Tampereen yliopisto

Antti Välipakka

KRYPTOKAAPPAUS JA SEN TORJUNTA

Diplomityö
Informaatioteknologian ja viestinnän tiedekunta
Tarkastajat: Marko Helenius
ja Jukka Koskinen
Maaliskuu 2022

TIIVISTELMÄ

Antti Välipakka: Kryptokaappaus ja sen torjunta
Diplomityö
Tampereen yliopisto
Tietotekniikka, DI
Maaliskuu 2022

Tämän diplomityön tavoitteena oli selvittää kryptokaappausten eri variaatioiden toimintamallit ja miten näiltä variaatioilta suojaudutaan. Työ tehtiin kirjallisuuskatsauksena. Pääsääntöisesti tietoa haettiin Tampereen yliopiston tarjoamalla Andor-hakupalvelulla. Lähteiksi valikoitui tieteellisiä artikkeleita ja tutkimuksia. Muutama lähde haettiin eri tietoturvayhtiöiden nettisivuilta. Nämä lähteet olivat esimerkiksi tietoturvayhtiöiden koostamia vuosiraportteja haittaohjelmista. Tiedonhakumenetelmänä käytettiin helmenkasvatusmenetelmää.

Kryptokaappaus tarkoittaa tilannetta, jossa hyökkääjä ottaa luvattomasti uhrinsa laitteen haltuunsa ja alkaa louhia valitsemaansa kryptovaluuttaa alustalla ilman laitteen omistajan lupaa. Kryptokaappauksissa suositaan yleensä kryptovaluutta Moneroa sen tarjoaman vahvan anonymiteetin takia. Kryptokaappauksen yhteydessä hyökkääjän on mahdollista asentaa kaapatulle alustalle muitakin haittaohjelmia, asentaa takaovi myöhempää käyttöä varten ja varastaa tietoa. Varsinkin yrityskohteissa tiedon joutuminen vääriin käsiin on vaarallista.

Kryptokaappaukset voidaan jakaa kahteen kategoriaan: tiedostopohjaisiin ja selainpohjaisiin. Tiedostopohjaisessa kryptokaappauksessa uhri huijataan asentamaan kryptolouhijan sisältävä tiedosto tai tiedosto ujutetaan uhrin laitteelle jotakin tietoturva-aukkoa hyödyntäen. Selainpohjainen kryptokaappaus tapahtuu nimensä mukaisesti nettiselaimessa. Selainpohjainen kryptokaappaus tapahtuu, kun uhri vierailee kryptolouhijan sisältävällä nettisivulla.

Kryptokaappauksista aiheutuvia haittoja ovat prosessorin kulutus, laitteiston mahdollinen hajoaminen, kaappauksen yhteydessä tulevat muut haittaohjelmat ja tiedon varastaminen. Prosessorin kulutus ilmenee siten, että laite toimii hitaasti tai pahimmassa tapauksessa laitteen suorituskyky romahtaa ja tekee laitteen käyttökelvottomaksi. Laitteiston hajoaminen koskee lähinnä älypuhelimia, jotka ovat haavoittuvaisia selainpohjaisille kryptokaappauksille. Tiedostopohjaisissa kryptokaappauksissa on helppo ujuttaa muita haittaohjelmia kryptolouhijan lisäksi.

Kryptokaappauksilta suojautumiseen on useita tapoja. Tärkein tapa on tietoturvavalppaus, jolla estetään hyökkäystä tapahtumasta. Tehokkainkaan suojautumismekanismi ei estä kryptokaappauksia ja muita haittaohjelmia, jos laitteen käyttäjän tietoturvavalppaus ei ole ajan tasalla. Kryptokaappauksen tapahduttua tarvitaan muita suojautumiskeinoja, kuten esimerkiksi mustalistaukseen perustuva havainnointi, jota voidaan hyödyntää myös nettiselainten selainlaajennuksissa. Laitteen verkkoliikennettä ja suorituskykyä voidaan myös analysoida ja tutkia kryptokaappausten havainnoimiseksi. Pilvipalveluille, jotka ovat otollisia kohteita kryptokaappauksille niiden lähes rajattomien resurssien takia, on olemassa nimenomaan pilvipalveluille suunniteltuja suojausmekanismeja ja -työkaluja. Tällaisia työkaluja ovat esimerkiksi RADS ja MineGuard. Yksityishenkilöiden laitteita voidaan suojata joissakin määrin perinteisillä virustentorjuntaohjelmistoilla, mutta niillä on omat rajoitteensa kryptolouhijoiden ja muiden haittaohjelmien käyttämän hämäännyttämisen takia.

Työn tuloksena huomattiin, että kryptokaappaukset ovat jatkuvasti kehittyvä uhka ja että ne aiheuttavat huomattavia kuluja varastaessaan kaappaamansa alustan laskentatehoa. Kulut nousevat isoiksi varsinkin pilvipalvelualustoilla. Yrityskohteissa tiedon varastaminen kryptokaappauksen ohella on myös iso riski.

Avainsanat: louhintahaittaohjelma, kryptokaappaus, kryptovaluutta

ABSTRACT

Antti Välipakka: Cryptojacking and protection from it
Master's thesis
Tampere University
Information Technology, MSc
March 2022

The aim of this master's thesis was to figure out the operating principles of cryptojacking and how to protect from them. This study was done as a literature review. Information search was mainly conducted using the Tampere university's Andor search service. Scientific articles and research were chosen as sources. The sources also included a few information security company web pages. The search method used was pearl growing.

Cryptojacking means a situation where an attacker takes the control of a victim's device without permission and uses this device to mine a cryptocurrency without the permission of the device's owner. Cryptocurrency Monero is often used in these cryptojackings due to the strong anonymity it provides. During the cryptojacking, it is possible for the attacker to install other malware on the hijacked device, install a backdoor for further use or steal information. Information theft is especially dangerous for companies.

Cryptojacking can be categorized into two categories: file-based and browser-based. In a file-based cryptojacking, the victim is manipulated into installing a crypto miner containing file or the file is planted into the victim's device using an exploit. Browser-based cryptojacking happens as its name suggests in a browser. Browser-based cryptojacking happens when a victim visits a website which has a crypto miner.

Damages caused by cryptojacking include processor usage, possible hardware failure, other malware installed during the cryptojacking and information theft. Processor overusage can be detected when the device operates slowly or in the worst case becomes inoperable. Hardware failure mainly concerns mobile devices which are vulnerable to browser-based cryptojacking. During file-based cryptojacking, it is easy for the attacker to plant other malware in addition to the crypto miner on the hijacked device.

There are many protection ways against cryptojacking. The most important one is information security awareness, which prevents the cryptojacking from happening. Even the most effective protection mechanism does not prevent cryptojackings and installation of other malware if the device's operator's information security awareness is not up to date. In the case cryptojacking happens, other protection mechanisms are needed, such as awareness based on blacklisting which can also be used in browser add-ons. A device's network activity and performance can be analyzed and inspected to detect cryptojacking. For cloud-based services, which are favorable targets for cryptojacking due to their almost limitless resources, there are protection mechanisms and tools which are specifically designed for cloud-based services. RADS and MineGuard are examples of these kinds of tools. Personal devices can be somewhat protected with traditional antivirus softwares, but they have their own limits due to the obfuscation used by the crypto miners and other malware.

As the results of this review, it was noticed that cryptojacking is a constantly developing threat and causes significant costs by stealing the computing power of the hijacked device. The costs quickly go up especially when cloud-based services are targeted. Information thefts are also a significant risk for corporations in addition to the cryptojacking.

Keywords: crypto miner, cryptojacking, cryptocurrency

ALKUSANAT

Työn aiheen valitseminen oli helppoa. Aihe liittyy läheisesti kandityöni aiheeseen kiristyshaittaohjelma ransomwareen. Hyvää lähdemateriaalia aiheeseeni liittyen löytyi runsaasti ja ongelmaksi meinasikin välillä muodostua lähteiden karsiminen. Diplomityön tekeminen on ollut opettavainen kokemus.

Haluan kiittää ohjaajiani Marko Heleniusta ja Jukka Koskista hyvästä tuesta ja ohjaamisesta. Kiitos myös vanhemmilleni ja siskolleni avusta työn oikoluvussa ja hyvistä vinkeistä työn parantamiseen.

Tampereella, 8.3.2022

SISÄLLYSLUETTELO

1. JOHDANTO 1
    1.1 Tutkimusongelma 1
    1.2 Tutkimusmenetelmä 2
    1.3 Tulokset 2
    1.4 Työn rakenne 2
2. MENETELMÄT 3
    2.1 Käytetyt tietokannat 3
    2.2 Google-haut 3
    2.3 Mendeleyn ehdottamat artikkelit 4
3. KRYPTOVALUUTOISTA 6
    3.1 Lohkoketju 6
    3.2 Louhintaprosessi 7
    3.3 Louhinta-altaat 8
    3.4 Kryptovaluuttalompakko 8
    3.5 Louhinnan tuottavuus 9
4. KAAPPAAJAN TOIMINTAPERIAATE 12
    4.1 Selainpohjainen kryptokaappaus 12
    4.2 Tiedostopohjainen kryptokaappaus 16
5. HYÖKKÄYSKOHTEET 19
    5.1 Yksityishenkilöt 19
    5.2 Yritykset 20
    5.3 Pilvipalvelut 20
        5.3.1 Smominru 23
        5.3.2 CryptoSink 24
        5.3.3 Zealot 24
        5.3.4 Adylkuzz 24
        5.3.5 WannaMine 25
        5.3.6 RubyMiner 25
        5.3.7 Tesla-hyökkäys 25
        5.3.8 Jenkins Miner 25
        5.3.9 Coinreg Monero 26
        5.3.10 Norman 26
        5.3.11 Graboid 26
    5.4 Muut kohteet 26
6. KRYPTOKAAPPAUSTEN HAITAT 28
    6.1 Prosessorin käyttö 28
    6.2 Laitteiston hajoaminen 29
    6.3 Muut haittaohjelmat 29

6.4 Tiedon varastaminen 30
7. TORJUNTA 32
7.1 Tietoturvavalppaus 32
7.2 Mustalistaus 33
7.3 Suorituskykyanalyysi 34
7.4 Verkkoanalyysi 35
7.5 Torjunta yritysten näkökulmasta 36
7.6 RADS – Pilvipalveluille suoja 36
7.7 MineGuard 37
7.8 Virustentorjuntaohjelmistojen tehottomuus 37
8. POHDINTA 39
8.1 Mikä on kryptokaappaus ja mikä ei? 39
8.2 Kryptolouhintaa virustentorjuntaohjelmistoissa 40
9. YHTEENVETO 41
LÄHTEET 42

LYHENTEET JA MERKINNÄT

AES	Advanced Encryption Standard, edistynyt salausstandardi
CUDA	Compute Unified Device Architecture, laskennallisesti yhtenäinen laitearkkitehtuuri; Nvidia-yrityksen kehittämä ohjelmointirajapinta
DNS	Domain Name System, verkkotunnusnimisysteemi; käytetään laitteiden tunnistamiseen internetissä
HPC	Hardware performance counter, laitteistosuorituskykylaskuri; prosessoreissa oleva laskuri
HTML	Hypertext Markup Language, hypertekstin merkintäkieli; nettisivustoissa käytetty merkintäkieli
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla; palvelinten käyttämä tiedonsiirtoprotokolla
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
RADS	Real-Time Anomaly Detection System for Cloud Infrastructures
SHA-256	Secure Hash Algorithm, turvallinen tiivistealgoritmi
TCP	Transmission Control Protocol, siirtohallintaprotokolla; tiedonsiirrossa käytetty tietoliikenneprotokolla

1. JOHDANTO

Kryptokaappaus tarkoittaa tilannetta, jossa hyökkääjä valjastaa käyttäjän tietokoneen tai vastaavan alustan kryptovaluuttojen louhinta-alustaksi ilman käyttäjän lupaa. Louhinnan toteuttavat erityisesti tätä tarkoitusta varten suunnitellut louhintahaittaohjelmat. Kryptokaappauksen kohteeksi voi joutua yksityinen käyttäjä, yritys tai pilvipalveluratkaisuja tarjoava yritys. Kryptokaappauksella on kaksi toimintaperiaatetta: tiedostopohjaiset ja selainpohjaiset kryptokaappaukset. Molemmissa tapauksissa kryptolouhija louhii kryptovaluuttoja käyttäen uhrinsa alustan tehoja tienatakseen omistajalleen rahaa.

Tavanomaisesti haittaohjelmat ovat ottaneet kohteekseen vain Microsoft Windows -käyttöjärjestelmällä toimivia tietokoneita. Viimeisen kymmenen vuoden aikana haittaohjelmia ja samalla kryptokaappauksia on kuitenkin alkanut näkyä yhä enemmän myös Linux-pohjaisilla alustoilla. Tietoturvayritys Symantecin vuonna 2018 koostaman tietoturvaraportin mukaan kyberrikolliset ovat siirtyneet kiristyshaittaohjelma ransomwaren käytöstä kohti kryptolouhintaa kryptokaappausten avulla [1].

Tässä luvussa esitellään aluksi työn tutkimusongelma, jonka tukena on kaksi tutkimuskysymystä. Sen jälkeen esitellään lyhyesti työn tutkimusmenetelmä. Lopuksi käydään läpi vielä työn tulokset ja työn rakenne.

1.1 Tutkimusongelma

Kryptokaappaukset ovat relevantti uhka nykypäivän tietoyhteiskunnassa ja ovat mielenkiintoisia. Suomeksi ei ole tehty kryptokaappauksia koskevaa kirjallisuuskatsausta. Tässä työssä tehtiin kirjallisuuskatsaus kryptokaappausten toimintaan. Tutkimuskysymyksinä tutkimusongelman tueksi ovat:

1. Mitkä ovat kryptokaappausten eri variaatioiden toimintamallit?
2. Miten näiltä eri variaatioilta suojaudutaan?

Koska kryptokaappauksia on tämän työn kirjoitushetkellä kahdenlaisia, tiedosto- ja selainpohjaisia, tämä työ keskittyy näiden kahden eri kryptokaappausvariantin tutkimiseen. Kryptokaappausten toimintamallien lisäksi käsitellään myös kryptokaappauksista koituvia haittoja, hyökkäysten kohteita ja lopuksi vielä kryptokaappauksilta suojautumista.

Kryptokaappauksiin liittyvät lähteet ovat pääsääntöisesti alle viisi vuotta vanhoja tieteellisiä julkaisuja. Osa lähteistä on eri tietoturvayhtiöiden tekemiä raportteja kryptolouhijoista ja niiden toiminnasta. Kryptovaluuttoja ja niiden toimintaperiaatteita koskevat lähteet ovat hieman vanhempia. Osa niistä on jopa kuusi vuotta vanhoja.

1.2 Tutkimusmenetelmä

Tämä työ on toteutettu kirjallisuuskatsauksena tutustumalla kryptokaappauksiin liittyviin tieteellisiin julkaisuihin ja tutkimuksiin. Nämä lähteet löytyivät käyttämällä muutamaa eri tietokantaa. Kirjallisuuskatsaus toteutettiin helmenkasvatusmenetelmällä. Luvussa 2 tutkimusmenetelmästä kerrotaan yksityiskohtaisemmin.

1.3 Tulokset

Tuloksena saatiin, että kryptokaappaukset ovat todellinen ongelma ja niitä vastaan tarvitaan tehokkaita torjuntametodeja. Kryptokaappausten muuttuessa hyökkääjien kehittäessä jatkuvasti tehokkaampia ja paremmin piilossa olevia hyökkäyksiä, myös torjuntametodien tulee kehittyä jatkuvasti. Tällä hetkellä olevat torjuntametodit ovat tehokkaita ja monipuolisia. Eri torjuntametodien yhdistely ja vanhojen metodien päivittäminen esimerkiksi mustalistauksen muodossa ovat tulevaisuuden kryptokaappausten varalta oleellisia.

1.4 Työn rakenne

Luvussa 2 käsitellään tässä työssä käytettyjä menetelmiä. Luvussa 3 käsitellään kryptovaluuttoja ja niiden toimintaperiaatetta yleisellä tasolla. Luvussa 4 käsitellään kryptokaappaajan toimintaperiaatetta tiedosto- ja selainpohjaisten kryptokaappausten osalta. Luvussa 5 käsitellään kryptokaappausten hyökkäyskohteita. Luvussa 6 käsitellään kryptokaappauksista koituvia haittoja niin yksityishenkilöille kuin yrityksille. Luvussa 7 käsitellään kryptokaappausten torjuntamenetelmiä. Luvussa 8 pohditaan mikä on kryptokaappaus ja mikä ei. Lopuksi luvussa 9 esitetään yhteenveto.

2. MENETELMÄT

Tämä työ toteutettiin kirjallisuuskatsauksena. Lähteitä löytyi etsimällä muutamasta eri tietokannasta käyttämällä hakusanoina kryptokaappausta ja sen englanninkielistä vastinetta *cryptojacking*. Kryptovaluuttojen toimintaa varten hakusanana toimi *kryptovaluutat*. Tämän työn kannalta oleellisten kryptovaluuttojen osalta lähteinä toimivat näiden valuuttojen viralliset internetsivustot ja sieltä löytyvät tarkat tekniset dokumentaatiot kyseisen kryptovaluutan toiminnasta ja ominaisuuksista.

Päämetodina toimi helmenkasvatusmenetelmä [2]. Tämän menetelmän ideana on aluksi valita hakusanat. Näillä hakusanoilla etsitään oman aiheen kannalta oleellisia artikkeleita ja julkaisuja. Kattavan ja oleellisen julkaisun löydyttyä tutustutaan sen lähdeluetteloon ja etsitään sieltä relevantteja lähteitä. Seuraavaksi tutustutaan taas luettuun julkaisuun ja sen lähdeluetteloon. Tässä työssä tietokantojen hakusanoina toimivat *cryptojacking* (suom. kryptokaappaus) ja *cryptocurrency* (suom. kryptovaluutta). Kryptokaappausten torjuntaa varten tietoa etsittiin hakusanalla haittaohjelma ja sen englanninkielisellä vastineella *malware.* Etsittäessä tarkkaa tietoa jostakin tietystä kryptovaluutasta hakusanana toimi kryptovaluutan nimi.

Systemaattinen kirjallisuuskatsaus [3] olisi myös sopinut tämän työn menetelmäksi, mutta sen tarkat säännöt ja tiukat rajat olisivat vaikeuttaneet kirjoitusprosessia. Helmenkasvatusmenetelmän vapaammat säännöt tuntuivat itselleni mielekkäämmiltä. Tässä luvussa käydään läpi lähteidenhakuprosessissa käytetyt tietokannat ja palvelut.

2.1 Käytetyt tietokannat

Tässä työssä käytetyt tietokannat ovat Andor ja Google Scholar. Andor on Tampereen yliopiston tarjoama hakupalvelu, joka hakee muun muassa artikkeleita, konferenssijulkaisuja ja kirja- ja lehtikokoelmia [4]. Andorin kautta löytämäni julkaisut löytyivät hyvin usein IEEE:n (engl. Institute of Electrical and Electronics Engineers) tietokannasta. IEEE:n tietokanta sisältää teknillisiä julkaisuja eri aiheista. Google Scholar on Googlen tarjoama hakupalvelu, jonka avulla löytyy pääsääntöisesti tieteellisiä julkaisuja [5].

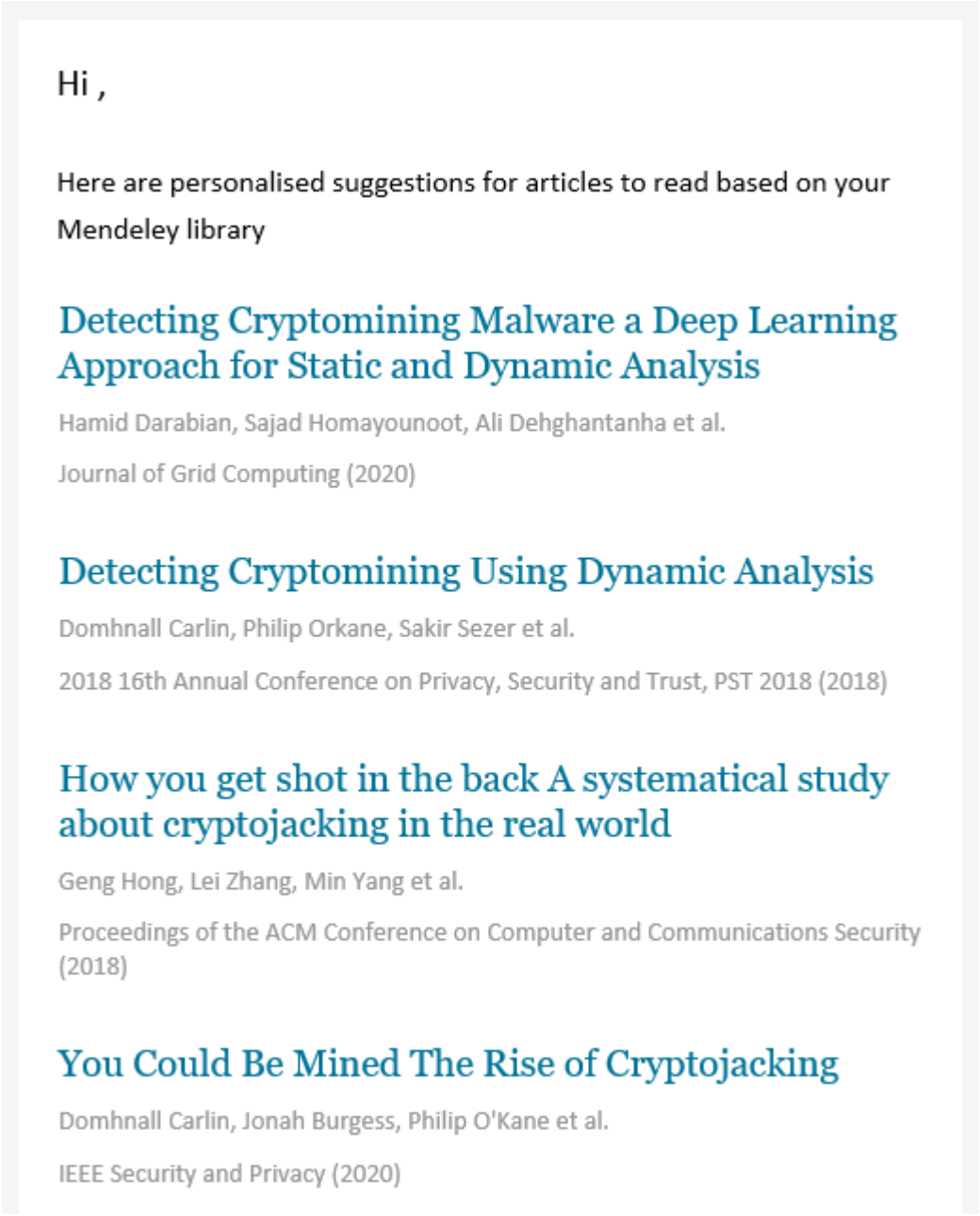
2.2 Google-haut

Googlen hakukonetta käytettiin tässä työssä tämän työn kannalta oleellisten kryptovaluuttojen virallisten dokumentaatioiden etsimiseen. Esimerkiksi kryptovaluutta Moneron

osalta Googlen haun avulla löytyi Moneron virallinen dokumentaatio. Työn alkuvaiheessa Googlen hakua käytettiin etsimään mahdollisia suomenkielisiä artikkeleita kryptokaappauksista, koska Andoria ja Google Scholaria käyttämällä niitä ei löytynyt. Jotkut tietoturvayhtiöt kertoivat omilla sivustoillaan jonkin verran kryptokaappauksista, mutta näiden artikkeleiden sisältö vaikutti paikoittain huonosti käännetyltä, ja näistä artikkeleista puuttuivat usein myös lähdemerkinnät. Näin ollen tämän työn kannalta nämä suomenkieliset artikkelit ja ylipäätään suomenkieliset hakutulokset kryptokaappausten osalta hylättiin.

2.3 Mendeleyn ehdottamat artikkelit

Tämän työn kirjoitusprosessin apuna käytettiin Mendeley-nimistä lähteidenhallintatyökalua. Halutessaan tätä työkalua käyttävä voi tilata sähköpostiinsa artikkelikoosteen, joka sisältää ehdotuksia perustuen omassa lähdekirjastossa oleviin artikkeleihin.



Kuva 1 *Mendeleyn artikkelikooste*

Mendeleyn ajoittain lähettämä artikkelikooste (Kuva 1) sisältää linkkejä artikkeleihin ja julkaisuihin perustuen käyttäjän aikaisemmin keräämiin lähteisiin. Linkit näihin artikkeleihin ja julkaisuihin sisältävät tiivistelmän teoksen sisällöstä, julkaisun tekijän tiedot ja julkaisun sijainnin. Näiden tietojen avulla teosta voi etsiä esimerkiksi aikaisemmin mainitusta Andor-tietokannasta ja samalla voi myös varmistaa julkaisujen luotettavuuden. Kuvan 1 artikkeleiden osalta päädyin käyttämään kaikkia kuvassa mainittuja artikkeleita lähteinäni.

3. KRYPTOVALUUTOISTA

Kryptovaluutta on digitaalinen valuutta, jota luodaan käyttämällä tietokoneen laskentatehoa. Kryptovaluutat ovat desentralisoituja eli ne eivät ole minkään yksittäisen tahon säätelemiä. Kryptovaluutoilla tehdyt transaktiot tallentuvat valuutasta riippuen joko julkisesti saatavilla olevaan tai piilotettuun tietokantaan. Kryptovaluutat itsessään säilötään digitaalisen lompakkoon, jota käyttäjä voi säilyttää itsellään esimerkiksi omalla tietokoneellaan tai USB-tikulla. Digitaalisen lompakon voi myös säilöä kolmannen osapuolen tarjoamalle alustalle. [6]

Bitcoin on ensimmäinen kryptovaluutta. Sen kehitti vuonna 2009 vain pseudonyyminä tunnettu Satoshi Nakamoto. Bitcoinin alkuaikoina sen louhinta oli vielä helppoa, mutta myös sen arvo oli olematon. Mitä enemmän Bitcoinin arvo kasvoi, sitä vaikeammaksi Bitcoinin louhinta muuttui.

Nykyään kryptovaluuttoja on useita erilaisia ja uusia luodaan jatkuvasti. Uusia kryptovaluuttoja luodaan esimerkiksi siksi, että tarvitaan johonkin tiettyyn käyttötarkoitukseen sopivampi valuutta. Uuden valuutan toivotaan myös tulevan suosituksi, jotta valuuttaan aikaisin sijoittaneet saisivat mahdollisimman isot voitot. Tämän työn kannalta kryptovaluutta Monero on kuitenkin oleellisin sen tarjoaman vahvan tietoturvan takia. Monero toimii Bitcoinin tavoin, mutta näillä kahdella on joitakin suuria eroja. Monero on suunniteltu louhittavaksi tavallisilla tietokoneilla, toisin kuin Bitcoin. Monero tarjoaa myös paremman anonymiteetin kuin Bitcoin. Tämä tekee siitä otollisen kryptovaluutan rikollisten käyttöön. [1]

Tässä luvussa käsitellään aluksi suurimmasta osasta kryptovaluutoista löytyvää lohkoketjua ja lohkoketjun toiminnan kannalta oleellista tiivistefunktiota. Seuraavaksi käsitellään kryptovaluuttojen louhintaprosessia. Louhintaprosessin käsittelyn jälkeen käydään läpi louhintaprosessin yhdistäminen muiden käyttäjien kanssa louhinta-altaiksi. Sen jälkeen käydään läpi, miten kryptovaluuttoja säilytetään digitaalisissa lompakoissa. Lopuksi käsitellään Bitcoinin ja Moneron hintakehitystä, jotta saadaan parempi käsitys kryptovaluuttojen tuottavuudesta.

3.1 Lohkoketju

Suurin osa kryptovaluutoista - suosituimpien joukosta Bitcoin ja Monero - käyttää erityisiä tietokantoja tallentamaan kaikki kyseisellä valuutalla tehdyt transaktiot. Näitä tietokantoja kutsutaan lohkoketjuiksi. Lohkoketju sisältää kaikki tietyllä kryptovaluutalla tehdyt siirrot.

Yksi lohkoketjun lohko sisältää useita transaktioita. Transaktiot ovat kryptovaluutalla tehtyjä kauppoja eli valutaan lähettämistä ja vastaanottamista. Lohkoketjun perään lisätään aina uusi lohko sitä mukaa, kun valuutalla tehdään lisää transaktioita. Lohkoketjun lohkot voidaan todentaa aidoiksi hyödyntämällä kryptografiaa. Jokainen ketjun lohko sisältää transaktioiden lisäksi myös edellisen lohkon tiivistearvon (engl. hash), aikaleiman ja tunnistearvon. [7]

Tiivistefunktio (engl. hash function) on matemaattinen algoritmi, joka muuttaa satunnaisen kokoisen syötteen kiinteän kokoiseksi merkkijonoksi. Tätä merkkijonoa kutsutaan tiivisteeksi. Tiivistefunktion tulee olla nopea, jotta se olisi käyttökelpoinen. Lohkoketjun tiiviste muodostetaan käyttämällä kryptografiaa hyödyntävää tiivistefunktiota. Nämä kryptografiset tiivistefunktiot ovat tavallisiin tiivistefunktioihin verrattuna tietoturvallisempia kolmella tavalla:

1. Yksisuuntaisuus: Yksittäisen tiivistearvon avulla on mahdotonta selvittää syötearvo.
2. Heikko yhteentörmäyksen esto: Tietystä syötteestä lasketulle tiivistearvolle täytyy olla käytännössä mahdotonta löytää toinen syöte, joka antaa saman tiivistearvon.
3. Vahva yhteentörmäyksen esto: Täytyy olla käytännössä mahdotonta löytää kaksi syötearvoa, jotka antavat saman tiivistearvon.

[6]

Bitcoin käyttää SHA256^2 (engl. Secure Hash Algorithm) tiivistefunktiota [6]. Tämä tarkoittaa sitä, että SHA256-tiivistealgoritmia käytetään kaksi kertaa. Monero käyttää erityistä anonymiteettiä tarjoavaa CryptoNight-nimistä tiivistefunktiota [8]. CryptoNight perustuu salausalgoritmi AES:iin (engl. Advanced Encryption Standard) [8]. Lohkoketjun lohkojen sisältämät aikaleimat ovat digitaalinen todiste siitä, että yksittäinen transaktio tapahtui. Aikaleima koostuu transaktiodatan tiivistearvosta [6].

3.2 Louhintaprosessi

Louhintaprosessissa lohkoketjuun lisätään uusia lohkoja. Louhinnassa käytetään tietokoneen tai vastaavan laitteen prosessorin, näytönohjaimen tai erillisten louhimista varten suunniteltujen laitteistojen laskentatehoa. Louhintaprosessi on valuuttakohtaisesti erilainen, mutta esimerkiksi Bitcoinin tapauksessa louhintaprosessin vaikeus ja samalla valuutan arvo johtuu Bitcoinin louhintaprosessia käytettävästä ”nollasäännöstä”. Tämä sääntö tarkoittaa sitä, että jokaisen louhitun lohkon tiivistearvossa täytyy olla ennalta

määrätty määrä nollia. Vaadittujen nollien määrää on helppo muokata ja samalla louhintaprosessi vaikeutuu. Louhintaprosessin vaikeutuessa valuutan arvo nousee. Kun halutun tiivistearvon antava lohko saadaan louhittua, louhija tai louhijat saavat palkkion. Palkkio on jokin tietty valuuttakohtainen osa louhittua valuuttaa. Louhinta voidaan suorittaa yksin tai louhinta-altaissa. [6]

Louhintaprosessissa louhijat valitsevat lohkoon sisällytettävät transaktiot niiden tärkeysjärjestyksen perusteella. Lohkon tulee sisältää isolla prioriteetilla olevia transaktioita, mutta muuten lohkon voi täyttää louhijan valitsemilla transaktioilla. Ideaalisesti lohko halutaan täyttää transaktioilla, joilla on isot transaktiokustannukset tuoton maksimoimiseksi. Transaktiokustannukset ovat suoraan verrannolliset transaktion kokoon eli mitä isompi transaktio on tehty, sitä isommat transaktiokustannukset ovat. [9]

Kryptokaappausten tapauksessa louhintaprosessi on samanlainen kuin itse tehtävässä louhinnassa. Kryptokaappauksessa tosin louhintaan tarvittava laskentateho varastetaan kaappausten uhreilta ja kaappaajat saavat itselleen voitot.

3.3 Louhinta-altaat

Bitcoinin alkuaikoina kaikki louhinta tapahtui yksin. Pikkuhiljaa louhintaprosessin vaikeuduttua louhijat yhdistivät louhintavoimansa perustaen louhinta-altaita. Ensimmäisiä louhinta-altaita alkoi ilmestyä vuoden 2010 aikana. Louhinta-altaat tarjoavat hitaamman, mutta varman tuoton. Yksin tehtävä louhinta saattaa olla tuottoisampaa, jos käytössä on useampi nimenomaan louhintaan tarkoitettu laite. Louhinta-altaissa voitonjako tapahtuu ennalta määriteltyjen sääntöjen mukaisesti. Usein voitonjako tapahtuu altaaseen annetun oman louhinta-ajan ja tehon mukaan. Näin voitonjako on reilua. Louhinta-allasta valittaessa kannattaa kuitenkin varmistaa altaan luotettavuus. Juuri perustettu louhinta-allas ei välttämättä ole luotettava. [10] Kryptokaappausten tapauksessa hyökkääjän kaappaamat ja kryptolouhintaan valjastamat laitteet muodostavat yksittäisen louhinta-altaan, koska nämä kaikki kaapatut laitteet siirtävät louhintavoittonsa samaan kryptovaluuttalompakkoon. [11]

3.4 Kryptovaluuttalompakko

Kryptovaluuttalompakko on sovellus, joka helpottaa kryptovaluuttatransaktioiden tekemistä. Tällaisia lompakoita on erilaisia. Lompakon avulla voidaan vastaanottaa ja lähettää kryptovaluuttoja. Lompakko ei kuitenkaan sisällä kryptovaluuttoja, koska ne sijaitse-

vat lohkoketjussa. Lompakon sisältämällä yksityisellä avaimella pääsee käsiksi lohkoketjussa sijaitseviin omiin varoihin. Toisin sanoen, kryptovaluuttalompakko sisältää ainoastaan yksityisen avaimen, jolla muualla (lohkoketjussa) sijaitseviin varoihin päästään käsiksi. Lompakko tarvitaan, jotta kryptovaluutoilla voidaan tehdä transaktioita. Lompakon yksityiselle avaimelle luodaan lompakon luonnin yhteydessä julkinen avain. Tätä julkista avainta käytetään valuuttojen vastaanottamiseen. [10]

Kryptovaluuttalompakkotyypeistä käytetyimmät ovat lokaalisti säilytettävät sovelluspohjaiset lompakot. Muita lompakkotyyppejä ovat rautapohjaiset, paperilompakot ja jonkin kolmannen osapuolen tarjoamat lompakkopalvelut. [10]

Sovelluspohjaiset lompakot ovat käyttäjän laitteelle ladattavia sovelluksia. Osa sovelluksista sisältää vain yksityisen avaimen, osa lataa koko lohkoketjun käyttäjän laitteelle sen tarkastelemista varten. Rautapohjaiset lompakot ovat fyysisiä laitteita, joita voi ostaa eri palveluntarjoajilta. Ne ovat sovelluspohjaisia lompakoita turvallisempia, koska ne liitetään tietokoneeseen vain transaktioiden tekemistä varten. Paperilompakot tarkoittavat vain oman yksityisen avaimen kirjoittamista paperille muistiin. Tällaisessa lompakkomallissa käyttäjä ei ole riippuvainen mistään ulkoisesta tahosta pitämään lompakkonsa turvassa, vaan käyttäjä itse vastaa sen turvallisuudesta. Toisaalta paperilompakon käytössä riskinä on paperin hukkaaminen ja paperilompakko on myös kömpelö käytettävyydeltään. Kolmannen osapuolen tarjoamissa lompakkopalveluissa käyttäjä joutuu luottamaan ulkoiseen tekijään, mutta toisaalta käyttäjän ei itse tarvitse huolehtia lompakon turvallisuudesta. Kuten oikeat pankit, tällaiset lompakkopalvelut saattavat joutua varkauden kohteeksi tai ne saattavat mennä konkurssiin. Osa palveluista kuitenkin tarjoaa tiettyyn pisteeseen asti vakuutuksen käyttäjille. [10]

Kryptokaappausten tapauksessa hyökkääjä asettaa valitsemansa louhijan asetuksiin oman kryptovaluuttalompakkonsa osoitteen eli julkisen avaimensa. Louhijasta riippuen asetuksiin voidaan myös kirjata louhinta-altaan osoite, jos louhinta halutaan suoritettavan jossakin tietyssä altaassa.

3.5 Louhinnan tuottavuus

Louhinnan tuottavuus on sidottuna louhittavan valuutan arvoon. Alla olevista kuvista nähdään Bitcoinin (Kuva 2) ja Moneron (Kuva 3) hintakehitys vuodesta 2014 ja 2015 alkaen. Näistä kuvista nähdään, että kryptovaluutat ovat arvokkaita ja näin ollen niitä kannattaa louhia. Niiden arvo on heittelehtinyt mutta noussut moninkertaiseksi hintakehityksen seurannan aloitukseen nähden. Louhinta kuitenkin kuluttaa sähköä ja se vaatii

runsaasti laskentatehoa. Rikollisten suorittama kryptokaappaus ja näin ollen muiden laitteilla suoritettu louhinta tuo rikollisille pelkkää voittoa, koska he eivät joudu huolehtimaan louhinnasta aiheutuvista kuluista. Toisaalta rikollisille aiheutuvat kuluvat ovat kaappauksiin kulunut aika.

Kuva 2 *Bitcoinin hintakehitys vuodesta 2014 alkaen* [12]

Kuva 2 esittää Coinmarketcap-sivuston kokoaman hintakehityskartan Bitcoinin arvolle vuodesta 2014 lähtien vuoteen 2021 saakka. Bitcoinin seurannan korkein arvo 57 737 € saavutettiin vuoden 2021 lokakuussa. Bitcoinin arvon äkilliseen nousuun vuoden 2021 tienoilla vaikutti Teslan ilmoitus siitä, että se oli sijoittanut 1,5 miljardin dollarin edestä Bitcoiniin. Tämä toi Bitcoinin vielä enemmän julkisuuteen.

Kuva 3 *Moneron hintakehitys vuodesta 2015 alkaen* [13]

Kuva 3 esittää Moneron hintakehityksen vuodesta 2015 alkaen Coinmarketcap-sivuston keräämän datan perusteella. Moneron seurannan korkein arvo 396,42 € saavutettiin vuoden 2017 joulukuussa. Moneron äkillisille arvonmuutoksille ei ole yksinäistä selitystä.

Vuonna 2018 tapahtunut Moneron arvon äkillinen nousu johtuu todennäköisesti selainpohjaisissa kryptokaappauksissa käytetyn Coinhive-palvelun perustamisesta. Moneron ja muiden kryptovaluuttojen arvo vaihtelee nopeasti ja isoihin arvon muutoksiin vaikuttaa esimerkiksi julkisuuden henkilöiden tai tunnettujen yritysten tekemä sijoitus kryptovaluuttoihin.

Kryptovaluuttoja voidaan louhia joko käyttämällä tietokoneen prosessoria tai näytönohjainta. Osa kryptovaluutoista suosii prosessorin avulla suoritettua louhintaa ja osa näytönohjaimella. Esimerkiksi kryptokaappauksissa usein louhittua Moneroa suositaan louhittavan prosessorilla näytönohjaimen sijaan, koska Moneron louhinta-algoritmi suosii prosessorilla tehtävää louhintaa [14].

4. KAAPPAAJAN TOIMINTAPERIAATE

Kryptokaappauksia on kahdenlaisia, selainpohjaisia ja tiedostopohjaisia. Selainpohjainen kryptokaappaus tuottaa vain rahaa kaappaajalle, mutta tiedostopohjaisessa kryptokaappauksessa voidaan myös esimerkiksi varastaa kohdelaitteelta tietoja kryptolouhinnan lisäksi. Selainpohjaisessa kryptokaappauksessa kryptokaappaus tapahtuu uhrin vieraillessa kryptolouhijalla saastutetulla nettisivustolla. Kohdealustoja näille hyökkäyksille ovat kaikki laitteet, joilla toimii nettiselain. Tiedostopohjaisessa kryptokaappauksessa kryptolouhija ujutetaan uhrin laitteelle tiedostona. Tiedostopohjaisessa kryptokaappauksessa on myös helppo ujuttaa kryptolouhijan lisäksi muita haittaohjelmia uhrin laitteelle ja tälle laitteelle asennetaan usein myös etäyhteys, jotta hyökkääjä voi hyödyntää saastuttamaansa laitetta myöhemmin. Zimba et al. esittävät [15], että kryptokaappaajat suosivat yleensä selainpohjaista kryptokaappausmenetelmää sen passiivisen ominaisuuden takia. Julkaisussa todettiin myös, että tiedostopohjainen kryptokaappaus on monimutkaisempi toteuttaa ja se epäonnistuu yleisesti ottaen helpommin kuin selainpohjainen kryptokaappaus.

Tässä luvussa esitellään aluksi selainpohjainen kryptokaappaus ja sen toimintamalli. Samalla käydään läpi selainlaajennusten kryptokaappaukset. Sen jälkeen käydään läpi tiedostopohjainen kryptokaappaus ja sen toimintamalli.

4.1 Selainpohjainen kryptokaappaus

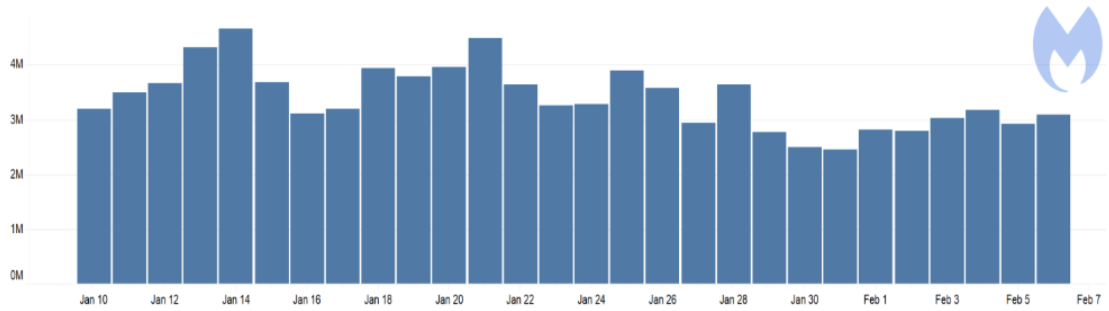
Mainosten näyttämisen sijaan jotkut sivustot ovat alkaneet tarjota käyttäjilleen mahdollisuuden tukea sivustoa antamalla luvan kryptolouhintaan selaimessa. Varsinkin laittomia suoratoistopalveluita ja piraattisisältöä tarjoavat sivustot ovat siirtyneet perinteisistä mainoksista vapaaehtoisen kryptolouhintamahdollisuuden tarjoamiseen. [16]

Selainpohjainen kryptokaappaus tehdään injektoimalla JavaScript-ohjelmointikielellä tehty skripti nettisivulle. Tämä skripti sisältää louhinnassa tarvittavat käskyt, ja se suoritetaan automaattisesti sivulla vierailtaessa. Selainpohjaisen kryptokaappauksen toiminta ei ole tietystä alustasta riippuvainen. Selainpohjainen kryptokaappaus tarvitsee toimiakseen vain laitteen, jolla pääsee vierailemaan nettisivustoilla. Tällainen laite voi olla esimerkiksi tietokone tai älypuhelin. Kaappauksessa käytetty JavaScript voidaan ottaa helposti kokonaan pois käytöstä selaimesta tai vastaavasta verkkosovelluksesta, mutta tämä johtaa yleensä eri nettisivustojen toiminnallisuuden hajoamiseen. Kryptolouhijan

sisältämän nettisivun sulkeminen riittää lopettamaan louhinnan ja samalla kryptokaappauksen. [17]

Aziz *et al.* kuvailevat [18] selainpohjaisten kryptokaappausten hyödyntävän niin sanottua ”drive-by” hyökkäystä. Tällainen hyökkäys tapahtuu, kun uhri vierailee nettisivulla ja erikseen mitään klikkaamatta saa automaattisesti selaimeensa haitallista koodia. Tällainen hyökkäys jättää harvoin jälkeensä haitallisia tiedostoja, jotka virustentorjuntaohjelmistot saattaisivat huomata. Näin ollen uhri ei välttämättä edes tiedä tulleensa hyökkäyksen kohteeksi.

Selainpohjaiset kryptokaappaukset olivat kovassa nousussa vuosien 2017 ja 2018 aikana, kun Coinhive-niminen palvelu avasi ovensa. Coinhive oli palvelu, joka tarjosi käyttäjilleen helppokäyttöisen skriptin, jonka nettisivujen omistajat pystyivät laittamaan omille nettisivuilleen. Skriptin ideana oli louhia sivustolla vierailevan selaimessa kryptovaluutta Moneroa. Ennen louhimista käyttäjältä kysyttiin lupa, ja louhinnan syyksi kerrottiin vieraillun sivuston tukeminen. Pian kuitenkin tätä Coinhiven tarjoamaa skriptiä muokattiin siten, että se ei enää kysynytkään lupaa louhimiseen. Tietoturvayritys Malwarebytesin mukaan [19] tätä ”hiljaista”, lupaa kysymätöntä versiota Coinhiven skriptistä käytettiin kolme miljoonaa kertaa päivässä aikavälillä 10.1.2018–6.2.2018 (Kuva 4). [18]



Kuva 4 *"Hiljaisen" Coinhive -skriptin käyttöaste 2018* [19]

Selainpohjaiset kryptolouhijat kuuluvat tiedostottomien haittaohjelmien kategoriaan. Tiedostoton haittaohjelma on haittaohjelma, joka ei käytä hyökkäyksessään tiedostoa (esimerkiksi suoritettavaa .exe-tiedostoa tai Microsoft Wordin .docx-dokumenttitiedostoa). Tiedostojen sijaan tiedostottomat haittaohjelmat leviävät esimerkiksi nettiselainten välityksellä. [20]

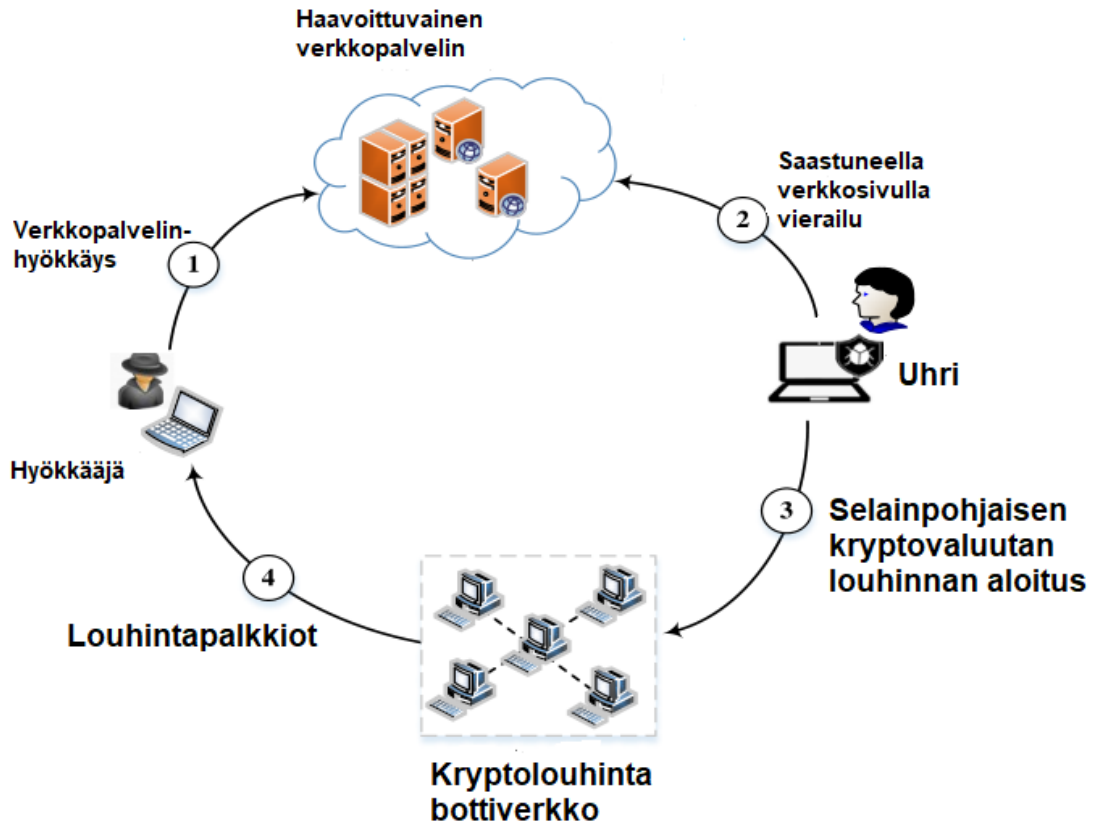
Selainpohjaisissa kryptokaappauksissa louhinta tapahtuu hyödyntämällä laitteen prosessoria. Tämä johtuu siitä, että selainpohjaisessa kryptolouhinnassa käytetty JavaScript tarjoaa prosessoripohjaisen louhinnan kannalta oleellisia ominaisuuksia. JavaScript mahdollistaa periaatteessa näytönohjainpohjaisen kryptolouhinnan, mutta tämä

on hyvin rajoittunutta JavaScriptin ominaisuuksien takia. Näin ollen selainpohjaiset kryptolouhijat on paljon järkevämpi asettaa louhimaan prosessorin avulla näytönohjaimen sijaan. Lisäksi näytönohjainpohjainen kryptolouhinta vaatii tehokkaan ja samalla kalliin näytönohjaimen ollakseen tehokasta. Näytönohjainpohjaista louhintaa varten kaappaajan tulisi siis pystyä valitsemaan kohteensa tarkasti eli se ei ole kannattavaa. [21]

Nykyaikaisiin selaimiin on mahdollista lisätä laajennuksia, joiden avulla voidaan esimerkiksi muokata nettisivustojen ulkonäköä poistamalla nettisivustojen mainoksia. Näitä selainlaajennuksia ladataan pääsääntöisesti selaimen omasta laajennuskaupasta, mutta laajennuksia on myös mahdollista ladata kolmannen osapuolen tarjoamista alustoista. Ajoittain näiden laajennusten mukana joko tulee haittaohjelma tai sitten itse laajennus on haittaohjelma.

Vuonna 2017 Googlen Chrome-selaimen laajennuskaupassa oli kryptokaappaajan sisältävä laajennus. Vain muutamassa päivässä laajennus ehti kerätä yli 100 000 latausta. Vastaavia tapauksia tapahtuu ajoittain, ja Chrome ei ole ainoa selain, jonka laajennuksista löydetään haittaohjelmia ja kryptolouhijoita. [22]

Kuva 5 esittää tavanomaisen selainpohjaisen kryptokaappauksen toimintamallin. Selainpohjaisissa kryptokaappauksissa hyödynnetään yleensä haavoittuvaista verkkopalvelinta, jonka avulla sivustolla vierailevan uhrin selaimessa voidaan louhia kryptovaluuttoja. Kaapattuja verkkopalvelimia voidaan muokata monella tavalla ja niille voidaan esimerkiksi ujuttaa halutunlaisia skriptejä.



Kuva 5 *Selainpohjaisen kryptokaappauksen toimintamalli lähteeseen* [15] *perustuen*

Hyökkääjä voi käyttää jotakin luotettua kolmatta osapuolta välikätenä ottaessaan verkkopalvelimen käyttöönsä. Tämä voidaan toteuttaa esimerkiksi ujuttamalla varmenteen myöntäjän kautta saastunut selainlaajennus suoraan uhrille tai verkkopalvelimen kautta. Jos hyökkäyksessä hyödynnetään jotakin varmenteen myöntäjää, uhri luottaa todennäköisesti sivuston tarjoamaan selainlaajennuksen enemmän kuin jos sivustolla ei olisi varmentajaa. Nettisivuston omistaja voi myös itse asettaa omalle sivustolleen kryptolouhintaskriptin. Selainpohjaisen kryptokaappauksen toimintamalli voi olla seuraavanlainen:

1. Hyökkääjä ottaa suoraan haavoittuvaisen verkkopalvelimen käyttöönsä ilman luotettavan kolmannen osapuolen apua. Tällainen hyökkäys onnistuu, jos kohdepalvelin on haavoittuvainen.

2. Uhri vierailee saastuneella nettisivulla.

3. Saastuneella nettisivulla vierailun johdosta uhrin selaimessa aletaan louhia kryptovaluuttaa, ja uhri on nyt samalla osa kryptolouhinta-allasta.

4. Uhrien selaimissa louhitut kryptovaluutat päätyvät lopulta hyökkääjän haltuun.

Jotkut selainpohjaiset kryptokaappaukset on suunniteltu ottamaan huomioon älypuhelimet. Vaikka selainpohjainen kryptokaappaus onnistuu älypuhelinten selaimessa, se on usein kannattamatonta. Älypuhelinten suorittimet eivät ole yleensä kovinkaan tehokkaita, jolloin niillä tapahtuva louhinta ei ole tuottavaa. Laitteen jumiutuminen ja näin ollen selainpohjaisesta kryptokaappauksesta kiinnijäämisen riski kasvaa. [23]

Välttääkseen kiinnijäämistä, jotkut louhintaskriptit avaavat uuden pienen selainikkunan, joka on piilotettu käyttöjärjestelmästä riippuen jollakin tavalla tehtäväpalkin alle. Tämän louhinnan voi kuitenkin lopettaa Windows-pohjaisissa käyttöjärjestelmissä tehtävienhallintaa käyttäen. Käyttäjän tulee kuitenkin ensin huomata laitteensa kova suoritinkäyttö. [24]

4.2 Tiedostopohjainen kryptokaappaus

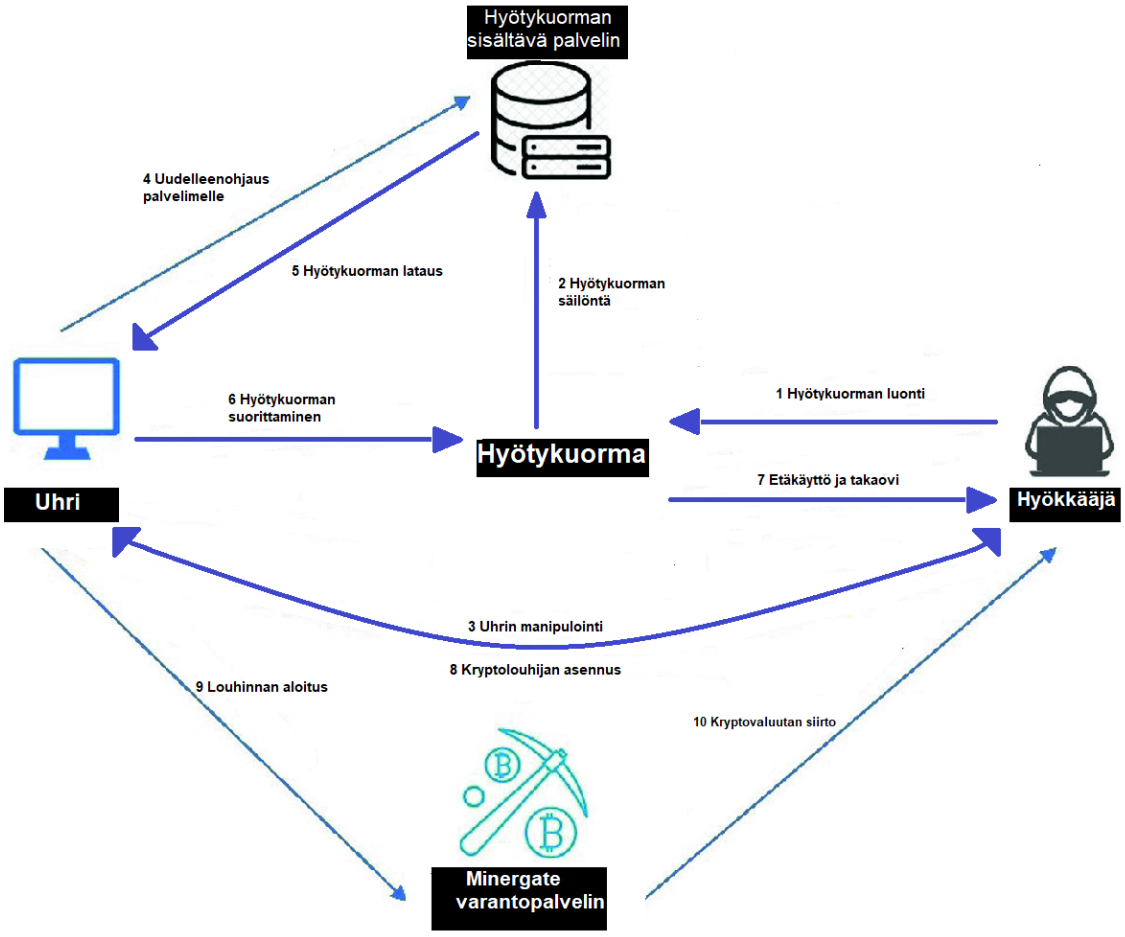
Tiedostopohjainen kryptokaappaus perustuu siihen, että uhri saadaan joko itse lataamaan kryptolouhijan sisältämä haittaohjelma(paketti) tai se ujutetaan jotakin tietoturva-aukkoa hyväksi käyttämällä ilman uhrilta vaadittavaa lataustoimenpidettä [25]. Levitysväylänä voivat toimia esimerkiksi kopiosuojausten osalta murretut ohjelmat ja pelit. Tiedostopohjaiset kryptolouhijat louhivat joko hyväksikäyttämällä kohdealustansa prosessoria tai näytönohjainta.

Selainpohjaisissa kryptokaappauksissa louhitaan pääsääntöisesti uhrin prosessoria hyväksikäyttämällä JavaScriptin rajoitteiden takia. Tämä johtaa siihen, että tiedostopohjaiset kryptolouhijat voivat valita vapaammin louhittavan kryptovaluutan. Selainpohjaisissa kryptokaappauksissa usein louhittava valuutta on Monero sen tarjoaman vahvan yksityisyyden ja tehokkaan prosessoripohjaisen louhinnan takia. Selainpohjaisessa kryptokaappauksessa voitaisiin toki louhia jotakin muuta kryptovaluuttaa, mutta Moneron tarjoama vahva yksityisyys on otollista rikollisessa käytössä. Koska Moneroa on tehokasta louhia vain prosessoria hyödyntämällä, hyökkääjät joutuvat käyttämään jotakin toista kryptovaluuttaa kuten Bitcoinia tai Ethereumia louhiessaan näytönohjaimella.

Tiedostopohjaisessa kryptokaappauksessa on myös se etu hyökkääjän näkökulmasta, että hyökkääjät voivat ottaa kohteeksi paljon erilaisempia alustoja kuin selainpohjaisessa kryptokaappauksessa. Tällaisia alustoja ovat esimerkiksi tehtaissa käytetyt valvontatietokoneet, joilla on käytössään valtavasti laskentatehoa. Niissä ei kuitenkaan välttämättä ole nettiselainta, jonka kautta selainpohjainen kryptokaappaus voisi tapahtua. Kohdelaitteella tulee kuitenkin olla internetyhteys, jotta louhinta on mahdollista. [26]

Tiedostopohjainen kryptokaappaus luo rahaa hyökkääjälle aina, kun uhrin tietokone on päällä. Selainpohjaisessa kaappauksessa hyökkääjä saa rahaa ainoastaan silloin, kun uhrin selain on yhdistetty louhijalla saastutetulle nettisivulle. [27]

Tiedostopohjaisen kryptokaappauksen toimintamalli sisältää joitakin samoja piirteitä kuin selainpohjainen kryptokaappaus. Kuva 6 esittää tavanomaisen tiedostopohjaisen kryptokaappauksen toimintamallin. Tiedostopohjaisissa kryptokaappauksissa voidaan käyttää useita erilaisia tietoturvahaavoittuvuuksia.



Kuva 6 *Tiedostopohjaisen kryptokaappauksen toimintamalli lähteeseen* [28] *perustuen*

Tiedostopohjaisen kryptokaappauksen toimintamalli on yleensä seuraavanlainen:

1. Aluksi hyökkääjä valitsee hyökkäyksessä käytettävän haittaohjelmapaketin eli hyötykuorman (engl. payload). Hyötykuormaksi kelpaa tähän tarkoitukseen esimerkiksi avointa lähdekoodia oleva Metasploit-kehys (engl. framework).
2. Hyökkääjä säilöö hyötykuorman hallitsemalleen palvelimelle.

3. Hyökkääjä manipuloi uhriaan klikkaamaan esimerkiksi sähköpostin mukana tullutta liitetiedostoa tai linkkiä, jotta uhri lataisi itselleen hyökkääjän valmisteleman hyötykuorman.
4. Uhri uudelleenohjataan hyötykuorman sisältävälle palvelimelle.
5. Uhrin laitteelle ladataan hyötykuorma yleensä jotakin tietoturva-aukkoa hyväksikäyttämällä.
6. Uhrin laitteella suoritetaan hyötykuorma.
7. Hyötykuorman suorittaminen uhrin laitteella antaa hyökkääjälle etäkäyttöoikeudet ja avaa samalla uhrin laitteelle takaoven.
8. Hyökkääjä asentaa saamansa etäkäyttöyhteyden avulla uhrin laitteelle kryptolouhijan. Hyökkääjä voisi myös asentaa samaa etäkäyttöyhteyttä hyväksikäyttäen muitakin haittaohjelmia.
9. Uhrin laitteella aloitetaan hyökkääjän valitseman kryptovaluutan louhinta. Louhintaa varten hyökkääjä on tässä tapauksessa valinnut välikädeksi Minergate-nimisen palvelun, jonne uhrin laitteella louhitut kryptovaluutat säilötään.
10. Louhitut kryptovaluutat siirretään välikäsipalvelimen kautta hyökkääjälle.

Periaatteessa hyötykuorman käyttö ei ole pakollista tiedostopohjaisessa kryptokaappauksessa. Hyökkääjä voi manipuloida uhrinsa lataamaan pelkän kryptolouhijan hyötykuorman sijaan, mutta silloin hyökkääjä ei saa luotua takaovea uhrinsa laitteelle ja näin uhrin laitteen käyttö esimerkiksi osana bottiverkkoa ei onnistu. Jos hyökkääjän ainoa motiivi on luoda rahaa kryptolouhinnalla, hyökkääjän ei edes kannata käyttää hyökkäyksessään muita haittaohjelmia kuin kryptolouhijaa.

5. HYÖKKÄYSKOHTEET

Kryptokaappausten hyökkäyskohteeksi voi joutua minkälainen taho tahansa yksityishenkilöistä yrityksiin ja jopa pilvipalvelutarjoajiin saakka. Selainpohjaisten kryptokaappausten uhreiksi kelpaa mikä tahansa laite, jolla on nettiselain. Tähän kategoriaan sopivat yksityishenkilöt ja yritykset. Tiedostopohjaiset kryptokaappaukset koskevat kaikkia kolmea kategoriaa: yksityishenkilöitä, yrityksiä ja pilvipalveluita.

Tässä luvussa käydään läpi eri kryptokaappausten hyökkäyskohteet. Aluksi käsitellään yksityishenkilöt. Sen jälkeen käydään läpi yritykset kryptokaappausten kohteena. Seuraavaksi käsitellään pilvipalvelut ja samalla tutustutaan isoimpiin pilvipalveluihin kohdistuneisiin hyökkäyksiin. Lopuksi käsitellään muut kohteet eli supertietokoneet ja luvattomasti käytetyt yliopistojen tehokkaat tietokoneet.

5.1 Yksityishenkilöt

Selainpohjaisten kryptokaappausten osalta yksi tehokkaimmista tavoista saada tuottoa on sijoittaa louhintaskriptit nettisivustoille, jotka tarjoavat käyttäjilleen suoratoistopalveluita. Koska tällaisilla sivustoilla vieraillaan yleensä useita tunteja, ne ovat otollisia tuoton kannalta. [29]

Yksityishenkilöiden käyttämät tietokoneet ja nettiselaimet ovat usein tietoturvan osalta puutteellisia, mikä tekee niistä otollisia kohteita kryptokaappauksille. Toisaalta suuri osa selainpohjaisista kryptokaappauksista tapahtuu niin sanottuina ”drive-by” -hyökkäyksinä, eli selainkaappaus tapahtuu ilman käyttäjän tekemää klikkausta. Pelkkä saastuneella nettisivulla vierailu riittää kryptokaapatuksi tulemiseen. Kryptolouhijaa on usein myös vaikea huomata, koska louhinta käyttää vain prosessorin tehoa, joka ilmennee nettisivun ja selaimen suorituskyvyn hidastumisena. Käyttäjä saattaa kuvitella selaimensa hidastumisen johtuvan vain vierailemansa nettisivun mainoksista. [30]

Tiedostopohjaisille kryptokaappauksille tehokkaita levittämiskanavia ovat kopiosuojauksien osalta murretut laittomasti levitettävät ohjelmat ja pelit. Tällaisiin tiedostoihin rikollisten on helppo lisätä oma haittaohjelmansa. Haittaohjelmien leviämistä tätä kautta edistää se, että murrettuja ohjelmia ja pelejä levittävät tahot neuvovat käyttäjiään ottamaan virustentorjuntaohjelmiston pois päältä asennuksen ajaksi. Asennustiedosto neuvotaan myös usein suorittamaan järjestelmävalvojan oikeuksia käyttäen, mikä edelleen edistää haittaohjelmien levittämisessä.

Tietoturvayhtiö Avast raportoi blogissaan vuoden 2021 kesäkuussa [31] uudesta, mahdollisesti tšekkiläistä alkuperää olevasta haittaohjelmasta Crackonosh. Tämän haittaohjelman tärkein tehtävä oli asentaa Moneroa louhiva haittaohjelma uhrinsa tietokoneelle. Crackonosh oli ujutettu useiden suosittujen murrettujen uutuuspelien mukaan. Crackonosh oli erittäin tehokas ja vaarallinen haittaohjelma siksi, että se onnistui poistamaan kaapatulta tietokoneelta kaikki virustentorjuntaohjelmat Windowsin oman virustentorjuntaohjelma mukaan lukien. Crackonosh myös otti Windowsin päivitykset pois päältä ja muokkasi Windowsin tehtäväpalkissa näkyvän Windows Defender -virustentorjuntaohjelman kuvakkeen näyttämään normaalilta, vaikka oikeasti koko Windows Defender oli poistettu tietokoneelta.

5.2 Yritykset

Yritysten kirjautumisportaalit ja kotisivut ovat otollisia kohteita rikollisille minkä tahansa haittaohjelman levityksen kannalta, myös kryptolouhijoiden. Hyökkääjä voi yrittää ujuttaa haittaohjelmansa, tässä tapauksessa tiedostopohjaisen kryptolouhijan, yrityksen kirjautumisportaaliin tai vastaavaan yritysten työntekijöiden käytössä olevaan palveluun. Sitä kautta hyökkääjä saa levitettyä haittaohjelmansa tehokkaasti ympäri yrityksen sisäverkkoa. Tällaisen hyökkäyksen nimi on niin sanottu ”watering hole” -hyökkäys. Tällaisen hyökkäyksen onnistuttua hyökkääjät onnistuvat parhaimmillaan saastuttamaan kymmeniä tuhansia laitteita, joissa louhintaskriptit pyörivät useita tunteja luoden suuret voitot hyökkääjille. [29]

5.3 Pilvipalvelut

Pilvipalvelut ovat otollisia kohteita kryptokaappauksille, koska niissä on tarjolla lähes rajattomat resurssit. Jotkut pilvipalvelut, kuten esimerkiksi Amazon ja Microsoft, tarjoavat myös mahdollisuuden näytönohjainpohjaiselle louhinnalle tarjoamalla erityisiä näytönohjaimen sisältäviä pilvipalvelimia kuluttajille. Näytönohjainpohjainen louhinta tarjoaa yleensä enemmän tuottoa verrattuna prosessoripohjaiseen louhintaan, koska useiden suosittujen kryptovaluuttojen louhinta-algoritmit suosivat näytönohjainlouhintaa. Pilvipalveluissa louhintaa voi olla hankala huomata, koska pilvipalvelut käyttävät lähtökohtaisesti paljon resursseja. [32]

Rikolliset voivat hakkeroida yksityisten ja yritysten vuokraamia pilvipalvelutunnuksia ja valjastaa ne louhintaan, jolloin kärsivänä osapuolena on tunnuksen omistaja. Kirjautumistunnusten salasanaa ei kuitenkaan vaihdeta, jotta tunnusten oikea omistaja ei huomaa jonkin olevan pielessä. Pilvipalveluita tarjoavilta yrityksiltä vuokrataan usein tietty

määrä laskentatehoa, kiintolevytilaa ja nettikaistaa. Kryptolouhijat syövät tätä vuokrattua laskentatehoa, ja näin ollen ne tulevat kalliiksi tunnuksen vuokranneelle taholle. Pilvipalveluita tarjoavilta yrityksiltä voi joissakin tilanteissa ostaa myös loputtomasti tilaa. Tällainen tila on kryptolouhijoille täydellinen kohde. [32]

Jotkut pilvipalvelutarjoajat tarjoavat opiskelijoille ja opetuskäyttöön ilmaiseksi pieniä pilvipalvelulohkoja. Joukko tutkijoita onnistui rakentamaan kryptolouhijaverkoston käyttämällä pelkästään edellä mainittuja ilmaisia pilvipalvelulohkoja. He ehtivät tuottaa useiden tuhansien dollarien edestä kryptovaluuttoja ennen kuin he itse lopettivat louhinnan. Loppujen lopuksi he eivät edes jääneet kiinni louhintaoperaatiostaan, ja siksi he toivoivatkin pilvipalveluyhtiöiden kiinnittävän enemmän huomiota tarjoamiensa ilmaisten ja maksullisten pilvipalvelulohkojen kryptolouhijoiden automaattivalvontaan. [33] Pilvipalveluita tarjoava yritys Google kielsi ja esti omissa pilvipalveluissa kaiken kryptolouhintaan liittyvän toiminnan. [32]

Pilvipalveluita kohteeksi ottaneita haittaohjelmia on löydetty vuodesta 2017 lähtien useita. Taulukkoon 1 on listattu laajan mittakaavan hyökkäyksiä. Valintaan vaikutti hyökkäyksien laajuus, haitallisuus ja hyökkääjien tienaamat voitot. Tiedot näistä hyökkäyksistä on kerätty eri tietoturvayritysten ja -tutkijoiden toimesta. Jayasinghe ja Poravi [34] koostivat näiden hyökkäysten tiedot.

Taulukko 1 Pilvipalveluihin kohdistuneet haittaohjelmat

Hyökkäys	Löytö pvm.	Alusta	Käytetty heikkous	Uhri	Työkalut/teknologia
Smominru	tammikuu 2018	Windows Server 2003, 2008, 2012 Windows XP ja 7	EternalBlue	~90 000 alustaa	NVIDIA CUDA API
CryptoSink	maaliskuu 2019	Windows/Linux	Elasticsearch	Elasticsearch Systems	XMRig-louhija

Zealot	maaliskuu 2017	Windows/Linux	EternalBlue	Apache Struts -palvelimet	Mule-krypto-louhija
Adylkuzz	toukokuu 2017	Windows	EternalBlue	Yrityspalvelimet	EternalBlue
WannaMine	lokakuu 2017	Windows	EternalBlue	Yli 75 000 alustaa	PowerShell
RubyMiner	tammikuu 2018	Windows/Linux	HTTP webpalvelin haavoittuvuudet	~700 web palvelinta	XMRig-louhija
Tesla-hyökkäys	helmikuu 2018	Amazon AWS Kubernetes-palvelmiet	Salasanasuojausten puute	Teslan Kubernetes-konsoli	CloudFlare
JenkinsMiner	helmikuu 2018	Windows/Linux	Jenkins haavoittuvuus	Jenkinspalvelimet	XMRig-louhija
Coinreg Monero	maaliskuu 2018	Windows	-	Autovalmistajan Etelä-Amerikan toimisto	Coinreg Monero, Mimikatz
Norman	elokuu 2019	Windows	-	Tietyn verkon palvelimet	XMRig-louhija
Graboid	lokakuu 2019	Dockerkontit	Suojaamattomat Dockerkontit	Yli 2000 Dockerkonttia	XMRig algoritmi

[34]

Taulukossa 1 mainitut EternalBlue ja EternalSynergy ovat haavoittuvuuksia, joka alun perin löydettiin vuonna 2017. Tällöin WannaCry-niminen kiristyshaittaohjelma levisi te-

hokkaasti hyödyntäen EternalBlue-haavoittuvuutta. Nämä haavoittuvuudet ovat Yhdysvaltojen tiedusteluvirasto NSA:n (National Security Agency) kehittämiä tietoturvahaavoittuvuuksia Windows-alustoilla. Haavoittuvuus antaa hyökkääjille mahdollisuuden suorittaa haluamaansa koodia etänä ja näin mahdollistaa pääsyn kohteensa verkkoon. [35]

Näissä hyökkäyksissä usein käytetty työkalu XMRig-louhija on suunniteltu kryptovaluutta Moneron louhintaan. XMRig on ilmainen ja sen lähdekoodi on avoin. Louhija on alun perin tarkoitettu Windows-pohjaisille alustoille, mutta sen avoin lähdekoodi on mahdollistanut louhijan muokkaamisen ja sitä kautta toiminnan myös Linux-alustoilla.

Kaikissa taulukossa 1 listatuissa hyökkäyksissä lukuun ottamatta Tesla-hyökkäystä louhittiin Moneroa. Louhinnalla ansaitut summat vaihtelevat radikaalisti neljästä ja puolesta tuhannesta dollarista aina kolmeen miljoonaan dollariin asti. Kaikista hyökkäyksistä ei kuitenkaan saatu selville louhinnalla tienattua voittoa. Louhinnalla tienattu summa saatiin selville tutkimalla haittaohjelman lähdekoodia ja poimimalla sieltä hyökkääjän lompakon osoite. Osoitteen perusteella voitiin selvittää kaikki tätä tiettyä lompakkoa koskevat transaktiot. Kaikissa tapauksissa osoitetta ei saatu selville esimerkiksi haittaohjelmassa käytetyn vahvan hämäännyttämisen takia.

Hyökkäyksissä saastutettujen laitteiden valtava määrä kertoo siitä, että kryptokaappaukset ovat huomattava ongelma pilvipalveluille. Toisaalta isossa osassa näitä hyökkäyksiä käytettiin EternalBlue-haavoittuvuutta, joka on poikkeuksellisen vakava haavoittuvuus. Vaikka vanhoja tietoturva-aukkoja paikataan kovaa vauhtia, uusien aukkojen ilmestyminen on vain ajan kysymys.

5.3.1 Smominru

EternalBlue-haavoittuvuutta hyväksikäyttävä Smominru saastutti elokuuhun 2019 mennessä yli 90 000 laitetta pääsääntöisesti Kiinassa, Taiwanissa, Venäjällä, Brasiliassa ja Yhdysvalloissa. Louhinnallaan se tuotti 1 500 000 dollaria. Smominrun onnistuttua saastuttamaan laite, se lataa isäntäpalvelimeltaan haitallisen hyötykuorman. Tämän hyötykuorman avulla Smominru esimerkiksi vakoilee kohteensa tietoja, varastaa tunnuksia ja muuta dataa. Poikkeuksellisesti Smominru myös lataa muun muassa näytönohjaimia valmistavan NVIDIA-yrityksen CUDA-kirjaston (engl. Compute Unified Device Architecture), joka mahdollistaa tavallista tehokkaamman louhinnan näytönohjaimella. [34], [36]

5.3.2 CryptoSink

CryptoSink käyttää hyökkäyksissään XMRig-louhijaa. Hyökkäykset kohdistuvat sekä Windows- että Linux-alustoille. Se tuotti vain 4 500 dollaria. Hyökkäykset tapahtuvat hyväksikäyttämällä Elastic-yrityksen luoman Elasticsearch-hakusysteemin [37] tietoturva-aukkoa. Hyökkäys tapahtuu lähettämällä kohteisiin haitallisia HTTP-pyyntöjä (engl. Hypertext Transfer Protocol). Sopivan kohteen löytyessä kohdealustalle ladataan hyötykuorma, joka sisältää kryptolouhijan ja takaoven avaavan haittaohjelman. CryptoSink myös asentaa itsensä uudestaan, muokkaamalla Linux-alustoilla poistokomento rm:n toimintaa. CryptoSinkin huomattiin myös havaitsevan muut kryptolouhijat kohdealustallaan. Havaittuaan toisen kryptolouhijan CryptoSink uudelleenohjaa niiden liikenteen lopettaen niiden toiminnan kokonaan. [34], [38]

5.3.3 Zealot

Zealot käyttää hyväkseen EternalBlue- ja EternalSynergy-haavoittuvuuksia. Se tuotti 8 500 dollaria. Zealot otti kohteekseen Apache HTTP-palvelimien Struts-ohjelmistoja. Zealot louhii Moneroa erityisellä Apache Struts -palvelimille suunnitellulla algoritmilla. Zealotista tekee erityisen sen lähdekoodin monimutkaisuus ja useat hienostuneet ominaisuudet. Zealot myös käyttää vahvaa hämäännyttämistä peitelläkseen hyökkäyksensä. Poikkeuksellisesti Zealot vain louhii laitteellaan eikä lataa laitteelle usean muun vastaavan kryptolouhijan tavoin muita haittaohjelmia. [34], [39]

5.3.4 Adylkuzz

Adylkuzz hyväksikäyttää Smominrun tavoin EternalBlue-haavoittuvuutta. Adylkuzzin kohteena ovat yrityskäytössä olevat Windows-pohjaisia laitteita sisältävät verkot ja palvelimet. Adylkuzz levisi pääsääntöisesti Venäjällä, Ukrainassa, Taiwanissa, Brasiliassa ja Intiassa. Muiden kryptolouhijoiden tavoin Adylkuzz louhii Moneroa ja tuotti 22 000 dollaria. Adylkuzz on kuitenkin yhteydessä komentopalvelimelleen, josta käsin on mahdollista käskyttää saastuneita laitteita lataamaan ja suorittamaan hyökkääjän haluamia ohjelmia. Adylkuzzin ei ole kuitenkin huomattu tekevän muuta kuin louhintaa kaappaamillaan laitteilla. Mielenkiintoisena lisäyksenä Adylkuzz estää muita haittaohjelmia hyväksikäyttämästä EternalBlue-haavoittuvuutta sulkemalla tälle haavoittuvuudelle oleellisen palvelun saastuttamaltaan laitteeltaan. Tällaista haittaohjelmien valtataistelua kohdelaitteensa herruudesta nähtiin myös Smominrun yhteydessä. [40]

5.3.5 WannaMine

WannaMine hyväksikäyttää Oraclen WebLogic -palvelimista löytynyttä tietoturva-aukkoa ja EternalBlueta leviämisessään. WannaMinen kohteena ovat erilaiset Oraclen WebLogic -ohjelmaa käyttävät palvelimet, jotka ovat suurimmaksi osaksi yrityskäytössä. Lokakuuhun 2017 mennessä WannaMine oli hyökännyt yli 75 000 laitteeseen. WannaMine samankaltaisista louhijoista poiketen skannaa kohdeverkkonsa portteja löytääkseen lisää haavoittuvaisia kohteita ja uusia leviämiskohteita. [34], [36]

5.3.6 RubyMiner

Useaa HTTP-palvelimien tietoturva-aukkoa hyväksikäyttäen RubyMiner saastutti noin 700 webpalvelinta ympäri maailmaa. Kohdealustoillaan RubyMiner louhi monen muun kryptolouhijan tavoin Moneroa käyttäen XMRig-louhijaa. Ylläpitääkseen louhintaansa, RubyMiner muokkaa kohdealustaansa siten, että se lataa itsensä uudelleen tunnin välein saastuttamalleen alustalle. [41], [42]

5.3.7 Tesla-hyökkäys

Tesla-hyökkäys on siinä mielessä poikkeuksellinen, että tässä hyökkäyksessä ei käytetty mitään tietoturva-aukkoa hyödyksi. Tuntemattomaksi jäänyt hyökkääjä huomasi Teslan eräältä Amazonilta ostamalta pilvipalvelupalvelimelta puuttuvan salasanan kokonaan. Sisään päästyään hyökkääjä yritti piilotella hyökkäystään mahdollisimman paljon, jotta palvelimelle asennettu kryptolouhija ei jäisi kiinni. CloudFlare-yrityksen tarjoamaa IP-suojaa käytettiin piilottamaan kryptolouhijan käyttämän louhinta-altaan oikea IP-osoite. Tämä esti mahdollisen mustalistaukseen perustuvan torjunnan. Louhijan käyttämää prosessoritehoa oli myös rajoitettu, jotta louhija herättäisi vähemmän huomiota. [43]

5.3.8 Jenkins Miner

Jenkins-järjestelmää käyttäviä palvelimia kohteeksi ottava Jenkins Miner käyttää hyökkäyksissään Moneroa louhivan XMRig-louhijan ja etäkäyttötroijalaisen (Remote Access Trojan, RAT) yhdistelmää. Jenkins Miner käytti hyväkseen Jenkins-järjestelmän tietoturva-aukkoa. Jenkins Minerin keräämän tuoton arvo huomattiin olevan yli kolme miljoonaa dollaria eli selvästi eniten taulukon 1 listalla. [44]

5.3.9 Coinreg Monero

Coinreg Moneron kohteena olivat eteläamerikkalaisen autoja valmistavan yrityksen palvelimet. Hyökkäys tapahtui maalis-huhtikuussa vuonna 2018. Hyökkäykseen käytettiin Windows-pohjaisilta alustoilta löytyvän PowerShell-työkalun skriptejä. Hyökkäyksessä kohdelaitteelle ujutettiin Coinreg Monero -louhija ja kirjautumistunnuksia varastava avointa lähdekoodia oleva Mimikatz-työkalu. Varastetuilla kirjautumistunnuksilla hyökkääjät levittivät haittaohjelmiaan eteenpäin yrityksen verkossa. Hyökkääjät myös varastivat yritykseltä erinäistä dataa. [36]

5.3.10 Norman

Tietoturvaratkaisuja tarjoava yritys Varonis [45] löysi eräästä yrityksestä uuden kryptolouhijan, jolle annettiin nimeksi Norman. Melkein jokainen yrityksen palvelimista ja tietokoneista oli Normanin saastuttama. Norman käytti XMRig-louhijasta muokattua, paremmin omaan käyttötarkoitukseensa sopivaa versiota. Muiden kryptolouhijoiden tavoin Norman yritti vältellä kiinnijäämistään vahvalla hämäännyttämisellä. Se käytti myös erillistä DNS-nimipalvelinta peitelläkseen yhteydenottonsa isäntäpalvelimelleen. Isoin eroavaisuus muihin kryptolouhijoihin verrattuna oli se, että Norman asennutti itsensä saastuttamilleen laitteille käyttämällä avointa lähdekoodia olevaa Windows-pohjaista asennustyökalua. Tällä samalla asennustyökalulla voidaan asentaa myös aivan tavallisia ohjelmia. Sitä ei juurikaan oleva tavattu käytettävän haittaohjelmien yhteydessä. Norman osasi myös sulkea oman prosessinsa, jos laitteella avattiin tehtävienhallintatyökalu. Tehtävienhallintatyökalun sulkeuduttua, Norman käynnisti itsensä uudelleen. [46]

5.3.11 Graboid

Graboidin kohteena olivat poikkeuksellisesti Docker-ohjelmiston kontit. Näissä konteissa voidaan suorittaa erilaisia ohjelmistoja, ja tietyn verkon kontit voivat kommunikoida keskenään. Graboid saastutti yli 2 000 suojaamatonta Docker-konttia. Tavalliset yrityskäyttöön suunnitellut tietoturvaohjelmistot eivät tarkkaile konteissa tapahtuvaa toimintaa ja käsiteltävää dataa. Näin ollen Graboid pysyi huomaamattomana pitkään. Saastutettuaan yhden kontin Graboid tutki muut samassa verkossa toimineet kontit etsien muita suojaamattomia kontteja ja niiden löytyessä levisi niihin jatkaen eteenpäin etenemistä. [47]

5.4 Muut kohteet

Muita kohteita luvattomalle kryptolouhinnalle ovat esimerkiksi yliopistojen ja tutkimuslaitosten supertietokoneet. Supertietokoneet ovat erittäin oivallisia kryptolouhinnalle niiden

tarjoaman valtavan laskentatehon takia. Toisaalta niiden käyttöä valvotaan tarkasti väärinkäytön varalta. Kuitenkin silloin tällöin opiskelijoita, tutkijoita ja työntekijöitä jää kiinni tällaisten supertietokoneiden luvattomasta käytöstä.

Vuonna 2014 Yhdysvalloissa eräs tutkija käytti luvattomasti kahdella eri yliopistokampuksella sijaitsevia supertietokoneita Bitcoinin louhintaan. Tutkija ehti tienata louhinnallaan 8 000–10 000 dollaria ennen kiinnijäämistään. Tutkija yritti perustella louhinnan kuuluvan osaksi tekemäänsä tutkimusta, mutta väitteelle ei löytynyt perää. Teostaan tutkija menetti valtionlaajuiset tutkijanlupansa. [48]

Silloin tällöin myös opiskelijoita jää kiinni luvattomasta louhinnasta yliopistojen tietokoneilla. Esimerkiksi Harvardissa opiskellut nuori koki omalla tietokoneellaan kryptolouhinnan tehottomaksi ja päätti näin käyttää yliopiston tietokoneita louhintaan [49]. Toisessa esimerkkitapauksessa Lontoossa sijaitsevassa Imperial College -yliopistossa eräs opiskelija käytti yliopistonsa tietokonelaboratoriota useana iltana kryptolouhintaa varten [50].

6. KRYPTOKAAPPAUSTEN HAITAT

Selainpohjaisten kryptokaappausten isoin haitta uhreille on nettiselaimen ja samalla koko tietokoneen tai muun käytettävän laitteen hidastuminen. Toisaalta Hong *et al.* esittävät [23], että useat kryptokaappaushaittaohjelmat rajoittavat prosessin käyttöä välttääkseen kiinnijäämistään. Tiedostopohjaisessa kryptokaappauksessa on selainpohjaisten kaappausten tapaan sama haitta tietokoneen hidastumisen muodossa, jos louhija käyttää prosessoria louhintaan. Prosessorin raskas hyväksikäyttö myös pienentää sen elinikää [51]. Näytönohjainpohjainen louhinta rasittaa vain näytönohjainta, ja tällaisen rasituksen huomaa helposti vasta tilanteessa, jossa käyttäjä tarvitsisi itse näytönohjaintehoa jonkin sovelluksen suorittamiseen. Tiedostopohjaisten kryptokaappausten mukana saattaa usein tulla muita haittaohjelmia, ja hyökkääjä saattaa myös jättää uhrinsa laitteelle takaoven myöhempää varten. Uhrin laite saatetaan myös valjastaa bottiverkkokäyttöön.

Tässä luvussa käydään aluksi läpi prosessorin käyttöön liittyvät haitat. Sen jälkeen käydään läpi lähinnä älypuhelimia koskeva laitteiston hajoaminen. Sitten käydään läpi kryptokaappausten yhteydessä tulevat muut haittaohjelmat. Tämän jälkeen käydään läpi muiden haittaohjelmien yhteydessä mahdollisesti tulevaa bottiverkko-ongelmaa. Lopuksi käydään läpi lähinnä yrityksiä koskeva kryptokaappausten yhteydessä varastettu tieto.

6.1 Prosessorin käyttö

Kryptokaappauksista aiheutuvista haitoista helpoiten huomattavissa on prosessorin käyttö. Prosessorin käyttö ilmenee käytettävän laitteen suorituskyvyn hidastumisena ja pahimmillaan totaalisena jumiutumisena. Jos prosessorin rajulle käytölle ei ole mitään järkevää selitystä, tilanteeseen saattaa olla syypäänä kryptokaappaus. Toisaalta joissakin tapauksissa kryptolouhijat on asetettu käyttämään vain tietyn verran saatavilla olevasta prosessointitehosta, jotta vältytään kiinnijäämiseltä.

Selainpohjaisissa kryptokaappauksissa Hong *et al.* huomasivat [23], että heidän keräämistään kryptolouhijanäytteistä 70 % rajoitti jollakin tavalla prosessorin käyttöä. Tämä rajoite oli välillä 3–90 %. Yksittäiseen kryptolouhijaan asetettu rajoite ei kuitenkaan vaihtele satunnaisesti, vaan rajoitteen arvo on kiinteä. Tämä rajoite tarkoittaa sitä, että osa kryptolouhijoista käyttää vain 3 % prosessorin tehoista louhintaan. Louhijat, jotka käyttivät 90 % prosessorin tehoista todennäköisesti rampauttivat uhrinsa laitteen. Tämän rajoitteen ideana on vähentää kiinnijäämisriskiä, mutta toisaalta luoda mahdollisimman

paljon tuottoa. Nämä rajoitteet osasivat myös ottaa huomioon nykyaikaisten prosessorien useat säikeet ja ytimet jakamalla louhintakuorman yhden säikeen tai ytimen sijasta usealle.

Joissakin kryptokaappauksissa hyökkääjät ovat asettaneet kryptolouhijansa louhimaan käyttäen 100 % prosessorin tehoista. Vaikka tämä tuottaa hetkellisesti isoja tuottoja, se ei ole pitkäkestoisesti järkevää. Uhri ei pysty käyttämään tietokonettaan tai vastaavaa alustaansa lainkaan kryptolouhijan viedessä kaiken prosessoritehon. Näin ollen uhri huomaa nopeasti jonkin olevan vialla laitteessaan. Joissakin tapauksissa täydellä teholla suoritettu louhinta on johtanut prosessorien hajoamiseen ylikuumenemisen takia. [52]

Papadopoulos *et al.* esittävät tutkimuksessaan [27], että kryptolouhijan sisältämällä nettisivustolla vierailuminen käyttää 59-kertaisesti enemmän prosessoritehoa kuin tavallisten mainosten sisältämällä nettisivustolla vierailu. Samalla laitteen lämmöntuotto kasvoi 53 % ja virran kulutus oli kaksinkertainen.

6.2 Laitteiston hajoaminen

Kryptokaappaus laskee aina kohdelaitteistonsa suorituskykyä varaamalla itselleen joko prosessori- tai näytönohjainkapasiteettia kryptolouhijasta riippuen. Koska nykyaikaisilla älypuhelimilla on nettiselain, selainpohjaiset kryptolouhijat toimivat myös niillä.

Android-pohjaisilta laitteilta löydettiin vuonna 2017 kryptolouhintahaittaohjelma, jolle annettiin nimeksi Loapi. Se louhi kryptovaluutta Moneroa niin aggressiivisesti, että osa sen saastuttamista laitteista hajosi fyysisesti. Loapia testattiin tietoturvayhtiö Kasperskyn laboratoriossa. Kahden päivän louhinnan jälkeen puhelimen akku pullistui, mikä hajotti puhelimen kuoret. [26]

6.3 Muut haittaohjelmat

Selainpohjaisissa kryptokaappauksissa hyökkääjien ei ole kannattavaa ujuttaa uhreilleen muita haittaohjelmia, koska niistä jää helpommin kiinni. Pelkkää kryptolouhimista on vaikeaa huomata saastuneella nettisivulla vierailtaessa, mutta tiedoston automaattinen latautuminen on helpompi huomata. Pelkkä tiedoston automaattinen lataaminen uhrin laitteelle ei vielä riitä, vaan se pitäisi myös suorittaa.

Tiedostopohjaisissa kryptokaappauksissa tilanne on kuitenkin toisenlainen. Aiemmin esitetyssä tiedostopohjaisen kryptokaappauksen toimintamallissa (Kuva 6) nähdään,

että hyökkääjät avaavat usein takaoven uhrinsa laitteelle tiedostopohjaisen kryptolouhijan suoritusvaiheessa. Näin ollen hyökkääjä voi halutessaan ladata ja suorittaa uhrinsa laitteella muita haittaohjelmia. [28]

Osana tiedostopohjaista kryptokaappausta uhri saattaa joutua osaksi bottiverkkoa. Bottiverkko tarkoittaa haittaohjelmalla saastuneista laitteista koostuvaa verkostoa, jota hallitsee jokin tietty taho. Näitä saastuneita laitteita hallinnoidaan niin sanotusta komentokeskuspalvelimesta käsin. Mitä enemmän saastuneita laitteita bottiverkossa on, sitä tehokkaampi bottiverkko on hyökkääjän näkökulmasta. Bottiverkkoja käytetään esimerkiksi palvelunestohyökkäyksiin, roskapostitukseen, uhrien tietojen keräämiseen ja kryptolouhintaan. Varsinkin kryptolouhinta on otollista hyökkääjälle, koska se ei vaadi bottiverkon hallitsijalta juurikaan toimenpiteitä ja se on huomaamatonta toimintaa uhrien laitteilla. [53]

6.4 Tiedon varastaminen

Tiedostopohjaisissa kryptokaappauksissa kryptolouhijan mukana tulee yleensä muita haittaohjelmia. Viimeistään hyökkäyksen yhteydessä yleensä avattu takaovi mahdollistaa muiden haittaohjelmien ujuttamisen uhrin laitteelle. Yksittäisen yksityishenkilön laitteella ei todennäköisesti ole varastamisen arvoista dataa. Toisaalta esimerkiksi eri palveluiden käyttäjätunnusten varastaminen on mahdollista. Yleensä kuitenkin tiedon varastaminen kryptokaappausten tapauksessa koskee yrityksiä ja pilvipalveluita.

Esimerkiksi aikaisemmin mainittu eteläamerikkalaisen yrityksen kohteeksi ottanut Coinreg Monero on hyvä esimerkki tietoa varastavista kryptokaappauksista. Tässä tapauksessa kryptokaappauksen kohteena oli nimenomaan tietty yritys. Yrityksen verkossa louhittiin kryptovaluuttoja, mutta samalla yrityksen verkosta varastettiin erinäistä dataa. Hyökkäyksestä ei selvinnyt, oliko hyökkäyksen motiivina kryptolouhinta vai tiedon varastaminen. Toinen esimerkki tiedon varastamisesta on Tesla-hyökkäys, jossa varastettiin myös arvokasta Teslan kehitysdataa.

Kryptokaappaukset niin kuin muutkin haittaohjelmahyökkäykset tulee suunnitella etukäteen. Tämä tarkoittaa sitä, että hyökkääjän tulee päättää etukäteen, haluaako hän harrastaa pelkkää kryptolouhintaa vai haluaako hän myös levittää laitteille muita haittaohjelmia tai varastaa niiltä dataa. Mitä enemmän haittaohjelmia hyökkääjä ujuttaa uhrien laitteille, sitä todennäköisemmin siitä jää kiinni. Tämä johtuu siitä, että haittaohjelmat tekevät usein muutoksia järjestelmässä, ja tästä jää aina merkintä johonkin. Laite saattaa myös toimia haittaohjelmista johtuen epätavallisesti, minkä laitteen käyttäjä saattaa huomata. Pelkkä kryptolouhija ei tee muutoksia laitteen rekisteriarvoihin tai tiedostoihin.

Kryptolouhijat jäävät usein kiinni, kun laitteen prosesseja ruvetaan tutkimaan ja huomataan, että jokin prosessi vie huomattavasti prosessointitehoa ilman järkevää syytä.

7. TORJUNTA

Tavanomaiset kryptokaappausten torjuntamenetelmät luottavat usein prosessorin tai näytönohjaimen kulutuksen seurantaan. Selainpohjaisia kryptokaappauksia yritetään usein torjua mustalistaamalla tunnettuja kryptolouhinnassa käytettyjä nettisivustoja. Nämä metodit eivät kuitenkaan ole aina kovinkaan tarkkoja, ja esimerkiksi raskaat sovellukset saattavat virheellisesti joutua merkityksi kryptolouhijoiksi. Rikolliset myös yrittävät jatkuvasti tehdä louhijoistaan vaikeampia huomata. [54]

Haittaohjelmien torjuntametodit voidaan lajitella kahteen kategoriaan: staattiseen ja dynaamiseen analysointiin. Staattisessa analysoinnissa etsitään tiettyjä haittaohjelmille tyypillisiä piirteitä ja sormenjälkiä tiedostoista. Näitä piirteitä ja sormenjälkiä verrataan aikaisemmin tunnistettujen haittaohjelmien piirteisiin ja sormenjälkiin. Dynaamisessa analysoinnissa tutkitaan jo käynnissä olevien ohjelmien ja prosessien piirteitä ja käyttäytymistä. [55]

Tässä luvussa käydään aluksi läpi tietoturvavalppaus, joka sisältää yleisiä taitoja haittaohjelmia ja samalla kryptokaappauksia vastaan suojautumiselta. Seuraavaksi käsitellään mustalistaus, joka tarkoittaa jo tunnettujen kryptolouhintaan assosioitujen osoitteiden mustalistaamista ja tällä tavalla kryptokaappausten estämistä. Sen jälkeen käsitellään suorituskyky- ja verkkoanalyysi, jotka ovat jo käynnissä olevien kryptokaappausten havainnoimiseen suunniteltuja torjuntatapoja. Sitten pohditaan kryptokaappauksilta suojautumista yritysten näkökulmasta. Tämän jälkeen esitellään vielä kaksi työkalua kryptokaappauksilta suojautumiseen: RADS ja MineGuard. Lopuksi käsitellään vielä perinteisten virustentorjuntaohjelmistojen roolia kryptokaappauksilta suojautumisessa.

7.1 Tietoturvavalppaus

Tärkein suojautumistapa kryptokaappaukselta ja samalla muilta haittaohjelmilta on tietoturvavalppaus. Paraskaan virustentorjuntaohjelma tai erityinen kryptokaappauksia vastaan luotu työkalu ei suojaa kryptokaappauksilta, jos laitteen käyttäjän tietoturvavalppaus ei ole kunnossa. Tietoturvavalppaus yhdistää tietoturvataidot, asennoitumisen omaan tietoturvaan ja tietoisuuden tietoturvaan liittyvistä uhkista. Tiedostopohjaiset kryptokaappaukset voidaan estää täysin, jos käyttäjä ei suorita lataamaansa hyötykuormaa. Eräs tavanomainen uhrin hämäystapa tiedostopohjaisissa kryptokaappauksissa on naamioida ladattava tiedosto toisentyyppiseksi tiedostoksi. Esimerkiksi sähköpostin liitetiedostona tuleva ”dokumentti.txt.exe” saattaa näyttää nopealla vilkaisulla tekstitiedostolta,

vaikka sen oikea tiedostopääte on .exe eli se onkin suoritettava tiedosto. Toinen yleinen haittaohjelmalevityskanava on Microsoft Wordin tiedostoissa olevat haitalliset makrot. Tällaisten huijausten huomaaminen ei ole vaikeaa edistyneemmälle tietotekniikkaan perehtyneelle henkilölle, mutta tietoteknisesti ei niin orientoituneelle se onkin jo vaikeampaa. On siis tärkeää, että varsinkin yrityksissä koulutetaan henkilöstö ymmärtämään tavanomaiset haittaohjelmien yhteydessä olevat hämäysyritykset. Toisaalta yrityksissä olisi myös hyvä rajata käyttöoikeuksia siten, että kuka tahansa työntekijä ei voi suorittaa mitä tahansa tiedostoja varsinkaan tärkeillä laitteilla.

Tietoturvavalppaus ei yksinään riitä suojautumaan kryptokaappauksilta ja muilta haittaohjelmilta. Jo käynnissä olevaa kryptokaappausta on joskus todella vaikea huomata, koska iso osa kryptolouhijoista peittelee jälkiään tehokkaasti. Siksi tarvitaankin edistyneempiä ja tehokkaita ratkaisuja.

7.2 Mustalistaus

Hong *et al.* esittivät julkaisussaan [23], että pelkkä yksinkertainen kryptokaappauksista tunnettujen skriptien ja verkkosivustojen mustalistaus ei ole riittävää tulevaisuuden varalta. Nykyhetkellä se on hyvä alku kryptokaappausten torjumisessa, mutta rikolliset kehittävät jatkuvasti uusia kryptolouhintaskriptejä ja ottavat käyttöön uusia nettisivuja. Tämä tarkoittaa sitä, että mustalistaus jää auttamatta jossakin kohtaa jälkeen. Esimerkiksi kryptolouhintaskriptillä Minr on mahdollista tehdä automaattista lähdekoodinsa muokkaamista mustalistauksen kiertämiseksi ja mahdollisten virustentorjuntaohjelmistojen hämäännyttämiseksi [20].

Mustalistauksen parantamista varten Hong *et al.* kehittivät uuden *CMTracker*-nimisen ohjelman. Tämän ohjelman ideana oli kerätä dataa nykyisistä tunnetuista kryptokaappausnettisivustoista. Ohjelman avulla kerättiin 2770 kryptokaappausnäytettä, kun vierailtuja nettisivustoja oli 850 000. Näistä kerätyistä näytteistä 53,9 % oli täysin uusia ja tunnistamattomia näytteitä jo olemassa olevien vastaavien ohjelmien keräämiin näytteisiin verrattuna. Ohjelma myös keräsi tietoa louhintaskripteistä eri nettisivustoilla. Hong *et al.* kuitenkin painottivat, että heidän ohjelmansa ei ratkaise tulevaisuuden kryptokaappausongelmaa, mutta ohjelman keräämää dataa voitaisiin hyödyntää tulevaisuudessa. [23]

Selainpohjaisia kryptokaappauksia vastaan on olemassa selainten omista laajennuskaupoista ladattavia kryptokaappausten estäviä laajennuksia. Nämä laajennukset perustuvat pääsääntöisesti mustalistaukseen eli ne estävät yhteyden tunnettuihin kryptolouhintaosoitteisiin. Esimerkkejä tällaisista laajennuksista ovat NoCoin [56] ja NoMiner [57].

Tämänkaltaisten mustalistaukseen perustuvien lisäosien kiertäminen hyökkääjän näkökulmasta on kuitenkin helppoa. Saad *et al*. testasivat [17] aluksi näiden laajennusten toimivuutta laatimalla oman Coinhiven louhintaskriptiin perustuvan louhintaskriptin ja ujuttamalla sen heidän omalle testisivustolleen. Molemmat näistä selainlaajennuksista huomasivat kryptolouhinnan ja estivät sen. Sen jälkeen skriptistä vaihdettiin suoraan Coinhiveen viittaava osoite toiseen osoitteeseen, joka uudelleenohjaa pyynnön Coinhiven osoitteeseen. Tämän jälkeen selainlaajennuksia testattiin uudelleen ja huomattiin, että ne eivät enää estäneet louhintaa. Näin osoitettiin, että mustalistaukseen perustuva kryptokaappausten esto on todella helposti kierrettävissä.

Mustalistaukseen perustuvissa selainlaajennuksissa voidaan myös yhdistää mustalistaus ja käyttäytymiseen perustuva torjunta. Razali ja Shariff kehittivät CMBlock-nimisen [58] mustalistaukseen ja käyttäytymiseen perustuvan selainlaajennuksen. Tämän työkalun ideana oli yhdistää jo olemassa oleva mustalistaukseen perustuva kryptokaappausten havainnointi ja kryptolouhinnassa tavanomaisesti esiintyvät piirteet, jotta saataisiin mahdollisimman tehokas suojausmekanismi selainpohjaisia kryptokaappauksia vastaan. CMBlock havaitsee nettisivuston HTML-koodiin ujutetun kryptolouhintaskriptin. CMBlock tunnistaa myös tilanteet, joissa louhintaskripti käyttää uudelleenohjauspalvelinta kiertääkseen tavallisen mustalistaukseen perustuvan torjunnan. Tässä työkalussa käytetty mustalistaustoiminnallisuus on sama kuin NoCoin-selainlaajennuksessa, koska se on avointa lähdekoodia ja sen on huomattu olevan tehokas mustalistausmetodi. CMBlock-työkalua testattiin vain muutamalla nettisivustolla, joissa se toimi halutulla tavalla. Kryptolouhintaskriptejä on kuitenkin useita erilaisia, minkä takia CMBlock:ia olisi pitänyt testata kattavammin. Työkalun tekijät toisaalta toivovatkin, että työkalu otettaisiin jatkokehitykseen, koska sillä on lupaava alku.

7.3 Suorituskykyanalyysi

Suorituskykyanalyysi perustuu laitteen suorituskyvyssä tapahtuviin isoihin muutoksiin. Pelkästään isojen suorituskykymuutosten perusteella tehty prosessien kryptolouhijoiksi merkitseminen ja sulkeminen on myös virhealtista, ja vääriä prosesseja tulee helposti suljetuksi. Sekä suorituskyvyssä tapahtuvien normaalien muutosten että ennalta tunnettujen kryptolouhijoiden tunnistaminen vaatii taustatietoa. Tällaisen taustatiedon hankkiminen on vaikeaa. [59]

Suorituskykyanalyysin perusideana on tutkia laitteen suorituskykyä ja huomata, jos suorituskyvyssä tapahtuu ennalta määritetyn rajan ylitys. Suorituskykyanalyysi ei tällaisenaan toimi, koska se ei ottaisi huomioon esimerkiksi raskaita videon striimauspalveluita.

Jotkut haittaohjelmat myös rajoittavat tarkoituksella käyttämiänsä resursseja välttääkseen kiinnijäämisensä. Suorituskykyanalyysi tarvitseekin avukseen esimerkiksi koneoppimista, jotta kryptolouhijat jäävät kiinni tehokkaasti ilman vääriä havaintoja. [21]

Gomes *et al.* [21] kehittivät koneoppimiseen perustuvan selainpohjaisten kryptolouhijoiden torjuntametodin. Aluksi he kävivät eri nettisivustoja läpi ohjelmointikieli Pythonilla ohjelmoidulla skriptillä. Skripti latasi vierailluilta nettisivustoilta sivustojen käyttämät skriptit, jotta ne voitaisiin myöhemmin syöttää koneoppimisalgoritmiin. Jokaiselta vierailtulta nettisivustolta kirjattiin ylös sivuston käyttämä prosessorin kulutus. Vertailukohteeksi kerättiin myös tavallisen kryptolouhijavapaan nettisivuston prosessorinkulutus. Sitten vierailtiin myös tarkoituksella nettisivustolla, jossa tiedettiin olevan kryptolouhija. Näin saatiin vertailuun toinen ääripää. Sopivan koneoppimisalgoritmin löytäminen tähän tarkoitukseen osoittautui työlääksi. Eri koneoppimisalgoritmit toimivat joissain osa-alueissa paremmin kuin toiset, mutta mikään algoritmeista ei ollut täydellinen. Parhaimmaksi valitun algoritmin tarkkuus oli 99.7 % kryptokaappaajien löytämiseen nettisivustoilta. Samalla algoritmi ei antanut yhtään väärää osumaa nettisivustoista, joiden tiedettiin sisältävän kryptolouhija.

7.4 Verkkoanalyysi

Kryptolouhijat ovat yhteydessä louhinta-altaaseensa käyttämällä jotakin tiettyä tähän tarkoitukseen sopivaa protokollaa. Yksi käytetyimmistä tällaisista protokolloista on Stratum. Tämä protokolla toimii TCP-protokollan (engl. Transmission Control Protocol) päällä käyttäen satunnaisesti valittua porttia, joka tekee porttipohjaisen seurannan mahdottomaksi. Stratum-protokollan viestiessä asiakkaan (tässä tapauksessa kryptolouhijalla saastunut laite) ja kohdepalvelimen välillä viestiketjussa esiintyy viisi viestiä:

1. Mining.subscribe: Yhteyden aloitusviesti, jossa asiakas ilmoittaa palvelimelle olevansa valmis louhintaan.
2. Mining.set_difficulty: Palvelin ilmoittaa louhinnan ”vaikeusasteen”.
3. Mining.authorize: Asiakas lähettää palvelimelle tunnistetietoja.
4. Mining.notify: Palvelin ilmoittaa asiakkaalle louhinnassa käytettävän datan.
5. Mining.submit: Asiakas lähettää palvelimelle louhinnassa löytyneen datan. [60]

Munoz *et al.* analysoivat [60] tätä Stratum-protokollan siirtämää dataa. He huomasivat, että dataa siirretään tasaiseen tahtiin ja palvelimelta lähetään huomattavasti enemmän dataa asiakkaalle kuin asiakkaalta lähetetään dataa palvelimelle. He myös generoivat paljon louhinnassa käytettävää dataa louhimalla itse eri kryptovaluuttoja. Tästä datasta

ja Stratum-protokollan käyttäytymismallista he loivat koneoppimista hyödyntäen algoritmin havaitsemaan kryptokaappauksia. Omissa testeissään he saivat algoritmilleen noin 90 % tarkkuuden. Heidän algoritminsa on myös kevyt kuluttamiensa resurssien osalta, ja algoritmi on myös jatkokehitettävissä yhä tarkemmaksi.

7.5 Torjunta yritysten näkökulmasta

Yritysten näkökulmasta on tärkeää aluksi selvittää, kuinka otollisia kohteita kryptokaappauksille yrityksen verkko ja laitteet ovat. Yritykset, joilla on jonkinlainen kirjautumisportaali, ovat erittäin otollisia kohteita kryptokaappauksille nopean haittaohjelmalevitysmahdollisuuden takia watering hole -hyökkäyksen avulla. [29] Keskeisen kirjautumisportaalin kautta levitetyn haittaohjelman estämiseksi on tärkeää rajata käyttäjien käyttöoikeuksia. Yrityksen laitteita ja verkkoa tulee myös valvoa valvontatyökaluilla. Yksittäisen laitteen saastuttua on tärkeää reagoida nopeasti haittaohjelman leviämisen estämiseksi. Samoilla valvontatyökaluilla voidaan myös havaita mahdollisten epärehellisten työntekijöiden harrastama kryptolouhinta. Laitteiden säännöllinen varmuuskopiointi on myös hyvä muistaa, koska tiedostopohjaisten kryptolouhijoiden mukana tulee usein muitakin haittaohjelmia. Näitä muita haittaohjelmia on usein vaikeampi poistaa verrattuna pelkkiin kryptolouhijoihin. Palauttamalla laite edelliseen ja varmistettuun puhtaaseen tilaan voi olla nopeampi ja helpompi tapa puhdistaa saastumiset.

7.6 RADS – Pilvipalveluille suoja

Barbhuiya *et al.* kehittivät pilvipalveluille suojausmekanismin, jonka nimi on RADS. RADS on reaaliaikainen poikkeavuuksien havainnointisysteemi pilvipalveluille. RADS:n ideana on tunnistaa pilvipalveluihin kohdistuvia kryptokaappaushyökkäyksiä, sekä palvelunestohyökkäyksiä. RADS:n ideana on aluksi tunnistaa ja oppia jollekin pilvipalvelulle tyypillinen nettiliikenne ja prosessorin kulutus. [61]

RADS luo hyvän pohjan tehokkaalle pilvipalvelusuojalle, mutta sen isoin ongelma on se, että se ei tee selvää eroa palvelunestohyökkäyksen ja kryptokaappauksen välillä. RADS tunnistaa kryptokaappaukset korkean prosessorin kulutuksen perusteella ja palvelunestohyökkäykset korkean nettiliikenteen perusteella. Se ei kuitenkaan ota huomioon kryptokaappauksissa tapahtuvaa nettiliikennettä. Myöskään kryptokaappaushyökkäyksiä usein kylkiäisinä tulevia muita haittaohjelmia ja takaovimahdollisuutta RADS ei ota huomioon. RADS olettaa kryptokaappausten käyttävän kaiken tai lähes kaiken saatavilla

olevasta prosessoritehosta. Joissakin kryptokaappauksissa prosessorin käyttöä rajoitetaan ja näin ollen tämän kaltaiset hyökkäykset jäisivät kokonaan huomaamatta RADS:n toimesta. [34]

7.7 MineGuard

Tahir *et al.* kehittivät uudenlaisen työkalun, *MineGuardin*, [32] tiedostopohjaisten kryptokaappausten havaitsemiseen. Työkalu soveltuu niin yksityishenkilöiden käyttöön kuin yritys- ja pilvipalvelukäyttöönkin. MineGuardin ideana on seurata nykyaikaisten prosessoreiden sisältämää HPC-laskuria (engl. Hardware performance counter). Kaikkien kryptovaluuttojen louhinta muuttaa HPC:n arvoa radikaalisti, mikä voidaan havaita MineGuardilla. HPC:n arvoa ei voi pienentää, joten hyökkääjät eivät voi sen arvoa laskemalla piilottaa toimiaan. Toisaalta hyökkääjät voivat säätää kryptolouhijansa louhimaan pienillä tehoilla, mikä näkyy vain pienenä muutoksena HPC:n arvossa. Tällä tavoin hyökkääjät voivat yrittää piilottaa kryptokaappauksensa MineGuardilta. RADS:n tavoin myöskään MineGuard ei ota huomioon kryptokaappauksissa mahdollisesti mukana tulevia muita haittaohjelmia.

7.8 Virustentorjuntaohjelmistojen tehottomuus

Virustentorjuntaohjelmistojen tarkoituksena on havaita ja neutralisoida haittaohjelmia. Tämä tapahtuu käyttämällä erilaisia tekniikoita, joista yksi yleisimmistä on tiedoston digitaaliseen sormenjälkeen perustuva havainnointi. Tässä tekniikassa tiedoston sisältöä verrataan tunnettujen haittaohjelmien sormenjälkien tietokantaan. Haittaohjelma voi olla sisällytetty toiseen tiedostoon, joten koko tiedosto tulee käydä läpi mahdollisen haittaohjelman havaitsemiseksi. Digitaaliseen sormenjälkeen perustuva havainnointi on hyödytön niin sanottuja nollapäivähaavoittuvuuksia vastaan. Tällaiset haavoittuvuudet ovat tietoturva-aukkoja, joille ei ole vielä saatavilla korjausta. Virustentorjuntaohjelmistot ovat myös voimattomia hämäännyttämistä harrastavia haittaohjelmia vastaan, koska tällaisten haittaohjelmien digitaalinen sormenjälki vaihtelee eri näytteiden kohdalla, vaikka itse haittaohjelma olisi sama. [62]

Ilmaiset virustentorjuntaohjelmistot eivät auta taistelussa selainpohjaisia kryptokaappauksia vastaan, koska ne eivät sisällä selainsuojauksia. Maksulliset virustentorjuntaohjelmistot kuitenkin yleensä sisältävät jonkinlaisen nettiselainsuojan. Tiedostopohjaisia kryptokaappauksia vastaan virustentorjuntaohjelmistot auttavat siinä tapauksessa, että käyttäjän laitteelleen lataama tiedosto sisältää jo aikaisemmin tunnistetun sormenjäljen,

joka viittaa kryptokaappaajaan. Uuden ja vain vähän aikaa levityksessä olevan kryptolouhijan sisältämää tiedostoa virustentorjuntaohjelmisto ei todennäköisesti havaitse, koska sitä ei ole vielä havaittu aikaisemmin, ja näin ollen sitä ei ole lisätty haittaohjelmatietokantaan. Jos ladatussa tiedostossa on käytetty hämäännyttämistä esimerkiksi salakirjoittamalla tai pakkaamalla tiedosto, virustentorjuntaohjelmisto ei havaitse sitä todennäköisesti siinäkään tapauksessa. [63]

8. POHDINTA

Kryptokaappausten estäminen on monimutkainen prosessi. Torjuntametodien ja -työkalujen tulee samaan aikaan olla sekä tehokkaita että tarpeeksi helppokäyttöisiä. Vaikka todella monimutkainen työkalu olisi tehokas, siitä ei ole iloa kuin tietoteknisesti edistyneille käyttäjille. Ideaali torjuntatyökalu olisi samaan aikaan helppokäyttöinen ja tehokas. Sellaiseen työkalun luomiseen tietysti pyritään, mutta sellainen on vaikea luoda. Esimerkiksi Stratum-protokollaa analysoineet Munoz *et al.* [60] kehittivät tehokkaan, mutta samalla melko vaikeakäyttöisen torjuntametodin. MineGuard [32] taas oli lähtökohtaisesti suunniteltu yritys- ja pilvipalvelukäytön lisäksi myös yksityiseen käyttöön, joten se on huomattavasi helppokäyttöisempi.

Tässä luvussa pohditaan aluksi, milloin kyseessä on kryptokaappaus ja milloin ei. Sen jälkeen käydään läpi tuore tapaus vuoden 2021 kesäkuulta, jossa virustorjuntaohjelmiston mukana tarjotaan käyttäjille mahdollisuus kryptolouhintaan.

8.1 Mikä on kryptokaappaus ja mikä ei?

Nettisivustojen ylläpitäjät ovat joutuneet taistelemaan sivustoillaan vierailevien käyttäjien mainostenesto-ohjelmia vastaan jo pitkään. Kryptovaluuttojen käytön helpottuessa ja niiden yleistyminen loi mainoksille korvaajan, nettisivustoilla tapahtuvan kryptolouhinnan. Mainosten sijaan sivustolla vieraileville saatetaan tarjota mahdollisuus tukea nettisivustoa hyväksymällä selaimessa tapahtuva louhinta. Näin sivuston omistaja saa rahaa. Tilanne on molemmille osapuolille hyvä: käyttäjän ei tarvitse katsoa ärsyttäviä mainoksia, ja sivuston omistaja saa todennäköisesti enemmän rahaa louhinnasta kuin pienistä mainostuloista.

Toisaalta kryptolouhinnassa tällaisessa tilanteessa on omat ongelmansa. Ymmärtääkö sivustolla vieraileva varmasti, mitä kryptolouhinta tarkoittaa ja mitä mahdollisia ongelmia siitä saattaa seurata? Sivustojen tulee myös ilmoittaa selkeästi tapahtuvasta louhinnasta ja käyttäjälle tulee antaa mahdollisuus kieltäytyä louhinnasta.

Yhdysvalloissa eräs selainpohjaiseen kryptolouhintaan erikoistunut yritys joutui lopettamaan yrityksensä jouduttuaan oikeudellisiin ongelmiin. Valtakunnansyyttäjä totesi tapaukseen, että nettisivut eivät saa valjastaa käyttäjän laskentatehoa käyttöönsä ilmoittamatta selkeästi asiasta ja antamatta käyttäjälle mahdollisuutta kieltäytyä louhinnasta. [26]

Selaimessa tapahtuvan kryptolouhinnan ja selainpohjaisen kryptokaappauksen ero on häilyvä. Jos käyttäjälle ei ilmoiteta mitenkään tapahtuvasta louhinnasta, kyseessä on kryptokaappaus. Jos käyttäjälle ilmoitetaan sivustolla pienessä ilmoituslaatikossa, että sivustolla vierailevat louhivat kryptovaluuttoja, kyseessä on edelleen kryptokaappaus. Vaikka kryptolouhinnasta ilmoitetaan käyttäjälle, ilmoituksen pitää olla selkeä ja riittävän iso, että käyttäjä varmasti huomaa asian. Käyttäjällä tulee myös aina olla mahdollisuus irtisanoutua louhinnasta. Jotkut nettisivustot tarjoavat käyttäjälle mahdollisuuden tukea sivustoa antamalla luvan kryptolouhintaan sen sijaan, että sivustolla näytettäisiin mainoksia. Tällainen toiminta ei ole kryptokaappausta, koska käyttäjältä on kysytty lupa louhintaan.

8.2 Kryptolouhintaa virustentorjuntaohjelmistoissa

Kesäkuussa 2021 tietoturvayritys Norton alkoi tarjota virustentorjuntaohjelmistoaan käyttäville valikoiduille asiakkaille mahdollisuuden louhia Ethereumia suoraan Nortonin Norton 360 -virustentorjuntaohjelmistossa. Louhinta tapahtuu vain käyttäjän luvalla nappia painamalla. Norton vie 15 % käyttäjän louhimista tuotoista. Tammikuussa 2022 Norton laajensi kryptolouhintamahdollisuuden kaikille Norton 360 -asiakkaille. [64]

Nortonin emoyhtiö NortonLifeLock, joka omistaa myös tietoturvayhtiö Aviran, lisäsi kryptolouhintamahdollisuuden myös Aviran antivirusohjelmistoihin. Lisäys tapahtui tammikuussa 2022 samaan aikaan, kun kaikki Norton 360 -käyttäjät saivat mahdollisuuden kryptolouhintaan. Avira vie louhintavoitoista saman 15 % kuin Norton. [65]

Ongelmallista tästä kryptolouhintamahdollisuudesta tekee sen, että tavallinen käyttäjä ei välttämättä ymmärrä kryptolouhinnasta mitään. Aviran ja Norton virustentorjuntaohjelmistojen käyttäjiä on yhteensä 80 miljoonaa [65]. Aviran ja Nortonin ohjelmissa kryptolouhinnasta ei kerrota yksityiskohtaisesti. Louhinnan aloittaminen on kuitenkin tehty todella helpoksi: käyttäjän tarvitsee vain painaa louhinnan aloittavaa nappia. Vaikka tässä tapauksessa kyseessä ei ole kryptokaappaus, koska louhintaa ei aloiteta ilman käyttäjän lupaa, tilanne on silti poikkeuksellinen. Virustentorjuntaohjelmistojen tulisi suojella käyttäjää kryptokaappauksilta, mutta nyt ne itse tarjoavat kryptolouhintaa. Tilanteesta tekee myös huvittavan se, että vielä syyskuussa 2021 Virustotal-palvelu [66], joka tarjoaa selainpohjaista tiedoston tarkistamista haittaohjelmien varalta, ilmoitti Aviran virustentorjuntaohjelmiston asennustiedoston sisältävän haitallista sisältöä [65].

9. YHTEENVETO

Kryptokaappaukset ja niistä aiheutuvat muut uhkat ovat tällä hetkellä iso uhka muiden haittaohjelmien lisäksi. Kaappausten kohteina ovat yksityisten käyttäjien lisäksi myös yritykset ja varsinkin pilvipalveluita tarjoavat yritykset. Pilvipalveluita tarjoavat yritykset ovat otollinen kohde kryptokaappauksille pilvipalveluiden tarjoaman valtavan laskentatehon takia. Yrityskäyttöön vuokratut pilvipalvelut sisältävät todennäköisesti myös arvokasta tietoa ja dataa, joka on yleensä sellaisenaan varastettavissa hyökkääjän jo päästyä esimerkiksi tietoturva-aukkoa pitkin palvelimelle.

Tällä hetkellä olemassa olevat torjuntamekanismit luovat hyvän pohjan tulevaisuuden kryptokaappauksia vastaan. Kryptokaappausten muuttuessa myös niiden torjuntametodien tulee päivittyä. Mustalistaus tarjoaa suojan isolle osalle kryptokaappauksista, mutta vahvaa hämäännyttämistä käyttäviä vastaan se ei anna suojaa. Myöskään tiettyä käyttäjäkuntaa tai alustaa varten suunnitellut kryptokaappaukset eivät jää helposti mustalistauksen piiriin. Mustalistauksen kanssa olisikin hyvä olla jokin muu tehokas suoja kryptokaappauksia vastaan. Esimerkiksi helppokäyttöinen ja yksityiskäyttöönkin soveltuva kryptolouhinnassa käytetty prosessorin HPC-laskurin seurantaan perustuva työkalu olisi hyvä lisä mustalistauksen pariksi. Täytyy kuitenkin muistaa, että vahvinkaan suojausmekanismi ei ole riittävä, jos käyttäjän oma tietoturvavalppaus ei ole kunnossa.

Tämän työn tarkoituksena oli selvittää eri kryptokaappausvariaatioiden toimintamallit ja niiden torjunta. Tutkimuskysymyksinä olivat:

1. Mitkä ovat kryptokaappausten eri variaatioiden toimintamallit?
2. Miten näiltä eri variaatioilta suojaudutaan?

Näiden variaatioiden eli tiedostopohjaisen ja selainpohjaisen kaappauksen toimintamallit jakavat joitakin yhtenäisiä piirteitä, kuten jonkin tietoturva-aukon käyttö. Molemmissa tapauksissa voidaan myös louhia prosessoritehoa käyttämällä. Toisaalta selainpohjaisissa kryptokaappauksissa kannattaa louhia pelkästään prosessoripohjaisesti, koska näytönohjainpohjainen louhinta on kannattamatonta JavaScriptin rajoitteiden takia.

Tässä työssä käsiteltiin useita erilaisia torjuntametodeja. Ajan puutteen vuoksi niitä ei kuitenkaan voitu etsiä lisää. Olisi myös ollut mielenkiintoista kehittää kokonaan uusi metodi kryptokaappausten havaitsemiseen. Olemassa olevia torjuntametodeja olisi myös kiinnostavaa yrittää yhdistää ja hioa yksityiskäyttöön sopivaksi eli riittävän helppokäyttöiseksi.

LÄHTEET

[1] Symantec, “ISTR Internet Security Threat Report Volume 23,” 2018. Accessed: Nov. 01, 2021. [Online]. Available: https://docs.broadcom.com/doc/istr-23-2018-en

[2] R. W. Schlosser, O. Wendt, S. Bhavnani, and B. Nail-Chiwetalu, “Use of information-seeking strategies for developing systematic reviews and engaging in evidence-based practice: the application of traditional and comprehensive Pearl Growing. A review,” *International journal of language & communication disorders*, vol. 41, no. 5, pp. 567–582, 2006, doi: 10.1080/13682820600742190.

[3] C. Okoli, “A guide to conducting a standalone systematic literature review,” *Communications of the Association for Information Systems*, vol. 37, no. 1, pp. 879–910, 2015, doi: 10.17705/1cais.03743.

[4] Tampereen yliopisto, “Andor.” https://andor.tuni.fi (accessed Jan. 02, 2022).

[5] Google, “Google Scholar”, Accessed: Jan. 02, 2022. [Online]. Available: https://scholar.google.com/intl/us/scholar/help.html#coverage

[6] P. Franco, “Understanding bitcoin : cryptography, engineering and economics.,” pp. 49–158, 2015, Accessed: Nov. 30, 2021. [Online]. Available: https://ebookcentral.proquest.com/lib/tampere/detail.action?docID=1823060

[7] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & information systems engineering*, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[8] Monerodocs, “CryptoNight.” https://monerodocs.org/proof-of-work/cryptonight/ (accessed Dec. 06, 2021).

[9] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, “Bitcoin and Blockchain: Security and Privacy,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10288–10313, 2020, doi: 10.1109/JIOT.2020.3004273.

[10] A. Szmigielski, “Bitcoin essentials : gain insights into Bitcoin, a cryptocurrency and a powerful technology, to optimize your Bitcoin mining techniques.” Packt Publishing, Birmingham, pp. 82–85, 2016. Accessed: Dec. 30, 2021. [Online]. Available: https://www.oreilly.com/library/view/bitcoin-essentials/9781785281976/

[11] H. Darabian *et al.*, “Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis,” *Journal of grid computing*, vol. 18, no. 2, pp. 293–303, 2020, doi: 10.1007/s10723-020-09510-6.

[12] Coinmarketcap, “Bitcoin to EUR Chart.” https://coinmarketcap.com/currencies/bitcoin/ (accessed Nov. 03, 2021).

[13] Coinmarketcap, “Monero to EUR Chart.” https://coinmarketcap.com/currencies/monero/ (accessed Nov. 03, 2021).

[14] Getmonero, “Mining Monero.” https://www.getmonero.org/get-started/mining/ (accessed Nov. 03, 2021).

[15] A. Zimba, Z. Wang, H. Chen, and M. Mulenga, “Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks,” *KSII Transactions on Internet and Information Systems*, vol. 13, no. 6, pp. 3258–3279, Jun. 2019, doi: 10.3837/tiis.2019.06.027.

[16] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld, “Digging into Browser-based Crypto Mining,” in *Proceedings of the Internet Measurement Conference 2018*, Oct. 2018, pp. 70–76. doi: 10.1145/3278532.3278539.

[17] M. Saad, A. Khormali, and A. Mohaisen, “End-to-End Analysis of In-Browser Cryptojacking,” Sep. 2018, Accessed: Feb. 15, 2022. [Online]. Available: https://arxiv.org/abs/1809.02152

[18] A. Binti Abdul Aziz, S. bin Ngah, Y. Ti Dun, and T. Fui Bee, “Coinhive’s Monero Drive-by Crypto-jacking,” in *IOP Conference Series: Materials Science and Engineering*, Jun. 2020, vol. 769, no. 1. doi: 10.1088/1757-899X/769/1/012065.

[19] Malwarebytes, “The state of malicious cryptomaining,” 2018. https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/ (accessed Nov. 04, 2021).

[20] D. Carlin, J. Burgess, P. O’Kane, and S. Sezer, “You Could Be Mine(d): The Rise of Cryptojacking,” *IEEE security & privacy*, vol. 18, no. 2, pp. 1–1, 2019, doi: 10.1109/MSEC.2019.2920585.

[21] F. Gomes and M. Correia, “Cryptojacking Detection with CPU Usage Metrics,” in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, Nov. 2020, pp. 1–10. doi: 10.1109/NCA51143.2020.9306696.

[22] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark, “A First Look at Browser-Based Cryptojacking,” in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 58–66. doi: 10.1109/EuroSPW.2018.00014.

[23] G. Hong *et al.*, “How you get shot in the back: A systematical study about cryptojacking in the real world,” in *Proceedings of the ACM Conference on Computer and Communications Security*, Oct. 2018, pp. 1701–1713. doi: 10.1145/3243734.3243840.

[24] J. Segura, “Persistent drive-by cryptomining coming to a browser near you,” *Malwarebytes*, Nov. 29, 2017. https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/ (accessed Nov. 23, 2021).

[25] S. Pastrana and G. Suarez-Tangil, “A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth,” Jan. 2019, [Online]. Available: http://arxiv.org/abs/1901.00846

[26] J. Burgess, D. Carlin, P. O’Kane, and S. Sezer, “MANiC: Multi-step assessment for cryptominers,” Jun. 2019. doi: 10.1109/CyberSecPODS.2019.8885003.

[27] P. Papadopoulos, P. Ilia, and E. Markatos, “Truth in Web Mining: Measuring the Profitability and the Imposed Overheads of Cryptojacking,” 2019. Accessed: Nov. 08, 2021. [Online]. Available: https://doi-org.libproxy.tuni.fi/10.1007/978-3-030-30215-3_14

[28] V. and S. B. P. R. K. Khiruparaj T. P. and Abishek Madhu, “Unmasking File-Based Cryptojacking,” in *Intelligence in Big Data Technologies—Beyond the Hype*, 2021, pp. 137–146. Accessed: Nov. 08, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-5285-4_13

[29] K. Sigler, “Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom,” *Computer fraud & security*, vol. 2018, no. 9, pp. 12–14, 2018, doi: 10.1016/S1361-3723(18)30086-1.

[30] J. Norman, “How not to become a crypto-jacking statistic,” *Computer Fraud & Security*, vol. 2019, no. 4, pp. 18–19, Apr. 2019, doi: 10.1016/S1361-3723(19)30043-0.

[31] D. Beneš, “Crackonosh: A New Malware Distributed in Cracked Software,” *Avast*, Jun. 24, 2021. https://decoded.avast.io/danielbenes/crackonosh-a-new-malware-distributed-in-cracked-software/ (accessed Nov. 11, 2021).

[32] R. Tahir *et al.*, “Mining on Someone Else’s Dime: Mitigating Covert Mining Operations in Clouds and Enterprises,” in *Research in Attacks, Intrusions, and Defenses*, 2017, vol. 10453, pp. 287–310. doi: 10.1007/978-3-319-66332-6_13.

[33] A. Greenberg, “How Hackers Hid a Money-Mining Botnet in the Clouds of Amazon and Others,” *Wired*, Jul. 24, 2014. https://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/ (accessed Nov. 11, 2021).

[34] K. Jayasinghe and G. Poravi, “A Survey of Attack Instances of Cryptojacking Targeting Cloud Infrastructure,” in *Proceedings of the 2020 2nd Asia Pacific Information Technology Conference*, 2020, pp. 100–107. doi: 10.1145/3379310.3379323.

[35] MS-ISAC, “EternalBlue,” *Multi-State Information Sharing & Analysis Center*, Jan. 2019. https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf (accessed Jan. 06, 2022).

[36] B. O’Gorman, “Cryptojacking: A Modern Cash Cow,” Jul. 2018. Accessed: Jan. 08, 2022. [Online]. Available: https://docs.broadcom.com/doc/istr-cryptojacking-modern-cash-cow-en

[37] Elastic, “Elasticsearch.” https://www.elastic.co/elasticsearch/ (accessed Jan. 07, 2022).

[38] A. Shalnev and M. Zavodchik, “‘CryptoSink’ Campaign Deploys a New Miner Malware,” *F5 Labs*, Mar. 13, 2019. https://www.f5.com/labs/articles/threat-intelligence/-cryptosink--campaign-deploys-a-new-miner-malware (accessed Jan. 07, 2022).

[39] M. Zavodchik and L. Segal, “Zealot: New Apache Struts Campaign Uses EternalBlue and EternalSynergy to Mine Monero on Internal Networks,” *F5 Labs*, Jan. 18, 2018. https://www.f5.com/labs/articles/threat-intelligence/zealot-new-apache-struts-campaign-uses-eternalblue-and-eternalsynergy-to-mine-monero-on-internal-networks (accessed Jan. 07, 2022).

[40] J. Křoustek, “Meet Adylkuzz: Cryptocurrency-mining malware spreading using the same exploit as WannaCry,” *Avast blog*, May 18, 2017. https://blog.avast.com/meet-adylkuzz-cryptocurrency-mining-malware-spreading-using-the-same-exploit-as-wannacry (accessed Jan. 07, 2022).

[41] Certego, “Ruby RCE pushing Monero Coinminer,” *Certego*, Jan. 11, 2018. https://www.certego.net/en/news/ruby-rce-used-to-push-monero-coinminer/ (accessed Jan. 08, 2022).
[42] Checkpoint Research, “‘RubyMiner’ Cryptominer Affects 30% of WW Networks,” *Checkpoint Research*, Jan. 11, 2018. https://research.checkpoint.com/2018/rubyminer-cryptominer-affects-30-ww-networks/ (accessed Jan. 08, 2022).
[43] RedLock CSI Team, “Lessons from the Cryptojacking Attack at Tesla,” *Redlock blog*, Feb. 20, 2018. https://redlock.io/blog/cryptojacking-tesla (accessed Jan. 08, 2022).
[44] Check point, “Jenkins Miner: One of the Biggest Mining Operations Ever Discovered,” *Check point Research*, Feb. 15, 2018. https://research.checkpoint.com/2018/jenkins-miner-one-biggest-mining-operations-ever-discovered/ (accessed Jan. 08, 2022).
[45] Varonis, “Varonis.” https://www.varonis.com/ (accessed Feb. 11, 2022).
[46] D. Taler, “Varonis Uncovers New Malware Strains and a Mysterious Web Shell During a Monero Cryptojacking Investigation,” *Inside Out Security Blog*, Feb. 05, 2020. https://www.varonis.com/blog/monero-cryptominer (accessed Jan. 08, 2022).
[47] J. Chen, “Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub,” *Unit42*, Oct. 16, 2019. https://unit42.paloaltonetworks.com/graboid-first-ever-cryptojacking-worm-found-in-images-on-docker-hub/ (accessed Jan. 08, 2022).
[48] Office of Inspector General, “Semiannual report to congress,” *National Science Foundation*, Mar. 2014. https://nsf.gov/pubs/2014/oig14002/oig14002.pdf (accessed Jan. 08, 2022).
[49] T. R. Delwiche, “Harvard Research Computing Resources Misused for ‘Dogecoin’ Mining Operation,” *The Harvard Crimson*, Feb. 20, 2014. Accessed: Jan. 08, 2022. [Online]. Available: https://www.thecrimson.com/article/2014/2/20/harvard-odyssey-dogecoin/
[50] A. Hern, “Student uses university computers to mine Dogecoin,” *The Guardian*, Mar. 04, 2014. Accessed: Jan. 08, 2022. [Online]. Available: https://www.theguardian.com/technology/2014/mar/04/dogecoin-bitcoin-imperial-college-student-mine
[51] A. Yazdinejad, H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, G. Srivastava, and M.-Y. Chen, “Cryptocurrency malware hunting: A deep Recurrent Neural Network approach,” *Applied Soft Computing*, vol. 96, p. 106630, Nov. 2020, doi: 10.1016/j.asoc.2020.106630.
[52] W. B. T. Handaya, M. N. Yusoff, and A. Jantan, “Machine learning approach for detection of fileless cryptocurrency mining malware,” in *Journal of Physics: Conference Series*, Mar. 2020, vol. 1450, no. 1. doi: 10.1088/1742-6596/1450/1/012075.
[53] A. Zareh and H. R. Shahriari, “BotcoinTrap: Detection of Bitcoin Miner Botnet Using Host Based Approach,” in *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, 2018, pp. 1–6. doi: 10.1109/ISCISC.2018.8546867.
[54] A. Kharraz *et al.*, “Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild,” in *The World Wide Web Conference*, 2019, pp. 840–852. doi: 10.1145/3308558.3313665.
[55] D. Tanana, “Behavior-Based Detection of Cryptojacking Malware,” in *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, May 2020, pp. 0543–0545. doi: 10.1109/USBEREIT48449.2020.9117732.
[56] Keraf and A. Diaa, “No Coin,” *Firefox Browser Add-Ons*. https://addons.mozilla.org/en-US/firefox/addon/no-coin/ (accessed Feb. 15, 2022).
[57] chYer, “NoMiner - Block Coin Miners,” *Chrome Web Store*. https://chrome.google.com/webstore/detail/nominer-block-coin-miners/jfnangjojcioomick-mmnfmiadkfhcdmd (accessed Feb. 15, 2022).
[58] M. A. Razali and S. Mohd Shariff, “CMBlock: In-Browser Detection and Prevention Cryptojacking Tool Using Blacklist and Behavior-Based Detection Method,” in *Advances in Visual Informatics*, vol. Vol 11870, Malaysia: Springer, 2019, pp. 404–414. doi: 10.1007/978-3-030-34032-2_36.
[59] G. Gomes, L. Dias, and M. Correia, “CryingJackpot: Network Flows and Performance Counters against Cryptojacking,” Nov. 2020. doi: 10.1109/NCA51143.2020.9306698.
[60] J. Z. i Munoz, J. Suarez-Varela, and P. Barlet-Ros, “Detecting cryptocurrency miners with NetFlow/IPFIX network measurements,” in *2019 IEEE International Symposium on Measurements & Networking (M&N)*, 2019, pp. 1–6. doi: 10.1109/IWMN.2019.8804995.
[61] S. Barbhuiya, Z. Papazachos, P. Kilpatrick, and D. S. Nikolopoulos, “RADS: Real-time Anomaly Detection System for Cloud Data Centres,” Nov. 2018, Accessed: Feb. 09, 2022. [Online]. Available: https://arxiv.org/abs/1811.04481

[62] P. O'Kane, S. Sezer, and K. McLaughlin, "Obfuscation: The Hidden Malware," *IEEE security & privacy*, vol. 9, no. 5, pp. 41–47, 2011, doi: 10.1109/MSP.2011.98.
[63] D. Carlin, P. O'Kane, S. Sezer, and J. Burgess, "Detecting Cryptomining Using Dynamic Analysis," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 2018, pp. 1–6. doi: 10.1109/PST.2018.8514167.
[64] R. Gayathri, "Introducing Norton Crypto!," *Norton Blog*, Jun. 20, 2021. https://community.norton.com/en/blogs/product-service-announcements/introducing-norton-crypto (accessed Jan. 31, 2022).
[65] KrebsonSecurity, "500M Avira Antivirus Users Introduced to Cryptomining," *KrebsonSecurity*, Jan. 08, 2022. https://krebsonsecurity.com/2022/01/500m-avira-antivirus-users-introduced-to-cryptomining/ (accessed Jan. 31, 2022).
[66] Virustotal, "Virustotal." https://www.virustotal.com/gui/home/upload (accessed Jan. 31, 2022).