Scattered Spider snared financial orgs before targeting shops in Britain, America

By Jessica Lyons

Published: 2025-05-21 · Archived: 2026-04-05 17:52:17 UTC

interview Scattered Spider snared financial services organizations in its web before its recent spate of retail attacks in the UK and US, according to Palo Alto Networks' Unit 42.

"We saw several instances in the financial services space, and now we're starting to see instances in the retail-oriented, customer-facing space," Unit 42 principal threat researcher Kristopher Russo told *The Register*.

Russo declined to name the victim companies, but noted that all of the organizations that brought in Unit 42's incident-response team were English-speaking.

Echoing warnings from Mandiant CTO Charles Carmakal, Russo said he expects the loosely knit cybercrime crew to soon lose interest in retail and move on to the next shiny target.

> They tend to shift from industry to industry

"They tend to shift from industry to industry," Russo said. "It's more the amorphous nature of this group, where they're bringing people in and losing people all the time, and you have people that have specialties in software that's used by a specific industry."

These criminals typically have experience in particular industries, and they use this "insider knowledge" about various sectors for evil, he added.

"Early on, this group was focused on cryptocurrency theft," Russo said. "Business process outsourcers were a huge target for a while. We saw them shift to financial services, and now this retail shift seems to be the latest in the bouncing around that this group does."

Moving on to crypto?

Meanwhile, some unknown miscreants have reportedly targeted large cryptocurrency exchanges, including Binance and Kraken, using the same type of social-engineering attacks that criminals employed to break into Coinbase and steal customer data.

Kraken declined to comment on the unsuccessful break-in, reported by Bloomberg, and Binance did not respond to *The Register*'s inquiries.

In the case of Binance, the crooks called some of the biz's users in Israel and tried to trick them into transferring funds into an attacker-controlled wallet, according to the report, which noted: "The caller had a posh British accent."

One of the hallmarks of Scattered Spider's social engineering campaigns is their native-English speakers' skill at convincing help desks, company employees — or really anyone on the other end of the phone — to disregard their own policies and do what the scammers say.

- Ex-NSA bad-guy hunter listened to Scattered Spider's fake help-desk calls: 'Those guys are good'
- Coinbase extorted for $20M. Support staff bribed. Customers scammed. One hell of a SNAFU
- Cyber fiends battering UK retailers now turn to US stores
- Marks & Spencer admits cybercrooks made off with customer info

"The key to this is to make sure that your help desk does not violate its internal procedures, and that you test that so they're not changing a password and an MFA on the same call, and they are not bypassing any of their authentication types," Russo said.

When asked if he's seen any indication of a link between the crypto hacks and Scattered Spider, Russo said he doesn't have any evidence. But he also wouldn't be surprised if they turn out to be connected.

"A year ago, cryptocurrency firms were a prime target for this group, and we were able to do some attributions back then," Russo said. "It would not surprise me at all to see that they're still active in this space."

Coinbase, when asked if they've identified any suspects or attributed the breach to a particular group, emailed *The Register* the following statement:

"We have notified and are working with the DOJ and other US and international law enforcement agencies and welcome law enforcement's pursuit of criminal charges against these bad actors," Coinbase Chief Legal Officer Paul Grewal said. ®
