

Forum:[Hack Forums](#)

Thread: [ShinyHunters](#)

Tyr - September 30, 2026, 12:21 pm

Anyone been following the crazy breaches and campaigns these lads have been running?

ShinyHunters is a prominent black-hat cybercriminal and extortion group, active since 2019, responsible for some of the largest corporate data breaches globally. They are notorious for infiltrating enterprise systems, exfiltrating massive customer databases, and extorting organizations by threatening to leak sensitive data on dark web markets like BreachForums, which they have actively administered.

Key Tactics & Modus Operandi
SaaS & Supply Chain Exploitation: Rather than targeting traditional network perimeters, the group frequently compromises third-party integrations, OAuth tokens, and trusted connected applications.

Social Engineering: They rely heavily on sophisticated vishing (voice phishing) and smishing campaigns targeting corporate employees or third-party vendors to gain initial access.

Extortion: Following data exfiltration, the group typically demands large cryptocurrency ransoms, auctioning the data to other cybercriminals if the victim refuses to pay.

Major Recent Breaches (2025–2026)
FBI (September 2026): Claimed responsibility for compromising FBIJobs.gov, the bureau's recruiting portal, stealing highly sensitive personal data belonging to thousands of federal agents and applicants.

Salesforce Connected Apps Wave (August 2025): Exploited OAuth tokens and trusted SaaS integrations (such as Salesloft Drift) to seamlessly pivot into hundreds of downstream enterprise Salesforce environments, compromising data from organizations including Google, Workday, Adidas, and Louis Vuitton.

Mixpanel (November 2025): Compromised the third-party analytics provider via smishing, subsequently extracting analytics datasets to extort downstream clients including OpenAI and Pornhub.

Pre-2025 Targets: The group previously gained notoriety for massive breaches involving Ticketmaster, Santander Bank, AT&T, and Wattpad.

Law Enforcement Status

Law enforcement agencies have actively targeted the syndicate's leadership, though operations have historically continued through crackdowns. In June 2025, French authorities arrested four suspected members linked to the group's administrative roles. Most recently, in late September 2026, Dutch police—coordinating with the FBI—arrested an alleged leader of the group in Rotterdam.

Sources:

Spoiler ([Click to View](#))

<https://www.pbs.org/newshour/nation/fbi-investigates-hackers-claim-to-have-stolen-employee-data-compromised-jobs-website>

<https://www.reuters.com/world/us/fbi-official-tells-shinyhunters-hackers-we-know-how-find-you-following-dutch-2026-09-29/>

<https://www.nytimes.com/2026/09/29/us/politics/shinyhunters-fbi-hacking-cybercriminal-group.html>

HerrWinston - September 30, 2026, 12:28 pm

I havent been actively following them and their doings but I heard the name from time to time, do you think all of them are arrested now?

Very nice thread, was a good read Tyr!

Omniscient - September 30, 2026, 12:35 pm

Cooligans been missing lately. Just saying. :)

And yes, this group is getting street cred right now. I kind of like their name ShinyHunters.

Sift - September 30, 2026, 12:58 pm

Yea they are quite a group.

HerrWinston - September 30, 2026, 1:03 pm

(Sep 30, 2026 12:58 PM)Sift Wrote: [\[CITE\]](#) Yea they are quite a group.

I admit this post got me laughing lmao, i agree they are infact quite a group xD

Tyr - September 30, 2026, 3:18 pm

(Sep 30, 2026 12:28 PM)HerrWinston Wrote: [\[CITE\]](#) I havent been actively following them and their doings but I heard the name from time to time, do you think all of them are arrested now?

Very nice thread, was a good read Tyr!

Haha, absolutely not. They're quite active and obviously have sophisticated TTP to evade detection between members whether it be segmenting and isolating CoC via members to evade detection or utilizing connections throughout the globe. Of most APT's I've seen over the years, based on my general knowledge, there's literally 0 chance that they rounded everyone up who is involved in the group. Tbh they are likely funded by a large nation state group or breakaway rogue insiders from within larger enterprise organizations and/or even law enforcement gone bad (likely a mix of everything tho).

I gotta say they got some balls though, they went after literally everyone's data in the freaking FBI and were trying to hold them ransom for it. They got around 2 to 3 TB of data about individuals who applied for jobs, as well as current and former special agents and intelligence analysts. Not to mention they broke into one state's DMV like it was cake.

I'd love to see where the future takes them, not that I condone any blackhat activity but cannot help but be very impressed by their breaches.

(Sep 30, 2026 12:35 PM)Omniscient Wrote: [\[CITE\]](#) Cooligans been missing lately. Just saying. :)

And yes, this group is getting street cred right now. I kind of like their name ShinyHunters.

Yeah, it's p cool. I wonder why they chose the name. /shrug

RiveR29 - October 1, 2026, 12:58 am

I just yesterday watched a video about these guys, I had not known anything before that. But I must say that this is pretty cool to see.

And all but the truth is that the FBI most likely will go after them in some capacity. But that will be seen on a later date.

plops - October 1, 2026, 5:32 am

i always heard shinyhunters through bf some years ago. youd think its some government sanctioned group to be running this strong for 7 years.

junooo - October 1, 2026, 6:51 am

Some guy from the Netherlands got arrested like 2 days ago! It's actually really funny. The guy, some guy named Pepijn, had already been arrested before for hacking. He then went on a podcast and said that he would never do it again. He said something along the lines of "I would be stupid if I did something like that again" because he got let go early out of jail.

That reminds me, there is some other case of some teenagers hacking big companies, after which they got arrested. I remember one of them committed suicide because they couldn't live without their computer or something like that? It kinda reminds me of this case. I see a lot of these young hackers committing crimes over and over because I assume that they love the rush it gives.

Hacking ain't all about money anyway!

DemonAsylum - October 1, 2026, 5:58 pm

(Sep 30, 2026 03:18 PM)Tyr Wrote: [\[CITE\]](#) Yeah, it's p cool. I wonder why they chose the name. /shrug

It would be funny if it's as simple as what I thought of when I first saw the thread title, Pokemon lol. Shiny hunting is a big thing in Pokemon and that has been around since some of the early releases on Gameboy.

Scrub - October 1, 2026, 6:01 pm

(Oct 1, 2026 05:58 PM)DemonAsylum Wrote: [\[CITE\]](#) It would be funny if it's as simple as what I thought of when I first saw the thread title, Pokemon lol. Shiny hunting is a big thing in Pokemon and that has been around since some of the early releases on Gameboy.

This is what I was thinking it was from

DemonAsylum - October 1, 2026, 6:07 pm

(Oct 1, 2026 06:01 PM)Scrub Wrote: [\[CITE\]](#) This is what I was thinking it was from
It seems plausible, no? Shiny Hunting has been a thing since the early days of the Pokemon Gameboy games and as time has gone on it has only gotten more and more popular. Not to mention alongside how long it's been around, Pokemon is obviously one of the biggest and most recognized franchises in the world. It seems entirely possible that there is a connection between that and the name. Maybe they're big Pokemon fans lol.

Tyr - October 2, 2026, 8:13 pm

(Oct 1, 2026 05:58 PM)DemonAsylum Wrote: [\[CITE\]](#) It would be funny if it's as simple as what I thought of when I first saw the thread title, Pokemon lol. Shiny hunting is a big thing in Pokemon and that has been around since some of the early releases on Gameboy.

Man, that's probably what it is. I completely blanked out on shiny pokemon and their rarity etc. That's pretty funny. I wonder what team they primarily play in Pokemon GO? ?

(Oct 1, 2026 06:51 AM)junooo Wrote: [\[CITE\]](#) Some guy from the Netherlands got arrested like 2 days ago! It's actually really funny. The guy, some guy named Pepijn, had already been arrested before for hacking. He then went on a podcast and said that he would never do it again. He said something along the lines of "I would be stupid if I did something like that again" because he got let go early out of jail.

That reminds me, there is some other case of some teenagers hacking big companies, after which they got arrested. I remember one of them committed suicide because they couldn't live without their computer or something like that? It kinda reminds me of this case. I see a lot of these young hackers committing crimes over and over because I assume that they love the rush it gives.

Hacking ain't all about money anyway!

Well apart the darker suicide part, that's almost as funny as this article I just read where apparently these fools didn't even notice their data was exfiltrated until they were told, lmao

<https://nltimes.nl/2026/05/16/odido-noticed-theft-62-million-peoples-data-hackers-informed>

DemonAsylum - October 2, 2026, 8:27 pm

(Oct 2, 2026 08:13 PM)Tyr Wrote: [\[CITE\]](#) Man, that's probably what it is. I completely blanked out on shiny pokemon and their rarity etc. That's pretty funny. I wonder what team they primarily play in Pokemon GO? ?

I'm genuinely thinking that might be it lmao. From a logical perspective it makes complete sense and seems entirely plausible. If it happens to be a coincidence is all then I assume it's just an inside thing for them having that name. My money would be on the influence from Pokemon though. Seems like too unique of a term and that is too big of a thing in Pokemon for it to not be any bit related.

Phantom_NiNja - October 5, 2026, 10:44 am

How are they doing it? just looking up exploits in the wild and just using those exploits that is already patched and computers fail to install updates in time?

HerrWinston - October 5, 2026, 11:41 am

(Oct 2, 2026 08:27 PM)DemonAsylum Wrote: [\[CITE\]](#) I'm genuinely thinking that might be it lmao. From a logical perspective it makes complete sense and seems entirely plausible. If it happens to be a coincidence is all then I assume it's just an inside thing for them having that name. My money would be on the influence from Pokemon though. Seems like too unique of a term and that is too big of a thing in Pokemon for it to not be any bit related.

Well considering they have a pokemon as theyre picture its 100% that, still funny to me that such a large group decides to call themselves after that, imagine the original group met over a pokemon game/forum...

DemonAsylum - October 5, 2026, 1:04 pm

(Oct 5, 2026 11:41 AM)HerrWinston Wrote: [\[CITE\]](#) Well considering they have a pokemon as theyre picture its 100% that, still funny to me that such a large group decides to call themselves after that, imagine the original group met over a pokemon game/forum...

Oh shit well that seals it for sure then. Apologies, I was unaware they had such a picture as representation for themselves lol.

SUI-3183372 - October 5, 2026, 9:07 pm

(Sep 30, 2026 03:18 PM)Tyr Wrote: [\[CITE\]](#) Haha, absolutely not. They're quite active and obviously have sophisticated TTP to evade detection between members whether it be segmenting and isolating CoC via members to evade detection or utilizing connections throughout the globe. Of most APT's I've seen over the years, based on my general knowledge, there's literally 0 chance that they rounded everyone up who is involved in the group. Tbh they are likely funded by a large nation state group or breakaway rogue insiders from within larger enterprise organizations and/or even law enforcement gone bad (likely a mix of everything tho).

I gotta say they got some balls though, they went after literally everyone's data in the freaking FBI and were trying to hold them ransom for it. They got around 2 to 3 TB of data about individuals who applied for jobs, as well as current and former special agents and intelligence analysts. Not to mention they broke into one state's DMV like it was cake.

I'd love to see where the future takes them, not that I condone any blackhat activity but cannot help but be very impressed by their breaches.

Yeah, it's p cool. I wonder why they chose the name. /shrug
Helps being from Africa.

Shiny Hunters, Scattered Spider, and LAPSUSS have merged into SHINY LAPSUS HUNTERS, and internal power struggle ousted the Dutch dude who got arrested a few weeks ago, new leader

of the joint group stems from Africa, I think Jordan if I remember correctly. Small fish are a bunch of kids from the EU who go down all the time, bigger fish are more out of reach.

(All three groups still run independently as well, but the shiny lapsus hunters drama has harmed Shiny Hunters)

Tyr - October 9, 2026, 7:29 pm

(Oct 5, 2026 09:07 PM)SUI-3183372 Wrote: [\[CITE\]](#) Helps being from Africa.

Shiny Hunters, Scattered Spider, and LAPSUSS have merged into SHINY LAPSUS HUNTERS, and internal power struggle ousted the Dutch dude who got arrested a few weeks ago, new leader of the joint group stems from Africa, I think Jordan if I remember correctly. Small fish are a bunch of kids from the EU who go down all the time, bigger fish are more out of reach.

(All three groups still run independently as well, but the shiny lapsus hunters drama has harmed Shiny Hunters)

I've heard of Scattered Spider but never knew they were affiliated.

[This](#) has a ton of information that I also didn't know about if anyone following this is interested.

XtremeDiscount - October 9, 2026, 7:33 pm

Wow sounds like quite a group