Data n.d.)

Verkkoliikenteen analyysia varten SOC pystyy hyödyntämään myös Network Traffic Analysis (NTA) työkaluja. SOC kykenee tämän avulla tarkastelemaan verkkoliikennettä ja analysoimaan verkon sisällä tapahtuvia toimia, tehden hyökkäyshavaintoja laitteilta ja sovelluksilta, joita on muuten hankala varustaa valvottavaksi. NTA-ratkaisut käyttävät koneoppimisen ja käyttäytymisanalytiikan yhdistelmää luodakseen lähtötilanteen, joka kuvastaa sitä, miltä organisaation normaali verkkokäyttäytyminen näyttää. Kun epätavallisia liikennemalleja tai epäsäännöllisiä verkkotoimintoja havaitaan, nämä työkalut varoittavat tietoturvatiimiä mahdollisesta uhasta. (What Is Network Traffic Analysis? n.d.)

SOC hyötyy NTA-työkalujen valvonnasta yrityksen rajan ylittävän pitkittäisliikenteen seurannan lisäksi poikittaisliikenteen valvonnasta, eli yrityksen verkon laitteiden välillä, analysoimalla verkkoliikennettä tai virtaustietoja. NTA-ratkaisun avulla nähdään, kuinka uhka on siirtynyt sivusuunnassa organisaation sisällä antaen SOC:in nähdä, mitkä muut laitteet voivat olla saastuneet. (What Is Network Traffic Analysis? n.d.)

Loppukäyttäjien työasemia sekä yksittäisten päätelaitteiden valvonnassa voidaan hyödyntää Endpoint Protection Platform (EPP) -ratkaisua, joka on tiedostomuotoisten haittaohjelmien torjuntaan sekä haitallisen toiminnan suorittamisen havaitsemiseen käytetty ohjelmisto. EPP-ratkaisujen etu on, että tietoturvavalvomo saa näkyvyyden päätelaitteille ja kykenee näkemään hyvin yksityiskohtaisesti työaseman toimintaa. SOC voi esimerkiksi valvoa käynnissä olevia prosesseja, verkkoyhteyksiä sekä tiedostojen muutoksia, ja epätavallisista löydöksistä EPP-ohjelma aiheuttaa tietoturvaherätteen SOC-valvomolle. Tyypillisen EPP-ratkaisun mekanismi päätelaitteiden suojaamisessa perustuu verrata tietokantaan jo tallennettujen uhkien allekirjoituksia (engl. hash)

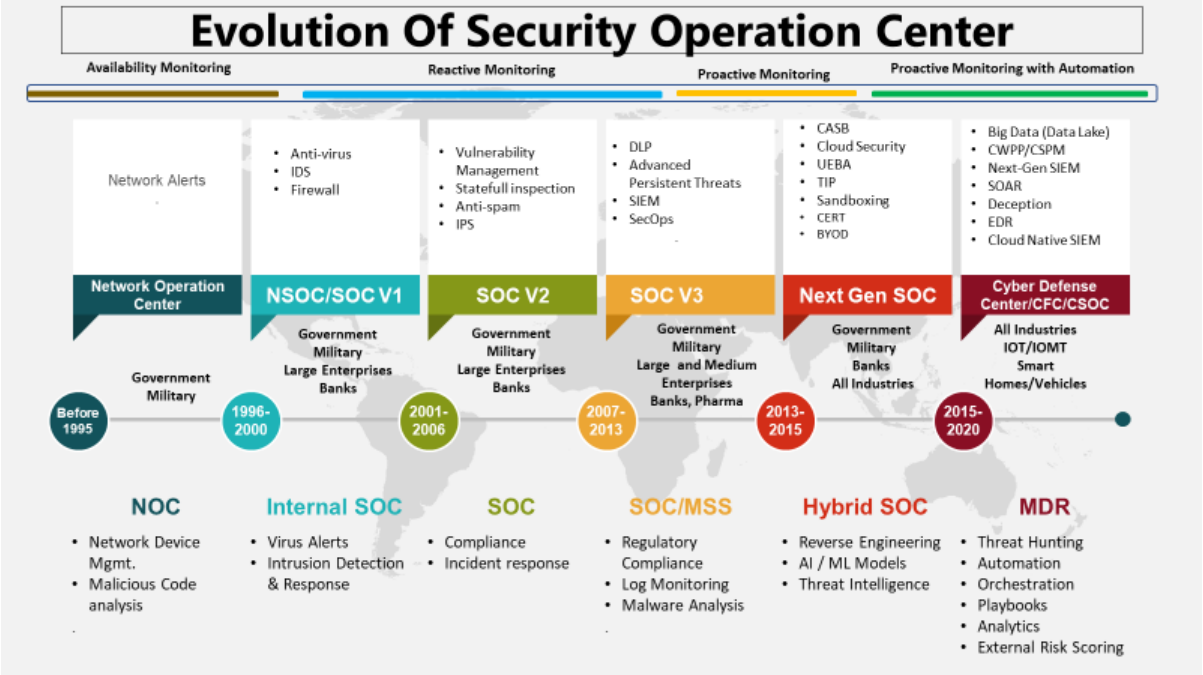
sekä tarkistettavan tiedoston allekirjoituksia, jonka avulla voidaan määrittää, onko suoritettava tiedosto haitallinen vai ei. (Chandel, Yu, Yitian, Zhili & Yusheng 2019; Endpoint Security n.d.)

Tunkeutumisen havainnointijärjestelmä (IDS) on myös yleisesti käytetty tietoturvateknologia, joka on SOC-toiminnassa hyödyllinen ohjelmisto, joka on kehitetty automatisoimaan tunkeutumisen havaitsemisprosessin. Tätä on laajennettu tunkeutumisen estojärjestelmäksi (IPS), jolla on kaikki tunkeutumisen havaitsemisjärjestelmän ominaisuudet, mutta se kykenee myös pysäyttää mahdolliset tapahtumat. IPS-tuotetta voidaan halutessa käyttää myös vain IDS-järjestelmänä, poistamalla käytöstä estoprosessiin liittyvät toimet. IDS-järjestelmä kykenee esimerkiksi havainnoimaan luotujen sääntöjen pohjalta, jos päätelaitteen käyttäjä yrittää muodostaa yhteyden valvottuun järjestelmään johon käyttäjällä ei olisi normaalitilanteessa lupaa päästä. (Scarfone & Mell 2007, 2-1.)

3.3.3 SOC-toimijat

SOC-toiminta on kehittynyt vuosien aikana hyvin erilaiseksi, ja ensimmäiset SOC-toiminnat maailmalla ovat olleet pienemmässä mittakaavassa kuin nykypäivän SOC-toiminta. Eriytettyjä SOC-toimijoita alettiin kehittämään 2000-luvun vaihteessa, ja aluksi ne toteutettiin valtion ja puolustusalan organisaatioille ja sen päävastuu oli virushälytysten, tunkeutumisen havainnoinnin ja reagoinnin käsittely. Vuoden 2000 jälkeen valvontatoimintaa toteutettiin myös suurille yrityksille ja pankeille valtio- ja sotilasjärjestöjen lisäksi. (Kaliyaperumal 2020.)

Erityisesti vuosien 2007–2013 välillä SOC-toiminta kehittyi suuressa mittakaavassa ja teki muodonmuutosta kohti nykypäivän toimintaa. Kyberturvallisuuden ekosysteemiin tuli monia tärkeitä tietoturvaratkaisuja, jotka ovat avainasemassa turvallisuuden seurannassa, kuten esimerkiksi SIEM-työkalut. Edistynyt pysyvä hyökkäystoiminta, eli APT-toiminta, saavutti huippunsa tänä aikana, ja SOC:illa oli tärkeä rooli APT-toimijoiden havaitsemisessa ja ehkäisemisessä. Lokien yhdistäminen, säännösten noudattaminen, haittaohjelmien analysointi ja tietovuotojen valvonta ovat tietoturvatoimintojen keskeisiä tavoitteita tänä aikana. Nykypäivien SOC-toimintaan on otettu mukaan enemmän automaatiota sekä pilvipalveluratkaisuja, jolloin uhkakuvat ovat muuttuneet myös laajemmiksi. Kehitystä kuvataan tarkemmin kuvion 11 avulla. (Kaliyaperumal 2020.)



Kuvio 11. Security Operations Center-toiminnan kehitys (Kaliyaperumal 2020)

SOC-toimijoita on maailmalla useita ja ala on ollut suuressa kasvussa viime vuosien aikana. Maailmalla erityisesti suuret sekä globaalit IT- ja teknologiayhtiöt hallitsevat tällä hetkellä SOC-toimintaa MSSP-palveluitansa hyödyntäen, joista suurin osa on perustettu sekä aloittanut toimintansa jo ennen SOC-toiminnan kehittymistä kuvion 11 mukaisesti ”SOC V3”-tasolle. Kyseiset yritykset työllistävät useita tuhansia henkilöitä ja huomattavan suuri osa yhtiöistä on lähtöisin Pohjois-Amerikassa tai pitää kotipaikkaansa siellä. (Top 15 Best Managed Security Service Providers (MSSPs) In 2022 2022)

Suomessa SOC-toimintaa pitää tällä hetkellä yllä keskikokoiset- ja suuryritykset. Näistä osa on keskittynyt pelkästään tietoturvaan, kun taas osa yrityksistä tarjoaa kokonaisia keskitettyjä IT-ratkaisuja. Suurista globaaleista yrityksistä *Accenture* harjoittaa toimintaa myös Suomessa tarjoten kyberturvallisuuspalveluita. SOC-toimintaa Suomessa tuottaa ainakin seuraavan luettelon kaupalliset toimijat (List of SOC service providers 2021):

- Accenture
- CGI
- Cinia
- DNA
- Elisa

- Enfo
- Fiarone
- Fujitsu
- Insta
- Loihde
- Nixu
- Telia Cygate
- TietoEVRY

3.3.4 SOC-toiminnan haasteet

Valvottavien ympäristöjen kiihtyvässä kasvussa automatisoinnin rooli SOC:in tietoturva-analyytikolle tulee olemaan entistä tärkeämmässä roolissa. Nykypäivän käytössä olevien kehittyneiden ja uusien työkalujen ansiosta automatisointi kykenee optimaalisessa tilanteessa hoitamaan suurimman osan tietoturvapoikkeamista ilman, että ihmisen tarvitsee tehdä konkreettisia toimenpiteitä. Nämä toimenpiteet eivät kuitenkaan ole onnistuneet pitämään työkuormaa tietoturva-analyytikoilla samassa suhteessa kasvavien järjestelmien kanssa. (Kaliyaperumal 2020.)

Trend Micron julkaiseman raportin mukaan kuitenkin 54 % maailmalla toimivista tietoturvahallintakeskuksista sekä tietoturvatiimeistä kärsivät ylikuormituksesta tietoturvahälytysten liiallisesta määrästä johtuen. Lisäksi 68 % suomalaisista SOC-ylläpitäjistä tunnustaa, etteivät he ole varmoja kyvyistään priorisoida ja käsitellä hälytyksiä. Tutkimuksen mukaan tämä on enemmän kuin muualla maailmassa, sillä kansainvälisellä tasolla saman ongelman kokee 55 % vastaajista. Tutkimuksen perusteella voidaan todeta, että automatisointia ei tehdä oikein toimenpitein tai riittävän tehokkaasti. (Security Operations on the backfoot 2021; 81 % suomalaisista tietoturva-asiantuntijoista ylikuormittuu vääristä hälytyksistä 2021.)

Tietoturva-analyytikot joutuvat päivittäisen työn aikana vaihtamaan useiden järjestelmien sekä hallintakonsoleiden välillä tutkiakseen sekä reagoidakseen tapauksiin. Resurssien kouluttaminen useisiin teknologioihin lyhyessä ajassa koetaan myös haasteelliseksi. Tietoturvahäiriöiden ohjekirjojen dokumentointi ja päivittäminen sekä ajan tasalla olevan tietokannan ylläpitäminen ovat avainasemassa kaikissa turvallisuustoimintokeskuksissa, jotka vaativat paljon ihmistyötä. Kuviossa 12 listataan tarkemmin ongelmakohtia SOC-toiminnassa. (Kaliyaperumal 2020.)

Kuvio 12. Security Operations Centerin haasteet (Kaliyaperumal 2020)

4 Kiristyshaittaohjelma – isku yhteiskuntaa vastaan

Kiristyshaittaohjelmien hyökkäykset vaikuttavat yhteiskunnan toimivuuteen ja aiheuttavat harmia sekä ongelmia ihmisten arkeen pysäyttämällä kriittisten tietojärjestelmien toimivuuden. Pahimmissa tapauksissa oikein kohdistetut ja tarpeeksi laajat kiristyshaittaohjelmahyökkäykset kykenevät lamauttamaan yhteiskunnan, tai esimerkiksi valtion, selviytymiseen sekä toimivuuteen vaikuttavat toimialat aiheuttaen kriisin yhteisön sisällä. Myös yksittäiselle yritykselle kiristyshaittaohjelman aiheuttama ongelma on myös yritykselle itsessään jo kriisi, sillä se vaarantaa yrityksen tulevaisuuden, kun sisäiseen tietoon on päässyt ulkopuolinen taho käsiksi. Kiristyshaittaohjelman hyökkäyksen havaitseminen paljastaa uhrille välittömästi, että heidän tietoturvansa on pettänyt jollain tasolla eikä heidän IT-infrastruktuurinsa ole enää turvallinen.

Kyberuhista ja -hyökkäyksistä kertovan arkipäivän uutisoinnin määrän kasvu mediassa ja sen seurauksena myös kiristyshaittaohjelmia hyödyntävät hyökkäykset ovat nousseet mediassa suuremmin esille niiden seurauksien vuoksi. Esimerkkinä Saksassa vuonna 2020 uutisoitu tapaus, jossa sairaalaan matkalla ollut potilas kuoli sairaalan toiminnan lamauttaneen kiristyshaittaohjelman seurauksena, aiheutti maailmalla laajaa uutisointia ja poliisin suorittaman henkirikostutkinnan

(Heikkilä 2020). Usein uutisoinnissa hyökkäyksien seurauksia korostetaan eikä teknisestä taustaa tuoda esille kovin tarkasti. Toisaalta vakavien seurauksien esille tuonnilla voi olla tulevaisuudessa tietoturvaa parantava vaikutus, kun hyökkäysten estämiseksi sekä IT-järjestelmien suojaamiseen käytetään enemmän huomiota sekä resursseja. Seurauksista lukemalla median lukija kykenee pohtimaan mitä kiristyshaittaohjelman aiheuttamat tuhot merkitsisivät toimintaan yksilö- tai yritystasolla.

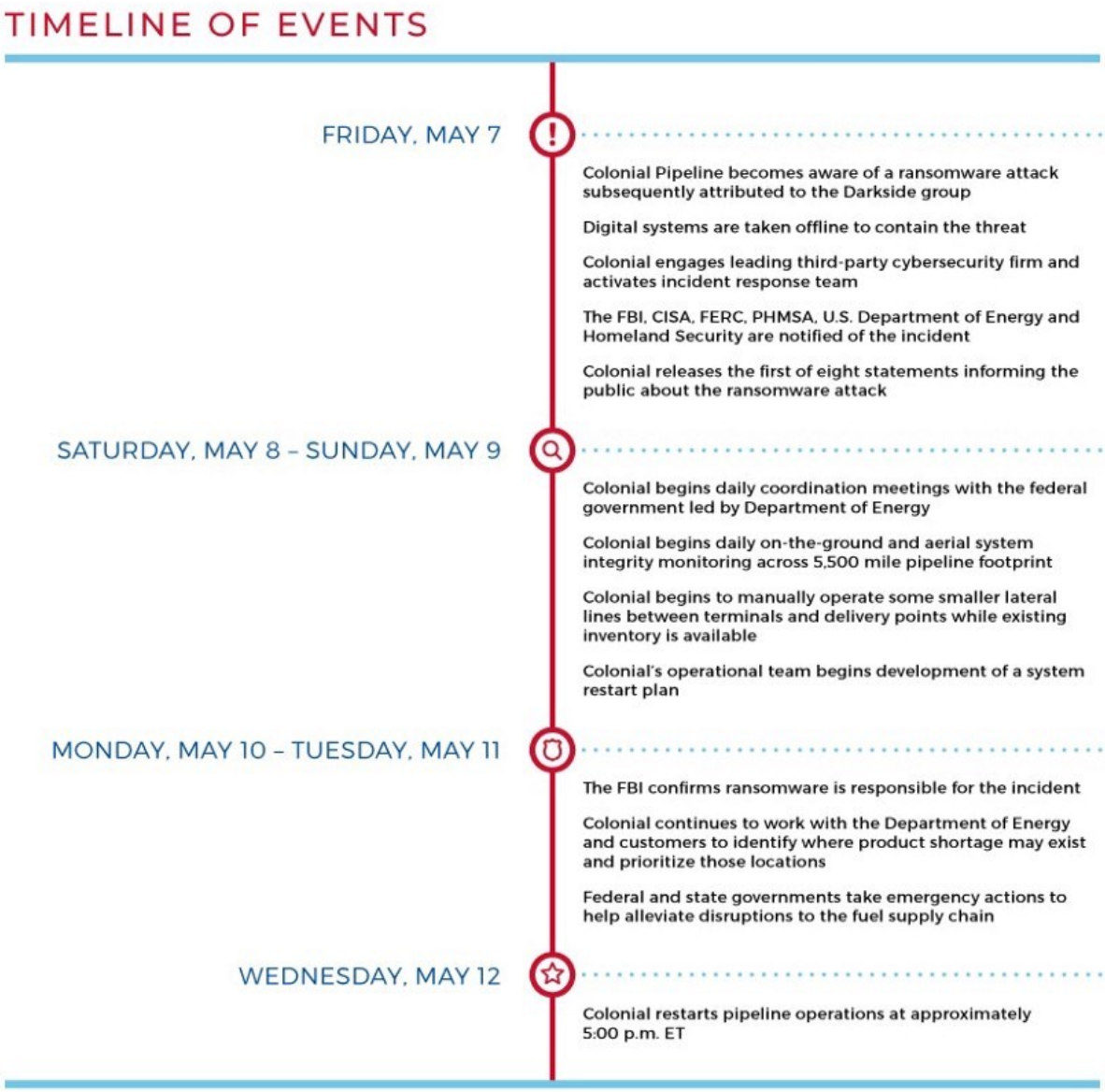
4.1 Kiristyshaittaohjelmahyökkäykset viime aikoina – Case Colonial Pipeline

Pelkästään vuoden 2021 aikana maailmalla on raportoitu useita suuriksi luokiteltuja kiristyshaittaohjelmia hyödyntäviä kyberhyökkäyksiä. Hyökkäyksen kohdistuessa suureen yritykseen ovat nämä pahimmillaan lamauttaneet koko toiminnan sekä aiheuttaneen globaaleja ongelmia välillisesti. Yhtenä myös kansanvälisesti suurena tarkasteltu hyökkäys tapahtui toukokuussa 2021, jolloin Yhdysvaltalainen *Colonial Pipeline* joutui kiristyshaittaohjelman uhriksi. Kyseessä on amerikkalainen öljyputkijärjestelmä, joka kuljettaa bensiiniä ja lentopolttoainetta Texasista pääasiassa Kaakkois-Yhdysvaltoihin. Hyökkäys vaikutti yrityksen putkilinjaa hallinnoiviin tietokoneisiin, jolloin Colonial Pipeline joutui pysäyttämään kaikki putkilinjaston toiminnan hyökkäyksen torjumiseksi. (Bing & Kelly 2021; Segers 2021.)

Hyökkäyksen epäillyksi pystyttiin poliisitutkinnan aikana nimeämään nopealla aikataululla *Darkside* niminen ryhmittymä. Kyseinen ryhmittymä vaati Colonial Pipeline:lta lunnaiksi noin 4,4 miljoonan Yhdysvaltain dollarin vastaavaa määrää bitcoin kryptovaluuttaa. Yritys maksoi muutaman tunnin kuluessa vaaditut lunnaat ryhmittymälle, jolloin Darkside toimitti Colonial Pipeline:lle purkutyökalun järjestelmän palauttamiseksi. Kyseisen työkalun salauksen käsittelyaika todettiin kuitenkin erittäin pitkäksi, jotta tuotanto saataisiin riittävän ajoissa toimintaan ongelmien välttämiseksi. (Jacobs, Riley & Turton 2021.) Tämän seurauksena Yhdysvaltain liikenneministeriön alaisuudessa toimiva FMCSA joutui antamaan alueellisen hätäjulistuksen 17 osavaltiolle ja Yhdysvaltain pääkaupungille polttoaineen syöttölinjojen pitämiseksi auki (Falconer 2021).

CNN artikkeliin perustuen (2021) polttoaineen jakelun keskeyttämisen syynä oli kuitenkin laskutusjärjestelmän vaarantuminen. Yrityksessä oltiin huolissaan siitä, etteivät he pystyisi jälkikäteen selvittämään, kuinka paljon heidän pitäisi laskuttaa asiakkaitaan saamastaan polttoaineesta. Artikkelin väitteen mukaan laskutusjärjestelmä on keskeisessä roolissa putkilinjan esteettömän toiminnan

kannalta. Colonial Pipeline ei kuitenkaan myöntänyt tätä lehdelle vaan ilmoitti, että yritys on ennakoivasti sulkenut tietyt järjestelmät uhan hillitsemiseksi. (Bertrand, Perez, Cohen, Sands & Campbell 2021.) Colonial Pipelinen tapauksen kulkua ajallisesti kuvataan kuvion 13 avulla.



Kuvio 13. Colonial Pipeline hyökkäyksen aikajana (Enn 2021)

4.1.1 Syitä hyökkäyksen onnistumiseen

Kyberhyökkäyksissä tyypilliseen tapaan uhri harvoin viestittää ulospäin varsinaisia syitä miksi hyökkäys on onnistunut ja mitkä tekijät siihen ovat johtaneet. Yritysten sisällä tällaiset tapahtumat kuitenkin halutaan usein selvittää perusteellisesti, jotta niiltä voidaan jatkossa välttyä sekä kehittää oman IT-ympäristön tietoturvaa. Hyökkäyksen uhriksi joutunut voi pyytää tapauksen selvittämiseen myös ulkopuolista konsultaatioapua tietoturvaan perehtyneiltä kaupallisilta toimijoilta. Kyseinen toiminta kutsutaan digitaalisen forensiikaksi sekä tietoturvaloukkausten selvitykseksi (DFIR).

Colonial Pipelinen tapauksessa yhtiön toimitusjohtaja kommentoi julkisesti noin kuukausi hyökkäyksen jälkeen tapahtuman syitä. Colonial Pipeline -toimitusjohtaja kertoi Yhdysvaltain senaatin komitealle, että hyökkäys tapahtui käyttämällä vanhaa VPN-järjestelmää (Virtual Private Network), jossa ei ollut käytössä monivaiheista tunnistautumista (MFA). Tämä tarkoittaa, että sitä voi käyttää salasanalla ilman toista vaihetta, kuten tekstiviestiä, jossa käyttäjä autentikoidaan salasanan syöttämisen jälkeen. Lausunnossa ei tuotu esille, miten salasana on saatu hyökkääjien haltuun, mutta hänen mukaansa salasana on ollut riittävän monimutkainen eikä helposti arvattavissa. (Kelly & Resnick-ault 2021.)

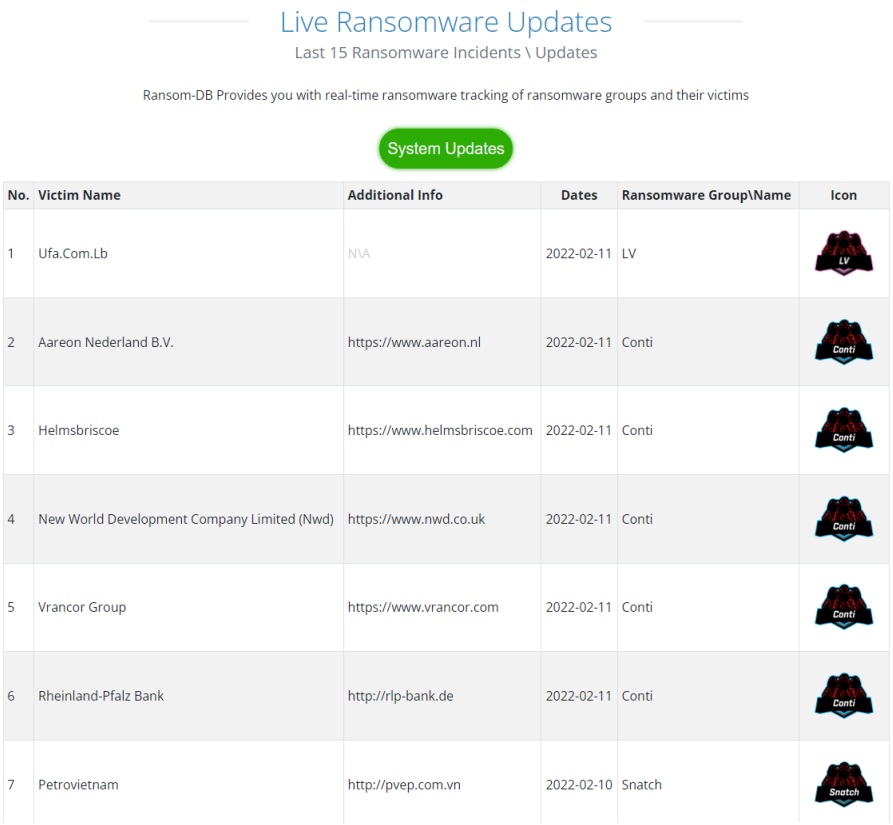
MFA-protokollan käyttöä suositellaan nykypäivänä laajasti, ja on ilmeistä, että sen käyttämättä jättämisellä Colonial Pipelinen VPN-järjestelmässä on ollut merkittävä tekijä, joka on mahdollistanut hyökkäyksen. Salasanan haltuun saaminen hyökkääjälle on ollut mahdollista esimerkiksi väsytyshyökkäyksen (engl. Brute Force) avulla, joka tehokkaalla ja optimoidulla algoritmin avulla suoritettuna mahdollistaa haastavien salasanojenkin murtamisen kohtuullisessa ajassa. Aktiivinen Brute Force -toiminta on kuitenkin myös mahdollista havaita esimerkiksi SOC-palvelutuottajan käytössä olevilla työkaluilla.

4.2 Aktiiviset hyökkäykset ja nykytila

Aktiivisten kiristyshaittaohjelmahyökkäysten ryhmittymät voivat vaihdella nopeasti, eikä yksittäinen hyökkäyksiä toteuttava ryhmittymä välttämättä halua olla koko ajan esillä. Ryhmittymien aktiivisuuteen vaikuttaa muun muassa poliittiset tilanteet sekä hyökkääjien omat intressit. Esimerkiksi kriittisiä infrastruktuureja vastaan hyökkäävät ryhmittymät voivat herättää kielteisiä tunteita

muissa ryhmittymissä tai jopa valtiollisissa toimijoissa, jolloin alkuperäisen hyökkäyksen aloittanutta ryhmittymää vastaan voidaan kohdistaa aggressiivisia toimia. Venäjältä käsin toimivaa REvil-ryhmittymää vastaan toteutettiin vastaavia toimia syksyllä 2021 valtiollisesti johdettuna, kun REvil-ryhmittymän palvelimia kaapattiin vastahyökkäyksessä haltuun (Virtanen 2021).

Tuoreimmista kiristyshaittaohjelmista kertovista hyökkäyksistä leviää yleisesti ottaen aluksi tietoa pimeän verkon kautta, jossa keskustelu tapahtuu teknisesti ja käytännöllisesti anonyymisti. Tämä tarjoaa hyökkääjille mahdollisuuden esimerkiksi myydä varastamia tietojaan tai muuten vain jakaa sitä. (Freed 2021.) Internetissä toimii myös kolmansien osapuolien ylläpitämiä sivustoja, joihin listataan aktiivisesti hyvin pienellä viiveellä tapahtuneita kiristyshaittaohjelmaiskuja sekä aktiivisia ryhmittymiä. Kyseiset sivustot voivat kerätä tietoa esimerkiksi pimeän verkon kautta tai käyttäjät voivat itse ilmoittaa sivustolla hyökkäyksiä. Tällainen on esimerkiksi ”Ransomware Database” niminen sivusto, joka raportoi tietoja aktiivisesti. Viimeaikaisista hyökkäyksistä on esimerkki kuviossa 14 ja kuviossa 15 tuodaan esille aktiivisia toimijoita.



Live Ransomware Updates

Last 15 Ransomware Incidents \ Updates

Ransom-DB Provides you with real-time ransomware tracking of ransomware groups and their victims

System Updates

No.	Victim Name	Additional Info	Dates	Ransomware Group\Name	Icon
1	Ufa.Com.Lb	N\A	2022-02-11	LV	
2	Aareon Nederland B.V.	https://www.aareon.nl	2022-02-11	Conti	
3	Helmsbriscoe	https://www.helmsbriscoe.com	2022-02-11	Conti	
4	New World Development Company Limited (Nwd)	https://www.nwd.co.uk	2022-02-11	Conti	
5	Vrancor Group	https://www.vrancor.com	2022-02-11	Conti	
6	Rheinland-Pfalz Bank	http://rlp-bank.de	2022-02-11	Conti	
7	Petrovietnam	http://pvep.com.vn	2022-02-10	Snatch	

Kuvio 14. Aktiivisia viimeaikaisia kiristyshaittaohjelmahyökkäyksiä (Live Ransomware Updates n.d.)

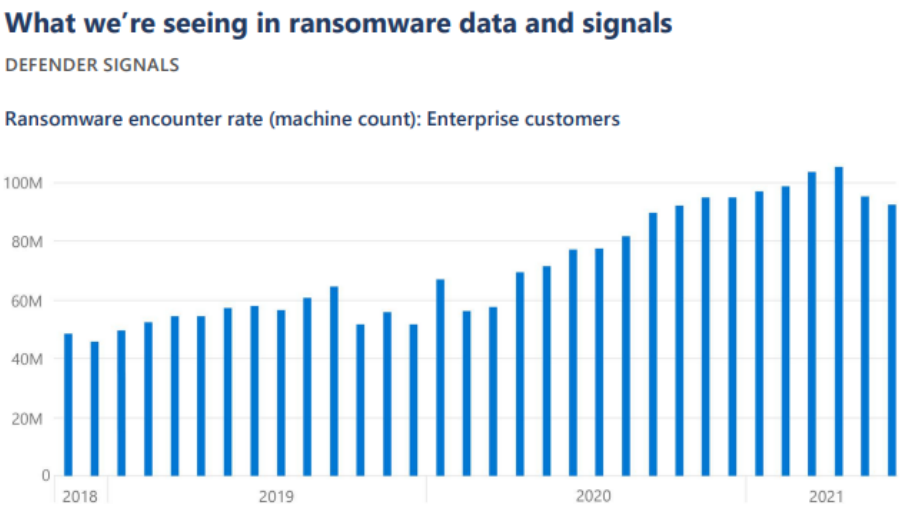
Ransomware Groups

No.	Group Name	Description	Last Incident \ Victim	Victim Count	Last Seen	Icon
1	Conti	Read more	Aareon Nederland B.V. (2022-02-11-02:05)	682	Online	
2	LockBit 2.0	Read more	ibasis.com | part 1 (2022-02-08-18:20)	588	Online	
3	Pysa (Mespinoza)	Read more	Chr Solutions (2021-12-06)	309	Online	
4	REvil Sodinokibi	Read more	PTT Exploration and Production - 720GB (2021-10-14)	286	Online	
5	MAZE	Read more	Club Fitness (2020-11-05)	266	Offline	
6	Egregor	Read more	Haggard & Stocking Associates Inc (2020-12-30)	206	Offline	
7	DoppelPaymer	Read more	Yuba County (2021-06-24)	201	Offline	

Kuvio 15. Aktiivisia kiristyshaittaohjelma toimijoita (Ransomware Groups n.d.)

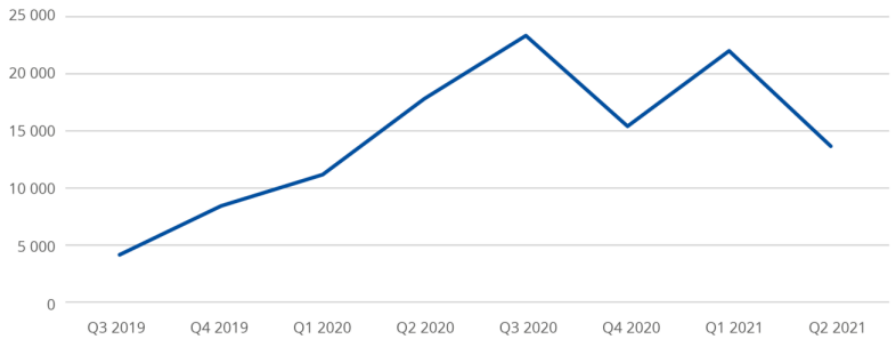
Yhdysvaltain kyberturvallisuusviranomainen (CISA) raportoi ilmoituksessaan helmikuussa 2022 kiristyshaittaohjelmien edellisen vuoden trendin osoittavan lisääntyneen globalisoituneen uhan. Ilmoituksen mukaan kyberturvallisuusviranomaiset Yhdysvalloissa, Australiassa ja Yhdistyneessä kuningaskunnassa havaitsivat kehittyneiden kiristysohjelmien lisääntyvän kriittisen infrastruktuurin organisaatioita vastaan maailmanlaajuisesti. Yhdysvalloissa raportoitiin 14 kiristysohjelmiin liittyviä tapauksia Yhdysvaltain kaiken kaikkiaan 16 kriittisen infrastruktuurin sektorista, mukaan lukien puolustusteollisuudessa, hätäpalveluissa, elintarvike- ja maataloudessa, valtion laitoksissa ja tietotekniikkasektoreilla. Lisäksi ilmoituksen mukaan kiristyshaittaohjelmatoimijat ovat lisänneet toimiaan erityisesti pilvi-infrastruktuureja, teollisia prosesseja sekä ohjelmistojen toimitusketjuihin. Kyberrikollisten on havaittu kohdistavan myös yhä laajempia hyökkäyksiä yhdysvaltalaisia yksiköitä vastaan erityisesti juhlapäivinä ja viikonloppuisin kun kohdeorganisaation henkilöstö ei ole töissä. (Alert (AA22-040A) 2022.)

Suurista teknologiatoimijoista myös Microsoft on ilmoittanut raporteissaan kiristyshaittaohjelmien havaintojen kasvun. Erityisesti yritystoimintaa kohden kiristyshaittaohjelmatapausten määrä on selkeästi yli kaksinkertaistunut vuodesta 2018 tarkasteltuna. Tarkempi kehitys on nähtävissä kuviossa 16, joka on Microsoftin vuoden 2021 digitaalinen puolustusraportista.



Kuvio 16. Kiristyshaittaohjelmien kohtaamisprosentti yritysasiakkailla (Microsoft Digital Defense Report 2021, 17)

ENISA on raportoinut myös vuoden 2021 uhkaraportissan kiristyshaittaohjelman osalta lunnasvaatimusten kasvamisesta. Raportissa verrattiin vuoden 2019 ja 2020 Coveware yrityksen tuottamia tietoja, jossa ajassa maksettujen lunnaiden keskiarvo lähes kaksinkertaistui. Kuviossa 17 on kuvattu lunnaiden kehitystä. (Enisa Threat Landscape 2021, 39.)



Kuvio 17. ENISA:n esittämät keskimääräiset lunnaat perustuen Coveware:n tietoihin (Enisa Threat Landscape 2021, 39)

Lähiaikoina myös Suomessa toimivaan suuren yritykseen on kohdistunut kiristyshaittaohjelmahyökkäys. Huhtamäki ilmoitti tammikuussa 2022 joutuneensa Intiassa tietomurron kohteeksi kiristyshaittaohjelmahyökkäyksen yhteydessä, jonka seurauksena arkistoituja tietoja varastettiin. Yrityksen käsityksen mukaan vaarantuneet tiedot olivat kuitenkin suurelta osin vanhentuneita. Tapauksen ollessa hyvin tuore opinnäytetyön kirjoittamisen hetkellä, on siitä julkisesti tietoa saatavilla vain hyvin rajatusti muun muassa edelleen aktiivisen tutkinnan seurauksena. (Statement: Data breach in India 2022.)

Helmikuussa 2022 myös Savonia-ammattikorkeakoulu ilmoitti joutuneena kiristyshaittaohjelman uhriksi. Ammattikorkeakoulun järjestelmiin ja verkkolevyille asentui tiettävästi Lockbit2.0-kiristysohjelma, joka on aluksi kopioinut tiedot hyökkääjän haltuun ja tämän jälkeen lukinnut tiedostoja. Niiden avaamiseksi hyökkääjä on vaatinut maksua bitcoineina. Aluksi ammattikorkeakoulu viestitti, että arkaluontoisia tietoja ei olisi vaarantunut, mutta myöhemmin tuli ilmi, että opiskelijoiden tietoja on kuitenkin julkaistu kaikkien saataville pimeässä Tor-verkossa. Savonian mukaan tapauksesta on tehty rikosilmoitus ja poliisi tutkii tapahtunutta. (Salokangas & Remes 2022; Rytkönen 2022.)

4.3 Kiristyshaittaohjelma hyökkäykset tulevaisuudessa

Kiristyshaittaohjelmien tulevaisuuden suhteen on puhuttu kasvavasta trendistä useiden asiantuntijoiden sekä toimijoiden toimesta. Esimerkiksi Trend Micro yrityksen tuottaman globaalin tutkimuksen mukaan yli 90 prosenttia suomalaisista IT- ja yrityspäättäjistä olisi huolissaan kiristyshaittaohjelmahyökkäyksistä (Kiristyshaittaohjelmien kasvava uhka vaatii toimia yritysten ylimmältä johdolta 2022). Lisäksi vuoden 2021 aikana kyberturvallisuusviranomaiset Yhdysvalloissa, Australiassa ja Yhdistyneessä kuningaskunnassa havaitsivat edistyneiden kiristysohjelmien lisääntyvän kriittisen infrastruktuurin organisaatioita vastaan maailmanlaajuisesti. CISA on raportissaan tuonut esille kiristyshaittaohjelmien taktiikoiden ja tekniikoiden kehittymisen vuonna 2021, mikä osoittaa kiristyshaitallisten toimijoiden kasvavan teknologisen kehittyneisyyden ja lisääntyneen kiristysohjelmauhan organisaatioille maailmanlaajuisesti. (2021 Trends Show Increased Globalized Threat of Ransomware 2022.)

Myös Euroopan unionin verkko- ja tietoturvavirasto on julkaissut raportteja säännöllisesti uhkakuvista ja kiristyshaittaohjelma on mainittu näissä toistuvasti viime vuosien aikana. ENISA mainitsee

vuoden 2021 lokakuun raportissa kiristyshaittaohjelmatoimijoiden hakevan tulevaisuudessa jatkuvasti uusia uhreja kasvattaakseen ”liiketoimintamahdollisuuksiaan”. Sen voidaan alkaa hyödyntämään niin sanottuja kolmannen osapuolen uhreja, jotka ovat hyökkääjille ihanteellisia levittäjiä uusien lunnaiden pyytämiseen tai jopa uusien kiristysohjelmakampanjoiden aloittamiseen käyttämällä aiemmissa hyökkäyksissä hankittuja tietoja uusien hyökkäysten toteuttamiseksi. (Enisa Threat Landscape 2021, 36-37.)

ENISA tuo esille myös uhreille sisäisenä uhkana toimivan työntekijöiden aktiivisen rekrytoinnin monimutkaisempien kiristyshaittaohjelmakampanjoiden aikana. Esimerkiksi elokuussa 2020 Venäjän kansalainen tuomittiin Tesla:n työntekijän aktiivisesta kohdistamisesta ja rekrytoinnista tähän tarkoitukseen. Työntekijän oli suoritettava yrityksensä tietokonejärjestelmään haittaohjelma, joka suodattaisi tietoja yrityksen verkosta. Lopulta kiristäjä olisi uhannut paljastaa tiedot verkossa, ellei yritys maksaisi lunnaita. Työntekijä saisi puolestaan miljoona Yhdysvaltain dollarin arvota bitcoineja haittaohjelman asennuksen jälkeen. (Enisa Threat Landscape 2021, 36.)

5 Kiristyshaittaohjelmien havainnot ja torjuntamahdollisuudet SOC-toiminnassa

Kiristyshaittaohjelmien hyökkäysten nykytilan selvittämiseksi opinnäytetyössä tarkasteltiin tilastojen avulla aikaisempia tapahtumia saatavilla olleen materiaalin perusteella. Selvittämisessä hyödynnettiin muun muassa toimeksiantajan kautta saatuja tunnuslukuja tietoturvaherätteiden määristä tunnistamattomassa muodossa sekä muiden toimijoiden ilmoittamia lukumääriä ja avoimen tietokannan raportointeja. Vertailemalla näitä havaintoja keskenään sekä yhdistämällä havaintoja julkisissa lähteissä kerrottuun tietoon saadaan muodostettua tilannekuva kiristyshaittaohjelmahyökkäysten kehityssuunnalle sekä selvitettyä syitä mitkä ovat mahdollistaneet hyökkäyksiä.

SOC-toiminnan kehittämistä kiristyshaittaohjelmien varalta voidaan onnistuneiden hyökkäysten syiden selvityksen perusteella tuoda esille. Lisäksi esille nousee tekijöitä, joita jokaisen organisaation olisi syytä toteuttaa, jotta riskiä joutua hyökkäyksen uhriksi voidaan minimoida. Näiden avulla eri SOC-toimijat voivat arvioida muun muassa oman valvonnan toimivuutta uhkien varalta ja kehittää omaa toimintaa tarvittaessa kasvattaakseen kyseisten uhkien, ja samalla kirityshaittaohjelmien

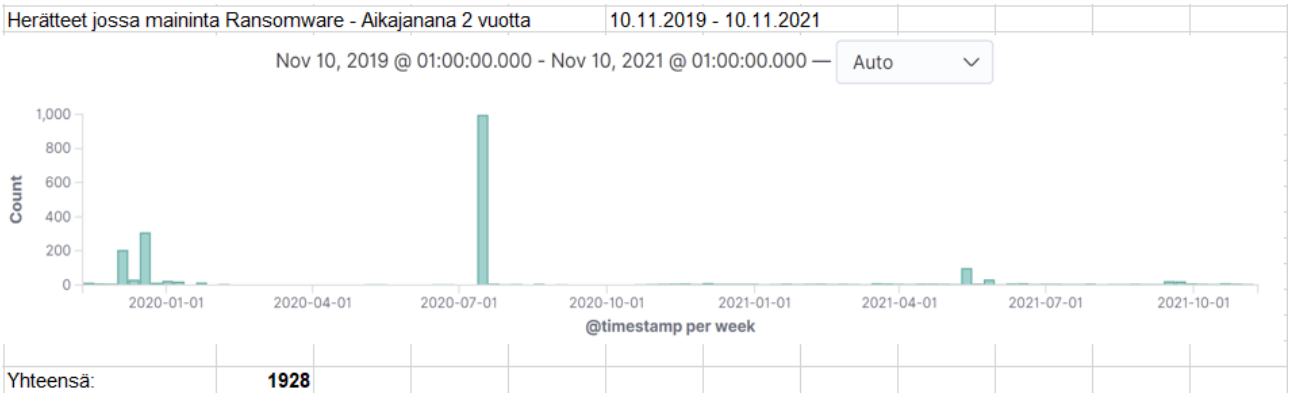
torjuntamahdollisuuksia. Koska SOC-toimijoiden kehityssuunnat voivat olla hyvin toisistaan poikkeavia ja yksilöllisiä, on syytä myös tarkastella ratkaisuja, joiden avulla kaikki SOC-toimijat kykenisivät hyödyntämään riittävän nopeasti ajantasaista tietoa.

5.1 Telia Cygate SOC

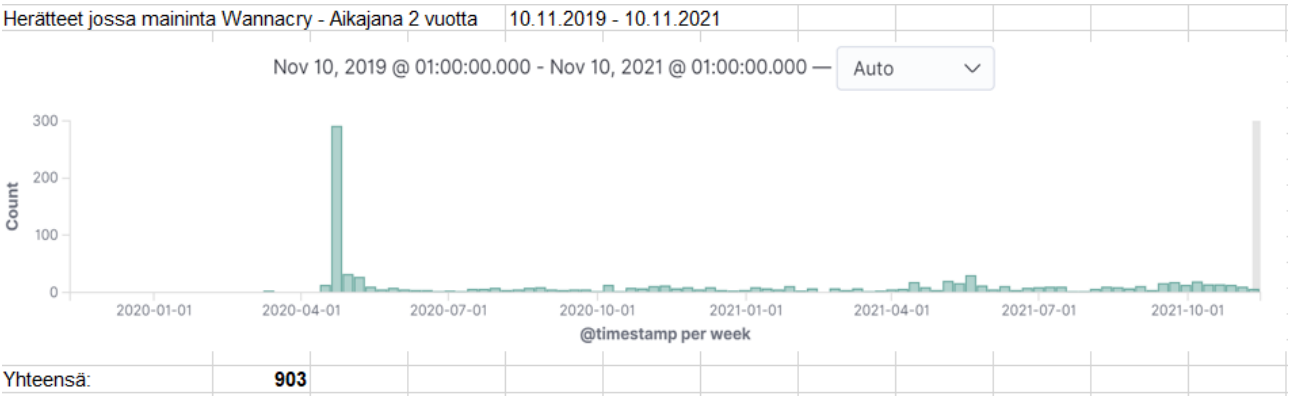
Telia Cygate:n SOC-valvomo toimii ympärivuorokautisesti vuoden jokaisena päivänä, jolloin reagointia uhkiin voidaan suorittaa mahdollisimman pienellä viiveellä. Kiristyshaittaohjelmien varalta SOC-toimintaan on luotu herätteitä, jotka aktivoituvat tiedettyjen kriteerien täyttyessä. Tällöin SOC kykenee reagoimaan hälytykseen ja analysoi onko kyseessä oikea uhka vai väärä hälytys. Herätteet pohjautuvat esimerkiksi epäilyttävien aikamääreiden täyttymiseen tai lähde- sekä kohdeverkko-osoitteiden ollessa kyseenalaisia. Myös käytössä olevat automaatiojärjestelmät kykenevät valvomaan yhtäaikaisesti useiden eri kriteerien täyttymistä ja yhdistämällä näitä yhdeksi hälytykseksi.

SOC-toiminnan herätetilastoja pystyttiin yksilöimään sekä selvittämään jälkikäteen tarkasti, jolloin näistä voitiin tehdä hakuja tietyllä aikavälillä. Opinnäytetyössä selvitettiin saadun materiaalin perusteella herätteiden määriä, joissa mainitaan sanat ”Ransomware” sekä ”Wannacry” kahden vuoden ajanjaksolla. WannaCry-kiristyshaittaohjelmalle on luotu yksilöllinen heräte, joka aktivoituu sen toiminnalle erikseen tyypillisellä tavalla. On kuitenkin syytä huomioida, että WannaCry-kiristyshaittaohjelma ei ole lähiaikoina erityisen aktiivinen, vaikkakin sitä edelleen raportoitu maailmalla. Kyseisen kiristyshaittaohjelman huippu pohjautuu vuoteen 2017, jonka ajalta tähän opinnäytetyöhön ei saatu tilastointia herätteiden määrästä. (Gregory 2021.)

Herätteiden tarkastelun perusteella voidaan tehdä arviota, onko molempien herätetyyppien perusteella nähtävissä kiristyshaittaohjelmahyökkäysten kasvua, ja onko niillä lopulta yhteyksiä todettuihin tapauksiin. Herätteiden määrät sekä jakautuminen kyseisellä ajanjaksolla on nähtävillä kuvioissa 18 sekä kuviossa 19.



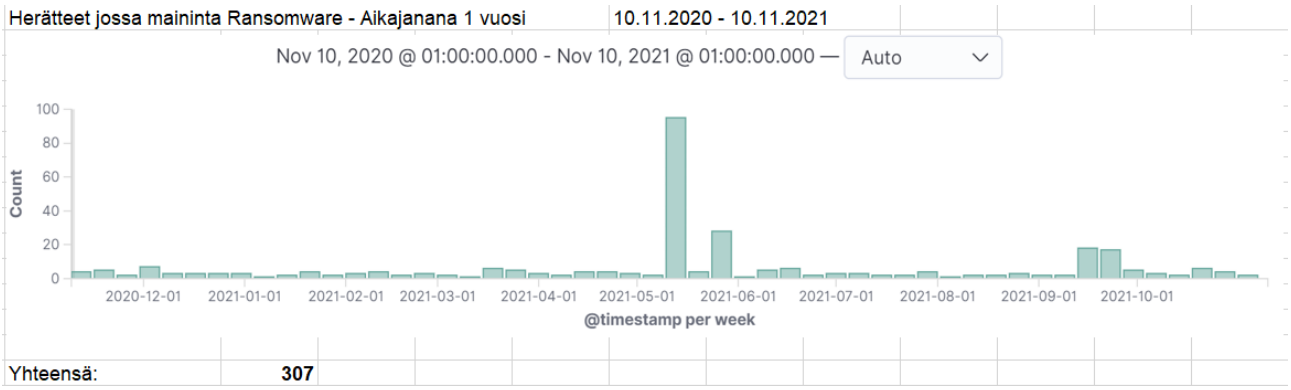
Kuvio 18. Telia Cygaten SOC-herätteiden määrä 2 vuoden ajalla sanasta "Ransomware"



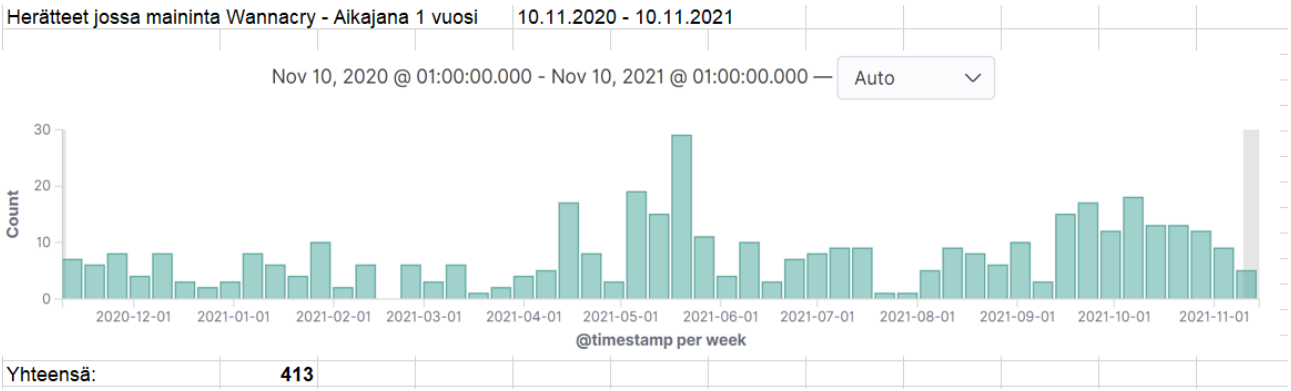
Kuvio 19. Telia Cygate SOC-herätteiden määrä 2 vuoden ajalla sanasta "Wannacry"

Herätteiden määristä voidaan molemmissa kuvioissa havaita selkeä piikki hyvin pienellä ajanjaksolla. Sanan ”Ransomware” kohdalla piikki osuu kuvion 18 perusteella heinäkuulle 2020, jolloin herätteitä on rekisteröity yhden viikon aikana yli 1000 kappaletta. Kyseessä on hyvin poikkeuksellinen määrä, sillä seuraavat piikit ovat alle 400 kappaleen määrillä vuoden 2020 alkupuolella. Kyseinen yli 1000 kappaleen määrä vaikuttaa selkeälle tilastoa muokkaavalle virheelle, joka voi syntyä esimerkiksi, jos herätteen hälytyssääntöön tehdään konfiguraatiomuutoksia, joka osoittautuu virheelliseksi. Tällöin heräte saattaa aktivoitua useamman kerran yhdestä hälytyksestä tai väärien asetettujen arvojen perusteella aiheuttaen vääristymää tilastoissa. Tämän perusteella ei voida toisaalta pois sulkea tapausta, että kyseisenä aikana olisi tapahtunut kiristyshaittaohjelmahyökkäyksiä, jotka ovat osuneet Telia Cygaten SOC-toiminnan alle. Tarkastelun aikajanaa on syytä pienentää yhden vuoden ajanjaksolle, jolloin tapaukset eivät osu kuviossa 18 näkyviin kolmeen selkeään piikkiin.

Sanan ”Wannacry” osalta on havaittavissa myös yksi selkeä piikki kuvossa 19. Herätteet tämän osalta vaikuttavat kahden vuoden tarkastelujaksolla kuitenkin piikkiä lukuun ottamatta sijoittuvan tasaisemmin. Kyseinen piikki kuviossa 19 on noin yhden kolmasosan (noin 300 kappaletta) kaikista herätteiden lukumäärästä (903 kappaletta) tarkastelujakson aikana. Myös tämän tarkastelun aikajanaa on syytä rajata yhden vuoden ajanjaksolle, että kyseinen poikkeama saadaan rajattua tarkastelusta pois.



Kuvio 20. Telia Cygaten SOC-herätteiden määrä 1 vuoden ajalla sanasta "Ransomware"



Kuvio 21. Telia Cygate SOC-herätteiden määrä 1 vuoden ajalla sanasta "Wannacry"

Kuviota 20 sekä kuviota 21 tarkastellessa huomataan, että herätteiden määrissä on edelleen havaittavissa selkeitä kohoamia pienien ajanjaksojen aikana. Kuviossa 20 ilmenevä poikkeama toukokuussa on kuitenkin kokonaismäärässä alle 100 kappaleen, mutta huomattavan korkea verrattuna herätteiden normaaliin ilmenemiseen, joka on alle 10 kappaleen viikkotasolla. Vuoden ajanjaksolla tarkasteltuna herätteiden määrät ovat kuitenkin realistisia, joten kuvion 20 määristä olisi syytä

epäillä, että johtuuko toukokuussa ilmennyt poikkeama todellisesta tilanteesta. Tapauksia tarkasteltaessa tältä ajalta, ei kuitenkaan ilmennyt todellisia tapauksia, joilla olisi yhteyttä kyseiseen poikkeamaan.

Kuviossa 21 on havaittavissa graafisesti suurempia muutoksia vuoden tarkastelujaksolla. Kuviossa on kuitenkin syytä huomioida, että kuvion korkein lukumäärä on noin 30 herätteen määrässä viikkotasolla. Näin ollen, kun muutoksia verrataan kuvion 20 määriin, voidaan todeta herätteiden määrän kuviossa 21 olevan melko tasainen ilman suuria poikkeamia. Lisäksi ilmenevien poikkeamien määrä viikkotasolla on realistinen eikä herätteiden määristä voida tässä tapauksessa todeta johtopäätöksiä oikeiden tapausten lukumäärään ilman tarkempaa tutkimista. Kuviossa 21 on myös syytä huomioida, että sanaan ”Wannacry” viittaavia herätteitä on ollut 106 kappaletta enemmän kuin sanaan ”Ransomware” viittaavia tapauksia samalla ajanjaksolla, vaikka WannaCry-kiristyshaittaohjelma ei ole ollut aktiivinen viime vuosien aikana. Eroavaisuus viittaa todennäköisesti suureen määrään vääriin hälytyksiin korreloivista herätteistä. Lisäksi herätteiden määristä on pääteltävissä, että hälytyssääntö on konfiguroitu hälyttämään jo pienistä yleisitä poikkeamista, jotka viittaavat WannaCry:n toimintaan.

Telia Cygaten SOC-toiminnassa herätteitä analysoiva tietoturva-asiantuntija tarkistaa muun muassa herätteen arvojen perusteella onko tapauksessa aihetta tarkempiin jatkotarkastuksiin. Kokenut asiantuntija kykenee yleensä muutamien minuuttien aikana arvioinnilla havaitsemaan todelliseen uhkaan viittaavat tekijät herätteistä sekä pois sulkemaan tapaukset, joissa heräte on aktivoitunut, vaikka uhkaa ei todellisuudessa ole. Tapaukset, joita on syytä tutkia tarkemmin tason 2 analyytikon toimesta tai tapaukset, joiden selvittäminen vaatii muita toimia, kirjataan kyseisestä tapahtumasta tietoturvapoikkeamatiketti. Kyseiseen tikettiin kirjataan kaikki oleelliset havainnot sekä aikaleimat tapauksesta, sekä myöhemmissä tutkimuksissa havaitut muutokset tai havainnot.

Erikseen kiristyshaittaohjelmiin liittyviä tietoturvapoikkeamatikettejä pystyttiin Telia Cygaten SOC-toiminnassa hakemaan viiden vuoden aikajanalla tikettijärjestelmän kautta. Tämän avulla pystytään tarkastelemaan, onko tikettien määrässä havaittavissa muutosta kiristyshaittaohjelmiatapausten suhteen. Tarkastelun aikana tikettimääristä ei ole eroteltu tapauksia, mitkä on jälkitarkastelussa todettu vääriksi poikkeamiksi, joten tikettimäärä ei kerro suoraan todellisten kiristyshaittaohjelmatapausten määriä.

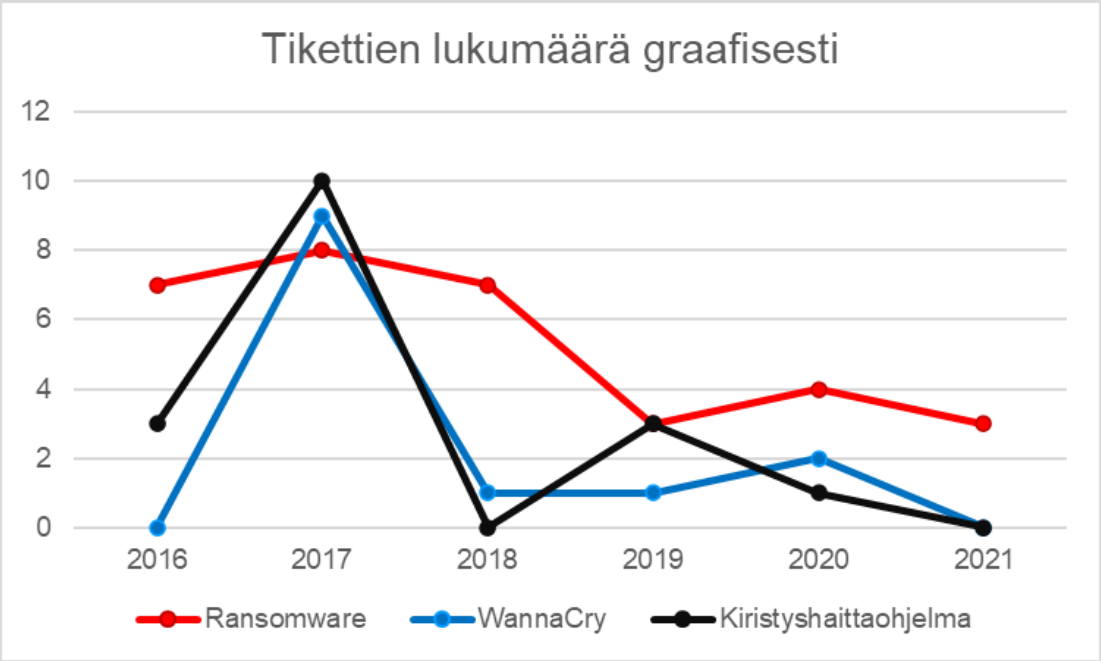
Taulukossa 1 on havainnoitu Telia Cygaten tikettimääriä vuositasolla, joiden otsikossa esiintyy kiristyshaittaohjelmiin viittaava sana. Alla olevassa taulukossa on syytä havainnoida, että tikettien määrä vuodelta 2021 on tarkasteltu marraskuun 2021 aikana, jolloin siinä ei ole kokonaiseen vuoteen viittaavia määriä esitetty.

Taulukko 1. Avattujen tietoturvapoikkeamatikettin lukumäärä vuositasolla

Mainittu sana	2016	2017	2018	2019	2020	2021
Ransomware	7	8	7	3	4	3
WannaCry	0	9	1	1	2	0
Kiristyshaittaohjelma	3	10	0	3	1	0
Yhteismäärä	10	27	8	7	7	3

Taulukon 1 tietojen perusteella voidaan havaita, että avattujen tikettien lukumäärät herätteisiin verrattuna ovat hyvin pieniä ja vain muutamia tikettejä päätyy jatkotarkasteluun. Taulukon tiedot eivät toisaalta myöskään erittele, onko kyseinen tiketti avattu suoraan herätteestä, sillä poikkeama voidaan SOC-toiminnassa avata myös muusta lähteestä tulleen tiedon perusteella. Tiketeissä on myös syytä huomioida käytetty kieli, sillä osa tiketeistä on tehty suomeksi, kun taas osa tehtiin englanniksi. Tällöin esimerkiksi sanojen ”Ransomware” ja ”Kiristyshaittaohjelma” summa kertoo todellisen lukumäärän samasta asiasta.

Lisäksi SOC-toiminnan kehittyessä Telia Cygate:lla on otettu käyttöön kesken tarkastelujakson aikana rinnakkainen uudempi tikettijärjestelmä, jolloin osa tiketeistä on rekisteröity uuteen järjestelmään. Materiaalin tutkimisen aikana tikettejä tarkasteltiin vain vanhan järjestelmän kautta, eikä uuden järjestelmän tikettimääriä saatu vertailuun mukaan mikä vääristää osittain viimeisempien vuosien tuloksia. Vanhan tikettijärjestelmän tikettien määrää voidaan kuitenkin tarkastella graafisessa muodossa, joista kehityssuuntaa on helppo tulkita. Tämä on kuvattu kuviossa 22.



Kuvio 22. Tietoturvapoikkeamatikettien lukumäärä graafisessa muodossa

Kuvion 22 perusteella huomataan, että tikettien lukumäärä on laskevassa suhteessa, ja vaihtelut vuositasolla tikettien lukumäärissä voivat olla suhteessa edelliseen vuoteen verrattuna suuria. Toisaalta WannaCry:n osalta tapausta voidaan selittää nimenomaisesti vuoden 2017 suurimmalla aktiivisuudella maailmanlaajuisesti, jolloin tapauksia on tutkittu Telia Cygaten SOC-toiminnassa myös eniten. Kuvaajan perusteella tarkasteltaessa kiristyshaittaohjelmien kehitystä olisi tutkintoja viime vuosien aikana kuitenkin vähemmän ja kehityssuunta olisi laskeva.

Kaikkien tikettien lukumäärät ovat kuitenkin kokonaisuudessaan vähäisiä, jolloin graafinen kuvaaja luo myös suuria muutoksia lukumääriin aiheuttaen isoja muutoksia kiristyshaittaohjelmien kehityssuunnassa. Automaatikan kehittyminen sekä uusien työkalujen hyödyntäminen SOC-toiminnassa ovat mahdollistaneet tehokkaamman torjunnan myös kiristyshaittaohjelmissa, jolloin esimerkiksi rajatapaukset eivät ole vaatineet välttämättä tikettiä, mikä voi selittää omalta osaltaan tikettimäärän laskua. Pelkästään herätteiden sekä tikettimäärien perusteella on kuitenkin hankalaa arvioida kiristyshaittaohjelman kehityssuuntaa tai syitä muutoksille, jolloin on syytä tutkia myös muiden toimijoiden havaintoja.

5.2 Kyberturvallisuuskeskus

Kyberturvallisuuskeskus on Liikenne- ja viestintävirasto Traficomin alaisuudessa toimiva organisaatio, joka kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa tietoturvallisuuden tilannekuvaa Suomessa. Kyberturvallisuuskeskuksella on useita tehtäviä sisältäen muun muassa kyberturvallisuusharjoitteiden organisointia, valtiollista CERT-toimintaa (Computer Emergency Response Team) sekä sääntely- ja valvontatehtäviä. (Kyberturvallisuuskeskus n.d.) Kyberturvallisuuskeskuksen kautta on mahdollista saada ajantasaista tilannetietoa, joka ottaa huomioon myös muut organisaatiot, sillä se toimii yhteistyössä tietoturvaan keskittyneiden organisaatioiden kanssa sekä tietoturvahyökkäyksistä kärsivien uhrien kanssa.

Kyberturvallisuuskeskus ylläpitää myös avointa Autoreporter-tietokantaa, jonka perusteella kuka vain voi hakea sinne ilmoitettuja tietoturvauhkia eri kategorioiden mukaan. Autoreporter-palvelun avulla voidaan lähettää verkkojen ylläpitäjille automaattisesti tietoja heidän verkossaan havaituista tietoturvaa uhkaavista tekijöistä. Palvelun tarkoitus on antaa verkkojen ylläpitäjille tietoja, joiden avulla he voivat puuttua heidän tietojaan yleisesti vaarantaviin tietoturvapoikkeamiin ja tehdä tarvittavia muutoksia sen perusteella. Kyberturvallisuuskeskus osallistuu haittaohjelmien torjuntaan yhteistyössä teleyritysten kanssa. Autoreporter-järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä ja välittää tietoa liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen. (Autoreporterin haittaohjelmahavainnot 2022; Autoreporter-kategoriat n.d.)

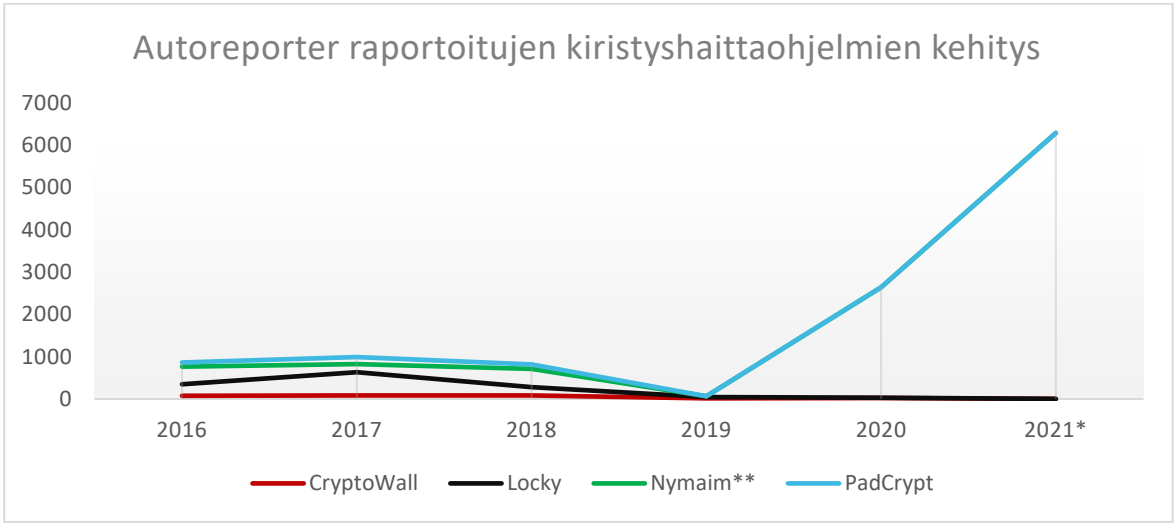
Autoreporter-palveluun on listattuna Bot-alikategoria, joka sisältää havaintoja haittaohjelman saastuttaman tietokoneen viestinnästä bottiverkon komentopalvelimen kanssa. Kiristyshaittaohjelmiksi luokiteltavista on saatavissa yhteensä 5 eri haittaohjelman havainnot, jotka luokitellaan Bot-alikategoriaan. Suodatuksen avulla voidaan Swagger-työkalun kautta hakea kyseiseen alikategoriaan listattuja määriä kiristyshaittaohjelmien osalta. Tietokannan Bot-alikategoria sisältää seuraavat kiristyshaittaohjelmat: CryptoWall, Dynamer, Locky, Nymaim sekä PadCrypt. Kyseisten kiristyshaittaohjelmien raportointimääriä viiden vuoden ajanjaksolla on listattu taulukossa 2.

Taulukko 2. Autoreporter ilmoitusten lukumäärä kiristyshaittaohjelmista 28.10.2021

Vuosiluku		2016	2017	2018	2019	2020	2021*	Yht.
Kiristyshaittaoh-jelma	CryptoWall	74	84	84	13	20	3	278
	Dynamer	-	-	-	-	-	-	-
	Locky	275	549	195	31	13	0	1063
	Nymaim**	412	188	432	21	2606	6282	9941
	PadCrypt	104	169	103	0	0	0	376
	Yhteensä vuodessa havaintoja kaikista kiristyshaittaohjelmista	**865**	**990**	**814**	**65**	**2639**	**6285**	

* Kesken vuotta tarkasteltu
** Ollut aktiivinen myös ennen 2016

Taulukon 2 tietoja tarkastellessa, huomataan suuria eroja eri kiristyshaittaohjelmien välillä. Esimerkiksi vuoden 2021 osalta Nymaim-haittaohjelma, jota voidaan käyttää kiristyshaittaohjelmien asennukseen, on ollut taulukon kiristyshaittaohjelmista erityisen aktiivinen yli 6000 kappaleen ilmoitusmäärällä, kun taas seuraavana tuleva CryptoWall-kiristyshaittaohjelma on raportoitu Autoreporter-palvelussa vain kolme kertaa. Erityisenä huomiona on myös Dynamer-kiristyshaittaohjelma, jota ei ole Autoreporteriin raportoitu ollenkaan viiden vuoden aikana. Lisäksi PadCrypt-kiristyshaittaohjelma ei ole ollut aktiivinen taulukon tietoihin perustuen vuoden 2018 jälkeen. Kyseisten kiristyshaittaohjelmien trendiä taulukon 2 Autoreporter-palveluun perustuen esitetään alla olevassa kuviossa 23.



Kuvio 23. Autoreporter raportoitujen kiristyshaittaohjelmien kehitys

Kuvion 23 ja taulukon 2 havaintojen perusteella voidaan tiettyjen kiristyshaittaohjelmien kehityksen kasvaneen moninkertaisesti viiden vuoden tarkastelujakson aikana. Lukumäärällisesti kiristyshaittaohjelmatapausten määrä on kasvanut erityisesti vuoden 2020 ja 2021 aikana, ja pelkästään näiden vuosien välillä aktiivisen Nymaim-kiristyshaittaohjelman havaintojen määrä on kolminkertaistunut. 2021 vuoden havaintojen lukumääriä tutkittaessa, havaitaan kiristyshaittaohjelmatapausten yli kuusinkertaistuneen vuodesta 2018, johon asti vertailussa olleiden kiristyshaittaohjelmien määrä on ollut vielä alle 1000 kappaleen yhteistasolla.

Vertailussa olleiden kiristyshaittaohjelmien perusteella havaitaan myös aaltomainen efekti yksittäisten kiristyshaittaohjelmien tasolla. Yksittäinen kiristyshaittaohjelma saattaa olla aktiivinen muutaman vuoden, jonka aikana tapauksia ilmenee kiihtyvällä tahdilla, jonka jälkeen kyseisen kiristyshaittaohjelman tapaukset vähenevät merkittävästi tai jopa loppuvat kokonaan ennen mahdollista uutta aktivoitumista. Tämä ilmenee esimerkiksi Nymaim kiristyshaittaohjelmalla, joka on ollut maailmalla aktiivinen erityisesti myös vuonna 2013 (Nymaim – obfuscation chronicles 2013).

Kyberturvallisuuskeskukselta saatiin opinnäytetyötä varten myös erikseen tilasto, josta ilmenee tunnistamattomasti heille ilmoitettujen kiristyshaittaohjelmatapauksista kirjattujen tikettien määrä vuoden 2016 alusta vuoteen 2021 marraskuun loppuun saakka. Tilasto toimitettiin kuukausitasollisesti ja tilastosta koostettiin taulukkomuotoon kirjattujen tikettien lukumäärä vuositasolla (Jauhiainen 2021). Kuukausimuotoa tarkasteltaessa poikkeavana havaintona oli toukokuussa 2017 ilmoitettujen tapausten suuri määrä (17), joka selittyy muun muassa maailmalla erityisen aktiivisena olleena WannaCry-kiristyshaittaohjelmalla. Taulukossa 3 esitetään vuositasollisesti Kyberturvallisuuskeskuksessa kirjatut kiristyshaittaohjelmien tutkittavat tapausmäärät ja siinä on mukana myös yksityishenkilöiden tekemiä ilmoituksia kiristyshaittaohjelmatapauksista. (Opinnäytetyö - tausta-aineiston saatavuus 2021.)

Taulukko 3. Kyberturvallisuuskeskukselle ilmoitettujen kiristyshaittaohjelmatapauksien määrä 1.1.2016-30.11.2021 (mukaillen Jauhiainen 2021)

Vuosi	2016	2017	2018	2019	2020	2021*
Tikettejä yht.	18	27	3	11	48	52

*Tietoja vain marraskuuhun saakka

Taulukon 3 tietoja tarkastellessa huomataan selkeää kasvua erityisesti vuosien 2019 ja 2020 välillä, jolloin kasvu on ollut suurinta. Aaltoefekti on havaittavissa myös vuoden 2018 osalta, jolloin tapauksia on raportoitu edellisvuotta selkeästi vähemmän. Kyberturvallisuuskeskukselle raportoitujen tapausten määrä on lähes kolminkertaistunut viiden vuoden aikana. Kehityskulkua esitetään kuviossa 24 tarkemmin.

Kuvio 24. Kyberturvallisuuskeskukselle ilmoitettujen kiristyshaittaohjelmatapauksien määrä (mukaillen Jauhiainen 2021)

5.3 Poliisin näkökulma ja rikostilastot

Kyberrikollisuus terminä sisältää kaiken tietoverkoissa tapahtuvan tai tietoverkkoja hyödyntävän rikollisen toiminnan. Tietoverkossa tapahtuvien rikosten yhteydessä käytetään usein jakoa tietoverkkosidonnaisien ja tietoverkkoavusteisien rikoksien välillä. Tietoverkkosidonnaiset rikokset kohdistuvat itsessään tietoverkkoihin ja tietojärjestelmiin ja kyseisten rikoksien tekeminen on mahdollista ainoastaan tietokoneita ja tietoverkkoja käyttäen. Tällaisia tekoja ovat esimerkiksi tietojärjestelmän häirintä, tietomurrot sekä datavahingonteko. (Kyberrikokset n.d.) Kiristyshaittaohjelman käyttö voidaan luokitella tietoverkkosidonnaiseksi rikokseksi, sillä sen tarkoituksena on nimenomaisesti vaikuttaa tietojärjestelmiin. Kiristyshaittaohjelman käyttämisestä aiheutuneet muut seuraukset voivat toisaalta täyttää myös tietoverkkoavusteisen rikoksien tunnusmerkistöjä, jos esimerkiksi hyökkäyksen aikana haltuun saatua tietoa käytetään muuhun tarkoitukseen.

Kiristyshaittaohjelmien kehityssuuntaa tarkastellessa, voidaan tutkia rikostilastoja mitkä kiristyshaittaohjelman käyttö täyttää. Kiristyshaittaohjelmasta itsessään ei ole rikoslakiin säädetty pykälää, mutta sen käyttö voidaan luokitella rikkovan Suomen rikoslain pykäliä (21.4.1995/578). Rikoksien tunnusmerkistöjen täyttyminen kuitenkin on hyvin tapauskohtaista ja se riippuu myös pitkälti kiristyshaittaohjelman tyypistä. Rikoksien pykälien ja tunnusmerkintöjen täyttymistä tiedusteltiin Keskusrikospoliisin rikoskomisario Marko Leposelta. Sähköpostivastauksessa Leponen (2021) toi esiin rikoksien tunnusmerkkejä kiristyshaittaohjelman osalta.

> *Yleisesti ottaen sillä menetelmällä, jolla kiristyshaittaohjelma järjestelmään saadaan, on merkitystä sen alkurikoksen osalta. Kiristyshaittaohjelmalla aiheutettu vahinko kohdejärjestelmän sisällä voidaan lähtökohtaisesti luokitella datavahingonteoksi taikka sen törkeäksi tekomuodoksi. Sen sinne ujuttamiseksi usein tarvitsee tehdä tietomurto. (Leponen 2021.)*

Leponen (2021) viittasi lisäksi vastauksessaan yleisiin lainkonkurrenssia koskevien periaatteisiin, jonka perusteella jokin rikoksen tunnusmerkistö voi syrjäyttää tietyn rikoksen tunnusmerkistön muiden merkistöjen täyttyessä. Kiristyshaittaohjelman osalta tämä koskee erityisesti tietomurron osuutta rikoksessa.

> *Yleisten lainkonkurrenssia koskevien periaatteiden ja tietomurron toissijaisuuslausekkeen tukemana tietomurto voi siis väistyä, mikäli teko täyttää myös datavahingonteon. (Leponen 2021.)*

Lisäksi vastauksessa Leponen (2021) toi esille tietojärjestelmän häirinnän tunnusmerkistön täyttymisen, joka riippuu kiristyshaittaohjelman hyökkäyksen tarkoituksesta ja halusta vaikuttaa järjestelmän käytettävyyteen. Vastaus korostaa myös rikostutkinnan eri vaiheiden aikana mahdollisimman tarkan motiivin selvittämistä, jotta pystytään käyttämään todellisia rikosnimikkeitä, vaikka motiivi ei välttämättä ole vielä alkuvaiheessa selvillä.

> *Kiristyshaittaohjelmahyökkäys voisi myös täyttää tietojärjestelmän häirinnän (miksen myös tietoliikenteenhäirinnän) tunnusmerkistön, mikäli sen tarkoituksena on häiritä tietojärjestelmän (taikka tietoliikenteen, eli viestinvälityksen) toimintaa. Kuten huomaat, teon motiivilla on ratkaiseva merkitys tunnusmerkistön täyttymisessä. Usein teon motiivi ei ole selvillä. Silloin joudutaan pohtimaan sitä mikä kyseisen haittaohjelman tarkoitus voisi olla, taikka mihin hyökkääjä on jälkien perusteella pyrkinyt. (Leponen 2021.)*

Asiantuntijalausunnon perusteella voidaan havaita, että rikosnimikkeet, jotka liittyvät kiristyshaittaohjelmien käyttöön ovat datavahingonteko, tietomurto, tietojärjestelmän häirintä. Myös näiden rikosten yritys-, lievä- sekä törkeämuotoiset nimikkeet on syytä ottaa huomioon kiristyshaittaohjelmien kanssa. Tätä tapausta tukee myös Savonian ammattikorkeakoulun tietomurto keväällä 2022, josta julkaistun artikkelin mukaan kyseistä tapausta tutkitaan törkeänä tietojärjestelmän häirintänä, törkeänä tietomurtona ja törkeänä datavahingontekona (Rytkönen 2022).

Opinnäytetyötä varten poliisihallitukselta tiedusteltiin saatavuutta ajankohtaisiin tilastoihin, joissa ilmenisi kyseisten rikoksien ilmoitusmääriä poliisille sekä myös muiden lähelle osuvien rikoslain luvun 38 nimikkeisiin nähden. Poliisihallituksen edustajalta saatiin tammikuussa 2022 taulukkomuodossa rikosten ilmoitusmäärät viiden vuoden ajanjaksolla alkaen vuodesta 2016.

Taulukko 4. Poliisille ilmoitetut rikokset koko maassa (Helenius 2022)

Poliisille ilmoitetut rikokset koko maassa

Ilmoitettu Kpl	2016	2017	2018	2019	2020	2021
DATAVAHINGONTEKO	14	7	14	8	11	16
DATAVAHINGONTEON YRITYS	1	0	0	0	1	1
LIEVÄ DATAVAHINGONTEKO	0	2	1	3	1	2
TÖRKEÄ DATAVAHINGONTEKO	3	1	1	2	2	2
TIETOJÄRJESTELMÄN HÄIRINNÄN YRITYS	0	0	0	0	0	1
TIETOJÄRJESTELMÄN HÄIRINTÄ	38	24	20	9	16	27
TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	16	14	8	6	6	4
TIETOMURRON YRITYS	13	18	22	16	67	57
TIETOMURTO	409	411	509	804	1 107	1 501
TÖRKEÄ TIETOMURTO	8	19	8	6	16	9
TÖRKEÄN TIETOMURRON YRITYS	0	8	0	0	0	0
Summa	**502**	**504**	**583**	**854**	**1 227**	**1 620**

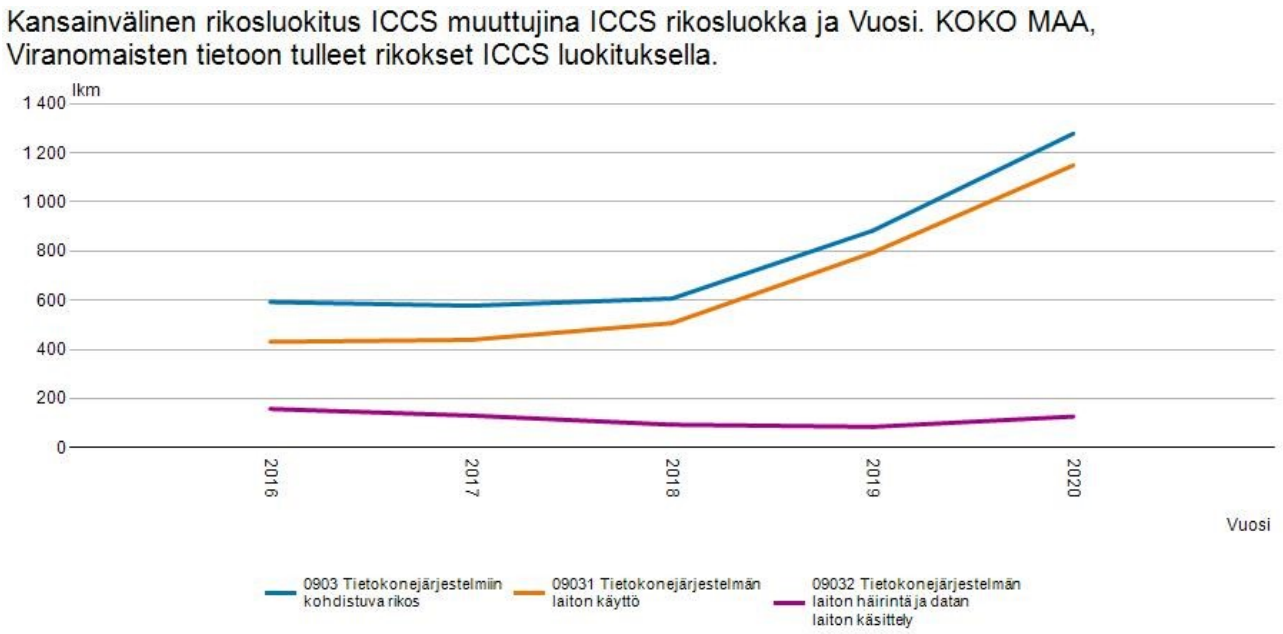
Taulukon 4 (Helenius 2022) tuloksia tarkasteltaessa havaitaan varsinkin suuri määrä tietomurtoja sekä kirjattujen tietomurtojen lukumäärän kasvaneen erityisesti vuodesta 2019 alkaen. Kasvu on ollut koko ajan kiihtyvää tarkastelujakson päättymiseen saakka, ja viimeisen kahden vuoden aikana ilmoitusmääriä on ollut lähes 400 kappaleen verran enemmän. Viiden vuoden aikana tietomurtojen määrä on myös yli kolminkertaistunut.

Tietomurtojen yritysten kohdalla kasvu on ollut vielä suurempaa, ja räjähdysmäinen kasvu on tapahtunut vuosien 2019 ja 2020 aikana. Vuoteen 2016 verrattuna myös tietomurtojen yritysten määrä on yli nelinkertaistunut, vaikkakin ilmoitusmäärät ovat olleet joka vuosi alle 70 kappaleen lukumäärissä, joka on verrattain pieni määrä varsinaisiin tietomurtoihin verrattuna.

Muiden ilmoitettujen rikosnimikkeiden osalta ei ole havaittavissa selkeitä suuria muutoksia. Datavahingontekojen määrä on viiden vuoden ajanjaksolla pysynyt pieniä vuosittaisia muutoksia lukuun ottamatta tasaisena, ja tietojärjestelmän häirinnän osalta ei ole merkittäviä muutoksia havaittavissa. Mielenkiintoisena havaintona törkeän tietojärjestelmien häirintä ilmoitusten määrä on pienentynyt tai pysynyt samana aina edellisiin vuosiin verrattuna, ja vuoden 2021 verrattuna ilmoitusten lukumäärä on enää neljäsosa vuodesta 2016.

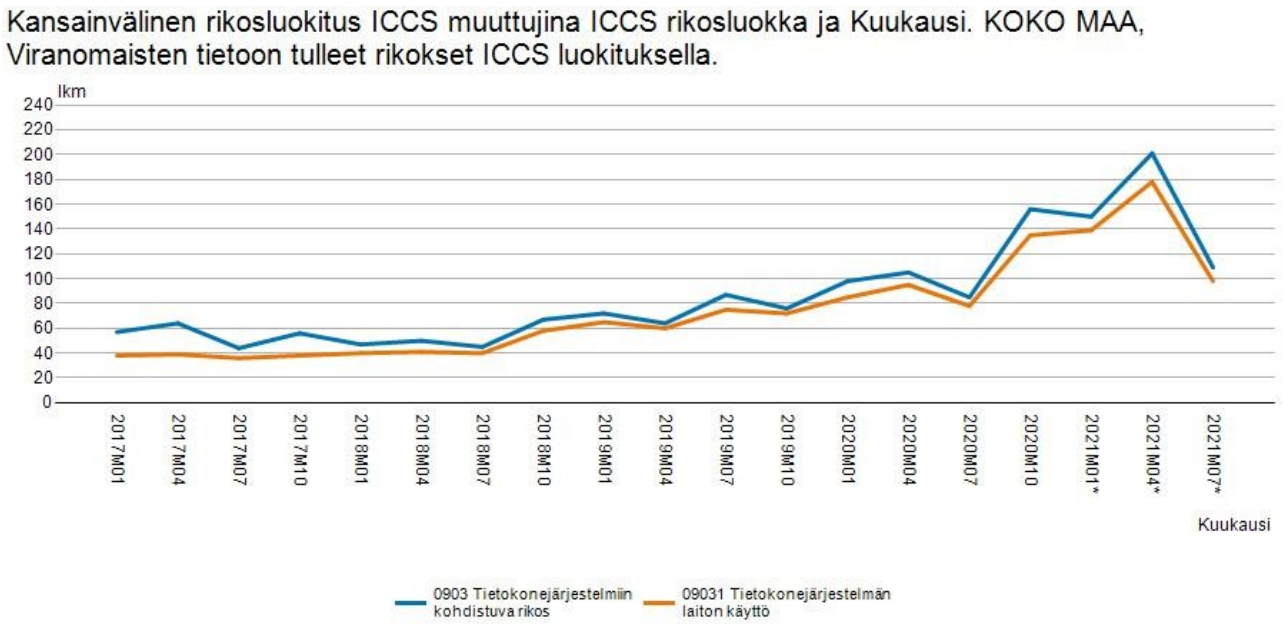
Lakien ollessa erilaisia maittain, on lakien seuranta usein haastavaa kansainvälisellä tasolla. Tätä varten on kehitetty myös kansainvälinen rikosluokitus ICCS (engl. International Classification of Crimes), jonka avulla voidaan parantaa kansainvälisten rikostilastojen laatua, yhtenäistää rikostilastoja ja helpottaa kansainvälisten tietojen vertailtavuutta. ICCS-luokitus perustuu lainkohtien sijaan teonkuvauksiin. Sen avulla luodaan kehikko, joka mahdollistaa eri lähteistä, kuten hallinnollisista aineistoista ja kyselytutkimuksista saatavan tilastotiedon vertailun. (Haapakangas 2018.)

Tilastokeskuksen verkkosivuilta on saatavissa ajankohtainen Suomen virallinen StatFin-tilastotietokanta rikos- ja pakkokeinotilastojen osalta, jotka noudattavat ICCS-luokitusta. Hakusivulta on erikseen eroteltavissa rikosluokat, joiden mukaan tilastoja voidaan vertailla. ICCS-rikosluokat, jotka osuvat lähelle kiristyshaittaohjelmien osalta poliisin virallisten rikosnimikkeiden kohdalla ovat seuraavat: tietokonejärjestelmiin kohdistuva rikos, tietokonejärjestelmän laiton käyttö sekä tietokonejärjestelmän laiton häirintä ja datan laiton käsittely. (Selvitettyihin rikoksiin syylliseksi epäillyt kansainvälisen rikosluokitukset ICCS mukaan, 2013-2020 n.d.) Hakutuloksista voidaan hakea suoraan graafisessa muodossa viranomaisten tietoon tulleet rikokset Suomessa. Tämä on esitetty kuviossa 25.



Kuvio 25. Rikosluokitukset vuositasolla ICCS-muuttujina (Kansainvälinen rikosluokitus ICCS muuttujina ICCS rikosluokka ja Vuosi n.d.)

Kuviossa 25 on havaittavissa selkeää kasvua vuodesta 2018 alkaen tietokonejärjestelmiin kohdistuvissa rikoksissa ja tietokonejärjestelmien laittomassa käytössä. Molemmat rikosluokat ovat kasvaneet lähes samalla nopeudella kahden vuoden aikana, ja molempien luokkien viranomaisten tietoon tulleiden ilmoitusten määrät ovat kaksinkertaistuneet vuoteen 2020 menneessä. Trendi on ollut samansuuntainen taulukon 4 tietoihin nähden, jossa kasvu on ollut toisaalta vielä suurempaa. Kuviossa 25 olleet ICCS-luokat eivät toisaalta välttämättä sisällä kaikkia nimikkeitä, jotka on esitetyt taulukossa 4, joka voi selittää kasvuvauhdin eroa siihen verrattuna.



Lähde: Rikos- ja pakkokeinotilasto, Tilastokeskus

Kuvio 26. Rikosluokitukset neljännesvuositasoin ICCS-muuttujina (Kansainvälinen rikosluokitus ICCS muuttujina ICCS rikosluokka ja Kuukausi n.d.)

Kuviossa 26 esitetään sama tilasto verrattuna kuvion 25 kahden merkittävän muuttujan osalta, mutta tulokset ovat kolmen kuukauden tarkastelujaksossa. Erona on myös, että tuloksia on esitetty vuodesta 2017 alkaen ja päättyen vuoden 2021 heinäkuuhun asti. Kuvion 26 tuloksista huomataan molempien rikosluokkien aaltomainen ja tasainen kasvu vuoden 2020 heinäkuuhun asti, jolloin rikoksia on kirjattu kolmen kuukauden aikana selvästi enemmän. Tietotekniikkajärjestelmien rikokset ovat vertailun ajassa myös lähes kaksinkertaistuneet.

Molempien esitettyjen kuvioiden perusteella voidaan tulkita, että yleisesti tietotekniikkaa kohtaan tapahtuvat rikokset ovat kasvaneet merkittävästi viime vuosien aikana aikaisempiin havaintoihin nähden. Nämä eivät suoraan indikoi kiristyshaittaohjelmien kasvua, mutta yhteys molempien kasvujen selityksen kohdalla on kuitenkin olemassa. Kiristyshaittaohjelmien kasvun totesi myös rikoskomisario Leponen (2021), joka toi esille poliisin näkökulmasta katsottuna kiristyshaittaohjelmien tilannetta.

> *Kiristyshaittaohjelma-hyökkäykset ovat viime vuosina kasvaneet räjähdysmäisesti ja tulevat kasvamaan myös tulevaisuudessa niiden melko helpon toteuttamisen vuoksi. Lisäksi tuotto-panos suhde niissä on suhteellisen hyvä rikollisten näkökulmasta. (Leponen 2021.)*

Leponen (2021) toi vastauksessaan esille myös kiristyshaittaohjelmahyökkäysten seurauksia uhrille, sekä miten rikollisuutta tämän osalta olisi organisaatioiden mahdollista torjua jo ennakkoon. Vastauksessa ilmenee myös, miten organisaatioiden toimintamallit rahoituksen suhteen tietoturvallisuuden suhteen voidaan pahimmillaan ajatella.

> *Mielestäni on tärkeä saada näkyväksi se, miten kallista toipuminen tämän tyyppisestä toiminnasta on ja erityisesti se, miten pienellä osalla vahinkojen arvosta, tämän tyyppistä rikollisuutta voitaisiin torjua jo ennakolta. Haasteena usein on se, että torjutut hyökkäykset ja niihin panostettu raha "ei näy missään", kun mitään ei lopulta tapahtunutkaan. (Leponen 2021.)*

Kokonaisuudessa tarkasteltuna kyberrikosten sekä ongelmien määrästä päätellen voidaan olettaa näillä olevan yhteyttä myös kiristyshaittaohjelmien havaintojen määrään, mitä on raportoitu myös Traficomin toimesta. Vaikka ajallisesti tarkasteltuna ilmoitusmäärät poliisin ja Traficomin määrien muutoksissa eivät ilmene täysin samaan aikaan samalla tavalla, voidaan tätä selittää esimerkiksi ilmoituskäytäntöjen eroavaisuudella tai ilmoitusajoissa saman tapahtuman välillä, joissa voi olla eroja. Molempien organisaatioiden tilastoissa on kuitenkin havaittavissa yhteisenä tekijänä selkeää kasvua juuri viimeisen kahden vuoden aikana.

5.4 SOC-toiminnan rooli

SOC-toiminnan rooli kiristyshaittaohjelmahyökkäyksen kohdatessa voidaan jakaa useampaan vaiheeseen. Ensivasteena kun SOC tunnistaa aktiivisen hyökkäyksen, on tärkeä rajoittaa hyökkäyksen leviäminen ja estää lisävahingot tämän seurauksena. Toiminta voidaan tehdä esimerkiksi tunnistamalla sekä etsimällä haavoittuneet kohdejärjestelmät ja eristämällä nämä verkosta. SOC-päivystäjän pitäisi kyetä tekemään toimenpide EDR-työkalun avulla, ellei tätä toteuteta jo automaattisesti, jolloin reagointiaika pystytään lyhentämään.

Usein toisessa vaiheessa SOC kykenee suorittamaan lisätutkimuksia hyökkäyksen aiheuttajasta. Tärkeä on tunnistaa kiristyshaittaohjelman tyyppi, sekä monitoroida mahdollisen lisäaktiviteetin varalle. SOC:in on syytä myös olettaa, että kohdejärjestelmien kaikki tieto on vaarantunut, mihin

kiristyshaittaohjelma on päässyt käsiksi. Materiaali on syytä tunnistaa esimerkiksi organisaation SIRT-toiminnan (Security Incident Response Team) kanssa ja ymmärtää kyseisen tiedon joutumisen ulkopuolisten käsiin aiheuttaman riskin omalle organisaatiolle. Lisäksi tässä vaiheessa on syytä selvittää mitä reittiä kiristyshaittaohjelma on päässyt kohdejärjestelmään. Jos tapauksessa havaitaan haavoittuvuuden hyväksikäyttöä, tulisi saman haavoittuvuuden uudelleen käyttö estää mahdollisimman pian, jos mahdollista.

Prosessin lopussa on mahdollisuus suorittaa tarkempaa ja syvällisempää analyysiä miksi kiristyshaittaohjelman käyttö on onnistunut. Loppuvaihe sisältää esimerkiksi digitaalista forensiikkaa, jonka avulla voidaan saada arvokasta tietoa haittaohjelman kulusta ja toiminnasta. Myös onnistuneessa forensiikasta voidaan selvittää, onko esimerkiksi kaikki kohdejärjestelmän tiedot vaarantuneet. On kuitenkin syytä ymmärtää, että varsinkin edistyneiden kiristyshaittaohjelmien osalta forensiikka ja muut selvitystyöt voivat olla haasteellisia, ellei jopa mahdottomia, jos haittaohjelma on salannut tai peittänyt omia jälkiään. Kuitenkin onnistuneesti tämän vaiheen avulla voidaan toteuttaa toimenpiteitä, jolla vastaavilta hyökkäyksiltä voidaan välttyä tulevaisuudessa.

Pelkkä SOC-toiminta ei kuitenkaan kykene estämään kiristyshaittaohjelmahyökkäystä, jos sitä on tarkoituksena käyttää kohdejärjestelmään nopeasti ja järjestelmälle ei toteuteta riittävää ylläpitoa. SOC kykenee toimimaan ja reagoimaan ainoastaan hyökkäyksen rajaamisessa ja estämään mahdollisesti laajemmat uhat suojattavissa kohteissa. Toisaalta kiristyshaittaohjelma voi olla suunnitellun laajemman hyökkäysketjun viimeinen osa, koska se lamauttaa koko järjestelmän ja paljastaa tietomurron uhrille. Jos hyökkääjän suunnitelmat pystytään pysäyttämään jo ennen kiristyshaittaohjelman käyttöä, voidaan siinä välttää osa vahingosta.

Päätelaitteiden ja servereiden säännölliset päivitykset sekä ylläpito ovat tärkeimmässä roolissa henkilöstön tietoturvaosaamisen lisäksi, jotta hyökkäysten riski voidaan minimoida. Hyökkäyksien osalta onkin havaittu kasvua varsinkin nollapäivähaavoittuvuuksien hyödyntämisestä ja myös entistä nopeammalla vasteajalla (Enisa Threat Landscape 2021, 42). Päätelaitteiden ja servereiden fyysinen päivittäminen on myös syytä tehdä, kun päivitystuki vanhoille laitteille loppuu. Lisäksi säännöllinen penetraatiotestaus haavoittuvuuksien löytämiseksi on suositeltavaa, jonka avulla voidaan kartoittaa haavoittuvia kohteita paremmin.

ENISA on listannut myös vuoden 2021 uhkakuvaraportissaan tekijöitä, joiden avulla organisaatiot voivat suojautua kiristyshaittaohjelmilta. Nämä sisältävät muun muassa seuraavia suosituksia (Enisa Threat Landscape 2021, 43):

- Pääsynhallinnan toteutuksen auditointi
- Kehitys- ja tuotantoympäristöjen erottaminen toisistaan
- Tietojen jakaminen tapahtumista viranomaisten kanssa
- Rajoitetaan pääsyä tunnettuihin kiristysohjelmasivustoihin
- Valtuutettujen laitteiden, prosessien ja käyttäjien henkilöllisyydet sekä valtuustiedot on myönnettävä, hallittava, varmennettava, peruutettava ja tarkastettava
- Käyttöoikeuksia ja käyttöoikeuksia tulee hallita vähiten etuoikeuksien ja -periaatteiden mukaisesti

SOC-toiminnassa viime vuosina yleistyneet automaatiojärjestelmät kykenevät myös keräämään ja yhdistelemään tietoa useista eri lähteistä. Kyseiset järjestelmät ovat laajasti optimoitavissa, ja riittävän tehokkaasti toteutettu tiedonkeräys mahdollistaa useiden eri tyypillisten kiristyshaittaohjelmapiirteiden yhdistämisen yhdeksi tapahtumaksi, jolloin myös havainnointi ja reagointitoimet voidaan toteuttaa nopeammin. Esimerkiksi Microsoftin Azure Sentinel on vastaava kaupallinen tuote, jonka avulla voidaan hyödyntää useiden muuttujien vertailua keskenään.

5.5 Kysely SOC-toimijoille

Kybermaailmassa hyökkääjiä on monesti useita, ja jokaisella toimijalla voi olla omat tapansa suorittaakseen kyberhyökkäyksiä. Tästä johtuen myös uhkatietoa on saatavilla runsaasti, minkä perusteella uhkatoimijoita voidaan tunnistaa. Uhkatieto sisältää muun muassa IP-osoitteita, tiivisteitä (engl. hash), URL-osoitteita sekä verkkotunnuksia (engl. domain). Uhkatiedon jakaminen ei itsessään aiheuta vaaraa, vaan sen avulla voidaan puolustautua paremmin, kun tiedetään mahdollisesta hyökkääjästä tietoa.

Suomessa Kyberturvallisuuskeskus toimii tällä hetkellä valtiollisena tiedon jakajana muun muassa uhkatiedon osalta. Sen toiminta perustuu muun muassa valtiolliseen haluun torjua Suomessa haitallista liikennettä ja haittaohjelmia. Kyberturvallisuuskeskus toimii ikään kuin välikätenä yhdistäen muun muassa SOC-toimijoita, joiden kesken esimerkiksi eri huoltovarmuuskriittisten toimijoiden SOC-palveluita tuotetaan. Kyberturvallisuuskeskus jakaa tietoa myös osittain avoimesti esimerkiksi eri raporttien ja uutisten muodoissa. Osa uhkatiedosta Kyberturvallisuuskeskus jakaa kuitenkin

myös luokitellusti, jolloin se ei ole kaikkien saatavilla. Esimerkiksi kaikkein kriittisempää tietoa ei jaeta avoimesti ja sen eteenpäin jakamista valtuutettujen vastaanottajien toimesta voidaan kieltää. Koska uhkatiedon jakaminen ei aiheuta vaaraa, herää kysymys pitäisikö tätä kuitenkin jakaa entistä nopeammin ja mahdollisesti myös suoraan toimijoiden välillä?

On syytä myös olettaa, että Traficomin ja Kyberturvallisuuskeskuksen tilastoista havaitut kiristyshaittaohjelmatapausten kasvu näkyy myös useilla eri toimijoilla SOC-toiminnan kaupallisuuden myötä. Kiristyshaittaohjelmatapausten ollessa erityisen aktiivisia tietyillä toimialoilla, ei tapaukset välttämättä ole lisääntyneet samassa suhteessa toimijoiden kesken.

Kiristyshaittaohjelmien tilannekuvan selvittämiseksi muiden toimijoiden osalta sekä SOC-toimijoiden keskinäisen yhteistyön nykytilan selvittämiseksi toteutettiin opinnäytetyössä kysely ulkoisille SOC-toimijoille. Sähköinen kysely kohdistettiin 8 eri yritykselle Suomessa, jolla on aktiivista SOC/CSOC-toimintaa. Kysely toteutettiin anonyymisti, jolloin yrityksen edustajat voivat antaa rehellisen kuvan kiristyshaittaohjelmien ajankohtaisesta tilanteesta. Kyselyn vastauksia kerättiin yritysten SOC-managereilta tai tietoturvapalveluista vastaavilta henkilöiltä tammi- ja helmikuussa 2022. Kyselyllä pyrittiin kartoittamaan useamman eri organisaation mielipidettä eri SOC-toimijoiden yhteistyön kasvattamiseksi ja uhkatiedon jakamiseksi, sekä kiristyshaittaohjelmien kasvusta aiheutuneita vaikutuksia organisaation SOC:ille. Kyselylomake on opinnäytetyön liitteenä 1.

6 Tulokset

Kiristyshaittaohjelmien osalta tämän otsikon alla esitellään viimeaikaista ja nykyistä kehityssuuntaa, joka on todettu useiden eri julkisten lähteiden, opinnäytetyön toimeksiantajan kautta saadun tilastotiedon, Kyberturvallisuuskeskukselle raportoitujen ilmoitusten määrien, poliisin ilmoitusten sekä SOC-toimijoiden antamien vastauksien perusteella. Aikaisempien julkaistujen artikkelien ja raporttien perusteella voidaan tehdä yhteenveto kiristyshaittaohjelmien tämänhetkisten kohteiden ja yhteisten piirteiden esittämiseksi. Myös SOC-toimijoiden välisen yhteistyön tilan selvittämistä organisaatioiden välillä ja mahdollisia kehittämistoimia tuodaan kyselyn vastauksien perusteella esille.

SOC-toimijoille lähetetyssä kyselyssä saatiin vastauksia 2 kappaletta. Molemmat saadut vastaukset olivat tuloksellisesti toisistaan osittain poikkeavia, erityisesti kyselyn jälkimmäisen osan kannalta,

joka käsitteli SOC-toiminnan yhteistyötä. Kysely lähetettiin sähköpostilla erikseen valitulle kohderyhmälle. Vastausaikaa kyselyssä oli yhteensä kolme viikkoa ja kyselyn vastaukset annettiin noin kahden viikon erolla tammi- ja helmikuussa 2022.

6.1 Kiristyshaittaohjelmien trendi

Kiristyshaittaohjelmien osalta hyökkäysten kehityssuuntana voidaan todeta olevan kasvava viimeisien vuosien aikana, ja erityisesti viimeisen kahden vuoden aikana tapausmäärien suhteen kasvu on ollut räjähdysmäistä. Kiristyshaittaohjelmat eivät kuitenkaan ole olleet jatkuvassa kasvussa, vaan suurimassa osassa tarkastelussa käytetystä datasta on huomattavissa aaltomainen muutosefekti. Esimerkiksi Telia Cygaten herätemäärät sekä Kyberturvallisuuskeskuksen tikettimäärät ja Autoreporter-palvelun ilmoitusmäärät noudattavat aaltoefektiä, jotka ovat ajallisesti ja kehityssuunnaltaan hyvin samantapaisia. Merkittävänä havaintona on kuitenkin viimeisen kahden vuoden aikana havaittu jyrkkä ilmoitus- ja havaintomäärien kasvu.

Tyypillisesti kyberturvallisuuden suhteen eri haittaohjelmat ja hyökkäysmetodit ovat vaihtuneet nopeilla muutamien vuosien ajanjaksoilla, on kiristyshaittaohjelmat myös samoin muuttaneet erityisen aktiivisia aikojaan. Opinnäytetyön tarkastelujaksossa käytetty viiden vuoden ajanjakso huomioi erityisesti WannaCry:n aktiivisuuden vuoden 2017 aikana sekä vuoden 2019 jälkeen alkanut kiihtyvä kasvu kiristyshaittaohjelmien käytössä.

Poliisille ilmoitettujen rikosten tilastoja tarkastellessa huomataan, että monien rikosnimikkeiden kohdalla esiintyy myös aaltoefekti viiden vuoden tarkastelujakson aikana. Erityisesti tietojärjestelmän häirinnän, törkeän tietomurron, tietomurron yrityksen sekä datavahingonteon osalta muutokset ovat olleet muista poikkeavia edellisiin vuosiin verrattuna. Perustasoinen tietomurto, joka koskee suurintaosaa ilmoituksista, on kuitenkin ollut vuosittain kasvavassa vauhdissa, eikä efektiä ole tässä nähtävissä. Varsinkin kohdennetuissa kiristyshaittaohjelmahyökkäyksissä, kuten esimerkiksi Savonian ammattikorkeakoulun tapauksessa, alustavat rikosnimikkeet ovat usein törkeitä. Koska rikostilastot sisältävät myös muita kuin kiristyshaittaohjelmista johtuvia rikoksia, on pelkän kyseisen tilaston pohjalta vaikea arvioida kiristyshaittaohjelmien kasvua. Kuitenkin kasvavat määrät eri tietotokone- ja tietotekniikkajärjestelmiin kohdistuvista rikoksista sekä asiantuntijanlausunto tukevat myös käsitystä kiristyshaittaohjelmien viimeaikaisesta kasvusta, erityisesti vuodesta 2019 alkaen.

ENISA:n sekä CISA:n raportoimat havainnot kiristyshaittaohjelmien kasvun suhteen ovat myös linjassa aikaisempien havaintojen suhteen. Molemmat toimijat ovat raportoineet kiristyshaittaohjelmien kasvusta, kehityksestä sekä laajuuden muuttumisesta ja nostaneet sen uhkakuvaksi myös tulevaisuudessa. CISA on julkaissut oman oppaan kirityshaittaohjelmien vuoksi (Ransomware Guide 2020) monien muiden toimijoiden tapaan, ja ENISA on puolestaan tunnistanut vuosiraportissaan kiristyshaittaohjelmat yhdeksi suurimmaksi uhaksi viime vuosilta.

Myös SOC-toimijoille suunnatussa kyselyssä molemmat vastaajat totesivat kyselyn ensimmäisessä kysymyksessä kiristyshaittaohjelmien lisääntyneen SOC-toiminnassa viimeisen viiden vuoden aikana. Toinen vastaajista avasi tarkemmin myös kehityssuuntaa ja toimialakohtaista tilannetta. Vastaaja totesi, että noin viisi vuotta sitten havaittiin selvä ylöspäin suuntautunut muutos onnistuneissa kiristyshaittaohjelmahyökkäyksissä, mutta viimeisen vuoden aikana onnistuneiden tapausten suhteen kehityssuunta on ollut laskeva. Vastaaja nosti esiin myös näkökohdan, jonka mukaan onnistuneiden kiristyshaittaohjelmahyökkäysten määrä ei ole vähentynyt, mutta henkilöstön koulutus on onnistunut torjumisen suhteen. Vastaaja ei havainnoinut erityisiä tiettyjä toimialakohtaisia muutoksia hyökkäysten suhteen, vaan torjuntaa on tehty lähes kaikilta osa-alueilta.

Uhkatason arvioinnissa molemmilla kyselyn vastaajilla oli kuitenkin selkeä eroavaisuus. Kyselyn toinen vastaaja, joka avasi kehityssuuntaa tarkemmin aikaisemmin, arvioi kiristyshaittaohjelmien uhkatason SOC-toiminnassa suureksi, kun taas toinen vastaajista arvioi uhan pieneksi. Vastauksien eroavaisuus voi selittyä esimerkiksi puolustettavien tietojärjestelmien eroavaisuudella sekä hyökkääjien intresseillä, jolloin kiristyshaittaohjelmahyökkäykset eivät jakaudu tasaisesti SOC-toimijoiden välillä.

Nymaim-haittaohjelman aktivoitumisen suhteen molemmat vastaajat eivät olleet havainneet aktiivisuuden lisääntymistä omassa SOC-toiminnassaan. Vastaus voi selittyä myös torjuntatoimenpiteiden onnistumisilla, sillä kyseessä on vanha haittaohjelma, josta on paljon tunnistetietoja saatavilla. Tällöin itse haittaohjelma ei pääse vaikuttamaan kohdejärjestelmiin, kun ohjelman suorittaminen estetään EDR-työkalujen avulla. Toinen vastaajista kertoi myös viitteistä Qakbot-haittaohjelmaperheen ja Everest-kiristyshaittaohjelmaryhmittymään kysyttäessä muiden kiristyshaittaohjelmien korostumisesta SOC-toiminnassa. Vastaaja kuitenkin korosti, että hyökkäykset on tyypillisesti havaittu jo ennen kuin ne pääsevät itse kiristyshaittaohjelman suorittamiseen asti.

6.2 Hyökkäysten kohteet ja yhteiset piirteet

Kiristyshaittaohjelmien osalta hyökkäyksissä on poikkeuksetta hyödynnetty uhrin heikkoa tietoturvaa. Erityisesti eri kiristyshaittaohjelmaryhmittyvät etsivät tarkoituksellisesti helppoja uhreja, jotka ovat esimerkiksi jättäneet internettiin avoimia haavoittuvia palveluja. Myös vanhentuneet päivittämättömät sovellukset ovat hyökkääjille erinomaisia kohteita, sillä niistä löytyy ajan kuluessa yhä enemmän haavoittuvuuksia. Esimerkiksi Colonial Pipeline tapauksessa käytettiin julkisten lähteiden mukaan hyökkääjien toimesta tätä taktiikkaa.

Yrityksen tai organisaation olisi syytä myös panostaa henkilöstön koulutukseen tietoturvan suhteen. Loppukäyttäjää voidaan hyväksikäyttää myös kiristyshaittaohjelmien saamiseksi haluttuun järjestelmään sisään. Eri haittaohjelmatoimijat lähettävät kohdennetusti yrityksen henkilöstölle huijaustarkoituksessa sähköposteja, joiden avulla pyritään saamaan joko käyttäjätunnuksia haltuun tai asennuttamaan käyttäjän päätelaitteelle haittaohjelma. Tätä tapaa on hyödynnetty myös kiristyshaittaohjelmien saamiseksi haluttuun kohteeseen, sillä se on yleensä nopea ja helppo toteuttaa. Sähköpostikampanjat tapana ei ole uusi ongelma, mutta edelleen varsin aktiivinen tapa uhkatoimijoiden toimesta. Myös kehittyneiden kiristyshaittaohjelmien osalta on havaittavissa, että hyökkäyksen kaikki vaiheet halutaan suunnitella ja kehittää entistä huolellisemmin, jolloin myös ensimmäisen vaiheen sähköpostiviestit on luotu mahdollisimman aidoiksi erehdyttämään käyttäjä.

Kiristyshaittaohjelmien toiminta ei kuitenkaan rajoitu vain tietyille toimialoille, vaan uhka on olemassa jokaisella toimialalla. Uhkatasoissa on kuitenkin eroja ja etenkin terveydenhuoltoalan, asiantuntijaalan sekä kuluttajapalvelut olivat vuonna 2020 ja 2021 kiristyshaittaohjelmista eniten kärsiviä toimialoja (ks. kuvio 6 ja 7). Myös koulutustoimintaan on havaittavissa selkeää kohdennettua kiristyshaittaohjelmatoimintaa maailmanlaajuisesti ja myös CISA on todennut tämän yhteenvedossaan muun muassa Iso-Britannian kohdalla (Alert (AA22-040A) 2022). Oppilaitokset nähdään helppoina uhreina päästä haluttuihin tietoihin käsiksi esimerkiksi tietämättömien oppilaiden tai henkilökunnan kautta sekä mahdollisesti käyttäjäystävällisemmän mutta samalla tietoturvattomamman ympäristön vuoksi. Koulutusympäristöt sisältävät myös arvokasta tietoa hyökkääjille, joiden avulla hyökkääjien lunnasvaatimuksiin voidaan suostua helpommin.

Viimeisimpien raporttien mukaan myös vuoden 2021 osalta kiristyshaittaohjelmia käytettiin myös laajasti eri toimialoja vastaan. Suurimmat kohteet toimialoittain ovat olleet yhä edellä mainittuja,

mutta järjestykset kärkikohteissa vaihtuvat kuitenkin nopeilla aikajaksoilla. Esimerkiksi vuoden 2021 viimeisellä neljänneksellä asiantuntijapalvelut kokivat selkeästi eniten kiristyshaittaohjelmia noin 20 prosentin osuudella, kun taas terveydenhuoltoon kohdistuvat hyökkäykset olivat pudonneet alle 8 prosenttiin (Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021 2022).

6.3 SOC-toimijat

SOC-toimijoiden toimintatavat voivat vaihdella käytössä olevien työkalujen sekä ohjeistuksen vuoksi. Kiristyshaittaohjelmien osalta jokin toimintamalli voi toimia paremmin kuin toinen, joka vaikuttaa muun muassa ajallisesti, miten nopeasti SOC kykenee reagoimaan kiristyshaittaohjelman tuottamaan uhkaan. Vaikka kaikki toimijat pyrkivät samaan lopputulokseen estäessä kyberuhkien pääsyn valvottuun ympäristöön, korostuu nykypäivänä entistä enemmän SOC-toimijoiden kyky havainnoida todelliset uhat ja reagoida niihin tarvittavan nopeasti. Tällä voi olla merkittävä rooli myöhemmin todellisen uhan aiheuttamien seurauksien tarkastelussa. Tämän vuoksi opinnäytetyön kolmantena tutkimuskysymyksenä nousi esiin SOC-toiminnan kehittäminen ja reagoinnin parantaminen kiristyshaittaohjelmahyökkäyksiä vastaan.

6.3.1 SOC-toimijoiden yhteistyö

Opinnäytetyön yhtenä näkökulmana oli syytä tarkastella SOC-toimijoiden välistä yhteistyötä. SOC-toimijoiden välinen perusteellinen yhteistyö voidaan kokea hyödylliseksi varsinkin kasvavien ja massiivisempien kyberuhkakuvien mahdollisessa realisoitumisessa. Yhteistyön tilan selvittämiseksi opinnäytetyössä lähetetty kyselyn loppuosa sisälsi kysymyksiä, jonka pohjalta arvioitiin nykyistä tilaa sekä mahdollisia kehittämistarpeita.

SOC-toimijat ovat nykyisellä toimintamallilla melko itsenäisiä toimijoita omina organisaatioina. Tähän on syynä muun muassa kilpailutilanne yrityksien välillä, jolloin kilpailijalle ei haluta luovuttaa tietoa. Organisaatioiden välissä toimii yhdistävänä tekijänä tällä hetkellä Kyberturvallisuuskeskus, joka pyrkii puolueettomasti parantamaan kansallista kyberturvallisuutta. Kyberturvallisuuskeskus jakaa myös tietoa, jonka se luokittelee omien tiedonvaihtokäytäntöjen mukaisesti.

Kyselyssä kuudentena kohtana esitettiin toimijoille kysymys halusta kasvattaa SOC-organisaatioiden keskinäistä yhteistyötä. Etuna tämän tapaisessa toiminnassa olisi muun muassa yritysten välisen tiedon nopeampi levitettävyys ja yhteisten toimivien työkalujen hyödyntäminen. Kyselyn toinen vastaajista halusi kasvattaa yhteistyötä, kun taas toinen vastaaja ei osannut sanoa. Yhteistyön kasvattamista kannattanut vastaaja totesi jatkokysymyksessä yhteistyön kasvattamisesta seuraavasti, kun kysyttiin miten sekä minkä osa-alueiden yhteistyötä pitäisi kasvattaa.

> *Ehdottomasti pitäisi, kaikilla osa-alueilla. Olen itse yrittänyt omien tuttujeni kautta saada moista tapahtumaan, mutta toistaiseksi se ei ole ottanut tuulta alleen. Tiedän että halukkaita ja kiinnostuneita on, mutta koska osallistujat työskentelevät tietoturvan parissa, on se myös meidän kompastuskivi. Kukaan ei ole valmis kertomaan mitään omasta toiminnastaan, ettei a. hyökkääjä saa tuota tietoa, b. ettei kilpailija saa etua, c. lisää foliota. Uskon että se on tehtävissä, mutta voi olla välttämätöntä saada osallistujat allekirjoittamaan NDA:n vähintään.*

Kyselyn toinen vastaajista, kuka ei osannut sanoa yhteistyön kehittämiseen vastausta, toi esille erilaisen näkökulman tiedonjaon suhteen.

> *Huom: nykyinen tiedonjako tapahtuu KTK:n kautta, mikä ei ole välttämättä ollenkaan huono ratkaisu ottaen huomioon eri SOC-toimijoiden kilpailutilanteen.*

Kyselyn tuloksista SOC-yhteistyön suhteen on havaittavissa eroavaisuuksia mielipiteiden välillä. Kyselyn pienellä otannalla on kuitenkin vaikea arvioida luotettavasti, miten yhteistyön kasvattaminen koetaan. Tämän seurauksena kyselyn kohderyhmän ja vastausmäärien tulisi olla suurempia, jotta saadaan parempi käsitys yhteistyön toimivuudesta. Kuitenkaan nykyistä mallia, jossa tiedoksianto tapahtuu Kyberturvallisuuskeskuksen kautta, ei myöskään kritisoitu. Kyseinen malli on kehitetty toimimaan nykyisessä kilpailutilanteessa tehokkaasti, joka poistaa samalla ensimmäisen vastaajan mainitsemia kompastuskiviä toimijoiden väliltä.

6.3.2 Reagoinnin parantaminen

SOC-toiminnassa riittävän nopea reagointi on yksi tärkeimmistä tekijöistä uhkien torjunnassa. Uhkatoimijoiden ryhmittyessä, hyökkäysten automatisoituessa ja hyökkäysten kohdentuessa entisestään vähentävät nämä SOC-toiminnassa käytössä olevaan aikaan havaita, tunnistaa sekä torjua hyökkäykset. Esimerkiksi pahimmissa tapauksissa SOC-toimijoilla on vain minuutteja aikaa suorittaa alkutoimenpiteet, jos hyökkäyksen aiheuttamat haitat halutaan minimoida.

Valvottavien ympäristöjen lisääntyessä korostuu SOC-toiminnassa optimoitu herätehallinta. Vähäisillä asiantuntevilla henkilöstöresursseilla ongelmaksi voi muodostua herätemäärien liiallinen kasvu, jolloin SOC ei kykene enää tunnistamaan hälytysten joukosta oikeita uhkia ja reagoimaan näihin riittävän nopeasti. Riittävän henkilöstön varmistaminen ja osaamistason ylläpitäminen auttaa SOC-henkilöstöä priorisoimaan jo ensihavainnoista alkaen todelliset uhat.

SOC:in käytössä olevien työkalujen on myös syytä olla tehokkaita ja ajanmukaisia. Tietoturva-analyytikko kykenee myös hahmottamaan tilannekuvan nopeammin, kun kaikki tapaukseen liittyvä data on tarkasteltavissa yhden portaalin tai työkalun kautta samasta näkymästä. Myös mahdolliset ensitoimenpiteet, kuten esimerkiksi verkkolaitteen eristäminen verkosta, on syytä olla selkeästi toteutettavissa mieluiten samojen työkalujen avulla. Useamman eri käyttöliittymän tai hallintajärjestelmän kautta tehty tietoturvauhan analysointi hidastaa ja vaikeuttaa toimenpiteiden suorittamista.

Uhkatilanteiden sattuessa myös valmiiksi kehitetyt automaatiotoimet ovat erittäin hyödyllisiä vasteaikojen pienentämisessä sekä henkilöstön työmäärän vähentämisessä. Automaatiojärjestelmien riittävällä integroinnilla ja kehittämisellä voidaan valvoa monivaiheisten toimenpiteiden sekä prosessien suorittamista, mikä on varsinkin edistyneissä kiristyshaittaohjelmahyökkäyksissä yleistä. Nämä voivat sisältää samanaikaisesti esimerkiksi useiden epätyypillisten prosessien suorittamista, yhteydenottoyrityksiä internettiin IP-osoitteisiin ja sivuttaissuuntaista verkkoliikennettä sisäverkossa.

6.3.3 Kehittäminen tulevaisuudessa

SOC-toiminnan kehittämisen osalta tulevaisuudessa nousee erityisesti esiin uhkatiedon jakamisen tarve. Verkkoympäristöjen puolustajille nopealla uhkatiedon saannilla ja hyödyntämisellä on suuri merkitys, kun pystytään varautumaan ja estämään jo ennakkoon haitallisiksi havaitut toimijat sekä ohjelmat. SOC-toimijoille suunnatussa kyselyssä kysyttiinkin kahdeksantena kysymyksenä uhkatiedon laajemman jakamisen suhteen mielipidettä. Kyselyn molemmat vastaajat kannattivat laajempaa jakamista SOC-toimijoiden välillä.

Ensimmäinen vastaaja nosti jatkokysymyksessä esiin IoC-tietojen jakamisen, eli esimerkiksi haitalliseksi todetut IP-osoitteet, ohjelmien tiivistearvot sekä URL-osoitteet. Ongelmana nousee kuitenkin esiin, että varsinkin uusien toimijoiden ja esimerkiksi heidän käyttämiään IP-osoitteita on hankala pystyä todistamaan IoC-toimeksi, ennen kuin sitä on käytetty jotain uhria vastaan. Toisaalta nopealla IoC-tietojen jakamisella pystytään pienentämään riskiä useampiin organisaatioihin kohdistuvien hyökkäyksien osalta.

Kyselyn toinen vastaajista nosti esiin jatkokysymyksessä, että uhkatiedon olisi syytä sisältää tunnistamatonta uhkatietoa liian pitkälle edenneistä tapauksista. Nimettömänä jaettu tieto voisi kannustaa organisaatioita jakamaan myös tietoa herkemmin, kun havaittuja toimia ei pystyttäisi yhdistämään esimerkiksi minkään yrityksen tai asiakkaan liiketoimiin. Toisaalta tämän tyylisessä toiminnassa on oltava tarkka mitä tietoa pystytään jakamaan esimerkiksi hyökkäyksien kulun suhteen, jolloin taas jaetussa uhkatiedossa on riski jäädä liian vähäiseksi, että siitä olisi myös muille riittävää hyötyä.

7 Pohdinta

Opinnäytetyössä käytettiin soveltavaa tutkimusta, jonka tavoitteena oli selvittää realiteetteja toimeksiantajan määrittämiin tutkimuskysymyksiin tutkimalla nykytilannetta ja viime vuosien tapahtumia. Näiden pohjalta oli tarkoituksena vastata tutkimuskysymyksiin ja luoda niiden pohjalta ratkaisuehdotuksia tutkimuskysymyksissä koettuihin haasteisiin. Kaikkiin tutkimuskysymyksiin onnistuttiin saamaan vastauksia, mutta varsinkin toisen tutkimuskysymyksen kohdalla yhteisten piirteiden löytäminen kiristyshaittaohjelmahyökkäyksistä osoittautui odotettua vaikeammaksi, sillä julkisten lähteiden perusteella hyökkäyksistä oli hankala saada riittävästi luotettavaa tietoa. Ongelmana myös viimeaikaisten hyökkäysten osalta oli edelleen aktiivisesti käynnissä olleet tutkinnat, jonka vuoksi tarvittavia tietoja ei ole ollenkaan saatavilla julkisesti. Kuitenkin yleisenä piirteenä tutkimuskysymyksen osalta pysyttiin todentamaan, että kiristyshaittaohjelmathyökkäyksissä on viime aikoina hyödynnetty erityisesti internettiin auki olevia etäyhteyksiä, sähköpostikampanjoita ja haavoittuvia sovelluksia.

Kiristyshaittaohjelmahyökkäysten nykytilan selvittämisessä onnistuttiin tutkimusmateriaalin avulla todistamaan hyökkäysten kasvavaa määrää. Lähes kaikki vertailussa tutkittu materiaali osoitti sen, että kiristyshaittaohjelmahyökkäykset ovat viimeisen viiden vuoden aikana kasvaneet ja erityisesti

viimeisen kahden vuoden aikana. Tutkimuskysymys osoittautui myös äärimmäisen ajankohtaiseksi aiheeksi, sillä mediassa uutisointi kiristyshaittaohjelmien osalta on muuttunut lähes arkipäiväiseksi ja ne tavoittavat entistä enemmän lukijoita. Selvityksen pohjalta opinnäytetyön lukija kykenee saaman monipuolisen ja useisiin lähteisiin pohjautuvan vertailun kehityskulusta.

SOC-toiminnan reagoinnin parantamista kiristyshaittaohjelmia vastaan pyrittiin tarkastelemaan erityisesti hyödyllisten toimintatapojen sekä SOC-toimijoiden nykytilan suhteen. Tuloksina onnistuttiin antamaan yleistasollisesti ohjeita, miten SOC-toiminnassa pystytään reagointia parantamaan. Konkreettisten ja yksityistasoisten ohjeiden antaminen osoittautui erittäin hankalaksi, sillä SOC-toiminnassa ei ole olemassa julkisesti selkeää yhteistä toimintakuvaa kiristyshaittaohjelmien suhteen, vaan se voi olla jokaisella toimijalla omakehitteinen muun muassa eri työkalujen vuoksi.

SOC-toiminnan kehittämisen suhteen nousi selkeästi esille toimijoiden välisen yhteistyön merkitys. Opinnäytetyössä toimi avainasemassa SOC-toimijoille suunnattu kysely, jonka avulla haluttiin selvittää näkökulmia laajemmin kiristyshaittaohjelmien tilan sekä SOC-toiminnan kehittämisen suhteen. Kyselyn tuloksia tarkasteltaessa kuitenkin ymmärrettiin, että alhaisen vastausmäärän perusteella oli hankala muodostaa riittävää laaja-alaista näkökulmaa kehittämisen suhteen. Kysely olisi pitänyt suunnata suuremmalle kohderyhmälle, jolloin myös mahdollisesti vastausprosentti olisi ollut suurempi ja kehityssuunnan selvittäminen helpompaa. Toisaalta kaksi osittain toisistaan poikkeavaa vastausta toi esille sen, että näkökanta yhteistyön kehittämisen suhteen ei ole yksimielinen ja selkeä.

Yhteistyön parantamisen osalta uhkatiedon jakaminen korostui kuitenkin kyselyssä. Tätä varten SOC-toiminnan kehittämiseksi hyödyllisenä yhteisenä työkaluna voisi olla kaikkien toimijoiden yhteinen MISP-järjestelmä. Kyseessä on ilmainen avoimeen lähdekoodiin perustuva jakamisalusta, joka auttaa jakamaan tietoa uhkien ja kyberturvallisuuden IoC-tiedoista ja muista indikaattoreista (Dulaunoy 2017). Ohjelman ollessa kyberturvallisuudessa muutenkin laajasti käytetty työkalu, olisi sen käyttäminen monille toimijoille helppoa ja integraatiot SOC-toimijoiden omiin järjestelmiin mahdollista. Kyseisen yhteisen järjestelmän hyödyt ja käyttöönotto ilmeni selkeäksi opinnäytetyön jatkokehityskohteeksi.

Työstä erottui selkeästi kaksi erillistä merkittävää käsitettä: Kiristyshaittaohjelma ja SOC. Lisäksi ajankohtainen kyberturvallisuustilanne vaikutti molempien käsitteiden esiintyviin muutoksiin. Selkeän käsitejaon avulla opinnäytteen teoreettiskäsitteelliset lähtökohdat onnistuttiin esittämään työssä erittäin kattavasti luotettavien, monipuolisten ja useiden eri lähteiden avulla. Perusteellisen tietoperustan avulla pystyttiin tukemaan varsinaisten tutkimuskysymysten vastauksien selvittämistä sekä luomaan pohja tutkimusmateriaalin läpikäyntiä ajatellen.

Opinnäytetyön luotettavuutta tarkasteltiin prosessin kaikkien vaiheiden aikana. Luotettavuuden osalta tutkimuksen eri vaiheita kuvattu riittävän selkeästi, kattavasti ja yksityiskohtaisesti, jotta tuloksia pystytään vertailemaan myös muihin vastaaviin tutkimuksiin ja johtopäätöksiin. Luotettavuuden parantamiseksi opinnäytetyön aikana käytettiin paljon luotettavia verkkolähteitä ja ammattialan tutkimusjulkaisuja. Myös useiden eri julkaisujen keskinäisellä vertailulla ja hyödyntämisellä pyrittiin parantamaan tulosten arvoa.

Tutkimuseettisesti opinnäytetyöprosessi onnistuttiin myös toteuttaman huolellisesti. Työssä ei tuotu esille toimeksiantajan liikesalaisuuksia tai tutkimusmateriaalina saatua sensitiivistä informaatiota. Työn aikana kiinnitettiin huomiota erityisesti kerätyn tiedon tunnistamattomuuteen sen osalta, joka ei ollut julkisesti saatavilla.

Opinnäytetyön prosessin aikana ongelmaksi muodostui työn rajaaminen. Käsitteinä kiristyshaittaohjelma sekä SOC-toiminta ovat suuria, jolloin molempien näiden käsitteleminen kasvattivat työn laajuutta. Käsitteet eivät linkity myöskään toisiinsa suoraan, jolloin yhdistävänä tekijänä ollut kyberturvallisuuden tilannekuva toi työhön myös uuden näkökulman. Työssä kerätty tutkimusmateriaali ei myöskään joidenkin näkökulmien kannalta antanut yksiselitteisiä vastauksia, jolloin johtopäätösten tekeminen jätti tulkinnanvaraa ja osa johtopäätöksistä jäi hyvin yleisluontoisiksi. Kokonaisuudessaan kuitenkin kaikkiin opinnäytetyön aikana ilmenneihin kysymyksiin pystyttiin antamaan jonkinlainen vastaus tai ratkaisu, eikä tutkimuskysymykset jääneet selvittämättä.

Lähteet

2021 Trends Show Increased Globalized Threat of Ransomware. 2022. Yhdysvaltain liittovaltion kyberturvallisuusviraston julkaisema raportti kiristysohjelmien lisääntyneen globalisoituneeseen uhkaan. Viitattu 12.2.2022. https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf.

21.4.1995/578. Suomen rikoslain luku 38. Viitattu 12.3.2022. http://www.finlex.fi, ajantasainen lainsäädäntö.

81 % suomalaisista tietoturva-asiantuntijoista ylikuormittuu vääristä hälytyksistä. 2021. Trend Micro yrityksen tilaama tutkimus SOC-päättäjistä. Viitattu 13.1.2022. https://www.mynewsdesk.com/fi/trend-micro-finland/pressreleases/81-percent-suomalaisista-tietoturva-asiantuntijoista-ylikuormittuu-vaeaeristae-haelytyksistae-3102264.

Abrams, L. 2022. New data-wiping malware used in destructive attacks on Ukraine. Viitattu 25.3.2022. https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/.

Alert (AA22-040A). 2022. CISA:n ilmoitus kiristyshaittaohjelmien trendin osoituksista vuoden 2021 osalta. Viitattu 18.3.2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

Al-rimy, M., Maarof, M. & Shaid, S. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Viitattu 15.11.2021. https://www.sciencedirect.com/science/article/pii/S016740481830004X.

Ang, C. 2021. The Most Significant Cyber Attacks from 2006-2020, by Country. Viitattu 25.3.2022. https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/.

Autoreporterin haittaohjelmahavainnot. 2022. Kyberturvallisuuskeskuksen verkkosivulla oleva esittely Autoreporter-työkalun haittaohjelmahavainnoista. Viitattu 6.3.2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot.

Autoreporter-kategoriat. N.d. Kyberturvallisuuskeskuksen verkkosivulla oleva esittely Autoreporter-työkalusta sekä sen kategorioista. Viitattu 6.3.2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporter-kategoriat.

Bertrand, N., Perez, E., Cohen, Z., Sands, G. & Campbell, J. 2021. Colonial Pipeline did pay ransom to hackers, sources now say. Viitattu 5.2.2022. https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html.

Bing, G & Kelly, S. 2021. Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. Viitattu 5.2.2022. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

Chandel, S., Yu, S., Yitian, T., Zhili, Z. & Yusheng, H. 2019. Endpoint Protection - Measuring the effectiveness of remediation technologies and methodologies for insider threat. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 81-82. doi: 10.1109/CyberC.2019.00023. Viitattu 11.1.2022. https://janet.finna.fi/, IEEE.

de Groot, J. 2020. What is a Security Operations Center (SOC). Viitattu 4.10.2021. https://digitalguardian.com/blog/what-security-operations-center-soc.

Drozhzhin, A. 2016. Ransomware's history and evolution in facts and figures. Viitattu 22.1.2022. https://www.kaspersky.com/blog/ransomware-blocker-to-cryptor/12435/.

Dulaunoy, A. 2017. MISP threat sharing platform. Viitattu 20.3.2022. https://media.ccc.de/v/SHA2017-23-misp_threat_sharing_platform#t=199.

Endpoint Security. N.d. Esittelyartikkeli Paloalto yrityksen verkkosivuilla EPP-ratkaisuista ja sen tärkeydestä. Viitattu 11.1.2022. https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-security.

Enisa Threat Landscape 2021. 2021. Euroopan unionin verkko- ja tietoturvaviraston tuottama vuosiraportti vuodelta 2021 kyberturvallisuuden uhkakuvista. doi: 10.2824/324797. Viitattu 13.3.2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Enn, B. 2021. The Colonial Pipeline Hack. Viitattu 5.3.2022. https://medium.com/@brandyhn/the-colonial-pipeline-hack-timeline-and-how-ransom-funds-were-retrieved-887c2de214a0.

Falconer, R. 2021. Emergency declaration issued in 17 states and D.C. over fuel pipeline cyberattack. Viitattu 5.2.2022. https://news.yahoo.com/biden-admin-declares-state-emergency-011332752.html.

FireEye cyber threat map. N.d. Reaaliaikainen kyberuhkien karttakuva FireEye yrityksen verkkosivulla. Viitattu 11.3.2022. https://www.fireeye.com/cyber-map/threat-map.html.

Freed, A. 2021. What is the Dark Web Ransomware Marketplace?. Viitattu 11.2.2022. https://www.cybereason.com/blog/what-is-the-dark-web-ransomware-marketplace.

Fruhlinger, J. 2020. Ransomware explained: How it works and how to remove it. Viitattu 15.11.2021. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

Gast, K. 2021. What is SIEM? And How Does it Work?. Viitattu 10.1.2022. https://logrhythm.com/what-is-siem/.

Goodin, D. 2013. You're infected—if you want to see your data again, pay us $300 in Bitcoins. Viitattu 28.12.2021. https://arstechnica.com/information-technology/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/.

Gregory, J. 2021. What Has Changed Since the 2017 WannaCry Ransomware Attack?. Viitattu 18.2.2022. https://securityintelligence.com/articles/what-has-changed-since-wannacry-ransomware-attack/.

Greig, J. 2022. CISA, FBI warn US orgs of WhisperGate and HermeticWiper malware. Viitattu 12.3.2022. https://www.zdnet.com/article/cisa-fbi-warn-us-orgs-of-whispergate-and-hermeticwiper-malware/.

Haapakangas, K. 2018. Kansainvälinen rikosluokitus auttaa vertailemaan maita ja trendejä. Viitattu 13.3.2022. https://www.tilastokeskus.fi/tietotrendit/artikkelit/2018/kansainvalinen-rikosluokitus-auttaa-vertailemaan-maita-ja-trendeja/.

Harris, S. 2010. CISSP All-in-One Exam Guide. 5. p. McGraw-Hill/Osborne. Viitattu 28.11.2021. https://janet.finna.fi, Skillsoft.

Heikkilä, M. 2020. Nainen kuoli ambulanssiin, kun kyberhyökkäys jumitti saksalaisen sairaalan tietojärjestelmän – syyttäjä avasi harvinaisen henkirikostutkimuksen. Viitattu 5.2.2022. https://yle.fi/uutiset/3-11553530.

Helenius, J. 2022. MS Excel-tiedosto. Poliisille ilmoitettujen rikosten lukumäärä kiristyshaittaohjelman osalta. Saatu sähköpostin liitteenä poliisihallituksen erikoissuunnittelija J. Heleniukselta 7.1.2022.

Hiles, A., FBCI, H. & EloSCM. 2016. Service Level Agreements: A Rothstein publishing collection. Brookfield: Rothstein Publishing. Viitattu 24.10.2021. https://janet.finna.fi, Ebook Central.

History Of Ransomware. 2021. Crowdstrike yrityksen esittely Ransomware haittaohjelman historiasta sekä tulevaisuudesta. Viitattu 3.10.2021. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

How to Create Your Own Ransomware. 2017. BluEnt yrityksen blogikirjoitus kiristyshaittaohjelman rakentamisesta. Viitattu 9.11.2021. https://www.bluent.net/blog/how-to-create-your-own-ransomware/.

Hu, Y. 2017. A brief summary of encryption method used in widespread ransomware. Viitattu 30.11.2021. https://resources.infosecinstitute.com/topic/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/#gref.

Hyvärinen, N. Ransomware Timeline: 2010 – 2017. Viitattu 22.1.2022. https://blog.f-secure.com/ransomware-timeline-2010-2017/.

Jacobs, J., Riley, M. & Turton, W. 2021. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. Viitattu 5.2.2022. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom.

Jauhiainen, J. 2021. MS Excel-tiedosto. Kyberturvallisuuskeskuksen kiristyshaittaohjelmatapauksien määrä. Saatu sähköpostin liitteenä Kyberturvallisuuskeskuksen tietoturva-asiantuntija J. Jauhiaiselta 20.12.2021.

Kaliyaperumal, L. 2020. Evolution Of Security Operations Center. LinkedIn 4.11.2020. Viitattu 12.1.2022. https://www.linkedin.com/pulse/evolution-security-operations-center-lakshminarayanan-kaliyaperumal.

Kansainvälinen rikosluokitus ICCS muuttujina ICCS rikosluokka ja Vuosi. N.d. Suomen virallinen tilasto (SVT): Rikos- ja pakkokeinotilasto. Helsinki: Tilastokeskus. Viitattu 25.10.2021. https://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/.

Kansainvälinen rikosluokitus ICCS muuttujina ICCS rikosluokka ja Kuukausi. N.d. Suomen virallinen tilasto (SVT): Rikos- ja pakkokeinotilasto. Helsinki: Tilastokeskus. Viitattu 25.10.2021. https://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/.

Karlamaa, K. 2022. Ukrainan kriisi heijastuu myös kybermaailmaan. Viitattu 12.3.2022. https://www.ficom.fi/ajankohtaista/uutiset/ukrainan-kriisi-heijastuu-myos-kybermaailmaan/.

Kelly, S. & Resnick-ault, J. 2021. One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. Viitattu 10.2.2022. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

Kiristyshaittaohjelmien kasvava uhka vaatii toimia yritysten ylimmältä johdolta. 2022. Trend Micro yrityksen tiedote koskien yrityksen tuottamaa raporttia. Viitattu 12.2.2022. https://www.mynewsdesk.com/fi/trend-micro-finland/pressreleases/kiristyshaittaohjelmien-kasvava-uhka-vaatii-toimia-yritysten-ylimmaeltae-johdolta-3159052?utm_source=rss&utm_medium=rss&utm_campaign=Alert&utm_content=pressrelease.

Knell, N. 2013. Top 10 Countries Where Cyber Attacks Originate. Viitattu 25.3.2022. https://www.govtech.com/security/hacking-top-ten.html.

Kyberrikokset. N.d. Poliisin verkkosivuilla oleva esittely kyberrikollisuudesta. Viitattu 12.3.2022. https://poliisi.fi/kyberrikokset.

Kybersää Tammikuu. 2022. Kyberturvallisuuskeskuksen julkaisema kybersää-raportti koskien Suomen kyberturvallisuuden tilannetta tammikuussa 2022. Viitattu 12.3.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20tammikuu%202022.pdf.

Kybersää. 2022. Esittelyartikkeli Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen sivulla koskien kyberturvallisuuden tilannekuvaa. Viitattu 24.1.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa.

Kyberturvallisuuskeskus. N.d. Suomen kyberturvallisuuskeskuksen verkkosivuston etusivu. Viitattu 6.3.2022. https://www.kyberturvallisuuskeskus.fi/fi/.

Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021. 2022. Coveware yrityksen viimeinen neljännesvuosiraportti vuodelta 2021 kiristyshaittaohjelmista. Viitattu 20.3.2022. https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021.

Leponen, M. 2021. Opinnäytetyö - Tausta-aineiston saatavuuskysely. Sähköpostiviesti 16.12.2021. Vastaanottaja A. Aarnio. Keskusrikospoliisin rikoskomisarion asiantuntijalausunto kiristyshaittaohjelmien rikoksien tunnusmerkistöjen täyttymistä varten.

Leponen, M. 2021. Opinnäytetyö - Tausta-aineiston saatavuuskysely. Sähköpostiviesti 25.10.2021. Vastaanottaja A. Aarnio. Keskusrikospoliisin rikoskomisarion asiantuntijalausunto kiristyshaittaohjelmien kasvuun liittyen.

Lifecycle of a ransomware incident. N.d. Uuden-Seelannin valtiollisen CERT-toimijan julkaisema kuvaus ihmisohjatun kiristyshaittaohjelmahyökkäyksen etenemisestä. Viitattu 27.3.2022. https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident.pdf.

List of SOC service providers. 2021. Verkkosivusto, jossa luettelo Security Operation Center (SOC) -yrityksistä Suomessa. Viitattu 12.1.2022. https://csoc.fi/.

Live Ransomware Updates. N.d. Listaus viimeisimmistä raportoiduista kiristyshaittaohjelmahyökkäyksistä Ransomware Database sivustolla. Viitattu 12.2.2022. https://www.ransom-db.com/real-time-updates.

Log4j Zero-Day Vulnerability Response. 2022. Artikkeli CIS-verkkosivulla koskien Log4j haavoittuvuutta. Viitattu 12.3.2022. https://www.cisecurity.org/log4j-zero-day-vulnerability-response.

Loman, M. 2019. How Ransomware Attacks. Viitattu 27.12.2021. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-ransomware-behavior-report.pdf.

Lu, G., Liu, Y., Chen, Y., Zhang, C., Gao, Y. & Zhong, G. 2020. A Comprehensive Detection Approach of Wannacry: Principles, Rules and Experiments. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 41-49. doi: 10.1109/CyberC49757.2020.00017. Viitattu 15.11.2021. https://janet.finna.fi/, IEEE.

Marinho, T. 2018. Ransomware encryption techniques. Viitattu 30.11.2021. https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9.

Martin, N. 2021. Why hackers rely on Bitcoin for ransom payments. Viitattu 28.12.2021. https://www.dw.com/en/why-hackers-rely-on-bitcoin-for-ransom-payments/a-58213490.

Microsoft Digital Defense Report. 2021. Microsoftin tietoturvaasiantuntijoiden tuottama raportti puolustautumisesta kyberuhkia vastaan. Viitattu 26.3.2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

Nymaim – obfuscation chronicles. 2013. Welivesecurity sivuston artikkeli Nymaim-kiristyshaittaohjelma analyysistä. Viitattu 6.3.2022. https://www.welivesecurity.com/2013/08/26/nymaim-obfuscation-chronicles/.

Opinnäytetyö - tausta-aineiston saatavuus. 2021. Sähköpostiviestiketju Kyberturvallisuuskeskuksen ja Arttu Aarnion välillä 13.10.2021–20.12.2021. Saatu sähköpostina Kyberturvallisuuskeskuksen tietoturva-asiantuntija J. Jauhiaiselta 20.12.2021.

Palozza, F. 2018. The Origin of Ransomware and Its Impact on Businesses. Viitattu 22.1.2022. https://blog.radware.com/security/2018/10/origin-of-ransomware/.

Partida, D. 2021. 5 Reasons we're seeing more ransomware attacks than ever before. Viitattu 23.1.2022. https://cybersecurity.att.com/blogs/security-essentials/5-reasons-were-seeing-more-ransomware-attacks-than-ever-before.

Pilkey, A. 2017. What the GDPR says about ransomware. Viitattu 12.3.2022. https://blog.f-secure.com/what-the-gdpr-says-about-ransomware/.

Pompon, R. 2020. Ransomware: How It Has Evolved to Be Faster, Stealthier, and Strike Harder. Viitattu 19.11.2021. https://www.f5.com/labs/articles/threat-intelligence/ransomware-how-it-has-evolved-to-be-faster-stealthier-and-strike-harder.

Ransomware Attack – What is it and How Does it Work. N.d. Checkpoint yrityksen esittelyartikkeli kiristyshaittaohjelmasta sekä sen toiminnasta. Viitattu 15.11.2021. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

Ransomware Groups. N.d. Listaus viimeisimmistä aktiivisista raportoiduista kiristyshaittaohjelmatoimijoista Ransomware Database sivustolla. Viitattu 12.2.2022. https://www.ransomdb.com/ransomware-groups.

Ransomware Guide. 2020. Yhdysvaltain kyberturvallisuus ja infrastruktuurin turvallisuusviraston julkaisema kiristyshaittaohjelma opas. Viitattu 9.11.2021. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands. 2021. Coveware yrityksen kvartaaliraportti kiristyshaittaohjelmista vuodelta 2020. Viitattu 23.1.2022. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.

Ransomware. N.d. Austraalian kyberturvallisuuskeskuksen artikkeli kiristyshaittaohjelmasta. Viitattu 9.11.2021. https://www.cyber.gov.au/ransomware.

Redfern, E. 2021. The Yahoo Cyber Attack & What should you learn from it?. Viitattu 17.10.2021. https://www.cashfloat.co.uk/blog/technology-innovation/yahoo-cyber-attack/.

Rytkönen, A. 2022. Tietomurrossa uusi käänne: Savonian opiskelijoiden tietoja julkaistiin Tor-verkossa. Viitattu 12.3.2022. https://yle.fi/uutiset/3-12319469.

Salokangas, K. & Remes, M. 2022. Savonia-ammattikorkeakouluun tehty massiivinen tietoturvahyökkäys – kiristysohjelma lukinnut tietoja. Viitattu 22.2.2022. https://yle.fi/uutiset/3-12302764.

Scarfone, K. & Mell, P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). Viitattu 11.1.2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

Schofield, J. 2016. How can I remove a ransomware infection?. Viitattu 9.11.2021. https://www.theguardian.com/technology/askjack/2016/jul/28/how-can-i-remove-ransomware-infection.

Schwartz, S. 2021. Identity crisis: Why ransomware groups rebrand — and disappear. Viitattu 30.11.2021. https://www.cybersecuritydive.com/news/ransomware-ryuk-conti-revil-2021/608845/.

Security Information and Event Management system. N.d. Esittely SIEM järjestelmästä Metastore yrityksen verkkosivulla. Viitattu 25.10.2021. https://www.metastore.eu/security/security-operations/siem/.

Security Operations on the backfoot. 2021. Trend Micro yrityksen tilaama tutkimus SOC-toiminnasta ja henkilöstöstä. Viitattu 13.1.2022. https://www.trendmicro.com/explore/en_gb_soc-research/00792-v1-en-tmr.

Segers, G. 2021. Cyberattack prompts major pipeline operator to halt operations. Viitattu 5.2.2022. https://www.cbsnews.com/news/colonial-pipeline-cyberattack-shut-down/.

Selvitettyihin rikoksiin syylliseksi epäillyt kansainvälisen rikosluokitukset ICCS mukaan, 2013-2020. N.d. Tilastokeskuksen verkkohakupalvelu tilastotietokannoille. Viitattu 13.3.2022. https://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin__oik__rpk__kans/statfin_rpk_pxt_11tb.px/.

SIEM Architecture: Technology, Process and Data. N.d. Artikkeli Exabeam-verkkosivustolla. Viitattu 10.1.2022. https://www.exabeam.com/siem-guide/siem-architecture/.

Singh, A. 2021. Guide to How to Recover and Prevent a Ransomware Attack. Viitattu 23.1.2022. https://www.backblaze.com/blog/complete-guide-ransomware/.

Smith, S. 2021. Managed security service provider (MSSP). Viitattu 24.10.2021. https://searchitchannel.techtarget.com/definition/MSSP.

SOC as a service. 2021. Telia Cygaten esittely tarjoamastaan SOC toiminnasta yrityksen verkkosivulla. Viitattu 3.10.2021. https://www.teliacygate.fi/fi/tietoturvapalvelut/soc-as-a-service.

Statement: Data breach in India. 2022. Huhtamäki-yrityksen virallinen tiedote tietomurrosta yrityksen verkkosivuilla. Viitattu 11.2.2022. https://www.huhtamaki.com/en/highlights/recent/statement-data-breach-in-india/.

Telia Cygate. 2021. Toimeksiantaja Telia Cygaten yritysesittely yrityksen verkkosivulla. Viitattu 3.10.2021. https://www.teliacygate.fi/fi/lyhyesti-meista.

The Impact of Ransomware. N.d. Artikkeli Ascend yrityksen verkkosivuilla kiristyshaittaohjelmien vaikutuksista. Viitattu 23.1.2022. https://www.ascenditsolutions.com/blog/executive-summary/65-the-impact-of-ransomware.

The Modern Security Operations Center, SecOps and SIEM: How They Work Together. N.d. Artikkeli Exabeam-verkkosivustolla. Viitattu 25.10.2021. https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/.

Top 15 Best Managed Security Service Providers (MSSPs) In 2022. 2022. Listausartikkeli suurimpien MSSP-palveluiden tuottajista maailmalla. Viitattu 12.1.2022. https://www.softwaretesting-help.com/managed-security-service-providers/.

Torres, A. 2015. Building a World-Class Security Operations Center: A Roadmap. SANS Institute. Viitattu 24.10.2021. https://www.academia.edu/38868050/Building_a_World_Class_Security_Operations_Center_A_Roadmap.

Tutkimusasetelma. N.d. Jyväskylän ammattikorkeakoulun ohjeet opinnäytetyön tutkimusasetelmasta. Viitattu 10.10.2021. https://oppimateriaalit.jamk.fi/raportointiohje/4-opinnaytetyon-rakenne/4-2-opinnaytetyon-runko-osa/4-2-4-tutkimusasetelma/.

Työelämän tutkiva kehittämistoiminta. N.d. Jyväskylän ammattikorkeakoulun ohjeistus tutkivasta kehittämistoiminnasta. Viitattu 10.10.2021. https://oppimateriaalit.jamk.fi/yamk-kasikirja/tyoelaman-tutkiva-kehittamistoiminta/.

Vielberth, M., Böhm, F., Fichtinger, I. & Pernul, G. 2020. Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, 8, 227756-227779. doi: 10.1109/ACCESS.2020.3045514. Viitattu 4.10.2021. https://janet.finna.fi/, IEEE.

Virtanen, J. 2021. Venäläiset saivat maistaa omaa lääkettään – pahamaineinen roistojoukko sai netistä kenkää, johtaja pakeni. Viitattu 11.2.2022. https://www.tivi.fi/uutiset/venalaiset-saivat-maistaa-omaa-laakettaan-pahamaineinen-roistojoukko-sai-netista-kenkaa-johtaja-pakeni/7fe52592-71a5-486e-96d2-724bd82ec62f.

Volz, D. 2016. Yahoo says hackers stole data from 500 million accounts in 2014. Viitattu 17.10.2021. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P.

Webb, N. 2021. Remove COOL Ransomware Virus (DECRYPT .cool FILES). Viitattu 28.12.2021. https://geeksadvice.com/remove-cool-ransomware-virus/.

What is cybersecurity?. N.d. Artikkeli IBM yrityksen verkkosivulla koskien yleistä kyberturvallisuutta. Viitattu 24.1.2022. https://www.ibm.com/topics/cybersecurity.

What Is Network Traffic Analysis?. N.d. Esittelyartikkeli Cisco yrityksen verkkosivuilla NTA-ratkaisuihin liittyen. Viitattu 10.1.2022. https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html#~nta-features.

What Ransomware Allows Hackers to Do Once Infected. N.d. Checkpoint yrityksen esittelyartikkeli kiristyshaittaohjelman pääsystä tietoihin käsiksi. Viitattu 15.11.2021. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/what-ransomware-allows-hackers-to-do-once-infected/.

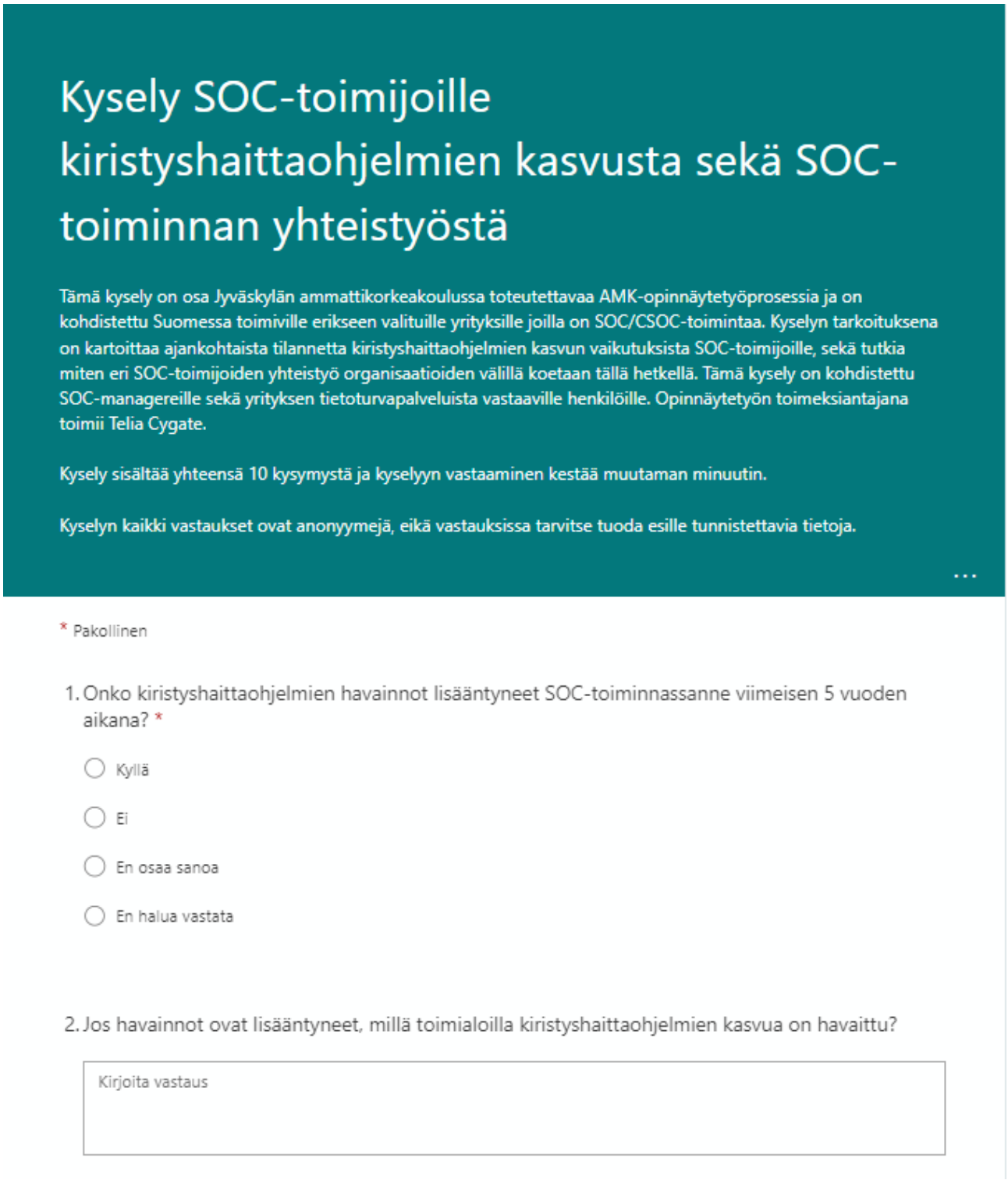
Why is a soc (Security Operations Center) essential today?. 2020. Artikkeli Linkbynet yrityksen verkkosivustolla SOC toiminnasta. Viitattu 17.10.2021. https://www.linkbynet.com/en/news/why-is-a-soc-essential-today.

Yoo, G. 2021. The Importance Of Time And Speed In Cybersecurity. Viitattu 17.10.2021. https://www.forbes.com/sites/forbestechcouncil/2021/01/22/the-importance-of-time-and-speed-in-cybersecurity/?sh=726ac7a436a9.

Zimmerman, C. 2014. Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE. Viitattu 24.10.2021. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

Liitteet

Liite 1. Kysely SOC-toimijoille



Kysely SOC-toimijoille kiristyshaittaohjelmien kasvusta sekä SOC-toiminnan yhteistyöstä

Tämä kysely on osa Jyväskylän ammattikorkeakoulussa toteutettavaa AMK-opinnäytetyöprosessia ja on kohdistettu Suomessa toimiville erikseen valituille yrityksille joilla on SOC/CSOC-toimintaa. Kyselyn tarkoituksena on kartoittaa ajankohtaista tilannetta kiristyshaittaohjelmien kasvun vaikutuksista SOC-toimijoille, sekä tutkia miten eri SOC-toimijoiden yhteistyö organisaatioiden välillä koetaan tällä hetkellä. Tämä kysely on kohdistettu SOC-managereille sekä yrityksen tietoturvapalveluista vastaaville henkilöille. Opinnäytetyön toimeksiantajana toimii Telia Cygate.

Kysely sisältää yhteensä 10 kysymystä ja kyselyyn vastaaminen kestää muutaman minuutin.

Kyselyn kaikki vastaukset ovat anonyymejä, eikä vastauksissa tarvitse tuoda esille tunnistettavia tietoja.

...

* Pakollinen

1. Onko kiristyshaittaohjelmien havainnot lisääntyneet SOC-toiminnassanne viimeisen 5 vuoden aikana? *

- ○ Kyllä
- ○ Ei
- ○ En osaa sanoa
- ○ En halua vastata

2. Jos havainnot ovat lisääntyneet, millä toimialoilla kiristyshaittaohjelmien kasvua on havaittu?

Kirjoita vastaus

3. Kuinka suureksi arvioisit kiristyshaittaohjelman aiheuttaman hyökkäyksen uhkatason SOC-toiminnassanne? *

- ◯ Suuri
- ◯ Keskitaso
- ◯ Pieni
- ◯ Ei ollenkaan uhka
- ◯ En halua vastata

4. Viimeisen kahden vuoden aikana Nymaim-nimisen kiristyshaittaohjelman tapauksia on rekisteröity Traficomin avoimen tietokannan mukaan merkittäviä määriä enemmän Suomessa verrattuna edellisiin vuosiin. Onko kyseisen kiristyshaittaohjelman aktivoituminen näykynyt SOC-toiminnassanne? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa
- ◯ En halua vastata

5. Ovatko jotkut muut kiristyshaittaohjelmat/ryhmittymät erityisesti korostuneet SOC-toiminnassanne?

Kirjoita vastaus

6. Pitäisikö Suomessa toimivien SOC-toimijoiden kasvattaa organisaatioiden välistä yhteistyötä? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa
- ◯ En halua vastata

7. Jos vastasit kysymykseen 6 - "Kyllä", miten sekä minkä osa-alueiden yhteistyötä pitäisi mielestäsi kasvattaa?

Kirjoita vastaus

8. Pitäisikö uhkatietoa SOC-toimijoiden välillä jakaa laajemmin? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa
- ◯ En halua vastata

9. Jos vastasit kysymykseen 8 - "Kyllä", mitä jaettavan uhkatiedon olisi hyvä sisältää?

Kirjoita vastaus

10. Mahdollinen vapaa sana

Kirjoita vastaus