MAANPUOLUSTUSKORKEAKOULU

LÄHI-IDÄSSÄ KÄYTETYT KYBERASEET

Kandidaatintutkielma

Kadetti
Henri Ojala

98. kadettikurssi
maasotalinja

maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
98. kadettikurssi	maasotalinja
Tekijä: Kadetti Henri Ojala	
Tutkielman nimi: **Lähi-idässä käytetyt kyberaseet**	
Oppiaine, johon työ liittyy: Sotatekniikka	Säilytyspaikka: Kurssikirjasto (MPKK:n kirjasto)
Aika maaliskuu 2014	Tekstisivuja 24 Liitesivuja 3

TIIVISTELMÄ

On vaikeaa kuvitella, että tulevaisuuden sodat käytäisiin ilman kyber-elementtiä. Tämä uusi sodankäynnin ulottuvuus luo uusia haasteita sekä mahdollisuuksia valtioille. Tästä on osoituksena mm. valtioneuvoston tekemä kyberturvallisuusstrategia tammikuussa 2013 sekä Viestintävirastoon perustettu Kyberturvallisuuskeskus tammikuussa 2014. Mielestäni kyberpuolustuksen kannalta on todella tärkeää kartoittaa eri kyberaseiden toimintamahdollisuudet kyberavaruudessa sekä mahdolliset vaikutukset kohdejärjestelmissä.

Pääkysymys tutkimuksessani on: *Mitkä ovat kyberaseiden käyttötarkoitukset ja miten niitä on käytetty Lähi-idässä?*

Olen toteuttanut tutkimukseni laadullisen tutkimuksen periaattein, tutkimusmenetelmänä on kirjallisuuskatsaus. Olen tutustunut aihealueeni muihin tutkimuksiin ja koonnut niistä saadut tiedot yhteen ja tehnyt päätelmät aineiston luotettavuudesta. Valitsin kyseisen tutkimusmenetelmän sen takia, että oma tietopohjani aiheesta tutkimuksen alkuvaiheessa oli melko suppea. Usean eri lähteen kautta olen pystynyt muodostamaan paremmin oman näkemykseni kyseisestä aiheesta.

Kyber on vielä melko epäselvä kokonaisuus sen monimutkaisuudesta johtuen. Esimerkiksi kyberavaruus on kenttänä vielä todella epäselvä valtioille sekä niiden turvallisuusviranomaisille. Lähi-itä on selkeästi toiminut testikenttänä uuden tyyppisille haittaohjelmistoille sekä kyberaseille.

AVAINSANAT

Kyberase, kyberavaruus, kyberuhka, Stuxnet, Flame, Duqu, Mahdi, Shamoon, Gauss, Wiper.

LÄHI-IDÄSSÄ KÄYTETYT KYBERASEET

SISÄLLYS

LÄHTEET

LIITTEET

LÄHI-IDÄN KYBERASEET JA HAITTAOHJELMISTOT

1 JOHDANTO

On vaikeaa kuvitella, että tulevaisuuden sodat käytäisiin ilman kyber-elementtiä. Tämä uusi sodankäynnin ulottuvuus luo uusia haasteita sekä mahdollisuuksia valtioille. Tästä näkyvänä esimerkkinä on Suomen valtioneuvoston julkaisema kyberturvallisuusstrategia tammikuussa 2013. Yhtenä suurimpana haasteena kyberin osalta on tällä hetkellä kuinka määritellään erilaiset kyberiä koskevat käsitteet. Kyberillä tarkoitetaan yleisesti toimintoja sähköisessä viestinnässä sekä tietokonejärjestelmissä.

1.1 Tutkimuskysymykset ja -aineisto

Tämän tutkimuksen tarkoituksena on kartoittaa mitä ovat nykyaikaiset kyberaseet ja kuinka ja missä niitä on käytetty. Tässä tutkimuksessa tarkastellaan mm. Stuxnetin, Flamen ja Duqun käyttöä, ominaisuuksia sekä niiden käytön mahdollisia tavoitteita. Tutkimuksen ensimmäisessä asialuvussa selvitetään mitä ovat kyberaseet ja mikä on niiden toimintaympäristö. Toisessa asialuvussa tarkastellaan Lähi-idässä käytettyjä kyberaseita. Tutkimuksessa tarkasteltavia käsitteitä ovat mm. kyberaseet ja kyberavaruus.

Pääkysymys tutkimuksessani on: *Mitkä ovat kyberaseiden käyttötarkoitukset ja miten niitä on käytetty Lähi-idässä?*

Tutkimuksen alakysymykset:

1. Millainen haittaohjelman täytyy olla, jotta se on kyberase?
2. Mikä on kyberaseiden toimintaympäristö?
3. Millainen on kyberaseiden rakenne?
4. Miten kyberaseet ovat levinneet Lähi-idässä?

Tutkimusaineistona käytän pääosin ulkomaisia artikkeleita. Tämä johtuu siitä, että suomalaisia tutkimuksia aiheesta on tehty todella vähän. Olen kuitenkin pystynyt hyödyntämään tutki-

muksessani myös joitain kotimaisia lähteitä. Kaikki tiedot joita tutkimukseen olen kerännyt, olen pyrkinyt mahdollisuuksien mukaan varmistamaan useasta eri lähteestä.

Ensimmäisessä asialuvussa olen käyttänyt lähteenä sotilasaikakauslehden artikkeleita kyberaseista sekä kyberavaruudesta. Kyberaseen rakenteen olen koonnut Timo Kiravuon ajatuksista, kenen tekstejä olen lainannut niin sotilasaikakauslehden artikkelista sekä Johtamisen ja sotilaspedagogiikan laitoksen julkaisusta The Fog of Cyber Defence. Kyberaseen määrittelyyn olen käyttänyt CGI:n näyttöesitystä kyberaseista.

Toisen asialuvun sekä koko työn pääasiallisena lähteenä olen käyttänyt ulkomaisten tietoturvayhtiöiden Internet-artikkeleita. Suurimpana yksittäisenä lähteenä työssäni on ollut Kaspersky Lab, joka on tehnyt selvästi kattavimmat raportit eri kyberaseiden rakenteesta ja käytöstä.

1.2 Tutkimusmenetelmä ja tutkimuksen tarpeellisuus

Olen toteuttanut tutkimukseni laadullisen tutkimuksen periaattein, tutkimusmenetelmänä on kirjallisuuskatsaus. Olen tutustunut aihealueeni muihin tutkimuksiin ja koonnut niistä saadut tiedot yhteen ja tehnyt päätelmät aineiston luotettavuudesta. Valitsin kyseisen tutkimusmenetelmän sen takia, että oma tietopohjani aiheesta tutkimuksen alkuvaiheessa oli melko suppea. Usean eri lähteen kautta olen pystynyt muodostamaan paremmin oman näkemykseni kyseisestä aiheesta.

Tutkimus kyseisestä aiheesta on todella ajankohtainen, koska huoli kyberturvallisuudesta kasvaa kokoajan. Tästä on osoituksena mm. valtioneuvoston tekemä kyberturvallisuusstrategia tammikuussa 2013 sekä Viestintävirastoon perustettu Kyberturvallisuuskeskus tammikuussa 2014. Mielestäni on todella tärkeää kartoittaa eri kyberaseiden toimintamahdollisuudet kyberavaruudessa sekä mahdolliset vaikutukset kohdejärjestelmissä.

1.3 Tutkimuksen rakenne, aiemmat tutkimukset ja rajaus

Tutkimukseen kuuluu neljä päälukua, joista luvut kaksi ja kolme ovat tutkimuksen varsinaisia tutkimuslukuja. Luku neljä on tutkimuksen yhteenveto-osio. Tutkimuksen tärkeimpänä lukuna on luku kolme, jossa vastataan tutkimuksen pääkysymykseen.

Tutkimuksen ensimmäisessä luvussa käsitellään tutkimuksen toteuttamiseen liittyviä asioita. Luvussa esitellään tutkimuksen pääkysymys sekä alakysymykset. Lisäksi luvussa kerrotaan tutkimuksen tutkimusmenetelmä, aiemmat tutkimukset ja tutkimuksen rajaus.

Luvussa kaksi käydään läpi mitä ovat kyberuhat ja niiden aiheuttajat. Luvassa käsitellään kyberaseiden rakennetta sekä toimintaympäristöä. Tässä luvussa vastataan tutkimuksen alakysymyksiin 1 - 3.

Kolmannessa luvussa vastataan tutkimuksen pääkysymykseen sekä neljänteen alakysymykseen. Näihin kysymyksiin vastataan erittelemällä Lähi-idässä käytettyjä kyberaseita sekä listaamalla niiden eri ominaisuuksia. Luvussa käsitellään mm. Stuxnetin ominaisuuksia, sen käyttöä sekä sen tekemää vaikutusta kohteeseen.

Tutkimuksen viimeinen luku on yhteenveto, jossa verrataan eri kyberaseita ja haittaohjelmistoja toisiinsa. Luvussa käsitellään niiden leviämistä Lähi-idässä sekä epäiltyjä tekijöitä.

Rajaan tutkielmaani siten, että käsittelen työssä Lähi-idässä käytettyjä kyberaseita aikaväliltä 2005 – 2013. Jätän työssäni myös käsittelemättä kyberaseen alakäsitteet, kuten virukset ja madot. Nämä käsitteet olen kuitenkin avannut käsitteissä, jotka on koottu tutkimuksen loppuun.

2 KYBERASEET JA NIIDEN TOIMINTAYMPÄRISTÖ

Tulevaisuudessa valtiot ovat enenevissä määrin riippuvaisia tietokoneista, sähköstä, elektroniikasta ja tietoverkoista. Tämän takia on todella vaikeaa kuvitella, että tulevaisuuden sodissa ei olisi mukana jonkin asteista kybersodankäyntiä. [1, 9]

Kyberavaruus on uusi ja jatkuvasti kehittyvä ympäristö. Syyskuussa 2010 Yhdysvaltojen entinen puolustusministerin sijainen, William J. Lynn määritteli kyberavaruuden viidenneksi sodankäynnin ulottuvuudeksi (maa, meri, ilma, avaruus). Tämän jälkeen on pyritty pääsemään yksimielisyyteen kansainvälisestä lainsäädännöstä joka koskee kyberavaruutta. Lainsäädännön määrittelyssä on suuria haasteita, koska esimerkiksi kyberavaruudessa toimijoiden jäljittäminen on epävarmaa sekä on vaikeaa määritellä, milloin kyberhyökkäystä voidaan pitää aseellisena hyökkäyksenä. [2, 5] Tästä syystä kyberavaruutta koskeva lainsäädäntö on todella puutteellista ja suurin osa siihen liittyvistä termeistä on vielä määrittelemättä. [1, 7]

Kyberavaruus toimii toimintaympäristönä kyberaseille ja kyberiskuille. Kyberavaruus on läsnä kaikkialla ja sen toimintaa kontrolloivat individuaalit sekä yritykset. Se ei siis ole valtiokeskeinen ympäristö. Kuten maalla, merellä, ilmassa ja avaruudessa, myös kyberavaruudessa kyetään operoimaan asevoimilla. [1, 7] Tässä työssä kyberavaruus on toimintaympäristö, joka tarkoittaa tietojärjestelmien sekä niiden välisen digitaalisen tiedonsiirron muodostamaa kokonaisuutta.

2.1 Kyberuhat ja niiden tekijät

Mahdolliset kyberuhat voivat kohdistua rajojen sisältä tai ulkoa, joko välillisesti tai suoraan järjestelmiä ja/tai kansalaisia vastaan. Kyberuhat on mahdollista luokitella monella eri tavalla. Tässä työssä on käytetty Martti Lehdon sotilasaikakauslehteen tekemää viisi tasoista uhkamallia. [3, 10]

Kyberuhat:

1. Kyberaktivismi (kybervandalismi, hakkerointi, haktivismi)
2. Kyberrikollisuus
3. Kybervakoilu
4. Kyberterrorismi
5. Kybersodankäynti [3, 10 – 11]

Kyberuhat eivät muodostu tyhjästä vaan uhat tarvitsevat tekijän, jolla on tavoite, kohde sekä keinot uhan toteuttamiseen. Näitä kyberuhkien muodostajia ovat hakkerit, rikolliset, terroristit sekä valtiot. [4, 26]

Hakkereiden motiivina on toimia jonkin asian puolesta, joko yksin tai ryhmässä. Tai he voivat toimia myös pelkän harrastuksen takia. Kohteina hakkereilla ovat yleensä henkilöt, media, yhteisöt, yritykset ja jopa valtiot. Hakkerit kykenevät levittämään disinformaatiota, tekemään palvelunestohyökkäyksiä sekä tekemään tietomurtoja. [4, 26]

Rikolliset hakevat toiminnallaan taloudellista hyötyä. Kohteina heillä ovat yksittäiset henkilöt, yhteisöt tai yritykset. Yleensä rikolliset tekevät identiteettivarkauksia, verkkopetoksia tai tietokonekaappauksia. [4, 26]

Terroristit ovat kybertoimijoista luokka joka on toistaiseksi ollut passiivinen, mutta odotettavissa on, että jossain vaiheessa terroristitkin aktivoituvat kyberkentällä. Terroristit pyrkivät teoillaan ideologisiin päämääriin. Terroristien kohteina ovat media, yritykset sekä valtiot. Oletettavasti terroristit tekevät hakkereiden tapaan palvelunestohyökkäyksiä, tietomurtoja sekä levittävät disinformaatiota. [4, 26]

Valtiot hakevat kyberoperaatioillaan strategista, operatiivista ja/tai jopa taktista hyötyä [2]. Valtion kyberoperaatioiden kohteena voivat olla niin henkilöt, media, yhteisöt, yritykset kuin toisetkin valtiot. Keinoina kyberoperaatioiden suorittamiseen valtioilla on disinformaation levittäminen, palvelunestohyökkäykset, tietomurrot, vakoilu ja valvonta sekä fyysinen tuhoaminen. [4, 26]

2.2 Kyberaseet

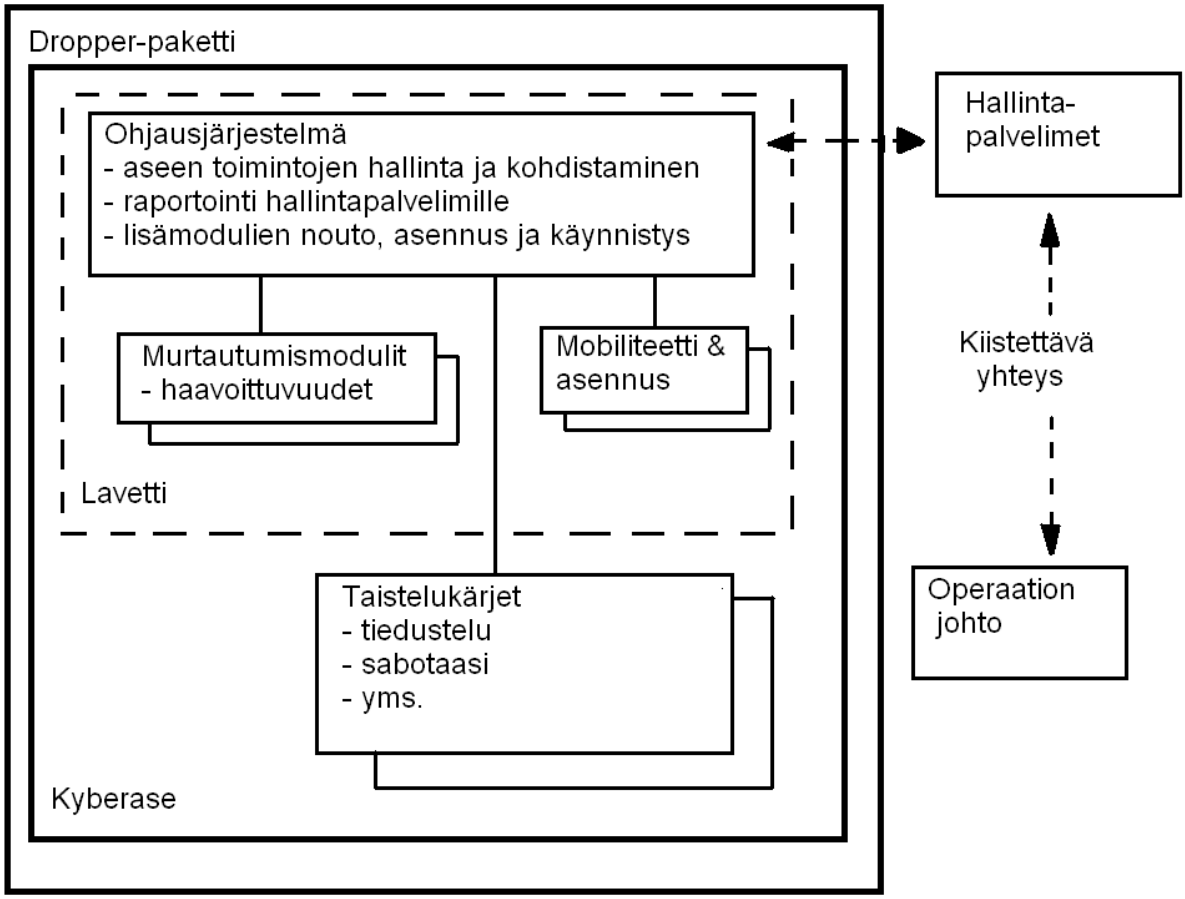
Kyberase keskustelussa on tärkeää huomioida, että kansainväliset säädökset eivät vielä tarkkaan määrittele kyberasetta. Tämä tuottaa lakien suunnitteluun suuren haasteen. Yksi määrittelyn kannalta tärkeä aukko on se, että milloin haittaohjelmasta tulee ase. [2, 6]

Tässä tutkimuksessa kyberase on sähkömagneettisessa ympäristössä vaikuttava haitta, jonka taustalla on valtio tai voimaltaan sitä vastaava ryhmittymä. Kyberaseet kohdennetaan yleensä tarkoin valittuun kohteeseen, kun taas normaalit haittaohjelmat kohdistetaan satunnaisesti kaikkia mahdollisia kohteita vastaan. Kyberaseen tavallisia kohteita ovat sotilaalliset kohteet, valtion organisaatiot, kriittinen infrastruktuuri sekä yritykset. Tavoitteena sillä on tietyn opera-

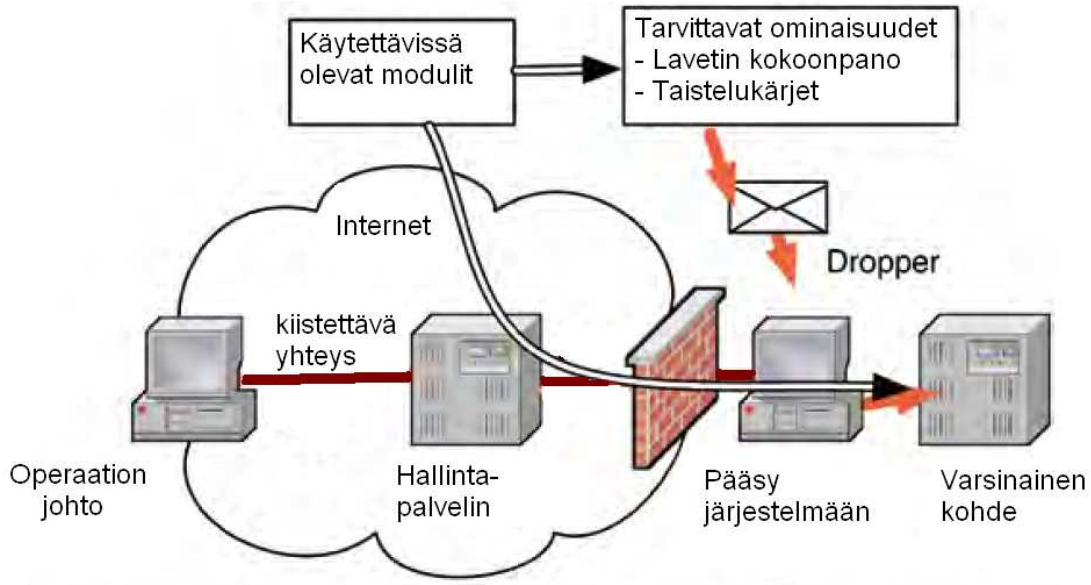
tiivisen vaikutuksen aikaansaaminen, kuten esimerkiksi kohteen valvonta, tiedustelu ja/tai tuhoaminen. Kyberaseet käyttävät hyväkseen mm. nollapäivä haavoittuvuuksia sekä kohdeympäristön fyysisen- tai henkilöturvallisuuden heikkouksia päästäkseen sisään kohdejärjestelmään. [5, 16 - 17]

2.2.1 Kyberaseiden yleinen rakenne

Useimmat tunnetut kyberaseet ovat ns. modulaarisia hyökkäysohjelmistoja. Modulaarisuus tarkoittaa sitä, että kyberase on rakennettu useasta eri osasta. Kyberaseesta on usein havaittavissa itse toiminnan suorittava taistelukärki sekä kyberasetta kuljettava lavettiosa. Kyberaseen lavettiosaan kuuluu ohjausjärjestelmä, murtautumismoduulit sekä mobiliteetti- ja asennusmoduuli. [6, 47]



Kuvio 1. Esimerkki modulaarisen kyberaseen arkkitehtuurista [6, 47]



Kuvio 2. Yleiskuva kyberoperaatioista [1, 220]

Kuvio 2 näyttää kuinka kyberase on koottu eri moduuleista ja sitä levitetään sähköpostin liitetiedostona, joka ohittaa kohdejärjestelmän palomuurin. Kun ase on aktivoitunut, ottaa se yhteyden hallintapalvelimiin ohjeita ja päivityksiä varten. Esimerkiksi kaikki tuhoa tekevät tai tiedustelua suorittavat taistelukärjet voidaan asentaa vasta jälkeenpäin kyberaseeseen. Tämä tehdään sen takia, että mikäli ase paljastuu ennen aikojaan, se ei paljasta moduuleita jotka voivat aiheuttaa vastahyökkäyksen. [1, 220]

Jotta ase kyetään toimittamaan kohdejärjestelmään, voidaan käyttää erillistä dropper-pakettia lavetin kuljettamiseen. Dropper-paketti pakkaa kyberaseen mahdollisesti sähköpostiin, Internet-sivulle, ohjelmistopäivitykseen tai esimerkiksi USB-tikkuun. Kun dropper-paketti aktivoituu, asentaa se kyberaseen koodin kohdejärjestelmään ja aktivoi aseen. Tämä aktivoitava koodi saattaa näkyä esimerkiksi ohjelmistopäivityksenä ja se on koodattu siten, että kohdejärjestelmä tunnistaa sen oikeana päivityksenä. [1, 224]

Kyberaseet kykenevät liittämään itsensä melko huomaamattomasti kohteen käyttöjärjestelmään, käyttämällä hyväksi järjestelmän sertifiointia [6, 47]. Samassa tilanteessa kyberase voi mahdollisesti asentaa jonkinasteisen rootkit toiminnon käyttöjärjestelmään, jolloin kyberaseen käynnistämiä prosesseja on lähes mahdotonta havaita [6, 47]. Dropper-pakettiin voidaan sisällyttää suoraan kaikki halutut kyberaseen osat tai mikäli mahdollista osa kyberaseen moduuleista voidaan ladata myöhemmin Internetin kautta [1, 224].

2.2.2 Kyberaseiden lavettiosa sekä taistelukärjet

Kuten edellä mainittiin, lavettiosaan kuuluu ohjausjärjestelmä-, murtautumis- sekä mobiliteetti- ja asennusmoduuli. Ohjausjärjestelmä hallitsee aseen toimintoja hallintapalvelimien käskyjen mukaan, mikäli yhteys hallintapalvelimiin on muodostettu. Jos yhteyttä hallintapalvelimiin ei ole suunniteltu käytettävän, on ohjausjärjestelmään ohjelmoitu valmiiksi suoritettavat operaatiot. Ohjausjärjestelmän päätehtävinä voidaan pitää taistelukärkien ohjausta ja käynnistämistä. [1, 219]

Murtautumismoduulien tehtävänä on mahdollistaa aseen pääsy kyberaseen todellisiin kohteisiin kohdejärjestelmässä. Tällainen kohde voi olla esimerkiksi ydinvoimalan sentrifugien ohjausjärjestelmä, joka on sijoitettu korkeamman turvallisuusluokan tiloihin. Murtautumismoduulit hyödyntävät esimerkiksi kohdejärjestelmän mahdollisia nollapäivä-haavoittuvuuksia. [1, 219]

Mobiliteetti- ja asennusmoduulia käytetään aseen koodin asentamiseen ja kopiointiin. Mobiliteetti- ja asennusmoduuli käyttää hyväkseen murtautumismoduulien tekemiä murtoja kohdejärjestelmään. [1, 219]

Yksi tunnetuimmista kyberaseiden laveteista on Tilded, jota käytettiin Stuxnetissä sekä Duqussa. Todennäköisesti kyseistä lavettia on käytetty myös muihin haittaohjelmiin, joita ei ole vielä tunnistettu. Tilded on kehitetty vuoden 2007 lopulla. Sen rakenne koki huomattavan muutoksen vuonna 2010, jotta se ei olisi paljastunut uusille virustorjuntaohjelmistoille. [7]

Lavettiosan lisäksi kyberaseeseen kuuluu taistelukärjet. Niiden avulla kyberase pyrkii suorittamaan sille määrätyn tehtävän. Kaikki muut kyberaseen osat tukevat taistelukärkien toimintaa. Kyberaseelle määrätyn tehtävän laatu määrittelee sen mitä moduuleja ja taistelukärkiä aseessa tullaan käyttämään. [1, 219 – 220]

Taistelukärkien tehtävät vaihtelevat. Kaksi tunnetuinta päätehtävää ovat tiedustelu ja tuhoaminen. Tiedustelu voi pitää sisällään mm. tietyn tyyppisten tiedostomuotojen etsinnän, salasanojen tiedustelun näppäimistöltä ja salakuuntelun tietokoneen mikrofonin kautta. Tuhoa tekevä taistelukärki etsii esimerkiksi automaatiojärjestelmiä joiden tietokantoihin taistelukärki kykenee vaikuttamaan korruptoimalla dataa ja tehden muuta vahinkoa. [6, 47] Kolmas mahdollinen tehtävä taistelukärjelle voi olla disinformaation jakaminen. Todennäköisesti tällainen taistelukärki kohdistetaan tarkalleen määrättyä kohdetta kohti, kuten tiettyä tietopankkia vas-

taan. Tällaisilla taistelukärjillä on valtavasti potentiaalia, mikäli ne kykenevät pääsemään sellaiseen tietoon käsiksi, joita vastustajan päättäjät käyttävät. Tähän mennessä kuitenkaan tämän kaltaista kyberasetta tai haittaohjelmaa ei ole ilmaantunut. Todennäköisesti tämän tapaiset ohjelmistot tulisivat käyttöön, mikäli kyberoperaatioita käytettäisiin esimerkiksi strategisessa iskussa tai laajamittaisessa hyökkäyksessä. [1, 221]

2.2.3 Kyberaseiden ominaispiirteitä

Valmisteltujen moduulien lisäksi kyberaseella on tiettyjä ominaisuuksia, jotta se onnistuisi todennäköisemmin tehtävässään. Tällaisia omaisuuksia ovat muun muassa salassa pysyminen, vastatoimet paljastumisen jälkeen, itsetuho ja allekirjoitukset. [1, 225]

Lähtökohtaisesti alhainen paljastumisriski on kyberaseelle todella tärkeä ominaisuus. Pois lukien tilanne jolloin kyberaseella halutaan hämätä vastustajaa. Jotta kyberaseelle saadaan alhainen paljastumisriski, täytyy sen kaikkien komponenttien olla suunniteltu mahdollisimman hyvin. Paljastuminen on lopulta kiinni kokonaisuudesta, eikä yksittäisestä komponentista.
Paljastuminen kyetään mahdollisesti välttämään mikäli kyberase:

- leviää kohdejärjestelmässä tarpeeksi hitaasti
- on pieni kokoinen
- kykenee piiloutumaan kohdejärjestelmään
- kykenee jäädyttämään toimintansa silloin, kun ihmiskäyttäjät ovat paikalla [1, 225]

Kyberase kykenee tuhoamaan kaikki aiheuttamansa jäljet välttääkseen paljastumisen sekä tietoturvayhtiöiden analyysit. Järkevin toimintatapa on poistaa kaikki ne komponentit, kuten dropper -paketti, heti kun niitä ei enää tarvita. Mikäli vain mahdollista, aseen tulisi välttää kohdejärjestelmän varmuuskopiointipalvelua. [1, 225]

On mahdollista, että kyberase kykenee tulevaisuudessa puolustamaan itseään paljastumisen jälkeen. Jotta kyberase kykenee tähän, on sillä oltava tieto paljastumisestaan. Tärkein yksittäinen indikaattori paljastumisesta on se, kun aseen tiedostoja tutkitaan kohdejärjestelmässä. Mikäli ase arvioi, että se on paljastunut aloittaa se vastatoimet. Päämääränä vastatoimilla on aikavoiton saavuttaminen lisäämällä puolustajan työmäärää. Vastatoimien tavoitteena ei siis ole niinkään paljastumisen välttäminen. [1, 226]

Mahdolliset vastatoimet:

- nopea leviäminen viruksen tavoin
- rakenteensa täydellinen muuttaminen
- piilotetun kopion muodostaminen itsestään tai aivan uudesta aseesta [1, 226]

Kyberoperaatio voidaan haluta pysäyttää monesta erilaisesta syystä. Niillä aseilla joilla on yhteys Internetiin on usein mahdollisuus pysäyttää aseen toiminnot hallintapalvelimien kautta. Toinen mahdollinen keino pysäyttää kyberase voisi olla valmisteltu koodi, joka aktivoituessaan antaa herätteen virustorjuntaohjelmistolle. Tällöin virustorjuntaohjelmisto tunnistaa kyberaseen ja poistaa sen.

Joissain tapauksissa kyberaseen tekijä voi haluta, että hänet kyetään tunnistamaan, jolloin tekijä kykenee muodostamaan pelotevaikutuksen. Kyberaseessa voi tällöin olla salattua dataa, jonka salausavaimen paljastamalla kyberaseen tekijä todistaa osallistumisensa kyberoperaatioon. [1, 226]

3 STUXNET JA SEN JÄLKELÄISET

3.1 Stuxnet

Stuxnetin oli Yhdysvaltain ja Israelin yhteisprojektina tehty monimutkainen haittaohjelmisto [1, 221]. Stuxnetillä oli selkeä poliittinen päämäärä: hidastaa Iranin ydinohjelmaa välttämällä tavanomaisten asevoimien käyttöä [1, 221]. Kohteena Stuxnetillä oli Iranin Natanzin ydinvoimala. Stuxnet verkkomato paljastui kesäkuussa 2010 [8]. Ensimmäiset versiot Stuxnetistä ovat olleet tosin käytössä jo vuodesta 2005 [9; 10, 1]. Monet asiantuntijat pitävät tätä tapahtumaa ensimmäisenä todellisena kyberiskuna. Arvioiden mukaan Stuxnet saastutti yli 100 000 tietokonetta [11; x2], joista yli puolet oli Iranissa. Tosin jotkin arvioivat tartuntojen määräksi jopa 300 000 [12]. Muita maita joissa Stuxnet havaittiin, oli mm. Intia, Kiina, Etelä-Korea, Yhdysvallat, Iso-Britannia, Australia, Saksa ja Suomi. [11] Merkittävä syy Stuxnetin paljastumiseen oli sen leviäminen myös normaaleihin kotitietokoneisiin [9].

Stuxnet operaation suunnittelussa on arvioitu olleen 50 – 100 ohjelmoijaa sekä muuta tietokoneasiantuntijaa. Tämän lisäksi operaatiossa on ollut mukana mm. tiedusteluosia, jotka ovat todennäköisesti työn tilaajia. Näinkin laaja organisaatio mahdollistaa kyberaseiden sekä haittaohjelmistojen todella nopean teon. Stuxnetin budjetin arvioidaan olleen joitain miljoonia Yhdysvaltain dollareita. Ennen kuin Yhdysvaltain hallinto päätti paljastaa osallistumisensa Stuxnetiin, ei kyetty todistamaan kenen tekemä Stuxnet oikeasti oli. [1, 221 – 228]

Stuxnet saastutti tietokoneita vaikka kohdejärjestelmät eivät olleet kytkettynä Internetiin. Stuxnetin leviäminen ydinvoimalaan tapahtui USB-muistitikun avulla. Se pääsi kohdejärjestelmään SCADA:n (valvomo-ohjelmisto) kautta, käyttäen Windows – käyttöjärjestelmässä ollutta haavoittuvuutta hyväkseen. Stuxnetin tehtävänä oli ohjelmoida uudelleen ydinvoimalan sentrifugien ohjausjärjestelmä ja tämän lisäksi vakoilla kohdetietokoneita. [13; 1, 221]

Kesäkuussa 2010 paljastuneeseen Stuxnet –versioon liittyviä tapahtumia:

17.6.2010 Tietoturvayhtiö VirusBlokAda löysi uuden haittaohjelman, joka käytti hyväkseen Windows-käyttöjärjestelmän linkkitiedostojen haavoittuvuutta. Stuxnet nimi tuli ohjelmakoodista löytyneen tiedostokansion mukaan.

15.7.2010 Alle kuukaudessa useimmat virustorjuntaohjelmat tunnistivat Stuxnetin.

16.7.2010 Microsoft julkaisi tiedotteen, jossa ilmoitettiin Stuxnetin käyttämä haavoittuvuus.

20.7.2010 Symantec alkoi tutkia liikennettä, joka tapahtui tartunnan saaneista koneista hallintapalvelimille.

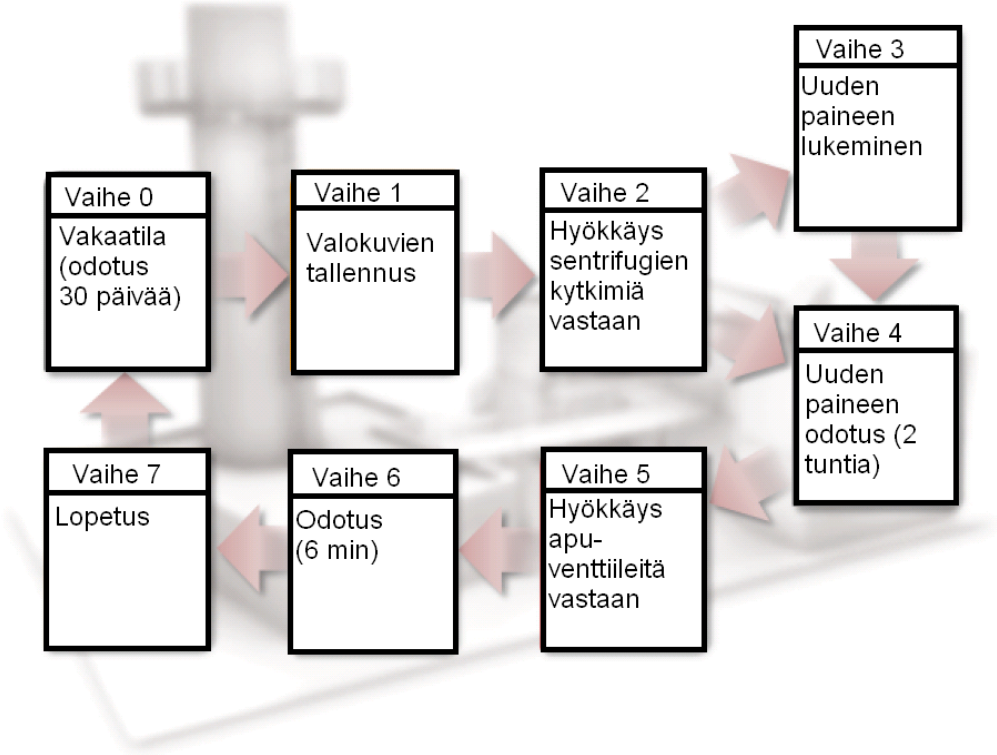
2.8.2010 Virallinen ohjelmistopäivitys julkaistiin, joka korjasi linkkitiedostoihin liittyvän haavoittuvuuden.

6.8.2010 Julkaistiin tieto, että Stuxnet kykenee muuttamaan teollisuusautomaatio-ohjainten toimintaa.

14.9.2010 Tulostinpalveluissa olevaan haavoittuvuuteen julkaistiin virallinen ohjelmistopäivitys. [14]

Tapahtumien kulusta on mielestäni huomioitava se, että uudet päivitykset ja haavoittuvuudet tulivat nopeasti kaikkien tietoon sen jälkeen, kun Stuxnet oli ensimmäisen kerran havaittu. Eli paljastumisen jälkeen Stuxnetillä ei ollut kauaa aikaa vaikuttaa kohteessa. Verrattuna siihen, että todellisuudessa haittaohjelma on voinut toimia kohteessa useita vuosia ennen paljastumista.

Tietoturvayhtiö Symantec on listannut useita eri versioita Stuxnetistä. Symantec on pystynyt selvittämään neljän eri version rakenteet, jotka ovat v0.500; v1.001; v1.100 ja v1.101. Symantecin mukaan v0.500:n hallintapalvelimet ovat aloittaneet toimintansa jo marraskuussa 2005. Tämä versio oli ohjelmoitu niin, että se lopetti kommunikoinnin hallintapalvelimien kanssa tammikuussa 2009 ja saman vuoden heinäkuussa versio lopetti kaiken toiminnan myös kohdejärjestelmissä. Sen tehtävänä oli sulkea sentrifugien kytkimiä Symantecin laatiman 8-vaiheisen toimintaperiaatekaavion mukaan. Stuxnet 0.500 levisi kohdejärjestelmässä Siemensin valmistaman SIMATIC STEP 7–ohjelman kautta, joka on tehtaisiin suunniteltu automaatiojärjestelmä. Se ei käyttänyt hyväkseen mitään Microsoftin omia haavoittuvuuksia, toisin kuin uudemmat tunnetut versiot. [10, 1 – 2]



Kuvio 2. Stuxnet v0.500:n toimintaperiaate [10, 10]

Ei ole täysin selvää onnistuiko v0.500 tehtävässään. Mutta voidaan epäillä, että tämä versio ei onnistunut kaikissa tavoitteissaan, koska uudet versiot (1.x) olivat tehty erilaiselle alustalle. Tästä seurasi se, että uudet versiot olivat aggressiivisempia sekä niiden vaikutukset sentrifugeihin muuttuivat. Uudemmissa versioissa Stuxnet lähetti virheellisiä arvoja taajuusmuuttujille, jotka ohjasivat sentrifugien moottorien kierrosnopeutta. Tämän seurauksena sentrifugit vahingoittuivat. [13; 10, 1 – 2]

Stuxnet v0.500 oli rakennettu samankaltaiselle alustalle kuin Flame, kun taas v1.x oli pääasiallisesti samanlaisia Tilded-alustan kanssa. Usean eri alustan käyttö eri versioiden kesken viittaa vahvasti siihen, että Stuxnetin taustalla oli monia eri kehittäjiä. [10, 3]

Kaikilla tunnetuilla Stuxnetin versioilla on ollut rajalliset käyttömahdollisuudet hallintapalvelimiin. Esimerkiksi v0.500 ei tarjoa tekijöilleen kunnon mahdollisuutta hallita ohjelmistoa. Stuxnet 0.500 kykenee ainoastaan lataamaan uutta koodia ja päivittämään itseään. Tämä johtuu osittain siitä, että Stuxnet on luotu alun perin olemaan mahdollisimman itsenäinen ohjelmisto, koska sen on täytynyt levitä ilman pääsyä Internetiin. [10, 4]

3.2 Flame

Tietoturvayhtiö Kaspersky Lab havaitsi Flamen ensimmäisen kerran toukokuussa 2012. Näyttää kuitenkin siltä, että Flame on ollut toiminnassa jo vuoden 2010 maaliskuusta. Nimensä se on saanut yhdestä sen päämoduuleista. [15] Kaspersky Labin mukaan Flame tarkoittaa samaa kyberasetta kuin SkyWiper tai Flameriksi kutsutut kyberaseet [16]. Flame paljastui, kun tietoturvayhtiöt tutkivat Wiper-nimistä kyberasetta [17].

Tämä kyberase saastutti arviolta n. 5 000 järjestelmää [12]. Kaspersky Lab havaitsi tartuntoja noin 700. Suurimpana kohteena Kaspersky Labin mukaan oli Iran, 189 saastuneella koneella. Muita tartuntoja oli mm. Israelissa (98), Sudanissa (32) sekä Syyriassa (30). [16]

Flame on kybease, jota pidetään jopa paljon tehokkaampana kuin Duqua tai Stuxnetiä. Joidenkin tietoturvasiantuntijoiden mukaan se on jopa monimutkaisin haittaohjelmisto mitä on koskaan tehty. Flamen ohjelmakoodi on noin 20-kertainen Stuxnetiin verrattuna. Eikä sen ohjelmointitavassa ole juurikaan yhtäläisyyksiä Stuxnettiin tai Duquun. Tosin Flamen tekijöillä on mahdollisesti ollut pääsy samoihin haavoittuvuuksiin kuin Stuxnetin tekijöillä. On siis mahdollista, että ne tahot jotka vastasivat Stuxnetistä, halusivat vain rinnakkaisen projektin, jotta ”kaikki munat eivät olisi samassa korissa”. [16]

Flame levisi järjestelmiin USB-muistitikun kautta, johon oli ohjelmoitu kaksi eri tapaa levitä kohdejärjestelmässä. Näiden lisäksi Flame levisi tulostimissa olleen haavoittuvuuden kautta. Flame kykeni myös leviämään mikäli, saastunut kone teki etätöitä toiselle koneelle tai mikäli saastunut kone oli kirjautuneena järjestelmänvalvojana. Flamen tiedetään levinneen verkon kautta tietokoneeseen jossa oli täysin päivitetty Windows 7.

Flame pystyi tekemään useita erilaisia toimintoja saastuneelle tietokoneelle. Sitä voidaan pitää niin takaovena, troijalaisena kuin matona. [18, 1 – 2; 16]

Flame:

- keräsi tietoja saastuneesta tietokoneesta ja lähiverkosta
- etsi ja varasti ennalta määrättyjä tiedostoja
- nauhoitti keskusteluja mikrofonin kautta, joita käytiin tietokoneen lähettyvillä
- otti kuvankaappauksia (screenshot)
- skannasi paikallisia Bluetooth laitteita [18, 1 – 2; 16]

Flame käytti noin 20 erilaista moduulia tehdäkseen edellä mainittuja toimia, mutta kaikkien tarkoitusta ja toimintaperiaatetta ei ole kyetty vielä selvittämään. Moduulit asennettiin hallintapalvelimien kautta ja se asensi vain tietyt moduulit tiettyihin järjestelmiin, eli sillä ei ollut tarkoituskaan asentaa kaikkia moduuleita kaikkiin saastuneisiin koneisiin. Kaikki kerätty data lähetetään hallintapalvelimille suojatun SSL–kanavan kautta tietyin aikavälein. Flamessa on olemassa moduuli, jonka avulla ohjelma kykenee poistamaan itsensä järjestelmästä. Toisin kuin Stuxnetissä, siihen ei ole ohjelmoitu erillistä itsetuho aikaa. [16]

Flamen rakenteessa oli paljon erikoisuuksia verrattuna perinteisiin haittaohjelmiin. Esimerkiksi Flame käytti LUA-ohjelmointikieltä, jota harvoin käytetään haittaohjelmien tekoon. Flamen tiedostokoko oli myös todella suuri. Sen suurus on lähes 20Mt, kun se on täysin toiminnassa. Perinteiset haittaohjelmat on koodattu mahdollisimman pieniksi, jotta niitä olisi mahdollisimman vaikea löytää. Flameen oli sen sijaan tehty niin paljon koodia, että sen tutkiminen oli todella haastavaa. Flamesta teki erikoisen myös sen lukuisat eri tavat kerätä informaatiota kohdejärjestelmistä. Esimerkiksi se otti kuvankaappauksia aina silloin, kun kohdejärjestelmässä käynnistettiin tietyt ”kiinnostavat” ohjelmat. [16]

Jotta tutkijat eivät saisi selville Flamen tekoaikaa, tekijät vaihtoivat tiedostojen luonti päivämääriä. Flamessa oli tiedostoja esimerkiksi vuosiluvuilla 1992, 1994, ja 1995, mutta on selvää, että nämä päivämäärät ovat tekaistuja. Kaspersky Labin tutkijan mukaan Flame luotiin noin helmi-maaliskuussa 2010. On kuitenkin hyvä huomioida, että moduuleita on päivitetty ja tehty lisää tuon jälkeen. On myös mahdollista, että Flamesta on ollut käytössä jokin aiempi versio ennen vuotta 2010. [16]

Flame keräsi kaikkea tietoa mitä se vain kykeni löytämään. Sen tavoitteena ei näyttänyt olevan esimerkiksi jokin tietty ydinvoimala. Flamen kohteena olivat niin yksilöt, koulutuslaitokset kuin hallituksien eri organisaatiot. Ei voida pois sulkea mahdollisuutta, että seuraava lisättävä moduuli olisi ollut jollain tavalla hyökkäyksellinen, jolla olisi kyetty tekemään Stuxnetin tapaista tuhoa. Näyttää kuitenkin siltä, että Flamen tavoitteena on ollut kerätä ainoastaan tietoja tiettyjen Lähi-idän valtioiden salassa pidettävistä asioista. [18, 1 - 2; 16] Tämän takia on todennäköistä, että Flamen suunnittelijoina on ollut jokin valtio. Tätä väitettä tukee myös se fakta, että Flame on todella monimutkainen ohjelmisto verrattuna muihin tunnettuihin kyberaseisiin. [16]

3.3 Duqu

Ensimmäinen Duqun tekemä hyökkäys havaittiin huhtikuussa 2011 unkarilaisen CrySyS Lab:in toimesta. Hyökkäykset jatkuivat aina lokakuun puoleenväliin asti, jolloin Duqusta uutisoitiin virallisesti. Kyberaseen paljastuttua sen hallintapalvelimet suljettiin todella nopeasti. CrySyS Lab nimesi haittaohjelman ”DQ” –tiedostonimen pohjalta. [19 ja 20, 1 - 2]

Duqu on troijalainen, jonka pääasiallisena tehtävänä on toimia takaovena kohdejärjestelmään, josta se varastaa tietoja. Pääsääntöisesti Duqu varastaa salasanoja, ottaa kuvankaappauksia sekä varastaa tiettyjä tiedostotyyppejä. Huomion arvoista on, että Duqu ei kykene kopioimaan itseään toisiin tietokoneisiin, kuten Stuxnet. Tämä haittaohjelma käyttää leviämisessään Word-tiedostoa jonka kautta se pystyy käyttämään hyväksi Windowsin nollapäivähaavoittuvuutta. On kuitenkin todennäköistä, että Duqu kykenee leviämään kohteisiin myös muilla tavoin. [19; 20, 1 - 2] Lähtökohtaisesti Duqu poistaa itsensä 30 päivän jälkeen asennuksesta, mikäli siihen ei ole ohjelmoitu erikseen pidempää operaatioaikaa [1, 225].

Duqun päämoduulissa on paljon samankaltaisuuksia Stuxnetin vastaavan kanssa. Niiden rakenne ja käyttäytyminen ovat todella lähellä toisiaan. Tämän takia jotkin tahot ovat sitä mieltä, että Duqun ja Stuxnetin ovat ohjelmoineet samat henkilöt, mutta tästä ei ole toistaiseksi näyttöä. Yhtenä suurena erona näiden kahden haittaohjelman välillä on Kaspersky Labin tutkijan mukaan se, että Duqu saastuttaa vain pienen määrän tarkasti valittuja järjestelmiä toisin kuin Stuxnet, joka saastuttaa mahdollisimman paljon eri järjestelmiä. Näyttää myös siltä, että jokainen Duqun saastuttama järjestelmä sisältää hieman erilaiset haittaohjelmamoduulit. Nämä tiedostot on räätälöity juurikin jokaista kohdetta varten erikseen. [21, 1 - 2]

Duqun dropper-paketti odottaa niin kauan kunnes kohdejärjestelmän näppäimistö on ollut käyttämättä 10 minuuttia. Tämän jälkeen se aloittaa haittaohjelman asentamisen koneeseen. [1, 224]

Duqu käyttää http ja https yhteyksiä kommunikoidakseen hallintapalvelimien kanssa. Hallintapalvelimien avulla se kykenee lataamaan itseensä lisää toiminnallisuuksia ja päivittämään vanhoja ominaisuuksia. Duqulla on myös mahdollisuus käyttää välityspalvelimia, mutta se ei käytä niitä ensisijaisena vaihtoehtona. Hallintapalvelimia on havaittu Intiassa, Belgiassa sekä Vietnamissa. Näiden palvelimien IP-osoitteet eivät ole enää käytössä. On mahdollista, että kyseiset palvelimet eivät ole hallintapalvelimia, vaan ne vain lähettävät tietoa eteenpäin varsi-

naisiin hallintapalvelimiin. Tällä toiminnalla yritetään vaikeuttaa varsinaisten hallintapalvelimien tunnistamista sekä palauttamista. [20, 2]

Duqun saastuttamia koneita on ympäri maailmaa vain noin 50 ja tästä syystä Duqun tutkiminen on ollut todella hankalaa. Tämän kyberaseen painopisteenä on ollut Iran, joten voidaan olettaa, että sillä on ollut selkeä tavoite kuten Stuxnetillä. [19, 10]

3.4 Gauss

Kaspersky Lab:n tekemien analyysien mukaan Gauss aloitti toimintansa syyskuussa 2011 [22]. Gauss löydettiin kesäkuussa 2012 Flamen tutkimisen seurauksena [22]. Gauss on tiedusteluun tarkoitettu kyberase, jonka tekijöiksi epäillään samoja henkilöitä jotka ovat tuottaneet Flamen. [23, 3 – 4] Kuten Duqu perustui samaan Tilded-lavettiin Stuxnetin kanssa, Gauss perustuu Flame-lavettiin. Gaussilla on niin ikään samanlaisia toiminteita kuten Flamella. Gaussin epäillään olevan jonkin valtion tuottama kyberase. [24]

Gauss keräsi tietoa libanonilaisista pankeista. Päätavoitteena Gaussilla oletetaan olleen tiettyjen henkilöiden tunnistaminen sekä tiedonkeruu kohteistaan. Näiden tietojen avulla se olisi kyennyt jopa varastamaan kohteiden tileiltä rahaa. Tätä on syytä pitää epätodennäköisenä, koska Gaussin epäillään olleen valtiotason kyberase. [24]

Gauss on modulaarinen ohjelmisto, johon operaattorit kykenevät päivittämään uusia ominaisuuksia etäyhteydellä. Nämä uudet ominaisuudet muodostetaan liitännäisinä (plugin) tietokoneeseen. [24] Gaussin nimi tulee yhdestä tämän ohjelmiston monista moduuleista. Kaspersky Lab nimesi haittaohjelmiston Gaussiksi johtuen siitä, että kyseinen moduuli kerää kaikkein kriittisintä tietoa kohdejärjestelmästä [23, 3]. Gaussista on havaittu seuraavia moduuleita:

Gauss – asentaa uudet liitännäiset jotka keräävät Internet-selaimen evästeitä ja salasanoja
Cosmos – kerää tietoja CMOS ja BIOS:sta
Kurt, Godel – saastuttaa USB –asemat dataa varastavalla moduulilla
Tailor – kerää tietoa Internet rajapinnasta
McDomain – kerää tietoa käyttäjän verkkotunnuksista
UsbDir – kerää tietoa kohdetietokoneen eri asemista
Lagrange – asentaa “Palida Narrow” fontin
ShellHW – ohjausjärjestelmä [23, 8]

Päämoduuli Gauss on kooltaan hieman yli 200kt. Kuten edellä mainittu, tämä moduuli kykenee lataamaan uusia moduuleja kohdejärjestelmiin. Mikäli yhteen järjestelmään saataisiin ladattua kaikki moduulit, tulisi yhteiskooksi noin 2Mt. Tämä on vain kolmannes Flamen päämoduulista. Gaussilla saattaa olla löydettyä enemmän moduuleja, jotka hallintapalvelimet aktivoivat vain tietyllä ajanhetkellä. [24]

Gaussin hallintapalvelimet sulkeutuivat pian haittaohjelman löytymisen jälkeen heinäkuussa 2012. Hallintapalvelimien sulkeuduttua Gauss meni valmiustilaan odottamaan palvelimien uudelleen käynnistymistä. [22]

Kaspersky Lab aloitti Gaussin tutkimisen kesäkuun alussa 2012. Tämän seurauksena Kaspersky Lab teki havainnon, että Gauss oli levinnyt pääsääntöisesti kolmeen Lähi-idän maahan. Suurin tartuntojen määrä oli Libanonissa, 1600 saastuneella tietokoneella. Seuraavaksi laajimmat määrät tartuntoja olivat Israelissa (n. 500) ja Palestiinan alueella (n. 250). Saastuneiden koneiden kokonaismääräksi tulee näin ollen noin 2500. Tässä luvussa täytyy kuitenkin huomioida, että kyseessä on vain Kaspersky Lab:n ohjelmistojen käyttäjät. Todellisuudessa saastuneita koneita voi olla kymmeniätuhansia [12]. [23, 5 – 6]

Gauss toimii pääasiallisesti 32-bittisissä Windows – käyttöjärjestelmissä. Windows 7 (35%), Windows XP Professional SP2 (26%) ja XP Professional SP3 (18%) ovat suosituimpia Gaussin kohde käyttöjärjestelmiä. Gaussille suunnitellut Kurt ja Godel – modulit kykenevät saastuttamaan myös 64-bittisen käyttöjärjestelmän. [23, 7 – 8]

3.5 Shamoon

Elokuussa 2012 Israelilainen tietoturvayhtiö Seculert havaitsi uuden kyberaseen jonka kohteena oli Saudi Arabialainen öljy- ja kaasuyhtiö Aramco. Toimiessaan Shamoon haittaohjelmisto tuhosi tiedostoja noin 30 000 eri tietokoneesta ja palvelimesta. Tämä aiheutti Aramcon järjestelmille suurta tuhoa, joiden korjaamiseen kului useita kuukausia. [25]

Toisin kuin useimmat kyberaseet, Shamoon oli todella aggressiivinen ja näkyvä ohjelmisto. Tämä johtui siitä, että sen päämääränä oli saada tietokoneiden käyttöjärjestelmät käyttökelvottomiksi eli sen ei ollut tarkoituskaan pysyä salassa koko operaatiota. Shamoonin tarkoituksena on saattanut olla peittää jonkin toisen haittaohjelman jäljet. [26]

Shamoonia ei pidetä kovinkaan monimutkaisena ohjelmistona. Yhtenä syynä tähän pidetään sitä, että suurin osa sen koodista oli todennäköisesti kopioitu. [25] Seculertin mukaan Shamoon suorittaa hyökkäyksensä kaksi-vaiheisesti. Ensimmäisessä vaiheessa se saastuttaa Internet-yhteydessä olevan tietokoneen ja muuttaa sen välityspalvelimeksi. Tätä kautta haittaohjelma kommunikoi hallintapalvelimien kanssa. Tämän jälkeen se leviää muihin yrityksen tietokoneisiin, joilta se varastaa tiedostoja. Shamoon varastaa tärkeitä tiedostoja tietokoneiden “Käyttäjät”, ”Omat tiedostot” sekä ”System32” –kansioista. Varastettuaan tiedostot, se alkaa ylikirjoittaa tiedostoja, joita kohde tarvitsee käynnistymiseen. Suoritettuaan tehtävänsä se kommunikoi vielä uudelleen hallintapalvelimien kanssa. Shamoon on rakennettu Windows 95, Windows 98, Windows XP, Windows 2000, Windows Vista, Windows NT, Windows ME, Windows 7, Windows 2003 sekä Windows Server 2008 -käyttöjärjestelmiä vastaan. [27]

Shamoon haittaohjelmiston tiedostokoko on 900 kilotavua ja kuten useimmissa haittaohjelmissa myös Shamoonissa on tunnistettavissa eri moduuleita. Yksinkertaistettuna Shamoonissa on kaksi eri moduulia. Toinen näistä moduuleista on yhteydessä hallintapalvelimiin ja toinen näistä moduuleista levittää tiettyä kuvatiedostoa tietokoneen tärkeisiin kansioihin. [28]

Kuvatiedosto leviää tietokoneen käynnistykseen tarvittaviin kansioihin. Näissä kansioissa oleviin tiedostoihin kyseinen kuvatiedosto ylikirjoittaa itseään. Tavoitteena on, että tietokone ei pysty enää käynnistymään. Leviävä kuva ei ole kokonainen vaan siinä on kuvattuna yläreuna palavasta Yhdysvaltain lipusta. Shaamonin tekijä haluaa mahdollisesti tällä kuvalla ilmaista oman mielipiteensä Yhdysvalloista. [28]

Kuva 1. Shamoonin kuvan suhde alkuperäiseen kuvaan [29]

3.6 Mahdi

Mahdi tuli julkisuuteen ensimmäistä kertaa heinäkuussa 2012 Seculert -tietoturvayhtiön toimesta. Kuten useimmissa kyberaseissa, nimi saatiin sen levittämästä tiedostosta, jonka nimi oli Mahdi. Nimi tarkoittaa Islamissa vapahtajaa, joka saapuu poistamaan maailmasta vääryyden, epäoikeudenmukaisuuden sekä tyrannian. [30; 31]

Mahdin kohteena oli noin 800 tietokonetta eri puolilla Lähi-itää. Suurin osa saastuneista koneista oli Iranissa (387) sekä Israelissa (54) [30; 31]. Kaspersky Lab:n tutkijan Costin Raiun mukaan kyseessä ei ole kovinkaan monimutkainen ohjelmisto, vaikka se kykeneekin päivittämään itseään hallintapalvelimien kautta. Näiden hallintapalvelimien kautta Mahdi voi ladata moduuleja itseensä, joilla se kykenee varastamaan dokumentteja, tarkkailemaan näppäimistön käyttöä, ottamaan kuvankaappauksia sähköposteista sekä tallentamaan ääntä. Kyberase latasi uusia ominaisuuksia itseensä käyttämällä Google-hakukoneen näköistä selainsivua. Kun käyttäjä avasi omasta mielestään kyseisen hakukoneen, latasi haittaohjelma samaan aikaan uusia moduuleita tietokoneeseen [30]. Tutkijat eivät ole löytäneet tarkkaa kohdetta haittaohjelmalle. Kohteena on ollut mm. kriittistä infrastruktuuria valvovia yrityksiä, valtioiden virastoja ja lähetystöjä. [32]

Seculert tietoturvayhtiö sai ensimmäisen havainnon Mahdista helmikuussa 2012. Havainto saatiin sähköpostista, jonka liitteenä oli Word-dokumentti, joka sisälsi verkkoartikkelin marraskuulta 2011. Kyseinen artikkeli käsitteli Israelin suunnitelmia käyttää elektronisia aseita Irania vastaan. Mikäli käyttäjä aukaisi sähköpostin sisältämän liitteen, muodosti se takaoven hallintapalvelimiin. Mahdi käytti myös PDF ja PowerPoint-tiedostoja takaoven muodostamiseen. Kaspersky Labin mukaan, esimerkiksi yksi PowerPoint-tiedosto esitteli sarjan uskonnollisia sekä trooppisia kuvia. Näiden avulla ohjelma hämäsi käyttäjää niin, että virusvaroitukset jäivät mahdollisesti huomiotta, jolloin Mahdi sai yhteyden hallintapalvelimiin. Kaspersky Labin mukaan kaikki takaovet, olivat koodattu Delphi-nimisellä ohjelmalla. Tämä viittaa siihen, että koodaajina on ollut joukko amatöörejä tai kehittäjiä joilla on ollut todella kiire saada kyberase valmiiksi. [32; 31]

Kuva 3. Yksi PowerPoint -tiedostossa olleista kuvista [31]

Vanhimmat löydetyt versiot Mahdista ovat olleet aktiivisia jo joulukuusta 2011. Haittaohjelman sisällöstä on löydetty viitteitä siitä, että se on koodattu ennen vuoden 2011 syyskuuta. Mahdi kommunikoi viiden eri palvelimen kanssa, joista yksi oli Tehranissa ja neljä muuta Kanadassa. Yksi näistä palvelimista oli vielä aktiivinen heinäkuussa 2012, vaikka haittaohjelman löytyminen oli tullut jo julkisuuteen. [32]

Mahdi ja Flame ovat samankaltaisia haittaohjelmistoja. Seculert ja Kaspersky Lab eivät ole saaneet mitään viitteitä siitä, että näiden haittaohjelmistojen tekijöillä olisi kuitenkaan mitään yhteyttä toisiinsa. Kun Mahdi ottaa yhteyttä hallintapalvelimiin, käyttää se persian kieltä, Farsia, kommunikointiin. Mahdi myös käyttää päivämääriin persialaista kalenteria. Tämäkin viittaa jo siihen, että Mahdilla ja Flamella on eri kehittäjät. [32]

3.7 Wiper

Wiper havaittiin tekevän hyökkäyksiä joulukuusta 2011 aina huhtikuuhun 2012. Hyökkäyksien kohteena oli Iranin kansallinen öljy-yhtiö sekä öljyministeriö [33]. Suurin osa hyökkäyksistä tapahtui huhtikuun kymmenenä viimeisenä päivänä. Ei ole selvää minkä takia painopiste oli luotu juuri huhtikuun loppuun. Ei tiedetä oliko kyseessä vain sattuma vai oliko haittaohjelman alun perinkin tarkoitus iskeä voimalla juuri huhtikuun lopussa. [17]

Tavoitetilana Wiperilla oli, että kohdejärjestelmää ei kyetä enää käynnistämään eikä sen kiintolevyn tiedostoja kyetä palauttamaan. Muutaman sadan gigatavun kiintolevyn pyyhkiminen vie liian kauan aikaa, joten Wiper keskittyi pyyhkimään vain tärkeimpiä tiedostoja. Tässä Wiper onnistui todella hyvin. Kyberase oli kirjoitettu niin hyvin, että aina kun se aktivoitui, kaikki data hävisi kohteesta. Wiperin tekijät ovat olleet todella huolellisia siivotessaan ohjelman jättämät jäljet. Kaikissa Kaspersky Labin tutkimissa tapauksissa Wiper oli pyyhkinyt lähes kaiken tiedon itsestään. [17]

Kaspersky Lab:n arvion mukaan ei välttämättä saada ikinä tietää sitä mikä Wiper oikeasti oli. He ovat melko varmoja siitä, että se ei ole sukua Flamelle. Mutta pieniä viitteitä on siitä, että Wiperilla olisi jonkin asteinen yhteys Duquun ja Stuxnettiin. Tämä johtuu siitä, että Wiper käytti samantyylisiä tiedostonimiä. Kaiken kaikkiaan Wiper oli erittäin tehokas haittaohjelma. Se on varmasti innoittanut muita haittaohjelman tekijöitä ohjelmoimaan Wiperin tapaisia ohjelmia (esimerkiksi Shamoon). [17]

4 YHTEENVETO

Kyber on vielä melko epäselvä kokonaisuus sen monimutkaisuudesta johtuen. Esimerkiksi kyberavaruus on kenttänä vielä todella epäselvä valtioille sekä niiden turvallisuusviranomaisille [1, 7].

Käsitellyt modulaariset kyberaseet sekä haittaohjelmat ovat todella laajoja ohjelmistoja joiden poistaminen vaatii usein uusia päivityksiä kohdejärjestelmiin. Tulevaisuudessa olisi todella tärkeää, että hyökkäyksen kohteena olleet yritykset, valtion virastot ym. tekisivät yhteistyötä kyseisten uhkien poistoon. Tämän yhteistyön avulla yritykset kykenisivät mahdollisesti huomaamaan tulevat verkkohyökkäykset. Vaikka yritykset ja valtion virastot kykenisivät parantamaan yhteistyön avulla suojautumista verkkohyökkäyksiltä, niiden toimintaa rajaa suuresti lainsäädäntö, joka ei välttämättä mahdollista mm. tehokasta verkon valvontaa.

Perinteiset virustorjunnat sekä palomuurit eivät kykene täydellisesti estämään nopeasti leviäviä kyberaseita sekä haittaohjelmia [2]. Suurin syy siihen on se, että näiden haittaohjelmistojen leviäminen tapahtuu kohdejärjestelmän sisällä. Tällainen uhka ei leviä ulkoapäin yritysten tietokoneisiin vaan, kun se on saanut jalansijan yhteen yrityksen tietokoneeseen, kykenee se saastuttamaan kaikki yrityksen tietokoneet sekä muita mahdollisia tietojärjestelmiä, kuten automaatiojärjestelmät.

Käsiteltyjen kyberaseiden sekä haittaohjelmistojen leviäminen tapahtui pääsääntöisesti Lähi-idässä. Niiden saastuttamien tietokoneiden lukumäärät ovat arvioiden mukaan seuraavanlaisia:

Ohjelmisto	Arvio saastuneiden koneiden kokonaismäärästä
Stuxnet	100 000 - 300 000
Gauss	10 000
Flame	5000 – 6000
Duqu	50 – 60
Shamoon	30 000
Mahdi	800

Näyttää siltä, että suurin osa käsitellyistä kyberaseista ja haittaohjelmistoista ovat jollain tavalla yhteydessä toisiinsa. Vuonna 2010 löydettyä Stuxnettiä voidaan pitää ensimmäisenä kyberaseena (kyberaseen määritelmästä riippuen). Kun Duqu löydettiin 2011, havaittiin sen käyttä-

vän samaa Tilded-lavettia kuin Stuxnet. Voidaan siis olettaa, että näillä kahdella on sama kehittäjä. Alun perin vuonna 2012 löydetyn Flamen oletettiin olevan osa Yhdysvaltojen kyberoperaatioita Lähi-idässä. Kuitenkaan suoraa yhteyttä Stuxnettiin ei löydetty. Jotkin tietoturvayhtiöt kuitenkin epäilevät, että Flame ja Stuxnet ovat saman organisaation tuottamia. Myöhemmin vuonna 2012 Gaussin paljastuttua, huomattiin myös Gaussilla olevan selkeä yhteys Flameen. Näin ollen kaikki edellä mainitut ohjelmistot muodostavat yhteyden toisiinsa. Tämä osoittaa, mikäli edellä olevat olettamukset ovat oikeita, että Yhdysvalloilla on kyky tuottaa hyvin erilaisia kyberaseita sekä haittaohjelmia, kokoamalla useista kehittämistään moduuleista tarvittava kokonaisuus. [1, 227 – 228] Lähi-itä on selkeästi toiminut testikenttänä uuden tyyppisille haittaohjelmistoille sekä kyberaseille.

LÄHTEET

[1] Jari Rantapelkonen, Mirva Salminen. *The Fog of Cyber Defence.* 2. painos. Helsinki: Maanpuolustuskorkeakoulu / Johtamisen ja sotilaspedagogiikan laitos, 2013. 234 s. ISBN 978-951-25-2430-3.

[2] Stefano Mele. Cyber-weapons: Legal and strategic aspects [verkkojulkaisu]. Machiavelli Editions [viitattu 5.11.2013]. Saatavissa: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf

[3] Martti Lehto. *Kybermaailman määrittely.* Sotilasaikakauslehti, 2013. no. 12 p. 9 – 17. ISSN 0038-1675

[4] Petri Huovinen, Anssi Kärkkäinen, Mikko Lehto, Lauri Noronen, Kimmo Pispa, Ville Viita. *Sotilaalliset kybersuorituskyvyt – Toimintaympäristön tarkastelu, osa 1.* Sotilasaikakauslehti, 2013. no. 12 p. 20 – 27. ISSN 0038-1675

[5] CGI. Offensiivioperaatiot, Kyberaseet. Näyttöesitys. [viitattu 30.1.2014]

[6] Timo Kiravuo, Mikko Särelä, Jukka Manner. *Kybersodan taistelukentät.* Sotilasaikakauslehti, 2013. no. 3 p. 46 – 49. ISSN 0038-1675

[7] Jessica Beder. Tilded platform. [viitattu 30.1.2014] Saatavissa: http://searchsecurity.techtarget.com/definition/Whatiscom-definition-Tilded-platform

[8] Lee Ferran. Stuxnet [verkkojulkaisu]. abcNEWS [viitattu 2.8.2013]. Saatavissa: http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/

[9] Kaspersky Lab. Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected [verkkojulkaisu]. Kaspersky Lab [viitattu 2.8.2013]. Saatavissa:

http://www.kaspersky.com/about/news/virus/2012/resource_207_kaspersky_lab_research_proves_that_stuxnet_and_flame_developers_are_connected

[10] Geoff McDonald, Liam O Murchu, Stephen Doherty, Eric Chien. *Stuxnet 0,5: The Missing Link.* Symantec Security Response

[11] Mikko Hyppönen. On Stuxnet, Duqu and Flame [verkkojulkaisu]. F-Secure [viitattu 2.8.2013].
Saatavissa: http://www.f-secure.com/weblog/archives/00002376.html

[12] Alexander Gostev. Kaspersky Security Bulletin 2012. Cyber Weapons. [viitattu 16.12.2013] Saatavissa:
http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons

[13] Jarmo Myyrä. *Kybersota.* Sotilasaikakauslehti, 2013. no. 3, p. 44 – 45. ISSN 0038-1675

[14] Cert.fi. Tietoturvakatsaus 3/2010. [viitattu 5.8.2013]. Saatavissa:
http://www.cert.fi/katsaukset/2010/tietoturvakatsaus_3_2010.html

[15] Alexander Gostev, Kaspersky Lab Expert. What is Flame? [viitattu 16.12.2013] Saatavissa: http://www.kaspersky.com/flame

[16] Aleks, Kaspersky Lab Expert. The Flame: Questions and Answers. [viitattu 16.12.2013] Saatavissa:
http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

[17] GReAT, Kaspersky Lab Expert. What was that Wiper thing? [viitattu 17.12.2013] Saatavissa: https://www.securelist.com/en/blog/208193808/

[18] ITU (International Telecommunication Union). FAQs on Flame [verkkojulkaisu]. [viitattu 29.4.2013]. Saatavissa:
http://www.itu.int/cybersecurity/Articles/ FAQs_on_FLAME.pdf

[19] Ryan Naraine. Duqu FAQ [verkkojulkaisu]. Kaspersky Lab. 2012, [viitattu 2.5.2013] Saatavissa: http://www.securelist.com/en/blog/208193178/Duqu_FAQ

[20] Symantec. W32.Duqu - The precursor to the next Stuxnet. [viitattu 17.12.2013] Saatavissa: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

[21] Kaspersky Experts. The Mystery of Duqu: Part One – Part Ten [verkkojulkaisu]. Securelist [viitattu 2.8.2013]. Saatavissa: http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One

[22] Kaspersky Lab. Kaspersky Lab Discovers “Gauss” – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts. [viitattu 17.12.2013] Saatavissa: http://www.kaspersky.com/about/news/virus/2012/kaspersky_lab_and_itu_discover_gauss_a_new_complex_cyber_threat_designed_to_monitor_online_banking_accounts

[23] Kaspersky Lab Global Research and Analysis Team. Gauss: Abnormal Distribution [verkkojulkaisu]. Kaspersky Lab 2012. [viitattu 21.5.2013]. Saatavissa: https://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf

[24] GReAT, Kaspersky Lab Expert. Gauss: Nation-state cybe-surveillance meets banking Trojan [verkkojulkaisu]. Kaspersky Lab 2012. [viitattu 21.5.2013]. Saatavissa: https://www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan

[25] Seculert.com The Shamoon Malware: Looking Back and Seeing What’s Ahead. [viitattu 20.11.2013]. Saatavissa: http://www.seculert.com/blog/2013/05/the-shamoon-malware-looking-back-and-seeing-whats-ahead.html

[26] Paul Wagensell. “Shamoon” spyware searches then destroys. [viitattu: 13.12.2013]. Saatavissa: http://www.nbcnews.com/technology/shamoon-spyware-searches-then-destroys-950609

[27] Jack Clark, reporter, technology researcher. Shamoon malware infects computers, steals data, then wipes them. [viitattu 13.12.2013] Saatavissa: http://www.zdnet.com/shamoon-malware-infects-computers-steals-data-then-wipes-them-7000002807/

[28] GReAT, Kaspersky Expert. Shamoon The Wiper – Copycats at Work. [viitattu 20.11.2013]. Saatavissa: http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work

[29] Symantec. The Shamoon Attacks. [viitattu: 13.12.2013] Saatavissa: http://www.symantec.com/connect/blogs/shamoon-attacks

[30] Aviv Raff. Mahdi – The Cyberwar Savior? [viitattu: 13.12.2013] Saatavissa: http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html

[31] GReAT, Kaspersky Lab Expert. The Madi Campaing – Part I. [viitattu 14.12.2013] Saatavissa: https://www.securelist.com/en/blog/208193677/The_Madi_Campaign_Part_I

[32] Kim Zetter. Mahdi, the Messiah, Found Infecting Systems in Iran, Israel. [viitattu 13.12.2013]. Saatavissa: http://www.wired.com/threatlevel/2012/07/mahdi/

[33] Kim Zetter. Wiper Malware That Hit Iran Left Possible Clues of Its Origins. [viitattu 17.12.2013] Saatavissa: http://www.wired.com/threatlevel/2012/08/wiper-possible-origins/

[34] *Suomen kyberturvallisuusstrategia.* 1. painos. Helsinki: Turvallisuus- ja puolustusasiain komitean sihteeristö, 2013. 13 s. ISBN: 978-951-25-2434-1.

LIITELUETTELO

KADETTI OJALAN TUTKIELMAN LIITE 1

Tutkielman käsitteet

Kyber- ei usein käytetä yksinään, vaan se toimii yhdyssanan ensimmäisenä osana. Kyber tarkoittaa yleisesti toimintaa sähköisessä viestinnässä ja tietokonejärjestelmissä. [34, 12]

Kyberturvallisuus on tavoitetila, kun käsittelemme turvallisuutta kybertoimintaympäristössä. Tällöin toimintaympäristöön voi luottaa ja sen toiminta on turvattu. [34, 13]

Kyberavaruus on toimintaympäristö, joka tarkoittaa tietojärjestelmien sekä niiden välisen digitaalisen tiedonsiirron muodostamaa kokonaisuutta.

Kybersodankäynti (cyber-warfare) tarkoittaa toimintaa johon kuuluu kriittisen infrastruktuurin sabotaasi, vakoilu ja lamauttaminen. Kybersodankäynti voidaan jakaa kolmeen kokonaisuuteen: strateginen kybersodankäynti, taktis-operatiivinen kybersodankäynti sekä kybersodankäynti sotaa alemmissa kriiseissä [3, 10 - 11].

Kyberhyökkäyksellä (cyber-attack) tarkoitetaan tietoverkoissa suoritettua hyökkäystä, jonka päämääränä voi olla esimerkiksi vakavat energiantuotanto- tai ympäristöongelmat.

Kyberpuolustus tarkoittaa virustorjuntojen ja palomuurien käyttöä, yhteistyötä eri toimijoiden kesken turvallisuuden parantamiseksi ja kyber-rikollisten etsintää ja kiinniottoa virkavallan voimin. Kyberpuolustuksen päämääränä on saavuttaa kyberturvallisuus.

Kyberase on sähkömagneettisessa ympäristössä vaikuttava haitta, jonka taustalla on valtio tai voimaltaan sitä vastaava ryhmittymä. Kyberaseet kohdennetaan yleensä tarkoin valittuun kohteeseen, kun taas normaalit haittaohjelmat kohdistetaan satunnaisesti kaikkia mahdollisia kohteita vastaan. Kyberaseen tavallisia kohteita ovat sotilaalliset kohteet, valtion organisaatiot, kriittinen infrastruktuuri sekä yritykset. Tavoitteena sillä on tietyn operatiivisen vaikutuksen aikaansaaminen, kuten esimerkiksi kohteen valvonta, tiedustelu ja/tai tuhoaminen. Kyberaseet käyttävät hyväkseen mm. nollapäivä haavoittuvuuksia sekä kohdeympäristön fyysisen- tai henkilöturvallisuuden heikkouksia päästäkseen sisään kohdejärjestelmään. [5, 16 - 17]

Haittaohjelma (Malware) on yläkäsite viruksille, madoille, troijalaisille ja takaoville.

Virus on haittaohjelma, joka tarvitsee kohdetietokoneessa isäntäohjelman, jonka avulla virus leviää tietokoneessa muihin ohjelmiin.

Mato on pieni ohjelma, joka leviää itseään kopioimalla tietokoneessa. Mato ei tarvitse isäntäohjelmaa tietokoneessa, kuten virus.

Troijalainen on haittaohjelma, jonka tarkoituksena on avata portti kohdetietokoneeseen. Tämän avatun portin kautta tietokoneeseen pääsee lisää haittaohjelmia, jotka pystyvät tekemään todella merkittävää haittaa tietokoneelle.

Takaovi (backdoor) on vakoiluohjelma, jolla pyritään selvittämään kohdetietokoneessa käytettyjä käyttäjätunnuksia ja salasanoja.

Rootkit toimii nimensä mukaan järjestelmän juuressa. Rootkit antaa pääsyn järjestelmän sisälle, niin että hyökkääjällä on pääsy kaikkiin toimintoihin ja palveluihin joita käyttöjärjestelmälläkin on.

Nollapäivähaavoittuvuus on haavoittuvuus johon ei ole olemassa korjauspäivitystä. Ohjelmiston kehittäjä ei välttämättä edes tiedä haavoittuvuudesta, ei ole ehtinyt korjata ohjelmistoa tai ei yksinkertaisesti välitä haavoittuvuudesta.

Eväste (Cookie) tarkoittaa pientä määrää dataa, jonka lähettäjänä toimii web-palvelin. Kyseinen palvelin lähettää tiedon tietokoneeseen, jonka jälkeen se tallennetaan. Tallennuksen jälkeen esimerkiksi kyseinen Internetsivu näkyy käyttäjän tietokoneessa oikein.

Vertaisverkko (Peer-to-Peer) tarkoittaa sellaista verkkoa, jossa ei ole erillistä palvelinta vaan kaikki verkkoon liitetyt tietokoneet toimivat palvelimina.

SSL –protokolla on salausprotokolla, jota käytetään mm. verkkopankkien aitouden varmistamiseen.

Kyberaktivismi (kybervandalismi, hakkerointi, haktivismi) on yleensä vaikutukseltaan lyhytaikainen ja osin vaaraton. Yrityksen tai yksilön kannalta kyberaktivismi voi aiheuttaa merkittäviäkin taloudellisia vahinkoja. [3, 10 - 11]

Kyberrikollisuus tarkoittaa rikoksia, jotka suoritetaan sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai niitä vastaan. [3, 10 - 11]

Kybervakoilu on toimintaa jolla hankitaan salaisia tietoja yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta. Kybervakoilua suoritetaan, jotta saavutetaan poliittista, sotilaallista tai taloudellista hyötyä. Vakoilun suorittamiseen joudutaan käyttämään laittomia menetelmiä Internetissä, verkoissa, ohjelmistoissa ja/tai tietokoneissa. [3, 10 - 11]

Kyberterrorismi on terrorismia, jossa tietoverkkoja käytetään hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan. Tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen sekä painostaa poliittista johtoa taipumaan terroristien vaatimuksiin. [3, 10 - 11]

Tietojärjestelmä käsittää niin ihmiset, tietojenkäsittelylaitteet, tiedonsiirtolaitteet sekä ohjelmistot.

Välityspalvelin (proxy) tarkoittaa palvelinta, joka voidaan määrittää tietokoneeseen. Kun tietokone ottaa yhteyden johonkin Internetsivuun välityspalvelimen kautta, näkyy tietokoneen käynti Internetsivulla välityspalvelimen tietoina.