Scattered Spider group a unique challenge for cyber cops, FBI leader says

By Martin Matishak

Published: 2024-05-07 · Archived: 2026-04-05 20:48:03 UTC

SAN FRANCISCO — The FBI must “evolve” if it hopes to successfully thwart a group of hackers who have wrought chaos on some of the largest companies in the U.S., according to a senior bureau official, who urged the public to be patient as law enforcement fights the criminal network.

The hacking collective known as Scattered Spider drew international attention last year over its paralyzing cyberattacks on casino giants MGM Resorts and Caesars Entertainment. Identified by analysts in 2022, the hackers use social engineering to lure users into giving up their login credentials or one-time password codes to bypass multifactor authentication.

Once inside, the group — also known as Star Fraud, UNC3944, and Octo Tempest — establishes persistence in networks, living off the land as some nation-state hackers do, before they deploy ransomware or pilfer data and extort victims for ransoms.

“We have to continue to evolve as they evolve. We have to innovate as they innovate,” Brett Leatherman, deputy assistant director of the FBI’s cyber division, told Recorded Future News during a sit-down interview at the RSA Conference in San Francisco on Monday.

“If you look at Scattered Spider, it is very consistent that we need private sector victims who have been compromised by Scattered Spider to come forward quickly enough to provide us with information that would help us in that enforcement operation,” including new indicators of compromises and insight into technical infrastructure.

“If we can get that right away, we can sometimes use core authorized capabilities to go after that infrastructure and collect new information that allows us to conduct a disruption operation,” he said.

The Scattered Spider network is an offshoot of a larger pool of online criminals who dubbed themselves "the Community," or "the Com.” The group’s size, expertise in social engineering and alleged coordination with Russian ransomware gangs like BlackCat/AlphV, pose a unique challenge for the FBI, which has increased its operational tempo against hacking groups over the last two years.

The bureau’s ultimate goal for such actions is to dismantle an adversary’s ability to reconstitute and target U.S. entities, he said.

However, not all disruptions are equal, Leatherman admitted.

For instance, last year the U.S. and its allies announced they had eradicated a global network of computers infected by malware that Russia's state security services allegedly used for nearly 20 years to steal secrets from

Western nations.

“That operation has sustained … meaning the Russians have not been able to reconstitute,” Leatherman said. “We reassess they haven't been able to reconstitute that capability since then.”

Meanwhile, international authorities continue to shine a light on the notorious ransomware gang LockBit, unmasking and sanctioning its alleged leader on Tuesday — months after police hijacked the cybercriminal group’s dark web site and publicly shared information about its members. The LockBit operation had been going on for two years, in one form or another.

But in the case of Scattered Spider, such tactics might not apply.

“I don't know that I could answer that it's possible to dismantle” groups like Scattered Spider, Leatherman said, comparing them to street gangs in major cities.

Whenever law enforcement arrests individuals associated with such a group “there is a disruptive period of time where the gang is trying to figure out what happened,” he explained.

“Some people are leaving as they don't want to be involved in any sort of enforcement action going forward. But then you start to see others start to rise to the surface and engage in similar activity.

“It's very difficult to dismantle large organizations like this. We will always endeavor to do it.”

The FBI has come under intense scrutiny for the seeming lack of action against the collection, save the January arrest of a 19-year-old Floridian named Noah Urban on charges of stealing $800,000 in cryptocurrency.

“There's always a demand to ask for the U.S. government to act,” Leatherman said, adding “there are actions we have taken that are not currently public.”

The public should be “somewhat assured that even when they're not hearing about some of the disruption activity, we are putting our best folks forward on that disruption — especially in a group like Scattered Spider,” he said.

Read More: Live updates from the 2024 RSA Conference

No previous article

No new articles

Martin Matishak

is the senior cybersecurity reporter for The Record. Prior to joining Recorded Future News in 2021, he spent more than five years at Politico, where he covered digital and national security developments across Capitol Hill, the Pentagon and the U.S. intelligence community. He previously was a reporter at The Hill, National Journal Group and Inside Washington Publishers.
