Are Scattered Spider and ShinyHunters one group or two? And who did France arrest? (1) - DataBreaches.Net

Published: 2025-08-03 · Archived: 2026-04-09 02:09:09 UTC

When DataBreaches was a kid, the “new math” they were experimenting with had us learning binary and other systems. It didn’t go over well with us, our teachers, or our parents back then. Now the “new math” for me is UNCs — specifically 6040, 5537, 3944, and 6240.

6040+5537+3944 +6240 = Scattered Spider + ShinyHunters

But does Scattered Spider = ShinyHunters?

According to a statement made by ShinyHunters yesterday, they are one and the same.

What a Tangled Web

Google Threat Intelligence Group has published several blogs since May that consider whether certain threat actors might be related to Scattered Spider, ShinyHunters, or both.

The June 4th post on UNC 6040 seemed somewhat self-contradictory. GITG defines 6040 as

> .. a financially motivated threat cluster that specializes in voice phishing (vishing) campaigns specifically designed to compromise organizations’ Salesforce instances for large-scale data theft and subsequent extortion. Over the past several months, UNC6040 has demonstrated repeated success in breaching networks by having its operators impersonate IT support personnel in convincing telephone-based social engineering engagements. This approach has proven particularly effective in tricking employees, often within English-speaking branches of multinational corporations, into actions that grant the attackers access or lead to the sharing of sensitive credentials, ultimately facilitating the theft of organization’s Salesforce data. In all observed cases, attackers relied on manipulating end users, not exploiting any vulnerability inherent to Salesforce.

The preceding paragraph might suggest that 6040 is linked to ShinyHunters, since that group has claimed responsibility for the Salesforce-related attacks and extortion demands to some victims have been signed “ShinyHunters.” But then, the blog post continues:

> In some instances, extortion activities haven’t been observed until several months after the initial UNC6040 intrusion activity, which could suggest that UNC6040 has partnered with a second threat actor that monetizes access to the stolen data. During these extortion attempts, the actor has claimed affiliation with the well-known hacking group ShinyHunters, likely as a method to increase pressure on their victims.

So UNC6040 is not ShinyHunters but is Scattered Spider who partners with ShinyHunters? Google tried to clarify by issuing yet another UNC number: 6240. *BleepingComputer* reports:

> GTIG attributes multiple incidents impacting Salesforce instances to UNC6040. In at least some cases, the follow-on extortion activity, which we attribute to the distinct threat cluster UNC6240, has used the ShinyHunters brand," Stark told *BleepingComputer*.
>
> The extortion activity is attributed to UNC6240 instead of UNC6040 due to a significant time gap between the initial data theft activity and the subsequent extortion activity. We have not confirmed the nature of the relationship between these intrusions and the prior use of this handle on underground forums.

Abrams addresses the attribution confusion in a recent post:

> The breaches have caused confusion among the cybersecurity community and the media, including BleepingComputer, with the attacks attributed to Scattered Spider (tracked by Mandiant as UNC3944), as those threat actors were also targeting the aviation, retail, and insurance sectors around the same time and demonstrated similar tactics.
>
> However, threat actors associated with Scattered Spider tend to perform full-blown network breaches, culminating with data theft and, sometimes, ransomware. ShinyHunters, tracked as UNC6040, on the other hand, tends to focus more on data-theft extortion attacks targeting a particular cloud platform or web application.
>
> It is BleepingComputer's and some security researchers' belief that both UNC6040/UNC6240 and UNC3944 consist of overlapping members that communicate within the same online communities. The threat group is also believed to overlap with "The Com," a network of experienced English-speaking cybercriminals.

Is the time gap between attack and extortion attempt really significant or an indicator for attribution? According to someone knowledgable about ShinyHunters' operations, there is a simple explanation for the gap: the threat actors are planning to do a mass extortion campaign simultaneously on every affected company. Qantas and Allianz Life were extorted immediately after they made a public disclosure, but other victims who have not publicly disclosed have not been extorted yet.

DataBreaches has also tried to sort out the attribution and whether Scattered Spider and ShinyHunters are collaborating or have shared affiliates, or … something. Was ShinyHunters just providing extortion services for Scattered Spider, or is there more to the relationship?

Enter @Sp1d3rhunters

While some news outlets were attributing breaches to DragonForce and Scattered Spider, DataBreaches was seeing — or thought she was seeing — indications of involvement by ShinyHunters.

DataBreaches' investigation into the PowerSchool attack and extortion attempt — and then the second round of extortion attempts — had yielded a ToxID and a BTC wallet used by the threat actors/extortionists.

DataBreaches first reached out to the Tox account on June 11 to ask about the second round of extortions, but received no reply at the time. DataBreaches also attempted to do a blockchain analysis of the BTC wallet that was

in the extortion demand email. That analysis eventually led to two payments made to the wallet that would be consistent with what a source had told me — PowerSchool paid almost $3 million to the wallet, divided into two payments over five days. But there was also another payment DataBreaches spotted — one for 4 BTC on June 4. At the time, DataBreaches did not know the source of that payment, but later learned from a source with knowledge of the situation that LVMH had informed law enforcement that they had paid ShinyHunters 4 BTC in response to extortion demands stemming from attacks on some of its brands, including Dior and Tiffany.

So ShinyHunters wasn't just allowing their name to be used as part of extortion demands. They were also receiving payments.

On some date unknown to DataBreaches, a new Telegram account appeared: @Sp1d3rhunters. Was this an account used for collaboration between ShinyHunters and Scattered Spider? Was it a troll?

DataBreaches messaged that account yesterday with a question: "So.. is there going to be any announcement that ShinyHunters and ScatteredSpider are merging, or will there be any formal acknowledgement of collaboration on some activities?'

Somewhat to my surprise, I received an answer. And even more shockingly, it appeared to be from ShinyHunters himself — the leader/owner of ShinyHunters who was supposed to be in a prison in France. I will refer to him as "Shiny" in the following section. As background, DataBreaches has chatted with "Shiny" many times over the past few years. Many of the chats occasionally wander off into other matters where only he would know what we had discussed and what he had said in the past.

Whoever answered me certainly wrote like Shiny, but given that France had announced his arrest and the person they arrested is still currently detained in prison there, I needed to try to authenticate whoever was answering me on this Telegram account. While the obvious inquiry might be for a pgp-signed message, sources had told me that more than one person had access to the PGP key, so that would not be conclusive. Over the course of the ensuing chat, I asked Shiny some questions that only he and I would know the answers to, based on our previous chats over the past few years. And because the chat was in real-time, I could see that there was no hesitation or delay in answering certain questions. The person I refer to as Shiny is a high-IQ individual, possibly diagnosed with ASD, and he has an amazing memory for past conversations and events. Towards knowledge-based authentication (KBA):

One of the first questions I asked him was to name someone we both hated. Without hesitation, he correctly named the person and added three aliases the individual used. I've redacted his answer in the screengrab, but it was correct.

During the chat, Shiny also showed me several screengrabs of chats of ours in the past.

At one point, he spontaneously inquired about someone he had asked me about several times in the past — someone he cares about.. He asked how that person was doing now, which is a question he had often asked me.

Shiny also made other statements about his interactions with someone that I won't describe here except to say that his statements were fairly specific and I was able to confirm the accuracy of his claims.

At another point, I asked him about a former moderator and he abruptly answered that he didn't care about that person. His dismissive response was totally consistent with his past comments to me about that person.

Not once during our chat did Shiny claim he didn't remember in response to any question I asked him. And the writing style was totally consistent with all of our past chats.

If I was being trolled, this was the best troll ever.

But if I wasn't being trolled and if Shiny isn't in a French prison and being represented by Juan Branco, then who is sitting in that prison? Did French law enforcement really make two incorrect arrests or attributions?

The media had reported that the lawyer representing the French national accused of being "TriHash" was not "TriHash," but was a student. DataBreaches does not know what has happened in that case, but "TriHash," who is also known as "Hollow," appears to be active on the resurrected BreachForums as an administrator, and Shiny also volunteered that French law enforcement had not caught him. That leaves the supposed leader, who Shiny says is not him, "Noct" and "Depressed." DataBreaches does not know what each of those men is actually charged with, but Shiny stated that "Noct" was known more recently as Sanggiero on BreachForums. Shiny described Sanggiero as an "affiliate," but see the update of August 13 below this post.

As to who Juan Branco is representing, Shiny claims that Branco's client is just an associate, and compared the situation to the arrest of "Sezyo" (Sebastien Raoult), where law enforcement made a big deal about someone who was not a major factor. In email communications to DataBreaches, Branco agrees with Shiny that his client is not the leader of ShinyHunters.

So Now Back to the Two Groups or One Group Question

Because it seemed that the person I was chatting with was really the leader of ShinyHunters, I returned to my original question:

> Dissent: There is talk that SH is coming up with its own ransomware. Is that true, or were they talking about Scattered Spider? I think the two groups are getting mixed up sometimes.
>
> Shiny: Both groups are the same now.
>
> Dissent: But no wedding announcement and wedding invites? OK. 🙂
>
> Shiny: They've always been the same.
>
> Shiny: Who says PowerSchool wasn't done by Scattered Spider lol

DataBreaches does not know whether they truly have always been the same, but the question about Scattered Spider being involved in PowerSchool gave me pause. Matthew Lane had acquired an employee's credentials from an infostealer, a method that is frequently seen in Scattered Spider attacks. Was Lane overlapping with Scattered Spider or someone in "The Com?" DataBreaches does not know, but Shiny also commented to DataBreaches that the second extortion attempts had not been authorized by him:

I've had some affiliates who don't listen. I didn't extort PS clients, the affiliates took it upon themselves to extort PS clients for more money.

Is Your Head Spinning Yet?

Even though "Sp1d3rhunters" doesn't seem to be any official name for the combination, it may be the most accurate way to think of them going forward.

DataBreaches has been shown some of the recent court injunctions stemming from cyberattacks on Qantas in Australia and the Legal Aid Agency (LAA) in the UK. Both injunctions were served on ShinyHunters. If Scattered Spider was also involved and if the two entities are not really one group, are the injunctions somewhat deficient if they don't also name Scattered Spider as defendants to be bound by the terms of the injunction?

But for now: did France really arrest the man who is the leader of ShinyHunters? If they did, who has taken over and who was able to answer so many questions yesterday on Telegram? And if France didn't arrest the leader as they had claimed to have done, do they know they didn't get him?

DataBreaches has tried to reach out to the FBI to see if they believe that France has arrested the leader of ShinyHunters. If a response is received, this post will be updated.

Update of August 13: In a Telegram channel today, a voice chat purportedly involving Baphomet, Sanggiero, and others was posted. Shiny wrote, “Here we go again, another episode of (fed) BreachForums. I’m sure we all know that Baphomet and some know Sanggiero were feds.” This seems to contradict what he said recently that “Noct” was “Sanggiero,” and “Sangierro” was an “affiliate.” DataBreaches asked Shiny to explain what seemed like a contradiction, and he explained that when he called someone a “fed,” it didn’t necessarily mean an employee of the FBI. The term is also used to describe someone who may have been raided or caught and then snitches or reveals information on others to the FBI during interrogations.
