Scattered Spider spins a troublesome web

blog.barracuda.com/2023/12/22/scattered-spider-spins-a-troublesome-web

December 22, 2023

Note: This was originally published at SmarterMSP.

The Itsy-Bitsy Spider may have crawled up the waterspout, but the Scattered Spider could be crawling into your email box.

CISA is sounding the alarm about Scattered Spider and the havoc it can wreak.

The CISA bulletin says: *"Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs."*

Experts agree that this is a threat that should be monitored, but not for every entity. "They seem very selective in who they are going after; manufacturers, schools, and government agencies, at least so far, seem largely spared," says Stan Spencer, a cybersecurity specialist in Toledo, Ohio, who has studied Scattered Spider in the past.

Scattered Spider, or UNC3944, is a sophisticated cybercriminal group targeting large organizations. "They seem especially keen on hitting telecommunications, hospitality, retail, media, and financial services industries," Spencer warns.

And what sets them apart is their social engineering prowess. Spencer adds, “They have even been able to trick people who should know better because their emails are so convincing, compelling, and timely. In addition to looking very realistic, they’ll use social engineering, phishing, and SIM-swapping attacks to gain initial access to victim networks.”

MSPs must remain vigilant

MSPs must be on the lookout for how Scattered Spider uses legitimate tools to do their damage rather than malware. “Once inside, Scattered Spider employs various techniques to steal data, deploy ransomware, and disrupt operations,” Spencer advises. “I have seen them use legitimate remote access tools, which makes the initial breach more difficult to spot.”

They are also constantly evolving and changing their methodology. “Just when you think you know them and their methods, they change again,” Spencer explains. Some of the more recent, noteworthy attacks can be traced to Scattered Spider:

Ubiquiti Networks: In December 2022, they attacked Ubiquiti Networks, a networking equipment manufacturer. The threat actors accessed Ubiquiti’s systems by phishing an employee and stealing their credentials. They then stole a large amount of data, including source code, customer information, and financial records. Ubiquiti was forced to shut down its systems for several days and lost millions of dollars in revenue. “The Ubiquiti attack was classic Scattered Spider, a combination phishing and credential stealing operation,” Spencer says.

MGM Resorts: In September, researchers and authorities found that Scattered Spider collaborated with ALPHV, a ransomware group, to attack MGM Resorts. Attackers gained access to MGM’s systems by posing as an employee and calling the company’s help desk. They then stole data, including customer information and financial records. MGM ultimately paid $200 million to recover the stolen data. “It would take a lot of quarters in the slot machines to add up to $200 million,” Spencer mused.

Money is the motivating factor

As is the case with most cybercrime, the motivation is money. They target organizations with valuable assets like intellectual property, customer data, or financial records. “Scattered Spider goes after the prized data that fetches the most money on the dark web,” Spencer notes.

Protecting against Scattered Spider

Spencer agrees with most of CISA’s mitigation recommendations, which include:

Auditing Remote Access Tools (RAT): “This is a huge one because this is Scattered Spider’s bread and butter,” Spencer says. Organizations and their MSPs need to know what RATs are being used.

Reviewing logs for execution of remote access software: “You’ll be able to quickly detect abnormal use of programs running as a portable executable,” Spencer advises. “That is one of Scattered Spider’s signatures.”

Using security software: This is to detect instances of remote access software being loaded only in memory. “This is yet another invaluable tool when combatting Scattered Spider,” Spencer says.

Requiring authorized remote access solutions: This is to be used only from within your network over approved remote access solutions, such as VPNs or virtual desktop interfaces (VDIs). “These are all commonsense steps, along with user education, that can be done to help tilt the odds in your favor, but Scattered Spider is one of the best at getting through defenses, and they are tenacious. They’ll probe every weak spot until they find a way in,” Spencer adds.