https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

Illustration: Mark Harris

William Ralston
Backchannel
May 4, 2021 7:00 AM

They Told Their Therapists Everything. Hackers Leaked It All

A mental health startup built its business on easy-to-use technology. Patients joined in droves. Then came a catastrophic data breach.

Jere woke up on the morning of October 24, 2020, expecting what Finnish college students call *normi päivä*, an ordinary day. It was a Saturday, and he'd slept in. The night before, he had gone drinking by the beach with some friends. They'd sipped cheap apple liqueur, listened to Billie Eilish on his boom box. Now Jere (pronounced "yeh-reh") needed to clear his head. He was supposed to spend this gray fall day on campus, finishing a group physics project about solar energy. The 22-year-old took a walk around the lake near his apartment outside Helsinki. Then, feeling somewhat refreshed, he jumped on the bus.

The day went quickly. Jere caught up with his friends, many of whom he hadn't seen since the pandemic began. They chatted about their Christmas plans, ordered pizzas from a favorite local spot, and knuckled down to work in the cafeteria.

At around 4 pm, Jere checked Snapchat. An email notification popped up on his screen. His hands began to shake. The subject line included his full name, his social security number, and the name of a clinic where he'd gotten mental health treatment as a teenager: Vastaamo. He didn't recognize the sender, but he knew what the email said before he opened it.

A few days earlier, Vastaamo had announced a catastrophic data breach. A security flaw in the company's IT systems had exposed its entire patient database to the open internet—not just email addresses and social security numbers, but the actual written notes that therapists had taken. A group of hackers, or one masquerading as many, had gotten hold of the data. The message in Jere's inbox was a ransom demand.

"If we receive €200 worth of Bitcoin within 24 hours, your information will be permanently deleted from our servers," the email said in Finnish. If Jere missed the first deadline, he'd have another 48 hours to fork over €500, or about $600. After that, "your information will be published for all to see."

Jere had first gone to Vastaamo when he was 16. He had dropped out of school and begun to self-harm, he says, and was consuming "extreme amounts" of Jägermeister each week. His girlfriend at the time insisted he get help; she believed it was the only way Jere would see his 18th birthday.

During his therapy sessions, Jere spoke about his abusive parents—how they forced him, when he was a young kid, to walk the nearly 4 miles home from school, or made him sleep out in the garden if he "was being a disappointment." He talked about using marijuana, LSD, DMT. He said he'd organized an illegal rave and was selling drugs. He said he'd thought about killing himself. After each session, Jere's therapist typed out his notes and uploaded them to Vastaamo's servers. "I was just being honest," Jere says. He had "no idea" that they were backing the information up digitally.

In the cafeteria, Jere grabbed his bag and told his friends he'd turn in his portion of the physics project the next day. On the bus ride home, he frantically texted his best friend to come over. Then his mother called; as the adult listed on his old account, she'd received the ransom note too. She and Jere were on good terms now, but if she got involved she might learn what he'd said in his sessions. Then, he says, he'd probably lose her from his life completely. He told his mother not to worry. That afternoon, he filed an online police report.

Jere poured himself a shot of vodka, then two or three more. He found his vape pen and took a Xanax, prescribed to him years earlier for anxiety. He'd stored a few pills in his bedroom drawer just in case, but he never believed he'd need them again. He passed out shortly after his friend arrived.

The next morning, Jere checked Twitter, where he was both horrified and relieved to learn that thousands of others had received the same threat. "Had I been one of the only people to get the mail, I would have been more scared," he says.

Vastaamo ran the largest network of private mental-health providers in Finland. In a country of just 5.5 million—about the same as the state of Minnesota—it was the "McDonald's of psychotherapy," one Finnish journalist told me. And because of that, the attack on the company rocked all of Finland. Around 30,000 people are believed to have received the ransom demand; some 25,000 reported it to the police. On October 29, a headline in the

Helsinki Times read: “Vastaamo Hacking Could Turn Into Largest Criminal Case in Finnish History.” That prediction seems to have come true.

If the scale of the attack was shocking, so was its cruelty. Not just because the records were so sensitive; not just because the attacker, or attackers, singled out patients like wounded animals; but also because, out of all the countries on earth, Finland should have been among the best able to prevent such a breach. Along with neighboring Estonia, it is widely considered a pioneer in digital health. Since the late 1990s, Finnish leaders have pursued the principle of “citizen-centered, seamless” care, backed up by investments in technology infrastructure. Today, every Finnish citizen has access to a highly secure service called Kanta, where they can browse their own treatment records and order prescriptions. Their health providers can use the system to coordinate care.

Vastaamo was a private company, but it seemed to operate in the same spirit of tech-enabled ease and accessibility: You booked a therapist with a few clicks, wait times were tolerable, and Finland’s Social Insurance Institution reimbursed a big chunk of the session fee (provided you had a diagnosed mental disorder). The company was run by Ville Tapio, a 39-year-old coder and entrepreneur with sharp eyebrows, slicked-back brown hair, and a heavy jawline. He’d cofounded the company with his parents. They pitched Vastaamo as a humble family-run enterprise committed to improving the mental health of all Finns.

For nearly a decade, the company went from success to success. Sure, some questioned the purity of Tapio’s motives; Kristian Wahlbeck, director of development at Finland’s oldest mental health nonprofit, says he was “a bit frowned-upon” and “perceived as too business-minded.” And yes, there were occasional stories about Vastaamo doing shady-seeming things, such as using Google ads to try to poach prospective patients from a university clinic, as the newspaper *Iltalehti* reported. But people kept signing up. Tapio was so confident in what he’d created that he spoke about taking his model overseas.

Before “the incident,” Tapio says, “Vastaamo produced a lot of social good.” Now he is an ex-CEO, and the company he founded is being sold for parts. “I’m so sad to see all the work done and the future opportunities suddenly go to waste,” he says. “The way it ended feels terrible, unnecessary, and unjustified.”

Tapio grew up in a “peaceful and green” neighborhood in northern Helsinki during a bad recession. His mother, Nina, was a trauma psychotherapist, and his father, Perttu, a priest. His grandparents gave him a used Commodore 64 when he was 10, which led him to an interest in coding. Something in his brain resonated with the logical challenge of it, he says. He also saw it as a “tool to build something real.”

The obsession endured: In middle school Tapio coded a statistics system for his basketball team, and in high school he worked for the Helsinki Education Department, showing teachers how to use their computers. Rather than going to college, he set up an online shop selling computer parts—his first business, funded with “a few tens of euros,” he says. A couple of years later, at age 20, he joined a small management consultancy.

The idea for Vastaamo came to Tapio when he was working with the Finnish Innovation Fund, a public foundation that invests in solutions to social and environmental problems. The fund sent him on a survey of health care systems in Western Europe. Being his mother’s son, he noticed that the Netherlands and other countries seemed to do a better job of providing mental health services than Finland did; the public system at home was known for patchy coverage and long wait times. Ever the coder, he wondered whether a web-based counseling service would help. It could sell vouchers to cities and towns, which could distribute the vouchers for free to residents. People could use the service anonymously. They wouldn’t have to worry about the stigma of seeking care, and they’d have access anytime, anyplace.

In 2009, the Finnish Innovation Fund backed Tapio’s idea with an initial grant of about $12,000. He and his parents used the money—along with more than $13,000 of their own savings—to start Vastaamo, Finnish for “a place where you get answers from.” Tapio registered the company as a social enterprise, meaning that the bulk of its profits would be poured back into its mission to improve mental health services. He would own around 60 percent, and most of the remainder would belong to his parents. Perttu would serve as CEO.

Clients could send a message to Vastaamo, and within 24 hours they’d get a personal response from a qualified therapist. (Wahlbeck, of the mental health nonprofit, notes that such services aren’t regulated by the government.) But counseling by internet “was not enough for customers,” Tapio says. Many of them needed access to in-person therapy.

One way to meet that need was to grow Vastaamo into a network of brick-and-mortar clinics. Tapio planned to digitize whatever he could, from bookings to invoices to medical records—everything but the appointment itself. The idea was that independent therapists would join Vastaamo to avoid dealing with their own administrative headaches. Freed by automation, they’d have more time to spend with clients (and rack up billable hours).

To deliver on this vision, Vastaamo needed an electronic medical record system, but Tapio didn’t like the options he found. Either the systems bristled with irrelevant features or they were too tightly tailored to a different area of medicine. The lack of good software, Tapio says, was one of the “main reasons” nobody had done what Vastaamo was about to attempt.

Rather than use an existing system, the company designed its own. It launched in late 2012, around the same time Vastaamo’s first in-person clinic opened, in the Malmi district of Helsinki. Tapio wouldn’t go into technical

detail about the system, but in court documents he suggests it was browser-based and stored patients' records on a MySQL server. More important for Vastaamo's purposes, the interface was easy to use. When therapists applied for a job at the company, they heard all about how much it would quicken their work.

But the slick exterior concealed deep vulnerabilities. Mikael Koivukangas, head of R&D at a Finnish medtech firm called Onesys Medical, points out that Vastaamo's system violated one of the "first principles of cybersecurity": It didn't anonymize the records. It didn't even encrypt them. The only thing protecting patients' confessions and confidences were a couple of firewalls and a server login screen. Anyone with experience in the field, Koivukangas says, could've helped Vastaamo design a safer system.

At the time, though, fears of a breach were far from Tapio's mind. The summer after Vastaamo's first clinic opened its doors, he took over as CEO and set the company on a path toward expansion.

In 2014 there was a change in the regulations around Vastaamo's business. The Finnish Parliament decided to split medical information systems into two categories. Class A systems would connect with Kanta, the national health data repository, so they'd need to meet strict security and interoperability standards. Anyone who planned to keep their patients' records in long-term electronic storage would have to use a Class A system.

Smaller organizations, the kind that kept vital records in manila envelopes and filing cabinets, would be allowed to use Class B systems. These weren't as tightly regulated, in part because they wouldn't make very interesting targets for a hacker. Class B operators would simply self-certify to the government that their setup met certain requirements. "The government" being, in this case, a single man—Antti Härkönen—whose purview includes all 280 Class B systems in Finland.

The new law gave Vastaamo several years to adopt a Class A system. The problem, Tapio says, is that the Finnish government hadn't specified how psychotherapy practices should format their data. Vastaamo could build a Class A system and plug into Kanta, but there was "no way to stop, for example, general practitioners at health care centers or occupational health physicians from accessing" therapy records, he says.

Outi Lehtokari, Kanta's head of services, pushes back against this claim. "Tapio might have misunderstood how Kanta works," she says. Patients can choose to restrict access to their information.

In any event, on June 29, 2017, Vastaamo registered a Class B system. As Tapio tells it, the company was eager to upgrade to Class A as soon as the government released formatting specs for psychotherapy. But that didn't happen. Instead, when the specs came out, Vastaamo kept on going with its Class B.

Tapio says that Finland's "supervisory authorities" then signed off on the system "numerous times" in the years ahead. Härkönen, who is one of those authorities, says that to monitor all the Class B systems carefully would be "mission impossible" for him. He adds, however, that there should be more "proactive inspections."

By 2018, Vastaamo was operating nearly 20 clinics and employing around 200 therapists and staff. By the end of 2019, annual revenue had risen to more than $18 million. The company drew the interest of Intera Partners, a Finnish private equity firm, which bought out the majority of Tapio's and his parents' stakes. Tapio took home nearly $4 million from the deal.

With each new clinic that opened, the original process repeated: Härkönen reviewed Vastaamo's self-certification and gave the thumbs-up. More patient data flowed into the MySQL server. And the reservoir behind the dam rose a little higher.

Tapio first heard from the hacker on September 28, 2020. The demand was 40 bitcoin, around half a million dollars at the time. The message came to him and a pair of developers he'd hired in 2015, Ilari Lind and Sami Keskinen. Lind was responsible for maintaining the company's IT systems, including its servers and firewalls; Keskinen was the data protection officer.

According to a statement Tapio made to Helsinki District Court, he immediately notified various government authorities, including the police. Lind sifted through Vastaamo's network traffic logs but reported finding no evidence of a hack. Tapio hired a security company called Nixu to investigate further. Two days later, Tuomas Kahri, COO of Intera Partners and chairman of the board of Vastaamo, sent an email to Tapio to thank him for his diligence in handling the breach. Kahri would later say that some of his own loved ones had been targeted in the attack.

In early October, Tapio got another shock. Keskinen and Lind called with a confession: Just before they'd joined Vastaamo, they had been arrested as part of a security breach at Tekes, the Finnish Funding Agency for Technology and Innovation. Lind had discovered that he could download Tekes' entire database, containing information on as many as 20,000 companies, by changing the URL on a funding application. He informed Tekes, which fixed the vulnerability—but he also notified Keskinen, who downloaded the database. There was a pretrial investigation for aggravated fraud, breach of confidentiality, and burglary, but the prosecution could not establish that Lind and Keskinen had used the database for financial gain.

Tapio says that if he had known about the two men's histories, he would never have hired them. (Keskinen and Lind declined to comment.) As it was, though, he had more pressing problems to worry about.

On the morning of Wednesday, October 21, the hacker posted a message on Ylilauta, an anonymous public discussion board. “We have attempted to negotiate with the Ville Tapio, the CEO of vastaamo, but he has stopped responding to our emails,” they wrote in English. Until they got their 40 bitcoin ransom, they were going to leak 100 patient records each day. The first batch was already up on a Tor server. Anyone who wanted to could go read them.

The hacker started emailing with Henrik Kärkkäinen, a reporter at the newspaper *Ilta-Sanomat*. To prove they were the real McCoy, they uploaded a file to the Tor server called “henrik.txt”—a snippet of their exchange. In emails to Kärkkäinen, the hacker scorned Vastaamo: A company with security practices that weak was the real criminal, he recalls them writing. They claimed to have been sitting on the stolen database for 18 months, unaware of its value.

When Ylilauta’s moderators removed the posts, the conversation migrated to Torilauta, a popular discussion forum on the dark web. The hacker took on a name: ransom_man. At least one desperate person offered to pay the full 40 bitcoin. Another wrote, in English, “I have discussed about very private things with my therapist and will literally kys myself if they are released.” They had their bitcoin ready: “I can send it in minutes, I’m constantly refreshing this page.” About 30 payments ended up going to the hacker’s Bitcoin wallet, according to Mikko Hyppönen, the chief research officer at F-Secure, a global cybersecurity company. It is unclear whether ransom_man actually deleted anyone’s information.

The hacker did follow through on another promise, however. On October 22, they leaked 100 more patient records. Some belonged to politicians and other public figures. They contained details about adulterous relationships, suicide attempts, pedophilic thoughts. The next batch came around 2 am the following morning. The hacker also put all the records they’d leaked so far into a single file called “Vastaamo.tar.”

And then something strange happened. Ransom_man replaced the first “Vastaamo.tar” with a much bigger one. It was 10.9 gigabytes—the entire leaked database. This file also contained a Python script that the hacker had used to organize the therapy records. The 10.9 GB upload seems to have been a mistake, because it disappeared in a matter of hours, along with the entire Tor server. Some speculated that Vastaamo had paid the 40 bitcoin, though company officials denied it.

One victim had their bitcoin ransom at the ready. “I can send it in minutes,” they wrote. “I’m constantly refreshing this page.”

Either way, ransom_man soon changed tactics and started extorting individual patients. This was unusual. Most of the time, cybercriminals go after institutions, according to Hyppönen. He knew of only one earlier instance of patients being singled out—in late 2019, after a breach at the Center for Facial Restoration in Miramar, Florida. (Since the Vastaamo attack, he adds, two other hacks have also targeted patients of plastic surgery clinics.) “Most attackers want money, and health care data is not directly monetizable,” Hyppönen says. But with real-world examples of the crime paying off, he adds, “it could become more common.”

Vastaamo reacted by offering patients a free counseling session. Therapy continued as normal. One patient says her therapist advised her to consider that not everything being said in the news was true. Some patients picked up a physical copy of their records, to learn what had been stolen, and others joined Facebook groups dedicated to victim support. Jere, however, opted not to; he wanted to minimize his online presence. He changed his phone number and purchased credit protection. He never seriously considered paying the hacker, he says, because “there was absolutely no guarantee they would obey” their own terms.

A Vastaamo clinic location in Turku.
Illustration: Mark Harris

On the Monday after the breach became public, Tapio went to Vastaamo headquarters in Helsinki. He’d been summoned there by Tuomas Kahri, the Intera COO who a month earlier had thanked him. Instead of speaking to Tapio face to face, Kahri had a consultant hand him a letter. It said that Tapio’s contract as CEO was terminated.

Hours later, the company announced Tapio’s dismissal. Shortly after that, in response to a legal motion filed by Intera, the Helsinki District Court ordered the temporary seizure of $11.7 million worth of the Tapio family’s assets—exactly what Intera had paid for its share of Vastaamo. Kahri declined several requests to comment on Intera’s claims, but they’re described in public (albeit redacted) court documents.

In its filings, Intera says it became aware of two previously unreported breaches at Vastaamo, in late 2018 and the spring of 2019. The second date fell shortly before the buyout went through. “Based on the information received so far, it is reasonable to assume that Ville Tapio was aware of the breach,” Intera argues. Not only that, but he “sought to conceal” it. Intera wanted to dissolve the transaction and reclaim the purchase price.

Tapio, as the defendant, submitted written testimony in rebuttal. He claims to have been blindsided by the news of the 2019 breach. The reason he didn't find out about it at the time, he writes, is that Keskinen and Lind—the "system architects"—never told him about it.

On the morning of March 15, Vastaamo's servers crashed and the patient database was replaced with a blackmail message. Tapio notified staff of the crash at 11:18 am, but no one appears to have discussed the possibility of a breach in either of the reports submitted to the government.

According to Tapio's testimony, Keskinen and Lind—who shared an administrator account—told him that the crash might have been caused by some minor adjustments they'd made shortly beforehand. But he says that Nixu, the cybersecurity company he hired in September, found something else: The shared account read the ransom message and deleted it.

In Tapio's version of events, then, whoever was using that account covered up the March breach. And the reason they did it, he contends, was to conceal a vulnerability they'd created themselves—one that had left Vastaamo's patient database "without firewall protection" for more than a year.

There were supposed to be three levels of security surrounding the database, Tapio tells me: one firewall at the network level, which blocked connections from the public internet; another around the individual server that stored the patient database; and the server configuration itself, which prevented connections from outside accounts. In November 2017, Lind spent a few hours configuring the server to allow remote access. Tapio believes that Lind and Keskinen wanted to be able to manage the server from offsite, and that instead of going to the trouble of setting up a VPN, they simply peeled back the firewalls.

"Those are two professionals that know much more about the network and firewall and server management than I," Tapio says. "I was not responsible."

Keskinen and Lind have not testified in the Intera case. They declined to comment on Tapio's numerous allegations. Until the dispute is resolved, the $11.7 million that Intera wants back—the fortune that Vastaamo built—will remain frozen.

In early January of this year, the Vastaamo patient database reappeared on at least 11 anonymous file-sharing services across the public internet. The file contained all the same records as before but was a fraction as big, so it spread easily. Without an accompanying message, the motivations for the upload are hard to discern—but it did appear fewer than 48 hours before Vastaamo's board was due to discuss the company's future. Was this a spiteful push to bring the

If so, then it was a success. On January 28, Vastaamo was put into liquidation, and it filed for bankruptcy two weeks later. In early March, its staff and services were transferred to Verve, a provider of occupational welfare services. The acquisition did not include Vastaamo's customer data, and Verve will use a Class A system.

Almost immediately after the hack happened, Parliament fast-tracked legislation that would allow victims like Jere to change their social security numbers in case of a serious breach. But patients were spooked, one counselor told the newspaper *Helsingin Sanomat*. "Not everyone who needed help may have sought treatment," he said. Some argue that therapists should never be able to enter session notes into Kanta; now more than ever, patients will not risk having their data travel beyond the consultation room.

In wider medicine, Koivukangas says, the Vastaamo scandal has highlighted the "unmet demand" for electronic medical record systems that are scalable, easy to use, and—crucially—secure. This is an area ripe for disruption, he says, and "prior to this breach, many thought with good reason that Vastaamo would've been one of those disruptors." Until the marketplace improves, he says, expect more bespoke solutions, and more breaches.

Unless ransom_man is caught and the Finnish authorities sort out everything that happened at Vastaamo, it will be impossible to know exactly how "the incident" began. Would it have happened, for example, if Finland had been more proactive in policing electronic medical systems? Or if Tapio had implemented a more secure system? What's clear is how it ended—in the most painful way possible for tens of thousands of patients. As more health care systems across the world go digital, the risk of that outcome rises.

"Being honest about my mental health turned out to be a bad idea," Jere says. He worries about identity theft, about some debt collection company calling him out of the blue and demanding tens of thousands of euros. He worries that his history of teenage alcoholism, so well documented on the web, will make it hard for him to find meaningful work as an adult. And he still worries that his mother may read his file one day. It's somewhere in the ether, accessible to anyone.

William Ralston *(@RalstonWilliam9)* is a writer based in London.