2020 Finland Vastaamo data breach

Informatics Law
Student: Zehra Irem Kuyucu
Group: ITVfu-21

What was Vastaamo.fi?

- **Finnish private psychotherapy service provider founded in 2008.**
- **Vastaamo operated as a sub-contractor for Finland's public health system.**
- **It was a firm with twenty-five therapy centers throughout the Nordic country of 5.5 million people.**

The Data Breach

- **Ville Tapio, CEO of Vastaamo first heard from the cybercriminal on 28 September 2020.**
- **Immediately notified government authorities.**
- **Vastaamo received a ransom demand for 450,000 euros in Bitcoin.**
- **On 21 October 2020, Vastaamo announced that its confidential treatment records of approximately 36,000 psychotherapy patients and 400 employees had been compromised.**

Hello Finnish colleagues. We have hacked the psychothera...

OP No. 135981511 Oct 21, 2020, 6:05:13 AM (edited) +3

Hello Finnish colleagues.

We have hacked the psychotherapy clinic "vastaamo.fi" and taken tens of thousands of patient records including extremely sensitive session notes and social security numbers.

We requested a small payment of 40 bitcoins (nothing for a company with yearly revenues close to 20 million euros), but the CEO has stopped responding to our emails. We are now starting to gradually release their patient records, 100 entries every day.

You can view the data at http://3wnug3445ja7qj47.onion.pet/

Enjoy!

press contact: vastaamopress@tutanota.com

Extortion

- **As the company resisted to pay the ransom, the hacker published the therapist session notes of at least 300 patients, including politicians and police officers, on a public forum through the Tor network.**
- **The hacker approached victims of the security breach directly with extortion emails demanding ransoms.**

[MRS/MR] [FIRST NAME] [SURNAME] [MMDDYY-XXXZ]

As you probably already know from the news, we have broken into
the medical database of the medical records of the antitrust agency, we are contacting you because you are
you have used the therapy and/or psychiatric services provided by the Response Centre.

Because the management of this company has refused to take responsibility
for their own mistakes, we regret that we will have to ask you to pay
to keep your personal information safe.

Please follow the instructions below to send Bitcoins to our address.
If we receive €200 worth of Bitcoins within 24 hours,
your data will be permanently deleted from our servers.

If we do not receive this payment within 24 hours, you will still have
another 48 hours to acquire and send us €500 worth of Bitcoins.
If we still do not receive our money after this period, your details will be published
for all to see, including your name, address, phone number,
your social security number, as well as your detailed medical history which includes
including transcripts of your conversations with a therapist/psychiatrist at the Vastaamo.

The Full Leak Appears

vastaamo.tar	23-Oct-2020 02:01	10918912000

- **A 10 GB file containing private notes about 2,000 patients and their therapists had appeared on Tor.**
- **Patient information was stolen during two attacks. This first intrusion on Vastaamo's database took place in November 2018, and the systems were penetrated between the end of November 2018 and March 2019**

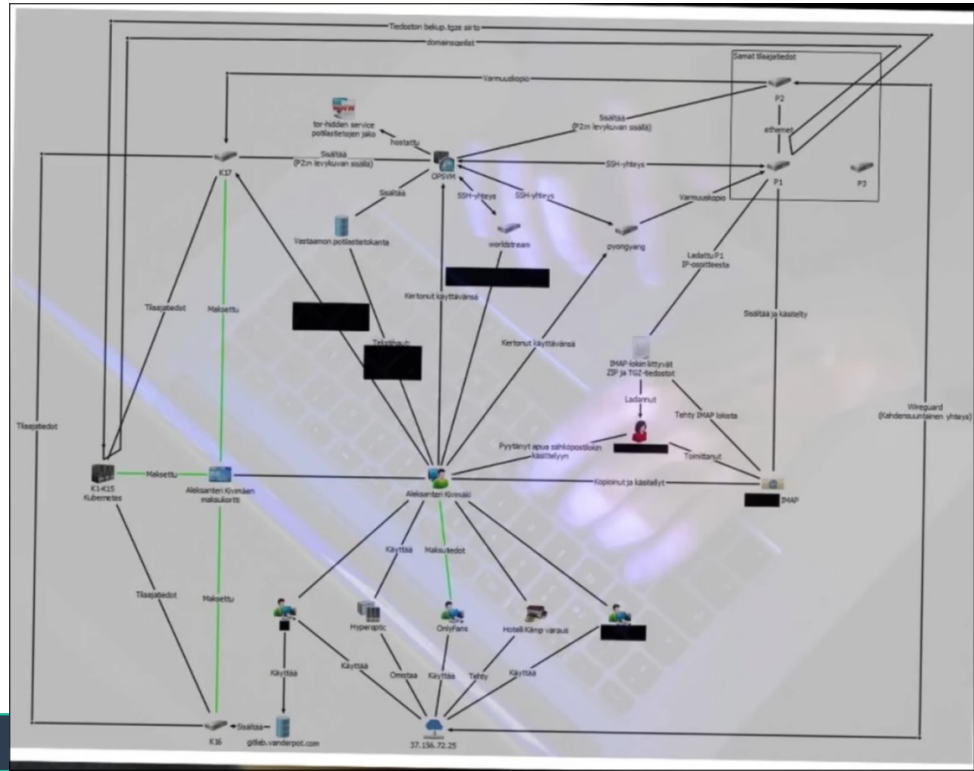
Operational Security Mistakes

- **The hacker accidentally archived his home directory using “tar”.**

ransom_man##HIbGCf 2020-10-23 (Pe) 15:xx:yy

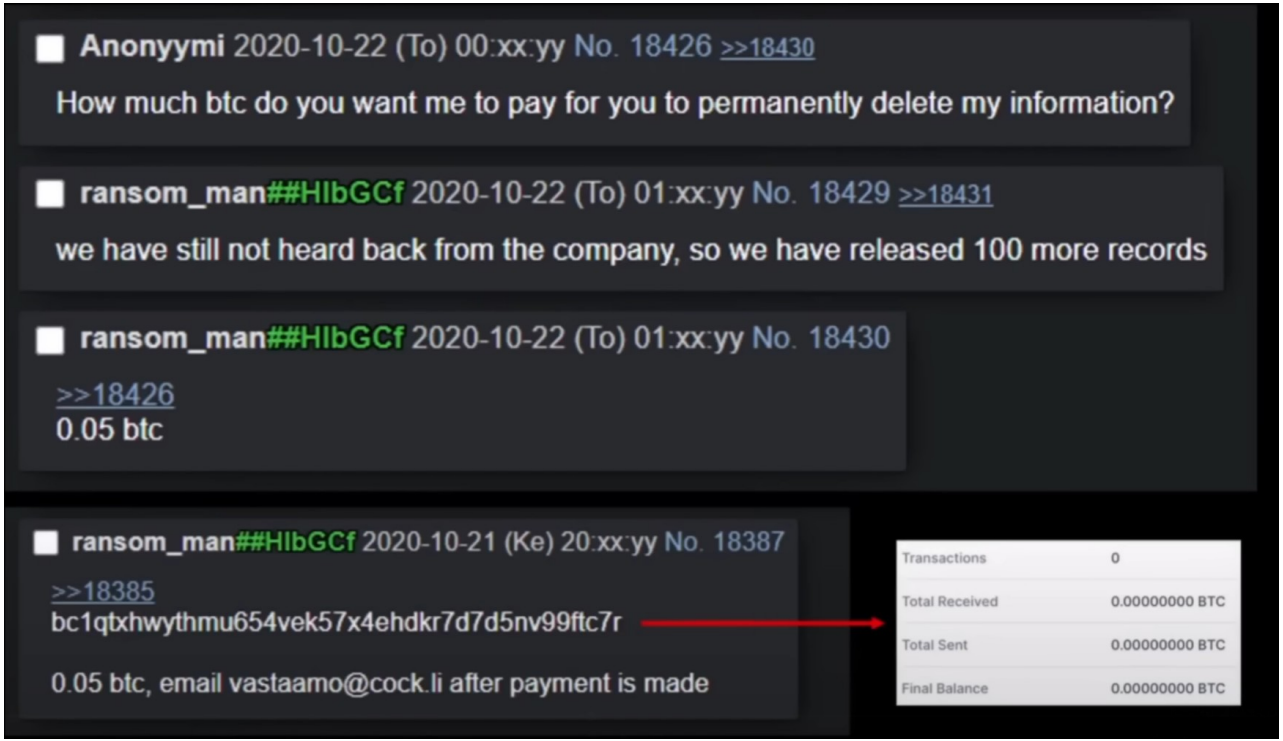
whoopsie :D

enjoy big tar



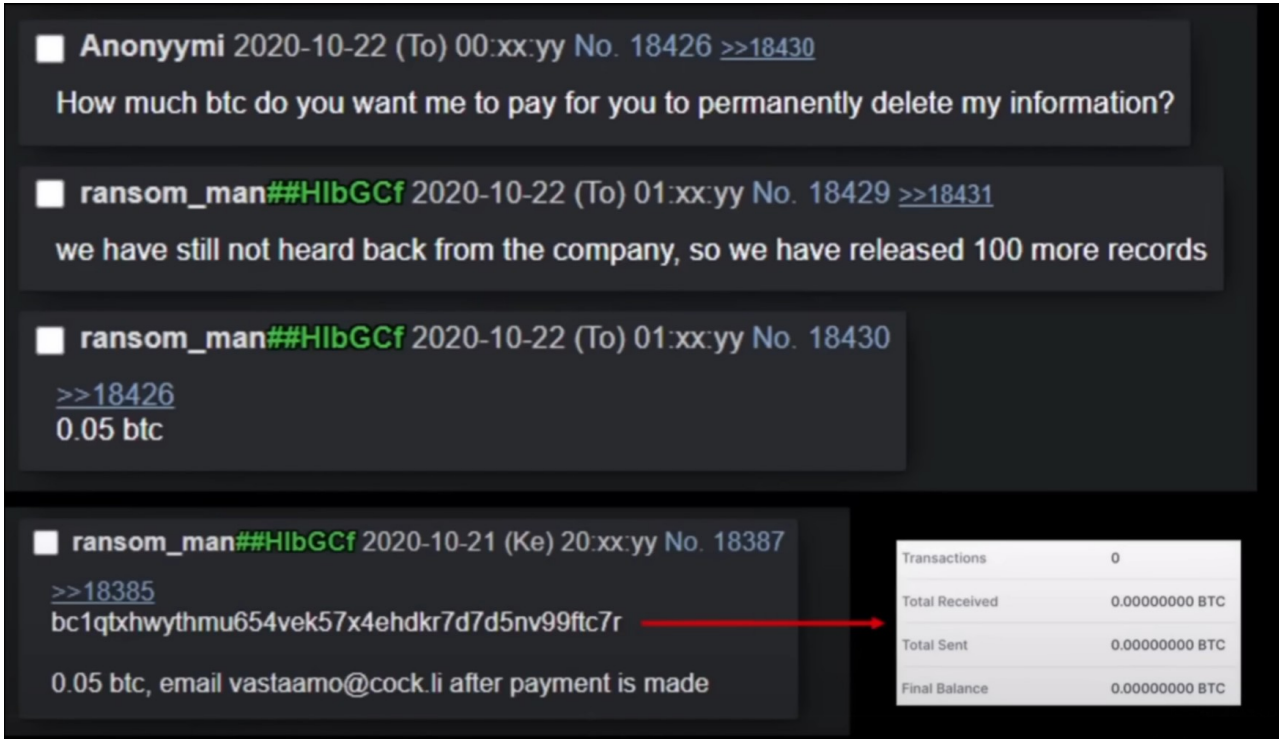
Correlating Bitcoin Payments

Should have used Monero!



Correlating Bitcoin Payments

Should have used Monero!



Legal Aftermath

- On October 28, 2022, the National Bureau of Investigation (NBI) named the suspect behind the breach as 25-year-old Aleksanteri Julius Kivimäki.
- Helsinki District Court remanded the Finnish man in absentia because of his suspected role in breaching Vastaamo, at the request of NBI.
- An arrest warrant was filed with Europol and Interpol against Kivimäki stating that he was in Dubai.

Legal Aftermath

Legal Aftermath

- **Kivimäki was arrested in France on 3 February 2023.**
- **In February 2023, he was extradited to Finland from France.**
- **The District Court of Länsi-Uusimaa has sentenced Kivimäki to six years and three months of unconditional imprisonment during his trial on 7 February 2024.**

Legal Aftermath

- **According to the court, Kivimäki committed more than 30,000 offences. He was charged with aggravated data breach, 9,231 counts of distribution of information infringing private life, 20,745 counts of attempted aggravated extortion, and 20 counts of aggravated extortion, blackmail, breach of confidentiality and falsification of evidence.**
- **Throughout the trial, Kivimäki denied committing any crimes. His defense criticized the investigation by the authorities and said the evidence presented in the case does not show his guilt.**

Legal Aftermath

- **Measured by the number of victims, the criminal case is the largest in Finnish history.**
- **He was sentenced to six years and three months in prison.**

What about Vastaamo.fi?

- **The company's security practices were found to be inadequate: the sensitive data was not encrypted and anonymized and the system root did not have a defined password.**
- **In December 2021, the Finnish Data Protection Authority (DPA) fined Vastaamo 608,000 euros for violating the provisions of the General Data Protection Regulation (GDPR).**

What about Vastaamo.fi?

- **PTK Midco, a holding company owned by Intera Partners, a Finnish private equity firm, which acquired a 70% stake in Vastaamo in May 2019. The company has asked for inquiry into acquisition and also requested that its acquisition of the company be cancelled and the purchase price be returned for failure to disclose hacking.**
- **Vastaamo was declared bankrupt by the decision of the Helsinki District Court in February 2021**

Sources

- Tietosuoja. (2022). Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations. Retrieved from https://tietosuoja.fi/en/-/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations
- Krebs, B. (2022). Hacker charged with extorting online psychotherapy service. Krebs on Security. Retrieved from https://krebsonsecurity.com/2022/11/hacker-charged-with-extorting-online-psychotherapy-service/
- The Guardian. (2023). Man accused of Finland psychotherapy hack charged with 21,000 counts of extortion. Retrieved from https://www.theguardian.com/world/2023/oct/18/man-accused-of-finland-psychotherapy-hack-charged-with-21000-counts-of-extortion
- Ralston, W. (2020). Finland's mental health data breach: What happened at Vastaamo? Wired. Retrieved from https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/
- Wikiwand. (n.d.). Vastaamo data breach. Retrieved from https://www.wikiwand.com/en/articles/Vastaamo_data_breach
- IS. (2022). Etsintäkuulutettu Julius Kivimäki kertoo elinoloistaan HS:lle: väittää omistavansa rahastoihin liittyvän yrityksen. Retrieved from https://www.is.fi/digitoday/art-2000009198343.html
- IS. (2024). Tällaisen tuomion Julius Kivimäki sai. Retrieved from https://www.is.fi/digitoday/art-2000010395492.html