Iran-linked hackers attack Israeli education and tech organizations

therecord.media/iran-linked-hackers-target-israel-education-tech-sectors

Image: Robert Bye via Unsplash

Daryna Antoniuk
November 6th, 2023

Hackers suspected of being tied to Iran's government have been deploying new destructive malware against Israeli organizations, according to recent research.

The attacks, attributed to an Iranian state-backed hacker group known as Agonizing Serpens, are part of a broader offensive campaign targeting Israel during its war with the Palestinian militant group Hamas, according to U.S. cybersecurity firm Palo Alto Networks.

The company said on Monday it had blocked a series of destructive cyberattacks on Israel that began in January and continued at least until October of this year, with the hackers primarily targeting educational and technology organizations.

The group was going after sensitive data, such as personally identifiable information and intellectual property. The attackers shared stolen information, including passport scans, emails, and victims' full addresses, on social media and Telegram channels, likely to sow fear or inflict reputational damage, according to the research.

To cover their tracks and cause even more disruption, the hackers deployed wipers — a type of malware designed to delete or wipe out data.

Researchers have discovered three previously unknown wipers used in the latest attacks, including MultiLayer Wiper, PartialWasher, and BFG Agonizer Wiper, as well as a custom tool to extract information from database servers known as Sqlextractor.

Some of these tools have code similarities with other wipers previously used by Agonizing Serpens, while others were brand new. The overlaps between the tools may indicate that they share a codebase or were written by the same team of developers, according to the report.

To gain initial access to the victim's environment, the group exploited vulnerable internet-facing web servers. To obtain credentials of users with administrative privileges, the attackers tried multiple methods. For example, they used Mimikatz, an exploit on Microsoft Windows that extracts passwords stored in memory.

Researchers said that Agonizing Serpens “is investing significant efforts and resources” trying to bypass security measures. This includes their practice of rotating between various known tools as well as custom-made tools.

Iranian hackers

Agonizing Serpens, also known as Agrius and BlackShadow, has been active since 2020. The group is known for its destructive wiper and fake ransomware attacks. Earlier in May, the hackers used a new ransomware strain called Moneybird in its attacks against Israeli organizations.

In the most recent attacks, the attackers did not demand a ransom; instead, the potential outcome of the attacks was significant data loss and disruptions to business continuity, researchers said.

Israel has been an attractive target for Iranian hackers recently. In late October, researchers detected a cyberattack on at least two Israeli entities by a long-running group connected to the Iranian government called MuddyWater.

Israel’s cyber defense chief told CNN that he’s “very concerned” that Iran could escalate its cyberattacks on the country’s infrastructure amid the Israeli-Palestinian war.

Iran, whose support for Hamas is driven by shared anti-Israel and anti-Western sentiments, can use cyberattacks to project power, as it can act more freely in cyberspace than in physical space, according to Gaby Portnoy, the head of the Israel National Cyber Directorate.

So far, suspected Iranian cyberattacks appear to have had minimal impact on their publicly claimed targets in Israel, according to Portnoy.

Portnoy said they want to keep cyberspace from becoming “another front” in the war with Hamas.

No previous article

No new articles

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.