

Meet Rey, the Admin of ‘Scattered Lapsus\$ Hunters’

Published: 2025-11-26 · Archived: 2026-07-28 02:00:44 UTC

A prolific cybercriminal group that calls itself “**Scattered LAPSUS\$ Hunters**” has dominated headlines this year by regularly stealing data from and publicly mass extorting dozens of major corporations. But the tables seem to have turned somewhat for “Rey,” the moniker chosen by the technical operator and public face of the hacker group: Earlier this week, Rey confirmed his real life identity and agreed to an interview after KrebsOnSecurity tracked him down and contacted his father.

Scattered LAPSUS\$ Hunters (SLSH) is thought to be an amalgamation of three hacking groups — [Scattered Spider](#), [LAPSUS\\$](#) and [ShinyHunters](#). Members of these gangs hail from many of the same chat channels on the **Com**, a mostly English-language cybercriminal community that operates across an ocean of Telegram and Discord servers.

In May 2025, SLSH members launched [a social engineering campaign](#) that used voice phishing to trick targets into connecting a malicious app to their organization’s Salesforce portal. The group later launched a data leak portal that threatened to publish the internal data of three dozen companies that allegedly had Salesforce data stolen, including **Toyota**, **FedEx**, **Disney/Hulu**, and **UPS**.

The screenshot shows a dark-themed web portal titled "Scattered LAPSUS\$ Hunters". At the top right are links for "Victims", "Contact", and "Telegram Audience". The main content area features a large card for "Salesforce, Inc." with the text "989.45m/~1B+ records". Below this, it says "Contact us to negotiate this ransom or all your customers data will be leaked. If we come to a resolution all individual extortions against your customers will be withdrawn from. Nobody else will have to pay us, if you pay, Salesforce, Inc." A purple button indicates "Salesforce, Inc. deadline: 10-10-2025 | Status: Negotiation required". A "VIEW DETAILS" button is also present. Below this, a section titled "For: Salesforce customers" lists three companies: Toyota Motor Corporations (64GB, breach date 01-05-2025), FedEx (1.1TB, breach date 31-08-2025), and Disney/Hulu (36GB, breach date 01-05-2025). Each company entry includes a "DATA-THEFT" label and a "Breach Date".

Company	Category	Data Volume	Breach Date
Toyota Motor Corporations	AUTO MOTIVE	64GB	01-05-2025
FedEx	TRANSPORTATION	1.1TB	31-08-2025
Disney/Hulu	ENTERTAINMENT	36GB	01-05-2025

The new extortion website tied to ShinyHunters, which threatens to publish stolen data unless Salesforce or individual victim companies agree to pay a ransom.

Last week, the SLSH Telegram channel featured an offer to recruit and reward “insiders,” employees at large companies who agree to share internal access to their employer’s network for a share of whatever ransom payment is ultimately paid by the victim company.

SLSH has solicited insider access previously, but their latest call for disgruntled employees started making the rounds on social media at the same time news broke that the cybersecurity firm **CrowdStrike** had fired an employee for [allegedly sharing screenshots of internal systems](#) with the hacker group (CrowdStrike said their systems were never compromised and that it has turned the matter over to law enforcement agencies).

scattered LAPSUS\$ hunters part 7

544 subscribers

Pinned message

DM us to sell your IA on % locking with all major lockers depending on target; must be ready to run AD commands

scattered LAPSUS\$ hunters part 7

DM us to **sell your IA on % locking** with all major lockers depending on target; must be ready to run **AD commands** or **Okta commands**, or show `/etc/openldap/ldap.conf` `/var/log` and `ip -a addr && ssh -i /home/$$/ssh/*pem $$@(ip addr ip's)` or anything else you find relevant to showing us

Rules:

- no companies under 500M revenue
- no RF/PRC/DPRK/Belarus companies
- no health

IA rates:

25% for any AD joined system.

10% for Okta, Azure portal, AWS IAM root, etc

were also recruiting employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefoinica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Lcaweb, and other similar)

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

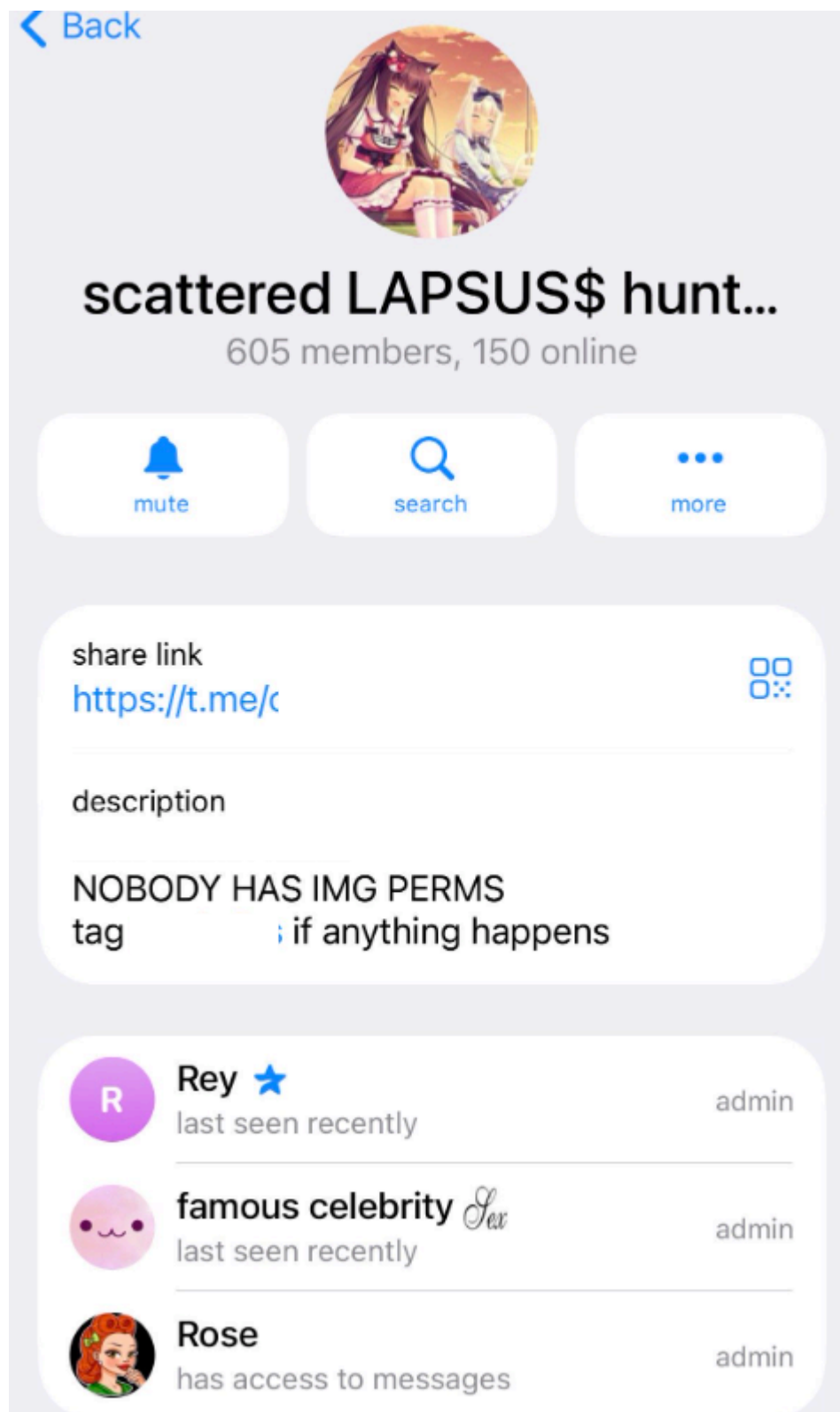
TO NOTE: WE ARE NOT LOOKING FOR DATA, WE HAVE IT ALL ALREADY, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

note: we are mainly focused on US AU UK CA FR

The Telegram server for the Scattered LAPSUS\$ Hunters has been attempting to recruit insiders at large companies.

Members of SLSH have traditionally used other ransomware gangs' encryptors in attacks, including malware from ransomware affiliate programs like ALPHV/BlackCat, Qilin, RansomHub, and DragonForce. But last week, SLSH announced on its Telegram channel [the release of their own ransomware-as-a-service operation](#) called **ShinySp1d3r**.

The individual responsible for releasing the ShinySp1d3r ransomware offering is a core SLSH member who goes by the handle “Rey” and who is currently one of just three administrators of the SLSH Telegram channel. Previously, Rey was an [administrator](#) of the data leak website for **Hellcat**, a ransomware group that surfaced in late 2024 and was involved in attacks on companies including **Schneider Electric**, **Telefonica**, and **Orange Romania**.



A recent, slightly redacted screenshot of the Scattered LAPSUS\$ Hunters Telegram channel description, showing Rey as one of three administrators.

Also in 2024, Rey would take over as administrator of the [most recent incarnation of BreachForums](#), an English-language cybercrime forum whose domain names have been seized on multiple occasions by the FBI and/or by international authorities. In April 2025, Rey [posted on Twitter/X](#) about another FBI seizure of BreachForums.

On October 5, 2025, the FBI [announced](#) it had once again seized the domains associated with BreachForums, which it described as a major criminal marketplace used by ShinyHunters and others to traffic in stolen data and facilitate extortion.

“This takedown removes access to a key hub used by these actors to monetize intrusions, recruit collaborators, and target victims across multiple sectors,” the FBI said.

Incredibly, Rey would make a series of critical operational security mistakes last year that provided multiple avenues to ascertain and confirm his real-life identity and location. Read on to learn how it all unraveled for Rey.

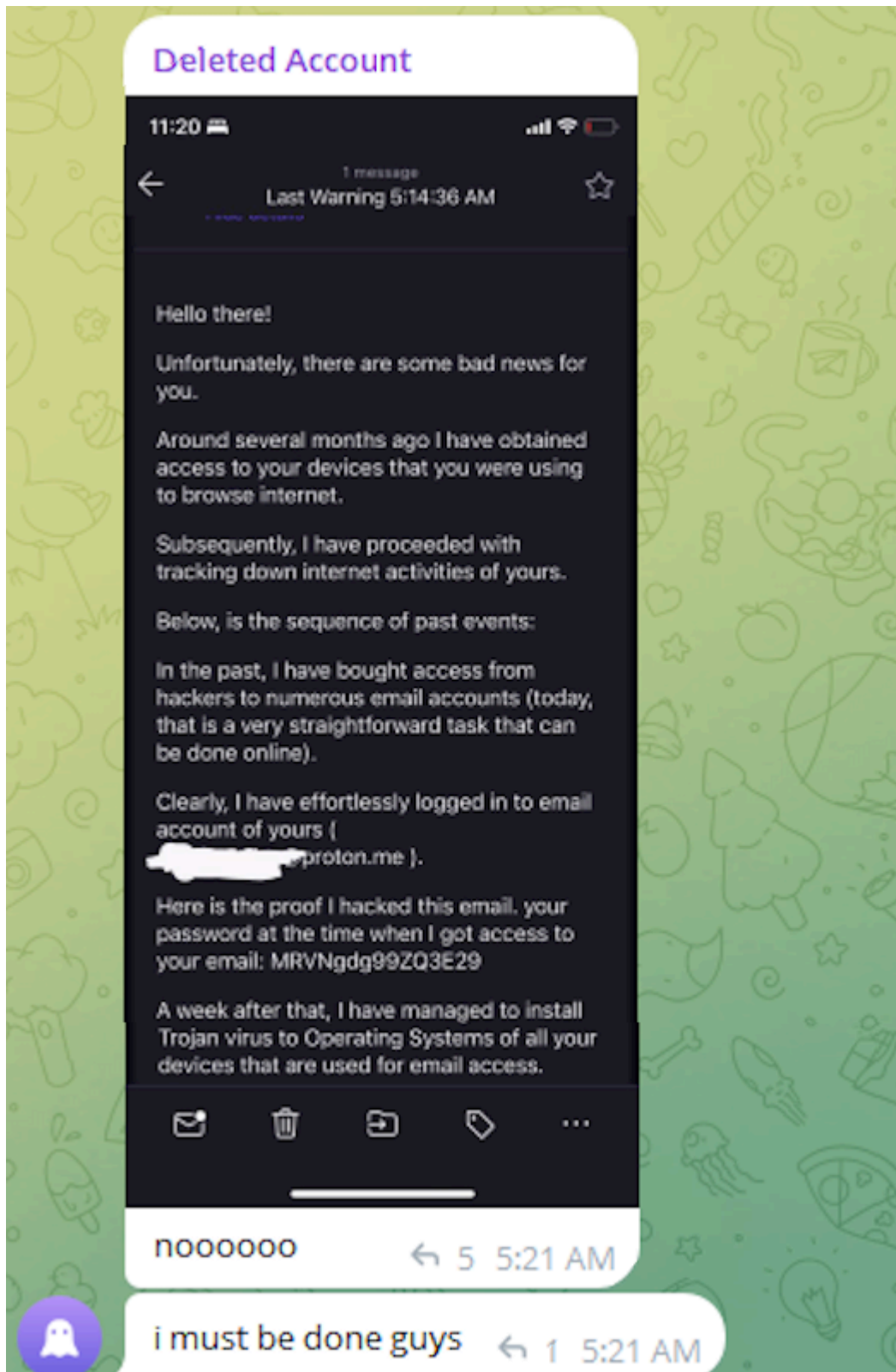
WHO IS REY?

According to the cyber intelligence firm **Intel 471**, Rey was an active user on various **BreachForums** reincarnations over the past two years, authoring more than 200 posts between February 2024 and July 2025. Intel 471 says Rey previously used the handle “**Hikki-Chan**” on BreachForums, where their first post shared data allegedly stolen from the **U.S. Centers for Disease Control and Prevention (CDC)**.

In that February 2024 post about the CDC, Hikki-Chan says they could be reached at the Telegram username **@wristmug**. In May 2024, @wristmug posted in a Telegram group chat called “Pantifan” a copy of an extortion email they said they received that included their email address and password.

The message that @wristmug cut and pasted appears to have been part of an [automated email scam](#) that claims it was sent by a hacker who has compromised your computer and used your webcam to record a video of you while you were watching porn. These missives threaten to release the video to all your contacts unless you pay a Bitcoin ransom, and they typically reference a real password the recipient has used previously.

“Nooooooo,” the @wristmug account wrote in mock horror after posting a screenshot of the scam message. “I must be done guys.”



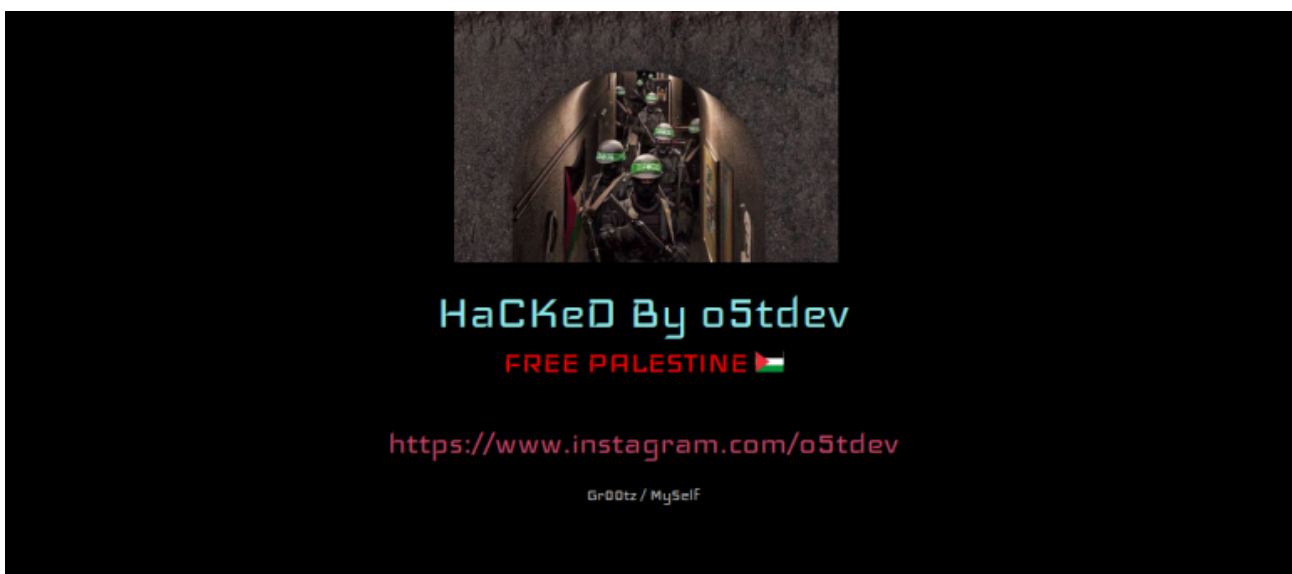
A message posted to Telegram by Rey/@wristmug.

In posting their screenshot, @wristmug redacted the username portion of the email address referenced in the body of the scam message. However, they did not redact their previously-used password, and they left the domain portion of their email address (@proton.me) visible in the screenshot.

O5TDEV

Searching on @wristmug's rather unique 15-character password in the breach tracking service **Spycloud** finds it is known to have been used by just one email address: **cybero5tdev@proton.me**. According to Spycloud, those credentials were exposed at least twice in early 2024 when this user's device was infected with an infostealer trojan that siphoned all of its stored usernames, passwords and authentication cookies (a finding that was [initially revealed](#) in March 2025 by the cyber intelligence firm **KELA**).

Intel 471 shows the email address cybero5tdev@proton.me belonged to a BreachForums member who went by the username **o5tdev**. Searching on this nickname in Google brings up at least two website defacement archives showing that a user named o5tdev was previously involved in [defacing sites with pro-Palestinian messages](#). The screenshot below, for example, shows that O5tdev was part of a group called **Cyb3r Drag0nz Team**.



Rey/o5tdev's defacement pages. Image: archive.org.

A 2023 report from **SentinelOne** described Cyb3r Drag0nz Team as a hacktivist group with a history of launching DDoS attacks and cyber defacements as well as engaging in data leak activity.

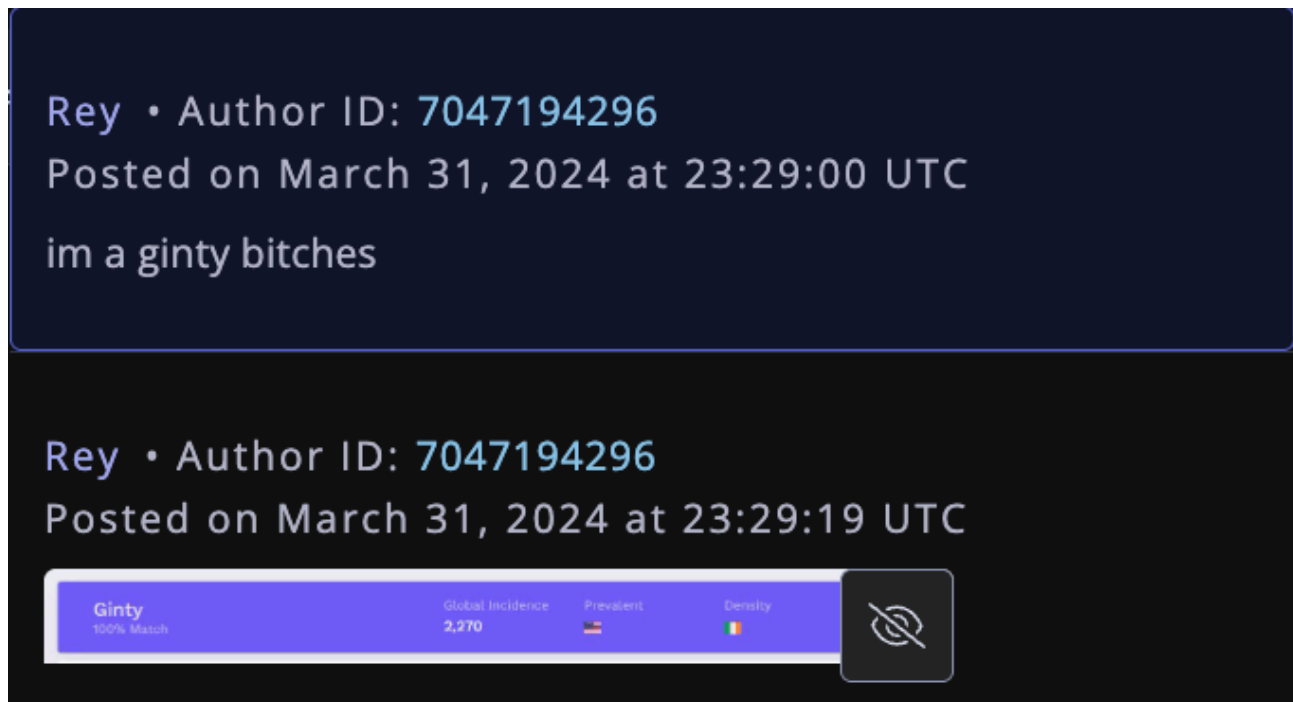
“Cyb3r Drag0nz Team claims to have leaked data on over a million of Israeli citizens spread across multiple leaks,” SentinelOne [reported](#). “To date, the group has released multiple .RAR archives of purported personal information on citizens across Israel.”

The cyber intelligence firm **Flashpoint** finds the Telegram user @o5tdev was active in 2023 and early 2024, posting in Arabic on anti-Israel channels like “Ghost of Palestine” [full disclosure: Flashpoint is currently an advertiser on this blog].

‘I’M A GINTY’

Flashpoint shows that Rey's Telegram account (ID7047194296) was particularly active in a cybercrime-focused channel called **Jacuzzi**, where this user shared several personal details, including that their father was an airline pilot. Rey claimed in 2024 to be 15 years old, and to have family connections to Ireland.

Specifically, Rey mentioned in several Telegram chats that he had Irish heritage, even posting a graphic that shows the prevalence of the surname “**Ginty**.”



Rey, on Telegram claiming to have association to the surname “Ginty.” Image: Flashpoint.

Spycloud indexed hundreds of credentials stolen from cybero5dev@proton.me, and those details indicate that Rey’s computer is a shared Microsoft Windows device located in Amman, Jordan. The credential data stolen from Rey in early 2024 show there are multiple users of the infected PC, but that all shared the same last name of Khader and an address in Amman, Jordan.

The “autofill” data lifted from Rey’s family PC contains an entry for a 46-year-old **Zaid Khader** that says his mother’s maiden name was Ginty. The infostealer data also shows Zaid Khader frequently accessed internal websites for employees of **Royal Jordanian Airlines**.

MEET SAIF

The infostealer data makes clear that Rey’s full name is **Saif Al-Din Khader**. Having no luck contacting Saif directly, KrebsOnSecurity sent an email to his father Zaid. The message invited the father to respond via email, phone or Signal, explaining that his son appeared to be deeply enmeshed in a serious cybercrime conspiracy.

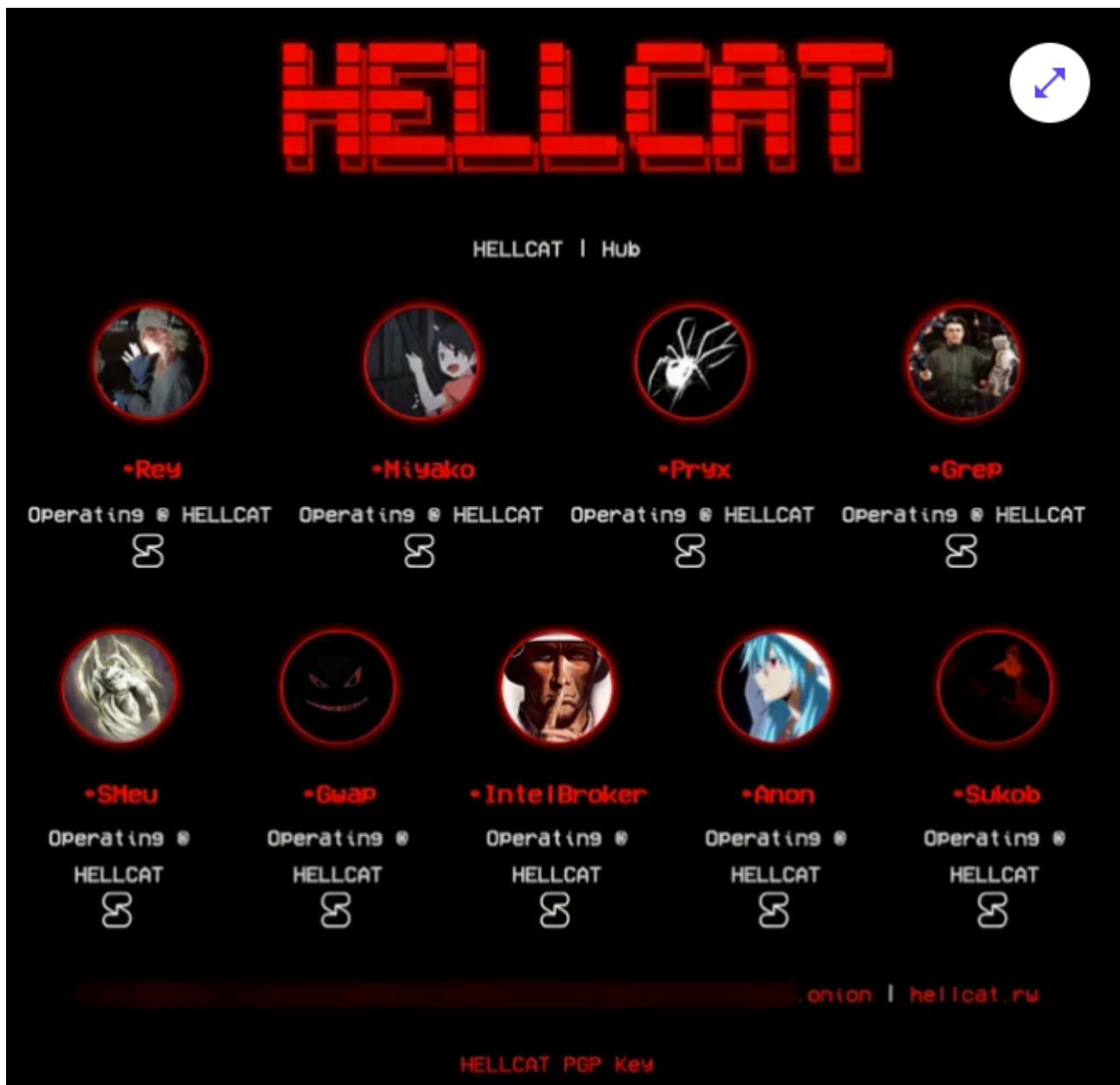
Less than two hours later, I received a Signal message from Saif, who said his dad suspected the email was a scam and had forwarded it to him.

“I saw your email, unfortunately I don’t think my dad would respond to this because they think its some ‘scam email,’” said Saif, who told me he turns 16 years old next month. “So I decided to talk to you directly.”

Saif explained that he’d already heard from European law enforcement officials, and had been trying to extricate himself from SLISH. When asked why then he was involved in releasing SLISH’s new ShinySp1d3r ransomware-

as-a-service offering, Saif said he couldn't just suddenly quit the group.

“Well I cant just dip like that, I'm trying to clean up everything I'm associated with and move on,” he said.



The former Hellcat ransomware site. Image: Kelacyber.com

He also shared that ShinySp1d3r is just a rehash of Hellcat ransomware, except modified with AI tools. “I gave the source code of Hellcat ransomware out basically.”

Saif claims he reached out on his own recently to the Telegram account for **Operation Endgame**, the codename for an ongoing law enforcement operation [targeting cybercrime services, vendors and their customers](#).

“I’m already cooperating with law enforcement,” Saif said. “In fact, I have been talking to them since at least June. I have told them nearly everything. I haven’t really done anything like breaching into a corp or extortion related since September.”

Saif suggested that a story about him right now could endanger any further cooperation he may be able to provide. He also said he wasn't sure if the U.S. or European authorities had been in contact with the Jordanian government about his involvement with the hacking group.

"A story would bring so much unwanted heat and would make things very difficult if I'm going to cooperate," Saif said. "I'm unsure what's going to happen they said they're in contact with multiple countries regarding my request but it's been like an entire week and I got no updates from them."

Saif shared a screenshot that indicated he'd contacted Europol authorities late last month. But he couldn't name any law enforcement officials he said were responding to his inquiries, and KrebsOnSecurity was unable to verify his claims.

"I don't really care I just want to move on from all this stuff even if it's going to be prison time or whatever they gonna say," Saif said.

Source: <https://krebsonsecurity.com/2025/11/meet-rey-the-admin-of-scattered-lapsus-hunters/>