

Hackers claim to publish prominent Israeli hospital's patient data

By Daryna Antoniuk

Published: 2023-09-07 · Archived: 2026-04-05 21:39:42 UTC

Hackers who breached an Israeli hospital near Tel Aviv last month said they started leaking stolen data because no ransom was paid.

The [ransomware attack](#) on Mayanei Hayeshua Medical Center resulted in the shutdown of its administrative computer systems, leading the hospital to redirect new patients and those requiring emergency care to other medical centers.

The Ragnar Locker ransomware gang claimed responsibility for the attack this week and said it is releasing the first batch of the hospital's internal files. Israeli news outlet JNS has reported that the list of affected patients [potentially includes](#) top government officials, lawmakers and senior rabbis.

So, if there was a negotiation, it was not successful, as the Ragnar Locker gang just started leaking files from the medical center.



"According to our rules we are publishing the data which were compromised during security research of the MYMC network."

Security research?

pic.twitter.com/JKO9SHtVU6

— MalwareHunterTeam (@malwrhunterteam) [September 6, 2023](#)

The disclosed data set is said to contain “a lot of personal information, internal emails, finances, medical cards, and other highly sensitive data,” according to [a post from the group](#) shared by the MalwareHunterTeam account on social media site X.

The hackers said they didn't encrypt the files on the hospital's network because they didn't want to damage medical equipment.

The Record couldn't independently verify the hackers' claims and the authenticity of the stolen data. Mayanei Hayeshua Medical Center didn't respond to a request for comment.

Israeli Prime Minister Benjamin Netanyahu [received treatment](#) for prostate-related issues at Mayanei Hayeshu hospital in 2015. It remains unclear whether his records were among those exposed by hackers.

Israel's privacy protection authority, which investigated the incident, confirmed to local media that some sensitive personal information indeed [had been exposed](#) but did not specify what type of data was stolen.

The Ragnar Locker hackers said the hospital refused to negotiate and didn't pay the ransom, which was previously [reported](#) to be “tens of millions of shekels” (1 shekel is about 0.25 dollars).

“We tried to draw their attention to the network issues and called them for discussion,” the hackers said. “After multiple attempts to contact the management, it becomes clear to us that the management doesn’t care about the privacy of their own patients.”

The hackers said they plan to release more data and the hospital's internal emails in the next few days.

“Those organizations who are collecting and storing private data should be in charge of its privacy,” hackers claim.

The Ragnar Locker group is not associated with any particular country. It has targeted various entities in the past, including Portugal's national airline, the Japanese gaming company Capcom, computer chip manufacturer Adata, and aviation giant Dassault Falcon.

The FBI reported that from April 2020 to March 2022, the Ragnar Locker ransomware was used to attack the networks of [at least 52 organizations](#) across various critical infrastructure sectors in the U.S.

The hackers’ attack on Mayanei Hayeshua Medical Center raised concerns among security researchers.

“Absolutely appalled by the latest RagnarLocker attack and data leakage on Mayanei Hayeshua Medical Center in Israel. Attacking healthcare facilities is not just immoral, it's devastating on so many levels,” [said](#) Ohad Zaidenberg, founder of CTI League, a global group of cybersecurity volunteers who defend hospitals from cyberattacks.

“Leaking this data can break families and push vulnerable individuals over the edge,” Zaidenberg added.

 Recorded Future®

Know what matters.

Act first.

Get started





[Daryna Antoniuk](#)

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.

Source: <https://therecord.media/israel-hospital-data-leaked-ragnar-locker-ransomware>