Tampereen yliopisto

Noora Kukkonen

IOT BOTTIVERKKOJEN KEHITTYMINEN DDOS HYÖKKÄYSTEN VÄLINEENÄ

Diplomityö
Tekniikan ja luonnontieteiden tiedekunta
Tarkastajat: Jari Seppälä
Mikko Salmenperä
Tammikuu 2024

TIIVISTELMÄ

Noora Kukkonen: IoT bottiverkkojen kehittyminen DDoS hyökkäysten välineenä
Diplomityö
Tampereen yliopisto
Automaatiotekniikka
Tammikuu 2024

Esineiden internet (IoT) on joukko toisiinsa internetin yli liitettyjä, laskentaan kykeneviä laitteita. Nykyään on yleistä, että monet aikaisemmin Internetistä riippumattomat laitteet, esimerkiksi kodinkoneet ja kellot, yhdistetään myös verkkoon. Tämä on tuonut haasteita tietoturvan kannalta. Eräs ongelma on hajautetut palvelunestohyökkäykset (DDoS), joissa kohteen palveluiden käyttöä yritetään estää lähettämällä sille kutsuja useasta eri lähteestä.

Tämän työn alussa käydään läpi, miten DDoS-hyökkäykset toimivat ja miten niitä voidaan toteuttaa. Sen jälkeen käydään läpi, miksi palvelunestohyökkäyksiä tehdään ja miten niiltä voisi suojautua palveluntarjoajan puolelta. Loppuosa työstä keskittyy siihen, miten IoT-laitteita hyödynnetään osana DDoS-hyökkäyksiä ja miten niistä rakennetaan bottiverkkoja. Työssä käydään läpi myös mitä toimia EU ja Suomi ovat tehneet pienentääkseen IoT-laitteista aiheutuneita tietoturva riskejä.

Työssä esitellään viimevuosilta yhdeksän IoT laitteista koostuvaa DDoS-kykenevää bottiverkkoa ja selvitetään miten bottiverkot ovat kehittyneet ajan saatossa. Tuloksissa huomattiin muun muassa, että 2016 oli merkittävä vuosi haittaohjelmien osalta. Kyseisenä vuonna löydetty bottiverkko Mirai oli selkeä käännekohta, jonka jälkeen monet DDoS-hyökkäyksiin keskittyvät haittaohjelmat olivat Mirai johdannaisia, tai Mirain pohjalta rakennetun haittaohjelman muunnelmia.

Avainsanat: IoT, bottiverkko, DDoS, haittaohjelma

ABSTRACT

Noora Kukkonen:
Master of Science Thesis
Tampere University
Automation technology
January 2024

Internet of Things (IoT) is network of devices which are connected to each other over the Internet. Nowadays it is common, that many devices that had not initially been designed to have an Internet connection, for example watches and home appliances, are now connected. This brings with itself a range of security challenges. One of these are Distributed Denial of Service (DDoS) attacks, where an attacker tries to make a target service unreachable for its clients.

This paper introduces how DDoS-attacks work and how they are executed and what are the motives behind them. Also introduced are some methods for service providers to decrease the risks of being targeted by such attacks. Rest of the paper focuses on how IoT devices are exploited as parts of DDoS attacks. Additionally it is explained how botnets using IoT devices can be built and how they function. One section of the paper also goes over some of the actions taken by the EU and Finland to mitigate the security risks associated with IoT devices

This thesis introduces nine DDoS capable botnets that were created from IoT devices. The focus of the thesis is on how these botnets have evolved over time. By analysing the botnets it was found that 2016 was an important year in the history of IoT malware. During that year a botnet known as Mirai was found. Many of the DDoS capable malwares that were found after Mirai were either based or derived from Mirai.

Keywords: IoT, botnet, DDoS, malware

ALKUSANAT

Pitkän mietinnän jälkeen päädyin kirjoittamaan diplomityöni omasta aiheesta. Tämän päätöksen pohjalta sain rakentaa työstä haluamani ja keskittyä hyvin mielenkiintoiseen aiheeseen, mutta se myös johti kirjoitusprosessin venymiseen, sillä tein töitä koko kirjoittamisen ajan. Työ opetti paljon ja olen siinä onnellisessa asemassa, että se on vihdoin valmistunut.

Isot kiitokset ohjaajilleni Jari Seppälälle ja Mikko Salmenperälle Tampereen Yliopistolta kommenteista ja ohjauksesta prosessin aikana. Lisäksi suuri kiitos ystäville ja perheelle tuesta ja luotosta kykyihini, mitä ilman olisin varmasti luovuttanut moneen kertaan viime vuoden aikana.

Tampereella, 14. tammikuuta 2024

Noora Kukkonen

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

C&C	Järjestelmän arkkitehtuurityyppi, komenna ja kontrolloi. Käytetään myös C2 (engl. Command and control)
CVE	Systeemi, jolla jaoitellaan yleisiä tietoturva heikkouksia sekä altistumisia (engl. Common Vulnerabilities and Exposures)
CWE	Yhteisön kehittämä lista sovellus sekä laitteistojen heikkous tyyppejä (engl. Common Weakness Enumeration)
DDoS	Hajautettu palvelunesto (engl. Distributional Denial of Service)
DNS	Internetin nimipalvelujärjestelmä, muuntaa verkkotunnuksia IP-osoitteiksi (engl. Domain name system)
GDPR	Yleinen tietosuoja-asetus (engl. General Data Protection Regulation)
GIF	Häviötön bittikarttagrafiikan tallennusformaatti (engl. Graphics Interchange Format)
HTTP	Hypertekstin siirtoprotokolla (engl. Hypertext Transfer Protocol)
HTTPS	Hypertekstin siirtoprotokollan ja TSL/SSL-protokollan yhdistelmä, jota käytetään suojattuun tiedonsiirtoon. (engl. Hypertext Transfer Protocol)
ICMP	Verkkokerroksen protokolla, jota verkkolaitteet käyttävät virheviestien sekä muiden toiminnallisten tietojen välittämiseen (engl. Internet Control Message Protocol)
IoT	Esineiden Internet (engl. Internet of things)
IP	Internet protokolla
IRC	Eräs Internetin pikaviestintäpalvelu (engl. Internet Relay Chat)
ISO	Kansainvälinen standardointiorganisaatio
JPEG	Häviöllistä pakkausta käyttävä bittikarttagrafiikan tallennusformaatti (engl. Joint Photographic Experts Group)
MAC	Verkon varaamisen ja liikennöinnin hoitava osajärjestelmä (engl. Medium access control)
NVD	Yhdysvaltojen hallituksen tietoturvaheikkouksien tietokanta, joka listaa CVE:t (engl. National Vulnerability Database)

SQL	Relaatiotietokannan kyselyiden tekemiseen käytetty standardoitu kieli (engl. Structured Query Language)
SSH	Salattuun tietoliikenteeseen tarkoitettu protokolla, jota käytetään yleisimmin etäyhteyksien muodostamiseen (engl. Secure Shell)
TCP	Kuljetuskerroksen tietokoneiden väliseen luotettavaan tiedonsiirtoon käytettävä protokolla (engl. Transmission control protocol)
UDP	Yksinkertainen tietosähke-pohjainen kuljetuskerroksen protokolla (engl. User Datagram Protocol)
URI	Merkkijono, joka sisältää tietoverkossa sijaitsevan tiedon tunnisteen. Voi sisältää sijainnin, nimen tai molemmat. (engl. Uniform Resource Identifier)
URL	URI:n erikoistapaus, jota käytetään osoittamaan WWW-sivuja (engl. Uniform Resource Locator)

1. JOHDANTO

Esineiden internet (IoT) on laaja verkko toisiinsa Internetin yli yhteydessä olevia laskentaan kykeneviä laitteita. Nykykielessä IoT-laitteiksi ei kuitenkaan lueta esimerkiksi henkilökohtaisia tietokoneita, vaan ennemmin laitteita, joita ei ole aiemmin mielletty olevan yhteydessä Internetiin. Tähän kategoriaan kuuluvia laitteita on esimerkiksi valvontakamerat, älytelevisiot ja älylamput. [1] [p. 2] Vuonna 2016 IDATE DigiWorld julkaisi tutkimuksen, jonka mukaan jo vuonna 2015 maailmassa oli 42 miljardia IoT laitetta ja arvio laitteiden määrä kasvaisi jopa 155 miljardiin vuoteen 2025 mennessä [2]. Statistan arviot olivat huomattavasti maltillisemmat IDATE:n lukuihin verrattuna. Heidän mukaansa vuonna 2019 internettiin yhdistettyjen IoT -laitteiden määrä olisi vuonna 2021 11,28 miljardia ja se kasvaisi vuoteen 2030 mennessä 29,42 miljardiin [3]. Katsoi kumpaa arviota vaan, voidaan todeta, että IoT-laitteiden markkinat ovat laajoja ja sisältävät lukuisia toimijoita.

Laajan markkinan ja kovan hintakilpailun mukana on tullut ongelma IoT-laitteiden tietoturvan heitteillejätöstä. Koska laitteet on pitänyt saada markkinoille mahdollisimman nopeasti ja halvalla, ei ole ollut mikään ihme, että tietoturva on ollut projektien huomiotta jäänyt osa. Hintapaineiden lisäksi IoT-laitteilla on myös muita syitä, miksi tietoturvan toteuttaminen on ollut haastavaa. Laitteiden tekniikka ja ohjelmisto vaihtelevat toisistaan paljon sekä laitteissa voi lisäksi olla henkilökohtaista tietokonetta paljon vähemmän laskentakapasiteettiä sekä muistia.

Hajautetut palvelunestohyökkäykset (DDoS hyökkäykset) nousevat ongelmaksi, kun heikon tietoturvan omaavia laitteita liitetään verkkoon paljon. Tämän työn tarkoituksena on tutkia ja vastata kysymykseen, miten DDoS-kykenevät IoT-laitteisiin kohdistuvat haittaohjelmat ovat kehittyneet viimevuosien aikana. Tutkimusmenetelmänä käytetään teoreettista tutkimusta aiheesta löytyvän kirjallisuuden pohjalta. Aineistoina käytetään niin eri firmojen julkaisemia tutkimustuloksia haittaohjelmista kuin akateemisia julkaisuja.

Luvussa 2 analysoidaan kerätyn aineiston laatua. Luku 3 puolestaan keskittyy Internetiin sekä DDoS-hyökkäyksen taustoihin; miksi DDoS-hyökkäykset ovat mahdollisia, mitä motiiveja hyökkäysten tekijöillä on taustalla, millaisia hyökkäystyyppejä on olemassa sekä lyhyt katsaus mitä toimia palvelun ylläpitäjä voi tehdä hyökkäysten estämiseksi. Tämän jälkeen luku 4 keskittyy siihen, miten IoT-laitteita käytetään osana bottiverkkoa, jolla DDoS-hyökkäyksiä voidaan toteuttaa. Luvussa käydään läpi IoT-laitteen värväys, tartuttaminen

sekä kommunikointi bottiverkossa eli verkon arkkitehtuurimallit. Luvussa 5 käydään nopeasti läpi, mitä toimia IoT-laitteiden suojaamisen eteen on tehty. Luvussa 6 käydään läpi yksittäisiä haittaohjelmia, sekä haittaohjelmien tartuttamien IoT-laitteiden muodostuneita bottiverkkoja, viimeisen kymmenen vuoden ajalta. Työn viimeinen luku kokoaa näistä bottiverkoista sekä haittaohjelmista saadun datan yhteen ja analysoi saatuja tuloksia.

2. TIEDONHANKINTA JA AINEISTO

Tässä luvussa käydään läpi, miten aineisto on haettu työn kirjallisuuskatsaukseen sekä analysoidaan haun tuloksia.

2.1 Aineiston haku

Hakukoneina on käytetty pääasiassa Tampereen yliopiston verkkokirjaston hakua Andoria sekä Googlea. Monesti käytössä oli näiden rinnalla Googlen tieteellisiin artikkeleihin keskittyvä hakukone Google Scholar, jonka tulosten käyttöä jonkun verran rajoitti se, mihin aineistoihin oli pääsy. Mahdollisuuksien mukaan myös haut rajoitettiin vartaisarvioituihin tuloksiin.

Seuraavassa listassa on hakulauseita, mitä käytettiin aineistojen hakemiseen Google Scholar ja Andor hakukoneista:

- ("IoT"OR "Internet of Things") AND "malware"
- ("IoT"OR "Internet of Things") AND "botnet"
- ("DDoS"OR "Distributed Denial of Service") AND "botnet"
- ("DDoS"OR "Distributed Denial of Service") AND "malware"
- "haittaohjelman nimi"AND "botnet"
- "haittaohjelman nimi"AND "malware"
- "haittaohjelman nimi"AND "attack"

"Haittaohjelman nimi"kohdan etsinnöissä korvattiin aina halutun haittaohjelman nimellä, josta tietoa oltiin etsimässä. Haittaohjelmien nimet saatiin ensimmäisten hakulauseiden tuottaessa muutaman vertaisarvioidun artikkelin, jossa oli koostettu aikaisempia IoT botti-verkkoja. Näiden lisäksi Googlesta haettiin hakulauseilla "big IoT botnets", "big IoT botnet attacks"sekä näitä vastaavilla eri muotoa olevilla uutisia, joista löydettiin uudempia botti-verkkoja tarkasteluun.

Aineiston valinnassa on käytetty omaa harkintaa. Tulosten sopivuutta arvioitiin muun muassa lukemalla tiivistelmiä artikkeleista ja arvioimalla liittyykö kyseinen artikkeli työhön. Työtä tehdessä pyrittiin priorisoimaan vertaisarvioituja tieteellisiä artikkeleita, mutta näiden löytyminen oli työn isoin haaste varsinkin uudempien haittaohjelmien kohdalla.

Tämän takia työssä on käytetty paljon firmojen julkaisemia nettiartikkeleita sekä blogipostauksia.

2.2 Aineiston analyysi

Tässä työssä käytetyn aineiston laatu vaihtelee hyvin paljon. Kaikki teoreettinen pohjatieto luvuissa 3 sekä 4 pohjautuu oppikirjoihin, tietokirjoihin sekä vertaisarvioituihin artikkeleihin. Luvun 5 viranomaistoimia etsin Googlen avulla EU:n kyberturvallisuuskeskus ENISAn, EU komission tai Trafikomin sivuilta. Samassa luvussa esitetyt palvelunestohyökkäyksen suojaustoimet etsin ja tiivistin Traficomin ohjeistuksista.

Työn haittaohjelmia ja bottiverkkoja käsittelevä lukuun 6 löydetyn aineiston laatu on hyvin kirjavaa. Osaan isoista vanhemmista bottiverkoista, kuten XorDDoS 6.1, BASHLITE 6.2, Mirai 6.3 sekä Mozi 6.6 löydettiin haittaohjelmista tehtyjä akateemisia tutkimuksia, joista pystyttiin etsimään ainakin suurin osan halutuista tiedosta. Kuitenkin pienimmistä ja uusimmista bottiverkoista tiedot jouduttiin pohjaamaan pitkälti nettiartikkeleihin. Muutamia haittaohjelmia myös tässä vaiheessa jouduttiin hylkäämään tutkimuksesta vähäisen tiedon määrän löytymisen vuoksi. Nettijulkaisuissa priorisoitiin suurien yritysten julkaisemia tutkimustuloksia. Yrityksiä olivat muun muassa IBM, Microsoft, Unit 42 sekä Cloudflare. Näillä on toki omien tuotteiden myynti taustalla julkaisuihin, mutta osaan haittaohjelmien tuloksista löytyi myös useamman eri yrityksen tutkimusten tulosta. Muutamissa tapauksissa jouduttiin ottamaan mukaan myös yksittäisten henkilöiden julkaisemia esimerkiksi Medium alustalla kirjoitettuja blogipostauksia, sillä tieteellisen artikkelin hakukoneet (Andor, Google Scholar) eivät antaneet relevantteja tuloksia yllä esitetyillä hakusanoilla eikä isojen yrityksen tutkimuksia myöskään löydetty. Nämä tapaukset ovat erikseen mainittu tekstissä.

3. INTERNET JA HAJAUTETTU PALVELUNESTOHYÖKKÄYS

Palvelunestohyökkäyksen eli DoS-hyökkäyksen tavoite on pyrkiä estämään hyökkäyskohteena olevan palvelun käyttö sen oikeilta käyttäjiltä. Hajautettu palvelunestohyökkäys eli DDoS-hyökkäys johon tämä työ keskittyy, on palvelunestohyökkäyksen tyyppi, jossa hyökätään koordinoidusti kohdetta kohti käyttäen hyväksi useita laitteita, jolla saadaan hyökkäys toteutettua useasta kohteesta. [4] [5] [6]

Tässä luvussa käydään läpi ensin mitä motivaatioita palvelunestohyökkäysten takana voi olla. Sen jälkeen käydään läpi hieman Internetiä ja miksi palvelunestohyökkäyksien tekeminen on ensinnäkään mahdollista. Kolmantena käydään läpi, millaisia erilaisia tapoja palvelunestohyökkäyksiä on teknisesti tehdä ja syvennytään palvelunestohyökkäyksien yksityiskohtiin. Viimeisenä luvussa käydään läpi, millaisia mahdollisuuksia on estää palvelunestohyökkäys palveluntarjoajan näkökulmasta tai miten pienentää palvelunestohyökkäyksen tapahtumisen todennäköisyyttä.

3.1 Internet

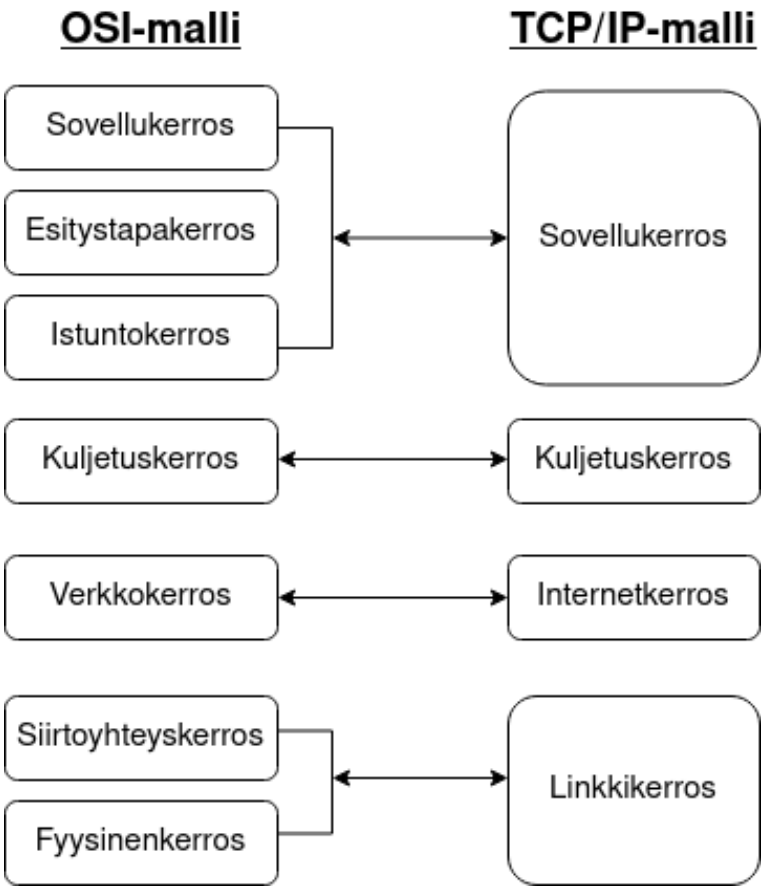
Nykyisen Internetin pohjalla on ajatus, että kahden toimijan välillä saadaan lähetettyä paketteja mihin päin maailmaa tahansa. Internet ei ole itsessään mikään yhdessä paikassa oleva ydin, vaan termi on yleistynyt käyttöön kuvaamaan maailman laajuista yhteyttä, verkkojen verkkoa. Näin Internetillä saadaan muodostettua yhteys kahden missä tahansa päin maailmaa olevan tietokoneen välille. [7] Tässä luvussa käydään läpi OSI- sekä TCP/IP-malli, että puhutaan lyhyesti protokollista.

3.2 OSI-malli ja TCP/IP-malli

OSI-malli (engl. Open System Interconnection model) ja TCP/IP-malli ovat abstrakteja, tietoliikenne viestintää kuvaavia malleja, joiden tarkoitus on auttaa ymmärtämään, miten informaatio liikkuu kahden tietokoneen välillä. OSI-malli sisältää seitsemän kerrosta ja TCP/IP-malli puolestaan neljä, jotka ovat yhdistelmä OSI-mallin kerroksia. Jokainen yksittäinen kerros kommunikoi viereisten kerrostensa kanssa, ja mallin mukaan informaatio liikkuu lähettävältä taholta ylimmästä protokolla kerroksesta alimpaa. Vastaanottavassa

päässä data puolestaan liikkuu alimmasta kerroksesta takaisin ylimpään. [8]

OSI-mallin rinnalla käytetään informaation liikkumisen kuvaamiseen suppeampaa TCP/IP-mallia. TCP/IP-mallissa on yhdistelty OSI-mallin kerrosten määrä seitsemästä neljään: sovelluskerrokseen, kuljetuskerrokseen, internetkerrokseen sekä linkkikerrokseen. [9] [10] Kuva siitä, miten nämä kaksi mallia vertautuvat keskenään löytyy 3.1. Kun tässä työssä viitataan tulevissa luvuissa kerroksiin, missä protokollat sijaitsevat, puhutaan TCP/IP-mallista. Tämä siksi, että sitä käytetään yleisemmin DDoS-hyökkäysten kanssa protokollista puhuttaessa.



Kuva 3.1. *OSI- sekä TCP/IP-malli*

3.2.1 OSI-malli

OSI-mallin kerroksia ovat ylhäältä alaspäin sovelluskerros, esitystapakerros, istuntokerros, kuljetuskerros, verkkokerros, siirtoyhteyskerros sekä fyysinen kerros. Jokainen kerros sisältää omat protokollansa eli standardoidut tavat välittää viestejä. [8] [10]

Fyysinen kerros on OSI-mallin alin kerros, joka sisältää signaalia kuljettavan fyysisen olemuksen. Se sisältää myös tavan, miten fyysisessä maailmassa kuljetettu signaali luetaan laitteelle sopivaan muotoon tai miten laitteen lähettämä signaali muutetaan fyysiseksi ole-

mukseksi, minkä voi lähettää toiselle laitteelle. Fyysisellä kerroksella käytetty yksikkö on bitti. [11]

Siirtoyhteyskerroksen tehtävänä on osoittaa fyysiseltä kerrokselta tuleva data oikeaan osoitteeseen käyttäen laitteiden MAC osoitteita. MAC (engl. Media Access Control) osoite on valmistajien laitteiden verkkosovittimiin lisäämä uniikki tunniste [11]. Siirtoyhteyskerrokselle tuleva data ylemmiltä kerroksilta, muutetaan lähetykseen sopiviin kehyksiin ja näihin lisätään kerroksella tieto siitä, mihin tämä tieto ollaan lähettämässä. Siirtoyhteyskerros tekee myös virhekatselmointia fyysiselle kerrokselle menevään dataan. [8] Protokollia, jotka kuuluvat tähän kerrokseen ovat muun muassa IEEE 802.3 Ethernet sekä IEEE 802.11 WiFi.

Verkkokerroksen tarkoituksena on määritellä paras reitti, millä tieto saadaan kuljetettua kohteesta määränpäähän. Siinä missä siirtoyhteyskerros käytti laitteille yksilöityä MAC osoitetta, verkkokerroksen käyttävät osoitteet tulevat käyttöjärjestelmästä, esimerkkinä tästä on IP-osoite. Kuljetettava data tässä kerroksessa on paketit. Tämän kerroksen protokolliin kuuluu muun muassa IPv4 sekä IPv6. [10] [11]

Kuljetuskerroksen vastuulla on kommunikaatioyhteyden muodostaminen isäntien välillä. Lisäksi kuljetuskerros hallinnoi loogisia portteja, jotka takaavat sen, että tuleva ja lähtevä liikenne kulkee halutulle sovellukselle tai palvelulle laitteen sisällä. Pääprotokollat tällä kerroksella ovat TCP (engl. Transmission Control Protocol) ja UDP (engl. User Datagram Protocol). [11] [8] Näistä protokollista voi lukea lisää luvuissa 3.7.1 ja 3.7.3.

Istuntokerroksen tarkoituksena on hallita käyttöjärjestelmän sisällä istuntoja, mitkä on muodostettu verkon yli ja ovat isäntien välillä. Hallinta sisältää istunnon perustamisen, yhteyden synkronoimisen sekä istunnon tuhoamisen. Protokollia, jotka toimivat tällä kerroksella ovat muun muassa NetBIOS ja SQL. [11] [8]

Esitystapakerros muuntaa dataa haluttuun muotoon joko sovelluskerrokselle tai puolestaan lähetettävään muotoon. Datan muokkaus voi sisältää esimerkiksi koodikonversiota, datan paketointia ja tiedostojen salausta. Tämän kerroksen protokollia ovat muun muassa JPEG ja GIF. [11] [8]

Sovelluskerroksen tarkoitus on kommunioida sovelluksen käyttäjän ja muiden verkkotason protokollien välissä. Sovelluskerros ei siis ole sovellus itse vaan se sisältää protokollat, jotka kuljettavat viestejä järjestelmien välillä. Sen päätavoite on esittää dataa käyttäjän ymmärtämässä muodossa. Näitä protokollia ovat muun muassa HTTP (engl. Hyper Text Transfer Protocol) sekä DNS (engl. Domain Name System). [9]

3.2.2 TCP/IP-malli

TCP/IP-mallissa linkkikerros sisältää samat toiminnot kuin OSI-mallin fyysinen kerros sekä siirtoyhteyskerros. Tämä malli ei kuitenkaan erota näitä kahta omiksi kerroksikseen vaan katsoo niiden olevan samassa tasossa. Toisin sanoen linkkikerroksen tehtävänä on toimittaa internetkerrokselta tulevat paketit oikeaan kohteeseen eikä TCP/IP-mallissa ole OSI-mallin tavoin katsottu tarpeelliseksi jakaa tätä tasoa pienempiin osiin. [10] [12]

Seuraavat kaksi kerrosta TCP/IP-mallissa, internetkerros sekä kuljetuskerros, vertautuvat OSI-mallin vastaaviin ja sisältävät samat protokollat kuin ne. [10]

Sovelluskerros puolestaan TCP/IP-mallissa sisältää kaikki OSI-mallin kolme kerrosta kuljetuskerroksen päällä. TCP/IP-mallissa ajatellaan näiden kaikkien kerroksien tekevän samaa toiminnallisuutta, olemaan datan välittäjänä kuljetuskerroksen ja sovelluksen käyttäjän välissä. Näin ollen sovelluskerroksen tehtävinä TCP/IP-mallissa on istuntojen hallintaa, datan esitysmuodon muokkaamista loppukäyttäjän ymmärrettävään muotoon sekä olemaan rajapintana käyttäjän ja muiden kerrosten välillä. [9] [10]

3.3 Motivaatiot palvelunestohyökkäysten takana

DDoS-hyökkäykset ovat EU-alueella kiristyshaittaohjelmien ohella isoin kyberuhka [13]. Tässä luvussa käsitellään DDoS-hyökkäyksien erilaisia motivaatioita. Enisan vuoden 2022 kyberhyökkäysraportista voi löytää kolme motivaatiota DDoS-hyökkäyksille [14]:

- Taloudellinen
- Ideologinen
- Häiriön aiheuttaminen

Raportissa mainitaan myös, että hyökkäyksien motivaatiot jakautuivat edellä mainittujen alle kohtalaisen tasaisesti [14].

Yksi yleisimmistä syistä tehdä DDoS-hyökkäyksiä on taloudellinen motivaatio. Hyökkääjä, tai hyökkäyksen ostaja, voi pyytää uhriltaan rahaa vastineeksi, joko olla tekemättä DDoS-hyökkäystä tai lopettaa käynnissä oleva DDoS-hyökkäys[15]. Toinen tapa saada taloudellista hyötyä DDoS-hyökkäysten avulla, on ylläpitää niin kutsuttuja DDoS-ostettuna (engl. "DDoS-as-hire") palveluita. Näissä häiriötä haluava henkilö tai taho voi ostaa palvelun ylläpitäjältä korvausta vastaan DDoS-hyökkäyksiä. [13] [16]

Toisena isona motivaationa voidaan mainita ideologiset motiivit. Viimeaikaisista isoista tapahtumista esimerkkeinä Venäjän Ukrainaan kohdistama hyökkäyssota sekä COVID-19 pandemia. Vuonna 2022 Venäjän Ukrainaa kohtaan aloittama hyökkäyssota mullisti DDoS-hyökkäysten käytön sodankäynnin välineenä. Molempien sodan osapuolien palveluihin kohdistui merkittäviä DDoS-hyökkäyksiä. [14] Loppuvuodesta 2022 myös Suomen

Kyberturvallisuuskeskus uutisoi haktivismin eli hakkeroinnin kautta aktivismia tekevien rikollisten ryhmittymien noususta. Varsinkin Killnet niminen järjestö on tehnyt töitä Ukraina mielisiä tahoja kohtaan hyökkäyksiä. Killnet on aiemmin ollut palvelunestohyökkäyksiä myyvä taho. [17] Ideologiset motivaatiot voivat myös sijaita sotien ulkopuolella, kuten jo mainitut COVID-19 pandemian aikana tehdyt hyökkäykset COVID-19 vastaan taistelevia tahoja kohtaan [13].

Kolmantena motiivina on häiriön tuottaminen. Tästä esimerkkeinä voisi mainita bottiverkko Mirain 6.3 tekemän hyökkäyksen Dyn-nimipalveluun tai nettipeleihin kohdistuvat hyökkäykset, joita tekivät muun muassa XorDDoS sekä JenX bottiverkot. XorDDoS sekä JenX bottiverkoista lisää luvuissa 6.1 sekä 6.5. JenX tapauksessa palvelun ylläpitäjällä oli myös taloudellinen motivaatio, sillä kyseessä oli jo edellä mainittu DDoS-ostettuna palvelu. Kuitenkin itse hyökkäyksen tekemisen motivaatio oli muille pelaajille häiriön tuottaminen. Mirain tapauksessa hyökkäysten takana ei ole liikkunut rahaa eikä vieläkään tiedetä syytä, miksi verkon ylläpitäjä teki näin massiivia hyökkäyksiä. Syitä voidaan siis vain spekuloida ja eräinä mahdollisuuksina voidaan pitää esimerkiksi hakkerointiyhteisön kunnioitus tai vallan tunne.

Ideologisen ja häiriöntuottamisen rajalle motiivissaan menevät myös pienempien henkilöryhmien organisoimat DDoS-hyökkäykset. Tästä esimerkiksi voidaan ottaa vuonna 2010 niin kutsuttu "Operation Payback"(suoraan suomennettuna operaatio takaisinmaksu), jossa ryhmä 4chan keskustelukanavan käyttäjiä hallinnoi keskenään DDoS-hyökkäyksen Recording Industry Association of America (RIAA) järjestön sivustoja vastaan. Syynä tähän oli keskustelujen mukaan "The Pirate Bay"sivuston alasajo. "The Pirate Bay"on palvelu, jolta sai laittomasti ladattua tekijänoikeudellisia tiedostoja kuten musiikkia ja elokuvia. Kyseinen hyökkäys tehtiin käyttämällä avoimen lähdekoodin LOIC-nimistä (engl. "Low Orbit Ion Canon") ohjelmaa. Käyttäjät pystyivät lataamaan ohjelman omille laitteilleen ja jaetun ohjeistuksen avulla osallistumaan hyökkäykseen. [18] [19]

3.4 Palvelunestohyökkäyksen tavoite

Tässä luvussa käydään läpi, mitä erilaisia mahdollisuuksia on hyökkääjällä saavuttaa palvelunestohyökkäyksellä kahdesta eri näkökulmasta. Ensin käydään läpi, mitä hyökkäyksellä halutaan saavuttaa uhrin loppukäyttäjän näkökulmasta, onko hyökkäys hävittävä vai alentava. Näiden lyhyen kuvailun jälkeen käydään läpi puolestaan, mitä eri tavoitteita hyökkääjällä voi olla uhrin näkökulmasta. Tästä läpi käydään väsytyshyökkäys (engl. "brute force attack") sekä resurssientyhjentämishyökkäys palvelunestostrategioina.

Hävittävän DDoS -hyökkäyksen tavoite on täysin estää loppukäyttäjiä käyttämästä hyökkäyksen uhrin palveluita. Tänä päivänä käytännössä kaikkien hyökkäyksien lopullisena tavoitteena on hävittävä hyökkäys. Kuitenkin DDoS -hyökkäyksen tavoite voi olla myös palvelun saamisen hidastaminen tai alentaminen tietyllä osuudella. Tällaisien hyökkäyk-

sien huomaaminen voi olla merkittävästi vaikeampaa, mitä kokonaan palvelun käytön estäminen. Vaikka tämän tyylisen hyökkäyksen hetkellinen vaikutus ei olisikaan niin iso kuin täysin palvelun estävä hyökkäys, jos hyökkäys ehtii olla havaitsemattomana tarpeeksi pitkään, voi sen vaikutukset uhrin toiminnalle kuitenkin olla merkittävät. [20]

Väsytyshyökkäyksessä hyökkääjä lähettää uhrille valtavan määrän paketteja, jotka tukkivat tietoliikenneyhteyksiä ja mahdollisesti myös laskennallisia resursseja. Väsytyshyökkäyksiä on karkeasti jaoteltuna kahdenlaisia. Toiset ovat tulvahyökkäyksiä ja toiset vahvistushyökkäyksiä. Tulvahyökkäyksissä valitun protokollan mukaisia paketteja lähetetään niin paljon, että kohteen liikenne tukkeutuu, eikä palveluun tai verkkoon haluttua liikennettä voida erottaa hyökkääjän liikenteestä. Vahvistushyökkäyksessä puolestaan lähetetään uhrille kevyitä kyselyitä, joiden vastaukset ovat raskaita, näin saadaan uhri käyttämään resurssejaan hyökkääjää enemmän. Perusajatus vahvistushyökkäyksessä siis on, että pienellä määrällä resursseja saadaan aikaiseksi enemmän vahinkoa. Molemmat näistä silti kuuluvat väsytyshyökkäyksen alle, sillä ne seuraavat protokollien asettamia sääntöjä. [20]

Resurssientyhjentämishyökkäyksessä hyökkääjä yrittää väärinkäyttää palveluita joko lähettämällä protokollan vastaisia tai viallisia paketteja, väärinkäyttämällä sovellusta itseään tai väärinkäyttämällä protokollia ja tällä tavoin kuluttaa hyökkäyksen uhrin resursseja. [20]

3.5 Palvelunestohyökkäyksen mahdollistajat

DDoS-hyökkäyksen mahdollistaa monen tekijän summa. Näitä ovat Internetin rakenne, sen suojattomuus sekä resurssien rajallisuus.

Pakettien lähettämiseen on sovittu tiettyjä protokollia, jotta kaikki laitteet pystyvät välittämään näitä toisilleen sekä tietävät, mikä laite on mikäkin. Internet ei sisällä itsessään mitään tietoturvaa, koska...

Laitteiden välisen kommunikoinnin sääntöjen noudattaminen on siis kiinni laitteista itsestään. Jos toinen laite ei pidä kiinni sovituista säännöistä tai käyttää hyväksi protokollista löytyviä porsaanreikiä, ei itse Internet voi tätä estää. [21]

Esimerkkinä mahdollisuus käyttää hyväksi protokollia on itse Internet protokolla (IP). Internetin monen muun protokollan paketeissa, esimerkkinä TCP paketeissa oletetaan, että lähettäjän paketeista löytyy lähettäjän IP-osoite. Tämän osoitteen oikeellisuutta ei kuitenkaan mitenkään varmenneta Internetin toimesta, mikä antaa mahdollisuuden IP osoitteiden väärennykselle ja IP:n väärinkäytölle. Tällöin lähettäjä voi lähettää paketteja täysin väärällä IP-osoitteella tai jonkin toisten laitteen osoitteella. Hyökkääjä voi näin suojata itseään ja huonontaa jäljitysmahdollisuuksia tai hyväksikäyttää protokollia, jos palautettava paketti lähetetään uhrille. [20] Protokollien hyödyntämisestä lisää alaluvussa 3.7.

Internetin hallinta on hajautettu. Jokainen sen aliverkko sekä palvelu on vastuussa omasta ylläpidostaan ja lokaalit verkot voivat puolestaan noudattaa omia paikallisia toimintatapojaan. Internetillä ei ole olemassa globaalia turvallisuusmekanismia, joka pätisi samanarvoisesti kaikkialla maailmassa. Tämä ei muutenkaan olisi mahdollista, koska mailla on eri lainsäädännöt koskien esimerkiksi tietoliikennettä. Tästä seuraa se, että verkkojen välisen liikenteen tutkiminen on paikallisten eriävien yksityisyydensuojien vuoksi monesti mahdotonta. [20] [21]

Hyökkäyksten kohdepalveluiden kaista on aina julkisen verkon kaistaa paljon kapeampi. Tämä johtaa siihen, että hyökkääjä voi halutessaan lähettää Internetin yli niin paljon liikennettä, että uhrin kaistalta loppuu leveys kesken ja haluttu liikenne ei pääse enää läpi. Tämä johtuu siitä, että verkkojen kaistat ovat selkeästi isompia kuin loppupalveluiden. [21]

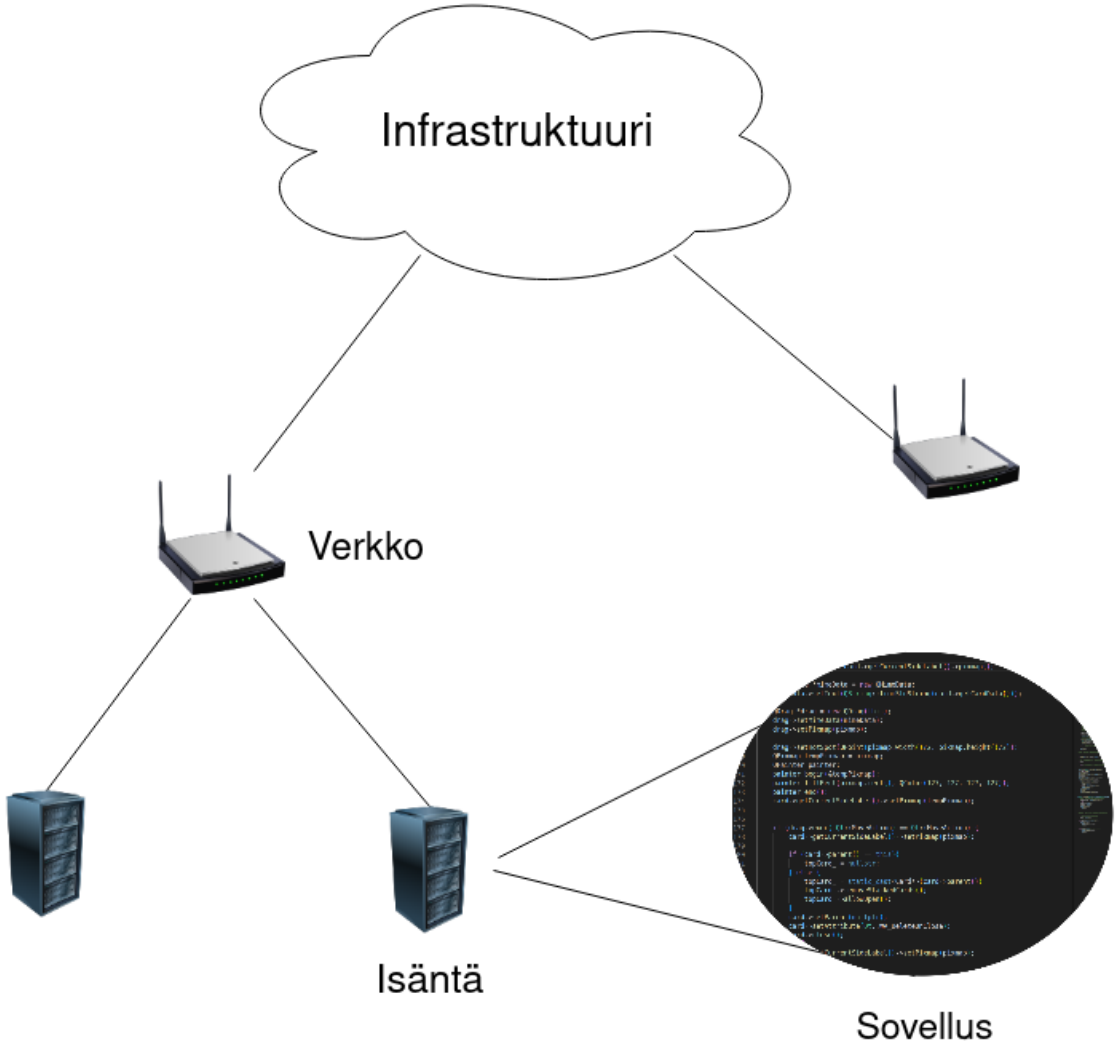
Kaikilla palveluilla on rajallinen määrä resursseja. Kaikilla palvelimilla, isännillä ja verkoilla on olemassa jonkin raja, jonka ylittäessä niiden tehot eivät riitä kattamaan kuormaa. [21] Tästä seuraa se, että jos hyökkääjä saa resursseja omaan käyttöönsä yli uhrin resurssien määrän, saadaan nämä palvelut kaadettua tai vähintään niiden toimintaa hidastettua. [20]

3.6 Palvelunestohyökkäyksen kohde

Hyökkäyksen tyypistä riippuen DDoS-hyökkäys voi kohdistua uhrin palvelun eri osiin; sovellukseen, isäntään, verkkoon tai koko infrastruktuuriin. Kuva palvelun osista löytyy 3.2. Tässä luvussa käydään läpi, mitä eroavaisuuksia hyökkäyksillä on riippuen siitä, mihin kohtaan palvelua hyökkäys kohdistuu. Luvussa mainituista hyökkäyksistä voi löytää lisätietoa luvusta 3.7.

Sovellukseen kohdistuvan hyökkäyksen tavoite on saada yksi tai useampi toiminto sovelluksesta käyttökelvottomaksi oikeilta käyttäjiltä ja mahdollisesti estää tai hidastaa resurssien hakemista isäntäkoneesta. Jos yhteiset resurssit eivät ole täysin estettyjä, ei hyökkäys kohdistu hyökkäyskohdesovelluksen tai toiminnon ulkopuolelle. Sovellukseen kohdistuvat hyökkäykset ovat vaikeita huomata juuri siitä syystä, ettei hyökkäyksellä ole vaikutusta hyökkäyskohteen ulkopuolelle. Hyökkäyksen liikenne ei myöskään ole välttämättä normaalista poikkeavaa, vaikka hyökkäys olisi onnistunut. Lisäksi hyökkäykseen käytettävät paketit ovat käytännössä erottamattomia sallitusta liikenteestä ja erojen huomaamiseen tarvitaan ymmärrystä kohdesovelluksen toiminnasta. Jos kuitenkin erot hyökkääjän aiheuttamassa liikenteessä verrattuna haluttuun liikenteeseen huomataan, ei sovelluksen puolustus ei vaadi merkittäviä määriä resursseja. Esimerkkinä sovellukseen kohdistuvasta hyökkäyksestä voisi olla HTTP tulvahyökkäys, josta voi lukea lisää luvussa 3.7.6. [21]

Isäntään kohdistuva hyökkäyksen tarkoituksena on evätä koko isäntäkoneen käyttö täysin joko ylikuormittamalla, estämällä liikenne tai pakottamalla isäntä uudelleen käynnis-



Kuva 3.2. *Kohdepalvelun osat*

tämään hajoamisen jälkeen. Hyökkäyksen onnistumiseen tarvitaan kuitenkin iso määrä paketteja sekä liikennettä, jonka huomaaminen on kohtuullisen helppoa. Isäntä ei kuitenkaan pysty yksin estämään itseensä kohdistuvaa hyökkäystä vaan tarvitsee avukseen esimerkiksi palomuurin kaltaisen järjestelmän. [21]

Verkkoon kohdistuvat hyökkäykset ovat puhtaasti verkkoliikenteen määrän tason, eikä niinkään sisällön hyväksikäytön hyökkäyksiä. Verkkoon kohdistuvissa hyökkäyksissä yritetään tukkia kaistaa uhriin kohdistuvalla pakettimassalla ja ne ovat tästä syystä helposti huomattavia hyökkäyksiä. Estääkseen verkkoon kohdistuvat hyökkäykset, uhrin täytyy kuitenkin pyytää apua ylemmältä tasolta, sillä se ei itse kykene hallitsemaan pakettimäärää. [21]

Infrastruktuuriin kohdistuvissa hyökkäyksissä kohde on mikä tahansa hajautettu palvelu. Nämä palvelut ovat tärkeitä joko globaaleille Internet operaatioille tai aliverkon operaatioille. Esimerkkeinä näistä hyökkäyksistä ovat ne, jotka kohdistuvat Internetin nimipalve-

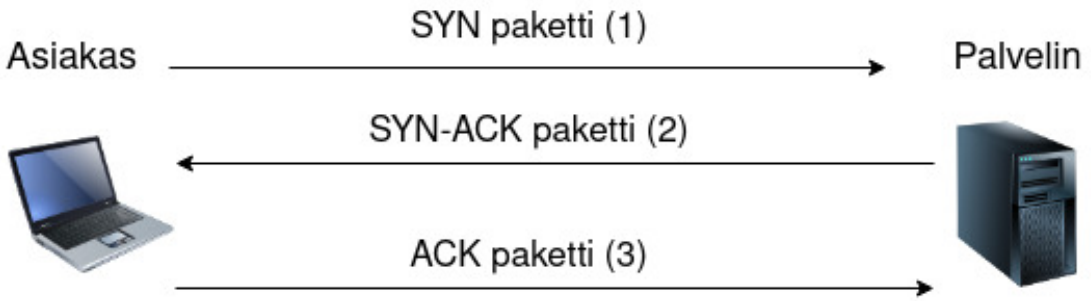
luihin, sertifikaatti palveluihin, isoihin ydin reitittimiin ja muihin vastaaviin monen palvelun käytössä oleviin järjestelmiin. Erilaista muiden osa-alueiden hyökkäyksiin on tässä se, että hyökkääjän pitää yhtäaikaisesti hyökätä useihin kohteisiin, missä uhrin palveluita ylläpidetään, jotta hyökkäykset saadaan onnistumaan. [21] Tästä esimerkkinä on osa Mirain 6.3 tekemiä iskuja vuonna 2016, joista yksi kohdistui nimipalveluun nimeltään Dyn ja se aiheutti vahinkoa useille suurille palveluntarjoajille, joihin kuuluu muun muassa Netflix, Github, Reddit ja Visa. [20]

3.7 Protokollien hyödyntäminen

Tässä luvussa käydään läpi, miten erilaisia protokollia hyödynnetään erilaisia DDoS-hyökkäyksiä tehdessä.

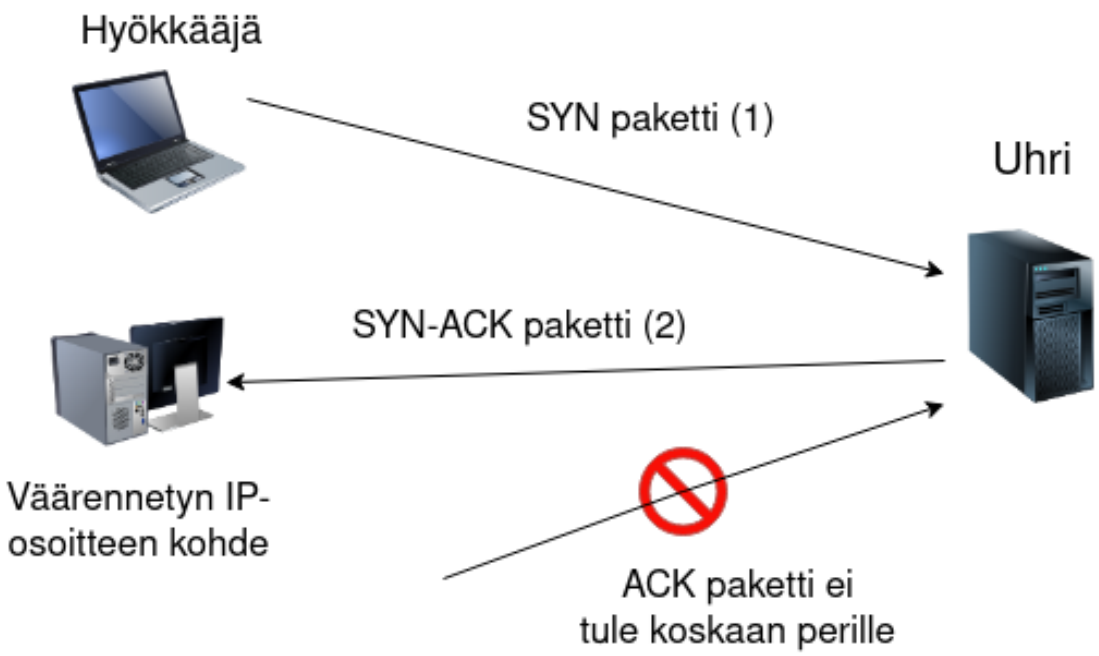
3.7.1 TCP SYN-ACK

TCP SYN-ACK-protokolla on osa TCP-yhteyden muodostamisen vaihetta, jossa kolminkertainen kättely mahdollistaa luotettavan yhteyden syntymisen. TCP protokolla sijoittuu TCP/IP-mallissa 3.2.2 kuljetuskerrokselle. Kuva oikeaoppisesta kättelyprotokollasta on 3.3. Kättely aloitetaan, kun asiakas lähettää SYN-paketin palvelimelle. Palvelin vastaa SYN-ACK-paketilla, joka kertoo vastaanottaneensa asiakkaan pyynnön ja ilmoittaa valmiudesta vastaanottaa tiedonsiirtoa. Lopuksi asiakas vahvistaa yhteyden lähettämällä ACK-paketin palvelimelle, jolloin yhteys on luotu onnistuneesti. [22] [23]



Kuva 3.3. *TCP kättely*

TCP SYN-tulvahyökkäyksessä hyökkääjä lähettää valtavan määrän SYN-paketteja palvelimelle. Näissä paketeissa hyökkääjä käyttää väärennettyjä IP-osoitteita, jotta hyökkäyksen lähde näyttää tulevan eri lähteistä. Palvelin vastaa jokaiseen SYN-pakettiin SYN-ACK-paketilla normaalisti, odottaen ACK-pakettia yhteyden vahvistamiseksi. Väärennetyn IP-osoitteen takia ACK paketti jää kuitenkin lähettämättä, jolloin palvelimen resurssit sitoutuvat odottamaan vahvistusta yhteydelle, jota ei koskaan tapahdu. Tämä johtaa siihen, että palvelin käyttää resurssejaan ylläpitämällä avoimia, odottavia yhteyksiä, mikä puolestaan estää tai hidastaa palvelun oikeita käyttäjiä saamasta muodostettua yhteyksiä. Mallin tästä hyökkäyksestä näkee kuvassa 3.4 [22] [23]



Kuva 3.4. *TCP tulvahyökkäys*

3.7.2 TCP PSH-ACK

TCP protokollassa paketit, jotka lähetetään kohteelle, on puskuroitu TCP pinon sisällä, eikä paketteja lähetetä vastaanottajalle ennen kuin puskuri tulee täyteen. Kuitenkin kutsun lähettäjä voi pyytää vastaanottavaa systeemiä purkamaan puskurin sisällön jo ennen kuin se täyttyy kokonaan käyttämällä PSH lippua. [24]

PUSH ja ACK hyökkäyksessä kohteelle lähetetään TCP paketteja PSH ja ACK lippujen kanssa. Lippujen tarkoitus on purkaa kohteen kaikki data TCP puskurilta, riippumatta siitä kuinka täynnä puskuri oikeasti on. Puskurin purkamisen jälkeen ACK paketti ilmoittaa hyökkääjälle (tai väärälle IP osoitteelle hyökkäystarkoituksessa tehdyssä kutsussa), että kaikki data on onnistuneesti ladattu. Kun paljon vastaavia kutsuja lähetetään samanaikaisesti tai lähellä toisiaan, saadaan käytettyä suuria määriä uhrin resursseja. Hyökkäyksen onnistuessa kohdelaite kaatuu.

PUSH ja ACK hyökkäys on tyypiltään resurssientyhjentämishyökkäys. [20] [24]

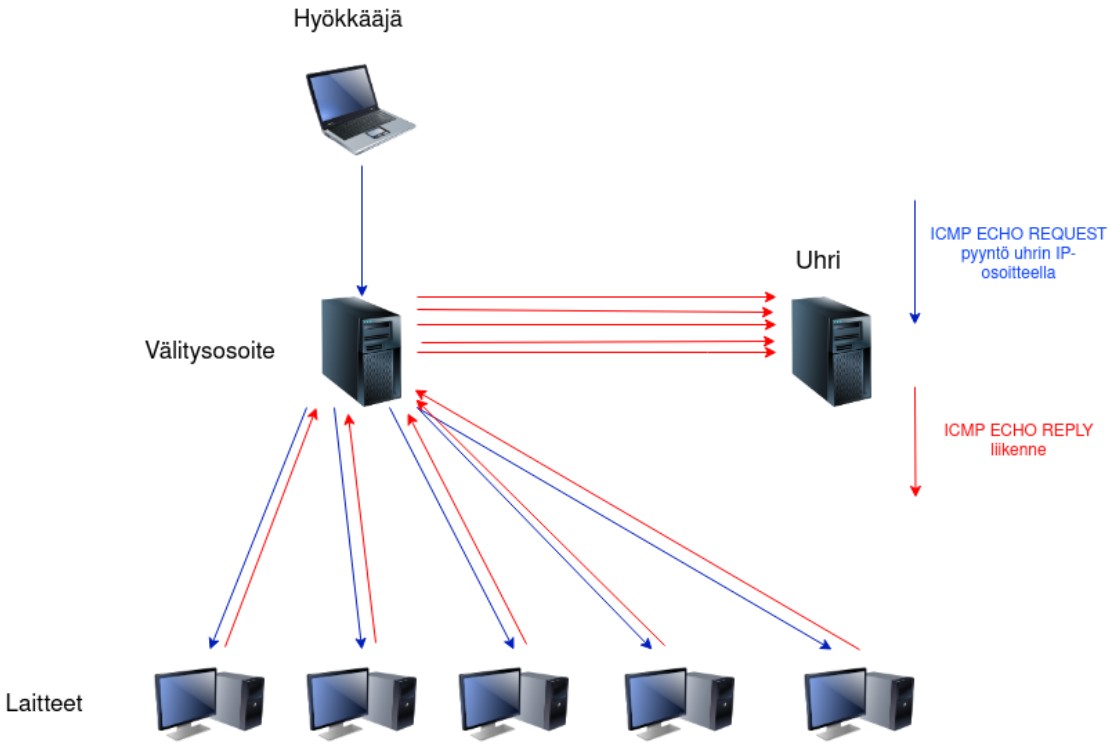
3.7.3 UDP

UDP (engl. User Datagram Protocol) tulvahyökkäyksessä kohde lähettää UDP paketteja väärennetyillä lähettäjän IP osoitteella kohteelle, johonkin kohteen porttiin. Oikein toimitussa protokollassa UDP protokollassa kohde tarkastaa onko kyseisessä portissa sovellusta pyörimässä ja jos sovellusta ei ole pyörimässä uhri lähettää ICPM (engl. Internet Control Message Protocol, puhekielessä käytetään myös termiä "ping") paketin lähettä-

jän toimittamaan IP osoitteeseen. TCP protokollan tavoin UDP sijoittuu TCP/IP-mallissa 3.2.2 kuljetuskerrokseen. Yleensä hyökkäystilanteissa IP osoite on väärennetty, mutta toisin kuin TCP SYN-ACK protokollassa, väärennetyllä IP osoitteella ei ole roolia itse hyökkäyksen toteutuksessa. Väärennetyn IP osoitteen merkitys on kutsun lähettäjän identiteetin piilottaminen. Jos hyökkääjä lähettää paljon vastaavia paketteja kohteelle, tämä kuormittaa kaistaa, ja vie resursseja oikeilta käyttäjiltä. UDP tulvahyökkäys kuuluu luokituksessaan kaistanestohyökkäykseen. [20] [25] [26]

3.7.4 ICMP

ICMP tulvahyökkäys on monin tavoin samaa kaavaa noudattava kuin UDP tulvahyökkäys. ICMP protokolla kuitenkin sijoittuu TCP/IP-mallissa 3.2.2 verkkokerrokselle, TCP sekä UDP protokollista poiketen. ICMP tulvahyökkäyksessä kohteelle lähetetään ICMP ECHO REQUEST paketteja, tuttavallisemmin puhutaan myös "ping"kutsuista. Kutsuja lähetetään niin paljon, että kaikkiin niihin vastaaminen tukkii uhrin laskenta yksikköä, kun lukuisia kutsuja joudutaan käsittelemään. [20]



Kuva 3.5. *Smurf-hyökkäys*

ICMP protokollaa hyödyntävä vaarallisempi versio on niin kutsuttu smurf-hyökkäys (engl. Smurf-attack). Smurf-hyökkäyksessä ICMP ECHO REQUEST kutsuja lähetetään välitysosoitteeseen (engl. broadcast addresses) eli osoitteeseen, joka yhdistää useita laitteita samassa osoitteessa. Kutsu sisältäen uhrin IP-osoitteen, johon kaikki välitysosoitteessa olevat laitteet puolestaan lähettää vastauksensa. Jos lähetettyjen kutsujen määrä on n ja

välitysosoitteessa kiinni olevien laitteiden määrä m saadaan vastausten määräksi $n * m$, jolloin saadaan hyödynnettyä smurf-hyökkäyksessä monistumista. Vastaavanlaista monistumista UDP tulvahyökkäyksen kanssa kutsutaan nimellä murtumishyökkäys. [27]

3.7.5 DNS

Nimipalvelujärjestelmä (DNS engl. Domain Name System) tulvahyökkäyksessä hyökkääjä lähettää hyvin paljon huijattuja IP osoitteita sisältäviä DNS paketteja kohteelle. DNS on kriittinen TCP/IP-mallissa 3.2.2 sovelluskerrokseen sijoittuva Internetin palvelu, jossa käyttäjä pyytää kohteen IP osoitetta nettiosoitteesta. Koska kohteen on vaikea sanoa, mitkä näistä paketeista on oikeaa haluttua liikennettä ja mitkä hyökkäystä, se yrittää vastata kaikkiin tuleviin paketteihin. Hyökkääjän epätoivottu liikenne ruuhkauttaa DNS palvelimen resursseja, jolloin oikealle liikenteelle on vain vähän tai ei ollenkaan resursseja. [20] [28] [29]

DNS vahvistushyökkäys (engl. DNS amplification attack) eroaa DNS tulvahyökkäyksestä siten, että sen tarkoitus on ruuhkauttaa resurssien sijaan tiedonsiirtokaistaa. Koska pieni DNS kysely voi aiheuttaa merkittävästi isomman DNS vastauksen, DNS vahvistushyökkäys tarvitsee vähemmän laskennallisia resursseja hyökkääjän puolelta. [20] [29]

3.7.6 HTTP

Hypertekstin siirtoprotokolla (HTTP, engl. HyperText Transfer Protocol) tulvahyökkäyksessä HTTP paketteja lähetetään suuri määrä uhrille, jonka tarkoitus on ruuhkauttaa liikennettä. HTTP protokolla on DNS tavoin TCP/IP-mallissa 3.2.2 sovelluskerrokselle sijoittuva protokolla ja tämän vuoksi hajautetun HTTP tulvahyökkäyksen aikana on hyvin vaikeaa erottaa palveluun toivottua liikennettä haitallisesta ja turhaan kuormittavasta. Hyökkääjä voi halutessaan maksimoida hyökkäyksen tehoa tekemällä isoja data kyselyitä, esimerkiksi ladata kuvia sivustolta. Tällainen epätoivottu liikenne voidaan kuitenkin erinäisillä toimilla estää sivustolta. Hyökkääjä voi pienentää havaitsemisen mahdollisuutta hyödyntäen HTTP kutsuissa vastauksena tulevia sivuja. Esimerkiksi sivustoista voidaan poimia linkkejä, joihin seuraavat HTTP kutsut tehdään. Näin saadaan rekursiivisesti lähetettyä useita kutsuja eri sivuston osiin siten, että liikenne näyttää mahdollisimman paljon normaalin sivuston käyttäjän toiminnalta. [20] [30]

3.8 Palvelunestohyökkäysten estäminen

On olemassa paljon erilaisia tapoja estää DDoS-hyökkäyksiä palveluntarjoajan roolissa. Kuten aikaisemmin on todettu, osaa hyökkäyksistä on vaikeaa tai lähes mahdotonta estää täysin. Useisiin edellisessä luvussa esitettyihin hyökkäyksiin on myös tutkittu ja löydetty erityisiä havaitsemis- ja puolustautumismekanismejä juuri kyseistä hyökkäystyyppiä vas-

taan. Koska tämä työ ei kuitenkaan keskity pelkästään DDoS-hyökkäysten estämiseen, käydään luvussa pintapuolisesti läpi toimia, joilla hyökkäyksiä voidaan estää tai niiden uhkaa voidaan minimoida. Luvun tiedot on kerätty käyttäen lähteenä Suomen Kyberturvallisuuskeskuksen julkaisemaa palvelunestohyökkäysten ehkäisyä- ja torjuntaa käsittelemää ohjeistusta [31].

Reverse-proxy- tai välimuistiratkaisulla vältetään turhia rinnakkaisia sivunlatauksia. Myöskin järjestelmien resurssien huomattava ylimitoitus on toinen tapa ehkäistä palvelun ylikuormittumista. [31]

Voi olla myös järkevää hajauttaa palvelut eri paikkoihin niin, että jos yhteen, esimerkiksi asiakkaille näkyvään verkkosivuun hyökätään, ei sisäiset palvelut ole alhaalla. Näin saadaan minimoitua vahinkoja, vaikkei niitä täysin estettäisikään. Todella isot palveluntarjoajat saattavat myös haluta hajauttaa samalla tavalla kaikki verkkopalvelunsa niin, että samalla nimellä löytyvät palvelut pyörivät useassa IP-osoitteessa samanaikaisesti. Näin yhden IP-osoitteen takana olevan palvelun kaataminen ei kokonaan estä palvelun käyttöä vaan ainoastaan hidastaan. [31]

Suomessa voi myös toimia tietyissä palveluissa liikenteen suodattaminen IP-osoitteen maantieteellisen sijainnin perusteella. Kuten tässäkin työssä tullaan huomaamaan luvussa 6 bottiverkoilla on yleensä suurin osa boteista Suomen, ja itse asiassa koko Euroopan, ulkopuolella. Suodatusta voi myös tehdä protokollan vastaisen liikenteen suodattamisella esimerkiksi, jos paketit ovat liian isoja tai niissä on ylimääräisiä kenttiä. Tämä kuitenkin tarvitsee verkko- tai sovellusliikenteen suodattamiseen kykeneviä laitteita esimerkiksi palomuureja, joilta löytyy kyseiset ominaisuudet. [31]

Hyökkäystilanteen tunnistaminen ja siihen nopea reagointi edellyttää tietoliikenteen valvontaa. Valvonta ei toki estä palvelunestohyökkäyksiä, mutta minimoi hyökkäystilanteessa vahingot. [31]

4. IOT-LAITE OSANA TOTEUTETTAVAA HYÖKKÄYSTÄ

IoT-laitteet ovat olleen jatkuvasti kasvava teknologiateollisuuden ala. Eri tahoilla on kuitenkin vaihteleva käsitys, mikä laitteet kuuluvat IoT käsitteen alle. IBM määritelmä IoT:sta on seuraava: verkko fyysisiä laitteita, ajoneuvoja, kodinkoneita ja muita fyysisiä kohteita, joihin on sulautettu antureita, ohjelmistoa sekä verkkoyhteys ja niiden on sallittu kerätä sekä jakaa dataa [32]. Tällöin on tulkinnanvaraista, kuuluuko esimerkiksi WLAN-tukiasema IoT-määritelmän alle, sillä se on fyysinen laite, joka on merkittävä osa IoT-kokonaisuutta liittäen monia laitteita laajempaan verkkoon.

IoT-markkinat on kilpailtu ala, jolla liikkuu paljon rahaa. Vuonna 2016 IDATE DigiWorld julkaisi tutkimuksen, jonka mukaan jo vuonna 2015 maailmassa oli 42 miljardia IoT-laitetta ja arvio laitteiden määrä kasvaisi jopa 155 miljardiin vuoteen 2025 mennessä [2]. Statistan 2019 tehdyn arvioiden mukaan Internettiin yhdistettyjen IoT-laitteiden määrä olisi vuonna 2021 11,28 miljardia ja se kasvaisi vuoteen 2030 mennessä 29,42 miljardiin [3]. IoT-teknologioiden nopea kehittyminen, kilpailtu markkina sekä halu muuttaa kaikki laitteet älykkääksi teknologiasti, on johtanut tilanteeseen, jossa verkossa on kiinni valtava määrä huonosti suojattuja laitteita. Näiden laitteiden liittäminen haittaohjelmilla niin kutsuttuihin bottiverkkoihin ja bottiverkkojen hyödyntäminen esimerkiksi tässä työssä käsiteltävissä DDoS-hyökkäyksissä, on muodostunut paljon käytetyksi tavaksi tehdä kyberrikoksia. [20]

Bottiverkkoja hyödyntävän DDoS-hyökkäyksen voi jakaa karkeasti neljään eri vaiheeseen: värväykseen, tartuttamiseen, kommunikointiin ja hyökkäykseen. [20] Tässä luvussa käsitellään värväys 4.1, tartuttaminen 4.2 sekä kommunikointi 4.3. Bottiverkon hyökkäysvaihe ei itsessään eroa DDoS-hyökkäyksistä mitenkään muuten, kuin että bottiverkkoa käytetään tahona, joka tuo hajautuksen hyökkääjän haluamalle palvelunestohyökkäykselle. Hyökkäysvaihe itsessään on sen verran iso kokonaisuus, että DDoS-hyökkäyksille on tässä työssä omistettu kokonaan oma lukunsa 3.

4.1 IoT-laitteiden värväys

Erilaiset IoT-laitteiden skannausstrategiat liittyvät tiiviisti yhteen bottiverkkojen levittämisen kanssa. IoT-laitteiden värväys bottiverkkoihin tehdään nykyään lähes aina joko automaattisen tai semiautomaattisen skannauksen voimin. Skannausstrategian tavoitteena on etsiä ja löytää laitteet, joilla on potentiaalia tulla liitetyksi bottiverkkoon eli ne sisältävät

haavoittuvuuksia, joita kyseinen bottiverkko hyväksikäyttää verkkoon liittämiseen.

Skannausstrategia voi olla joko automaattinen, semiautomaattinen tai manuaalinen. Usein hyökkääjät yhdistelevät monia skannaus strategioita ennemmin kuin keskittyvät yhteen, joka kasvattaa hyökkäyksien laajuutta. Automaattisessa skannauksessa bottiverkko hoitaa skannauksen ilman ihmisen ohjausta tai jatkuvaa valvontaa, kun taas manuaalisessa strategiassa hyökkääjä on etsimässä itse haavoittuvia laitteita esimerkiksi hakukoneiden avulla. Nykyään suurin osa bottiverkoihin liitettävistä laitteista etsitään automaattisesti, koska näin tavoitetaan suurempia määriä laitteita. Tässä luvussa käydään läpi erilaisia skannausstrategioita keskittyen automaattisiin ja semiautomaattisiin, aikaisemmin mainitusta syystä johtuen.

4.1.1 Satunnainen skannaus

Satunnaisessa skannauksessa hyökkääjä koittaa rekrytoida eri satunnaisesti valittujen IP-osoitteiden kohteissa olevia uhreja. Valinnassa jokainen verkon skannaava isäntä (esimerkiksi jo verkkoon liitetty botti tai ohjauspalvelin) käyttää eri siemenlukua, jolla arvotaan satunnainen IP-osoite. Tästä osoitteesta testataan, onko se laite, jolta löytyy haluttuja haavoittuvuuksia, jotka tekevät laitteesta sellaisen, että se voidaan liittää osaksi verkkoa. Satunnainen skannaus kuitenkin aiheuttaa paljon liikennettä, koska samasta laitteesta tulevat skannauksen kohteet ovat todennäköisesti eri verkoissa. Koska arvottavat IP-osoitteet ovat satunnaisia, voi tässä strategiassa tulla tilanne, että useampi skannaava isäntä tekee hyökkäystä samaan laitteeseen. Liikenteen suuri määrä voi myös johtaa verkon paljastumiseen. Satunnainen skannaus ei ole kovin tehokas tapa löytää uusia laitteita. [21]

4.1.2 Hyökkäyslista skannaus

Hyökkäyslista on skannausstrategia, jossa bottiverkko käy valmista IP-osoitelistaa uhreista järjestelmällisesti läpi. Kun haavoittuva laite on löydetty, lähetetään osa jäljellä olevasta listasta tälle uudelle bottiverkkoon liitetylle laitteelle, jolloin se voi jatkaa bottiverkon kasvattamista omalta osaltaan. Hyökkäyslistan hyviä puolia on nopea verkon kasvattaminen eikä yhteentörmäyksiä tapahdu, koska laitteilla on selkeät omat kohteensa. Huonoina puolina on se, että lista uhreista pitää olla etukäteen valmiina. IP-osoitteita pitää löytää huomaamattomista lähteistä, kuten haavoittuvia osoitteita ja aukinaisia portteja jakavista Internet-sivustoista tai tekemällä skannauksia itse, joka puolestaan vie paljon aikaa ja on työlästä. Toinen huono puoli on, että jos hyökkäyslista on pitkä, se aiheuttaa paljon liikennettä, joka voi altistaa paljastumiselle. Jos taas lista on liian lyhyt, ei bottiverkosta kasva kovin suurta. [21]

4.1.3 Muunnelmaskannaus

Muunnelmaskannaus on pseudo-satunnainen skannaus strategia. Se käyttää pohjana rajattua hyökkäyslistaa, josta skannaus aloitetaan. Kun listalta löydetään laite, joka saadaan tartutettua, tämä laite alkaa skannaamaan läpi oman IP-osoitteensa muunnelmia. Jos käy niin, että laite löytää jo tartutetun laitteen, se valitsee uuden satunnaisen IP-osoitteen, mistä lähtee jatkamaan. [21]

Tartutettu laite aloittaa skannauksen aina satunnaisesta muunnelmasta. Tämä skannaus strategia saa hyötyjä sen satunnaisuudesta eli kattaa laajan määrän eri IP-osoitteita, mutta pysyy silti jollain tasolla koordinoidumpana ja kokonaisvaltaisempana entä puhdas satunnainen skannaus, koska muunnelmissa käytetään pohjalla eri IP-osoitteita. [21]

4.1.4 Paikallisen aliverkon skannaus

Paikallisen aliverkon skannauksen voi lisätä mihin tahansa yllä olevaan skannausstrategiaan mukaan. Kun on löydetty haavoittuva kohde, käydään läpi kaikki muutkin osoitteet, jotka ovat liitettynä samaan aliverkkoon. Näiden osoitteiden laitteet yritetään myös tartuttaa. [21]

4.1.5 Kalastelu

Bottiverkkoja voidaan kasvattaa myös niin kutsutun kalastelun (engl. phishing) avulla. Siinä hyökkääjä lähettää laitteelle, jolla käyttäjä pystyy avaamaan sähköpostin, tekstiviestin tai muun kommunikaatiosovelluksen, johon hyökkääjä lähettää viestin. Tämä viesti voi sisältää linkin, jota painamalla uhrin käyttämälle laitteelle asennetaan automaattisesti haittaohjelma, jolla laite liitetään bottiverkkoon. Tästä strategiasta esimerkkinä voidaan pitää vuodesta 2007 vuoteen 2009 välillä haitannutta Zeus nimistä bottiverkkoa, joka levittäytyi kalastelun avulla. Zeus oli haittaohjelma, jonka tarkoitus oli kalastella muun muassa ihmisten pankkitunnuksia, kun koneille asennetut haittaohjelmat keräsivät laitteilta kirjautumistietoja ja lähettivät ne hyökkääjälle. Zeuksen arvellaan levinneen 3.6 miljoonaan Windows koneeseen. [33] [34]

Tässä työssä käsiteltävät IoT-laitteista muodostetut bottiverkot eivät käytä kasvamiseensa kalastelua. Bottiverkkojen perinteisesti käyttämät IoT-laitteet kuten kamerat ja digitaaliset videonauhurit eivät sisällä kalastelun hyödyntämiä ominaisuuksia, kuten laitteen kautta sähköpostin lukemista. On kuitenkin hyvä tunnistaa, että tämä on eräs bottiverkkojen kasvattamiseen käytettävä tapa, jota käytetään varsinkin verkoissa, jotka koostuvat mobiililaitteista tai henkilökohtaisista tietokoneista.

4.2 IoT-laitteen tartuttaminen

IoT-laitteen tartuttamisvaihetta voidaan pitää myös IoT-laitteeseen kohdistuvana hyökkäyksenä.

Jos mietitään bottiverkon kasvattamista, ovat IoT-laitteet, bottiverkkoyhteydessä kutsutut botit, niin sanottuja toissijaisia uhreja. IoT-laitteeseen kohdistuva hyökkäys ei kuitenkaan tarkoita sitä, että hyökkääjä itse olisi tekemässä jokaista hyökkäystä manuaalisesti. Jotta bottiverkoista saadaan tarpeeksi iso, nykyään hyökkäykset lähes poikkeuksetta tapahtuvat automaattisesti joko ohjauspalvelimen tai verkon muiden bottien toimesta.

4.2.1 Sanakirjahyökkäys

Yleinen tartuttamistapa haittaohjelmilla on sanakirjahyökkäykset. Sanakirjahyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkäävä taho käy läpi listassa olevia kirjautumistietoja hyökättävän IoT-laitteen kirjautumisjärjestelmää vastaan esimerkiksi telnet tai SSH-yhteyden kautta ja yrittää saada pääkäyttäjäoikeudet tällä tavoin. Listan kirjautumistiedot voivat olla esimerkiksi oletussalasana ja -käyttäjätunnus pareja laitteille tai muuten yleisesti käytössä olevia kirjautumistietoja. [35]

Tästä muokattu versio on painotettu sanakirjaversio, missä hyökkääjällä on painotettu kirjautumistunnus lista, jossa tunnukset on jaettu alakategorioihin. Hyökkäyksen aikana valitaan satunnaisesti yksi näistä alakategorioista, joka käydään läpi. Tämä tartuttamistyyli vähentää hyökkäämisen onnistumisen todennäköistä, mutta nostaa tartutettavien laitteiden skannausnopeutta. [35]

4.2.2 Yleisten haavoittuvuuksien käyttö

Toisena isompana tartuttamiskokonaisuutena on CVE eli yleisten haavoittuvuuksien luettelon (engl. Common Vulnerability Enumeration) käyttö laitteiden tartuttamisessa. CVE:n käyttö laitteiden tartuttamisessa on sanakirjahyökkäystä tehokkaampi tapa hyökätä uhreihin, mutta on myös vaikeampi toteuttaa. [35]

Kaikki löydetyt CVE:t voi löytää NVD:stä eli Yhdysvaltojen kansallisesta haavoittuvuus tietokannasta (engl. National Vulnerability Database), josta haavoittuvuuksia voi selata ja etsiä vapaasti. [36]

Luokka	Nimi	Kuvaus
CWE-20	Sopimatonta syötteen validointia	Tuotteella on syötteitä, jotka joko jätetään validoimatta, niille tehdään vääriä tai vajaita validointeja
CWE-22	Sopimattomia rajoitteita hakemistopolun rajoitettuun hakemistoon	Tuote käyttää ulkopuolelta hallittavaa syötettä tiedostopolun luomiseen tilanteessa, jossa tiedosto tai kansio on rajoitetun vanhemman alla, mutta ei tee tarvittavia neutralisointeja tietyille elementeille tiedostonimessä. Tämä voi johtaa tiedostonimen muokkaantumiseen niin, että hyökkääjä pääsee sille tarkoitetun tiedostopolun ulkopuolelle.
CWE-74	Sopimatonta tulosteen neutralisointia (’Injektio’)	Tuote luo kaikki tai osan komennosta, datarakenteet tai tallenteet käyttäen ulkoa ohjattavaa syötettä, mutta ei neutralisoi tai neutralisoi väärin tietyt elementit, jotka voisivat muokata sitä, kuinka se on rakennettu tai tulkitaan kun se on lähetetty komponentille
CWE-77	Erikoiselementtien sopimationta neutralisointia komento käytössä (’Komentoinjektio’)	Tuote luo kaikki tai osan komennosta käyttäen ulkopuolelta vaikutettavaa syötettä, mutta ei neutralisoi tai neutralisoi väärin tietyt elementit, jotka voi muokata haluttua komentoa, kun se lähetetään ajoon.
CWE-78	Erikoiselementtien sopimatonta neutralisointia käyttöjärjestelmän komennoissa (’Käyttöjärjestelmän komentoinjektio’)	Tuote luo kaikki tai osan käyttöjärjestelmä komennosta käyttäen ulkopuolelta vaikutettavaa syötettä, mutta ei neutralisoi tai neutralisoi väärin tietyt elementit, jotka voi muokata haluttua käyttöjärjestelmäkomentoa, kun lähetetään ajoon.
CWE-79	Sopimaton sisääntulon neutralisointia nettisivulla (’Cross site scripting’)	Tuote ei neutralisoi tai väärin neutralisoi käyttäjän kontrolloimaa syötettä ennen kuin se laitetaan tulosteeseen, jota käytetään nettisivulla ja joka on muiden käyttäjien käytössä.
CWE-89	SQL komentojen käytössä olevien sisääntulojen sopimatonta neutralisointia (’SQL injektio’)	Tuote luo kaikki tai osan SQL komennosta käyttäen ulkopuolelta hallittavaa syötettä, mutta ei neutralisoi tai neutralisoi väärin tiettyjä elementtejä, jotka voi muokata haluttua SQL komentoa, kun se lähetetään ajoon.
CWE-94	Koodin tuottamisen sopimatonta valvontaa (’Koodi injektio’)	Tuote luo kaikki tai osan koodisegmentistä käyttäen ulkopuolelta vaikutettavaa syötettä, mutta ei neutralisoi tai neutralisoi väärin tietyt elementit, jotka voivat muokata syntaksia tai koodisegmentin haluttua käyttäytymistä.

Jatkuu seuraavalle sivulle

Taulukko 4.1. *Haittaohjelmien levittämisessä käytettävät haavoittuvuus-luokat*

Jatkoa edelliseltä sivulta

Luokka	Nimi	Kuvaus
CWE-119	Sopimattomia rajoitteita operaatioihin, jotka liittyvät muistipuskuriin	Tuote suorittaa operaatioita muistipuskuriin, mutta se voi lukea tai kirjoittaa muistipaikkaan, joka on puskurille tarkoitettujen rajojen ulkopuolella.
CWE-122	Pinopohjaisen muistipuskurin ylivuoto	Pinon ylivuoto on puskurin ylivuoto, jossa puskuri, joka voidaan ylikirjoittaa on allokoitu pino-osaan muistia, yleisesti tarkoitettu puskuri on allokoitu käyttäen malloc() kaltaista rutiinia.
CWE-134	Ulkopuolella muotoillun merkkijonon käyttö	Tuote käyttää funktioita, jota hyväksyvät muotoillun merkkijonon muuttujana, mutta muotoiltu merkkijono tulee ulkopuoliselta lähteeltä.
CWE-284	Sopimaton pääsyn valvonta	Tuote ei rajoita tai rajoittaa väärin pääsyä resursseihin luvattomalta käyttäjältä.
CWE-287	Sopimaton autentikointi	Kun käyttäjä väittää antaneensa identiteetin, tuote ei todista tai todistaa riittämättömästi onko tämä väite totta.
CWE-306	Puuttuva autentikointi kriittisille funktioille	Tuote ei suorita autentikointia toiminnallisuuksille, jotka vaativat todistettavaa käyttäjä identiteettiä tai käyttää merkittävän määrän resursseja.
CWE-352	Cross-site request forgery (CSRF)	Nettipalvelu ei todenna, tai ei voi todentaa, että hyvin muotoiltu, validi ja jatkuva kysely on tarkoituksenmukaisesti tarjottu kyselyn lähettäneelle käyttäjälle.
CWE-425	Suora kysely (’Pakotettu selaus’)	Nettipalvelut alttiina suorien kyselyiden hyökkäyksille, tekevät usein vääriä oletuksia, että sellaiset resurssit voidaan saavuttaa pelkästään suoraan annetun navigointipolun kautta ja täten vaativat valtuutusta vain tietyille polun osille.
CWE-522	Riittämätön tunnusten suojaus	Tuote tallentaa autentikointiin tarkoitettuja tunnuksia, mutta käyttää turvatonta metodia estääkseen näiden saamisen ja/tai hakemisen ei halutuilta tahoilta.
CWE-787	Kirjoittaminen rajojen ulkopuolelle (’out-of-bounds write’)	Tuote kirjoittaa dataa yli sallittujen puskuri rajojen
CWE-798	Muistiallokaatio liian isolle arvolle	Tuote allokoi arvolle muistia epäluotettavalle, suurelle arvolle tarkastamatta arvon suuruutta, mahdollistaen allokoinnin mielivaltaiselle määrälle muistia

CVE:t voidaan luokitella CWE:lla eli yleisten haavoittuvuuksien luetteloinnilla (engl. Common Weakness Enumeration). Lähes jokainen CVE voidaan luokitella yhden tai useamman CWE avulla alaluokkiin. Taulukosta 4.1 voi nähdä kaikki tässä työssä käytettävien CWE nimet sekä kuvaukset.

4.3 Bottiverkkojen kommunikointi

Bottiverkkojen ohjaus vaatii kommunikointiyhteyden hyökkääjältä kaikille boteille, jotta hyökkäykset voidaan suorittaa synkronoidusti hajautetuista lähteistä huolimatta. Tämä edellyttää ennalta suunnitellun infrastruktuurin käyttöä, joka mahdollistaa hyökkääjän kommunikoinnin kaikille verkkoon liitetyille boteille. Tässä luvussa tarkastelemme erilaisia arkkitehtuureja, joita erilaiset bottiverkot käyttävät kommunikaatioyhteyden mahdollistamiseksi. Tarkemmat esimerkit bottiverkoista ja niiden arkkitehtuureista löytyvät luvusta 6. Arkkitehtuurit voidaan karkeasti jakaa kahteen kategoriaan: keskitettyihin ja hajautettuihin arkkitehtuureihin. Keskitettyjä arkkitehtuureja joita tässä luvussa käydään läpi ovat ohjauspalvelinmalli 4.3.1, heijastinmalli 4.3.2 sekä IRC- 4.3.3 ja web-pohjaiset mallit 4.3.4. Hajautettuja arkkitehtuureja edustaa vertaisverkkomalli 4.3.5.

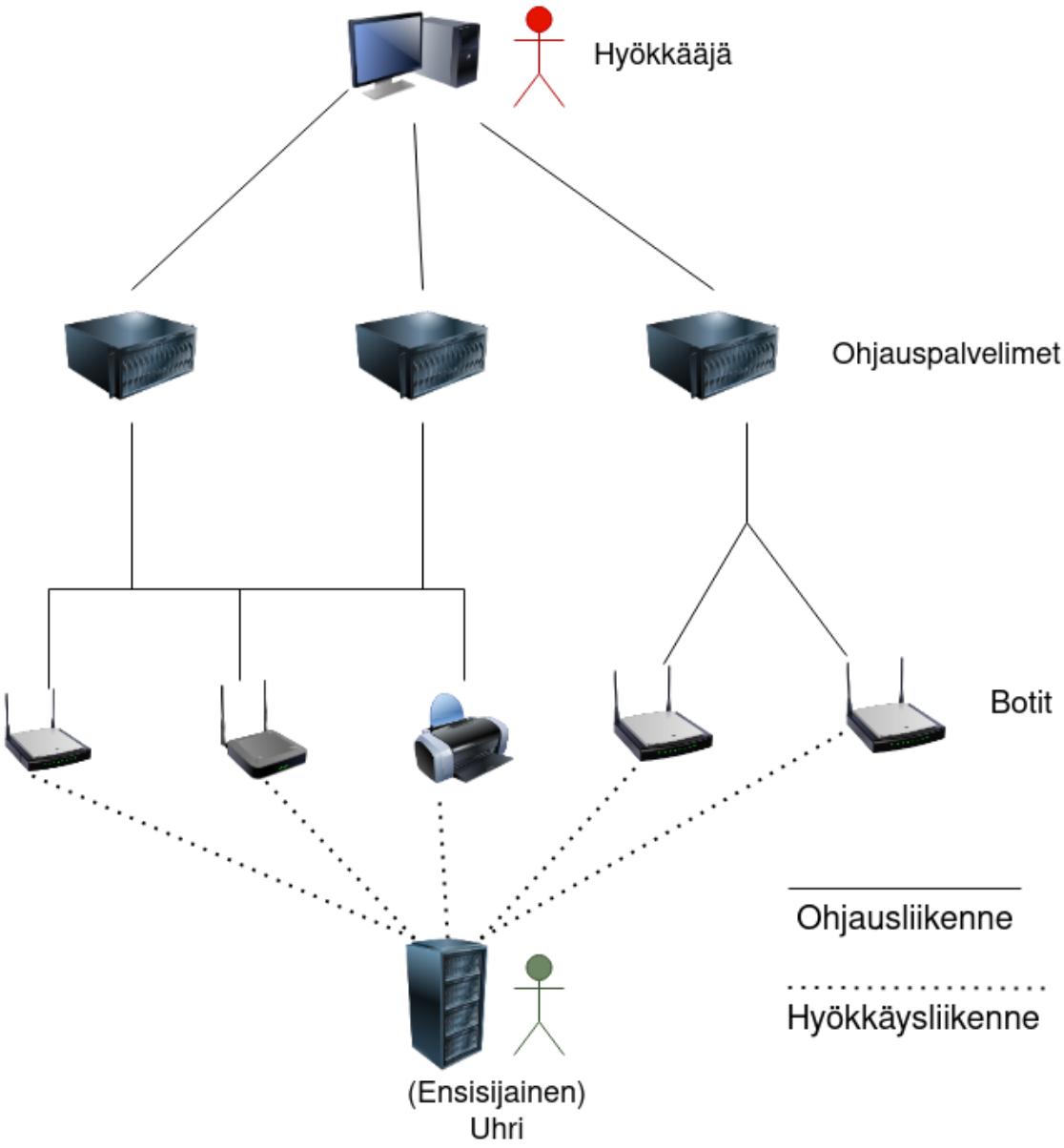
4.3.1 Ohjauspalvelinmalli

Ohjauspalvelinmalli (engl. agent-handler) arkkitehtuurimalli on esimerkiksi Miraissa 6.3 käytetty arkkitehtuurimalli. Tämä malli koostuu pääasiassa kahdesta kerroksesta, ohjauspalvelimista sekä boteista. Lisäksi mallista löytyy ensisijainen uhri, joka on bottiverkon suorittavan hyökkäyksen kohde, sekä hyökkääjä, joka hallinnoi bottiverkkoa. [37] Ohjauspalvelin arkkitehtuurin voi nähdä kuvassa 4.1.

Ohjauspalvelinmallissa itse ohjauspalvelimet ovat sovelluspaketteja, jotka tartuttavat Internetissä kiinni olevia verkkoresursseja. Tätä resurssia hyökkääjä käyttää välikätenä kommunikointiin bottien kanssa. Ohjauspalvelimia voi olla verkossa joko yksi tai useampia. Boteilla puolestaan tarkoitetaan sekä koodia, joka pyörii tartutetulla laitteella, että itse bottiverkkoon kiinnitettyä laitetta. Botilla tartutetusta laitteesta puhutaan myös hyökkäyksen sekundäärisenä uhrina. [20] [38]

Yleensä tartutettujen laitteiden käyttäjät eivät ole tietoisia heidän laitteensa on yhdistetty bottiverkkoon, sillä se ei estä laitteen normaalia käyttöä. Laitteen omistajan voi olla hyvin vaikeaa huomata laitteen olevan osana isompaa kokonaisuutta. [37] Riippuen haittaohjelman suunnittelusta, voi botin ohjaus tapahtua joko yhden tai useamman ohjauspalvelimen kautta. [20] [38]

Jos hyökkääjä käyttää tätä kyseistä arkkitehtuuria, on sen intressien mukaista käyttää ohjauspalvelimina resursseja, joiden läpi kulkee jo valmiiksi suuri määrä liikennettä. Tästä syystä ohjauspalvelimet ovat yleensä esimerkiksi reitittimiä tai palvelimia. Tämän tarkoitus



Kuva 4.1. *Ohjauspalvelin arkkitehtuuri*

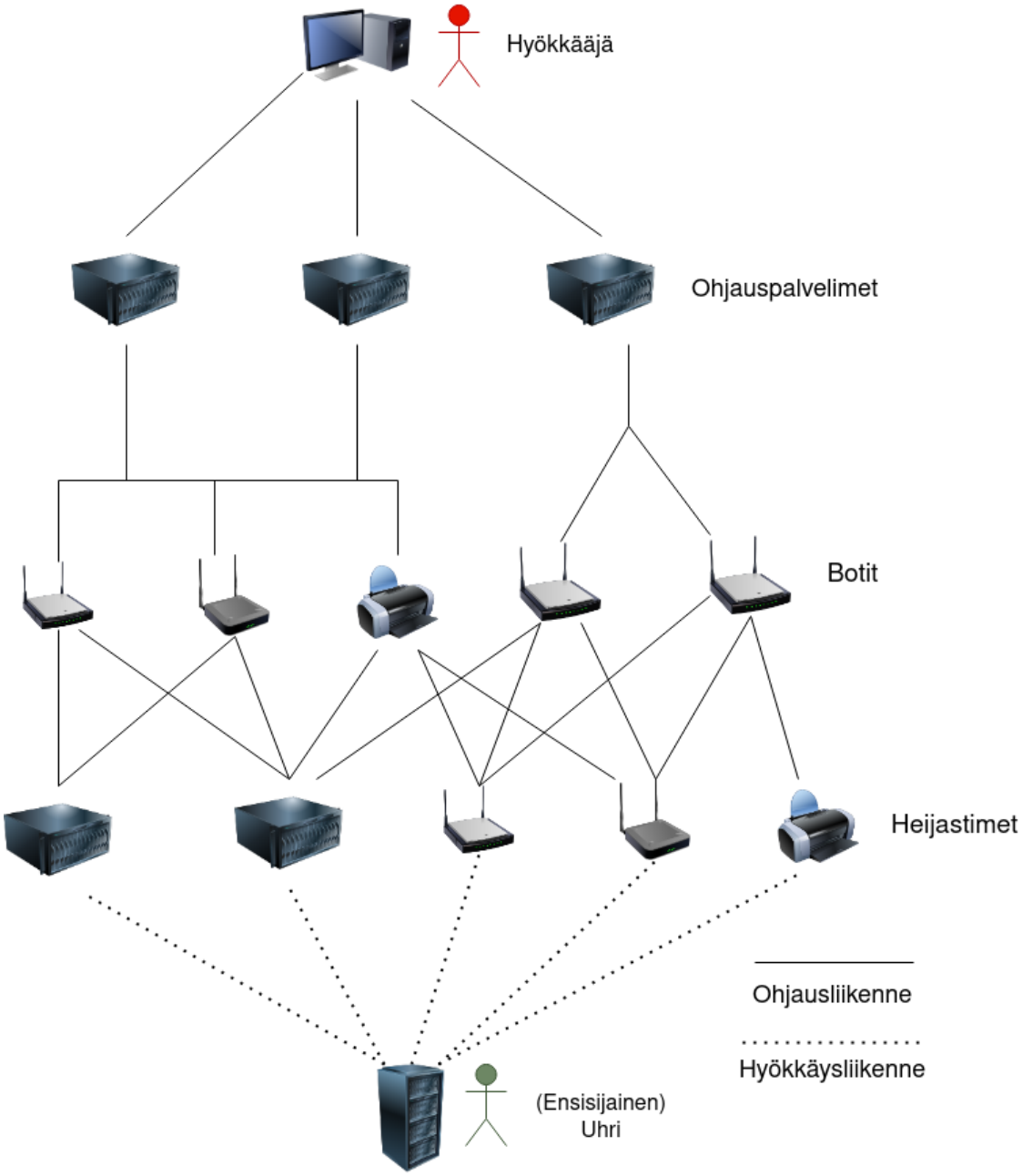
on piilottaa bottien ohjausliikenne muun liikenteen sekaan ja näin pienentää bottiverkon ohjausliikenteen paljastumisen mahdollisuutta. [20] [37]

Huono puoli tässä arkkitehtuurissa on, että bottien ja ohjauspalvelimien pitää tietää toistensa identiteetti voidakseen kommunikoida keskenään. Esimerkiksi ohjauspalvelimen IP-osoite voi olla kovakoodattuna haittaohjelmaan, joka tartuttaa botin. Tämän seurauksena yksittäisen botin löytäminen voi aiheuttaa koko verkon tunnistamiseen. [20]

4.3.2 Heijastinmalli

Heijastin arkkitehtuurimalli on hyvin samanlainen kuin ohjauspalvelinmalli. Ero piilee tavassa lähettää hyökkäysliikennettä boteilta ensisijaiselle uhrille. Siinä missä ohjauspalve-

linmallissa botit lähettävät hyökkäysliikenteen suoraan uhrille, käytetään heijastinmallissa apuna heijastimia. Kuva arkkitehtuurista löytyy 4.2, josta voi nähdä arkkitehtuuri rakenteen.



Kuva 4.2. *Heijastin arkkitehtuuri*

Heijastin voi olla mikä tahansa Internetissä kiinni oleva laite, joka pystyy vastaamaan kutsuihin IP-osoitteen perusteella. Botit lähettävät heijastimelle haluamaansa kutsun, joka sisältää ensisijaisen uhrin IP-osoitteen. Näin heijastin lähettää kutsun vastauksen ensisijaiselle uhrille. Heijastinmallilla voidaan myös monistaa liikennettä, josta voi lukea lisää luvusta 3.7.4. Luvussa kerrotaan muun muassa Smurf-hyökkäyksestä, joka käyttää hyväkseen monistamista. [20] [38]

Heijastinmalli tuo lisäsuojakerroksen bottiverkolle. Vaikka heijastimet on helppo jäljittää hyökkäysliikenteen perusteella, on bottien jäljittäminen väärän lähettäjä IP:n perusteella vaikeaa. [20]

4.3.3 IRC-pohjainen malli

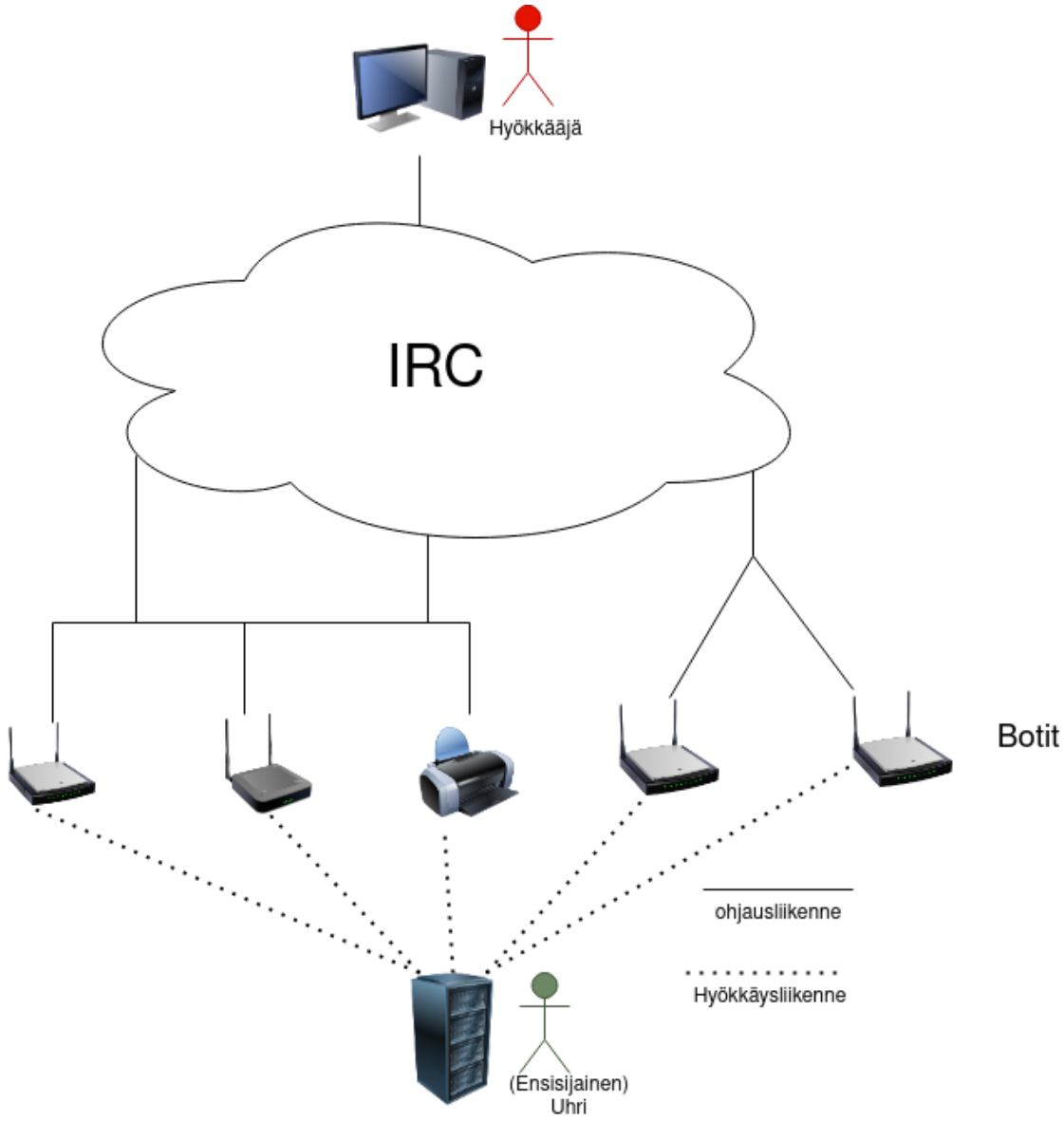
IRC-malli (engl. Internet relay chat) on hyvin samankaltainen ohjauspalvelinmallin kanssa. Erona on se, että IRC-kanavia käytetään kommunikaatiovälineenä bottien ja hyökkääjän välissä ohjauspalvelimien sijasta. Kuva IRC-arkkitehtuurimallista löytyy 4.3. [38] IRC on sovellustason protokolla, jota käytetään monikanava, monikäyttäjä viestintäjärjestelmään asiakas/palvelin arkkitehtuurilla. IRC-mallissa bottiverkon hallitsija luo IRC-kanavan bottien kanssa kommunikointiin ja niiden ohjaamiseen. [20] Tähän arkkitehtuurikategoriaan voisi luokitella bottiverkot, jotka käyttävät myös muita pikaviestisovelluksia esimerkiksi Telegramia tai Whatsappia korvaamalla IRC-kanavan käytetyllä ohjelmalla.

Hyviä puolia IRC-pohjaisen arkkitehtuurin käyttämiseen kommunikaation välittäjänä on monia. Hyökkäyksen ohjaukseen tarkoitettua liikennettä on vaikea erottaa muuhun viestintään käytetyistä paketeista, sillä liikenteen määrä on suuri. Verkon bottien ylläpito on helppoa tässä mallissa, sillä riittää, että botit lisätään niille tarkoitetulle serverille, kun ne yhdistetään verkkoon. Näin listan boteista voi saada ulos pelkästään kaivamalla IRC-palvelimeen liitetyt laitteet. Viimeisenä jos on luotu hajautettu ylläpito useammille IRC-palvelimille ja kanaville, yhden botin paljastuminen aiheuttaa vain kyseisen bottiin liitetyn IRC-kanavien ja -palvelimien nimet. [20]

4.3.4 Web-pohjainen malli

Web-pohjainen malli on rakenteeltaan samanlainen IRC-pohjainen malli, mutta IRC-kanavan sijasta kommunikaatiovälineenä käytetään verkkosivustoa. Suurin osa boteista on konfiguroitu ja ohjattu monimutkaisilla ohjelmilla, joissa kommunikointi tapahtuu suojatulla yhteydellä käyttäen HTTP/HTTPS-protokollia. Osa boteista on puolestaan jätetty raportoimaan bottiverkon tilastoja verkkosivuille. [20] [39]

Web-pohjaisessa mallissa on IRC-pohjaiseen verrattuna omat hyvät puolensa. Ensinnäkin verkkosivu on helppo pohjustaa ja laittaa pystyyn. Verkkosivuun saa sisäänrakennettua myös hyvin monimutkaisiakin raportointi ja komento-ominaisuuksia, sillä mahdollisuudet ovat käytännössä rajattomat, jos osaa ohjelmoida. Verkkosivu on myös helppo käyttää ja hankkia, ja liikenne voidaan naamioida ja filteröidä. [20]

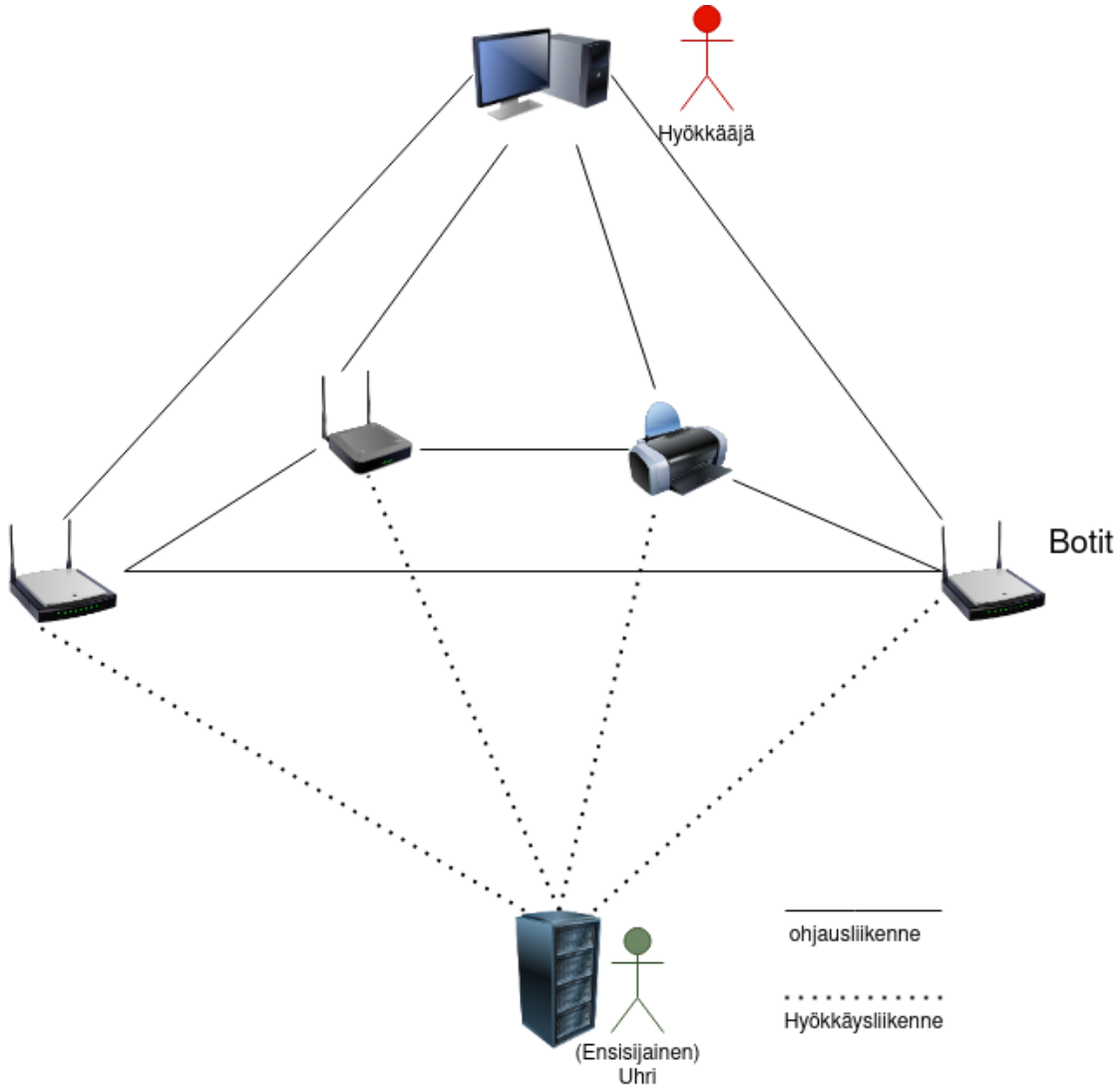


Kuva 4.3. *IRC-pohjainen arkkitehtuurimalli*

4.3.5 Vertaisverkko

Vertaisverkon käyttö on ainoa hajautettu malli luvussa esitellyistä arkkitehtuureista ja sitä käytetään uudemmissa bottiverkoissa. Siinä missä kaikki edellä mainitut mallit ovat erilaisia C&C (engl. Command and control) arkkitehtuureja, vertaisverkko ei nojaa erilliseen ohjauskerrokseen hyökkääjän ja bottien välillä. Vertaisverkossa komentojen välittäminen on kaikkien bottien vastuulla, samoin kuin resurssit, tehtävät ja työkuorma jaetaan kaikille verkkoon liitetyille boteille. [20]

Vertaisverkko on aikaisempiin vaihtoehtoihin verrattuna vikasietokykyisempi vaihtoehto tehtävien hajauttamisen ansiosta. Tämä malli tuo hyökkääjälle erityisen lisäturvan, sillä hyökkääjän komennot ponnahtelevat verkosta laitteelta toiselle, tehden viestin alkuperäisen lähettäjän tunnistamisesta haastavaa. Vertaisverkkoarkkitehtuuri tekee myös verkon



Kuva 4.4. *Vertaisverkko arkkitehtuuri*

alasajosta erittäin vaikeaa, sillä siinä missä aikaisemmin kuvatuista C&C-arkkitehtuurien verkoista komentojen välittäjän, joko ohjauspalvelimien, IRC:n tai verkkosivun alasajo riittää, pitää vertaisverkosta irrottaa jokainen botti, että koko bottiverkosto saadaan hajotettua. [20]

5. IOT-LAITTEIDEN SUOJAAMINEN

Vaikka IoT-laitteiden tietoturva ei olekaan mitenkään hyvällä taholla, on älylaitteiden tietoturvan varmistamisen eteen tehty töitä niin EU kuin Suomenkin tasolla. Tässä luvussa esitellään muutamia toimia, joita on otettu paremman tietoturvan tulevaisuuden puolesta.

5.1 Viranomaisten rooli IoT-laitteiden tietoturvan varmistamisessa

IoT-laitteiden heikko tietoturva ja siihen liittyvät uhat ovat jo tunnistettu EU-tasolla, ja toimia uhkien vähentämiseksi on jo aloitettu [40]. EU on asettanut radiolaitedirektiivin, joka velvoittaa EU-alueella myytävät, internetissä kiinni olevat laitteet täyttämään EU:n asettamat tietoturvavaatimukset. Tietoturvavaatimusten tavoitteena on suojata viestintäverkkoja, varmistaa käyttäjien yksityisyydensuoja ja estää taloudelliseen hyötyyn tähtääviä, internetissä kiinni olevia laitteita hyödyntäviä petoksia. Kyseinen direktiivi tuli voimaan vuonna 2022, mutta siirtymäaikaa on vuoteen 1.8.2024 asti [41]. EU-komissio on myös mukana monissa projekteissa, joiden tavoitteena on lisätä IoT-tietoturvaa EU-alueella [42]. On hyvä tässä myös huomioida, että datan säilytyksen ja keräyksen läpinäkyvyyden osalta EU-alueella on jo olemassa GDPR-direktiivi (engl. General Data Protection Regulation), joka koskee myös IoT-laitteita, jos ne säilyttävät henkilökohtaista tietoa. [43]

Suomi on ollut edelläkävijä IoT-laitteiden tietoturvan parantamisessa jo ennen EU:ta. Vuonna 2019 Suomessa julkaistiin Tietoturvamerkki, joka takaa käyttäjille tietyt tietoturvan perusominaisuudet [44]. Tietoturvamerkin sertifiointiprosessi perustuu ETSI EN 303 645 -standardiin, jonka tarkoituksena on ehkäistä kuluttajakäyttöön tarkoitettujen IoT-laitteiden altistumista yleisimmille uhille [45]. Standardi sisältää muun muassa vaatimuksen siitä, että laitteissa ei saa olla käytössä maailmanlaajuisia oletussalasanoja, ohjelmistot on pidettävä ajan tasalla, sisäänsyötettävä data on varmistettava ja muita vastaavia tietoturvavaatimuksia ja suosituksia. [45]

Lyhyesti voisi mainita, että vuonna 2022 on julkaistu IoT-laitteiden kyberturvallisuus standardi myös ISO/ETC informaatioteknologia standardisarjan 2700 alle. Standardi ei ollut tämän työn kirjoittamisajankohtana vielä käynyt vertaisarviointeja läpi. [46] Oman standardin kehittäminen kuitenkin osoittaa, että IoT-laitteiden tietoturvaongelmat on havaittu myös kansainvälisellä tasolla ja sen eteen on alettu tekemään töitä.

5.2 IoT-laitteiden haavoittuvuuksien paikkaaminen

Laitteiden valmistajilla on myös iso rooli IoT-laitteiden suojaamisen toteuttamisen osalta. Tässä luvussa käydään läpi, mitä toimia laitteiden valmistajat voivat tehdä tehdäkseen IoT-laitteistaan turvallisia hyökkäyksiä vastaan. Pohjana luvulle käytetään jo edellisessäkin mainittua IoT -laitteille suunnattua ETSI EN 303 645 -kyberturvallisuus standardia. Standardin ydinsisältö koostuu kahdesta osasta, kyberturvallisuus säännöksistä kuluttaja IoT-tuotteille, sekä datan suojaamisesta kuluttaja IoT-tuotteilla [47].

IoT-laitteiden tietoturvallisuutta voidaan parantaa useilla eri toimenpiteillä. Ensimmäinen askel on välttää oletussalasanojen käyttöä laitteissa. Kuten luvussa 6 tullaan huomaamaan, sanakirjahyökkäykset ovat olleet ja ovat valitettavasti vieläkin isona tietoturvaongelmana, kun puhutaan kuluttajille suunnatuista IoT-laitteista. Ohjelmiston päivittäminen on myös tärkeää, jotta mahdolliset tietoturvahaavoittuvuudet saadaan paikattua julkaisun jälkeenkin. Sensitiivisille turvallisuusparametreille tulee käyttää turvattua tallennusmenetelmää ja yhteyksien on oltava turvattuja. Hyökkäyspintoja tulee pyrkiä minimoimaan, ohjelmiston eheys on varmistettava ja henkilökohtainen data tulee olla turvattu. Järjestelmän on myös kyettävä toipumaan mahdollisista katkoksista. Helppo asennus- ja ylläpitoprosessi sekä henkilökohtaisen datan helppo poistettavuus ovat myös tärkeitä tekijöitä. Lisäksi sisääntulo data esimerkiksi syöttökenttien kautta tulee validoida. Tällä voidaan estää esimerkiksi SQL-injektiot, eli hyökkäykset, joissa syöttökenttiin laitettavia tietokanta lauseiden avulla voidaan käytännössä tehdä laitteen kantaan lähes mitä vain, kaiken tiedon hakemisesta koko kannan tuhoamiseen.

Jokaisesta edellä mainitusta kohdasta on lisäksi olemassa säännöksiä, jotka tarkentavat otsikkotason säännöksen tarkoitusperät. Näitä voisi olla esimerkiksi sensitiivisten parametrien turvallisen säilytyksen kohdalla, että kovakoodattuja parametrejä ei saa käyttää.

6. IOT BOTTIVERKOT

Tässä luvussa käsitellään viimevuosien isoimpia bottiverkkoja, jotka ovat olleen DDoS hyökkäykseen kykeneviä ja jotka koostuvat IoT-laitteista. Vaikka tässä luvussa käsiteltävät bottiverkot ovat IoT-laitteita koostuvia, on myös olemassa bottiverkkoja, jotka käyttävän hyväkseen enemmän laskentakapasiteettia omaavia laitteita, kuten virtuaalikoneita tai älypuhelimia. Tästä esimerkkinä voisi mainita Mantiksen (2022), joka on saanut vain noin 5000 botilla aikaiseksi 26 miljoonaa HTTPS-kutsua per sekunti. Mantis on evoluutio Meriksestä, johon palaamme aliluvussa 6.8. Toisin kuin Meris, joka käyttää hyväkseen IoT-laitteita, Mantis on ottanut kohteekseen virtuaalikoneet. [48] Vaikka tämä työ keskittyy IoT-laitteisiin kohdistuviin haittaohjelmiin, on silti huomioitava, että on olemassa bottiverkkoja, jotka käyttävät älypuhelimia sekä tietokoneita, virtuaalikoneita ja muita korkeatehoisia laitteita hyökkäyksien tekemiseen.

Tässä luvussa esiteltyjen bottiverkkojen datan koonti yhteen sekä datan analysointi on luvussa 7.

6.1 XorDDoS (2014)

XorDDoS on syyskuussa vuonna 2014 vuonna Malware Must Die -tiimin jäsenen löytämä Troijalainen haittaohjelma. Troijalainen tarkoittaa haittaohjelmaa, joka on naamioitu muuksi viattomaksi ohjelmaksi.

XorDDoS käyttää levittäytymisessään hyväkseen Linux-käyttöjärjestelmän vuonna 2015 havaittuun ShellShock haavoittuvuuteen. Bottiverkko tekee Secure Shell (SSH) -yhteyden kautta sanakirjahyökkäyksen, jonka jälkeen haittaohjelma asennetaan pääkäyttäjäoikeuksilla laitteille. [49] SSH on tietoliikenne yhteyden protokolla, jota käytetään yleisesti suojatun etäyhteyden muodostamiseen laitteille. [50]

XorDDoS-haittaohjelma ei ole pelkästään IoT-laitteisiin kohdistuva haittaohjelma, koska se käyttää hyväkseen Linux-käyttöjärjestelmän haavoittuvuuksia. Täten se voi liittää itseensä myös tietokoneita ja virtuaalikoneita, kunhan nämä käyttävät Linux-käyttöjärjestelmää. Monet IoT-laitteet kuitenkin on rakennettu eri Linux-käyttöjärjestelmien päälle, jonka takia tätä haittaohjelmaa käsitellään tässä työssä [50].

DDoS-hyökkäyksiä, mihin XorDDoS on kykeneväinen, on muun muassa SYN tulvahyök-

käys, UDP tulvahyökkäys ja DNS tulvahyökkäys [35]. Vuonna 2015 bottiverkon DDoS hyökkäysten teho ylsi 150Gbps ja se teki jopa 20 hyökkäystä päivässä. XorDDoS-bottiverkon arkkitehtuuri on ohjauspalvelinmalli 4.3.1. [49]

XorDDoS-haittaohjelman tartunnan saaneista laitteista monet ovat myöhemmin altistuneet myös Tsunami-nimiselle haittaohjelmalle, joka asentaa laitteille XMRig-louhijan. Vaikka XorDDos haittaohjelmasta ei suoraa löydetty Tsumanim asentamiseen käytettävää ohjelmaa, ei ole pois suljettu vaihtoehto, että Tsunami asennetaan jatkotoimenpiteenä. [50]

Vaikka XorDDoS-haittaohjelma on löydetty jo vuonna 2014, se ei ole kadonnut mihinkään vaan leviää edelleen verkossa. Vuonna 2021 IBM kertoi raportissaan useiden haittaohjelmien, mukaan lukien XorDDoS, lisänneen kohteisiinsa myös Docker-ympäristössä pyöriviä palveluita. [51] Tämän jälkeen vuonna 2022 Microsoft kertoi tutkimustuloksiaan, jossa selvisi XorDDoS-haittaohjelman aktiivisuuden kasvaneen jopa 254%. [50]

6.2 BASHLITE (2014)

Bashlite, tunnetaan myös nimillä Lixkebab, Torlus ja Gafgyt, on 2014 vuonna löydetty haittaohjelma, jonka koodipohjat ovat avointa lähdekoodia, eli julkaistu nettiin kaikkien saataville. [35] Todennäköisesti tämä on syynä sille, että Bashliten muunnelmia on löytynyt paljon myöhemminkin [52]. Bashliten kohteena on ollut muun muassa valvonta kameroita sekä kotireitittimiä [53].

Bashlite haittaohjelma perheen bottiverkojen koon on arvioitu vuosina 2014–2016 yltäneen jopa miljoonaan bottiin ja sen aiheuttamat hyökkäykset ovat olleet jopa 400 Gbps. [35]

Hyökkäykset, joita Bashlite on ollut kykenevä tekemään, ovat olleet alkuperäisessä haittaohjelmassa SYN ja UDP tulvahyökkäyksiä. [53] Sen arkkitehtuuria on lähteestä riippuen sanottu joko ohjauspalvelinmalliksi tai IRC-malliksi 4.3.3 [35] [53]. Bashliten kohteita ovat olleet tietokonepeleissä tai niihin liittyvissä oheistoiminnassa käytettyjä portteja: XboxLive (3074), Minecraft (25565), Valve (27015) ja Teamspeak (9987) [53].

Bashlite haittaohjelman muunnelmissa levittäytymistapoja on laajennettu puhtaasta sanakirjahyökkäyksestä myöhemmin myös yleisiin haavoittuvuuksiin. Näitä ovat olleet muun muassa CVE-2017-17215, CVE-2018-10561. CVE-2017-17215 on CWE-20 tyyppinen haavoittuvuus, joka koskee Huawei HG532 laiteita. Joissain versioissa koodin etäajolla tunnistautunut hyökkääjä voi lähettää haitallisia paketteja porttiin 37215 laukaistakseen hyökkäyksiä. Onnistunut sisäänpääsy voi johtaa mielivaltaisen koodin etäajamiseen. CVE-2018-10561 puolestaan koskee Dasan GPON koti reitittimiä. Niissä on mahdollista ohittaa tunnistautuminen lisäämällä "?image"minkä tahansa reitittimen tunnistautumista vaativan URL:n perään. Samoja haavoittuvuuksia voi löytää muun muassa Zerobotin haavoittuvuuslistasta 6.4. Bashliten muunnelmat ovat myös laajentaneen hyökkäysvekto-

reitaan myös HTTP/HTTPS, kun ottanut osakseen myös Mirain lähdekoodeja. [52]

6.3 Mirai (2016)

Mirai on varmaankin tämän hetken tutkituin ja tunnetuin haittaohjelma. Mirain aiheutti monen tunnetun ja ison järjestelmän kaatumisen tekemällä lokakuussa 2016 DDoS hyökkäyksen nimiavaruuspalveluun nimeltä Dyn. [54] Näihin palveluihin kuuluin paljon korkean profiilin palveluita muun muassa Netflix, PayPal, Reddit, Twitter, Amazon ja Spotify. [55]

Mirai käytti levittäytymiseen hyväkseen sanakirjahyökkäystä, johon olivat kovakoodattu 62 autentikointi tunnusta, millä se sai haltuunsa lukuisia reitittimiä, kameroita ja digitaalisia videonauhureita, jotka oli pääasiassa XiongMai Technology nimisen yrityksen valmistamia. Mirain arkkitehtuuri oli ohjauspalvelinmalli 4.3.1 ja se pystyi suorittamaan laajaa ryhmää eri protokollia käyttäviä hyökkäyksiä. Näihin kuului muun muassa UDP, HTTP ja TCP. [20]

Mirain koon arvioidaan olleen parhaimmillaan suunnilleen puoli miljoonaa tartutettua laitetta ja sen hyökkäystehon arvioidaan olleen 1200 GBps. [20] [35]

Mirain lähdekoodit on julkaistu avoimeen levitykseen. Ensimmäinen lähdekoodien levitys tapahtui HackForums.net nimisellä sivustolla 30. syyskuuta vuonna 2016 käyttäjänimellä "Anna-Sensai". Tämän jälkeen lähdekoodit ilmestyivät hiljakseen myös muihin palveluihin kuten esimerkiksi GitHubiin. Mirain lähdekoodien julkaisu on kiistämättä ollut vauhdittamassa bottiverkkojen levitystä ja vielä nykyäänkin on paljon haittaohjelmia, jotka pohjaavat Miraihin. Tässä työstä löytyviä, isoiksi nousseita Miraihin pohjaavia haittaohjelmia ovat muun muassa Reaper 6.4 ja Echobot 6.7. [20]

6.4 Reaper (2017)

Reaper, tunnetaan myös nimellä IoTroop, havaittiin lokakuussa 2017. Kuten monet muut haittaohjelmat Mirain jälkeen, myös Reaper arvellaan käyttävän pohjalla Mirai:n lähdekoodeja. Reaper kuitenkin eroaa muista tähänastisista haittaohjelmista, koska se ei käytä tartuttamisessa pelkästään sanakirjahyökkäystä, vaan yhdeksää eri yleisesti tunnettua haavoittuvuutta, jotka löytyvät taulukosta 6.1. [35]

Reaperin epäillään olleen syypäänä tammikuussa 2018 tapahtuneeseen DDoS hyökkäykseen finanssi ja pankkisektoria vastaan. Hyökkäyksiä tapahtui muun muassa Venäjän ja Ukrainan pankkeihin. Reaperin hyökkäystehon arvioidaan ollen 30 GBps edellä mainitun finanssiala hyökkäyksen perusteella ja sen koon noin 20000 bottia. [35]

Luokka (CWE)	Haavoittuus	Kuvaus	Laite tai Sovellus
CWE-119	CVE-2013-4980	Sallii etäkäyttäjän aiheuttaa laitteen kaatumisen ja mahdollsuuden ajaa mielivaltaista koodia pitkän merkkijonon URI:ssa kautta RTSP SETUP kutsussa	RTSP Packet Handler in AVTECH AVN801 DVR
CWE-119	CVE-2013-4981	Sallii etäkäyttäjän aiheuttaa laitteen kaatumisen ja mahdollsuuden ajaa mielivaltaista koodia pitkän merkkijonon Network.SMTP.Receivers muuttujassa	AVTECH AVN801 DVR
CWE-522	CVE-2017-8225	Pääsy .ini tiedostoihin (sisältävät kirjautumistietoja) ei ole oikein tarkastettu. Hyökkääjä pystyy ohittamaan tunnistautumisen tarjoamalla tyhjää loginuse muuttujaa ja tyhjää loginpas muuttujaa URI:ssa	WIFICAM langattomat IP kamerat
CWE-798	CVE-2017-8224	Laitteissa on takaovi pääkäyttäjälle TELNET:n kautta	WIFICAM langattomat IP kamerat

Taulukko 6.1. *Reaperin käyttämät haavoittuvuudet [56]*

6.5 JenX (2018)

JenX on Radwaren paljastama bottiverkko, joka on esimerkkinä DDoS hyökkäys ostettuna palvelusta. Hyökkäyksien kohteena JenX:lla on GTA moninpeli pelaajat, joita kohtaan se teki maksua vastaan hyökkäyksiä. Bottiverkko on ollut kykeneväinen tekemään ainakin 300 GBps hyökkäyksiä, joita se teki 20 dollarin maksua vastaan. [57]

Radwaren tutkimukset johti ohjauspalvelimelle, jota ylläpidettiin verkkotunnuksen 'sancalvicie.com' alla. Sivustolta löytyi kolme ostettavaa pakettia. Yksi niistä oli GTA San Andreas moninpelaaja pelin ylläpitopalvelin, mutta yksi paketeista oli myös DDoS hyökkäyksiä muihin palveluihin. 'Corriente diviena' -niminen (espanjaa ja tarkoittaa jumalallista virtaa) palvelu lupasi Valve Source Engine (VSE) Quetry käyttäen, 32-tavuisilla, TS3 skriptillä ja "Down OVH"asetuksella tehtyjä tulvahyökkäyksiä. OVH asetuksella todennäköisesti viitattiin hyökkäykseen kohodistuen OVH:n ylläpitämään palvelimeen. OVH on tunnettu pilvipalvelu, joka on ylläpidostaan esimerkiksi monipeli Minecraftia. [57] Sivusto ei ollut enää pystyssä tämän työn kirjoittamisen aikana, joten oletettavasti ylläpito palvelimet ovat jossain välissä vuoden 2018 ja 2023 vuoden aikana saatu ajettua alas.

JenX arkkitehtuuri on Radwaren mukaan ohjauspalvelinmalli 4.3.1, jossa keskitetyt pal-

velimet hoitavat kaiken muun paitsi itse hyökkäysten tekemiset, esimerkiksi uusien laitteiden löytämisen ja tartuttamisen. Tällöin bottien vastuulle jää pelkästään hyökkäyksen toteutus. [57]

IoT-laitteiden tartuttamiseen se on käyttänyt pääasiassa kahta CVE:ta, CVE-2014-8361 ja CVE-2017–17215, jotka ovat haavoittuvuuksia Huawei HG532 ja Realtek RTL81XX Wifi reitittimissä. [57] Molemmat näistä kuuluvat CWE-20 haavoittuvuus luokkaan. Helmikuussa 2018 julkaistun Medium artikkelin mukaan JenX käyttäisi myös D-LINK reitittimen CVE-2015–2051 haavoittuvuutta [58], joka kuuluisi CWE-77 haavoittuvuusluokkaan. Tämän haavoittuvuuden käytöstä ei kuitenkaan ollut muissa lähteissä mainintoja, eikä Medium artikkelissa näkynyt näyttökaappauksia tai muita todisteita, joissa olisi dataa tämän haavoittuvuuden käytöstä.

Palo alton Unit 42 löysi vuonna 2019 Bashlite 6.2 muunnoksen, joka kilpaili samassa markkinaraossa JenX kanssa. Tämä käytti samoja haavoittuvuuksia JenX kanssa bottien tartuttamiseen, mutta näiden lisäkäsi käytössä oli CVE-2017-18368, haavoittuvuusluokka CWE-78, joka lisäsi yhden reitittimen lisään mahdollisesti tartuttavien laitteiden joukkoon. [59]

Unit 42 löytämän muunnelma on kykeneväinen VSE hyökkäyksien lisäksi perinteisimpiin HTTP tulvahyökkäykseen, sekä ajamaan alas sen botit halutessaan (engl. kill switch). Muunnelmalla oli myös käytössään JenX tavoin nettisivusto, mistä pystyi halutessaan ostaa DDoS hyökkäyksiä haluttuun IP osoitteeseen. Sivustolla oli San Calvicie sivustosta poiketen useaan hintaluokkaan sopivia hyökkäyksiä, hinnat nousivat muutamasta dollarista 150 dollariin. [59]

Unit 42 mukaan, mahdollisesti tartutettavia laitteita, joilta löytyy JenX sekä Unit 42 tutkiman muunnelman käyttämät haavoittuvuudet, oli vuonna 2019 noin 32000 kappaletta kiinni verkossa. [59] Koska näiden bottiverkkojen oikeita kokoja ei tiedetä, käytetään tätä maksimiarvoa viitteellisenä kehysarvona bottiverkkoja vertaillessa.

6.6 Mozi (2019)

Mozi on vertaisverkko 4.3.5 arkkitehtuuria käyttävä haittaohjelma, joka löydettiin vuonna 2019. Mozi on monien muiden bottiverkkojen tavoin ottanut koodia avoimeen levitykseen laitetuista haittaohjelmista kuten Bashlitesta 6.2 ja Miraista 6.3 [60] [61]. Tästä johtuen pystyy se tekemään paljon samoja hyökkäyksiä kuin Bashlite ja Mirai kuten UDP, TCP ja HTTP. [60]

Mozin kohteita ovat olleet pääasiassa reitittimet sekä digitaaliset videonauhurit. [62] Bottiverkon aktiivisten laitteiden määrä oli syyskuuhun vuoteen 2020 asti suunnilleen 200 000, jonka jälkeen se alkoi laskea [63]. Määrä pyöri vielä vuonna 2021 noin 10 000 ja 22 000 välillä [60].

Luokka (CWE)	Haavoittuvuudet	Laitteet tai Sovellukset
CWE-20	CVE-2014-8361, CVE-2017-17215	D-LinkDIR, HuaweiHG532
CWE-77	CVE-2015-2051, WAN Kaukosäädin komentoinjektio, UPnP SOAP TelnetD komentoinjektio	D-LinkDIR, Eir D1000 Wireless Router
CWE-78	CVE-2018-10562	Dasan GPON reitittimet, MVPowerDVR TV-7104HE
CWE-287	CVE-2018-10561	Dasan GPON reitittimet
CWE-352	CVE-2016-6277	NetgearD/R reitittimet
EI CWE LUOKITUSTA	CVE-2008-4873, Etänä koodin ajo	SPBOARD, NetgearDGN1000, CCTV-DIR

Taulukko 6.2. *Mozin käyttämät haavoittuvuudet [61] [60]*

6.7 Echobot (2019)

Echobot on 2019 vuonna löydetty Mirain pohjalta kehitetty haittaohjelma. Echobot käytti hyvin laajaa haavoittuvuuslistaa, joka parhaimmillaan sisälsi jopa 70 eri haavoittuvuutta. Ottaen huomioon, että Echobot kehitettiin Mirain pohjalta, voidaan olettaa hyökkäyksien, joita se on kykeneväinen tekemään, on samat mitä Mirailla. Echonbotin arkkitehtuuri on ollut ohjauspalvelinjärjestelmä 4.3.1. [35]

Käytettyjen haavoittuvuuksien ikähaitari on hyvin laaja. Vanhimmat käytetyt ovat jo vuodelta 2003 ja koska Echobottia päivitettiin aktiivisesti vuonna 2019, on uusimmat haavoittuvuudet samana vuonna löydettyjä. Echobotin uhrit olivat laajasti kaikilta IoT osaalueelta, mikä ei ole mitenkään ihme, kun ottaa huomioon laaja haavoittuvuus listan. [35] Kaikista käytetyistä haavoittuvuuksista ei löytynyt erottelua, mutta löydetyt on koottu taulukkoon 6.3. Echobotin haavoittuvuuslista eroaa muista IoT bottiverkoista myös se, että perinteisempien IoT-laitteiden, reitittimien ja käyttöjärjestelmiin liittyvien haavoittuvuuksien lisäksi se tähtäsi myös teollisuudessa käytettyihin laitteihin muun muassa laitteisiin Mitsubishilta. [64]

Luokka (CWE)	Haavoittuvuudet	Laitteet tai Sovellukset
NVD-CWE-Other	CVE-2006-4000	Barracuda Spam Firewall

CWE-20	CVE-2009-0545, CVE-2014-8361, CVE-2017-6316	ZeroShell, Realtek SDK, Citrix NetScaler SD-WAN
CWE-22	CVE-2016-0752	Ruby on Rails
CWE-74	CVE-2019-2725	Oracle WebLogic palvelin
CWE-77	CVE-2009-5156, CVE-2010-5330, CVE-2016-10760, CVE-2017-18377	ASMAX AR-804gu, AirMax ISP, Seowon Intech retittimissä, WIFICAM IP kamerat
CWE-78	CVE-2013-5758, CVE-2017-14135, CVE-2017-14127, CVE-2017-5173, CVE-2018-11138, CVE-2018-11510, CVE-2018-14933, CVE-2018-15887, CVE-2018-20841, CVE-2018-6961, CVE-2019-12780, CVE-2019-14931, CVE-2019-15107, CVE-2019-16072, CVE-2019-17270	Yealink VoIP Phone SIP-T38G, opendreambox, Technicolor TD5336, Geutebruck IP kamera, Quest KACE, ASUSTOR ADM, NUUO NVRmini, ASUS DSL-N12E_C1, HooToo TripMate Titan HT-TM05 sekä HT-05 reitittimet, VeloCloudin VMware NSX SD-WAN Edge, Belkin Wemo Enabled Crock-Pot, Mitsubishi Electric ME-RTU, Webmin, NETSAS Enigma NMS, Yachtcontrol
CWE-89	CVE-2018-7841	U.motion Builder ohjelmisto
CWE-94	CVE-2013-5912, CVE-2018-17173	Thomson reitittimet
CWE-284	CVE-2016-6255	Portable UPnP SDK, LG Super-Sign CMS
CWE-78, CWE-79	CVE-2019-3929	Useita laiteohjelmistoja
CWE-78, CWE-134	CVE-2017-16608, CVE-2017-16602	Netgain Enterprise Manager, NetGain Systems Enterprise Manager
CWE-122, CWE-787	CVE-2019-18296	SPPA-T3000 MS3000
CWE-306, CWE-425	CVE-2019-14927	Mitsubishi Electric ME-RTU

Etäkomentojen ajo		ACTi ASOC 2200 Web Configurator, AVCON6 systems management platform - OGNL, Sar2HTML
Etänä koodin ajo		CCBILL CGI, 3Com OfficeConnect reititin

Taulukko 6.3. *Echobotin käyttämiä haavoittuvuuksia [64] [65] [66]*

Echobotin koon arvellaan olleen miljoonia tartutettuja laitteita [67], mutta tarkkoja tietoja siitä ei löytynyt. Myöskään hyökkäyksistä, mitä kyseisellä bottiverkolla olisi toteutettu, ei ole löytynyt tietoa. Kaikki uutiset Echobotista löytyy vuodelta 2019, eikä haittaohjelmasta ole sen jälkeen kuulunut mitään. Myöskään akateemisia julkaisuja kyseisestä bottiverkosta ei ole julkaistu.

6.8 Meris (2021)

Meris on vuonna 2021 Qrator löytämä laajalle levinnyt ohjauspalvelinmallin haittaohjelma [68]. Bottiverkko tuli myös CloudFlaren tietoisuuteen, kun se toteutti 17,2 miljoonan HTTP kutsua sekunnissa DDoS-hyökkäyksen heidän asiakastaan vastaan. Meris bottiverkon kohteina olivat vuonna 2021 muun muassa pankit, rahoitussektori, vakuutukset, peli/uhkapeli ja IT-palvelut. Vuonna 2021 Meriksen havaittiin tekevän keskimäärin 50 hyökkäystä päivässä. [69]

Meriksen botit ovat pääasiassa latvialaisen MikroTikin valmistamia. Meriksen hyväksikäyttämä haavoittuvuus on RouterOS-käyttöjärjestelmästä löytyvä CVE-2018-14847, jonka luokitus on CWE-22. Tämän haavoittuvuuden ansiosta todentamattomat etähyökkääjät voivat lukea satunnaisia tiedostoja ja todennetut hyökkääjät voivat kirjoittaa satunnaisia tiedostoja WinBox-käyttöliittymän tiedostohallinta haavoittuvuuden läpi. [69] [70] [68]

Vaikka MikroTik korjasi haavoittuvuuden RouterOS-käyttöjärjestelmästään, oli verkossa kiinni paljon haavoittuvuudelle altistuvia laitteita. Meris botnetin koko arvioitiin olevan laajimmillaan jopa 250 000 bottia. [69]

Epäillään, että koska Meris ei käytä kaikkea potentiaaliaan DDoS-hyökkäyksissään voi bottiverkon sekundaarisena kohteena olla kryptovaluutan louhinta. Tätä väitettä tukee myös tieto, että myös MikroTikin laitteisiin kohdistunut U6 bottiverkko paria vuotta aikaisemmin ja U6 päätoiminta oli kryptolouhinta hyökkääjälle. [70] Meris haittaohjelman tekemälle louhinnalle ei kuitenkaan ole löydetty todisteita, joten väite on jäänyt puhtaasti spekuloinniksi.

6.9 Zerobot (2022)

Zerobot on 2022 vuonna löydetty haittaohjelma, jonka toimintamalli on DDoS-hyökkäys ostettuna. Hinnat Zerobotilla vaihtelivat viidestä dollarista 6500 dollariin, jolla sai ostosivuston ylläpitäjien mukaan koko bottiverkon kapasiteetin käyttöön. [71]

Zerobotin haavoittuvuuslista on päivittynyt useita kertoja vuoden 2022 lopussa. Lisättyjen haavoittuvuuksien lisäksi haavoittuvuuksia myös poistettiin, esimerkkinä tästä CVE-2018-12613 poistettiin haittaohjelman ylläpitäjien toimesta. Haittaohjelman käyttämiä haavoittuvuuksia on koottu taulukkoon 6.4 Microsoftin ja CujoAI:n julkaisujen perusteella [72] [73]. Haittaohjelman kohdistamat laitteisiin kuuluu muun muassa palomuurilaitteita, reitittimiä sekä verkossa kiinni olevia kameroita [72].

Haavoittuvuuksien lisäksi Zerobot käyttää sanakirjahyökkäystä. Haittaohjelmalla on käytössä kahdeksan yleistä käyttäjänimeä ja 130 salasanaa, joita yhdistelemällä se tekee hyökkäyksiä IoT laitteisiin SSH ja telnet yhteyksien läpi portteihin 23 sekä 2323. Lisäksi Zerobot yrittää avata ennalta suljettuja portteja niin kutsutulla porttikoputus (engl. port knocking) hyökkäyksellä portteihin 80, 8080, 8888 sekä 2323. [72]

Zerobot on ohjauspalvelinmallinen bottiverkko 4.3.1. [74]

Luokka (CWE)	**Haavoittuus**	**Laite tai Sovellus**
CWE-20	CVE-2014-8361, CVE-2017-17215	Reraltek SDK, Huawei HG532
CWE-22	CVE-2021-41773, CVE-2021-42013	Apache HTTP Palvelimet
CWE-77	CVE-2016-20017, CVE-2022-25075, CVE-2022-26186, CVE-2022-26210, CVE-2022-33891, CVE-2022-34538	D-Link DSL-2750B, TOTOLink, Apache Spark UI, Digital Watchdog DW MEGApix IP kamerat
CWE-78	CVE-2017-17105, CVE-2020-10987, CVE-2020-25223, CVE-2020-25506, CVE-2021-36260, CVE-2021-46422, CVE-2022-30525, CVE-2022-31137, CVE-2022-37061, ZSL-2022-5717	Zivif PR115-204-P-RS, kameroita, Tenda AC15 AC1900, Sophos SG UTM, D-Link DNS-320 FW, Hikvision tuotteet, Telesquare SDT-CW3B1, Zyxel, Roxy-WI, All FLIR AX8 lämpökamera, MiniDVBLinux
CWE-94	CVE-2022-22965	Spring MVC ja Spring WebFlux
CWE-306	CVE-2022-1388	F5 BIG-IP

CWE-78, CWE-287	CVE-2018-10561/10562	Dasan GPON kotireititin
CWE-78, CWE-119, CWE-352	CVE-2019-10655	Grandsteam useampi tuote
CWE-77, CWE-787	CVE-2021-35395	Realtek Jungle SDK
Koodin etäajaminen	CVE-2020-7209	LinuxKI
Komento-injektio		Sapido RB-1732 reititin, PHP 8.1.0-dev

Taulukko 6.4. *Zerobotin käyttämät haavoittuvuudet [73] [72]*

DDoS-hyökkäyksien lista, mitä bottiverkko pystyy tekemään, on pitkä. Listalta löytyy verkkokerrokseen kohdistuvia hyökkäyksiä kuten TCP SYN/ACK tulvahyökkäys, UDP ja ICMP tulvahyökkäykset sekä sovelluskerrokseen kohdistuvia hyökkäyksiä esimerkkinä HTTP-tulvahyökkäys. [72]

Zerobotin skannausstrategia on satunnainen 4.1.1. Se satunnaisgeneroi numeron 0 ja 255 välillä, jota se käyttää ensimmäisenä IP-osoitteen lukuna. Tämän jälkeen haittaohjelma alkaa käymään läpi IP-osoitteita, alkaen arvotusta arvosta. Kun hyökkäyskohteen IP-osoite on valittu, tehdään sille vielä katsaus kuuluko kyseiset IP-osoitteet 61 IP-aliverkon listaan, joka sisältää niin kutsuttuja "hunajapurkkeja". Nämä osoitteet sisältävät tahoja, jotka on luotu varta vasten keräämään informaatiota verkossa leviävistä haittaohjelmista. Näiden avulla tehdään tutkimusta, jotta tulevaisuudessa voidaan löytää ja torjua bottiverkkoja käyttäviä hyökkääjiä. Jos IP-osoite löytyy kyseiseltä listalta, osoitteen skannausta vältetään. [72]

7. TULOKSET JA PÄÄTELMÄT

Tässä luvussa käsitellään tuloksia liittyen haittaohjelmista kerättyyn tietoon perustuen. Ensin esitellään bottiverkoista koostettu koko, hyökkäysteho, haavoittuvuuksien määrä sekä arkkitehtuuri tiedot kuvaajina sekä taulukoina selitteiden kanssa, jonka jälkeen esitellystä datasta yritetään etsiä trendejä bottiverkoista. Analyysia datasta on luvussa 2.

7.1 Bottiverkkojen data

Zerobot ja Echobot jouduttiin jättämään pois bottiverkkojen koko ja hyökkäysteho taulukoista, sillä niistä ei löytynyt dataa näihin vertailuihin. Echobotista kokojen arviot olivat vain summittaisia ja Zerobotin arvojen puuttuminen johtuu todennäköisesti siitä, että se on suhteellisen uusi, eikä tutkimusta ole vielä ehditty tehdä tai julkaista.

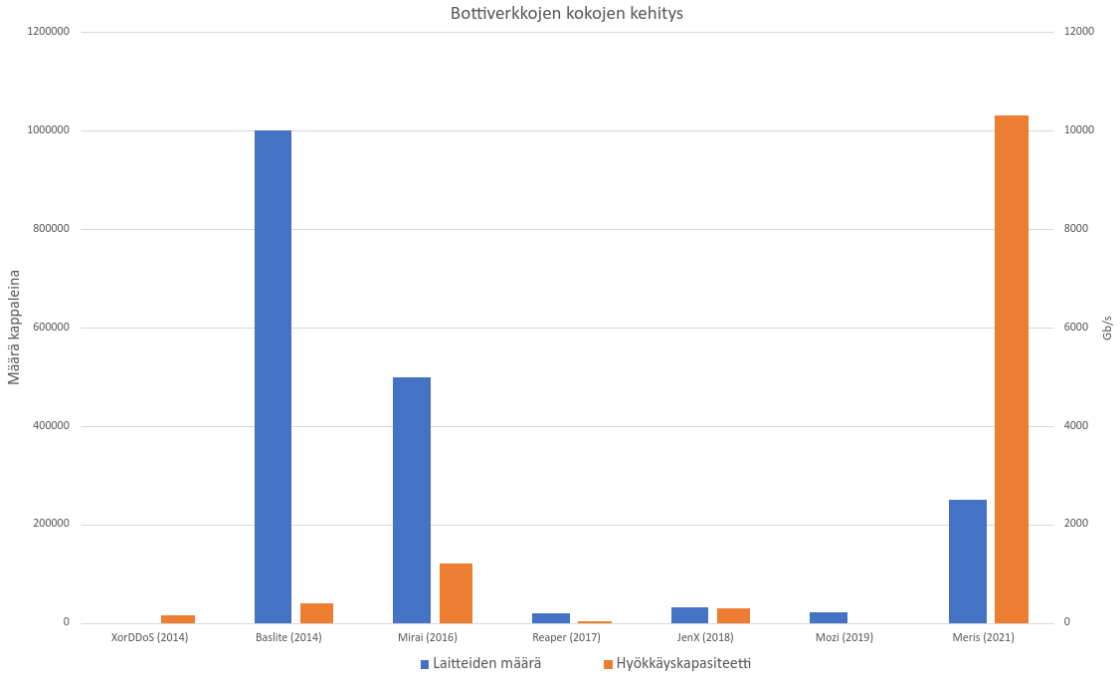
Vajaata tietoa löytyi muutamasta bottiverkosta. XorDDoS haittaohjelman leviämislaajuudesta vuodelta 2015, jolloin se oli laajimmillaan, ei löytynyt, mutta sen tekemistä hyökkäyksistä löytyi koko tietoa. Vuoden 2019 Mozi verkosta puolestaan oli tehty tutkimusta, jolloin sen levittäytymislaajuus löytyi, mutta siitä ei löytynyt hyökkäyskapasiteetti tietoja. JenX ei löytynyt bottiverkon virallista kokoa ei löytynyt, joten siitä käytetään haavoittuvaisten laitteiden viitteellistä maksimi arvoa 32000, jonka Palo Alton Unit 42 oli arvioinut.

Meriksen hyökkäysteho löytyi yksikössä rps (engl. request per second, kutsuja sekunnissa). Saadakseen muihin verrannollista dataa, täytyy tämä muuttaa GBps muotoon. Vaikka HTTP kutsujen koot vaihtelevat paljon lähtien 200 tavusta yli 2 kilotavuun, SPDY projekti on kertonut keskimääräisen HTTP kutsun otsikkotietojen kooksi noin 700–800 B [75]. Kun käytetään tätä 800B HTTP kutsun kokona saadaan hyökkäystehoksi

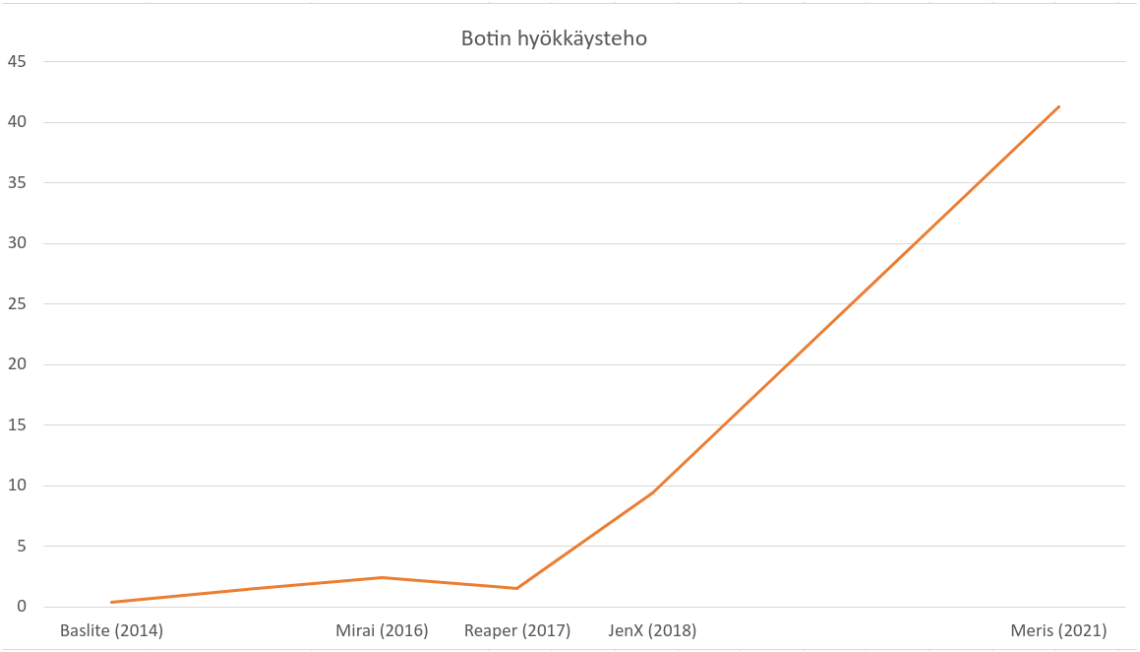
$$17200000000rps * 800B * 10^{-9} = 13760GBps \tag{7.1}$$

jota voidaan käyttää arvona vertailuja tehdessä. Kuvaajissa 7.1 ja 7.2 on koottu yhteen bottiverkkojen kokoja ja niiden hyökkäystehoja.

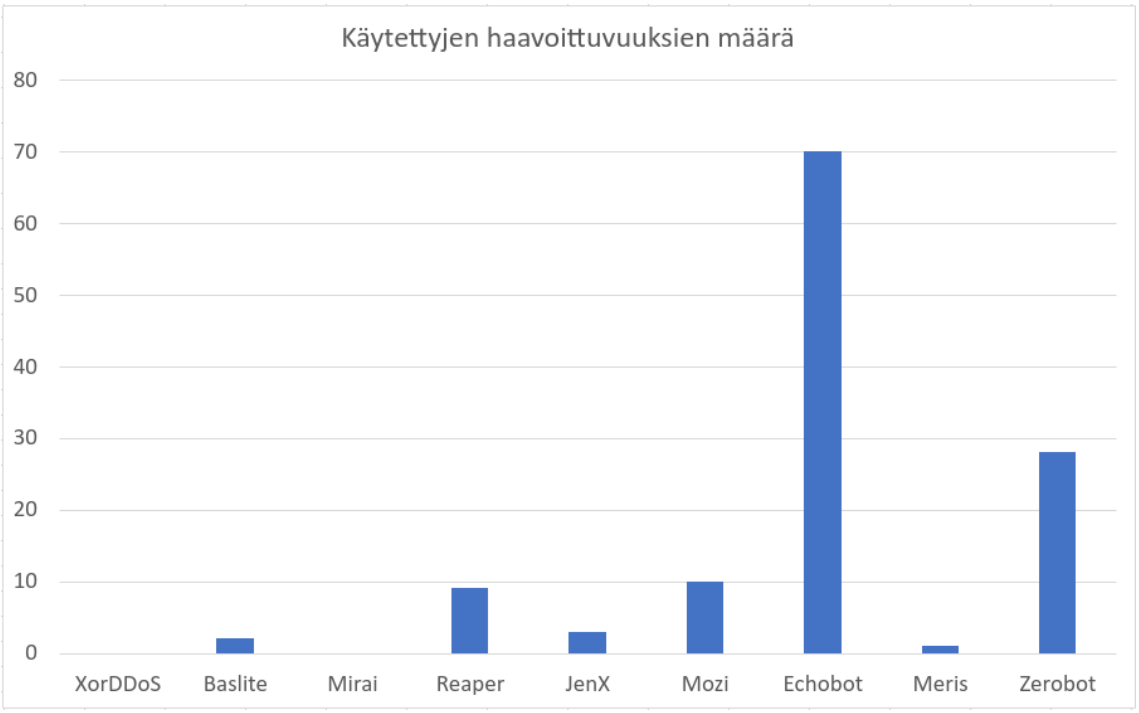
Kuvaajasta 7.3 näkyy, montako haavoittuvuutta on käytössä missäkin haittaohjelmassa. Luvuissa ei ole otettu mukaan sanakirjahyökkäystä, sillä se oli käytössä kaikissa haittaohjelmissa.



Kuva 7.1. *Bottiverkkojen koot ja hyökkäystehot*



Kuva 7.2. *Hyökkäysteho/bottien määrällä*



Kuva 7.3. *Bottiverkoissa käytettyjen haavoittuvuuksien määrä*

Haittaohjelma	**Arkkitehtuuri**
XorDDoS	Ohjauspalvelinmalli
BASHLITE	Ohjauspalvelinmalli tai IRC-malli
Mirai	Ohjauspalvelinmalli
Reaper	Arkkitehtuurimalli puuttuu
JenX	Ohjauspalvelinmalli
Mozi	Vertaisverkko
Echobot	Ohjauspalvelinmalli
Meris	Ohjauspalvelinmalli
Zerobot	Ohjauspalvelinmalli

Taulukko 7.1. *Haittaohjelmien arkkitehtuurit*

Taulukkoon 7.1 on koottu kaikkien työssä käsiteltyjen haittaohjelmien kommunikaatio arkkitehtuurit listaan.

7.2 Haittaohjelmien trendit

Alun perin tutkimusta aloittaessa ajateltiin, että haittaohjelmien arkkitehtuureissa olisi siirrytty keskitetyistä bottiverkoista käyttämään laajemmin vertaisverkko arkkitehtuuria 4.3.5 sen monien hyötyjen vuoksi. Kuitenkin datan perusteella voidaan huomata, että ohjauspalvelinmalliset verkot ovat selkeästi vielä enemmistössä. Tämä näkyy selkeästi taulukosta 7.1, johon on koottu kaikkien tässä työssä käsiteltyjen haittaohjelmien arkkitehtuurit.

Tämän voisi ajatella johtuvan siitä, että edelleen iso osa haittaohjelmista pohjaa Mirain 6.3 julkaistuihin lähdekoodeihin. Avoimen jaon piiriin ei ole vielä tähän päivään mennessä julkaistu vertaisverkkoarkkitehtuurin koodeja, vaikka sen arkkitehtuurin omaavia haittaohjelmia kuten Mozi 6.6 aina välillä luodaan.

Bottiverkkojen koosta ja hyökkäystehoista saatu data oli hyvin vajaata. Maksimihyökkäystehoja ei saatu selvitettyä, mutta taulukoissa käytettiin bottiverkkojen suurimpien hyökkäysten tehoja ja bottiverkkojen koot olivat parhaimmassakin tapauksessa arvioita.

Datasta saatiin selville, ettei bottiverkkojen koot eivät bottimäärällisesti ole kasvaneet merkittävästi viime vuosien aikana. Missä bottiverkot puolestaan ovat kehittyneet, miten botteja hyödynnetään. Kuten kuvaajasta 7.2 voi nähdä, voidaan vetää johtopäätös siitä, että yksittäisiä botteja saadaan hyödynnettyä nykyään paremmin.

Bottiverkkojen kasvun puutetta ei mielestäni kannata ajatella johtuvan siitä, että tietoturva olisi parantunut, koska edelleen bottiverkkoja nousee pintaan, vaan enemmänkin siitä, ettei massiivisille bottiverkoille ole tarvetta. Koska myös pienillä bottiverkoilla, kuten JenX 6.5, voidaan saavuttaa merkittäviä taloudellisia etuja DDoS-palveluna kaltaisella liiketoiminnalla keskittyen toimialoihin, kuten peliteollisuus tai muihin pienempiin hyökkäyskohteisiin, ei ylläpitäjillä ole tarvetta käyttää resursseja massiivi bottiverkkojen muodostamiseen.

Tämän sanottua, verkot kuten Meris 6.8 kuitenkin osoittavat, etteivät suuret bottiverkot suurine hyökkäystehoineen ole katoamassa mihinkään. Meriksestä on jo tehty muunnos nimeltään Mantis, joka kylläkin keskittää hyökkäyksensä virtuaalikoneisiin sekä palvelimiin, jonka takia se ei ole ollut mukana tässä vertailussa [48].

Kuvaajasta 7.3 voidaan nähdä sanakirjahyökkäyksistä poikkeavien haavoittuvuuksien käytön nousseen selkeästi vuoden 2016 jälkeen. Kuvaajasta voidaan myös huomata, että haavoittuvuuksien määrä on ollut muutamista kymmeniin. Selkeä poikkeus on Echobot, joka oli tunnettu suuresta varastosta haavoittuvuuksia 6.7. Kuitenkin on olemassa haittaohjelmia, jotka selkeästi tähtäävät tiettyyn laitevalmistajaan tai laitteryhmään sen sijaan,

että yrittävät levittäytyä mahdollisimman laajalle. Tästä esimerkkinä Meris 6.8, joka käytti vain muutamaa haavoittuvuutta hyväkseen ja keskittyi levittäytymään näihin laitteisiin.

CVE:t mitä haittaohjelmat käyttävät, sisältävät yleensä päivitettyjä haavoittuvuuksia samalta vuodelta, miltä haittaohjelma julkaistaan. Haavoittuvuudet mitä käytetään kuuluvat datan, bottiverkoista eriteltyjen haavoittuvuuksien mukaan, kuitenkin yleensä kategoioihin CWE-78, CWE-77 sekä CWE-20. Kuitenkin muita satunnaisia kategorioita voi löytyä joukosta.

7.3 Muita merkittäviä havaintoja

Viimeisenä huomiona voisi sanoa, että vanhat haittaohjelmat eivät ole kadonneet mihinkään uusien tieltä. Esimerkiksi XorDDoS 6.1 haittaohjelmasta Microsoft oli vuonna 2022 tehnyt havaintoja sen aktiivisuuden selkeästä noususta. Tiettyihin haittaohjelmiin on sisäänrakennettu tapa päivittää niiden koodeja, tällainen oli esimerkiksi Echobotilla 6.7, joka päivitti sen käyttämiä haavoittuvuuslistaa olemassaolonsa aikana. Haavoittuvuuksia lisättiin, mutta niitä myös poistettiin.

Viimeinen tapa, millä haittaohjelmat ovat pysyneet elossa on työssä jo moneen kertaan mainittu muunnosten tekeminen. Suurin osa tässä työssä käsiteltävistä haittaohjelmista on muunnelmia jo jostain aikaisemmin julkaistuista haittaohjelmasta tai niiden yhdistelmistä. Jos muunnelmat ovat itsessään kasvaneen isoiksi, tai niihin on tehty paljon koodimuutoksia, on ne katsottu olevan uusia haittaohjelmia.

IoT-laitteet, joihin haittaohjelmien hyökkäykset ovat kohdistuneet, ovat todella paljon riippuvaisia CVE:sta, joita haittaohjelma käyttää, mutta muutamia kestosuosikkeja selkeästi on havaittavissa. Reitittimet, valvontajärjestelmät, kamerat ja digitaaliset videonauhurit ovat olleet suuria suosikkeja hyökkäyslaitteissa.

Bottiverkot eivät ole katoamassa mihinkään. Niin kauan kuin laitteista tullaan löytämään haavoittuvuuksia, tullaan niitä myös käyttämään haitallisiin tarkoituksiin. Bottiverkkojen koot eivät välttämättä tule kasvamaan, mutta haittaohjelmien määrät voivat hyvinkin lisääntyä ennestään. Mitä enemmän haittaohjelmia julkaistaan avoimeen jakeluun, sitä enemmän uusilla hyökkääjillä on työkaluja muodostaa uusia verkkoja.

Tutkimusta haittaohjelmista tarvittaisiin lisää, jotta voitaisiin paremmin ymmärtää ja vastata näiden uhkien kasvavaan monimutkaisuuteen ja esiintyvyyteen sekä mahdollisesti ennustaa tulevia uhkia. Nykypäivän digitaalisessa maailmassa haittaohjelmat ovat vakava tietoturvariski niin yksityishenkilöille kuin organisaatioillekin. Varsinkin akateemista tutkimusta aiheesta oli hyvin rajallisesti, eivätkä yritysten julkaisut vastanneet kaikkiin kysymyksiin.

8. YHTEENVETO

IoT-laitteiden yleistymisen myötä, myös niiden tietoturvaongelmat ovat nousseet merkittäväksi haasteeksi. Yhtenä isona ongelmana ovat bottiverkot ja näiden mahdollisuus tehdä DDoS-hyökkäyksiä eri yksityisyrityksistä julkisiin palveluihin. Tämän työn tavoitteena on tutkia, miten viime vuosien aikana DDoS-kykenevät IoT-laitteista koostuvat bottiverkot ovat kehittyneet ja minkälaisia pääpiirteitä niissä on havaittavissa. Työssä käyty läpi DDoS-hyökkäyksien mahdollistajia, motiiveja sekä bottiverkkojen yleistä toimintamallia. Työssä myös lyhyesti käytiin läpi mitä tekoja on tehty EU:ssa, Suomessa ja mitä voidaan tehdä yrityksissä DDoS-hyökkäysten haittavaikutusten minimoimiseksi. Työn aihe valikoitui omasta kiinnostuksesta sekä sen ajankohtaisuudesta, vaikka tämä toikin omat haasteensa työhön.

Tutkimusmetodina käytettiin kirjallisuuskatsausta. Käsiteltävä aineisto etsittiin pääasiassa eri yritysten julkaisuista sekä akateemista tutkimusta IoT-haittaohjelmista ja tartutetuista laitteista koostuvista bottiverkoista. Tämä yhdistelmä antoi mahdollisuuden tarkastella yhdeksän valikoidun haittaohjelman piirteitä. Löydetyn tieto koottiin luvussa 7 yhteen sekä tehtiin johtopäätöksiä haittaohjelmien kehityksen suhteen.

Työn tutkimuskysymys oli, miten DDoS-kykenevät IoT-laitteista koostuvat bottiverkot ovat kehittyneet viimevuosien aikana. Tutkimustuloksiksi saatiin, ettei haittaohjelmissa ole tapahtunut noin vuoden 2016 jälkeen isoja merkittäviä muutoksia arkkitehtuureissa tai bottien määrissä. Haittaohjelmissa käytössä olleiden haavoittuvuuksien määrä on CVE käytön mukaan tulon jälkeen myös vuonna 2016 pysynyt mukana, mutta nekään ei ole merkittävästi kasvanut. Kuitenkin yksittäisten bottien hyökkäysteho on datan mukaan kasvanut jonkun verran. Myös eräs löydös haittaohjelmia tutkiessa oli, että useat haittaohjelmat olivat jo ennalta käytössä olleiden muunnelmia. Pohjalla käytettiin monesti, ja käytettiin myös uudemmissa haittaohjelmissa, Mirai 6.3 haittaohjelmaa, jonka lähdekoodit julkaistiin verkossa vuonna 2016.

Eräs työn haaste oli vetää raja siihen, mikä lasketaan IoT-laitteeksi ja mihin vetää raja, mitä bottiverkkoja otetaan mukaan tutkimukseen. Lopulta päädyttiin DDoS-kykeneviin verkkoihin, koska se oli selkeä kokonaisuus ja näitä bottiverkkoja löytyi paljon. Toinen, mikä olisi voinut olla vaihtoehto, olisi ollut kryptolouhintaan keskittyvät verkot, mutta näiden määrä on huomattavasti rajatumpi ja aineiston hankkiminen olisi ollut entistä haasta-

vampaa. Kryptolouhintaan kykenevät bottiverkot voisi olla eräs ehdotus jatkotutkimusaiheeksi. IoT-laite rajaus puolestaan oli haastava. Monet verkot liittävät itseensä selvästi IoT-laitteisiin luettavien verkossa kiinni olevien kameroiden, digitaalisten videonauhurien, kotien valvontajärjestelmien lisäksi myös reitittimiä, joiden IoT-laite status ei ole selkeä. Missä menee raja IoT-laite pohjaiselle bottiverkolle, jos verkko liittää itseensä pelkästään reitittimiä? Tämmöisiä tapauksia ei tullut tutkimuksessa onneksi vastaan, mutta IoT-termi on yleisesti hyvin haastava, vaikka sitä paljon käytetään.

Toinen haaste oli löytää tarpeeksi luotettavaa aineistoa. Akateemista aineistoa yksittäisistä haittaohjelmista löydettiin hyvin rajatusti ja se peilautuu myös tutkimustuloksiin. Esimerkiksi bottiverkkojen kokojen arvioita ja niiden hyökkäyskapasiteetteja tai edes bottiverkoilla tehtyjä hyökkäyksiä oli haastava löytää. Aineistohaussa huomattiin, että IoT-laitteista koostuvista bottiverkoista tehty akateeminen tutkimus keskittyi pariin isoimpaan ja tunnetuimpaan haittaohjelmaan. Näitäkin artikkeleita löydettiin alle kymmenen. Yritysten tekemiä tutkimuksia löytyi huomattavasti enemmän, mutta silti yksittäisiin IoT-haittaohjelmiin keskittyviä akateemisia julkaisuja olisi kaivannut lisää. Jatkotutkimusehdotuksena olisikin, että IoT-haittaohjelmien teknistä analysointia sekä niiden elinkaarien seurantaa voisi tehdä enemmän.

LÄHTEET

[1] M. Ramgir, *Internet of Things*, eng, 1st edition. Pearson Education India, 2019, ISBN: 93-5394-152-0.

[2] “Internet of things”. (May 7, 2016), [Online]. Available: https://en.idate.org/internet-of-things-2/ (visited on 02/10/2023).

[3] “Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030”. (Jul. 2022), [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (visited on 02/10/2023).

[4] N. Hoque, D. K. Bhattacharyya ja J. K. Kalita, ”Botnet in DDoS Attacks: Trends and Challenges”, eng, *IEEE Communications surveys and tutorials*, vol. 17, nro 4, s. 2242–2270, 2015, ISSN: 1553-877X.

[5] R. Swami, M. Dave ja V. Ranga, ”Software-defined Networking-based DDoS Defense Mechanisms”, eng, *ACM computing surveys*, vol. 52, nro 2, s. 1–36, 2019, ISSN: 0360-0300.

[6] “Understanding denial-of-service attacks”. (Nov. 4, 2009), [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-015 (visited on 02/10/2023).

[7] P. J. Deitel, *Internet & World Wide Web : how to program*, 5th edition. Pearson, 2012.

[8] G. Davies, *Networking fundamentals : develop the networking skills required to pass the Microsoft MTA networking fundamentals exam 98-366*, eng, 1st edition. Birmingham, England ; Packt, 2019, ISBN: 1-83864-874-7.

[9] C. Mishra, *Mastering Wireshark : analyze data network life a professional by mastering Wireshark- from 0 to 1337*, eng, 1st edition, sarja Community experience distilled. Birmingham: Packt Publishing, 2016 - 2016, s. 2–5, ISBN: 1-78398-953-X.

[10] I. S. Syngress Media ja Syngress, *Designing a Wireless Network: Understand How Wireless Communication Works*, eng. Rockland: Elsevier Science & Technology Books, 2001, s. 74–81, ISBN: 9781928994459.

[11] C. Panek, *Networking fundamentals*, eng, 1st edition. Sybex, 2020, s. 45–68, ISBN: 1-119-65069-0.

[12] M. M. Alani, *Guide to OSI and TCP/IP Models*, eng, 1. painos, sarja SpringerBriefs in Computer Science. Cham: Springer International Publishing AG, 2014, ISBN: 3319051512.

[13] E. E. U. A. F. Cybersecurity. ”Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape”. (3. marraskuuta 2022), (viitattu 23. 05. 2023).

[14] ”Enisa Threat Landscape 2022”, European Union Agency For Cybersecurity, tekninen raportti, lokakuu 2022.

[15] ”What is a ransom DDoS attack?” (), url: https://www.cloudflare.com/en-gb/learning/ddos/ransom-ddos-attack/ (viitattu 13. 04. 2023).

[16] A. N. S. Team. ”2022 in review: DDoS attack trends and insights”. (21. helmikuuta 2023), (viitattu 23. 05. 2023).

[17] Kyberturvallisuuskeskus. ”Kyberturvallisuuskeskuksen viikkokatsaus - 52/2022”. (30. joulukuuta 2022), (viitattu 23. 05. 2023).

[18] A. Tsotsis. “Riaa goes offline, joins mpaa as latest victim of successful ddos attacks”. (Sep. 19, 2010), [Online]. Available: https://techcrunch.com/2010/09/19/riaa-attack/ (visited on 06/02/2023).

[19] A. Maxwell. “4chan to ddos riaa next – is this the protest of the future?” (Sep. 19, 2010), [Online]. Available: https://torrentfreak.com/4chan-to-ddos-riaa-next-is-this-the-protest-of-the-future-100919/ (visited on 06/02/2023).

[20] M. De Donno, N. Dragoni, A. Giaretta ja A. Spognardi, ”DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation”, eng, *Security and communication networks*, vol. 2018, s. 1–30, 2018, ISSN: 1939-0114.

[21] J. Mirkovic ja P. Reiher, ”A taxonomy of DDoS attack and DDoS defense mechanisms”, eng, *Computer Communication Review*, vol. 34, nro 2, s. 39–53, 2004, ISSN: 0146-4833.

[22] S. H. C. Haris, R. B. Ahmad ja M. A. H. A. Ghani, ”Detecting TCP SYN Flood Attack Based on Anomaly Detection”, eng, teoksessa *2010 Second International Conference on Network Applications, Protocols and Services*, IEEE, 2010, s. 240–244, ISBN: 1424480485.

[23] B. N. Ramkumar ja T. Subbulakshmi, ”Tcp Syn Flood Attack Detection and Prevention System using Adaptive Thresholding Method”, eng, *ITM Web of Conferences*, vol. 37, s. 1016–, 2021, ISSN: 2271-2097.

[24] S. Specht ja R. Lee, ”Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures”, eng, 16. toukokuuta 2003.

[25] “What is a udp flood attack?” (), [Online]. Available: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (visited on 05/13/2023).

[26] “What is a udp flood ddos attack?” (), [Online]. Available: https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack (visited on 05/13/2023).

[27] S. Kumar, ”Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet”, eng, teoksessa *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, IEEE, 2007, s. 25–25, ISBN: 0769529119.

[28] Ö. KASIM, ”A Robust DNS Flood Attack Detection with a Hybrid Deeper Learning Model”, eng, *Computers & electrical engineering*, vol. 100, s. 107 883–, 2022, ISSN: 0045-7906.

[29] R. Alonso, R. Monroy ja L. A. Trejo, ”Mining IP to Domain Name Interactions to Detect DNS Flood Attacks on Recursive DNS Servers”, eng, *Sensors (Basel, Switzerland)*, vol. 16, nro 8, s. 1311–, 2016, ISSN: 1424-8220.

[30] D. S. M. Gonçalves, R. S. Couto ja M. G. Rubinstein, ”A Protection System Against HTTP Flood Attacks Using Software Defined Networking”, eng, *Journal of network and systems management*, vol. 31, nro 1, s. 16–, 2023, ISSN: 1064-7570.

[31] ”Ohje 3/2016 Palvelunestohyök- käysten ehkäisy ja torjunta”. (maaliskuu 2016), url: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf (viitattu 24. 04. 2023).

[32] ”What is the internet of things (IoT)?” (), url: https://www.ibm.com/topics/internet-of-things.

[33] H. Binsalleeh, T. Ormerod, A. Boukhtouta et al., ”On the analysis of the Zeus botnet crimeware toolkit”, eng, teoksessa *2010 Eighth International Conference on Privacy, Security and Trust*, IEEE, 2010, s. 31–38, ISBN: 9781424475513.

[34] R. McGarvey, ”Zeus Botnets Are Taken Down by Unique Team”, eng, *Credit Union Times*, 2012, ISSN: 1058-7764.

[35] B. Vignau, R. Khoury, S. Hallé ja A. Hamou-Lhadj, ”The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives”, eng, *Journal of systems architecture*, vol. 116, s. 102 143–, 2021, ISSN: 1383-7621.

[36] ”National Vulnerability Database”. (), url: https://nvd.nist.gov/ (viitattu 28. 08. 2023).

[37] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah ja R. Alfaris, ”Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art”, eng, *International journal of computer applications*, vol. 49, nro 7, s. 24–32, 2012, ISSN: 0975-8887.

[38] P. Kumari ja A. K. Jain, ”A comprehensive study of DDoS attacks over IoT network and their countermeasures”, eng, *Computers & security*, vol. 127, s. 103 096–, 2023, ISSN: 0167-4048.

[39] ——, ”A comprehensive study of DDoS attacks over IoT network and their countermeasures”, eng, *Computers & security*, vol. 127, 2023, ISSN: 0167-4048.

[40] ”Kyberturvallisuus: miten EU torjuu kyberuhkia?” (23. tammikuuta 2023), url: https://www.consilium.europa.eu/fi/policies/cybersecurity/ (viitattu 02. 04. 2023).

[41] ”Älylaitteiden heikko tietoturva sääntelyllä kuriin”. (27. tammikuuta 2023), url: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alylaitteiden-heikko-tietoturva-saantelylla-kuriin (viitattu 02. 04. 2023).

[42] ”Secure solutions for the Internet of Things”. (7. kesäkuuta 2022), url: https://digital-strategy.ec.europa.eu/en/policies/secure-internet-things (viitattu 02. 04. 2023).

[43] ”GDPR and Internet of Things (IoT)”. (), url: https://legalitgroup.com/en/gdpr-and-internet-of-things-iot/ (viitattu 12. 10. 2023).

[44] Kyberturvallisuuskeskus. ”Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa”. (26. marraskuuta 2019), url: https://www.kyberturvallisuuskeskus.

fi / fi / ajankohtaista / suomi - aloittaa - alylaitteiden - turvallisuuden - varmistamisen - ensimmaisena-euroopassa (viitattu 02. 04. 2023).

[45] DEKRA. ”What is ETSI EN 303 645 Cybersecurity Standard?” (19. heinäkuuta 2021), url: https://www.dekra-product-safety.com/en/what-is-etsi-en-303-645-cybersecurity-standard (viitattu 02. 04. 2023).

[46] ”ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines”. (2022), url: https://www.iso.org/standard/44373.html (viitattu 17. 04. 2023).

[47] ”CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”, ETSI EUROPEAN STANDARD, Sophia Antipolis Cedex - FRANCE, Standard, kesäkuu 2020.

[48] CloudFlare. ”Mantis - the most powerful botnet to date”. (14. heinäkuuta 2022), url: https://blog.cloudflare.com/mantis-botnet/ (viitattu 04. 04. 2023).

[49] J. W. Seo ja S. J. Lee, ”A study on efficient detection of network-based IP spoofing DDoS and malware-infected Systems”, eng, *SpringerPlus*, vol. 5, nro 1, s. 1878–1878, 2016, ISSN: 2193-1801.

[50] M. 3. D. R. Team. ”Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices”. (12. syyskuuta 2022), url: https://www.microsoft.com/en-us/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices (viitattu 12. 04. 2023).

[51] ”2021 IBM Security X-Force Cloud Threat Landscape Report”. (2021), url: https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775 (viitattu 24. 08. 2023).

[52] T. Seals. ”Gafgyt Botnet Lifts DDoS Tricks from Mirai”. (15. toukokuuta 2021), url: https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/ (viitattu 21. 04. 2023).

[53] A. Marzano, D. Alexander, O. Fonseca et al., ”The Evolution of Bashlite and Mirai IoT Botnets”, eng, teoksessa *2018 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, 2018, s. 00 813–00 818, ISBN: 9781538669501.

[54] A. Saracino ja P. Mori, ”Towards a Framework for Testing the Security of IoT Devices Consistently”, eng, teoksessa *Emerging Technologies for Authorization and Authentication*, sarja Lecture Notes in Computer Science, vol. 11263, Switzerland: Springer International Publishing AG, 2018, s. 88–102, ISBN: 9783030043711.

[55] ”Cyber Case Study: The Mirai DDoS Attack on Dyn”. (10. tammikuuta 2022), url: https://coverlink.com/case-study/mirai-ddos-attack-on-dyn/ (viitattu 24. 08. 2023).

[56] P. Moriuchi ja S. Chohan, ”Mirai-variant iot botnet used to target financial sector in january 2018”, *Recorded Future Cyber Threat Analysis Report*, s. 118–140, 2018.

[57] ”JenX: A New Botnet Threatening All”. (31. tammikuuta 2018), url: https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/jenx/ (viitattu 18. 04. 2023).

[58] M. Smii. ”JenX , New IoT Botnet”. (3. helmikuuta 2018), url: https://medium.com/secjuice/jenx-new-iot-botnet-c412d5a446ee (viitattu 18. 04. 2023).

[59] A. Davila. ”Home & Small Office Wireless Routers Exploited to Attack Gaming Servers”. (31. lokakuuta 2019), url: https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/ (viitattu 18. 04. 2023).

[60] T.-F. Tu, J.-W. Qin, H. Zhang, M. Chen, T. Xu ja Y. Huang, ”A comprehensive study of Mozi botnet”, eng, *International journal of intelligent systems*, vol. 37, nro 10, s. 6877–6908, 2022, ISSN: 0884-8173.

[61] D. McMillen, W. Gao ja C. DeBeck. ”Botnet Attack: Mozi Mozied Into Town”. (17. syyskuuta 2020), url: https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/ (viitattu 05. 04. 2023).

[62] David Atch and Gil Regev and Ross Bevington. ”How to proactively defend against Mozi IoT botnet”. (19. elokuuta 2021), url: https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/ (viitattu 05. 04. 2023).

[63] B. Wang, Y. Sang, Y. Zhang, S. Li ja X. Xu, ”A longitudinal Measurement and Analysis Study of Mozi, an Evolving P2P IoT Botnet”, teoksessa *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2022, s. 117–122. DOI: 10.1109/TrustCom56396.2022.00027.

[64] E. Kreminchuker ja M. Zavodchik. ”Echobot Malware Now up to 71 Exploits, Targeting SCADA”. (17. joulukuuta 2019), url: https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada# (viitattu 24. 04. 2023).

[65] L. Cashdollar. ”Latest ECHOBOT: 26 Infection Vectors”. (13. kesäkuuta 2019), url: https://www.akamai.com/blog/security/latest-echobot-26-infection-vectors (viitattu 24. 04. 2023).

[66] R. Nigam. ”Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities”. (13. joulukuuta 2019), url: https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/ (viitattu 24. 04. 2023).

[67] M. Safaei Pour, A. Mangino, K. Friday et al., ”On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild”, eng, *Computers & security*, vol. 91, s. 101 707–20, 2020, ISSN: 0167-4048.

[68] QratorLabs. ”Mēris botnet, climbing to the record”. (9. syyskuuta 2021), url: https://qratorlabs.medium.com/m%C4%93ris-botnet-climbing-to-the-record-f992271120f (viitattu 12. 04. 2023).

[69] V. Ganti ja O. Yoachimik. ”A Brief History of the Meris Botnet”. (11. syyskuuta 2021), url: https://blog.cloudflare.com/meris-botnet/ (viitattu 12. 04. 2023).

[70] V. Petkauskas. ”We’ve seen just the tip of the Mēris botnet iceberg”. (14. maaliskuuta 2021), url: https://cybernews.com/security/weve-seen-just-the-tip-of-the-meris-botnet-iceberg/ (viitattu 12. 04. 2023).

[71] C. Glover. ”Zerobot is the next big botnet-for-hire. Enterprise IoT devices don’t stand a chance”. (25. tammikuuta 2023), url: https://techmonitor.ai/technology/cybersecurity/zerobot-botnet-enterprise-iot (viitattu 25. 04. 2023).

[72] R. Sde-Or, I. Sivan, G. Regev et al. ”Microsoft research uncovers new Zerobot capabilities”. (21. joulukuuta 2022), url: https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/ (viitattu 18. 04. 2023).

[73] G. Lupták. ”The Zerobot Botnet: Vulnerabilities Targeted and Exploits Used in Detail”. (3. tammikuuta 2023), url: https://cujo.com/the-zerobot-botnet-vulnerabilities-targeted-and-exploits-used-in-detail/ (viitattu 18. 04. 2023).

[74] C. Lin. ”Zerobot – New Go-Based Botnet Campaign Targets Multiple Vulnerabilities”. (6. joulukuuta 2022), url: https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities (viitattu 18. 04. 2023).

[75] ”PageSpeed: Minimize request size”. (), url: https://www.chromium.org/spdy/spdy-whitepaper/ (viitattu 12. 10. 2023).