Ex-NSA bad-guy hunter listened to Scattered Spider's fake help-desk calls: 'Those guys are good'

By Jessica Lyons

Published: 2025-05-18 · Archived: 2026-04-05 13:24:20 UTC

INTERVIEW The call came into the help desk at a large US retailer. An employee had been locked out of their corporate accounts.

But the caller wasn't actually a company employee. He was a Scattered Spider criminal trying to break into the retailer's systems - and he was really good, according to Jon DiMaggio, a former NSA analyst who now works as a chief security strategist at Analyst1.

Scattered Spider is a cyber gang linked to SIM swapping, fake IT calls, and ransomware crews like ALPHV. They've breached big names like MGM and Caesars, and despite arrests, keep evolving. They're tracked by Mandiant as UNC3944, also known as Octo Tempest.

DiMaggio listened in on this call, which was one of the group's recent attempts to infiltrate American retail organizations after hitting multiple UK-based shops. He won't name the company, other than to say it's a "big US retail organization." This attempt did not end with a successful ransomware infection or stolen data.

"But I got to listen to the phone calls, and those guys are good," DiMaggio told *The Register*. "It sounded legit, and they had information to make them sound like real employees."

Scattered Spider gave the help desk the employee's ID and email address. DiMaggio said he suspected the caller first social-engineered the employee to obtain this data, "but that is an assumption."

"The caller had all of their information: employee ID numbers, when they started working there, where they worked and resided," DiMaggio said. "They were calling from a number that was in the right demographic, they were well-spoken in English, they looked and felt real. They knew a lot about the company, so it's very difficult to flag these things. When these guys do it, they're good at what they do."

Luckily, the target was a big company with a big security budget, and it employs several former government and law enforcement infosec officials, including criminal-behavior experts, on its team. But not every organization has this type of staffing or resources to ward off these types of attacks where the would-be intruders are trying to break in from every access point.

> They are resourceful, they're smart, they're fast

"They are resourceful, they're smart, they're fast," Mandiant CTO Charles Carmakal told *The Register*.

"One of the challenges that defenders have is: it's not the shortage of network alerts," he added. "You know when Scattered Spider is targeting a company because people are calling the help desk and trying to reset passwords.

They are running tools across an enterprise that will fire off on antivirus signatures and EDR alerts, tons and tons and tons of alerts. They operate at a speed that can be hard to defend against."

In this case, sometimes the best option — albeit a painful one — is for the organization to break its own IT systems before the criminals do.

- Cyber fiends battering UK retailers now turn to US stores
- Marks & Spencer admits cybercrooks made off with customer info
- British govt agents step in as Harrods becomes third mega retailer under cyberattack
- Here's what we know about the DragonForce ransomware that hit Marks & Spencer

Co-op pulled its own plug

This appears to have been the case with British retailer Co-op, which pulled its systems offline before Scattered Spider could encrypt its files and move throughout its networks.

"Following the malicious third-party cyber-attack, we took early and decisive action to restrict access to our systems in order to protect our Co-op," a spokesperson told *The Register*. "We are now in the recovery phase and are taking steps to bring our systems gradually back online in a safe and controlled manner."

The outfit said customers will see "improved stock availability in our food stores and online" beginning this weekend, and added it is "working closely" with suppliers to restock its brick-and-mortar stores.

All payment forms and systems are now up and running across the business, we're told. ®
