ShinyHunters sent Google an extortion demand; Shiny comments on current activities - DataBreaches.Net

Published: 2025-08-08 · Archived: 2026-04-09 02:21:24 UTC

Yesterday morning, DataBreaches woke up to a message on Telegram:

> Even the NSA can't stop or identify us anymore. The FBI and everyone else is irrelevant and incompetent as far as we're concerned :).

When DataBreaches asked ShinyHunters if anything in particular had inspired that statement, "Shiny[1]" responded:

> I heard the NSA is investigating and analyzing voice call recordings from companies who were affected and attempts by us. The companies that are receiving SE calls are Scattered Spider then providing us the access to dump these companies if successful.

DataBreaches followed up by asking Shiny why he thought the voice analyses would be nonproductive and that NSA was incompetent. He replied:

> Those are AI generated voices. For example, they won't be able to locate anyone based off background noises such as powerline humming noise that you can't hear. They can't cross reference the power companies logs with time frames of us calling these companies since theres fluctuations in the frequencies, it's not always 60hz but ours is consistently 60-12hz. They can use such information to get an approximate location but in our case no, not possible. Forget about triangulation technology too, that wouldn't work. We were providing state of the art SIP providers.

Note: Less than 24 hours after publication, a several people claimed that the above statement was factually inaccurate (although that is not the words they used). They claimed that Scattered Spider is using their real voices on the calls. Could their opsec really be that bad? DataBreaches does not know.

There were other topics also discussed in the chat yesterday, and some of what we discussed is reported below.

France

Shiny was not only mad at law enforcement and Google, it seems, but also **LVMH**, the parent company of Dior and Tiffany, two brands that were attacked as part of the Salesforce campaign. At one point, Shiny commented that he didn't think law enforcement would be going after them so hard if it wasn't for pressure by LVMH. DataBreaches asked if Shiny really thought that LVMH had that much effect and were making a difference.

> Yes, those multi hundred billionaires think they have a say and power but they don't.
>
> If trillionaires like Google can't stop us then billionaires are nothing. Law enforcement doesn't have such funding or massive budgets either. They will forget about us in a month or two once we're done.

> Then we'll come back and launch another several months to year long sophisticated campaign, Snowflake 3.0. Next time it's going to be much much worse.

DataBreaches asked Shiny if he thought that pressure from LVMH had pushed French law enforcement into making faster arrests?

"France rushed to make FALSE, INACCURATE arrests," he replied, adding, "I, personally, am not no where near France." But of course, we would expect him to say that even if he is in France.

It is not obvious to DataBreaches why LVMH would be so allegedly aggressive in pursuing ShinyHunters. Certainly a lot of companies have been hit a lot worse. Sources with knowledge of the attacks and LVMH's response had previously told DataBreaches that LVMH had paid about 4 BTC in extortion to cover all of their breached brands, meaning Dior, Tiffany, and (although it has not been publicly disclosed by LVMH or the brand), Celine.

But Shiny clearly has a lot of anger towards France, and states that they are aggressively targeting France now: "My only directives are to target the USA, UK, AU, CA, and France. And to not touch Russia, China, and North Korea at all."

Australia

Targeting Australia seems to be related to Scattered Spider members. During the chat, Shiny stated:

> Half of the Scattered Spider is in the USA, UK, or Australia. Why do you think we suddenly hit Qantas and other major Australian companies? Some kid was begging us to hack them.
>
> Any significant arrests yield from our counterpart, Scattered Spider? No. Forget the four UK arrests, those guys were retards hence why I didn't ransom M&S for them, amoung others.

But mentioning Qantas apparently reminded Shiny of the injunction they had been sent, and he shared a copy of their response to Qantas with DataBreaches, saying it had been emailed to Qantas:

> Thank you but we will not be complying with any court orders as we have no obligation to do so since we reside outside of your jurisdiction. Even if we resided within your jurisdiction, we do not care, and we wouldn't comply. Keep in mind this data will be going public very soon. We gave you a chance and we are willing to give one last chance for you to comply, negotiate, and resolve this situation.
>
> When we start leaking the data, we will first start off by leaking the data of every federal judge and every federal officer of Australia. If you do not comply at that point we will leak the entire thing.
>
> Stop doing what you did with Optus, AFP. This time injunction orders won't stop us. You are irrelevant, weak, and incompetent. Good luck with the "external parties" you redacted from the documents, as we already know who they are.
>
> You have 24 hours to start negotiating, we dropped the price by another $1m. The offer now remains at $1m. Stop this nonsense and make the correct decision and pay the ransom. If you keep stalling, it will be leaked. Do not waste time.

Shiny states they also emailed the following to the AFP, ASD, and Home Affairs of Australia:

> Hello, we are responsible for the Qantas Airways Limited cyber attack as you know and we will be responsible for the many forthcoming cyber incidents affecting various Australian industries in the coming days and weeks ahead.
>
> We wanted to let you know this ourselves to expose what we view as systemic ignorance and arrogance within Australia's cyber security landscape: – this message is being issued directly to highlight the consequences of the decision to not to meet our demands in Qantas Airways Limited settlement which was intended to prevent widespread disruption across Australia. Once our campaign concludes, we will begin contacting the affected organizations individually.
>
> We trust this will serve as a clear demonstration of the impact of that decision and hope our future demands are met, which would put a stop to our widespread disruption campaign across Australia.
>
> – ShinyHunters

"Complete idiots to think such court orders have any relevancy or affect," Shiny commented after sharing the correspondence.

ShinyHunters' response to the injunction actually makes a point DataBreaches had raised in a July 18 commentary on such injunctions in general. DataBreaches had written:

> **The reality is that criminals who would leak the data or sell it via the internet generally don't give a damn about any court injunctions and will leak it anyway.** The only ones who are then really affected by injunctions or superinjunctions are media outlets who would want to report on the situation to inform the public and members of the public who might be affected by a breach but not know about it if the entity has not been transparent in any disclosure.

More on Google

Yesterday morning, ShinyHunters also stated that they had sent Google an extortion demand. He didn't not reveal the exact time, but it was after Google had publicly revealed the breach in an update on their blog. The extortion demand reportedly included attached samples of files. DataBreaches was not shown any copy of the email or demand.

"Within 1 hour [of sending the email] they saw our email and downloaded the samples multiple times," Shiny stated, adding, "I bet they were waiting for the email LOL. I purposely sent it from my main email… I hope I don't get banned again."

Shiny later commented, "I wasn't going to ransom them because when we start leaking the data of companies who haven't paid I wanted to drop Google's database first aince its the most hottest one."

He declined to reveal how much the demand was and what deadline Google had been given.

Minutes later, Shiny somewhat casually announced, "Going to attack them again >.>"

When DataBreaches asked if he was serious, he replied, “Yes why wouldn’t I? They are not stopping this. We are still dumping more companies by the day. And those poor companies have no idea.”

Shiny posted this graphic during the chat with a comment, “GTIG and FBI looking at me (Scattered Spider) drastically changing the TTPs and IoCs right when they post an update LOL.”

Shiny would not indicate when the next attack on Google would be, but DataBreaches contacted GITG to alert them of Shiny’s claim because Shiny’s past claims about hacking Google had proven true.

DataBreaches also emailed Google’s press contact to ask if they would comment on the claims about the extortion demand and ShinyHunters’ statement that they would be attacking Google again. Google responded that they will not be providing comment. but thanks for updating them and the communications.

---

[1] A note on “Shiny:”

DataBreaches uses the name”Shiny” to refer to the individual who this blogger has communicated via Telegram over the past few years. Although French police claim to have arrested the leader of ShinyHunters on June 23, doubts have been raised by this blogger and a number of people who have communicated with “Shiny” before and after the arrest date, and who are convinced that the person they are communicating with now on the Sp1d34hunters account is the same individual (and head of ShinyHunters) that they communicated with for years on various Telegram accounts or on Jabber. Keep in mind that for some accounts, more than one person could be posting or writing on a Telegram account or Jabber account, but all of us recognize the person who is currently posting on the Sp1d3rhunters account.

Because someone is still detained in a French prison and is supposedly the leader of ShinyHunters, all DataBreaches can say at this time, then, is that we are curious as to who the French have arrested. Shiny has told DataBreaches that it is an “associate” and to think of the individual or arrest as another “Sezyo” (referring to the arrest of Sebastien Raoult).

DataBreaches also knows that some people believe we have not been communicating with the head of ShinyHunters but a close associate like “Hollow” (aka TriHash, aka Clownpiece, aka Felix) or “Anastasia” (another account that has been used by more than one person). We also know that one or more other people used

the Sp1d3rhunters account in the past. But we all recognize the person currently on Sp1d3rhunters as the same person we dealt with in the past.

Either we are all wrong or the French prosecutors are. Time will tell.

As with many things Shiny has told me over the years, DataBreaches does not always have the ability to confirm or refute claims made during a chat by a threat actor, but notes that Shiny's statements about the attack on Google, Salesforce attacks, and Scattered Spider have all subsequently been verified directly or indirectly — in some cases by updates to Google's Threat Intelligence Group blog entries.

Intel analysts and intel firms will likely treat all of the claims and statements reported about Shiny in this post as "low confidence" resports. That's perfectly understandable and appropriate. I am putting this all out there so that others can pursue it and try to verify it or disconfirm it using their own tools and methods.**]**

This post was updated to add Google's response and then updated again to add a note that several people who had read this article claimed that Shiny's claims were not true and that Scattered Spider was using their real voices on calls.

Source: https://databreaches.net/2025/08/08/shinyhunters-sent-google-an-extortion-demand-shiny-comments-on-current-activities/