The Record.
Recorded Future® News

MA'AYANEI HAYESHUAH MEDICAL CENTER IN BNEI BRAK, ISRAEL. IMAGE: DR. AVISHAI TEICHER PIKIWIKI ISRAEL / WIKIMEDIA COMMONS / CC BY 2.5

Daryna Antoniuk

September 7th, 2023

Cybercrime News

Hackers claim to publish prominent Israeli hospital's patient data

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.

MalwareHunterTeam · Aug 30, 2023
@malwrhunterteam · **Follow**
Replying to @malwrhunterteam and @IdoNaor1

So much silence. The most obvious explanation would be that they have started negotiating...
🤔

MalwareHunterTeam
@malwrhunterteam · **Follow**

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?
😂

9:23 PM · Sep 6, 2023

9 Reply Share

Read 1 reply

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.

Tags

Healthcare Israel Ragnar Locker

Previous article

Next article

DARYNA ANTONIUK

Daryna Antoniuk is a freelance 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.

BRIEFS

Ukraine's intelligence claims cyberattack on Russia's state tax service

December 12th, 2023

FCC reminds mobile phone carriers they must do more to prevent SIM swaps

December 12th, 2023

Long-running Clearview AI class action biometric privacy case settles

December 11th, 2023

Alleged leader of Kelvin Security hacker gang arrested in Spain

December 11th, 2023

TV service in UAE hacked to show alleged atrocities in Palestine

December 11th, 2023

More evidence of Russian intelligence exploiting old Outlook flaw

December 8th, 2023

Leader of Russian hacktivist group Killnet 'retires,' appoints new head

December 8th, 2023

Russian opposition activists use QR codes to spread anti-Putin messages

December 7th, 2023

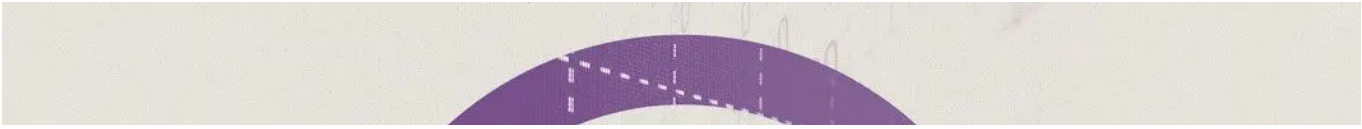
Russian citizen pleads guilty to operating Bitzlato crypto exchange used by cybercriminals

December 7th, 2023

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK "DOPPELGÄNGER" SIGNALS EVOLVING TACTICS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK "DOPPELGÄNGER" SIGNALS EVOLVING TACTICS

CRYPTO COUNTRY: NORTH KOREA'S TARGETING OF CRYPTOCURRENCY



CRYPTO COUNTRY: NORTH KOREA'S TARGETING OF CRYPTOCURRENCY

AS BLACK FRIDAY APPROACHES, 3 KEY TRENDS OFFER INSIGHTS FOR MITIGATING ONLINE SHOPPING SCAMS

AS BLACK FRIDAY APPROACHES, 3 KEY TRENDS OFFER INSIGHTS FOR MITIGATING ONLINE SHOPPING SCAMS

IMPROVING AUTOMATION AND ACCESSIBILITY DRIVE $100 BILLION IN PROJECTED AD FRAUD LOSSES

IMPROVING AUTOMATION AND ACCESSIBILITY DRIVE $100 BILLION IN PROJECTED AD FRAUD LOSSES

CHARTING CHINA’S CLIMB AS A LEADING GLOBAL CYBER POWER

CHARTING CHINA’S CLIMB AS A LEADING GLOBAL CYBER POWER