MAANPUOLUSTUSKORKEAKOULU

DOS- JA DDOS-HYÖKKÄYKSIEN KÄYTTÖ JA VAIKUTUKSET VERKOSSA

Kandidaatintutkielma

Kadetti
Joe Lindberg

Merikadettikurssi 81
Johtamisjärjestelmäopintosuunta

Maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
81. Merikadettikurssi	Merisotalinja
Tekijä Kadetti Joe Lindberg	
Tutkielman nimi **DoS- ja DDoS-hyökkäyksien käyttö ja vaikutukset verkossa**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika Maaliskuu 2014	Tekstisivuja 24 Liitesivuja 0

TIIVISTELMÄ

Tutkimuksen tarkoituksena on selvittää lähdemateriaalin avulla mitä DoS- ja DDoS-hyökkäykset ovat, kuinka niitä voidaan hyödyntää ja mitä vaikutuksia niillä on verkossa. Tutkimuksessa vastataan kysymyksiin: mitä ovat DoS- ja DDoS-hyökkäykset, mikä merkitys botnet-verkoilla on DDoS-hyökkäyksissä, mitä vaikutuksia voidaan saavuttaa DoS- ja DDoS-hyökkäyksillä ja minkälaisia tunnettuja DoS- ja DDoS-hyökkäysmalleja on olemassa. Tutkimuksen tavoitteena on kasvattaa lukijan teknistä ymmärrystä palvelunestohyökkäyksistä yhtenä verkkohyökkäyksen keinona. Tutkimuksessa käytetty lähdemateriaali koostuu mittavilta osin internetpohjaisista lähteistä ja julkisista artikkeleista. Aihe on ajankohtainen ja jatkuvasti tekniikan mukana kehittyvä, eikä uusinta tietoa iskuista ole aina painettu kirjoihin. Aiheen teknisiä perusperiaatteita käsittelevissä osuuksissa on käytetty lähdemateriaalina myös kirjallisuuslähteitä. Tutkimusmenetelmänä tutkimuksessa on laadullinen kirjallisuuskatsaus.

Palvelunestohyökkäykset ovat ajankohtainen tapa hyökätä erilaisia verkkoja vastaan globalisoituvassa maailmassa. Hyökkäysten tavoitteena on vaikuttaa kohteeseen lamauttaen kohdeverkko määritetyksi tai määrittelemättömäksi ajaksi ja näin edesauttaa hyökkääjän ajamia motiiveja hyökkäyksen toteuttamiseksi. Teknisiä malleja toteuttaa hyökkäys on lukemattomia, mutta lukuisat eri protokollia hyödyntävät mallit ovat usein perusrakenteeltaan hyvin samankaltaisia ja tunnistettavia. Palvelunestohyökkäykset ovat kustannustehokas ja nykyaikainen vaikutuksen keino haluttuun kohteeseen, useissa eri käyttötarkoituksissa.

AVAINSANAT

DoS, DDoS, Palvelunesto, Palvelunestohyökkäys, Botnet-verkko, Zombie-kone, Verkkohyökkäys

KANDIDAATIN TUTKIELMA – DOS- JA DDOS-HYÖKKÄYKSIEN KÄYTTÖ JA VAIKUTUKSET VERKOSSA

SISÄLLYS

LÄHTEET

KUVALUETTELO

1 JOHDANTO

Tietotekniikka on lyhyen historiansa aikana kasvanut valtavaa vauhtia mahdollistaen lähes koko maailman verkottumisen internetin myötä. Internetin yleistymisen myötä on saavutettu suuria hyötyjä ja valtavaa kasvua verkostoitumisessa. Hyötyjen ohella on kuitenkin syntynyt myös menetelmiä joilla verkkoa voidaan käyttää väärin, tai näkökulmasta riippuen verkon ominaisuuksia ja heikkouksia hyödyntäen tavoitella etua henkilölle, järjestölle tai organisaatiolle. DoS- ja DDoS-hyökkäykset ovat yksi menetelmä jolla voidaan hyökätä verkkoa vastaan aiheuttaen tietyksi ajaksi vahinkoa verkolle, hidastaen näin verkkoa tai estäen kokonaan verkon toiminnan.

DoS- ja DDoS-hyökkäykset ovat olleet merkittävässä roolissa verkkohyökkäysten saralla 2000-luvulla. Suurista DoS- ja DDoS-hyökkäyksistä uutisoidaan lähes kuukausittain. DoS- ja DDoS-hyökkäykset ovat yhä ajankohtainen keino vaikuttaa kohteeseen, hidastaen ja lamauttaen kohteen tärkeät verkot. DDoS-hyökkäyksiä voidaan käyttää useiden eri motiivien vuoksi. Motiivit voivat olla poliittisia tai henkilökohtaisia, eikä hyökkäyksen toteuttamiseen välttämättä tarvita valtavia resursseja. DoS- ja DDoS-hyökkäykset ovatkin verrattain yksinkertainen, halpa ja tehokas keino vaikuttaa haluttuun kohteeseen.

Tutkielmassa tutkin DoS- ja DDoS-hyökkäysten toimintaperiaatteita. Tutkielman tarkoitus on osoittaa DoS- ja DDoS-hyökkäyksien ominaisimmat tekniset toimintamallit, käytetyt menetelmät ja käytön tyypillisimmät vaikutukset hyökkäyskohteena olevaan tietoverkkoon.

1.1 Tutkimusmenetelmät ja lähteet

Tutkimus on laadullinen kirjallisuuskatsaus. Tutkimuksessa käytetään lähteinä pääosin internetlähteitä aiheen jatkuvan kehityksen ja muutoksen vuoksi, tämän lisäksi tutkimuksen lähteinä on käytetty kirjallisuutta joka käsittelee aiheen ajattomia perusperiaatteita. Tutkimuksessa ei oteta kantaa aiempiin aiheesta tehtyihin tutkimuksiin. Tutkimus on itsenäinen katsaus aihealueen keskeisistä universaaleista teknisistä tekijöistä.

1.2 Tutkimuskysymykset

”Mitä ovat DoS- ja DDoS-hyökkäykset?” on tutkimuksen pääkysymys jossa selvitän DoS- ja DDoS-hyökkäyksen tunnusomaiset piirteet ja tekniset käyttömahdollisuudet. Kysymykseen vastataan luvuissa kaksi ja kolme.

”Mikä merkitys botnet/zombie–verkoilla on osana DDoS-hyökkäystä?” on tutkimuksen ensimmäinen alakysymys, joka tarkentaa DDoS-hyökkäyksen rakennetta ja jossa tutkin zombie–koneiden ja botnet–verkkojen rakentumista oleellisena osana DDoS-hyökkäyksen rakennetta. Kysymykseen vastataan luvussa kaksi.

”Mitä vaikutuksia voidaan saavuttaa DoS-tai DDoS-hyökkäyksellä?” on tutkimuksen toinen alakysymys, jossa esitän DoS- ja DDoS-hyökkäysten mahdollista vaikutusta kohteeseen. Kysymykseen vastataan luvuissa neljä ja viisi.

”Minkälaisia tunnettuja DDoS-malleja on olemassa?” on tutkimuksen kolmas alakysymys jossa tutkin valittuja ja tunnettuja DDoS-malleja ja analysoin näiden yhtäläisyyksiä sekä eroja. Tutkimuksessa otan myös kantaa näiden mallien syntymiseen ja käyttötarkoitukseen. Kysymykseen vastataan luvussa kolme.

1.3 Tutkielman rakenne

Tutkielmassa esittelen DoS- ja DDoS-hyökkäykset, hyökkäysten toimintaperiaatteet ja yleisimmät mallit joilla toteuttaa näitä hyökkäyksiä. Johdannon jälkeen avaan tutkielmassa yleisimmin käytetyt vieraskieliset termit.

Tutkielman ensimmäisessä tekstiluvussa esittelen yleisesti DoS- ja DDoS-hyökkäykset ja mitä ne käsitteenä tarkoittavat, tämän lisäksi alaluvuissa esittelen DoS-hyökkäyksistä puhuttaessa oleellisina käsitteinä Zombie-koneen sekä Botnet-verkon.

Tutkielman toisessa tekstikappaleessa esittelen tunnettuja DoS- ja DDoS-hyökkäysmalleja, sekä alakappaleena esittelen erikseen nollapäivähaavoittuvuuden merkityksen DDoS-hyökkäyksissä.

Kolmannessa tekstiluvussa analysoin DoS- ja DDoS-hyökkäysten vaikutusta kohteeseen sekä analysoin hyötyjä joita hyökkäyksellä voidaan saavuttaa.

Neljännessä varsinaisessa tekstiluvussa esittelen ja analysoin muutamia yleisesti tunnettuja tapauksia, joissa on käytetty joko DoS- tai DDoS-pohjaista hyökkäystä. Luvussa pohdin mitä hyökkäyksillä on pyritty saavuttamaan ja analysoin tilannetta sotilaallisen käytön näkökulmasta.

Viimeinen tekstiluku sisältää johtopäätökset jossa analysoin esitettyjen mallien pohjalta DoS- ja DDoS-hyökkäysten käyttömahdollisuuksia yleisesti, sekä sotilaskäytössä. Summaan luvussa yhteen tutkielmassa esitetyt mielipiteet ja pohdin DDoS-hyökkäysten merkitystä kyberiskuissa.

1.4 Yleisimmin käytetyt termit ja lyhenteet

Alla keskeisimmät käytetyt vieraskieliset lyhenteet. Useimmat lyhenteistä selitetään tarkemmin tekstiluvuissa lähdeviittauksineen.

DoS on lyhennös englanninkielisestä termistä Denial of Service, joka tarkoittaa palvelunestohyökkäystä. DoS-hyökkäyksessä hyökkäslähteitä on yleensä vain yksi.

DDoS on lyhennös englanninkielisestä termistä Distributed Denial of Service, joka tarkoittaa hajautettua palvelunestohyökkäystä. Toisin kuin DoS-hyökkäyksessä, DDoS-hyökkäyksessä hyökkäyslähteitä on useita ja hyväksi käytetään usein Botnet-verkkoa.

Botnet-verkko on haittaohjelmin kaapatuista tietokoneista koottu verkko, jota käytetään DDoS-hyökkäysten muodostamiseen. Nimi muodostuu englanninkielisistä sanoista robot ja network, eli botnet.

Zombie-kone on haittaohjelmalla kaapattu tietokone, jota käytetään usein osana botnet-verkkoa.

TCP/IP on lyhennös englanninkielisestä termistä Transmission Control Protocol/Internet Protocol. TCP/IP on yleisimmin käytössä oleva alemman tason tietoverkkoprotokolla, joka vastaa internetissä päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä.

DNS on lyhennös englanninkielisestä termistä Domain Name Server. Kyseessä on internetin nimipalvelu, joka muuttaa selkokielisiä verkkotunnuksia IP-osoitteiksi. DNS palvelun haa-

voittuvuuksia on käytetty useissa tapauksissa hyväksi DDoS-hyökkäyksissä. Esimerkkinä tapaus Spamhaus tutkielman tekstiluvussa viisi.

Nollapäivähaavoittuvuus on ohjelmassa tai ohjelmistossa oleva tietoturva-aukko, josta ohjelman valmistaja tai ohjelman ohjelmoinut taho ei ole vielä tietoinen.

2 MITÄ OVAT DOS JA DDOS HYÖKKÄYKSET

DoS-hyökkäyksellä tarkoitetaan menetelmää, jolla hyökkääjä pyrkii estämään jonkin verkkopalvelun käytön kyseisen palvelun tavanomaisilta käyttäjiltä. DoS-hyökkäyksestä puhuttaessa tarkoitetaan yleensä yksinkertaista palvelunestohyökkäystä, joka laukaistaan yhdestä lähteestä. [1] On olemassa useita eri tapoja toteuttaa tämänkaltainen palvelun käytön estäminen. Eri tapoja toteuttaa palvelunestohyökkäys ovat esimerkiksi [2]:

1. ”Flooding” eli verkon täyttäminen liikenteellä - jolloin palvelin ruuhkautuu eikä näin ollen enää kykene käsittelemään oikeaa liikennettä.
2. Kahden laitteen välisen yhteyden häiritseminen - estäen näin pääsy palveluun.
3. Yksittäisen henkilön pääsyn estäminen tiettyyn palveluun tai yhteyden estäminen palvelusta tiettyyn järjestelmään tai henkilöön.

DDoS-hyökkäys on DoS-hyökkäystä vastaava palvelunestohyökkäys, jossa lähteenä käytetään hyväksi laajaa eri osoitteiden verkostoa. Hyökkäävät verkot koostuvat yleensä saastutetuista zombiekoneista ja näin voidaan myös peittää hyökkääjän jäljet, saattaen kohdekoneen näkökulmasta hyökkääjän osoitteeksi botkoneiden osoitteet.[3, luku 18.3]. Esecurityplanetin internetsivujen DoS- ja DDoS-hyökkäyksien torjuntaa käsittelevässä artikkelissa mainitaan DDoS-hyökkäyksesta seuraavaa: “DDoS-hyökkäyksessä uhrin palvelimen hukuttava verkkoliikenne voi olla peräisin jopa sadoista tuhansista tai useammista osoitteista” [1].

DDoS-hyökkäyksessä käytetyt menetelmät ja vaikutukset ovat yhteneväisiä DoS-hyökkäyksissä käytettyjen menetelmien kanssa. DDoS-hyökkäykset ovat laajuudeltaan suurempia ja hyökkäys toteutetaan samanaikaisesti lukuisista eri lähteistä, käyttäen yleensä hyväksi botverkkoa. DDoS-hyökkäys on yksinkertaiseen DoS-hyökkäykseen nähden huomattavasti vaikeampi torjua, johtuen hyökkäyksen eri kerroksista ja lähteistä. Yksittäisestä jatkuvasta lähteestä tulevan DoS-hyökkäyksen voi sulkea yksinkertaisesti katkaisemalla yhteyden kyseiseen IP-osoitteeseen, mutta DDoS-hyökkäyksessä lähteitä ja osoitteita voi olla tuhansia ympäri maailmaa.[4, s. 1026]

DoS- ja DDoS-hyökkäykset voivat olla hyvin monimuotoisia ja niitä voidaan käyttää eri muodoissaan useita eri palveluita vastaan. Cert.org määrittelee internetsivuillaan hyökkäyksen kolme perustyyppiä [2]:

1. Hyökkäys joka kohdistuu kohteen vähäisten, rajallisten tai uusiutumattomien resurssien kuluttamiseen.
2. Hyökkäys joka tuhoaa tai muuttaa järjestelmän konfiguraatiotietoja.

3. Hyökkäys joka fyysisesti tuhoaa tai muuttaa tietoverkon komponentteja.

Nämä hyökkäyksen perustyypit voidaan toteuttaa käyttäen hyväksi mitä mielukuvituksellisimpia keinoja. Hyökkäykset voidaan toteuttaa joko käyttäen ulkoisia resursseja, tai vastaavasti käyttämällä hyökkäyksen kohteena olevan tietokoneen tai verkon omia ominaisuuksia itseään vastaan. [2]

2.1 Zombiekone

Ennen DoS- ja DDoS-hyökkäysten tunnettujen hyökkäysmallien tarkastelua on hyvä tutustua zombie-koneen ja botnet-verkon käsitteisiin. Botnet-verkko on suuressa roolissa DDoS-hyökkäyksistä puhuttaessa. Zombie-koneella tarkoitetaan yksittäistä tietokoneohjelman saastuttamaa konetta, joka on ohjelmoitu suorittamaan jokin hyökkääjän määrittämä toimenpide. Zombie-kone voi toteuttaa myös useita toimenpiteitä ja siitä voidaan puhekielessä käyttää myös muita termejä, kuten esimerkiksi orjakone tai botti.

” A zombie machine is a computer connected to the Internet that has been successfully attacked by a computer virus, worm, or trojan horse. A hacker will compromise thousands of such machines to create a “Zombie Army” or a “BotNet” [5]. Zombie–kone on internetiin yhteydessä oleva tietokone, joka on onnistuneesti saastutettu tietokoneviruksella, madolla tai troijalaisella hevosella. Hakkeri käyttää tuhansia tämänkaltaisia koneita luodakseen ”Zombie-armeijan” tai Botnet-verkon.

Useimmat käyttäjät eivät tiedä koneensa toimivan zombie-koneena ja tämän havaitseminen voi olla vaikeaa [5]. Zombie-konetta voidaan käyttää DDoS-hyökkäysten lisäksi myös roskapostin, tai minkä tahansa muun materiaalin lähettämiseen niin kaupallisessa kuin huijaustarkoituksessa [6]. Tässä tutkimuksessa käsittelen Zombiekonetta ja Botverkkoa teknisestä näkokulmasta, sekä niiden käyttöä yksinomaan osana palvelunestohyökkäystä.

2.2 Botnet-verkko

Botnet-verkko saa nimensä yhdistettynä kahdesta englanninkielestä sanasta ro*bot ja net*work eli *botnet*, suomeksi botverkko tai vieraskielisenä lainauksena botnet-verkko. Botin tai zombien tarkoittaessa yksittäistä hakkerin haltuunsa ottamaa konetta, tarkoittaa botnet-verkko useamman saastutetun koneen yhdessä muodostamaa verkkoa. [7]

Botnet-verkko on lähes välttämätön DDoS-hyökkäyksen suorittamiseksi. Suorittaakseen DDoS-hyökkäyksen on hyökkääjän ensin muodostettava botnet-verkko, joka yleensä toteutetaan luomalla tietokonevirus. Tietokonevirus itsenäisesti monistaa ja jakaa itseään internetin välityksellä. Viruksen saastutettua koneet, virus aktivoituu tiettynä määritettynä ajankohtana, jolloin kaikki viruksen saastuttamat koneet lähettävät samanaikaisesti yhteyspyynnön hyökkäyksen kohteena olevaan osoitteeseen, tukkien kohteen verkkoliikenteen. [8]

3 TUNNETTUJA DOS JA DDOS HYÖKKÄYSMALLEJA

Dos- ja DDoS-hyökkäyksistä ovat hyökkäyksiä, jolla tukitaan kohdekoneen tai verkon liikenne. Tämä vaikutus voidaan saada aikaan useammalla eri tekniikalla ja menetelmällä. Tässä kappaleessa analysoin muutamia hyvin tunnettuja hyökkäysmalleja. Analysoin näiden mallien toimintaperiaatteita, yhtäläisyyksiä sekä eriävyyksiä muodostaen näin yleiskuvan DoS- ja DDoS-hyökkäysten ominaispiirteistä.

3.1 Smurf–hyökkäys

Smurf-hyökkäys tuli tunnetuksi 90-luvulla ja oli aikansa pahimpia käytössä olevia DoS-hyökkäyksiä. Smurf–hyökkäyksessä hyödynnetään ICMP-protokollaa väärentämällä ICMP echo request paketin lähettäjäksi kohdekoneen IP-osoite. [9, 10] ICMP eli Internet Control Message Protocol on IP-pakettien virhe-, ohjaus ja muita viestejä varten luotu järjestelmä, joka on kiinteä pari IP-protokollalle. ICMP echo request pakettia käytetään määrittämään vastaako jokin tietty kone lähetettyihin pyyntöihin internetissä. [10, 11]

Hyökkääjä hyödyntää ICMP–protokollaa lähettämällä ICMP echo request paketin kohdekoneen IP-osoitteen nimissä kaikille kohdekoneen verkossa oleville koneille, saaden näin kaikki koneet vastaamaan kohdekoneen IP-osoitteelle ICMP echo reply paketeilla. Verkossa olevien koneiden määrästä riippuen, kaikkien koneiden vastatessa tukkiutuu kohdekoneen verkko valtavan vastausliikenteen rasituksessa ja näin normaalille liikenteelle ei enää jää kaistaa. Pahimmassa tapauksessa koko verkko lamaantuu täysin ja sen toiminta lakkaa. [10]

Smurf-hyökkäyksen tehokkuudesta ja tuhoisuudesta huolimatta, sen yksinkertaisuus mahdollistaa myös hyökkäyksen helpon torjumisen. Hyökkäys voidaan torjua yksinkertaisesti konfiguroimalla reititin olemaan vastaamatta ICMP echo request paketteihin, sekä reitittimet voidaan ohjelmoida varmistamaan, että lähetysosoitteeseen lähetettyjä viestejä ei välitetä eteenpäin. [9, 12]

Nykypäivänä smurf-hyökkäyksen ei tarjoa niin suurta hyötyä hyökkääjille helpon torjuttavuuden takia. Smurf-hyökkäystä voidaan silti yhä käyttää tehokkaasti varautumattomia kohteita vastaan. Smurf-hyökkäyksen hyökkäysmalli osoittaa kuinka yksinkertaiset DoS-hyökkäykset toimivat ja kuinka verkko voidaan tukkia käyttämällä ainoastaan verkon oman protokollan sisäisiä viestejä. Smurf-hyökkäyksen kaltaisia hyökkäyksiä jotka toimivat samalla periaatteella on useita, kuten Fraggle joka käyttää ICMP protokollan sijaan UDP (User Data Protocol) protokollan viestejä. [12]

3.2 Ping of Death–hyökkäys

Ping of Death on historiallinen hyökkäys, joka käyttää hyväkseen TCP/IP protokollan pakettien sirpaloimisen mahdollistamaa haavoittuvuutta. Ping of Death perustuu TCP/IP protokollan ominaisuuteen ”fragmentation” eli sirpaloiminen, jossa yksittäinen IP-paketti jaetaan useaan pieneen osaan. Tätä ominaisuutta tarvittiin aikanaan, sillä tyypillinen internetyhteys ei tukenut paketteja jotka olivat kooltaan suurempia kuin muutama tuhat bittiä. IP-protokolla taasen mahdollisti 64 kilobitin pakettien lähettämisen, jolloin nämä paketit tuli sirpaloida osiin. IP-protokollassa paketti ei voi ylittää 65536-bittiä, mutta pieninä palasina tämän koon ylittäminen oli mahdollista, jolloin sirpaleiden yhteenlaskettu koko oli tätä pakettikokoa suurempi. Ping of death hyödynsi tätä haavoittuvuutta, sillä järjestelmälle pakettikoon ylittäminen oli niin sanottu mahdottomuus, aiheutti tämänkaltaisen paketin lähettäminen kohdejärjestelmän kaatumisen. Nykypäivänä suurin osa järjestelmistä on päivitetty ja tämä haavoittuvuus on korjattu. [13]

Vaikka ping of death-hyökkäykset ovatkin suurelta osin historiaa ja kyseistä haavoittuvuutta ei enää suurimmassa osassa verkkoja ole mahdollista hyödyntää, se on erinomainen esimerkki palvelunestohyökkäysten historiassa. Ping of death osoittaa kuinka palvelunesto voidaan toteuttaa yksittäistä haavoittuvuutta hyväksikäyttäen. Toisin kuin smurf-hyökkäyksessä, ping of death mahdollisti kohdejärjestelmän kaatumisen käyttäen hyväksi suoraa lähetystä kohdekoneeseen ja se voitiin suorittaa käyttämättä suurta datamäärää. Ping of death mahdollisti kuitenkin vain lievän vaikutuksen kohdejärjestelmään, saamalla järjestelmän ainoastaan kaatumaan. Se ei varsinaisesti tukkinut tämän toimintaa pidemmäksi aikaa. Tämänkaltainen hyökkäys voisi kuitenkin olla vakava iskettäessä järjestelmään jonka toiminta ei saa keskeytyä, esimerkiksi kesken tiedon prosessointia.

3.3 SYN Flood ja tulva-hyökkäykset

Suuri osa palvelunestohyökkäyksistä perustuu ”tulvaamiseen” (Flooding). Tulvaaminen on palvelunestohyökkäyksille ominainen tapa saavuttaa haluttu lopputulos, eli palvelun esto. Palvelunestohyökkäyksiä tarkastellessa voidaan loogisesti todeta lähes jokaisen hyökkäysmallin perustuvan eräänlaiseen tulvaefektin aiheuttamiseen, eli suuren tietoliikennemäärän lähettämiseen kerralla kohteeseen tai muodostamalla loputtoman loopin. Tällöin data kiertää kohdekoneessa tai palvelimessa loputtomasti vieden kohteen muistia, saattaen kohteen kaatumaan tai

kyvyttömäksi vastaanottamaan muuta liikennettä. Tässä alakappaleessa käsittelen tyypillisiä tulvahyökkäyksiä, joista otan tarkasteluun muutaman yleisesti tunnetun mallin.

Yksinkertaisin tapa toteuttaa tulva lienee jo käsitelty Smurf-hyökkäys jota voidaan käyttää DDoS-mallin mukaisesti täyttämään vastaanottajan kaista liikenteellä. Käytettäessä Zombie-koneita voi yhtäaikainen rasitus tulla miljoonilta koneilta, jolloin koko verkko tukkeutuu tulvan vaikutuksesta. [14]. Tässä kappaleessa käsittelen tarkemmin Smurf–hyökkäyksestä poikkeavia tulvahyökkäyksiä joka eivät keskity koko kaistan viemiseen vaan ainoastaan hyökkäämään kohdekoneen tiettyjen resurssien käyttöä vastaan.

Tiettyyn resurssiin kohdennetusta hyökkäyksestä käytetään yleisesti termiä ”Flood” eli tulva. Tämänkaltainen hyökkäys kohdistuu yhteen tai useampaan kohdennettuun resurssiin ja hyökkäyksen tavoitteena on estää näiden resurssien toiminta kuormittamalla niitä suurella määrällä yhdenaikaisia pyyntöjä. Esimerkiksi sähköpostipalvelin voidaan tukkeuttaa lähettämällä tuhansia turhia viestejä palvelimelle lyhyessä ajassa. Tällöin kaista voi olla tarpeeksi laaja käsittelemään kaiken liikenteen, mutta sähköpostiohjelma tai palvelin ei tähän kykene, jolloin pääsy sähköpostiin estyy ja palvelunesto toteutuu. Toisena esimerkkinä voidaan mainita tilanne, jossa esimerkiksi yrityksen verkossa olevalle tulostimelle ohjataan useita suuria tulostustehtäviä samanaikaisesti. Tulostimen prosessoidessa valtavaa pyyntöjen määrää ei tulostinta voida käyttää muihin tehtäviin. Tämä voidaan toteuttaa tahallisena palvelunestona tai tämänkaltainen esimerkki voi myös tapahtua vahingossa, ajattelemattoman työntekijän toiminnan seurauksena. Kyseessä on tilanteesta riippumatta tulvahyökkäysmallin mukainen palvelunesto. [14]

SYN Flood–hyökkäyksessä on tyypillistä käyttää hyväkseen joko TCP tai UDP protokollaa hieman Smurf–hyökkäys mallin mukaisesti. Useimmat palvelut nykyinternetissä pohjautuvat TCP protokollaan kuten http eli hyper text transfer protocol, joka paremmin tunnetaan maailmanlaajuisen verkon palveluna (world wide web, eli www). SYN Flood-hyökkäyksessä ”SYN” tarkoittaa synkronointilippua (flag) TCP paketissa joka lähetetään vastaanottajalle. SYN-lippu asetetaan viestiin heti ensimmäisellä yhteyskerralla kun järjestelmä lähettää paketin käyttäen TCP protokollaa. Synkronointilippu osoittaa vastaanottavalle järjestelmälle, että sen tulisi varastoida tämä pakettiin liitetty järjestysnumero. TCP paketti sisältää kaksikymmentä bittiä. TCP paketin kahdestakymmenestä bitistä kuusi bittiä muodostaa viestin lipun, jolla voidaan osoittaa TCP paketille eri tarkoituksia kuten alkuperäinen järjestysnumero (SYN), kuittausviesti (ACK), yhteyden uudelleenmuodostamisviesti (RST) tai yhteyden sulkemisviesti (FIN). SYN Flood-väärennöshyökkäyksessä hyökkäävä järjestelmä käyttää tätä

bittijonoa hyväkseen väärentämällä lähteen IP-osoitteen, jolloin SYN-viesti vaikuttaa aidolta. Väärennetty lähdeosoite osoittaa kuitenkin järjestelmään jota ei oikeasti ole olemassa, joten lähetyksen päättävää kuittausviestiä (ACK) ei ikinä lähetetä kohteelle. Tämä johtaa tilanteeseen jossa kohdekoneelle jää auki puoliavoimia yhteyksiä jotka eivät johda mihinkään. Nämä puoliavoimet yhteydet vievät serverin resursseja lopulta eväten aitojen yhteyksien muodostamisen, jolloin palvelunesto toteutuu. Tämänkaltainen palvelunestohyökkäys voidaan toteuttaa myös DDoS-hyökkäyksenä jolloin toimintametodi on sama, mutta väärennettyjä SYN viestejä lähettäviä koneita on useita. [15, s. 2-4]

SYN Flood voidaan toteuttaa myös suorasti väärentämättä lähteen IP-osoitetta, jolloin puhutaankin suorasta SYN Flood-tulvahyökkäyksestä. Suorassa hyökkäyksessä hyökkääjä lähettää tavallisia, aitoja SYN-viestejä toistuvasti suuria määriä. Viestien tulva aiheuttaa kohdekoneen tukkeutumisen. Tähän malliin voidaan liittää DDoS-elementti jolloin useat koneet lähettävät samanaikaisesti SYN-viestejä lisäten suoran hyökkäyksen kapasiteettia huomattavasti. Tällöin hyökkäävä kone täytyy kuitenkin asettaa olemaan vastaamatta SYN-ACK kuittausviesteihin, jotta liikenne ei siirry kuitatuksi ja tule näin ollen torjutuksi. Hyökkääjä voi toteuttaa tämän yksinkertaisilla palomuuriasetuksilla jotka estävät hyökkäävän järjestelmän kuittausviestien lähettämisen. [15, s. 2-4]

TCP tai UDP protokollaa hyödyntävä SYN Flood-hyökkäys voikin siis toimia kolmella eri tavalla, joita ovat suora hyökkäys, levitetty suora hyökkäys (DDoS) tai väärennöshyökkäys (Spoofing attack). [15, s. 2.4] Menetelmiä toteuttaa tulvahyökkäys on monia ja niiden toteuttamiseen voidaan hyödyntää useita eri haavoittuvuuksia. Esimerkiksi myöhemmin käsittelemässäni Spamhaus hyökkäyksessä käytettiin DNS-nimipalvelimien haavoittuvuutta väärennöshyökkäyksen suorittamiseen. Tällaisessa hyökkäyksessä hyökkääjä valjastaa botnet-verkon suorittamaan lukemattomia väärennettyjä DNS-vastauspyyntöjä haavoittuvuuden omaaville järjestelmille. Järjestelmät ohjaavat liikenteen palvelunestohyökkäyksen kohteena olevaan palvelimeen tai koneeseen, luullen vastaavansa botverkon koneille jotka pyynnöt ovat lähettäneet. [16] Tästä kerron lisää Spamhaus tapauksesta kertovassa luvussa.

3.4 Nollapäivähaavoittuvuudet

Nollapäivähaavoittuvuus on ohjelmassa tai ohjelmistossa oleva tietoturva-aukko, josta ohjelman valmistaja tai ohjelman ohjelmoinut taho ei ole vielä tietoinen. Hakkerit voivat löytää tällaisen haavoittuvuuden ennen kuin ohjelman tuottanut taho on itse tietoinen haavoittuvuudes-

ta. Haavoittuvuutta voidaan käyttää hyväksi erilaisissa hyökkäyksissä. Kun ohjelman tuottanut taho lopulta saa tietää haavoittuvuudesta, alkaa yleensä kilpailu haavoittuvuutta hyödyntävien tahojen ja ohjelman tuottavan tahon välillä, tuottavan tahon pyrkiessä korjaamaan aukon ja rikollisten tahojen pyrkiessä hyödyntämään aukkoa ennen kuin korjaus saadaan tehtyä. [17]

Nollapäivähaavoittuvuuksia voidaan käyttää hyödyksi myös DoS-hyökkäyksissä, jotkin haavoittuvuudet voivat olla sellaisia, että ne mahdollistavat laitteeseen hyökkäämisen tavalla joka estää palvelun käytön. Kun palvelun käyttö estetään, kyse on DoS-hyökkäyksestä. Esimerkkejä tällaisista haavoittuvuuksista on esimerkiksi Apache–servereissä havaittu nollapäivähaavoittuvuus, joka mahdollistaa hyökkääjälle helpon keinon toteuttaa DoS-hyökkäys vain yhdeltä koneelta, joka voi jumiuttaa serverin ja vaatii serverin uudelleenkäynnistämistä korjaukseksi. [18]

Eräs esimerkki nollapäivähaavoittuvuudesta, joka mahdollistaa tulvahyökkäyksen kohteeseen on Windows järjestelmissä havaittu haavoittuvuus IPv6-protokollassa. IPv4-osoitteet käytetään asiantuntijoiden arvioiden mukaan loppuun muutamassa vuodessa, jolloin tullaan siirtymään IPv6-osoiteavaruuteen. IPv6 on kuitenkin jo olemassa, vaikka siihen ei ole vielä kokonaisvaltaisesti siirrytty. Uusissa Windows järjestelmissä IPv6 on esiasennettu ja perusasetuksena toiminnassa. ICMP6v reititysilmoitukset IPv6-reitittimeltä havaitaan automaattisesti verkon jokaisen isäntäkoneen toimesta. Tämä tarkoittaa, että aina kun järjestelmä vastaanottaa reititysilmoituksen, se päivittää reititinlistan tämän mukaan. Jos ilmoituspaketissa oleva lippu (flag) on asetettu autokonfiguraatioksi, valitsee isäntäkone tällöin minkä tahansa IPv6-osoitteen reititinavaruudesta. Reititinlistan päivitys ja IPv6-osoitteen konfiguroiminen vievät suuren määrän prosessorin laskentatehoa ja RAM-muistin kapasiteettia. Tällöin DoS-hyökkäys voidaan suorittaa tulvaamalla kohdejärjestelmä IPv6-reititysilmoituksilla. [19]

Nollapäivähaavoittuvuudet ovat oman analyysini pohjalta tällä hetkellä merkitsevin tapa toteuttaa niin DoS hyökkäyksiä, kuin tietomurtoja ja järjestelmän kaappauksia. Nollapäivähaavoittuvuudet ovat myös käypää kauppatavaraa markkinoilla. Sellaisen löytäminen esimerkiksi Windows-käyttöjärjestelmästä voi tuoda löytäjälleen suuret rahat jos se myydään taholle joka haluaa kyseistä haavoittuvuutta hyödyntää. Näitä haavoittuvuuksia voivat haluta sekä valtiot, rikollisjärjestöt, kuin myös yksittäiset ihmiset jotka haluavat joko terrorisoida tai hyötyä muilla tavoin haavoittuvuuksista. Nollapäivähaavoittuvuus ei varsinaisesti ole yksittäinen metodi jolla hyökkäys toteutetaan, vaan nollapäivähaavoittuvuus on aukko järjestelmässä joka mahdollistaa esimerkiksi perinteisen tulvahyökkäyksen käyttäen hyödyksi suojaamatonta, tai vir-

heellistä ohjelmakoodia jolla järjestelmä voidaan saada esimerkiksi loputtomaan looppiin ajamaan tiettyä komentoa. Loopin aikaansaaminen voi syödä kohdejärjestelmän muistin osittain, tai kokonaan. Tietomurroista ja palvelunestohyökkäyksistä puhuttaessa nollapäivähaavoittuvuuksien konseptin ja merkityksen ymmärtäminen nykypäivänä tietotekniikan kehittyessä, sekä ohjelmien kasvaessa ja monimutkaistuessa oleellisen tärkeää. Haavoittuvuuksilta pitää pystyä sekä suojautumaan, että niitä pitää olla mahdollista hyödyntää kovassa tilanteessa kybersodan taistelukentillä.

4 MITEN JA MIKSI PALVELUNESTOHYÖKKÄYKSIÄ KÄYTETÄÄN

Erinäisten DoS- ja DDoS-hyökkäysmallien ja hyökkäystapojen tuntemisen lisäksi, oleellista on ymmärtää miten ja miksi palvelunestohyökkäyksiä käytetään ja mitä hyötyjä niillä pyritään ja voidaan saavuttaa. Syitä ja motiiveja suorittaa palvelunestohyökkäys on useita. Yksinkertaisimmillaan kyse voi olla kiusanteosta, tai eräänlaisen voimannäytön sekä viestin lähettämisestä kohteelle. Toisaalta palvelunestohyökkäyksistä voidaan hyötyä myös rahallisesti, sotilaallisesti tai poliittisesti. Usein vain ihmisen mielikuvitus on rajana siinä, mihin kaikkeen palvelunestoa voidaan hyödyntää. On myös mahdollistaa yhdistää palvelunestohyökkäys osaksi suurempaa hyökkäystä, jossa pyritään estämään jonkin tietyn palvelun toiminta, mahdollistaen muiden metodien hyödyntäminen samaan tai toiseen kohteeseen. Seuraavissa esimerkeissä esittelen erilaisia motiiveja ja käyttötarkoituksia palvelunestohyökkäyksille. Esimerkit ovat joko toteutuneiden hyökkäysten analysointia tai teoriassa mahdollisten skenaarioiden pohtimista.

Eräs hyvinkin ajankohtainen esimerkki löytyy Bitcoin–virtuaalirahan markkinoiden manipuloimisesta DDoS-hyökkäyksien avulla. Bitcoin on virtuaaliraha joka perustuu P2P jakamiselle ja jossa ”rahan” eli bitcoinin arvo määräytyy sen käyttäjien määrän ja heidän koneidensa prosessointitehon mukaan. Uutta rahaa luodaan ”louhimalla”, eli lahjoittamalla prosessointitehoa bitcoin verkolle. Bitcoinin arvo on jatkuvassa liikkeessä ja bitcoineja generoidaan laskevalla vauhdilla, jossa louhintaverkoston kasvaminen hidastaa louhimisesta saatuja tuottoja. Bitcoinin arvo perustuu louhintaverkon toimintaan ja matemaattiseen algoritmiin, mikä tekee siitä myös otollisen kohteen verkon väärinkäytöksille, kuten palvelunestohyökkäyksille. [20]

Bitcoiniin on kohdistunut erinäisiä hyökkäyksiä ja väärinkäytösyrityksiä. Eräs näistä väärinkäytösyrityksistä on 2013 keväänä tapahtuneet suuret DDoS-hyökkäykset, joiden avulla hyökkääjät saivat suoraa rahallista hyötyä hyödyntämällä DDoS-hyökkäystä manipuloiden bitcoin–markkinoita edukseen. Kyseisissä hyökkäyksissä hyökkääjät odottivat bitcoinin arvon nousevan huippuunsa, jonka jälkeen he myivät hankkimansa bitcoinit korkeaan hintaan. Tämän jälkeen hyökkääjät aloittivat palvelunestohyökkäyksen, joka sai markkinat epävakaaksi ja ihmiset paniikinomaisesti hankkiutumaan eroon bitcoineistaan. Aikaansaatu paniikki sai bitcoinin arvon laskemaan. Kun bitcoinin arvo oli laskenut tarpeeksi, hyökkääjät keskeyttivät palveluneston ja ostivat bitcoineja niin paljon kuin pystyivät alennettuun hintaan ja jäivät odottamaan taas arvon palautumista. Toistamalla kyseisen iskun useampaan kertaan hyökkääjät saavat huomattavaa rahallista hyötyä palvelunestohyökkäystä hyödyntäen. [21]

Bitcoin–hyökkäykset ovat hyvä esimerkki siitä, mihin globaali virtualisoituminen on menossa. Virtuaalirahana bitcoin on laajentunut nopeasti ja luonut uudenlaista taloutta maailmaan. Tulevaisuudessa vastaavat ilmiöt tulevat mitä luultavimmin vain lisääntymään, mikä taas luo uusia mahdollisuuksia verkkorikollisille, ja miksei tulevaisuudessa myös valtioille. Palvelunestohyökkäyksiä voidaan soveltaa monipuolisesti vastaavankaltaisissa tilanteissa. Valtiot voivat esimerkiksi hyödyntää DDoS-hyökkäyksiä talouden epästabiloimiseen harmaan vaiheen aikana, tai vaikka poliittiseen painostukseen katkaisemalla jokin laajaksi ja ihmisten elämään oleelliseksi osaksi kasvanut palvelu kokonaan määräajaksi. Tällöin hyökkääjä voi manipuloinnin lisäksi kiristää kohdetta tärkeän palvelun palauttamiseksi takaisin toimintaan. Tämä on mielestäni kysymys joka tulisi tulevaisuudessa ottaa huomioon myös sotilaallisella tasolla. Teknisesti hyökkäykset ovat hyvin samankaltaisia, mutta samaa tekniikkaa hyödyntäen voidaan saavuttaa useita erilaisia vaikutuksia.

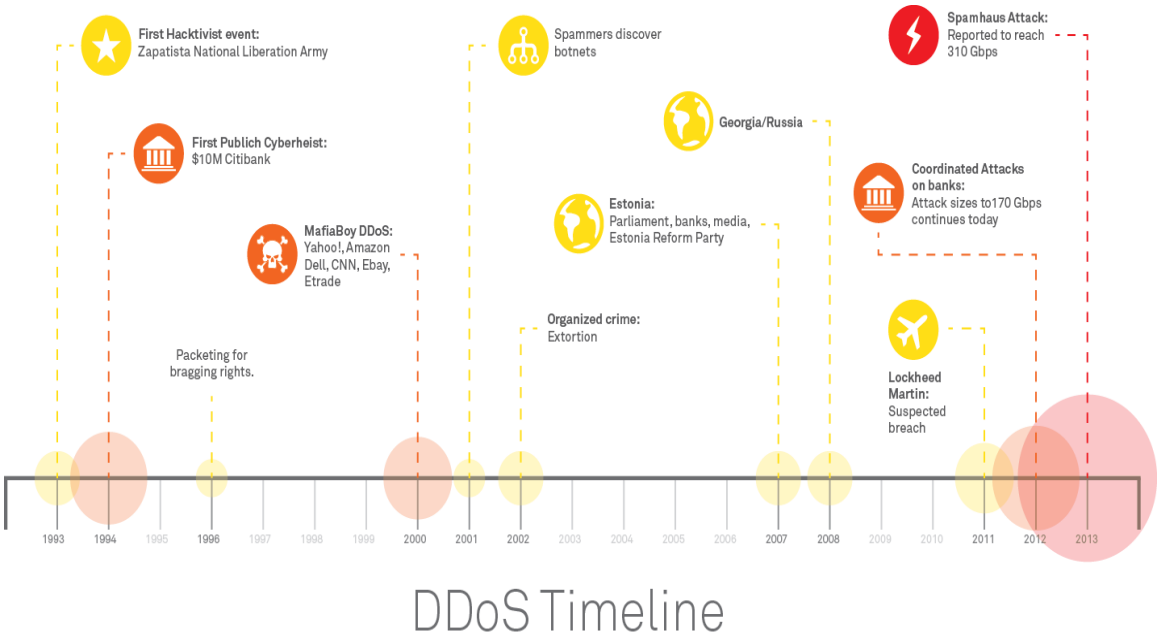
Bitcoin–palvelimiin tehty hyökkäys on hyvä esimerkki siviilipuolen sovellutuksista joita DDoS-hyökkäysmallit voivat tarjota hyökkääjille. DDoS-hyökkäykset soveltuvat kuitenkin myös suuremman mittakaavan hyökkäyksiin, jossa tavoitteena ei ole raha vaan jokin muu motivaattori. Esimerkkinä voidaan käyttää Etelä-Korean valtion sivustoja vastaan toteutetut palvelunestohyökkäykset vuosina 2009-2013, jossa eri tapauksissa hyökättiin valtion hallinnollisia sivuja vastaan saastuneiden palvelimien avulla. Etelä-Korean hyökkäyksissä käytettiin aikapommimenetelmää, jossa haittaohjelmin saastutettu, pääosin palvelimista koostuva botverkko on ajastettu toteuttamaan hyökkäys ennalta määritettynä ajankohtana. Hyökkäykset johtivat pahimmillaan useiden Etelä-Korean valtion sivujen kaatumiseen. Sivut pysyivät alhaalla jonkin aikaa ennen kuin hyökkäys saatiin torjuttua. Threatpost.com artikkelin mukaan hyökkääviä tahoja oli näissä eri tapauksissa useita. [22]

Etelä-Koreaan tehdyt hyökkäykset ovat näyttöä siitä, kuinka DDoS-hyökkäyksiä voidaan hyödyntää poliittiseen painostukseen, tai kuinka DDoS-hyökkäyksillä voidaan antaa tietynlaisia voimannäyttöjä. Sotatilanteessa voi olla mahdollista hyödyntää laajoja DDoS-hyökkäyksiä kaatamaan esimerkiksi valtion tiedotuskanavia tai estämään toisen valtion propagandasivustojen toimintaa, kuten myöhemmin käsittelemässäni Georgian sodan tapauksessa. Threatpost.com artikkelissa mainitaan, että hyökkääjät eivät todennäköisesti olleet samoja eri hyökkäyksissä, mutta hyökkäykset olivat silti osin hyvin samantyyppisiä. Tämä näyttää mielestäni hyvin toteen sen tosiasian, että DDoS-hyökkäykset ovat tekniseltä rakenteeltaan usein hyvin samankaltaisia ja saman mallin mukaisesti toteutettuja. Menetelmät hyökkäyksen valmisteluun ja botverkon rakentamiseen voivat vaihdella. Tämä näyttää toteen myös sen, että DDoS-

hyökkäyksen alkuperää ja tekijää voi olla hankala todentaa – jos hyökkääjä ei sitä itse ilmoita - sillä hyökkäykset ovat hyvin samankaltaisia hyökkääjästä riippumatta. Voidaan vain käydä spekulaatiota siitä, kuka tai mikä taho on lopullisen hyökkäyksen takana ja voiko mukana olla myös valtiollista toimintaa.

5 TUNNETTUJA DOS- JA DDOS-HYÖKKÄYKSIÄ

Tähän lukuun olen valinnut kolme hyvin tunnettua DDoS-hyökkäystä jotka kuvastavat DDoS-hyökkäysten teknistä suorituskykyä eri kohteita vastaan. Valitsemiani hyökkäyksiä yhdistää se, että niistä on uutisoitu laajalti ja ne omaavat jotain erityispiirteitä kuten erityisen laajan, sotilaallisen, erityisen tärkeän tai hyvin suojatun kohteen kaatumisen tai toiminnan estymisen. Tapausten tarkoitus on tuoda esiin DDoS-hyökkäyksen vaikutukset kohteessa, sekä niiden teknisen toteuttamisen vaatimukset tunnettujen esimerkkien avulla. Käsittelyyn olen valinnut verrattain uusia ja lähivuosina tapahtuneita hyökkäyksiä, jolloin käytetyt tekniikat ja menetelmät vastaavat nykyaikaisia verkkoja ja iskujen kohteena olevien koneiden ja palvelinten tekniikkaa. Tapausten lähteinä olen käyttänyt hyökkäyksistä tehtyjä uutisointeja, verkkoyritysten blogikirjoituksia ja asiantuntijoiden julkisia lausuntoja.



Kuva 1: Tunnettuja DDoS-hyökkäyksiä aikajanalle sijoitettuna [23]

5.1 Kyberiskut Viroon sekä Georgiaan: Tapaus Viro

Viime vuosikymmenen lopun näkyvimmät kyberiskut lienevät oletetut Venäjän hyökkäykset sekä Viroon pronssisoturikiistan yhteydessä, että laajat Georgian sodan yhteydessä toteutetut iskut vastustajan hallinnollisille ja kaupallisille internetsivuille. Viron tapauksessa voidaan käydä spekulaatioita siitä, että oliko kyseessä yksittäisten aktivistien toteuttamat iskut vai valtion toteuttama koordinoitu hyökkäys. Georgian sodan kohdalla ei varmuutta valtion osallisuudesta voida aukottomasti todistaa, vaan kyse on julkisten lausuntojen mukaan ollut kansallismielisestä toiminnasta. [24]

Viron tapauksessa iskut saivat oletetusti alkunsa pronssisoturikiistaksi Suomalaisessa mediassa nimetystä tapauksesta, jossa Virolaiset poistivat Tallinnasta vanhan neuvostoaikaisen pronssipatsaan vuonna 2007. [25]. Pian tapauksen jälkeen Virossa raportoitiin mittavista iskuista jotka kohdistuivat Viron taloudellisiin ja hallinnollisiin internetsivuihin, kuten median, pankkien ja hallituksen sivuihin. Tämä aiheutti suuria taloudellisia tappioita rahaliikenteen häiriintyessä tai estyessä kokonaan. [26]. Iskujen havaittiin tulevan ulkomailta, mikä johti usean nettisivun päätökseen sulkea ulkomaanliikenne kokonaan palvelimiltaan. Ulkomaanliikenteen sulkeminen johti taloudellisiin menetyksiin, sekä ulkomaisten asiakkaiden menettämiseen monilla tahoilla. [26]. Virossa arveltiin jo hyökkäysten alkuvaiheessa Venäjän olevan hyökkäysten takana ja scmagazine.com artikkelin mukaan duumassa on myönnetty osallisuus iskuihin, joskaan Venäjän hallitus ei ole kuitenkaan suoraan ottanut vastuuta iskuista. [27, 28]

Tekniseltä toteutukseltaan kyseessä on ollut erittäin tyypillinen DDoS-hyökkäys jossa on käytetty hyväksi laajaa, tuhansista koneista koostuvaa botnet-verkkoa. Virolaisiin sivuihin kohdistunut hyökkäys on malliesimerkki botnet-verkkoa hyödyntävästä tulvahyökkäyksestä, jossa botnet-verkon tuhannet eri koneet ovat samanaikaisesti lähettäneet verkkosivuilla valtavan määrän sivukyselyitä tukkien palvelimet. [26, 28]

Viroon kohdistunut isku ei ole teknisesti lainkaan poikkeuksellinen ja toteutustavaltaan se vastaa hyvin tyypillistä DDoS-hyökkäystä, jossa käytetään raakaa voimaa ja laajaa botnet-verkkoa liikennetulvan luomiseen. Tällaisissa tapauksissa tekniseltä kannalta mielenkiintoisempaa onkin botnet-verkon luomiseen käytetyt metodit ja se kuinka suuria botnet-verkkoja luodaan ja hallinnoidaan tällaisia hyökkäyksiä varten. Kuten botnet-verkkoja käsittelevässä luvussa olen selittänyt, voidaan tällaisia botnet-verkkoja hankkia myös valtiollisella tasolla helposti ulkopuolisilta tahoilta, jolloin hyökkäystä voi olla vaikea kohdentaa esimerkiksi Viron tapauksessa Venäjän valtion toteuttamaksi. Toteuttamalla hyökkäys käyttäen hyväksi jo olemassa olevaa ulkopuolisen tahon luomaa botnet-verkkoa - esimerkiksi vuokraamalla verk-

ko - voidaan hyökkäyksen jäljet peittää tehokkaasti, oli hyökkääjänä sitten valtio tai jokin muu taho joka ei halua paljastua.

5.2 Kyberiskut Viroon sekä Georgiaan: Tapaus Georgia

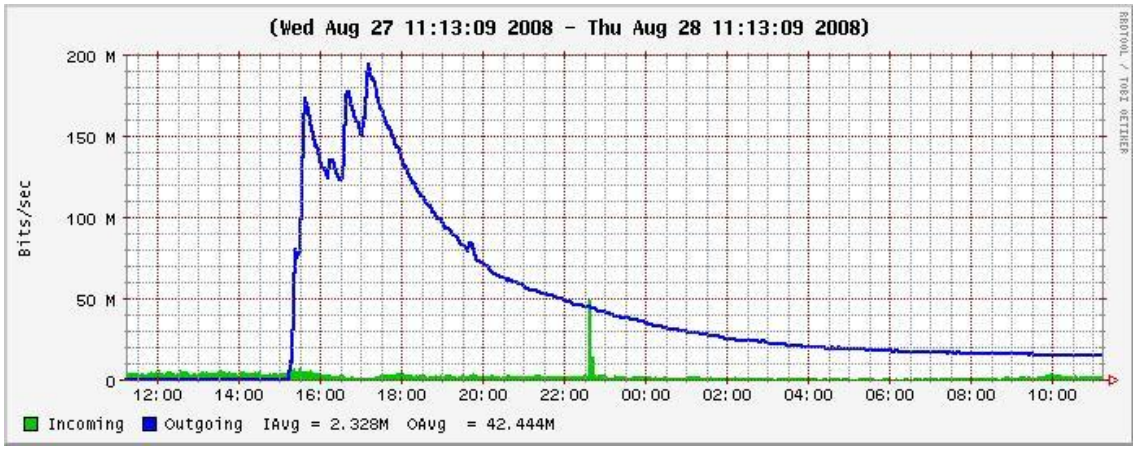
2008 elokuussa oletetusti Venäjä iski Georgiaan pitkällisen epävakauden jälkeen ja aloitti lyhyet, mutta tehokkaat sotatoimet neljällä rintamalla; maalla, merellä, ilmassa ja verkossa. Georgian sota oli ensimmäinen kerta kun valtiollisella tasolla toteutetaan laajoja verkkoiskuja koordinoidusti muiden aselajien kanssa. Iskujen jälkeen onkin puhuttu verkkohyökkäyksestä ns. ”neljäntenä ulottuvuutena” tavanomaisen sodankäynnin rinnalla.[29, s. 1 ja 2] Venäjä käytti Georgiaan kohdistuneissa hyökkäyksissä laajalti hyväkseen DDoS-hyökkäyksiä kaataen tai hidastaen useita Georgian hallinnon tiedonantokanavia, sekä valtiollisia sivuja vaikeuttaen näin Georgian kommunikointia ulkomaailmaan iskun aikana. Edellämainituin toimin Venäjä edesauttoi myös omia propagandatoimiaan.[29, s. 3 ja 4] Georgian tapauksessa voidaan olettaa Venäjän valtion olleen vähintäänkin osallisena iskujen koordinoimisessa, joskin iskuja ovat tiettävästi toteuttaneet myös monet siviilitahot, kuten kansallismieliset aktivistit ja hakkerit, joista käytetään myös termiä ”hacktivistit”. Iskut ovat jakautuneet monen tahon suorittamiksi kansallismielisiksi erillisiskuiksi, mutta suurinta vahinkoa ovat aiheuttaneet juurikin DDoS-hyökkäykset jotka on koordinoitu tarkasti ajoittumaan sotilaallisten iskujen yhteyteen. [30]

Tekniikka jota iskuissa on käytetty on hyvin samankaltainen Viroon kohdistuneiden iskujen kanssa ja useissa Georgiaan kohdistuneista iskuista on voitu käyttää hyväksi vuokrattuja botnet-verkkoja joista maininta myös Viron tapauksessa. Tällaiset verkot ovat lähestulkoon kenen tahansa saatavissa korvausta vastaan. Kyberturvallisuusanalyytikko Danko Danchev käsittelee botnet-verkkojen vuokrausta harjoittavaa palvelua loads.cc, joka on vain yksi esimerkki monista botnet-verkkoja vuokraavista palveluista. Esimerkiksi loads.cc palvelussa veloitetaan käyttäjää latausten määrän mukaan, jolloin käytettävissä olevien varojen mukaan voidaan muodostaa tarvittavan suuruinen liikenne haluttuun kohteeseen. [31]

Sekä Georgian, että Viron tapauksissa on käytetty hyväksi monimutkaista, mutta käyttöperiaatteeltaan yksinkertaista menetelmää toteuttaa laajoja DDoS-hyökkäyksiä korkean prioriteetin kohteisiin. Molemmissa tapauksissa on esittämäni mukaan valjastettu hyökkäyksen tueksi kansallismielisiä aktivisteja ja käytetty hyväksi ulkopuolisten palveluntarjoajien luomia botnet-verkkoja, tämä tekee DDoS-hyökkäyksen määrittelemisestä sotatoimeksi erityisen hankalaa. Georgian tapaus näyttää, että on erittäin tehokasta käyttää hyväksi tämänkaltaista toimin-

taa osana laajempaa sotilaallista iskua. Georgian tapauksessa on myös huomattavaa kuinka iskut eivät kohdistuneet elintärkeisiin kohteisiin, kuten voimalajärjestelmiin tai öljylaitoksiin. Hyökkääjä kuitenkin osoitti kykynsä iskeä myös näihin kriittisiin järjestelmiin niin halutessaan. [29, s. 4]

Georgian ja Viron tapauksissa keskeisintä on, kuinka yksinkertaisia työkaluja hyödyntäen voidaan luoda verrattain mittavaa vahinkoa niin sotilaallisessa, taloudellisessa kuin poliittisessa mittakaavassa. Tarkoituksellisesti olen jättänyt yksityiskohtaisen tarkastelun yksittäisten ryhmien toteuttamista iskuista ja motiiveista pois ja keskittynyt suuremman kuvan luomiseen. Etenkin Georgian sodan tapauksessa DDoS-hyökkäykset ovat näyttäneet voimansa ja vaikutuskykynsä myös sotilaallisessa toiminnassa.



Kuva 2: Georgian hallituksen sivun http://mfa.gov.ge liikenteen muutokset vuorokauden sisällä DDoS-hyökkäyksen aikaan (piikki näyttää hyökkäyksen kulminoitumisen). [32]

5.3 Tapaus: Spamhaus

Spamhaus on voittoa tavoittelematon organisaatio jonka tavoitteena on taistella internetin spammia - eli roskapostia - vastaan erinäisin keinoin. Spamhaus tarjoaa anti-spam palveluita, jäljittää tunnettuja roskapostin lähettäjiä ja pyrkii tukemaan päättäjiä roskapostiin liittyvän lainsäädännön säätämisessä. [33]

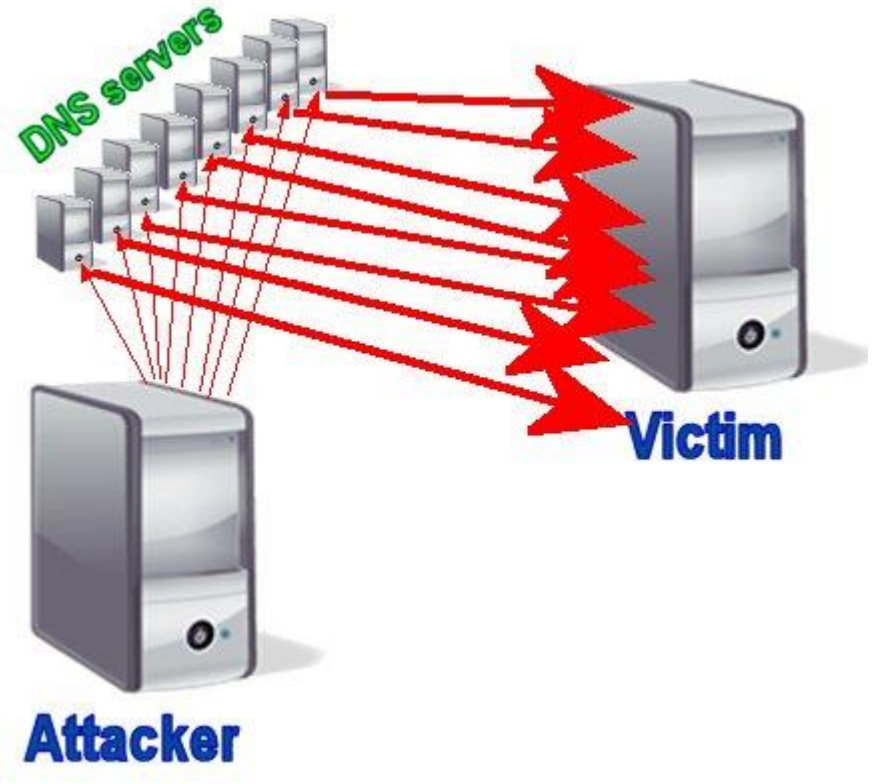
Viimeisin suuri ja laajalti mediahuomiota saanut DDoS-hyökkäys tapahtui alkuvuodesta 2013 Spamhaus organisaation palvelimia vastaan. Spamhaus organisaatioon kohdistuneen hyökkäyksen seurauksena Spamhaus otti yhteyttä Cloudfare nimiseen yritykseen hyökkäyksen torjumiseksi. Cloudfare on uutisoinut tapauksesta laajasti ja avoimesti internetblogissaan, jonka lisäksi tapauksesta on julkaistu artikkeleita useissa eri verkkomedioissa. [34, 35] Cloudfarelle

kävi nopeasti selväksi, että kyseessä oli mittakaavaltaan erittäin suuri hyökkäys joka oli kykenevä kaatamaan koko Spamhausin verkkosivuston. ”These very large attacks, which are known as Layer 3 attacks, are difficult to stop with any on-premise solution. Put simply: if you have a router with a 10Gbps port, and someone sends you 11Gbps of traffic, it doesn't matter what intelligent software you have to stop the attack because your network link is completely saturated”[34].

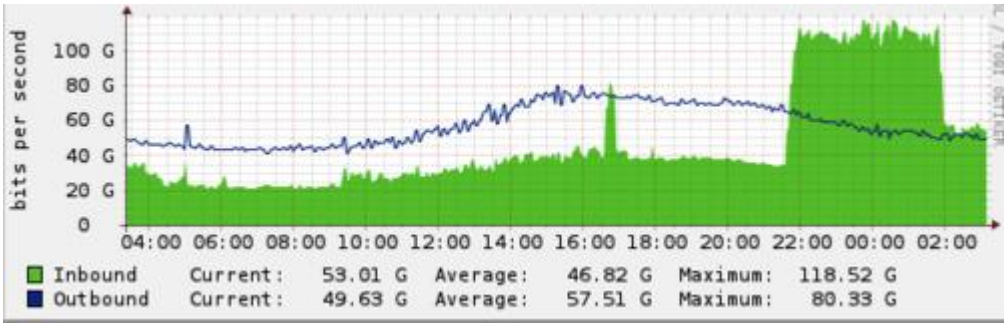
Hyökkäys tehtiin käyttämällä hyväksi DNS-resolvereita, eli palvelimia jotka vastaavat verkkotunnusten nimikyselyihin. Nämä koneet muuntavat verkkotunnukset IP-osoitteiksi. Hyökkäys toteutetaan pyytämällä DNS-resolvereilta suuria DNS-zone tekstitiedostoja jotka sisältävät verkkotunnusten nimitiedot ja IP-osoitteet. Hyökkääjä kuitenkin väärentää pyynnön lähettäjän IP-osoitteeksi hyökkäyksen kohteen IP-osoitteen, jolloin DNS-resolverit lähettävät DNS-zone tiedostot virheellisesti hyökkäyksen kohteena olevaan koneeseen. DNS-zone tiedostot voivat olla kooltaan huomattavasti suurempia, kuin pyynnöt joita hyökkääjä DNS-resolvereille lähettää, jolloin hyökkääjä voi moninkertaistaa hyökkäyksen kohteeseen kohdistuvan liikenteen verraten hyökkääjällä itsellään käytössä olevaan kaistanleveyteen. [34]

Suora kappalelainaus Cloudfaren internetblogista esittää hyvin kuinka DNS-resolvereiden avulla toteutettu hyökkäys toteutetaan ja kuinka verkkoliikenne voidaan verrattain pienellä botverkolla moninkertaistaa kohdekoneessa:

” In the Spamhaus case, the attacker was sending requests for the DNS zone file for ripe.net to open DNS resolvers. The attacker spoofed the CloudFlare IPs we'd issued for Spamhaus as the source in their DNS requests. The open resolvers responded with DNS zone file, generating collectively approximately 75Gbps of attack traffic. The requests were likely approximately 36 bytes long (e.g. dig ANY ripe.net @X.X.X.X +edns=0 +bufsize=4096, where X.X.X.X is replaced with the IP address of an open DNS resolver) and the response was approximately 3,000 bytes, translating to a 100x amplification factor. We recorded over 30,000 unique DNS resolvers involved in the attack. This translates to each open DNS resolver sending an average of 2.5Mbps, which is small enough to fly under the radar of most DNS resolvers. Because the attacker used a DNS amplification, the attacker only needed to control a botnet or cluster of servers to generate 750Mbps -- which is possible with a small sized botnet or a handful of AWS instances. It is worth repeating: open DNS resolvers are the scourge of the Internet and these attacks will become more common and large until service providers take serious efforts to close them” [34].



Kuva 3: DNS servereiden hyödyntämisestä DDoS-hyökkäyksessä [36].



Kuva 4: Spamhaus verkkosivuston liikenteestä hyökkäyksen aikana, suurin piikki alkoi noin klo 22:00 [37]

Spamhaus hyökkäyksen takana olevia henkilöitä ei ole varmasti pystytty tunnistamaan, mutta poliisi on ottanut kiinni ja kuulustellut iskujen takana olevana henkilönä pidettyä Sven Kamphausia, joka on Alankomaissa sijaitsevan Cyberpunker palvelun ylläpitäjä. [38] Tämän lisäksi iskuihin osallisena on ollut pidätettynä brittiläinen 16-vuotias poika. [39]

Teknisesti ei ole olennaista kuka on ollut iskujen takana, tai mikä iskun perimmäisenä motiivina on hyökkääjillä ollut. Todennäköisesti kyseessä on laajempi verkosto hyökkäykseen enemmän tai vähemmän osallisia henkilöitä. Tapaus kuitenkin osoittaa vahvasti kuinka valtavia DDoS-iskuja voidaan toteuttaa verrattain pienillä resursseilla jopa yksittäisten henkilöiden tai yhteisen tavoitteen omaavien verkkorikollisten muodostaman pienen verkoston voimin. Kuten Cloudfiren internetblogissa mainitaan, perustui Spamhaus hyökkäys DNS-servereissä oleviin haavoittuvuuksiin, joiden korjaamiseksi vaaditaan toimenpiteitä, mutta joita ei haavoittuvuuden tunnettavuudesta huolimatta ole huomioitu kaikkien internetpalveluiden tarjoajien kohdalla. Tämä altistaa verkkosivustot yhä uusille hyökkäyksille kunnes haavoittuvuudet korjataan. Esimerkkinä Spamhaus tapaus on oivallinen ja se selittää kattavasti kuinka yksinkertaisella tavalla voidaan valjastaa suuri määrä raakaa voimaa halutun palvelun kaatamiseksi. Tällaisia tapauksia tapahtuu maailmalla jatkuvasti useita, eikä kaikista välttämättä uutisoida kuten Spamhaus tapauksen kohdalla uutisoitiin.

6 JOHTOPÄÄTÖKSET

Tutkielmassa olen esittänyt kuinka erilaiset palvelunestohyökkäykset rakentuvat ja millaisia vaikutuksia niitä käyttämällä voidaan saada aikaan. Teknisen tarkastelun ja eri esimerkkien avulla voidaan näyttää toteen palvelunestohyökkäyksien olevan nykyaikainen ja suhteellisen tehokas vaikutuskeino kyberiskuissa tai kybersodankäynnissä. Palvelunestohyökkäyksiä käytetään yhä ja on käytetty jo toista vuosikymmentä laajasti maailmalla niin pienemmässä kuin suuremmassakin mittakaavassa. Palvelunestohyökkäyksillä on useita ominaisia piirteitä jotka ovat säilyneet läpi historian hyvin samankaltaisina, ainoastaan hyödynnettävät haavoittuvuudet ja eri tekniikat toteuttaa näitä ajattomia periaatteita ovat muuttuneet. Palvelunestohyökkäys on yksinkertainen, tehokas ja halpa tapa toteuttaa iskuja joilla voidaan saada aikaan tuloksia moneen eri käyttötarkoitukseen. Palvelunestohyökkäykset ovat pääsääntöisesti profiloituneet verkkorikollisten keinoksi edesauttaa omia motiivejaan ja tuoda ääntään kuuluville, mutta kuten Georgian sodan ja Viron tapaukset osoittavat, voidaan palvelunestohyökkäyksiä valjastaa suoraan tai epäsuorasti myös valtiollisen tason painostukseen, tai jopa suoranaisena osana sotilaallista operaatiota.

Hyökkääjän kannalta palvelunestohyökkäykset tarjoavat halvan ja pienillä resursseilla toteutettavan keinon ajaa alas kohteena olevan tahon verkkopalveluita. Palvelunestohyökkäykset ovat erityisen tehokkaita yllätyksellisesti toteutettuna ja etenkin Spamhaus tapauksen kaltaisissa hyökkäyksissä varautuminen etukäteen on erittäin vaikeaa, tai jopa mahdotonta. Palve-

lunestohyökkäyksille on ominaista, että niiden toteuttaminen vaatii tiettyä yllätyksellisyyttä ja jonkin hankalasti torjuttavan haavoittuvuuden hyödyntämistä. Yleensä hyökkääjät pyrkivätkin hyödyntämään järjestelmien ja verkkojen sisällä tapahtuvaa aitoa liikennettä hyökkäyksissään. Hyödyntämällä haavoittuvuuksia ja manipuloimalla aitoa liikennettä käyttäytymään hyökkääjän haluamalla tavalla voidaan toteuttaa hyökkäyksiä, joita järjestelmät eivät itsenäisesti tunnista haitalliseksi, jolloin manipuloinnin onnistuessa voidaan palvelunesto saada suurella todennäköisyydellä onnistumaan.

Palvelunestohyökkäyksillä on kuitenkin myös omat heikkoutensa. Palvelunestohyökkäykset ovat lopulta suhteellisen yksinkertaisia torjua, olettaen että kohteella on olemassa osaamista ja resursseja iskun torjumiseen. Yksinkertaisimmillaan palvelunestohyökkäykset voidaan torjua manuaalisesti katkaisemalla suuria datamääriä lähettävät yhteydet. Joissakin tapauksissa tämäkin voi osoittautua hankalaksi kuten Spamhaus tapauksessa, jossa lähettäviä IP-osoitteita on järjestelmän kannalta käytännössä virtuaalisesti rajaton määrä. Palvelunestohyökkäyksillä ei usein saada aikaan pitkäaikaista vaikutusta kohteeseen vaan parhaimmillaankin kohteet ovat alhaalla päiviä tai tunteja, jonka jälkeen yhteydet yleensä saadaan reititettyä uudestaan ja haitalliset yhteydet katkaistua. Häiriötä kohteisiin voidaan aiheuttaa pidempiä aikoja, mutta tällöin myös aikaansaatu vaikutus on huomattavasti vähäisempi kuin tilanteessa jossa kohde saatetaan täysin toimintakyvyttömäksi.

Mielestäni palvelunestohyökkäykset soveltuvat parhaiten tilanteisiin joissa ei vaadita kohteen pitkäaikaista lamauttamista. Palvelunestohyökkäystä voidaan sotilaallisissa sovellutuksissa käyttää ajamaan hetkellisesti alas vastustajan verkkopalveluita. Georgian sodan esimerkin mukaisesti palvelunestohyökkäyksiä voitaisiin hyödyntää nopean toiminnan operaatioissa joissa vastustajan tärkeiden verkkopalveluiden kaatuminen yhdeksikin päiväksi riittäisi edesauttamaan operaatiota. Tällaisia iskuja voisivat olla iskut energiantuotantoon, tiedonkulkuun tai taloudellisiin instansseihin kuten Viron tapauksessa. Palvelunestohyökkäykset soveltuvat mielestäni erityisesti harmaan vaiheen edeltäviin vaiheisiin, sekä harmaan vaiheen aikana tapahtuvaan painostukseen juuri edellä mainittujen tapaisten palvelujen käyttöä rajoittamalla.

Palvelunestohyökkäykset ovat nykyaikana yhä enemmän arkipäiväistyvä ilmiö ja tekniikan kehittymisen myötä, myös palvelunestohyökkäyksillä saadaan aikaan yhä suurempia vaikutuksia kohteisiin. Voidaankin todeta, että mitä enemmän jollakin tietyllä taholla on toimintoja verkossa, sitä alttiimpi se on palvelunestohyökkäyksille. Vaikka en tutkielmassa käsittelekään

palvelunestohyökkäyksiltä suojautumista, on hyökkäyksenkin kannalta tärkeää tunnistaa tulevaisuuden muutokset verkkojen kasvussa ja rakenteissa. Yhä enemmän palveluita siirtyy verkkomaailmaan mikä muodostaa yhä suurempia haavoittuvuuksia. Esimerkkinä palveluiden verkoittumisesta on esimerkiksi bitcoinin yleistyminen ja rahaliikenteen siirtyminen yhä vahvemmin verkkoihin. Georgian sodan viitoittamalla tiellä uskon myös valtioiden olevan tulevaisuudessa yhä vahvemmin mukana kehittämässä ja luomassa botverkkoja, tai kaivamassa nollapäivähaavoittuvuuksia globaalissa verkossa. Palvelunestohyökkäykset ovat yksinkertaisesti niin kustannustehokas keino vaikuttaa kohteeseen tai vastustajaan, että yksikään valtio ei voi sivuuttaa niiden huomioimista.

LÄHTEET

[1] Esecurityplanet. How to prevent DoS attacks [verkkojulkaisu] [viitattu 13.5.2013] Saatavissa: www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html

[2] Cert. Denial of Service [verkkojulkaisu] [viitattu 13.5.2013] Saatavissa: www.cert.org/tech_tips/denial_of_service.html

[3] Gary C. Kessler ja Diane E. Levine (Edited by Seymoyr Bosworth, M.E. Kabay, Eric Whine). Computer security handbook 5th edition: Denial of Service Attacks. John Wiley & Sons Inc, 2009.

[4] Xue Li, Zhanhuai Li, Osmar R. Zaïane. Advanced Data Mining and Applications: Second International Conference, ADMA 2006, Xi'an, China, August 14-16, 2006. Springer, 2006.

[5] Mysecurecyberspace. Zombie-machine [verkkojulkaisu] [viitattu 24.7.2013] Saatavissa: http://www.mysecurecyberspace.com/encyclopedia/index/zombie-machine.html

[6] Consumerfraudreporting. Zombies [verkkojulkaisu] [viitattu 24.7.2013] Saatavissa: http://www.consumerfraudreporting.org/zombies.php

[7] Microsoft. What Is Botnet [verkkojulkaisu] [viitattu 25.7.2013] Saatavissa: http://www.microsoft.com/security/resources/botnet-whatis.aspx

[8] Mysecurecyberspace. Distributed Denial of Service [verkkojulkaisu] [viitattu 25.7.2013] Saatavissa: http://www.mysecurecyberspace.com/encyclopedia/index/distributed-denial-of-service-ddos.html#msc.encyclopedia.ddos

[9] Ddosprotection. Smurf attack explained [verkkojulkaisu] [viitattu 7.9.2013] Saatavissa: http://www.ddosprotection.net/smurf-attack-explained/,

[10] Cert. Smurf IP denial-of-service attacks [verkkojulkaisu] [viitattu 7.9.2013] Saatavissa:

http://www.cert.org/advisories/CA-1998-01.html

[11] Oppimateriaalit.internetix.fi. IP- ja ICMP-protokollat [verkkojulkaisu] [viitattu 7.9.2013] Saatavissa: http://oppimateriaalit.internetix.fi/fi/avoimet/6tekniikkatalous/verkko/ip_ja_icmp_protokollat

[12] Techopedia. Smurf-attack [verkkojulkaisu] [viitattu 7.9.2013] Saatavissa: http://www.techopedia.com/definition/17294/smurf-attack

[13] ISS. Ping of Death [verkkojulkaisu] [viitattu 7.9.2013] Saatavissa: http://www.iss.net/security_center/advice/Intrusions/2000012/default.htm

[14] Surasoft. Denial of Service Attacks [verkkojulkaisu] [viitattu 8.9.2013] Saatavissa: http://www.surasoft.com/articles/ddosa.php

[15] Mitko Bogdanovski, Tomislav Shuminoski, Aleksandar Risteski. International Journal of Computer Security 2013 Analysis of the SYN Flood DoS Attack, 8, 1-11. MECS 2013. Saatavissa: http://eprints.ugd.edu.mk/6729/1/IJCNIS-V5-N8-1.pdf

[16] WatchGuard. Anatomy of DNS DDoS Amplification attack [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://www.watchguard.com/infocenter/editorial/41649.asp

[17] PCtools. Zero Day Vulnerability [verkkojulkaisu] [viitattu 10.9.2013] Saatavissa: http://www.pctools.com/security-news/zero-day-vulnerability/

[18] Softpedia. Zero Day Remote DoS Exploit Threatens Apache Servers [verkkojulkaisu] [viitattu 10.9.2013] Saatavissa: http://news.softpedia.com/news/Zero-Day-Remote-DoS-Exploit-Threatens-Apache-Servers-218642.shtml

[19] Kumar Sourav. DoS/DdoS Attack Prevention and zero day DoS vulnerability in IPv6 [verkkojulkaisu] [viitattu 10.9.2013] Saatavissa: http://www.hcon.in/uploads/1/8/1/9/1819392/dos_ddos.pdf

[20] Bitcoin. What is Bitcoin [verkkojulkaisu] [viitattu 18.1.2013] Saatavissa: http://bitcoin.org/en/faq#what-is-bitcoin

[21] RT. Are DdoS attacks being used to fix Bitcoin rates? [verkkojulkaisu] [viitattu 18.1.2014] Saatavissa: http://rt.com/usa/users-gox-ddos-bitcoin-707/

[22] Threatpost. Behind the South Korean government DdoS attacks [verkkojulkaisu] [Viitattu 21.1.2013] Saatavissa: http://threatpost.com/behind-the-south-korean-government-ddos-attacks/102507

[23] Ddosattacks. DdoS Timeline [verkkojulkaisu] [viitattu 21.1.2014] Saatavissa: http://www.ddosattacks.biz/media/ddos-timeline.png

[24] Telegraph. Georgia-Russia conducting cyber war [verkkojulkaisu][viitattu 21.1.2014] Saatavissa: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

[25] Helsingin Sanomat. Patsaan paikka kiristää Venäjän ja Viron välejä [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://www.hs.fi/ulkomaat/artikkeli/Patsaan+paikka+kirist%C3%A4%C3%A4+Ven%C3%A4j%C3%A4nja+Viron+v%C3%A4lej%C3%A4/1135226762377

[26] Secure 64. Russian DdoS Attacks on Estonia [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://www.secure64.com/news-russian-ddos-attacks-estonia

[27] Scmagazine. Russia confirms involvement with estonia DDoS attacks [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://www.scmagazine.com/russia-confirms-involvement-with-estonia-ddos-attacks/article/128737/

[28] The Guardian. Russia accused of unleashing cyberwar to disable Estonia [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://www.theguardian.com/world/2007/may/17/topstories3.russia

[29] David Hollis. Small Wars Journal: Cyberwar Case Study: Georgia 2008

[30] Zdnet. Coordinated Russia vs Georgia cyber attack in progress [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: (http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

[31] D. Danchev blogi. loadsccs: DDoS for hire service [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://ddanchev.blogspot.fi/2008/03/loadsccs-ddos-for-hire-service.html

[32] D. Danchev blogi. Graph of mfa.gov.ge network traffic [verkkojulkaisu] [viitattu 22.1.2014] Saatavissa: http://4.bp.blogspot.com/_wICHhTiQmrA/SPZIdRd6kMI/AAAAAAAAACTA/fkKSEaSfIXc/s1600-h/ddos_attack_graph_georgia_russia.JPG%20

[33] Spamhaus. Organization [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://www.spamhaus.org/organization/

[34] Cloudfare (blogi). The DDoS that knocked spamhaus offline [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

[35] Cloudfare (blogi). The DDoS that almost broke the internet [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

[36] PC Magazine. DNS Reflection graph [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://www4.pcmag.com/media/images/380558-dns-reflection.jpg?thumb=y

[37] Cloudfare (blogi). Spamhaus DDoS attack graph [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://blog.cloudflare.com/static/images/spamhaus_ddos_attack.png.scaled500.png

[38] Informationweek. Spamhaus DDoS suspect arrested [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa: http://www.informationweek.com/attacks/spamhaus-ddos-suspect-arrested/d/d-id/1109732 23.1.2014

[39] Techworld. British Teen accused of massive spamhaus DDoS attack arrested months ago [verkkojulkaisu] [viitattu 23.1.2014] Saatavissa:

KUVALUETTELO