Timo Koskimäki

PIMEÄN VERKON HYÖDYNTÄMINEN ENNAKOIVAN KYBERTILANNEKUVAN LUONNISSA JA YLLÄPIDOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Koskimäki, Timo
Pimeän verkon hyödyntäminen ennakoivan kybertilannekuvan luonnissa ja ylläpidossa
Jyväskylä: Jyväskylän yliopisto, 2024, 52 s.
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaajat: Lehto, Martti ja Niemelä, Mikko

Kybertoimintaympäristön uhkatoimijat operoivat ja toimivat erityisesti pimeän verkon anonymiteettien alla. Tässä tutkimuksessa lähestytään pimeän verkon hyödyntämistä ennakoivan kybertilannekuvan luonnissa ja ylläpidossa Shakarian (2017) esittämän neliportaisen Kyberuhkatiedustelun tasomallin mukaisesti. Tämän Pro gradu -tutkimuksen tuloksena voidaan sanoa, että kattavan ja aktiivisen kyberuhkatiedustelun avulla voidaan tuottaa laadukasta ja ennakoivaa kybertilannekuvaa. Ennakoivan kybertilannekuvan avulla voidaan varautua ja puolustautua uhkaavilta toimijoilta. Tutkimus ei tuota mitään täsmäasetta kyberuhkiin, vaan kertoo yleispätevästi mallin, jonka avulla on mahdollista tuottaa tietoa omasta kybertoimintaympäristöstään siten, että tämän tiedon avulla saadaan puolustautumista aktiivisesti säädettyä ajan trendien ja uhkatoimijoiden resurssien mukaiseen muotoon.

Asiasanat: pimeä verkko, kybertilannekuva, ennakoiva kybertilannekuva, kyberuhkatiedustelu

ABSTRACT

Koskimäki, Timo
Utilizing the dark web in creating and maintaining a proactive cyber situational awareness
Jyväskylä: University of Jyväskylä, 2024, 52 pp.
Security and strategic analysis, Master's Thesis
Supervisors: Lehto, Martti and Niemelä, Mikko

Threat actors in the cyber environment operate especially under the anonymity of the dark web. This study approaches the use of the dark web in creating and maintaining a proactive cyber situational awareness in accordance with the four-step level model of cyber threat intelligence presented by Shakaria (2017). As a result of this Master's thesis, it can be said that comprehensive and active cyber threat intelligence can be used to produce high-quality and predictive cyber situational awareness. Proactive cyber situational awareness can be used to prepare for and defend against threatening actors. The study does not produce any precision weapon for cyber threats but provides a general model that makes it possible to produce information about one's own cyber operating environment in such a way that this information can be used to actively adjust defence in accordance with current trends and the resources of threat actors.

Keywords: dark web, cyber situational awareness, proactive cyber situational awareness, cyber threat intelligence, CTI

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Nykypäivänä IT-infrastruktuurin jatkuva kehitys ja päättymätön innovointi digitaalisissa teknologioissa tekee järjestelmistä yhä monimutkaisempia (Tounsi & Rais, 2018). Järjestelmien kehittyessä monimutkaisemmiksi, tulee niistä aina vähemmän turvallisia (Schneier, 2000). Kyberturvallisuus on jatkuvaa kamppailua hyökkääjän ja puolustajan välillä (Schneier, 2012). Puolustautuakseen kyberuhilta paremmin, on tunnettava toimintaympäristö ja pyrittävä ennakoimaan toimintaympäristön muutoksia ja uhkakuvia. Ennakoivan kybertilannekuvan luominen ja ylläpitäminen vaadittavalla tasolla antaa strategiselle päätöksenteolle tärkeitä lähtöarvoja resursoida puolustus kyberuhilta oikealla tavalla ja tehokkaasti. Tässä tutkimuksessa keskitytään erityisesti siihen, miten voidaan hyödyntää pimeästä verkosta saatavaa tietoa, ylläpitääkseen hyvää kybertilannekuvaa.

1.1 Tutkimusongelma ja tutkimuskysymykset

Maailman digitalisoitumisen ja verkottumisen myötä organisaatioiden toimintamuodot ovat hyvin riippuvaisia toimivasta ja turvallisesta verkkoympäristöstä. Osatakseen suojautua ja varautua kybermaailman uhkiin, on hyvä tiedostaa ympäröivä kyberympäristö ja sen muut toimijat ja tapahtumat. Nykypäivän uhkatoimijat liikkuvat ja toimivat etenkin pimeän verkon puolella, sen sisältämän vahvan anonymiteetin takia. Tämän tutkimuksen tarkoituksena on selvittää vastaukset seuraavaan tutkimuskysymykseen:

Miten muodostetaan ennakoivaa kybertilannekuvaa?

Lisäksi tutkimuksessa pyritään vastaamaan seuraaviin apukysymyksiin:

Mistä kybertilannekuva muodostuu?
Miksi ennakoivaa kybertilannekuvaa muodostetaan?

Kyberturvallisuudesta on tullut yhteiskunnallinen ongelma, jolla on laajat seuraukset niin teollisuuden kuin julkisen sektorin ja hallinnon aloille. Kriittiset infrastruktuurit ja monimutkaiset järjestelmät ovat tulleet yhä riippuvaisemmaksi teknologiasta, joita uhkaavat erilaiset kyberhyökkäykset. (Benjamin, Valacich & Chen, 2019) Tästä syystä on ensiarvoisen tärkeää tutkia ennakoivan kybertilannekuvan tarjoamia hyötyjä ja mahdollisuuksia kyberpuolustuksessa. Jokaisen kyberturvallisuuden parissa työskentelevän henkilön on ymmärrettävä kuinka louhia tietoa syvästä ja pimeästä verkosta nykyajan digitalisoituneessa maailmassa (Khera, 2020).

Tutkimus toteutetaan laadullisena sisällön analyysinä, jota edeltää kirjallisuuskatsaus aiheeseen. Kirjallisuuskatsauksen kappale 6 tehdään yhteistyössä Kasperi Leppäsen kanssa. Tutkimuksen empiirinen osuus toteutetaan Shakarian (2017) Kyberuhkatiedustelun taso -mallin pohjalta ja sen luomiseen hyödynnetään kaupallisen palveluntarjoajan, Cyber Intelligence Housen (CIH) pimeän verkon analyysityökalua, Cyber Exposure Platformia (CEP). Tämä työkalu antaa syötettä pimeän verkon sisällöstä, jota analysoimalla pyritään vastaamaan tutkimuskysymykseen.

1.2 Aiempi tutkimus

Jyväskylän yliopistossa on tehty aihepiiriä lähellä olevia tutkimuksia jonkin verran. Miia Pudas (2023) tutki Pro gradu -tutkielmassaan APT-hyökkäysten havaitsemista kyberuhkatiedustelun avulla. Mira Stenhammar (2022) tutki Pro gradu -tutkielmassaan syvän ja pimeän verkon keskusteluja sekä keskustelijoita. Mikko Ruotsalainen (2021) käsitteli Pro gradu -tutkielmassaan Rikollista kaupankäyntiä Tor-verkon suomenkielisissä piilopalveluissa. Juha Matilainen (2021) tutki Pro gradu -tutkielmassaan kyberuhkatiedustelua organisaation kyberturvallisuudessa.

Paulo Shakarian (2017) käsittelee raportissaan ”The enemy has a voice” uhkien ymmärtämistä älykkään kyberpuolustuksen rakentamisessa. Hän esittelee raportissaan Kyberuhkatiedustelun tasot -mallin, jota myös tässä Pro gradu -tutkielmassa hyödynnetään tutkimuksen runkona.

Vasileos Mavroeidis sekä Siri Bromander (2017) esittelevät tutkimuksessaan uuden kyberuhkatiedustelun mallin, joka pääosin esittelee, minkälaista tietoa tarvitaan kehittyneessä kyberuhkien tiedustelussa.

2 KYBERTILANNEKUVA

Kyberturvallisuuden tilannekuvalla tai kybertilannekuvalla tarkoitetaan yksilön tai organisaation kykyä ymmärtää ympäröivää kybertoimintaympäristöä, sekä sen tuomia potentiaalisia uhkia ja haavoittuvuuksia. Kybertilannetietoisuus pitää myös sisällään tämän tiedon hyödyntämistä päätöksenteossa, omaisuuden suojaamisessa ja uhkiin sekä tapahtumiin reagoimisessa. (Renaud & Ophoff, 2021) Tilannetietoisuus auttaa päätöksentekijöitä pitämään selkeän suunnan toiminnassaan, sekä konkreettisesti auttaa tekemään hyviä päätöksiä (Horneman, 2019).

Organisaatioiden johdolle on elintärkeää toimintaympäristötietoisuus ja toimintaympäristön ymmärtäminen. Nämä ovat edellytyksiä sille, että johto osaa tehdä hyviä ja oikea-aikaisia päätöksiä. Kybertilannekuvan sisältö ja tarve ovat hyvin organisaatiokohtaista, joten ei olekaan mahdollista määritellä yhtä oikeata mallia kybertilannekuvan muodostamiseen. Kybertilannekuvan sisältö ja tarve vaihtelevat suuresti eri johtamistasojen ja toimijoiden välillä. Lisäksi organisaatioiden koko ja toimintaympäristö vaihtelevat suuresti, jolloin myös kybertilannekuvan muodostaminen vaihtelee niiden mukana. (Huoltovarmuusorganisaatio, 2022)

Tilannetietoisuutta voidaan lähestyä muutaman peruspilarin kautta: ”Tiedä mitä pitäisi olla. Seuraa sitä mitä on. Päättele, milloin ”pitäisi olla” ja ”on”, eivät täsmää. Tee jotain tälle erolle.” (Horneman, 2019) Tämä ajatus voidaan tuoda suoraan myös kybertilannekuvan yhteyteen. Sinun pitää tietää, mitä ympäröivässä kyberympäristössä pitäisi olla. Tiedät oman positiosi kybermaailmassa ja ymmärrät sinun suhteesi muihin ympäristön toimijoihin. Sinun täytyy seurata sitä, mitä kyberympäristössä on ja mitä siellä tapahtuu. Sinun täytyy ymmärtää, kun jokin kyberympäristössä ei ole siten kuin pitäisi. Sinun täytyy tehdä tälle puutokselle jotain. Esimerkiksi, tunnet oman organisaatiosi, ja tunnet organisaatiosi kyberturvallisuuskulttuurin ja toimintatavat ja käytänteet. Seuraat kybertoimintaympäristöä aktiivisesti ja havaitset ympäristössä muutoksen. Ympäristöön on muodostumassa tai aktivoitumassa uusi uhkatekijä. Tarkistat oman organisaation suhteen tähän uhkatekijään ja teet tarvittavia toimenpiteitä neutralisoimaan uhkatekijän uhkavektorin omaa organisaatiotasi

kohtaan. Oli se sitten tietoturva-aukon paikkaaminen, laitteiston päivittäminen, henkilöstön kouluttaminen tai uuden toimintamallin omaksuminen, on se joka tapauksessa kybertilannetietoisuuden tarkoituksellinen päämäärä. Tuntemalla oman organisaatiosi toiminnan ja seuraamalla kybertoimintaympäristöä ymmärrät, mikä organisaatiotasi uhkaa ja miten siltä suojaudutaan.

3 KYBERUHKAT

Kyberuhkatoimija on henkilö, organisaatio tai ryhmittymä, joka tarkoituksellisesti aiheuttaa harmia digitaalisessa maailmassa. Nämä toimijat hyödyntävät laitteiden, verkkojen tai järjestelmien heikkouksia suorittaakseen vahingollisia hyökkäyksiä yksittäisiä henkilöitä tai organisaatioita vastaan. Kyberuhkatoimijoita voi olla muun muassa kyberrikolliset, valtiolliset toimijat, haktivistit, terroristit, sisäpiiriläiset ja trollit. (Crowdstrike, 2023) Näiden kyberuhkatoimijoiden kyberhyökkäyksiä voivat olla esimerkiksi kiristys- ja haittaohjelmahyökkäykset, hajautetut palvelunestohyökkäykset (DDoS), tietojen kalastelut ja SQL-injektiohyökkäykset (Biju & Prakash, 2019). Toisaalta muun muassa tietoturvayhtiö Trend Micro eriyttää kyberrikolliset muista kyberuhkatoimijoista. Trend Micron määritelmän mukaan uhkatoimijat toimivat tiettyä kohdetta vastaan tarkoituksellisesti, motivoituneesti, pitkäjänteisesti ja järjestelmällisesti, kun taas kyberrikolliset toimivat keskimäärin summittaisemmin ja pääsääntöisesti toimet eivät kohdistu tiettyyn tahoon pelkästään. (Trend Micro, ei pvm.)

Microsoft jakaa vuosittaisessa ”Digital Defence” -raportissaan (2023) uhkatoimijat viiteen eri kategoriaan: valtiolliset toimijat, taloudellisesti motivoituneet, yksityisen sektorin kyberoffensiiviset palveluntarjoajat, informaatiovaikuttamisen operaatiot sekä tuntemattomat ja kehittyvät ryhmät (Microsoft, 2023). Teknologiayhtiö IBM (ei pvm.) tekee kyberuhkatoimijoiden jakamisen Microsoftia yksinkertaisemmin ja selkeämmin. IBM jakaa kyberuhkatoimijat kuuteen osaan: valtiolliset toimijat, kyberrikolliset, haktivistit, jännityksen etsijät, sisäpiirin uhat ja kyberterroristit. Tässä tutkimuksessa uhkatoimijoista pyritään käyttämään hyvin yksinkertaistettuja ja helposti ymmärrettäviä ensitason määritelmää, joten IBM malli sopii tähän yhteyteen erinomaisesti. Crowdstrike (2023) esittelee myös neljä yksinkertaista keinoa välttyä kyberuhkatoimijoiden hyökkäysten onnistumiselta (taulukko 1), tämän jälkeen määritellään tutkimuksen kannalta relevanteimpia kyberuhkatoimijoita IBM:n (ei pvm.) jakolinjan mukaisesti.

TAULUKKO 1 Kyberuhkatoimijoiden torjumisen ABC

Työntekijöiden ajantasainen koulutus kyberturvallisuuden aiheista
Monivaiheisen tunnistautumisen käyttöön ottaminen organisaation järjestelmiin ja laitteisiin, sekä salasanojen säännöllinen vaihtaminen
Työntekijöiden toimintojen monitoroiminen mahdollisten sisäpiirin uhkien torjumiseksi ja tunnistamiseksi
Toimiva virustorjunta

Crowdstriken (2023) mukaisesti kyberuhkatoimijoilta puolustautumisen peruspilarit

3.1 Advanced persistent threat

Advanced Persistent Threat (APT) eli kehittyneet ja sitkeät uhat ovat niitä, joita valtiot ja monet organisaatiot pelkäävät ja haluavat puolustautua niiden vaaroilta (Alshamrani, Myneni, Chowdhary & Huang, 2019). APT on monivaiheinen ja kohdistettu tietoverkkohyökkäys tai uhka, jonka hyökkääjä kohdistaa tiettyyn kohteeseen. Tämä hyökkäys tehdään haittaohjelmien sekä muiden toimintojen avulla. Tämä hyökkäys voi kohdistua esimerkiksi yritykseen, valtiohallinnon organisaatioon, tai henkilöihin. Tavoitteena hyökkäyksellä on kohteesta tai kohteen järjestelmistä kriittisen tiedon saaminen, tai kohteen toiminnan muuttaminen. (Turvallisuuskomitea, 2018) APT-hyökkääjät pyrkivät tavoitteisiinsa toistuvasti ja pitkään. Ne myös mukautuvat puolustuksen kehitykseen. (Kissel, 2019) APT-toimijoiden tavoitteina on usein vakoilu, datavarkaudet ja verkkojen sekä erilaisten järjestelmien häiritseminen tai tuhoaminen (CISA, ei pvm.). Nykypäivänä APT hyökkäyksissä käytetyt tekniikat sekä menetelmät ovat usein samanlaisia kuin taloudellisesti motivoituneilla kyberrikollisilla. Samojen toimijoiden on myös tunnistettu tekevän sekä taloudellisesti motivoituneita hyökkäyksiä että vakoiluoperaatioita. (Albrecht & Balaam, 2023)

APT:t ovat monivektorisia ja monivaiheisia uhkia. APT:t määritellään hienostuneiksi tietoverkkohyökkäyksiksi, joissa hyökkääjä pyrkii pääsemään verkkoon sisälle niin kauan, että se siinä onnistuu. Tämän jälkeen hyökkääjä pyrkii pysymään verkossa huomaamattomana niin pitkään kuin mahdollista. APT-hyökkäysten tarkoituksena on varastaa dataa, eikä niinkään aiheuttaa vahinkoa kohdeverkossa. APT-hyökkäysten kohteina on organisaatiot, joilta he saavat tarpeeksi arvokasta tietoa. Esimerkiksi tällaisista organisaatioista on valtioiden eri virastot tai rahoitusalan organisaatiot. (Tounsi & Rais, 2018) APT hyökkääjät ovat hyvin rahoitettuja ja heillä on pääsy kehittyneisiin välineisiin ja menetelmiin toteuttaakseen APT–hyökkäyksen. Päästyään sisälle kohdejärjestelmään, hyökkääjät pyrkivät pysymään järjestelmässä sisällä niin kauan kuin on mahdollista. APT-toimijoilla on käytössä erilaisia välttelytekniikoita, joilla he pyrkivät estämään kohteen havaitsevan hyökkääjät järjestelmässä. Suurin uhka APT–hyökkäyksissä on usein arkaluontoisen tiedon menettäminen tai kriittisten komponenttien tai tehtävien estäminen. (Alshamrani ym., 2019)

Suojelupoliisi (SUPO) lähestyy aihetta otsikolla ”APT on kybervakoojan työkalupakki”. Supon mukaan ”APT on ohjattua, suunnitelmallista valtiollista kybervakoilua”. APT-operaatioissa ei Supon mukaan aina käytetä ohjelmakoodia, vaan APT-operaatioita voidaan toteuttaa myös antamalla verkon yli käsin syötettyjä komentoja kohdejärjestelmän ohjelmistoille. Supon mukaan APT nimityksen Advanced eli kehittynyt tai edistyksellinen tarkoittaa tässä yhteydessä sitä, että kybervakoiluoperaatioissa käytettävä koodi tai hyökkäysmenetelmä on edistyksellistä. Kehittyneen sijaan Supon mukaan kuvaavampi termi olisi tavoitteellinen, sillä termi on otettu käyttöön aikana, jolloin valtiollisten toimijoiden menetelmät olivat kehittyneitä ja edistyksellisiä, mutta nykyään myös muilla toimijoilla on kykyä edistyksellisiin hyökkäysmenetelmiin. Persistent eli sitkeä terminä kuvaa erityisesti APT-operaatioille tyypillistä tietyn kohteen sisälle pääsemistä ja siksi tekijä kokeilee sitkeästi erilaisia menetelmiä, kunnes se pääsee juuri kyseisen kohteen järjestelmiin sisälle. Threat eli uhka tarkoittaa tässä yhteydessä kansallista turvallisuutta uhkaavaa toimintaa. Tavoitteena APT-operaatioissa on hankkia kriittistä tietoa kohdevaltioista. (Supo, ei pvm.)

Kiinaan kytkeytyvän APT31-hakkeriryhmän on todettu iskeneen Suomen eduskuntaan vuosina 2020–2021 (Supo, 2021). APT31 on iskenyt myös yhdysvaltalaisiin yrityksiin, virastoihin, Kiina-kriitikoihin ja yksittäisiin hallinnon työntekijöihin (U.S. Department of Justice, 2024). Tietoturvayhtiö Mandiantin mukaan Kiinan hallintoon kytkeytyvän APT31 kohdealoja on paljon. Se kohdistaa hyökkäyksiä muun muassa valtioiden hallintoihin, kansainvälisiin rahoitusjärjestöihin ja ilmailu- ja puolustusorganisaatioihin sekä huipputeknologian, rakentamisen, suunnittelun, televiestinnän, median sekä vakuutukseen aloille. APT31 keskittyy nimenomaan hankkimaan Kiinan hallitukselle ja valtion omistamille yrityksille poliittisia, taloudellisia ja sotilaallisia etuja. (Mandiant, ei pvm.)

Valtiollisten toimijoiden kyberoperaatioiden kohteena on toisten valtioiden päätöksentekojärjestelmät, ylikansalliset elimet, ei-valtiolliset organisaatiot, kriittinen infrastruktuuri sekä koulutusjärjestelmät. Suurimman uhan länsimaisille yhteiskunnille tuottaa Kiinan, Venäjän, Iranin ja Pohjois-Korean harjoittamat kyberoperaatiot. Valtiollinen kyberoffensiivinen toiminta voi olla vakoilua, taloudellisesti motivoitunutta toimintaa tai kostoa. (Microsoft, 2023) Valtiohallinnot rahoittavat kyberuhkatoimijoitaan kerätäkseen salassa pidettävää tietoa tai häiritäkseen toisen hallinnon kriittistä infrastruktuuria. Näiden toimijoiden rahoitus on usein runsasta ja tällä rahoituksella hyökkäyksistä on kehitetty monimutkaisia ja hankalasti havaittavia. (IBM, ei pvm.)

Tutkimukset ovat osoittaneet, että Pohjois-Korealaiset APT-toimijat ovat rahoittaneet maan ydinaseohjelmaa ja vakoilutoimintaa varastetulla kryptovaluutalla. Venäläiset APT-toimijat ovat hyödyntäneet venäjää puhuvia lunnashaittaohjelma-toimijoita sekä haktivisteja edistääkseen omaa agendaa. (Albrecht & Balaam, 2023) Helmikuussa 2024 tapahtunut kiinalaisen tietoturvayhtiön tietovuoto paljasti Kiinan hallinnon kilpailuttavat kansallisia kybervakoiluja hakkerioperaatioita yksityisomistuksessa olevilla yrityksillä. Osalla näistä

yrityksistä on selviä kytköksiä tunnistettuihin kiinalaisiin APT-toimijoihin. (Unit 42, 2024)

APT-toimijat eivät välttämättä siis ole aina valtioiden turvallisuuspalveluiden suorassa hallinnassa, mutta valtioilla on niihin tiukat siteet ja näillä toimijoilla on molempia hyödyttävä yhteistyösuhde valtiohallintojensa kanssa. Joten APT-toimijat eivät aina ole valtiollisia toimijoita, mutta useimmiten he toimivat valtiohallintonsa intressien mukaisesti ja ohjeistuksessa.

3.2 Kyberrikollisuus

Kyberrikolliset ovat yksittäisiä henkilöitä tai rikollisorganisaatioita, jotka käyttävät teknologiaa tehdäkseen pahantahtoisia toimia digitaalisiin järjestelmiin tai verkkoihin tarkoituksenaan hyötyä siitä taloudellisesti (Trend Micro, ei pvm.). ”Laajasti ottaen kyberrikokset käsittävät kaiken tietoverkoissa tapahtuvan tai tietoverkkoja hyödyntävän rikollisuuden” (Poliisi, ei pvm.). Kyberrikollisuuden voi jakaa tietoverkkosidonnaisiin ja tietoverkkoavusteisiin rikoksiin. Tietoverkkosidonnaiset rikokset on kohdistettu juuri tietoverkkoihin ja tietojärjestelmiin. Tällaisia rikoksia on muun muassa palvelunestohyökkäykset, erilaiset tietomurrot ja datavahingonteot. Tietoverkkoavusteisissa rikoksissa taas hyödynnetään rikoskokonaisuuden osana tietoverkkoja tai tietojärjestelmiä. Tässä yhteydessä rikos tapahtuu perinteiseen tapaan esimerkiksi huumausainerikoksena tai petoksena, mutta rikoksen toteutuksessa hyödynnetään tietoverkkoja tai tietojärjestelmiä. (Poliisi, ei pvm.) Kyberrikokset ovat usein valtioiden rajat ylittäviä (Sisäministeriö, ei pvm). Yleisiä kyberrikoksia on muun muassa sähköpostihuijaukset, identiteettivarkaudet, lunnashaittaohjelmat, tietojen väärentämiset ja kalastelut ja verkkosaalistajat. (FBI, ei pvm.)

Myös kyberrikollisuus on kaupallistettu. Esimerkiksi digitaalisten laitteiden saastuttaminen haittaohjelmilla ei vaadi nykypäivänä enää laajoja teknisiä valmiuksia. Riittää kun osaat käyttää jotain verkon hakukonetta ja hakea sieltä tietoa, kuinka päästä pimeään verkkoon. Sieltä taas löydät helposti hakkereita, jotka myyvät haittaohjelmia, kalastelutyökaluja, palvelunestohyökkäyksiä tai vaikkapa tekevät sinulle väärennettyjä nettisivuja rahaa vastaan. (Div, 2017). Näitä kutsutaan yleisesti rikospalveluiksi, eli Crime as a Service (CaaS) (Fairman, 2021).

Eritysesti Ransomware as a Service (RaaS) -toimintamalli on yleistynyt viimevuosien aikana. Kyseessä on ikään kuin ohjelmistopalveluja tarjoava Software as a Service (SaaS) -toimintamalli mutta rikollisilla lunnashaittaohjelmilla tehtynä (Crowdstrike, 2023). Tämän toimintamallin myötä lunnashaittaohjelmakehittäjät tekevät rahansa myymällä ohjelmistoonsa käyttöoikeuksia toisille rikollisille, jotka suorittavat haittaohjelman istuttamisen kohdejärjestelmään. Tämä toimintamalli mahdollistaa henkilöiden, joilla ei ole ohjelmointitaitoja osallistua aktiivisesti hyökkäystoimintaan ja toiseksi tämä toimintamalli mahdollistaa RaaS -palveluntarjoajien keskittyvän ainoastaan ohjelmistokehitykseen. (Meland, 2020) Lunnashaittaohjelmista maksettujen lunnaiden arvo oli

2023-vuoden aikana arviolta n. 1,1 miljardia Yhdysvaltain dollaria (Chainanalysis, 2024). Lunnaista kertovaa tilastoa on haastavaa tuottaa tarkasti, muun muassa siitä syystä, että monet tahot eivät halua ilmoittaa maksamistaan lunnaista tai kohtaamistaan lunnashaittaohjelmista järjestelmissään. Toisaalta monet lunnashaittaohjelmatoimijat ilmoittavat omilla verkkosivuillaan uhreistaan ja näiden maksustatuksista. Kuitenkin varauksellakin tilastoja lukien nähdään mittava lunnashaittaohjelmien ”markkina” edelleen kasvavana ja suurena ongelmana läpi toimintasektorien.

3.3 Haktivismi

Haktivismi tulee sanoista ”hacker & activism” (Horstmann, 2022). Tämä siis tarkoittaa suomeksi ”hakkeroivaa aktivismia”. Henkilöä, joka harjoittaa haktivismia, kutsutaan haktivistiksi (Horstmann, 2022). Cambridgen Yliopiston sanakirjan mukaan haktivismilla tarkoitetaan laitejärjestelmiin tunkeutumista poliittisia päämääriä tavoitellen (Cambridge University, ei pvm.). Teknologiayritykset TechTarget (2021) sekä IBM (ei pvm.) lisäävät omassa määritelmässään laitejärjestelmien lisäksi kohteeksi erilaiset tietoverkot ja motivaatioksi he määrittelevät poliittisten syiden lisäksi sosiaaliset syyt. Stanfordin yliopiston määritelmä muistuttaa edellä mainittujen lisäksi haktivismin olevan oikeudellisesti epäselvää tai laitonta. Stanfordin yliopiston haktivismin määritelmä haluaa myös selkeästi erottaa haktivismin verkkoaktivismista. Siinä missä verkkoaktivismi on verkossa tapahtuvaa aktivismia, haktivismi on sitä myös, mutta sisältää aina myös hakkeroinnin aspektin. (Stanford University, ei pvm.)

Haktivismin tarkoitus on herättää ihmisten huomio johonkin, minkä haktivistit itse uskovat olevan tärkeä syy tai aihe. Esimerkiksi ihmisoikeudet, tiedon vapaus, tai uskonnolliset syyt voivat olla haktivismin perustana. Haktivismi ilmenee esimerkiksi viesteinä tai kuvina tietyn organisaation verkkosivuilla, jonka haktivistit ajattelevat olevan aatteeltaan tai toiminnaltaan väärässä. Haktivistit ovat yleensä yksittäisiä henkilöitä, mutta myös haktivisti-ryhmiä löytyy. Tunnetuimpia haktivisti-ryhmiä on vaikkapa Anonymous ja LuzSec. (TechTarget, 2021)

3.4 Muut kyberuhkat

Muita tutkimuksen kannalta relevantteja kyberuhkia on sisäpiirin uhkat, kyberterrorismi sekä jännityksen etsijät. Myös muita kyberuhkatoimijoita löytyisi, kuten trollit ja botit, mutta tässä tutkimuksessa niiden määrittelemisellä ei nähdä sen suurempaa tieteellistä arvoa tämän kyseisen tutkimuksen kannalta.

Sisäpiirin uhkatoimijat eivät välttämättä tee toimiaan pahantahtoisesti eikä tahallaan. Jotkut toimijat saattavat vahingoittaa organisaatiotaan tahattomasti virheitä tekemällä. Tällaisia tapahtumia voisi olla esimerkiksi viruksen sisäl-

tämän tiedoston lataaminen työlaitteelle tai työlaitteen hävittäminen. Myös pahantahtoisia ja tarkoituksellisia sisäpiirin uhkatoimijoita löytyy. Tyytymätön työntekijä voi varastaa yrityksen tietoja saadakseen taloudellista hyötyä tai työntekijä voi tuhota tai vahingoittaa yrityksen tietoja tai järjestelmiä turhautumisestaan yhtiötä tai sen toimintaa kohtaan. (IBM, ei pvm.) Sisäpiirin uhkatoimijan ei tarvitse olla yhtiön työntekijä, vaan toimija voi olla joku, jolla on pääsy yhtiön järjestelmiin sisälle, kuten vaikkapa konsultit tai hallituksen jäsenet. (Crowdstrike, 2023)

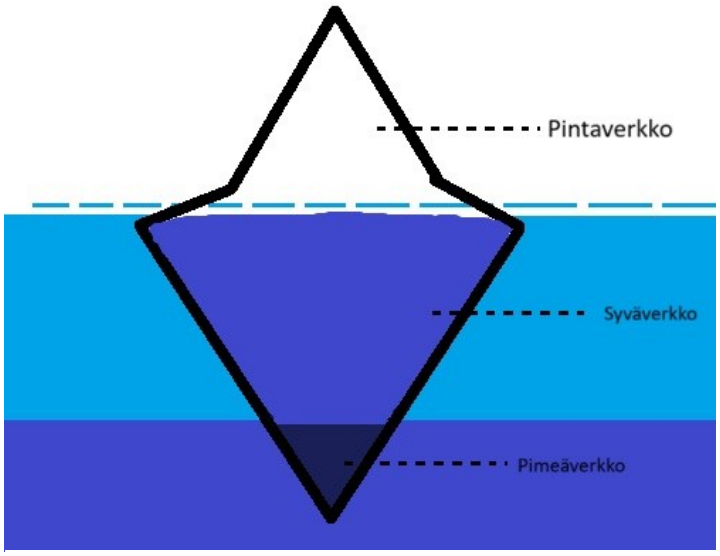
Kyberterroristit ovat poliittisesti tai ideologisesti motivoituneita kyberhyökkääjiä. Jotkin kyberterroristit voivat olla myös valtiollisia toimijoita, toiset taas yksittäisiä henkilöitä tai ei-valtiollisia ryhmiä. (IBM, ei pvm.)

Jännityksen etsijät tekevät nimensä mukaisesti iskuja saadakseen jännitystä ja huvia elämäänsä. Jotkut haluavat selvittää, kuinka paljon arkaluonteista tietoa he voivat varastaa, toiset taas hakkeroivat järjestelmiä ja verkkoja selvittääkseen niiden toimintalogiikoita. Osaa tästä porukasta kutsutaan nimellä ”Script Kiddies”, sillä heillä ei ole teknisiä valmiuksia tehdä omia hakkerointeja, mutta he hyödyntävät valmiita työkaluja ja tekniikoita hyökätäkseen haavoittuvaisia järjestelmiä kohtaan puhtaasti huvin vuoksi. Vaikka ”Script Kiddies” eivät välttämättä tahtoisi pahaa toiminnallaan, voivat he usein aiheuttavat vahinkoa verkkoon ja jättää esimerkiksi ovia auki tuleville kyberhyökkäyksille. (IBM, ei pvm.)

4 TIETOVERKOT

Monet ihmiset käyttävät termejä Internet ja World Wide Web synonyymeinä, mutta sitä ne eivät todellisuudessa ole. Internet ja World Wide Web ovat kaksi erillistä mutta toisiinsa liittyvää asiaa. Internet on massiivinen verkkojen verkosto, joka yhdistää miljoonia laitteita toisiinsa globaalisti. Tällä tavoin internet muodostaa verkoston, jossa jokainen siinä oleva laite voi kommunikoida toisen laitteen kanssa, kunhan molemmat ovat yhdistettynä internetiin. Vastaavasti World Wide Web on tapa saada tietoa internetin kautta. Se on tiedonjakomalli, joka on rakennettu internetin päälle, eli World Wide Web on internetin osa, joskin iso sellainen. (Chertoff & Simon, 2015)

Internet voidaan jakaa kolmeen eri tasoon: pintaverkkoon, syvään verkkoon sekä pimeään verkkoon. Tässä kappaleessa käydään nämä tasot läpi eriyttäen tasot toisistaan kertomalla kunkin tason ominaisuudet, erityispiirteet sekä eroavaisuudet muista tasoista. Kuviossa 1 on kuvattu verkon eri tasoja Finklean (2017) mukaisesti jäävuorivertauksella. Merenpinnan yläpuolella nähdään pintaverkko, eli perinteinen näkyvä internet. Meren pinnan alapuolella on syvä verkko ja tätäkin syvemmällä meressä nähdään pimeä verkko. Kappaleen lopussa nähdään taulukko 2, jossa käydään tasojen ominaisuudet vertaillen läpi yksinkertaistettuna taulukkomuotoisesti.



KUVIO 1 Verkon eri tasot jäävuorivertauksessa (Finklea, 2017)

4.1 Pintaverkko

Pintaverkko (Surface web), joka tunnetaan myös nimellä näkyvä verkko, on se osa internetiä, jota voidaan käyttää normaaleilla verkkoselaimilla, kuten Firefox tai Google Chrome (Khera, 2020). Hakukoneilla tietoa etsiessä voi internetin käyttäjä siirtyä tulosten perusteella sivustolta toiselle. Tällöin internetin käyttäjä käyttää internetin pintaverkkoa. (Vienažindyté, 2021) Pintaverkko on se internetin osa, joka on yleisesti saatavilla ja avoin kaikille internetin käyttäjille. Se on hakukoneilla indeksoitu ja helposti haettavissa erilaisilla hakukoneilla. (Varma, 2018)

4.2 Syvä verkko

Vaikkakin syvä verkko (Deep web) kuulostaakin arveluttavalta, käyttävät ja hyödyntävät kaikki internetin käyttäjät sitä. Kun käytetään sähköpostia, sosiaalisen median yksityisviestejä, nettipankkia tai erilaisia verkkolehtiä, joista luetaan asiakastilaajille tarkoitettua maksullista sisältöä, käytetään tällöin syvää verkkoa. (Vienažindyté, 2021) Syvä verkko viittaa internetissä olevaan sisältöluokkaan, jota erilaisista teknisistä syistä ei ole indeksoitu internetin hakukoneilla (Chertoff & Simon, 2015). Syvä verkko kattaa erilaisia tietokantoja, joita hakukoneiden, kuten Google tai Bing, avulla ei voi saavuttaa. Syvä verkko kattaa tietokannat, joihin voi päästä ainoastaan organisaation sisältä. Se kattaa maksumuurien takana olevat sisällöt, sivut, joissa sisältöä luodaan dynaamisesti joka kerta, kun niille siirrytään, sekä sivut, joihin pääsee ainoastaan sivuston hakujärjestelmän kautta. Lisäksi sähköpostit ja erilaiset keskustelulokit ovat osa syvää verkkoa. (Hatta, 2020) Jo vuonna 2000 syvä verkko oli 1000 – 2000 kertaa isompi kuin pintaverkko (Bergman, 2001). Vuonna 2013 Barker ja Barker totesivat syvän verkon olevan yli 500 kertaa isompi kuin pintaverkko (Chertoff & Simon, 2015). Varma puolestaan totesi vuonna 2018 syvän verkon kattavan noin 90% internetistä, 10% jäädessä pintaverkolle. Internetin sisältämän tiedon suuren kokoluokan takia pintaverkon tai syvän verkon kokoja on mahdoton vertailla tai mitata (Finklea, 2017). Joka tapauksessa, huomattavan suuri määrä verkosta löytyvästä tiedosta kuuluu juuri syvään verkkoon.

4.3 Pimeä verkko

Pimeä verkko (Dark web) on osa syvä verkkoa, joka on tarkoituksellisesti piilotettu ja saavuttamaton tavallisilla verkkoselaimilla. Pimeän verkon käyttäminen mahdollistaa lähes täydellisen anonymiteetin verkossa salaamalla datapaketit ja lähettämällä ne useiden verkkosolmujen läpi. Tätä verkkosolmu -rakennetta kutsutaan sipuliverkoksi, sen verkkokerrosten mukaisesti. (Chertoff & Simon,

2015) Tämän teknologian mukanaan tuoma anonymiteetti houkuttelee pimeään verkkoon internetin käyttäjiä, jotka syystä tai toisesta haluavat toimia salassa. Pimeän verkon toimintaan kuuluvat muun muassa laittomien tuotteiden myyntiä, vaarallisen tai laittoman sisällön jakamista ynnä muuta laitonta ja arveluttavaa toimintaa. Tämän lisäksi pimeää verkkoa käyttävät ja hyödyntävät myös esimerkiksi toisinajattelijat tai muista syistä vaarassa olevat henkilöt tai esimerkiksi journalistit. Pimeän verkon anonymiteetin ansiosta he pystyvät suojaamaan itsensä ja estämään digitaalisen jäljittämisen. (Vienažindyté, 2021)

Taulukko 2:ssä vertaillaan vielä lyhyesti Varman esittämän mallin mukaisesti pintaverkon, syvän verkon sekä pimeän verkon ominaisuuksia keskenään lisäämällä kuitenkin pimeän verkon sisältökohtaan myös laillisuusaspektin. Varman mallissa pimeän verkon sisältö oli pelkästään laitonta, mutta tämän tutkimuksen mukaan pimeä verkko sisältää myös laillista sisältöä, kuten edellä mainitut toisinajattelijoiden ja journalistien erilaiset keskustelu- ja tiedonjakoalustat.

TAULUKKO 2 Verkon tasot

	Pintaverkko	**Syvä verkko**	**Pimeä verkko**
Kuvaus	Sisältö, jonka hakukoneet voivat löytää	Sisältö, jota hakukoneet eivät voi löytää	Sisältö, joka on piilotettu tarkoituksellisesti
Tunnettu myös	Näkyvä verkko, Indeksoitu verkko, Surface web	Näkymätön verkko, Piilotettu verkko, Deep web	Dark web
Sisältö	Laillista	Laillista + Laitonta	Laitonta + laillista
Löytyvä tieto	4 %	96 %	-
Selaimet	Mozilla Firefox, Google Chrome…	-	TOR-selain ym.

Vertailussa Pintaverkko, Syvä verkko ja Pimeä verkko, mukaillen Varman (2018) mallia

5 INDIKAATTORIT

Myös kyberturvallisuuden yhteydessä käytetään erilaisia indikaattoreita. Indikaattorit ilmaisevat kohdeilmiön olemassaolosta, ominaisuudesta tai monitoroidun ympäristön tai aineiston muutoksesta (Valtiovarainministeriö, 2023).

5.1 Vaarantumisindikaattori

Nykypäivänä eniten käytettyjä indikaattoreita on vaarantumisindikaattorit (Indicatros of Compromise, IoC). IoCt ovat todisteita siitä, että joku voi olla murtautunut tai murtautumassa organisaation tietoverkkoon. Näitä indikaattoreita käytetään haitallisen toiminnan havaitsemiseen varhaisessa vaiheessa sekä tunnettujen uhkien estämiseen. Yleisimpiä IoCita on IP osoitteet, DNS nimet sekä tiedostojen liittäminen tai niiden muuttaminen. (Anashkin & Zhukova, 2022) IoC keskittyy hyökkäyksen tapaan, eli vastaa käytännössä kysymykseen « Miten hyökkäys tapahtuu? » (Brown, ei pvm.). Tällä indikaattorilla saatava data ei ainoastaan kerro potentiaalisesta uhasta, vaan se voi myös ilmaista hyökkäyksestä, kuten haittaohjelmasta, vaarantuneista tiedoista tai tietovuodosta. IoCita voidaan etsiä tapahtumalokeista, laajennetuista havaitsemis- ja vastausratkaisuista sekä tietoturvatietojen ja tapahtumien hallintaratkaisuista. Tapahtuvan hyökkäyksen aikana IoCta voidaan hyödyntää uhan poistamiseen ja vahinkojen lieventämiseen. Tapahtuman ja tapahtumasta toipumisen jälkeen IoCt voivat auttaa organisaatiota ymmärtämään paremmin mitä tapahtui ja sitä kautta vahvistaa puolustusta ja turvallisuutta ehkäisten samankaltaisia hyökkäyksiä jatkossa. (Microsoft, ei pvm.)

IoC ei kuitenkaan ole vedenpitävä menetelmä havaitsemaan kaikkia järjestelmää koestavia uhkia. IoC ei välttämättä tunnista edistyneiden ja ammattimaisten hyökkääjien käyttämiä uusia tai muokattuja hakkerointityökaluja niiden ainutlaatuisuuden vuoksi. IoC ei välttämättä toimi, mikäli hyökkääjä lähettää paljon vääriä indikaattoreita. Täyttyy tällöin tietokannat indikaattorikohinalla. Tässä tapauksessa puolustajan on suodatettava suuri määrä indikaattori-

tietoja, jolloin on vaarana, että todelliset indikaattorit hukkuvat melun sekaan. Tämä johtaa myös luottamuksen laskuun olemassa olevia indikaattoreita kohtaan. IOC ei välttämättä toimi, mikäli hyökkääjä ei käytä tiedostomuotoista haittaohjelmatekniikkaa, vaan tiedoston sijaan hyökkääjä lataa haittaohjelmakoodin kohdejärjestelmän standardiominaisuuksien, kuten PowerShellin kautta. IoC ei toimi myöskään ennakoivasti, vaan IoC on suunniteltu toimimaan reaktiivisesti. Muun muassa näiden syiden takia IoC ei aina toimi moderneja hyökkäysmenetelmiä vastaan, joten tarvitaan myös muita indikaattoreita valvomaan järjestelmien turvallisuutta. (Anashkin & Zhukova, 2022) Seuraavaksi käydään läpi erilaisia esimerkkejä vaarantumisindikaattoreista (taulukko 3).

TAULUKKO 3 Vaarantumisindikaattori (IoC)

Epätavallista saapuvaa tai lähtevää verkkoliikennettä organisaation tietoverkoissa
Poikkeavaa maantieteellistä liikennettä, eli liikennettä maista, joissa organisaatiolla ei ole toimintaa
Tuntemattomia sovelluksia, tiedostoja tai prosesseja järjestelmässä
Epätavallista toimintaa järjestelmänvalvojalta tai muilta erityisoikeuksia omaavilta käyttäjiltä
Virheellisten kirjautumis- tai käyttöpyyntöjen lisääntyminen (Bruteforce Attack)
Muu epätavallinen toiminta, kuten tietokannan huomattava kasvu
Suuri määrä käyttöpyyntöjä samalle tiedostolle
Epätavalliset DNS-pyynnöt ja rekisterimääritykset
Luvattomat asetusten muutokset
Suuret määrät pakattuja tiedostoja tai tietopaketteja väärissä paikoissa

Esimerkkejä Vaarantumisindikaattoreista Trend Micro (ei pvm.) ja Crowdstriken (2022) mukaisesti

5.2 Hyökkäysindikaattori

Hyökkäysindikaattori (Indicator of Attack, IoA) on digitaalinen tai fyysinen todiste kyberhyökkääjän aikomuksesta hyökätä. IoA:n havainnointi ei keskity pelkästään hyökkääjän käyttämiin työkaluihin tai menetelmiin vaan erityisesti hyökkääjän motiiveihin suorittaa hyökkäys. IoA tutkii ympäristöä Miksi - kysymyksen kautta. « Miksi joku haluaa hyökätä meitä vastaan?» IoA:n varhaisen vaiheen ilmoituksen avulla voidaan ennaltaehkäistä tietomurtoja. (Brown, ei pvm.)

IoAn avulla voidaan saada selville epäillystä hyökkääjästä useita kriittisiä tietoja, kuten « Kuinka he murtautuivat verkkoon? », « Hyödynsivätkö he takaovia järjestelmässä? » tai « Mitä kriittisiä pääsytietoja he saivat haltuunsa? ». Tämänkaltainen informaatio saattaa auttaa puolustajaa havaitsemaan jopa tuntemattomia hyökkääjiä tai hyökkäysmenetelmiä. Koska IoA keskittyy epäilyttävän toiminnan varhaiseen vaiheeseen, voi indikaattori hälyttää jo ennen kuin hyökkääjä on murtautunut järjestelmään sisälle. (Brown, ei pvm.)

IoA on toiminnan seuraamisen työkalu eli sääntö, johon on sisällytetty tapa, jolla mahdollisesti hyökkääjä hyökkää järjestelmää kohtaan. Tämä hyök-

käystapa ja tekniikka on etukäteen ohjelmoitu indikaattoriin erilaisten hyökkäyksiä selittävien teorioiden ja tekniikoiden avulla. (Anashkin & Zhukova, 2022) Näitä tekniikoita ja teorioita käydään läpi luvussa 6. Näissä teorioissa nähdään hyökkääjien toimintatapoja ja niiden avulla voidaan järjestelmää valvoa tämänkaltaisten hyökkäysten varalta. Mikäli indikaattori huomaa teorioiden kaltaista liikettä järjestelmässä, antaa se siitä hälytyksen. Näitä indikaattoreita voidaan luoda myös oman kokemuksen perusteella tarkemmiksi ja tehokkaammiksi. IoAn voidaan kokea oikein toteutettuna olevan tehokkaampi kuin IoC, sillä hyökkääjien on hankalampi vaihtaa tekniikoita, taktiikoita ja menetelmiään kuin esimerkiksi IP osoitetta, DNS nimeä tai tiedostomuotojaan. (Anashkin & Zhukova, 2022)

5.3 Käyttäytymisindikaattori

Käyttäytymisindikaattorit (Indicators of Behavior, IOB) ovat digitaalisen käyttäytymisen monitorointiin kehitetty heräte, jonka avulla voidaan ymmärtää käyttäjien käyttäytymiseen liittyviä riskejä organisaatiossa. IOB pystyy havaitsemaan tunkeilijan organisaation järjestelmässä, sisäpiiriläisen pahantahtoiset toimet tai huolimattoman käyttäjän toiminnat, jotka eivät vastaa turvallisuuskäytänteitä tai -ohjeistusta. Käyttäytymisindikaattori voi olla esimerkiksi varoitus etäkirjautumisesta, ulkoisten medioiden käyttäminen organisaation järjestelmissä, etähallintaohjelmien käyttäminen tai useiden palvelimien käyttäminen järjestelmässä. Käyttäytymisindikaattoreilla on mahdollista havaita tunkeilijoita järjestelmässä, sisäpiiriläisen rikkomukset tai turvallisuusvaatimusten noudattamatta jättämistä, luottamuksellisen tiedon vuotamista ynnä muita järjestelmää ja organisaatiota vaarantavia toimia. (Anashkin & Zhukova, 2021)

Käyttäytymisindikaattoreista on myös kehittyneempiä versioita, kuten Käyttäjien Käyttäytymisen Analytiikka eli ”User Behavior Analytics, UBA”. UBA on tekoälyn ja koneoppimismallien tukema tekniikka, jolla pyritään aluksi määrittämään käyttäjien perustoiminnot, jonka jälkeen tekoäly sekä koneoppimismallit alkavat keräämään tietoa käyttäjien toimista, jotka poikkeavat normaalista ja näin aiheuttavat hälytyksen järjestelmän ylläpitäjälle. (Cyberark, ei pvm.)

User Behavior Analytics -tekniikasta on vielä kehittyneempi versio, User and Entity Behavior Analytics (UEBA) eli Käyttäjien ja Kokonaisuuksien Käyttäytymisen Analytiikka. UEBA tekee siis saman kuin UBA, mutta ottaa lisäksi huomioon erilaiset laitteet, verkot ja järjestelmät organisaatiossa. UEBA monitoroi esimerkiksi IoT-laitteiden tuottamaa dataa. (Shashanka, Shen, & Wang, 2016)

6 APT-KYBERHYÖKKÄYSMALLIT

Kyberhyökkäyksen mallintamisella pyritään jakamaan kyberhyökkäys eri vaiheisiin ja näin hahmottamaan sen eri ominaisuuksia. Mallintamisella pyritään myös tunnistamaan erilaisia taktiikoita, tekniikoita ja menetelmiä, joita hyökkääjä käyttää hyökkäyksessään. Eri malleja ja tietämystä eri tekniikoista voidaan siten käyttää tunnistamaan oman puolustuksen aukkoja sekä ennakoimaan ja välttämään tulevia hyökkäyksiä (Lehto, 2022; Leppänen, 2022). Tämä kappale 6 on kirjoitettu yhteistyössä Kasperi Leppäsen kanssa vuonna 2024.

6.1 Yleinen kyberhyökkäysmalli

Artikkelissaan Lehto käy läpi mainitut kyberhyökkäysmallit ja muodostaa niistä yleismallin, joka jakautuu kolmeen eri vaiheeseen. Ensimmäinen vaihe Lehdon mallissa on strateginen päätös hyökkäykseen ryhtymisestä, toinen vaihe koskee hyökkäyksen valmistelua ja kolmas vaihe käsittelee itse hyökkäyksen. (Lehto, 2022; Leppänen, 2022)

6.1.1 Hyökkäyksen esivaihe

Hyökkäyksen esivaihe koskee Lehdon mukaan valtiollisten toimijoiden APT-hyökkäyksiä. Tässä vaiheessa hyökkääjä tekee strategisen päätöksen kyberhyökkäyksen kohteesta ja tavoitteista ja kuinka päätös ja toimet vaikuttavat muihin strategisiin tavoitteisiin (Lehto, 2022; Leppänen, 2022).

6.1.2 Hyökkäyksen valmisteluvaihe

Toinen vaihe, eli hyökkäyksen valmistelun vaihe, käsittää kaksi osaa: tiedustelun ja aseistamisen, joista tiedustelu sisältää vielä kaksi vaihetta. Tiedustelun ensimmäisessä vaiheessa hyökkäyksen suunnittelijat pyrkivät muodostamaan tilannekuvan kohdeorganisaatiosta. Valmistelijat tekevät tutkimusta siitä, mitkä

kohteet tarjoavat heille pääsyn tavoitteisiin. Tiedusteluvaiheessa pyritään keräämään kohdeorganisaatiosta tietoa niin paljon kuin mahdollista. (Lehto, 2022; Leppänen, 2022)

Tiedustelun toisessa vaiheessa hyökkääjän fokus siirtyy tietoverkkojen skannaukseen. Skannausvaiheessa pyritään löytämään mahdollisimman paljon tietoa kohteen tietojärjestelmistä. Tavoitteena tässä vaiheessa on löytää tietoja kohteen käyttämistä suojattomista ohjelmistoista, joita hyökkääjä voisi käyttää pyrkiessään sisään tietoverkkoihin. Seuraava toisen vaiheen osuus on nk. aseistaminen. Aseistamisella tarkoitetaan esimerkiksi räätälöidyn haittaohjelman tai väärennetyn internet-sivuston valmistamista hyökkäystä varten. Aseistaminen tehdään räätälöidysti sen mukaan, millaisia tietoja kohteesta on tiedusteluvaiheessa saatu. (Lehto, 2022; Leppänen, 2022)

6.1.3 Hyökkäysvaihe

Lehdon mallin mukaan hyökkäysvaihe koostuu viidestä eri vaiheesta. Näitä vaiheita ovat sisäänpääsyn vaihe (joka on jaettu viiteen eri portaaseen), lateraalisen liikkeen vaihe, komento- ja kontrollivaihe, täytäntöönpanovaihe ja loppuvaihe. (Lehto, 2022; Leppänen, 2022)

Sisäänpääsyn vaiheessa hyökkääjän tavoitteena on tunkeutua kohteen tietoverkkoon toteuttaakseen hyökkäyksen. Hyökkääjän tavoitteena on saada järjestelmänvalvojan oikeudet. (Lehto, 2022) Alle on kuvattu sisäänpääsyvaiheen portaat ja se, mitä hyökkääjä missäkin vaiheessa pyrkii saavuttamaan. (Lehto, 2022; Leppänen, 2022).

1) Ensimmäinen porras, tunkeutuminen: Hyökkääjä kohdentaa toimiaan kohdeorganisaation yksittäisiä käyttäjiä vastaan. Menetelmä, jolla hyökkääjä pyrkii tunkeutumaan järjestelmään, voi olla esimerkiksi kohdennettu kalasteluviesti, sosiaalinen hakkerointi tai jokin järjestelmässä oleva tekninen haavoittuvuus. Käytettävän menetelmän avulla pyritään toimittamaan haittaohjelma kohteen tietoverkkoon.
2) Toinen porras, jatkuvuus: Hyökkääjä toimittaa haittaohjelman kohteen tietojärjestelmään ja pyrkii saamaan jalansijan tietoverkossa. Tavoitteena on kyetä saamaan jatkuva pääsy tietoverkkoon sen ulkopuolelta. Tyypillinen toteutustapa on asentaa jatkuva takaportti uhrijärjestelmään pidemmäksi aikaa.
3) Kolmas porras, hyödyntäminen: Hyökkääjä käyttää löytämiään haavoittuvuuksia saadakseen pääsyn kohdeverkkoon ja ajaakseen siellä haitallista koodia. Tavoitteena on saada järjestelmänvalvojan oikeudet kohteen tietoverkkoon. Haavoittuvuuksia voi löytyä käyttäjistä, teknologiasta tai prosesseista. Tehokkaimpia ovat nk. nollapäivähaavoittuvuudet, eli ohjelmistohaavoittuvuudet, joihin ei ole olemassa korjausta, ja jotka voivat olla vielä ”löytämättömiä” virheitä ohjelmistoissa.

4) Neljäs porras, asennus: Kun heikkoudet on hyödynnetty, haittaohjelma asentuu kohdejärjestelmään. Hyökkääjä voi edelleen jatkaa tunkeutumistaan syvemmälle tietoverkkoon.
5) Viides porras, välttely: Hyökkääjä pyrkii toimimaan salassa ja välttämään paljastumasta.

Lateraalisen liikkeen vaiheessa hyökkääjä pyrkii levittäytymään kohteen tietoverkkoon mahdollisimman laajalle. Tavoitteena hyökkääjällä on oppia lisää kohdeympäristöstä, laajentaa hyökkäyspinta-alaa ja käyttöoikeuksia, sekä saastuttamalla pääsemään käsiksi suurempaan määrään resursseja. (Lehto, 2022; Leppänen, 2022)

Komennon ja kontrollin vaiheessa hyökkääjä asettaa kohdetietoverkkoon koodia, joka antaa tälle työkaluja hallintaan ja kommunikointiin kohdeverkossa. Tavoitteena on edelleen syventää ja varmistaa hyökkääjän jatkuva kontrolli uhrin verkkoon kohdeverkon ulkopuolelta. (Lehto, 2022; Leppänen, 2022)

Toteutusvaiheessa hyökkääjä pyrkii toteuttamaan hänelle asetetun tehtävän. Tehtävät ja kohteet vaihtelevat riippuen siitä, mikä on tavoiteltava lopputulos. Tavoitteena APT-hyökkäyksillä voi Lehdon mukaan olla esimerkiksi erilaiset tietovarkaudet, tiedot yrityssopimuksista tai -neuvotteluista tai sotilaalliset tiedot. Tavoitteena voi olla myös datan manipulointi, jota pidetään yhtenä vaarallisimmista hyökkäyksistä. (Lehto, 2022; Leppänen, 2022)

Päätösvaiheessa, hyökkäyksen saavuttaessa tavoitteensa, pyrkii hyökkääjä ”poistumaan” huomaamatta. Hyökkääjä pyrkii siivoamaan kaikki jäljet toiminnastaan kohteen tietojärjestelmässä. Hyökkääjä voi myös jäädä kohdejärjestelmään ”odottamaan” uusia mahdollisuuksia kerätä muuta arvokasta tietoa. Tässä vaiheessa voidaan myös rakentaa uusia vaikeammin löydettäviä ”takaovia” siltä varalta, että toiset paljastuvat tulevaisuudessa. (Lehto, 2022; Leppänen, 2022)

6.2 Cyber Kill Chain

Lockheed Martinin Cyber Kill Chain perustuu ajatukseen tiedustelujohtoisesta tietoverkkojen puolustamisesta APT-toimijoita vastaan. Sen kuvataan olevan riskienhallintastrategiaa, joka käsittelee uhkakomponenttia osana riskiä, sisältäen analyysin vastustajista ja heidän kyvyistään, tavoitteistaan, doktriineistaan ja rajoitteistaan. Tämä tiedustelujohtoinen tietoverkkojen puolustaminen on jatkuva prosessi, joka hyödyntää indikaattoreita löytääkseen uutta toimintaa ja vielä uusia indikaattoreita hyödynnettäväksi. Tämä lähestymistapa vaatii ymmärrystä tietoverkkoihin tunkeutumisista, ei niinkään yksittäisinä tapahtumina, vaan vaiheittaisen etenemisen näkökulmasta. (Hutchins ym., 2011)

Kill Chain -malli kuvataan systemaattiseksi prosessiksi, jossa kohdistetaan voimankäyttö vastustajaan haluttujen vaikutusten aikaansaamiseksi. Yhdysvaltojen kohdentamisdoktriini määrittelee prosessin vaiheet seuraavasti:

1. Löydä vastustajalta hyökkäykseen sopivat kohteet
2. Paikanna kohteiden sijainti
3. Seuraa ja tarkkaile
4. Valitse sopiva ase tai resurssi halutun vaikutuksen aikaansaamiseksi
5. Hyökkää
6. Arvioi vaikutukset

Tämä prosessi kuvataan kokonaisprosessina tai ketjuna, jonka yhdenkin vaiheen tai lenkin heikkous keskeyttää koko prosessin. (Hutchins ym., 2011)

Hutchins ym. laajentavat em. konseptia tietoverkkotunkeutumisten kentälle. Cyber Kill Chain perustuu ajatukselle siitä, että tunkeutumisen ydin on hyökkääjään kehittämä haitake (payload), jonka se tarvitsee murtautuakseen kohteeseen, luodakseen läsnäoloa tässä ympäristössä, ja tätä läsnäoloa hyödyntäen suorittaa tavoitteidensa mukaisia toimia. Nämä toimet voivat olla lateraalista liikettä kohteen tietoverkossa tai järjestelmän luottamuksellisuuden, eheyden tai saavutettavuuden heikentämistä. (Hutchins ym., 2011)

Tältä pohjalta Hutchins ym. kehittivät seitsenportaisen mallin; tiedustelu, aseistaminen, toimitus, hyödyntäminen, asentaminen, komento ja kontrolli sekä toimenpiteet tavoitteisiin.

Tiedustelun vaiheessa hyökkääjä tekee tutkimusta, identifioi ja valitsee kohteet. Tiedonhankinnassa lähteenä voidaan käyttää eri internetsivuja, esimerkiksi konferenssijulkaisuja tai sähköpostilistoja, sosiaalisia suhteita tai tietoa spesifeistä teknologioista.

Aseistamisen vaiheessa hyökkääjä muovaa etäkäytettävästä troijalaisesta ja järjestelmän hyödynnettävästä heikkoudesta toimitettavan haitakkeen. Yleensä tämä tapahtuu automatisoidulla työkalulla ja lopulta tämä haittakuorma toimitetaan pdf-, tai Word-tiedostona.

Toimitusvaiheessa edellisessä vaiheessa luotu ”ase” toimitetaan kohdeympäristöön. Toimitustapoja (mallin luomisen aikaan) voivat olla mm. sähköpostin liitetiedostot, internet-sivut tai usb-muistit.

Hyväksikäyttämisvaiheessa käytetään aseistamisen vaiheessa luotua ”asetta”. Kun ”ase” on toimitettu kohdeympäristöön, se käyttää hyväkseen haavoittuvuutta ja suorittaa hyökkääjän koodia. Haavoittuvuuden hyväksikäyttö voi kohdistua johonkin ohjelmaan tai käyttöjärjestelmään, tai se voi hyödyntää käyttäjiä tai saada käyttöjärjestelmän suorittamaan koodia automaattisesti.

Asentamisen vaiheessa hyökkäystä asennetaan ”etäkäytettävä troijalainen” tai ”takaovi” järjestelmään, joka mahdollistaa hyökkääjän ylläpitää läsnäoloaan kohdejärjestelmässä.

Komennon ja kontrollin vaiheessa muodostetaan kohdeverkosta komentokanava hyökkääjän suuntaan. Tätä kanavaa käyttäen hyökkääjällä on suora etäyhteys kohdeverkkoon.

Viimeisessä vaiheessa hyökkääjä tekee toimenpiteensä tavoitteensa mukaan tai siihen päästäkseen. Tämä vaihe sisältää tyypillisesti datan poistamista, joka tarkoittaa sen keräystä, kryptaamista, ja lopuksi sen lataamista pois kohdeverkosta. Muita mahdollisia tavoitteita voi olla datan eheyden tai saavutettavuuden heikentäminen. Mahdollista on myös, että hyökkääjälle riittää tässä

vaiheessa vain pääsy tiettyyn uhrilaitteeseen, josta tämä voi myöhemmin siirtyä toisiin järjestelmiin ja liikkua näin lateraalisesti kohdejärjestelmässä.

Edellä kuvattu malli, tappoketju tai kill chain, muuntuu toimintakelpoiseksi tiedustelujohtoiseksi tietoverkkojen puolustamiseksi, kun puolustajat muovaavat organisaation puolustukselliset kyvyt vastaamaan niitä prosesseja, joita hyökkääjän on käytettävä hyökätessään kyseessä olevaan kohteeseen. Hyödyntämällä mallia hyökkääjän toimista, tietoverkon puolustajat pystyvät mittaamaan suorituskykyään ja toimiensa tehokkuutta, sekä suunnittelemaan investointeja korjatakseen mahdollisia puutteita kyvykkyydessään. Kaiken kaikkiaan malli on muodostettu puolustuksen kehittäminen mielessä; ymmärtämällä miten vastustaja toimii, pystytään tekemään parempia päätöksiä turvallisuuden eteen. (Hutchins ym., 2011)

6.2.1 Kritiikkiä Cyber Kill Chainista

Cyber Kill Chain on suosiostaan huolimatta saanut osakseen myös kritiikkiä. Sen on katsottu sopivan vain tietyntyyppisiin hyökkäyksiin, jossa käytetään esimerkiksi haittaohjelmaa tai toisaalta sen ei ole katsottu kuvaavan hyökkäyksiä, jossa hyödynnetään etäyhteyksiä, sosiaalista manipulaatiota tai sisäpiiriläisten osallisuutta. (Pols, 2017) Yksi yleisimmistä kritiikin aiheista on myös CKC:n keskittyminen tiukasti organisaation verkkorajanpinnan turvaamiseen, eikä se vastaa esimerkiksi muuttuvaan tilannekuvaan yritysten siirtyessä pilvipalveluiden käyttäjiksi. Vaikka CKC on edelleen hyödyllinen työkalu, kyberhyökkäysten elinkaarta on vaikeampi ennustaa kuin sen luodessa oli. Ei ole tavatonta, että hyökkääjä yhdistää joitain vaiheita, jättäen puolustajalle entistä vähemmän aikaa reagointiin. Toisaalta mallin yleisyys voi auttaa taas hyökkääjää päättelemään kuinka kohteen puolustus on organisoitu. (The Cyber Kill Chain, 2022)

6.3 Laliberten Kill Chain

Tietoturva-asiantuntija Marc Laliberte esittää vuonna 2016 julkaistussa artikkelissaan *A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack* muutoksia Hutchinsin ym. luomaan Lockheed Martinin CKC malliin. Myös Laliberten mallissa hyökkäys on jaettu seitsemään eri vaiheeseen, mutta Laliberte on poistanut omasta mallistaan aseistamisen vaiheen prosessin alkupäästä ja lisännyt lateraalisen liikkeen vaiheen prosessin loppupuolelle toiseksi viimeiseksi. (Laliberte, 2016)

Laliberte perustelee kehittämäänsä mallia sillä, että hyökkääjä tunkeutuu kohdeverkkoon haavoittuvimman järjestelmän kautta – ei suinkaan suoraan lopulliseen kohteeseensa. Hyökkäämällä heikointa lenkkiä vastaan hyökkääjä saa jalansijan kohdeverkosta ja levittäytymällä lateraalisesti verkon sisällä se pääsee kohti kohdettaan. Toisaalta Laliberte perustelee aseistamisen vaiheen

pois jättämistä, koska se on vaihe hyökkääjän toimissa, ei puolustava taho voi tehdä mitään siltä puolustautuakseen. Lateraalisen liikkeen voi sen sijaan havaita ja estää. (Laliberte, 2016)

Laliberten malli pyrkii paljastamaan ja puolustautumaan tietyntyyppistä JavaScriptiin perustuvaa drive-by download -hyökkäystä vastaan (Laliberte, 2016). Se on kapeahko tietyntyyppistä hyökkäysvektoria kuvaava malli, eikä se niinkään pyri toimimaan yleismallina esimerkiksi APT-toimijoiden hyökkäystapaa kuvatessa. Laliberten malli ei myöskään korjaa puutteita, joita esimerkiksi Pols mainitsee CKC:sta.

7 KYBERUHKATIEDUSTELU

Kyberuhkatiedustelun avulla kerätään ja analysoidaan tietoa niin pintaverkosta, syvästä verkosta kuin pimeästä verkosta (Khera, 2020). Kyberuhkatiedustelu on todisteisiin perustuvaa tietämystä (Bromander, Swimmer, Muller, Jøsang, Skjøtskift, Eian & Borg, 2022). Tässä tutkimuksessa keskitytään pimeästä verkosta saatavan tietoon ja sen hyödyntämiseen ja analysoimiseen kyberuhkatiedustelussa. Tämän tiedon avulla pyritään ymmärtämään hyökkääjän motivaatio hyökkäykselle ja koitetaan ennustaa sen tulevaisuuden toimet. Tämä antaa päätöksenteolle tarvittavaa näkökulmaa puolustuksen järjestämiseen reaktiivisesta toiminnasta proaktiiviseen toimintaan.

Uhkatiedustelulla viitataan tietoon, kontekstiin ja näkemykseen, joka on saavutettu analysoimalla laajoja fyysisiä-, geopoliittisia- ja kyberuhkia (Flashpoint, ei pvm.). Kyberuhkatiedustelulla tarkoitetaan datan keräämistä, käsittelemistä ja analysoimista ja tästä on saatua ymmärrystä uhkatoimijoiden motiiveista, kohteista ja hyökkäysmenetelmistä. Kyberuhkatiedustelu auttaa tekemään nopeampia, paremmin tiedostettuja ja dataperusteisia turvallisuuspäätöksiä. Kyberuhkatiedustelun avulla voidaan siirtyä reaktiivisesta puolustuksesta proaktiiviseen taisteluun uhkatoimijoita vastaan. (Baker, 2023) Uhkatiedustelulla ja kyberuhkatiedustelulla on nyanssiero: uhkatiedustelu ottaa kaikki uhat huomioon, kyberuhkatiedustelu vain digitaaliset uhat (Flashpoint, ei pvm.).

Kyberuhkatiedustelu (CTI) voidaan jakaa strategiseen, operationaaliseen ja taktiseen tasoon. Strateginen taso vastaa organisaation resurssien oikeasta kohdentamisesta. Organisaation tietoturvajohdon on oltava perillä turvallisuusuhista ja toimintaympäristön tilasta osatakseen kohdentaa resursseja oikeisiin asioihin. (Samtani, Li, Benjamin, Chen, 2021) Strateginen kybertiedustelu on vastuussa uhkien tunnistamisesta lähteiden, tavoitteiden ja mahdollisten seurauksien osalta (Basheer & AlKhatib, 2021). Operatiivinen taso vastaa uhkien kartoittamisesta, arvioimisesta ja tapausten ilmoittamisesta strategiselle tasolle (Samtani & ym., 2021). Operatiivinen taso kerää tietoa hyökkääjien kyvykkyyksistä ja resursseista ja ennakoi tulevia kohteita ja käytettäviä menetelmiä (Basheer & AlKhatib, 2021). Taktinen taso keskittyy vaarantumisindikaattorei-

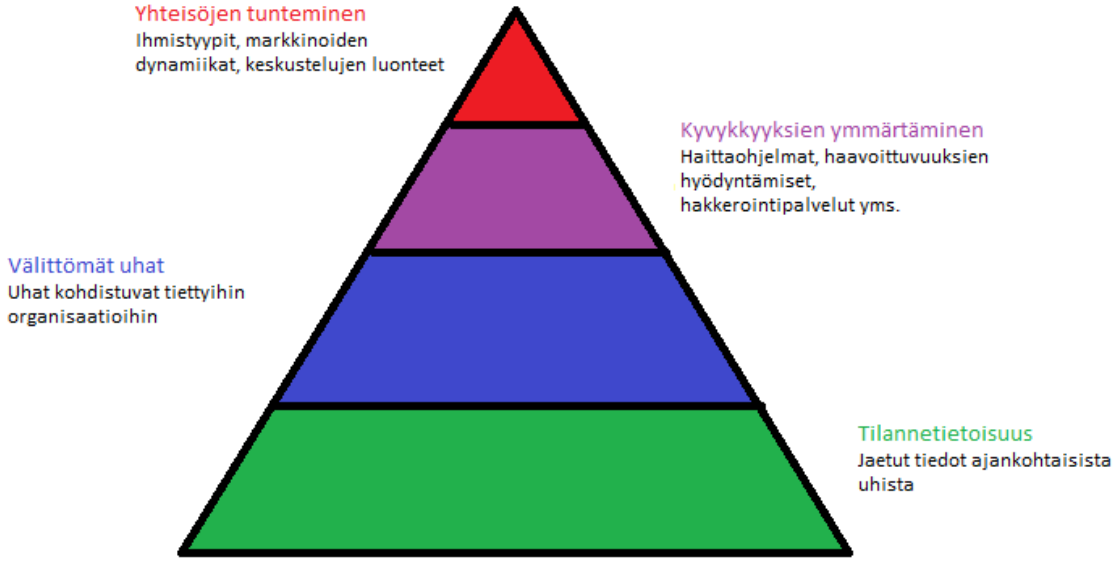
den (IOC) valvontaan ja korjaustoimenpiteiden tekemiseen. (Samtani & ym., 2021) Taktinen tai tekninen kybertiedustelu antaa tietoa hyökkääjien käyttämistä reaaliaikaisista menetelmistä ja työkaluista ja määrittelee niihin vastatoimia sekä puolustusstrategioita, joita organisaatiot sitten toteuttavat (Basheer & AlKhatib, 2021).

CTI on tietojärjestelmä, joka palvelee niin julkisen kuin yksityisenkin sektorin organisaatioita. CTI:n avulla voidaan havaita, tunnistaa, monitoroida ja vastata kyberuhkiin. Näiden avulla pystytään ymmärtämään uhkatoimijoiden taktiikoita, tekniikoita ja menetelmiä (TTP). Kaiken kaikkiaan CTI antaa organisaatiolle ajoittaisia turvallisuushälytyksiä ja muita tietoja, riippuen siitä, mihin tarkoitukseen kyseinen CTI-järjestelmä on luotu. (Basheer & AlKhatib, 2021)

CTI vastaa kysymyksiin: Kuka, Mitä, Missä, Miten ja Milloin. CTI voi kerätä tietoa monista eri lähteistä. Lähteet voivat olla sisäisiä, kuten verkkotapahtumalokitiedostot, palomuurilokit, hälytykset, vastaukset aiempiin tapauksiin, hyökkäyksiin käytetyt haittaohjelmat ja verkkojen tietoliikenne. Lähteet voivat olla myös ulkoisia, kuten muiden instituutioiden tai hallitusten raportit ja alan asiantuntijoiden kirjoitukset. Vaikuttavan ja tehokkaan CTI:n tulee olla oikeaaikaista, osuvaa, tarkkaa, täsmällistä ja toimivaa. (Basheer & AlKhatib, 2021)

7.1 Kyberuhkatiedustelun kerrokset

Kyberuhkatiedustelu (Cyber Threat Intelligence, CTI) voidaan jakaa neljään kerrokseen (kuvio 2): Tilannetietoisuuteen, välittömiin uhkiin, kyvykkyyksien ymmärtämiseen ja yhteisöjen tuntemiseen (Shakarian, 2017). Tilannetietoisuus pitää sisällään viimeaikaisista hyökkäyksistä tietoisuuden ja niiden analysoimisen. Välittömät uhat pitää sisällään muun muassa sen, että pysyy ajan tasalla siitä, minkälaisiin organisaatioihin iskuja on kohdistunut. Kyvykkyyksien ymmärtäminen pitää sisällään hakkereiden kyvykkyyksien kehittymisen arvioinnin. Yhteisöjen tunteminen pitää sisällään hakkereiden käytöksen monitoroinnin hakkeriyhteisöissä ja muutosten seuraamisen hakkerimarkkinoilla. (Basheer & AlKhatib, 2021)



KUVIO 2 Kyberuhkatiedustelun tasot (Shakarian, 2017)

7.2 Kyberuhkatiedustelun ajallinen segmentointi

Kyberuhkatiedustelu on ennen kaikkea datalähtöinen prosessi. Tämän takia se on hyvä jakaa muutamaan eri ajalliseen segmenttiin: Tiedustelun suunnittelu ja strategia, Datan kerääminen ja yhdistäminen, Uhka-analyysi ja Tiedustelutiedon käyttäminen ja levittäminen. (Samtani, Abate, Benjamin, Weifeng, 2019)

Tiedustelun suunnittelemisen tavoite on tunnistaa organisaation tiedustelutarpeet, kriittiset resurssit ja niiden haavoittuvuudet. Tiedustelun suunnitteluvaihe keskittyy uhkatrendeihin ja haavoittuvuusarviointiin. Datan keräämisen vaiheessa pyritään keräämään asiaankuuluvaa dataa uhka-analyysia varten. Datalähteitä tässä vaiheessa on sisäisen verkon data, ulkoisten uhkien syötteet ja OSINT. Uhka-analyysin vaihe keskittyy analysoimaan kerättyä dataa kehittääkseen asiaankuuluvaa, ajankohtaista ja saavutettavissa olevaa tiedustelutietoa. Analyysin kohteina voi olla esimerkiksi haittaohjelmat, tapahtumien korrelaatiot tai visualisoidut tuotteet. Tiedustelutiedon käyttämisen ja levittämisen vaiheessa pyritään lieventämään uhkia ja jakamaan tiedustelutietoa manuaalisesti tai automatisoidusti toteutettuna uhkavastauksina ja tiedusteluviestinnän standardeilla. (Samtani & ym., 2019)

Tässä tutkimuksessa keskitytään erityisesti segmenttiin ”Tiedustelun suunnittelu ja strategia”. Tutkimuksessa kuitenkin esitellään datan keräämistä ja yhdistämistä yksinkertaisesti ja esimerkkiluontoisesti.

7.3 OSINT & Web Crawlerit

Avointen lähteiden tiedustelu (OSINT) määritellään tiedon järjestelmälliseksi keräämiseksi ja hyödyntämiseksi julkisista lähteistä tiedusteluvaatimuksien täyttämiseksi. Tiedon etsiminen, kerääminen ja seuranta ovat OSINT:n tärkeimpiä prosesseja. Pintaverkon OSINT hyödyntää muun muassa edistynyttä hakukonekyselyä ja indeksointia, sosiaalisen median louhintaa ja seurantaa ynnä muita tekniikoita. Pimeän verkon OSINT vaatii hieman poikkeavia tekniikoita. (Block, 2023)

Web crawlerit ovat ohjelmistoja, jotka käyvät järjestelmällisesti World Wide Webiä läpi löytääkseen kaiken saatavilla olevan tiedon. Crawlerit toimivat muutaman perusaskeleen logiikalla (taulukko 4, Kalpakis, Tsikrika, Cunningham, Iliou, Vrochidis, Middleton & Kompatsiaris, 2016):

TAULUKKO 4 Crawlereiden toimintalogiikka

1. Indeksointi aloitetaan alku-URL:llä (seed URL)
2. Haetaan ja jäsennellään sisältöä
3. Otetaan hyperlinkit talteen sivuilta
4. Laitetaan talteen otetut hyperlinkit tarkastelujonoon
5. Tehdään haku jokaisella jonon URL:lla
*Tätä prosessia toistetaan iteratiivisesti niin kauan, että halutut lopetusehdot täyttyvät (esimerkiksi haettujen sivujen määrä)

Crawlereilla on monia erilaisia käyttötarkoituksia erilaisissa ohjelmissa ja tutkimusaiheissa. Erityisesti niitä käytetään hakukoneissa. Hakukoneissa crawlerit indeksoivat verkkosivuja, jotta hakukonekäyttäjän hakiessa tietoa hakukoneesta, osaisi se hakea tiedon nopeasti ja helposti hakusanojen mukaisesti. Crawlereita käytetään myös verkkoarkistoinnissa. Tässä yhteydessä crawlerit keräävät ja arkistoivat valtavia sivukokonaisuuksia tulevaisuuden hyödyntämistä varten. (AlKhatib & Basheer, 2019)

Tutkimuksessa käytettävän Cyber Intelligence Housen pimeän verkon analyysialusta Cyber Exposure Platform (CEP) mahdollistaa tietojen hakemisen sekä pintaverkosta että syvästä ja pimeästä verkosta ilman itse toteutettavaa OSINTia tai Web Crawlereiden asettamista. Näiden termien ja toimintojen esittely on kuitenkin tärkeää siltä kannalta, mikäli CEPin kaltaista alustaa ei olisi käytettävissä tutkimuksessa tai myöhemmin sitä sovellettaessa muussa yhteydessä.

8 KÄYTETYT MENETELMÄT JA TUTKIMUKSEN TULOKSET

Tässä luvussa kuvataan aluksi käytetyt tutkimusmenetelmät. Tämän jälkeen käydään läpi tutkimuksen toteutus Shakarian (2017) tasomallin mukaisesti yksi taso kerrallaan.

8.1 Tutkimusmenetelmät

Tutkimuksen runkona toimi Shakarian (2017) esittämä Kyberuhkatiedustelun tasot -malli (kuvio 2). Tutkimuksessa keskityttiin pääosin kyberuhkatiedustelun strategiseen tasoon. Tutkimus tehtiin hyödyntäen Cyber Intelligence Housen (CIH) tarjoamaa Cyber Exposure Platform (CEP) pimeän verkon analyysialustaa. Shakarian Kyberuhkatiedustelun tasot -mallia käytiin vaihe vaiheelta läpi, ja haettiin CEP:ista näihin vaiheisiin relevanttia tietoa. Tutkimusta ei tehty ”case-tyylisenä”, vaan tutkimuksessa pyrittiin saamaan yleispätevää ja mahdollisimman monikäyttöistä tutkimustietoa aiheesta.

Tutkimus toteutettiin laadullisena sisällön analyysinä Elo, Kajula, Tohmola ja Kääriäisen (2022) tutkimuksen ”Laadullisen sisällönanalyysin vaiheet ja eteneminen” esittämää toimintatapaa mukaillen. Tutkimuksen alussa määriteltiin tutkimuksen aihe ja tutkimuskysymykset, sekä tehtiin aiheen tiimoilta kirjallisuuskatsaus. Tämän jälkeen tutkimuksen rungoksi valittiin Shakarian (2017) esittämän ”Kyberuhkatiedustelun tasot” -malli. Malli koostuu neljästä tasosta, joten tiedonkeruu ja analysointi jaoteltiin tämän neliportaisen mallin mukaisesti. Tutkimuksessa käytetty tieto kerättiin Cyber Intelligence Housen Cyber Expocure Platformilta Shakarian esittämien tasojen ja niiden selitysten muodostamien vaatimusten mukaisesti. Jokaiselle tasolle pyrittiin saamaan yleisesti pätevää ja yleistettävissä olevaa aineistoa, jota analyysin ja käsittelyn jälkeen hyödynnettiin tutkimuksessa.

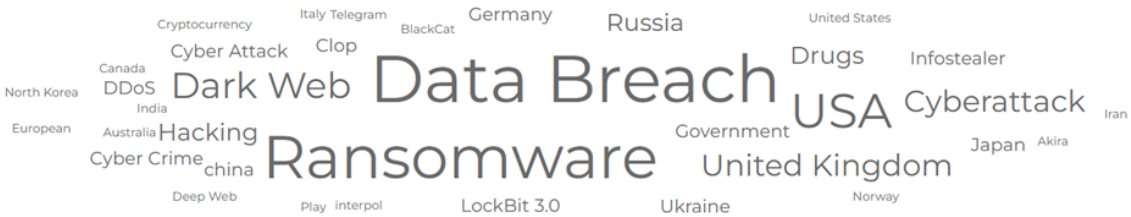
8.2 Tilannetietoisuus

Shakarian (2017) mallin alimmalla ”Tilannetietoisuuden” tasolla pyritään tiedostamaan viimeaikaisia tapahtumia ja analysoimaan niitä. Millaisia hyökkäyksiä on tapahtunut? Ketkä niitä tekevät? Millaisia resursseja näillä hyökkääjillä on? Mitä menetelmiä hyökkääjät ovat käyttäneet? Mitä seurauksia hyökkäyksillä on ollut? Näiden viimeaikaisten hyökkäysten ja tapahtumien analysoiminen antaa tietoa siitä, minkälaisia uhkia myös oma organisaatio todennäköisesti voisi kohdata. Näitä tapahtumia analysoimalla ja niitä peilaamalla oman organisaation puolustus- ja varautumiskyvykkyyksiin, voidaan todentaa ja kehittää omaa puolustusvalmiutta samankaltaisten tapausten varalta.

Tilannetietoisuus on kyberuhkatiedustelun ensimmäinen ja laajin taso Shakarian (2017) mallissa. Tällä tasolla halutaan ymmärtää oman organisaation positio toimintaympäristössä. Tiedostetaan millaisia ne muut toimintaympäristön organisaatiot ovat ja millaisia mahdollisia uhkia tämä toimintaympäristö kohtaa. Tässä yhteydessä toimintaympäristön muiden toimijoiden kanssa on hyvä jakaa tietoa siitä, mitä toimintaympäristössä tapahtuu, mitkä käytänteet ovat havaittu hyviksi ja toimiviksi, sekä millaisia uhkia organisaatiot ovat tahoillaan kokeneet tai havainneet. Näitä tiedonjakoyhteisöjä kutsutaan ISAC-tiedonvaihtoryhmiksi (Information Sharing Analysis Centre) (Enisa, ei pvm.). Tällä tasolla lisäksi ylläpidetään omien sensoreiden, esimerkiksi IOC, IOA ja IOB, keräämää tietoa. Tuntemalla toimintaympäristön ja valvomalla indikaattoreita saadaan jo hyvää perustason tilannetietoisuutta. Tätä tietoa jakamalla muille toimintaympäristön toimijoille, ylläpidetään laajempaa yhtenäistä tilannetietoisuutta. Kun mahdollisista vertaisorganisaatioihin kohdistuneista hyökkäyksistä voidaan tämän jaetun tiedon muodossa oppia yhdessä, voi tämä oppi jalostua nopeastikin erilaisiksi puolustustoimenpiteiksi läpi toimintaympäristön.

Tilannetietoisuuden hallintaan kuuluu toimintaympäristön eri uhkien tunnistaminen ja tiedostaminen. Organisaation on tiedostettava kyberympäristön eri uhkia, ymmärrettävä niiden aiheuttamat riskit ja mahdolliset riskien realisoitumisesta aiheutuvat seuraukset. Organisaation on tunnistettava eri uhkatoimijoiden painokertoimet, joilla arvioidaan miten vakavia eri uhkaskenaariot ovat. Näiden arvioiden perusteella organisaatio voi resursoida puolustuksellisia resurssejaan parhaaksi katsomallaan tavalla. Organisaation on tiedostettava eri APT-toimijoiden, kyberrikollisten, haktivistien, sisäpiirin uhkan sekä muiden kyberuhkatoimijoiden painoarvot toimintaympäristössään ja tehtävä toimenpiteitä sen mukaisesti, että nämä näiden toimijoiden muodostama uhka minimoitaisiin mahdollisimman tehokkaalla tavalla.

Tässä tutkimuksessa Shakarian (2017) mallin tilannetietoisuutta rikastettiin analyysin ja pohdinnan lisäksi Cyber Intelligence housen CEP-alustan tiedoilla. Alustalta kerättiin tietoa viimeaikaisista kybertapahtumista ja toimijoista: kybertapahtumien avainsanoja (kuvio 3), aktiivisia lunnashaittaohjelmatoimijoita (kuvio 4) sekä uusia lunnashaittaohjelmatoimijoita (kuvio 5).



KUVIO 3 Viimeisen vuoden ajalta kybertapahtumien avainsanoja (Cyber Intelligence House, 22.05.2024)

KUVIO 4 Aktiivisia lunnashaittaohjelmatoimijoita (Cyber Intelligence House, 22.05.2024)

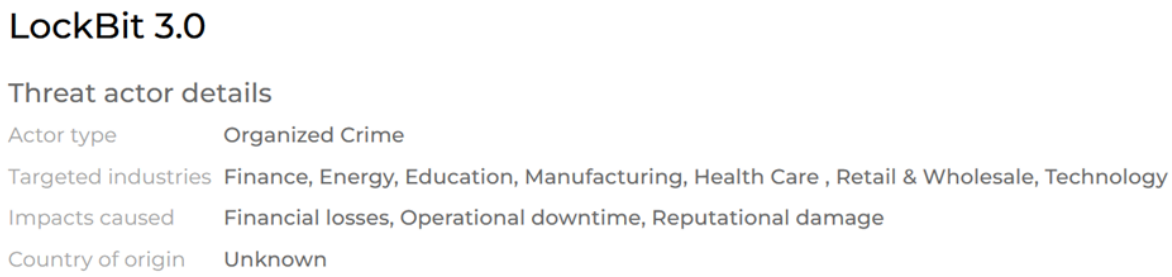
KUVIO 5 Uusia lunnashaittaohjelmatoimijoita (Cyber Intelligence House, 22.05.2024)

8.3 Välittömät uhkat

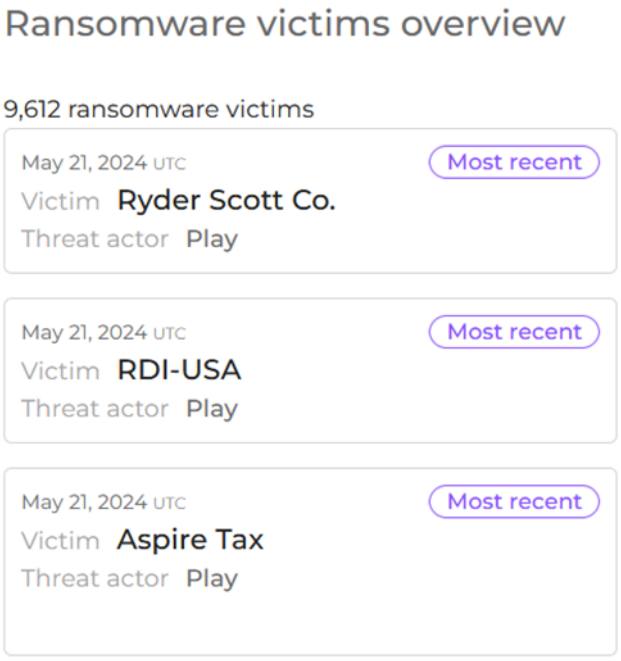
Tämä Shakarian (2017) Kyberuhkatiedustelun tasomallin toinen taso, ”Välittömät uhkat”, on käsiteltävistä tasoista yksinkertaisin. Tämän tason tarkoitus on nimensä mukaisesti tunnistaa välittömät uhkat organisaatiota kohtaan. Käytännössä yksinkertaisin tapa, miten tätä välittömien uhkien tilannekuvaa voidaan tuottaa, on asettamalla pimeän verkon alustoille Web Crawlereita tai suorittaa itse pimeän verkon OSINTia ja selvittää, onko organisaatiosta käyty keskustelua jollain pimeän verkon alustalla. Tällaiset keskustelut voisivat indikoida tulevia hyökkäyksiä organisaatiota kohtaan. Tutkimuksessa käytettävä CEP-

työkalu mahdollistaa pimeän verkon keskustelualustojen aktiivisen indikoinnin organisaatio-osumien varalta, jolloin organisaation itse ei tarvitse luoda erikseen minkäänlaisia crawlereita tai tehdä OSINTia. Tämän simuloiminen tutkimuksessa vaatisi tietyn kohdeorganisaation ja heidän henkilötietojen käyttöluvan. Tutkimuksessa näitä ei kuitenkaan lähdetty tekemään, vaan pidättäydyttiin yleispätevissä menetelmissä.

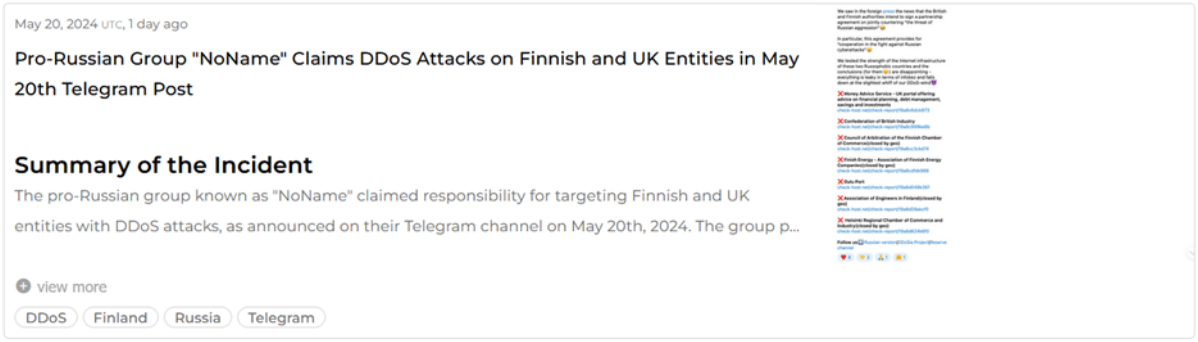
Toinen tapa tunnistaa organisaatiota uhkaavia toimijoita on tunnistaa, minkälaisia iskuja omalle toimintasektorille kohdistuu ja minkälaisia uhkatoimijoita iskuja tekevät tahot ovat. Esimerkiksi kuvio 6 käsittelee uhkatoimijan tietoja, jotka kattavat muun muassa kohdesektorin ja iskujen vaikutuksia. Lisäksi tutkittiin, millaisia uhreja eri uhkatoimijoilla on ollut (kuvio 7). Yksittäisiä kybertapahtumia tarkasteltiin myös lähemmin tapahtumakohtaisesti (kuvio 8, 9, 10, 11 & 12).



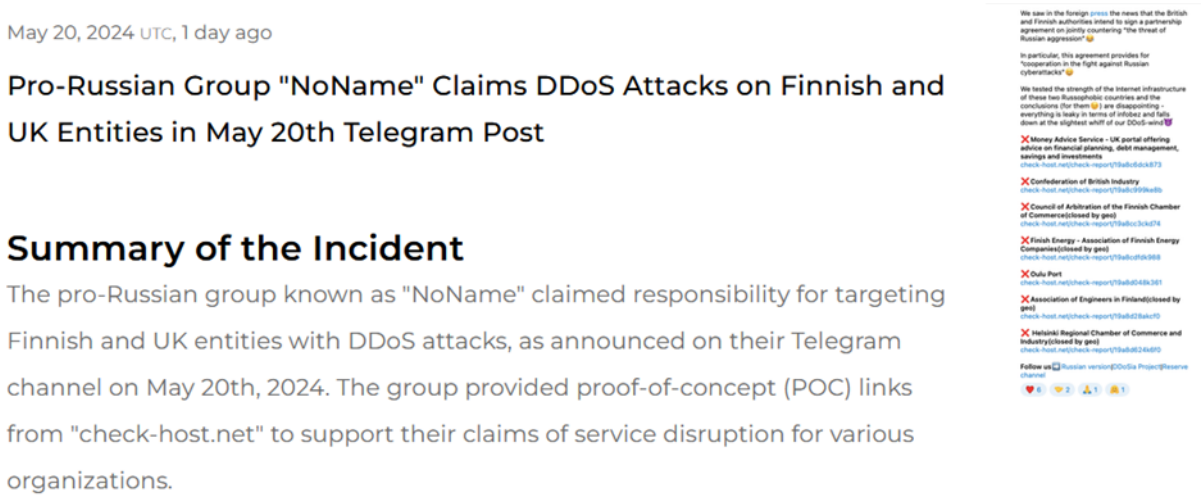
KUVIO 6 LockBit tietoja (Cyber Intelligence House, 23.05.2024)



KUVIO 7 Lunnashaittaohjelmien uhreja (Cyber Intelligence House, 22.05.2024)



KUVIO 8 Kybertapahtuma otsikkotasolla (Cyber Intelligence House, 22.05.2024)



KUVIO 9 Kybertapahtuman yhteenveto (Cyber Intelligence House, 22.05.2024)

Details of the Attack

Entities Targeted on May 20th, 2024:

1. **Council of Arbitration of the Finnish Chamber of Commerce (closed by geo)**
   - Check-host report: check-host.net/check-report/19a8cc3ckd74
2. **Finnish Energy - Association of Finnish Energy Companies (closed by geo)**
   - Check-host report: check-host.net/check-report/19a8cdfdk988
3. **Oulu Port**
   - Check-host report: check-host.net/check-report/19a8d048k361
4. **Association of Engineers in Finland (closed by geo)**
   - Check-host report: check-host.net/check-report/19a8d28akcf0
5. **Helsinki Regional Chamber of Commerce and Industry (closed by geo)**
   - Check-host report: check-host.net/check-report/19a8d624k6f0

The original post can be found on their Telegram channel: **https://t.me/noname05716eng**

KUVIO 10 Hyökkäyksen tietoja (Cyber Intelligence House, 22.05.2024)

Additional Information Shared by NoName

DDoSia Project: t.me/+igupZcC_O45jMGY1

Stickers: t.me/addstickers/NoName057_16_bears

Russian Version: t.me/noname05716

Reserve Channel: t.me/noname05716_reserve

Contact: noname057_16_official@proton.me

Their Telegram channel has 7,422 subscribers at the time of writing this report.

KUVIO 11 Lisäinformaatiota (Cyber Intelligence House, 22.05.2024)

KUVIO 12 Hyökkääjän aiempia kohteita tapaukseen liittyen (Cyber Intelligence House, 22.05.2024)

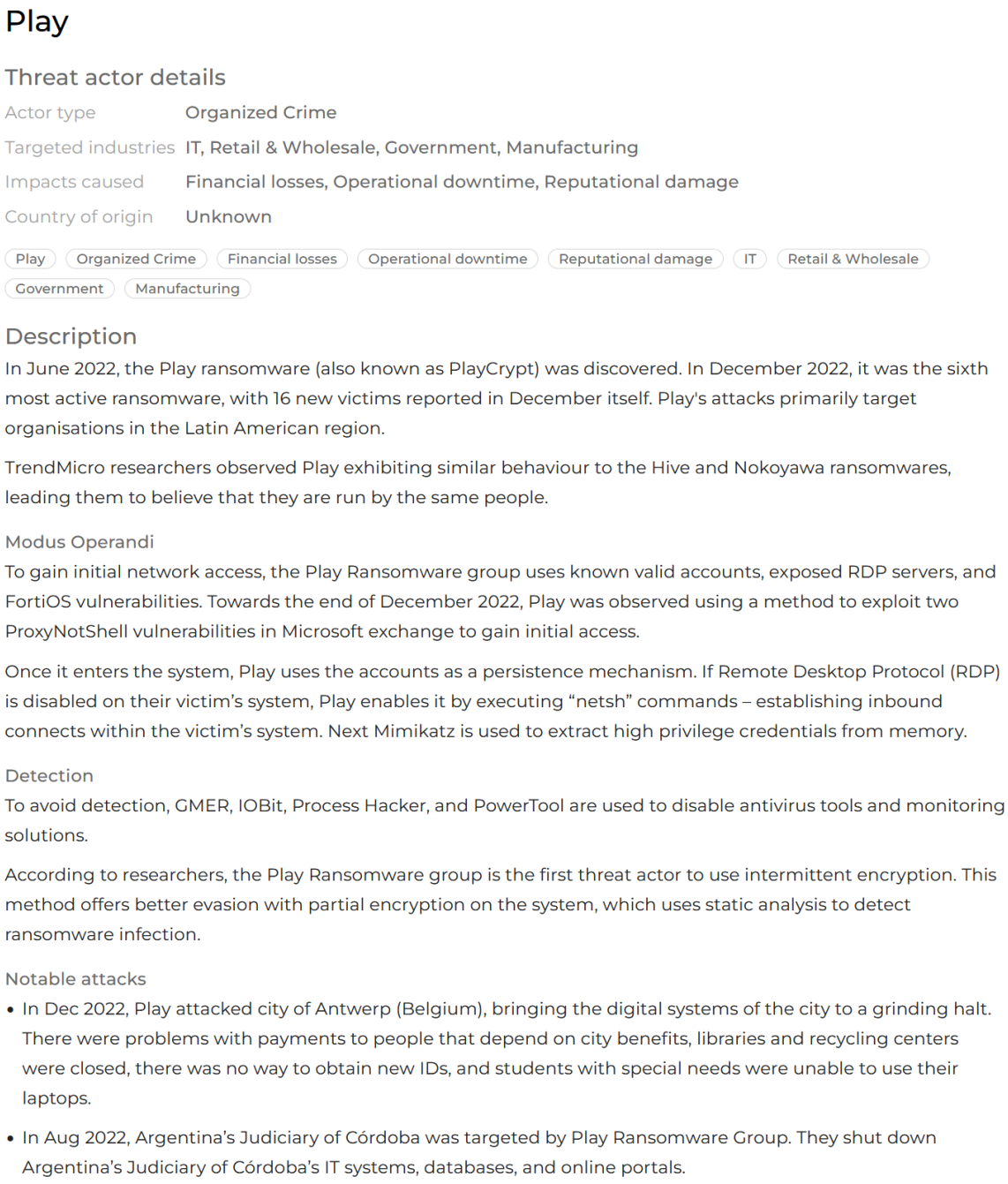
Edellä kuvattujen esimerkkien, sekä muiden vastaavien tietomuotojen avulla saadaan koottua tietoa, jolla tunnistetaan organisaatiota uhkaavia toimijoita sekä hyökkäysmuotoja. Olkoon se sitten lunnashaittaohjelma tai DDoS hyökkäys, voidaan näihin kaikkiin hyökkäysmenetelmiin varautua ennalta. Mikäli tunnistetaan organisaatiota tai sen toimintaympäristöä uhkaavia toimijoita tai hyökkäysmenetelmiä ennen uhkan realisoitumista, voidaan varautua siihen näiden tilannetietojen avulla huomattavasti tehokkaammin, kuin ilman niitä. Tilannekuvan pohjalta voidaan analysoida mihin kohdeorganisaatioihin, mille sektorille, mille maantieteelliselle tai vaikkapa minkälaisen poliittisen taustan omaavalle taholle hyökkäyksiä on kohdistettu. Tilannekuvan avulla saadaan myös tietoon, minkälaisia uhkia toimintaympäristö kohtaa ja havaitsee. Näitä analysoimalla voidaan arvioida, missä määrin nämä uhkat kohdistuvat myös omaan organisaatioon.

8.4 Kyvykkyyksien ymmärtäminen

Seuraavana tasona Shakarian (2017) Kyberuhkatiedustelun taso -mallissa on kyvykkyyksien ymmärtäminen. Tämä vaihe on jo hieman edistyneempi ja eteenpäin nojaavampi. Tässä vaiheessa pyritään ymmärtämään, miten hakkereiden kyvykkyydet kehittyvät. Millaisia ohjelmia tai menetelmiä hakkereilla on käytössään tai kehitteillä. Puolustuksen pitäisi pyrkiä pysymään tässä kehityksessä mahdollisimman tehokkaasti mukana.

Tutkiessa aktiivisia kybertoimijoita kybertoimintaympäristössä, on erittäin tärkeää seurata näiden toimijoiden toimintaa ja niissä tapahtuvia muutoksia. Muutoksissa kybertoimijat ovat reagoineet puolustuksen kehitykseen ja tehneet toiminnastaan tehokkaampaa, joka hyödyntää kohteiden heikkouksia mahdollisesti eri tavalla kuin aiemmin. Näissä tilanteissa erityisesti on pureuduttava kyberuhkatoimijan kyvykkyyksien ymmärtämiseen ja tuntemiseen, jotta voidaan oma puolustus järjestää siten, että uhka pystyttäisiin minimoimaan. Yksinkertaisimmillaan tämä tapahtuu siten, että informoidaan oman organisaation, sekä mahdollisesti eri sidosryhmien jäseniä muuttuneesta uhkasta ja kerrotaan toimintatavat, joilla tätä uhkaa pystytään vähentämään. Esimerkiksi, mikäli jonkin uhkatoimijan on havaittu tekevän uudenlaista sosiaalista hakkerointia tai kalastelua, on näissä tapauksissa oman henkilöstön käyttäytyminen ja toimintamenetelmät avainasemassa uhan neutralisoimisessa. Ihan pelkällä työntekijöiden informoimisella ja kouluttamisella saadaan jo erinomaisia tuloksia tämänkaltaisissa tapauksissa.

On hyvä tietää, miten aktiiviset uhkatoimijat tekevät hyökkäyksiään ja millaisia haittaohjelmia he käyttävät. Kuviossa 13 nähdään muun muassa aktiivisen uhkatoimijan hyökkäysten kohdesektori, toimintamenetelmät, sekä esimerkkejä uhkatoimijan hyökkäyksistä.



Play

Threat actor details

Actor type	Organized Crime
Targeted industries	IT, Retail & Wholesale, Government, Manufacturing
Impacts caused	Financial losses, Operational downtime, Reputational damage
Country of origin	Unknown

Play | Organized Crime | Financial losses | Operational downtime | Reputational damage | IT | Retail & Wholesale | Government | Manufacturing

Description

In June 2022, the Play ransomware (also known as PlayCrypt) was discovered. In December 2022, it was the sixth most active ransomware, with 16 new victims reported in December itself. Play's attacks primarily target organisations in the Latin American region.

TrendMicro researchers observed Play exhibiting similar behaviour to the Hive and Nokoyawa ransomwares, leading them to believe that they are run by the same people.

Modus Operandi

To gain initial network access, the Play Ransomware group uses known valid accounts, exposed RDP servers, and FortiOS vulnerabilities. Towards the end of December 2022, Play was observed using a method to exploit two ProxyNotShell vulnerabilities in Microsoft exchange to gain initial access.

Once it enters the system, Play uses the accounts as a persistence mechanism. If Remote Desktop Protocol (RDP) is disabled on their victim's system, Play enables it by executing "netsh" commands – establishing inbound connects within the victim's system. Next Mimikatz is used to extract high privilege credentials from memory.

Detection

To avoid detection, GMER, IOBit, Process Hacker, and PowerTool are used to disable antivirus tools and monitoring solutions.

According to researchers, the Play Ransomware group is the first threat actor to use intermittent encryption. This method offers better evasion with partial encryption on the system, which uses static analysis to detect ransomware infection.

Notable attacks

- In Dec 2022, Play attacked city of Antwerp (Belgium), bringing the digital systems of the city to a grinding halt. There were problems with payments to people that depend on city benefits, libraries and recycling centers were closed, there was no way to obtain new IDs, and students with special needs were unable to use their laptops.
- In Aug 2022, Argentina's Judiciary of Córdoba was targeted by Play Ransomware Group. They shut down Argentina's Judiciary of Córdoba's IT systems, databases, and online portals.

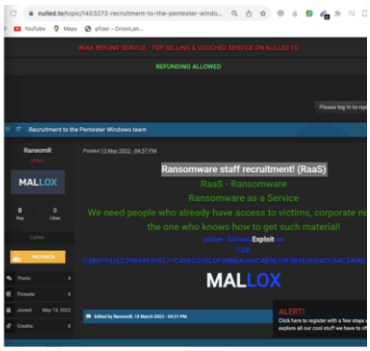
KUVIO 13 Play -uhkatoimijan tietoja (Cyber Intelligence House, 03.06.2024)

8.5 Yhteisöjen tunteminen

Viimeisenä ja strategisimpana tasona Shakarian (2017) Kyberuhkatiedustelun taso -mallissa nähdään yhteisöjen tunteminen. Tämä yhteisöjen tunteminen tarkoittaa sitä, että täytyy pyrkiä tuntemaan mahdollisimman laajalla ja syvällisellä tasolla haitallisten hakkerointiyhteisöjen toimintaa. Tämä kattaa niin pimeiden markkinoiden dynamiikan ymmärtämisen, tiettyjen avainhenkilöiden mer-

kityksen niissä, sekä eri yhteisöalustojen nousut ja laskut. Tieto näillä yhteisöalustoilla on saatavilla usein vain rajoitetun ajan, jonka takia tiedon keräämisen on oltava jatkuvaa.

Näiden keskustelualustojen keskustelun luonteen ja sisällön tunteminen on erityisen tärkeää. Erilaisilla alustoilla käy keskustelua hyvin monenlaiset kyberuhkatoimijat. Esimerkiksi (kuviot 14 & 15) lunnashaittaohjelmatoimijat saattavat julkaista niissä rekrytointi-ilmoituksia. Tämä kertoo aktiivisista ja kasvavista uhkatoimijasta, joiden kehitystä on syytä seurata tulevaisuudessa.



Aug 13, 2023 UTC, 9 months ago

****Recruitment of Affiliates for Ransomware by Russian Threat Actors in Russian-Speaking Forums****

Executive Summary:

This report outlines the recruitment activities undertaken by Russian threat actors within Russian-speaking hacking and cybercrime forums, aiming to expand their ransomware operations through the enlistment of affiliates. The report sheds light on their recruitment strategies, affiliations, and the platforms utilized to engage potential partners.

Threat Actor Details:

- **Aliases:** Ransomr, MALLOX
- **Suspected Affiliation:** Linked to the "Mallox" ransomware group
- **Forum Memberships:** community.xyz, forumteam.life, bdf.ac, darknet.ug, nulled.to, codby.net, 4chat.com, deepweb.to

Recruitment Activities and Findings:

1. **Forum:** community.xyz
   - **Date:** February 2, 2023
   - **Post Title:** Набор в команду - Пентестинга! (Recruitment to the Team - Pentesting!)
   - **URL:** "https://comunity.xyz/viewforum.php?f=22"
   - **Avatar:** "Mallox ransomware"
2. **Forum:** forumteam.life
   - **Date:** February 2, 2023
   - **Post Title:** Recruitment to the Team - Pentesting!
   - **URL:** "https://forumteam.life/tags/ransomware/"
   - **Contact Details:** Jabber: Some@exploit.im, TOX: C3807932EC298049310277C45EC059CDF08BBA566C4B9E33F0B5E0D0ACC64C3406E79DD2441E"
   - **Note:** Forum has dedicated "ransomware" section for recruitment
3. **Forum:** bdf.ac
   - **Date:** February 3, 2023
   - **Post Title:** Recruitment to the Team - Pentesting!
   - **URL:** "https://bdf.ac/threads/nabor-v-komandu-pentestinga.153204/"
   - **Contact Details:** Jabber: Some@exploit.im, TOX: C3807932EC298049310277C45EC059CDF08BBA566C4B9E33F0B5E0D0ACC64C3406E79DD2441E"
   - **Tags:** "ransomware", "mallox"
   - **Avatar:** "Mallox ransomware"
4. **Forum:** darknet.ug
   - **Date:** February 2, 2023
   - **Post Title:** Recruitment to the Team - Pentesting!
   - **URL:** "https://darknet.ug/threads/nabor-v-komandu-pentestinga.4167/"
   - **Avatar:** "Mallox ransomware"
5. **Forum:** nulled.to
   - **Date:** May 13, 2022
   - **Post Title:** Ransomware Staff Recruitment! (RaaS)
   - **URL:** "https://www.nulled.to/topic/1403272-recruitment-to-the-pentester-windows-team/"
   - **Avatar:** "Mallox ransomware"
6. **Forum:** codby.net
   - **Date:** February 2, 2023
   - **Post Title:** Team Recruitment - Pentesting
   - **User Profile:** "https://codeby.net/members/ransomr.252869/"

KUVIO 14 Rekrytointi-ilmoitus (1/2) (Cyber Intelligence House, 03.06.2024)

7. **Forum:** 4chat.com

- **Date:** February 2, 2023
- **Post Title:** Recruitment to the Team - Pentesting!
- **URL:** "https://4cht.com/threads/%D0%9D%D0%B0%D0%B1%D0%BE%D1%80-%D0%B2-%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D1%83-%D0%BF%D0%B5%D0%BD%D1%82%D0%B5%D1%81%D1%82%D0%B8%D0%BD%D0%B3%D0%B0.263352/"
- **Avatar:** "Mallox ransomware"

3. **Forum:** deepweb.to

- **Date:** March 10, 2023
- **Post Title:** Recruitment to the Team - Pentesting!
- **URL:** "https://deepweb.to/threads/nabor-v-komandu-pentestinga-raas.135266/"

Analysis and Implications:

The recruitment efforts of Russian threat actors "Ransomr" and "MALLOX" signify their intent to expand their ransomware operations by enlisting skilled individuals. Their cross-forum presence indicates a coordinated effort to establish a network of affiliates with the technical expertise required for ransomware attacks. The affiliation with the "Mallox" ransomware group further raises concerns about the potential amplification of their malicious activities.

Recommendations:

1. Continuously monitor the activities of "Ransomr" and "MALLOX" across forums to identify new recruitment efforts.
2. Collaborate with law enforcement agencies to disrupt the recruitment and operation of ransomware groups.
3. Enhance threat intelligence sharing to enable proactive defense against emerging ransomware threats.

Conclusion:

The recruitment activities by Russian threat actors underscore the evolving tactics employed by ransomware groups to expand their operations. The need for proactive countermeasures, international collaboration, and raising public awareness are critical to mitigating the threat posed by these actors and their affiliates.

view less

Mallox Ransomware Russia

KUVIO 15 Rekrytointi-ilmoitus (2/2) (Cyber Intelligence House, 03.06.2024)

9 JOHTOPÄÄTÖKSET JA POHDINTA

Tutkimuksessa pohdittiin, miten ennakoivaa kybertilannekuvaa muodostetaan, mistä kybertilannekuva muodostuu, ja miksi ennakoivaa kybertilannekuvaa muodostetaan.

Tutkimuskysymykseen ”Miten muodostetaan ennakoivaa kybertilannekuvaa” tutkimus esittää Shakarian (2017) neliportaisen Kyberuhkatiedustelun tasomallin mukaisen ratkaisun. Tutkimuksessa todetaan, että laadukkaalla kyberuhkatiedustelulla saadaan aikaan ennakoivaa kybertilannekuvaa. Tämä osaltaan vastaa myös tutkimuksen apukysymykseen, ”Miten kybertilannekuva muodostuu”. Ennakoivaa kybertilannekuvaa muodostetaan, jotta voitaisiin valmistautua kybertoimintaympäristön erilaisiin uhkatekijöihin mahdollisimman tehokkaasti ja kattavasti, sekä ennen kaikkea ennakoivasti.

Ennakoivaa kybertilannekuvaa voidaan muodostaa monella eri tavalla. Tässä tutkimuksessa lähestytään aihetta Shakarian (2017) Kyberuhkatiedustelun tasot -mallin kautta. Kyberuhkatiedustelulla aikaan saatujen tietojen pohjalta syntyy kybertilannekuvaa. Käytetty tasomalli jakaa kyberuhkatiedustelun neljään eri tasoon: tilannetietoisuus, välittömät uhat, kyvykkyyksien ymmärtäminen ja yhteisöjen tunteminen. Kun organisaatio hallitsee nämä neljä aihealuetta, on ennakoiva kybertilannekuva jo hyvällä tasolla.

On ensiarvoisen tärkeää, että niin kyberuhkatiedustelun kuin siitä muodostettavaan kybertilannekuvan tuottamiseen käytetään verkon jokaista osa-aluetta. Niin pintaverkkoa, syvää verkkoa kuin pimeää verkkoa. Tässä tutkimuksessa korostettiin pimeän verkon roolia tiedon lähteenä, sillä kyberuhkatoimijat toimivat ja kommunikoivat pääosin pimeän verkon alustoilla. Syynä tälle on pimeän verkon sisään rakennettu vahva anonymiteetti.

Voidaan todeta, että kybertilannekuvaa muodostetaan hyvällä ja johdonmukaisella kyberuhkatiedustelulla. Tutkimuksessa kyberuhkatiedustelua toteutetaan neliportaisella mallilla, jossa tilannetietoisuus on kaiken perusta. Hyvä tuntemus omasta kybertoimintaympäristöstä ja sen ajankohtaisista kybertapahtumista on avain hyvään tilannetietoisuuteen. Hyvän tilannetietoisuuden päälle tulee rakentaa välittömien uhkien tunnistamisen menetelmät. Näillä menetelmillä pyritään tunnistamaan omaan organisaatioon kohdistuvat uhkat. Välit-

tömien uhkien tunnistamisen jälkeen siirrytään uhkatoimijoiden kyvykkyyksien ymmärtämiseen. On tiedostettava, millaiset resurssit eri uhkatoimijoilla on käytössään, eli millaisia haittaohjelmia tai hyökkäysmenetelmiä he käyttävät. Tämän tiedon avulla puolustava organisaatio pystyy paremmin organisoida ja resursoida omaa puolustustaan. Viimeisenä tasona kyberuhkatiedustelun toteuttamisen mallissa keskitytään uhkatoimijoiden yhteisön tuntemiseen. Tuntemalla tämän yhteisön käytöksessä tapahtuvat muutokset, voidaan niihin myös pyrkiä reagoimaan nopeasti erilaisin vastatoimin.

Shakarian (2017) Kyberuhkatiedustelun tasomallin voidaan todeta olevan hyvä pohja strategisen kyberuhkatiedustelun suunnittelussa. Malli kattaa kyberuhkatiedustelun melko kattavalla perspektiivillä, lähtien isosta ”scoupista” kohti pienempiä ja suppeampia teemoja. Tällä Shakarian tasomallilla voidaan arvioida ja järjestää alustavasti omaa kyberuhkatiedustelua oikeansuuntaiseksi toiminnaksi. Malli kertoo karkeasti sen, mitä vähimmillään organisaation tulee hallita laadukkaan kyberuhkatiedustelun aikaansaamiseksi. Jokainen kategoria tarkentuu ja kehittyy oman organisaation position ja toimintakentän mukaisesti. Tämä malli ohjaa ja viitoittaa kohti kattavaa ja selkeää kyberuhkatiedustelun suunnittelua tai jo olemassa olevan järjestelmän auditoimista. Tutkimuksessa tuotettiin Cyber Intelligence Housen Cyber Exposure Platformin avulla Shakarian mallin mukainen kyberuhkatiedustelutieto geneerisesti ja esimerkinomaisesti. Shakarian (2017) mallin tarkempi arviointi vaatisi tapaustutkimuksen ja sen avulla tehtävän tarkemman arvioinnin kyberuhkatiedustelun suunnittelusta, toteutuksesta sekä toimivuudesta.

Tutkimuksen haasteena oli erityisen vaikea aihe. Aihe on vaikea siksi, että tutkittavat uhkatoimijat ovat ammattimaisia ja hyvin resursoituja toimijoita, jotka tekevät kaikkensa sen eteen, että niiltä olisi hankala puolustautua. Tämä valittu aihe on erittäin tärkeä sekä ajankohtainen ja tämän vuoksi tutkimusta aiheesta on saatava lisää. Digitalisaation myötä lähestulkoon kaikki yhteiskunnan toiminnot ovat siirtyneet jollain tasolla verkkoon. Kaikki mikä on yhteydessä verkkoon, on myös haavoittuvaista. Tämän vuoksi kyberturvallisuuden tutkimusta ja ennen kaikkea ennakoivaa kybertilannekuvaa olisi ensiarvoisen tärkeä tutkia ja kehittää entistä paremmaksi.

Tutkimuksen luotettavuutta arvioitaessa on otettava huomioon tutkimuksen verrattain laaja teoriapohja. Tutkimusta lähestyttiin hyvin laajalla teoriaotannalla, jossa määriteltiin eri käsitteitä sekä malleja hyvin monipuolisesti. Jokaisen käsitteen, mallin tai aihealueen määrittelyyn pyrittiin saamaan useista lähteistä eri näkökantoja aiheesta. Alan käsitteistöä on esitelty, käytetty ja muodostettu osittain myös eri teknologiayhtiöiden tai järjestöjen toimesta. Teoriaosuuden lähteistä osa koostuukin juuri verkkolähteistä, joiden takana on toisinaan kaupallinen toimija. Erityisesti näitä verkkolähteitä, joissa taustalla on jokin kaupallinen tai muulla tavalla sidonnainen toimija, pyrittiin tutkimuksessa arvioimaan tarkasti. Lähdettä arvioitaessa kiinnitettiin tällöin erityisesti huomiota lähteen objektiivisuuteen, loogisuuteen, johdonmukaisuuteen sekä yhteneväisyyteen muun aihetta käsittelevän yhteisön kanssa. Tutkimuksessa käytettyjen verkkolähteiden avulla pyrittiin määrittelemään kaikista yksinkertaisim-

pia ja yleisesti hyvin yhtenevästi määriteltyjä käsitteitä. Monimutkaisempiin aiheisiin pyrittiin aina löytämään vertaisarvioituja tutkimuksia, joiden objektiivisuutta ja totuuspohjaa arvioitiin perinteisen akateemisen lähdekritiikin näkökulmasta.

Kappaleessa 5 esitellään erilaisia indikaattoreita sekä monitorointityökaluja, joita ei tässä tutkimuksessa kuitenkaan aseteta käytäntöön. Näiden indikaattoreiden ja monitorointityökalujen käyttöönotto vaatisi tapaustutkimuksen kohdeorganisaatiosta, jolloin näitä työkaluja voitaisiin käyttää organisaation verkoissa. Kyseiset työkalut on hyvä kuitenkin tuoda tutkimuksessa esiin, sillä tutkimusta sovellettaessa tapaustutkimukseen tai käytännön toimintaan, on hyvä tuntea nämä työkalut, jotta kyseisiä toimintoja voidaan tehdä. Tämän tutkimuksen tutkimusosuuden kaikki analyysi- ja monitorointityökalut löytyvät Cyber Intelligence Housen Cyber Exposure Platformilta. Tutkimuksessa on pyritty esittelemään eri työkaluja ja ratkaisuja sitä ajatellen, että tutkimusta vastaavan tapaustutkimuksen pystyisi tekemään ilman CEP alustaa. Kappaleessa 7 esitellään myös OSINT ja Web Crawlereita, joita ei sellaisenaan oteta käyttöön tutkimuksessa. Tutkimuksessa OSINT ja Web Crawlereiden työn hoitaa CIH CEP -alusta. Tässäkin tarkoituksena on esitellä työkalut, joita tulisi käyttää, mikäli CIH CEP -alustan kaltaista työkalua ei olisi käytettävissä.

Tämän tutkimuksen ajatuksena oli perehtyä ennakoivaan kybertilannekuvaan yleisellä ja helposti sovellettavalla tavalla. Tutkimuksen lähtökohtana ei ollut luoda ”case esimerkki” -tyylistä tapaa toteuttaa ennakoivaa kybertilannekuvaa, vaan kertoa yleisellä tasolla, miten sitä voisi toteuttaa. Tämä toi tutkimukseen myös haasteita. Pimeän verkon syötteestä ei voitu suoraan hakea esimerkiksi organisaation verkkorakenteellisia haavoittuvuuksia, pimeän verkon keskusteluja organisaatioon viittaavilla tunnisteilla, organisaation sektoria tai toimialaa uhkaavia tekijöitä, taikka organisaation domain nimiä tai sähköpostiosoitteiden esiintyvyyttä tietomurtojen tai -vuotojen yhteydessä. Nämä edellä mainitut toimenpiteet olisivat luoneet konkreettisia malleja siitä, miten voidaan kohdistaa organisaation resursseja ennakoivan kybertilannekuvan saralla. Ensisijainen syy sille, miksi tällaista esimerkkiorganisaatiota ei otettu tutkimukseen mukaan oli se, että tällaisessa tilanteessa olisi tullut esimerkiksi organisaation henkilötietojen käsittelyoikeudet ja niistä sopimusten tekemiset kyseeseen. Tutkimusta suunnitellessa koettiin helpommaksi ja toteutuskelvollisemmaksi tehdä tutkimus yleisellä tasolla, ilman esimerkkiorganisaatiota.

Jatkotutkimusideana olisi samankaltainen tutkimus kohdeorganisaation perspektiivistä, eli case-tutkimuksena. Tällöin saataisiin hyvin konkreettiset raamit haettavalle tiedolle, sekä suojattavalle toiminnalle omassa toimintaympäristössään. Lisäksi tulokset olisivat helpommin nähtävissä ja arvioitavissa, kun saataisiin oikeasta toiminnasta esimerkkituloksia ilman yleistystä.

LÄHTEET

Albrecht, J., Balaam, K. (19.07.2023). Why Should You Care About APTs and Nation-State Attacks ? https://www.lookout.com/blog/mobile-apt-cyber-espionage

AlKhatib, B. & Basheer, R. (2019). Crawling the Dark Web: A conceptual Perspective, Challenges and Implementation. Journal of Digital Information Management.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851-1877

Baker, K. (23.03.2023). What is Threat Intelligence ? Crowdstrike : Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Basheer, R. & AlKhatib, B. (2021). Threats from the Dark: A Review over Dark Web investigation Research for Cyber Threat Intelligence

Benjamin, V., Valacich, J. S, & Chen, H. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. MIS Quarterly, 43, 1–22.

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 7(1).

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. International Research Journal of Engineering and Technology

Block, L. (2023) The long history of OSINT.

Bromander, S., Swimmer, M., Muller, L. P., Jøsang, A., Skjøtskift, G., Eian, M. & Borg, F. (2022). Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange. Digital Threats: Research and Practice, Vol. 3, No. 1, Article 6.

Brown, S. (ei pvm). Indicator of Attack (IOA) Seurity. https://www.strongdm.com/what-is/indicator-of-attack-ioa-security

Cambridge University (ei pvm). Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/hacktivism

Chainanalysis (07.02.2024). Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. Ransomware 2024. https://www.chainalysis.com/blog/ransomware-2024/

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security.

Crowdstrike (05.10.2022) Indicators of Compromise (IOC) Security. Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

Crowdstrike (30.01.2023). Ransomware as a Service (RaaS) Explained How It Works & Examples. Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Crowdstrike (28.02.2023). Threat actor. Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/threat-actor/

Cyberark (ei pvm.). What is User Behavior Analytics? https://www.cyberark.com/what-is/user-behavior-analytics/

Cybersecurity & Infrastructure Security Agency, CISA (ei pvm). Nation-State Cyber Actors. Cyber Threats and Advisories. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Cyber Intelligence House (ei pvm). Cyber Exposure Platform.

Div, L. (2017). Cyber crime as a service forces changes in information security. Network World (Online).

Elo, S., Kajula, O., Tohmola, A. & Kääriäinen, M. 2022. Laadullisen sisällönanalyysin vaiheet ja eteneminen.

European Union Agency For Cybersecurity, Enisa (ei pvm). Information Sharin and Analysis Centers (ISACs) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Fairman, D. (2021). The Illegal Economy and Crime as a Service. ITNow, 63(3), 14-15.

Federal Bureau of Investigation, FBI (ei pvm.). The Cyber Threat. What We Investigate. https://www.fbi.gov/investigate/cyber

Finklea, K. (2017). Dark Web. Congressional Research Service.

Hatta, M. (2020). Deep web, dark web, dark net: A taxonomy of "hidden" Internet. Annals of Business Administrative Science, 19(6), 277–292.

Horneman, A. (09.09.2019). Situational Awareness for Cybersecurity: An Introduction. https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/

Horstmann, N. D. (2022). The Power to Selectively Reveal Oneself: Privacy Protection among Hacker-activists. Ethnos, 87(2), 257-274.

Huoltovarmuusorganisaatio (2022). Turvallisen Digitalisaation Työkalupakki Yritysjohtajille. Digipooli #Strategia22-projekti.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

International Business Machines Corporation, IBM (ei pvm). What is a threat actor? https://www.ibm.com/topics/threat-actor

Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J. &Kompatsiaris, I. (2016). OSINT and the Dark Web. Springer International Publishing.

Khera, V. (02.10.2020). The Web Layers: Introduction to Surface, Deep and Darknet. https://cyberprotection-magazine.com/the-web-layers-introduction-to-surface-deep-and-darknet

Kissel, R. (03.07.2019) Glossary of Key Information Security Terms. NISTIR 7298 Revision 2. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Lehto, M. (2022). APT Cyber-attack Modelling: Building a General Model. International Conference on Cyber Warfare and Security, 17(1), 121–129.

Leppänen, J. (2022). Sosiaalinen hakkerointi APT-kyberhyökkäyksissä. Poliisiammattikorkeakoulu päättötyö.

Lowenthal, M. M. (2020). Intelligence: From secrets to policy (8. p.). Sage Publishing.

MacDowell, D. (2001). Strategic intelligence: A handbook for practitioners, managers and users. Istana Enterprises.

Mandiant (ei pvm.). Advanced Persistent Threats (APTs). https://www.mandiant.com/resources/insights/apt-groups

Martelius, J. (2020). Tiedustelutieto kansallisen turvallisuuden päätöksenteossa. Suomalaisen tiedustelukulttuurin jäljillä.

Matilainen, J. (2020). Using Cyber Threat Intelligence as a Part of Organisational Cybersecurity. Pro gradu Jyväskylän yliopisto.

Mavroeidis, V., Bromander, S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standard, and Ontologies within Cyber Threat Intelligence. 2017 European Intelligence and Security Information Conference.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & security, 92, 101762-9.

Microsoft (2023). Microsoft Digital Defence Report 2023. Microsoft Threat Intelligence.

Microsoft (ei pvm). What are indicators of compromise (IOC)? Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc

Poliisi (ei pvm.). Kyberrikokset. https://poliisi.fi/kyberrikokset

Pudas, M. (2023). Tapaustutkimus kolmen APT-hyökkäyksen mahdollisten indikaattoreiden havaitsemisesta kyberuhkatiedustelun avulla. Pro gradu Jyväskylän yliopisto.

Renaud, K., Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Procress and People. Vol 1 No. 1, 2021, pp 24-46.

Ruotsalainen, M. (2021). Rikollinen kaupankäynti TOR-verkon suomenkielisissä piilopalveluissa. Pro gradu Jyväskylän yliopisto.

Samtani, S., Abate, M., Benjamin, V., Weifeng, L. (2019). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance.

Samtani, S., Li, W., Benjamin, V., Chen, H. (2021). Informing Cyber Threat Intelligence through Dark Web Situational Awareness: The AZSecure Hacker Assets Portal. Digital Threats: Research and Practice, Vol. 2, No. 4, Article 27.

Schneier, B. (2000). Software complexity and security. IEEE Security & Privacy, vol. 10, no. 2, pp. 104-104

Schneier, B. (2012). How Changing Technology Affects Security.

Shakarian, P. (2017). The Enemy Has a Voice: Understanding Threats to Inform Smart Investment in Cyber Defense. Policy File.

Shashanka, M., Shen, M. -Y. & Wang, J. (2016). User and entity behavior analytics for enterprise security.

Sisäministeriö, (ei pvm). Kyberturvallisuus osana kansallista turvallisuutta. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Sisäministeriö (ei pvm.). Kyberrikollisuus ylittää rajat tietoverkoissa. Kyberrikollisuus. https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö (2017). Siviilitiedustelun ja suojelupoliisin ohjauksen kehittäminen sisäministeriön hallinnonalalla: Työryhmän raportti. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80032/Siviilitiedustelun%20ja%20suojelupoliisin%20ohjaus_NETTI.pdf

Stanford University (ei pvm). Hacktivism is Hacking. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

Stenhammar, M. (2022). ”Arvon Nyymit…” Tutkimus syvän ja pimeän verkon keskusteluista ja keskustelijoista. Pro gradu Jyväskylän yliopisto.

Suojelupoliisi (ei pvm.). APT on kybervakoojan työkalupakki. APT-operaatiot. https://supo.fi/apt-operaatiot

Suojelupoliisi (18.3.2021). Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi. https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi

TechTarget (2021). Hacktivism. Definition. https://www.techtarget.com/searchsecurity/definition/hacktivism

Tounsi & Rais (2018). A survey on technical threat intelligene in the age of sophisticated cyber attacks.

Trend Micro (ei pvm). Cybercriminals. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

Trend Micro (ei pvm). Indicators of compromise. https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise

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

Unit 42 (23.02.2024). Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns. Paloalto Networks. https://unit42.paloaltonetworks.com/i-soon-data-leaks/

U.S Department of Justice (25.03.2024). Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians. Press Release. https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

Valtiovarainministeriö (2023). Valtionavustustoiminnan sanasto, 2. laajennettu laitos. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164836/VM_2023_33.pdf

Varma, C. S. (18.04.2018). CISO Guide: Surface Web, Deep Web and Dark Web – Are they different? https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

Vienažindyté, I. (13.06.2021). Syväverkko: mikä on deep web ja minkälaisia vaaroja siihen liittyy? Anonymiteetti. https://nordvpn.com/fi/blog/mika-on-deep-web/