

A A R N O

M A L I N

**r a n s o m
_ m a n**

VASTAAMON TAPAUS JA

ALEKSANTERI KIVIMÄEN HAKKERIHISTORIA

atena

© Aarno Malin ja Atena / Kustannusosakeyhtiö Otava 2025

Jyväskylä

Tekstin- ja tiedonloushintaa kielletty.

ISBN 978-951-1-50326-2

OTAVA
KIRJAPAINO
Keuruu 2025



Sisällys

Johdanto	7
----------------	---

Osa 1: HACK THE PLANET

Häiriköstä rikolliseksi	19
Julkaisut eli zinet.....	27
Yhdeksän syytekohtaa	33
FBI:n asiakirjat	44

Osa 2: LIZARD SQUAD

Kostaja	55
Straterin perheen painajainen	66
Tietomurtoja ja tihutöitä.....	74
Hakkeri, joka pilasi joulun.....	87

Osa 3: VASTAAMON TAPAUS

Kiristysoperaatio	105
Jälkien seuraaminen	118
Kuinka hakkeri napataan.....	127
Uhrit	133

Osa 4: PIMEÄN VERKON RIKOKSET

Taustaa	139
Silkkitien kiristäjä	148
Kaiken takana on Dnstats	154
Inhimillinen tekijä	162
 Lopuksi	 167
 Lähteitä	 171

Johdanto

Kirjoitin *Suomen Kuvalehteen* vuonna 2021 jutun otsikolla »Tor-verkon suurin huijari saattaa olla suomalainen». Kerroin siinä henkilöstä, joka oli tienannut erilaisilla hämärillä operaatioilla ehkä jopa pari miljoonaa euroa Tor-verkossa eli niin sanotussa pimeässä verkossa. Huijari tunnettiin nimellä Dnstats. Hän oli erikoistunut viemään rahat ihmisiltä, jotka yrittivät ostaa huumeita netistä. Uskoin tuolloin, ettei hänen henkilöllisyytensä tulisi koskaan paljastumaan, sillä hän vaikutti todella taitavalta rikolliselta.

Psykoterapiakeskus Vastaamon kiristäjä käytti Tor-verkkoa, julkaisi siellä näytteitä varastetuista potilasasiakirjoista ja keskusteli yleisön kanssa. Seurasin tapahtumia alusta saakka reaaliaikaisena ja onnistuin hankkimaan itseleni tiedoston, joka piti sisällään varastetut potilasasiakirjat ja muuta kiristäjälle kuulunutta dataa. Toimitin tiedoston tietoturvayhtiö F-Securelle siinä toivossa, että se voisi auttaa kiristäjän jäljittämässä.

Aleksanteri Kivimäki otettiin kiinni Ranskassa alkuvuodesta 2023 epäiltynä Vastaamon tietomurrosta ja kiristyksestä. Kun Keskusrikospoliisi julkaisi tapauksen esitutkintapöytäkirjan, perehdyin siihen ja vakuutuin Kivimäen syyllisyydestä. Myöhemmin KRP julkaisi lisätutkin-

nan, jonka myös hankin itselleni, ja sitä lukiessani olin pudota tuolilta. Olin vuosia seurannut Tor-verkossa toimivaa Dnstats-huijaria, ja kun yhdistin kaikki hänestä keräämäni tiedot siihen, mitä lisätutkinnassa kerrottiin, minulle syntyi vahva epäily siitä, että Dnstats saattaisi olla Kivimäki.

Oikeudenkäynti Kivimäkeä vastaan alkoi Länsi-Uudenmaan käräjäoikeudessa lokakuussa 2023. Hän oli tuolloin 26-vuotias. Kotimainen media seurasi oikeudenkäyntiä herkeämättä, ja siitä uutisoitiin myös ulkomailla. Kivimäestä tuli julkkis.

Oikeuden mukaan Kivimäki murtautui Vastaamon tietokantaan ja varasti yli 33 000 asiakkaan potilasasiakirjat. Ne pitivät sisällään kunkin asiakkaan kaikki henkilötiedot sekä terapeutin kirjoittamat muistiinpanot tapaamisista. Joistakin asiakkaista muistiinpanoja oli kymmeniä sivuja, ja niissä saatettiin kuvailla äärimmäisen arkaluontoisia asioita, joita asiakkaat eivät olleet uskaltaneet paljastaa kenellekään muulle kuin terapeutille.

Sitten Kivimäki aloitti kiristämisen. Hän otti yhteyttä Vastaamon toimitusjohtajaan ja vaati 40 bitcoinia eli tuon ajan kurssilla noin 400 000 euroa siitä hyvästä, ettei julkaise varastettuja potilasasiakirjoja. Myöhemmin hän lähetti kiristysviestejä Vastaamon asiakkaille. Kesken kiristysoperaation Kivimäki kuitenkin mokasi ja levitti vahingossa kaikki varastamansa potilasasiakirjat nettiin. Seuraukset olivat tuhoiset. Jotkut Vastaamon asiakkaat päätyivät riistämään hengen itseltään.

Huhtikuussa 2024 käräjäoikeus tuomitsi Kivimäen kuudeksi vuodeksi ja kolmeksi kuukaudeksi vankeuteen. Rangaistusta on pidetty naurettavan pienenä, varsinkin ulkomailla, mutta Suomen lain mukaan se on melkein mak-

simirangaistus Kivimäen rikoksista. Kivimäki on kiistänyt syyllisyytensä ja on valittanut tuomiosta hovioikeuteen.

Suomessa Kivimäki tunnetaan Vastaamon rikosvyyhdistä, mutta se on pelkkä jäävuoren huippu. Kivimäki on yksi tunnetuimmista hakkereista koko maailmassa. Hän opetteli lapsena erilaisia ohjelmointikieliä, ja sen jälkeen hän on aiheuttanut uskomattoman määrän vahinkoa ja inhimillistä kärsimystä. Yhdysvaltain liittovaltion poliisi FBI on tutkinut hänen rikoksiaan jo vuodesta 2013 saakka.

Myös tämä kirja on vain jäävuoren huippu. Kerron tässä vain niistä konnuuksista, jotka ovat selkeästi yhdistettävissä Kivimäkeen. Kaikki muu jää piiloon, ehkä ikuisiksi ajoiksi. Vain Kivimäki itse tietää, mitä kaikkea hän on tehnyt.

Kivimäki ei ole peitellyt elämäntyyliään, johon ovat kuuluneet kalliit autot, luksushotellit ja hienot asunnot eri puolilla Eurooppaa. Oikeudessa yritettiin selvittää, kuinka hän oli rahoittanut tuon kaiken, sillä hänellä ei ollut lainkaan tuloja. Mysteeri jäi ratkaisematta.

Tämä kirja saattaa tarjota vastauksen mysteeriin. Perkaan myös Vastaamon tapauksen, mutta ensin kerron, millaisen tien Kivimäki kulki ennen kuin päätyi toteuttamaan rikosvyyhdin, josta hänet tullaan aina muistamaan.

Kiristämisen anatomia

Vuonna 2022 julkaistussa kirjassani *Pimeyden ytimeen* kerroin Tor-verkon rikollisuudesta, kuten huumekaupasta, palkkamurhista ja lasten hyväksikäytöstä – sekä tietysti Vastaamosta.

Olen tutkinut Tor-verkkoa vuosikymmenen, ja sinä aikana olen törmännyt kiristämiseen yllättävän harvoin. Oikeastaan kiristäminen liittyy olennaisena osana vain joihinkin pedofiilien sivustoihin.

Tor-verkon huumemaaailmassa on paljon mahdollisuuksia kiristämiseen, mutta silti ilmiö on siellä marginaalinen. Kun asiakas tilaa kauppasivustolta huumeita, antaa hän yhteystietonsa, jotta myyjä voi lähettää huumeet oikeaan osoitteeseen. Myyjä siis tietää asiakkaan henkilöllisyyden ja hänellä on todisteet siitä, että asiakas yrittää ostaa huumeita. Myyjän olisi helppo kiristää asiakasta uhkaamalla toimittaa tiedot poliisille, mutta silti tällaista ei juurikaan tapahdu. Suomessa on ollut vain yksi huumekauppiaksi tekeytynyt kiristäjä.

Kauppasivustot pyrkivät aina antamaan itsestään mahdollisimman luotettavan kuvan. Ne vakuuttelevat, että kaikki tilaustiedot ja yksityisviestit ovat kryptattuja ja tuhoutuvat tietyn ajan kuluttua. Maaliskuussa 2024 Incognito Market -niminen kauppasivusto kohahdutti ilmoittamalla, että sillä oli tallessa kaikkien käyttäjien yksityisviestit, tilaukset ja kryptovaluuttasiirrot, ja jokaisen käyttäjän, joka ei halunnut tietojaan julkisuuteen, tuli maksaa tietty summa. Incognito Market on ääriesimerkki, en muista toista vastaavaa tapausta.

Minäkin olen joutunut kiristyksen uhriksi. Kiristäjä tehtiin suomenkielisiä huijaussivustoja Tor-verkkoon, ja kun varoitin hänestä blogissani, hän lähetti minulle viestin, jossa kertoi, että hänellä oli valokuvia minusta ja läheisistäni sekä meidän yhteystietomme. Hän käski minua poistamaan blogini, ja kun en sitä tehnyt, hän julkaisi kuvat ja yhteystiedot Tor-verkossa. Samalla hän aloitti

massiivisen mustamaalauskampanjan ja yllytti ihmisiä käymään kimppuuni. Muistan hyvin, miten eräs kaverini neuvoi minua hankkimaan pesäpallomailan eteiseen. On myönnettävä, että tuon kokemuksen jälkeen olen ollut varovaisempi sen suhteen, mitä kirjoitan. Liian varovaiseksi en kuitenkaan voi ryhtyä, muuten tämäkin kirja olisi jäänyt tekemättä.

Mielestäni on kuvaavaa, että vaikka Tor-verkko kuhisee rikollisia, kiristäminen on suhteellisen harvinaista. Vanhan sanonnan mukaan tilaisuus tekee varkaan. Tor-verkossa jokainen on anonyymi, joten siellä tilaisuus tekee monesta huijarin, mutta harva valitsee kiristyksen.

Pitkään ihmettelin, miten Aleksanteri Kivimäki kykeni toteuttamaan kiristysoperaationsa ilman ilmeisiä tunnon-tuskia. Sitten perehdyin hänen rikolliseen uraansa, enkä ihmetellyt enää. Nyt pidän Vastaamon rikosvyyhtiä vain luontevana jatkona hänen aiemmille rikoksilleen.

Kyberrikossanastoa

Kyberrikokset on aihepiiri, jota moni pitää monimutkaisena ja vaikeana, mutta minä olen halunnut tehdä kirjasta mahdollisimman selkeän ja helppolukuisen. Välttelen siis erikoissanastoa ja pyrin kirjoittamaan kansantajuisesti. Joi-takin hakkereihin liittyviä sanoja minun on kuitenkin käytettävä, jotta kerronta olisi sujuvaa.

Dossaus tai **dossaaminen** tarkoittaa palvelunestohyökkäyksen tekemistä. Sana tulee englannin kielen termistä *distributed denial-of-service attack*, joka usein lyhennetään muotoon *DDoS attack*. Dossauksessa verkkosivustoon

kohdistetaan niin paljon liikennettä, että se hidastuu tai kaatuu.

Doksaus tai **doksaaminen** tarkoittaa ihmisen henkilötietojen selvittämistä ja julkaisua verkossa. Toiminnalla pyritään kyseisen ihmisen vahingoittamiseen. Doksaus tulee tule englannin kielen sanasta *doxing*, joka puolestaan on johdettu sanasta *docs*, joka on lyhenne sanasta *documents* eli asiakirjat.

Swattaus tarkoittaa poliisin usuttamista viattoman henkilön kimppuun. Tämä tapahtuu antamalla viranomaisille perätön vaarailmoitus. Yhdysvalloissa poliisi käyttää piiritys- ja panttivankitilanteissa erikoisyksiköitä, joita kutsutaan SWAT-ryhmiksi, ja swattauksen tavoitteena on saada tällainen ryhmä tekemään rynnäkkö uhrin kotiin.

Palvelin eli **serveri** on tietokoneen kaltainen laite. Niitä on moneen eri tarkoitukseen, mutta tämän kirjan kannalta olennaista on tietää, että jokainen verkkosivusto on jollain palvelimella. Jos sivustoa dossataan, kohdistuu hyökkäys käytännössä palvelimeen.

IP-osoite on numerosarja, jonka avulla verkkoon kytetty laite voidaan tunnistaa. Jokaisella verkon laitteella, kuten palvelimella tai pelikonsolilla, on oma IP-osoitteensa.

Mustahatut ja **valkohatut** ovat hakkereita, mutta motiiveiltaan erilaisia. Mustahatut ovat verkkorikollisia, kun taas valkohatut ovat niin sanottuja eettisiä hakkereita. He toimivat lain mukaan ja käyttävät taitojaan muiden hyväksi, esimerkiksi tietoturva-aukkojen paikkailuun.

IRC tulee sanoista *Internet Relay Chat*, ja se on tekstipohjainen pikaviestipalvelu. IRC-keskustelut käydään eri kanavilla, ja niitä voi kuka tahansa perustaa lisää. Keskusteluissa voi olla yhtä aikaa mukana suuri määrä ihmisiä, mut-

ta kanavan ylläpitäjä voi halutessaan päättää, ketkä saavat olla kanavalla.

Tor-verkko on sellainen osa nettiä, jossa liikennettä ei voi jäljittää, ja siksi sinne on pesiytynyt paljon rikollisuutta. Tor-verkkoon pääsee Tor-selaimella, ilmaisella ja laillisella ohjelmistolla, jonka voi asentaa tietokoneelle tai puheliimeen.

Pimeä verkko eli *dark web* tai *dark net* tarkoittaa kaikkia sellaisia sivustoja, joihin pääsy edellyttää erityistä ohjelmistoa, kuten Tor-selainta.

Epätavallinen nuorukainen

Kivimäen koko nimi oli alun perin Julius Aleksanteri Tomminpoika Kivimäki. Hän esiintyi pitkään Julius Kivimäkenä, kunnes 2020-luvun alussa poisti ensimmäisen etunimen tiedoistaan. Minä kutsun häntä kirjassa Aleksanteriksi, koska sillä nimellä suomalaiset ovat oppineet hänet tuntemaan Vastaamon tapauksen myötä.

Nimi Julius tulee silti nousemaan kirjassa esiin useasti. Tämä johtuu siitä, että alaikäisenä Kivimäki teki rikoksia täysin avoimesti omalla nimellään. Tyhmyydestä siinä ei ollut kyse, vaan ilmeisesti maineen kartuttamisesta ja vastaavasta uskosta siihen, ettei hän joudu teoista vastuuseen.

Tyypillinen mielikuva hakkerista on tietokoneensa ääressä kyhjöttävä nörtti, joka pelkää ihmisiä ja hautautuu kotiinsa. Kivimäki on tämän mielikuvan vastakohta. Jo alaikäisenä hän matkusti ilman vanhempiaan ulkomaille ja tutustui ihmisiin. Kun hän oli 17-vuotias, televisiokanava Sky News julkaisi haastattelun, jossa hän esiintyi rennosti

ja sulavasti englantia puhuen. Kivimäki on 192 senttiä pitkä, ja täyden pituutensa hän saavutti jo varhain, joten hän vaikutti ikäistään vanhemmalta.

Verkkorikokset on helppo mieltää pelkäksi tietokoneen näppäimistön naputteluksi, jolla on vaikutusta vain näkymättömään bittimaailmaan. Oikeasti verkkorikoksilla voi tehdä uhrien elämästä helvettiä, ja niillä voi aiheuttaa suunnatonta taloudellista vahinkoa. Rangaistukset verkkorikoksista ovat joskus mitättömän pieniä.

Tämä kirja perustuu valtaosin omaan tutkimustyöhöni, mutta mukana on myös haastatteluja. Aleksanteri Kivimäeltä en saanut haastattelua. Olen kerännyt tietoa monenlaisista lähteistä, kuten poliisin esitutkintapöytäkirjoista, jotka pitävät sisällään muun muassa kuulustelukertomuksia ja FBI:n asiakirjoja. Tärkeitä lähteitä ovat olleet myös netistä löytämäni kirjoitukset ja somepostaukset, joita Kivimäki ja hänen edustamansa hakkeriryhmät ovat julkaisseet. Kivimäestä on kirjoitettu paljon lehtijuttuja, varsinkin Yhdysvalloissa, mutta niiden tarjoama tieto on usein epätarkkaa ja jopa virheellistä. Onneksi hänestä on kirjoitettu myös asiantuntevia tekstejä. Minulle on ollut suureksi avuksi Wayback Machine, joka arkistoi nettisivuja. Kun kaikki muut lähteet ovat tarjonneet sekavaa ja keskenään ristiriitaista tietoa siitä, mitä netissä on tapahtunut, olen parhaassa tapauksessa voinut tarkistaa todellisen tapahtumien kulun Wayback Machinella.

Kirjan loppuun olen listannut tärkeimmät lähteet luvuitain, jotta lisätiedoista kiinnostunut lukija voi jatkaa omaa tutkimusmatkaansa.

En moralisoi kirjassa Kivimäkeä enkä yritä analysoida

hänen luonnettaan. Kirjaa tehdessäni yritin tietysti kuumaisesti ymmärtää, mitä hänen päässään liikkuu, mutta pohdiskeluni lopputulos on vain minun henkilökohtainen mielipiteeni. En halua tarjota lukijalle mielipiteitä vaan faktoja. Kivimäen teot puhukoot puolestaan.

Vastaamon rikosvyyhtiä käsitellään seuraavaksi Helsingin hovioikeudessa. Käsittely alkaa vasta tämän kirjan julkaisun jälkeen, elokuussa 2025.

Kirja jakautuu neljään osaan. Ensimmäinen osa kertoo Hack the Planet -nimisestä hakkeriryhmästä, johon Kivimäki liittyi 14-vuotiaana. Toinen osa kertoo Lizard Squad -nimisestä ryhmästä, johon hän liittyi seuraavaksi. Kolmas osa käsittelee Vastaamoa ja neljäs huijauksia, joiden takana Kivimäki saattaa olla.

Toivon kirjan avaavan lukijan silmät sille, miten tuhovoimainen ase tietokone voi väärissä käsissä olla ja miten huonosti Suomen lainsäädäntö on asiaan varautunut.

The background is a solid black field densely populated with white, hand-drawn geometric shapes. These shapes include various polygons, rectangles, and lines, some of which are nested or overlapping, creating a complex, layered visual effect. The overall impression is one of digital noise or a corrupted image.

Osa 1:

HACK

THE PLANET