

“Covid-19 and its impact on the Security Posture in Healthcare”



Viesturs Bambans, CISSP, CHFI, CNDA, CEH
Ph.D. candidate.
Research Assistant, Visiting Lecturer
viesturs.bambans@va.lv
www.va.lv

CASE ANALYSIS «Psychotherapy Center Vastaamo»

Finland shocked by therapy center hacking, client blackmail

Finland's interior minister has summoned key Cabinet members into an emergency meeting Sunday after hundreds — and possibly thousands — of patient records at a Finnish psychotherapy center were accessed by a hacker or hackers now demanding ransoms

By JARI TANNER Associated Press

26 October 2020, 02:28 • 3 min read



October 21st, 2020

“Psychotherapy Centre Vastaamo announced that it had become a victim of a data system break-in and extortion.”

Press release October 26, 2020:
«Investigation into the Vastaamo data system break-in – shortcomings in information security in the background»

CASE ANALYSIS «Psychotherapy Center Vastaamo»

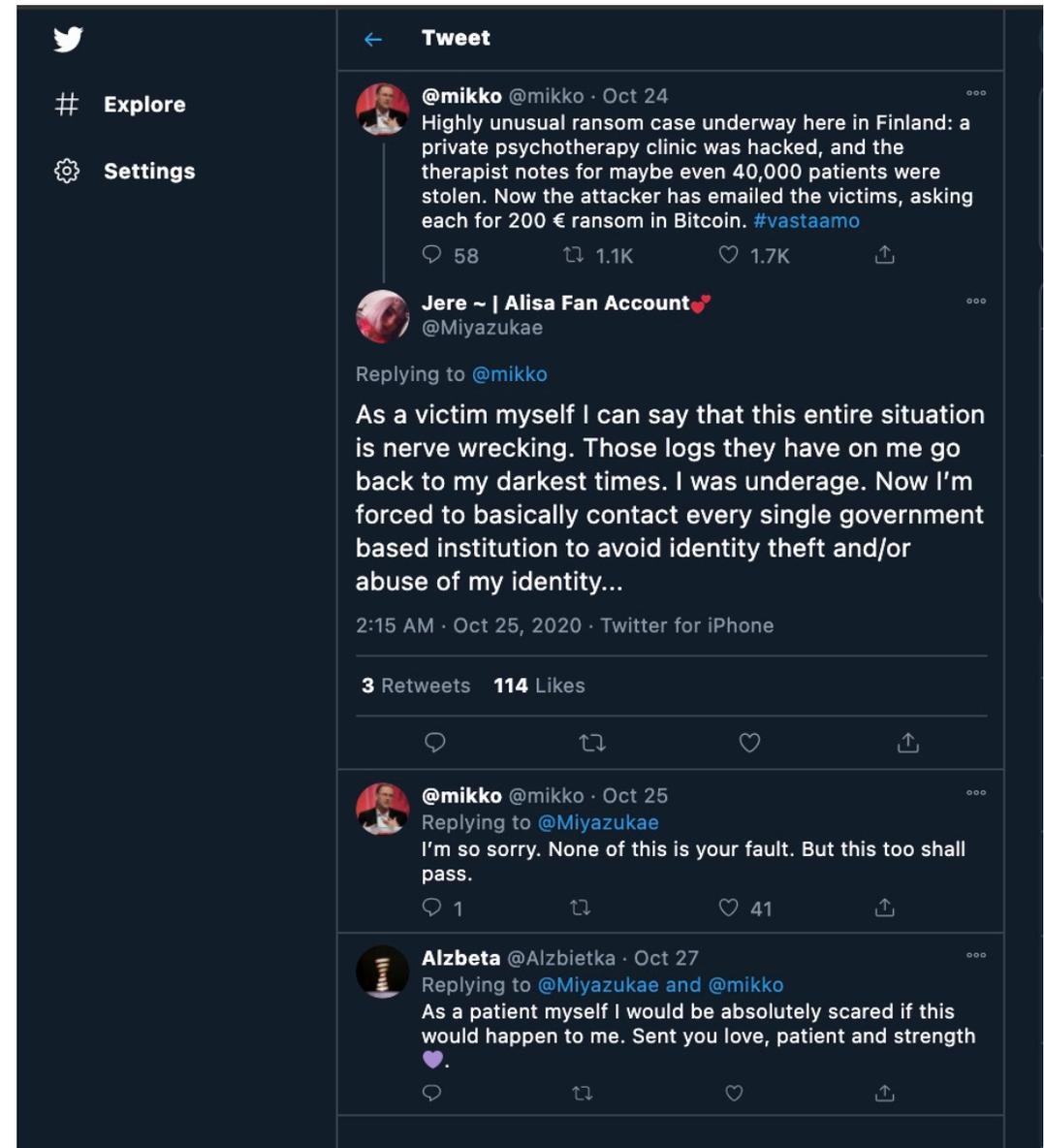
RESULTS of the investigation at the Psychotherapy Centre Vastaamo determined:

- Break in have been possible until mid-March 2019;
- The database wasn't stolen after November 2018; however, some individual data items have been viewed /copied;
- There was additional data breach in mid-March 2019.
- As result of request to fill police reports, till November 10t, 2020 there was filled 25000 reports according to the National Bureau of Investigation of Finland,

CASE ANALYSIS «Psychotherapy Center Vastaamo»

IMPACT ON HUMAN LIFE

FINANCIAL IMPACT



The screenshot shows a Twitter thread with three tweets. The first tweet, from @mikko on Oct 24, reports a ransom case at a private psychotherapy clinic in Finland, where 40,000 therapist notes were stolen and victims were asked for 200 € in Bitcoin. The second tweet, from Alisa Fan Account (@Miyazukae) on Oct 25, replies to @mikko, stating she is a victim and the situation is nerve-wrecking, as her logs go back to her darkest times and she is forced to contact government institutions to avoid identity theft. The third tweet, from Alzbeta (@Alzbietka) on Oct 27, replies to both @Miyazukae and @mikko, expressing fear as a patient and offering love and strength.

Tweet 1: @mikko @mikko · Oct 24
Highly unusual ransom case underway here in Finland: a private psychotherapy clinic was hacked, and the therapist notes for maybe even 40,000 patients were stolen. Now the attacker has emailed the victims, asking each for 200 € ransom in Bitcoin. #vastaamo
58 replies · 1.1K retweets · 1.7K likes

Tweet 2: Jere ~ | Alisa Fan Account ❤️ @Miyazukae
Replying to @mikko
As a victim myself I can say that this entire situation is nerve wrecking. Those logs they have on me go back to my darkest times. I was underage. Now I'm forced to basically contact every single government based institution to avoid identity theft and/or abuse of my identity...
2:15 AM · Oct 25, 2020 · Twitter for iPhone
3 Retweets 114 Likes

Tweet 3: @mikko @mikko · Oct 25
Replying to @Miyazukae
I'm so sorry. None of this is your fault. But this too shall pass.
1 reply · 41 likes

Tweet 4: Alzbeta @Alzbietka · Oct 27
Replying to @Miyazukae and @mikko
As a patient myself I would be absolutely scared if this would happen to me. Sent you love, patient and strength
1 like

Covid-19 on the Security Posture in a Healthcare environment?

STAGE 1

- Catalogue: Online Presence. Catalogue Presentation. Downloadable Forms

STAGE 2

- Transactions: Services and Forms On-line. Working Databases supporting online transactions

STAGE 3

- Vertical Integrations: Local systems linked to higher level systems; Within similar functionalities

STAGE 4

- Horizontal Integration: Systems integrated across different functions; - Real one stop shopping for citizens.

e-government is not static, but is constantly changing environment, which consist of following stages, (Karen Layne, 2001):

Covid-19 on the Security Posture in a Healthcare environment



Latvijas Republikas E-veselības sistēma

Twitter Facebook YouTube RSS A A A Lapas karte

Pieslēgties

ĀRSTIEM!

Būtiskas izmaiņas un risinājumi, kas ir spēkā arī pēc **ĀRKĀRTĒJĀ STĀVOKĻA** beigām:

1. Izmaiņas **darbnespējas lapu izrakstīšanā** no 2020. gada 22. marta.
2. Izmaiņas **medicīnisko ierīču izrakstīšanā** E-veselības sistēmā.



**PACIENTU UN ĀRSTU DROŠĪBAI - PIRMS
DODIES, ZVANI!**

Pieslēgties

Izmaiņas un risinājumi, kas ir spēkā arī pēc **ĀRKĀRTĒJĀ STĀVOKĻA** beigām

Par E-veselību

E-veselības lietošana

E-recepte

E-darbnespējas lapa

E-nosūtījums

Pakalpojumi

E-veselības interaktīvā karte

E-veselības portālā iespējams izrakstīt nosūtījumu uz Covid-19 analīzēm un apskatīt rezultātus

17.11.2020.

Pieaugot iedzīvotāju interesei par Covid-19 analīžu saņemšanas kārtību, Nacionālais veselības dienests (NVD) informē, ka E-veselības portālā joprojām tiek nodrošināta iespēja ne tikai nosūtīt pacientu uz Covid-19 analīzēm, bet arī saņemt veikto Covid-19 analīžu rezultātus. Informācija tiek sniegta gan par negatīviem testa rezultātiem, gan arī par pozitīviem un grūti interpretējamiem rezultātiem.

Lasīt vairāk ▶

No 9. novembra līdz 6. decembrim NVD klātienē pakalpojumus klientiem sniegs attālināti

07.11.2020.

Ņemot vērā valstī izsludināto ārkārtējo situāciju, no 9. novembra līdz šā gada 6. decembrim, Nacionālais veselības dienests (NVD) klātienē pakalpojumus klientiem sniegs attālināti.

Lasīt vairāk ▶

Lietotāju atbalsta dienests
iedzīvotājiem
67 803 300

Lietotāju atbalsta dienests
speciālistiem
67 803 301

VIDZEMES
AUGSTSKOLA

WEAKEST POINTS

ROUTERS - It is very difficult from the InfoSec viewpoint treat the router as BYOD.

? Do you have policies and guidelines, which can be align to telework and applies directly to a router security management and privacy according to the GDPR?



Covid-19 on the Security Posture in a Healthcare environment



Covid-19 on the Security Posture in a Healthcare environment

ASSUMPTION, that **you will be able to update a router**, to maintain required security level – **not always true**, due to:

- Some manufacturers don't provide updates at all;
- Some manufacturers sell product, which cannot be updated, due to limitation of initial product design;

Some ROUTERS have:

- add-on software firewall for additional fee;
- built-in hardware firewall;
- provide a Cloud management

Covid-19 on the Security Posture in a Healthcare environment

Peter Weidenbach and Johannes vom Dorp

“Home Router Security Report 2020”

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE

- Attention paid on 127 routers
- following versions were found from the Linux Kernel 2.4.20 to the Linux Kernel 4.4.60.

https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf



Covid-19 on the Security Posture in a Healthcare environment

Version of Linux Kernel	Initial publishing date	Number of vulnerabilities listed at the https://cve.mitre.org/
Linux Kernel 2.4.20	November 29 th , 2002	4, oldest -2002, newest - 2003
Linux Kernel 2.6.22	July 8 th , 2007	18, oldest - 2005, newest - 2012
Linux Kernel 2.6.31	September 9 th , 2009	21, oldest – 2009, newest - 2015
Linux Kernel 2.6.35	August 1 st , 2010	16, oldest – 2010, newest - 2011
Linux Kernel 2.6.36	October 20 th , 2010	36, oldest – 2010, newest - 2014
Linux Kernel 3.10.10	August 30 th , 2013	1, oldest/newest - 2013
Linux Kernel 3.10.14	October 1 st , 2013	316. oldest - 2013 , newest – 2019 (https://www.cvedetails.com/)
Linux Kernel 3.10.20	November 20 th , 2013	47, oldest -2014, newest – 2019 (https://www.cvedetails.com/)
Linux Kernel 3.10.39	May 6 th , 2014	194, oldest – 2014, newest – 2019, (https://www.cvedetails.com/)
Linux Kernel 3.10.49	July 17 th , 2014	194, oldest - 2014, newest – 2019 (https://www.cvedetails.com/)
Linux Kernel 3.10.70	February 26 th , 2015	194, oldest - 2015, newest – 2019 (https://www.cvedetails.com/)
Linux Kernel 3.14.43	May 17 th , 2015	189, oldest - 2017, newest – 2019 (https://www.cvedetails.com/)

Without detailed look at each vulnerability, it cannot be assumed, that all of them can be applied towards router and its built-in hardware limitations. However, there is necessary only for one weakest link in the chain, or one weakest spot in the metal crystal structure.

Conclusion – Takeaway

1. Focus on **People-Process-Product**, when you try to determine at which e-government stage your company, organization, division, etc. currently exist;
2. Create **audit of all routers** in your organization – including those, which are used by your personnel to work from home and determine:
 - How old is the device?
 - Does it have latest updates?
 - Can it be updated?
 - Does it provide any firewall functions?
 - Does it support VPN function?
 - Does it capable to close ports above 1023 or it only able to manage ports from 0 to 1023, and rest of ports are open by the device?

Conclusion – Takeaway

If the router is used as BYOD, when working from home, does it provide adequate security level?

For IP address scanning you can use: <https://www.shodan.io/> ,

it will allow you to determine whether on the network are exploitable devices, which can be used either to acquire/monitor your organizations personnel or be used to exploit your company with malicious intent;

Useful Links:

ARTSS projekts ietver informāciju par drošiem pamatservisiem (<https://artss.rtu.lv/lv>):

- **IKT infrastruktūras un datortīkla apdraudējumu identificēšana**
- **Droši telemedicīnas servisi** : Prasības IKT nodrošinājumam telemedicīnas servisu nodrošināšanai
- **Droši attālinātā darba servisi** : Efektīvas komunikācijas sistēmas risinājums
- **Droši biznesa servisi** : Mobilitātes nodrošināšanas servisi ārkārtas situācijās

**The Cavalry isn't coming. It falls to you. Be a voice of reason.
Drive cybersecurity for public safety and human life.**

<https://iamthecavalry.org/>

Securing Telehealth Remote Patient Monitoring Ecosystem <https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth>

Regarding Vastaamo – update by Wiliiam Ralstom “A dying man, a therapist and the ransom raid that shook the world”, published on January 10th, 2020 <https://www.wired.co.uk/article/finland-mental-health-data-breach-vastaamo>



Kontakti:

Cēsu iela 4, Tērbatas iela 10,
Valmiera, LV - 4201, Latvija
info@va.lv

T.+371 64207230 (Cēsu iela 4)

T.+371 26603322 (Cēsu iela 4)

T.+371 25443379 (Tērbatas iela 10)

www.va.lv