Scattered Spider is NOT quiet. They're just under another name now. - DataBreaches.Net

Published: 2025-08-05 · Archived: 2026-04-09 02:21:29 UTC

Citing a July 30 report in *The Hacker News*, SC Media reports:

> Following recent arrests of alleged Scattered Spider members in the UK, Google Cloud's Mandiant Consulting has reported a noticeable pause in the group's activities, offering a "critical window of opportunity" for organizations to bolster their defenses, reports The Hacker News.

THN had reported, in part:

> "Since the recent arrests tied to the alleged Scattered Spider (UNC3944) members in the U.K., Mandiant Consulting hasn't observed any new intrusions directly attributable to this specific threat actor," Charles Carmakal, CTO of Mandiant Consulting at Google Cloud, told The Hacker News in a statement.
>
> "This presents a critical window of opportunity that organizations must capitalize on to thoroughly study the tactics UNC3944 wielded so effectively, assess their systems, and reinforce their security posture accordingly."
>
> Carmakal also warned businesses not to "let their guard down entirely," as other threat actors like UNC6040 are employing similar social engineering tactics as Scattered Spider to breach target networks.

DataBreaches recently suggested that attempting to distinguish the groups or to attribute incidents to one or the other is fraught with difficulty because they appear to be one now, as claimed by the leader of ShinyHunters in a statement to DataBreaches.

Today, DataBreaches asked ShinyHunters to respond to Carmakal's statements to THN. He replied:

> Mr. Charles Carmakal and the rest of the Google Threat Intelligence Group appear to be tunnel visioned. They've been saying the same thing for a year now.
>
> Their analysis compared to BleepingComputer or DataBreaches.net is inaccurate.
>
> Mandiant is just upset they can't directly link which name (group) is doing this and we have them exactly where we want them to be, just like the entirety of threat intelligence and law enforcement.

In a follow-up inquiry, DataBreaches asked ShinyHunters to respond more specifically to the claim that Mandiant had not detected any new intrusions by Scattered Spider (UNC3944) since the arrests of four alleged members of Scattered Spider. "Have members of Scattered Spider been active since those arrests, attacking new victims?" DataBreaches asked. "If so, can you give me any clues or insight as to who they have been attacking?

ShinyHunters replied:

> They've been working with us. Despite everyone's efforts to halt the Salesforce-related attacks, we continue to attack multi-billion to multi hundred billion dollar companies daily and successfully dump them. We urge law enforcement and Google Threat Intelligence to collaborate closely with CrowdStrike and Unit221b to effectively counter and put an end to this threat. Google Threat Inteligence and law enforcement have showed nothing but incompetence and inaccuracy.
>
> Google Threat Intelligence has been actively monitoring the situation, particularly tracking activity and TTPs associated with the four alleged members of Scattered Spider arrested in the U.K. Those four individuals do not constitute the entirety of Scattered Spider.

ShinyHunters' reply is consistent with his prior statement to DataBreaches that ShinyHunters and Scattered Spider are now one.

While Mandiant and others continue to use the two labels for the groups, DataBreaches continues to think that it might be more productive to think of one entity, "Sp1d3rHunters" or some other combination name, recognizing that individuals and affiliates will have different roles and approaches that may be utilized in different campaigns.

Growing/Integration Challenges?

ShinyHunters had generally appeared to be a fairly well-controlled operation over the past few years. Since last year, however, things seem a little less well-controlled. DataBreaches is aware of at least two incidents where things did not go as ShinyHunters wanted. The atypical incidents may be a result of new people being incorporated or the combination of the two groups.

One incident involved the second round of extortion in the PowerSchool incident, when some clients of PowerSchool received extortion demands on May 6 signed "ShinyHunters" and using the same ToxID and BTC wallet used in the original December extortion of PowerSchool. The attempt made the news quickly, and just as quickly, it was dropped. At the time, DataBreaches had expressed significant surprise at the attempt because ShinyHunters had never attempted to "double-dip" as far as this blogger knew. ShinyHunters later told DataBreaches that affiliates had not listened to him and had tried to extort the clients.

A second example is more recent. ShinyHunters contacted DataBreaches this week and told me that despite their firm and longstanding prohibition on hitting the healthcare sector, an affiliate who was previously associated with Scattered Spider had dumped a major health insurance firm. ShinyHunters gave me the name of the victim, its url, and asked me to notify them that they had been hit (it was a Salesforce-related attack). Shiny also gave me the dates of the dump to facilitate the insurer's forensics, assured me that the insurance company will not be extorted, and was taking steps to make sure that the data had been deleted from their server.

ShinyHunter's actions might surprise some people, but they did not surprise me because unlike groups that claim they won't hit the healthcare sector and then do, ShinyHunters has really adhered to the prohibition on hitting the healthcare sector.

That affiliate "has since been removed and will never return. We actually mean this unlike Lockbit," ShinyHunters told me.

In the meantime, DataBreaches continues to read the perspective of others who continue to try to deal with two entities as opposed to one combined one. Hopefully one day soon we will all have greater clarity.
