# Excerpt from “If It's Smart, It's Vulnerable”

Mikko Hypponen

## CASE Vastaamo

The security breach at Vastaamo is one of the most important cases of my entire career, being unprecedented in its scope and cruelty. Although all the victims were within Finland's borders, the case is of international significance. It is also the largest case in Finnish criminal history, based on the number of reports to the police.

Vastaamo was a private psychotherapy provider established in 2008. Over the years, it grew into a center that employed 250 therapists, but something was forgotten: the patient database and its customer information were poorly protected.

In 2018, an unknown attacker found Vastaamo's patient database online and stole it. The database contained the personal information of 31,980 patients—their names, addresses, personal identity numbers, and email addresses. This included therapists' notes of discussions with patients. These notes covered the entire spectrum of life, some happy moments, but mainly sadness: depression, fear, marital issues, substance abuse, dependency, divorces, and fear of death. In therapy, people discuss matters they don't mention elsewhere. A therapist hears things that are never told to anyone else and notes down patients' opinions and thoughts of their nearest and dearest: children, spouses, sisters, brothers, and bosses. To make matters worse, some of the patients were children.

This type of health information is extremely sensitive for the rest of a person's life. Of course, health data and doctors' notes are always personal, but the fact that you had eczema or took medication for gout is only mildly embarrassing – especially if it happened 20 years ago. Things said in psychotherapy, however, can easily tear wounds open decades later.

This is what makes storing health information safely so difficult. How can we ensure that all public and private hospitals, health centers, and clinics will continue to protect their confidential data for years and for decades?

## Patient Registry

Vastaamo was unable to protect the data it was storing. Its data system had been developed in-house, storing patient data on a MySQL server that was on the public Internet for two years or longer.

Vastaamo's patient registry was so poorly protected that it was breached at least twice. The patient registry used for extortion had already been stolen in 2018, and the breach went unobserved. At least the later breach in March 2019 was noticed, having probably been orchestrated by someone who used a network scanning tool to find Vastaamo's systems. Scanners like these find poorly protected systems sooner or later. No substantial amount of information was stolen in the security breach of 2019, which was such a clumsy attempt that even Vastaamo noticed it, and patient databases were moved to a safer location. Vastaamo probably thought that it had survived with a bad scare, and no reports were made of patient data being jeopardized. Neither was the matter mentioned in June 2019, when a capital investment company bought a majority share in Vastaamo.

Everything collapsed on September 28, 2020. An attacker, calling himself Ransom_man, sent an email to key people at Vastaamo. He threatened to publish patient records online unless a ransom of 40 bitcoin was paid. At the time, this was worth around $500,000. Vastaamo contacted the police and negotiated

with the extortionist. Apparently, the management considered paying some form of ransom but could not agree on the matter.

The case became public on Wednesday, October 21, 2020. In the early hours of the morning, the attacker performed a series of actions, setting up a server on the Tor Hidden Service network and leaking patient data there. Next came a public message, left on three Finnish-language message boards: Ylilauta, Torilauta, and /r/suomi on Reddit. On Reddit, the attacker created the username /u/vastaamo. On Torilauta, the name ransom_man##HIbGCf was used. In this case, HIbGCf is a unique identifier (also known as a *flair*) that nobody else can use. It allowed anyone participating in the conversation to verify that the person claiming to be the attacker was genuine.

The extortionist wrote in English, briefly explaining the extortion attempt and that, as Vastaamo would not pay the ransom, the attacker would start releasing patient data. The attacker also provided the media with a personal email address, seeking maximum visibility for the case in order to put Vastaamo under pressure.

The email address was from tutanota.com and was quickly closed, forcing the attacker to switch to an anonymous address from cock.li. In addition, the attacker used the Protonmail service to send messages to Vastaamo and journalists.

## Technologies

All the technologies used by the attacker were designed to be unbreakable. The Tor network, Tor Hidden Service, anonymous email services, and bitcoin all protect their user. Tor Hidden Service is specifically designed to obscure the physical location of the network's servers. If the servers cannot be found, they

cannot be investigated, and information on them cannot be taken offline. Information on the Tor network is not as easy to find as on the regular Web, but Tor is fairly easy to use. The simplest way to enter the Tor network is to install the Tor Browser on your smartphone from the App Store or Google Play.

Both Reddit and Ylilauta quickly deleted the extortionist's messages, after which the conversation switched to Torilauta. Set up in 2017, Torilauta was a Finnish discussion board on the Tor network. Its topics focused on illegal narcotics, above all. Torilauta was designed for Finnish users and tried to keep foreign spammers out. Posting on Torilauta required passing a language test: you had to confirm each message by choosing Finnish sentences from a list of five randomly selected ones, some of which were in Finnish and others in Estonian. Although telling the difference between these languages is not obvious for a foreigner, the test was not 100 percent foolproof. However, it was one factor that aroused our suspicions regarding Ransom_man's nationality.

In his messages, Ransom_man wanted to project himself as a confident cybercriminal with an international gang routinely involved in this type of extortion, which had simply happened to pick on a psychotherapy clinic from Finland. True to his threats, Ransom_man leaked the therapy details of 100 new people every morning: 100 on Wednesday, 100 on Thursday, and 100 on Friday, by when details on 300 innocent Finns could be found online. Many Internet users actively refused to read the information leaked online, while others devoured it. The victims included celebrities and politicians, in addition to ordinary people.

The case immediately became massive news as an exceptional case of extortion on both the international and Finnish scene. To be clear, this was not a ransomware trojan but flat-out extortion:

the attacker had not encrypted the data but simply stolen it and had threatened to expose the information.

As time went on, however, the image of a confident career criminal began to crumble. Ransom_man started to make mistakes.

## Vastaamo.tar

On Friday morning, the third day of the leak, I was scheduled to comment on the breach on the Finnish TV channel MTV's morning news. Just before entering the studio, at around 7:20 a.m., I checked the latest situation. On the attacker's Tor site, I noticed a new file called vastaamo.tar (TAR is a file format like ZIP, an archive that contains other files). What caught my eye was the massive size of the file. Up to that point, the attacker had been sharing individual patient records, with sizes varying between 2 and 100 kilobytes. However, vastaamo.tar was huge, at 10.9 gigabytes or 10.9 million kilobytes. By the time I left the newsroom, the attacker's site had vanished. During my interview, he had switched off his server or disconnected it from the network.

The course of the events was revealed later on Friday. At 3 a.m., the attacker had placed a TAR file on his server to enable easy downloading of all 300 published patient records. Sometime during the night, however, he had mixed up two files called vastaamo.tar. One TAR file had 300 patient records in txt format, and the other had a backup of the contents of the server used by Ransom_man. This backup contained information the attacker absolutely did not want to publish: server usage logs, passwords, source codes—and the Vastaamo database in its entirety. The backup was online from around 3 a.m. until around 7:30 a.m.

The attacker later commented on his mistake on Torilauta with the post "Whoopsie. Enjoy big tar." For an extortionist, there is probably no greater mistake than accidentally releasing the files you are holding for ransom. The TAR file was so large that no one had time to download all of it before the server was shut down. On the Tor network, all transfers are purposefully routed through several servers, which makes them slow. However, several users managed to download parts of the file, the start of which contained the databases with the therapy records.

For the investigators, vastaamo.tar included several leads and usable evidence. This leak makes it more likely that Ransom_man will be found one day. However, the leak also indicated that Ransom_man had been fairly skilled at using various technologies to protect his privacy.

## Extortion Messages

Following the leak, Ransom_man panicked and decided to switch tactics. On Saturday evening, tens of thousands of Vastaamo's customers received an extortion message by email. In this message, written in perfect Finnish, the extortionist demanded that each victim pay 200 euros or see their records published. The message came with instructions on how to send the money in bitcoin. The extortionist also recommended using the Finnish service Bittiraha to pay the ransom. He had generated tens of thousands of individual bitcoin addresses, one for each victim, writing the following to his victims:

> *As you are probably aware from the news, we have breached Vastaamo's patient database and are contacting You as a recipient of Vastaamo's therapy and/or psychiatry services.*

*Since the management of this company has refused to take responsibility for its mistakes, we must to ask You to pay us to keep your personal data safe. Please follow the instructions below for sending bitcoins to our address. If we receive the equivalent of 200 euros in bitcoin within 24 hours, Your data will be permanently deleted from our servers.*
*If we do not receive this payment within 24 hours,*
*You have a further 48 hours to send us the equivalent of 500 euros in bitcoin. If we do not receive the money by then,*
*Your records will be published for everyone to see, including Your name, address, telephone number, personal identity number, and Your exact patient record including items such as transcriptions of Your discussions with the therapist/psychiatrist at Vastaamo.*

*Purchasing bitcoin: The Finnish "Bittiraha" provides an easy service allowing you to purchase bitcoin. Go to the address https://bittiraha.fi/osta and fill in your contact information. In the "total" field at the top, enter the amount of payment (€200 or €500). In the form's third field, "your bitcoin address", copy our address 9JeUqJXu3u3Shf2ArBMZfc232PvD. This address is only for Your personal use, do not share it with others unless they are making the payment for You.*

That weekend, tens of thousands of people wrestled with a difficult question. Should I pay the ransom? Will the extortionist follow through on his threat? Should I apply for a credit ban in case of identity theft? What if my personal identity number is leaked online?

The Finnish Police received more than 25,000 reports on the case. In terms of the number of victims, this is the largest

individual crime in Finnish history. It is hard to imagine a real-world crime with tens of thousands of victims—it is only possible online.

We tried to track the money as it was transferred to the extortionist. I made a public appeal to those who paid the ransom, asking them to give the bitcoin address where they had paid the money. I posted this message to Twitter:

> *Message to #Vastaamo data breach victims:*
> *We are collecting bitcoin addresses to which ransom money has been paid in the Vastaamo case. We are trying to trace where the money went. If you are a Vastaamo victim *and you paid the ransom*, I would appreciate it if you contacted me. My email address is in my profile.*
> *Thank you.*

About 100 victims reached out to me. One was a young woman whose email message stated that she felt scared to tell me that she had paid the ransom. Only a few days earlier, I had appeared on TV instructing people not to pay it. I wrote back and told her that she was brave to contact me and help trace the criminal, adding that I could easily understand why some people would pay the ransom despite being urged not to.

Surprisingly many people wanted to pay the ransom but had been unable to do so. Sending bitcoin is not simple for a first-timer. Bittiraha had also stopped some of the transfers at the request of the Finnish National Bureau of Investigation. In the end, the police probably had no authority to do this, but Bittiraha complied anyway.

In the end, I gathered 33 bitcoin addresses to which ransom money had been successfully paid. As the bitcoin blockchain is public, I could track the money's movements there. The

extortionist started transferring the money on October 29, 2020. A couple of days later, the criminal exchanged bitcoins for dollars at an underworld over-thecounter (OTC) money exchange service. The total amount was ridiculously small: this ruthless crime with so many victims netted the perpetrator just a few thousand dollars.

## The Hunt for the TAR File

The databases related to the Vastaamo case were evidence, but having them in your possession was ethically suspect and probably illegal. When investigating the case, we were hesitant about patient data. Not wanting the victims' therapy information on our computers, we did not dare to download files from Ransom_man's server. F-Secure's Head of IT Security also explicitly banned the saving of such information on the company's computers. In retrospect, it is easy to see that this was a mistake. When a case is active, you should compile all the evidence you can. Unnecessary and illegal information can be deleted later.

Once I realized that we did not have a copy of the TAR file the attacker had accidentally leaked, I saw that we had dropped the ball. Luckily, I received a partial copy from researchers at the IT security company Nixu, who had been commissioned to investigate the case. They sent us all the data they could. Customer and patient records cannot be shared under any circumstances, but sharing data related to the attacker was possible.

Once I saw how valuable the contents of the file were, I tried to find more of it. The longer someone had downloaded vastaamo.tar, the more evidence they would have. It might contain a vital clue that we could use to catch the attacker. I turned

to the general public and, exceptionally, made a request for help on the Ylilauta message board, the Finnish equivalent of 4chan:

*Good evening, this is Mikko Hypponen.*

*We are continuing to investigate the Vastaamo case, and I have a request:*

*On the morning of October 23, 2020, the extortionist "Ransom_man" inadvertently shared a large file named vastaamo.tar, which contained important evidence. The file also contained the patient records of tens of thousands of victims, which are uninteresting from an investigative standpoint. However, other data inside the TAR file (such as source codes, web addresses, etc.) could lead us to Ransom_man.*

*Our investigation does not have access to the entire file, only part of it. Vastaamo.tar was available for a few hours (approximately 03:00–07:30 am) on Ransom_man's Tor server on October 23, 2020. The file size was 10.92 GB (10,918,912,000 bytes).*

*In a discussion on Torilauta, someone said that they had downloaded the entire 10.92 GB file. Another person said they had downloaded 5.64 GB before the connection closed. It would be invaluable for the researchers to have such files. If you have a copy of the vastaamo.tar file with several gigabytes in size, please contact me. My email address is mikko.hypponen@f-secure.com. Wickr: mikkohypponen. I will submit the file to the authorities and I will protect your*

*identity. If you prefer, you can delete the patient records (the directory therapissed/patients) from the TAR file.*

The discussion lit up on Ylilauta. I received dozens of messages, and a few people indeed had copies of the TAR file, two of which was offered copies of. We never saw a full copy of the TAR file, and we are still looking for a larger version of the file.

I had nurtured the hope that the patient records would not be distributed any further, but I hoped in vain. Three months after the original leak, an unknown individual wrapped the 31,980 patient records stolen from Vastaamo in a single archive and sent it to Anonfiles, where anyone could download it.

## Innocent Victims

Unlike many security breaches, the users had done nothing wrong on this occasion. There was no way that Vastaamo's customers could have prevented the breach. The therapists at Vastaamo were also innocent; they, too, had done nothing wrong, being victims just like the patients. It must have been horrifying to realize that their notes were in the wrong hands.

As a sort of silver lining, at least the case dissipated some of the shame and stigma related to psychotherapy. Vastaamo was just one private clinic in Finland, but it had almost 1 percent of Finns as customers. Seeking help is nothing to be ashamed of. You should always see a professional when you are in pain, whether on your leg or in your mind.

We have seen ransomware trojan attacks on hospitals, but ransom demands have rarely been sent directly to patients; even then, the targets have usually been plastic surgery clinics, the threats being related to photographs taken before and after

surgery. Such cases are very unfortunate, but notes from psychotherapy sessions are on an entirely different level of sensitivity.

Vastaamo was also exceptional because the breach took down the entire company: the company declared bankruptcy three months after Ransom_man made the case public. This is rare, companies almost never go bankrupt for getting hacked, no matter how bad the hack was.

You should never kick people who are already down. Only cowards do that, and that is exactly what Ransom_man did. He caused immeasurable suffering to both patients and therapists, for just a few thousand dollars.

Before the Vastaamo case, I was often asked about the security of healthcare information. I would console people concerned about their data by saying that health information is not a key target for cybercriminals. Most criminals want to make money, which is easier to do with credit card and bank information than health information. Having your health records stolen feels worse than having your credit card number stolen, but criminals prefer the latter. Unfortunately, this is no longer true. We can only hope that this type of extortion does not catch on.

Vastaamo kept me busier than any other case had in years. My phone rang constantly, and I received hundreds of tips. When working a case like this, adrenaline levels rise, and the days grow long.

About two weeks into the Vastaamo case, I was a studio guest on the Finnish Broadcasting Company's Friday morning radio show. I told the story of the young woman who contacted me despite her fear of confessing that she had paid the ransom and found myself moved to tears on live radio. At this point, I realized that I might be rather tired. I kept my phone switched off for the weekend. The hunt for Ransom_man continues.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.
Translated from “Internet”, published in Finnish in 2021 by Werner Söderström. Translation to English by Mikko-Heikki Heinonen with Paul Anderson.
Audiobook produced by RBmedia / Ascent Media / Gildan Media. Narrated by Rich Miller.
German version published by Verlag Chemie Wiley-VCH GmbH.
ISBN: 978-1-119-89518-3
ISBN: 9781119895183
ISBN: 978-1-119-89518
ISBN: 978-3-527-51150-1 (de)
ISBN: 978-1-119-89519-0 (ebk)
ISBN: 978-1-119-89520-6 (ebook)
ISBN: 9781663720405 (abk)
ISBN: 978-1-663-72040-5 (audiobook)
ISBN-13: 978-1119895183
ISBN-10: 1119895189
ASIN: B0BG6CKB2V
ASIN: B0B544M8N4
ASIN: B0BG6BGH9B
Library of Congress Control Number: 2022936101