Tommi Sampo

IoT ja hajautetut palvelunestohyökkäykset

Tietotekniikan kandidaatintutkielma

5. lokakuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Tommi Sampo

Yhteystiedot: tommi.sampo@gmail.com

Työn nimi: IoT ja hajautetut palvelunestohyökkäykset

Title in English: IoT and distributed denial of service attacks

Työ: Kandidaatintutkielma

Sivumäärä: 34+0

Tiivistelmä: IoT-laitteiden määrä on kasvanut viime vuosien aikana ja kasvun ennustetaan jatkuvan. Samanaikaisesti IoT-botnettien ja niiden avulla suoritettujen palvelunestohyökkäysten määrä on lisääntynyt. Tässä tutkielmassa tarkastellaan palvelunestohyökkäyksiä ja selvitetään IoT-laitteille ominaisia tietoturvahaavoittuvuuksia, jonka jälkeen käsitellään IoT-botnettejä yleisesti, sekä tämän hetken merkittävimpiä IoT-botnettejä tarkemmin. IoT-laitteissa on useita vakavuudeltaan eritasoisia haavoittuvuuksia. Niistä IoT-botnettien kannalta vakavimmat haavoittuvuudet ovat laitteiden saavutettavuus julkisen internetin yli, avoimet tai huonosti suojatut protokollat, kuten telnet ja UPnP sekä oletussalasanat. Tämänhetkisistä IoT-botneteistä merkittävin on Mirai, mutta sillä on useita varteenotettavia kilpailijoita.

Avainsanat: IoT, esineiden internet, DDoS, hajautettu palvelunestohyökkäys, botnet

Abstract: The number of IoT devices has grown in recent years and the growth is predicted to continue. Simultaneously, the number of IoT botnets and distributed denial of service attacks performed using these botnets has increased. The purpose of this study is to examine denial of service attacks and investigate vulnerabilities characteristic to IoT devices, as well as the general aspects of IoT botnets and the specifics of today's most prominent botnets. IoT devices possess several vulnerabilities of varying severity. The most significant of these in regards to IoT botnets are the accessibility of devices via the public internet, open or insecure protocols such as telnet or UPnP, and default passwords. Mirai is currently the most prominent IoT-botnet but it has several noteworthy competitors.

Keywords: IoT, Internet of Things, DDoS, Distributed Denial of Service attack, botnet

Kuviot

Sisältö

1 Johdanto

Tämän tutkielman tarkoituksena on tarkastella IoT-botnettien toimintaa hajautettujen palvelunestohyökkäysten näkökulmasta. Tähän sisältyy IoT-botnettien käyttämien palvelunestohyökkäystyyppien ja IoT-laitteille ominaisten tietoturvahaavoittuvuuksien selvittäminen, yleinen IoT-botnetin arkkitehtuuri, rakenne ja toiminta sekä tämän hetken merkittävimmät botnetit ja niiden yksityiskohtaisempi tarkastelu. Internet of Things (IoT) eli esineiden internet tarkoittaa sulautettujen laitteiden muodostamaa verkkoa, jotka ovat vuorovaikutuksessa ympäristönsä tai oman sisäisen tilansa kanssa ja pystyvät välittämään tätä tietoa eteenpäin (Gartner 2018). IoT-laitteiden määrä on kasvanut 6,4 miljardista vuonna 2016 yli 11 miljardiin vuonna 2018 ja määrän odotetaan nousevan yli 20 miljardiin vuoteen 2020 mennessä (Gartner 2017; Nordrum 2016). Useiden laitteiden suunnittelussa on kiinnitetty huomiota tietoturvallisuuteen vain vähän tai ei ollenkaan (Angrishi 2017). Tämän vuoksi iso osa laitteista ovat haavoittuvaisia eri tietoturva-aukkojen, kuten oletussalasanojen, injektiohyökkäysten ja salaamattoman tietoliikenteen kautta (Bertino ja Islam 2017; Kumar, Madhuri ja ChanneGowda 2017). Kuluttajille suunnatut IoT-laitteet ovat usein sulautettu arkipäiväisiin esineisiin, joten on hyvin mahdollista, ettei käyttäjä tiedä niiden haavoittuvaisuudesta. Vaikka monet tietoturvallisuutta ja yksityisyyttä koskevat periaatteet soveltuvat myös kuluttajalaitteille, kuluttajilla on harvemmin resursseja tai asiantuntemusta niiden toteuttamista varten (Lin ja Bergmann 2016). Tietoturva-aukkoja hyväksikäyttämällä laitteet pystytään tartuttamaan haittaohjelmilla ja luomaan hajautettu verkko toisiinsa yhdistettyjä laitteita eli botnet, jota käyttämällä voidaan suorittaa palvelunestohyökkäyksiä tai muita kyberrikoksia (Angrishi 2017; Bertino ja Islam 2017; Raghavan ja Dawson 2011). Yksi tämän hetken merkittävimmistä IoT-botneteistä on vuonna 2016 havaittu Mirai, jonka arvioidaan sisältävän hieman yli puoli miljoonaa laitetta (Angrishi 2017).

Luvussa 2 käsitellään ensin palvelunestohyökkäysten taksonomiaa ja yleisimpiä IoT-botnettien käyttämiä palvelunestohyökkäyksiä, jonka jälkeen luvussa 3 tarkastellaan IoT-laitteiden tietoturvallisuutta ja haavoittuvuuksia. Luvussa 4 tarkastellaan botnettien arkkitehtuuria, rakennetta ja toimintaa sekä tämän hetken merkittävimpiä IoT-botnettejä. Lopuksi luvussa 5 tehdään yhteenveto tutkimuksessa esille tulleista pääkohdista.

2 Palvelunestohyökkäykset

Palvelunestolla (engl. *Denial of Service, DoS*) on useita eri määritelmiä, mutta yleisesti ottaen se on tilanne, jossa normaalisti tavoitettavissa olevan palvelun tai palveluiden saavutettavuus on kompromisoitu, kun taas palvelunestohyökkäys puolestaan on tarkoituksellinen teko, jossa hyökkääjä pyrkii aiheuttamaan palvelunestotilanteen (Howard 1997). Hajautettu palvelunestohyökkäys (engl. *Distributed Denial of Service attack, DDoS attack*) eroaa tavallisesta palvelunestohyökkäyksestä siten, että se suoritetaan yksittäisen laitteen sijasta koordinoidusti suurella joukolla laitteita (Raghavan ja Dawson 2011, s. 11). Joissakin tapauksissa, kuten aliluvussa 4.3.5 käsiteltävän BrickerBotin kohdalla, hyökkäyksen päämääränä on saavuttaa pysyvä palvelunesto (engl. *Permanent Denial of Service, PDoS*). IoT-laitteiden määrän valtava kasvu yhdistettynä niiden verrattain heikkoon tietoturvaan tekevät niistä kannattavan alustan kyberrikollisille (Kolias ym. 2017), jonka seurauksena hajautettujen palveluksenestohyökkäysten määrä onkin kasvanut viime vuosien aikana (NETSCOUT Systems 2017). Palvelunestohyökkäyksiä on myös mahdollista ostaa palveluna (engl. *DDoS-as-a-Service, DDoSaaS*) niin kutsutuilta Booter-sivustoilta (Santanna ym. 2015).

2.1 Palvelunestohyökkäysten taksonomiaa

Aliluvussa 2.2 käsitellään joitakin IoT-botneteissä yleisimmin käytettäviä palvelunestohyökkäyksiä, ja lisäksi aliluvussa 4.3 katsotaan, mitä kaikkia palvelunestohyökkäyksiä tämän hetken merkittävimmistä IoT-botneteistä löytyy. Siksi on oleellista ymmärtää palvelunestohyökkäysten jaottelun malleja ja niiden eroavaisuuksia. Penttinen (2005) jakaa mekanismien kohteet kolmeen pääluokkaan: ohjelmisto (engl. *attacks that target software*), protokollat (engl. *attacks that target protocols*) ja kaistanleveys (engl. *attacks that target bandwidth*). Mirkovic ja Reiher (2004) taas jakavat hyökkäysmekanismit useampaan eri luokkaan. Näitä luokkia ovat automaation määrä (engl. *degree of automation*), hyväksikäytetty heikkous (engl. *exploited weakness*), lähdeosoitteen oikeellisuus (engl. *source address validity*), hyökkäystahdin dynaamisuus (engl. *attack rate dynamics*), luonnehdinnan mahdollisuus (engl. *possibility of characterization*), toimijaryhmän pysyvyys (engl. *persistence of agent set*), kohteen tyyppi (engl. *victim type*), sekä vaikutus kohteeseen (engl. *impact on the victim*). Ragha-

van ja Dawson (2011) vuorostaan erittelevät hyökkäysten muodot (engl. *mode of attack*) ja kohteet (engl. *target of attack*) ja jakavat nämä edelleen eri luokkiin. Hyökkäyksen muotoja ovat erilaiset nopean tahdin tulvahyökkäykset (engl. *high-rate flooding attacks*) ja semanttiset hyökkäykset (engl. *semantic attacks*). Hyökkäysten kohteet ovat puolestaan jaettu neljään eri luokkaan: verkkoihin (engl. *attacks targeting networks*), matkapuhelinverkkoon (engl. *attacks targeting cellular telecommunication network*), käyttöjärjestelmiin (engl. *attacks targeting operating systems*) ja sovelluksiin (engl. *attacks targeting applications, layer 7 attacks*). Mahjabin ym. (2017) jakavat hyökkäykset neljään pääluokkaan, joita ovat kaistanleveyteen kohdistuvat hyökkäykset (engl. *bandwith depletion attack*), resursseihin kohdistuvat hyökkäykset (engl. *resource depletion attack*), infrastruktuuriin kohdistuvat hyökkäykset (engl. *(infrastructure attack*) ja nollapäivähaavoittuvuuksiin kohdistuvat hyökkäykset (engl. *zero-day attack*). Näistä kaistanleveyteen kohdistuvat hyökkäykset jaetaan vielä protokollaa hyväksikäyttäviin hyökkäyksiin (engl. *protocol exploiting attack*) ja vahvistushyökkäyksiin (engl. *amplification attack*), ja resursseihin kohdistuvat hyökkäykset puolestaan protokollaa hyväksikäyttäviin hyökkäyksiin (engl. *protocol exploiting attack*) ja epämuodostuneiden pakettien hyökkäyksiin (engl. *malformed packet attack*). Zargar, Joshi ja Tipper (2013) jakavat tulvahyökkäykset (engl. *flooding attacks*) hyvin yksityiskohtaisesti, mutta tämän tutkimuksen kannalta oleellisinta on jako verkko- ja kuljetuskerroksen hyökkäyksiin (engl. *network/transport-level DDoS flooding attacks*) ja sovelluskerroksen hyökkäyksiin (engl. *application-level DDoS flooding attacks, layer 7 attacks*).

Kaupalliset tilastoja julkaisevat yritykset, kuten Netscout ja Verisign jakavat hyökkäykset paljon karkeammin kuin useat tutkijat. Tämän saattaa selittää se, että heitä kiinnostaa enemmän datan esittäminen selkeässä muodossa kuin täsmällinen jaottelu. Lisäksi kaikkia hyökkäystyyppejä ei esiinny suuria määriä, joten niiden esittäminen ei ole tarkoituksenmukaista. Netscoutin (2017) tapauksessa luokkia on kolme: kaistanleveyteen kohdistuvat hyökkäykset (engl. *volumetric attacks*), protokolliin kohdistuvat hyökkäykset (engl. *state-exhaustion attacks*) ja ohjelmistokerroksen hyökkäykset (engl. *application layer attacks*). Verisign (2018) taas jakaa hyökkäykset viiteen eri luokkaan: sirpaloituneiden IP[1]-pakettien hyökkäykset (engl.

1. IP: Internet Protocol

IP fragment attacks), TCP[2]:hen pohjautuvat hyökkäykset (engl. *TCP based*), UDP[3]:hen pohjautuvat hyökkäykset (engl. *UDP based*), sovelluskerroksen hyökkäykset (engl. *layer 7*) ja muut. Vuonna 2017 Netscout (2017) raportoi, että 75,7 % DDoS-hyökkäyksistä olivat kaistanleveyteen kohdistuvia, 11,8 % protokolliin kohdistuvia ja 12,4 % ohjelmistokerroksen hyökkäyksiä, kun taas vuonna 2018 vastaavat luvut olivat 42 %, 31 % ja 27 % (NETSCOUT Systems, Inc 2018). Netscoutin mukaan muutos on tapahtunut jo kolmen vuoden ajan ja johtuu siitä, että kaistanleveyteen kohdistuvia hyökkäyksiä on yhä vaikeampi saada läpi suojauksista, joten hyökkääjät ovat siirtyneet vaikeammin havaittaviin hyökkäyksiin (NETSCOUT Systems, Inc 2018, s. 15). Verisign (2018) puolestaan raportoi, että vuoden 2018 toisella neljänneksellä 56 % oli UDP:hen pohjautuvia hyökkäyksiä, 26 % TCP:hen pohjautuvia hyökkäyksiä, 10 % sirpaloituneiden IP-pakettien hyökkäyksiä, 5 % sovelluskerroksen hyökkäyksiä ja 3 % muita. Hyökkäykset voivat myös koostua useammasta eri hyökkäystyyppistä. Netscoutin raportin (2018) mukaan useamman tyypin (engl. *multi-vector*) hyökkäykset kasvoivat 48 %:sta vuonna 2017 67 %:iin vuonna 2018. Sen sijaan Verisignin (2018) mukaan 52 % hyökkäyksistä vuoden 2018 toisella puoliskolla käyttivät useampaa tyyppiä.

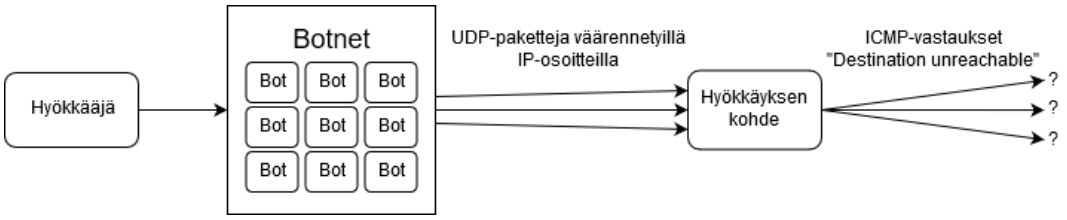
2.2 Esimerkkejä palvelunestohyökkäyksistä

Erilaisia palvelunestohyökkäyksiä on olemassa paljon: Mahjabin ym. (2017) esittävät tutkimuksessaan 18 erilaista hyökkäystä, eikä tämä edes sisällä kaikkia Mirai-botnetin hyökkäystyyppejä (Özçelik, Chalabianloo ja Gür 2017). De Donnon ym. (2018b) mukaan erilaiset tulvahyökkäykset sopivat erityisen hyvin IoT-pohjaisiin palvelunestohyökkäyksiin, sillä ne vaativat vain vähän kommunikointia laitteiden välillä, mahtuvat muistin puolesta pieneen tilaan ja ovat toteutettavissa perusohjelmointitaidoilla. Netscoutin (2018) raportoimien useamman tyypin hyökkäysten kasvaessa korostuu myös se, miten uudemmat botnetit pystyvät käyttämään useampia ja monimutkaisempia hyökkäyksiä (De Donno ym. 2018b). Koska tämän tutkielman kannalta ei ole tarkoituksenmukaista tietää jokaista eri palvelunestohyökkäystä ja niiden toimintaa, tässä kappaleessa keskitytään niihin, jotka esiintyvät yleisimmin IoT-

2. TCP: Transmission Control Protocol
3. UDP: User Datagram Protocol

botneteissä. De Donnon ym. (2018b) mukaan UDP flood, TCP SYN flood ja HTTP flood löytyvät lähes kaikista hajautettuihin palvelunestohyökkäyksiin kykenevistä IoT-botneteistä. Lisäksi käsitellään Miraista löytyvää DNS query floodia.

- UDP flood on kuljetuskerroksessa tapahtuva hyökkäys, joka käyttää hyväksi UDP-protokollaa ja pyrkii käyttämään kaiken kohteen käytössä olevan kaistanleveyden (Mahjabin ym. 2017). Hyökkääjä lähettää kohteeseen suuren määrän UDP-paketteja joko satunnaiseen tai yhteen tiettyyn porttiin, jolloin kohde yrittää selvittää paketin määränpään. Kun kohde ei löydä paketille määränpäätä se lähettää takaisin ICMP[4]-paketin, jossa se kertoo, ettei määränpää ole saavutettavissa. Koska hyökkääjän lähettämien pakettien IP-osoitteet ovat väärennetty, kohteen takaisin lähettämät paketit eivät johda mihinkään olemassa olevaan osoitteeseen, mutta siitä huolimatta niiden lähettäminen kuluttaa kohteen kaistanleveyttä. Lopputuloksena on tilanne, jossa nämä paketit käyttävät kaiken saatavilla olevan kaistanleveyden (Mahjabin ym. 2017). UDP floodin toiminta on esitetty kuviossa 1, joka on tehty Mahjabinin ym. (2017) vastaavan kuvan pohjalta.

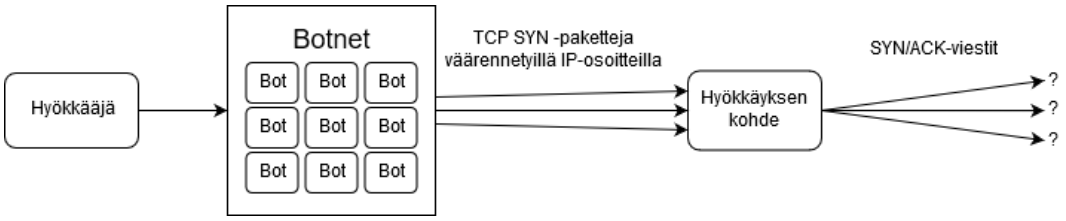


Kuvio 1. UDP flood

- TCP SYN flood on myös kuljetuskerroksessa tapahtuva hyökkäys, joka puolestaan käyttää hyväksi TCP-protokollaa johtaen kohteen verkkoresurssien loppumiseen (Mahjabin ym. 2017). Hyökkääjä lähettää palvelimelle suuren määrän TCP-protokollan määrittelemiä SYN-paketteja, mutta ei koskaan suorita TCP:n määrittelemää yhteyden muodostamista loppuun, jolloin kohde käyttää turhaan resursseja yhteyden käsittelyyn. TCP SYN flood, sekä muut kuljetus- ja verkkokerroksen hyökkäysmenetelmät kuitenkin eroavat huomattavasti tavanomaisesta verkkoliikenteestä, joka helpottaa niiden havaitsemista. Havaitsemisen helppous on suuri syy käyttää sovelluskerroksessa toimivaa hyökkäystä, joka muistuttaa hyvin paljon normaalia liikennettä ja on siten

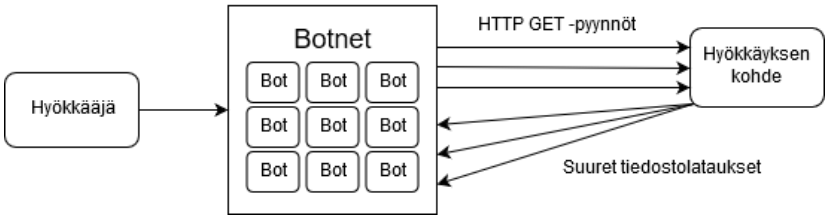
4. ICMP: Internet Control Message Protocol

vaikeampi havaita (Singh, Kumar ja Bhandari 2015). TCP SYN floodin toiminta on esitetty kuviossa 2, joka on tehty Mahjabinin ym. (2017) vastaavan kuvan pohjalta.



Kuvio 2. TCP SYN flood

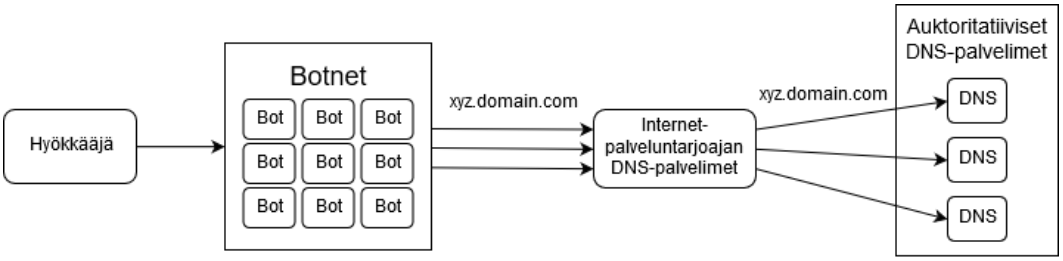
- HTTP flood on TCP SYN floodin tapaan hyökkäys, jossa hyökkääjä pyrkii käyttämään kaikki kohteen resurssit hyväksikäyttämällä protokollan ominaisuuksia, mutta se tapahtuu sovelluskerroksella. Hyökkäyksen ideana on joko pyytää (HTTP GET) tai lähettää (HTTP POST) palvelimelle niin suuri määrä pyyntöjä, ettei se pysty enää palvelemaan muita asiakkaita. Nämä komennot eivät käytä pelkästään verkkoresursseja vaan ne kuormittavat kohdetta muissakin suhteissa, sillä sen täytyy noutaa GET-pyynnön mukainen tiedosto tallennusvälineiltä ja pilkkoa se lähetettäviksi paketeiksi. HTTP-pyyntöjä varten hyökkääjän täytyy muodostaa TCP-yhteys kohteeseen, joka vaikeuttaa hyökkäyksen erottamista normaalista liikenteestä (Mahjabin ym. 2017). HTTP floodin toiminta on esitetty kuviossa 3, joka on tehty Mahjabinin ym. (2017) vastaavan kuvan pohjalta.



Kuvio 3. HTTP flood

- DNS query flood, Miraissa tunnettu nimellä ”DNS water torture”, on sovelluskerroksen hyökkäys, joka pohjautuu DNS:n hierarkisuuteen ja rekursiiviseen toimintaan. DNS:n ensisijainen tarkoitus on liittää IP-osoitteita niitä vastaaviin verkkotunnuksiin (engl. *domain*). Mikäli DNS-palvelimelta ei löydy DNS-kyselyn pyytämää tietoa, se lähettää rekursiivisen kyselyn hierarkiassa seuraaville palvelimille. DNS query floodissa hyökkääjä lähettää DNS-kyselyjä, joiden alkuosa (engl. *subdomain*) on näen-

näissatunnainen merkkijono, jota seuraa hyökkäyksen kohteena oleva verkkotunnus. Nämä kyselyt menevät ensin internet-palveluntarjoajan omille DNS-palvelimille, jotka puolestaan lähettävät ne edelleen kohdeverkkotunnuksen auktoritatiivisille DNS-palvelimille (engl. *authoritative DNS server*). Hyökkäävät botit saavat siis internet-palveluntarjoajan DNS-palvelimet suorittamaan palvelunestohyökkäyksen niiden puolesta (Angrishi 2017; Akamai Technologies 2018). DNS query floodin toiminta on esitetty kuviossa 4, joka on tehty Angrishin (2017) ja Akamain (2018) kuvien pohjalta.



Kuvio 4. DNS query flood

3 IoT-tietoturvallisuus ja haavoittuvuudet

Ennen kuin aliluvussa 4.3 käsitellään tämän hetken merkittävimpiä IoT-botnettejä tarkemmin, on tärkeää saada yleiskuva IoT-laitteiden tietoturvallisuudesta ja ymmärtää, mitä haavoittuvuuksia botnettien on mahdollista hyödyntää. IoT-laitteiden hyväksikäyttöä palvelunestohyökkäyksissä edistää pääasiassa niiden suuri lukumäärä ja tyypillisen IoT-laitteen heikompi tietoturva verrattuna perinteisiin tietokoneisiin. Angrishin (2017) mukaan IoT-laitteiden suunnittelussa kiinnitetään huomiota tietoturvallisuuteen hyvin vähän tai ei ollenkaan, jonka lisäksi hän väittää, että turvallisuus on yleensä vain jälkiajatus IoT-arkkitehtuurissa, jos sitäkään. De Donno ym. (2017) puolestaan mainitsevat IoT-laitteiden suosion hajautettujen palvelunestohyökkäysten suorittamisessa johtuvan siitä, että valmistajat suojaavat laitteensa heikosti ja käyttäjät ylläpitävät niitä huonosti. Useiden IoT-laitteiden käyttöön liittyy myös jonkinlainen pilvipalvelu, jolloin Zunnurhainin (2016) mukaan myös sen tietoturvallisuus pitää ottaa huomioon. Angrishin (2017) mukaan monien haavoittuvuuksien taustalla on laitteiden pieni hintamarginaali ja tarve saada kaupallinen tuote valmiiksi mahdollisimman nopeasti, jolloin toiminnallisuus menee usein tietoturvan edelle.

Ehdottomasti yksi suurimmista haavoittuvuuksista on laitteisiin käsiksi pääsy julkisen internetin kautta (Lin ja Bergmann 2016; Angrishi 2017). Tähän liittyen monissa laitteissa on myös ulospäin näkyviä avoimia portteja, jotka ovat helposti löydettävissä skannerityökaluilla (Bertino ja Islam 2017). Useat eri laitteet, etenkin web-kamerat, käyttävät vanhentunutta versiota MiniUPnP[1]-protokollasta tai salaamatonta telnet-palvelinta (Williams ym. 2017). Lisäksi Williamsin ym. (2017) mukaan useissa tulostimissa ja älytelevisioissa on oletuksena asennettu SNMP[2]-agentti ilman, että laitteen käyttäjä on tästä tietoinen. Suuressa osassa laitteita myös fyysinen saavutettavuus on huomattava haavoittuvuus (Lin ja Bergmann 2016). IoT-laitteet ovat usein vartioimattomia, joka helpottaa fyysisiä hyökkäyksiä, ja niiden välinen kommunikointi on usein langatonta, joka tekee salakuuntelusta helppoa (Atzori, Iera ja Morabito 2010). Laitteet ovat myös usein helppoja purkaa tai niissä on avoimia USB-portteja, jotka mahdollistavat pääsyn käsiksi laitteen ohjelmistoon (Bertino ja Islam 2017).

1. MiniUPnP: Mini Universal Plug and Play
2. SNMP: Simple Network Management Protocol

Jos kyseessä on kuluttajalaite, joka on yhdistettynä langattomaan verkkoon tai datasähköadapteriin, verkkoon pääsee käsiksi, vaikka itse talo olisi lukittu (Lin ja Bergmann 2016).

Ohjelmistopäivitykset ja niiden jakelu on huomattava haavoittuvuus. Monet laitteet eivät saa tietoturvapäivityksiä ollenkaan, sillä se ei ole valmistajan näkökulmasta taloudellisesti järkevää, eikä valmistajilla välttämättä ole tarvittavia taitoja päivitysten tekemiseen ja niiden jakeluun (Lin ja Bergmann 2016; Kumar, Madhuri ja ChanneGowda 2017). Päivitysmekanismit eivät usein ole tietoturvallisia, vaikka laitteet saisivatkin päivityksiä: päivitystiedostot eivät ole salattuja, niiden sisältämää tietoa ei ole varmistettu ennen tiedoston lähettämistä, itse päivityspalvelimet eivät ole tietoturvallisia ja tunnistetiedot saattavat olla kovakoodattuina laitteeseen (Bertino ja Islam 2017). Nämä mahdollistavat laiteohjelmistonkorvaushyökkäykset (engl. *firmware replacement attack*) useita IoT-laitteita vastaan (Zunnurhain 2016; Kumar, Madhuri ja ChanneGowda 2017). Myös riittämättön konfiguroitavuus tietoturvallisuuden suhteen ja tietoturvastandardien hidas käyttöönottonopeus ovat huomattavia haavoittuvuuksia. Suurin osa kuluttajalaitteista toteuttavat vain joitakin tai ei yhtäkään tietoturvallista lähestymistapaa (Lin ja Bergmann 2016). Lisäksi laitteissa ja niihin liittyvissä ohjelmistoissa on heikot salasanavaatimukset ja niistä puuttuu usein tietoturvaloki, tiedonsalausmenetelmät, tietoturvaan liittyvät ilmoitukset sekä järjestelmänvalvojien ja käyttäjien erottamisen mahdollistava käyttöoikeusmalli (Bertino ja Islam 2017).

Kumarin, Madhurin ja ChanneGowdan (2017) sekä Bertinon ja Islamin (2017) mukaan laitteisiin liittyvät pilvipalvelut ja käyttöliittymät ovat usein haavoittuvaisia. Oletussalasanoja ei välttämättä pysty vaihtamaan ja niissä tapauksissa, joissa tämä on mahdollista, monet laitteet hyväksyvät heikkoja salasanoja. Lisäksi järjestelmät eivät lukkiudu epäilyttävien sisäänkirjautumisien seurauksena ja unohtuneen salasanan palauttaminen ei välttämättä ole tietoturvallista, vaan se saattaa jopa paljastaa kirjautumistiedot hyökkääjälle. Käyttöliittymät saattavat myös olla alttiita HTML-injektioille (engl. *cross-site scripting, XSS*), sivujen väliselle pyynnön väärentämiselle (engl. *cross-site request forgery*) ja SQL[3]-injektioille. Linin ja Bergmannin (2016) mukaan suurin haavoittuvuus kuluttajamaailmassa on tietoturvaosaajien puute, sillä kuluttajat harvoin osaavat asentaa ja hallita laitteitaan tietoturvallisesti, eikä heillä ole usein resursseja osaavien henkilöiden palkkaamiseen.

3. SQL: Structured Query Language

Muita haavoittuvuuksia on IoT-laitteiden heikko suorituskyky, joka estää niitä toteuttamasta muun muassa perinteisiä salausmenetelmiä (Lin ja Bergmann 2016; Atzori, Iera ja Morabito 2010; Angrishi 2017), järjestelmien heterogeenisyys, joka johtaa ohjelmistopäivitysten ja dokumentaation huonoon saatavuuteen (Lin ja Bergmann 2016; Bertino ja Islam 2017) sekä salauksen ja tiedon eheyden varmistamisen puute kuljetusvaiheessa erityisesti kirjautumistietojen osalta (Bertino ja Islam 2017). Lisäksi monien laitteiden kohdalla on syytä olla huolissaan yksityisyydestä, sillä ne keräävät tarpeetonta käyttäjätietoa, paljastavat henkilötietoja, lähettävät arkaluontoista tietoa ilman anonymisaatiota, säilyttävät tietoa pidempään kuin on tarpeen, eivätkä tarjoa riittäviä asetuksia sen suhteen, kuka pääsee tietoon käsiksi (Bertino ja Islam 2017).

4 IoT-botnetit

Kuten kappaleessa 2 mainittiin, hajautettu palvelunestohyökkäys edellyttää laitteiden välistä koordinaatiota, joka tapahtuu erityisesti IoT:n tapauksessa botnetin avulla. Botnet koostuu joukosta laitteita, joiden toimintaa pystytään kontrolloimaan koordinoidusti internetin välityksellä yhdeltä laitteelta käsin (Tiirmaa-Klaar 2013, s. 42). Edellisessä luvussa mainittujen haavoittuvuuksien yleisyys ja vakavuus saavat aikaan tilanteen, jossa kyberrikollisten on helppo saavuttaa suuri määrä heikosti suojattuja laitteita levittämään botnettejä haittaohjelmien (engl. *malware*) välityksellä. Botnet-haittaohjelmat kuitenkin eroavat tavanomaisista haittaohjelmista siten, että niillä on omat viestintäkanavansa ja ne pysyvät usein toimimattomina niin kauan kunnes ne vastaanottavat käskyjä botnetin kontrolloijalta eli botmasterilta (Tiirmaa-Klaar 2013, s. 42). Botmaster vuorostaan ohjaa botnettiä ohjaus- ja valvontapalvelinten (engl. *command and control severs, C&C, C2*) välityksellä (Tiirmaa-Klaar 2013, s. 49). Vaikka tässä tutkielmassa tarkastellaankin botnettejä vain palvelunestohyökkäysten näkökulmasta, niitä käytetään myös muihinkin tarkoituksiin, kuten kryptovaluuttojen louhintaan (F5 Networks, Inc. 2018), spämmin levittämiseen tai henkilökohtaisten tietojen keruuseen (Schiller 2007; Tiirmaa-Klaar 2013, s. 47-57)

4.1 IoT-botnettien arkkitehtuuri

De Donno ym. (2018b) esittävät tutkimuksessaan viisi eri arkkitehtuurimallia hajautettujen palvelunestohyökkäysten suorittamiseen. Näitä ovat agentti-käsittelijä-malli (engl. *agent-handler model*), peilausmalli (engl. *reflector model*), IRC[1]-pohjainen malli (engl. *IRC-based model*), verkkopohjainen malli (engl. *web-based model*) ja vertaisverkkomalli (engl. *P2P-based model*). Alomari ym. (2012) puolestaan esittävät näistä vain agentti-käsittelijä-mallin, IRC-pohjaisen mallin ja verkkopohjaisen mallin. De Donnon ym. (2018b) mukaan yksikään hajautettuihin palvelunestohyökkäyksiin kykenevä botnet ei käytä peilausmallia tai verkkopohjaista mallia, joten ne eivät ole olennaisia tämän tutkielman kannnalta. Heidän mukaansa vain agentti-käsittelijä-malli ja IRC-pohjainen malli ovat laajassa käytössä hajautettuihin palvelunestohyökkäyksiin kykenevissä IoT-botneteissä, mutta vielä ei pysty sanomaan kum-

1. IRC: Internet Relay Chat

pi niistä on suositumpi. Viime aikoina on kuitenkin tullut esiin myös vertaisverkkomallia käyttäviä hajautettuja botnettejä, joista eniten huomiota on saanut Hajime (Edwards ja Profetis 2016; Herwig ym. 2019). Hajimea ei ole toistaiseksi käytetty palvelunestohyökkäyksissä, mutta kuten aliluvussa 4.3.3 tullaan näkemään, monet pitävät sen tapahtumista tulevaisuudessa todennäköisenä. Näistä syistä johtuen tässä tutkielmassa käsitellään vain agentti-käsittelijä-mallia, IRC-pohjaista mallia ja vertaisverkkomallia.

Alomari ym. (2012) ja De Donno ym. (2018b) kuvaavat agentti-käsittelijä-mallin koostuvan asiakkaista (engl. *clients*), käsittelijöistä (engl. *handlers, masters*) ja agenteista tai boteista (engl. *agents, bots*). Asiakas on laite, jonka kautta hyökkääjä on yhteydessä muuhun palvelunestojärjestelmään. Käsittelijät ovat ympäri internetiä sijaitsevia ohjelmia, jotka pitävät listaa agenteista ja mahdollistavat asiakkaan kommunikoinnin agenttien kanssa. Havaitsemisen vaikeuttamiseksi hyökkääjät pyrkivät sijoittamaan käsittelijät esimerkiksi kytkimiin tai palveilimiin, joiden läpi kulkee normaalisti paljon liikennettä, jolloin hyökkäyksen viestintä on vaikeampaa erottaa normaalin liikenteen joukosta. Agentilla tai botilla tarkoitetaan hyökkäyksen suorittavaa ohjelmaa tai tämän ohjelman tartuttamaa laitetta. Mallin huono puoli on se, että käsittelijöiden ja agenttien pitää tietää toistensa IP-osoitteet, joten yksittäisen botin löytäminen saattaa pahimmillaan paljastaa koko botnetin. Agentti-käsittelijä-mallia käyttäviä botnettejä ovat muun muassa Bashlite ja Mirai (De Donno ym. 2018b).

IRC-pohjainen malli malli on hyvin samanlainen, kuin agentti-käsittelijä-malli, mutta siinä IRC-viestikanava korvaa käsittelijöiden roolin. Tällä tavalla toimivaa botnettiä on vaikeaampaa jäljittää, sillä agentit käyttävät tavanomaisia IRC-portteja viestittämiseen ja IRC-palvelimet käsittelevät tavallisestikin suurta määrää liikennettä, jolloin hyökkäyksen liikenne ei erotu helposti normaalin liikenteen joukosta. Lisäksi IRC-palvelin pitää listaa aktiivisista agenteista, jolloin hyökkääjän ei tarvitse tehdä sitä itse. Yhden agentin löytyminen paljastaa myös vähemmän tietoa botnetistä kuin agentti-käsittelijä-mallissa (Alomari ym. 2012; De Donno ym. 2018b). IRC-pohjaista mallia käyttävät esimerkiksi Remaiten ja IRCTelnet (De Donno ym. 2018b).

De Donnon ym. (2018b) mukaan vertaisverkkomallin tarkoituksena on välttää agenttien keskitettyä kontrollointia, joka on kahden edellämainitun arkkitehtuurin selkeä heikko kohta. Hajautetussa rakenteessa agentit pystyvät jakamaan käsittelijän tai IRC-palvelimen roolin

tasaisesti itse agenttien välille, joten yhden agentin löytyminen paljastaa hyvin vähän tietoa. Keskitetty botnet on mahdollista pysäyttää ottamalla haltuun kaikki sen kontrollointipalvelimet, mutta hajautetun botnetin tapauksessa vastaava on käytännössä mahdotonta, sillä se edellyttäisi jokaisen agentin haltuunottoa. Lisäksi hyökkääjä on hyvin vaikea jäljittää, sillä botnetin komennot hyppivät useiden agenttien välillä. Esimerkiksi Hajime on vertaisverkkomallia käyttävä botnet, jossa viestintä tapahtuu BitTorrentin uTP-protokollan avulla (Edwards ja Profetis 2016).

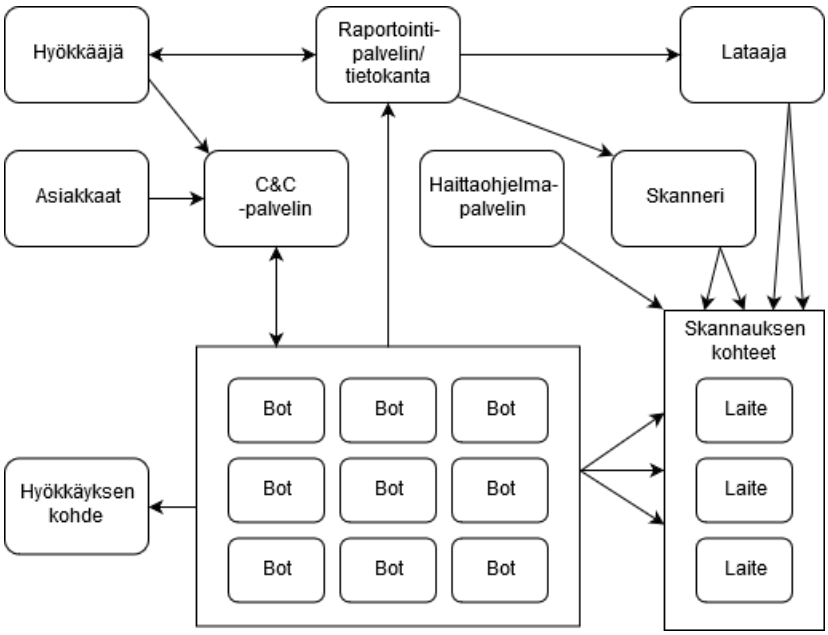
4.2 IoT-botnettien rakenne ja toiminta

Seuraavaksi käsitelty yleinen botnetin rakenne ja toiminta kuvaavat lähimmin agentti-käsittelijä-mallia käyttäviä botnettejä, kuten Bashliteä ja Miraita. Lähes kaikki botnetit kuitenkin toimivat hyvin samalla tavalla, joten suurimmat erot löytyvät C&C-arkkitehtuurista ja käytetyistä haavoittuvuuksista. Botneteistä suurin osa sisältää seuraavat kuusi komponenttia (Marzano ym. 2018; Angrishi 2017):

- C&C-palvelimet tarjoavat hyökkääjälle rajapinnan botnetin käyttämiseen. Ne pitävät yllä yhteyksiä botteihin ja välittävät niille tarvittavat komennot.
- Botit ovat haittaohjelman tartuttamia laitteita, jotka raportoivat tilaansa C&C-palvelimille ja suorittavat niiltä saadut komennot.
- Skannerit (engl. *scanners*) tiedustelevat haavoittuvaisia laitteita.
- Lataajat (engl. *loaders*) kirjautuvat sisään löydetyille haavoittuvaisille laitteille ja lataavat niille halutut haittaohjelmat.
- Raportointipalvelin (engl. *reporting server*) tai tietokanta kerää tiedot skannausten tuloksista ja pitää kirjaa aktiivista boteista.
- Haittaohjelmapalvelimet (engl. *malware distribution servers*) tarjoavat itse haittaohjelman ja muut tarvittavat tiedostot uuden laitteen tartuttamiseksi.

Yksittäinen laite voi myös ajaa useamman komponentin virkaa, kuten Mirain botit, jotka toimivat myös skannereina (Marzano ym. 2018). Yleinen IoT-botnetin rakenne on esitetty kuviossa 5, joka on tehty Kambourakisin ym. (2017), Marzanon ym. (2018) ja Angrishin (2017) kuvien pohjalta.

Kolias ym. (2017), Angrishi (2017), Kambourakis, Kolias ja Stavrou (2017) kuvaavat yleisen botnetin toiminnan. Sen voidaan ajatella alkavan haavoittuvaisten laitteiden skannaamisesta, jonka saattaa hoitaa joko C&C-palvelin, skanneri tai jo olemassa oleva botti. Skannaaminen eroaa hieman eri haittaohjelmien välillä, mutta yleisesti sen tarkoituksena on löytää haavoittuvainen laite, jonka botnet-haittaohjelma pystyy tartuttamaan. Kun haavoittunut laite on löydetty, haittaohjelma yrittää saada laitteen haltuunsa esimerkiksi murtautumalla laitteeseen ennaltamääritetyillä kirjautumistiedoilla. Mikäli sisäänkirjautuminen onnistuu, laitteen tiedot, kuten IP-osoite ja kirjautumistiedot tallennetaan raportointipalvelimelle. Seuraavaksi lataaja tai C&C-palvelin kirjautuu laitteelle käyttäen raportointipalvelimelta löytyviä tietoja ja lataa sille tartuttamiseen tarvittavat tiedostot haittaohjelmapalvelimelta. Ladatun haittaohjelman suorituksen myötä botti aktivoituu ja pyrkii tukkimaan mahdollisimman monta haavoittuvuutta, jottei muut haittaohjelmat pääsisi laitteeseen käsiksi. Lisäksi se pyrkii poistamaan kaikki muut haittaohjelmat laitteelta, mikäli se havaitsee niitä. Lopuksi botti yhdistää itsensä botnettiin, jonka jälkeen se jää odottamaan käskyjä. Huomionarvoista on, että useimmat botnet-haittaohjelmat eivät vaikuta huomattavasti laitteen toimintaan hyökkäysten ulkopuolella, pitäen paljastumisen mahdollisuuden alhaisena (Angrishi 2017).



Kuvio 5. Yleinen IoT-botnetin rakenne

4.3 Merkittävimmät IoT-botnetit

Tässä aliluvussa käsitellään tämän hetken merkittävimpiä IoT-botnettejä painottaen niitä, jotka ovat jo suorittaneet hajautettuja palvelunestohyökkäyksiä. Joukossa on kuitenkin myös sellaisia, jotka ovat olleet ainakin toistaiseksi passiivisia hyökkäysten osalta, kuten Hajime, tai ovat asiaankuuluvia muista syistä, kuten BrickerBot ja VPNFilter. De Donnon ym. (2018a) mukaan palvelunestohyökkäyksen häiritsevyyden määräävä tekijä on botnetin koko, joten se on oleellinen kriteeri merkittävimmille botneteille. Botnettien määrä on kuitenkin nousussa (De Donno ym. 2018b), joten monet eri haittaohjelmat kilpailevat samojen laitteiden tartuttamisesta ja yksittäisen botnetin koko pysyy huomattavasti pienempänä kuin siinä tapauksessa, että niitä olisi vain muutama (Mansfield-Devine 2017). Radwaren asijantuntijan Pascal Geenensin mukaan suurin uhka onkin se, että yksittäinen botnet päihittäisi kaikki edelliset joka tilanteessa ja muodostaisi ennennäkemättömän suuren botnetin (Radware Ltd. 2017b). Kaikki botnet-haittaohjelmat, kuten Mirai, eivät myöskään ole pysyviä (engl. *persistent*) eli ohjelma katoaa laitteelta, jos se käynnistetään uudelleen (Mansfield-Devine 2017). Lisäksi botmasterit saattavat rajoittaa botnettiensä kasvua pysyäkseen mahdollisimman huomaamattomana (Vervier ja Shen 2018) ja eri tahot, kuten operaattorit saattavat tehdä toimenpiteitä vähentääkseen bottien määrää (Antonakakis ym. 2017). Botnettien koko siis saattaa vaihdella hyvin paljon pienelläkin aikavälillä, kuten Antonakakis ym. (2017) huomasivat Mirain kohdalla. Koon vaikutuksen lisäksi De Donnon ym. (2018b) mukaan uudemmat botnetit tukevat sekä enemmän, että monimutkaisempia hyökkäyksiä, jotka usein tehostavat niitä verrattuna vanhempiin botnetteihin. Esimerkiksi Marzanon ym. (2018) mukaan Mirai käyttää Bashliteen verrattuna enemmän TCP:tä tai sovelluskerrosta hyödyntäviä hyökkäyksiä, jotka vaativat botnetiltä vähemmän resursseja saman lopputuloksen aikaansaamiseksi. On syytä myös ottaa huomioon, että periaatteessa kuka vain voi luoda oman muunnelman eli variantin (engl. *variant*) avoimen lähdekoodin haittaohjelmista, kuten Bashlitestä tai Miraista, joka alentaa kynnystä uusien botnettien tekemiselle.

Yhdysvaltalainen New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) esittää sivuillaan yleiskatsauksen tämän hetken vallitsevista botneteistä, joilla saattaa olla vaikutusta yhdysvaltalaisiin (NJCCIC 2019). He mainitsevat, ettei lista ole tyhjentävä, mutta sekin pitää sisällään jo 46 eri botnettiä. Kaikki näistä eivät kuitenkaan ole olennaisia tämän

tutkielman kannalta, sillä osa niistä ovat liian pieniä suorittamaan merkittäviä palvelunestohyökkäyksiä ja osa on tehty muihin tarkoituksiin, kuten kryptovaluuttaa louhiva PyCryptoMiner (F5 Networks, Inc. 2018). De Donno ym. (2018b) puolestaan esittävät 13 erilaista hajautettuihin palvelunestohyökkäyksiin kykenevää IoT-botnettiä. Kaikki nämäkään eivät kuitenkaan ole enää kovin kovin merkittäviä, sillä osa niistä ovat verrattain pieniä ja nykyään on saatavilla kehittyneempiä avoimen lähdekoodin haittaohjelmia, kuten Bashlite ja Mirai (De Donno ym. 2018b). Tätä puoltaa myös se, että NJCCIC (2019) ei listaa kaikkia De Donnon ym. (2018b) mainitsemia haittaohjelmia, eli heidän arvionsa mukaan niillä ei todennäköisesti ole vaikutusta ainakaan yhdysvaltalaisiin.

4.3.1 Bashlite

Vaikka IoT-botnettejä on ollut olemassa jo vuodesta 2008, ensimmäinen vielä nykyäänkin hyvin merkittävä IoT-botnet, Bashlite, tunnistettiin ensimmäisen kerran vuonna 2014 (De Donno ym. 2018b). Tunnettu myös monilla muilla nimillä, kuten Bashlight, Bash0day, Bashdoor, Lizkebab, Torlus ja gafgyt, se skannaa satunnaisia IP-osoitteita ja yrittää kirjautua niihin telnetin avulla käyttäen ennaltamääritettyjä kirjautumistietoja (Angrishi 2017). De Donno ym. (2018b) luokittelevat Bashliten arkkitehtuuriksi agentti-käsittelijä-mallin, vaikka sen viestintäprotokolla pohjautuukin IRC:hen. Tämä johtuu siitä, että Bashliten käyttämää protokollaa on muokattu niin paljon, ettei se ole enään riippuvainen IRC:stä. Sen rakenne ja toiminta vastaavatkin hyvin läheisesti kappaleen 4.2 kuvausta. Bashliten hyökkäykset ovat kuitenkin verrattain yksinkertaisia, sillä siitä löytyy vain yksinkertaisia tulvahyökkäyksiä, kuten kappaleessa 2.2 esitetyt UDP- ja TCP SYN floodit (De Donno ym. 2018b). Bashliten lähdekoodi vuoti osittain vuonna 2015, joka johti useisiin variantteihin (Angrishi 2017). Moni pitää Bashliteä myös tämän hetken suurimman botnetin, Mirain edeltäjänä (Marzano ym. 2018; Angrishi 2017), mutta De Donno ym. (2018b) kuitenkin väittävät, ettei Bashlitellä ollut suoraa vaikutusta Mirain kehitykseen. Level 3 Threat Research Labs ja Flashpoint havaitsivat vuoden 2016 tutkimuksessaan parhaimmillaan yli miljoona hyökkäykseen osallistuvaa bottia ja yksittäisen C&C-palvelimen, joka viesti lähes 120 000 botin kanssa (Level 3 Threat Research Labs 2016).

4.3.2 Mirai

Mirain tunnisti ensimmäisenä tietoturvatukijaryhmä MalwareMustDie vuonna 2016 (MalwareMustDie 2016a), mutta se saavutti julkisuuden kolmen suuren hajautetun palveluestohyökkäysten sarjan jälkeen, jonka kohteina olivat Krebs on Security -blogi, OVH-pilvipalvelu ja DYN-verkkotietoturvapalvelu (Antonakakis ym. 2017). OVH:hon kohdistuvaan hyökkäykseen osallistui lähes 150 000 IoT-laitetta ja se olikin yksi ajan suurimpiaan kaistanleveydeltään (Kolias ym. 2017; Angrishi 2017). Pian näiden hyökkäysten jälkeen myös Mirain lähdekoodi vuoti johtaen tässäkin tapauksessa useisiin variantteihin (Kolias ym. 2017; Angrishi 2017). Antonakakis ym. (2017) kuvaavat tutkimuksessaan Mirain koon pysyneen pitkään noin 200 000-300 000:n laitteen välillä, kunnes se saavutti 600 000:n laitteen huippunsa marraskuussa 2016, jonka jälkeen sen koko laski noin 100 000:een vuoden 2017 alussa. Mirai käyttää agentti-käsittelijä-arkkitehtuurimallia (De Donno ym. 2018b), se toimii lähes täysin kappaleen 4.2 kuvaamalla tavalla ja sen rakenne vastaa hyvin laajalti kuviossa 5 esitetyn yleisen IoT-botnetin rakennetta. Mirai leviää lähettämällä TCP SYN -paketteja näennäissatunnaisiin IP-osoitteisiin, poislukien niihin, jotka ovat merkitty ennaltamääritetylle mustalle listalle (Antonakakis ym. 2017). Löytäessään haavoittuvaisen laitteen se yrittää kirjautua telnetin kautta sisään käyttäen sanakirjahyökkäystä (engl. *dictionary attack*) eli käyttämällä ennaltamääritetyssä listassa olevia kirjautumistietoja (Antonakakis ym. 2017).

Mirai hyökkäsi alunperin pelkästään valvontakameroihin liitettyihin tallennuslaitteisiin (engl. *DVR, digital video recorder*) (Mansfield-Devine 2017) käyttäen telnet-portteja 23 ja 2323, mutta kehittyi myöhemmin käyttämään useampia protokollia ja hyökkäämään useampiin laitteisiin (Antonakakis ym. 2017). Mirain sisältämät hyökkäykset ovat SYN flood, UDP flood, ACK flood, VSE[2] query flood, DNS water torture, GRE[3] IP flood, GRE ethernet flood, ja HTTP layer 7 flood (De Donno ym. 2018b), eli suhteessa Bashliteen se sisältää sekä enemmän, että monimutkaisempia hyökkäyksiä. Angrishin (2017) mukaan Mirai ei ole niin hienostunut kuin kuin jotkut kilpailevat botnetit, vaan sen menestys pohjautuu yksinkertaisuuteen. Samoin Mansfield-Devinen haastattelema tietoturva-asijantuntija Ken Munro sanoo Mirain olleen lähes kaunis yksinkertaisuudessaan (Mansfield-Devine 2017). Vervierin

2. VSE: Valve Source Engine
3. GRE: Generic Routing Encapsulation

ja Shenin (2018) mukaan Mirai on tällä hetkellä hallitseva tekijä IoT-botnettien keskuudessa ja De Donno ym. (2018b) väittävät Mirain olevan tämän hetken voimakkain ja häiritsevin palvelunestohyökkäyksiin kykenevä IoT-botnet.

4.3.3 Hajime

Hajime on yksi tämän hetken kehittyneimpiä botnettejä (Radware Ltd. 2017b) ja sen havaitsi ensimmäisen kerran Rapidity Networks vuonna 2016 (Edwards ja Profetis 2016). He kuvaavat sen tartuttamismenetelmien muistuttavan Miraita, mutta lähemmän tarkastelun myötä sen toiminta osoittautui hyvin erilaiseksi. Hajime ei ole ainoa havaittu botnet, joka noudattaa kappaleessa 4.1 kuvattua vertaisverkkomallia (Bertino ja Islam 2017; Karuppayah 2018, s. 1), mutta se on niistä tutkituin ja kooltaan suurin. Edwards ja Profetis (2016) arvioivat vuonna 2016 Hajimen kooksi noin 130 000-185 000, ja Kasperskyn raportin mukaan sen koko oli vuonna 2017 noin 300 000 bottia (Kaspersky Lab 2017). Hajimen tarkoituksesta ei ole varmaa tietoa ja sitä ei ole toistaiseksi käytetty hyökkäyksiin (Edwards ja Profetis 2016). Päinvastoin, se väittää tekemissään tulosteissa olevansa eettisen valkohattuhakkerin (engl. *white hat hacker*) tekemä, jonka tarkoituksena on suojata laitteita (Kaspersky Lab 2017). Kyberturvayritys Radwaren asiantuntija Pascal Geenens kuitenkin kyseenalaistaa Hajimen tekijän hyväntahtoisuuden (Bleeping Computer 2017b). Hän viittaa muun muassa sen käyttävän hyökkäyksiin viittaavia prosessien nimiä ja siihen, miten se sulkee Mirain hyväksikäyttämiä portteja, mutta avaa itseään varten uusia. Lisäksi Geenens on huolissaan siitä, että kyberrikolliset saisivat kaapattua Hajimen (Bleeping Computer 2017b), mutta myöntää, että toistaiseksi se on auttanut estämällä muita haittaohjelmia pääsemästä käsiksi haavoittuvaisiin laitteisiin (Radware Ltd. 2017b). Rapidity Networks (2016) ei sulje pois mahdollisuutta, että Hajime olisi tutkimus- tai harrastusprojekti, mutta pitävät todennäköisenä, että se on tällä hetkellä leviämisvaiheessa ja uskovat sen tarkoituksena olevan suorittaa hyökkäyksiä tulevaisuudessa.

4.3.4 Reaper

Reaper (tunnettu myös nimillä IoTroop ja IoT_Reaper) huomattiin ensimmäisen kerran lokakuussa 2017 (360 Netlab 2017). Check Point Researchin (2017) mukaan Reaper jakaa huo-

mattavan osan lähdekoodistaan Mirain kanssa, mutta se eroaa pääosin C&C palvelimien toteutuksen, viestintäprotokollan, hyväksikäytettävien haavoittuvuuksien ja hyökkäystoimintojen osalta. Radwaren (2017b) mukaan itse C&C-arkkitehtuuri on kuitenkin hyvin samanlainen kuin Miraissa. Mirain salasanahyökkäyksistä poiketen Reaperista löytyy työkalu, joka skannaa tiedossa olevia laite- tai arkkitehtuurikohtaisia haavoittuvuuksia (Check Point Research 2017) ja itse skannausten määrä on Miraita vähäisempi, mutta perusteellisempi (Radware Ltd. 2017b). Reaper ei myöskään sisällä Mirain DDoS-toiminnallisuutta, mutta siitä löytyy Lua-ohjelmointikieltä käyttävä ajoympäristö, jonka avulla boteille on mahdollista antaa mielivaltaisia käskyjä (Check Point Research 2017). Recorded Future (2018) arvioi Reaperin olevan mahdollisesti vastuussa palvelunestohyökkäyksestä hollantilaisia pankkeja kohtaan vuoden 2018 alussa, mutta varmistettuja tapauksia ei toistaiseki ole. Netscoutin (2017) mukaan vuonna 2017 Reaperin koko vaihteli 10 000 ja 20 000 botin välillä, mutta he tunnistivat myös noin 2 miljoonaa laitetta, jotka Reaper voisi halutessaan tartuttaa.

4.3.5 Muita huomionarvoisia IoT-botnettejä

Linux/IRCTelnet on MalwareMustDien vuonna 2016 löytämä botnet, joka sisältää ominaisuuksia monesta muusta botnetistä (MalwareMustDie 2016b). Sen pohjana toimii Aidra-botnet, mutta sen IRC-pohjainen viestintä on samanlainen kuin Kaiten-botnetissä, skannaus ja tartuttaminen on otettu Bashlitestä ja kirjautumistietojen lista on otettu Miraista. IRC-Telnetillä ei ole toistaiseksi tehty palvelunestohyökkäyksiä, mutta De Donnon ym. (2018b) mukaan se on Mirain vahvin kilpailija uusien laitteiden tartuttamisen suhteen. Leet puolestaan on botnet, joka hyökkäsi vuoden 2016 lopussa kyberturvallisuusyritys Impervan verkkoon kahdella peräkkäisellä TCP SYN floodilla, joista jälkimmäisen kaistenleveys saavutti parhaimmillaan 650 Gbps (Imperva 2016). Vaikka Miraista löytyykin TCP SYN flood -hyökkäys ja se kykenisi suorittamaan näin suuren hyökkäyksen, Imperva huomasi, että hyökkäyspakettien koot ja sisällöt eivät vastanneet Mirain toimintaa. Shobana ja Rathi (2018) listaavat Leetin kooksi 400 000, mutta eivät tarjoa tälle lähdettä, joten luku ei todennäköisesti ole luotettava.

Remaiten on tietoturvayritys ESETin vuonna 2016 löytämä botnet, jossa yhdistyy Tsunami-botnetin hyökkäykset ja Bashliten skannausominaisuudet (ESET 2016). Skannausta on kui-

tenkin tehostettu ja lisäksi Bashlitestä poiketen sen arkkitehtuuri on IRC-pohjainen. Amnesia on myös Tsunamiin pohjautuva botnet, jonka tunnisti Palo Alto Networksin tutkijaryhmä, Unit 42, vuonna 2017 (Palo Alto Networks 2017). Se käyttää hyväkseen haavoittuvuutta TVT Digitalin valmistamissa videotallennuslaitteissa, joiden määräksi he arvioivat 227 000. Amnesiaa ei ole vielä toistaiseksi käytetty tekemään hajautettuja palvelunestohyökkäyksiä, mutta Palo Alto Networksin mukaan Amnesia voisi mahdollisesti pystyä vastaaviin hyökkäyksiin kuin Mirai. Persirai on Trend Micron vuonna 2017 löytämä IP-kameroihin kohdistuva botnet, joka pohjautuu Mirain lähdekoodiin (Trend Micro Inc 2017). Se käyttää hyväkseen haavoittuvuutta UPnP-protokollassa, jota useat IP-kamerat käyttävät muodostaakseen verkkoyhteyden muihin laitteisiin. Persiraitakaan ei ole toistaiseksi käytetty palvelunestohyökkäyksissä, mutta Trend Micro havaitsi noin 120 000 sille haavoittuvaista IP-kameraa.

BrickerBotin havaitsi ensimmäisenä Radware vuonna 2017 (Radware Ltd. 2017a). Se on hieman erilainen haittaohjelma, sillä sen tarkoituksena ei ole luoda botnettiä vaan aiheuttaa tartuttamilleen laitteille pysyvä palvelunesto eli toisin sanoen tehdä laitteista käyttökelvottomia ylikirjoittamalla niiden laiteohjelmisto (engl. *firmware*). BrickerBot tunkeutuu laitteille Mirain tavoin telnetin kautta käyttäen valmista listaa käyttäjänimistä ja salasanoista (Radware Ltd. 2017a). Haittaohjelman luoja väitti hajottaneensa yli 200 000 laitetta ja myöhemmin samaa nimimerkkiä käyttänyt henkilö nosti tämän luvun kahteen miljoonaan (Bleeping Computer 2017a). Tietoturva-asiantuntija Ken Munro mainitsee, että BrickerBotin menetelmissä on kaksi hyvin suurta epäkohtaa: ensinnäkin se tuhoaa ihmisten omaisuutta ja siten aiheuttaa laitteen omistajalle enemmän haittaa kuin Mirai tai muu vastaava haittaohjelma. Toiseksi hän uskoo, että BrickerBot hajotti muita kuin tarkoittamiaan videotallennuslaitteita, eikä myöskään usko haittaohjelman luojan väitöksiin hajotettujen laitteiden määrästä (Mansfield-Devine 2017).

VPNFilter on Ciscon Talos-tutkijaryhmän vuonna 2018 löytämä botnet (Cisco Talos Intelligence Group 2018), jonka on arvioitu tartuttaneen ainakin 500 000 laitetta. Se on yksi tämän hetken monimutkaisimmista haittaohjelmista ja toimii kolmessa vaiheessa. Ensimmäisen vaiheen tarkoituksena on tehdä haittaohjelmasta pysyvä eli tartuttaa laite siten, että haittaohjelma ei poistu, vaikka laitteen käynnistäisi uudelleen. Toinen vaihe tarjoaa alustan liitännäisille kolmatta vaihetta varten sekä itsetuhotoiminnallisuuden, joka tekee laitteesta

käyttökelvottoman. Kolmas vaihe sisältää liitännäisiä, jotka muun muassa sieppaavat laitteen verkkoliikennettä ja viestivät C&C-palvelimien kanssa Tor-verkon kautta. VPNFilter ei vaikuta olevan tehty palvelunestohyökkäyksiä varten, mutta Talos pitää erityisesti itsetuhotoiminnallisuutta huolestuttavana.

5 Yhteenveto

IoT-laitteiden ja niiden avulla suoritettujen palvelunestohyökkäysten määrä on nousussa, eikä kummankaan kohdalla näytä siltä, että suunta olisi muuttumassa niin kauan kuin laitteiden tietoturvallisuutta ei paranneta eikä jo olemassa olevia haavoittuvuuksia paikata. Tässä tutkielmassa nähtiin, että itse palvelunestohyökkäyksiä on useita erilaisia ja niitä voidaan jaotella monen eri piirteen perusteella, mutta IoT-botnetit käyttävät näistä useimmiten tulvahyökkäyksiä niiden yksinkertaisuuden vuoksi. Itse IoT-laitteiden tietoturva on hyvin heikko verrattuna tavanomaiseen tietokoneeseen ja niistä löytyy hyvin suuri joukko erilaisia haavoituuvuuksia. Näistä IoT-botnettien kannalta huomattavimmat ovat laitteiden saavutettavuus julkisen internetin yli, avoimet tai huonosti suojatut protokollat kuten telnet ja UPnP sekä oletussalasanat ja niiden muuttamiseen liittyvät haasteet. Lisäksi monet botnetit käyttävät hyväksi laite-, ohjelmisto- tai protokollakohtaisia haavoittuvuuksia.

Laitteiden haavoittuvuuksia hyväksikäyttämällä kyberrikolliset pystyvät tartuttamaan parhaimmillaan miljoonia laitteita omilla haittaohjelmillaan ja sitä kautta luomaan botnetin, jota voi käyttää monenlaisiin eri kyberrikoksiin, kuten palvelunestohyökkäyksiin. Useimmat IoT-botnetit käyttävät arkkitehtuurinsa puolesta joko agentti-käsittelijä-mallia, IRC-pohjaista mallia tai vertaisverkkomallia. Erityisesti näistä kahden ensimmäisen välillä on kuitenkin hyvin paljon yhtäläisyyksiä ja vertaisverkkomalliakin edustavat eroavat niistä lähinnä hajautetun viestintänsä osalta. Monet botnetit ovat myös rakenteensa kannalta hyvin samanlaisia, vaikka itse käytännön toteutuksissa olisikin eroja.

Botnettien hyökkäyspotentiaalin vertailu on haastavaa, sillä niiden koko vaihtelee paljon ja eri botneteistä löytyy eritasoisia hyökkäysmenetelmiä. Usea eri taho on kuitenkin sitä mieltä, että Mirai on tämän hetken merkittävin IoT-botnet erityisesti palvelunestohyökkäysten näkökulmasta. Sillä on tosin myös monia kilpailijoita, joista esimerkiksi Hajime on sitä huomattavasti kehittyneempi. Botnettien määrä on myös nousussa, jonka seurauksena yksittäisen botnetin koko pysyy suhteellisen pienenä. Suurimpana uhkana pidetäänkin sitä, että yksi botnet olisi joka suhteessa kaikkia muita parempi ja muodostaisi ennennäkemättömän suuren botnetin.

Lähteet

360 Netlab. 2017. “IoT_reaper: A Rappid [sic] Spreading New IoT Botnet”. Viitattu 15. syyskuuta 2019. https://web.archive.org/web/20190915145059/https://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/.

Akamai Technologies, Inc. 2018. “Whitepaper: DNS Reflection, Amplification, & DNS Water-torture”. Viitattu 29. huhtikuuta 2019. https://web.archive.org/web/20190428231609/https://www.akamai.com/de/de/multimedia/documents/technical-publication/dns-reflection-vs-dns-mirai-technical-publication.pdf.

Alomari, Esraa, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah ja Rafeef Alfaris. 2012. “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art”. *International Journal of Computer Applications* 49, numero 7 (heinäkuu): 24–32. ISSN: 09758887. doi:10.5120/7640-0724.

Angrishi, K. 2017. “Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets”. *ArXiv e-prints* (helmikuu). arXiv: 1702.03681 [cs.NI].

Antonakakis, Manos, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric ym. 2017. “Understanding the Mirai Botnet” [kielellä en]. Teoksessa *2017 26th USENIX Security Symposium,* 19. ISBN: 978-1-931971-40-9.

Atzori, Luigi, Antonio Iera ja Giacomo Morabito. 2010. “The Internet of Things: A survey”. *Computer Networks* 54 (15): 2787–2805. ISSN: 1389-1286. doi:https://doi.org/10.1016/j.comnet.2010.05.010. http://www.sciencedirect.com/science/article/pii/S1389128610001568.

Bertino, E., ja N. Islam. 2017. “Botnets and Internet of Things Security”. *Computer* 50, numero 2 (helmikuu): 76–79. ISSN: 0018-9162. doi:10.1109/MC.2017.62.

Bleeping Computer. 2017a. “BrickerBot Author Claims He Bricked Two Million Devices”. Viitattu 23. syyskuuta 2019. https://web.archive.org/web/20190923142519/https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/.

———. 2017b. “Security Experts Worry as Hajime Botnet Grows to 300,000 Bots”. Viitattu 20. syyskuuta 2019. https://web.archive.org/web/20190920170916/https://www.bleepingcomputer.com/news/security/security-experts-worry-as-hajime-botnet-grows-to-300-000-bots/.

Check Point Research. 2017. “IoTroop Botnet: The Full Investigation”. Viitattu 27. elokuuta 2019. https://web.archive.org/web/20190826213958/https://research.checkpoint.com/iotroop-botnet-full-investigation/.

Cisco Talos Intelligence Group. 2018. “New VPNFilter malware targets at least 500K networking devices worldwide”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190921144358/https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/.

De Donno, M., N. Dragoni, A. Giaretta ja A. Spognardi. 2017. “Analysis of DDoS-capable IoT malwares”. Teoksessa *2017 Federated Conference on Computer Science and Information Systems (FedCSIS),* 807–816. Syyskuu. doi:10.15439/2017F288.

De Donno, Michele, Nicola Dragoni, Alberto Giaretta ja Manuel Mazzara. 2018a. “AntibIoTic: Protecting IoT Devices Against DDoS Attacks”. *Proceedings of 5th International Conference in Software Engineering for Defence Applications:* 59–72. ISSN: 2194-5365. doi:10.1007/978-3-319-70578-1_7. http://dx.doi.org/10.1007/978-3-319-70578-1_7.

De Donno, Michele, Nicola Dragoni, Alberto Giaretta ja Angelo Spognardi. 2018b. “DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation”. *Security and Communication Networks* 2018:1–30. ISSN: 1939-0114, 1939-0122. doi:10.1155/2018/7178164.

Edwards, Sam, ja Ioannis Profetis. 2016. *Hajime: Analysis of a decentralized internet worm for IoT devices* [kielellä en]. Rapidity Networks Security Research Group. https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

ESET. 2016. “Meet Remaiten – a Linux bot on steroids targeting routers and potentially other IoT devices”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190921144358/https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/.

F5 Networks, Inc. 2018. “New Python-Based Crypto-Miner Botnet Flying Under the Radar”. Viitattu 15. syyskuuta 2019. https://web.archive.org/web/20190915143823/https://www.f5.com/labs/articles/threat-intelligence/new-python-based-crypto-miner-botnet-flying-under-the-radar.

Gartner, Inc. 2017. “Gartner Says 8.4 Billion Connected "Things"Will Be in Use in 2017, Up 31 Percent From 2016”. Viitattu 18. maaliskuuta 2018. https://web.archive.org/web/20180307034831/https://www.gartner.com/newsroom/id/3598917.

———. 2018. “Gartner IT Glossary - Internet of Things”. Viitattu 27. maaliskuuta 2019. https://web.archive.org/web/20190223182825/https://www.gartner.com/it-glossary/internet-of-things/.

Herwig, Stephen, Katura Harvey, George Hughey, Richard Roberts ja Dave Levin. 2019. “Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet”. Teoksessa *Proceedings 2019 Network and Distributed System Security Symposium.* Internet Society. ISBN: 978-1-891562-55-6. doi:10.14722/ndss.2019.23488. https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-3_Herwig_paper.pdf.

Howard, J. 1997. “An Analysis Of Security Incidents On The Internet 1989 - 1995”. Väitöskirja, Carnegie Mellon University. Viitattu 11. kesäkuuta 2019. https://web.archive.org/web/20190611172525/https://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf.

Imperva. 2016. “650Gbps DDoS Attack from the Leet Botnet”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190920224325/https://www.imperva.com/blog/650gbps-ddos-attack-leet-botnet/.

Kambourakis, G., C. Kolias ja A. Stavrou. 2017. “The Mirai botnet and the IoT Zombie Armies”. Teoksessa *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM),* 267–272. Lokakuu. doi:10.1109/MILCOM.2017.8170867.

Karuppayah, Shankar. kirjoittaja. 2018. *Advanced Monitoring in P2P Botnets : A Dual Perspective.* 105. SpringerBriefs on Cyber Security Systems and Networks. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-10-9050-9.

Kaspersky Lab. 2017. “Hajime, the mysterious evolving botnet”. Viitattu 19. syyskuuta 2019. https://web.archive.org/web/20190919185350/https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/.

Kolias, C., G. Kambourakis, A. Stavrou ja J. Voas. 2017. “DDoS in the IoT: Mirai and Other Botnets”. *Computer* 50 (7): 80–84. ISSN: 0018-9162. doi:10.1109/MC.2017.201.

Kumar, N., J. Madhuri ja M. ChanneGowda. 2017. “Review on security and privacy concerns in Internet of Things”. Teoksessa *2017 International Conference on IoT and Application (ICIOT),* 1–5. Toukokuu. doi:10.1109/ICIOTA.2017.8073640.

Level 3 Threat Research Labs. 2016. “Attack of Things!” Viitattu 19. syyskuuta 2019. https://web.archive.org/web/20161003194500/http://blog.level3.com/security/attack-of-things/.

Lin, Huichen, ja Neil W. Bergmann. 2016. “IoT Privacy and Security Challenges for Smart Home Environments” [kielellä English]. Date revised - 2016-10-01; Last updated - 2016-10-04, *Information* 7, numero 3 (0): 44. https://search.proquest.com/docview/1825565152?accountid=11774.

Mahjabin, Tasnuva, Yang Xiao, Guang Sun ja Wangdong Jiang. 2017. “A survey of distributed denial-of-service attack, prevention, and mitigation techniques”. *International Journal of Distributed Sensor Networks* 13 (12): 1550147717741463. doi:10.1177/1550147717741463. eprint: https://doi.org/10.1177/1550147717741463. https://doi.org/10.1177/1550147717741463.

MalwareMustDie. 2016a. “MMD-0055-2016 - Linux/PnScan ; ELF worm that still circles around”. Viitattu 3. toukokuuta 2019. https://web.archive.org/web/20190503212644/http://blog.malwaremustdie.org/2016/08/mmd-0054-2016-pnscan-elf-worm-that.html.

———. 2016b. “MMD-0059-2016 - Linux/IRCTelnet (new Aidra) - A DDoS botnet aims IoT w/ IPv6 ready”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190921003646/http://blog.malwaremustdie.org/2016/10/mmd-0059-2016-linuxirctelnet-new-ddos.html.

Mansfield-Devine, Steve. 2017. “Weaponising the Internet of Things”. *Network Security* 2017 (10): 13–19. ISSN: 1353-4858. doi:https://doi.org/10.1016/S1353-4858(17)30104-6. http://www.sciencedirect.com/science/article/pii/S1353485817301046.

Marzano, A., D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. P. C. Chaves, Í. Cunha, D. Guedes ja W. Meira. 2018. “The Evolution of Bashlite and Mirai IoT Botnets”. Teoksessa *2018 IEEE Symposium on Computers and Communications (ISCC),* 00813–00818. Kesäkuu. doi:10.1109/ISCC.2018.8538636.

Mirkovic, Jelena, ja Peter Reiher. 2004. “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”. *SIGCOMM Comput. Commun. Rev.* (New York, NY, USA) 34, numero 2 (huhtikuu): 39–53. ISSN: 0146-4833. doi:10.1145/997150.997156. http://doi.acm.org/10.1145/997150.997156.

NETSCOUT Systems, Inc. 2017. “Reaper Madness”. Viitattu 15. syyskuuta 2019. https://web.archive.org/web/20190915154913/https://www.netscout.com/blog/asert/reaper-madness.

NETSCOUT Systems, Inc. 2018. “NETSCOUT Arbor’s 14th Annual Worldwide Infrastructure Security Report”. Viitattu 10. kesäkuuta 2019. https://web.archive.org/web/20190610194915/https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf.

NETSCOUT Systems, Inc. 2017. “NETSCOUT Arbor’s 13th Annual Worldwide Infrastructure Security Report”. Viitattu 20. maaliskuuta 2018. https://web.archive.org/web/20180320005527/https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf.

NJCCIC. 2019. “Botnets, New Jersey Cybersecurity and Communications Integration Cell”. Viitattu 22. elokuuta 2019. https://web.archive.org/web/20190821231047/https://www.cyber.nj.gov/threat-profiles/botnets/.

Nordrum, A. 2016. “The internet of fewer things [News]”. *IEEE Spectrum* 53, numero 10 (lokakuu): 12–13. ISSN: 0018-9235. doi:10.1109/MSPEC.2016.7572524.

Palo Alto Networks. 2017. “New IoT/Linux Malware Targets DVRs, Forms Botnet”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190920235832/https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/.

Penttinen, Tuomo. 2005. “Distributed denial-of-service attacks in the Internet”. Tutkielma. http://urn.fi/URN:NBN:fi:jyu-200662.

Radware Ltd. 2017a. “”BrickerBot” Results In PDoS Attack”. Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190921165553/https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/.

———. 2017b. “Why the World is Under the Spell of IoT_Reaper”. Viitattu 1. lokakuuta 2019. https://web.archive.org/web/20191001192511/https://blog.radware.com/security/2017/10/iot_reaper-botnet/.

Raghavan, S.V., ja E. Dawson, toimittaneet. 2011. *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks : Critical Information Infrastructure Protection.* 348. India: Springer India. http://dx.doi.org/10.1007/978-81-322-0277-6.

Recorded Future, Inc. 2018. "Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018". Viitattu 15. syyskuuta 2019. https://web.archive.org/web/20190616021241/https://go.recordedfuture.com/hubfs/reports/cta-2018-0405.pdf.

Santanna, J. J., R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville ja A. Pras. 2015. "Booters — An analysis of DDoS-as-a-service attacks". Teoksessa *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM),* 243–251. Toukokuu. doi:10.1109/INM.2015.7140298.

Schiller, Craig A. 2007. *Botnets : The Killer Web Applications.* Syngress. ISBN: 9781597491358. http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=nlebk&AN=184406&site=ehost-live.

Shobana, M., ja S. Rathi. 2018. "IOT Malware : An Analysis of IOT Device Hijacking" [kielellä en]. Teoksessa *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 10. ISSN: 2456-3307.

Singh, B., K. Kumar ja A. Bhandari. 2015. "Simulation study of application layer DDoS attack". Teoksessa *2015 International Conference on Green Computing and Internet of Things (ICGCIoT),* 893–898. Lokakuu. doi:10.1109/ICGCIoT.2015.7380589.

Tiirmaa-Klaar, Heli. kirjoittaja. 2013. *Botnets.* 97. SpringerBriefs in Cybersecurity. London: Springer London. http://dx.doi.org/10.1007/978-1-4471-5216-3.

Trend Micro Inc. 2017. "Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras". Viitattu 21. syyskuuta 2019. https://web.archive.org/web/20190921001552/https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/.

Verisign, Inc. 2018. “Verisign Q2 2018 DDoS Trends Report”. Viitattu 10. huhtikuuta 2019. https://web.archive.org/web/20190410201119/https://www.a10networks.com/sites/default/files/a10-tps-eb-verisign-distributed-denial-of-service-trends-report-vol-5-issue-2.pdf.

Vervier, Pierre-Antoine, ja Yun Shen. 2018. “Before Toasters Rise Up: A View into the Emerging IoT Threat Landscape”. Teoksessa *Research in Attacks, Intrusions, and Defenses,* toimittanut Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis ja Sotiris Ioannidis, 556–576. Cham: Springer International Publishing. ISBN: 978-3-030-00470-5.

Williams, R., E. McMahon, S. Samtani, M. Patton ja H. Chen. 2017. “Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach”. Teoksessa *2017 IEEE International Conference on Intelligence and Security Informatics (ISI),* 179–181. Heinäkuu. doi:10.1109/ISI.2017.8004904.

Zargar, S. T., J. Joshi ja D. Tipper. 2013. “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”. *IEEE Communications Surveys Tutorials* 15, numero 4 (FourthFourth): 2046–2069. ISSN: 1553-877X. doi:10.1109/SURV.2013.031413.00127.

Zunnurhain, Kazi. 2016. “Vulnerabilities with Internet of Things” [kielellä eng]. *Proceedings of the International Conference on Security and Management (SAM):* 83. https://jyu.finna.fi/PrimoRecord/pci.proquest1855394808.

Özçelik, M., N. Chalabianloo ja G. Gür. 2017. “Software-Defined Edge Defense Against IoT-Based DDoS”. Teoksessa *2017 IEEE International Conference on Computer and Information Technology (CIT),* 308–313. Elokuu. doi:10.1109/CIT.2017.61.