Suspected Chinese hackers behind attacks on ten Israeli hospitals

bleepingcomputer.com/news/security/suspected-chinese-hackers-behind-attacks-on-ten-israeli-hospitals/

Bill Toulas

By
Bill Toulas

- October 18, 2021
- 10:55 AM
- 1

A joint announcement from the Ministry of Health and the National Cyber Directorate in Israel describes a spike in ransomware attacks over the weekend that targeted the systems of nine health institutes in the country.

In the joint announcement, the Israeli government states that the attempts resulted in no damage to the hospitals and the medical organizations, thanks to national-level coordination and the quick and decisive response of the local IT teams.

The two authorities had carried out numerous defensive activities in the health sector to identify open vulnerabilities and secure them before the weekend arrived, mostly in response to a Wednesday attack on the Hillel Yaffe Medical Center.

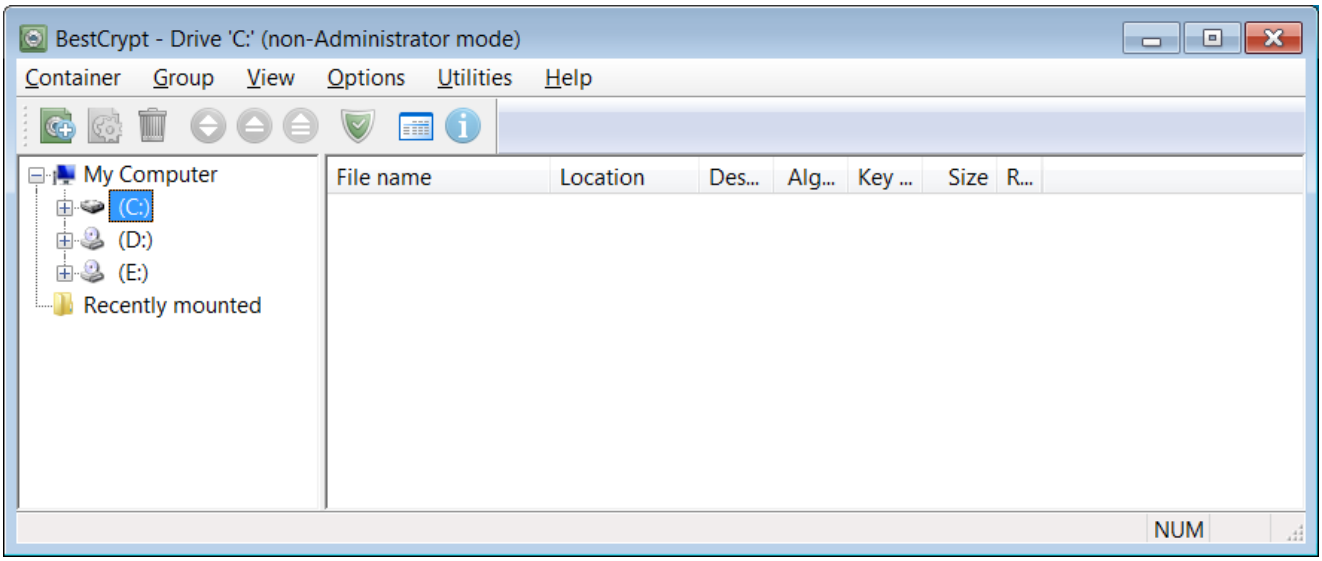
As it seems, though, these efforts weren't enough to secure the exposed endpoints, and some healthcare organizations were still breached over the weekend.

Fingers point to Chinese hackers

According to local media reports, the attack is attributed to a Chinese group of actors using the 'DeepBlueMagic' ransomware strain, which first appeared in the wild in August this year.

DeepBlueMagin is known to disable security solutions that usually detect and block file encryption attempts, allowing for successful attacks.

Testing the IOCs shared by the authorities, BleepingComputer determined that the threat actors are using the 'BestCrypt' hard drive encryption tool to encrypt devices.



BestCrypt used for the encryption of the files

Israel's National Cyber Directorate has released indicators of compromise (IOCs) in the form of file hashes that have been seen in related attacks.

The agency suggests that Israeli organizations perform the following steps:

1. Review the IOCs in the CSV file and check if they have been observed in their environment.
2. Perform an active scan of all systems and include the file hashes in the organization's AV/EDR solutions.
3. Make sure all VPN and email servers are upgraded to the latest version to resolve any vulnerabilities that threat actors can use to gain access to internal networks.
4. If servers are not up to date, update them and perform password resets for all users.
5. Increase monitoring for unusual events in the corporate networks.
6. Report any breaches or unusual activity to the Israeli Israel National Cyber Directorate.

Hille Yaffe still struggling

In the meantime, the Hillel Yaffe Medical Center in the north of Tel Aviv is still struggling with the restoration of its systems, and the staff is using "pen a paper" to admit patients and circulate exams for the sixth day now.

Even though there's hope that the Hillel Yaffe Medical Center will return to normal operations in a few days, there are fears that some medical records will be unrecoverable.

This is because the ransomware actors reportedly accessed the backup system, wiping all copies stored there for emergency cases like cyberattacks.

Reuven Eliyahu, the cybersecurity chief in the Health Ministry has confirmed that the mid-week attack was carried out by Chinese hackers in a statement today, and described the actors' motives as "purely financial".

"This is probably a Chinese hacker group that broke away from another group and started working in August," Eliyahu said in an interview with Army Radio. "The motive for the attack was purely financial."

However, a source in the cybersecurity industry has told BleepingComputer that the attribution to China is weak and that the attacks may have simply been port scans or probes into a network's defenses.

As for the ransom payment, the Hillel Yaffa center is a government-owned hospital, and as such, it won't negotiate with hackers.

Update 10/18/21 02:31 PM EST: Added further information about attribution to China.

Related Articles:

Clop ransomware gang is back, hits 21 victims in a single month

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.