Länsi-Uudenmaan käräjäoikeus | **Tuomio** 24/119144
Annettu kansliassa
30.04.2024 | Asianumero R 23/3965

Puheenjohtaja Laamanni Ilkka Lahtinen

Jäsenet Käräjätuomari Mette Manninen
Käräjätuomari Klaus Kekki

Syyttäjät Aluesyyttäjä Bo-Niklas Lundqvist
Aluesyyttäjä Harri Mäkelä
Aluesyyttäjä Pasi Vainio

Vastaaja Aleksanteri Tomminpoika Kivimäki

Asianomistajat Asianomistajat erillisellä liitteellä (Salattu)

Psykoterapiakeskus Vastaamo Oy:n konkurssipesä

Asia Törkeä kiristys ym.

Vireille 18.10.2023

Tuomion julkisuus

Käräjäoikeus on oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain 6 §:n 1 momentin 1 kohdan ja 24 §:n 2 momentin 1 kohdan nojalla määrännyt asianomistajien henkilöllisyydet salassa pidettäviksi.

Lisäksi käräjäoikeus on lain 9 §:n 1 momentin 2 kohdan ja 10 §:n nojalla määrännyt asianomistajien esitutkintapöytäkirjat ja kirjalliset todisteet S12, S38, S50 (osittain), S68 ja S81 (osittain) salassa pidettäviksi.

Salassapitoaika päättyy 17.10.2083.

Oikeudenkäynti asiassa on toimitettu yleisön läsnäolematta oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain 15 §:n 1 momentin 2 kohdan nojalla siltä osin kuin oikeudenkäynnissä on käsitelty edellä mainittuja kirjallisia todisteita.

Selostus asiasta

Asianomistajien korvausvaatimusten erottaminen erillisissä oikeudenkäynneissä käsiteltäväksi

Käräjäoikeus on 18.10.2023 tekemällään päätöksellä määrännyt, että asianomistajien tämän syyteasian yhteydessä esittämät mahdolliset yksityisoikeudelliset vaatimukset käsitellään erikseen riita-asiain oikeudenkäynnistä säädetyssä järjestyksessä, ja ettei sanottuja vaatimuksia käsitellä esillä olevan syyteasian yhteydessä.

Asianomistajista noin 6.500 on ilmoittanut käräjäoikeudelle yhtyvänsä syyttäjien syytteeseen.

Eurooppalainen pidätysmääräys

Kivimäki on Helsingin käräjäoikeuden 27. ja 28.10.2022 tekemillä päätöksillä vangittu poissaolevana.

Versaillesin muutoksenhakutuomioistuin on 15.2.2023 tekemällään päätöksellä antanut suostumuksensa siihen, että Kivimäki luovutetaan Suomen valtion oikeusviranomaiselle eurooppalaisen pidätysmääräyksen nojalla rikossyytteen ajamista varten ajalla 25.–28.11.2018, 28.9.2020, 21. ja 23.10.2020, 24.10.2020 ja ajalla 25.3.2019–11.10.2021 Helsingissä, Tuusulassa ja Turussa tehdyistä törkeästä tunkeutumisesta tietojärjestelmään, törkeästä kiristysyrityksestä, yksityisyyttä loukkaavien tietojen törkeästä levittämisestä, kiristyksestä ja kiristysyrityksestä, tietojärjestelmään tunkeutumisesta, kirjesalaisuuden rikkomisesta ja todisteen väärentämisestä.

Versaillesin muutoksenhakutuomioistuin on lisäksi 29.11.2023 tekemällään päätöksellä antanut suostumuksensa sille, että Aleksanteri Kivimäki asetetaan syytteeseen muun ohella 24.10.2020 Tuusulassa tehdyksi epäillyistä törkeistä kiristyksistä ja törkeistä kiristyksen yrityksistä ja tietokonejärjestelmään tunkeutumisessa.

Kaksoisrangaistavuusselvitys

Yhdistyneen kuningaskunnan Eurojustin yhteyssyyttäjä on antanut syyttäjien tiedusteluun vastauksen, jossa on todettu, että Vastaamon asiakkaisiin kohdistuneet teot katsottaisiin Englannin lain mukaan kiristysrikoksiksi huolimatta siitä, ovatko asiakkaat maksaneet vaaditut rahamäärät. Rikoksille ei ole vanhentumisaikaa, ja rangaistuksena voidaan tuomita vankeutta enintään 14 vuotta.

Valtakunnansyyttäjän syytemääräys

Apulaisvaltakunnansyyttäjä Rappe on 16.2.2024 tekemällään päätöksellä määrännyt aluesyyttäjät Vainion, Lundqvistin ja Mäkelän nostamaan syytteet Kivimäkeä vastaa niistä törkeän kiristyksen yrityksistä ja törkeistä kiristyksistä, jotka on tehty Yhdistyneessä kuningaskunnassa ja joiden ulkomaisia asianomistajia ei voida rinnastaa suomalaisiin rikoslain 1 luvun 5 §:ssä kerrotulla tavalla.

Tietosuojavaltuutetun lausunto

Tietosuojavaltuutettu on 25.9.2023 antanut asiassa lausunnon, jonka syyttäjät ovat toimittaneet käräjäoikeudelle 18.10.2023.

Syyttäjän rangaistusvaatimukset

1. Törkeä tietomurto
2400/R/0000206/20
Rikoslaki 38 luku 8a § 1 / 1-2

25.11.2018 - 26.11.2018 Pori

Kivimäki on yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa käyttämällä hänelle kuulumatonta käyttäjätunnusta tai turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutunut mielenterveyspalveluja tuottavan Psykoterapiakeskus Vastaamo Oy:n (jälj. Vastaamo) tietojärjestelmään.

Ennen tietojärjestelmään tunkeutumista vastaaja on selvittänyt internetissä olevia palvelimia, joissa on ollut haavoittuvuuksia, kuten avoimia tietoliikenneportteja ja tavanomaisia ja helposti arvattavia salasanoja, tai ei salasanaa ja/tai käyttäjätunnusta (skannaus).

Kun vastaajalle on selvinnyt, että Vastaamon palvelimessa on ollut tekoaikaan edellä kuvattuja haavoittuvuuksia, on vastaaja tunkeutunut oikeudettomasti Vastaamon potilastietokannan sisältäneeseen palvelimeen. Tunkeutuminen on suoritettu siten, että vastaaja on luonut yhteyden Vastaamon MySQL-palvelimeen, käyttänyt hänelle kuulumatonta käyttäjätunnusta ja salasanaa ja ladannut Vastaamon potilastietokannan käyttöönsä.

Potilastietokanta on sisältänyt tunkeutumisen ja lataamisen aikaan noin 33000 potilaan erittäin arkaluonteiset henkilö- ja potilastiedot sekä potilaiden käyntimerkinnät.

Teko on tehty erityisen suunnitelmallisesti. Teossa on käytetty useita eri maissa sijainneita palvelimia, salattuja VPN-yhteyksiä ja salausavaimia. Käytetyissä palvelimissa on ollut käytössä voimakkaita salausmenetelmiä. Tietomurtoon ja sen valmisteluun on käytetty haavoittuvuuksien selvittämiseen ja tietomurtoihin suunniteltuja ohjelmistoja, joita ei ole julkisesti saatavilla.

Teko on myös kokonaisuutena arvostellen törkeä.

2. Törkeän kiristyksen yritys
2400/R/0000206/20
Rikoslaki 31 luku 4 § 2

28.09.2020 - 23.10.2020 Helsinki

Kivimäki on yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa lähettänyt Vastaamolle sähköpostitse kiristysviestin, jossa hän on vaatinut yrityksen edustajia luopumaan taloudellisesta edusta, johon hänellä ei ole ollut oikeutta uhaten samalla yritystä epäedullisilla toimilla, jos hänen vaatimuksiinsa ei suostuta. Kivimäki on vaatinut viestissään yritystä maksamaan 40 bitcoinia (366.000,00 euroa) vastineeksi siitä, että ei julkaise hallussaan olleita erittäin arkaluonteisia henkilö- ja potilastietoja sekä potilaiden käyntimerkintöjä julkiseen internetiin.

Kun asianomistaja ei ole suostunut vaatimuksiin ja suorittanut maksua, on vastaaja julkaissut ensin 100 potilastietoa 21.10.2020 ja 100 potilastietoa 22.10.2020.

23.10.2020 vastaaja on käynnistänyt ohjelmakäskyjen sarjan, jonka tarkoituksena on ollut julkaista jatkossa 100 potilastietoa päivässä, kunnes kaikki potilastiedot on julkaistu. Käskyjen sarjassa olleen komennon vuoksi vastaaja on kuitenkin julkaissut kaikki potilastiedot kerralla, kun tarkoituksena on ollut ajastaa julkaisut tapahtuvaksi 100 potilastiedon osissa.

Vastaaja on tällä tavoin julkaissut yhteensä noin 33000 henkilön erittäin arkaluonteiset henkilö- ja potilastiedot sekä potilaiden käyntimerkinnät.

Rikoksella on pyritty samaan asianomistaja luopumaan erittäin arvokkaasta taloudellisesta edusta uhkaamalla vakavanlaatuisella rikoksella, joka vaarantaisi toisen hengen tai terveyden ja teko on myös kokonaisuutena arvostellen törkeä.

Vastaamon puolesta vaatimukseen ei ole suostuttu, joten teko on jäänyt yritykseksi.

Teko on myös kokonaisuutena arvostellen törkeä.

3. 9231 törkeää yksityiselämää loukkaavan tiedon levittämistä
2400/R/0000206/20
Rikoslaki 24 luku 8a §

21.10.2020 - 23.10.2020 Espoo

Kivimäki on yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa kohdassa 2 kerrotulla tavalla julkaissut yhteensä noin 33000 henkilön erittäin arkaluonteiset henkilö- ja potilastiedot sekä potilaiden käyntimerkinnät kolmessa erässä.

Ottaen huomioon Psykoterapiakeskus Vastaamo Oy:n asema mielenterveyspalveluja tuottavana yrityksenä, on Kivimäki teollaan yksityiselämää loukkaavassa tiedon levittämisessä aiheuttanut suurta kärsimystä tai sen vaaraa taikka erityisen suurta vahinkoa tai sen vaaraa asianomistajille ja rikos on myös kokonaisuutena arvostellen törkeä.

4. 20745 törkeän kiristyksen yritystä
2400/R/0000206/20
Rikoslaki 31 luku 4 § 1
Rikoslaki 5 luku 1§

24.10.2020 Espoo

Kivimäki on yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa 24.10.2020 lähettänyt Vastaamon potilastietokannasta ilmeneville henkilöille kiristysviestin, jossa hän on uhkauksella vaatinut heitä luopumaan taloudellisesta edusta, johon vastaajalla ei ole ollut oikeutta.

Vastaaja on vaatinut asianomistajilta 200 tai 500 euron maksua kryptovaluuttana uhaten samalla julkaista kyseisen henkilön erittäin arkaluonteiset henkilö- ja potilastiedot sekä käyntimerkinnät internetiin, mikäli vaatimukseen ei suostuta.

Kiristyksessä on uhattu vakavanlaatuisella rikoksella, joka vaarantaisi toisen hengen tai terveyden sekä käytetty häikäilemättömästi hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa ja teko on myös kokonaisuutena arvostellen törkeä.

Asianomistajat eivät ole maksaneet Kivimäelle vaadittua summaa, joten teko on jäänyt yritykseksi.

5. 20 törkeää kiristystä
2400/R/0000206/20
Rikoslaki 31 luku 4 § 1

24.10.2020 - 26.10.2020 Espoo

Kivimäki on yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa 24.10.2020 lähettänyt Vastaamon potilastietokannasta ilmeneville henkilöille kiristysviestin, jossa hän on uhkauksella vaatinut heitä luopumaan taloudellisesta edusta, johon vastaajalla ei ole ollut oikeutta.

Kivimäki on vaatinut asianomistajilta 200 tai 500 euron maksua kryptovaluuttana uhaten samalla julkaista kyseisen henkilön erittäin arkaluonteiset henkilö- ja potilastiedot sekä käyntimerkinnät internetiin, mikäli vaatimukseen ei suostuta. Asianomistajat ovat maksaneet vaaditun summan.

Kiristyksessä on uhattu vakavanlaatuisella rikoksella, joka vaarantaisi toisen hengen tai terveyden sekä käytetty häikäilemättömästi hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa ja teko on myös kokonaisuutena arvostellen törkeä.

Asianomistajien vaatimus

Asianomistajan korvausvaatimus syytekohdissa 1 ja 2

Psykoterapiakeskus Vastaamo Oy:n konkurssipesä on yhtynyt syyttäjän rangaistusvaatimukseen kohdissa 1 ja 2 sekä vaatinut, että Kivimäki velvoitetaan korvaamaan konkurssipesän oikeudenkäyntikulut rikosasiasssa korkoineen.

Muut asiassa esitetyt vaatimukset

Rikoksentekovälineen menettäminen

Kivimäki on tuomittava menettämään valtiolle:

TVP/1 (P1-palvelin) kohdat 2-11 (laitteiden sisältämä data)
TVP/2 (P2-palvelin) kohdat 2-3 (laitteiden sisältämä data)
TVP/3 (K1-palvelin kohdat 2-3 (laitteiden sisältämä data)
TVP/4 (K2-K15 -palvelimet) kohdat 15-28 (laitteiden sisältämä data)
TVP/6 (P3-palvelin) kohdat 2-3 (laitteiden sisältämä data)
TVP/8 (K16-K17 -palvelimet) kohdat 1-17 (laitteiden sisältämä data)

Vastaaja on tuomittava menettämään valtiolle laitteiden sisältämä data, koska dataa on käytetty tahallisen rikoksen tekemisessä ja sen hallussapito on laitonta. Menettämisseuraamus on tarpeen myös uusien rikosten ehkäisemiseksi.

Rikoslaki 10 luku 4 §

Todistelukustannusten korvaaminen

Kivimäki on velvoitettava korvaamaan valtiolle todistelukustannukset.

Laki oikeudenkäynnistä rikosasioissa 9 luku 1 §

Rikosuhrimaksu

Kivimäki on velvoitettava suorittamaan rikosuhrimaksu 80 euroa.

Laki rikosuhrimaksusta 2 §, 3 § ja 4 §

Muu vaatimus

Vaaditaan, että TVP/12 kohdat 1 ja 2 (Amet Asan -nimellä ja Kivimäen kuvalla varustetut henkilökortti ja passi) määrätään menetetyksi, koska matkustusasiakirjat ovat vääriä asiakirjoja, joita on tuotettu, valmistettu tai aikaansaatu rikoksella ja koska menettämisseuraamus on tarpeen uusien rikosten ehkäisemiseksi ja matkustusasiakirjat ovat erityisen soveliaita rikosten kohteeksi tai rikolliseen käyttöön.

Muu vaatimus

Pyydetään, että seuraava omaisuus määrätään palautettavaksi omistajalleen tuomion saatua lainvoiman:

TVP/1 (P1-palvelin) kohta 1
TVP/2 (P2-palvelin) kohta 1
TVP/3 (K1-palvelin) kohta 1
TVP/4 (K2-K15 -palvelimet) kohdat 15-28
TVP/6 (P3-palvelin) kohta 1
TVP/8 (K16-K17 -palvelimet) kohdat 1-17
TVP/9 (Ranskassa takavarikoitu omaisuus) kohdat 2, 3, 4, 6 ja 7
TVP/10 (Iphone-puhelin) kohta 1
TVP/11 (Kivimäen puhelimet) kohdat 1-2

Syyttäjien käsityksen mukaan:

P1, P2, P3 omistaja on Hetzner Suomi (TVP/1, (TVP/2), (TVP/6).
K1 omistaja on Hetzner Suomi (TVP/3).
K2-K15 omistaja on Hetzner Suomi (TVP/4).
K16-K17 omistaja on Saksan poliisi (lunastanut Hetzner Saksalta) (TVP/8).
Ranskassa takavarikoidun omaisuuden omistaja on Aleksanteri Kivimäki (TVP/9).
iPhone puhelimen omistaja on Dinu (TVP/10).
Kivimäen puhelimien omistaja on Aleksanteri Kivimäki (TVP/11).

Muu vaatimus

Kivimäki on ollut vapautensa menettäneenä 3.2.2023 lukien.

Kivimäki on pidettävä edelleen vangittuna.

Vastaus

Syytekohta 1

Kivimäki on kiistänyt syytteen. Tekijä ei ollut Kivimäki. Joka tapauksessa kysymys ei ollut törkeästä tietomurrosta.

Syytekohdat 2, 4 ja 5

Kivimäki on kiistänyt syytteet. Kivimäki ei ollut kiristänyt tai yrittänyt kiristää Vastaamoa tai sen asiakkaita. Tekijä oli joku muu kuin Kivimäki. Kiristyksessä käytetyt sähköpostiosoitteet eivät olleet Kivimäen taikka häneen yhdistettävissä.

Syytekohta 3

Kivimäki on kiistänyt syytteen. Joku muu kuin Kivimäki oli jakanut potilastietoja Tor-verkossa.

Kivimäen asian tutkintaan kohdistama arvostelu

Kivimäen mukaan tutkinta asiassa on ollut puutteellista, keskeneräistä ja subjektiivista, eikä yhteyttä häneen ole miltään osin näytetty. Tutkinnassa ja pääkäsittelyssä epäselvät asiat on hänen mukaansa ohitettu ja asiassa tehty kevyitä johtopäätöksiä. Rikoksentekijän selvittäminen on johdettu yksinomaan Kivimäkeen yhtenä palvelimen käyttäjänä. Ristiriitaiset asiat on tutkinnassa ja pääkäsittelyssä sivuutettu, eikä samaa tekijää epäiltyjen tekojen osalta ole voitu esitetyllä näytöllä todentaa.

Menettämisseuraamus

Kivimäki on vastustanut syyttäjän vaatimuksia menettämisseuraamusten osalta koskien palvelimilla olevaa dataa. Palvelimilla oli myös muille henkilöille kuuluvaa dataa.

Kivimäki ei ole vastustanut menettämisseuraamusta väärennettyjen asiakirjojen osalta.

Todistelu

Kirjalliset todisteet

Syyttäjät

OSIO 1 TAKAVARIKKOPÖYTÄKIRJAT

S1. Takavarikkopöytäkirja 2400/R/206/20/TVP/1 (P1) (Liite 1.1)
S2. Takavarikkopöytäkirja 2400/R/206/20/TVP/2 (P2) (Liite 1.2)
S3. Takavarikkopöytäkirja 2400/R/206/20/TVP/3 (K1) (Liite 1.3)
S4. Takavarikkopöytäkirja 2400/R/206/20/TVP/4 (K2-15) (Liite 1.4)
S5. Takavarikkopöytäkirja 2400/R/206/20/TVP/5 (Liite 1.5)
S6. Takavarikkopöytäkirja 2400/R/206/20/TVP/6 (P3) (Liite 1.6)
S7. Takavarikkopöytäkirja 2400/R/206/20/TVP/8 (K16-17) (Liite 1.7)
S8. Takavarikkopöytäkirja 2400/R/206/20/TVP/9 (Liite 1.8)
S9. Takavarikkopöytäkirja 2400/R/206/20/TVP/10 (Liite 1.9)

OSIO 2 VALOKUVA- JA VIDEOLIITTEET

S10. Valokuvaliite kuvatiedostosta beach.jpg (Liite 2.1)
S11. Valokuvaliite ransom_man -nimimerkin viesteistä Torilaudalla (Liite 2.2)
S12. Valokuvaliite testtest-nimimerkin viesteistä Ylilaudalla (Liite 2.3)
SALASSAPIDETTÄVÄ
S13. Valokuvaliite Hacker News -keskustelusta (Liite 2.4)
S14. Valokuvaliite kuva Lundbergin ajopäiväkirjasta (Liite 2.5)
S15. Valokuvaliite Waybackmachine-työkalulla haettuja historiatietoja eri sivustoista (Liite 2.6)
S16. Valokuvaliite Spamclan-nimimerkin Ylilaudalla julkaisema kuva (Liite 2.7)
S17. Valokuvaliite 3wnug3445ja7qj47.onion-sivustosta (Liite 2.8)

OSIO TIETOTEKNISEN TUTKINNAN RAPORTIT

S18. Raportti KRP/VRT/110/22 (P1) (Liite 3.1)
S19. Raportti KRP/VRT/98/22 (OPSVM) (Liite 3.2)
S20. Raportti KRP/VRT/31/23 (P2) (Liite 3.3)
S21. Raportti KRP/VRT/33/23 (K16) (Liite 3.4)

S22. Raportti KRP/VRT/114/22 (5650/R/38053/19) (Sähköpostiloki) (Liite 3.5)
S23. Raportti KRP/VRT/35/23 (SES-loki) (Liite 3.6)
S24. Raportti KRP/VRT/36/23 (pyongyang) (Liite 3.7)
S25. Raportti KRP/VRT/34/23 (K17) (Liite 3.8)
S26. RaporttiKRP/VRT/58/23 (Dinun puhelin) (Liite 3.9)
S27. Raportti KRP/VRT/59/23 (R-ilmoituksen 2400/R/268/14 datat) (Liite 3.10)
S28. Raportti KRP/VRT/111/22 (K1-K15-palvelimet) (Liite 3.11)
S29. Raportti KRP/VRT/32/23 (P3) (Liite 3.12)

OSIO TIEDONSAANTIPYYNTÖJEN VASTAUKSET

S30. Hetzner (Liite 4.1)
S31. Paypal (Liite 4.2)
S32. Google (Liite 4.3
S33. M247 (Liite 4.4.)
S34. Automatia (Liite 4.6)
S35. Worldstream (Liite 4.7)
S36. Hotelli Kämp (Liite 4.8)
S37. Apple (Liite 4.9)
S38. Ylilauta (Liite 4.10) **SALASSAPIDETTÄVÄ**
S39. OnlyFans (Liite 4.11)
S40. Osuuspankki (Liite 4.12)
S41. Ficolo (Liite 4.13)
S42. Bittiraha.fi (Liite 4.14)
S43. Sixt (Liite 4.15)
S44. Transferwise (Liite 4.16)
S45. AirBnb (Liite 4.18)
S46. Tuve (Liite 4.19)
S47. Digi- ja väestötietovirasto (Liite 4.20)
S48. Hyperoptic (Liite 4.22)
S49. LocalBitcoins (Liite 4.23)

OSIO PSYKOTERAPIAKESKUS VASTAAMO
S50. Kiristysviestit (Liitteet 5.1.1-5.1.14) **OSITTAIN SALASSAPIDETTÄVÄ**
S51. Ohjeistus potilasasiakirjojen laatimisesta (Liite 5.2.2)

OSIO LAUSUNNOT

S52. KRP sormenjälkilausunto (Liite 7.1)

OSIO LISÄTUTKINNAT

S53. Tekninen raportti KRP/VRT/102/23 (Lisätutkintapöytäkirja 3, liite 1)
S54. Forensiikkaraportti Lundbergin matkapuhelimesta (Lisätutkintapöytäkirja 3, liite 2)
S55. Yhteystieto- ja IMAP -loki sekä tiliote (Lisätutkintapöytäkirja 3, liite 3)
S56. Asiantuntijalausunto Nurmi (Lisätutkintapöytäkirja 4)
S57. Asiantuntijalausunto Mononen (Lisätutkintapöytäkirja 5)
S58. Heznerin sähköposti 27.10.2020 (Lisätutkintapöytäkirja 6, Liite 1)
S59. Heznerin sähköposti (Lisätutkintapöytäkirja 6, Liite 2)
S60. Kivimäen VTJ-ote (Lisätutkintapöytäkirja 6, Liite 3.1)
S61. Ruhasen VTJ-ote (Lisätutkintapöytäkirja 6, Liite 3.2)

S62. Tuve-lokiin liittyvät viestit (Lisätutkintapöytäkirja 6, Liite 4)
S63. Ip-osoitteen 37.156.72.25 whois-tiedot (Lisätutkintapöytäkirja 6, Liite 5)
S64. Hyperopticin asiakkuustiedusteluun liittyvä vastaus 11.9.2023 (Lisätutkintapöytäkirja 6, Liite 6.1 ja 6.2)
S65. Computopin vastaus pseudonymisoidusta luottokorttinumerosta (Lisätutkintapöytäkirja 6, Liite 7.2)
S66. Tietotekninen raportti KRP/VRT/85/23 (Lisätutkintapöytäkirja 7, Liite 1)
S67. Scanifi LLC:n liityntä tutkinnassa esille tulleisiin palvelimiin (Lisätutkintapöytäkirja 8)
S68. 100 ensin julkaistua potilastietoa (Lisätutkintapöytäkirja 9)
SALASSAPIDETTÄVÄ
S69. Listaus suoritetuista maksuista (Lisätutkintapöytäkirja 10)

S70. Computop -vastaus (Lisätutkintapöytäkirja 11, liite 1)

S71. OP -kirjautumistiedot (Lisätutkintapöytäkirja 11, liite 2)
S72. OP ote kirjautumisista (Lisätutkintapöytäkirja 11, liite 3)
S73. Whois -tiedot (Lisätutkintapöytäkirja 11, liite 4)
S74. Hetzner GmbH -palveluntarjoajan ticketit (Lisätutkintapöytäkirja 12, liitteet 1-6)
S75. Raportti tietoteknisestä tutkinnasta KRP/VRT/86/23 (Lisätutkintapöytäkirja 14, liite 3)
S76. Raportti tietoteknisestä tutkinnasta KRP/VRT/134/23 (Lisätutkintapöytäkirja 14, liite 4)
S77. Raportti tietoteknisestä tutkinnasta KRP/VRT/121/23 (Lisätutkintapöytäkirja 14, liite 5)
S78. Keskustelut,joissa nimimerkki ransom_man (Lisätutkintapöytäkirja 14, liite 6)
S79.Hetznerin tiedonsaantipyynnön vastaus koskienasiakkaan tilillään tekemiä toimintoja (Lisätutkintapöytäkirja15, liite 1)
S80. Asiantuntijalausunto ja CV Robert Cornel (Lisätutkintapöytäkirja 16, liitteet 1-3)

S81. Raportti virtuaalivaluutta-analyysista **OSITTAIN SALASSAPIDETTÄVÄ**
S82.Raportti tietoteknisestä tutkinnasta KRP/VRT/135/23 (Lisätutkintapöytäkirja 18 Liite 2)
S83. Osoiterypäs Y (Lisätutkintapöytäkirja 18 liite 3)
S84. Osoiterypäs X–Binance (Lisätutkintapöytäkirja 18 liite 4)
S85. Osoiterypäs Y–Binance (Lisätutkintapöytäkirja 18 liite 5)
S86. Coinbase John Frisberg–perustiedot jatunnistautumiskuvat (Lisätutkintapöytäkirja18 liite 6)
S87. Onnistuneet XMR siirrot (Lisätutkintapöytäkirja18 liite 7)

S88. Binance – Anussucker@cs.email (Lisätutkintapöytäkirja 18 liite 10)
S89. Binance – fucfuckfuck@cs.email (Lisätutkintapöytäkirja 18 liite 11)
S90. Swaplab-vastaus (Lisätutkintapöytäkirja 18 liite 12)
S91. Osoiterypäs C (Lisätutkintapöytäkirja 18 liite 13)
S92. Request for disclosure (Lisätutkintapöytäkirja 18 liite 14.1)
S93. Julius Aleksanteri TomminpoikaKivimäki-accounts_balance (Lisätutkintapöytäkirja 18 liite 14.2)
S94. Julius Aleksanteri Tomminpoika Kivimäki-txn_exported(Lisätutkintapöytäkirja 18 liite 14.3)

S95. JAT_transaktiot (Lisätutkintapöytäkirja 18 liite 14.4)
S96. Localbitcoins - Top-BTC (Lisätutkintapöytäkirja 18 liite 15)
S97. Osoiterypäs Z (Lisätutkintapöytäkirja 18 liite 17)
S98. Daniel Newhard Onfido report (Lisätutkintapöytäkirja 18 liite 18.1)
S99. Transaction history & Login (Lisätutkintapöytäkirja 18 liite 18.2)
S100. Top-BTC käännökset (Lisätutkintapöytäkirja 18 liite 19)
S101. Osoiterypäs C (Lisätutkintapöytäkirja 18 liite 20)
S102. Raportti tietoteknisestä tutkinnasta KRP/OF/4/24 (Lisätutkintapöytäkirja 20 Liite 5)
S103. Raportti tietoteknisestä tutkinnasta KRP/OF/8/24 (Lisätutkintapöytäkirja 20 Liite 7)
S104. Tiedot espanjalaisesta ip-numerosta (Lisätutkintapöytäkirja 21 Liite 1)
S105. Siena-kyselyjen tiedot (Lisätutkintapöytäkirja 21 Liite 2)
S106. Ylilauta (Lisätutkintapöytäkirja 21 Liite 3 ja 4)
S107. Eucaris-tiedot (Lisätutkintapöytäkirja 21 Liite 5)
S108. Arvostelu 0532 KWP (Lisätutkintapöytäkirja 21 Liite 6)
S109. Maksutiedot daniel@safe.im (Lisätutkintapöytäkirja 21 Liite 7)

Vastaaja

V1. S64 (Lisätutkintapöytäkirja 6 s. 17-19, liite 6.2)
V2. Vuokrasopimus 20.9.
V3. Hyperoptic staattinen osoite (https://www.hyperoptic.com/faq/posts/how-do-i-set-up-port-forwarding/) ja lisämaksu
V4. S19, Etptk s.781, liite 3.2 OPSVM
V5. S19, Etptk s. 782-783, liite 3.2 OPSVM
V6. S19, Etptk s. 798, liite 3.2 kohta 5.2.1 openmysqlcreds
V7. S19, Etptk, s. 798, liite 3.2 kohta 5.2.2.1 mysql.tgz/95.175.109.219
V8. S19, Etptk s.799, liite 3.2 kohta 5.2.4.1 Vastaamoon liittyvä haku
V9. S19, Etptk s. 821, liite 3.2 joku tallentaa Simonin tiedostoon (simons)
V10. S19, Etptk s. 825, liite 3.2 tallennetaan nykyiselle P1, rivit 6098-6100
V11. S20, Etptk s. 908, liite 3.3 Silasdev virtuaalipalvelin, ntopng valvontatyökalu vrt s. 1538 Netflow-loki
V12. S20, Etptk s.1005-1006, liite 3.3 Wireguard-avaimet 13 kpl.
V12.1 S20, Etptk s. 1008, liite 3.3
V13. S20, Etptk s. 1038 ja s. 1023, liite 3.3
V14. S20, Etptk s. 1043, liite 3.3 Projekti scan/pma
V15. S21, Etptk s. 1141, liite 3.4 K16
V16. S24, Etptk s. 1243 ja -1285, liite 3.7 Pyongyang
V17. S30, Etptk s. 1505, liite 4.1.1
V18. S30, Etptk s. 1518 ja s. 1532, liite 4.1.2
V19. S30, Etptk s. 1536, liite 4.1.2
V20. S31, Etptk s. 1547, liite 4.2.2
V21. S32, Etptk s. 1551 -, liite 4.3.1; S33, Etptk s. 1556 -, liite 4.4.1
V21.1 Etptk s. 1559-1561, liite 4.5.1
V22. S38, Etptk s. 1728-1733, liite 4.10.2
V23. S38, Etptk s. 1734, liite 4.10.2
V24. S50, Etptk s. 2065, liite 5.1.1
V25. S30, Etptk s. 1509 ja 1513, liite 4.1.1
V26. S31, Etptk s. 1539, liite 4.2.1
V27. Hetznerin sähköpostiviesti
V28. Brade (kryptovaluutta-asiantuntija), asiantuntijalausunto

V29. S19, s. 774 ja 908-909, lisäptk 8, s. 315, lisäptk 14, s. 9 ja 149 ja aikajana.
V30.1. Kuvankaappaus IP-osoitteesta 147.161.123.116
V30.2. IP-osoite, rivit 131-762 (merkitty punaisella)
V31. S19, liite 3.2., s. 840
V32. Lisätutkintaptk 20 Liite 3 liite 1: K17 /root/. bash-history sivut 50-54 rivinrot 2027-2213
V33. Lisätutkintaptk 20 Liite 3 liite 2: proxyshop /root/. zsh_history sivu 134 rivinrot 2877-2883, 2922-2923 sivu 179 rivinrot 4824- 4827
V34. Lisätutkintaptk 20 Liite 4 Liite 1: Asetustiedostot K17 s. 220-223
V35. Lisätutkintaptk 20 Liite 4 Liite 3: Asetustiedostot P2 s. 248-253
V36. Lisätutkintaptk 20 Liite 4 Liite 4. Asetustiedostot K1 s. 256-261
V37. Linkedin ote Vanderpot

Muu oikeudenkäyntiaineisto

Syyttäjät

SO1. Vastaamo.tar -jälkeiset tapahtumat (Lisätutkintapöytäkirja 14, liite 1)
SO2. Aleksanteri Kivimäen käyttämät tunnistetiedot (Esitutkintapöytäkirjan liite 8.3)
SO3. Aikajana (Liite 8.1)
SO4. Keskeiset palvelinyhteydet (Liite 8.2)
SO5. Havaintokuva Monero Co-Spend (Lisätutkintapöytäkirja 18 liite 8)
SO6. Havaintokaavio P3–anussucker–fuckfuckfuck (Lisätutkintapöytäkirja 18 liite 9)
SO7. Havaintokaavio P3ja kiristys (Lisätutkintapöytäkirja 18 liite 16)
SO8. Vastaukset puolustuksen väitteisiin (Lisätutkintapöytäkirja 18 liite 21)
SO9. Orbituary for Robert Francis Cornell
SO10. Mason Drive 3 - Google Maps
SO11. Mason Drive 3 milford Robert Cornell
SO12. Aikajana

Vastaaja

VO38. Europolin artikkeli IP-osoitteiden jakamisen riskeistä (https://www.europol.europa.eu/media-press/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online)
VO39. Artikkeli IP-osoitteiden jakamisesta (LTE / 5G-reitittimet - Carrier Grade NAT:n selittäminen – Zyxel Support Campus EMEA.)
VO40. Artikkeli ”Digiavain tarjoaa tilaisuuden tietovarkaalle” (Editor Helsinki)
VO41. Pro Gradu -tutkielma ”Tunkeutumisen ja käyttäjän todennuksen poikkeamien
havaitseminen verkkoliikenteessä koneoppimista hyödyntämällä” Henri Hämäläinen s. 54 4.3 Käyttäjän todennuksen hyökkäykset ja SSH-protokolla

Henkilötodistelu

1. Vastaaja Kivimäki
2. Todistaja Lähteenlahti
3. Todistaja Väänänen
4. Todistaja Ruhanen

5. Asiantuntija Nurmi
6. Asiantuntija Mononen
7. Todistaja Berg
8. Todistaja Lilja
9. Todistaja Rantalainen
10. Asiantuntija Mäntymaa
11. Todistaja Pursiainen
12. Todistaja Naughton
13. Asiantuntija Brade

Tuomion perustelut

Asian taustaa

Psykoterapiakeskus Vastaamo Oy:stä

Psykoterapiakeskus Vastaamo Oy (jatkossa myös Vastaamo) on vuonna 2008 perustettu suomalainen yritys, joka on toiminut eri puolilla Suomea. Yhtiöllä on ollut lupa tuottaa lääkärin ja erikoislääkärin vastaanottotoimintaa, psykologin palveluita sekä terapeuttista toimintaa eli fysioterapiaa ja psykoterapiapalveluita. Vastaamon asiakaskunta on ollut laaja, ja sillä on ollut sen toiminnan aikana lähes 50.000 asiakasta sekä noin 600.000 asiakaskäyntiä. Vastaamo on tuottanut maksusitoumuksilla palveluita muun muassa julkiselle sektorille, vakuutusyhtiöille, eläkelaitoksille ja yksityisille yrityksille. Sen asiakkaina on ollut niin ala- kuin täysikäisiäkin henkilöitä. Asiakkaat ovat pääosin olleet Suomen kansalaisia ja asuneet Suomessa, mutta osalla heistä on ollut ulkomainen kansalaisuus ja osa heistä on asunut tai muuttanut syytteessä kerrottujen tapahtumien jälkeen ulkomaille.

Vastaamon psykoterapia- ja psykologin palveluita saaneilla asiakkailla on ollut erilaisia ja eriasteisia pääosin jaksamiseen tai mielenterveyteen liittyviä ongelmia. Lievimmillään ongelmat ovat liittyneet esimerkiksi opiskelu- tai työelämässä jaksamiseen taikka parisuhteen tilanteeseen. Vakavimmillaan Vastaamon potilailla on ollut itsetuhoisia ajatuksia.

Vastaamon toiminta on ollut valtakunnallista ja laajamittaista, ja sillä on ollut toiminnassaan velvollisuus noudattaa palveluitaan koskevaa lainsäädäntöä sekä toimivaltaisten viranomaisten antamia määräyksiä ja ohjeita. Yhtiöllä on ollut asiakkaitaan koskeva potilasrekisteri ja potilastietokanta, johon asiakkaiden henkilö- ja yhteystiedot sekä käynnit ja käyntien sisältö on Vastaamon toimintaa koskevan ja yhtiössä sitä varten annetun ohjeistuksen ja koulutuksen mukaisesti kirjattu. Lääkäreiden ja esimerkiksi yhtiön psykoterapeuttien tekemät kirjaukset ovat olleet sisällöltään vaihtelevia, vaihdellen pelkkää käyntikertaa koskevasta kirjauksesta aina yksityiskohtaisiin potilaan vointia ja hoitosuunnitelmaa koskeviin kirjauksiin. Kirjaukset ovat sisältäneet hyvinkin arkaluonteisia, potilaiden mielenterveyteen ja yksityiselämään liittyviä erittäin arkaluonteisina pidettäviä tietoja.

Vastaamon toiminta on syytteessä kerrottujen tapahtumien jälkeen päättynyt. Yhtiö on ollut selvitystilassa 28.1.–15.2.2021 välisen ajan ja asetettu konkurssiin Helsingin käräjäoikeuden 15.2.2021 tekemällä päätöksellä.

Psykoterapiakeskus Vastaamo Oy:n potilastietokannasta ja siihen tunkeutumisesta

Vastaamon potilastietokanta on ollut sähköinen yhtiön itse valmistama MySQL-tietokanta, johon on ollut esillä olevan asian tapahtuma-ajankohtana kirjattuna yli 30.000 potilaan käyntitiedot. Potilastietokanta on ollut

tallennettuna ulkoisen palveluntarjoajan palvelimelle. Vastaamo osti sanotut palvelinpalvelut aikaisemmin saksalaiselta Hetzner Online GmbH:lta (jatkossa myös Hetzner) Saksasta, mutta alkuvuonna 2018 se siirsi Saksasta vuokratun palvelimen Ficolo Oy:n palvelinsaliin Poriin. Syytteessä kerrottujen rikosten tapahtuma-aikana potilastietokannan sisältänyt palvelin sijaitsi siten Suomessa.

Vastaamon tietojärjestelmään on ollut pääsy internetin kautta siihen oikeutetuille henkilöille eli esimerkiksi yhtiön psykoterapeuteille. Pääsy potilastietokantaan on ollut avoin ainakin 26.11.2017 ja 13.3.2019 välisen ajan. Yhtiön tietojärjestelmässä on ollut 23.11.2017 lukien tietoturva-aukko, joka on mahdollistanut järjestelmään tunkeutumisen ulkopuolelta. Tietojärjestelmään ja potilastietokantaan pääsy ei ole tuolloin edellyttänyt tiettyä vain oikeutettujen tahojen hallussa ollutta salasanaa tai salasanoja, vaan pääsy on ollut mahdollista ilman salasanaa.

Vastaamon potilastietokannan lokitietojen mukaan potilastietokannan niin sanotussa http-portissa on käyty ulkopuolisen toimijan toimesta ensin 25.11.2018 klo 20:48:45 (UTC). Syyttäjät ovat kutsuneet tätä internetin skannauksen yhteydessä tapahtuneeksi ”haisteluksi”. Vastaamon palvelinpalvelut tarjonneen Ficolo Oy:n palvelimen niin sanotun netflow-datan mukaan potilastietokantaan on otettu uusi yhteys heti seuraavana päivänä 26.11.2018 klo 04:38:03 (UTC). Tämä potilastietokannan porttiin 3306 otettu yhteys on kestänyt klo 04:41:56 (UTC) saakka. Sanotun yhteyden aikana Vastaamon potilastietokanta on pystytty ulkopuolisen toimijan toimesta oikeudettomasti kopioimaan.

Psykoterapiakeskus Vastaamo Oy:öön kohdistuneesta kiristyksestä

Tietojärjestelmään tunkeutuminen ja potilastietokannan oikeudeton kopioiminen on tullut Psykoterapiakeskus Vastaamo Oy:n tietoon vasta 28.9.2020, kun Vastaamon toimitusjohtaja ja kaksi yhtiön järjestelmäarkkitehtia saivat tapahtunutta koskevan sähköpostiviestin. Viestissä heille ilmoitettiin, että viestin lähettäjällä on hallussaan kopio yhtiön potilastietokannasta. Vastaamo sai seuraavan asiaa koskevan viestin 29.9.2020, ja sen jälkeen, kun viestiin vastattiin 30.9.2020, Vastaamolta vaadittiin samana päivänä 40 bitcoinin eli tapahtuma-aikaan noin 366.000 euron suuruisia lunnaita uhkaamalla julkaista potilastietoja, jos vaatimuksiin ei suostuta. Vastaamo ei suostunut maksamaan kiristäjälle tämän vaatimia lunnaita. Sen sijaan yhtiö ilmoitti 30.9.2020 asiasta poliisille, joka kirjasi tapahtuneesta rikosilmoituksen.

Edellä kerrotun jälkeen sähköpostikirjeenvaihto kiristäjän kanssa jatkui Keskusrikospoliisin toimesta. Tämän kirjeenvaihdon yhteydessä kiristäjä lähetti Vastaamolle 7.10.2020 muun muassa Vastaamon MySQL-tietokannan niin sanotut taulut sekä ohjeita bitcoinien hankkimisesta. Lisäksi kiristäjä toimitti Vastaamolle esimerkkeinä hallussaan olevista tiedoista yksittäisten potilaiden tietoja, jotka vastasivat yhtiön potilastietokannan tietoja. Tämän jälkeen Keskusrikospoliisi teki kiristäjän Vastaamolle ilmoittamaan bitcoin-osoitteeseen 0,1 bitcoinin suuruisen maksun eli niin sanotun valeoston, jonka siirtymistä eteenpäin virtuaalivaluuttana se ryhtyi myöhemmin s elvittämään.

Vastaamon potilastietojen julkaisemisesta Tor-verkon keskustelupalsta Torilaudalla

Sen jälkeen, kun Vastaamo ei suostunut maksamaan kiristäjän vaatimia lunnaita, nimimerkki ransom_man ilmoitti 21.10.2020 Tor-verkon keskustelupalstalla Torilaudalla saaneensa haltuunsa Vastaamon

potilastietokannan. Tämän jälkeen samana päivänä kiristäjä pystytti Tor-verkkoon piilopalvelun eli niin sanotun Onion-sivuston ja latasi sinne 100 ensimmäisen Vastaamon potilaan potilastiedot. Nimimerkki ransom_man ilmoitti julkaisevansa 100 potilastietoa lisää joka päivä, kunnes lunnasvaatimukseen suostutaan. Nimimerkin viestissä oli myös linkki edellä kerrottuun Tor-verkon piilopalveluun. Seuraavana päivänä eli 22.10.2020 tekijä lisäsi uhkaamallaan tavalla onion-sivustolle 100 uutta potilastietoa. Lisäksi ransom_man julkaisi torilautaviesteissään 23.10.2020 Vastaamon toimitusjohtajan kotiosoitteen sekä potilastietokannassa olleita poliisimiesten sähköpostiosoitteita.

Lokakuun 23. päivänä 2020 kiristäjä teki virheen ladatessaan edellä kerrottuun piilopalveluun vastaamo.tar-nimisen tiedoston, joka sisälsi 100 uuden Vastaamon asiakkaan potilastietojen asemesta julkaisemisessa käytetyn OPSVM-nimisen virtuaalipalvelimen pääkäyttäjän koko kotihakemiston. Virheen tapahduttua nimimerkki ransom_man kommentoi sitä Torilaudalla. Pian tämän jälkeen piilopalvelu poistettiin Tor-verkosta. Keskusrikospoliisi ja eräs ulkoinen toimija ehtivät kuitenkin ladata piilopalvelun pääkäyttäjän kotihakemiston sekä osan potilastietokannasta ennen piilopalvelun poistamista.

Vastaamon potilaisiin kohdistuneesta kiristyksestä ja kiristyksen yrityksestä

Edellisessä kappaleessa kerrottua virhettä seuranneena päivänä eli 24.10.2020 kiristäjä lähetti lähes 28.000 Vastaamon asiakkaan sähköpostiosoitteeseen kiristysviestin. Viestissä asiakkaita vaadittiin maksamaan 200 euron arvosta bitcoineja vuorokauden kuluessa tai 500 euron arvosta bitcoineja kolmen vuorokauden kuluessa. Jokaisessa viestissä oli yksilöllinen bitcoin-osoite, johon maksu piti suorittaa.

Vastaamon asiakkaista 20 suoritti kiristäjälle tämän vaatiman maksun, muut eivät maksua suorittaneet.

Nimimerkki ransom_man ilmoitti 24.10.2020 Torilaudalla olevansa myös Vastaamon asiakkaiden kiristäjä.

Syyttäjien syytteestä ja Kivimäen vastauksesta

Syyttäjien syyte

Syyttäjien syyte perustuu keskeisiltä osin Keskusrikospoliisin tekemään tietotekniseen tutkintaan, jossa poliisi on syyttäjien mukaan kiristäjän tekemän virheen jälkeen pystynyt selvittämään kohdissa 1–5 kuvatuissa rikoksissa käytetyn palvelinkokonaisuuden. Tämä kokonaisuuden palvelimet poliisi on nimennyt niiden tilaajatietojen perusteella P- ja K-palvelimiksi. Lisäksi Keskusrikospoliisi on pystynyt selvittämään syytteessä kerrottujen rikosten kannalta merkittävien palvelinten vahvan salauksen, tietomurrossa todennäköisesti käytetyt työkalut (ohjelmistot), palvelimilla käytetyt salausavaimet sekä IP-osoitteita, joista palvelimille on oltu tekoaikana yhteydessä. Keskusrikospoliisi on pystynyt syyttäjien mukaan oikeudenkäynnin aikana selvittämään myös sen, mihin sen tekemä 0,1 bitcoinin valeosto oli siirtynyt.

Syyttäjien mukaan tietotekninen tutkinta on osoittanut, että Kivimäki on käyttänyt edellä kerrottuja P- ja K-palvelimia sekä rikosten tekemisessä käytettyä P2-palvelimella ollutta OPSM-virtuaalipalvelinta. Kivimäki oli myös käyttänyt palvelinten salausavaimia ja ollut palvelimiin yhteydessä käytössään olleista IP-osoitteista välittömästi samana aikana, kun kohdissa 2–5 kuvatut

rikokset oli tehty. Lisäksi Kivimäki oli samaan aikaan osallistunut tapahtunutta koskevaan Ylilautakeskusteluun nimimerkillään Spamclan, minkä Kivimäki on myös tunnustanut. Keskusrikospoliisin valeostokin oli syyttäjien mukaan päätynyt Kivimäen käytössä olleelle Revolut-pankin tilille. Syytettä tuki syyttäjien mukaan vielä sekin, että Kivimäki oli syyllistynyt vastaaviin rikoksiin myös aiemmin.

Kivimäen vastaus

Kivimäki on kiistänyt syyttäjien syytteen. Hänen mukaansa syytteessä kerrotut rikokset olivat riidattomasti tapahtuneet, mutta hän ei ollut niihin syyllistynyt.

Kivimäki ei ollut käyttänyt edellä kerrottuja palvelimia syyttäjien esittämällä tavalla. Poliisin P-palvelimiksi nimeämiä palvelimia tai OPSVM-nimistä virtuaalipalvelinta hän ei ollut juurikaan käyttänyt. K-palvelimet taas olivat olleet Scanifi LLC -nimisen (jatkossa myös Scanifi) yhtiön palvelimia, joita Kivimäki on käyttänyt vain laillisessa tarkoituksessa. Scanifin salausavaimina käytetyt SSH-avaimet olivat olleet Scanifissa omaksutun käytännön mukaisesti jaettuja, ja sellaisina hän on niitä mahdollisesti käyttänyt. Scanifin palvelimia ja salausavaimia on käyttänyt moni muukin henkilö kuin Kivimäki.

Mikään palvelimilla tehty toimi, salausavaimilla tapahtunut kirjautuminen tai kirjautumissa käytetty IP-osoite ei Kivimäen mielestä osoittanut, että hän olisi syyllistynyt niihin rikoksiin, joista syyttäjät ovat vaatineet hänelle rangaistusta. Vaikka Kivimäki oli osallistunut kiristysrikosten aikaan Ylilaudalla käytyyn keskusteluun Spamclan-nimimerkillä ja jakanut tuolloin linkin piilopalveluun, jossa Vastaamon asiakkaiden tietoja oli jaettu, syytteessä kerrottujen rikosten tekemiseen hän ei ollut kuitenkaan osallistunut. Kivimäen Ylilaudalla käymän keskustelun ajallinen yhteys syytteessä kerrottuihin rikoksiin samoin kuin Kivimäen Revolut-tilille tehdyt suorituksetkaan eivät antaneet aihetta arvioida Kivimäen syyllisyyttä toisin.

Asiassa esitetystä näytöstä

Keskusrikospoliisin tietoteknisestä tutkinnasta

Keskusrikospoliisi aloitti tapahtunutta koskevan tietoteknisen tutkinnan saatuaan kiristäjän 23.10.2020 tekemän potilastietojen julkaisemisessa käytetyn ns. vastaamo.tar-paketin konfigurointivirheen jälkeen ladattua Tor-verkossa OPSVM-nimisen virtuaalipalvelimen root-käyttäjän kotihakemiston sekä osan Vastaamon potilastietokannasta. Kotihakemiston kautta Keskusrikospoliisi sai selvitettyä OPSVM-palvelimelle kirjautumisessa käytetyn salausavaimen eli SSH-avaimen ja tämän avaimen niin sanotun sormenjäljen WI8rxlR/gE5C95FQ/EKzA2DEDwiLzC3fPiyQl5eL0hc (jatkossa myös WI8-avain). Lisäksi Keskusrikospoliisi sai selvitettyä Hyperoptic-nimisen palveluntarjoajan IP-osoitteen 37.156.72.25, josta OPSVM-palvelimelle oli oltu yhteydessä 30.5. ja 26.10.2020 välisenä aikana. Tämän jälkeen Keskusrikospoliisi pystyi selvittämään, että OPSVM-palvelimelta oli oltu edellä kerrottua WI8-avainta käyttäen yhteydessä Hetzner GmbH:n Tuusulassa sijainneeseen palvelimeen, jonka Keskusrikospoliisi nimesi P1-palvelimeksi ja jonka se takavarikoi 25.10.2023. Hetzneriltä saamiensa P1-palvelimen tilaajatietojen perusteella Keskusrikospoliisi löysi Hetznerin samasta palvelinsalista kaksi muutakin palvelinta, jotka se nimesi P2- ja P3-palvelimiksi. Keskusrikospoliisi takavarikoi P2-palvelimen 26.10.2020 ja P3-palvelimen 2.2.2021. P1- ja P2-palvelinten kiintolevyt oli suojattu samalla vahvalla suojauksella, jonka

Keskusrikospoliisi sai avattua. P2-palvelin oli kuitenkin ehditty tyhjentää ennen takavarikkoa, samoin P3-palvelin pääosin. Keskusrikospoliisi sai kuitenkin luettua osan levyjen tiedoista.

Takavarikoidun P1-palvelimen teknisessä tutkinnassa Keskusrikospoliisi sai selvitettyä, että siltä oli oltu yhteydessä palvelimeen, joka sijaitsi sekin Hetznerin palvelinsalissa Tuusulassa. Keskusrikospoliisi nimesi tämän palvelimen K1-palvelimeksi, ja sen tilaajatietojen perusteella poliisi löysi 16 muutakin palvelinta (K2-K17), joista palvelimet K2–K15 sijaitsivat Hetznerin palvelinsalissa Tuusulassa ja palvelimet K16 ja K17 Hetznerin Saksassa sijainneessa palvelinsalissa. K17-palvelin poikkesi muista palvelimista erittäin suuren massamuistinsa osalta, ja siltä Keskusrikospoliisi löysi varmuuskopion edellä kerrotusta P2-palvelimesta, jolla OPSVM-niminen virtuaalipalvelin on vuodesta 2019 lukien sijainnut. K1-palvelin on takavarikoitu 26.10.2020, K2–K15-palvelimet 9.12.2020 ja K16–K17-palvelimet 18.07.2022.

Syyttäjien mukaan Keskusrikospoliisin tietotekninen tutkinta on osoittanut, että niin syytekohdassa 1 kerrottu tietomurtorikos kuin syytekohdissa 2–5 kerrotut kiristysrikokset ja yksityiselämää loukkaava tiedon levittämisrikoskin on tehty OPSVM-nimisellä virtuaalipalvelimella, joka kohdissa 2–5 kuvattujen tekojen aikaan sijaitsi P2-palvelimella. OPSVM-palvelimen kotihakemiston poliisi sai ladattua kiristäjälle tapahtuneen konfigurointivirheen jälkeen, ja itse palvelimen poliisi löysi K17-palvelimella sijainneesta P2-palvelimen varmuuskopiosta.

Syyttäjät ovat kohdassa 1 vedonneet OPSVM-palvelimen komentohistoriaan, josta Keskusrikospoliisi on löytänyt tietomurrossa käytetyn ecatel-nimisen palvelimen komentohistorian. Sen mukaan ecatel-palvelimella oli 25.11.2018 skannattu koko internetiä ja lopulta 29.11.2018 siirretty muun muassa mysql.tgz-niminen tiedosto OPSVM-palvelimelle. Tämä mysql.tgz-tiedosto on sisältänyt internetissä skannattuja IP-osoitteita, joista yksi on ollut Vastaamon potilastietokannan IP-osoite. Skannauksessa käytetyn selaimen tunnistetieto on lisäksi Keskusrikospoliisin tekemässä tietoteknisessä tutkinnassa löytynyt Vastaamon potilastietokannan lokitiedoista.

OPSVM-virtuaalipalvelimelta on lisäksi löytynyt kohdissa 2 ja 3 kuvatun Vastaamon kiristämisen ja sen asiakkaiden tietojen levittämisen aikainen komentohistoria, jonka mukaan OPSVM-palvelinta oli käytetty Vastaamon potilastietokannan käsittelyyn. Potilastietokannasta oli tehty kiristyksessä käytetyt potilaskohtaiset niin sanotut tekstitiedostot, joihin on tekoaikana myös kohdistettu suomenkielentaitoa edellyttäneitä hakuja. OPSVM-palvelimella oli myös pystytetty tietojen levittämisessä ja kiristyksessä käytetty Tor-piilopalvelu eli niin sanottu onion-sivusto, ja ylläpidetty sitä. OPSVM-palvelimelta on myös löytynyt muun muassa kiristysviestien lähettämiseen käytetyt Vastaamon asiakkaiden sähköpostiosoitteet sisältänyt tiedosto. OPSVM-virtuaalipalvelimella ylläpidetystä piilopalvelusta taas on löytynyt keskustelupalsta Ylilaudalla käytyjä kiristystoimien aikaisia keskusteluketjuja.

Viimeksi mainittujen kohdissa 2 ja 3 kuvattujen rikosten tekoaikana OPSVM-palvelimelle oli kirjauduttu SSH-avaimella, jonka sormenjälki oli WI8-alkuinen. Sanottuja yhteyksiä oli myös otettu Hyperoptic-nimisen palveluntarjoajan Lontoossa sijainneesta IP-osoitteesta 37.156.72.25.

Syyttäjien mukaan Kivimäki on käyttänyt kaikkia edellä kerrottuja palvelimia P1–P3 ja K1–K17 sekä palvelimilla sijainneita eri virtuaalipalvelimia kuten OPSVM-palvelinta, ja ollut sormenjäljeltään WI8-alkuisen pääkäyttäjätasoisen

SSH-avaimen ainoa käyttäjä. IP-osoite 37.156.72.25 taas on sijainnut Lontoossa olleessa asunnossa, jossa Kivimäki on tekoaikana asunut. Kivimäki on myös tehnyt Vastaamon tietomurtoon liittyneitä Ylilauta-viestejä Spamclan-nimimerkillä juuri syytekohdissa 2 ja 3 kerrottujen rikosten tekoaikoina. Oikeudenkäynnin aikana jatketussa teknisessä tutkinnassa on syyttäjien mukaan lisäksi pystytty selvittämään, että Keskusrikospoliisin tekemän valeoston arvo on siirtynyt lopulta Kivimäen Revolut-pankissa olevalle tilille.

Asiakokonaisuuden kannalta merkitykselliset palvelimet

Tekokokonaisuuteen liittyy sekä fyysisiä palvelimia että Proxmox-virtualisointiohjelmistolla ylläpidettyjä lukuisia eri virtuaalipalvelimia. Poliisi on ryhmitellyt tapauskokonaisuuteen kuuluvat fyysiset palvelimet P-sarjaksi ja K-sarjaksi. P-sarjassa olleet palvelimet on jaettu palvelimiin P1–P3 ja K-sarjassa olleet palvelimet puolestaan K1–K17. Vastaamo-kokonaisuuden kannalta olennaisia virtuaalipalvelimia ovat olleet lähinnä virtuaalipalvelimet, jotka on nimetty nimillä rooter, vpn, irc, gogs, silasdev ja OPSVM. Virtualisointiohjelmisto, jolla virtuaalipalvelimet ovat sijainneet, on ollut P2-palvelimella.

Kivimäen kertomus palvelinten käyttämisestä

Kivimäki on kertonut käyttäneensä poliisin P-palvelimiksi nimeämiä palvelimia vain P2-palvelimella olleen Antipeace-nimimerkin tarjoaman niin sanotun VPN-palvelun vuoksi. Poliisin K-palvelimiksi nimeämät palvelimet olivat sen sijaan olleet Scanifi LLC -nimisen yhtiön palvelimia. Kivimäki oli toiminut sanotussa yrityksessä, ollut yksi sen omistajista ja esimerkiksi maksanut K-palvelinten vuokria. Kivimäki on myös kertonut käyneensä silloin tällöin OPSVM-palvelimella, tosin lähinnä mielenkiinnosta käydessään katsomassa, mitä se oli sisältänyt. Lisäksi Kivimäki oli kertomansa mukaan mahdollisesti käyttänyt yhtiön salausavaimina käytettyjä SSH-avaimia. Sanotut salausavaimet olivat kuitenkin olleet Scanifissa omaksutun käytännön mukaisesti jaettuja.

Kivimäki oli kertomansa mukaan käyttänyt Scanifin palvelimia ja SSH-avaimia nimenomaan Scanifin liiketoimintaan liittyneisiin laillisiin toimiin. Scanifin palvelimia oli lisäksi käyttänyt moni muukin henkilö kuin Kivimäki, samoin kirjautumisessa käytettyjä jaettuja SSH-avaimia. Jokaista K-palvelinta tai palvelimilla olleita virtuaalipalvelimia Kivimäkikään ei ollut käyttänyt.

Kivimäki on myöntänyt osallistuneensa aktiivisesti Ylilaudalla kiristysrikosten aikaan käytyyn keskusteluun ja jakaneensa tuolloin linkin edellä kerrottuun Tor-verkossa olleeseen piilopalveluun. Syytteessä kerrottujen rikosten tekemiseen hän ei ollut kuitenkaan osallistunut.

Scanifi LLC:n toiminnasta ja toiminnan tarkoituksesta

Kivimäki on kertonut perustaneensa Delawaren osavaltioon Yhdysvaltoihin rekisteröidyn Scanifi LLC -nimisen yrityksen yhdessä jo yli 10 vuotta tunteneensa Vanderpotin kanssa. He ja Naughton omistivat yrityksestä kukin yhden kolmasosan ja toimivat vuorollaan sen toimitusjohtajina. Kivimäki ei ole muistanut, milloin yritys perustettiin, mutta syytteessä kerrotun tietomurron aikana vuonna 2018 sen toiminta ei ollut vielä alkanut.

Scanifin liikeideana oli skannata internetissä olevien palvelimien tietoliikenneportteja ja hankkia näin toimimalla historiallista dataa eri

toimijoiden tietoturvan tasosta ja heikkouksista. Tätä dataa tai tietoa oli sen jälkeen tarkoitus tarjota kybervakuutuksia tarjoaville yrityksille niiden liiketoimintaa varten. Kivimäki ja Vanderpot olivatkin aiemmin seuranneet kahta yritystä, joiden liikeidea oli ollut sama, mutta jotka eivät heidän mielestään olleet onnistuneet tuotteistamaan palveluaan.

Scanifin toimintaa varten tarvittiin palvelimia, ja ne vuokrattiin vuodesta 2019 alkaen Hetzneriltä. Sopimukset palvelinten vuokraamisesta teki Vanderpot, ja niiden vuokrat maksettiin Vanderpotin ja Kivimäen luottokorteilla. Se, että fyysiset palvelimet sijaitsivat Suomessa, oli Kivimäen mukaan puhdasta sattumaa. Palvelimia oli yhteensä 17, ja niillä muodostettiin niin sanottu klusteri. Palvelimilla kehitettiin muun muassa skannaustyökalua ja ylläpidettiin esimerkiksi projektinhallintaohjelmaa.

Scanifin toiminnassa tekninen osaaminen oli Vanderpotilla ja liiketoiminnallinen osaaminen ja sijoittajien hankkimista koskeva ymmärrys Kivimäellä. Kivimäki ei käsittääkseen edes osallistunut Scanifin työkalujen tekniseen kehittämiseen. Scanifin liiketoiminta ei Kivimäen mukaan ehtinyt aiheuttaa suuria menoja. Hän oli keskustellut yhtiön toiminnasta eri sijoittajien kanssa, mutta tuloja liiketoiminnalla ei ehditty saada. Scanifin liiketoimintaa ei lopulta saatu koskaan käyntiin.

Todistajana oikeudenkäynnissä kuultu Naughton on kertonut Scanifin liiketoimintaideasta pääosin samalla tavoin kuin Kivimäki. Yrityksen tavoitteena oli kehittää internetin skannaustyökalu ja kerätä sillä historiadataa, jota olisi voitu myydä eri yrityksille. Tuotekehityksen pohjana käytettiin skannaustyökalua, jonka ilmeisesti Vanderpot oli jostain tuonut. Scanifin lopullinen tavoite oli kehittää skannaustyökalu sellaiseksi, että se olisi voitu myydä eteenpäin. Skannaustyökalua ei Naughtonin mukaan saatu kuitenkaan koskaan toimimaan. Naughton on arvioinut, että tuotteen valmiusaste jäi lopulta vain noin kymmeneen prosenttiin eikä sitä koskaan päästy edes testaamaan. Scanifin toiminta päättyi viimeistään, kun poliisi takavarikoi yrityksen palvelimet. Naughton oli takavarikosta kertomansa mukaan ”shokissa”. Kivimäki kuitenkin rauhoitteli häntä ja Vanderpotia kertomalla, että palvelimet oli jo tyhjennetty.

Naughton ei ollut mukana Scanifin toiminnassa sen alusta lukien vaan liittyi mukaan myöhemmin. Hän toimi yrityksessä tuotekehitystehtävissä. Hänen mukaansa yrityksen toiminnassa olivat mukana Kivimäen ja Vanderpotin lisäksi hän ja Stephen Tong -niminen henkilö. Kivimäkeä Naughton on kuvannut yhtiön visionääriksi, joka ymmärsi liiketoiminnasta enemmän kuin he muut. Naughtonin mukaan Kivimäki oli Scanifin toiminnassa mukana olleista henkilöistä innostunein. Tästä esimerkkinä Naughton on kertonut sen, että Kivimäki halusi heidät kaikki aina yhteen miettimään silloin, kun kehitystyö ei edennyt.

Scanifi tarvitsi toimintaansa varten palvelimia, jotka hankittiin Hetzneriltä, koska yhtiöllä oli hyvä maine ja edulliset hinnat. Nauhgton ei osallistunut palvelinten vuokraamiseen, mutta saattoi joskus maksaa niiden vuokria. Naughtonin mukaan palvelimia oli ehkä viisi, ja hänen mielestään palvelimille oli tarkoitus tallentaa vain Scanifin toimintaan liittynyttä materiaalia. Muun materiaalin tallentamista palvelimille ei ollut kuitenkaan kielletty.

Kysyttäessä Naghton on kertonut, että Scanifin palvelimilla käytettiin Vanderpotin aloitteesta SSH-avaimia. Hänen mukaansa jokaisella yrityksen

toiminnassa mukana olleella oli oma SSH-avain. Omaa SSH-avaintaan Naughton ei jakanut muille, mutta siitä, jakoivatko muut avaimia, hän ei ole osannut muiden puolesta kertoa.

P-palvelimet

P-sarjan palvelimista P1-palvelin on asennettu 12.1.2019 ja P2-palvelin 4.1.2019 (S66). Molempien palvelimien tiedostojärjestelmä oli suojattu vahvalla salauksella siten, että palvelimet oli mahdollista käynnistää ainoastaan kirjautumalla WI8-avaimella, minkä lisäksi on vielä tarvittu erillinen 64-merkkinen salasana. P3-palvelin oli suurelta osin tyhjennetty, kun se oli saatu takavarikkoon. Tämän vuoksi palvelimen mahdollista salausmekanismia ei ollut kyetty selvittämään. Tutkinnassa oli kuitenkin selvinnyt, että P3-palvelimelle oli 11.2.2020 kirjauduttu niin ikään WI8-avaimella. (S66)

P-palvelinsarjan tilaaja on palvelimet vuokranneelta Hetzneriltä saatujen tietojen mukaan ollut Leena Patel -niminen henkilö. Leena Patelin tilaajaprofiilin yhteyssähköpostiosoitteena Hetznerille on ollut mathewlukeberry@gmail.com (S30). Kyseinen sähköpostiosoite on Googlen tilaajatietojen mukaan rekisteröity 29.10.2018 Mathew Berry -nimiselle henkilölle. Sähköpostin niin sanottuna palautussähköpostiosoitteena (recovery e-mail) on ollut puolestaan lenapat012@protonmail.com (S32). Kyseiselle sähköpostitilille on kirjauduttu useista Mullvadin osoiteavaruuteen kuuluvista eri IP-osoitteista (S32 ja S33). Ainakin yksi näistä IP-osoitteista on ollut sama kuin mistä Kivimäki on julkaissut viestejä Ylilaudalle (S38 s. 1762 ja S33). Yleisesti tiedossa on, että kuka tahansa voi hankkia itselleen ilmaisen gmail- tai protonmail-sähköpostiosoitteen, ja ettei sähköpostitilin takana olevan henkilön henkilöllisyyttä tiliä luotaessa tällöin tarkisteta.

Yhteyssähköpostiosoite mathewlukeberry@gmail.com on 23.10.2020 kello 15:24:57 (CEST) vaihdettu muotoon matthewlukeberry@cock.li (S30). Samaan aikaan myös Hetznerin asiakastilin hallintapaneeli on ollut aktiivisessa käytössä (S74 ja S79). Kirjallisista todisteista S74 ja S30 ilmenee, että P-palvelimista on tiedusteltu ja pyydetty saamaan etäkäyttöyhteys P1-palvelimelle. Sähköposti on lähetetty edellä mainitusta muuttuneesta sähköpostista 23.10.2020 kello 15:26:09 (CEST) eli vain hetki yhteyssähköpostiosoitteen muuttamisen jälkeen. Hetznerilta on tämän jälkeen ilmoitettu, että vastaus on annettu jo aikaisemmin ja ilmoitettu viranomaisten takavarikoineen palvelimen. Muuttuneesta yhteyssähköpostista on vielä tämän jälkeen kello 15:51 (CEST) pyydetty ilmoittamaan viranomaisille, että nämä palauttaisivat palvelimen pikaisesti sekä tiedusteltu takavarikon suorittaneen viranomaisen yhteystietoja taikka kopiota etsintäluvasta, mihin Hetzner on vastannut siirtäneensä pyynnön vastattavaksi toiselle osastolle (S30). Muutamia päiviä myöhemmin 26.10.2020 myös Kivimäen yrityksen Scanifin sähköpostista hello@scani.fi on tiedusteltu K-sarjan palvelimiin liittyen ”Server - Remote Console”. Palvelimia on kuitenkin koskenut Hetznerin sisäinen varoitus, ettei asiakkaan pyyntöihin suostuta, ja 27.10.2020 Hetzneriltä on ilmoitettu yritykselle viranomaisten takavarikoineen palvelimen ja samalla ilmoitettu keskusrikospoliisin tutkijan yhteystiedot lisätietoja varten (S74).

P-sarjan palvelimet on maksettu luottokorteilla ja Deng Haitao -nimiselle henkilölle kuuluvalla PayPal-tilillä hyipdownline@hotmail.com. Deng Haitao -niminen henkilö on tullut esiin myös P-palvelinsarjan yhteydessä, kun Leena Patelin tilaajatiedoilla tilattuja palvelimia on maksettu 23.10.2020 P2-palvelimen osalta syys-lokakuussa 13.1.2008 rekisteröidyltä Paypal-tililtä.

Kyseinen tili on rekisteröity Deng Haitao -nimiselle henkilölle (S30 ja S31). Kyseiseen tiliin on ilmoitettu sähköpostiosoite hyipdownline@hotmail.com sekä Kiinan suuntanumeroilla +86 olevia puhelinnumeroita sekä kiinalaisia osoitteita ja yksi ukrainalainen osoite. Kirjallisen todisteen mukaan viimeisimmät maksut palvelimista on maaliskuussa vuonna 2022 maksettu Paypalin kautta, eikä laskuja tämän jälkeen ole enää maksettu (S30). Vuodelta 2019 on löytynyt muutama maksu Leena Patelin luottokortilta. Näistä ei ole kirjallisen todisteen (S30) mukaan löytynyt muuta tietoa. Syyttäjät ovat käräjäoikeuden istunnossa ilmoittaneet, että kortteja on pyritty selvittämään. Syyttäjät ovat yhden Visa- ja kahden Mastercard-luottokortin osalta ilmoittaneet, että korteista kaksi on ilmoitettu kadonneeksi ja yksi korteista on ollut lukittuna.

Ainoa P-palvelimien hallintapaneeliin Mullvad-VPN-verkon ulkopuolelta tehty yhteydenotto oli tapahtunut 12.11.2020. Sky Limited -yhtiöltä (V21 ja V21.1) saadun tiedon mukaan kyseinen IP-osoite oli tuona aikana yhdistynyt Lontoossa olleeseen Adrian Ioan Badescu -nimiseen henkilöön, jolle oli toimitettu internetkäyttöön tarkoitettuja verkkolaitteita.

Kivimäki on häntä käräjäoikeudessa kuultaessa ensin kiistänyt käyttäneensä P1–P3-palvelimia. Hän on myöhemmin kuulemisessaan kertonut ilmeisesti käyttäneensä P1-palvelinta jollain tavalla, mutta hänen mukaansa esitutkintamateriaalista ilmenee, ettei hänellä ole ollut kuitenkaan pääkäyttäjätason oikeuksia kyseiselle palvelimelle. Kivimäki on myöhemmin kertonut, että hän oli käyttänyt myös P2-palvelimella ollutta VPN-palvelua, jonne johtavan asennustiedoston hän oli saanut joltain. Kivimäki oli alkanut käyttää VPN-palvelua, kun ”Antipeace”-nimimerkki oli sitä hänelle suositellut. Kivimäen mukaan tämä ei ollut oleellista vaan pääasia oli että palvelu toimi. Kivimäen mukaan oli sinänsä ihan sama, mitä VPN-palvelua hän oli käyttänyt, koska hän ei osallistunut mihinkään sellaiseen toimintaan, jota olisi pitänyt salailla. Hän on lisäksi kertonut käyneensä saamallaan SSH-avaimella katsomassa palvelimilla eri hakemistoja ja niiden sisältöjä. Joku oli vihjannut hänelle palvelimilta löytyneistä tietokannoista ja lähdekoodeista, joita hän oli käynyt katsomassa. Kivimäki ei ole tarkemmin osannut sanoa, mikä tämä SSH-avain oli ollut ja minne kaikkialle sillä oli ollut pääsy.

Kysyttäessä, milloin Kivimäki oli huomannut, ettei hän päässyt P-palvelimille, hän on vastannut, ettei hänellä ole asiasta muistikuvaa. Mikäli palvelimet olivat lakanneet toimimasta, asialla ei ollut hänelle merkitystä, koska hän oli alkanut käyttää vaihtoehtoista VPN-yhteyttä. Kivimäen mukaan palvelimiin liittyi myös keskusteluryhmä, jonka nimi oli hänen mukaansa ”HAX”. Kun ryhmässä oli alettu keskustella vuodetuista tiedoista, Kivimäki oli muistinsa mukaan pyytänyt, ettei häntä sotkettaisi asiaan, koska hän oli suomalainen ja yhteydessä palvelimiin. Hän ei ollut koskaan saanut vuodettuja tietoja haltuunsa, eikä hän myöskään olisi ollut niistä kiinnostunut.

Käräjäoikeus toteaa, että Kivimäen kertomus on vahvassa ristiriidassa aikaisemmin tuomiossa P-palvelimien vahvasta salauksesta sekä yleisestä tietoturvasta kerrotun kanssa. On epäuskottavaa, että ulkopuolisille henkilöille olisi jaettu pääsy palvelimille, joilla on mahdollisesti säilytetty laittomasti hankittuja tietokantoja ja muuta arkaluonteista materiaalia.

K-palvelimet

K-palvelinsarjan palvelimissa tilaajatietona on Hetzneriltä saadun tiedon mukaan ollut Scanifi LLC ja Alex Vanderpot. K-sarjan palvelimet on

asennettu ajalla 4.2.2019–4.8.2020. Ajallisesti ensimmäisenä on asennettu K1 ja viimeisenä on K17. Palvelimet on aluksi maksettu käyttäen Alex Vanderpotin luottokorttia ja huhtikuusta 2020 alkaen käyttäen Kivimäelle kuuluneita luottokortteja. Palvelinsarjan maksamisessa käytettyjä Kivimäen luottokortteja on lisäksi käytetty Kivimäen PayPal-tilillä ja 7.6.2020 tehdyssä automaattinostossa (S31 ja S34). Toinen maksuissa käytetty luottokortti on lisäksi takavarikoitu Kivimäen hallusta Ranskassa.

Tekokokonaisuuden kannalta merkityksellisimmiksi K-sarjan palvelimista ovat nousseet palvelimet, jotka ovat tutkinnassa saaneet nimet K1, K16 ja K17.

K1-palvelimen osalta syyttäjät ovat katsoneet, että tämä palvelin on kuulunut Kubernetes-palvelinryppääseen yhdessä palvelimien K2–K15 kanssa. Palvelimelta on löytynyt bekup.tgze- ja domainscanlist-nimiset tiedostot, jotka ovat identtiset P1-palvelimelta löytyneiden vastaavien tiedostojen kanssa. P1-palvelimen root-käyttäjän komentohistoriassa on myös ne komennot, joilla nämä tiedostot on kopioitu K1-palvelimelle.

Tutkinnassa on ilmennyt, että root-käyttäjä on 25.10.2020 poistanut K1-palvelimelta kaikki hyväksytyt SSH-avaimet ja tyhjentänyt järjestelmän kirjautumislokeja. Root-käyttäjä on lisännyt palvelimelle yhden SSH-avaimen, jonka kommenttina on ollut ryan_thinkpad.

K16-palvelin on asennettu 18.5.2020, ja siinä on ollut käytössä GitLab-versionhallintaohjelmisto, joka on tarjonnut erilaisia palveluita esimerkiksi ohjelmistokehityksen helpottamiseksi. Palvelimella on kehitetty ohjelmistoja, joista osa on ollut samankaltaisia kuin P2-palvelimella sijainneella gogs-virtuaalipalvelimella internetin skannaamiseen sekä tietokantapalvelujen käyttäjätunnusten ja salasanojen arvaamiseen kehitetyt ohjelmistot. GitLab-palvelussa on ollut käyttäjätunnuksia useille eri käyttäjille, muun ohella Kivimäelle. Kirjallisen todisteen S21 mukaan GitLabista on K16-palvelimen tietorakenteessa ollut useita varmuuskopioita, joista ensimmäinen kopio on ajalta 23.9.2020 ja myöhäisempi kopio ajalta 15.11.2020.

Kivimäelle riidattomasti kuuluva käyttäjätunnus ”r” (aleksanteri@scani.fi) on kirjautunut GitLab-palveluun IP-osoitteesta 37.156.72.25 useita eri kertoja (S21). Aikaisemmassa kopiossa käyttäjätunnuksen ”r” tila on aktiivinen, ja se on kirjautunut onnistuneesti 20.8.2020. Viimeisin kirjautuminen on IP-osoitteesta 185.65.135.221. Kirjautumisia on yhteensä 46, eikä epäonnistuneita yrityksiä ole ollut. Varmuuskopiosta 15.11.2020 puolestaan ilmenee, että Kivimäen käyttäjätunnus ”r” on estetty (blocked) jossain kohtaa 23.9. ja 15.11.2020 välisenä aikana. Kirjautumisista aikaisempi on ollut 9.10.2020 kello 13:27:32 ja viimeisin 26.10.2020 klo 02:10:10. Viimeisin kirjautuminen on tapahtunut IP-osoitteesta 37.156.72.25. Onnistuneita kirjautumisia on 49, eikä epäonnistuneita kirjautumisyrityksiä kopiossa ole. Poliisi on myöhemmin jäljentänyt käyttäjätilit. Tällä jäljentämishetkellä käyttäjätunnuksella ”r” on 15.11.2020 päivättyyn kopioon verrattuna havaittavissa yhteensä kahdeksan epäonnistunutta kirjautumisyritystä, vaikka muuten käyttäjätunnuksen ”r” tiedot ovat täysin samat. Raportin mukaan tietokannassa 15.11.2020 on kyseisen käyttäjän kohdalla viimeisin muokkausaikaleima ollut 27.10.2020 kello 19:53:30. Tämä osoittaa raportin mukaan, että jotain on muuttunut käyttäjätilin tiedoissa tuona ajankohtana. Ajallisesti edellä mainittuun ajankohtaan liittyy myös kirjallisista todisteista S58 ja S74 ilmenevästi se, että Vanderpotin niin sanotulta robottitililtä on 26.10.2020 kello 21:59 (CEST) kysytty etäkäyttömahdollisuutta

marriott-palvelimelle (K1-palvelin). Viestiin on vastattu palvelimen takavarikon jälkeen 27.10.2020 kello 05:08 (CEST).

Kivimäki on 26.10.2020 kirjautunut viimeisen kerran GitLabiin, ja tästä on pääteltävissä, että hänet on aikavälillä 26.10.–15.11.2020 asetettu ”blocked” tilaan eli hänen kirjautumisensa on estetty. GitLab-palvelussa on ollut kaksi tunnusta, joilla on ollut pääkäyttäjän oikeudet. Näiden käyttäjätunnusten kirjautumisajankohdista on pääteltävissä, että estäjä on ollut käyttäjänimi vanderpot.

K17-palvelin eroaa (S30) muista K-sarjan palvelimista huomattavan suuren 150 teratavun suuruisen massamuistinsa osalta. Palvelimella on myös muista K-sarjan palvelimista poiketen ajettu käyttöjärjestelmänä Ubuntu Linux -käyttöjärjestelmän asemesta Debian Linux -käyttöjärjestelmää, jonka Kivimäki on itse käräjäoikeudessa kertonut olevan hänen suosikkijakeluversionsa.

Poliisin suorittamassa tutkinnassa K17-palvelimen on todettu sisältäneen muun muassa Plex-mediapalvelinohjelmiston ja runsaasti siihen liittyviä mediatiedostoja sekä typosquatting-nimellä tunnettuun virheellisesti kirjoitettujen verkko-osoitteiden hyödyntämiseen liittyvää materiaalia.

Todistaja Naughton on käräjäoikeudessa kertonut K17-palvelimen osalta, ettei Scanifilla ollut hänen mielestään vielä yhtiön toiminnan ollessa vasta aivan alkuvaiheessa tarvetta näin suurella tallennustilalla varustetulle palvelimelle ja että palvelimen koko olikin tullut hänelle yllätyksenä.

Kivimäki on myöntänyt, ettei Scanifilla ollut vielä K17-palvelimen hankinta-aikaan mitään sellaista dataa, jolla K17-palvelimen kaltainen levytilaltaan suuri palvelin olisi täytetty. Palvelin oli kuitenkin ollut kannattavaa hankkia, koska isolla levytilalla varustetuista palvelimista oli ollut tuohon aikaan pulaa. Palvelin oli haluttu tilata hyvässä ajoin, jottei pula tallennustilasta estäisi liiketoimintaa.

Syyttäjät ovat esittäneet, että K17-palvelin ei ole kuulunut Scanifi-yhtiön palvelinlaitteistoihin vaan on ollut vain Kivimäen käytössä. Kivimäki itse on puolestaan esittänyt, että K17-palvelimen oli tilannut Vanderpot. Hän on perustellut tätä kirjallisella todisteella (S21 ja V15), jossa on esitetty ote palvelimella K16 olleesta Scanifin käytössä olleen GitLab-palvelun tehtävästä, jossa käyttäjätunnus ”alex” asettaa tehtävän hankkia nimellä big data -nimetty palvelin. Nimimerkki ”r” sulkee tehtävän myöhemmin kommentoituaan, että palvelin on toimitettu. Kirjallisesta todisteesta 103 on nähtävissä, että mainittu r-käyttäjän kommentti palvelimen toimittamisesta on tehty 4.2.2019 kello 14.16:14, joka sopii K1-palvelimen asentamisajankohtaan 4.2.2019 eikä K17-palvelimen asentamisajankohtaan 4.8.2020.

P-palvelinten tyhjennys

Vastaamon potilastietojen julkaisemisessa on 23.10.2020 kello 02:00 (UTC) tapahtunut virhe, jonka seurauksena jo julkaistuista potilastiedoista koostuvien tekstitiedostojen asemesta tar-pakettiin oli tullut root-käyttäjä koko kotihakemisto. Potilastietojen julkaisussa tapahtuneen virheen jälkeen P2-palvelimella sijaitsevan OPSVM-virtuaalipalvelimen käyttäjä on kirjautunut 23.10.2020 kello 12.04 (UTC) ja alkanut tarkastaa, mitä on tapahtunut.

Edellä kerrotun virheen vuoksi poliisi on päässyt Vastaamoon kohdistuneen kiristyksen jälkeen kiristyksessä käytetyn palvelinlaitteiston jäljille ja antanut

määräyksen irrottaa P1-palvelin verkosta. Palvelin on irrotettu verkosta 23.10.2020 kello 11.45 ja takavarikoitu 25.10.2020. P-palvelimien yhteyssähköpostiosoitteesta mathewlukeperry@cock.li on 23.10.2020 kello 15.26 (UTC+2) lähetetty Hetznerille palvelupyyntö, jossa oli pyydetty saada etäkäyttöoikeus P1-palvelimelle.

Virheellisesti ajastetun vastaamo.tar-paketin luominen on aloitettu 23.10.2020 kello 02:00:01 (UTC), ja palvelimen levytila on loppunut 02:02:14 (UTC). Vastaamo.tar-paketti on ollut Tor-verkossa ladattavissa tämän jälkeen ajanhetkestä 02:02:14 eteenpäin. Esitutkinnassa tehdyn selvityksen perusteella yksikään paketin lataajista ei ole voinut ladata sitä pidempään kuin 1 tunnin 41 minuutin ajan, koska viimeistään kello 03:41 Tor-palvelin ei ole palvelintilan täytyttyä enää vastannut eikä siihen ole saatu yhteyttä ennen kuin OPSVM-palvelimen käyttäjä on aloittanut toimenpiteensä (S19).

Tutkinnassa on lisäksi selvinnyt, että poliisi oli saanut ladattua edellä mainittua vastaamo.tar-tiedostoa 85 minuutin ajan ja oli saanut ladatuksi sitä kaikkiaan 1.249,25 megatavua. Latausnopeus oli siten ollut noin 14,7 megatavua minuutissa (2 megabittia sekunnissa). Ainoa poliisin tietämä kolmas osapuoli oli saanut ladattua pakettia noin 58 minuuttia ja oli saanut ladatuksi sitä 2.132,66 megatavua latausnopeuden ollessa noin 36,8 megatavua minuutissa (5 megabittiä sekunnissa). Siten jokainen lataaja, jonka latausnopeus on ollut alle 74 megatavua minuutissa, eli noin 9,9 megabittia sekunnissa, on voinut ladata vastaamo.tar-paketista noin 100 minuutin aikana vain sellaisen osuuden, jossa kaikki potilastiedot sisältävä fi_vastaamo.sql-tiedosto ei ole ollut edes osittain.

Asiantuntija Nurmi on kuultaessa kommentoinut edellä esitettyjä latausnopeuksia järkeviksi ja yllättävän hyviksi sekä hyvinkin sellaisiksi, joita Tor-verkossa on mahdollista saada. Kysyttäessä olisiko latausnopeutta mahdollista saada jotenkin nopeutettua hän on vastannut, että teoriassa Tor-verkon välireititttimien määrää voisi saada vähennettyä. Varmaa ei kuitenkaan tällöinkään olisi, että nopeutuisiko verkkoliikenne, koska tiedossa ei ole, missä osassa Tor-verkkoa kulloinkin latausnopeutta hidastava välireititin on. Nurmi on vielä todennut olevan sinänsä mahdollista, että lataus aloitettaisiin eri kohdasta tiedostoa kuin sen alusta. Käräjäoikeus toteaa, ettei asiassa kuitenkaan ole ilmennyt, että OPSVM-virtuaalipalvelimella Tor-palve linta ajaneessa nginx-nimisessä palvelimessa olisi ollut tällainen ominaisuus.

Edellä olevan perusteella on hyvin suurella todennäköisyydellä pääteltävissä, että ainoastaan kiristäjällä on voinut olla hallussaan alkuperäinen Vastaamon potilastietokanta ja siten tieto kaikista Vastaamon asiakkaista. Tätä johtopäätöstä tukee osaltaan se, että Amazonilta saadusta niin sanotusta SES-lokista, joka on sähköpostipalvelimen loki, näkyy asiakkaiden kiristysviestin osalta niiden lähetystiedot (S23). Kyseisen SES-lokin mukaan osoitteesta no-reply@smileup.site on lähetetty onnistuneesti kiristyssähköposteja 27.966 uniikkiin sähköpostisoitteeseen. Viestit on lokin perusteella lähetetty 24.10.2020 kello 16:04:20 ja 21:29:21 (UTC) välisenä aikana. Kaikki nämä osoitteet löytyvät tuomiossa edellä kerrotuin tavoin OPSVM-palvelimella olevasta fi_vastaamo.sql-tietokantadumpista pois lukien sähköpostiosoite vastaamo@cock.li (S77).

Tietoteknisestä raportista (S77) ilmenee, että yhteensä viisi sähköpostiosoitetta on ollut sellaisia, joihin on onnistuttu lähettämään viesti, ja kaksi osoitetta sellaisia, joihin ei ole onnistuttu lähettämään viestiä ja jotka löytyvät tietokantadumpista ja SES-lokista, mutta jotka eivät ole OPSVM:n /root/therapissed/patients/-kansion tekstitiedostoissa. Näitä

sähköpostiosoitteita vastaavia tekstitiedostoja ei raportin mukaan ole olemassa johtuen siitä, että asiakkailla on ollut nimikaima tietokannassa (S77). Edellä kerrottu tukee johtopäätöstä siitä, että kiristäjällä on täytynyt olla käytössään itse tietokantadumppi, joka on sisältänyt kaikkien Vastaamon potilaiden tiedot. Vuotaneet tekstitiedostot ovat olleet tältä osin vaillinaiset.

Tekijä on tapahtuneen konfigurointivirheen jälkeen tutkinut mitä tiedostoja virheellisessä tar-paketissa on ollut ja virheellisessä tar-paketissa ollutta root-käyttäjän komentohistoriaa sekä annettujen python-komentojen historiaa ilmeisenä tarkoituksenaan tutkia, onko tar-paketissa ollut sellaisia tietoja, jotka voitaisiin yhdistää tekijään. Tekijä on tutkinut myös, löytyykö virheellisessä tar-paketissa olleesta sov.tgz-tiedostosta avainsanaa ”ryan”.

Tekijä on 23.10.2020 kello 15:30:33 (UTC) aloittanut P2-palvelimen hallitun sammuttamisen (S75) sammuttamalla Proxmoxin ylläpitämiä virtuaalipalvelimia saaden toimintansa päätöksen kello 13.39:09. P2-palvelimen kopiointi K17-palvelimelle on alkanut 23.10.2020 kello 13.56. Hertznerin toimittamasta Netflow-lokista (S30) on nähtävissä useita yhteydenottoja P2-palvelimelle Hyperopticin IP-osoitteesta 37.156.72.25.

Varmuuskopiointi on saatu suoritettua seuraavana päivänä kello 19.32 (UTC) mennessä. Poliisi on 26.10.2020 takavarikoinut P2-palvelimen, joka oli kuitenkin ehditty tyhjentää (S2). P2-palvelimen sisältö on kuitenkin löytynyt varmuuskopioituna K17-palvelimelta, jonka Saksan poliisi on myöhemmin takavarikoinut.

P- ja K-palvelimien yhteydet

Tutkinnassa on P- ja K-palvelinsarjojen välillä löytynyt yhteyksiä, jotka vahvasti puhuvat sen puolesta, että keskeisillä palvelinsarjojen palvelimilla P1–P2 ja K16–K17 on ollut yhteinen käyttäjä tai käyttäjiä.

Poliisin suorittamassa tutkinnassa on P1-palvelimelta löytynyt kaksi pyongyang-nimisen tietokoneen tiedostojärjestelmän kopiota (S24). Lisäksi P17-palvelimelta on löytynyt backup-nimisen tietokoneen tiedostojärjestelmän kopio, jossa on paljon yhtäläisyyksiä pyongyang-kopioiden kanssa. Kopioissa on lukuisia identtisesti nimettyjä tiedostoja, joilla on yhteinen aikaleima. Kaikissa kolmessa kopiossa on sama identtinen julkinen ja yksityinen SSH-avaintiedosto. Kopioissa on myös käyttäjätunnuksia, joilla on yhteinen nimi ja yhteinen yksilöllinen tunnistenumero. Näiden perusteella voidaan katsoa, että tiedostorakenteet ovat peräisin varsin todennäköisesti samasta l ähteestä.

Kuten edellä on todettu, P2-palvelimen kopio oli löytynyt K17-palvelimelta. Tutkinnassa on selvitetty K17-palvelimen komentohistoriasta, että käyttäjällä on P2-palvelimen levykuvaa kopioidessaan ollut pääkäyttäjätasoinen pääsy sekä P2- että K17-palvelimille. Tutkinnassa on lisäksi selvinnyt, että K17-palvelimelta löytynyt P2-levykuva oli suojattu täsmälleen samalla 64 merkkiä pitkällä salasanalla kuin mitä oli käytetty P1- ja P2-palvelimien kokolevysalauksessa (S20, s. 8).

Tutkinnassa on edelleen P1-palvelimelta löydetty bekup.tgze- ja domanscanlist-nimiset tiedostot, jotka on root-käyttäjän komentohistorian mukaan kopioitu K1-palvelimelle sen root-käyttäjän kotihakemistoon (S28). Tutkinnassa ei bekup.tgze-tiedoston sisältöä ole saatu selvitettyä sen ollessa salattu. Domainscanlist-tiedosto on sisältänyt yli viisisataa miljoonaa IP-osoitetta mukaan lukien Vastaamoon liittyviä IP-osoitteita.

P2-palvelimella olleen OPSVM-virtuaalipalvelimen root-käyttäjä on ollut yhteydessä muun muassa pyongyang-, worldstream-, ecatel- ja P1-palvelimille tai virtuaalipalvelimiin. Hänen SSH-asetuksissaan on lisäksi ollut valmiina SSH-yhteyden käyttöä nopeuttavat pika-asetukset muun ohella näille palvelimille tai virtuaalipalvelimille.

Vastaamoon tehdyssä tietomurrossa sekä yhtiön ja sen potilaiden kiristyksessä käytetyiltä palvelimilta on löytynyt edellä esitetyin tavoin vahvoja viitteitä siitä, että palvelimia on käyttänyt sama käyttäjä tai samat käyttäjät. Käytön tiiviydestä ja sen merkittävyydestä käyttäjälle kertoo se, että palvelimille ja virtuaalipalvelimille on luotu SSH-ohjelmiston asetuksiin omia pikakäyttöasetuksia yhteydenottoja varten. Käräjäoikeus katsoo tämän vahvasti viittaavaan siihen, että palvelinyhteydet ovat olleen kiinteitä ja usein toistuvia.

Kivimäen yhteydet P- ja K-palvelimiin

P1-palvelin ja IMAP-loki

P1-palvelimen bigvol-hakemistosta on löytynyt Lundberg-nimisen henkilön sähköpostitilin IMAP-loki (S18). Lundberg on Kivimäen siskon kummitäti. Palvelimen levypinnasta on löydetty myös jälkiä siitä, että mainittua IMAP-lokia on muokattu ja muokattu osa on välitetty eteenpäin transfer.sh-palveluun nimellä liitek9a.txt. Lundbergin tietokoneen sähköposteista on lisäksi löytynyt 11.4.2019 päivätty sähköposti, jossa on latauslinkki P1-palvelimella olevaan tiedostoon, joka on sisältänyt otteita mainituista IMAP-lokeista. Sähköpostista on edelleen löytynyt viesti, jossa Lundberg on 28.10.2019 lähettänyt liitek9a.txt-tiedoston eteenpäin kolmannelle henkilölle analysoitavaksi. Kivimäki on käräjäoikeudessa myöntänyt käsitelleensä IMAP-lokia P1-palvelimella.

Kirjallisena todisteena S14 on esitetty kopio Lundbergin ajopäiväkirjasta, jonka mukaan hänellä on ajalla 5.–7.4.2019 ollut muun ohella tietokoneen varmuuskopioimiseen liittyvä tapaaminen Barcelonassa IT-asiantuntija Kivimäen kanssa. Kivimäki on myöntänyt, että tällainen tapaaminen on ollut.

Kirjallisena todisteena S55 on Lundbergin tiliote, josta on nähtävissä, että Lundberg on 30.4.2019 tehnyt 4.990 euron suuruisen tilisiirron Kivimäen siskolle. Maksun viestikentässä lukee maksun kohdalla onnentoivotus kummitytön merkkipäivänä. Syyttäjien mukaan tutkinnassa ei kyseiselle ajankohdalle ole löydetty minkäänlaista siskon merkkipäivää.

Lundberg on 20.3.2019 tiedustellut Kivimäen äidiltä (S53), miten hän saisi tavoitettua Jn. Hän on saanut vastaukseksi puhelinnumeron +34684240415. Kivimäen äiti on ilmoittanut Lundbergille numeron olevan myös Jn WhatsAppissa käyttämä puhelinnumero. Lundberg on myöhemmin lähettänyt numeroon suomenkielisen soittopyynnön. Numero on tallennettu Lundbergin puhelimeen nimellä Julius.

Kirjallisena todisteena S80 on esitetty lausunto Lundbergin edellä mainituista sähköposteista. Lausunnon on allekirjoittanut Robert Cornel -niminen henkilö. Cornelin 2.11.2019 päivätyn lausunnon yhteystietoihin Cornelin puhelinnumeroksi on merkitty +34684240415. Lausunnon liitteenä olevassa ansioluettelossa Cornelin puhelinnumeroksi on merkitty +34684340415 eli puhelinnumeroissa on vain yhden numeron ero.

Kirjallisessa todisteessa S54 on esitetty Lundbergin matkapuhelimesta saatuja tietoja. Lundbergin puhelimeen on 6.4.2019 luotu

WhatsApp-yhteystieto, jonka viimeinen muokkauspäivä on 5.11.2020. Yhteystiedon nimeksi on merkitty Robert. Tähän WhatsApp-tiliin on liitetty Kivimäelle kuuluva puhelinnumero +34684240415. Edellä lausuttu huomioon ottaen sillä Kivimäen vetoamalla seikalla, että Lundbergin puhelimessa ollutta nimeä olisi muokattu (modified) 5.11.2020 ja nimi samalla vaihdettu, ei ole merkitystä. Kivimäen puhelinnumero ei ole kuitenkaan muuttunut Lundbergin puhelimen yhteystiedoissa.

Lundberg on myös 10.–11.11.2019 keskustellut Facebookissa äänipuheluin ja tekstiviestein Robert Cornel -nimellä puhelimeen nimetyn henkilön kanssa. Viestit ovat koskeneet Cornelin Lundbergille toimittamaa pdf-lausumaa. Syyttäjät ovat katsoneet, että Robert Cornel on tällöin tosiasiassa ollut Kivimäki, jolta Lundberg on ostanut edellä mainitun sähköpostitilin muokkauspalvelun.

Tältä osin asia on liittynyt toiseen vielä keskeneräiseen rikostutkintaan, mutta riidatonta kuitenkin on, että Kivimäkeä on pyydetty muokkaamaan lokitiedostoa. Kivimäki ei ole kuitenkaan häntä kuultaessa muistanut, miksi hän oli sitä P1:llä käsitellyt ja arvellut syyksi ”tilanpuutetta”. Kivimäen mukaan tiedostojen kopiointi ulkopuolelle oli hidasta, kun käytti VPN:ää. Sen sijaan sisäverkossa tämä oli Kivimäen mukaan nopeampaa.

P1-palvelin ja siltä löytyneet beach.jpg-kuva ja nettisivukopio

P1-palvelimella sijainneesta pyongyang-koneen tiedostorakenteen kopiosta kohdasta /sites/jwheare on löytynyt beach.jpg-niminen kuvatiedosto, joka Kivimäen mukaan on valokuva hänen isovanhempiensa mökiltä. Kivimäki on kuultaessa ollut tietämätön siitä, miten kuva on päätynyt pyongyang-koneen varmuuskopiolle. Kivimäki on kuitenkin arvellut kuvan olleen siellä useita vuosia ja todennut, että palvelimelle on ollut pääsy usealla henkilöllä. Kivimäki on kuitenkin myöntänyt sen, että hänellä on ollut pääsy kyseiselle pyongyang-koneelle, mutta todennut vielä, ettei kyseinen kone liittynyt mitenkään nyt esillä olevaan tekoon. Kivimäki on vielä viitannut siihen, että edellä mainitulta koneelta on löytynyt myös sinne tallentunut häntä itseään kritisoiva englanninkielinen kirjoitus ”Julius Kivi kant stop getting rooted” (V16). Kivimäen mukaan ei olisi mitään järkeä tallentaa itsestään tällaisia kirjoituksia ja jo tämä osoitti, ettei hän ole kopiota tehnyt. Edellä mainittu verkkosivu on syyttäjien esittämän selvityksen mukaan tallennettu tai tallentunut sinne kuitenkin jo 6.6.2014 (S24).

Pyongyangin kopioissa ovat sijanneet myös kansiot nimeltä ”h” sekä ”nigger” (S24). Edellä mainitut kaksi kansiota ”h” ja ”nigger” sekä ”jwheare” ovat jäljempänä tuomiosta ilmenevästi Kivimäen käyttämiä tunnuksia taikka muunnoksia niistä.

Virtuaalipalvelin irc

P2-palvelimella on ollut virtuaalipalvelin, jolle on palvelinkonfiguraatiossa annettu nimi irc. Virtuaalipalvelimella ollut käyttäjätunnus ”ircuser” on voinut kirjautua vain sormenjäljiltään WI8- ja item-alkuisilla SSH-avaimilla. Kirjallisen todisteen S20 mukaan kirjautumisia on ainoastaan WI8-avaimella, joka todisteen mukaan on kirjautunut 23.10.2020 kello 12:04:30–12:13:52, 12:08:24–12:08:33 ja 13:03:30–13:35:25 (UTC). Kyseiset ajankohdat ovat varsin lähellä sitä ajankohtaa, jolloin tar-paketin virheen selvittäminen on aloitettu. Käyttäjätunnus ”ircuser” on komentohistorian perusteella muun

muassa yrittänyt kesken virheenselvitystä etsiä irc-virtuaalipalvelimelta hakemistoa /var/www/html/vastaamo (S20). Hakemisto on kuitenkin sijainnut OPSVM-virtuaalipalvelimella.

Edelleen todisteesta numero S20 ilmenee, että P2-palvelimelle on ollut asennettuna myös virtuaalipalvelin silasdev. Palvelimella on ollut käytössä toiminnallisuus top_talkers, joka kerää tietokantaan tilastoa IP-osoitteista ja niiden tuottamasta liikennemäärästä verkkoon. Kyseisen tietokannan mukaan IP-osoite 37.156.72.25 on käyttänyt virtuaalikoneiden muodostamaa lähiverkkoa seitsemän kertaa (9.10.2020, 10.10.2020, 14.10.2020, 16.10.2020, 18.10.2020 sekä 20.10.2020), joista yhteensä neljä kertaa (9.10.2020, kaksi kertaa 16.10.2020 ja 18.10.2020) osuu sellaiseen ajankohtaan, kun P2-palvelimella olevalle irc-virtuaalipalvelimelle on kirjauduttu käyttäen SSH-avainta, jonka sormenjälkenä on WI8.

Kyseisellä irc-virtuaalipalvelimella on ollut asennettuna WeeChat-niminen IRC-asiakassovellus, jota on käytetty IRC-kanavilla käytyihin keskusteluihin. WeeChat-ohjelman asetuksissa on runsaasti erilaisia eri muodoissa olevia ryan-nimimerkkejä, minkä lisäksi ohjelman irc.conf-tiedostossa on efnet.nicks ja freenodelte.nicks-nimisille palvelimille määritelty käyttäjälle nimimerkiksi ”jwheare”, mikä sekin osaltaan edeltä ilmenevästi myös viittaa Kivimäkeen. WeeChat-ohjelmiston asetustiedostossa on lisäksi nimimerkkejä eri palvelimille. Nimimerkkeihin liittyvissä salasanoissa on paljon alatyylisiä sanoja. Kivimäki on kuultaessa kertonut pitävänsä hyvin mahdollisena, että hän on käyttänyt nimimerkkiä ”ryan” ainakin whitefire-palvelimella.

Todistajana kuultu Rantalainen on kertonut, että WeeChat on hänen mukaansa todennäköisesti yhdelle käyttäjälle tarkoitettu irc-asiakasohjelmisto.

Edellä kerrottu huomioon ottaen irc-virtuaalipalvelimella olleella WeeChat-ohjelmistolla on ollut vain yksi käyttäjä, joka WeeChat-ohjelmiston asennustiedostojen mukaan on erittäin suurella todennäköisyydellä ollut Kivimäki. Palvelimelle on tutkinnassa saatujen tietojen mukaan kirjauduttu vain käyttäen WI8-avainta. Käyttäjätunnus ”ircuser” ja WI8-avain on ollut kirjautuneena muun muassa niinä hetkinä, jolloin P2-palvelimella on tehty selvitystä virheellisen tar-paketin osalta.

Kivimäki ei ole häntä kuultaessa ensin ylipäätään muistanut käyttäneensä irc-palvelinta, mutta todennut tämän olleen mahdollista ehkä vuonna 2011 tai 2012. Edelleen ”Jwheare” oli todellinen henkilö nimeltään James Wheare. Se mitä SSH-avainta hän olisi palvelimella mahdollisesti käydessään käyttänyt, ei ollut hänen tiedossaan. Nimimerkin ”ryancleary” Kivimäki on puolestaan kertonut olevan ”googlettamalla” löytävä eräänlainen meemi.

K17-palvelin ja Plex-ohjelmisto

Kirjallisen todisteen S25 mukaan valtaosa K17-palvelimen levytilasta on käytetty Plex-mediapalvelinohjelmiston tarjoamien elokuvien ja tv-sarjojen säilömiseen. Plex-ohjelmiston tietokannassa on lueteltuna ne henkilöt, joille on luotu oma käyttäjätunnus ohjelmistoon. Tunnukset käyttäjille on luotu pääosin vuosien 2017–2021 aikana. Ohjelmiston asetustiedostossa on puolestaan mainittuna vain yksi käyttäjätunnus, ryanlopl, ja sähköpostiosoite kivimaki@tuta.io. Plex-ohjelmiston tietokannan mukaan mainittu käyttäjätunnus olisi luotu jo vuonna 2010 eli useita vuosia aikaisemmin kuin muut käyttäjätunnukset. Tunnus on myös ensimmäisenä käyttäjätietokannassa. Kivimäki on kuultaessa pitänyt epätodennäköisenä tunnuksen luontiaikaa ja todennut, että tunnuksen sijainti ensimmäisen viittaa siihen, että hän on

kirjautunut ensimmäisenä kyseiselle mediapalvelimelle. Kivimäki on kuitenkin pitänyt todennäköisenä, että hän on asentanut Plex-palvelinohjelmiston jollain toisella palvelimella ja että tämä olisi tapahtunut joskus ennen K17-palvelimen vuokraamista.

K17-palvelin ja väärin kirjoitettujen domain-osoitteiden hyödyntäminen (typosquatting)

K17-palvelimella on Plex-ohjelmiston lisäksi ollut myös gaymail-nimisen käyttäjätunnuksen kotihakemisto, jossa on ollut sähköpostilaatikko, jota tutkinnan mukaan on käytetty väärin kirjoitettujen domain-osoitteiden hyödyntämiseen (niin sanottu typosquatting). Ensimmäinen sähköpostilaatikkoon saapunut viesti on ollut lähettäjältä ryan@safe.im, mikä viittaa siihen, että tämän sähköpostin käyttäjä on mainitun huijauksen ylläpitäjä.

Sähköpostipalvelin safe.im on riidattomasti Kivimäen hallinnoima. Kivimäki yksilöityy muutoinkin useisiin palveluihin kuten Sixt-kuljetuspalveluun, Transferwise-rahansiirtopalveluun, asuntojen vuokraamiseen liittyvään Airbnb:hin sekä kryptovaluuttaan liittyvään LocalBitcoins-palveluun yrityksen tai palvelun mukaan nimettävillä etuliitteellä ja @safe.im-domainilla (S43-45 ja S49).

OPSVM-virtuaalipalvelin

K17-palvelimelta löytyneestä P2-palvelimen kopiosta on löytynyt virtuaalipalvelin, jolle oli palvelinkokonaisuudessa annettu nimi OPSVM. Virtuaalipalvelimen IP-osoite on ollut 10.69.69.112. Tällä virtuaalipalvelimella on kirjallisten todisteiden mukaan käsitelty Vastaamon potilastietokannasta peräisin olevia potilastietoja sekä tehty erilaisia tekstihakuja kyseisiin potilastietoihin. Potilastietojen julkinen levittäminen Tor-verkossa oli lisäksi tehty OPSVM-virtuaalipalvelimelle asennetulla Onion-piilopalvelulla. Virtuaalipalvelimella on myös etäohjattu palvelinkokonaisuuden ulkopuolella ollutta ecatel-virtuaalipalvelinta, jolta käsin varsinainen tietomurto Vastaamon palvelimiin on tehty.

OPSVM-virtuaalipalvelimelle ei ole palvelinkonfiguraatiossa ollut lainkaan suoraa pääsyä ulkopuolelta julkisen internetin puolelta, vaan virtuaalipalvelimeen on ollut pääsy ainoastaan sisäverkon kautta suojatun WireGuard-yhteyden avulla.

OPSVM-virtuaalipalvelimella on ollut kaksi käyttäjätunnusta, ”e” ja ”root”, jotka molemmat ovat voineet kirjautua virtuaalipalvelimelle ainoastaan käyttäen SSH-avaimia. Käyttäjätunnus ”e” ei ole ajanjaksolla 20.9.–23.10.2020 kirjautunut kertaakaan, joskin käyttäjätunnus ”root” on 11.10.2020 kirjautunut yhden kerran käyttäjätunnuksella ”e”.

Käyttäjätunnuksella ”root” on puolestaan ollut kirjautumiseen käytössään kaikkiaan kahdeksan eri SSH-avainta, mutta onnistuneita kirjautumisia on virtuaalipalvelimen kirjautumislokin perusteella tapahtunut ajanjaksolla 20.9.–23.10.2020 ainoastaan ml0- ja WI8-alkuisen sormenjäljen jättäneillä SSH-avaimilla.

Kivimäki on kertonut käyneensä OPSVM-virtuaalipalvelimella, muttei ole osannut sanoa, milloin ja missä hän on tuolloin asunut. Hän kertonut, että häntä olisi ryhmäkeskustelussa pyydetty käymään katsomassa siellä jotain linkkiä. Hänelle ei ole tarkkaa muistikuvaa, keitä siellä oli ”pyörinyt”, mutta OPSVM-palvelimelta oli löytynyt viittauksia Vanderpotiin.

Ecatel-palvelin

OPSVM-virtuaalipalvelimen komentohistoriassa on merkintöjä (S19, s. 37), joiden mukaan siltä käsin on 19.11. ja 26.11.2018 annettu sarja komentoja, joilla on ohjattu toista virtuaalipalvelinta, joka on OPSVM-virtuaalipalvelimella nimetty nimellä ecatel. OPSVM:llä on ollut sen käyttäjälle luotuna erilliset SSH-kirjautumista nopeuttavat asetukset muun muassa pyongyang-, worldstream-, ecatel- ja P1-palvelimille, jolloin OPSVM-palvelimelta on voitu olla yhteydessä näille palvelimille käyttämällä suoraan niille annettua aliasnimeä palvelimen IP-osoitteen asemesta. Tämä käräjäoikeuden näkemyksen mukaan viittaa vahvasti siihen, että näitä palvelimia on käytetty säännöllisesti OPSVM-virtuaalipalvelimelta käsin.

Ecatel-palvelin ei ole sijainnut yhdelläkään P- tai K-palvelinsarjan palvelimella vaan jossain niiden ulkopuolella. Kivimäki on kuultaessa kertonut sen sijaitsevan mahdollisesti Alankomaissa. Tutkinnassa ei ole onnistuttu saamaan haltuun ecatel-palvelinta eikä sen varmuuskopiota. OPSVM-virtuaalipalvelimen komentohistoriasta on sen sijaan nähtävissä, että sen root- eli pääkäyttäjä on suorittanut tietomurtoon olennaisesti liittyviä komentoja nimenomaisesti juuri ecatel-palvelimella OPSVM-palvelinta käyttämällä.

Ensimmäinen tietomurtoon liittyvä havainto OPSVM-virtuaalipalvelimella on se, että OPSVM-virtuaalipalvelimella annetaan 25.11.2018 komentoja ecatel-palvelimelle, joiden avulla käydään ensin Vastaamon potilasrekisterin http-portissa. Vastaamon potilasrekisterin taustapalvelimen lokiin tallentuu vastaava merkintä. Taustapalvelimen lokiin tallentuu myös käyttäjäagentti-merkkijono, jossa muun ohella mainitaan nimi Simon Smith ja sähköpostiosoite forensic@evestigator.com.au. Todistajana kuultu Rantalainen on kertonut, että user-agentin tarkoituksellinen käyttäminen siten, että se jää näkymään kohdepalvelun lokitiedostoon, on hyviin poikkeuksellista eikä millään tavoin tyypillistä tietomurtoja tehtäessä.

Rantalainen on lisäksi kertonut viitaten OPSVM-virtuaalipalvelimen komentohistoriaan, että palvelimen root-käyttäjä on 26.11.2018 suorittanut ecatel-virtuaalipalvelimella sarjan komentoja, joilla on skannattu verkko-osoitteita ja etsitty palvelimia, joissa on ollut käytössä phpmyadmin-niminen MySQL-tietokannan hallintatyökaluohjelmisto. Tämän skannaustoiminnan tulokset on siirretty takaisin OPSVM-palvelimelle, jossa olevalla ohjelmistolla on tehty väsytyshyökkäyksiä (brute force) edellä saatuihin palvelimiin. Vastaamo on ollut yksi hyökkäyksen kohteista, mutta hyökkäys ei kuitenkaan ole Vastaamon osalta tuottanut tulosta, sillä Vastaamossa ei ole ollut käytössä phpmyadmin-ohjelmistoa.

OPSVM-virtuaalipalvelimen komentohistoriasta ei ole löytynyt niitä komentoja, jolla Vastaamon potilastietokantaan kohdistunut tietomurto on tehty. Itse potilastietokanta on kuitenkin löytynyt OPSVM-virtuaalipalvelimelta, ja sen viimeisestä rivistä on pääteltävissä, että potilastietokanta on 26.11.2018 kello 4:50:40 (Suomen aika) kopioitu Vastaamon palvelimelta. Tätä aikaa tukee myös Ficolon netflow-loki (S41), jonka mukaan 26.11.2018, kello 6:38 ja 6:41 (UTC+2) on otettu kaksi kertaa yhteys Vastaamon MySQL-tietokannan porttiin 3306. Jälkimmäinen yhteydenotoista on ollut kestoltaan 7 minuuttia 19 sekuntia. Käräjäoikeus katsoo syyttäjien tavoin, että tämä on se hetki, jolloin Vastaamon potilastietokanta on kopioitu.

Kivimäki on vedonnut osaltaan siihen, että potilastiedot oli tuotu OPSVM-palvelimelle vuonna 2020 eikä vuonna 2018. Syyttäjät eivät kuitenkaan ole edes väittäneet, että tietokanta olisi tuotu vuonna 2018, vaan että tietokanta oli kopioitu ecatel-palvelimelle vuonna 2018 ja tuotu OPSVM-palvelimelle vuonna 2020.

Vastaamon potilastietokanta on tuotu 7.10.2020 kello 15.06.05 (UTC) OPSVM-palvelimelle, ja sen viimeinen muokkausaika on samana päivänä kello 15:09:28 (UTC). Tutkinnassa ei ole onnistuttu selvittämään, missä potilastietokanta on tarkalleen ottaen sijainnut 26.11.2018 ja 7.10.2020 välisen ajan. Käräjäoikeus kuitenkin katsoo, ettei tällä seikalla ole tekokokonaisuutta arvioitaessa merkitystä. OPSVM-palvelimen komentohistoriasta on selkeästi nähtävissä, että murtautumiseen liittyviä toimenpiteitä on tehty käyttäen ecatel-palvelinta, jota on käytetty OPSVM-palvelimelta.

OPSVM-virtuaalipalvelimelle on 7.10.2020 kello 15.19.13 (UTC) asennettu mysql-server-ohjelmisto. Kirjautuneena tällöin ovat olleet WI8- ja ml0-kirjautumisavaimet. Käyttäjä on alkanut käsitellä potilastietokantaa ja luoda siitä yksittäisiä tekstitiedostoja, joissa on henkilön nimi, yhteystiedot ja hänen potilasmerkintänsä. Kirjautuneena on tällöin ollut ainoastaan ml0-avain. Virtuaalipalvelimen root-käyttäjä on suorittanut 11.10.2020 edellä luoduissa tekstitiedostoissa erilaisia hakuja muun muassa tietyn espoolaisen asuinalueen postinumeroihin ja tässä yhteydessä numeroihin ”97”, minkä lisäksi on haettu poliisiin liittyviä hakuja. Hakuja espoolaiseen osoitteeseen ja postinumeroon on tehty jo heti ensimmäisten hakujen joukossa 11.10.2020 (S19). Osoitehaku ja postinumero viittaavat Kivimäen aikaisempaan asuinosoitteeseen ja -alueeseen. Hauissa on käytetty suomenkielisiä sanoja, minkä lisäksi sanojen taivuttaminen vaikeissakin sanoissa on virheetöntä. Tämä viittaa osaltaan siihen, että hakujen tekijä on suomalainen tai ainakin osaa suomea erityisen hyvin.

Tor-verkon Onion-piilopalvelu

OPSVM-palvelimen root-käyttäjä on 21.10.2020 pystyttänyt Tor-verkossa toimivan Onion-piilopalvelun ja testannut sen toimivuutta. Luodulla Onion-sivustolla on ollut potilastiedostojen lisäksi myös kopio Ylilaudalla olleesta mainitusta Onion-osoitteesta kertovasta viestiketjusta sekä tähän viestiketjuun liittyvät apu- ja tyylitiedostot. Kirjautuneena näitä toimenpiteitä tehtäessä on ollut WI8-avain (S19, s. 18).

Kysyttäessä edellä mainitusta viestiketjussa olleesta Ylilaudalle johtavasta linkistä Kivimäki on ilmoittanut, ettei linkki ollut asiayhteydessään ja että se oli ollut vastaus toiseen viestiin, joka ei ilmennyt tässä viestiketjukopiossa. Kiristäjän sivuillaan jakama viesti oli toisessa keskustelussa, jossa Kivimäen mukaan oli valitettavasti ollut myös potilastiedot, joita ei olisi pitänyt jakaa. Alkuperäinen kiristäjä keskusteli Ylilaudalla ja kiristäjä oli jakanut linkin keskusteluun. Kun tälle sivulle oli mennyt, oli tämä ensimmäinen asia, mitä siellä oli ollut ja mistä Kivimäki oli poiminut linkin arkistoituun keskusteluun. Kivimäen mukaan todisteissa ei ollut nähtävillä keskustelun asiayhteyttä, mutta siitä pystyi päättelemään, että siellä keskusteltiin tästä linkistä. Kivimäen mukaan hän olisi laittanut linkin kiristäjän etusivulle, jos hänellä olisi ollut tahtotila jakaa tietoja. Linkissä oli ollut vain kopio Ylilauta-keskustelusta, eikä siitä voi tehdä johtopäätöstä, mitä keskustelua siinä oli käyty. Kivimäki oli vastannut tiettyyn viestiin ja viestinumeroon vastaamalla ”siis tää” ja antamalla linkin. Linkistä olisi päässyt etusivulle vain muokkaamalla osoitteen linkkiä. Kivimäki arveli löytäneensä linkin käymällä kiristäjän etusivulla.

Syyttäjien mukaan Kivimäen esittämä ei kuitenkaan kerro sitä, mistä linkki on kopioitu, eivätkä syyttäjät ole edes väittäneet, että Kivimäki olisi ensimmäisenä ”postannut” Onion-linkin. Syyttäjät ovat tältä osin viitanneet kirjalliseen todisteeseen S19 (s. 791), josta ilmenee, että Onion-sivustolla on potilastiedostojen lisäksi ollut myös kopio Ylilaudan viestiketjusta, jossa tätä Onion-osoitetta on mainostettu. Sivun html-osuus sisältää viestien sisällön, mutta niiden asetteluun liittyvät apu- ja tyylitiedostot on lisätty Onion-sivustolle vasta 54 minuuttia myöhemmin. Tiedosto 000ylilauta.html lisättiin sivulle 21.10.2020 kello 04:22:59 ja aputiedostot kahden minuutin aikana 05:18 ja 05:19. Kivimäen Ylilaudalle nimimerkillään lähettämät edellä mainitut kaksi viestiä, joissa annetaan linkki Tor-sivulla sijaitsevaan viestiketjuun, on lähetetty 21.10.2020 kello 05:20:50 sekä 05:23:52. Edellä mainitut viestit on siten lähetetty vain alle kaksi minuuttia OPSVM-palvelimen käyttäjän tekemien toimenpiteiden jälkeen ja näillä toimilla on myös osaltaan varsin läheinen ajallinen yhteys potilastietojen julkaisuun Ylilaudalla. Tiedot on kuitenkin poistettu Ylilaudalta, minkä jälkeen Spamclan on ilmoittanut saman olevan Torilaudalla, mistä se on myös poistettu. Tämän jälkeen ohjaus on vaihtunut Onion-sivun puolelle.

Kiristäjä on 21.10.2020 kello 01:52:05 (UTC) lähettänyt sähköpostin Vastaamon toimitusjohtajalle, jossa hän on kertonut julkaisseensa ensimmäiset sata potilastiedosta. Hän on lisäksi kertonut Onion-osoitteesta, josta sadan ensimmäisen potilaan potilastiedot ovat ladattavissa (S50).

SSH-salausavaimet ja niiden käyttö

Kirjautuminen edellä mainituille palvelimille on ollut palvelinkokonaisuudessa toteutettu käyttämällä käyttäjätunnus ja salasana -yhdistelmän asemesta niin sanottuja SSH-avaimia. Liikenne kulloinkin halutulle P2-palvelimella sijaitsevalle virtuaalipalvelimelle on tapahtunut rooter- ja vpn-virtuaalipalvelimien kautta siten, että ulkoverkon puolelta on ensin otettu yhteys rooter-virtuaalipalvelimeen, josta liikenne on ohjautunut vpn-palvelimen kautta edelleen halutulle virtuaalipalvelimelle. Liikenne on ollut lisäksi suojattuna WireGuard-nimisellä VPN-ohjelmistolla.

Kirjautumisessa käytetty SSH-kirjautuminen on etäkäyttötapa, joka perustuu käyttäjällä ja palvelimella sijaitsevien SSH-ohjelmistojen luomiin ainutlaatuisiin avainpareihin (julkinen ja yksityinen avain), joiden avulla käyttäjä ja palvelin voivat luotettavasti tunnistaa toisensa. Avainparin julkinen avain sijaitsee palvelimella, jonne yhteys on tarkoitus ottaa, ja yksityinen avain puolestaan yhteydenottajan omalla tietokoneella SSH-ohjelmiston tätä tarkoitusta varten luomassa tekstitiedostossa. Käyttäjän ottaessa yhteyttä palvelimeen käyttäjän tietokoneella ja palvelimella olevat SSH-ohjelmistot huolehtivat avaimien vertaamisesta toisiinsa automaattisesti. Mikäli avaimet muodostavat parin, yhteydenotto sallitaan. Koska SSH-avaimet ovat yleensä varsin pitkiä, SSH-avaimista on mahdollista ottaa esimerkiksi niiden vertailua varten niin sanottu SSH-sormenjälki. Asiantuntijana kuullun Monosen mukaan palvelin kirjottaa lokiin sen avaimen sormenjäljen, jota on kulloinkin käytetty kirjautumisessa. Sormenjälki on ainutkertainen ja yhdenmukainen käyttäjän yksityisen avaimen kanssa.

Mononen on kertonut, että käytettäessä SSH-avaimia on mahdollista, että SSH-ohjelmisto kysyy käyttäjältä vielä erikseen salasanan tapaista salalauseketta, joka purkaa tarvittavan SSH-avaimen ja mahdollistaa kirjautumisen esimerkiksi halutulle palvelimelle. Mahdollista on myös, että SSH-avain on salaamaton, jolloin tällaista salalauseketta ei ole käytössä. Mononen on pitänyt tällaista salaamattoman SSH-avaimen käyttämistä

huonona ratkaisuna, koska se muodostaa tietoturvariskin. Asiassa esitetystä aineistosta ei ole nähtävissä, onko tässä asiassa ollut käytössä tällainen salalause.

Tutkinnassa on selvinnyt, että tämän asian kannalta keskeisille virtuaalipalvelimille (rooter, vpn, irc ja gogs) on voinut kirjautua SSH-avaimilla, joiden sormenjälki on ollut WI8- ja item-alkuinen.

Tietoteknisessä tutkinnassa ei ole ilmennyt, että item-avaimella olisi kirjaudutt kertaakaan eikä se vaikuta olleen muutoinkaan aktiivinen. Näin ollen on mahdollista, että tämä avain on jäänyt asetustiedostoihin aikaisemmista käyttökerroista. Avain on voinut olla käyttäjän aikaisemman tietokoneen SSH-avainparin julkinen avain, joka on jäänyt palvelimelle ja jota ei ole koettu tarpeelliseksi poistaa.

SSH-avain, jonka sormenjälki on ollut WI8-alkuinen

Tutkittavien rikosnimikkeiden osalta keskeiseksi on noussut SSH-avain, jonka sormenjälki on WI8-alkuinen. Kyseinen avain on ollut P-palvelinten pääkäyttäjätasoinen SSH-avain. Sillä on voinut kirjautua P1-P3-palvelimille ja rikoskokonaisuuden kannalta olennaisille virtuaalipalvelimille rooter, vpn, gogs, irc ja OPSVM.

Sekä P1- että P2-palvelin oli salattu vahvalla salauksella, ja palvelimille on ollut mahdollista kirjautua ainoastaan WI8-avaimella. Koska P3-palvelin oli takavarikoitaessa tyhjennetty, kyseisen palvelimen kirjautumisjärjestelyistä ei ole tietoa. Tutkinnassa on kuitenkin selvinnyt, että myös P3-palvelimelle on kirjauduttu WI8-avaimella ainakin kerran.

Lähes kaikki sekä Vastaamon että sen potilaiden kiristämisen kannalta olennaiset toimenpiteet on edellä esitetyin tavoin tehty OPSVM-virtuaalipalvelimella, kun kirjautuneena on ollut ainoastaan WI8-avain. Poikkeuksen muodostaa hetki, jolloin OPSVM-palvelimelle on asennettu MySQL-palvelinohjelmisto potilastietokannan käsittelyä varten. Tällöin kirjautuneena on ollut myös ml0-avain, joka on ollut kirjautuneena myös yksinään, kun Vastaamon potilastietokannasta on luotu potilaskohtaisia tekstitiedostoja python-ohjelmointikielellä luodulla skriptillä. Lisäksi kun potilastietokannasta luotuihin tekstitiedostoihin on tehty tekstihakuja, kirjautuneena on ollut WI8-avain lukuun ottamatta yhtä hakua, jonka oli tehty ml0-avaimella.

Onko WI8-alkuisen sormenjäljen jättäneellä SSH-avaimella ollut useita käyttäjiä

Syyttäjät ovat esittäneet, että Kivimäki on rikostapahtumien aikaan käyttänyt WI8-avainta ja ollut myös sen ainoa käyttäjä.

Kivimäen kertomus WI8-avaimen käyttämisestä on muuttunut oikeudenkäynnin aikana. Hän on oikeudenkäynnin alussa kertonut käyttäneensä kyseistä avainta ja kertonut lisäksi, että kysymyksessä oli usean käyttäjän kesken jaettu avain. Hän on myös todennut, että käyttäjien oikeuksia ja pääsyä palvelimille oli valvottu SSH-avainten asemesta WireGuard-ohjelmistolla.

Kivimäki on myöhemmin käräjäoikeudessa muuttanut kertomustaan ja todennut, ettei olekaan varma siitä, onko hän itse käyttänyt WI8-avainta. Hän on lisäksi kertonut, ettei hän toisaalta myöskään tunnistaisi, mikäli olisikin käyttänyt kyseistä avainta, koska tämä ei ole käyttäjälle tavallisesti näkyvä tieto.

Kivimäki on myös muuttanut käsitystään kirjallisesta todisteesta V12 oikeudenkäynnin aikana. Hän on oikeudenkäynnin alussa todennut, että kyseinen vpn-virtuaalipalvelimen WireGuard-ohjelmiston asetuksia sisältänyt tiedosto on sisältänyt kaikki WI8-avainta käyttäneet käyttäjät mukaan lukien hänet itsensä tunnuksella ”r”. Myöhemmin oikeudenkäynnin aikana Kivimäki on todennut, että koska hänelle kuuluva käyttäjätunnus ”r” on WireGuard-ohjelmiston asetuksissa vasta aivan loppupäässä niin sijaintinsa kuin IP-osoitteen viimeisen luvun perusteella, hän ei ole voinut olla kyseisen palvelimen omistaja eikä sen ylläpitäjä. Kivimäki on edelleen todennut, että WireGuard-asetusten listalla ensimmäisenä oleva käyttäjä, jonka IP-osoite on 192.168.3.77, on 20. lokakuuta kirjautunut virtuaalikoneelle käyttäen WI8-avainta, joten tämä käyttäjä on myös WI8-avaimen käyttäjä.

Kivimäen kertomuksen muuttuminen heikentää sen uskottavuutta. Uskottavuutta heikentää erityisesti se, että kertomus on muuttunut nimenomaan sen jälkeen, kun WI8-avaimen keskeinen merkitys tapahtumakokonaisuudessa on alkanut selvitä.

Usealle käyttäjälle jaetun SSH-avaimen käyttöä ei tue todistaja Naughtonin kertomus, jonka mukaan hänellä itsellään oli ollut oma henkilökohtainen SSH-avain, jota hän ei ollut jakanut kenenkään kanssa. Naughtonin mukaan SSH-avaimia oli alettu käyttää Scanifissa Vanderpotin ideasta. Vaikka Naughton onkin puhunut omasta käytännöstään Scanifissa ja K-sarjan palvelimilla, tukee tämä Scanifissa ja K-sarjan palvelimilla ollut käytäntö käsitystä siitä, että SSH-avaimet olivat olleet henkilökohtaisia.

Lisäksi Naughton on kommentoinut yksittäisiä potilastekstitiedostoja luovaa python-ohjelmointikielellä luotua ohjelmakoodia, ettei hän usko Kivimäen kirjoittaneen kyseistä koodia, koska se ei hänen mukaansa ole näyttänyt teknisesti sellaiselta koodilta, jota hän on nähnyt Kivimäen tehneen. Naughtonin mukaan Kivimäen kirjoittama koodi on ”sotkuista”. Tämä tukee johtopäätöstä, jonka mukaan ml0-avaimen käyttäjä on voinut olla joku muu henkilö kuin WI8-avaimen käyttäjä.

Käräjäoikeus katsoo, ettei WireGuard-asetustiedostosta ja kirjautumistiedoista ole mahdollista tehdä täysin varmaa ja tyhjentävää johtopäätöstä siitä, miten käyttäjähallinta P-sarjan palvelimilla oli toteutettu. Riidatonta on, että asetustiedostossa ensimmäisenä olevalla IP-osoitteella 192.168.3.77 oleva käyttäjä on pystynyt kirjautumaan vpn-palvelimelle WI8-avaimella. Näistä tiedoista ei kuitenkaan voi tehdä sitä päätelmää, etteivätkö myös muut asetustiedostossa olevat IP-osoitteet olisi voineet niin ikään kirjautua WI8-avaimella.

Mononen on pitänyt riskialttiina sellaista järjestelyä, jossa usealle eri käyttäjälle on annettu sama kirjautumiseen käytettävä SSH-avain. Tällöin ei Monosen mukaan voida todentaa, kuka avainta on käyttänyt ja ollut kirjautuneena minäkin ajankohtana. Mononen on pitänyt tietoturvan kannalta parempana ratkaisuna järjestelyä, jossa jokaisella käyttäjällä on oma henkilökohtainen SSH-avaimensa. Monosen kertomusta jokaisella käyttäjällä olevasta yksilöllisestä SSH-avaimesta tukee myös Naughtonin kertomus.

Käräjäoikeus pitää Monosen tavoin erittäin riskialttiina sellaista järjestelyä, jossa yhdellä pääkäyttäjätason kirjautumisavaimella olisi useita käyttäjiä. Tällainen järjestely ei mahdollista järjestelmän käyttäjien oikeuksien eikä kirjautumisen hallintaa ja on siten suuri tietoturvauhka. Menettely olisi käräjäoikeuden näkemyksen mukaan myös ilmeisessä ristiriidassa järjestelmän varsin pitkälle vietyjen tietoturvamenettelyiden kanssa, joihin on kuulunut

muun muassa salasanakirjautumisen estäminen, salattu verkkoliikenne myös palvelimien välillä sisäverkossa ja tehokkaasti kryptattu tiedostojärjestelmä. Tähänkin nähden Kivimäen edellä tuomiosta ilmenevä kertomus hänen joltain henkilöltä saamastaan SSH-avaimesta on epäuskottava.

Rikoskokonaisuuteen liittyvä WI8-avaimen johdonmukainen käyttö puhuu vahvasti sen puolesta, että WI8-avainta on kiristystoimenpiteiden aikaan käyttänyt yksi ja sama henkilö. Potilastietojen levitykseen ja kiristykseen liittyvät WI8-avaimella tehdyt toimenpiteet ovat olleet johdonmukaisia ja päämäärätietoisia. Toimenpiteitä on myös tehty juuri oikeassa järjestyksessä ajallisesti hyvinkin lähellä toisiaan. Ainoastaan tekokokonaisuuteen kuuluva MySQL-ohjelmiston asennus sekä tekstitiedostojen luominen Vastaamon potilastietokannasta on tehty käyttäen toista ml0-alkuista SSH-avainta. Tämä seikka puhuu syyttäjien esittämin tavoin toisen mahdollisen tekijän puolesta. Huomioon on tällöinkin otettava, että mahdolliset toisen tekijän toimenpiteet on tehty käyttäen kokonaan toista SSH-avainta eikä tällöinkään kirjautuneena ole ollut kahta henkilöä samalla WI8-avaimella.

Kivimäen asuminen ja IP-osoitteet 37.156.72.25 ja 147.161.123.116

Asuminen

Asiassa on riidatonta, että Kivimäki on asunut alkuvuodesta 2020 Barcelonassa Espanjassa ainakin osoitteessa Carrer de Gaziel 43 ja tämän jälkeen Lontoossa ainakin osoitteessa 70 Horseferry Road. Esille on tullut Espanjan osalta myös osoite Carrer Selva de Mar 12 3–1 ja osoitteeseen yhdistettävissä oleva IP-osoite 147.161.123.116, joista Kivimäki on kiistänyt tienneensä mitään. Riitaista asiassa on ollut Kivimäen asuminen Lontoossa ja Horseferry Roadin asuntoon yhdistettävissä olevan IP-osoitteen 37.156.72.25 käyttäminen etenkin syksyllä 2020. Kivimäki on väittänyt Horseferry Roadin asunnon jääneen pois Abell Housen vuokrasopimuksen allekirjoittamisen jälkeen 14.9.2020.

Kivimäki on kertonut muuttaneensa joskus kesän 2020 alussa Espanjasta Lontooseen. Lontooseen saavuttuaan Kivimäki oli asunut hetken hotellissa sekä tämän jälkeen tyttöystävänsä Khodykinan kanssa asunnossa Mayfairissä. Tämän jälkeen Kivimäki on kertonut muuttaneensa yhdessä tyttöystävänsä kanssa Horseferry Roadilla sijainneeseen asuntoon. Heidän kanssaan Lontoon asunnossa oli asunut myös todistaja Ruhanen, kunnes Ruhanen oli muuttanut Kivimäen Ruhaselle hankkimaan yksiöön. Kivimäelle oli tullut ero tyttöystävästään noin kuukautta ennen vuokrasopimuksen solmimista Abell Housen asunnosta. Kivimäki oli ennen muuttoa asunut kavereidensa ”nurkissa” ja tämän jälkeen vuokrannut asunnon Abell Housesta, mutta tarkkaa päivämäärää muutolleen hän ei ole muistanut. Kivimäki on tältä osin viitannut kirjalliseksi todisteeksi nimeämäänsä vuokrasopimukseen. Hän oli ottanut vuokraamaansa asuntoon myös Hyperopticin liittymän staattisella IP-osoitteella.

Kivimäki on vielä kertonut, että Hyperoptic oli Lontoossa yleinen palveluntarjoaja, eikä hän muistanut, mistä lähtien kyseisen palveluntarjoajan yhteys hänellä Lontoossa asuessaan oli ollut. Kivimäki on pitänyt mahdollisena sitä, että hän oli käyttänyt Horseferry Roadin asunnossa ollutta nettiliittymää, mutta kiistänyt tilanneensa taikka maksaneensa asunnon liittymästä mitään maksuja. Liittymän asuntoon oli mahdollisesti tilannut Khodykina. IP-numero 37.156.72.25 oli hänelle tuttu ainoastaan esitutkintapöytäkirjojen kautta. Myös Ruhanen oli mahdollisesti asunnossa asuessaan käyttänyt liittymää. Kysymys asunnossa oli enemmänkin

Hyperopticin käyttämästä CGNat-teknologiasta, jossa IP-osoitteita jaettiin jopa tuhansien asiakkaiden kesken.

Kivimäki on muutoinkin häntä kuultaessa vaikuttanut olevan hyvin tietämätön tai muistamaton siitä, millainen Horseferry Roadin asunnon verkkoliittymä oli ollut, kuka liittymän oli tilannut tai kuka sitä oli käyttänyt. Horseferry Roadilla ei ollut kiinteää IP-osoitetta, mutta asunnossa oli varmasti ollut wlan-tunnukset. Kivimäki on kiistänyt sen, että Horseferry Roadilla käytössä ollut liittymä olisi jollain tavoin jäänyt hänen käyttöönsä hänen Abell Houseen tapahtuneen muuttonsa jälkeen.

Kivimäki on lisäksi kertonut lähteneensä marraskuussa 2020 pakoon koronarajoituksia Dubaihin. Kivimäki oli kertomansa mukaan lentänyt Dubaihin yksin. Dubaissa Kivimäki oli tavannut sattumalta Khodykinan muutaman kerran. Syyttäjät ovat Dubain matkan osalta viitanneet Kivimäen esitutkintakertomukseen (esitutkintapöytäkirja 2400/R/206/20, s. 69), jossa Kivimäki on kertonut lähteneensä tyttöystävänsä perässä Dubaihin. Kivimäki on tältä osin käräjäoikeudessa selvittänyt kertomuksensa eroavuutta sillä, että esitutkintakertomukset eivät olleet tuoreita ja poliisi oli kirjannut kertomuksen ”niin kuin on kirjannut” ja että ilmaisut olivat voineet mennä sekaisin. Esitutkintakertomuksesta tuli Kivimäen mukaan ”hassu kuva”. Kivimäen mukaan he olivat Khodykinan kanssa lentäneet samalla lennolla, mutta he olivat olleet lentokoneen eri osissa. Dubaissa Kivimäki oli oleskellut noin kahdeksan kuukauden mittaisen ajan ja palannut tämän jälkeen takaisin Lontooseen kesän 2021 alussa. Kivimäki oli koko Dubaissa olonsa ajan maksanut Abell Housen vuokran, joka hänen muistikuviensa mukaan oli ollut noin 6.000 euroa kuukaudessa.

Todistaja Ruhanen on kertonut asumisestaan Espanjassa sekä Lontoossa Horseferry Roadilla yhdenmukaisesti Kivimäen kanssa. Ruhanen on kertonut käyttäneensä Kivimäen ja tämän tyttöystävän asunnossa ollutta internetliittymää toukokuun 2020 puolivälistä eteenpäin kestäneen noin 2–3 kuukauden mittaisen asumisensa aikana pelaamiseen ja normaaliin tekemiseen. Ruhanen oli muuttanut Kivimäen ja tämän tyttöystävän asunnosta omaan, samassa asuntokompleksissa sijainneeseen yksiöönsä loppukesästä 2020.

Ruhanen on Kivimäen Dubaihin lähdön osalta kertonut, että Kivimäki oli lähtenyt Dubaihin yhdessä tyttöystävänsä Khodykinan kanssa. Ruhasen käsitys oli ollut, että Kivimäki ja Khodykina olivat seurustelleet, eikä hän ollut havainnut eroa. Kivimäen ja Khodykinan suhde oli Ruhasen mukaan edennyt nopeasti, eikä Ruhanen tiennyt, missä vaiheessa Khodykinan ja Kivimäen suhde oli päättynyt ja mitä sille myöhemmin tapahtui. Mahdollisesti tammikuussa 2021, jolloin Ruhanen oli ollut jo Suomessa, oli Khodykina kysellyt häneltä ruokapaikoista Barcelonassa, ja tämä oli mahdollisesti indikoinut sitä, että Kivimäen ja Khodykinan suhde olisi päättynyt. Ruhanen ei ole osannut sanoa varmaksi sitä, oliko Kivimäki jo luopunut Barcelonan asunnostaan. Lisäksi hän on kertonut, että hänen luottokorttilaskunsa oli syksyllä 2020 mennyt Barcelonan osoitteeseen. Kivimäki oli laittanut Ruhaselle viestiä tästä laskusta kehottaen Ruhasta huolehtimaan laskusta.

Ruhanen on lisäksi Kivimäen asumista koskien kertonut, että Kivimäki oli jossain vaiheessa hankkinut Lontoosta myös toisen asunnon. Ruhanen ei muistanut tämän vara-asunnoksi kutsumansa asunnon osoitetta, mutta on kertonut sen sijainneen noin puolen kilometrin päässä Kivimäen ja Khodykinan asunnosta. Ruhanen ei missään vaiheessa ollut nähnyt Kivimäen asuvan kyseisessä vara-asunnossa. Ruhanen oli käynyt tässä asunnossa yhden

kerran antamassa jollekin kaverille avaimet sekä toisen kerran siten, että Kivimäki oli itse ollut asunnolla paikalla. Ruhanen on kertonut vielä siitä, että Kivimäen Lontoon asunnot olivat Kivimäen Dubain matkan aikana olleet Kivimäellä ”ihan normaalisti”. Pääasuntona Kivimäellä oli Ruhasen mukaan ollut asunto, jossa Kivimäki ja Khodykina olivat asuneet yhdessä.

Käräjäoikeus toteaa, että Kivimäki on pyrkinyt etäännyttämään itsensä Horseferry Roadin asunnosta, siellä olleesta internetliittymästä ja sen käyttämisestä. Kivimäki on väittänyt eronneensa tyttöystävästään Khodykinasta ja muuttaneensa Horseferry Roadilta Abell Housen asuntoon syyskuussa 2020. Kivimäen kirjalliseksi todisteeksi nimeämä vuokrasopimus Abell Housen asunnon osalta osoittaa ainoastaan, että kyseinen vuokrasopimus on solmittu syyskuussa 2020. Tämä ei kuitenkaan osoita tosiasiallista muuttoa asuntoon. Todistaja Ruhanen ei ole havainnut Kivimäen väittämää eroa ja on kertonut lisäksi vastoin Kivimäen kertomusta, että Kivimäki oli matkustanut Dubaihin yhdessä tyttöystävänsä kanssa. Lisäksi Ruhanen on kertonut Kivimäen hankkimasta vara-asunnosta omiin tarkoituksiinsa.

Kivimäen tietotekninen osaaminenkin huomioon ottaen uskottavaa ei ole, etteikö hän olisi tietoinen Horseferry Roadin asunnossa käytössä olleista tietoliikenneratkaisuista kuten siitä, minkälainen liittymä asunnossa on ollut, miten liittymää on jaettu, kuka liittymän tilaaja olisi ollut ja kuka sitä on myös maksanut. Kivimäki on itsekin kuulemisessaan selvittänyt tarvettaan muuttumattomalle, staattiselle IP-osoitteelle sekä VPN:n käyttämiselle. Kivimäen kertomuksen uskottavuutta on muutoinkin horjuttanut se, että Kivimäki on useasti häntä kuultaessa ja muutoinkin antamissaan selvityksissä etenkin tietoteknisissä asioissa pyrkinyt viittaamaan tarkalleen siihen, mitä asiassa jo esitetty kirjallinen todistelu hänen käsityksensä mukaansa osoittaa tai on osoittamatta. Kertomus on muutoinkin tiettyjen kirjallisten todisteiden osalta ollut hyvinkin yksityiskohtainen, jopa ilman, että kyseisestä kirjallisesta todisteesta sinänsä ilmenisi sitä, mistä Kivimäki on kertonut.

IP-osoitteet 37.156.72.25 ja 147.161.123.116

Horseferry Roadilla on Hyperopticin asiakastietojen mukaan ollut Hyperopticin liittymä (S64). Asiakkuustiedoista ilmenee, että asiakkuus sopimusnumerolla 440266 on rekisteröity Kristina Khodykinan nimellä 70 Horseferry Roadille osoittavin yhteystiedoin kuitenkin siten, että yhteyshenkilöksi (”nominated person”) on tilaajatiedoissa ilmoitettu ”Alex Kidimaki”. Kivimäki on tältä osin kertonut, ettei ole tietoinen, miten hänen nimensä on yhteyshenkilöksi päätynyt eikä hän tiedä, mitä sillä tarkoitettiin. Kivimäki on pitänyt mahdollisena, että hänellä oli ollut jossain vaiheessa tarve hallinnoida liittymää. Hän on kuitenkin todennut, että tuskin on tätä tietoa itse Hyperopticille ilmoittanut vaan että tieto oli jotenkin sinne päätynyt. Kyseinen sopimus numerolla 440266 on todisteesta ilmenevien maksutietojen mukaan ollut voimassa ainakin toukokuusta 2020 kesäkuuhun 2021 saakka. Edellä mainitun kirjallisen todisteen liittymän tilaajatiedoista ilmenee edelleen, että Hyperopticin liittymän tilaajatietoihin on puolestaan 23.9.2022 alkaneen sopimuksen numero 573195 osalta merkitty ”Aleksenteri Kivimäki ”ja yhteystiedoiksi alex@safe.im sekä 888-loppuinen puhelinnumero. Palvelu on koskenut 1 gigan kuituliittymää ja lisämaksuna palveluun on ostettu myös staattinen, muuttumaton IP-osoite. Palvelu on lopetettu 15.1.2023, ja 19 laskusta viimeiset 3 maksuerää on ollut myöhässä. Kivimäen tiedoilla on Hyperopticilta saatujen tietojen mukaan löytynyt tili, jossa yhteystiedoiksi on merkitty alex@safe.im sekä -4744 ja 0415-loppuiset puhelinnumerot.

Kivimäellä on ollut myös lisätili (”additional account”) edellä mainituilla yhteystiedoilla, mutta kuitenkin eri puhelinnumerolla, jonka loppuosa on ollut 0888 (S48).

Asiassa on selvitetty, että Ruhanen on asunut Kivimäen luona Lontoossa muutaman kuukauden kesällä 2020 ja käyttänyt tänä aikana asunnon internetyhteyttä. Ruhasen kirjautumiset OP-verkkopankkiin ajalla 20.5.¬31.7.2020 IP-osoitteesta 37.156.72.25 käyvät ilmi kirjallisesta todisteesta S40. Ruhasen muuttaessa elokuussa 2020 omaan yksiöön ja hankittuaan oman internetyhteyden (S48) on myös Ruhasen IP-osoite vaihtunut toiseksi (S72).

Kivimäki on pääkäsittelyn kuluessa myöntänyt riidattomaksi sen, että hän on käyttänyt IP-osoitetta 37.156.72.25 useaan otteeseen kesän 2020 aikana. IP-osoitteesta 37.156.72.25 on Kivimäen nimellä toukokuussa 2020 tehty varaus hotelli Kämpiin ajalle 31.5.–7.6.2020 (S36). Varauksesta ilmenee Kivimäen osoite Espanjaan Barcelonaan (Carrer 43) sekä Kivimäelle kuuluvat 4501-loppuinen puhelinnumero sekä sähköpostiosoite paypal@safe.im. Lisäksi IP-osoitteesta 37.156.72.25 Kivimäki on käyttämällään Spamclan-nimimerkillä tehnyt 12.6.2020 kello 14:09:36 Ylilaudalle ”postauksen”, missä viestin otsikkona on ollut ”bentleyt” (S38). Kivimäki on vielä rekisteröitynyt samaisesta IP-osoitteesta myös 15.6.2020 OnlyFans-palveluun ja tehnyt palveluntarjoajille maksuja kesä- ja heinäkuussa 2020 itselleen kuuluneella Mastercard-luottokortilla (S39).

Kivimäki on kuitenkin IP-osoitteen 37.156.72.25 osalta kiinnittänyt huomiota siihen, että tämä IP-osoite on joka tapauksessa esiintynyt jo ennen Kivimäen muuttoa Abell Houseen syksyllä 2020. Lisäksi yksikään aika, jolloin yhteyksiä kyseisestä IP-osoitteesta olisi otettu, ei täsmää yhteen väitettyjen rikosten tekoaikojen kanssa.

Kirjallisten todisteiden mukaan Hyperopticin IP-osoitteesta 37.156.72.25 on 23.10.2020 kello 12:04:24 ja 12:23:48 (UTC) välisellä ajalla otettu useita WireGuard-yhteyksiä P2-palvelimelle vastaamo.tar-virheen selvittyä (S19 ja S30). Syyttäjien käsityksen mukaan kirjautuja on sama henkilö kuin kiristäjä. Virheenselvityksen yhteydessä on myös tehty hakuja tiedoston mukana vuotaneiden tiedostojen nimiin sekä pääkäyttäjän kotihakemiston tietosisältöön, missä yhtenä hakuterminä on 23.10.2020 kello 13:12:58 ollut myös ”ryan” (S19). Nimimerkki ”ryan” on riidattomasti yksi niistä nimistä, joilla Kivimäkeä kutsutaan.

Kirjallisesta todisteesta S20 käy ilmi, että P2-palvelimella on ollut asennettuna myös silasdev-virtuaalipalvelin. Kuten tuomiossa on aikaisemmin todettu, tällä palvelimella on ollut käytössä top_talkers-toiminnallisuus, joka kerää tietokantaan tilastoa IP-osoitteista ja niiden tuottamasta liikennemäärästä verkkoon. Kyseisen tietokannan mukaan IP-osoite 37.156.72.25 on käyttänyt virtuaalikoneiden muodostamaa lähiverkkoa seitsemän kertaa (9.10.2020, 10.10.2020, 14.10.2020, 16.10.2020, 18.10.2020 sekä 20.10.2020), joista yhteensä neljä kertaa (9.10.2020, kaksi kertaa 16.10.2020 ja 18.10.2020) osuu sellaiseen ajankohtaan, kun P2-palvelimella olevalle IRC-virtuaalipalvelimelle on kirjauduttu käyttäen SSH-avainta, jonka sormenjälkenä on WI8.

Lisäksi Kivimäelle riidattomasti kuuluva käyttäjänimi ”r” (sähköpostiosoitteella aleksanteri@scani.fi) on kirjautunut useita kertoja IP-osoitteesta 37.156.72.25 K16-palvelimella olleeseen GitLab-palveluun (S21).

Kirjallisesta todistelusta käy ilmi, että IP-osoitteen 37.156.72.25 käyttö on toistuvaa ja pitkäaikaista. Tätä IP-osoitetta on käytetty aina alkukesästä 2020 vielä senkin jälkeen lokakuussa 2020, kun muutto Horseferry Roadilta Abell Houseen olisi Kivimäen mukaan jo tapahtunut. Tätä osoittaa muun muassa Kivimäen käyttäjätunnuksen ”r” kirjautuminen lokakuussa 2020 IP-osoitteesta 37.156.72.25. Myös se, että Hyperopticin maksutietojen mukaan maksut ovat jatkuneet vielä senkin jälkeen kun Kivimäki on väittämänsä mukaan muuttanut Abell Housen asuntoon syyskuussa 2020, tukee johtopäätöstä siitä, että Horseferry Roadin liittymää on käyttänyt Kivimäki yhtäjaksoisesti Lontooseen muutettuaan. Kivimäki on ottanut liittymän omiin nimiinsä elokuussa 2021 (S48 ja S64).

Kivimäki on kertonut tarpeestaan staattiselle IP-osoitteelle, koska tällöin sisäverkkoon pystyi ottamaan yhteyden myös asunnon ulkopuolelta käsin. Huolimatta siitä, ettei Hyperopticin sopimuksissa ole mainintaa staattisesta IP-osoitteesta ennen kuin vasta 23.9.2022 lukien,myös Ruhanen internetin käyttö on kesällä 2020 Horseferry Roadin asunnossa yhdistynyt nimenomaisesti IP-osoitteeseen 37.156.72.25. Edellä kerrottu osoittaa sen, että kysymys on ollut syyttäjien katsomin tavoin staattisesta IP-osoitteesta, jota Kivimäki on käyttänyt toukokuusta lokakuuhun 2020 saakka.

Kivimäki on WI8-avaimen käytön osalta vedonnut myös espanjalaisen IP-osoitteen 147.161.123.116 käyttöön (V30.2). Hän on nostanut näiltä osin esiin Silvana Novacovici sekä Daniel Fulgescu -nimiset henkilöt. IP-osoitetta on käytetty, kun P2-palvelimeen on otettu yhteyksiä aikavälillä 22.10.2020–23.10.2020. Näiden yhteyksien kanssa samaan aikaan OPSVM-virtuaalipalvelimella on tehty muun muassa potilastietojen julkaisun ajastaminen (S19). Kyseinen yhteys on ainoa, joka on aktiivisena, kun WI8-avainta käytetään.

Kivimäki on kiistänyt liittyvänsä espanjalaiseen IP-osoitteeseen tai sen sijaintiosoitteeseen millään tavalla. Hän on vedonnut siihen, ettei hän ole voinut olla tekijä ottaen huomioon hänen saman aikainen asumisensa Lontoossa. Kivimäki onkin pyytänyt oikeudenkäynnin aikana lisätutkintaa espanjalaisesta IP-osoitteesta 147.161.123.116.

Edellä kerrotusta IP-osoitteesta 147.161.123.116 on tehty tietopyyntö Ademo Telecom Iberia S.A.U:lle 21.3.2020–1.12.2020 ja 21.8.–1.12.2020 välisille ajoilla. Tietopyyntöön saadun vastauksen mukaan ajalla 21.8.2020–1.12.2020 IP-osoite on kuulunut henkilölle nimeltä Silvana Novacovici, CL Selva de Mar 12 3–1, 08019 Barcelona (S104). Yhteystietona kyseiselle henkilölle on ilmoitettu sähköpostiosoite silvananovacovici@yahoo.com sekä 839-loppuinen puhelinnumero. Katalaanin kieli huomioiden osoitteesta ilmenevä lyhenne CL voi myös syyttäjien selvityksen mukaan ilmetä muodossa Calle tai Carrer Selva de Mar.

Edellä mainittu osoite yhdistyy Kivimäkeen kirjallisena todisteena esitetyn Europolin Siena-kyselyjen tiedoissa (S105). Tiedoista ilmenee, että Kivimäki ja todistaja Ruhanen ovat ilmoittaneet Espanjan viranomaisille 23.2.2020 rikosasian yhteydessä osoitteekseen Calle Selva de Mar, número 12, piso 3 puerta 1, Barcelona.

Siena-kyselystä ilmenee myös, että edellä kerrottu osoite yhdistyy myös romanialaiseen Daniel Adrian Fulgescu -nimiseen henkilöön. Yhtenä osoitetietona Fulgesculle on kyseinen Calle Selva de Mar kahden muun osoitetiedon, Calle Mendizabal Valencia sekä Calle Gaziel 43 kanssa (S105). Viimeksi mainittu osoite on riidattomasti se osoite, jossa Kivimäki on asunut

Espanjassa asuessaan. Fulgescu-nimisen henkilön yhdistää Kivimäkeen myös Fulsgescun tiedoissa hänelle merkitty 0415-loppuinen puhelinnumero, joka sekin on riidattomasti kuulunut Kivimäelle.

Edellä mainitusta todisteesta ilmenee vielä sekin, että Asan Amet -niminen henkilö on 1.4.2022 tehnyt rikosilmoituksen 6.3.2022 varastetusta arvokellosta Espanjassa. Tämän rikosasian yhteydessä Asan Ametille osoitteeksi on niin ikään ilmoitettu kyseinen Carrer Selva de Mar. Asan Amet on Kivimäen käyttämä alias, ja tällä nimellä Kivimäki on esiintynyt helmikuussa 2023 jäädessään kiinni nyt käsillä olevassa rikosasiassa Ranskassa. Edelleen saman osoitetiedon, Carrer Selva de Mar, on 5.3.2022 tehdyn rikosilmoituksen yhteydessä ilmoittanut myös Miroshnichenko-niminen henkilö (S105), joka oli riidattomasti ollut Kivimäen tyttöystävä.

Carrer Selva de Marin osoitteeseen linkittyy myös BMW 740 -merkkinen ajoneuvo, espanjalaiselta rekisterinumeroltaan 0532 KWP. Todisteesta S107 ilmenee auton rekisteröintipäiväksi 29.4.2019 sekä auton omistajaksi sekä haltijaksi Daniel Fulgescu -niminen henkilö. Henkilön yhteystietona on jälleen osoite Carrer Selva de Mar.

Syyttäjän kirjallisesta todisteesta numero S106 ilmenee, että Kivimäen riidattomasti käyttämä nimimerkki Spamclan on 1.6.2021 postannut Ylilaudalle kuvan BMW-merkkisestä autosta. Todisteesta S108 ilmenee, että kyseistä autoa on ”ehostettu”. Arvostelun ehostamisesta on kirjoittanut ”Aleksanteri K 02/2020”. Arvostelu on kirjoitettu samaan aikaan kuin Kivimäki on tehnyt edellä mainitun 23.2.2020 päivätyn rikosilmoituksen. Auto on kirjallisen todisteen S105 mukaan 4.8.2021 katsastettu Saksassa Kivimäen romanialaisen puolison Dinun toimesta.

BMW:stä on kertonut myös todistaja Ruhanen. Ruhasen kuvaus Kivimäen autosta on myös vastannut Daniel Fulgesculle rekisteröidyn auton kuvausta. Todistaja Ruhanen on kertonut ajaneensa tätä autoa Barcelonassa. Tämän lisäksi autoa oli ajanut myös joku toinen henkilö, jonka nimi oli mahdollisesti alkanut d-kirjaimella. Ruhanen on kertonut, että tunnistaisi, jos hän näkisi henkilön valokuvan. Kun Ruhaselta on kysytty, olisiko henkilö voinut olla Daniel, Ruhanen on vastannut, että nimi kuulosti tutulta, mutta sukunimeä hän ei muistanut. Henkilö oli Ruhasen mukaan Juliuksen (Kivimäki) kaveri, ja he olivat käyneet yhdessä kasinolla ja pelanneet. Tämän jälkeen Ruhaselle oli näytetty valokuvaa jostain mieshenkilöstä, ja Ruhanen on kertonut, että kyseinen henkilö oli autoa ajanut henkilö. Kyseistä valokuvaa ei ole nimetty kirjalliseksi todisteeksi tai muuksi oikeudenkäyntiaineistoksi, eikä sitä ole pääkäsittelyn päätteeksi esitetyn pyynnön jälkeenkään toimitettu käräjäoikeudelle.

Osoite Carrer Selva de Mar yhdistyy Kivimäkeen myös Coinmotionin maksutietojen perusteella. Kirjallisesta todisteesta (S109) ilmenee, että daniel@safe.im sähköpostiosoitteesta on tehty erilaisia transaktioita Daniel Fulgescu -nimisen henkilön nimissä. Kyseiseen sähköpostiosoitteeseen yhdistyy kuitenkin useissa kohdin myös 0415-loppuinen puhelinnumero sekä safe.im-loppuinen sähköposti, jotka molemmat viittaavat Kivimäkeen.

Maksutiedoista ilmenee myös, että maksuja on tehty muun muassa Asianajotoimisto Lexialle, jossa Kivimäen puolustajat työskentelevät.

Muutamien maksujen viestitiedoista ilmenee englanniksi viestinä vuokranmaksu tai vuokravakuus sekä Fulgescun nimi ikään kuin vuokralaisen ominaisuudessa (rent payment, rent deposit, ”Rent payment RENTEE: Daniel

Fulgescu”) sekä jälleen osoite Carrer Selva de Mar. Todisteesta ilmenee sekin, että BMW 740 -merkkisestä autosta on 7.3.2019 maksettu Kechter Automobile oHG:lle 62.000 euroa viestillä ”bmw 740li payment for Daniel Fulgescu”. Auto on edeltä ilmenevästi reilu kuukautta myöhemmin rekisteröity Espanjaan Daniel Fulgesculle (S107).

Edellä mainittua sähköpostiosoitetta daniel@safe.im on käytetty 30.10.2021 Keskusrikospoliisille lähetetyssä sähköpostikyselyssä, jossa Daniel Tuominen -niminen henkilö on kysynyt esitutkintamateriaaleja Suomessa uutisoidusta tietovuotoon liittyvästä asiasta (S62). Poliisin vastattua kysyjälle siitä, että materiaali on maksullinen ja se voidaan toimittaa sähköisesti, on tähän viestiin vastattu takaisin heti 9.11.2021, kuitenkin sähköpostiosoitteesta akivimaki@safe.im. Viestissä on ilmoitettu poliisin ilmoittaman kuulostavan hyvältä, minkä lisäksi laskutustiedoiksi on annettu Kivimäen nimi sekä osoitetiedot Suomessa. Kivimäki on niin ikään käyttänyt kyseistä daniel@safe.im-sähköpostiosoitetta asioidessaan Digi-ja väestötietoviraston kanssa tehdessään sähköistä muuttoilmoitusta 25.1.2021 Abell Housen osoitteeseen (S46). Lasku muuttoilmoituksesta on puolestaan maksettu Kivimäen vaimon Dinun nimissä. Kivimäki ei ole kiistänyt edellä mainittuja tietoja. Kaikki edellä mainitut tiedot espanjalaisen IP-osoitteen osoitetiedon osalta yhdistyvät tavalla tai toisella Kivimäkeen.

Kivimäen pyynnöstä Ruhanen on kutsuttu käräjäoikeuteen uudelleen todistamaan Kivimäen asumisesta Espanjassa sekä Kivimäen yhteydestä osoitteeseen CL (Calle, Carrer) Selva de Mar 12 3–1, Barcelona. Ruhanen ei ole osannut kertoa osoitteesta ensin oma-aloitteisesti mitään. Näytettäessä Ruhaselle syyttäjän kirjallista todistetta numero S105 sekä kysyttäessä todisteesta ilmenevästä osoitteesta Carrer Selva de Mar ja siitä millä tavalla osoite on asiakirjoihin päätynyt, on Ruhanen kertonut jostain sanaharkasta ja että osoite oli mahdollisesti tämän sanaharkan tapahtumapaikka. Ruhasen mukaan riita oli mennyt fyysiseksi Rory Cornellin ja Kivimäen välillä ja kyseinen asunto oli paikka, missä ”Daniel ja porukat” asuivat. Paikalla olivat Ruhasen ja Kivimäen lisäksi Daniel, Rory ja joku muu kolmas henkilö. Ruhanen ei kertomansa ollut muistanut tätä asiaa, koska asia ei ollut ”mennyt vakavaksi”.

Ruhanen on vielä tämän jälkeen korjannut kertomustaan ja ilmoittanut, että esitetty kirjallinen todiste oli virkistänyt hänen muistiaan. Ruhasen mukaan tilanteessa oli ensin ollut sanaharkka asunnossa Roryn ja Kivimäen välillä. He olivat olleet lähdössä asunnolta eikä vartija ollut pitänyt siitä, että heidän autonsa oli ollut parkissa aukiolla. Tästä oli tullut sanaharkka, ja vartija oli lyönyt Kivimäkeä auton vieressä. Kysyttäessä Ruhaselta vielä erikseen sitä, miksi ja miten asunto oli merkitty asiassa tapahtumapaikaksi, on Ruhanen ensin kertonut, ettei muistanut miten poliisi oli tilanteessa ottanut osoitetiedot ylös ja vielä tämän jälkeen kertonut kielimuurista sekä vaikeuksista selvittää poliisien kysymyksiä. Hän ei tiennyt tai osannut kertoa sitä, miten asunnon osoite oli ilmoitukseen päätynyt. Kivimäki on pääkäsittelyssä vielä näyttänyt Ruhaselle kahta kuvaa taloista, joista Ruhanen on ensin ilmoittanut, ettei osannut sanoa näistä mitään. Puolustuksen nimenomaisen kysymyksen ja kuvien esittämisen jälkeen Ruhanen on ilmoittanut tunnistavansa talot. Hänen mukaansa kuvista toinen esitti heidän asuintaloaan Barcelonassa ja toisen kuvan esittävän edellä kuvatun väkivaltaisen tapahtuman tapahtumapaikkaa. Kyseisiä kuvia ei ole nimetty kirjallisiksi todisteiksi tai muuksi oikeudenkäyntiaineistoksi, eikä niitä ole pääkäsittelyn päätteeksi esitetyn pyynnön jälkeenkään toimitettu käräjäoikeudelle.

Selvitettäessä IP-osoitteen käyttötietoja saadaan lähtökohtaisesti tieto siitä, mistä ja kenen nimissä olevasta liittymästä yhteys otetaan. Dynaaminen IP-osoite muuttuu säännöllisesti, kun taas staattinen IP-osoite ei muutu. Käytettäessä staattista IP-osoitetta näyttää yhteys siltä kuin sitä käytettäisiin kyseisen asunnon sijainnista käsin riippumatta siitä, mikä käyttäjän sijainti todellisuudessa on ollut. VPN-palvelua käyttämällä, mistä käyttämisestä Kivimäki on itsekin kertonut, IP-osoite sekä käyttäjän virtuaalinen sijainti on helposti vaihdettavissa ja valittavissa jopa toiseen maahan ilman, että käyttäjän oikeaa sijainti selviää.

Espanjalaisen IP-osoitteen 147.161.123.116 tilaajan osoitetieto Calle Selva de Mar viittaa vuodesta 2019 aina vuoteen 2022 hyvin vahvasti Kivimäkeen huolimatta siitä, mitä liittymän tilaajatiedoista ilmenee. Ruhasen kertomus espanjalaisesta osoitteesta ja siitä, että se olisi hänen kuvailemansa väkivaltatilanteen tapahtumapaikka tai miten tämä osoite olisi poliiseille tilanteessa ilmoitettu, on ollut hyvin epämääräinen. Ruhanen on ensin vaikuttanut olevan hyvin tietämätön tapahtumista ja tapahtumapaikasta, mutta johdattelevien kysymysten sekä valokuvien näyttämisen jälkeen hän on kertonut muistavansa edellä kerrotun tapahtumien kulun sekä sen, miten osoite on poliisin tietoihin päätynyt.

Käräjäoikeus toteaa, että kaikki Daniel Fulgescu -nimiseen henkilöön viittaavat yhteystiedot yhdistyvät Kivimäkeen tai Kivimäen riidattomasti käyttämiin yhteystietoihin. Mikään asiassa esitetty ei siten osoita sitä, että kysymys olisi Kivimäen väittämin tavoin henkilöstä, joka toimisi Espanjasta käsin. Kaikki edellä kerrottu tukee vahvasti johtopäätöstä siitä, että Kivimäki on pystynyt käyttämään myös Silvana Novacovicin nimellä rekisteröityä IP-osoitetta 147.161.123.116. Se miten IP-osoitetta on käytetty, on jäänyt tarkemmin selvittämättä.

Kivimäen käyttämistä aliaksista, tunnuksista ja nimimerkeistä

Asiassa on riidatonta, että Kivimäki on käyttänyt Ranskassa 3.2.2023 kiinni jäädessään väärää henkilöllisyyttä Asan Amet. Kirjallisista todisteista ilmenee, että Kivimäen vaimon Dinun puhelimesta (S26) on jäljennetty Whatsapp-viesti, jossa 888-loppuiseen numeroon nimellä Andrew Ryan on toimitettu viesti ”Hey Andrew its Dominique we met in Dubai with Alex/ Ryan”. Edelleen vaimon puhelimen Signal-sovelluksesta on Kivimäen kiinnioton jälkeen 3.2.2023 aamulla lähetetty muun muassa kaksi englanninkielistä viestiä ”They got Ryan” ja ”They have Ryan”. Edelleen viesteistä on löydetty kuva passista Asan Amet-nimellä ja Kivimäen valokuvalla. Lisäksi viesteistä on löydetty neljä väärennettyä ajokorttia Kivimäen valokuvilla, mutta nimillä Alexandru Stan, Gheorghe-Ionut Furdui ja Valentin-Ilie Dobritoiu. Lisäksi puhelimesta on löytynyt valokuva arizonalaisesta ajokortista Kivimäen tiedoilla ja kuvalla. Kivimäki on kiistänyt nähneensä fyysisesti näitä vaimonsa puhelimesta löytyneitä väärennettyjä asiakirjoja Asan Ametia lukuun ottamatta ja kertonut sanoneensa, ettei halua sellaisia.

Kivimäki on riidattomasti käyttänyt useita eri nimimerkkejä kuten ”ryan”, jolla myös Kivimäen ystävät ja läheiset hänet tuntevat tai millä nimellä he häntä kutsuvat. Todistajana asiassa kuultu Naughtonkin on kertonut, että hän on tuntenut Kivimäen nimellä Ryan.

Kivimäki on tuomiosta edellä ilmenevin tavoin käyttänyt myös tunnusta ”r” sekä nimimerkkiä ”Spamclan”. Lisäksi useista kirjallisista todisteista (S26, S47, S48 ja S64) ilmenevä ”Alex” yhdistyy Kivimäkeen safe.im-sähköpostien

kautta. Kirjallisen todisteen S20 mukaan Kivimäki on käyttänyt jo vuosina 2011–2013 myös useita muunnoksia Ryan nimestä kuten Ryan Cleary, Ryancl, RyanCC, Ryan c, RyanH, Ryan Cleary (Jew) sekä lisäksi tunnuksia kuten ”h”, ”zeekill”, ”zee”, ”Jonathan”, ”ihateblackpeople12345”, ”lulzsecryan”, ”ryanh” ja ”Niggers1” (S27). Osaa edellä mainituista tunnuksista on käytetty myös salasanoina ja osa tunnuksista tai salasanoista on myös hyvin alatyylisiä kuten Niggers tai ihateblackpeople. Kirjallisesta todisteesta S27 ilmenee lisäksi, että Kivimäki on käyttänyt myös sellaisia harvemmin esillä olleita nimiä kuten Jim Wellman, Jonathan Sherred, Greg Gessler, Sean Wood ja Robert Walsh.

Käräjäoikeus toteaa, että Kivimäellä on jo pitkään ollut tapana sekä verkossa että sen ulkopuolella käyttää itsestään erilaisia keksittyjä nimiä tai nimimerkkejä taikka todellisten olemassa olevien henkilöiden nimiä. Edelleen Kivimäen kertomus siitä, ettei hän olisi fyysisesti nähnyt vaimonsa puhelimesta löydettyjä väärennettyjä henkilöllisyyksiä ja että hän olisi niistä kieltäytynyt, ei ole uskottava. Kaikki edellä esitetty osoittaa, että Kivimäki on yhtäältä halukas, mutta toisaalta myös kykenevä käyttämään sekä vääriä henkilöllisyyksiä että täysin keksittyjä nimiä peittääkseen oman todellisen henkilöllisyytensä.

Kivimäen käymät keskustelut ennen ja jälkeen tekoaikojen

Hacker News -keskusteluja koskevasta kirjallisesta todisteesta (S13) ilmenee vuosina 2017, 2018 ja 2020 englanniksi käytyjä keskusteluja, joihin nimimerkki ”Ryanlol” osallistuu. Kyseinen nimimerkki ja keskustelija on riidattomasti Kivimäki. Keskustelut on käyty sekä ennen nyt kysymyksessä olevien rikosten tekoaikoja että niiden jälkeen.

Marraskuussa 2017 käymässään keskustelussa ”Ryanlol” kertoo skannanneensa automaattisesti eri virustorjuntayritysten jakamaa dataa ja etsineensä sieltä arkaluonteisia asiakirjoja. Nimimerkki kertoo keskustelussa tallentavansa vain tiedostoja, joita skannerit eivät ole todenneet haittaohjelmiksi ja suodattavansa pois suuret, yleensä tylsät tiedostot sekä suodattavansa pois julkisesti saatavilla olevia asiakirjoja googlaamalla niitä. Tällä tavoin nimimerkki on kertonut keränneensä yli 20 teratavua dataa. Keskustelijan mukaan hän on löytänyt muun muassa ruotsalaisen pankin koko asiakastietokannan, tuhansia Git-säilöjä, satoja skannattuja passeja, kymmeniä gigatavuja arkaluonteisia lääketieteellisiä asiakirjoja, kymmeniä gigatavuja valtionhallinnon sisäisiä asiakirjoja, satojen tuhansien ihmisten palkkatietoja, kokonaisia sähköpostilaatikoita sekä valtionhallinnon että yritysten satoja verkkosivustotietokantoja eri muodoissa.

Edelleen nimimerkki ”Ryanlol” on keskustellut ja kommentoinut elokuussa 2018 kryptovaluuttahuijauksia. Lisäksi ”Ryanlol” on osallistunut keskusteluun 24.12.2020 sekä esittänyt mielipiteensä siitä, mikä on varastetun datan rooli ansaintatarkoituksessa. Nimimerkin ”Ryanlol” mukaan varastettua dataa on enimmäkseen hyvin vaikea myydä järkevään hintaan, "exit-huijauksen" olevan ajanhukkaa ja että rahaa saisi enemmän vaatimalla vain lunnaita vielä yhdeltä yritykseltä. Hän on myös todennut, että kun ansaitsee miljoonia kiristämällä yrityksiä, ei ole kovinkaan kiinnostunut myymään niiden dataa kymmenillä tai sadoilla tuhansilla.

Kivimäen toiminta väitettyjen tekojen tekoaikana

Palvelimilta, jotka ovat yhdistettävissä nyt kysymyksessä oleviin tekoihin, on tehty löydöksiä, jotka ovat yhdistettävissä Kivimäkeen. Osa löydöksistä on

todettu riidattomiksi, kuten muun muassa edellä tuomiossa kerrottu P1-palvelimella olleesta kopiosta löytynyt beach.jpg-niminen valokuva, joka on Kivimäen isovanhempien mökiltä (S10).

Vastaamon potilastietoja on 21.–23.10.2020 jaettu Ylilauta-nimisellä keskustelufoorumilla sekä Tor-verkossa toimineella Torilaudalla. Kirjallisista todisteista ilmenee, että OPSVM-virtuaalipalvelimella on sekä pystytetty että jaettu Onion-verkkosivusto 3wnug3445ja7qj47.onion (S19). Onion-verkkosivusto on ollut saavutettavissa vain Tor-verkossa. Ensimmäiset viestit Torilaudalla on julkaistu 21.10.2020 kello 01:xx:yy (UTC) nimimerkin ”ransom_man” toimesta (S11). Kellonajan esittäminen kyseisellä tavalla johtuu esitetyn selvityksen mukaan siitä, että aikaleimat Torilaudalla tallentuvat tunnin tarkkuudella yksityisyyden varmistamiseksi.

Ensimmäinen nimimerkiltä ransom_man tullut viesti on tullut englanniksi, jossa on muun muassa kerrottu Psykoterapiakeskus Vastaamon tietomurrosta sekä sieltä otetuista erittäin arkaluonteisista tiedoista, yrityksen johdon reagoinnista tilanteeseen sekä yritykseltä vaaditusta kiristyssummasta ja aikomuksesta ryhtyä julkaisemaan päivittäin sata potilastietoa kerralla. Viestissä on lisäksi ollut linkki Onion-sivustolle, jota on käytetty potilastietojen jakamiseen.

Viestit sadan uuden potilastiedon julkaisusta nimimerkki ransom_man on julkaissut 22.10.2020 kello 22:xx:yy (UTC). Seuraavat kaksi viestiä, joissa on julkaistu Vastaamon toimitusjohtajan kotiosoite sekä sata uutta potilastietoa, on julkaistu 23.10.2020 21:xx:yy (UTC). Seuraava julkaisu on tehty 23.10.2020 kello 22:xx:yy (UTC), ja siinä on julkaistu poliisien sähköpostiosoitteita. Seuraava viesti ”Whoopsie enjoy big tar” nimimerkiltä ransom_man on julkaistu 23.10.2020 12:xx:yy (UTC) tar-paketin pieleen menneen paketoinnin jälkeen. Nimimerkki ransom_man on aktiivinen keskustelun ylläpitäjä ja antaa keskusteluissa ymmärtää, että pyydetyn summan maksaminen kannattaa.

Edellä mainitun lisäksi kirjallisista todisteista S12 (salainen) ja S19 ilmenee, että testtest-nimimerkki on puolestaan Ylilaudalla 21.10.2020 kello 03:05:13 (UTC) julkaissut viestiketjun, joka on lisätty edellä kerrottuun Tor-verkon piilopalveluun 21.10.2020 kello 04:22:59 (UTC). Nimimerkki testtest ei ole ollut rekisteröity, eikä siitä ole saatu mitään tietoja. Raportista ilmenee edelleen, että kuvista ilmenevä vihreä OP-symboli ilmaisee kyseisen viestin olevan ketjun aloittajan (original poster) lähettämä viesti. Nimimerkki testtest on julkaissut viesteissään potilastietoja Ylilaudalla noin tunnin ajan siten, että viimeisin viesti on julkaistu 03:54:45 (UTC). Viesteihin on niiden sisällöstä päätellen valikoitu sellaisia potilastietoja tunnistustietoineen, joilla olisi mahdollisimman ”shokeeraava” vaikutus ja tällä tavoin myös osaltaan pyritty luomaan painetta kiristetyille.

Potilastietojen julkaisun yhteydessä Ylilaudalla on julkaistu muitakin tähän asiaan liittyviä viestejä, joihin riidattomasti liittyy myös Kivimäki. Asiassa on riidatonta, että Kivimäki osallistuu tähän keskusteluun omalla nimimerkillään ”Spamclan”, joka on keskusteluissa identifioitu ID-numerolla 87920921 (S38). Kivimäki on 21.10.2020 kello 04:29:27 (UTC) postannut Ylilaudalle lähetyssä viestissä ”tuolla torilaudan puolella näyttäis olevan sama lanka vielä pystyssä”. Kivimäki on tämän jälkeen postannut vielä kaksi viestiä kello 05:20:50 ja 05:23:52 viesteillä ”siis tää http://3wnug34 45ja7qj47.onion.pet/000ylilauta.html” ja ”siis http://3wnug34 45ja7qj47.onion.pet/000ylilauta.html.” Lisäksi 22.10.2020 kello 22:50:34 Kivimäki on julkaisut kirjoituksen, jossa Kivimäki on kirjoittanut ”Lympri

postas juuri listan vastaamon asiakkaina olleita poliiseja torilaudalle” (S38 s. 1726). Kivimäen käymät keskustelut ajoittuvat nimenomaan edellä mainittujen kiristysviestien väliin. Osa Kivimäen viesteistä on julkaistu sellaisesta IP-osoitteesta, josta on kirjauduttu myös P-palvelinten tilaajatietoihin liittyvälle mathewlukeperry-nimiselle sähköpostitilille (S33).

OPSVM-virtuaalikoneen komentohistoriasta on havaittavissa ajallisesti edellä kerrottuihin tapahtumiin lähellä olevaa toimintaa 21.–22.10.2020 kuten potilastietoihin tehdyt suomenkieliset haut sanojen taivutuksineen ja Onion-sivuston pystyttäminen kuten tuomiossa on jo aiemmin todettu. Poliisiin liittyviä tekstihakuja on tehty 22.10.2020 kello 12:21–12:22 sekä kello 22:48:25, ja noin kaksi minuuttia tämän jälkeen kello 22:50:34 Kivimäki on lähettänyt Ylilaudalle edellä mainitun viestin "Lymprin” poliisipostauksista torilaudalle. Keskustelu kiristyksistä on jatkunut 24.10.2020 Torilaudan puolella kiristysviestien lähettämisen jälkeen (S78). Nimimerkki ransom_man on 24.10.2020 21:xx:yy ilmoittanut ”this is us” sekä kysyttäessä vastannut englanniksi myöntävästi olevansa myös yksityishenkilöiden kiristyksen takana. Viesteissä pidetään yllä ajatusta siitä, että vaadittujen summien maksaminen kannattaa, maksuja sekä maksujen suorittajia seurataan, ja etteivät maksujen takarajat ole niin tiukkoja.

Kivimäki on syytteen kiistäessään vedonnut myös Onion-linkin julkaisua koskevaan kopiointiin ja siihen, ettei hän ole viesteissään tiennyt kiristäjän pyytämää rahasummaa ja että hän oli toistuvasti erehtynyt sekä kiristyssummasta että potilasmäärästä (V22, viestit nro 136131435 ja 135985090). Kyseisissä viesteissä nimimerkki Spamclan oli todennut, että ”jos noi kaikki 450k potilasta järjestäisi kolehdin niin ei se olisi kuin euro per pää” ja edelleen, että ”Lokakuun Kiristys langa on poistunut. Part 5”. Lisäksi Spamclan vastaa johonkin aikaisempaan viestiin, joissa Spamclan Kivimäen mukaan muun muassa varoittaa postaamasta linkkejä tai dataa tietomurrosta lankaan sekä kunnioittamaan potilaita. Vielä viestissä viitataan useassa kohdin ”Lympriin” ja tämän mahdolliseen pidätykseen sekä tietojen olemiseen kovan tietoturva-muurin takana. Lopuksi viestissä todetaan ”En liity tapaukseen. Tein vain keskustelulangan.”

Kivimäki on edellä olevan perusteella katsonut, ettei hän voi olla kiristäjä. Tekstit osoittavat Kivimäen mukaan hänellä asiasta olleita puutteellisia tietoja ja muutenkin tietämättömyyttä asiasta.

Useat Kivimäen edellä mainituista nimimerkillä Spamclan Ylilaudalla tekemistä ”postauksista” kuten muun muassa viestit 8.10.2020 ja 10.10.2020 on tehty Mullvadin osoiteavaruuteen kuuluvasta IP-osoitteesta 2a03:1b20:4:f011::a14d (S38 s. 1735). Samasta IP-osoitteesta on kirjallisesta todisteesta S42 ilmenevällä tavalla oltu 7.10.2020 kello 23:21:06 ja 23:21:08 (UTC+3) yhteydessä bittiraha.fi-sivustoon, ja heti tämän jälkeen 7.10.2020 kello 23:44 kiristäjä on neuvonut käyttämään nimenomaan bittiraha.fi-palvelua bitcoinien hankintaan (S50). Yksi Kivimäen aikaisemmistakin viesteistä Ylilaudalla (29.4.2020) on tullut samasta IP-osoitteesta 2a03:1b20:4:f011::a14d (S38 s. 1762).

Kivimäki on tehnyt myös 12.6.2020 nimimerkillä Spamclan postauksia Ylilaudalla Hyperopticin IP-osoitteesta 37.156.72.25 (S38 s. 1754), joka on yhdistettävissä Kivimäkeen. Lisäksi 10.11.2021 tehty ”postaus” on tullut IP-osoitteesta 185.120.144.105 (S38 s. 2020), josta Kivimäen yksilöivillä tiedoilla on julkisen hallinnon turvallisuusverkkotoiminnan Tuve-lokitietojen mukaan avattu suojattu sähköpostiviesti liittyen Kivimäen yhteydenottoon keskusrikospoliisiin (S46).

Muut asiassa esille nostetut henkilöt

Kivimäki on syyllisyytensä kiistäessään viitannut siihen, ettei asiassa esille tulleiden useiden eri henkilöiden mahdollista osallisuutta tekoihin ole lainkaan selvitetty tai että henkilöiden rooli asiassa on jäänyt vähintäänkin epäselväksi. Asiakokonaisuudessa on noussut esille useita henkilöitä kuten edellä mainitut Leena Patel, Mathew Luke Perry, Deng Haitao, Robert Cornel, Rory Cornel, Adrian Ioan Badescu, Daniel Fulgescu ja Silvana Novacovici, ja käräjäoikeuskäsittelyn aikana myös Daniel Newhard -niminen henkilö. Kivimäki on tuonut esiin myös erilaisia nimimerkkejä kuten ”Antipeace”, ”Kuroi”, ”Truedread” ja ”Darkoverlord” sekä 26.249-loppuisen IP-osoitteen ja kyseisen liittymän käyttäjän mahdollisen osallisuuden tekoon. Fulgescua ja Novacovia on käsitelty jo edellä tuomiossa.

Syyttäjät ovat katsoneet, että kysymys on henkilöiden osalta joko peitenimistä, aliaksista tai bulvaaneista sekä nimimerkkien osalta vaille konkretiaa jääneistä Kivimäen väitteistä. Käräjäoikeus toteaa edellä esitetystä seuraavan.

Leena Patel on P-palvelinsarjan tilaajatiedoista tuomiosta edellä ilmenevästi esiin tullut nimi (S30). Palvelinten tilaajatiedoista ilmenee Patelille osoite Yhdysvaltoihin, puhelinnumero sekä sähköpostiosoitteena edellä tuomiosta ilmenevä mathewlukeberry@gmail.com.

Europolin Siena-kyselyjen tuloksista (S105) ilmenee vuonna 1981 syntynyt ja Yhdistyneessä kuningaskunnassa asunut Leena Patel -niminen henkilö, joka on 20.4.2008 ilmoittanut joutuneensa varkauden uhriksi Barcelonassa.

Hetznerin asiakastilille on kirjauduttu kirjallisen todisteen mukaan 12.6.2020, 7. ja 17.9.2020 sekä viimeisimmäksi 6.10.2020 (S30). Tilin laskutus on tapahtunut kuukausittain, ja ensimmäinen lasku on muodostunut 4.1.2019.

Patelin edellä esitetyillä tiedoilla on tehty viranomaistiedusteluja, mutta muuta yhteyttä kuin edellä kerrottu nimitieto P-palvelinten tilaajatiedoissa hänen liittymisestään nimenomaisesti nyt kysymyksessä oleviin tapahtumiin ei ole löytynyt.

Edellä tuomiossa kerrotuin tavoin Leena Patelin tilaajatiedoilla tilattuja palvelimia on maksettu Deng Haitao -nimisen henkilön nimiin rekisteröidyllä PayPal-tilillä. Kivimäki on molempien henkilöiden osalta kertonut, ettei tunne tällaisia henkilöitä. Kivimäki on kertonut ainoastaan Coinstantiin liittyneestä kiinalaisesta henkilöstä, jonka nimeä hän ei ole muistanut ja jonka henkilöllisyyttä hän ei kertomansa mukaan ole myöskään selvittänyt. Kysymyksessä ei kuitenkaan ole ollut Deng. Kivimäki on vielä osaltaan viitannut IP-osoitteisiin, joista asiakashallintapaneeliin on 12.6.2020 ja 17.9.2020 kirjauduttu, sekä siihen, että 133X-loppuiset IP-osoitteet kuuluvat Chinamobilelle (V26). Käräjäoikeus toteaa, että edellä kerrotut kirjautumiset kiinalaisesta IP-osoitteesta ovat tekoaikojen ulkopuolella.

Kivimäki on tehnyt Hetznerille tiedustelun siitä, miten yhtiö tunnistaa asiakkaansa. Vastauksena Hetzner on ilmoittanut Kivimäelle, että heillä on tiettyihin riskeihin perustuvat tunnistusmenettelyt (V27). Käräjäoikeus toteaa, että viestissä on kerrottu asiakkaan tunnistamisesta ja tunnistamisen eri tasoista yleisellä tasolla avaamatta tätä kuitenkaan viestissä tarkemmin. Lisäksi tunnistaminen on vastauksen mukaan yhteydessä riskitekijöihin, joita ei myöskään viestissä avata. Vastauksesta ei voi siten tehdä sellaista

johtopäätöstä, että maksuja P-palvelimista suorittaneet Deng Haitao taikka Patel-nimiset henkilöt olisi tunnistettu jollakin luotettavalla tavalla ja siten, että heidän henkilöllisyydestään olisi todella kyetty varmistautumaan.

Edellä kerrottu huomioon ottaen käräjäoikeus pitää varsin todennäköisenä, että sekä Leena Patel että Deng Haitao ovat keksittyjä henkilöitä P-sarjan palvelimet todellisuudessa vuokranneen henkilön tai henkilöiden henkilötietojen salaamiseksi. Tätä johtopäätöstä tukee asiassa ilmennyt runsas VPN-yhteyksien, salattujen ja ilmaissähköpostiosoitteiden sekä anastettujen luottokorttitietojen käyttäminen.

Adrian Ioan Badescu -nimisen henkilön tilaaman internetliittymän IP-osoitteesta on 12.11.2020 kirjauduttu P-palvelimen yhteyssähköpostiosoitteeseen mathewlukeperry@gmail.com (V21 ja V21.1). Badesculle on ilmoitettu osoitetiedot Isoon-Britanniaan. Mainittuun sähköpostiosoitteeseen on kirjauduttu myös Mullvadin IP-osoitteista, joista puolestaan Kivimäki on postannut nimimerkillään Spamclan kirjoituksia Ylilaudalle (S32 ja S33). Kivimäki on osaltaan tältä osin vedonnut siihen, ettei hän tunne Badescu-nimistä henkilöä. Hän on lisäksi vedonnut siihen, että Badescuun liittyvä katuosoite on todellinen ja että on myös loogista, että henkilö hallinnoi palvelimia. Myös Badescu-nimistä henkilöä on kyseisillä tiedoilla tutkinnassa pyritty tavoittamaan, mutta tuloksetta. Edellä kerrotuilla tiedoilla Badescun liittyminen tapahtumiin on jäänyt kokonaisuudessa merkityksettömäksi.

Robert ja Rory Cornellin (Cornel) nimet sekä nimiin osaltaan yhdistyvä osoite, Mason Drive 3, on tullut esille muutamissa eri yhteyksissä, kuten Kivimäen hotelli Kämpin joulukuussa 2019 tehdyn hotellivarauksen (S36), Worldstream-nimisen palvelimen (S35) sekä Applelle tehdyn tietopyynnön (S37) yhteydessä. Lisäksi Robert Cornellin nimi on tullut esille Lundbergin IMAP-lokin yhteydessä.

Edellä kerrotun Kivimäen tekemän hotellivarauksen osoitteeksi on ilmoitettu Mason Drive 3 sekä jälleen safe.im-loppuinen sähköpostiosoite etuliitteellä paypal. Katuosoite on ilmennyt myös edellä mainitun Worldstream-palvelimen tiedoista, jonka yksi käyttäjistä ja maksajista on huhti-marraskuussa vuonna 2018 ollut yhtiö nimeltä Aegis Capital LLC/Kivimäki. Maksajan sähköpostiosoitteena on ollut paypal@safe.im. Kivimäki on ilmoittanut riidattomaksi sen, että hän on ollut kyseisen yhtiön osakas ja maksanut mainitusta palvelimesta maksuja. Osoite ilmenee niin ikään vastauksena Applelle tehtyyn tietopyyntöön, jossa Kivimäen osoitetiedoksi vuonna 2017 on merkitty sama katuosoite.

Rory Cornellin nimi ilmenee puolestaan Kivimäen Paypal-tilin asiakastietojen osoitetiedoissa osoitteella 9c Medway rd pmb 269 sekä päivämäärällä 19.12.2019 (S31). Syyttäjät ovat asiakastietojen osoitteiden osalta ilmoittaneet, että palvelu generoi itse osoitteet, mutta mitään tietoa siitä, miten se tapahtuu, ei ole esitetty. Kivimäki ei ole myöskään omassa kuulemisessaan tai kirjallisia todisteita kommentoidessaan kertonut mitään tarkempaa kyseisistä henkilöistä, vaan vain vedonnut siihen, että henkilöt ovat todellisia.

Rory Cornell -nimisestä henkilöstä ovat kertoneet myös todistaja Ruhanen sekä todistaja Naughton. Ruhasen mukaan Rory Cornell oli jotain Kivimäen kaveripiiriä, mutta hän ei osannut kertoa tästä tarkemmin. Ruhasen mukaan Rory Cornell oli villi poliitikko tai poliittisesti suuntautunut henkilö, jolla oli vahvat mielipiteet ja että tämä ”häsläsi ja sellaista”. Cornell asui Barcelonassa ja todistaja tapasi hänet useita kertoja. Todistaja Nauhgton on puolestaan

kertonut, ettei tuntenut Robert Cornell -nimistä henkilöä, mutta Rory-nimisen henkilön hän tiesi. Rory oli Kivimäen ystävä. Kivimäki oli kerran pyytänyt häntä suosittelemaan ”Rorya” General Electricsille, minkä vuoksi hän oli puhunut henkilön kanssa netissä sekä lisäksi tavannut henkilön henkilökohtaisesti myöhemmin Barcelonassa.

Syyttäjien oikeudenkäynnissä esittämän selvityksen mukaan edellä mainittu Kivimäen eri yhteyksissä käyttämä osoite Mason Drive 3 yhdistyy sinällään todelliseen henkilöön Robert F. Cornell, jolla on puolestaan poika nimeltä Robert James ”Rory” Connell. Julkisista internetlähteistä löytyvistä aineistoista ilmenee vuonna 2023 kuolleen Robert Cornellin muistokirjoitus (SO9), Google-haulla tehty haku henkilön nimellä ja osoitteella (SO11) sekä Google Street Viewsin näkymä kyseiseen osoitteeseen (SO10), josta ilmenee osoitteen ja Cornell-sukunimen välinen yhteys.

Edellä kerrottu huomioon ottaen osoite Mason Drive 3 viittaa kaikissa yhteyksissä Kivimäkeen. Käräjäoikeudella ei ole mitään syytä epäillä, etteivätkö kyseiset henkilöt olisi todellisia, mutta mikään asiassa esitetty ei viittaa siihen, että näillä henkilöillä olisi jotain liityntää nyt käsiteltävänä olevaan asiaan. Käräjäoikeus katsoo, että Robert Cornellina esiintynyt henkilö on todennäköisesti ollut Kivimäki. Tätä johtopäätöstä tukee se, että Kivimäelle ja Cornellille on ilmoitettu sama puhelinnumero, samoin kuin se, että Cornellin kirjoittamissa viesteissä on käytetty englannin kieltä tavalla, joka viittaa vahvasti siihen, että viestit on kirjoittanut joku muu kuin englantia äidinkielenään käyttävä henkilö. Lisäksi Lundbergin ajopäiväkirjan merkintä tapaamisesta Kivimäen kanssa sekä tapaamisen kanssa ajallisesti yhteensopiva tilisiirto Kivimäen lähipiiriin kuuluvalle henkilölle tukee tätä johtopäätöstä.

Alex Vanderpot on puolestaan tuomiosta edeltä ilmenevästi Kivimäen yhtiökumppani Scanifi:ssä. Vanderpot on K-palvelinten tilaaja ja osin myös niiden maksaja. Kivimäki on Vanderpotin osalta viitannut tiettyihin IP-numeroihin, domain-nimiin sekä palveluntarjoajiin, ja osaltaan vihjannut, että Vanderpot olisi tekijä taikka jollain tavoin osallinen tekoon. Kivimäki on väittänyt, että Vanderpot on avannut K17-palvelimella olleen P2-palvelimen varmuuskopion salauksen, käsitellyt sitä ja kopioinut sieltä proxyshop-virtuaalipalvelimen (V32–V36).

Vastaajan nimeämästä kirjallisesta todisteesta (V35) ilmenee, että proxyshop -virtuaalipalvelimen komentohistoriasta löytyy viittauksia IP-osoitteisiin 100.40.127.45 ja 24.22.128.241 sekä viittauksia gitlab.vanderpot.com-sivustoon. Ensin mainittu IP-osoite kuuluu kirjallisen todisteen V33 mukaan Verizon Business palveluntarjoajalle Rhode Islandin osavaltiossa. Myöhemmin elokuussa 2019 mainittu IP-osoite on Kivimäen mukaan korvattu WireGuard-konfiguraatiotiedostoissa viimeksi mainitulla IP-osoitteella, joka puolestaan kuuluu Seattlessa sijaitsevalle palveluntarjoajalle. Kivimäki on tältä osin viitannut vielä siihen, että Vanderpot on elokuussa 2019 muuttanut Providencesta Seattleen (V37). Kivimäki on sen vuoksi katsonut, että proxyshop-virtuaalipalvelin kuuluu Vanderpotille.

Syyttäjät ovat tältä osin ilmoittaneet, että Vanderpotia on alun perin epäilty rikoksesta, mutta tutkinnan kuluessa hänestä on tehty syyttämättäjättämispäätös. Vanderpot on Yhdysvalloissa kieltäytynyt tulemasta asiassa kuulluksi, eikä häntä ole tässä oikeudenkäynnissä myöskään kuultu. Asiassa esitetty ja edellä kerrottu näyttö huomioon ottaen proxyshop-virtuaalipalvelin ei ole noussut miltään osin merkitykselliseksi kokonaisuuteen nähden huomioon ottaen sekin, että

OPSVM-virtuaalipalvelimen komentohistoria ulottuu paljon pidemmälle varmuuskopion tekemiseen nähden. Asiassa esitetty näyttö myös osoittaa, että varmuuskopion tekijällä on pitänyt olla näkyvyys kopioinnin aikana molempiin P2- ja K17-palvelimiin.

Daniel Newhard -niminen henkilö on tullut pääkäsittelyn kuluessa esiin kryptovaluuttaan ja keskusrikospoliisin suorittaman valeostoon liittyvän jäljitystyön yhteydessä. Keskusrikospoliisin maksama 0,1 bitcoinia on selvityksen mukaan jakautunut Kivimäelle Revolut-tilin ja Newhardille Wirex-tilin kautta (S81) tuomiosta jäljempänä ilmenevin tavoin. Newhard on Virossa asuva Yhdysvaltain kansalainen. Hänet oli Virossa otettu kiinni, mutta hän oli kieltäytynyt kuulemisestaan. Newhardin hallussa olleita laitteistoja on myös takavarikoitu, ja asiassa on kirjattu uusi rikosilmoitus. Syyttäjät ovat tältä osin todenneet olevan on mahdollista, että Newhardilla on epäillysti käyttäjätili K16-palvelimen GitLab-instanssissa käyttäjätunnuksella me@danielnewhard.com (S21 s.1137). Kivimäen mukaan Newhard yhdistyy puolestaan SSH-avaimeen ml0, joka oli ollut yhteydessä OPSVM:lle ainakin 7.10.2020, sekä silasdev-virtuaalikoneen developer-käyttäjään.

Kivimäki on Newhardin osalta vielä kertonut, että tällä oli kirjallisista todisteista ilmenevästi pääsy palvelimelle ja että hänen nimensä löytyy GitLab-palvelimelta. Kivimäki oli kertomansa mukaan tavannut Newhardin kerran Hong Kongissa ja oli pitänyt tähän toisinaan yhteyttä. He myös liikkuvat samoissa keskusteluryhmissä. Yhteyttä pidettiin Signalilla. Heillä ei kuitenkaan ollut mitään taloudellista yhteyttä keskenään.

Myös todistaja Naughtonin on kertonut, että hän tiesi Newhardin ja oli tavannut hänet kahdesti. He eivät olleet kuitenkaan pitäneet toisiinsa mitään yhteyttä noin kahdeksaan vuoteen.

Kivimäen mukaan kirjallisesta todisteesta V29 ilmenee, että käyttäjätunnus developer on tallettanut potilastiedot silasdev-palvelimelle samaan aikaan kuin ne oli talletettu OPSVM-virtuaalipalvelimelle. Mainittuun developer-tunnukseen liittyy lisäksi virolainen IP-osoite 84.50.67.40. Hänen mukaansa developer on myös ollut 23.10.2020 kello 13:28–13.30 kirjautuneena silasdev-palvelimelle. Mainittu virolainen IP-osoite yhdistyy hänen mukaansa myös ml0-avaimeen OPSVM-virtuaalipalvelimella 11.10.2020 kello 13.45.

OPSVM-palvelimen kirjautumislokin (S19) mukaan ml0-avain on kirjautunut palvelimelle 11.10.2022 kello 13:45. Tämän jälkeen ml0-avaimella ei ole enää kirjauduttu palvelimelle. Kirjallisesta todisteesta (V29) puolestaan ilmenee, että tämä yhteydenotto on tapahtunut edellä mainitusta virolaisesta IP-osoitteesta. Edellä esitetyin tavoin ml0-avaimella on asennettu mysql-server-ohjelmisto OPSVM-palvelimelle sekä luotu kiristäjän myöhemmin käyttämät tekstitiedostot potilastietokannasta. Käräjäoikeus kuitenkin katsoo, että ml0-avaimen käyttäjän toimenpiteet kyseisenä ajankohtana ovat olleet hyvin rajattuja. Kaikki keskeiset toimenpiteet tänä aikana on tehty WI8-avaimella. Muutoinkin ml0-avaimella tehdyt toimenpiteet vaikuttavat lähinnä sellaisilta, joihin kiristysten tekijä on tarvinnut ulkopuolista apua.

Silasdev-palvelimelle on kirjauduttu 23.10.2020 kello 13:28:35 (UTC) 86ft-avaimella. Kirjautuja on tämän jälkeen tehnyt tiedonsiirron, jonka suunta ja sisältö on jäänyt tuntemattomaksi. Kirjautuminen on kestänyt vain hieman yli minuutin. Tämä on tapahtunut samaan aikaan kuin WI8-avaimen käyttäjä on suorittanut P2-palvelimella olleiden virtuaalipalvelimien alasajon.

Silasdev-palvelin on tuomiosta jäljempänä ilmenevin tavoin osaltaan liittynyt Tor-verkon kauppapaikoille tarkoitetun huijauksen rakentamiseen. Edellä kerrottu ja muu asiassa esitetty huomioon ottaen 86ft-avaimen käyttäjän toiminnasta ei ole tehtävissä sellaista johtopäätöstä, joka liittäisi kyseisen avaimen Vastaamoon kohdistuneeseen tietomurtoon tai kiristykseen.

Kivimäki on häntä kuultaessa tuonut esiin myös nimimerkkejä kuten ”Antipeace”, ”Kuroi”, ”Truedread” ja ”Darkoverlord”. Lisäksi Kivimäki on viitannut 26.249-loppuisen IP-osoitteen käyttäjän mahdolliseen osallisuuteen asiassa.

”Antipeace” on ollut Kivimäen mukaan hakkeripiireissä tunnettu nimimerkki ja pyörinyt siellä vuosikymmenten ajan. Nimimerkki on tarjonnut keskustelukanavilla pääsyä P2-palvelimelle ja jakanut SSH-avaimia. ”Antipeace” on Kivimäen käsityksen mukaan ollut P2-palvelimen ylläpitäjä.

”Truedread” on Kivimäen mukaan puolestaan WI8-avaimen käyttäjä, mitä tuki hänen mukaansa se, että OPSVM-palvelimen komentohistoriasta ilmeni komento ”ssh truedred.top” (V19). Lisäksi nimimerkki on ilmennyt komentohistoriassa, kun espanjalasesta IP-osoiteesta kirjautumalla on julkaistu potilastietoja (V31).

”Kuroi”-nimimerkki taas on keskusteluryhmissä pyörinyt henkilö, joka on esiintynyt Kivimäen mukaan myös nimimerkillä ”ryan”. ”Kuroi” on tunnettu kryptovaluuttoihin liittyvistä tietomurroista ja kiristyksistä.

”Darkoverlord” on puolestaan ”Kuroin” kaveri, ja yhdistynyt useisiin terveydenhuollon palveluja tarjoavien yritysten kiristämisiin. Kivimäen mukaan he olivat pitkään pyörineet ja vaikuttaneet nimimerkkien kanssa samoissa ”keskustelupiireissä”. Myös netistä löytyi laajasti tietoa näistä nimimerkeistä. Kivimäen mukaan nimimerkki oli myös kehuskellut kiristyksillä. Kivimäen mukaan ”Darkoverlord” ja ”Kuroi” olivat kyselleet Kivimäeltä joistain suomenkielisistä lauseista kiristyksen aikoihin, mutta ”niissä ei ollut järkeä”. Kivimäen mukaan Vanderpot saattaisi tietää nämä henkilöt.

Käräjäoikeus toteaa, ettei edellä olevista nimimerkeistä ole esitetty asiassa muuta selvitystä kuin Kivimäen oma kertomus sekä OPSVM-virtuaalipalvelimen komentohistoriassa oleva yksittäinen komento. Kivimäen kertomus näistä nimimerkeistä on ollut myös hyvin epämääräinen. Käräjäoikeus ei pidä Kivimäen kertomusta tai epäilyä nimimerkkien liittymisestä asiaan uskottavana.

Kivimäen esiin nostama 26.249-loppuinen IP-osoite on riidattomasti ilmennyt Ylilaudalla (S38) yöllä 21.10.2020 potilastietojen julkaisujen yhteydessä olevissa viesteissä. Kivimäki on kertonut, ettei hän ole edes pyynnöstä saanut mitään tietoa tästä IP-osoitteesta. Tältä osin syyttäjät ovat ilmoittaneet, että IP-osoite on tutkinnassa kuitenkin selvitetty. Sen haltija on Karjaalla asuva henkilö. Karjaan IP-osoitteen osalta kysymys on syyttäjien esittämän suullisen selvityksen mukaan ollut ilmaisesta Hola-nimisestä VPN -palvelusta, jonka käyttäminen on edellyttänyt käyttäjän oman IP-osoitteen luovuttamista palveluntarjoajan käyttöön. Tällöin kuka tahansa on pystynyt käyttämään tällä tavoin palveluntarjoajan käyttöön luovutettua IP-osoitetta ulostulo-osoitteena. Edellä kerrotun vuoksi tutkinta kyseisen henkilön osalta on syyttäjien mukaan lopetettu, koska häntä ei ole ollut syytä epäillä rikoksesta.

Kiristysviestit

Vastaamon toimitusjohtajalle sekä kahdelle Vastaamon it-asiantuntijalle on 28.9.2020 lähetetty kiritysviesti sähköpostiosoitteesta vastaamo@tutanota.com (S50). Viestin liitteenä on ollut esimerkkejä potilastiedoista, jotka on otettu suoraan tietokannasta. Viesti on aloitettu ensin suomeksi ilman skandinaavisia kirjaimia, minkä jälkeen viestin kieli on vaihtunut englanniksi. Kirjallisesta todisteesta (S50) ilmenee, että kiristäjä on 29.9.2020 lähettänyt toisen sähköpostiviestin edellä mainituille vastaanottajille. Viestissä on ollut lisää esimerkkejä potilastietokannan kirjauksista, jotka ovat kuitenkin eri muodossa kuin ensimmäisessä viestissä. Kiristäjän viestiin on tämän jälkeen Vastaamon toimitusjohtajan toimesta vastattu 30.9.2020. Kiristäjä on vastannut viestiin samana päivänä ilmoittaen vaativansa 40 bitcoinia osoitteeseen ”bc1qsznq4ts0zq29rcmyd67g78hkeukvpl43e55sjv”. Englanninkielisessä viestissä kiristäjä on myös ilmoittanut ladanneensa tietokannan useita kuukausia aikaisemmin IP-osoitteesta 95.175.109.219 sen ollessa avoinna internetissä. Kyseinen IP-osoite on ollut tuomiosta edeltä ilmenevästi Vastaamon potilastietokannan IP-osoite.

Kiristäjän lähettämään viestiin on vastattu 7.10.2020 kello 15:23 (UTC) sähköpostiosoitteesta WilliamFIN@protonmail.com. Kysymys on tällöin ollut kuitenkin poliisin lähettämästä viestistä. Viestissä ”WilliamFIN” on ilmoittanut harkitsevansa lunnaiden maksua ja haluavansa tietää, mitä tietoja kiristäjällä on. Kiristäjä on vastannut viestiin kello 18.51 (s. 2072) ja lähettänyt tietokannan taulujen nimet ja viimeiset potilaskirjaukset. Edelleen 7.10.2020 kello 17.22 WilliamFIN on ilmoittanut haluavansa maksaa ja varmistaa, miten hän voisi maksun hoitaa, koska hän ei ymmärrä bitcoineista paljoakaan. Lisäksi hän on ilmoittanut mahdollisista ongelmista pankin rikostentorjunnan kanssa kiristyssumman suuruudesta johtuen. Viestiin on vastattu ja neuvottu bitconien hankkimisessa ja mainittu eräänä palveluntarjoajana Suomessa toimiva Bittiraha.fi (S50). Kuten edellä tuomiosta ilmenee, IP-osoitteesta 2a03:1b20:4:f011::a14d on oltu yhteydessä Bittirahasivustoon 7.10.2020. Kyseinen käynti sivustolla on ollut läheisessä ajallisessa yhteydessä kiristysviestiin. Lisäksi Spamclan on edellä tuomiosta ilmenevästi käyttänyt samaa IP-osoitetta useita kertoja 30.6. ja 22.10.2020 välisenä aikana (S42 ja S38) Ylilaudalla käymissään keskusteluissa.

Kirjallisesta todisteesta numero S50 ilmenee, että WilliamFIN on käynyt 13.–14.10.2020 kiristäjän kanssa keskustelua muun muassa maksusta ja ilmoittanut edelleen uudella WilliamFIN2-nimellä aikaisemmin käyttämänsä sähköpostitilin sulkemisesta. Kiristäjä on vastannut viestiin ja epäillyt että ”ransom”-sanan käyttö olisi saattanut aiheuttaa tilin sulkemisen ja ilmoittanut uuden bitcoin-osoitteen ”bc1q70fguxj4rkjrtxfrlka309p3qq0aujh9p46xj3”. Samalla kiristäjä on ilmoittanut aikaisemmin mahdollisesti toimitettujen maksuosoitteiden jäävän voimaan (remain valid). Edelleen kiristäjä on 14.10.2020 ilmoittanut WilliamFIN2:lle vastaanottaneensa 0,1 bitcoinia ja tiedustellut, oliko tämä maksu testi.

Tämän jälkeen keskustelua on vielä jatkettu, ja kiristäjä on 21.10.2020 kello 04:52 lähettänyt Vastaamon toimitusjohtajalle, hallituksen jäsenelle ja WilliamFIN2:lle viestin, jossa on ilmoitettu ensimmäisten potilastietojen julkaisusta ja uhattu julkaista sata potilastietoa 24 tunnin kuluttua. Kiristäjä on 21.10.2020 kello 06:07 ilmoittanut sähköpostiosoitteensa vaihtumisesta osoitteeksi vastaamo@protonmail.com ja viitannut Onion-sivustoon (readme.txt). Vielä kyseisestä osoitteesta on 22.10.2020 kello 03.34 lähetetty Vastaamon toimitusjohtajalle, WillianFIN2:lle ja yhdelle Vastaamon hallituksen jäsenelle viesti, jossa on ilmoitettu sadan uuden potilastiedon

julkaisusta. Viestissä on lisäksi tiedusteltu muun muassa, miksi yritys ei ole halukas neuvottelemaan, ja ilmoitettu, ettei kiristäjiä kyetä tunnistamaan sekä ehdotettu maksusuunnitelman neuvottelemista ja 20.000 euron kuukausittaisen maksun suorittamista. Käräjäoikeus toteaa, että viestit on kirjoitettu kieliopillisesti huonolla englannin kielellä muun muassa siten, että sanajärjestykset viesteissä ovat väärin.

Kirjallisesta todisteesta S50 ilmenee, että Vastaamon asiakkaina olleet henkilöt ovat puolestaan saaneet 24.10.2020 henkilökohtaisen kiristysviestin sähköpostiosoitteesta no-reply@smileup.site. Näissä viesteissä asiakkailta on vaadittu 200 euron arvosta bitcoineja 24 tunnin kuluessa vastineeksi siitä, että potilastiedot poistetaan kiristäjän palvelimelta. Toisena vaihtoehtona kiristysviestissä on ollut maksaa bitcoineja 500 euron arvosta 48 tunnin kuluessa. Kirjallisesta todisteesta S69 ilmenee asianomistajien riidattomasti tekemät maksusuoritukset saamiinsa henkilökohtaisiin bitcoin-osoitteisiin. Näitä maksusuorituksia on ollut yhteensä 20.

Amazonilta saadusta sähköpostipalvelimen niin sanotusta SES-lokista käyvät ilmi asiakkaille lähetettyjen kiristysviestien lähetystiedot (S23). Tämän SES-lokin mukaan osoitteesta no-reply@smileup.site on lähetetty onnistuneesti kiristyssähköposteja 27.966 yksilölliseen sähköpostiosoitteeseen. Viestit on lokin mukaan lähetetty 24.10.2020 kello 16:04:20 ja 21:29:21 (UTC) välisenä aikana. Kaikki nämä osoitteet löytyvät OPSVM-palvelimella olevasta fi_vastaamo.sql-tietokantadumpista pois lukien sähköpostiosoite vastaamo@cock.li (S77).

Tietoteknisestä raportista (S77) ilmenee, että kaikista edellä kerrotuista sähköpostiosoitteista viisi on sellaisia, joihin on onnistuttu lähettämään viesti, ja kaksi osoitetta puolestaan sellaisia, joihin ei ole onnistuttu lähettämään viestiä. Nämä seitsemän sähköpostiosoitetta ovat löytyneet tietokantadumpista ja SES-lokista, mutta eivät OPSVM-palvelimen /root/therapissed/patients/-kansion tekstitiedostoista. Näitä sähköpostiosoitteita vastaavia tekstitiedostoja ei raportin mukaan ole olemassa johtuen siitä, että osalla asiakkaista on ollut nimikaima tietokannassa (S77).

Käräjäoikeus toteaa edellä kerrotun tukevan johtopäätöstä siitä, että kiristäjällä on täytynyt olla käytössään itse tietokantadumppi, joka on sisältänyt kaikki Vastaamon potilaat. Tekstitiedostot ovat olleet tältä osin vaillinaiset.

Virtuaalivaluuttoja koskeva selvitys

Asiassa on virtuaalivaluuttoja koskevan selvityksen osalta kuultu asiantuntijana Keskusrikospoliisin raportin laatinutta Mäntymaata. Mäntymaan laatimasta raportista ilmenee kryptovaluuttoihin liittyvät palvelinyhteydet, minkä lisäksi raportissa on käsitelty tarkemmin bitcoinin ja moneron lohkoketjuja ja vaihto-osoitteita sekä lisäksi monero-analyysin perusperiaatteita. Monero-analyysin osalta Mäntymaa on todennut, ettei sillä koskaan päästä absoluuttiseen varmuuteen vaan todennäköisimpään vaihtoehtoon siirron vastaanottajasta.

Esillä olevan asian tutkinnassa on ilmennyt, että P2-palvelimella olleella silasdev-virtuaalikoneella on rakennettu huijausta Tor-verkon kauppapaikalle. Tätä on raportista (S82) ilmenevästi testattu silasprod-virtuaalikoneella, joka on niin ikään sijainnut P2-palvelimella ja josta ohjelma on siirretty P3-palvelimelle käyttöön (S82). Tietoteknisestä raportista ilmenee edelleen, että edellä mainitulle ohjelmalle on annettu valmiit bitcoin-osoitteet, jotka muodostavat kaksi osoiterypästä, joita on esitutkinnassa ryhdytty selvittämään.

Bitcoin-osoitteet on analysoitu, ja näitä siirtoja on raportissa selvitetty. Selvitys on valmistunut pääkäsittelyn kuluessa. Kysymys on edellä mainitun huijauksen osalta ollut osin keskeneräisestä rikostutkinnasta, eikä asiaa ole käsitelty enemmälti.

Edellä kerrotut valmiit bitcoin-osoitteet ovat muodostaneet ryppäitä, joista ensimmäinen rypäs on muodostanut 62 osoitteen osoiteryppään, joka on nimetty osoiterypäs Y:ksi (S83). Toinen osoiterypäs on puolestaan muodostanut 18 osoitteen osoiteryppään, joka on nimetty osoiterypäs X:ksi (S84). Molempien osoiteryppäiden kaikkia osoitteita on hallinnoitu samalla yksityisellä avaimella, mikä raportin mukaan tarkoittaa sitä, että molempien osoiteryppäiden kaikki osoitteet ovat kuuluneet saman entiteetin hallintaan.

Raportin mukaan molempien edellä mainittujen osoiteryppäiden niin sanottu transaktiosormenjälki on epätyypillinen (V2, LT). Epätyypillisen transaktiosormenjäljestä tekee käytetty ”locktime”, joka on joissain lompakkosovelluksissa oleva valinnainen lisäasetus ja jonka avulla voidaan määritellä lohko, jossa aikaisintaan lähetetty transaktio voidaan lohkoketjussa varmentaa. Joissain lompakoissa, kuten Bitcoin Coressa, ”locktime” on vakioasetuksena ja asettuu automaattisesti sillä hetkellä lähinnä valmistumista olevaan lohkoon. Tältä osin kysymys on Mäntymaan kertomalla tavalla transaktion valmistumisen viivästyttämisestä tiettyyn lohkoon. Lisäksi osoiterypäs Y on käyttänyt sormenjälkeä ”SegWit” (Segregated Witness), joka on tyypillinen sormenjälki P2SH-osoitteessa (S81).

Asiantuntija Brade on puolestaan lausunnossaan (V28) kyseenalaistanut Mäntymaan päätelmän transaktiosormenjäljen epätyypillisyydestä. Braden mukaan tehokäyttäjien tekemissä transaktioissa V2 LT -sormenjälki ei ole epätyypillinen vaan jopa todennäköinen. Mäntymaa on häntä kuultaessa kuitenkin todennut, että rahajäljityksessä harvoin törmätään tähän sormenjälkeen ja tästä näkökulmasta katsoen kysymys oli epätyypillisistä jäljistä. Edelleen kuultaessa asiantuntijoita vastakkain kysymys on osaltaan ollut lähinnä eroista niin sanottujen tehokäyttäjien ja kasuaalikäyttäjien välillä. Käräjäoikeus siten toteaa, ettei asiantuntijoiden välillä lopulta ollut tältä osin eriävää näkemystä.

Mäntymaan laatimasta analyysistä ja kertomuksesta on ilmennyt, että osoiterypäs X on tehnyt 4 siirtoa noin 18.000 dollarin arvosta ja osoiterypäs Y puolestaan 18 siirtoa noin 9.000 dollarin arvosta Binancen anussucker@cs.email-tilille. Tälle tilille tulevat varat ovat puolestaan olleet peräisin osoiteryppäästä, johon P3-palvelimella toiminut huijausohjelma on siirtänyt virtuaalivaluuttaa. Kysymys on palvelinsarjasta, joka on linkitetty kiristäjään. Tällä tilillä bitcoinit on vaihdettu moneroon ja siirretty yksityiselle Monero-lompakolle ja josta ne ovat päätyneet tämän yhden välilompakon kautta toiselle Binancen tilille, jonka sähköpostiosoitteena on ollut fuckfuckfuck@cs.email.

Tileistä ”anussucker” ja ”fuckfuckfuck” saatu selvitys sekä näiden tilien väliset monero-siirrot

Binancelle on tehty tiedonsaantipyyntö siitä, kenelle edellä mainitut tilit kuuluvat. Binancen vastauksen mukaan ensin mainittu anussucker-tili, joka on luotu 13.5.2020 kello 00:00:15, kuuluu nimettömälle henkilölle, jonka sähköpostiosoitteeksi on annettu anussucker@cs.email (S88). Tähän nimettömään tiliin on raportin mukaan yritetty lisätä "John Frisberg"-nimisen henkilön henkilöllisyyspaperit, mutta Binance ei ole hyväksynyt näitä henkilöpapereita (S88). Raportin mukaan samalla henkilöllisyystodistuksella on rekisteröity tili 21.9.2017 myös Coinbase-palveluun. Kyseisellä tilillä on

edellä mainittujen Frisbergin henkilöllisyyspapereiden lisäksi sähköpostiosoite coinbase@safe.im (S86). Kyseinen safe.im on Kivimäelle riidattomasti kuuluva sähköpostipalvelin. Nimeäminen vastaa myös sitä tapaa, mistä Kivimäki on itsekin kertonut.

Binancen tili fuckfuckfuck@cs.email on puolestaan luotu 13.5.2020 kello 00:19:17. Kyseiselle tilille ei niin ikään ole mitään henkilötietoja tai tunnistuksia. Edellä mainittu anussucker-tili on luotu vain noin 19 minuuttia aikaisemmin kuin fuckfuckfuck-tili.

Kivimäki on tileistä kysyttäessä kertonut, ettei tiedä mitään Frisbergin henkilötiedoista, eikä tunne tämän nimistä henkilöä. Kivimäki on myöntänyt rekisteröityneensä Coinbase-palveluun, mutta kertonut, että joku muu oli hänen mukaansa yrittänyt aktivoida kyseisen tilin. Kivimäki on myös kuvannut sitä, miten Binancen tilin pystyi hankkimaan pyytämällä toista henkilöä toimimaan puolestaan.

Edelleen anussucker@cs.email-tililtä on tehty yhteensä 47 monero-siirtoa. Näistä siirroista 27 on kyetty jäljittämään erittäin suurella todennäköisyydellä yhden yksityisen Monero-lompakon kautta siirretyksi edellä mainitulle Binancen fuckfuckfuck@cs.email-tilille. Siirroista kolme on niin sanottuja co-spend siirtoja, joita on voitu seurata ja vahvistaa selkeä ja toistuva rahanpesun kaava tilin anussucker@cs.email - yksityinen monero-lompakko - fuckfuckfuck@cs.email-tilin välillä. Raportin mukaan polun toistuminen yhteensä 27 transaktiossa tekee päätelmästä käytännössä varman. Raportin mukaan tämän polun todistelu on merkityksellistä, kun osoitetaan vastaava määränpää kiristäjän tekemästä siirrosta SwapLab palvelusta fuckfuckfuck@cs.email yhden yksityisen monero-lompakon kautta.

Vastaamon kiristäjälle poliisin toimesta suoritetun 0,1 suuruisen bitcoin maksun seuraaminen

Kuten edeltä tuomiosta ilmenee, Vastaamolta on kiristetty varoja bc1q-alkuiseen osoitteeseen. Keskusrikospoliisi on Mäntymaan raportista (S81) ilmenevästi 14.10.2020 kello 19:56 suorittanut kyseiseen osoitteeseen 0,1 bitcoinin suuruisen maksun 25fb3-alkuisessa transaktiossa. Kyseinen osoite ei ole vastaanottanut muita varoja kuin Keskusrikospoliisin siirtämän 0,1 bitcoinin suuruisen summan.

Edelleen bc1q-alkuinen osoite on 20.10.2020 kello 23:29 siirtänyt varat eteenpäin SwapLab-vaihtopalveluun. Summana on ollut 0,099 bitcoinia. Varat on selvityksen mukaan vaihdettu 9,801255 moneroon ja siirretty eteenpäin. Transaktion sormenjälkinä ovat edellä mainitut V2, LT sekä SegWit. Siirrosta on syntynyt vaihto-osoite, jolle on tarkastushetkellä 29.11.2020 jäänyt 0,000809 bitcoinia. Vaihto-osoitetta ei ole kulutettu, ja kyseisellä osoitteella on ollut yhä saldona edellä mainittu summa.

SwapLab-vaihtopalveluun on lähetetty tiedonsaantipyyntö (S90), jossa on tiedusteltu mihin lohkoketjuun ja missä transaktiossa kyseinen transaktio on siirretty. SwapLab-palvelun ei raportin mukaan tarvitse antaa henkilötietoja, vaan palvelu suostuu tekemään valuutanvaihtoja asiakastaan tunnistamatta (S81). Tiedonsaantipyyntöön on siten saatu vastauksena pelkästään se tieto mihin valuuttaan, mihin osoitteeseen ja missä transaktiossa varat on siirretty ja vastauksena on siten saatu tieto siitä, mihin lohkoketjuun ja missä transaktiossa edellä mainittu siirto on siirretty SwapLabilta eteenpäin. Monerot on siirretty eteenpäin raportista tarkemmin ilmenevässä 3180c342e-alkuisessa transaktiossa. Edellä mainitun transaktion niin sanotut ”outputit” eli vastaanottajat ovat menneet puolestaan raportista tarkemmin ilmeneviin oikeat

vastaanottavat osoitteet korvanneisiin ”Stealth Addresseihin”, joiden tarkoitus on vaikeuttaa jäljittämistä. Kyseessä oleva siirto on raportin mukaan tehty yksityiseen lompakkoon, eikä se ole kuulunut mihinkään palveluun. Kyseiseltä yksityiseltä lompakolta varat on siirretty jälleen eteenpäin ja yksi transaktioista on mennyt selvityksen mukaan 21.10.2020 kello 00:08:04 Binancen vaihtopalveluun 5e9b713e-alkuisessa transaktiossa (S89, Deposit history-välilehti) tilille fuckfuckfuck@cs.email (S89).

Edellä mainitussa siirrossa tilille fuckfuckfuck@cs.email (S89, Deposit history-välilehti) on puolestaan tullut sisään 49,84 moneroa. Summa on raportin mukaan noin 40 moneroa suurempi kuin mitä alun perin SwapLab-palvelusta siirrettiin yksityiseen lompakkoon. Raportin mukaan samassa transaktiossa on ollut input-puolella myös neljä muuta siirtoa, mutta sitä mistä muut rahat ovat peräisin, ei ole esitutkinnassa selvitetty.

Edelleen edellä todetusti raha on tullut yksityiseltä lompakolta fuckfuckfuck-tilille 21.10.2020 kello 00:08:04. Fuckfuckfuck-tili on vaihtanut moneron bitcoiniksi Binancen-palvelun sisällä 21.10.2020 kello 00:15:03 (S98 välilehti Order History) ja siirtänyt varat eteenpäin bitcoineina 21.10.2020 kello 00:17:02 1M5Txg1f-alkuiselle osoitteelle (S98, välilehti Withdrawal History). Edellä mainittu osoite on siirtänyt varat eteenpäin 21.10.2020 00:50 848287b3-alkuisessa transaktiossa kolmelle osoitteelle siten, että siirrot ovat 1DmSk-alkuiseen osoitteeseen 0,2 bitcoinia, 1Gw9ePT-alkuiseen osoitteeseen 0,15 bitcoinia ja 1Pdyrov-alkuiseen osoitteeseen 0,13611074 bitcoinia. Raportin mukaan kaksi ensimmäistä summaa ovat selviä tasasummia, jotka ovat raportin mukaan selkeästi tarkoitettuja maksuja ja tällöin 0,13611074 bitcoinin suuruinen siirto on selkeä vaihto-osoite. Raportin mukaan on mahdotonta onnistua tekemään sellaista siirtoa, jonka vaihto-osoitteelle menevä summa olisi tasasumma ja tämän perusteella 1Pdyrov-alkuinen osoite on kuulunut erittäin todennäköisesti samaan lompakkoon 1M5Txg1f-alkuisen osoitteen kanssa.

Raportissa on nimetty tämä alkuvaiheen transaktioon menevät varat Polku A:ksi.

Myöhemmässä transaktiossa 1Gw9ePT-alkuisessa osoitteessa on käytetty samassa transaktiossa myös 1Pdyrov-alkuiselle osoitteelle menneet varat. Tästä on puolestaan voitu raportin mukaan muodostaa varmasti syntynyt osoiteklusteri, johon on kuulunut kolme raportista tarkemmin ilmenevää osoitetta. Muodostunut osoiterypäs on siirtänyt c7c3c98f70-alkuisessa transaktiossa aikaleimalla 21.10.2020 00:50 0,192 bitcoinia 1LqUSqLY-alkuiseen osoitteeseen, jonka siirron sormenjälki on ollut V2 LT. Tässä siirrossa on syntynyt puolestaan 1ENAwtigC-alkuinen vaihto-osoite. Tämä vaihto-osoite voidaan rypästää samaan ryppääseen, johon aiemmin kuului kolme osoitetta. Myöhemmässä transaktiossa 1ENAwtig-alkuinen osoite on kuluttanut varoja kuuden muun raportista tarkemmin ilmenevän osoitteen kanssa samanaikaisesti. Edelleen kukin näistä kuudesta osoitteesta on puolestaan vastaanottanut vähäisen määrän bitcoineja ennen rikoksen tekoaikaa, mutta analyysiä taaksepäin siitä, mistä varallisuus on ollut peräisin, ei ole tehty. Edellä yksityiskohtaisesti selitetyillä menetelmillä on raportista ilmenevästi voitu koota osoiteklusteri, johon ovat kuuluneet raportista tarkemmin ilmenevät 11 osoitetta, ja näiden osoitteiden muodostama osoiterypäs on nimetty raportissa osoiterypäs A:ksi.

Osoiterypäs A on lähettänyt 31.10.2020 kello 18:51 a138809-alkuisessa transaktiossa 0,10169502 bitcoinia 1EyWn-alkuiselle osoitteelle. Transaktiossa on ollut jälleen poikkeuksellinen V2 LT -sormenjälki. Viimeksi

mainittu osoite on muodostanut kahden osoitteen ryppään 13TNSm-alkuisen osoitteen kanssa. Kyseinen 13TNSm-alkuinen osoite on vastaanottanut aiemmin varoja, mutta analyysillä ei ole selvitetty, mistä varat ovat osoitteelle tulleet. Osoiterypäs on käyttänyt varat 1.11.2020 10:44 d04487924-alkuisessa transaktiossa siirtäen 0,12735034 bitcoinia 3Csj6zeEU-alkuiselle osoitteelle, joka on kuulunut vaihtopalvelu Wirexille. Transaktiossa on ollut jälleen V2 LT -sormenjälki, minkä lisäksi transaktiossa on käytetty RBF-toimintoa (replace by fee), joka mahdollistaa mahdollisimman pienten siirtokulujen tavoittelemisen. Edellä esitelty transaktio on synnyttänyt 1KpL2E4-alkuisen vaihto-osoitteen. Varojen vastaanottaja on Daniel Newhard -niminen henkilö. Raportin mukaan Newhardin tilillä bitcoinit on vaihdettu euroiksi ja kulutettu (S91 ja S98). Mäntymaan mukaan näyttäisi lähinnä siltä kuin kyse olisi ollut voitonjaosta kahden vastaanottajan Newhardin sekä Kivimäen välillä.

Edelleen osoiterypäs A:lta on lähtenyt myös toinen polku, joka on raportissa nimetty polku B:ksi. Aikaisemmin mainittu 1M5Txg-alkuinen osoite on 848287b37-alkuisella transaktiolla siirtänyt 0,2 bitcoinia 1DmSk-alkuiselle osoitteelle. Kyseinen osoite on myöhemmässä transaktiossa kuluttanut varoja yhdessä 1KGF5-alkuisen osoitteen kanssa. Edellä mainittu osoite on vastaanottanut aiemmin varoja, mutta analyysillä ei ole selvitetty sitä, mistä varat ovat olleet peräisin. Nämä osoitteet ovat muodostaneet tässä vaiheessa kahden osoitteen ryppään osoiterypäs B:ksi. Osoiterypäs B on siirtänyt 3169172e958-alkuisessa transaktiossa 28.10.2020 kello 14:06 1F2qwv4S-alkuiselle osoitteelle 0,25 bitcoinia. Viimeksi mainittu osoite on nimetty osoiterypäs C:ksi. Transaktiolla on sormenjälki V2 LT, ja siirrossa on syntynyt 1EMuzN-alkuinen vaihto-osoite. Vaihto-osoite on kuluttanut varoja viiden muun osoitteen kanssa, jotka ovat vastaanottaneet aiemmin varoja. Osoitteet, joiden kanssa edellä mainittu osoite on kuluttanut varoja yhdessä viiden muun raportista tarkemmin ilmenevän osoitteen kanssa, on rypästetty yhdessä 1EMuzN-alkuisen osoitteen kanssa osoiterypäs B:hen.

Edellä kerrottu osoiterypäs B on siirtänyt 7.11.2020 kello 21:37 1d6df75f6f-alkuisessa transaktiossa 0,1 bitcoinia osoiterypäs C:lle. Siirron sormenjälki on V2 LT, ja siitä on syntynyt 15Jvqe1F-alkuinen vaihto-osoite. Vaihto-osoite on kuluttanut varoja yhdessä viiden muun raportista tarkemmin ilmenevän osoitteen kanssa. Kukin näistä osoitteista on aiemmin vastaanottanut varoja muista lähteistä, mutta varojen alkuperää ei ole selvitetty. Edellä listatut osoitteet on rypästetty jälleen yhteen osoiterypäs B:n kanssa.

Osoiterypäs C on 327 osoitteen osoiterypäs, jonka osoitteet on rypästetty keskenään yhteen yhteisten siirtojen perusteella. Osoiterypäs C on pitänyt sisällään kirjallisesta todisteesta S91 ilmenevät osoitteet. Osoiterypäs C on raportin mukaan ollut toiminnassa 27.10.2020–6.7.2021 ja on tänä aikana vastaanottanut 118,4244247 bitcoinia ja lähettänyt saman verran eteenpäin.

Coinstant.es-palvelu

Analyysistä ilmenee edelleen, että edellä mainittu osoiterypäs C on lähettänyt ison osan sisään tulevista varoista suomalaiseen LocalBitcoins "peer-to-peer" eli kuluttajalta kuluttajalle -vaihtopalveluun (S101). Tässä palvelussa kuluttajat voivat käydä virtuaalivaluuttakauppaa keskenään.

LocalBitcoins-palvelusta on tiedusteltu, kenelle osoiterypäs C on siirtänyt varansa. Siirrot on raportin mukaan tehty "Top-BTC" nimimerkillä bitcoineja myyvälle käyttäjälle ja nimimerkki kuuluu erittäin todennäköisesti coinstant.es-palvelulle. Palvelun vahvin indikaattori raportin mukaan ovat

kaupankäynnin keskustelut (S100). Jokaisen vaihtotapahtuman lopussa palvelu lähettää linkin henkilölle, joka on bitcoineja ostanut, ja linkin kautta voi tarkistaa vaihtotapahtuman kuitin tai tositteen. Raportin mukaan kyseinen palvelu on epävirallinen vaihtopalvelu, joka lupaa välitöntä bitcoinin vaihtamispalvelua. Palvelua ei ole rekisteröity virallisesti, eikä palvelu ole vastannut viranomaisten tiedonsaantipyyntöihin.

Raportista ilmenee, että Coinstant.es ja osoiterypäs C toimivat erittäin todennäköisesti siten, että henkilön halutessa vaihtaa bitcoineja euroiksi, henkilö ilmaisee halukkuutensa coinstant.es-verkkosivujen tai oman portaalin kautta ja käynnistää vaihtotapahtuman. Coinstant.es-palvelusta käyttäjälle annetaan virtuaalivaluuttalompakon osoite, joka tässä tapauksessa on ollut joku osoiterypäs C:n osoitteista. Käyttäjä siirtää virtuaalivaluutat osoiterypäs C:lle ja saa samanaikaisesti coinstant.es-palvelun ”rahamuuleilta" euroja tilisiirtona haluamalleen tilille. Palvelu puolestaan siirtää osoiterypäs C:ltä bitcoinit Localbitcoins Top-BTC käyttäjälle, jonka kautta virtuaalivaluuttaa vaihdetaan euroiksi. Palvelu ottaa myyntitapahtumista kulun ja tekee tällä tavoin voittoa.

Kivimäen tili Revolut-pankissa

Kivimäellä on 6.8.2020 avattu Revolut-tili (S92), johon on liitetty kaksi maksukorttia.

Kivimäki on kysyttäessä tuloistaan ja varallisuudestaan vuosina 2020–2021 kertonut, että hänellä oli jo valmiiksi merkittäviä määriä kryptovaluuttoja, jotka oli hankittu vuosina 2012–2013. Arvonnousun takia kryptovaluutat olivat huomattavan arvokkaita, eikä hän ollut sen vuoksi tarvinnut työtuloja. Hän oli ollut matkatoimistossa töissä, eikä poliisi ollut kysellyt häneltä mitään palkkakuitteja. Kivimäki käytti Exodus- ja Ledger-lompakoita. Kysyttäessä kryptovaluuttojen tulouttamisesta Kivimäki on kertonut myyvänsä kryptoja euroiksi. Palveluja oli monia kuten Coinstant.es. Kivimäki on kertonut, että hänen Revolut-tilinsä varat olivat peräisin aiemmista säästöistä. Kysyttäessä erikseen Revolut-tilin tilitapahtumista syys-lokakuussa 2020 Kivimäki ei ole osannut sanoa mitään useista Top-BTC siirroista Aleksandar Zikovilta, Anna Tamrasova Tanasinilta tai Liliia Dushnalta hänen tililleen. Kivimäki on viitannut ajan kulumiseen, eikä hän siksi ole kertomansa mukaan voinut muistaa yli kolme vuotta aikaisemmin tapahtuneita rahasiirtoja.

Coinstant.es ja Kivimäen Revolut-tili

Edellä kerrotun tapahtuman coinstant.es-palvelun ja osoiterypäs C:n välillä on voinut raportin mukaan varmistaa vertailemalla Kivimäen Revolut-tilille tulevaa rahaliikennettä muutamilta eri henkilöiltä kuten Aleksander Zikovilta tai Liliia Dushnalta (S95). Kirjallisesta todisteesta numero S96 ilmenee, että muun muassa Zikov ja Dushna ovat olleet Top-BTC-tilin edunsaajia, eli henkilöitä, joille on tilitetty euroja myydyistä virtuaalivaluutoista. Samalla tavalla jokaisen, joka on siirtänyt varoja Kivimäen Revolut-tilille, nimi on löydettävistä palvelun Trade Chat -lokista (S96).

Edellä on jo esitelty transaktio osoiterypäs B:n ja C:n välillä, missä osoiterypäs B on siirtänyt 3169172e-alkuisessa transaktiossa 28.10.2020 kello 14:06 osoitteelle osoiterypäs C:lle 0,25 bitcoinia. Raportin mukaan tässä transaktiossa on siirtynyt osa seuratusta 0,1 bitcoinista, jonka Keskusrikospoliisi on alun perin maksanut Vastaamon kiristäjälle. Edelleen tarkasteltaessa Kivimäen Revolut-tilin tilitapahtumia edellä mainitulta päivältä, Kivimäen tilille on tullut rahaa Liliia Dushnalta ja Aleksander

Zikovilta (S95). Osoiterypäs B on siirtänyt coinstant.es Bitcoin-lohkoketjussa toimivalle osoitteelle 0,25 bitcoinia kello 14:06, ja kello 14:04 Kivimäen Revolut-tilille on siirretty Aleksander Zikovilta 2.490 euroa ja kello 14:08 Liliia Dushnalta 216 euroa. Top BTC:n LocalBitcoinin-tilin keskusteluhistoriasta ilmenee edelleen, että samalta päivältä 28.10.2020 Top BTC on myynyt bitcoineja ja ohjannut asiakkaan maksamaan bitcoineista Aleksander Zikoville (S100). Myyntitapahtumissa Top BTC -käyttäjä on antanut aina viestin lopussa linkin, joka on coinstant.es-palvelun sisäinen kuitti myyntitapahtumasta. Lisäksi merkittävää on se, että varoja on tilitetty saman nimisten henkilöiden tileille, joilta Kivimäen Revolut-tilille on tullut euroja. Raportin mukaan aikaleima bitcoin-siirrolle on aikaisempi kuin euro-siirrolle, koska bitcoin-siirron aikaleima on se hetki, kun koko lohko, jossa kyseinen transaktio on ollut, on vahvistettu.

Mäntymaa on myös raportissaan tarkastellut 31691-alkuista maksua, jossa siirtomaksua kyseisellä transaktiolla on ollut noin 47,6 dollaria per kB. Tämä transaktio on maksanut keskimääräistä enemmän kuluja, mikä raportin mukaan tarkoittaisi sitä, että kyseinen transaktio on todennäköisemmin tullut vahvistettavaan lohkoon melko nopeasti. Tarkasteltaessa tapahtuneen siirron summaa ja sen määrää euroina on raportissa todettu, että 28.10.2020 kello 14:00 0,25 bitcoinin arvo on ollut 3.315,54750 dollaria. Yksi dollari on vastannut 0,85 euroa, jolloin 0,25 bitcoinia on vastannut siirtohetkellä 2.818,21 euroa. Kivimäen Revolut-tilille on siirretty 2.706 euroa coinstant.es-palvelusta. Tilille tullut summa on lähes desimaalilleen neljä prosenttia pienempi kuin alkuperäinen summa. Mäntymaan kertomus huomioon ottaen edellä ilmennyt on vastannut määrältään sitä, mitä kyseisenlaiselta vaihtopalvelulta voi kuluina yleensä odottaa. Koska Coinstant.es ei ole rekisteröity palvelu mutta ei myöskään suoraan rahanpesupalvelu, ja sen rahanvaihdon menetelmä on virallista vaihtopalvelua monimutkaisempi ja kalliimpi, ei neljän prosentin kulu palvelusta ole Mäntymaan mukaan lainkaan erikoinen vaan hyvinkin odotettu.

Edellä mainittu huomioon ottaen voidaan Mäntymaan mukaan pitää erittäin todennäköisenä sitä, että osoiterypäs B:stä osoiterypäs C:lle tehty siirto on maksettu euroina Kivimäen Revolut-tilille samana ajanhetkenä. Raportissa on tarkasteltu myös toista samankaltaista vaihtotapahtumaa osoiterypäs B:n ja osoiterypäs C:n välisestä transaktiosta, jossa on ollut 1d6df75f6f8-alkuinen siirto, jossa osoiterypäs B on siirtänyt 0,1 bitcoinia osoiterypäs C:lle 7.11.2020 kello 21:37. Siirron siirtohetken arvo dollareina on ollut 1.482 dollaria ja euroina päivän kurssilla 1.259,70 euroa. Kun summasta on vähennetty oletettu neljän prosentin kulu, on summaksi saatu 1.197 euroa ja vastaavalla ajanhetkellä Kivimäen Revolut-tilille on jälleen tullut Aleksandar Zikovin tililtä 1.196 euroa.

Mäntymaa on vielä analyysissä käytetyn aikakorrelaation osalta todennut, että se on rahanjäljitysanalyysissä olennainen ja että kysymyksessä on ollut hänen mukaansa ”tahdikas rahanpesu”. Mäntymaan mukaan aikajänne on rahan liikuttelussa ollut yhtenäinen ja rahaa on liikuteltu ilman taukoja. Ketju on ollut myös ajallisesti yhtenäinen osoiterypäs B:hen saakka. Mäntymaan mukaan aikakorrelaatio on myös pitävä. Mäntymaa on vielä todennut, että kiristäjä hallitsee valeostoa eikä lompakkoa ole jaettu. Mäntymaan mukaan vuonna 2020 jaettavia lompakoita ei ollut vielä edes olemassa, vaikka nykyisin sellaisiakin on.

Asiantuntija Brade on ollut edellä mainitun johtopäätöksen osalta erimielinen siitä, voidaanko SwabLabin kautta vaihdettu 0,1 bitcoinia, joka puolestaan on muunnettu 9,8 moneroksi ja mennyt Binacen fuckfuckfuck-tilille, pitää

Mäntymaan kertomin tavoin todennäköisenä. Molemmissa poluissa (A ja B) on siirtynyt yli 0,1 bitcoinia, ja Braden mukaan ei ole mitään perustetta katsoa, että osoiterypäs B:stä osoiterypäs C:lle lähetetyt 0,25 bitcoinia ovat varmasti sisältäneet osan seuratusta 0,1 bitcoinista, koska koko summa on voinut siirtyä polku A:n kautta muualle, eikä ole mitään keinoa lohkoketjuanalyysin avulla määrittää siirtyykö seuratusta 0,1 bitcoinista polku B:n kautta 0 prosenttia, 100 prosenttia tai jotain siltä väliltä.

Braden mukaan Mäntymaan analyysissä on luotu tältä osin tietynlainen teoria sinänsä mahdollisesta rahan liikkeestä, mutta lohkoketjuanalyysin perusteella siihen liittyy epävarmuuksia. Hänen mukaansa tutkintamateriaalissa hyvin olennainen edellä tuomiossa kerrottu SwapLabista tehty 9,8 moneron suuruinen monero-siirto on tehty vain kerran ja siirron summa on muuttunut merkittävästi sillä hetkellä, kun monero-varoja on saapunut seuratulle Binance-tilille. Braden mukaan varmuudella ei siten voida sanoa, että SwapLabista lähetetyt 9,8 moneroa olisivat siirtyneet Binance-tilille fuckfuckfuck. Kyseinen Mäntymaan analyysi todistaa ainoastaan sen, että varat ovat voineet siirtyä kyseiselle tilille, mutta tämä on hänen mukaansa epävarmaa. Braden mukaan tältä osin kysymys on näiden ryppäiden osalta ainoastaan yksittäisestä eikä toistuvasta transaktiosta, eikä monerossa voida nähdä, minne kyseinen raha on siirtynyt ottaen huomioon useampi mahdollinen siirron päätepiste. Nämä seikat poistavat varmuuden.

Braden mukaan ajallinen yhteys siirroille on sinänsä olemassa, mutta muitakin selityksiä hänen mukaansa on. Siirtoja ryppäiden välillä on ollut lukuisia, ja rahaa on tullut paljon kaikille osoiteryppäille. Selvityksestä on myös jätetty pois muuta rahaliikennettä, ja lopputulos on Braden mukaan ainoastaan olettama siitä, että kaikki tilit olisivat olleet Kivimäen hallinnoimia.

Vastaamon asiakkaiden kiristäminen

Analyysin (S81) mukaan kiristäjä on vastaanottanut Vastaamon asiakkailta kiristettyjä varoja 33 osoitteen klusteriin ja tämä osoiterypäs on nimetty Z:ksi. Osoiterypäs Z on siirtänyt kaiken saadun rikoshyödyn eteenpäin.

Ryppään rahaliikenteen analyysi on ollut pääkäsittelyn aikana kesken, mutta tästä huolimatta Mäntymaa on todennut sormenjälkianalyysin perusteella osoiteryppään siirrot tehdyksi todennäköisesti samalla Bitcoin-lompakkosovelluksella kuin millä muiden osoiteryppäiden eli A:n, B:n, Y:n X:n ja Vastaamon kiristäjän tekemät siirrot on tehty. Lompakon transaktiosormenjäljet ovat olleet samanlaiset ja lompakkojen siirrot ovat sopineet tehdyiksi Bitcoin Core tai Electrum-lompakkosovelluksilla.

Virtuaalivaluuttaa koskevat johtopäätökset

Analyysissä on lopuksi todettu edellä lausutun perusteella olevan todennäköistä, että Kivimäki tosiasiallisesti hallinnoi Binancen tilejä anussucker@cs.email sekä fuckfuckfuck@cs.email. Anussucker@cs.email-tilin tarkoituksena on muuttaa sisään tulevat bitcoinit moneroon ja siirtää nämä monerot eteenpäin yksityiselle monero-lompakolle. Tilin fuckfuckfuck@cs.email tarkoituksena on vastaanottaa monerot yksityiseltä monero-lompakolta ja vaihtaa ne takaisin bitcoineiksi.

Johtopäätöksestä tekee raportin mukaan erittäin todennäköisen myös se, että varat ovat kulkeutuneet selkeää reittiä pitkin rikoksesta epäillyn käyttöön. Mikäli monero-jäljityksessä olisi tehty virhe, käytännössä mahdotonta on, että sattumalta olisi päädytty juuri sen henkilön tilitapahtumiin, jota alkuperäisestä rikoksesta epäillään. Asiassa käytetty rahanpesun polku ja päätepiste on

toistunut ainakin 28 siirrossa, jonka vuoksi virheen mahdollisuus on olematon ja on voitu todeta tilien anussucker@cs.email ja fuckfuckfuck@cs.email liittyvän kiinteästi toisiinsa.

Näytön arviointi

Näytön arvioinnin lähtökohdat

Oikeudenkäymiskaaren 17 luvun 3 §:n 1 momentin mukaan rikosasiassa kantajan eli rangaistusta vaativan syyttäjän tai asianomistajan on näytettävä ne seikat, joihin hänen rangaistusvaatimuksensa perustuu. Pykälän 2 momentin mukaan tuomion, jossa vastaaja tuomitaan syylliseksi, edellytyksenä on, ettei vastaajan syyllisyydestä jää varteenotettavaa epäilyä. Edelleen syyttömyysolettamasta seuraa, että todistustaakka syyksi lukevan tuomion perustavista seikoista on syyttäjällä ja ettei vastaajalle voida asettaa velvollisuutta todistaa syyttömyyttään.

Syyttäjän todistustaakasta huolimatta voi kuitenkin syntyä tilanteita, joissa rikosasian vastaajan voidaan edellyttää selvittävän niitä seikkoja, joihin hän on puolustuksekseen vedonnut (KKO 2012:27). Rikosasian kantajan tulee kuitenkin esittää riittävän vahva näyttö syytteen tueksi ennen kuin syytteelle vaihtoehtoista tapahtumainkulkua koskevan vastaajan kertomuksen epäuskottavuudelle voidaan antaa merkitystä syytteen tueksi esitetyn näytön todistusvoimaa harkittaessa. Näyttö vastaajan syyllistymisestä rikokseen koostuu usein monista riidattomista tai asiassa esitetyn näytön perusteella selvitetyiksi katsotuista seikoista, jotka ainoastaan niistä tehtävien johtopäätösten kautta välillisesti todistavat syytteessä kuvatusta teosta. Tällaiseen niin sanottuun aihetodisteluun perustuvassa todistusharkinnassa todisteiden kokonaisharkinnalla on yleensä keskeinen merkitys. Kokonaisharkinnan keskeisestä merkityksestä huolimatta tuomioistuin on velvollinen arvioimaan asiassa esiin tulleiden seikkojen merkityksen myös erikseen siten kuin oikeudenkäymiskaaren 17 luvun 1 §:n 2 momentissa edellytetään (KKO 2017:12).

Korkein oikeus on vielä edellä mainitussa ratkaisussaan todennut, että rikosasian vastaajan syyllistymisellä muihin rikoksiin ei ole yleensä merkitystä harkittaessa, onko vastaaja syyllistynyt syytteessä väitettyyn rikokseen. Kuitenkin jos vastaajan syyksi aikaisemmin luetuilla rikoksilla ja hänen tekemäkseen väitetyllä rikoksella on esimerkiksi samanlainen tekotapa ja muita yhdistäviä piirteitä, aikaisemmalla tuomiolla voi olla vaikutusta myöhemmän rikoksen näytön arvioinnissa. Vastaavasti syytettäessä vastaajaa useasta samankaltaisesta rikoksesta asiassa esiin tulleet sanotunlaiset yhteiset piirteet voivat vahvistaa muun syytettä tukevan näytön todistusvoimaa.

Selvää on, ettei näyttökynnys tietoverkkorikoksissa saa olla alempi kuin muissakaan rikoksissa, vaikka asian laadusta johtuen välittömän ja yksiselitteisen näytön hankkiminen voi kyseisenlaisissa rikoksissa olla hankalaa.

Yhteenveto ja johtopäätökset näytöstä

Käräjäoikeus toteaa, että syytteeseen johtanut tapahtumainkulku asiassa on pitkälti riidaton ja selvitetty. Psykoterapiakeskus Vastaamo Oy:n tietojärjestelmään on murtauduttu marraskuussa 2018, ja yhtiön potilastietokanta on tässä yhteydessä oikeudettomasti kopioitu. Vastaamoa ja sen asiakkaita on tämän jälkeen syys-lokakuun 2020 aikana kiristetty ja asiakkaiden erittäin arkaluonteisia tietoja levitetty. Syyttäjien syytteen ja Kivimäen vastauksen perusteella asiassa on lähtökohtaisesti kysymys siitä,

onko nimenomaan Kivimäki yksin tai yhdessä tuntemattomaksi jääneiden henkilöiden kanssa syyllistynyt syytteessä kuvattuihin rikoksiin.

Näytön arvioinnin osalta asiassa on keskeisiltä osin kysymys siitä, onko syytteessä kerrotut rikokset tehty OPSVM-virtuaalipalvelimella ja onko Kivimäki rikosten tekoaikana käyttänyt tätä palvelinta. Arvioitaessa sitä, onko Kivimäki tuolloin käyttänyt OPSVM-virtuaalipalvelinta, merkitykselliseksi nousee ensinnäkin sen selvittäminen, onko Kivimäki ollut sormenjäljeltään WI8-alkuisen SSH-avaimen käyttäjä ja osaltaan myös se, onko hän ollut tämän avaimen ainoa käyttäjä. Siltä osin, onko Kivimäki sanotun SSH-avaimen käyttäjä, merkityksellistä on myös sen selvittäminen, onko ja miten Kivimäki käyttänyt asiassa esille noussutta P- ja K-palvelinten kokonaisuutta, ja mitä SSH-avainta hän on tällöin käyttänyt. SSH-avaimen käyttämisen lisäksi näytön arvioinnissa on asian lopputuloksen kannalta merkitystä myös sillä, onko Kivimäki ollut myös IP-osoitteiden 37.156.72.25 ja 147.161.123.116 käyttäjä. Näistä IP-osoitteista erityisesti 37.156.72.25 on asian ratkaisemisen kannalta merkittävä.

Kohdissa 4 ja 5 kuvattujen rikosten osalta merkitystä on myös sillä, onko vastaamo.tar-paketin konfiguroinnissa tapahtuneen virheen seurauksena joku muu henkilö tai taho onnistunut lataamaan Vastaamon potilastietokannan kokonaisuudessaan haltuunsa.

Syyksilukemisen kannalta merkitykselliseksi nousee lopulta myös Kivimäen selvitettyjen ja osin myöntämien toimien sekä Vastaamon ja sen asiakkaiden kiristystoimien ajallinen yhteys. Merkitykselliseksi oikeudenkäynnin aikana on noussut myös se, onko Keskusrikospoliisin tekemä 0,1 bitcoinin valeosto päätynyt Kivimäelle.

Onko syytteessä kuvatut rikokset tehty OPSVM-virtuaalipalvelimella

Tietomurto

Keskusrikospoliisin suorittaman tietoteknisen tutkinnan ja todistajana kuullun Rantalaisen kertomuksen perusteella asiassa on selvitetty, että OPSVM-virtuaalipalvelimen root- eli pääkäyttäjä on 25.11.2018 skannannut internetiä ecatel-nimistä palvelinta käyttämällä. Tämän jälkeen 26.10.2018 Vastaamon potilastietokantaan on suoritettu väsytyshyökkäyksiä. OPSVM-palvelimen pääkäyttäjän kotihakemistosta löytyneen tietokantadumpin (fi_vastaamo.sql) viimeisen rivin ja Ficolon netflow-lokin perusteella hyökkäys on lopulta onnistunut ja Vastaamon potilastietokanta pystytty kopiomaan. OPSVM-palvelimen komentohistorian mukaan ecatel-palvelimelta on edellä kerrotun jälkeen 29.11.2018 siirretty muun muassa mysql.tgz- ja mysqllogins-nimiset tiedostot OPSVM-palvelimelle. Mysql.tgz-tiedosto on sisältänyt internetissä skannattuja IP-osoitteita, joista yksi on ollut Vastaamon potilastietokannan IP-osoite (95.175.109.219). Mysqllogins-tiedosto on sekin sisältänyt Vastaamon potilastietokannan IP-osoitteen ja sen lisäksi potilastietokannan käyttäjätunnuksen ja salasanan, mikä kenttä on kuitenkin ollut tyhjä. Vastaamon potilastietokannan kopio on lopulta tuotu OPSVM-palvelimelle 7.10.2020, ja tällöin palvelimelle on oltu kirjautuneena vain SSH-avaimella, jonka sormenjälki on ollut WI8-alkuinen.

Käräjäoikeus katsoo edellä ja aiemmin tuomiossa esitetyn perusteella näytetyksi, että kohdassa 1 kuvattu teko on tehty OPSVM-virtuaalipalvelimella ecatel-nimistä palvelinta käyttämällä.

Kiristys- ja yksityiselämää loukkaavan tiedon levittämisrikokset

Tietoteknisessä tutkinnassa OPSVM-palvelimelta on löytynyt muun muassa Vastaamon potilastietokannan kopio, potilastietokannasta muodostetut tekstitiedostot sekä kiristysviestien lähettämiseen käytetyt Vastaamon asiakkaiden sähköpostiosoitteet sisältänyt tietokantadumppi.

OPSVM-palvelinta on myös käytetty Vastaamon potilastietokannan käsittelyyn. Potilastietokannasta on muodostettu kiristyksessä käytetyt potilaskohtaiset niin sanotut tekstitiedostot ja näin muodostettuihin tekstitiedostoihin on tehty suomenkielentaitoa edellyttäneitä hakuja. OPSVM-palvelimella on myös pystytetty ja ylläpidetty tietojen levittämisessä ja kiristyksessä käytettyä Tor-piilopalvelua eli niin sanottua Onion-sivustoa, jolla Vastaamon potilaiden tietoja on julkaistu. Piilopalvelusta on myös löytynyt Ylilaudalla käytyjä kiristystoimien aikaisia keskusteluketjuja.

Kuten edellisessä kohdassa on todettu, myös Vastaamon potilastietokannan IP-osoite on löytynyt esimerkiksi mysql.tgz-nimisestä tiedostosta OPSVM-palvelimelta, jonne se oli siirretty heti tietomurron jälkeen 29.11.2018. Asian lopputuloksen kannalta merkittävää on, että Vastaamon kiristäjä on englanninkielisessä viestissään 30.9.2020 ilmoittanut ladanneena potilastietokannan sanotusta IP-osoitteesta useita kuukausia aikaisemmin sen ollessa avoinna internetissä.

Käräjäoikeus katsoo edellä ja aiemmin tuomiossa esitetyn perusteella näytetyksi, että myös kohdissa 2 ja 3 kuvatut teot on tehty OPSVM-virtuaalipalvelimella.

Onko ja miten Kivimäki käyttänyt OPSVM-virtuaalipalvelinta

Kivimäki on häntä kuultaessa kertonut käyttäneensä OPSVM-virtuaalipalvelinta, tosin lähinnä sen sisältöä koskeneesta mielenkiinnosta.

OPSVM-palvelimen tietoteknisessä tutkinnassa on selvitetty, että kohdissa 2 ja 3 kuvattujen toimien aikana palvelimelle on oltu kirjautuneena mysql-server-nimisen ohjelmiston asennushetkeä ja tekstitiedostojen luomisaikaa lukuun ottamatta vain SSH-avaimella, jonka sormenjälki on ollut WI8-alkuinen. Näiden kirjautumisten aikana OPSVM-palvelimelle on tehty muun muassa Kivimäen kotiosoitteeseen ja kotiseudun postiosoitteeseen liittyviä hakuja samoin kuin suomen kieltä oikein tavuttamalla tehtyjä hakuja. Tämän perusteella käräjäoikeus katsoo asiassa näytetyksi, että sormenjäljeltään WI8-alkuisen SSH-avaimen käyttäjän on täytynyt olla suomenkielentaitoinen. Tämä sekä palvelimella suoritetut suomenkieliset haut tukevat johtopäätöstä siitä, että Kivimäki on käyttänyt OPSVM-palvelinta myöntämäänsä enemmän eli myös rikosten tekoaikana, ja että hän käyttänyt SSH-avainta, jonka sormenjälki on WI8-alkuinen.

Siltä osin, onko nimenomaan Kivimäki sormenjäljeltään WI8-alkuisen SSH-avaimen käyttäjä, on merkityksellistä myös sen selvittäminen, onko, ja jos on niin miten, Kivimäki käyttänyt asiassa esille noussutta P- ja K-palvelinten kokonaisuutta sekä IP-osoitetta 35.156.72.25. Merkityksellistä syyksilukemisen kannalta on erityisesti myös sillä, mitä SSH-avainta hän on tällöin käyttänyt, ja onko hän ollut tämän SSH-avaimen ainoa käyttäjä. Näiltä osin käräjäoikeus toteaa yhteenvetona ja johtopäätöksenä seuraavan.

Onko Kivimäki käyttänyt P- ja K-palvelimia

Tuomiossa edellä jo esitetyn perusteella käräjäoikeus toteaa, että rikoskokonaisuuden kannalta keskeisillä fyysisillä palvelimilla eli P1- ja

P2-palvelimilla sekä K17-palvelimella on ollut paitsi palvelininfrastruktuuriin myös niiden käyttöön liittyneitä yhteyksiä toisiinsa. P- ja K-palvelimia on käytetty kokonaisuutena ja niiltä on löytynyt myös selkeitä liityntöjä Kivimäkeen.

Palvelin P1

P1-palvelimella olleesta pyongyang-nimisen palvelimen kopiosta on löytynyt suoraan Kivimäen yksityiselämään liittyvä valokuva ”beach.jpg” sekä kopio häntä käsittelevästä verkkosivusta. Käräjäoikeus pitää verkkosivun osalta sinällään mahdollisena, että Kivimäkeen negatiivisesti suhtautuva verkkosivusto olisi jonkun muun säilyttämä. Sen sijaan varsin epäuskottavaa on, että joku muu kuin Kivimäki olisi saanut vahvasti Kivimäen yksityiselämään liittyvän valokuvan haltuunsa ja säilyttäisi sitä verkossa olevalla palvelimella.

P1-palvelimelta on lisäksi löytynyt Kivimäen lähipiiriin kuuluneen henkilön kummitädin sähköpostin IMAP-loki, jota on myös käsitelty palvelimella ja josta on löytynyt liittymäkohtia Kivimäkeen edellä esitetyin tavoin.

Käräjäoikeus katsoo jo edellä kerrottujen seikkojen tukevan johtopäätöstä siitä, että Kivimäellä on liityntä P1-palvelimeen ja että hän on myös käyttänyt P1-palvelinta.

Palvelin P2

P2-palvelin on ollut niin sanottu virtualisointialusta, joka on sisältänyt useita eri virtuaalipalvelimia. Kivimäki on itse kertonut käyttäneensä P2-palvelinta vain sillä ollutta vpn-virtuaalipalvelinta käyttäessään. P2-palvelimen osalta syyttäjien näyttö siitä, että Kivimäki olisi käyttänyt myös sitä, perustuukin pääosin siihen, että sanotulle palvelimelle on kirjauduttu WI8-alkuisella SSH-avaimella. Tämä avain on ollut myös ainoa avain, jolla P1- ja P2-palvelimet on pystytty käynnistämään.

P2-palvelimella on ollut kuitenkin myös irc-niminen virtuaalipalvelin, jolla on ollut WeeChat-niminen asiakassovellus. Tämä asiakassovellus on mahdollistanut IRC-keskustelualustalla julkaistujen viestien seuraamisen myös sinä aikana, kun käyttäjä ei ole ollut alustalla paikalla tai muuten aktiivinen. Todistaja Rantalaisen mukaan WeeChat onkin ollut jo käyttötarkoituksensa perusteella todennäköisesti yhdelle käyttäjälle tarkoitettu IRC-asiakasohjelmisto. Weechat-asiakassovellusta on käytetty aktiivisesti erityisesti vastaamo.tar-paketin virheenselvityksen aikana käyttäjätunnuksella ircuser. Tällä käyttäjätunnuksella on ollut lukuisia eri nimimerkkejä, joista moneen on sisältynyt sana tai nimi ”ryan” samalla tai eri tavoin muotoiltuna. Yksi näistä nimimerkeistä on ollut ryan@whitefire. Kuten tuomiossa on jo aiemmin todettu, Kivimäki on käyttänyt runsaasti eri nimiä ja nimimerkkejä, joista keskeisimmäksi on noussut ”ryan”, jolla nimellä moni Kivimäen tunteneista on hänet myös tuntenut. Kivimäki on lisäksi kertonut käyttäneensä tai ainakin pitävänsä mahdollisena, että hän on käyttänyt whitefire-palvelimella nimimerkkiä ”ryan”.

IRC-virtuaalipalvelimelle kirjautuminen on edellyttänyt SSH-avainta, ja sen kirjautumislokin mukaan palvelimelle on kirjauduttu käyttäjätunnuksella ircuser onnistuneesti vain SSH-avaimella, jonka sormenjälki on ollut WI8-alkuinen. Käyttäjätunnus ircuser on ollut tällä avaimella kirjautuneena IRC-palvelimelle muun muassa niinä hetkinä, jolloin P2-palvelimella on tehty selvitystä virheellisen tar-paketin osalta.

Käräjäoikeus katsoo edellä kerrotun tukevan johtopäätöstä siitä, että Kivimäki on käyttänyt P2-palvelinta ja sillä olleita virtuaalipalvelimia myöntämäänsä enemmän ja myös aktiivisesti kohdissa 2 ja 3 kuvattujen rikosten tekoaikana. Edellä kerrottu tukee myös sitä, ja että palvelimille kirjautuessaan hän on käyttänyt SSH-avainta, jonka sormenjälki on ollut WI8-alkuinen.

Palvelimet K1–K17 ja Scanifi LLC

Käräjäoikeus katsoo Kivimäen ja todistaja Naughtonin kertomusten perusteella selvitetyksi, että poliisin K-palvelimiksi nimeämät fyysiset palvelimet ja niistä ainakin palvelimet K1–K16 ovat liittyneet tai ainakin voineet liittyä Scanifin liiketoimintaan. Scanifin toiminnan tarkoituksena ja liikeideana on ollut internetin skannaukseen soveltuvan työkalun kehittäminen. Skannaustyökalua ei Kivimäen ja Naugtonin kertomusten mukaan saatu kehitettyä valmiiksi, mutta jollain tavoin toimiva, ilmeisesti Vanderpotin toimesta yhtiölle tullut työkalu, yhtiöllä on kuitenkin ollut Naughtonin mukaan hallussaan. Selvää kuitenkin on, että Kivimäenkin kertoma Scanifi LLC:n liiketoiminta-ajatus liittyy oleellisella tavalla nyt esillä olevaan rikosasiaan.

Kivimäki on riidattomasti maksanut K-sarjan palvelinten maksuja omalla luottokortillaan huhtikuusta 2020 lukien. Palvelimista K1–K16 ovat edellä kerrotulla tavalla liittyneet olennaisesti Scanifi LLC:n toimintaan. Sen sijaan K17-palvelimen liityntä Scanifin toimintaan on jäänyt epämääräisemmäksi, eikä sitä ollut yhdistetty Scanifin Kubernetes-klusteriin. Yhtiössä mukana ollut Naughton ei ole ollut tietoinen koko palvelimesta, eikä yhtiöllä toisaalta ollut hänen mukaansa ollut tuolloin edes tarvetta niin suurella tallennustilalla varustetulle palvelimelle. K17-palvelimella on myös ollut Scanifin toimintaan liittyneen sisällön asemesta Plex-multimediapalvelinohjelmisto, joka käyttäjätunnuksen ”ryanlopl” sekä ohjelmiston asetuksissa olleen sähköpostiosoitteen kivimaki@tuta.io perusteella on mitä suurimmalla todennäköisyydellä Kivimäen omaan henkilökohtaiseen ja lähipiirinsä käyttöön asentama. Lisäksi palvelimella on ollut väärinkirjoitettujen domain-nimien hyödyntämiseen tarkoitettu sähköpostilaatikko, jossa sähköpostien lähettäjänä on sähköpostisoitteen ryan@safe.im perusteella ollut Kivimäki. Safe.im on ollut Kivimäen omistama ja hallinnoima sähköpostipalvelin.

Käräjäoikeus katsoo edellä sekä tuomiossa aiemmin esitetyn tukevan johtopäätöstä siitä, että Kivimäki on käyttänyt myös K-palvelinten kokonaisuutta ja että K17-palvelin on ollut nimenomaan hänen hallinnassaan. Lisäksi käräjäoikeus katsoo, ettei Kivimäen ja Naughtonin Scanifin liiketoiminnasta kertoma sulje pois sitä mahdollisuutta, että syytteessä kuvatut rikokset on voitu tehdä Kivimäen toimesta Scanifin palvelimilla ja palvelimilla olleella skannaustyökalulla. Syytteessä kerrottujen rikosten tekotavassa ja Scanifin liiketoiminta-ajatuksessa on merkittäviä samankaltaisuuksia.

Onko Kivimäki käyttänyt SSH-avainta, jonka sormenjälki on ollut WI8-alkuinen

Asiassa on selvitetty, että WI8-alkuisen sormenjäljen jättänyt SSH-avain on ollut palvelinkokonaisuudessa pääkäyttäjätasoinen SSH-avain. P1- ja P2-palvelinten käynnistäminen on edellyttänyt sen käyttämistä ja se on ollut myös asian ratkaisemisen kannalta merkityksellisten P2-palvelimella sijainneiden virtuaalipalvelimien root- eli pääkäyttäjän SSH-avain.

Lähes kaikki Vastaamon ja sen potilaiden kiristämisen kannalta merkitykselliset toimenpiteet on tehty OPSVM-virtuaalipalvelimella, kun sille on oltu kirjautuneena ainoastaan WI8-alkuisen sormenjäljen jättäneellä

SSH-avaimella. Poikkeuksen tähän muodostaa hetki, jolloin OPSVM-palvelimelle on asennettu MySQL-ohjelmisto potilastietokannan käsittelyä varten. Tällöin kirjautuneena on ollut myös ml0-alkuisen sormenjäljen jättänyt SSH-avain, jolla on myös oltu kirjautuneena yksinään silloin, kun Vastaamon potilastietokannasta on luotu potilaskohtaisia tekstitiedostoja python-ohjelmointikielellä luodulla skriptillä. Kun potilastietokannasta luotuihin tekstitiedostoihin on tehty suomenkielentaitoa edellyttäneitä tekstihakuja, kirjautuneena on jälleen oltu WI8-alkuisen sormenjäljen jättäneellä SSH-avaimella lukuun ottamatta yhtä hakua, jonka oli tehty ml0-alkuisen sormenjäljen jättäneellä SSH-avaimella.

Syyttäjien mukaan nimenomaan Kivimäki on käyttänyt syytteessä kuvattujen tekojen aikana SSH-avainta, joka on jättänyt WI8-alkuisen sormenjäljen. Kivimäki on kiistänyt tämän ja kertonut, että SSH-avaimia käytettiin Scanifi LLC:ssä jaettuna siten, että samaa avainta käytti useampi käyttäjä. Näin ollen WI8-alkuisen sormenjäljen jättäneen SSH-avaimen käyttäminen ei hänen mielestään osoittanut sitä, että juuri hän on käyttänyt OPSVM-virtuaalipalvelinta rikosten tekoaikana.

Käräjäoikeus toteaa, että Kivimäen vastaus ja kertomus omasta suhteestaan WI8-avaimen käyttämisestä on muuttunut oikeudenkäynnin aikana. Hän on oikeudenkäynnin alussa kertonut käyttäneensä kyseistä avainta kertoen tosin, että kysymyksessä oli usean käyttäjän kesken jaettu avain. Lisäksi hän on todennut, että käyttäjien oikeuksia ja pääsyä palvelimille oli valvottu SSH-avainten asemesta WireGuard-ohjelmistolla.

Kivimäki on oikeudenkäynnin aikana myöhemmin muuttanut vastaustaan ja todennut, ettei olekaan varma siitä, onko hän itse käyttänyt WI8-alkuisen sormenjäljen jättänyttä SSH-avainta. Hän on lisäksi kertonut, ettei hän toisaalta myöskään tunnistaisi, mikäli hän olisikin sitä käyttänyt, koska tämä ei ole käyttäjälle tavallisesti näkyvä tieto.

Kivimäki on muuttanut käsitystään myös kirjallisesta todisteesta V12 oikeudenkäynnin aikana. Hän on oikeudenkäynnin alussa todennut, että kyseinen vpn-virtuaalipalvelimen WireGuard-ohjelmiston asetuksia sisältänyt tiedosto on sisältänyt kaikki WI8-avainta käyttäneet käyttäjät mukaan lukien hänet itsensä tunnuksella ”r”. Myöhemmin oikeudenkäynnin aikana Kivimäki on todennut, että koska hänelle kuuluva käyttäjätunnus ”r” on WireGuard-ohjelmiston asetuksissa vasta aivan loppupäässä niin sijaintinsa kuin IP-osoitteensakin viimeisen luvun perusteella, hän ei ole voinut olla kyseisen palvelimen omistaja eikä sen ylläpitäjä. Kivimäki on edelleen todennut, että WireGuard-asetusten listalla ensimmäisenä oleva käyttäjä, jonka IP-osoite on 192.168.3.77, on 20.10.2020 kirjautunut vpn-virtuaalikoneelle käyttäen WI8-alkuisen sormenjäljen jättänyttä avainta, joten tämä käyttäjä on myös ollut tämän SSH-avaimen käyttäjä.

Käräjäoikeus toteaa Kivimäen kertomuksen muuttumisen heikentävän sen uskottavuutta. Uskottavuutta heikentää erityisesti se, että kertomus on muuttunut nimenomaan sen jälkeen, kun WI8-avaimen keskeinen merkitys tapahtumakokonaisuudessa on alkanut selvitä.

Kivimäen kertomusta SSH-avainten jakamisesta heikentää myös todistajana kuullun Naughtonin kertomus siitä, että hänellä itsellään oli Scanifin palvelimia käyttäessään ollut oma henkilökohtainen SSH-avain, jota hän ei ollut jakanut kenenkään kanssa. Vaikka Naughton onkin nimenomaisesti todennut, ettei hän osaa sanoa mitään siitä, olivatko muut käyttäjät jakaneet SSH-avaimia, tukee hänen kertomuksensa sitä, että SSH-avaimet olivat olleet

Scanifissa henkilökohtaisia. Tätä johtopäätöstä tukee myös asiantuntijana kuullun Monosen kertomus siitä, että SSH-avaimia käytetään tarkoituksensa kannalta oikein, kun jokaisella käyttäjällä on oma avaimensa ja että avainten jakaminen on niiden käyttötarkoituksenkin kannalta ongelmallista.

Myös WI8-alkuisen sormenjäljen jättäneen SSH-avaimen johdonmukainen käyttö kohdissa 2 ja 3 kerrottujen rikosten tekoaikana puhuu vahvasti sen puolesta, että avainta on sanottuna aikana käyttänyt yksi ja sama käyttäjä. Kiristykseen ja potilastietojen levitykseen liittyvät toimenpiteet ovat olleet johdonmukaisia ja päämäärätietoisia. Toimenpiteitä on myös tehty juuri oikeassa järjestyksessä ajallisesti hyvinkin lähellä toisiaan. Ainoastaan tekokokonaisuuteen kuuluva MySQL-ohjelmiston asennus sekä tekstitiedostojen luominen Vastaamon potilastietokannasta on tehty käyttäen toista ml0-alkuisen sormenjäljen jättänyttä SSH-avainta. Tämä seikka puhuu vahvasti toisen mahdollisen tekijän puolesta tältä osin. Huomioon on tällöinkin otettava, että toimenpiteet on tehty kokonaan toista SSH-avainta käyttäen eikä tällöinkään kirjautuneena ole ollut kahta käyttäjää samalla WI8-avaimella.

Käräjäoikeus katsoo edellä esitetyn tukevan johtopäätöstä siitä, että Kivimäki on käyttänyt SSH-avainta, jonka sormenjälki on ollut WI8-alkuinen, ja ettei sanotun avaimen käyttö ole ollut Kivimäen kertomalla tavalla jaettua.

Onko Kivimäki käyttänyt Hyperoptic-nimisen teleoperaattorin IP-osoitetta 37.156.72.25

Arvioitaessa sitä, onko Kivimäki käyttänyt WI8-alkuisen sormenjäljen jättänyttä SSH-avainta, on merkityksellistä myös sen selvittäminen, onko Kivimäki käyttänyt teleoperaattori Hyperopticin IP-osoitetta 37.156.72.25.

Asiassa on selvitetty, että Kivimäki on muuttanut Barcelonasta Lontooseen kevään tai kesän 2020 aikana ja asunut Lontoossa tyttöystävänsä Khodykinan kanssa Horseferry Roadilla sijainneessa asunnossa yhdessä ystävänsä Ruhasen kanssa. Asunnossa on ollut Hyperopticin internetliittymä, joka teleoperaattorin asiakastietojen mukaan on rekisteröity Khodykinan nimellä ja jonka yhteyshenkilöksi (nominated person) on tilaajatiedoissa ilmoitettu ”Alex Kidimaki”. Kyseinen sopimus on sen todisteesta ilmenevien maksutietojen mukaan ollut voimassa ainakin toukokuusta 2020 kesäkuuhun 2021.

Kivimäki on myöntänyt oikeudenkäynnissä riidattomaksi sen, että hän on kesällä 2020 käyttänyt IP-osoitetta 37.156.72.25. Asiassa on myös esitetty esillä olevaan rikosasiaan liittymätöntä näyttöä siitä, miten ja milloin Kivimäki on käyttänyt tätä IP-osoitetta. Tämän näytön perusteella Kivimäki on ensinnäkin tehnyt sanotusta IP-osoitteesta toukokuussa 2020 varauksen hotelli Kämpiin ajalle 31.5–7.6.2020, julkaissut Spamclan-nimimerkillä 12.6.2020 kello 14:09:36 Ylilaudalla viestin, jonka otsikkona on ollut ”bentleyt”, ja rekisteröitynyt 15.6.2020 OnlyFans-palveluun ja tehnyt siellä palveluntarjoajille maksuja kesä–heinäkuussa 2020 itselleen kuuluneella Mastercard-luottokortilla. Myös todistajana kuultu Ruhanen on asiassa esitetyn selvityksen mukaan kesän 2020 aikana Horseferry Roadin asunnolla asuessaan käyttänyt ainakin verkkopankkiin kirjautuessaan IP-osoitetta 37.156.72.25. Asiassa on näin ollen näytetty, että IP-osoite 37.156.72.25 on ollut Horseferry Roadilla olleen internetliittymän IP-osoite.

Kiistäessään syyllistyneensä syytteessä kuvattuihin rikoksiin, Kivimäki on kuitenkin esittänyt, ettei IP-osoitteen 37.156.72.25 käyttämiselle tule antaa asiassa syyttäjien kertomaa merkitystä, sillä sitä ovat hänen mielestään pystyneet käyttämään muutkin henkilöt kuin hän. Lisäksi hän on kertonut eronneensa Khodykinasta ja muuttaneensa syyskuussa 2020 eli ennen

syytteessä kuvattujen rikosten tekoaikaa Abell Housessa sijainneeseen asuntoon, jossa oli ollut oma internet-liittymänsä. Tästä todisteena Kivimäki on esittänyt syyskuussa 2020 solmitun vuokrasopimuksen Abell Housen asunnosta. Kivimäki oli kertomansa mukaan myös hankkinut uuteen asuntoon tarvitsemansa staattisen liittymän. Sitä, millainen liittymä Horseferry Roadin asunnossa ylipäätään oli ollut, Kivimäki ei ole tiennyt. Hän on kuitenkin esittänyt, että liittymä olisi ollut dynaaminen eli vaihtuva.

Todistaja Ruhanen ei ole kertomansa mukaan havainnut Kivimäen väittämää eroa. Lisäksi hän on kertonut vastoin Kivimäen kertomusta myös siitä, että Kivimäki oli matkustanut loppuvuodesta 2020 Dubaihin yhdessä tyttöystävänsä Khodykinan kanssa. Lisäksi Ruhanen on kertonut, että Kivimäki oli hankkinut vara-asunnon vain omiin tarkoituksiinsa.

Käräjäoikeus toteaa, että Kivimäellä on ollut erittäin hyvä tietotekninen osaaminen. Hän on kertomansa mukaan käyttänyt muun muassa Mullvad-nimisen yrityksen VPN-palvelua ja K2-palvelintakin nimenomaan palvelimella olleen vpn-virtuaalipalvelimen vuoksi. Tähän nähden käräjäoikeus ei pidä uskottavana, etteikö Kivimäki olisi ollut tietoinen Horseferry Roadin asunnossa käytössä olleista tietoliikenneratkaisuista kuten siitä, minkälainen liittymä asunnossa on ollut – staattinen vai dynaaminen, miten liittymää on jaettu, kuka liittymän tilaaja on ollut ja kuka sitä on myös maksanut. Kivimäki on myös kuulemisessaan selvittänyt tarvettaan muuttumattomalle, staattiselle IP-numerolle sekä VPN:n käyttämiselle. Kivimäen oikeudenkäynnin aikana esittämää onkin leimannut se, että hän on häntä kuultaessa ja muutoinkin pyrkinyt viittaamaan siihen, mitä asiassa jo esitetty kirjallinen todistelu hänen käsityksensä mukaansa osoittaa tai on osoittamatta. Lisäksi hän on kertomustaan tai esittämäänsä muuttamalla pyrkinyt sovittamaan kertomuksensa muusta todistelusta ilmeneviin seikkoihin.

Syyttäjien väitettä siitä, että Kivimäki on käyttänyt IP-osoitetta 37.156.72.25 vielä väittämänsä muuton jälkeen ja kohdissa 2 ja 3 kuvattujen rikosten tekoaikana, ja että sanottu IP-osoite on ollut nimenomaan Horseferry Roadin asunnon IP-osoite, tukee lopulta myös se, että Kivimäen käyttäjätunnuksella ”r” on sanottua liittymää käyttämällä kirjauduttu K16-palvelimella olleelle GitLab-sovellukselle 9.10.2020. Lisäksi IP-osoitteesta 37.156.72.25 on kirjauduttu P2-palvelimen lähiverkkoon 9.10., 10.10., 14.10., 16.10., 18.10. ja 20.10.2020 sekä useita kertoja 23.10.2020 P2-palvelimella olleelle vpn-virtuaalipalvelimelle, jota palvelinta Kivimäki on muussa yhteydessä nimenomaan kertonut P2-palvelimella käyttäneensä. Viimeksi kerrotut yhteydet ovat lisäksi tapahtuneet WI8-alkuisen sormenjäljen jättänyttä SSH-avainta käyttämällä.

Käräjäoikeus katsoo edellä esitetyn tukevan johtopäätöstä siitä, että Kivimäki on käyttänyt Horseferry Roadille hankitun liittymän IP-osoitetta 37.156.72.25 myöntämäänsä enemmän ja ainakin vielä 23.10.2020, jolloin P2 palvelimelle olleelle vpn-virtuaalipalvelimelle myös on kirjauduttu WI8-alkuisen sormenjäljen jättänyttä SSH-avainta käyttämällä. Sen jälkeenkin Kivimäki on vielä 26.10.2020 käyttänyt IP-osoitetta 37.156.72.25 kirjautuessaan GitLab-ohjelmistoon. Väitteellä siitä, että sanottu liittymä olisi ollut dynaaminen eli aika ajoin vaihtuva, ei edellä kerrottu toukokuun ja lokakuun lopun 2020 välisen ajan jatkunut Kivimäen ja Ruhasen käyttö huomioon ottaen ole merkitystä. Uskottavaa ei ole, että joku muu kuin Kivimäki olisi sattumalta kirjautunut sanotusta IP-osoitteesta esimerkiksi P2-palvelimella olleelle vpn-virtuaalipalvelimelle WI8-alkuisen sormenjäljen jättänyttä SSH-avainta käyttämällä.

Onko Kivimäki käyttänyt espanjalaista IP-osoitetta 147.161.123.116

Kivimäki on kiistäessään syytteen vedonnut vielä siihen, että P2-palvelimen lähiverkkoon oli 22.10. ja 23.10.2020 välisenä aikana otettu yhteys espanjalaisesta IP-osoitteesta 147.161.123.116 ja että juuri tähän aikaan OPSVM-palvelimelle oli kirjauduttu WI8-alkuisen sormenjäljen jättäneellä SSH-avaimella. Kivimäki onkin pyytänyt oikeudenkäynnin aikana lisätutkinnan tekemistä sanotusta espanjalaisesta IP-osoitteesta, johon hän tuolloin kertomansa mukaan ei ollut liittynyt millään tavalla.

Kuten käräjäoikeuden tuomiossa on edellä jo todettu, on IP-osoite 147.161.123.116 kuulunut Espanjasta saatujen tietojen mukaan 21.8. ja 1.12.2020 välisenä aikana Silvana Novacovici -nimiselle henkilölle, jonka osoitteeksi on liittymäsopimukseen kirjattu CL Selva de Mar 12 3–1, 08019 Barcelona. Sanottu osoite on sama, jonka Kivimäki on 23.2.2020 ilmoittanut Espanjan viranomaisille rikosasian yhteydessä, ja jonka osoitteen on osoitteekseen ilmoittanut myös Daniel Adrian Fulgescu -niminen henkilö. Fulgesculla on saatujen tietojen mukaan ollut myös toinen osoite (Calle Gaziel 43), jossa puolestaan Kivimäki on väestötietojen mukaan riidattomasti asunut.

Käräjäoikeus katsoo edellä ja tuomiossa aiemmin esitetyn tukevan johtopäätöstä siitä, että Kivimäellä on ollut selvä liityntä myös espanjalaiseen IP-osoitteeseen 147.161.123.116, ja että hän tietotekniset taitonsa huomioon ottaen on mahdollisesti kyennyt käyttämään sitä Lontoostakin käsin. Se miten IP-osoitetta on käytetty, on kuitenkin jäänyt asiassa tarkemmin selvittämättä. IP-osoitteen 147.161.123.116 ja WI8-alkuisen sormenjäljen jättäneen SSH-avaimen samanaikainen käyttö ei siten sulje pois sitä, etteikö Kivimäki olisi voinut käyttää sanottua IP-osoitetta ja WI8-alkuista SSH-avainta.

Onko Keskusrikospoliisin valeosto päätynyt Kivimäen Revolut-tilille

Kuten tuomiossa on aiemmin kerrottu, Keskusrikospoliisi kävi Vastaamon kiristäjän kanssa sähköpostikirjeenvaihtoa 30.9.2020 jälkeen. Tässä kirjeenvaihdossa kiristäjä toimitti ohjeita bitcoinien hankkimisesta, ja sen jälkeen Keskusrikospoliisi teki kiristäjän Vastaamolle ilmoittamaan bitcoin-osoitteeseen 0,1 bitcoinin suuruisen maksun eli niin sanotun valeoston, jonka siirtymistä eteenpäin virtuaalivaluuttana se on ryhtynyt myöhemmin tutkimaan.

Asiassa kuultu Mäntymaa on tehnyt edellä kerrotun tutkinnan ja laatinut tutkinnasta virtuaalivaluutta-analyysin. Kivimäki on puolestaan pyytänyt edellä kerrotusta virtuaalivaluutta-analyysiin liittyvästä lisätutkinnasta oman asiantuntijalausuntonsa. Tämän lausunnon on laatinut Coinmotion Oy:n perustaja Henry Brade. Poliisin tekemää virtuaalivaluutta-analyysiä ja Braden asiantuntijalausuntoa on esitelty edellä tässä tuomiossa tarkemmin.

Poliisin virtuaalivaluutta-analyysi on tehty P3-palvelimen tietoteknisen tutkinnan sekä virtuaalivaluuttapalveluntarjoajille tehtyjen tiedonsaantipyyntöjen perusteella. Virtuaalivaluutta-analyysin johtopäätöksenä Mäntymaa on esittänyt, että Vastaamon kiristäjä on ensin siirtänyt Keskusrikospoliisin kiristäjän ilmoittamaan lompakkoon suorittaman 0,1 bitcoinin maksun tästä lompakosta SwapLab-palveluun, jossa bitcoinit on vaihdettu moneroiksi. Sen jälkeen monerot on siirretty Swaplab-palvelusta edelleen virtuaalivaluutta moneron lohkoketjuun yksityiselle osoitteelle (lompakolle). Yksityiseltä osoitteelta sama henkilö on siirtänyt monerot

Binancen tilille fuckfuckfuck@cs.email. Tällä tilillä monerot on vaihdettu takaisin bitcoineiksi ja siirretty edelleen Aleksanteri Kivimäen Revolut-pankissa olevalle tilille.

Mäntymaan mukaan on todennäköistä, että Kivimäki on hallinnut tosiasiallisesti Binancen tilejä anussucker@cs.email sekä fuckfuckfuck@cs.email. Käräjäoikeus toteaa tätä johtopäätöstä tukevan sen, että molemmat tilit on luotu 13.5.2020 vain 19 minuutin välein toisistaan. Anussucker-tiliin on lisäksi yritetty kirjautumisen yhteydessä lisätä John Frisberg -nimisen henkilön henkilöllisyystodistus, mutta palvelu ei ole todistusta hyväksynyt. Samalla henkilöllisyystodistuksella on kuitenkin kirjauduttu 21.9.2017 Coinbase-palveluun, ja kyseiselle tilille on Frisbergin henkilöllisyystodistuksen lisäksi kirjattu sähköpostiosoite coinbase@safe.im. Safe.im on Kivimäen hallinnoima sähköpostipalvelin ja tilin nimeäminen vastaa tapaa, jota Kivimäki on myöntämällään tavalla eri palveluissa käyttänyt.

Varojen siirtymistä koskevalla niin sanotulla poissuljennalla tehty johtopäätös on ollut Mäntymaan mukaan erittäin todennäköinen myös siksi, että varat ovat kulkeutuneet selkeää reittiä pitkin rikoksesta epäillyn käyttöön. Mikäli Monero-jäljityksessä olisi tehty virhe, on Mäntymaan mukaan käytännössä mahdotonta, että jäljityksessä olisi sattumalta päädytty juuri sen henkilön tilitapahtumiin, jota alkuperäisestä rikoksesta epäillään. Asiassa käytetty rahanpesun polku ja päätepiste on toistunut ainakin 28 siirrossa, ja sen vuoksi virheen mahdollisuus on olematon.

Asiantuntija Brade on lausunnossaan sinällään todennut, että poliisin virtuaalivaluutta-analyysissä on erinomaisesti jäljitetty yksityisen monero-lompakon kautta kulkenut kahden Binance-tilin välinen toistuva rahapolku. Brade on muutenkin ollut analyysistä pitkälti samaa mieltä kuin Mäntymaa. Hän on kuitenkin kiinnittänyt huomiota siirrettyjen varojen määrän muuttumiseen siirtojen aikana sekä epävarmuuteen, mihin varat ovat lopulta päätyneet. Tämän vuoksi hän on katsonut, että analyysi vain osoittaa, että Keskusrikospoliisin suorittama maksu on voinut siirtyä Binancen tilille. Analyysin lopputulos on hänen mukaansa kuitenkin epävarma.

Käräjäoikeus toteaa Mäntymaan antaneen analyysinsä tekemisessä siirtojen suorittamisen ajalliselle yhteydelle merkityksen, jota Brade on häntä kuultaessa arvostellut. Käräjäoikeus kuitenkin katsoo, että varojen siirtotoimenpiteiden ajallisten yhteyksien käyttäminen analyysissä on Mäntymaan toteamin tavoin olennainen osa rahanjäljitystyötä. Virtuaalivaluuttalompakoissa ja vaihtopalvelussa selvitetyt nopeassa ketjussa edenneet tapahtumat ovat ajallisesti olleet merkityksellisessä yhteydessä Kivimäen Revolut-tilille tulleisiin varoihin. Käräjäoikeus toteaa, että Braden tekemää johtopäätöstä heikentää se, ettei hänellä ole ollut omaa lausuntoa laatiessaan käytössään P2- ja P3-palvelimia koskevia raportteja.

Edellä esitetyn ja aiemmin tässä tuomiossa esitetyn perusteella käräjäoikeus katsoo näytetyksi, että Keskusrikospoliisin suorittama 0,1 bitcoinin valeosto on erittäin suurella todennäköisyydellä päätynyt Kivimäen Revolut-pankissa olleelle tilille.

Mäntymaan mukaan niin sanotun transaktiosormenjälkianalyysin perusteella kansalaisten kirityksessä käytetyn osoiteryppään siirrot on tehty todennäköisesti samalla bitcoin-lompakkosovelluksella kuin millä Vastaajan

kiristäjän tekemät siirrot on tehty. Vastaamon asiakkaiden osalta virtuaalivaluutta-analyysi on ollut oikeudenkäynnin aikana vielä kesken, joten sen osalta pidemmälle meneviä johtopäätöksiä ei voi tehdä.

Kivimäen riidattomien ja selvitettyjen toimien sekä kiristäjän toimien ajallinen yhteys

Asian ratkaisemisen kannalta merkityksellisiä ovat myös Kivimäen selvitettyjen ja osin myöntämien toimien sekä Vastaamon ja sen asiakkaiden kiristystoimien ajalliset yhteydet. Mitä loogisemmassa ja nopeammassa yhteydessä ne ovat toisiinsa, sitä enemmän ajalliset yhteydet tukevat syyttäjien syytettä. Käräjäoikeus toteaa tältä osin yhteenvetona seuraavan.

Kivimäki on myöntänyt käyttäneensä nimimerkkiä Spamclan osallistuessaan Vastaamon tietomurtoa koskevaan keskusteluun Ylilaudalla. Spamclan on käyttänyt 8.10.2020 kello 12:15:49 samaa Mullvadin osoiteavaruuden IP-osoitetta, josta on käyty bittiraha.fi-sivustolla edellisenä päivänä 7.10.2020 kello 20:21:06 eli sen jälkeen, kun Vastaamo on Keskusrikospoliisin toimesta lähettänyt kiristäjälle sähköpostia ja ennen kuin Vastaamon kiristäjä on ehdottanut 7.10.2020 kello 20:43:42 bittiraha.fi-palvelun käyttämistä. Tämä tukee johtopäätöstä siitä, että Spamclan eli Kivimäki on Vastaamon kiristäjä.

Vastaamolta on 14.10.2020 kello 0:28:19 ja 14:57:37 vaadittu maksua 24 tunnin kuluessa. Vastaamo ja kiristäjä ovat tämän jälkeen käyneet sähköpostikirjeenvaihtoa 14.10.2020 kello 16:35:30–16:45:37 välisenä aikana. Käräjäoikeus toteaa, että IP-osoitteesta 37.156.72.25 on käytetty 14.10.2020 klo 6:43:00 P2-palvelimen lähiverkkoa. Samana päivänä klo 15:44:53, 16:50:46, 18:51:46 ja 19:02:21 irc-palvelimelle on kirjauduttu SSH-avaimella, jonka sormenjälki on WI8-alkuinen. Tämä tukee johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä.

Kivimäki on myöntänyt käyttäneensä käyttäjätunnusta ”r” K16-palvelimella olleessa GitLab-sovelluksessa. Käräjäoikeus toteaa, että käyttäjätunnus ”r” on käyttänyt 9.10.2020 kello 13:27.32 GitLabia IP-osoitteesta 37.156.72.25. Myös P2-palvelimen lähiverkkoa on käytetty samana päivänä 9.10.2020 kello 15:17:01 IP-osoitteesta 37.156.72.25, jota Kivimäen on selvitetty käyttäneen. Samasta IP-osoitteesta on käytetty P2-palvelimen lähiverkkoa 16.10.2020 kello 11:05:00 ja heti tämän jälkeen klo 11:05:29 irc-palvelimelle on kirjauduttu SSH-avaimella, jonka sormenjälki on WI8-alkuinen. P2-palvelimen lähiverkkoa on käytetty uudelleen 16.10.2020 klo 14:55:00 IP-osoitteesta 37.156.72.25 ja heti tämän jälkeen klo 14:55:30 irc-palvelimelle on kirjauduttu SSH-avaimella, jonka sormenjälki on WI8-alkuinen. Nämä seikat tukevat johtopäätöstä siitä, että Kivimäki on käyttänyt kohdassa 2 kuvatun rikoksen tekoaikana P- ja K-palvelimia, IP-osoitetta 37.156.72.25 ja SSH-avainta, jonka sormenjälki on WI8-alkuinen.

SSH-avaimella, jonka sormenjälki on WI8-alkuinen, on kirjauduttu OPSVM-virtuaalipalvelimelle 19.10.2020 kello 22:10:28. Välittömästi tämän jälkeen klo 22:10:40–22:11:29 välisenä aikana OPSVM:llä olleisiin tiedostoihin on tehty nimi- ja avainsanahakuja, jotka ovat tuottaneet etu- ja sukunimellä nimetyn tiedoston sisällön. SSH-avaimella, jonka sormenjälki on WI8-alkuinen, on kirjauduttu puolestaan irc-palvelimelle 21.10.2020 kello 2:41:25. OPSVM-palvelimella on tehty samana päivänä klo 3:08:16–3:10:34 suomenkielentaitoa edellyttäneitä tiedostohakuja avainsanoilla ”pedof”, ”politii”, ”politiikas”, ”politiikass”, ”kansanedu”. Kiristäjä on julkaissut samaan aikaan potilastietoja Ylilaudalla 21.10.2020 kello 3:06:21–3:11:41 välisenä aikana. Käräjäoikeus toteaa näiden seikkojen tukevan johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä.

Kiristäjä on julkaissut Ylilaudalla viestin 21.10.2020 kello 4:20:43 ja kopio Ylilaudan viestiketjusta on lisätty Tor-verkon piilopalveluun 21.10.2020 kello 4:22. Pian tämän jälkeen eli 21.10.2020 kello 4:29:27 nimimerkki Spamclan on julkaissut Ylilaudalla viestin ”tuolla torilaudan puolella näyttäis olevan sama lanka pystyssä”. Tämäkin tukee johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä.

Ylilaudan viestiketjuun on lisätty apu- ja tyylitiedostot 21.10.2020 kello 5:18 ja 5:19. Heti edellä kerrotun jälkeen 21.10.2020 kello 5:20:50 ja 5:23:52 nimimerkki Spamclan on julkaissut Ylilaudalla viestit, jotka ovat sisältäneet linkin viestiketjun sisällön sisältävään piilopalveluun. Tämäkin tukee johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä.

SSH-avaimella, jonka sormenjälki on WI8-alkuinen, on kirjauduttu OPSVM-virtuaalipalvelimelle 21.10.2020 kello 17:23:15. Heti tämän jälkeen OPSVM-palvelimella ollutta tiedostoa on muokattu ja tiedostoihin on tehty suomenkielentaitoa vaatineita hakuja avainsanoilla ”kuul”, ”kuuluis” ja ”kuuluisa”. Samalla SSH-avaimella on kirjauduttu OPSVM-palvelimelle myös 22.10.2020 kello 11:51:32. Tämän jälkeen kaikkiin OPSVM-palvelimella olleisiin tiedostoihin on tehty hakuja osin suomenkielisillä avainsanoilla ”poliisi”, ”polamk”, ”poliisi.fi”, ”intermin” ja ”keskusta”. Myös edellä kerrottu tukee johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä.

WI8-avaimella on kirjauduttu OPSVM-palvelimelle jälleen 22.10.2020 klo 22:04:49. Pian tämän jälkeen kello 22:08:08–22:13:42 välisenä aikana vastaamo.tar -paketti on luotu OPSVM-palvelimella. Kiristäjäksi ilmoittautunut nimimerkki ransom_man on julkaissut 22.10.2020 kello 22 jälkeen Torilaudalla viestin, jossa hän kertoo julkaisseensa vastaamo.tar -paketin. OPSVM-palvelimella olleisiin tiedostoihin on puolestaan tehty 22.10.2020 kello 22:48:25 ja 22:48:33 hakuja avainsanalla ”poliisi.fi”. Nimimerkki ransom_man on julkaissut 22.10.2020 kello 22 jälkeen Torilaudalla poliisien sähköpostiosoitteita, ja nimimerkki Spamclan 22.10.2020 kello 22:50:34 Ylilaudalla viestin ”Lympri postas juuri listan vastaamon asiakkaina olleita poliiseja torilaudalle”. Käräjäoikeus katsoo näiden seikkojen tukevan johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä ja Vastaamon asiakkaiden henkilö- ja potilastietojen levittäjä.

Vastaamo.tar-paketin konfigurointivirheen ja P1-palvelimen verkkojohdon irrottamisen jälkeen 23.10.2020 Hyperopticin ip-osoitteesta 37.156.72.25 on kello 12:04:27 alkaen otettu useita WireGuard-yhteyksiä P2-palvelimella olleeseen vpn-virtuaalipalvelimeen. Sanotut yhteydet on otettu SSH-avaimella, jonka sormenjälki on WI8-alkuinen. Välittömästi näiden yhteyksien aikana OPSVM-palvelimen pääkäyttäjä on muun muassa poistanut vastaamo.tar-paketin palvelimelta (klo 12:14:18), selvittänyt, kuinka moni on ladannut vastaamo.tar-tiedostoa (kello 12:19:34), käynnistänyt Tor-verkon piilopalvelun uudelleen (kello 12:20:37), vaihtanut Hetznerin yhteyssähköpostin (kello 12:24:00), laittanut piilopalvelussa 300 potilastietoa uudelleen jakoon (kello 13:08:27), hakenut onnistuneesti merkkijonoa ”ryan” (kello 13:12:58) ja yrittänyt ottaa yhteyttä P1-palvelimeen (kello 13:14:13). OPSVM-virtuaalipalvelin on sammunut tai sammutettu 23.10.2020 klo 13:35:25. Tämän jälkeen P2-palvelin on siirretty K17-palvelimelle. Käräjäoikeus katsoo näidenkin seikkojen tukevan johtopäätöstä siitä, että Kivimäki on Vastaamon kiristäjä ja Vastaamon asiakkaiden henkilö- ja potilastietojen levittäjä. Ottaen lisäksi huomioon, että sanotut toimenpiteet on tehty vastaamo.tar-paketin konfigurointivirheen jälkeen ja että Vastaamon

asiakkaille on lähetetty kiristyssähköpostiviestit heti 24.10.2024, edellä kerrotut seikat tukevat ajallisen yhteytensäkin vuoksi myös sitä, että Kivimäki on ollut myös Vastaamon asiakkaiden kiristäjä.

Vastaamo.tar-paketin konfiguroinnissa tapahtuneen virheen merkitys

Kuten tuomiossa edellä on jo todettu, kiristäjällä on täytynyt olla kiristyssähköpostit lähettäessään hallussaan koko Vastaamon potilastietokanta. Viestien lähettämisessä käytetyn sähköpostipalvelimen niin sanotusta SES-lokista ja OPSVM-palvelimella olleesta fi_vastaamo.sql-tietokantadumpista nimittäin ilmenee, että kiristyssähköposteja on lähetetty myös sellaisille Vastaamon asiakkaille, joista ei ollut muodostettu tekstitiedostoa OPSVM-palvelimella. Tämän vuoksi näytön arvioinnissa on merkitystä myös sillä, onko vastaamo.tar-paketin konfiguroinnissa tapahtuneen virheen jälkeen joku ulkopuolinen taho voinut saada koko potilastietokannan lataamalla haltuunsa.

Tietoteknisessä tutkinnassa on selvitetty, että muun muassa potilastietokannan sisältänyt vastaamo.tar-paketti on ollut sen konfigurointivirheen jälkeen ladattavissa tunnin ja 41 minuutin ajan ja ettei yksikään tiedossa oleva toimija ole saanut ladattua koko potilastietokantaa haltuunsa. Keskusrikospoliisi oli ladannut vastaamo.tar-pakettia 2 megabitin sekuntinopeudella ja eräs kyberturvayhtiö 5 megabitin sekuntinopeudella, mutta kumpikaan niistä ei ollut saanut koko potilastietokantaa ladattua. Tor-verkkoasiantuntijana kuultu Nurmi on häntä oikeudenkäynnissä kuultaessa pitänyt edellä kerrottuja latausnopeuksia hyvinä ja sellaisina, jotka ylipäätään ovat Tor-verkossa mahdollisia. Sitä, että latausnopeutta olisi voinut kasvattaa esimerkiksi Tor-verkon välireititttimiä vähentämällä Nurmi on pitänyt teoriassa mahdollisena, mutta lopputulokseltaan epävarmana. Nurmi on vielä todennut olevan sinällään mahdollista, että lataus olisi voitu aloittaa eri kohdista tiedostoa ja näin onnistua lataamaan koko potilastietokanta. Käräjäoikeus pitää tätäkin vaihtoehtoa teoreettisena, koska OPSVM-virtuaalipalvelimella Tor-palvelinta ajaneessa nginx-nimisessä palvelimessa ei ole selvitetty olleen tällaista ominaisuutta.

Käräjäoikeus katsoo edellä kerrotun tukevan johtopäätöstä siitä, että kiristäjällä on täytynyt olla hallussaan koko Vastaamon potilastietokanta ja että Vastaamon asiakkaiden kiristäjä on ollut sama taho tai henkilö kuin Vastaamon kiristäjä.

Asiassa esitetyn näytön kokonaisarviointi

Käräjäoikeus toteaa, ettei yksikään asiassa esitetty todiste yksinään osoita, että Kivimäki olisi syyllistynyt syytteessä kuvattuihin rikoksiin. Toisaalta yksikään todiste ei myöskään poissulje Kivimäen syyllisyyttä. Näin ollen asiassa esitettyä todistelua on arvioitava vielä kokonaisuutena, ja tämän kokonaisarvion jälkeen tehtävä johtopäätös Kivimäen syyllisyydestä.

Käräjäoikeus toteaa, että syytteessä kerrotut rikokset on tehty palvelinkokonaisuudella ja erityisesti OPSVM-virtuaalipalvelimella, jota Kivimäen on selvitetty käyttäneen myöntämäänsä enemmän. Vastaamon potilastietokantaan on murtauduttu ja potilastietokanta kopioitu OPSVM-palvelinta käyttämällä. Potilastietokanta on siirretty OPSVM-palvelimelle ja palvelimella potilastietokantaa on myös käsitelty. Potilastietokannasta on muodostettu potilaskohtaiset tekstitiedostot, ja tekstitiedostoihin on tehty hakuja, jotka ovat osin vaatineet suomenkielentaitoa ja liittyneet Kivimäkeen itseensä tai hänen lähipiiriinsä taikka alueeseen, missä

Kivimäki on asunut. OPSVM-palvelimella on myös pystytetty ja ylläpidetty kiristyksessä ja potilastietojen julkaisemisessa käytettyä Tor-verkon piilopalvelinta.

Kivimäen on myös selvitetty käyttäneen rikoskokonaisuuden kannalta merkityksellisiksi nousseita sormenjäljeltään WI8-alkuista SSH-avainta sekä IP-osoitetta 37.156.72.25 tavalla, jonka hän on oikeudenkäynnissä kiistänyt. Kivimäen kertomus siitä, että sanottu SSH-avain olisi ollut jaettu eli että sitä olisi pystynyt käyttämään useampi käyttäjä, on asiassa esitetyn selvityksen perusteella epätodennäköinen. Epätodennäköisenä on pidettävä myös Kivimäen kertomusta siitä, että IP-osoite 37.156.72.25 olisi ollut dynaaminen eli vaihtuva ja ettei sen käyttäminen rikosten tekoaikana millään tavoin liittyisi häneen.

Syyttäjien syytettä tukee edellä kerrotun lisäksi se, että erityisesti palvelimet K1–K16 ovat liittyneet Scanifi LLC -nimisen yhtiön toimintaan. Yhtiön liiketoiminta-ajatus internetin skannaustyökalun kehittämisestä sekä skannaamalla havaittujen tietoturvaongelmien kaupallisesta hyödyntämisestä liittyy olennaisella tavalla tapaan, jolla esillä oleva rikoskokonaisuus on toteutettu. Kivimäki on ollut yksi Scanifin omistajista ja vastannut esitetyn selvityksen mukaan nimenomaan Scanifin liiketoiminnasta. K17-palvelin, jolta rikoksen tekemisessä käytetty OPSVM-palvelin on lopulta löydetty, on esitetyn selvityksen mukaan todennäköisesti ollut Kivimäen omaan käyttöön tarkoitettu palvelin.

Johtopäätöstä Kivimäen syyllisyydestä tukee myös se, että hän on julkaissut Spamclan-nimimerkillä Ylilaudalla Vastaamon tietomurtoon ja kiristykseen liittyneet viestit tarkoituksenmukaisessa, päämäärätietoisessa ja kiinteästi ajallisessa yhteydessä kiristäjän selvitettyjen toimien kanssa. Epäuskottavaa on, että Kivimäki olisi pystynyt julkaisemaan viestit tekemällään tavalla, jos hän olisi ollut rikoskokonaisuudesta ulkopuolinen ja saanut siitä tiedon vain Ylilautakeskustelusta tai esimerkiksi tiedotusvälineistä. Tältä osin merkittävää on myös, että rikokset on selvitetty tehdyn nimenomaan palvelimilla, joihin Kivimäellä on ollut kiinteä ja vahva liityntä niin Scanifin liiketoiminnan kuin käytettyjen IP-osoitteiden ja salausavaintenkin kautta.

Syyksilukemisen kannalta merkitystä on myös sillä, että Keskusrikospoliisiin tekemän valeoston on näytetty mitä suurimmalla todennäköisyydellä päätyneen Kivimäen Revolut-pankissa olleelle tilille.

Kaikki edellä kerrottu osoittaa, että Kivimäki on syyllistynyt syytteessä kuvattuihin rikoksiin. Kohdassa 1 Kivimäen syyllisyyttä tukee jossain määrin myös hänen aikaisempi vastaava rikollisuutensa sekä edellä tuomiossa jo esitetty osallistumisensa Hacker News -keskusteluun vuosina 2017 ja 2018. Se, että myös myös Vastaamon asiakkaiden kiristäjällä on täytynyt olla hallussaan koko Vastaamon potilastietokanta ja ettei kukaan henkilö tai taho ole vastaamo.tar-paketin konfigurointivirheen jälkeen todennäköisesti pystynyt lataamaan koko potilastietokantaa, tukee puolestaan sitä, että Kivimäki on syyllistynyt myös kohdissa 4 ja 5 kuvattuihin rikoksiin. Kohtien 4 ja 5 teoilla on ollut välitön ajallinen yhteys kohtien 2 ja 3 tekoihin.

Kivimäen kiistämistä on puolestaan horjuttanut se, että hänen kiistämisensä perusteet ja kertomuksensa on oikeudenkäynnin aikana muuttunut sitä mukaa, kun todistelu on edennyt. Kivimäki on selvästi pyrkinyt sovittamaan esittämänsä ja kertomansa asiassa esitettyyn todisteluun ja niihin seikkoihin, jotka ovat nousseet asian ratkaisemisen kannalta merkittäviksi.

Näytön arvioinnin lopputulos ja syyksilukeminen

Kohta 1

Rikoslain 38 luvun 8 §:n 1 momentin mukaan tietomurrosta tuomitaan se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan. Edelleen jos tietomurto tehdään muun muassa erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä.

Lain esitöiden mukaan (HE 94/1993 vp) tietomurron rangaistavuuden edellytyksenä olisi se, että tietomurrossa tunkeutuminen tapahtuu järjestelmän turvajärjestely murtamalla. Esimerkkinä turvajärjestelystä mainitaan käyttäjätunnus, joka tietojärjestelmään pyrkivän on osattava päästäkseen käsiksi järjestelmän tietoihin ja turvajärjestely olisi läpäistävä jollakin nimenomaisella toimella, mutta rikos täyttyisi heti, kun tunnistuskontrolli on läpäisty. Oikean käyttäjätunnuksen tiedoksisaantitapa olisi rikoksen täyttymisen kannalta merkityksetön. Oikeudettomasta tunkeutumisesta ei kuitenkaan ole kyse silloin, kun pääsyn hankkimiselle suojattuihin tietoihin tunnuksen avulla on tunnuksen haltijan lupa. Turvajärjestelyn läpäisemistapaa kuvataan murtamisena, jota on käytetty korostamaan juuri sitä, että läpäisyn on oltava luvatonta.

Porttiskannauksella pyritään hallituksen esityksessä todetulla tavalla selvittämään tietojärjestelmän eri tietoliikenneporteissa toimivia ohjelmia ja käyttöjärjestelmiä sekä niiden haavoittuvuutta käyttäen hyväksi tätä varten laadittua ohjelmaa. Porttiskannausohjelmalla on mahdollista järjestelmällisesti selvittää tietojärjestelmien aukkoja ja niiden mahdollisia heikkoja kohtia ja toimenpiteen avulla kyetään saamaan tietoja, jotka mahdollistavat luvattoman pääsyn kohteena olevaan järjestelmään. Ohjelmaa käyttämällä hankitun tiedon avulla voidaan siten laissa tarkoitetuin tavoin murtaa tietojärjestelmän turvajärjestelyt.

Esillä olevassa asiassa rikoksen toteuttamista varten on luotu räätälöity työkalu, skannattu internetiä ja etsitty sieltä haavoittuvuuksia, ja tämän jälkeen murtauduttu Vastaamon palvelimelle, josta on kopioitu potilastietokanta sen myöhäisempää käyttöä varten. Tekninen toteutus asiassa on yksityiskohtaisesti suunniteltu. Teossa on käytetty useita lähinnä laittomaan toimintaan tarkoitettuja palvelimia, eikä palvelimilla ole lähtökohtaisesti ollut muuta tarkoitusta. Kivimäki on lisäksi pyrkinyt pienentämään kiinnijäämisriskiä muun muassa salattuja yhteyksiä ja salausavaimia sekä osaltaan jopa peitenimiä käyttämällä. Hänen motiivinsa on ollut yksinomaan hyötyä tietomurrolla saadusta aineistosta taloudellisesti. Niillä Kivimäen vetoamilla seikoilla, ettei salasanaa ole tarvittu tai ettei kohteena nimenomaisesti ole ollut Vastaamo, taikka ettei Kivimäki ole tiennyt, mitä materiaalia hän on porttiskannauksella tullut saamaan, ei ole syyksilukemisen kannalta merkitystä.

Kivimäki on tunkeutunut oikeudettomasti Vastaamon tietojärjestelmään ja ladannut tietojärjestelmästä Vastaamon potilastietokannan käyttöönsä. Näin toimiessaan hän on syyllistynyt tietomurtoon, jota rikoksesta aiheutunut vahinko ja Vastaamon tarjoamien palveluiden laatu sekä teon yleisesti aiheuttama uhka tietoturvallisuudelle on pidettävä myös kokonaisuutena arvostellen pidettävä törkeänä. Kivimäki on siten syyllistynyt kohdassa 1 siihen törkeään tietomurtoon, josta hänelle on vaadittu rangaistusta.

Kohta 2

Kivimäki on lähettänyt Vastaamolle kiristysviestin ja vaatinut viestissään 40 bitcoinin suuruista maksua vastineeksi siitä, ettei hän julkaise hallussaan olleita potilastietokannassa olleita tietoja internetissä. Näin toimiessaan hän on pyrkinyt saamaan Psykoterapiakeskus Vastaamo Oy:n luopumaan erittäin arvokkaasta taloudellisesta edusta uhkaamalla julkaista hallussaan olleita erittäin arkaluonteisia henkilö- ja potilastietoja ja potilaiden käyntimerkintöjä, joihin hänelle ei ole ollut oikeutta. Koska tekoa on edellä kerrotun perusteella pidettävä myös kokonaisuutena arvostellen törkeänä, Kivimäki on kohdassa 2 syyllistynyt siihen törkeän kiristyksen yritykseen, josta hänelle on vaadittu rangaistusta.

Kohta 3

Kivimäki julkaissut internetissä yhteensä noin 33.000 Vastaamon potilastietokannassa olleen henkilön tiedot kolmessa eri erässä. Hän on aiheuttanut rikoksellaan suurta kärsimystä ja erityisen suurta vahinkoa, koska tiedot ovat olleet erityisen arkaluonteisia. Asianomistajien määrää sekä julkaistujen potilastietojen laatu huomioon ottaen rikosta on pidettävä myös kokonaisuutena arvostellen törkeänä. Tämän vuoksi Kivimäki on kohdassa 3 syyllistynyt niihin 9.231 törkeään yksityiselämää loukkaavaan tiedon levittämiseen, josta hänelle on vaadittu rangaistusta.

Kohdat 4 ja 5

Kivimäki on lähettänyt Vastaamon potilastietokannassa olleille henkilöille kiristysviestin, jossa hän on vaatinut näiltä 200 tai 500 euron suuruista maksua bitcoineina vastineeksi siitä, ettei heidän tietojaan julkaista internetissä. Viestin saaneista henkilöistä 20 on maksanut Kivimäen vaatiman maksun. Kivimäki on asianomistajia kiristäessään uhannut heitä vakavalla rikoksella, joka vaarantaisi heidän henkensä tai terveytensä, sekä käyttänyt hyväkseen asianomistajien heikkoutta tai muuten turvatonta tilaa. Asianomistajien määrä on ollut suuri ja osa heistä on jo ollut erityisen heikossa ja turvattomassa asemassa. Tämän vuoksi ja julkaistujen potilastietojen laatu huomioon ottaen rikoksia on pidettävä myös kokonaisuutena arvostellen törkeänä. Kivimäki on siten kohdassa 4 syyllistynyt niihin 20.745 törkeän kiristyksen yritykseen ja kohdassa 5 niihin 20 törkeään kiristykseen, joista hänelle on vaadittu rangaistusta.

Rangaistusseuraamus

Kivimäen syyksi on luettu törkeä tietomurto, törkeän kiristyksen yritys, 9.231 törkeää yksityiselämää loukkaavan tiedon levittämistä, 20.745 törkeän kiristyksen yritystä ja 20 törkeää kiristystä. Kohdissa 2 ja 4–5 hänen syykseen luetut rikokset huomioon ottaen teoista voidaan tuomita ainoastaan vankeusrangaistus.

Syyttäjät ovat vaatineet Kivimäelle seitsemän vuoden vankeusrangaistusta, joka on ankarin mahdollinen yhteinen vankeusrangaistus esillä olevassa asiassa.

Rikoslain 6 luvun 3 §:n 1 momentin mukaan rangaistusta määrättäessä on otettava huomioon kaikki lain mukaan rangaistuksen määrään ja lajiin vaikuttavat perusteet sekä rangaistuskäytännön yhtenäisyys. Luvun 4 §:n mukaan rangaistus on mitattava niin, että se on oikeudenmukaisessa suhteessa rikoksen vahingollisuuteen ja vaarallisuuteen, teon vaikuttimiin sekä rikoksesta ilmenevään muuhun tekijän syyllisyyteen. Yhteistä rangaistusta

useasta rikoksesta mitattaessa on rikoslain 7 luvun 5 §:n mukaan otettava lähtökohdaksi siitä rikoksesta tuomittava rangaistus, josta tuomioistuimen harkinnan mukaan olisi tuleva ankarin rangaistus, sekä mitattava rikoksista yhteinen rangaistus siten, että se on oikeudenmukaisessa suhteessa myös rikosten lukumäärään, vakavuuteen ja keskinäiseen yhteyteen.

Kivimäen rikosrekisterin osaotteelta ilmenee, että hänet on vuosina 2015 ja 2020 ehdolliseen vankeusrangaistukseen. Viimeksi mainitun tuomion ohessa on tuomittu oheisseuraamus. Vuonna 2015 kysymys on ollut samankaltaisesta verkkorikollisuudesta nyt esillä olevan asian kanssa.

Asianomistajia on tässä rikoskokonaisuudessa ollut poikkeuksellisen paljon. Kivimäen syyksiluetut rikokset ovat olleet erittäin vahingollisia, koska asia nomistajien hyvin arkaluonteisia tietoja on jaettu internetiin täysin asianomistajien heikosta tilasta piittaamatta. Asianomistajia on myös kiristetty uhkaamalla julkaista näitä tietoja. Rikoksia on pidettävä erityisen moitittavina, ja ne osoittavat Kivimäessä hyvin suurta syyllisyyttä. Rikokset ovat lisäksi olleet häikäilemättömiä, suunnitelmallisia, valmisteltuja ja niihin liittynyt harkittuja valmistelutoimia. Rikoksilla on tavoiteltu huomattavaa taloudellista hyötyä. Kivimäen syyksi kohdissa 2–5 luetut rikokset muodostavat myös ajallisen ja toiminnallisen kokonaisuuden. Edellä mainituilla seikoilla on tuomittavaa rangaistusta korottava vaikutus.

Käräjäoikeus katsoo, että rikosoikeudellisesti vakavimpana tekona Kivimäen syyksi luetuista rikoksista on pidettävä kohdassa 5 kuvattua tekoa, vaikka inhimillisesti arvioiden kohtien 3 ja 4 rikokset ovat olleet asianomistajien näkökulmasta vakavampina. Tekotapa ja Kivimäen erittäin piittaamaton suhtautuminen huomioon ottaen yksin kohdan 5 rikoksesta olisi tuomittava 3 vuoden 6 kuukauden mittainen vankeusrangaistus. Muut Kivimäen syyksi luetut rikokset korottavat rangaistusta yli kolmella vuodella, jolloin yhteisen vankeusrangaistuksen pituudeksi tulisi noin 6 vuotta 7 kuukautta. Pituutensa perusteella vankeusrangaistus voi tulla tuomittavaksi ainoastaan ehdottomana.

Rangaistuksen lieventäminen ja kohtuullistaminen

Kivimäki on vedonnut siihen, että hänen rangaistustaan mitattaessa otettaisiin lieventämisperusteina huomioon se, että hän on ryhtynyt sopimaan ehdollisista korvauksista asianomistajien kanssa ja että asia on saanut huomattavaa mediajulkisuutta. Edelleen Kivimäki on vedonnut siihen, että hän on ollut passinmyöntämiskiellossa vuosina 2020–2023 ja että hän on tutkintavankeuden aikana ollut eristettynä aina syyskuuhun 2023 saakka.

Rikoslain 6 luvun 6 §:n 3 kohdan mukaan rangaistuksen lieventämisperusteita ovat tekijän ja asianomistajan välillä saavutettu sovinto, tekijän muu pyrkimys estää tai poistaa rikoksensa vaikutuksia taikka hänen pyrkimyksensä edistää rikoksensa selvittämistä. Korkein oikeus on esimerkiksi ratkaisussaan KKO 2018:23 todennut, että rikoslain 6 luvun 6 §:n 3 kohdan mukaisen lieventämisperusteen soveltaminen ei edellytä tekijän oma-aloitteisuutta tai edes vapaaehtoisuutta. Tekijän suhtautumisella tekoonsa ja toiminnan oma-aloitteisuudella sekä korvauksen suorittamisen ajankohdalla on kuitenkin merkitystä lieventämisperusteen arvioinnissa.

Kivimäki on puolustajansa välityksin ryhtynyt pääkäsittelyn kuluessa sopimaan ehdollisista sovintosopimuksista tuhansien korvausvaatimuksia esittäneiden asianomistajien kanssa. Kivimäki on myös lähestynyt Vastaamon konkurssipesää sovintoneuvotteluiden aloittamiseksi. Se, missä määrin tämä on ollut Kivimäen oma-aloitteisesta toiminnasta kiinni, on jäänyt jossain

määrin epäselväksi. Kivimäen pyrkimys sopia huomattavasta määrästä yksityisoikeudellisia vaatimuksia voidaan kuitenkin ottaa jossain määrin huomioon rangaistusta lieventävänä.

Rikoslain 6 luvun 7 §:n 1 kohdan mukaan rangaistusta lieventävänä seikkana on otettava huomioon tekijälle rikoksesta johtunut tai hänelle tuomiosta aiheutuva muu seuraus, jos vakiintuneen käytännön mukainen rangaistus johtaisi näistä syistä kohtuuttomaan tai poikkeuksellisen haitalliseen lopputulokseen. Lain esitöiden (HE 44/2002 vp) mukaan säännöksessä on kysymys moitearvosteluun kuulumattomista kohtuusperusteista, joissa rikoksen vakavuuden tai tekijän syyllisyyden arvottamisen sijasta paino on tekijälle tuomittavan seuraamuksen vaikutusten arvioimisessa, tarvittaessa sen kohtuullistamisessa ja tarpeettomien haittojen välttämisessä. Myös epävirallinen seuraus, kuten rikoksen saama poikkeuksellinen julkisuus, kuuluu säännöksen piiriin.

Lain esitöiden mukaan edellä kerrottu lainkohta on tarkoitettu poikkeussäännökseksi, eikä säännönmukainen mediajulkisuus itsessään vielä riitä lievennyksen perustaksi. Jos julkisuus nousee kohtuuttomiin mittasuhteisiin ja jos sillä on muita vakavia seuraamuksia tuomitun ja usein jo epäillyn elämään, kyseiset seuraukset voidaan ottaa kohtuuden mukaan huomioon rangaistusta määrättäessä. Kelvatakseen lieventämisperusteeksi sanktiokumulaation tulee olla keskimääräistä huomattavasti tuntuvampaa. Normaalit lisäseuraamukset eivät yleensä oikeuta soveltamaan säännöstä (HE 44/2002 vp).

Kivimäen rikoksiin on kohdistunut huomattavaa mediajulkisuutta, ja tapaus on ollut esillä niin valtakunnallisissa kotimaisissa medioissa kuin myös ulkomaisissa tiedotusvälineissä. Toisaalta Kivimäki on myös itse esiintynyt ja pyrkinyt esiintymään julkisuudessa. Ottaen tämän lisäksi huomioon rikosten poikkeuksellisen vakava luonne sekä niistä aiheutuneiden seurausten vakavuus, tapauksen saamaa julkisuutta ei kuitenkaan näissä olosuhteissa voida pitää laadultaan tai laajuudeltaan poikkeuksellisena, odottamattomana taikka mitenkään epäasiallisena. Edellä lausutut seikat huomioon ottaen asian saamasta julkisuudesta ei ole näytetty aiheutuneen Kivimäelle sellaisia tosiasiallisia kielteisiä seurauksia, jotka tulisi kohtuuden mukaan ottaa huomioon rangaistusta määrättäessä.

Edelleen selvää on, että vapaudenmenetys aiheuttaa kohteelleen aina jonkinasteista haittaa. Kivimäki on ollut tutkintavankeudessa, jossa hänelle on määrätty vaikeuttamisvaaran vuoksi yhteydenpidonrajoitukset, jotka on myöhemmin poistettu. Edelleen se, että Kivimäki ei tiettynä aikana ole saanut tai ettei hänelle ole myönnetty passia, ei ole sellainen peruste, jolla olisi merkitystä arvioitaessa rikoslain 6 luvun lieventämis- tai kohtuullistamisperusteita.

Edellä mainitut seikat huomioon ottaen käräjäoikeus arvioi oikeudenmukaiseksi rangaistukseksi Kivimäen syyksi luetuista rikoksista 6 vuotta 3 kuukautta vankeutta.

Menettämisseuraamus

Syyttäjät ovat vaatineet, että palvelimien P1–3, K1–15 ja K16–17 sisältämä data tuomitaan valtiolle menetetyksi. Syyttäjät ovat vedonneet siihen, että palvelimilla olevaa dataa on käytetty tahallisen rikoksen tekemisessä, että materiaalin hallussapito on laitonta ja että menettämisseuraamus on tarpeen myös uusien rikosten ehkäisemiseksi.

Kivimäki on vastustanut vaatimusta vedoten lähinnä siihen, että palvelimilla oli myös muille henkilöille kuin Kivimäelle kuuluvaa tai hänen omistamaansa dataa. Kivimäki ei ole yksilöinyt tarkemmin niitä henkilöitä taikka sellaista laillista dataa, joka kuuluisi muille kuin hänelle itselleen.

Rikoslain 10 luvun 4 §:n 2 momentin 1 kohdan mukaan valtiolle menetetyksi voidaan tuomita esine tai omaisuus, jota on käytetty tahallisen rikoksen tekemisessä. Edelleen edellä mainitun luvun 4 §:n 1 momentin 2 kohdan mukaan valtiolle menetetyksi on tuomittava rikoksen tekemisessä käytetty esine tai omaisuus, jonka hallussapito on rangaistavaa. Pykälän 3 momentin mukaan menetetyksi tuomitsemisen tarpeellisuutta harkittaessa on erityisesti kiinnitettävä huomiota uusien rikosten ehkäisemiseen. Säännöstä koskevien esitöiden (HE 80/2000 vp) mukaan menetetyksi tuomitsemisen tarpeellisuutta harkittaessa on arvioitava, onko esine ominaisuuksiltaan erityisen sovelias rikosten tekemiseen ja onko sillä ylipäätänsä mitään laillista käyttöä. Harkinnassa voidaan kiinnittää huomiota myös siihen, muodostaako esineen jättäminen juuri rikoksentekijän haltuun riskin sen käyttämisestä uudelleen rikoksen tekemisessä. Edelleen harkinnassa voidaan ottaa huomioon myös muut seikat kuin uusien rikosten ehkäiseminen.

Asiassa esitetty selvitys huomioon ottaen laittoman ja todennäköisesti rikollisin keinoin saadun materiaalin määrä edellä kerrotuilla palvelimilla on ollut huomattava. Toisaalta palvelimilla voi mahdollisesti olla myös jotakin sellaista dataa, jonka hallussapito ei ole kiellettyä tai jota ei ole saatu rikollisin keinoin. Kivimäki ei ole kuitenkaan lausunut menettämisseuraamuksesta edellä lausuttua enempää eikä hän ole yksilöinyt tarkemmin sitä dataa taikka niitä henkilöitä, joille kuuluvasta datasta voisi olla kysymys. Edellä lausuttu ja asian lopputulos huomioon ottaen takavarikoitujen palvelinten sisältämät tiedostot on tuomittava valtiolle menetetyksi.

Syyttäjät ovat lisäksi vaatineet, että Kivimäen hallusta takavarikoidut ja väärennetyt Amet Asan -nimellä ja Kivimäen kuvalla varustetut matkustusasiakirjat tuomitaan valtiolle menetetyiksi. Vastaaja Kivimäki ei ole vastustanut vaatimusta tältä osin. Edellä lausuttu huomioon ottaen edellä mainitut matkustusasiakirjat on tuomittava niin ikään valtiolle menetetyiksi.

Takavarikossa olevan muun omaisuuden palauttaminen

Syyttäjät ovat pyytäneet muun takavarikossa olevan omaisuuden osalta, että se palautetaan oikeille omistajilleen. Vastaaja ei ole kiistänyt sitä, etteikö omaisuus kuuluisi syyttäjien haastehakemuksessa ilmoittamille omistajille. Näin ollen omaisuus on palautettava niiden oikeille omistajilleen tuomiolauselmalta tarkemmin ilmenevällä tavalla.

Oikeudenkäyntikulut, puolustajien palkkiot ja korvausvelvollisuus valtiolle

Psykoterapiakeskus Vastaamo Oy:n konkurssipesän palkkiovaatimus

Psykoterapiakeskus Vastaamo Oy:n konkurssipesä on vaatinut oikeudenkäyntikulujensa korvaamista rikosasiassa yhteensä 28.308,23 eurolla. Konkurssipesän tuntiveloituksena on ollut 230 euroa tunnilta. Kivimäki ei ole lausunut konkurssipesän oikeudenkäyntikuluvaatimuksesta.

Konkurssipesän yksityisoikeudelliset vaatimukset on erotettu käsiteltäväksi eri oikeudenkäynnissä. Konkurssipesän oikeudenkäyntikululasku on liittynyt yksinomaan tämän rikosasian käsittelyyn. Asianajaja Haapamäen tuntilaskutus

on asianmukainen, ja laskusta ilmeneviä toimenpiteitä voidaan pitää rikosasian hoitamisen kannalta tarpeellisina. Asian lopputulos huomioon ottaen Kivimäki on velvoitettava suorittamaan konkurssipesälle sen oikeudenkäyntikulut.

Konkurssipesällä ei ole oikeutta vähentää laskuun sisältyvää arvonlisäveroa. Näin ollen Kivimäki velvoitetaan korvaamaan konkurssipesän oikeudenkäyntikululasku arvonlisäveroineen.

Puolustajille maksettavat palkkiot

Puolustajien laskut

Asianajaja Jaari on vaatinut laskussaan palkkionsa maksamista valmisteluistunnossa ja pääkäsittelyssä esiintymisen osalta 154,5 tunnin, pakkokeinokäsittelyissä esiintymisen osalta 23 tunnin, valmistautumisen osalta 619,5 tunnin, esitutkinnassa avustamisen osalta 52,5 tunnin ja jälkitoimien osalta 5 tunnin työmäärän perusteella. Jaari on myös vaatinut palkkion maksamista asianomistajien yksityisoikeudellisiin korvausvaatimuksiin ja niiden käsittelyyn liittyen yhteensä 73,5 tunnin työmäärän perusteella. Lisäksi Jaari on vaatinut korvaukseksi matkakuluista 492,54 euroa.

Jaari on vaatinut palkkionsa korottamista 20 prosentilla kaikkien toimenpiteiden osalta pois lukien 16.4.2024 pidetty pakkokeinokäsittely. Jaari on perustellut palkkion korottamista asian merkityksellä Kivimäelle sekä toisaalta asian vaativuudella.

Oikeustieteen maisteri Laurila on puolestaan vaatinut laskussaan palkkionsa maksamista pääkäsittelyssä esiintymisen osalta 111,75 tunnin, pakkokeinokäsittelyissä esiintymisen osalta 5,75 tunnin, valmistautumisen osalta 125,25 tunnin, esitutkinnassa avustamisen osalta 43,75 tunnin ja jälkitoimien osalta 2 tunnin työmäärän perusteella. Laurila on myös vaatinut palkkion maksamista asianomistajien yksityisoikeudellisiin korvausvaatimuksiin ja niiden käsittelyyn liittyen yhteensä 29,75 tunnin työmäärän perusteella. Lisäksi Laurila on vaatinut korvaukseksi matkakuluista 202,73 euroa.

Syyttäjien lausuma puolustajien laskuista

Syyttäjillä ei ole ollut huomautettavaa vaadituista matkakuluista, pääkäsittelytunneista taikka osallistumisesta kuulusteluihin. Syyttäjät ovat kuitenkin muutoin paljoksuneet puolustajien palkkiovaatimuksia.

Esitutkinnan pääpöytäkirja asiassa oli valmistunut 31.8.2023 ja loppulausuntoja asiassa oli pyydetty 2.10.2023 mennessä. Puolustus ei pyynnöstä huolimatta antanut loppulausuntoa tai esittänyt määräpäivään mennessä myöskään lisätutkintapyyntöjä, vaikka määräpäivään mennessä valmistelutoimenpiteitä oli laskun mukaan tuossa vaiheessa jo 182,25 tunnin edestä. Edelleen syytteeseen ei annettu pyydettyä ennakkovastausta, minkä lisäksi kirjallinen vastaus annettiin vasta puolustuksen asiaesittelyn jälkeen. Pääkäsittelyn aloittamiseen mennessä valmistelutoimenpiteitä oli laskun perusteella suoritettu kuitenkin jo 287,5 tunnin edestä. Tämä vastasi yli puolta kaikista valmistautumiseen käytetyistä työtunneista. Edelleen todisteiden teemoittelu esitettiin pääsääntöisesti vasta todisteiden nimeämisen tai osittain jopa todisteiden esittämisen jälkeen. Todisteista osa toimitettiin vasta juuri ennen niiden esittämistä ja joidenkin osalta vasta niiden esittämisen jälkeen, minkä lisäksi muutama todiste toimitettiin vasta syyttäjien loppulausunnon jälkeen. Edellä lausutut seikat huomioon ottaen työtunteja ei ole käytetty tarkoituksenmukaisesti prosessia sujuvoittaen, huolimatta siitä, että asia on

ollut luonteeltaan poikkeuksellinen ja teknisesti vaativa, eikä vaatimuksia yksin tuntimäärän perusteella sinänsä voida pitää kohtuuttomina.

Edellä lausutun perusteella syyttäjät ovat pitäneet kohtuullisina työtunteina asianajaja Jaarilta valmistumisen osalta 385 työtuntia ja pakkokeinojen osalta 44 työtuntia. Laurilan osalta syyttäjillä ei ole ollut huomautettavaa valmistautumisen osalta, mutta pakkokeinoihin käytettyjä tunteja syyttäjät ovat paljoksuneet 18,25 tunnin ylittäviltä osin.

Vielä syyttäjät ovat palkkion korottamista koskevan vaatimuksen osalta katsoneet, että vaikka pääkäsittely on sinänsä koskenut aihetta, jonka vuoksi oikeudenkäyntiä on voitu perustellusti luonnehtia vaativaksi, ei perustetta maksaa palkkiota kaikilta osin korotettuna ole . Arviolta 2/3 toimenpiteistä oli arvioitavissa vaativiksi. Edelleen laskussa ol i myös sellaisia toimenpiteitä kuten oikeuskäytännön selvittämistä (7,5 tuntia), median yhteydenottoja (1 tunti) sekä neuvotteluja Ranskaan, jotka eivät olleet erikseen korvattavia. Vielä asianomistajien korvausvaatimusten osalta syyttäjillä ei ollut mahdollisuuksia arvioida palkkiovaatimusten kohtuullisuutta ottaen huomioon se, ettei asianomistajien vaatimuksia ole käsittely rikosasian yhteydessä, eivätkä syyttäjät ole osallistuneet korvausvaatimuksia koskeviin sovintoneuvotteluihin.

Asianajaja Jaari on 28.3.2024 toimittanut käräjäoikeudelle lausumansa syyttäjien lausumasta.

Käräjäoikeus toteaa puolustajien laskuista seuravan.

Puolustaminen istunnoissa

Asiassa toimitettujen istuntojen kestot ilmenevät käräjäoikeuden pöytäkirjoista. Niiden mukaan pakkokeinoistunnot ovat kestäneet yhteensä 11 tuntia, valmisteluistunto 3 tuntia ja pääkäsittelyistunnot yhteensä 122,5 tuntia. Lounastunnilta ei oikeusavun palkkioperusteista annetun valtioneuvoston asetuksen mukaan makseta palkkiota.

Jaari on pöytäkirjojen mukaan esiintynyt pakkokeinoistunnoissa yhteensä 9,5 tuntia ja valmisteluistunnossa 3 tuntia sekä pääkäsittelyistunnoissa yhteensä 122,5 tuntia eli yhteensä 135 tuntia. Laurila on pöytäkirjojen mukaan esiintynyt pakkokeinoistunnoissa yhteensä 1,5 tuntia ja pääkäsittelyistunnoissa yhteensä 101 tuntia eli yhteensä 102,5 tuntia. Näin ollen heidän palkkionsa on istuntojen osalta maksettava näiden tuntien suuruisen työmäärän perusteella.

Esitutkinta ja valmistautuminen

Käräjäoikeudella ei ole syytä epäillä sitä, etteivätkö puolustajat olisi tehneet kaikkia laskuista ilmeneviä toimenpiteitä ja etteikö työtunteja olisi merkitty laskuihin oikein. Esitutkinnan osalta palkkio on asianmukainen kummankin puolustajan osalta ja siten hyväksyttävissä sellaisenaan. Valmistautumisen osalta kysymys on kuitenkin siitä, mitä voidaan pitää asian laatuun ja laajuuteen nähden kohtuullisena valmistautumisen määränä. Tältä osin käräjäoikeus toteaa seuraavan.

Esitutkinta-aineiston kokonaislaajuus asiassa on ollut huomattava. Vaikka syyttäjän kirjallinen todistelu on ollut mittavaa ja laajaa, on todistelutarkoituksessa kuultu vastaajan ja syyttäjän nimeäminä 12 henkilöä, joista kolmen syyttäjän nimeämän asiantuntijan osalta kertomusten ennakoitava keskeinen sisältö on dokumentoitu esitutkintaan liitettyihin raportteihin, jotka ovat olleet osa syyttäjän kirjallisia todisteita. Edelleen

todisteluteemaltaan suppeasti kuultujen Pursiaisen ja Ruhasen kertomukset on kirjattu kuulustelupöytäkirjaan. Vastaajan nimeämänä on lisäksi kuultu yhtä asiantuntijaa, ja tältäkin osin asiantuntijan kertomuksen ennakoitava keskeinen sisältö on dokumentoitu asiantuntijalausuntoon.

Laskuilla on toimenpiteitä, kuten yhteydenotot medialta, jotka eivät ole erikseen laskutettavia toimenpiteitä. Puolustaja ei voi myöskään erikseen laskuttaa perehtymisestään juridiikkaan, vaan sen hallitseminen kuuluu hänen ammattitaitoonsa vaikkakin vaikean juridiikan hallitseminen voi jutun laatuun ja juridiseen vaikeusasteeseen nähden tulla huomioiduksi valmistautumiseen käytetyn ajan osalta sitä korottaen.

Huomattavan määrän työtä ja siten valmistautumista ovat tässä asiassa vaatineet vaativat tietotekniset kysymykset ja niiden selvittäminen. Niissä vastaaja Kivimäki on myös itse ollut varsin aktiivinen. Puolustaja Jaari on ollut asiassa mukana heti Kivimäen kiinnijäämisestä lukien, minkä lisäksi Kivimäelle on myös määrätty asian laatuun ja laajuuteen nähden toinen puolustaja. Asiassa on myös asian laajuuden vuoksi pidetty valmisteluistunto, jonne puolustus ei pyynnöistä huolimatta toimittanut kirjallista vastausta taikka antanut lausumaa syyttäjien erikseen laatimista riitaisista taikka riidattomista kysymyksistä.

Asianomistajien korvausvaatimukset on erotettu käsiteltäväksi erikseen, ja niitä koskeva palkkio maksetaan valtion varoista niiden yhteydessä.

Edellä lausutut seikat, Jaarin päämiehen Kivimäen asema, asian laajuus ja sen vaatima työmäärä huomioon ottaen käräjäoikeus pitää kohtuullisena valmistautumisen määränä Jaarin osalta 500 tuntia ja Laurilan osalta 100 tuntia. Laurilan rooli Kivimäen toisena puolustajana on ollut asiassa huomattavasti vähäisempi. Edellä kerrottuja tuntimääriä ylittäviltä osin Jaarin ja Laurilan vaatimukset on hylättävä.

Matkakulut ja matka-aika

Oikeusavun palkkioperusteista annetun valtioneuvoston asetuksen 11 §:n 2 momentin mukaan korvausta matkakuluista maksetaan vain, jos avustajalle maksetaan tämän asetuksen mukaan palkkiota matka-ajalta.

Puolustajien laskuissa on vaadittu matkakulujen korvaamista, mutta Romeo-laskuissa tai niiden Excel-liitteissä ei ole kuitenkaan erittelyä matka-ajan osalta, eikä matka-aikaa ole niistä myöskään pääteltävissä. Näin ollen puolustajien vaatimukset matkakulujen osalta on hylättävä.

Jälkitoimet

Sekä asianajaja Jaari että oikeustieteen maisteri Laurila ovat vaatineet palkkiota jälkitoimien osalta yhteensä seitsemältä tunnilta. Sinänsä asiassa on asian laajuus huomioon ottaen oikeusavun palkkioperusteista annetun asetuksen mukaiset erityiset edellytykset maksaa palkkiota jälkitoimien osalta enemmän kuin yksi tunti. Laurilan puolustajanmääräys on kuitenkin päättynyt 12.4.2024, joten hänen osaltaan edellytyksiä palkkiolle jälkitoiminen osalta ei ole. Laurilan vaatimus on sen vuoksi tältä osin hylättävä. Asianajaja Jaarin osalta käräjäoikeus katsoo kohtuulliseksi korvaukseksi jälkitoiminen osalta hänen pyytämänsä 5 tuntia.

Palkkion korottaminen

Oikeusavun palkkioperusteista annetun asetuksen 8 §:n mukaan avustajan palkkiota korotetaan enintään 20 prosenttia muun ohella, jos tehtävä on poikkeuksellisen vaikea ja sen hoitaminen edellyttää erityistä asiantuntemusta, kokemusta ja ammattitaitoa tai avustajalla on tavallista tuntuvasti suurempi vastuu sen vuoksi, että kysymyksessä on huomattava taloudellinen etuus tai asialla muutoin on erityinen merkitys päämiehelle.

Käräjäoikeus on hyväksynyt valmistautumisen osalta asian laajuuteenkin nähden jo huomattava määrä työtä ottaen lähinnä huomioon asiaan liittyneet tietotekniset kysymykset. Tähän nähden asiassa ei ole perustetta hyväksyä vaatimusta korotuksesta sillä perusteella, että asian hoitaminen olisi edellyttänyt kaikkien toimien osalta erityistä asiantuntemusta.

Käräjäoikeus hyväksyy asianajaja Jaarin vaatimuksen korottamisesta ainoastaan valmistautumisen osalta yhteensä 150 tunnilta, joka käräjäoikeuden arvion mukaan vastaisi niitä toimenpiteitä, joiden osalta tehtävä on ollut poikkeuksellisen vaativa tai jossa asialla on muutoin ollut erityinen merkitys Kivimäelle.

Yhteenveto puolustajille maksettavista palkkiosta

Edellä lausuttu huomioon ottaen asianajaja Jaarin palkkio maksetaan istuntojen osalta yhteensä 135 tunnin, esitutkinnassa avustamisen osalta vaadittujen 52,5 tunnin, valmistautumisen osalta kohtuulliseksi harkitun 500 tunnin ja jälkitoimien osalta 5 tunnin työmäärän perusteella. Valmistautumiseen käytetyistä tunneista 150 tuntia maksetaan 20 prosentilla korotettuna.

Oikeustieteen maisteri Laurilalle maksetaan istuntojen osalta yhteensä 102,5 tunnin, esitutkinnassa avustamisen osalta vaadittujen 43,75 tunnin ja valmistautumisen osalta kohtuulliseksi harkitun 100 tunnin työmäärän perusteella.

Asianajaja Jaarille maksetaan siten palkkiona 79.475 euroa ja arvonlisäveron määränä 19.074 euroa. Oikeustieteen maisteri Laurilalle maksetaan palkkiona 27.087,50 euroa ja arvonlisäveron määränä 6.5501 euroa.

Käräjäoikeus on maksanut puolustajien välipalkkioina 15.1.2024 asianajaja Jaarille arvonlisäveroineen 49.600 euroa ja oikeustieteen maisteri Laurilalle 12.400 euroa. Välipalkkiot huomioon ottaen puolustajille nyt maksetusta kokonaispalkkiosta vähennetään välipalkkiolla maksetut määrät arvonlisäveroineen. Maksettavaksi tulee asianajaja Jaarille siten 39.475 euroa ja arvonlisäveron osuutena 9.474 euroa sekä oikeustieteen maisteri Laurilalle palkkiona 17.087,50 euroa ja arvonlisäveron osuutena 4.101 euroa.

Puolustajien palkkioiden korvaaminen valtiolle

Kivimäellä olisi käräjäoikeudelle toimitetun taloudellisen selvityksen mukaan oikeus oikeusoikeusapuun ilman omavastuuosuutta. Valtion varoista vastaajan puolustajille asianajaja Jaarille sekä oikeustieteen maisteri Laurilalle nyt maksettavat ja heille aikaisemmin välipalkkiona maksetut palkkiot jäävät siten oikeudenkäynnistä rikosasioissa annetun lain 2 luvun 11 §:n nojalla valtion vahingoksi.

Korvausvelvollisuus valtiolle

Kivimäki on velvollinen rikosuhrimaksusta annetun lain 2 ja 3 §:ien nojalla suorittamaan valtiolle rikosuhrimaksun.

Todistaja Pursiaista ja asiantuntija Bradea on kuultu Kivimäen nimeäminä. Näin ollen heille valtion varoista maksetut todistelukustannukset jäävät valtion vahingoksi. Todistajat Ruhanen ja Naughton ovat puolestaan olleet sekä syyttäjien että Kivimäen nimeämiä, ja näin ollen myös heille valtion varoista maksetut todistelukustannukset jäävät asiassa valtion vahingoksi.

Syyttäjän nimeämien todistajien Lähteenlahden ja Väänäsen kuulemiset ovat liittyneet riidattomiin seikkoihin. Edellä kerrottu huomioon ottaen todistajille valtion varoista maksetut palkkiot jäävät valtion vahingoksi.

Vangitsemisvaatimus

Koska Kivimäki tuomitaan huomattavasti yli kahden vuoden pituiseen vankeusrangaistukseen, hänet määrätään syyttäjien vaatimalla tavalla pidettäväksi edelleen vangittuna. Asiassa ei ole tullut esille mitään sellaista, että vangittuna pitäminen olisi myöskään kohtuutonta ottaen huomioon Kivimäen syyksi luettujen tekojen laatu, hänen ikänsä sekä muut hänen henkilökohtaiset olosuhteensa.

Lopputulos

Käräjäoikeuden ratkaisun lopputulos ilmenee oheiselta tuomiolauselmalta.

Ratkaisu on yksimielinen.

Vastaaja Aleksanteri Tomminpoika Kivimäki,

Syyksi luetut rikokset

1. Törkeä tietomurto
25.11.2018 - 26.11.2018
Rikoslaki 38 luku 8a § 1 / 1-2

2. Törkeän kiristyksen yritys
28.09.2020 - 23.10.2020
Rikoslaki 31 luku 4 § 2

3. 9231 törkeää yksityiselämää loukkaavaa tiedon levittämistä
21.10.2020 - 23.10.2020
Rikoslaki 24 luku 8a §

4. 20745 törkeän kiristyksen yritystä
24.10.2020
Rikoslaki 31 luku 4 § 1
Rikoslaki 5 luku 1§

5. 20 törkeää kiristystä
24.10.2020 - 26.10.2020
Rikoslaki 31 luku 4 § 1

Rangaistusseuraamukset

Yhteinen rangaistus
Syyksi luetut rikokset 1-5
6 vuotta 3 kuukautta vankeutta
Vapaudenmenetysaika 3.2.2023 - 5.2.2024 ja 24.2. - 29.4.2024

Muut rikosoikeudelliset seuraamukset

Laitteiden sisältämä data tuomitaan valtiolle menetetyksi seuraavasti:

- 2400/R/206/20/TVP/1 (P1-palvelin) kohdissa 2-11 laitteiden sisältämä data
- 2400/R/206/20/TVP/2 (P2-palvelin) kohdissa 2-3 laitteiden sisältämä data
- 2400/R/206/20/TVP/3 (K1-palvelin) kohdissa 2-3 laitteiden sisältämä data
- 2400/R/206/20/TVP/4 (K2-K15 -palvelimet) kohdissa 15-28 laitteiden sisältämä data
- 2400/R/206/20/TVP/6 (P3-palvelin) kohdissa 2-3 laitteiden sisältämä data
- 2400/R/206/20/TVP/8 (K16-K17 -palvelimet) kohdissa 1-17 laitteiden sisältämä data

Takavarikot 2400/R/206/20/TVP1-4, 6 ja 8 määrätään pidettäväksi voimassa, kunnes menettämisseuraamus pannaan täytäntöön tai asiasta toisin päätetään.

Amet Asan -nimellä olevat henkilökortti ja passi (kohdat 1 ja 2) tuomitaan valtiolle menetetyksi.

Takavarikko 2400/R/206/20/TVP12 määrätään pidettäväksi voimassa, kunnes menettämisseuraamus pannaan täytäntöön tai asiasta toisin päätetään.

Korvausvelvollisuus

Aleksanteri Tomminpoika Kivimäki velvoitetaan suorittamaan Psykoterapiakeskus Vastaamo Oy:n konkurssipesälle korvaukseksi oikeudenkäyntikuluista 28.308,23 euroa, mille määrälle on maksettava korkolain 4 §:n 1 momentin mukaista viivästyskorkoa kuukauden kuluttua tuomion antamispäivästä lukien.

Vastaaja Aleksanteri Tomminpoika Kivimäki määrätään suorittamaan valtiolle rikosuhrimaksu 80,00 euroa.
Laki rikosuhrimaksusta 2 §, 3 § ja 4 §

Valtion varoista maksetaan Kivimäen puolustajaksi määrätylle asianajaja Peter Jaarille 15.1.2024 maksettu välipalkkio huomioon ottaen palkkiona 39.475 euroa ja arvonlisäveron osuutena 9.474 euroa sekä oikeustieteen maisteri Laurilalle 15.1.2024 maksettu välipalkkio huomioon ottaen palkkiona 17.087,50 euroa ja arvonlisäveron määrä 4.101 euroa. Kivimäen taloudelliset olot huomioon ottaen valtion varoista puolustajille maksetut määrät jäävät valtion vahingoksi.

Muut lausunnot

Seuraavat takavarikot kumotaan ja takavarikoitu omaisuus määrätään palautettavaksi omistajilleen tuomion saatua lainvoiman seuraavasti:

- 2400/R/206/20/TVP/1 (P1-palvelin) kohta 1, omistaja on Hetzner Suomi
- 2400/R/206/20/TVP/2 (P2-palvelin) kohta 1, omistaja on Hetzner Suomi
- 2400/R/206/20/TVP/3 (K1-palvelin) kohta 1, omistaja on Hetzner Suomi
- 2400/R/206/20/TVP/4 (K2-K15 -palvelimet) kohdat 15-28, omistaja on Hetzner Suomi
- 2400/R/206/20/TVP/6 (P3-palvelin) kohta 1, omistaja on Hetzner Suomi
- 2400/R/206/20/TVP/8 (K16-K17 -palvelimet) kohdat 1-17, omistaja on Saksan poliisi (lunastanut Hetzner Saksalta)
- 2400/R/206/20/TVP/9 (Ranskassa takavarikoitu omaisuus) kohdat 2, 3, 4, 6 ja 7, omistaja on Aleksanteri Kivimäki
- 2400/R/206/20/TVP/10 (Iphone-puhelin) kohta 1, omistaja on Dinu
- 2400/R/206/20/TVP/11 (Kivimäen puhelimet) kohdat 1-2, omistaja on Aleksanteri Kivimäki

Pakkokeinolaki 7 luku 7 §, 17 § 2 momentti, 18 §, 20 § ja 23 §

Vastaaja määrätään pidettäväksi edelleen vangittuna. Hänet passitetaan vankilaan rangaistusta suorittamaan, jos hän tyytyy ratkaisuun tai muutoin siellä säilytettäväksi, kunnes rangaistuksen täytäntöönpano alkaa tai asiasta toisin määrätään. Passituspaikka: Vantaan vankila

Muutoksenhaku

Tähän ratkaisuun saa hakea muutosta valittamalla hovioikeuteen tai ennakkopäätösvalituksella korkeimmalta oikeudelta.

Lainvoimaisuus

Tuomio ei ole lainvoimainen.

Allekirjoitus

Laamanni Ilkka Lahtinen