Tampereen ammattikorkeakoulu

APT-operaatioiden luomat kyber-turvallisuusuhat keskisuurille ja suurille suomalaisorganisaatioille

Joonas Kiuru

OPINNÄYTETYÖ
Joulukuu 2024

Tietojenkäsittelyn tutkinto-ohjelma
Ohjelmistotuotanto

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma
Ohjelmistotuotanto

KIURU, JOONAS:
APT-operaatioiden luomat kyberturvallisuusuhat keskisuurille ja suurille suomalaisorganisaatioille

Opinnäytetyö 60 sivua, joista liitteitä 2 sivua
Joulukuu 2024

Tämän opinnäytetyön tarkoituksena on luoda ajantasainen katsaus APT-operaatioiden luomista uhista suurille ja keskisuurille suomalaisyrityksille sekä -organisaatioille. Toimeksiantajana toimi suomalainen tietoturvapalveluja tarjoava yritys.

Termi APT tulee englanninkielisistä sanoista *Advanced Persistent Threat,* ja käytännössä sillä tarkoitetaan edistynyttä, pitkäkestoista kyberuhkaa. Nämä kyberuhat toteutetaan operaatioina, jotka käsittävät allensa teollisuusvakoilua, sotilastiedustelua, ydinvoimaohjelmien vakoilua sekä paljon muutakin rikollistoimintaa, kuten pankkien ja kryptopörssien ryöstämistä, palvelunestohyökkäyksiä sekä lunnashaittaohjelmahyökkäyksiä. APT-operaatioita suorittavat tietyt erikoistuneet, yleensä valtiollisia sidoksia omaavat teknisesti taitavat ryhmät.

APT-operaatioista löytyy kohtalaisesti eri tietoturvayritysten, tutkimuslaitosten ja ajatushautomoiden raportteja sekä tutkimuksia. Tämän opinnäytetyön keskeisenä tavoitteena on koostaa yhteen suomalaisten keskisuurien ja suurien organisaatioiden kannalta olennaisimpia hyökkäystekniikoita, operaatioita sekä niitä toteuttavia ryhmiä.

Opinnäytetyötä varten haastateltiin kahta kyberturvallisuusalan ammattilaista, jotka pystyivät työnkuvansa ja/tai työkokemuksensa kautta tarjoamaan ajankohtaista tietoa suomalaisia organisaatioita uhkaavista tekijöistä ja tekniikoista. Haastatteluiden sekä muun aineiston pohjalta tehtiin johtopäätöksiä suomalaisia organisaatioita potentiaalisesti eniten uhkaavista APT-operaatioista.

Tutkimuksen tulokset tukevat aiempia havaintoja siitä, että suomalaisten organisaatioiden kannalta suurinta uhkaa tuottavat venäläiset, kiinalaiset ja pohjoiskorealaiset APT-operaatiot, kuten APT28, APT31 ja APT38. Nämä operaatiot osoittavat suurta kiinnostusta eurooppalaisia ja suomalaisia kohteita kohtaan, ja tästä syystä suomalaisten organisaatioiden tulisi olla hyvin perillä näiden operaatioiden toiminnasta. Koska APT-operaatioiden todellinen lukumäärä ei kuitenkaan ole täysin vedenpitävästi todennettavissa, on mahdotonta sanoa täydellä varmuudella, mitkä operaatiot uhkaavat konkreettisesti eniten suomalaisia organisaatioita.

Asiasanat: kyberrikollisuus, kyberturvallisuus, APT

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Software Production

KIURU, JOONAS:
Cybersecurity Threats Posed by APT Operations to Medium-Sized and Large Finnish Organisations

Bachelor's thesis 60 pages, appendices 2 pages
December 2024

The aim of this thesis is to provide insight into APT operations that pose the most notable risk to mid-sized and large Finnish companies and organisations. APT is an abbreviation for *Advanced Persistent Threat*. This term was created to describe the methodology and qualities that sophisticated, targeted cyber threats possess.

APT operations cover many kinds of activities ranging from military, industrial, energy and nuclear technology espionage to ransomware attacks and Distributed Denial-of-Service (DDoS) disruptions. APT operations are conducted by APT groups. These groups of hackers are highly skilled, well resourced, usually nation-state funded.

For this thesis, numerous articles and research papers from think tanks, cybersecurity companies, and research institutes were reviewed. Additionally, two cybersecurity professionals were interviewed, and they provided insight into the topic based on their experience.

Based on the research conducted for the thesis, key findings were formulated. These findings support previous observations that the most threatening APT operations for Finnish organisations are of Russian, Chinese and North Korean origin. These operations are conducted by groups such as APT28, APT31 and APT38. However, due to the hidden and sophisticated nature of APT operations, it is virtually impossible to say with absolute certainty which groups pose the most significant risk to Finnish companies and organisations.

Key words: cybercrime, cybersecurity, APT

SISÄLLYS

ERITYISSANASTO

APT	Advanced Persistent Threat, edistynyt pitkäkestoinen kyberuhka
DDoS	Distributed Denial of Service, hajautettu palvelunesto-hyökkäys
Ransomware	Lunnashaittaohjelma, haittaohjelma, joka salaa tietokoneen tiedot, ja purkaa salauksen lunnaita vastaan
RAT	Remote Access Trojan, troijalaisohjelma, haittaohjelma joka esiintyy jonain toisena luotettavana ohjelmana
Spearphishing	Kohdistettu tietojenkalasteluhyökkäys jotain strategisesti merkittävää henkilöä, positiota, tai ryhmää vastaan
TTP	Tactics, Techniques & Procedures, APT-operaatioiden käyttämät taktiikat, tekniikat sekä menetelmät

1 JOHDANTO

Yhteiskunnan digitalisoituminen on muuttanut maailmaa pysyvästi. Palvelut, kaupat, tapahtumat sekä sosiaalinen kanssakäyminen ovat siirtyneet verkkoon. Pankkiasioiden hoituminen hoituu muutamalla kätevällä sormennäpäytyksellä konttoriasioimisen sijasta, ja lähes kaikki tieto mitä ihminen voi päivittäisessä elämässään tarvita löytyy verkosta artikkelien, videoiden tai ääni- ja e-kirjojen muodossa.

Digitalisaatio tuo kuitenkin mukanaan muitakin puolia kuin vapaan tiedonvälityksen tai jokapäiväisten arkirutiinien helpottumisen. Rikolliset löytävät uuden teknologian siinä missä tavalliset kansalaisetkin ja hyödyntävät sitä parhaansa mukaan rikoshyödyn saamiseen. Kybermaailmaan sijoittuva rikollisuus aiheuttaa monenlaista päänvaivaa niin yksittäisille henkilöille, yrityksille kuin julkisen sektorin organisaatioille. Tästä eteenpäin termistön selkeyttämiseksi sekä toiston minimoimiseksi suomalaisia yrityksiä ja julkisen sektorin organisaatioita kuvataan yhteisellä termillä ”organisaatiot”.

Yksittäisten ihmisten kannalta suurimpia uhkia ovat nykymaailmassa erilaiset huijaukset. Näihin kuuluvat romanssihuijaukset, työhuijaukset sekä monet muunlaiset, joskus todella mielikuvituksellisetkin, petokset. Yleensä näissä rikoksissa tavoitellaan lähinnä taloudellista hyötyä, sillä hyvin harvoin yksittäinen siviili pystyy tarjoamaan muuta konkreettista hyötyä rikolliselle kuin raha.

Organisaatioiden kohtaamat uhat ovat kuitenkin paljon moninaisempia, ja kyberrikollisuuden myötä organisaatiot kohtaavat täysin uudenlaisia vaaroja, joihin ei ole ennen tarvinnut varautua. Erilaiset kyberhyökkäykset isoja organisaatioita, kuten pankkeja, vastaan ovat jo niin arkipäiväisiä, että niistä saa lukea uutisista lähes päivittäin.

Tavanomaisten yksittäisten kyberhyökkäysten lisäksi organisaatioiden tulisi varautua myös laajempaan uhkaan; APT-operaatioihin. APT eli *Advanced Persistent Threat* -operaatiot ovat yleensä valtioiden sponsoroimia kohdistettuja, pitkäkestoisia sekä edistyksellisiä kyberoperaatioita, joissa tavoitteena on usein saada

kriittistä informaatiota joko sotilas-, teollisuus-, energia- tai ydinteknologian alueelta edistääkseen hyökkääjäryhmän sponsorivaltion (tai muun tahon) etuja ja kyvykkyyksiä. APT-operaatiot voivat myös tavoitella taloudellista hyötyä, misinformaation levittämistä tai yhteiskunnallisen luottamuksen murentamista.

Tämä tutkimus käsittelee suomalaisten organisaatioiden kannalta ajankohtaisimpia kyberuhkia APT-operaatioiden näkökulmasta. Tutkimuksessä selvitettiin haastattelujen ja muun aineiston avulla, minkälaisia uhkia APT-operaatiot tuottavat suomalaisten organisaatioiden kannalta ja mitkä valtiot ovat niistä pääosin vastuussa.

2 TUTKIMUSASETELMA

2.1 Tutkimuksen merkitys ja tarpeellisuus

Erinäiset geopoliittiset kriisit, kuten sodat Ukrainassa ja Gazassa, ovat vaikuttaneet globaaliin kyberturvallisuusilmapiiriin ratkaisevasti. Kybermaailmassa tilannekuva muuttuu joka päivä, ja mitä ajankohtaisempia tutkimuksia on saatavilla, sitä merkityksellisempää tieto on. Kyberhyökkääjät uusivat metodologiaansa jatkuvasti, ja kyberpuolustajien on äärimmäisen tärkeää sisäistää ajantasainen tieto.

Tutkimuksen tarkoituksena on tuottaa hyödyllistä ja käyttökelpoista tietoa keskisuuria ja suuria suomalaisia organisaatioita koskevista ajankohtaisista APT-operaatioiden uhista. APT- operaatiot ovat osa useiden valtioiden harjoittamaa tiedustelutoimintaa, ja monet suuret organisaatiot pitävät hallussaan tietoa, jota vihamieliset valtiot voivat pitää arvokkaana teollisten, sotilaallisten tai teknologisten kyvykkyyksiensä parantamiseen. Myös erinäiset ei-valtiolliset toimijat, kuten haktivistiryhmät tai kybermaailman talousrikolliset, edustavat korkeaa uhkaa organisaatioille. Ajankohtainen tutkimus APT- operaatioista on erittäin tärkeää selvittämään minkälaisia hyökkäystekniikoita ja taktiikoita APT-operaatiot käyttävät, jotta niitä vastaan voidaan puolustautua.

2.2 Tutkimuskysymykset

Hyvin asetellut tutkimuskysymykset auttavat laadukkaan tutkimuksen suorittamisessa. Jos tutkimuskysymykset ovat huonosti tai muutoin huolimattomasti rakennettuja, ne voivat vähentää tutkimuksen arvoa ja hyödyllisyyttä. Tutkimuskysymyksiä on yhteensä 5, joista pääkysymyksiä on 2, ja alakysymyksiä 3.

Tutkimuksen pääkysymykset olivat seuraavat:

- Mitä kyberturvallisuusuhkia APT-operaatiot luovat suomalaisille keskisuurille ja suurille organisaatioille?

- Mitkä valtiot/ryhmät ovat kaikista vaarallisimpia suomalaisten organisaatioiden kannalta?

Tutkimuksen pääkysymyksiä tukemaan käytettiin seuraavia alakysymyksiä:

- Mitä taktiikoita, tekniikoita ja menetelmiä kyberhyökkääjät käyttävät?
- Ovatko suomalaisorganisaatiot varautuneet APT-operaatioihin?
- Minkälaiset organisaatiot ovat houkuttelevia kohteita APT-operaatioille?

2.3 Tutkimuksen rajaus

Tutkimuksen yksi keskeisimmistä haasteista oli tutkimuksen rajaus. Koska APT-operaatioita on huomattava määrä, joista kaikki tuskin ovat edes paljastuneet, täytyi tutkimus rajata niihin APT-operaatioihin, jotka olivat tutkimuksen kannalta keskeisimpiä.

Koska tutkimuksen tarkoituksena oli saada ajantasaista tietoa siitä, mitkä APT-operaatiot kohdistavat suurinta uhkaa suomalaisille organisaatioille, olivat tutkimuksen kannalta keskeisimmät APT-operaatiot niitä, jotka ovat tunnetusti vaikuttaneet eurooppalaisiin organisaatioihin. Eurooppalaisena valtiona Suomi on todennäköisesti samojen APT-operaatioiden kohde, jotka koskevat muitakin eurooppalaisia valtioita.

Tutkimusta täytyi myös rajata siltä osin, kuinka paljon teknisiä yksityiskohtia käsitellään. Koska tutkimuksen tarkoitus on antaa katsaus useampaan APT-operaatioon, ei teknisiä yksityiskohtia käsitellä kattavammin, kuin mikä antaa yleisluontoisen kuvan APT-operaation tai hyökkäyksen mekaniikasta.

2.4 Tutkimuksen rakenne

Tutkimus on rakennettu hyödyntäen IMRD (Introduction, Methods, Results and Discussion) -mallia. Mallin käyttö selkeyttää tutkimuksen rakennetta ja vakiinnuttaa tutkimuksen rakenteen yleisesti tunnettuun standardiin. IMRD-rakenteen an-

siosta lukijan on mahdollista löytää haluamansa tieto lukematta läpi koko tutkimusta. Tutkimusraportin ensimmäinen pääluku on johdanto, ja toinen pääluku käsittelee tutkimusasetelmaa.

Kolmas pääluku käy läpi tutkimuksen kannalta keskeisiä käsitteitä. Nämä käsitteet sisältävät APT-operaatioiden tyypillisimpiä taktiikoita, tekniikoita ja menetelmiä sekä tutkimukseen valikoitujen APT-operaatioita suorittavien APT-ryhmien taustoituksen. Kolmas pääluku sisältää myös katsauksen neljän Euroopan kannalta relevantin maan APT-toimintaan.

Neljäs pääluku tutkii Eurooppaan kohdistuneita APT-operaatioita. Esimerkeiksi valikoitui operaatioita, jotka ovat tutkimuskysymyksien kannalta ajankohtaisia kohdemaansa puolesta.

Viidennessä pääluvussa käydään läpi tutkimusta varten haastateltujen asiantuntijoiden lausuntoja. Haastattelut suoritettiin vapaamuotoisina teemahaastatteluina, ja haastateltavia asiantuntijoita oli kaksi.

Kuudes pääluku koostuu tutkimuksen johtopäätöksistä sekä tutkijan pohdinnasta. Pohdinta vetää tutkimuksen yhteen, sekä tarjoaa tutkijan henkilökohtaisen näkemyksen APT-operaatioista sekä suomalaisia organisaatioita uhkaavista kybervaaroista.

2.5 Tutkimuksen kritiikki

Koska tutkimusaineistoa tuli rajata ainoastaan tutkimuksen kannalta olennaisiin APT-operaatioihin, merkittävä osa APT-operaatioista ja ryhmistä rajautui tutkimuksen ulkopuolelle, pääosin ne, jotka suuntautuivat Euroopan maiden ulkopuolelle. Rajaus tehtiin saatavilla olevan aineiston ja haastatteluiden perusteella. Koska aineiston rajaus tehtiin tutkimuksen tekijän subjektiivisella arvioinnilla, on mahdollista, että toiset vastaavat tutkimukset aiheesta päätyisivät valitsemaan tutkimuksen kohteiksi eri APT-operaatioita.

Rajaus teknisistä yksityiskohdista tehtiin myös tutkijan subjektiivisen näkemyksen perusteella. Osalle tutkimuksen lukijoista tekniset yksityiskohdat voivat tuntua riittämättömiltä, kun taas toisille ne voivat ohjata huomion epäolennaisiin seikkoihin. Tutkimuksen tarkoituksena on kuitenkin tarjota osittain yleisluontoista katsausta tarkempaa tietoa APT-operaatioista, joten tiettyjen teknisten yksityiskohtien sisällyttäminen oli tarkoituksenmukaista.

2.6 Tutkimuksen aineisto

Tutkimuksen lähdeaineistona käytettiin kyberturvallisuusyritysten, ajatushautomoiden sekä tutkintatiimien raportteja APT-operaatioista, sekä APT-operaatioihin liittyvää kirjallisuutta. Myös haastattelut olivat olennainen osa aineistoa.

Haastavaksi tutkimusaiheen tutkimisen teki erityisesti se, että aineisto ei ollut kovinkaan usein erityisen kattavaa. APT-operaatioista kerrotaan tyypillisesti julkisuuteen sangen niukasti. Tämä on yleistä etenkin, jos operaatioiden kohteena on ollut jokin valtiollinen organisaatio. Tällöin tiedon niukkuus on helppo yhdistää kansallisen turvallisuuden suojelemiseen. Yksityiset organisaatiotkaan eivät kuitenkaan aina kerro julkisuuteen sen enempää yksityiskohtia, ehkäpä mainehaitan tai yritysturvallisuuden vuoksi.

2.7 Aikaisempi tutkimus

Valtiolliset tahot, tietoturvayritykset, tutkimuslaitokset sekä erilaiset ajatushautomot tutkivat jatkuvasti APT-operaatioita, niiden indikaattoreita sekä yhteyksiä niitä toteuttaviin valtioihin. APT-operaatioista löytyy useita aikaisempia tutkimuksia muun muassa verkossa julkaistavien raporttien muodossa.

Aina tuoretta tietoa ei kuitenkaan ole saatavilla, ja osa tutkimuksista on useita vuosia vanhoja. Aiheesta on kirjoitettu myös jonkin verran kirjallisuutta. Usein kuitenkin raportteja, uutisia ja muita internetissä esiintyviä kirjoituksia yhdistää se, että ne tarjoavat käytännössä samaa tietoa, ja syventävää tietoa on vaikea löytää.

3 APT

3.1 Yleiskatsaus APT-operaatioihin

Termi *APT* kehitettiin alun perin koodinimeksi Kiinaan linkittyviin kybervakoiluoperaatioihin yhdysvaltalaisia sotilasorganisaatioita vastaan. Termi on sittemmin kehittynyt kuvaamaan muitakin ympäri maailmaa tapahtuvia kehittyneitä kybervakoilu- ja rikosoperaatioita, joissa pyritään saada haltuun kriittistä dataa tai muutoin hyväksikäyttää uhrin järjestelmiä. APT-operaatiot ovat teknisesti hyvin edistyneitä, ja pystyvät ohittamaan monet perinteiset kybersuojausmekanismit, kuten antivirusohjelmistot. APT-operaatiot ovat tarkasti kohdistettuja ja datalähtöisiä, ja ne pyrkivät luomaan uhriorganisaatioon pysyvää jalansijaa tiedon vuotamiseen. (Cole 2012.)

Jokainen APT-lyhenteen sanoista merkitsee tärkeää, APT-operaatiolle ominaista piirrettä. APT-termiä käytetään maailmanlaajuisesti, eikä ilmaukselle ole vakiintunutta suomenkielistä vastinparia.

Advanced
Suomeksi käännettynä *advanced* tarkoittaa kehittynyttä tai edistyksellistä. Tällä viitataan siihen, että usein APT-operaatiot hyödyntävät viimeisintä teknologiaa, havaitsemattomia nollapäivähaavoittuvuuksia sekä mittavia resursseja hyökkäystensä toteuttamisessa.

Persistent
Persistent on suomeksi käännettynä sitkeä tai jatkuva. Tämä sana kuvastaa sitä, että vakoiluoperaatiot ovat usein pitkäkestoisia, ja operaatioihin liittyvät haittaohjelmat ja takaportit piileksivät uhriorganisaation järjestelmissä pitkään huomaamatta.

Threat
Threat tarkoittaa suomeksi uhkaa. Uhka viestittää, että APT-operaation onnistumisella on merkittäviä negatiivisia seurauksia kohteeksi joutuneen organisaation

kannalta, kuten tärkeän informaation valuminen vihamielisen ulkomaisen organisaation tai valtion käsiin.

APT-operaatioita vastaan puolustautumisen tekee hankalaksi tilanteen asymmetrisyys, joka koskee käytännössä jokaista muutakin kyberhyökkäystä. Hyökkäyksessä onnistuakseen hyökkääjän tarvitsee löytää vain yksi haavoittuvuus, jota hyödyntää, kun taas puolustavan organisaation täytyy tilkitä kaikki mahdolliset haavoittuvuudet minimoidakseen riskit. Kuitenkaan organisaatiot eivät usein ole tietoisia kaikista haavoittuvuuksista, mikä antaa edun epäilemättä hyökkääjän puolelle. (Cole 2012.)

APT-operaatioiden seuraamisen tekee haastavaksi se, että useat ajatushautomot, tietoturvayritykset ja muut tahot seuraavat omia nimeämiskäytäntöjään ryhmien suhteen, mikä voi luoda aika ajoin sekavan kuvan yksittäisten ryhmien toiminnasta. Yksittäisillä ryhmillä voi paikoittain olla jopa kymmenittäin eri nimiä. Taulukoissa 1, 2 ja 3 kuvataan CrowdStriken, Microsoftin sekä Palo Alto Networksin nimeämiskäytäntöjä.

TAULUKKO 1. CrowdStriken nimeämiskäytännöt (CrowdStrike n.d.-a).

Sana	**Selitys**
Panda	Kiinalaiset APT-ryhmät
Bear	Venäläiset APT-ryhmät
Kitten	Iranilaiset APT-ryhmät
Chollima	Pohjoiskorealaiset APT-ryhmät
Jackal	Haktivistiryhmät
Spider	Muut verkkorikollisryhmät

TAULUKKO 2. Microsoftin nimeämiskäytännöt (Lambert 2023).

Sana	**Selitys**
Typhoon	Kiinalaiset APT-ryhmät
Blizzard	Venäläiset APT-ryhmät
Sandstorm	Iranilaiset APT-ryhmät
Sleet	Pohjoiskorealaiset APT-ryhmät
Tempest	Taloudellisesti motivoituneet ryhmät
Storm	Kehittyvät ryhmät
Tsunami	Yksityisen sektorin ryhmät
Flood	Informaatio-operaatiot

TAULUKKO 3. Palo Alto Networks:in nimeämiskäytännöt (Olson 2022).

Sana	**Selitys**
Taurus	Kiinalaiset APT-ryhmät
Ursa	Venäläiset APT-ryhmät
Serpens	Iranilaiset APT-ryhmät
Pisces	Pohjoiskorealaiset APT-ryhmät
Draco	Pakistanilaiset APT-ryhmät
Gemini	Intialaiset APT-ryhmät
Lynx	Valkovenäläiset APT-ryhmät
Libra	Verkkorikollisryhmät yleisesti
Orion	BEC-ryhmät *(Business Email Compromise)*
Scorpius	Kiristyshaittaohjelmia käyttävät ryhmät

Virgo	Haktivistiryhmät

Kuten taulukoista huomaa, vaikka kategorioista löytyy paljon samankaltaisuuksia, on niissä merkittäviäkin eroja etenkin muiden kuin valtiollisten APT-ryhmien suhteen. Hienojakoisimmin kategoriat listaa Palo Alto Networks, joka on jaotellut rikollisryhmiä niiden käyttämien tekniikoiden mukaan. Muista poiketen Palo Alto on myös ottanut nimeämiskäytäntöihinsä mukaan valkovenäläiset, intialaiset ja pakistanilaiset ryhmät.

3.2 APT-operaatioiden tyypillisiä taktiikoita, tekniikoita ja menetelmiä

Kyberturvallisuudessa käytetään yleensä termiä *Tactics, Techniques and Procedures* (TTP, eli suomeksi *taktiikat, tekniikat ja menetelmät)* kuvaamaan tietyn kyberhyökkääjän käyttämää toimintatapojen viitekehystä hyökkäysten toteuttamiseksi (Raza 2023). Tässä tutkimuksessa käytetään edellä mainittua, yleisesti tunnettua englanninkielistä lyhennettä TTP selkeyden vuoksi.

Avoimen lähteen tiedustelu, eli *Open Source Intelligence* tai OSINT, on yksi tärkeimmistä työkaluista TTP-mallien seuraamiseen. Tietoa APT-operaatioista ja niiden toteutustavoista etsitään julkisesti saatavilla olevista lähteistä kuten artikkeleista ja raporteista. Kuitenkin OSINTia hyödyntäessä on hyvä muistaa, että myös hyökkääjät voivat lukea samaa materiaalia ja näin rakentaa hyökkäyksiä, jotka ohittavat pelkästään julkiseen tietoon perustuvat suojausmenetelmät. Tästä syystä organisaatioiden tulisi hyödyntää myös muita työkaluja, kuten MITRE ATT&CK-viitekehystä, joka auttaa tunnistamaan kyberhyökkäysten askelmerkkejä. (Jamil, Kiah, Mat & Yusoff 2024.)

Seuraamalla tunnettuja TTP-malleja organisaatio pystyy varautumaan yleisimpiä kyberuhkia vastaan sekä tunnistamaan mahdollisen hyökkääjän. TTP kuvastaa aina yksilöllisen kyberuhan käyttäytymismallia, ja yhden TTP:n tunteminen ei suojaa kaikilta APT-operaatioilta. TTP koostuu kolmesta eri komponentista, jotka

eroavat toisistaan laajuudessa. TTP:n voi ajatella kolmikerroksisena pyramidimaisena rakenteena, jossa alin kerros kuvastaa taktiikoita, keskimmäinen tekniikoita ja ylin kerros menetelmiä.

Taktiikat luovat pohjapiirroksen hyökkäyksen toteutukselle: taktiikka tarkoittaa toimintaa, jonka tarkoituksena on saavuttaa tietty lopputulos (Cambridge Dictionary n.d.). Esimerkkinä taktiikasta voisi olla esimerkiksi uhriorganisaation sivuston käyttäjätietojen varastaminen. (Exabeam n.d.)

Tekniikat kuvaavat tarkemmin toimenpiteitä, joita taktiikan toteuttaminen vaatii. Esimerkiksi käyttäjätietoja varastaakseen hyökkääjä voisi hyödyntää *XSS*- eli *Cross Site Scripting* -hyökkäystekniikkaa. (Exabeam n.d.)

Menetelmät kuvaavat tarkkoja yksilöllisiä prosesseja, joita hyökkääjän täytyy suorittaa onnistuakseen hyökkäyksessä. Menetelmät voisivat esimerkiksi kuvata, mitä tarkkoja funktioita hyökkääjä tarvitsee toteuttaakseen XSS-hyökkäyksen. (Exabeam n.d.)

Seuraavissa alaluvuissa käsitellään erilaisia APT-operaatioiden suosimia tunnettuja hyökkäystaktiikoita. Hyökkäystaktiikat eivät kuitenkaan rajoitu vain alla mainittuihin, vaan hyökkääjät vaihtelevat lukuisten eri keinojen välillä etsiessään pääsyä uhrin järjestelmiin.

3.2.1 DDoS – hajautettu palvelunestohyökkäys

Distributed Denial-of-Service eli DDoS, tai suomeksi hajautettu palvelunestohyökkäys, on kyberhyökkäys, jossa hyökkääjä yrittää ylikuormittaa sivuston palvelimet keinotekoisella liikenteellä ja näin häiritä sivuston toimintaa (Microsoft n.d.-a). DDoS-hyökkäysten uhreja voivat olla kaikenkokoiset organisaatiot toimialasta riippumatta. Hajautetulla tarkoitetaan tässä yhteydessä sitä, että haitallinen, kuormittava liikenne ohjataan palveluun usealta eri laitteelta yhden sijaan.

Hajautetut palvelunestohyökkäykset ovat tärkeä osa APT-ryhmien työkalupakkeja niiden helpon teknisen toteutettavuuden ja nopean sekä laajan vaikutuksen

vuoksi. Kuitenkin isoimmilla yrityksillä ja organisaatioilla on kykyä ja resursseja implementoida puolustusmekanismeja näihin hyökkäyksiin.

Onnistuessaan DDoS-hyökkäys saa aikaan monenlaista vahinkoa kohteeksi joutuneessa organisaatiossa. Kirjassaan *Critical Infrastructure Security: Cybersecurity Lessons Learned from Real-World Breaches* Toledano (2024) on tiivistänyt DDoS-hyökkäyksen haitalliset seuraukset neljään kategoriaan:

- **Palveluiden häiriöt:** DDoS-hyökkäyksen keskeisenä tarkoituksena on lamauttaa hyökkäyksen kohteena oleva palvelu. Tämä voi johtaa kommunikaatiokatkoksiin, häiriöihin liikenteessä, sähkökatkoihin ja muihin häiriöihin.
- **Datan & kontrollin menetys:** Hyökkääjät voivat myös hyödyntää DDoS-hyökkäystä savuverhona salatakseen muita samaan aikaan tapahtuvia operaatioita. Samalla kun organisaatio keskittyy palvelunestohyökkäyksen torjumiseen, hyökkääjä pyrkii saamaan hallinnan järjestelmistä muita keinoja hyödyntäen.
- **Julkisen turvallisuuden riskit:** Joissain tapauksissa onnistunut palvelunestohyökkäys voi luoda merkittäviä riskejä yleiseen turvallisuuteen. Jos esimerkiksi hätäkommunikaatiojärjestelmät tai liikenteenohjausjärjestelmät kytkeytyvät pois päältä, on perusturvallisuuteen kohdistunut merkittävää uhkaa.
- **Pitkän aikavälin vahinko:** Onnistunut palvelunestohyökkäys voi luoda säröjä organisaation imagoon, sekä kykyyn torjua kyberturvallisuusuhkia. Tämä voi pitkällä aikavälillä aiheuttaa tuhoisia taloudellisia tai poliittisia seurauksia organisaatiolle.
  (Toledano 2024)

Palvelunestohyökkäykset ovat Suomessakin äärimmäisen ajankohtaisia. Kyberturvallisuuskeskus kertoi tiedotteessaan helmikuussa 2024, että useat suomalaiset organisaatiot ovat venäläismielisten haktivistiryhmien kohteena (Kyberturvallisuuskeskus 2024). Haktivismilla tarkoitetaan hakkereita, joiden toimintaa ohjaa poliittinen tai muu aatteellinen motiivi (Fortinet n.d.-a). Yksi tunnetuimmista haktivistiryhmistä on maailmanlaajuisesti kuuluisa Anonymous.

Mitään varsinaista näyttöä ei sinänsä ole siitä, että nämä haktivistiryhmät eivät liittyisi myös APT-operaatioihin, sillä jos palvelunestohyökkäyksen taustalla on samanaikaisesti toteutettava APT-operaatio, ei ole takeita, että kyseinen operaatio paljastuisi palvelunestohyökkäyksen yhteydessä. APT-operaatiot pysyvät usein piilossa hyvinkin pitkiä aikoja, ja jos operaatio paljastuisi esimerkiksi kuukausia tai jopa vuosia myöhemmin, voisi olla hyvin vaikeaa yhdistää näitä kahta tapahtumaa vedenpitävästi toisiinsa. Selvää kuitenkin on, että APT-operaatiot käyttävät palvelunestohyökkäyksiä osana operaatioitaan hämäämään tai lamauttamaan hyökkäyksen kohteena olevia organisaatioita.

Erityistä huomiota palvelunestohyökkäykset saivat taas syyskuussa 2024, kun Nordea tiedotti pankkia piinaavasta palvelunestohyökkäysten sarjasta, joka sijoittui yhtäaikaisesti pankin järjestelmien huoltotöiden kanssa (Kavander & Pantsu 2024). Tämä tilanne aiheutti häiriöitä pankin käyttäjille jopa yli viikon ajaksi. Ongelma ei koskenut pelkästään suomalaisia asiakkaita, sillä Nordea tiedotti havainneensa laajoja palvelunestohyökkäyksiä kaikissa Pohjoismaissa (Nordea n.d.). Kuluttajien kannalta tällaiset häiriöt pankkitoiminnoissa voivat aiheuttaa arkielämässä huomattavaakin haittaa. Kuluttaja voisi esimerkiksi huomata maksutilanteessa, että maksaminen ei onnistu, ja ostokset jäisivät tekemättä. Tällaiset tilanteet onnistuvat usein rapauttamaan kuluttajien luottamusta pankkiin, ja useat kuluttajat päätyvätkin vaihtamaan asiakkuuttaan jatkuvien häiriöiden sattuessa kohdalle.

Hajautettuja palvelunestohyökkäyksiä vastaan voi kuitenkin suojautua monella eri tavalla. Akamai, Cloudflare, Radware ja NexusGuard ovat esimerkkejä IT-palveluntarjoajista, jotka tarjoavat suojauskeinoja DDoS-hyökkäyksiä vastaan. Näitä keinoja ovat muun muassa organisaation sivuston staattisten tiedostojen kuten kuvien säilöminen erillisellä palvelimella, verkkoliikenneruuhkien tunnistaminen sekä valekäyttäjien erottaminen oikeista monimutkaisten algoritmien avulla. Organisaatiot voivat käyttää myös pilvipalveluntarjoajien, kuten Googlen tai AWS:n, kuormantasausominaisuuksia (*Load Balancing)*, jolloin palvelu toimii katkeamatta myös DDoS-hyökkäyksen aikana. (Aucestovar 2022, 2.)

3.2.2 Phishing – tietojenkalastelu

Sosiaalinen manipulointi eli *social engineering* tarkoittaa petosta, jossa pahantahtoinen hyökkääjä esittää olevansa jokin toinen ihminen, ryhmä tai brändi, johon uhri todennäköisesti luottaa enemmän kuin tuntemattomaan ihmiseen, saadakseen uhrin suorittamaan toimenpiteitä, jotka ovat hyökkääjän edun mukaisia. Sosiaalinen manipulointi käyttää hyväkseen luottamusta, jota ihmiset luonnostaan osoittavat toisilleen. (Grimes 2024.)

Phishing eli tietojenkalastelu on eräs sosiaalisen manipuloinnin alalajeista. Tietojenkalastelussa hyökkääjä yrittää huijata uhria avaamaan haitallisen linkin tai sähköpostiliitteen naamioimalla se joksikin muuksi, uhria kiinnostavaksi sisällöksi. Tällöin hyökkääjä voi saada haltuunsa uhrin kriittistä dataa, kuten pankki- ja henkilötunnuksia sekä puhelinnumeroita. (F-Secure 2022.)

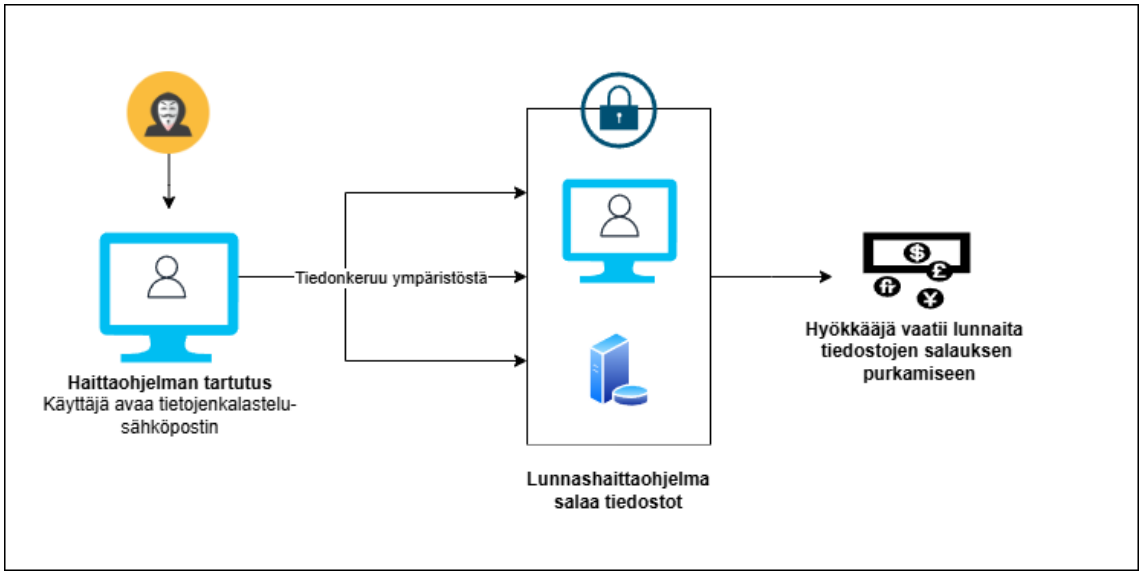
Spearphishing eli ”keihäskalastelu” viittaa tietojenkalasteluun, jossa hyökkääjä käynnistää tarkasti kohdistetun, räätälöidyn tietojenkalasteluoperaation tiettyä henkilöä, ryhmää, positiota tai organisaatiota vastaan (Grimes 2024). Tavanomainen tietojenkalasteluoperaatio asettaa uhrien määrän etusijalle, toisin kuin keihäskalastelu, joka keskittyy korkean arvon kohteisiin.

Hyökkääjä tutkii yleensä kohteensa tarkkaan hyödyntämällä avoimen lähteen tiedustelua sekä muita enemmän tai vähemmän moraalisesti kyseenalaisia tiedustelukeinoja ennen varsinaisen operaation käynnistämistä. Hyökkääjä saattaa esimerkiksi saada hyödyllistä tietoa yrityksen entiseltä työntekijältä sosiaalisen median alustoja hyödyntämällä ja pystyy täten räätälöimään keihäskalasteluoperaation yrityksen sisäisten prosessien mukaisesti.

3.2.3 Ransomware – lunnashaittaohjelmat

Ransomware eli lunnashaittaohjelma on haittaohjelma, joka *kryptaa* eli salaa tiedot uhrin laitteelta niin, että uhri ei pääse niihin käsiksi maksamatta hyökkääjälle vaadittuja lunnaita, kuten kuviossa 1 havainnollistetaan. Lunnashaittaohjelma on yksi haittaohjelmien yleisimmistä muodoista, ja lunnashaittaohjelmahyökkäykset

maksavat kohteiksi joutuneille organisaatioille vuosittain miljoonia dollareita. IBM:n X-Force® Threat Intelligence Index 2023 -raportin mukaan 20 % kaikista kyberhyökkäyksistä liittyi lunnashaittaohjelmiin. (Kosinski 2024.)



KUVIO 1. Lunnashaittaohjelmahyökkäyksen kulku (Akamai n.d., muokattu).

Lunnashaittaohjelmahyökkäysten suhteen ei ole myöskään takeita, että datan salaus purettaisiin tai tietoja ei julkaistaisi verkossa, vaikka uhriorganisaatio taipuisikin hyökkääjän vaatimuksiin ja maksaisi lunnaat. Rikollisten kanssa toimiessa onkin äärimmäisen tärkeä muistaa, että koskaan ei ole varmuutta, että rikollisten sana pitäisi ja lupaukset täytettäisiin. (Freed & Golden 2024.)

Yksi Suomessa kuuluisista lunnashaittaohjelmatapauksista sattui Keski-Uudenmaan koulutuskuntayhtymä Keudassa. Marraskuussa 2022 Keudaa vastaan kohdistettiin kyberhyökkäys *LockBit*-kiristyshaittaohjelmalla. Hyökkäys pysäytti koko Keudan IT-ympäristön täydellisesti lähes kuukaudeksi sekä saastutti 60 % Keudan kaikista työasemista ja palvelimista. Tutkinnassa havaittiin, että ainakin 219 työasemassa ja palvelimessa oli jälkiä haittaohjelmasta. (Anttolainen 2023.)

Hyökkääjät hyödynsivät Microsoft Azuren pilvipalvelimia sekä Microsoftin etähallintaohjelmisto RDP:tä (Remote Desktop Protocol) saadakseen jalansijaa Keudan IT-ympäristössä. Hyökkääjä oli aloittanut hyökkäyksensä kirjautumalla Azure AD Connect -palvelimelle RDP-palvelua hyödyntäen, joka oli virheellisesti

auki internetiin. Kuitenkaan tutkinnassa ei koskaan saatu selville, mistä hyökkääjä oli saanut tunnukset haltuunsa, joilla kirjautua palvelimelle. (Anttolainen 2023.)

Erityisen haasteen Keudan tapauksessa asetti hyökkäyksen ajankohta: hyökkäys tapahtui marraskuun lopussa, kun lukuvuosi läheni loppuaan ja osa oppilaista odotti jo innoissaan valmistumistaan. Tapaus sai kuitenkin siltä osin onnellisen lopun, että yksikään oppilas ei valmistunut myöhässä hyökkäyksen takia. (Anttolainen 2023.)

3.2.4 Watering-hole attack - juomapaikkahyökkäys

Watering-hole attack eli niin sanottu juomapaikkahyökkäys tarkoittaa hyökkäystä, jossa hyökkääjä saastuttaa muutoin täysin legitiimin sivuston, ja odottaa, että uhrit saapuvat sivustolle ja altistuvat hyökkäykselle. Hyökkäys juontaa nimensä eläinmaailmasta, jossa petoeläimet odottavat saaliseläimiä kärsivällisesti juomapaikalla, jossa saalis on haavoittuvaisimmillaan, ja iskevät, kun saalis on laskenut puolustuksensa juodakseen vettä. Tämä analogia kuvastaa hyökkäystä lähes täydellisesti. (Fortinet n.d.-b.)

Yleensä juomapaikkahyökkäykset suunnataan tietyille niche-sivustoille, joita tietty valikoitu käyttäjäryhmä todennäköisesti suosii. Tämä voisi esimerkiksi tarkoittaa sitä, että finanssisektorille suunnatut hyökkäykset voisivat esiintyä esimerkiksi joillakin taloustietoa tarjoavilla foorumeilla ja sivustoilla, joissa yritysten työntekijät vierailevat säännöllisesti. Juomapaikkahyökkäys ei ole kaikista tarkin hyökkäysmetodi kohdistaa tiettyyn henkilöön, vaan enemmänkin opportunistinen tekniikka maalittaa tiettyä ryhmää.

Juomapaikkahyökkäys on otollinen tekniikka APT-ryhmille, sillä usein APT-ryhmät yrittävät kohdistaa hyökkäyksiään tiettyihin, strategisesti merkittäviin käyttäjäryhmiin, kuten poliittisissa viroissa toimiviin henkilöihin. Esimerkiksi venäläistaustainen APT-ryhmä APT28 sekä pohjoiskorealainen APT38 ovat tunnetusti käyttäneet juomapaikkahyökkäyksiä osana kampanjoitaan (Sayegh 2023; XM Cyber n.d.).

3.2.5 Nollapäivähaavoittuvuudet

Nollapäivähaavoittuvuudet ovat kriittisiä haavoittuvuuksia, jotka turvallisuustutkijat tai hakkerit ovat onnistuneet löytämään järjestelmistä, mutta joista ohjelmiston valmistajat eivät ole tietoisia (Trend Micro n.d.). Tämä tekee niistä erityisen kriittisiä uhkia.

Nollapäivähaavoittuvuuden nimi juontuu siitä, että ohjelmiston kehittäjillä ei ole ollut aikaa korjata haavoittuvuutta, ennen kuin haavoittuvuus on julkaistu (eli toisin sanoen kehittäjillä on ollut ”nolla päivää” aikaa korjata haavoittuvuus). Ihannemaailmassa haavoittuvuuden havaitsija ilmoittaisi siitä mahdollisimman pian ohjelmiston kehittäjille, mutta valitettavasti usein nollapäivähaavoittuvuudet päätyvät hakkereiden käsiin, jolloin tieto nollapäiviähaavoittuvuudesta voi olla piilossa jopa vuosia. Nollapäivähaavoittuvuuksia hyödyntävät pahantahtoiset hakkerit voivat aiheuttaa mittaamattomia vahinkoja varastamalla tietoja tai asentamalla takaovia tai haittaohjelmia. (Zablackaitė 2024.)

Nollapäivähaavoittuvuudet ovat yksi voimakkaimmista kyberaseista, joita APT-ryhmät käyttävät. Nollapäivähaavoittuvuuksien luonteen vuoksi APT-operaatiot voivat kyteä uhriorganisaation järjestelmissä uhrien huomaamatta todella pitkiä aikoja ja näin altistaa vuosien saatossa suuria määriä kriittistä tietoa hyökkääjän silmille. Tämä tekee nollapäivähaavoittuvuuksista mittavan arvokkaita kyberrikollisille.

Microsoft tunnisti vuonna 2024 pohjoiskorealaisen *Citrine Sleet*-ryhmän käyttäneen hyödyksi nollapäivähaavoittuvuutta avoimen lähdekoodin Chromium-selaimessa (Microsoft 2024). Nollapäivähaavoittuvuus mahdollisti koodin suorittamisen etänä (RCE, *Remote Code Execution*) uhrin selaimessa. Hyökkäyksen kohteeksi joutuivat pääasiassa kryptovaluuttoihin liittyvät finanssiyritykset. Citrine Sleet kohdistaakin hyökkäyksensä pääasiassa finanssisektorille yrittäen saada taloudellista hyötyä kryptovaluuttojen muodossa.

Taloudellisen hyödyn tavoitteleminen on hyvin tyypillistä pohjoiskorealaisille hakkeriryhmille. Microsoft seuraa pohjoiskorealaisia hakkeriryhmiä nimikkeellä “Sleet” (tihkusade, räntä), ja Citrine Sleet omaakin yhtäläisyyksiä Diamond Sleet-

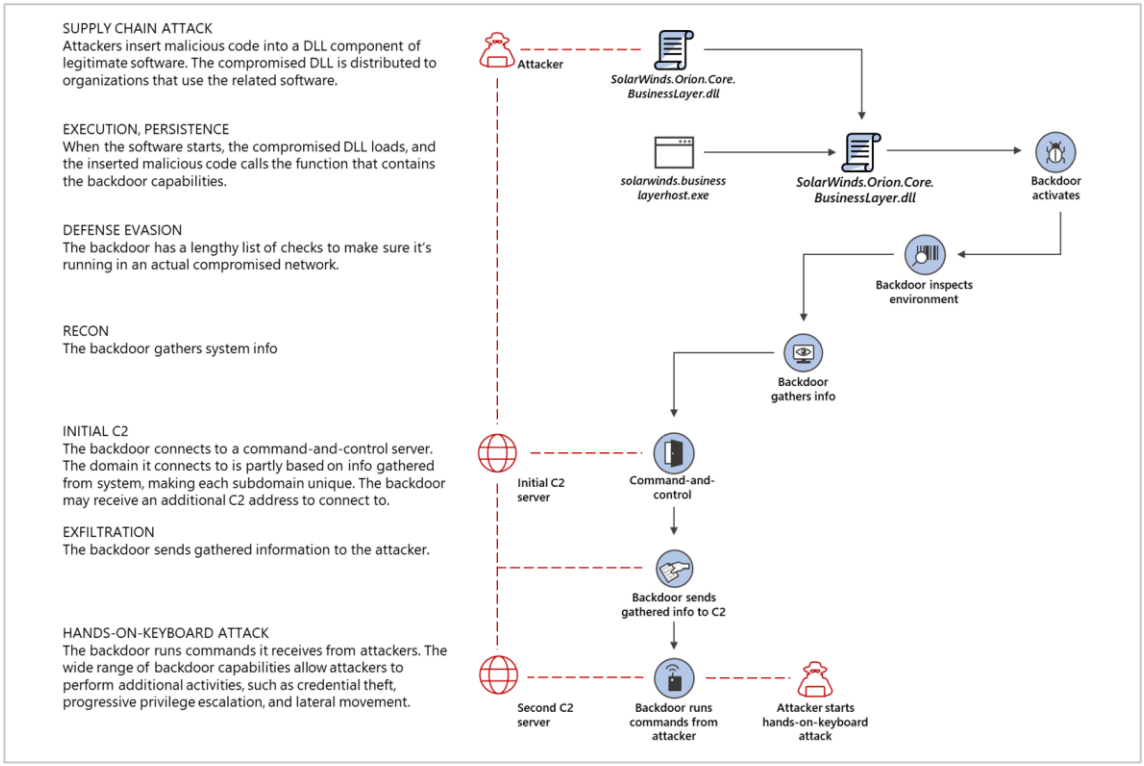
ryhmään, jonka monet muut tuntevat nimellä Lazarus Group. Usein Citrine Sleet, Diamond Sleet ja Sapphire Sleet -ryhmät niputetaankin yhteen Lazarus Group -nimen alle.

3.2.6 Toimitusketjuhyökkäykset

Toimitusketjuhyökkäyksessä hyökkääjä pääsee hyödyntämään olemassa olevaa luottamussuhdetta organisaation alihankkijoihin. Toimitusketjuhyökkäyksessä hyökkääjä saa jalansijan organisaatioon sen käyttämien palvelujen, verkostojen, tuotteiden tai avoimen lähdekoodin projektien kautta (Kyberturvallisuuskeskus 2022, 2). Ohjelmistot, laitteet, yhteistyökumppanit, palveluntarjoajat tai alihankkijat voivat toimia niin sanottuna ”Troijan puuhevosena” tarjoten hyökkääjälle tilaisuuden edetä varsinaisen kohdeorganisaation järjestelmiin.

Yksi tunnetuimpia toimitusketjuhyökkäyksiä oli IT-palveluntarjoaja SolarWindsiin kohdistunut hyökkäys vuonna 2020. SolarWindsin Orion-ohjelmistoon ujutettu haittakoodi latasi uhrin laitteelle takaoven, joka mahdollisti hyökkääjän huomaamattoman liikkumisen uhrin ympäristössä, kuten havainnollistettu kuviossa 2. Microsoftin uhkatiedustelu tunnisti hyökkääjän venäläiseksi Midnight Blizzardiksi, joka tunnetaan myös nimellä APT29. (Microsoft 2020.)

Hyökkäys onnistui vaikuttamaan tuhansiin organisaatioihin, ja jopa Yhdysvaltain hallituksen toimielimiin. Myös yritykset kuten Microsoft, Intel, Cisco ja Deloitte joutuivat hyökkäyksen uhreiksi. Hyökkäyksen mittava uhrimäärä johtui siitä, että Orion-ohjelmistoa käytettiin laajasti eri kansainvälisissä organisaatioissa ja valtiollisissa toimielimissä. (Kerner & Oladimeji 2023.)



KUVIO 2. SolarWindsiin kohdistuneen toimitusketjuhyökkäyksen kulku (Microsoft 2020).

3.3 APT-operaatiot maakohtaisesti

3.3.1 Johdanto APT-operaatioita suorittaviin maihin

Tämä luku sisältää katsauksen APT-operaatioista maittain. Eri mailla on maatyypillisiä tavoitteita, toimintatapoja sekä resursseja. APT-ryhmillä on myös kategorisia “lempinimiä” ryhmän alkuperämaan mukaan, kuten huomataan taulukoista 1, 2 ja 3.

APT-operaatioiden kohteiden perusteella Kiina, Venäjä ja Pohjois-Korea ovat ajantasaisimmat uhat suomalaisille organisaatioille, sillä Suomeen on todistettavasti kohdistunut APT-operaatioita näiden valtioiden toimesta. Yhdysvaltalaisjärjestelmien läsnäolo Suomessa DCA-sopimuksen ja Suomen Nato-jäsenyyden myötä voi taas mahdollisesti lisätä Iranin mielenkiintoa Suomea kohtaan.

APT-operaatioita suorittavat muutkin valtiot, kuten Vietnam (APT32). Myös Etelä-Amerikassa on tunnistettu APT-ryhmiä, kuten APT-C-36, joka on valikoinut kohteikseen Kolumbian valtionhallinnon sekä kolumbialaisia yrityksiä finanssi- öljy- sekä valmistusteollisuuden aloilta (Martinez 2021). Ei ole kuitenkaan viitteitä, että eteläamerikkalaiset tai vietnamilaiset APT-operaatiot uhkaisivat suomalaisia organisaatioita.

On mahdollista, että APT-operaatioita suorittavat lukuisat useammat maat kuin mitä yleisesti tiedetään, mutta koska APT-operaatiot ovat niin resurssi-intensiivisiä, ei ole todennäköistä, että kovinkaan moni pienempi valtio panostaisi erityisesti APT-operaatioihin perinteisen sotilaskaluston- ja koulutuksen sijaan. APT-operaatiot edellyttävät teknisiä resursseja, ja monet maat kärsivät esimerkiksi niin sanotun ”aivovuodon” tai puutteellisen koulutuksen aiheuttamasta teknisen pääoman vajavaisuudesta.

3.3.2 Iran

Iranilaiset APT-operaatiot on pääasiassa kohdistettu Yhdysvaltoja sekä Israelia, Saudi-Arabiaa, Libanonia ja muita Lähi-idän valtioita vastaan, muutamia poikkeuksia lukuun ottamatta. Tunnettuja Iranilaisia APT-ryhmiä ovat esimerkiksi APT33, APT34, APT35, APT39, APT45 sekä Rampant Kitten, Pioneer Kitten ja Static Kitten. (Shample 2023.)

Yhdysvaltojen Cybersecurity and Infrastructure Security Agencyn eli CISAn mukaan iranilaiset APT-ryhmät voisivat jopa vaikuttaa tämän tutkimuksen kirjoitushetkellä käynnissä oleviin Yhdysvaltojen presidentinvaaleihin 2024, sillä iranilaiset kybertoimijat yrittivät vaikuttaa yhdysvaltalaisiin äänestäjiin jo presidentinvaaleissa 2020. Tällöin iranilaiset ryhmät saivat haltuunsa yhdysvaltalaisten äänestäjien tietoja, lähettivät uhkaavia sähköposteja äänestäjille sekä levittivät disinformaatiota vaaleihin liittyen. CISAn mukaan samat ryhmät ovat kehittäneet uusia tekniikoita ja kyvykkyyksiä, joita nämä ryhmät voisivat käyttää häiritäkseen presidentinvaaleja vuonna 2024. (CISA 2024a.)

3.3.3 Kiina

Tietoturvayhtiö *Hunt & Hackettin* mukaan Kiina on kaikista maailman valtioista aktiivisin APT-operaatioiden saralla (Hunt & Hackett n.d.-a). Sivuhuomiona kuitenkin mainittakoon, että todistettujen APT-operaatioiden määrä ei kerro todellisten APT-operaatioiden määrästä, ja koska tietoturvayhtiöt käyttävät samoista ryhmistä monia eri nimityksiä omien nimityskäytänteidensä mukaisesti, on APT-operaatioiden konkreettista määrää vaikea arvioida. On kuitenkin selvää, että Kiina on investoinut merkittäviä määriä resursseja näiden operaatioiden luomiseen ja ylläpitämiseen.

Kiina ei pelkää käyttää länsimaisesti tarkasteltuna moraalisesti epäilyttäviä keinoja kyberhyökkäyskyvykkyyksiään kasvattaakseen. Amerikkalaisen *The Center for Security and Emerging Technology:n* tutkijan Dakota Caryn vuonna 2021 julkaisemassa raportissa esitellään kuuden kiinalaisen yliopiston yhteyttä kiinalaisiin APT-operaatioihin. Kiinalaiset yliopistot valmistelevat opiskelijoita kyberoperaatioihin tarjoamalla erilaisia hakkerointiin liittyviä kursseja, ja kiinalaiset APT-ryhmät palkkaavat opiskelijoita suoraan koulun penkiltä valeyritysten turvin. Tämä saumaton yhteistyö mahdollistaa jatkuvan uusien työntekijöiden virran APT-operaatioihin, ja näin operaatiot eivät pääse sakkaamaan työntekijäresurssien puuttumisen vuoksi. (Cary 2021.)

Yhdysvaltain kyberturvallisuusvirasto CISAn mukaan, jos Kiina kokisi ajautuvansa laajaan konfliktiin Yhdysvaltojen kanssa, se harkitsisi aggressiivisia kyberoperaatioita Yhdysvaltojen kriittistä infrastruktuuria sekä sotilaskohteita vastaan (CISA 2024b). Tämä julkinen tiedonanto ei kerro pelkästään siitä, kuinka tärkeää suurvalloille on ylläpitää jatkuvaa, kehittynyttä kyberpuolustusta toisen suurvallan kyberhyökkäysten varalle, vaan myös siitä, että Yhdysvallat pitävät Kiinan kyvykkyyttä suorittaa suurta vahinkoa aiheuttavia kyberhyökkäyksiä varteenotettavana ja merkittävänä uhkana.

Tämän huomioon ottaen tulisi myös eurooppalaisten, ja täten myös suomalaisten organisaatioiden ottaa Kiina-uhka hyvin vakavasti kyberpuolustustaan suunnitellessa. Kuten tämän tutkimuksen myöhemmissä luvuissa esitellyissä APT31:n operaatioissa Suomen sekä Norjan eduskuntaa vastaan huomataan, ovat myös

pohjoiseurooppalaiset kohteet kiinalaisille APT-operaatioille selkeästi erittäin kiinnostavia. Tätä kiinnostavuutta tuskin vähentää Suomen tuore NATO-jäsenyys sekä DCA-puolustusyhteistyösopimus.

3.3.4 Pohjois-Korea

Pohjoiskorealaisille APT-ryhmille on tietyissä yhteyksissä annettu lempinimi *“Chollima”,* joka tunnettaneen paremmin Pohjois-Korean hallinnon lanseeraamasta työväenliikkeestä, jonka tarkoitus oli kannustaa kansalaisia työskentelemään kovemmin Pohjois-Korean talouskasvun vauhdittamiseksi. Tämä kuvastaakin hyvin pohjoiskorealaista mentaliteettia sekä tiivistä yhteyttä APT-ryhmien ja Pohjois-Korean valtionhallinnon välillä. Chollima itsessään tarkoittaa pohjoiskorealaisessa mytologiassa esiintyvää Pegasoksen kaltaista siivekästä hevosta. (Korea Konsult n.d.)

Taloudelliset syyt ovatkin usein pohjoiskorealaisten APT-operaatioiden taustalla: pohjoiskorealaiset APT-ryhmät ovat oletettavasti vastuussa kybermaailman ryöstösaaliiltaan mittavimmista pankkiryöstöistä, sekä useista kryptopörsseihin kohdistuneista iskuista. Yksi esimerkki taloudellista hyötyä kerryttävästä iskusta on Lazarus Groupin 41 miljoonan dollarin varkaus nettikasino Stake.com:ilta syyskuussa 2023. Tällöin Lazarus Group varasti rahat hyödyntämällä Ethereum, Binance Smart Chain (BSC) sekä Polygon- kryptovaluuttojen lohkoketjua (FBI 2023).

Kuten muillakin APT-operaatioita harjoittavilla mailla, myös Pohjois-Korealla on muitakin tavoitteita kuin vain taloudellinen hyöty. Pohjois-Korea on suorittanut vakoiluoperaatioita muun muassa sotilaallisesti merkittäviä kohteita sekä ydinohjelmia vastaan, joista yhtenä esimerkkinä toimii APT45-ryhmän operaatio intialaista Kudankulamin ydinvoimalaa vastaan vuonna 2019 (Barnhart ym. 2024).

3.3.5 Venäjä

Venäjällä toimivat kyberoperaatioita toteuttavat ryhmät tulisi käytännössä jakaa kahteen pääkategoriaan: APT-ryhmät sekä muut järjestäytyneen rikollisuuden ryhmät (Hunt & Hackett n.d.-b). APT-ryhmät ovat Venäjän valtion sponsoroimia ryhmiä, kun taas muut järjestäytyneen rikollisuuden ryhmät eivät välttämättä suorita suoranaisia kybervakoiluoperaatioita, vaan ovat enemmän keskittyneitä taloudellisen hyödyn tavoitteluun tai misinformaation levittämiseen. Venäläiset kyberrikolliset tunnetaankin etenkin lunnashaittaohjelmien kuten *LockBit* käyttämisestä hyökkäyksissään.

Muutamia esimerkkejä tunnetuista kyberrikosorganisaatioista, jotka eivät varsinaisesti ole APT-ryhmiä ovat *Russian Business Network* ja *Internet Research Agency*. Russian Business Network eli RBN oli venäläinen palveluntarjoaja, joka tarjosi kotipaikan venäläiselle kyberrikollisuudelle 2000-luvun puolivälissä (Warren 2007). RBN vaikuttaisi kuitenkin olevan lakkautettu, sillä tuoretta tietoa organisaatioista ei käytännössä löydy. Internet Research Agency oli niin kutsuttu trollifarmi, eli misinformaatiota internetissä levittävä organisaatio (Ebbott, Saletta & Stearne 2021). Noin 300 työntekijän Internet Research Agency profiloitui vahvasti jo edesmenneeseen Wagner-palkka-armeijan perustajaan Jevgeni Prigožiniin. Prigožin tunnettiin myös lempinimellä “Putinin kokki” johtuen hänen perustamastaan ravintolasta, joka usein tarjoili Putinille sekä muille korkean profiilin vieraille (Harding 2019). Tämä korostaa Kremlin hyväksyntää trollifarmin toimille.

Tällä hetkellä yksi merkittävimmistä venäläislähtöisistä kyberrikollisorganisaatioista on *Evil Corp*. Evil Corp on onnistunut varastamaan pankkitunnuksia jopa sadoista pankeista sekä finanssialan yrityksistä yli 40 eri maassa, ja saavuttanut tätä kautta yli 100 miljoonaa dollaria rikoshyötynä. Evil Corp on erityisesti valinnut kohteiksiin finanssialan organisaatioita Yhdysvalloissa sekä Yhdistyneissä Kuningaskunnissa. (Yhdysvaltain valtiovarainministeriö 2019.)

Evil Corp on profiloitunut etenkin pahamaineisen *Dridex*-haittaohjelman luojana. Dridex varastaa arkoja tietoja uhrin tietokoneelta *keylogger*-ominaisuuden avulla koneeseen ujuttautumisen jälkeen. Usein Dridex-haittaohjelmaa yritetään ensin

levittää phishing-hyökkäyksen avulla. Jos uhri päätyy avaamaan tekaistuun sähköpostiin liitetyn haitallisen Microsoft Word tai Excel-tiedoston, Microsoft-dokumenteille tyypillinen makrokomento lataa Dridex-ohjelman uhrin koneelle uhrin tietämättä. Tämän jälkeen Dridex käyttää keylogger-ominaisuutta tallentaakseen uhrin jokaisen näppäimenlyönnin, mikä tekee esimerkiksi pankkitunnusten varastamisesta helppoa hyökkääjälle. (Gillis 2023.)

Yhdistyneiden kuningaskuntien rikostutkinta- ja lainvalvontaorganisaatio *NCA:n* raportin mukaan Evil Corp omasi huomattavan läheiset suhteet Venäjän hallintoon, joka korostaa Venäjän hallinnon sallivaa asennetta kyberrikollisiin, jotka valikoivat kohteekseen ulkomaisia organisaatioita. Raportin mukaan venäläiset tiedustelupalvelut jopa tilasivat Evil Corpilta hyökkäyksiä sekä tiedusteluoperaatioita NATO-jäsenmaita vastaan. Suhteita Venäjän hallintoon edisti erityisesti Evil Corpin johtajan Maksim Yakubetsin appi Eduard Benderskiy, joka on entinen korkea-arvoinen FSB:n virkamies. (NCA 2024, 4.)

3.4 APT-ryhmät

APT-operaatiot eivät toteudu itsekseen; ne tarvitsevat taakseen valtavat resurssit sekä päteviä työntekijöitä. APT-operaatioita toteuttaa ryhmä IT-ammattilaisia, joiden tehtävänä on varmistaa APT-operaatioiden sujuvuus. Näitä ryhmiä kutsutaan APT-ryhmiksi.

Seuraavissa alaluvuissa käydään läpi muutamia tunnetuimpia APT-ryhmiä, joilla on tunnettuja kytköksiä Euroopassa tapahtuneisiin kybervakoiluoperaatioihin tai muihin kyberhyökkäyksiin. Suuri osa APT-ryhmistä on ollut toiminnassa vuosia, jotkin jopa yli vuosikymmenen, josta johtuen operaatioita ja kampanjoita on kertynyt mittava määrä. Tämän tutkimuksen tarkoituksena on kuitenkin keskittyä niihin operaatioihin ja ryhmien tyypillisiin ominaisuuksiin, jotka antavat ajantasaista kuvaa siitä, minkälaista uhkaa suomalaisille organisaatioille näistä ryhmistä voisi olla. Osaa näistä erityisesti Eurooppaan kohdistuneista kybervakoiluoperaatioista ja hyökkäyksistä käydään tarkemmin läpi seuraavassa pääluvussa.

Aktiivisia APT-ryhmiä on kuitenkin huomattavasti paljon enemmän kuin tässä mainitut, ja niiden toimintatavatkin voivat poiketa toisistaan hyvin laajasti. Myös uusien tekoälyteknologioiden kehitys mahdollistaa uusien APT-operaatioiden sekä ryhmien syntymisen näiden teknologioiden ympärille.

Kuten aiemmissa luvuissa mainittua, APT-ryhmillä on monia eri nimiä riippuen kontekstista. Seuraavissa luvuissa esiteltyjen ryhmien monet eri nimet löytyvät tutkimuksen liitteenä olevasta taulukosta (liite 1).

3.4.1 Noname

Noname on Venäjä-myönteinen ja Nato-vastainen, mutta kansalaisuudeltaan toistaiseksi määrittelemätön hakkeriryhmä. Ryhmä on ollut aktiivinen maaliskuusta 2022. Noname onnistui häiritsemään Puolan hallinnon verkkosivustoa joulukuussa 2022 vastauksena siihen, että Puolan parlamentin alahuone eli *sejm* tunnusti joulukuun 2022 puolivälissä Venäjän roolin terrorismin rahoittamisessa. (Hegel & Milenkoski 2023.)

Noname on pääasiassa keskittänyt operaationsa maihin, jotka ovat olleet kriittisiä Venäjää kohtaan Venäjän aloitettua hyökkäyssodan Ukrainaa vastaan vuonna 2022 (tosin sodan voidaan katsoa käytännössä alkaneen Krimin valtauksesta vuonna 2014). Ensimmäiset hyökkäykset olivat pääosin ukrainalaisia uutissivustoja vastaan, mutta myöhemmin Noname on laajentanut operaatioitaan Nato-jäsenmaita vastaan. Ensimmäiset hyökkäykset, joista ryhmä otti vastuun, olivat palvelunestohyökkäykset ukrainalaisia uutis- ja mediasivustoja Zaxid, Fakty UA sekä muita vastaan maaliskuussa 2022. Ryhmän päämotivaationa vaikuttaisi olevan Venäjän vastaisten mielipiteiden vaientaminen. (Hegel & Milenkoski 2023.)

3.4.2 APT17 (Kiina)

APT17 on kiinalaisia yhteyksiä omaava APT-ryhmä. APT17 on kohdistanut hyökkäyksiään yhdysvaltalaisia valtionhallinnon elimiä, puolustusalan yrityksiä, lakiyrityksiä, IT-yrityksiä, kaivosyrityksiä sekä muita yksityisen sektorin toimijoita vastaan (MITRE ATT&CK 2024a).

Vuonna 2024 APT17 on kuitenkin alkanut kohdistamaan operaatioitaan eurooppalaisia kohteita vastaan, kuten Italian valtionhallinnon elimiä sekä italialaisia yrityksiä vastaan (Lakshmanan 2024). Yhdysvaltalaisen ajatushautomo Council on Foreign Relationsin (CRF) mukaan APT17:n jäsenillä on kytköksiä Kiinan turvallisuusministeriöön Jinanin kaupungissa (Council on Foreign Relations n.d).

APT17 on myös yhdistetty myös toisiin kiinalaisiin APT-ryhmiin, kuten Winnti Group, Wicked Panda (APT41), GREF, PassCV sekä Axiom. Yhdysvaltalaisen tietoturvayhtiö ProtectWisen (nykyään osa tietoliikenneyritys Verizonia) uhkatutkintatiimi 401TRG nimesi tämän ryhmittymän vuoden 2018 raportissaan *Winnti Umbrellaksi*. (Hegel 2018; Wilkens 2019.)

3.4.3 APT28 (Venäjä)

APT28, yksi tunnetuimmista venäläisistä APT-ryhmistä, on ollut aktiivinen jo vuodesta 2008 ja kohdistanut laajasti hyökkäyksiä Yhdysvaltoja ja läntistä Eurooppaa vastaan koko olemassaolonsa ajan. APT28, joka tunnetaan yleisesti myös nimillä Sofacy ja Fancy Bear, on valinnut kohteikseen laajasti eri sektoreita mukaan lukien ilmailu-, energia-, puolustus- ja valtiollisen sektorin. APT28:n tyypillisimpiä tekniikoita ovat tietojenkalastelu (*phishing)* sähköpostikampanjoiden avulla sekä tunnusten, kuten salasanojen ja käyttäjänimien, keräily (*credential harvesting*) väärennettyjä verkkosivuja hyödyntäen. APT28 on pääosin kohdentanut hyökkäyksiään perinteisille tietokoneille sekä mobiililaitteille. (CrowdStrike 2019.)

Yksi mielenkiintoisimmista tapauksista APT28:aan liittyen on APT28:n epäilty osuus Hillary Clintonin presidentinvaalikampanjan kyberhäirinnässä vuonna

2016. APT28 hyödynsi url-osoitteiden lyhentämiseen tarkoitettua *Bitly*-nimistä palvelua naamioidakseen haitallisia url-osoitteita, ja näin huijaten Clintonin vaalikampanjahenkilökuntaa avaamaan haitallisen linkin. Linkki ohjasi uhrin aidon näköiselle Googlen kirjautumissivulle, joka kuitenkin oli todellisuudessa hakkerien luoma kopiosivusto. Mikäli uhri päätyi syöttämään kirjautumistietonsa huijaussivulle, hakkerit saivat tiedot välittömästi käyttöönsä ja mahdollisuuden kirjautua uhrin Gmail-tilille. Kuitenkaan ei ole aukotonta tietoa siitä, onnistuiko hyökkäys tarkoitetulla tavalla. (Brewster 2016.)

Tietoturvayhtiö SecureWorksin mukaan haitallisia linkkejä oli kuitenkin avattu, joten mahdollisuus hyökkäyksen onnistumiseen on olemassa. SecureWorksin mukaan APT28 oli luonut 213 lyhennettyä linkkiä, jotka kohdistuivat 108 sähköpostiosoitteeseen *hillaryclinton.com*-domainilla. Noista 213:sta linkistä 20:ntä oltiin klikattu. (Brewster 2016.)

3.4.4 APT29 (Venäjä)

APT29 on venäläinen APT-ryhmä, joka on linkitetty Venäjän ulkomaantiedustelupalveluun SVR:ään. Ryhmä on ollut toiminnassa ainakin vuodesta 2008, usein kohdistaen hyökkäyksiään eurooppalaisia valtioita, Nato-jäsenmaita, tutkimuslaitoksia sekä ajatushautomoita vastaan. Yksi tunnetuimpia APT29:n suorittamia operaatioita oli tunkeutuminen Yhdysvaltain demokraattisen puolueen kansallisen komitean (*Democratic National Committee* eli DNC) tietoverkkoihin vuosina 2015 ja 2016 (MITRE ATT&CK 2024b). Hyökkäyksessä päästiin anastamaan tietoja DNC:n tietoverkoista. DNC:n tietomurtoon liittyi toinenkin venäläistaustainen ryhmä; myös APT28 oli osallisena tietomurtoon (CrowdStrike 2020.)

Tammikuun 30. päivä 2024 tietoturvayritys Zscalerin uhkatiedustelutiimi *ThreatLabz* havaitsi epäilyttävän PDF-tiedoston, jota APT29 oli käyttänyt operaatioissaan eurooppalaisia diplomaatteja vastaan. Näennäisesti Intian suurlähettiläältä saapuva PDF-tiedosto sisälsi kutsun viininmaistajaisiin helmikuussa 2024. Tämä kutsu piti sisällään linkin tekaistuun kyselyyn, joka uudelleenohjasi käyttäjät lataamaan saastuneen Zip-tiedoston. Tämän tiedoston ladattuaan uhrin laitteella aktivoitui obfuskoitua (eli *hämärrettyä* tai *peitettyä*) JavaScript-koodia sisältävä

haitallinen *wine.hta*-tiedosto, joka edelleen jatkoi hyökkäysketjua hyödyntämällä Windows-käyttöjärjestelmän omia DLL-kirjastoja. Hyökkäyksen myötä uhrin koneelle asentuu ironisen osuvasti nimetty ”WINELOADER”-takaovi, joka ottaa yhteyttä hyökkääjän palvelimelle. (Singh & Tay 2024.)

WINELOADER-takaovea käytettiin myös helmikuussa 2024, kun tietoturvayritys Mandiant tunnisti APT29:n suorittaman tietojenkalasteluoperaation, joka oli kohdistettu saksalaisia poliittisia puolueita vastaan. Hyökkäyksessä hyödynnettiin tekaistua illalliskutsua, joka lähetettiin suuren saksalaispuolueen *Christian Democratic Unionin* (CDU) nimissä. Tuttuun tapaan kutsu sisälsi hyökkääjän laatiman linkin, joka ohjasi uhrin lataamaan haitallisen Zip-tiedoston, joka käynnisti hyökkäysketjun, joka päättyy WINELOADER-takaoven asentumiseen uhrin laitteelle. (Black & Jenkins 2024.)

3.4.5 APT31 (Kiina)

APT31 on suomalaisille poikkeuksellisen tuttu nimi: Suojelupoliisi tunnisti Suomen eduskunnan tietojärjestelmiin vuonna 2020 kohdistuneen kybervakoiluoperaation APT31-ryhmän aikaansaannokseksi (Suojelupoliisi 2021). APT31 on myös kohdistanut operaatioitaan muihin EU-maihin sekä Yhdysvaltoihin.

Yhdysvaltojen mukaan APT31 on operoinut kulissiyhtiön, *Wuhan Xiaoruizhi Science and Technology Company* eli Wuhan XRZ:n takaa ainakin vuodesta 2010 vuoteen 2024, ja omaa väitetysti läheiset suhteet Kiinan valtion turvallisuusministeriöön (Ministry of State Security, MSS) Hubein provinssissa. (Pomfret & Tian 2024.)

Yhdysvaltojen *Diplomatic Security Servicen* (DSS) hallinnoima Rewards *for Justice* -ohjelma lupaa jopa 10 miljoonan dollarin palkkiota vihjeistä APT31-ryhmään liittyen. Tämä kuvastaa hyvin sitä, kuinka tosissaan Yhdysvaltain hallinto haluaa saada kiinalaiset kyberrikolliset oikeuden eteen.

3.4.6 APT38 (Pohjois-Korea)

APT38 eli “Lazarus Group” tai HIDDEN COBRA on Pohjois-Koreaan linkittyvä APT-ryhmä, joka on ollut aktiivinen vuodesta 2009. APT38:n laajat iskut finanssisektorille implikoisivat ryhmän olevan pääosin taloudellisesti motivoitunut, mutta osa hyökkäyksistä palvelee selkeästi Pohjois-Korean poliittista agendaa, kuten esimerkiksi Etelä-Koreaan tehdyt operaatiot. (Radware n.d.)

APT38 on kyberturvallisuusmaailmassa erityisen pahamainen; ryhmä on onnistunut vuoteen 2018 mennessä ryöstämään yli 1,1 miljardia dollaria erilaisilta finanssisektorin toimijoilta (Cannon, Fraser, O’Leary & Plan 2018). Myös ryhmän operaatio kansainvälistä elektroniikkajättiä Sonya vastaan on saanut suurta huomiota (Trend Micro 2018).

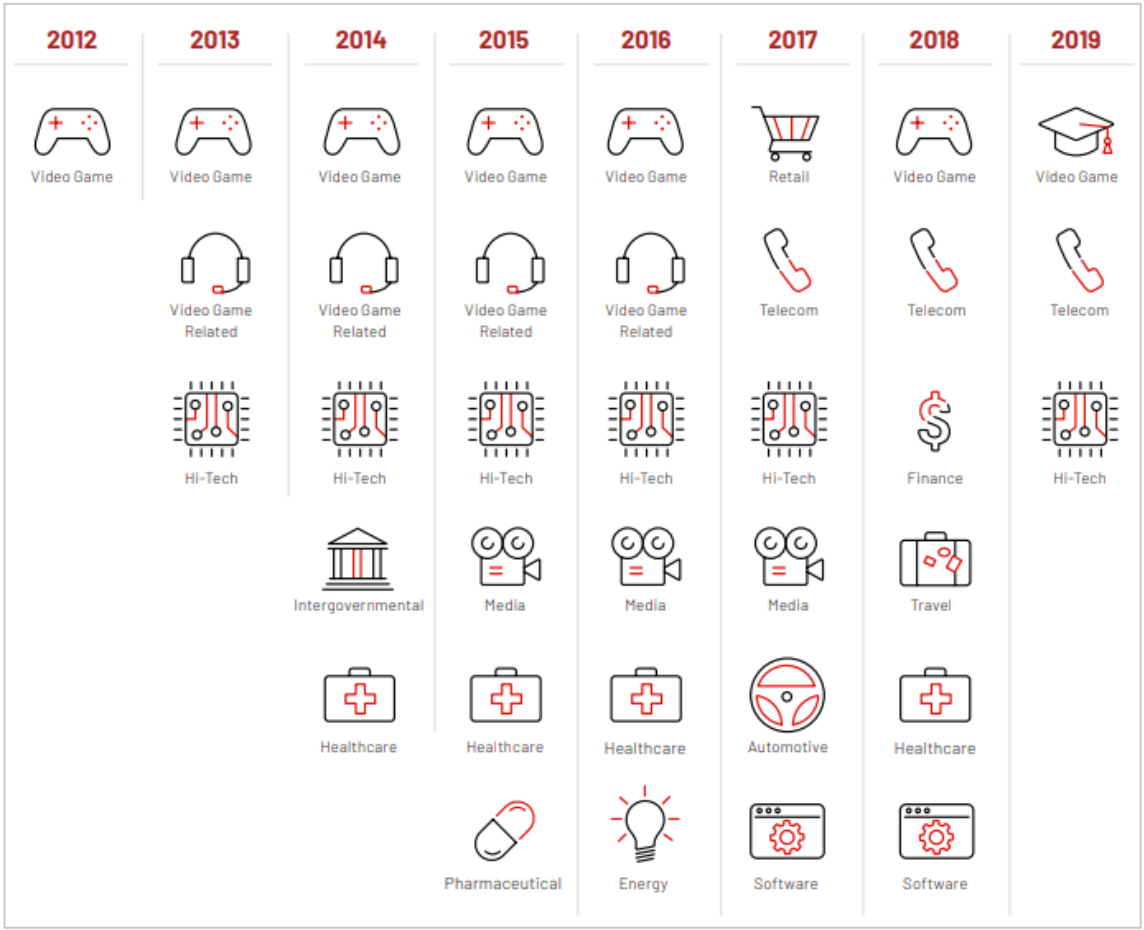
Sonyn tapauksessa APT38 sai vuodettua suuren määrän henkilökunnan tietoja julkisuuteen, ja jopa julkaisemattomia elokuvia vuodettiin internetiin ladattavaksi. Yksi näistä elokuvista oli vuoden 2014 sotaelokuva “Fury”, jota ladattiin erinäisiltä piratismisivustoilta 1,2 miljoonaa kertaa vuoden 2014 marraskuun loppuun mennessä. (Trend Micro 2014; Wallenstein & Lang 2014.)

APT38:n sanotaan olevan yhden maailman suurimmista lunnashaittaohjelmahyökkäyksistä, vuoden 2017 WannaCry-hyökkäyksen, takana. Toukokuussa 2017 WannaCry-lunnashaittaohjelma aiheutti mittavaa tuhoa levitessään 150 maahan yli 200 000 laitteelle. Uhreiksi joutuivat organisaatioita kuten FedEx, Honda, Nissan, ja Yhdistyneiden kuningaskuntien julkinen terveydenhuoltojärjestelmä National Health Service (NHS). Hyökkäys kuitenkin onnistuttiin pysäyttämään väliaikaisesti jo tuntien kuluttua hyökkäyksestä, sillä brittiläinen tietoturvatutkija Marcus Hutchins onnistui löytämään ohjelmasta niin sanotun ”tappokytkimen” (killswitch), joka pysäytti ohjelman leviämisen. Hutchins rekisteröi ohjelman koodissa esiintyneen verkko-osoitteen, ja huomattuaan että osoite on aktiivinen, ohjelma sulkeutui. (Woollacott 2022; Cloudflare n.d.)

3.4.7 APT41 (Kiina)

APT41 on kiinalainen, vuodesta 2012 aktiivinen ollut APT-ryhmä, joka on kohdistanut operaatioitaan terveydenhuolto-, videopeli-, teknologia-, telekommunikaatio- ja toimitusketjusektoreita vastaan, kuten kuvattu taulukossa 4. APT41:n operaatiot vaikuttivat aluksi olevan muista kiinalaisista APT-ryhmistä poiketen taloudellisesti motivoituneita, kunnes myöhemmin kohteet alkoivat muistuttaa muita Kiinan valtion alaisuudessa toimivia poliittisesti motivoituneita operaatioita. (Cannon ym. 2019, 5).

TAULUKKO 4. APT41:n kohdistamat operaatiot teollisuuden mukaan. (Cannon ym. 2019, 9.)



Vuoteen 2019 mennessä APT41 oli kohdistanut operaatioitaan ainakin 14 maata vastaan: Ranska, Intia, Italia, Japani, Myanmar, Alankomaat, Singapore, Etelä-Korea, Etelä-Afrikka, Sveitsi, Thaimaa, Turkki, Yhdistyneet kuningaskunnat ja

Yhdysvallat (Cannon ym. 2019, 6). Sittemmin uhreiksi ovat joutuneet myös yritykset Australiassa, Brasiliassa, Saksassa, Ruotsissa, Tiibetissä, Chilessä, Indonesiassa, Malesiassa, Pakistanissa ja Taiwanissa (FBI n.d.).

Kyseessä on toisin sanoen hyvin aktiivinen ryhmä, joka kohdistaa operaatioitaan ympäri maailmaa, Eurooppa mukaan lukien. APT41 on profiloitunut muun muassa toimitusketjuhyökkäyksissä, jossa kohdistetaan hyökkäyksiä toimitusketjun heikoimpia lenkkejä vastaan. APT41 käyttää tiedetysti hyökkäyksissään myös kiristyshaittaohjelmia.

Kuten APT31, myös APT41- ryhmän jäsenet ovat tunnistettu, ja ryhmän jäsenet ovat julkaistu kasvokuvineen Yhdysvaltain liittovaltion keskusrikospoliisi FBI:n sivustolla. FBI on julkaissut ryhmästä ”Wanted by the FBI”-ilmoituksen, mutta on oletettavaa, että ryhmän jäsenet eivät vielä ole päätyneet Yhdysvaltain oikeusjärjestelmän eteen, sillä ilmoitus on vielä tutkimusta tehdessä esillä FBI:n sivustolla. APT31 -ryhmästä poiketen APT41- ryhmään liittyvistä vihjeistä ei näyttäisi olevan tarjolla rahallista palkintoa *Rewards for Justice* -ohjelman sivustolla.

4 EUROOPPA APT-OPERAATIOIDEN KOHTEENA

4.1 Eurooppaan kohdistuneiden APT-operaatioiden taustaa

Tässä luvussa kuvataan erilaisia todellisia, toteutuneita kybervakoiluoperaatioita ja kyberhyökkäyksiä erilaisia eurooppalaisia organisaatioita vastaan. Eurooppalaiset yksityiset ja valtiolliset organisaatiot ovat aina olleet houkuttelevia kohteita vieraiden valtojen kyberoperaatioille. Lähes poikkeuksetta Eurooppaan kohdistuneiden APT-operaatioiden taustalla ovat autoritääriset diktatuurivaltiot idästä, kuten Venäjä, Kiina ja Pohjois-Korea. Myös Iran on kohdistanut operaatioita eurooppalaisia valtioita vastaan, joskin Iranin kohteiksi valikoituu useammin Yhdysvallat sekä Israel, Saudi-Arabia ja muut Lähi-idän valtiot.

4.2 APT17:n kohteena italialaiset yritykset ja Italian hallituksen toimielimet

Italialainen tietoturvayritys TGSoft paljasti APT17-ryhmän operaation, joka kohdistui italialaisiin yrityksiin, sekä Italian hallituksen toimielimiin. Operaatio käsitti kaksi hyökkäyskampanjaa, jotka tapahtuivat kesäkuun 6. ja heinäkuun 2. päivä 2024. Operaatiot hyödynsivät pääasiassa RAT 9002-haittaohjelmaa (*Remote Access Trojan*). (Tonello & Zuin 2024.)

Kesäkuun 24. päivä alkanut hyökkäyskampanja hyödynsi Microsoft Office -dokumenttia, kun taas jälkimmäinen heinäkuussa suoritettu kampanja hyödynsi linkkiä ilman Office-tiedostoa. Molemmat kampanjat kutsuivat käyttäjän lataamaan Skype for Business-paketin url-osoitteesta, joka muistutti Italian hallituksen käyttämiä osoitemuotoja. Tällä tavoin uhri saatiin johdettua harhaan haitalliselle sivustolle lataamaan haittaohjelman. (Tonello & Zuin 2024.)

4.3 APT28 vastaan Eurooppa

Venäjän sotilastiedusteluelimen GRU:n (*Glavnoje razvedyvatelnoje upravlenije*) alaisuudessa toimiva APT28 eli “Fancy Bear” kohdisti operaatioitaan 2020-luvulla lukuisia Euroopan maita vastaan. Kohteina olivat muun muassa Saksa, Tšekki, Liettua, Puola, Slovakia ja Ruotsi (Miller 2024). Saksassa hyökkäykset kohdistuivat muun muassa Saksan sosiaalidemokraattisen puolueen sähköpostiosoitteisiin (Goujard & Cerulus 2024). APT28 hyödynsi näissä operaatioissaan Microsoft Outlookista löytynyttä haavoittuvuutta.

APT28 on jo pitkään yrittänyt vaikuttaa Euroopan politiikkaan monissa eri yhteyksissä. Tästä kertoo APT28:n hyökkäys vuonna 2015 Saksan liittopäiviä vastaan. Tšekin ulkoministeriö taas kertoi vuonna 2024 Tšekin olleen jo pitkään APT28:n kohteena (Tšekin ulkoministeriö 2024). APT28:n yhtenä päätavoitteena näyttäisi toisin sanoen olevan poliittisen tilanteen epävakauttaminen Euroopassa. Tämä sopii hyvin yhteen Venäjän agendan kanssa luoda eripuraa, häiriöitä ja hybridivaikuttamista Euroopassa.

APT28:aa voidaan perustellusti pitää yhtenä suurimpana uhkana eurooppalaisille organisaatioille. Etenkin Suomen valtiolliset organisaatiot ovat todennäköisesti potentiaalisia kohteita tälle poliittisia tahoja vastaan hyökkäyksiään kohdistavalle APT-ryhmälle.

4.4 Pohjoismaiden eduskunnat APT31:n kohteena

Kiinalaiset APT-ryhmät tarjoavat monenlaista uhkaa eurooppalaisille päätöksentekoelimille. Seuraavissa alaluvuissa esitellään kiinalaisen APT31-ryhmän operaatioita Norjan sekä Suomen eduskuntaa vastaan.

4.4.1 Norjan eduskunta 2018

Vuonna 2018 Norjan eduskunta joutui kyberhyökkäyksen kohteeksi. Norjan poliisin turvallisuuspalvelun (Politiets sikkerhetstjeneste, PST) tutkimuksen mukaan

hyökkääjä onnistui saamaan ylläpitäjän oikeudet keskitettyihin järjestelmiin, joita käyttävät Norjan valtionhallinnon virastot koko maassa. Sen lisäksi hyökkääjä onnistui siirtämään dataa ulos näiden virastojen laitteilta. Tutkimus ei kuitenkaan onnistunut paljastamaan, mitä tietoja tarkalleen ottaen näiltä laitteilta saatiin, mutta näiden tietojen epäillään olleen valtionhallinnon työntekijöiden käyttäjänimiä sekä salasanoja. (Politiets sikkerhetstjeneste 2021.)

PST on sittemmin tunnistanut hyökkääjän kiinalaiseksi APT31-ryhmäksi. PST:n mukaan myös norjalainen pilvipalveluja tarjoava *Visma AG* joutui saman ryhmän hakkeroimaksi kesällä 2018. Kuitenkin kyberturvallisuusyritykset Rapid7 sekä Recorded Future tunnistivat omiin tietoihinsa nojaten hyökkäyksen APT10-ryhmän aikaansaannokseksi (Cimpanu 2021). Kuitenkin alkuperäinen raportti, joka viittaa Visma AG:n joutuneen APT10-ryhmän uhriksi on tutkimuksen kirjoitushetkellä nähtävästi poistettu internetistä, ja raportin johtopäätökset voidaan täten kyseenalaistaa.

4.4.2 Suomen eduskunta 2020

Suomen Suojelupoliisi tunnisti Suomen eduskuntaan kohdistuneen kybervakoiluoperaation vuonna 2020. Kybervakoiluoperaatiossa tunkeuduttiin onnistuneesti Suomen eduskunnan tietojärjestelmiin. Tapauksen yksityiskohtia on kommentoitu sangen niukkasanaisesti, ja tapauksen tekninen puoli jääkin suurimmilta osin pimentoon. Tapauksen jälkeen Suojelupoliisi tarjosi eduskunnan tietohallinnolle tietoja, joiden perusteella eduskunnan tietohallinto kykenee todentamaan mahdolliset hyökkäyksen jatkoyritykset. (Suojelupoliisi 2021.)

Tapausta tutkivat yhdessä sekä Suojelupoliisi että Keskusrikospoliisi, joista jälkimmäinen tutki operaatiota törkeänä tietomurtona, törkeänä viestintäsalaisuuden loukkauksena sekä törkeänä vakoiluna (Rautio & Happonen 2024). Operaatiossa siis toteutuivat törkeiden rikosten tunnusmerkistöt.

4.5 Suomen puolustusteollisuus ja Diamond Sleet / Lazarus Group

Microsoft julkaisi vuonna 2023 Itä-Aasiasta tulevia digitaalisia uhkia koskevan raportin, jonka mukaan Suomen puolustusteollisuus oli joutunut pohjoiskorealaisen Diamond Sleetin, eli Lazarus Groupin, hyökkäyksen kohteeksi (Microsoft 2023,15). Raportti ei sisältänyt yksityiskohtaista tietoa siitä, mikä tai mitkä suomalaisorganisaatiot hyökkäyksen kohteeksi olivat joutuneet.

Raportissa mainittiin, että Pohjois-Korealaiset APT-ryhmät Ruby Sleet ja Diamond Sleet olivat kohdistaneet hyökkäyksiään puolustussektorille marraskuun 2022 ja tammikuun 2023 välisenä aikana useissa eri maissa. Erityisesti kaksi aseidenvalmistusyritystä Saksassa ja Israelissa olivat joutuneet ryhmien hampaisiin tänä aikana. Tammikuun 2023 jälkeen Diamond Sleet oli kohdistanut operaatioitaan Suomen lisäksi myös Brasiliaan, Tsekkiin, Italiaan, Norjaan ja Puolaan. Operaatioiden tavoitteena on oletettavasti saada haltuunsa tietoa, jolla parantaa Pohjois-Korean sotilaallisia kyvykkyyksiä.

5 ASIANTUNTIJAHAASTATTELUT

5.1 Johdatus haastatteluihin

Tutkimusta varten haastateltiin kahta kyberturvallisuuden asiantuntijaa, jotka työnkuvansa tai muun ammattitaitonsa puolesta pystyivät tarjoamaan ajankohtaista tilannekuvaa organisaatioiden kyberturvallisuudesta. Haastattelut suoritettiin vapaamuotoisina teemahaastatteluina, mikä mahdollisti avoimen keskustelun haastattelun aiheesta, ja täten kumpikin haastattelu muodosti oman yksilöllisen kokonaisuutensa. Asiantuntijoita haastateltiin anonyymisti, ja heistä käytetään alla nimityksiä Asiantuntija A ja Asiantuntija B. Tässä luvussa käsitellään näiden asiantuntijoiden haastatteluissa antamia lausuntoja.

Haastatteluiden pohjana toimivat kahdeksan haastattelukysymystä, joista osaan kuului yksi tai useampia alakysymyksiä. Haastattelujen aikana esitettiin myös lisäkysymyksiä haastateltavan lausuntojen pohjalta. Kooste haastattelukysymyksistä löytyy liitteestä 2. Haastattelut litteroitiin *Amazon Web Services*:in eli AWS:n tarjoamaa *Transcribe*-palvelua hyödyntäen.

5.2 Ajankohtaiset uhat suomalaisille organisaatioille

Ensimmäinen teema käsitteli yleisluontoisesti kyberuhkia suomalaisille keskisuurille ja suurille organisaatioille. Tarkoituksena ei ollut käsitellä yksityiskohtaisesti hyökkäysten toteutustapoja, vaan saada yleiskuva suomalaisia organisaatioita kohtaavista kyberuhista.

Asiantuntija A mainitsi edelleen suomalaisille organisaatioille ajankohtaisiksi uhiksi kiristyshaittaohjelmat sekä palvelunestohyökkäykset. Asiantuntija A nosti esille, että vaikka palvelunestohyökkäykset aiheuttavat myös taloudellista vahinkoa sekä mahdollista mainehaittaa, on todennäköisesti kiristyshaittaohjelma sekä toiminnallisesti että taloudellisesti haitallisempi.

Asiantuntija B muistutti, että eri kyberhyökkäyksien ohella organisaatioille isoin riski on käytännössä ihminen itse; huolimattomalla toiminnalla organisaation henkilöstö voi altistaa organisaation mittaville vahingoille. Asiantuntija B mainitsi tietojenkalasteluhyökkäykset yhtenä tyypillisimmistä uhista organisaatioille.

5.3 Houkuttelevat kohdeorganisaatiot

Tässä teemassa käsiteltiin niitä tekijöitä, jotka tekevät organisaatiosta houkuttelevan kohteen kyberrikollisille. Yksiselitteisiä vastauksia tässä teemassa esitettyihin kysymyksiin ei ole, sillä eri APT-operaatioilla on hyvin erilaisia motiiveja.

Asiantuntija B mainitsi kiinnostavina kohdeorganisaatioina esimerkiksi teollisuusalan yritykset, jotka voisivat olla valmiita maksamaan rahaa lunnaita vaativille kyberrikollisille varastettuja liikesalaisuuksia vastaan. Asiantuntija B arveli myös sosiaali- ja terveysalan yritysten kiinnostavan rikollisia niiden käsittelemien arkaluonteisten tietojen vuoksi.

Asiantuntija A nosti kysymyksen keskiöön kyberhyökkääjän motiivin. Mikäli motiivi on hankkia lähinnä taloudellista etua, ovat mielenkiintoisia kohteita periaatteessa kaikki keskisuuret ja suuret yritykset. Asiantuntija A nosti tässä yhteydessä houkuttteleviksi kohteiksi myös vähittäiskaupat ja verkkokaupat. Mikäli motiivi on taas enemmän vakoilussa, ovat teknologiayritykset ja viranomaisorganisaatiot houkuttelevia kohteita.

Asiantuntija A arvioi kuitenkin, että suurin osa hyökkäyksen kohteeksi päätyvistä yrityksistä joutuu sellaisten rikollisryhmien kohteeksi, joiden motiivit ovat taloudellisia. Asiantuntija A:n näkemyksen mukaan yritykset ovat todennäköisesti houkuttelevampia kohteita kiristyshaittaohjelmille, sillä julkisen puolen organisaatiot eivät saa virallisten ohjeistuksien puitteissa maksaa lunnaita rikollisille.

5.4 Kybervakoiluoperaatioiden erovaisuus perinteisiin kyberhyökkäyksiin

Asiantuntija A piti selvänä, että APT-operaatiot vaativat sellaisia resursseja sekä taitoja, joita ei yksittäisellä kyberrikollisella välttämättä ole. Hän teki huomion, että APT-operaatioiden ero tavanomaisiin kyberhyökkäyksiin on käytännössä sisäänrakennettu jo APT-lyhenteeseen: *Advanced Persistent Threat* eli jatkuva pitkäkestoinen uhka. Yksittäiset kyberhyökkäykset ovat harvoin niin edistyneitä kuin APT:t tai tuottavat yhtä pitkäkestoista uhkaa.

Asiantuntija B korosti operaatioihin käytettävän ajan merkitystä: yksittäinen hyökkääjä ei esimerkiksi käytännössä pystyisi ylläpitämään hyökkäystä vuorokauden ympäri, kun taas hyvin resursoitu APT-ryhmä siihen kykenisi. Myös APT-operaatioissa käytettävä laitteisto voi olla edistyneempää kuin mitä yksittäinen hyökkääjä pystyisi itse kustantamaan.

5.5 Varautuminen APT-operaatioihin

Asiantuntija A arveli, että ainakin APT-operaatio Suomen eduskuntaan 2020 herätteli vähintäänkin julkisen puolen organisaatioita pitämään tietoturvastaan huolta. Hän mainitsi sääntelyn ja hallinnollisen ohjauksen lisääntyneen, mikä omalla tavallaan lisää organisaatioiden varautumista.

Samalla hän kuitenkin mainitsi haasteeksi etenkin yksityisen puolen organisaatioissa tietoturvatyön hinnan; tietoturvatyö maksaa paljon, mutta ei käytännössä tuota organisaatioille suoraa rahallista arvoa. Hän korosti, että henkilöstön tietoturvakoulutuksen määrää on kuitenkin jatkuvasti lisätty organisaatioissa, mikä lisää tietoturvaosaamisen määrää koko organisaatioissa.

Asiantuntija B arveli, että pääsääntöisesti organisaatiot ovat varautuneet tietoturvauhkiin, mutta kuitenkin viime aikoinakin lehdissä palstatilaa saaneet murrot ja palvelunestohyökkäykset näyttävät, että parantamisen varaakin on. Hän korosti,

että vaikka monivaiheinen tunnistautuminen, palomuurit ja muut tekniset asiat olisivat kunnossa, se ei välttämättä riitä, jos organisaation henkilöstö ei kiinnitä tietoturvariskeihin tarpeeksi huomiota.

5.6 Ulkopoliittiset tekijät

Asiantuntija A kertoi, että Suomen kuuluminen Euroopan unioniin ja tätä nykyä myös puolustusliitto Natoon lisää Suomeen kohdistuvaa mielenkiintoa etenkin Kiinan ja Venäjän suunnalta. Suomi saattaa näiden liittoutumien myötä pitää hallussaan tietoa, joka on Kiinalle ja Venäjälle erityisen houkuttelevaa. Hän ei pitänyt Suomen antamaa tukea Ukrainalle erityisen merkittävänä yksittäisenä tekijänä APT-operaatioiden näkökulmasta; käytännössä koko globaali länsi tukee Ukrainaa sen käymässä sodassa Venäjää vastaan.

Asiantuntija B arveli, että Ukrainalle annetun tuen myötä Suomi leimautuu yhä vahvemmin osaksi globaalia länttä ja täten mahdollisesti altistaa itsensä venäläismielisten tekijöiden kiusanteolle tai mahdollisille hyökkäyksille. Myös Suomen Nato-jäsenyys mahdollisesti lisää tällaisten operaatioiden mahdollisuutta, mutta asiantuntija näki myös mahdolliseksi, että Yhdysvaltojen tuen myötä myös pelotevaikutus on kasvanut, ja tämä voisi osaltaan jopa ennaltaehkäistä joitain toimia.

5.7 Vaarallisimmat valtiot ja APT-ryhmät

Asiantuntija A koki suurimmiksi uhiksi suomalaisten organisaatioiden kannalta Kiinan ja Venäjän. Hän ei kokenut, että rikollisryhmät näkisivät erityistä vaivaa valitakseen Suomen kohteekseen tai kehittäisivät työkaluja, jotka olisivat erityisesti suunnattuja suomalaisia organisaatioita vastaan. APT-operaatiot taas usein pyrkivät saamaan haltuunsa strategisesti tärkeää informaatiota, ja siinä suhteessa Suomi olisi kiinnostava kohde etenkin Kiinalle ja Venäjälle. Asiantuntija A tiivisti Kiinan ja Venäjän kybervakoiluoperaatiot virkkeeseen: “Venäjä varmaan yrittää enemmän, mutta Kiina onnistuu useammin.”

Asiantuntija A mainitsi, että usein Pohjois-Korean motiivit ovat myös taloudellisia, joten jos olisi sellainen tilanne, että olisi mahdollista iskeä myös Suomeen ja saada taloudellista hyötyä, silloin pohjoiskorealaiset rikollis- tai APT-ryhmät voisivat näin toimia. Kuitenkaan varsinaiseksi kohteeksi Pohjois-Korea tuskin valitsisi Suomea. Iranin Asiantuntija A kuvaili niin sanotuksi “tuntemattomaksi tekijäksi”, jonka motiivit ja operaatiot ovat vielä hieman hämärän peitossa. Kuitenkaan Irankaan tuskin erityisesti valitsisi Suomea operaatioiden kohteekseen.

Asiantuntija B korosti venäläismielisten ryhmien näkyvyyttä ajantasaisessa uhkaraportoinnissa. Hän nosti myös esille viime aikoina näkyneen huolestuttavan ilmiön; kun ennen osa rikollisryhmistä on saattanut ajatella, että kriittistä terveydenhuoltoa tai muita akuutisti ihmisen terveyden ja hengen kannalta kriittisiä organisaatioita vastaan ei hyökätä eettisistä syistä, nyt vaikuttaisi siltä, että tämäkin moraalipohja on sulanut pois ja mitkään kohteet eivät ole pois laskuista. Asiantuntija B kuvailikin tilannetta osuvalla englanninkielisellä fraasilla *”all bets are off”*, millä viitataan siihen, että kaikki keinot ovat käytettävissä tavoitteen saavuttamiseksi.

5.8 Suomen rooli APT-operaatioiden uhrina

Asiantuntija A näki, että Suomi on niin pieni markkina muuhun maailmaan verrattuna, että se vähentää jo itsessään hyvin paljon APT- ja rikollisryhmien kiinnostusta Suomeen. Kuitenkin Nato-jäsenyyden ja DCA-sopimuksen myötä Suomessa tulee olemaan myös Naton ja Yhdysvaltojen järjestelmiä, mikä saattaa lisätä mielenkiintoa nimenomaan näihin järjestelmiin. Silloin kohteena ei kuitenkaan sinänsä ole Suomi, vaan Nato tai Yhdysvallat, vaikka järjestelmien sijainti olisikin maantieteellisesti Suomessa.

Asiantuntija B jakoi Asiantuntija A:n näkemyksen siitä, että Suomi on pienenä maana vähemmän kiinnostava markkina. Asiantuntija B muisteli myös nähneensä tuoreen tutkimuksen, jonka mukaan Suomi on yksi kärkimaista kyberturvallisuuden suhteen, joten on mahdollista, että Suomen kyberpuolustus on kohtalaisen hyvällä tasolla jo oletusarvoisesti.

5.9 Tulevaisuuden uhkakuvat

Molemmat asiantuntijat mainitsivat tulevaisuuden uhkakuviksi kaksi murrosteknologiaa: tekoälyn ja kvanttilaskennan. Asiantuntija A arveli, että näistä kahdesta kvanttiteknologia tulee vaikuttamaan tietoturvaan jopa tekoälyä enemmän: yksi kriittisimmistä uhkakuvista, joihin tällä hetkellä varaudutaan, on se, että kun niin sanottu kvanttiherruus saavutetaan, niin nykyajan keskeisimmät salausmenetelmät menettävät tehonsa. Tämä tarkoittaisi sitä, että kaikki nykyajan salausmenetelmillä salatut digitaalisesti tallennetut tiedot olisivat selkokielellä luettavissa, mukaan lukien kriittisten alojen, kuten sairaanhoidon ja maanpuolustuksen, salaiset tiedot.

Asiantuntija B halusi korostaa, että vaikka uusia teknologioita, jotka vaikuttavat kyberturvallisuusriskeihin, nousee pinnalle aika ajoin, edelleen suurin yksittäinen kyberturvallisuusriski on ihminen itse. Kun ihmiset pitävät hyvää huolta laitteistaan, sekä siitä, kenen viesteihin he vastaavat ja mihin palveluihin he kirjautuvat, on taitavienkin kyberhyökkääjien vaikeampaa onnistua hyökkäyksissään.

6 JOHTOPÄÄTÖKSET JA POHDINTA

6.1 Johtopäätökset

Ensimmäinen päätutkimuskysymys käsitteli kyberturvallisuusuhkia, joita APT-operaatiot luovat suomalaisille organisaatioille. Tutkimusta tehdessä kävi ilmi, että vuonna 2024 APT-operaatiot ovat edelleen hyvin aktiivisia, ja toteuttavat hyökkäyksiään jatkuvasti. Teknisestä näkökulmasta uhkia muodostavat erilaiset hyökkäystaktiikat, joita APT-operaatiot käyttävät: DDoS-hyökkäykset, tietojenkalastelu, lunnashaittaohjelmat, juomapaikkahyökkäykset, nollapäivähaavoittuvuudet sekä toimitusketjuhyökkäykset. Jokainen edellä mainittu hyökkäystaktiikka vaatii omat yksilölliset suojausmenetelmänsä, ja on hyvin haasteellista suunnitella kyberpuolustus kattamaan erilaiset APT-operaatioiden käyttämät taktiikat, tekniikat ja menetelmät. Asiantuntijahaastatteluiden mukaan suomalaiset organisaatiot ovat kuitenkin pääosin tietoisia näistä uhista.

Toinen päätutkimuskysymys käsitteli Suomen kannalta vaarallisimpia valtioita ja APT-ryhmiä. Tutkimus osoittaa, että Suomen kannalta vaarallisimmat valtiot ovat ne, jotka ovat todistettavasti kohdistaneet APT-operaatioita Suomea vastaan: Venäjä, Kiina ja Pohjois-Korea. Nämä valtiot ovat valinneet Suomen lisäksi kohteikseen myös monia muita Euroopan valtioita, mikä viittaa siihen, että näiden valtioiden todellinen kohdealue on Eurooppa ja muu läntinen maailma, eikä ainoastaan Suomi. Kiinalaiset ryhmät kuten APT17, APT31 ja APT41, venäläiset ryhmät, kuten ATP28 ja APT29, sekä pohjoiskorealaiset ryhmät, kuten APT38 luovat suomalaisille organisaatioille todellista uhkaa, johon täytyy varautua huolellisuudella.

Tutkimuksen alakysymyksissä tarkasteltiin APT-operaatioiden taktiikoita, tekniikoita ja menetelmiä, suomalaisorganisaatioiden varautumista APT-operaatioihin, sekä sitä, mikä tekee organisaatiosta kiinnostavan APT-operaatiolle. Tutkimuksessa rajattiin, että yksityiskohtainen katsaus APT-operaatioissa käytettyihin tekniikoihin ja menetelmiin jää tutkimuksen ulkopuolelle, taktiikoita sen sijaan käsiteltiin tämän luvun ensimmäisessä kappaleessa. Rajauksen syynä on se, että

tutkimuksen tavoitteena oli luoda yleisluonteinen katsaus APT-operaatioiden uhkiin, eikä tarkastella niiden teknistä toteutusta yksityiskohtaisesti. Asiantuntijahaastatteluiden pohjalta APT-operaatioihin varautumisen suhteen organisaatioissa olisi vielä parannettavaa. Mekanismien luominen kehittyneiden kyberhyökkäysten estämiseen on työlästä, ja usein organisaatiot tarvitsevat siinä myös ulkopuolisten kyberammattilaisten apua, mikä voi tehdä siitä myös kallista. Kuitenkin kuten aiemmin todettu, suomalaisorganisaatiot ottavat kyberturvallisuuden pääasiallisesti hyvin huomioon. Kysymykseen siitä, mikä tekee organisaatiosta kiinnostavan kohteen, ei ole täysin yksiselitteistä vastausta. Kuitenkin mikäli organisaatio on taloudellisesti merkittävä, tai pitää hallussaan sotilaallisesti, poliittisesti tai teknologisesti kriittistä tietoa, se voi olla APT-operaatioita kiinnostava kohde.

6.2 Pohdinta

Tutkimus onnistui korostamaan jo ennestään tietoturva-ammattilaisille tuttua havaintoa: suomalaisten organisaatioiden kohdalla käytännössä suurinta uhkaa maantieteelliseltä pohjalta tarkasteltuna tuottavat Kiina, Venäjä sekä Pohjois-Korea. Kaikki näistä kolmesta valtiosta ovat todistettavasti kohdistaneet APT-operaatioita Suomea vastaan. Näistä valtioista aktiivisin APT-operaatioiden suhteen on Kiina. Ei ole sattumaa, että kaikki näistä edellä mainituista valtioista sijaitsevat idässä; 2020-luvulle tultaessa nämä valtiot ovat korostaneet itäisen ja läntisen maailman eroja entisestään ja onnistuneet luomaan entistä radikaalimpaa kahtiajakoa näiden osapuolten välillä.

Vuonna 2024 Venäjän jatkaessa hyökkäyssotaansa Ukrainassa miettii myös Kiina seuraavaa siirtoaan Taiwanin suhteen. Jatkuva uhittelu, painostus sekä sotaharjoitusten järjestäminen Taiwanin ympärillä lisäävät maailmanlaajuista levottomuutta muiden maiden arvuutellessa Kiinan mahdollisia sotilastoimenpiteitä Taiwanin suhteen. Mikäli Kiina yrittäisi liittää Taiwanin osaksi itseään sotilaallisin keinoin, voisi se olla askel lähemmäs suurempaa maailmanlaajuista konfliktia. Myös Pohjois-Korean kiihtynyt uhittelu Etelä-Koreaa kohtaan alleviivaa globaalin idän ja lännen välistä kiihtyvää vastakkainasettelua.

Maailmanlaajuiset konfliktit aiheuttavat muutoksia myös kybermaailmassa. Kyberhyökkäyksiä on käytetty tukemaan sotilaallista voimaa ennenkin, muun muassa Venäjän toimesta Georgiaa sekä Ukrainaa vastaan, mutta uusi laaja geopoliittinen konflikti voisi kiihdyttää teknologista kehitystä ja täten aktivoida laajan määrän uusia APT-operaatioita. Tähän tulevaisuuden uhkakuvaan organisaatioiden tulisi kiinnittää huomiota.

Tutkimuksesta voidaan myös päätellä, että Suomessa asiat ovat toistaiseksi kohtalaisen hyvin; Suomi on harvoin APT-operaatioiden ensisijainen kiinnostuksen kohde, sillä arvokkaampia kohteita on helppo löytää muualta. Suomen kyberpuolustuksen taso on yleisesti ansiokasta, eikä tavallisella kansalaisella ole syytä huolehtia siitä, että kriittiset organisaatiot olisivat jättäneet kyberturvallisuuden huomioimatta. Tästä pitää huolta myös Euroopan unionin kyberturvallisuusdirektiivi NIS2, joka määrittelee vähimmäisvaatimukset kyberturvallisuudelle yhteiskunnan kannalta kriittisille organisaatioille. Suomalaiset organisaatiot haluavat myös usein osoittaa luotettavuutensa asiakkaille esimerkiksi sertifioitumalla kansainväliseen ISO 27001-standardiin, joka määrittelee organisaation tietoturvallisuuden hallintajärjestelmän.

Tutkimuksessa nousi esiin, että APT-operaatioiden seuraamisesta tekee haasteellista se, että organisaatiot eivät halua aina paljastaa joutuneensa APT-operaation uhriksi. Tällöin tärkeää tietoa operaation taktiikoista, tekniikoista ja menetelmistä ei saada näkyväksi, ja jokin toinen organisaatio voi joutua saman operaation kohteeksi. Organisaatioilta toivottaisiinkin läpinäkyvyyttä, sillä avoin viestintä kriisin sattuessa voi jopa lisätä luottamusta organisaatioita kohtaan, ja muut organisaatiot voisivat välttää samat uhat.

Kuitenkin on aina syytä pitää mielessä, että APT-operaatiot ovat aina hyvin yksilöllisiä, ja vaikka tietäisi kuinka puolustautua yhtä vastaan, se ei riitä suojaamaan toisilta eri taktiikoita, tekniikoita ja menetelmiä käyttäviltä operaatioilta. Eri APT-operaatioita sponsoroivilla valtioilla on omia tyypillisiä toimintatapojaan, ja niiden tunnistaminen auttaa ehkäisemään potentiaalisimpia uhkia organisaatiolle. Esimerkiksi finanssi- ja talousalan organisaatiot ovat erittäin houkuttelevia kohteita pohjoiskorealaisille APT-operaatioille, joiden päämotiivina toimii rahallinen etu.

Tällöin olisi edullista olla selvillä pohjoiskorealaisten APT-ryhmien ajankohtaisista toimintatavoista.

Onneksi usein monet suuret organisaatiot saavat ajantasaista uhkatietoa muihin kyberturvapalveluihin kytkettynä. Tällöin tietoturva-analyytikot pääsevät luomaan tuoreisiin uhkakuviin pohjautuvia sääntöjä valvontajärjestelmiin, jotka estävät mahdolliset kyberhyökkäykset, ennen kuin hyökkääjät pääsevät murtautumaan järjestelmän sisälle. Ajantasaiseen uhkatietoon pohjautuvat, päivittyvät kybersuojausmenetelmät ovatkin paras keino suojautua APT-operaatiota vastaan teknisellä tasolla.

Yksi asia, johon jokainen voi organisaationsa koosta riippumatta kiinnittää huomiota, on oma henkilökohtainen kyberhygienia. Työvälineistä huolehtiminen ja tietojenkalasteluviesteiltä suojautuminen ovat yksinkertaisia, mutta toimivia keinoja APT-operaatioitakin vastaan suojautumisessa. Todella moni APT-operaatio alkaa yksinkertaisella tietojenkalasteluviestillä, mutta onnistuneesta tunnusten kalastelusta voi alkaa ketjureaktio, jonka seuraukset voivat olla vakavat. Tästä syystä yksittäisten työntekijöidenkin olisi hyvä olla perillä kyberrikollisten uusimmista toimintatavoista sekä muista kybermaailman ilmiöistä.

Kyberpuolustus onkin jatkuvaa kissa ja hiiri -leikkiä hyökkääjän ja puolustajan välillä, eikä kumpikaan taho aio luovuttaa ennen kuin on onnistunut tavoitteessaan. Onnistunut kyberpuolustus edellyttää resilienssiä ja kärsivällisyyttä, ja organisaatioiden on pystyttävä sitoutumaan pitkäjänteiseen kyberpuolustuksen ylläpitoon uhkien torjumiseksi. Organisaatioiden on kyettävä näkemään kyberpuolustus laajamittaisen liiketoiminnan mahdollistajana ylimääräisen kuluerän sijaan, sillä APT-operaation onnistuessa uhrina ei ole pelkästään organisaatio itse, vaan mahdollisesti myös sen palveluja hyödyntävät lukuisat loppukäyttäjät eli tavalliset ihmiset.

LÄHTEET

Akamai. n.d. What Is WannaCry Ransomware? Verkkosivu. Viitattu 24.11.2024. https://www.akamai.com/glossary/what-is-wannacry-ransomware

Anttolainen, V-H. 2023. Keudan loppuraportti kyberhyökkäyksestä on valmistunut. Keuda 10.3.2023. Verkkosivu. Viitattu 17.11.2024. https://www.keuda.fi/2023/03/10/keudan-loppuraportti-kyberhyokkayksesta-on-valmistunut/

Aucestovar, A. 2022. Detecting Application Layer DDoS Attacks Using TLS Fingerprinting. SANS Technology Institute 6.1.2022. Viitattu 3.12.2024. https://sansorg.egnyte.com/dl/1vcwc3nMJT

Barnhart, M., Johnson, J., Long, T., Plan, F. & Revelli, A. 2024. APT45: North Korea's Digital Military Machine. Mandiant 26.7.2024. Verkkosivu. Viitattu 18.11.2024. https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

Black, D. & Jenkins, L. 2024. APT29 Uses WINELOADER to Target German Political Parties. Mandiant 22.3.2024. Verkkosivu. Viitattu 21.11.2024. https://cloud.google.com/blog/topics/threat-intelligence/apt29-wineloader-german-political-parties

Brewster, T. 2016. Russian Hackers Targeted Hillary Clinton Campaign Google Accounts. Forbes 17.6.2016. Verkkosivu. Viitattu 21.11.2024. https://www.forbes.com/sites/thomasbrewster/2016/06/16/russian-hackers-hillary-clinton-google-gmail-attacks/

Cambridge Dictionary. n.d. Tactic. Verkkosivu. Viitattu 24.11.2024. https://dictionary.cambridge.org/dictionary/english/tactic

Cannon, V., Fraser, N., Leong, R., O'Leary, J., Perez, D., Plan, F. & Shen C. APT41: A Dual Espionage and Cyber Crime Operation. 2019. Mandiant 7.8.2019. Pdf-dokumentti. Viitattu 22.11.2024. https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

Cannon, V., Fraser, N., O'Leary, J. & Plan, F. 2018. APT38: Details on New North Korean Regime-Backed Threat Group. Mandiant 3.10.2018. Verkkosivu. Viitattu 22.11.2024. https://cloud.google.com/blog/topics/threat-intelligence/apt38-details-on-new-north-korean-regime-backed-threat-group

Cary, D. 2021. Academics, AI, and APTs - How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research. CSET 2021. Pdf-dokumentti. Viitattu 18.11.2024. https://cset.georgetown.edu/wp-content/uploads/CSET-Academics-AI-and-APTs.pdf

Cerulus, L. & Goujard, C. 2024. Elite Russian hackers breach Scholz's German socialist party. Politico 3.5.2024. Verkkosivu. Viitattu 22.11.2024. https://www.politico.eu/article/olaf-scholz-social-democratic-party-russian-hackers-fancy-bear/

Cimpanu, C. 2021. Norway says Chinese group APT31 is behind catastrophic 2018 government hack. The Record from Recorded Future News 19.6.2021. Verkkosivu. Viitattu 22.11.2024. https://therecord.media/norway-says-chinese-group-apt31-is-behind-catastrophic-2018-government-hack

CISA. 2024a. Iran Cyber Threat Overview and Advisories. Verkko-sivu. Viitattu 11.9.2024. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

CISA. 2024b. People's Republic of China Cyber Threat. Verkkosivu. Viitattu 18.11.2024. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

Cloudflare. n.d. What was the WannaCry ransomware attack? Verkkosivu. Viitattu 24.11.2024. https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Cole, E. 2013. Advanced persistent threat: understanding the danger and how to protect your organization. E-kirja. 1st edition. Boston: Syngress. Viitattu 17.11.2024. Vaatii käyttöoikeuden. https://www.oreilly.com/library/view/advanced-persistent-threat/9781597499491/

Council on Foreign Relations. n.d. APT 17. Verkkosivu. Viitattu 21.11.2024. https://www.cfr.org/cyber-operations/apt-17

CrowdStrike. 2019. Who is FANCY BEAR (APT28)? CrowdStrike 12.2.2019. Verkkosivu. Viitattu 21.11.2024. https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/

CrowdStrike. 2020. CrowdStrike’s work with the Democratic National Committee: Setting the record straight. CrowdStrike 5.6.2020. Verkkosivu. Viitattu 21.11.2024. https://www.crowdstrike.com/en-us/blog/bears-midst-intrusion-democratic-national-committee/

CrowdStrike. n.d.-a. Adversaries. Verkkosivu. Viitattu 17.11.2024. https://www.crowdstrike.com/adversaries/

Ebbott,E., Saletta,M. & Stearne, R. 2021. Understanding Mass Influence - A case study of the Internet Research Agency. The University of Melbourne 11.2.2021. Pdf-dokumentti. Viitattu 21.11.2024. https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/canberra/research/defence-research-institute/2023-02-Understanding-Mass-Influence---A-case-study-of-the-Internet-Research-Agency.pdf

Exabeam. n.d. What Are TTPs and How Understanding Them Can Help Prevent the Next Incident. Exabeam n.d. Verkkosivu. Viitattu 17.11.2024. https://www.exabeam.com/explainers/what-are-ttps/what-are-ttps-and-how-understanding-them-can-help-prevent-the-next-incident/

FBI. 2023. FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com. FBI 6.9.2023. Verkkosivu. Viitattu 18.11.2024.

https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom

FBI. n.d. APT 41 GROUP. Verkkosivu. Viitattu 22.11.2024. https://www.fbi.gov/wanted/cyber/apt-41-group

Fortinet. n.d.-a. Hacktivism—A Cyberattack? Meaning, Types, And More. Verkkosivu. Viitattu 17.11.2024. https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

Fortinet. n.d.-b. Watering Hole Attack. Verkkosivu. Viitattu 17.11.2024. https://www.fortinet.com/resources/cyberglossary/watering-hole-attack

Freed A.M & Golden, R. 2024. Ransomware and Data Extortion. E-kirja. O'Reilly Media, Inc. Vaatii käyttöoikeuden. Viitattu 5.8.2024. https://www.oreilly.com/library/view/ransomware-and-data/9781098169336/

F-secure. 2022. Mitä on tietojen-kalastelu? F-secure 28.10.2022. Verkkosivu. Viitattu 17.11.2024. https://www.f-secure.com/fi/articles/what-is-phishing

Gillis, A.S. 2023. Dridex malware. TechTarget 2023. Verkkosivu. Viitattu 21.11.2024. https://www.techtarget.com/searchsecurity/definition/Dridex-malware

Grimes, R.A. 2024. Fighting Phishing. E-kirja. Wiley. Viitattu 17.11.2024. Vaatii käyttöoikeuden. https://learning.oreilly.com/library/view/fighting-phishing/9781394249206/

Happonen, P. & Rautio, M. 2024. KRP ei ole vielä päässyt kuulemaan eduskunnan tietomurrosta epäiltyä – näin poliisi kuvailee harvinaista rikostutkintaa. Yle 26.3.2024. Verkkosivu. Viitattu 22.11.2024. https://yle.fi/a/74-20081005

Harding, L. 2019. Yevgeny Prigozhin: who is the man leading Russia's push into Africa? The Guardian 11.6.2019. Verkkosivu. Viitattu 21.11.2024. https://www.theguardian.com/world/2019/jun/11/yevgeny-prigozhin-who-is-the-man-leading-russias-push-into-africa

Hegel, T. 2018. Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. 401trg 3.5.2018. Verkkosivu. Viitattu 21.11.2024. https://401trg.com/burning-umbrella/

Hegel,T. & Milenkoski, A. 2023. NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO. SentinelLabs 12.1.2023. Verkkosivu. Viitattu 24.11.2024. https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/

Hunt & Hackett. n.d.-a Threat profile - China. Verkkosivu. Viitattu 18.11.2024. https://www.huntandhackett.com/threats/countries/china

Hunt & Hackett. n.d.-b. Threat profile - Russian Federation. Verkkosivu. Viitattu 18.11.2024. https://www.huntandhackett.com/threats/countries/russia

Jamil, N., Kiah, M., Mat, N. & Yusoff, Y. 2024. A systematic literature review on advanced persistent threat behaviors and its detection strategy. Journal of Cybersecurity, Volume 10, Issue 1 2.1.2024. Viitattu 3.12.2024. https://academic.oup.com/cybersecurity/article/10/1/tyad023/7504935

Kavander,A. & Pantsu, P. 2024. Syypäät Nordean verkkopankkihäiriöihin paljas-tuivat – pankki pahoittelee. Yle 20.9.2024. Verkkosivu. Viitattu 17.11.2024. https://yle.fi/a/74-20112889

Kerner, S. & Oladimeji, S. SolarWinds hack explained: Everything you need to know. TechTarget 3.10.2023. Verkkosivu. Viitattu 3.12.2024. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Korea Konsult. n.d. Pyongyang Chollima monument - the legendary flying horse. Verkkosivu. Viitattu 24.11.2024. https://www.koreakonsult.com/Attraction_Pyongyang_cholima_eng.html

Kosinski, M. 2024. What is ransomware? IBM 4.6.2024. Verkkosivu. Viitattu 17.11.2024. https://www.ibm.com/topics/ransomware

Kyberturvallisuuskeskus. 2022. Toimintaohje – Toimitusketjuhyökkäys. Kyberturvallisuuskeskus 2022. Pdf-dokumentti. Viitattu 18.11.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toimitusketjuhy%C3%B6kk%C3%A4ysToimintaohje.pdf

Kyberturvallisuuskeskus. 2024. Palvelunestohyökkäykset jatkuvat myös vuonna 2024. Kyberturvallisuuskeskus 2.2.2024. Verkkosivu. Viitattu 17.11.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-myos-vuonna-2024

Lakshmanan, R. 2024. China-linked APT17 Targets Italian Companies with 9002 RAT Malware. The Hacker News 17.6.2024. Verkkosivu. Viitattu 21.11.2024. https://thehackernews.com/2024/07/china-linked-apt17-targets-italian.html

Lambert, J. 2023. Microsoft shifts to a new threat actor naming taxonomy. Microsoft 18.4.2024. Verkkosivu. Viitattu 17.11.2024. https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/

Lang, B. & Wallenstein, A. 2014. Sony's New Movies Leak Online Following Hack Attack. Variety 29.11.2014. https://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/

Martinez, J.L.S. 2021. APT-C-36. MITRE 26.5.2021. Verkkosivu. Viitattu 18.11.2024. https://attack.mitre.org/groups/G0099/

Microsoft 2020. Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers. Microsoft 18.12.2020. Verkkosivu. Viitattu 3.12.2024. https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-

dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Microsoft. 2023. Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness. Pdf-dokumentti. Viitattu 22.11.2024. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

Microsoft. 2024. North Korean threat actor Citrine Sleet exploiting Chromium zero-day. Microsoft 30.8.2024. Verkkosivu. Viitattu 18.11.2024. https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

Microsoft. n.d.-a. What is a DDoS attack? Verkkosivu. Viitattu 17.11.2024. https://www.microsoft.com/en-us/security/business/security-101/what-is-a-DDoS-attack

Miller, M. 2024. The United States Condemns Malicious Cyber Activity Targeting Germany, Czechia, and Other EU Member States. U.S. Department of State 3.5.2024. Verkkosivu. Viitattu 22.11.2024. https://www.state.gov/the-united-states-condemns-malicious-cyber-activity-targeting-germany-czechia-and-other-eu-member-states/

Ministry of Foreign Affairs of the Czech Republic. 2024. Statement of the MFA on the Cyberattacks Carried by Russian Actor APT28 on Czechia. Ministry of Foreign Affairs of the Czech Republic 3.5.2024. Verkkosivu. Viitattu 22.11.2024. https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html

MITRE ATT&CK. 2024a. APT17. MITRE 4.9.2024. Verkkosivu. Viitattu 21.11.2024. https://attack.mitre.org/groups/G0025/

MITRE ATT&CK. 2024b. APT29. MITRE 3.9.2024. Verkkosivu. Viitattu 21.11.2024. https://attack.mitre.org/groups/G0016/

National Crime Agency. 2024. Evil Corp: Behind the Screens. Pdf-dokumentti. Viitattu 23.11.2024. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/732-evil-corp-behind-the-screens/file

Nordea. 2024. Päivitys: Palvelunestohyökkäykset voivat aiheuttaa hitautta Nordean digitaalisiin palveluihin kirjautumisessa. Nordea 23.9.2024. Verkkosivu. Viitattu 17.11.2024. https://www.nordea.com/fi/uutiset/paivitys-palvelunestohyokkaykset-voivat-aiheuttaa-hitautta-nordean-digitaalisiin-palveluihin-kirjautumisessa

Olson, R. 2022. Unit 42 Threat Group Naming Update. Palo Alto Networks 18.7.2022. Verkkosivu. Viitattu 17.11.2024. https://unit42.paloaltonetworks.com/unit-42-threat-group-naming-update/

Politiets sikkerhetstjeneste. 2021. Etterforskningen av datanettverksoperasjonen mot statsforvalterembeter henlegges. Politiets sikkerhetstjeneste17.6.2021.

Verkkosivu. Viitattu 22.11.2024. https://pst.no/alle-artikler/pressemeldinger/et-terforskningen-av-datanettverksoperasjonen-mot-fylkesmannsembetene-er-avsluttet/

Pomfret, J. & Tian, Y.L. 2024. APT31: the Chinese hacking group behind global cyberespionage campaign. Reuters 26.3.2024. Verkkosivu. Viitattu 22.11.2024. https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/

Radware. n.d. The Lazarus Group (APT38): North Korean Threat Actor. Verkkosivu. Viitattu 22.11.2024. https://www.radware.com/cyberpedia/DDoS-attacks/the-lazarus-group-apt38-north-korean-threat-actor/

Raza, M. 2023. What Are TTPs? Tactics, Techniques & Procedures Explained. Splunk 30.5.2023. Verkkosivu. Viitattu 17.11.2024. https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html

Rewards for Justice. n.d. APT31/Wuhan Xiaoruizhi Science & Technology Company, Ltd. Verkkosivu. Viitattu 24.11.2024. https://rewardsforjustice.net/rewards/apt31-wuhan-xiaoruizhi-science-technology-company-ltd/

Sayegh, E. 2023. APT28 Aka Fancy Bear: A Familiar Foe By Many Names. Forbes 28.2.2023. Verkkosivu. Viitattu 17.11.2024. https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/

Shample, S. 2023. Iranian APTs: An overview. Middle East Institute 10.2.2023. Verkkosivu. Viitattu 18.11.2024. https://www.mei.edu/publications/iranian-apts-overview

Singh, S. & Tay. R. 2024. European diplomats targeted by APT29 (Cozy Bear) with WINELOADER. Zscaler 27.2.2024. Verkkosivu. Viitattu 21.11.2024. https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-apt29-cozy-bear-wineloader

Suojelupoliisi. 2021. Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi. Suojelupoliisi 18.3.2021. Verkkosivu. Viitattu 21.11.2024. https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi

Toledano, S. A. 2024. Critical Infrastructure Security : Cybersecurity Lessons Learned from Real-World Breaches. E-kirja. First edition. Birmingham: Packt Publishing. Vaatii käyttöoikeuden. https://www.oreilly.com/library/view/critical-infrastructure-security/9781837635030/

Tonello, G. & Zuin, M. 2024. Italian government agencies and companies in the target of a Chinese APT. TG Soft. 9.7.2024. Verkkosivu. Viitattu 22.11.2024. https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng

Trend Micro 2014. The Hack of Sony Pictures: What We Know and What You Need to Know. Trend Micro 8.12.2014. Verkkosivu. Viitattu 22.11.2024.

https://www.trendmicro.com/vinfo/fi/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

Trend Micro. 2018. A Look into the Lazarus Group's Operations. Trend Micro 25.1.2018. Verkkosivu. Viitattu 22.11.2024. https://www.trendmicro.com/vinfo/fi/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

Trend Micro. n.d. Zero-Day Vulnerability. Verkkosivu. Viitattu 17.11.2024. https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

U.S. Department of the Treasury. 2019. Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. U.S. Department of the Treasury 5.12.2019. Verkkosivu. Viitattu 21.11.2024. https://home.treasury.gov/news/press-releases/sm845

Warren, P. 2007. Hunt for Russia's web criminals. The Guardian 15.11.2007. Verkkosivu. Viitattu 20.11.2024. https://www.theguardian.com/technology/2007/nov/15/news.crime

Wilkens, E. 2019. Verizon acquires ProtectWise, Inc., expanding network detection and response services for business customers. Verizon 1.3.2019. Verkkosivu. Viitattu 21.11.2024. https://www.verizon.com/about/news/verizon-acquires-protectwise-inc-expanding-network-detection-and-response-services-business

Woollacott, E. 2022. Marcus Hutchins on halting the WannaCry ransomware attack – 'Still to this day it feels like it was all a weird dream'. PortSwigger 12.5.2022. Verkkosivu. Viitattu 24.11.2024. https://portswigger.net/daily-swig/marcus-hutchins-on-halting-the-wannacry-ransomware-attack-still-to-this-day-it-feels-like-it-was-all-a-weird-dream

XM Cyber. n.d. Countermeasures for APT38. XM Cyber n.d. Verkkosivu. Viitattu 17.11.2024. https://xmcyber.com/blog/countermeasures-for-apt38/

Zablackaitė, Ž. 2024. Nollapäivähaavoittuvuudet, -hyökkäykset ja niiden hyödyntäminen: Kaikki mitä sinun tulisi tietää. NordVPN 27.3.2024. Verkkosivu. Viitattu 17.11.2024. https://nordvpn.com/fi/blog/nollapaivahaavoittuvuus/

LIITTEET

Liite 1. APT-ryhmien nimitaulukko

APT-ryhmien monista eri nimistä koostettu taulukko.
(Malpedia. n.d. https://malpedia.caad.fkie.fraunhofer.de)

APT-OPERAATIOIDEN NIMITAULUKKO
(Lähde: Malpedia, https://malpedia.caad.fkie.fraunhofer.de/)

Nimi	Muut nimet	Maa
NoName	05716nnm, Nnm05716, NoName057, NoName05716	Määrittelemätön
APT17	AURORA PANDA, Axiom, BRONZE KEYSTONE, Dogfish, G0001, G0025, Group 72, Group 8, HELIUM, Hidden Lynx, Tailgater Team	Kiina
APT28	APT 28, APT-C-20, ATK5, Blue Athena, BlueDelta, FANCY BEAR, FROZENLAKE, Fancy Bear, Fighting Ursa, Forest Blizzard, G0007, Grey-Cloud, Grizzly Steppe, Group 74, Group-4127, IRON TWILIGHT, ITG05, Pawn Storm, SIG40, SNAKEMACKEREL, STRONTIUM, Sednit, Sofacy, Swallowtail, T-APT-12, TA422, TG-4127, Tsar Team, TsarTeam, UAC-0028	Venäjä
APT29	ATK7, Blue Kitsune, BlueBravo, COZY BEAR, Cloaked Ursa, G0016, Grizzly Steppe, Group 100, IRON HEMLOCK, ITG11, Midnight Blizzard, Minidionis, Nobelium, SeaDuke, TA421, The Dukes, UAC-0029, YTTRIUM	Venäjä
APT31	BRONZE VINEWOOD, JUDGMENT PANDA, Red keres, TA412, Violet Typhoon, ZIRCONIUM, Zirconium	Kiina
APT38	Lazarus Group, APT 38, APT-C-26, ATK117, ATK3, Andariel, Appleworm, BeagleBoyz, Bluenoroff, Bureau 121, COPERNICIUM, COVELLITE, Citrine Sleet, DEV-0139, DEV-1222, Dark Seoul, Diamond Sleet, G0032, G0082, Genie Spider, Group 77, Hastati Group, Hidden Cobra, Labyrinth Chollima, Lazarus, Lazarus group, NICKEL GLADSTONE, NewRomanic Cyber Army Team, Nickel Academy, Operation AppleJeus, Operation DarkSeoul, Operation GhostSecret, Operation Troy, Sapphire Sleet, Stardust Chollima, Subgroup: Bluenoroff, TA404, Unit 121, Whois Hacking Team, ZINC, Zinc	Pohjois-Korea
APT41	Amoeba, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Blackfly, Brass Typhoon, Earth Baku, G0044, G0096, Grayfly, HOODOO, LEAD, Red Kelpie, TA415, WICKED PANDA, WICKED SPIDER	Kiina

Liite 2. Kooste haastattelukysymyksistä

Kooste tutkimuksessa käytetyistä haastattelukysymyksistä. (Kiuru 2024.)