

# Scattered LAPSUS\$ Hunters: the cybercrime alliance that will shake global businesses in 2025

By Florent Chassignol

Published: 2025-12-01 · Archived: 2026-07-28 02:00:14 UTC

Launched in August 2025, the **Scattered LAPSUS\$ Hunters** (SLSH) collective has rapidly established itself as one of the most formidable threats on today's cybercriminal landscape. This alliance brings together three of the most notorious English-speaking cybercriminal groups: **Scattered Spider**, **LAPSUS\$** and **ShinyHunters**. In just a few months, this organization has multiplied spectacular attacks against leading companies, stealing billions of pieces of data and perfecting the art of digital extortion.

## Table des matières

- [A strategic merger with financial motivations](#)
  - [The origins of an unprecedented alliance](#)
  - [Emergence on Telegram](#)
- [The Com ecosystem: a breeding ground for cybercriminals](#)
- [Rey: the public face of a criminal empire](#)
  - [Identity revealed](#)
  - [An early career in cybercrime](#)
  - [Cooperation with the authorities?](#)
- [Attack techniques: sophistication and social engineering](#)
  - [Vishing and identity theft](#)
  - [Bypassing multi-factor authentication](#)
  - [Supply chain attacks](#)
  - [Technical tactics mapping \(MITRE ATT&CK\)](#)
- [An impressive death toll](#)
  - [The Salesforce campaign: 760 companies compromised](#)
  - [The airline industry in turmoil](#)
  - [Jaguar Land Rover: an attack with historic economic consequences](#)
  - [British distribution paralyzed](#)
  - [Law enforcement and government agencies](#)
  - [The insider at CrowdStrike](#)
- [ShinySp1d3r: in-house ransomware-as-a-service](#)
  - [The launch of a RaaS infrastructure](#)
  - [Technical features](#)
  - [Spectacular threats](#)
- [Organizational structure: between fiction and reality](#)
  - [An architecture of personas](#)

- [The business model: extortion and services](#)
  - [Systematic double extortion](#)
  - [Extortion-as-a-service \(RaaS\)](#)
  - [Recruiting insiders](#)
- [Responses from the authorities](#)
  - [FBI seizures](#)
  - [Arrests in France](#)
  - [Advisories and alerts](#)
  - [The spectacular farewell of September 2025](#)
  - [Immediate return to business](#)
- [Protection recommendations](#)
  - [Securing identities and access](#)
  - [Endpoint hardening](#)
  - [Monitoring cloud and SaaS applications](#)
  - [Training and awareness](#)
- [Implications for the cybersecurity landscape](#)
  - [The evolution towards malware-free attacks](#)
  - [Identity as the new perimeter](#)
  - [The professionalization of cybercrime](#)
- [Conclusion: a persistent and evolving threat](#)

## A strategic merger with financial motivations

### The origins of an unprecedented alliance

Scattered LAPSUS\$ Hunters represents a major evolution in the cybercriminal ecosystem. Rather than a formal merger, it is a **federated identity** where several players collaborate, amplify each other and share a common infrastructure, while retaining a degree of operational autonomy. This decentralized structure is distinguished from traditional criminal organizations by its fluidity and resilience.

The three founding groups each bring their own specific skills to the table:

- **Scattered Spider**: advanced mastery of social engineering, vishing (voice phishing) and attacks on IT support centers;
- **LAPSUS\$**: expertise in SIM swapping, multi-factor authentication bypass techniques and high-profile extortion campaigns;
- **ShinyHunters**: specializing in massive data exfiltration and monetization on underground forums.

### Emergence on Telegram

The collective made its public appearance via Telegram on August 8, 2025, under the channel name “scattered lapsu\$ hunters – The Com HQ SCATTERED SP1D3R HUNTERS”. Since then, **the Telegram channel has been deleted and recreated 16 times since August 8, 2025**, a documented cadence that reflects both the pressure of the platform’s moderators and the group’s operational resilience.

The group uses sophisticated systems to maintain its presence, including a **laundering network based on Telegram’s Gift/Stars functionality**, enabling low-friction affiliate payments and channel boosts. This system facilitates the monetization of their ransomware-as-a-service model.

This presence on Telegram is not insignificant: it forms the **core of their brand identity**. This is where members stage their exploits, coordinate their actions, threaten their victims and recruit new accomplices. The latest channel, “scattered LAPSUS\$ hunters 7.0”, has also been deleted, with members indicating that they wish to enter a period of indefinite dormancy.

| Links to the Channel/Groups           | Activity Periods of Those Links                |
|---------------------------------------|------------------------------------------------|
| t[.]me/scatteredlapsusp1d3rhunters    | Created Aug. 8, 2025, banned Aug. 11, 2025     |
| t[.]me/scatteredsp1d3rhunters         | Created Aug. 9, 2025, banned Aug. 11, 2025     |
| t[.]me/fuckmandiantunit221bcr0wdshart | Created Aug. 10, 2025, banned Aug. 12, 2025    |
| t[.]me/sp1d3rlapsushunters            | Created Aug. 11, 2025, banned Aug. 12, 2025    |
| t[.]me/leavemealonefbi                | Created Aug. 12, 2025, disabled Aug. 22, 2025  |
| t[.]me/sc4ttered                      | Created Aug. 14, 2025, banned Aug. 15, 2025    |
| t[.]me/leavemealonemandiant           | Created Aug. 16, 2025, disabled Aug. 18, 2025  |
| t[.]me/sctt3rd                        | Created Aug. 28, 2025, disabled Sept. 16, 2025 |
| t[.]me/freejared                      | Created Aug. 30, 2025, disabled Sept. 9, 2025  |
| t[.]me/leavemealonenca                | Created Sept. 30, 2025, disabled Oct. 1, 2025  |
| t[.]me/johnlongmire                   | Created Oct. 1, 2025, disabled Oct. 1, 2025    |
| t[.]me/specialagentadam               | Created Oct. 2, 2025, disabled Oct. 2, 2025    |
| t[.]me/SLSH_kashpatel                 | Created Oct. 2, 2025, disabled Oct. 3, 2025    |
| t[.]me/brostopbanning                 | Created Oct. 3, 2025, disabled Oct. 4, 2025    |
| t[.]me/scatteredwizard                | Created Oct. 4, 2025, disabled Oct. 4, 2025    |
| t[.]me/andrewfedman and t.me/slsh69   | Created Oct. 2, 2025, disabled Oct. 15, 2025   |
| t[.]me/slshchat                       | Created Oct. 6, 2025, disabled Oct. 15, 2025   |
| t[.]me/ripalldaguyz                   | Created Oct. 15, 2025, disabled Oct. 17, 2025  |

Scattered LAPSUS\$ Hunters Telegram channel history – Source: Trustwave SpiderLabs

## The Com ecosystem: a breeding ground for cybercriminals

SLSH is part of a wider movement known as “**The Com**”, an informal, decentralized English-speaking cybercriminal ecosystem. This network functions more like a cybercriminal youth movement than a structured organization, bringing together mainly teenagers and young adults in their twenties.

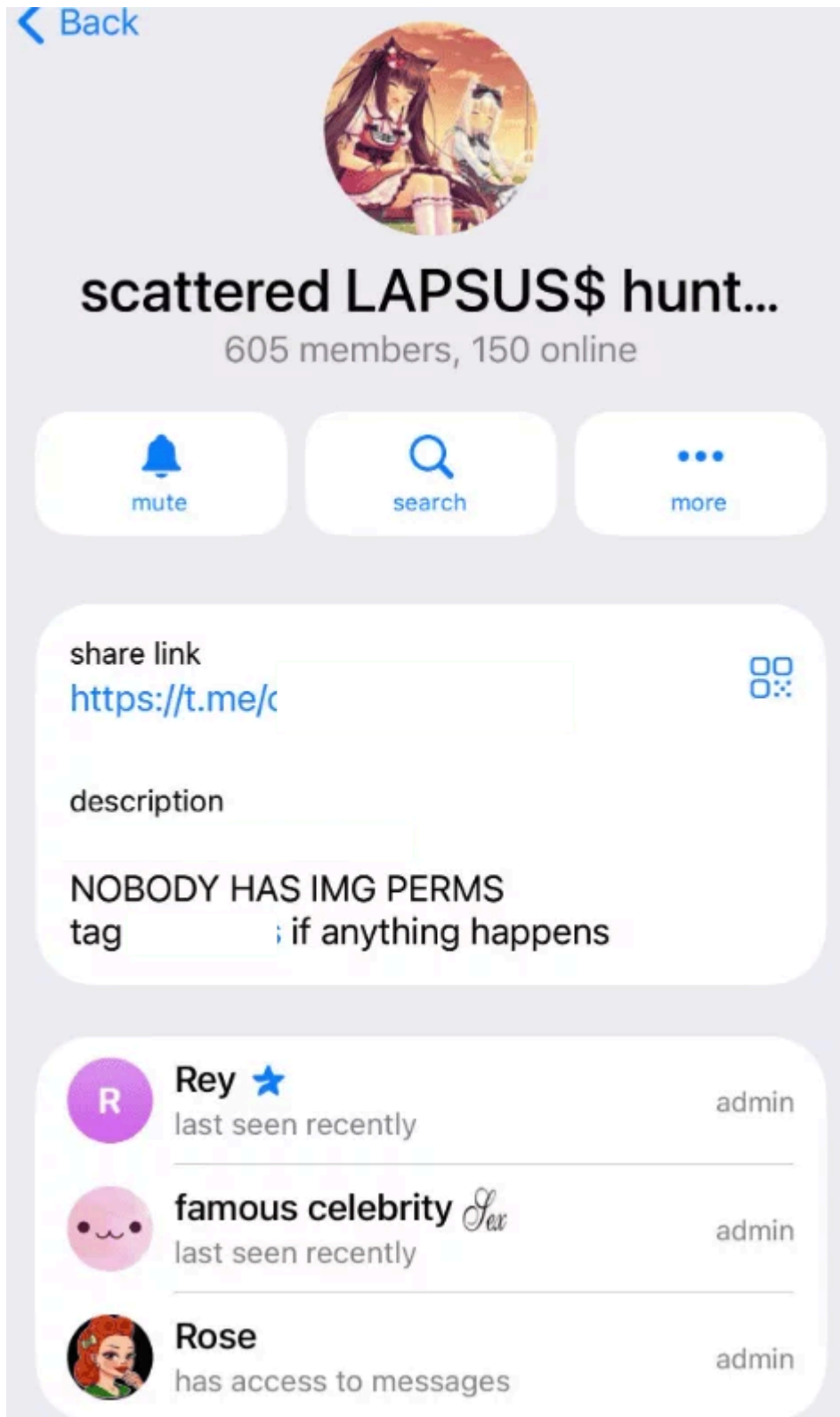
The FBI has issued a specific warning about the risks associated with participation in these movements, pointing out that many members are minors who do not fully appreciate the legal consequences of their actions.

## Rey: the public face of a criminal empire

### Identity revealed

In November 2025, cybersecurity journalist Brian Krebs revealed the real identity of “Rey”, one of the three administrators of SLSH’s Telegram channel and a central figure in the group. **Rey is actually Saif Al-Din**

**Khader, a 15-year-old Jordanian teenager** (16 in December 2025) whose father works as a pilot for Royal Jordanian Airlines.



Scattered LAPSUS\$ Hunters Telegram channel showing Rey as one of 3 admin – Source: KrebsOnSecurity

Rey's identification is the result of a series of operational security errors. In May 2024, Rey posted on Telegram a screenshot of a scam email claiming to have compromised his computer. In this screenshot, he had masked the username from his email address but left the domain (@proton(.)me) **and, above all, his password** visible. This oversight enabled the researchers to trace his full address.

Krebs' analysis was confirmed by FalconFeeds, who had direct access to one of the group's last private Telegram channels with 349 members. This source corroborates the identification of Saif Al-Din Khader as Rey and documents his rotation of aliases, notably from @jolt30n to Rey in October 2025.

## An early career in cybercrime

Before becoming administrator of Scattered LAPSUS\$ Hunters, Rey accumulated significant experience in the cybercriminal underground:

- **active user on BreachForums** under the pseudonym "Hikki-Chan", with over 200 posts between February 2024 and July 2025;
- **administrator of the Hellcat ransomware group's data leak site** in 2024, involved in attacks against Schneider Electric, Telefonica and Orange Romania ;
- **administrator of the latest incarnation of BreachForums**, a cybercriminal forum whose domains have been seized several times by the FBI;
- **participation in website defacements** as part of the "Cyb3r Drag0nz Team" group.

## Cooperation with the authorities?

During his exchange with Brian Krebs, Saif claimed to have been cooperating with European law enforcement agencies since June 2025, and to have contacted Operation Endgame (an international initiative targeting cybercriminal services). It claims to have ceased all intrusion and extortion activity since September 2025 and is seeking to withdraw from the group.

However, these claims could not be independently verified. Saif also stated that **ShinySp1d3r**, the group's new ransomware-as-a-service, is merely a **reuse of Hellcat source code modified with artificial intelligence tools**.

## Attack techniques: sophistication and social engineering

### Vishing and identity theft

The collective's main strength lies in its exceptional mastery of [social engineering](#). Attackers pretend to be legitimate employees or service providers in order to deceive IT help desks and gain privileged access. This technique, known as vishing (voice phishing), has been successfully used against many high-profile targets, including [MGM and Caesars casinos in 2023](#), where Scattered Spider, acting as an affiliate of the ALPHV/BlackCat ransomware, crippled the entire infrastructures of these Las Vegas giants after a simple phone conversation with the help desk.

In May 2025, SLSH launched a **large-scale social engineering campaign** targeting Salesforce. Attackers called employees and manipulated them into connecting a malicious application to their Salesforce portal, enabling

massive data exfiltration.

## Bypassing multi-factor authentication

The group uses several methods to bypass multi-factor authentication (MFA):

- **SIM swapping:** taking control of the victim's phone number by convincing the mobile operator to transfer the number to a SIM card controlled by the attackers;
- **MFA fatigue:** bombardment of MFA approval requests until the victim, exasperated, accepts one of them;
- **session cookie theft:** use of infostealer malware to steal authentication cookies to completely bypass MFA.

## Supply chain attacks

The group has specialized in **supply chain attacks**, targeting service providers to reach hundreds of customers simultaneously:

**Salesloft Drift (August 2025):** compromise of OAuth tokens stored in Salesloft's AWS environment after phishing a developer's GitHub account. This attack enabled access to the Salesforce instances of hundreds of customers.

**Gainsight (September 2025):** exploitation of secrets stolen during the Salesloft attack to compromise Gainsight, another Salesforce application provider. Google Threat Intelligence Group confirmed that **over 200 companies** were impacted, with names, business email addresses, phone numbers and support case content stolen.

**Zendesk (November 2025):** ReliaQuest discovered over 40 typosquatted domains targeting Zendesk, the customer support platform used by 100,000+ organizations. Attackers deploy fake SSO portals and submit fraudulent tickets to infect helpdesk staff, reusing infrastructure from their August Salesforce campaign.

This supply chain attack strategy is reminiscent of [massive ClOp campaigns exploiting vulnerabilities in third-party enterprise software](#), demonstrating that exploiting service providers has become a favored tactic of modern cybercriminals.

## Technical tactics mapping (MITRE ATT&CK)

For cybersecurity professionals, **Scattered LAPSUS\$ Hunters** ' techniques map precisely onto the MITRE ATT&CK v15 framework. FalconFeed researchers have documented the systematic use of several key tactics:

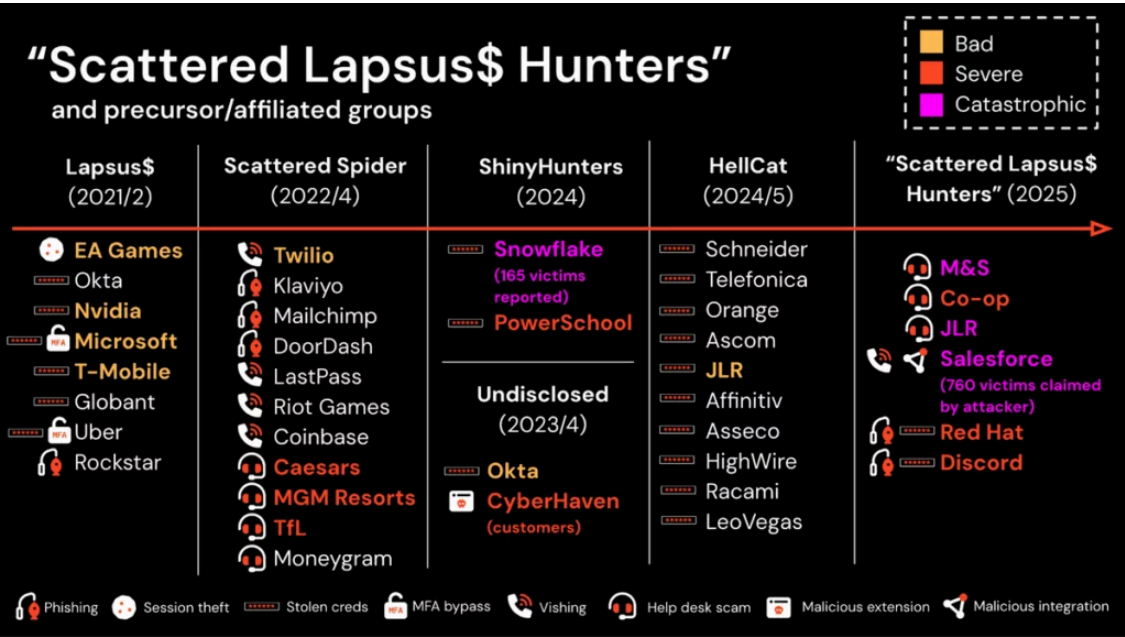
- **in the reconnaissance phase**, the group performs LinkedIn scraping and employee directory enumeration to identify help desk targets and super-administrators (T1589.002, T1593) ;
- **for initial access**, vishing via helpdesk impersonation combined with MFA fatigue and OAuth consent phishing (T1566.004), as well as buying or recruiting insiders to obtain domain administrator or Okta credentials (T1078.002) ;
- **for persistence**, theft of OAuth tokens and manipulation of refresh tokens on Salesforce, Microsoft 365 and GitHub (T1134, T1528);
- **for exfiltration**, exploitation of cloud APIs via connected Salesforce applications, SharePoint and GitHub repositories (T1567.002);

- **for impact**, a double extortion model combining leak site and direct negotiation (T1486).

This technical mapping enables security teams to prioritize detection and response controls specific to these attack vectors.

### An impressive death toll

According to consolidated analyses by FalconFeeds, which gained access to one of the group’s private Telegram channels, **it is believed to have been involved in over 1,500 intrusions** across the SaaS, retail and miscellaneous sectors. The group is said to have managed to extort **over \$370,000** documented, although the actual amount is likely to be much higher given the undisclosed payments.

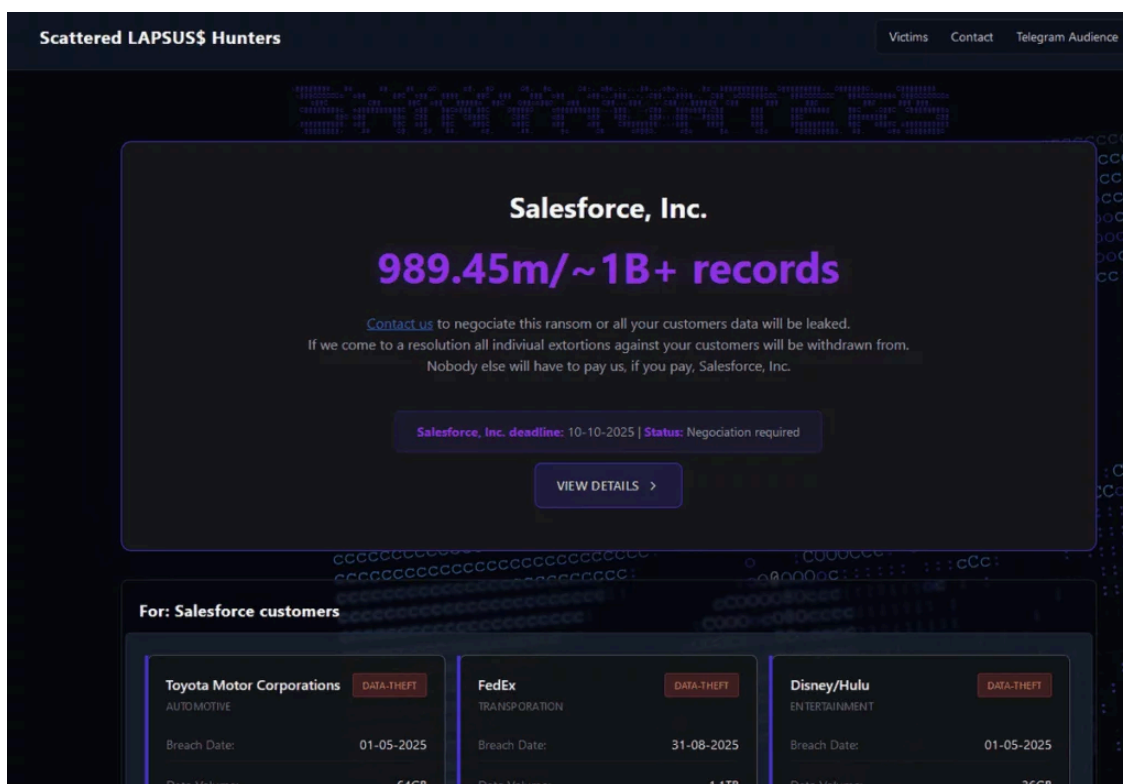


Timeline of major attacks by Scattered Lapsus\$ Hunters since 2021 – Source: Push Security

### The Salesforce campaign: 760 companies compromised

The campaign targeting the Salesforce ecosystem represents one of the most massive attacks in recent history. The attackers claim to have stolen **over 1.5 billion records** from 760 companies, including global giants such as “including global giants such as **Toyota, FedEx, Disney/Hulu, UPS, Cisco, Marriott, McDonald’s, Ikea, Walgreens** and retailer **Saks Fifth Avenue**.

The group launched a data leak site threatening to publish the internal information of three dozen companies that had not paid a ransom. This **double extortion** strategy maximizes the pressure on victims.



Scattered LAPSUS\$ Hunters extortion site targeting Salesforce victims – Source: KrebsOnSecurity

## The airline industry in turmoil

Airlines have been particularly targeted:

- **Qantas:** theft of personal data from nearly 6 million customers via a third-party customer service platform using Salesforce;
- **Hawaiian Airlines and WestJet:** cyberattacks attributed to Scattered Spider confirmed in June 2025, causing major operational disruptions.

## Jaguar Land Rover: an attack with historic economic consequences

The attack on Jaguar Land Rover (JLR) in August 2025 was **the most economically damaging cyber incident ever recorded in a G7 economy**. The attack brought global production to a complete halt for over three weeks, with losses estimated at £50 million (\$67 million) per week.

The impact spread to hundreds of suppliers, threatening to create a major crisis in the automotive ecosystem. The British government had to step in, guaranteeing a £1.5 billion (approx. \$2 billion) loan to mitigate the impact on the supply chain and national GDP.

## British distribution paralyzed

In the spring of 2025, several major British retailers were hit:

- **Marks & Spencer:** ransomware attack causing a 36-hour outage of online services, losses of £300 million and a fall in market capitalization of almost £1 billion ;

- **Co-op:** the company proactively disconnected its network to reduce further losses, however the damage from this attack is estimated at £80 million (\$107 million).

| <b>Cyber impact on H1 2025</b>              | <b>Cyber non-recurring costs -<br/>adjusted</b> | <b>Cyber estimated trade impact<br/>- not adjusted</b> | <b>Total cyber impact</b> |
|---------------------------------------------|-------------------------------------------------|--------------------------------------------------------|---------------------------|
| <b>Total Group revenue</b>                  | -                                               | <b>(£206m)</b>                                         | <b>(£206m)</b>            |
| Revenue excluding FRTS                      | -                                               | (£165m)                                                | (£165m)                   |
| Revenue through FRTS                        | -                                               | (£41m)                                                 | (£41m)                    |
| <b>Underlying operating (loss) / profit</b> |                                                 | <b>(£60m)</b>                                          | <b>(£60m)</b>             |
| <b>Operating (loss) /profit</b>             | <b>(£20m)</b>                                   | <b>(£60m)</b>                                          | <b>(£80m)</b>             |

Breakdown of Co-op's financial losses following the attack – Source: BleepingComputer/Co-op

## Law enforcement and government agencies

In a bold escalation, the group claims to have compromised several government and law enforcement systems, publishing screenshots purporting to show access to:

- the **National Instant Criminal Background Check System** (NICS E-Check) ;
- **Law Enforcement Notification System** (LENS);
- **UK National Crime Agency** systems.

These allegations, although not fully verified, have raised serious concerns about the security of sensitive systems.

## The insider at CrowdStrike

In November 2025, **CrowdStrike confirmed that an employee had shared screenshots of internal systems** with SLSH, who then published them on their Telegram channel. The employee was dismissed, and CrowdStrike claimed that none of his systems had been compromised. Bling Libra (aka ShinyHunters) confirmed that it had agreed to pay the insider \$25,000 to gain access to CrowdStrike's network.

This incident illustrates the group's strategy of **recruiting malicious insiders** within targeted organizations, an approach they have formalized with repeated Telegram posts soliciting disgruntled employees in the insurance, finance, automotive, hospitality and telecommunications sectors.

## ShinySp1d3r: in-house ransomware-as-a-service

### The launch of a RaaS infrastructure

On November 19, 2025, BleepingComputer revealed that SLSH was developing its own [ransomware-as-a-service](#) program called **ShinySp1d3r**. Historically, the group acted as an affiliate of several established ransomware-as-a-service programs, deploying [ALPHV/BlackCat](#), [Qilin](#), [RansomHub](#) and [DragonForce](#) encryptors in their attacks. This affiliation strategy enabled them to concentrate on their core expertise, initial access via social engineering, while leaving ransomware development and maintenance to others. The launch of ShinySp1d3r marks a strategic break: the group **now becomes a fully-fledged RaaS operator**, controlling the entire attack chain from intrusion to encryption, and now able to recruit its own affiliates.

According to Rey, ShinySp1d3r is simply a **modified version of the Hellcat ransomware** whose source code it has distributed, with modifications made using artificial intelligence tools. The ransomware currently only runs on Windows, but representatives of the group have indicated that they are working on versions for Linux and ESXi.

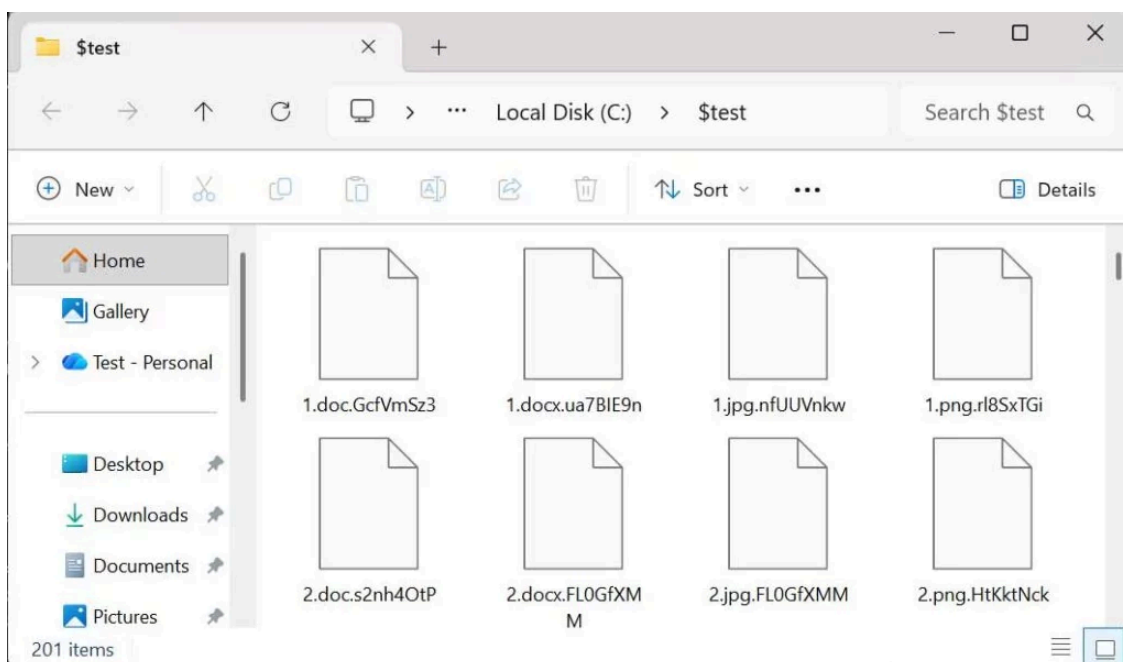
Interviewed by BleepingComputer, ShinyHunters confirmed the strategy behind this new RaaS: *” Yes, it will be run by me/us ‘ShinyHunters’ but operated under the Scattered LAPSUS\$ Hunters (SLH) brand, hence the name ShinySp1d3r, to demonstrate the ‘alliance’ or ‘cooperation’ between these groups. ”* The group also revealed it was working on a “lightning version” developed in pure assembler, similar to LockBit Green, optimized for encryption speed.



ShinySp1d3r ransomware wallpaper displayed on infected systems – Source: Unit 42

## Technical features

In-depth technical analysis reveals that ShinySp1d3r uses the **ChaCha20 encryption algorithm** with private key protected by **RSA-2048**. A notable feature distinguishes this ransomware: **each encrypted file receives a unique extension** generated according to a proprietary mathematical formula, making identification of compromised files more complex.

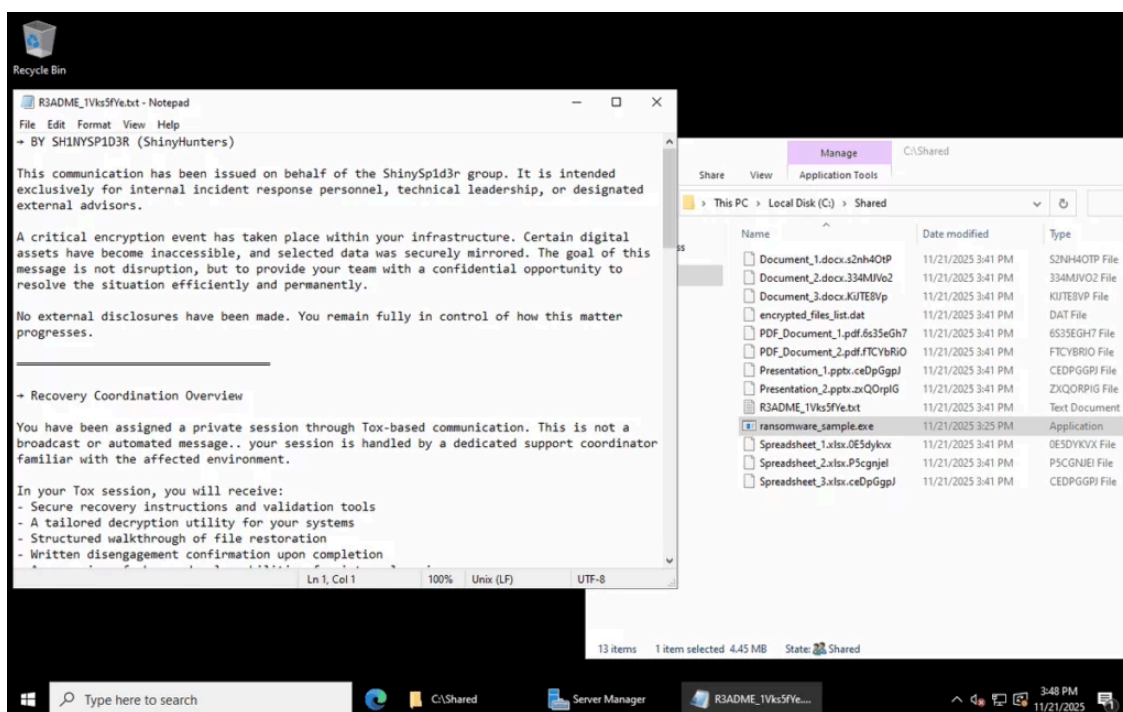


Files encrypted by ShinySp1d3r with unique extensions – Source: BleepingComputer

his ransomware has several advanced features:

- **encrypted file extension:** addition of the .shinysp1d3r extension ;
- **specific file header:** encrypted files contain a header starting with “SPDR” and ending with “ENDS”, including metadata on the original file, the file name and the encryption key;
- **anti-analysis hook:** use of the EtwEventWrite function hook to prevent event logging in Windows Event Viewer, complicating detection and forensic analysis;
- **free space deletion:** filling of free disk space with random data, making it impossible to recover deleted files using conventional restoration tools;
- **network propagation:** lateral propagation capabilities via SCM (Service Control Manager), WMI (Windows Management Instrumentation) or GPO boot scripts;
- **process kill:** automatic deletion of processes that keep files open and prevent their encryption, guaranteeing maximum encryption rates;
- **ransom note:** text file containing a unique victim ID and contact details via TOX ;
- **personalized wallpaper:** modification of the victim’s wallpaper to display a warning message from the group;
- **automatic clean-up:** batch script to erase deployment traces after encryption.

These features make ShinySp1d3r a particularly sophisticated and resilient ransomware. Unit 42 has published **indicators of compromise (IOCs) on GitHub** to enable organizations to detect this ransomware and implement appropriate protection measures.



ShinySp1d3r ransom note – Source : Unit 42

## Spectacular threats

On November 21, 2025, SLISH posted an explicit threat on Telegram: “*We will lock down the entire state and city of New York with ShinySp1d3r. Hold. My. Words.*” This statement, though potentially hyperbolic, illustrates the group’s boldness and ambition.

## Organizational structure: between fiction and reality

### An architecture of personas

Although some 30 active pseudonyms were observed on the associated channels, **linguistic analyses, the use of emojis and publication rhythms** suggest that fewer than five individuals actually run the operation. This multiplication of personas serves as both amplifier and shield, complicating attribution and ensuring continuity even when accounts are deleted.

Key personas include :

- **shinycorp** (aka @sp1d3rhunters, @slope48, @shinyc0rp): main orchestrator issuing claims of intrusions, mocking law enforcement and coordinating responses to channel closures ;
- **Rey**: public figure and administrator;
- **sevyuwu/Sevy**: narrative amplifier with a **documented alias rotation over 18 months** (May 2024 – November 2025). Analysis reveals multiple aliases including @KAngel\_uwu, @sevykitten, @ISEEITILIKEITIWANTITIG0TITxDUwU, @barbie, up to the current pseudonym @kAngel\_uwu with the bio “famous celebrity”. These frequent rotations complicate monitoring and testify to a studied operational hygiene;
- **Alg0d**: high-profile broker persona, mainly focused on data sales and trading ;

- **yuka/Yukari/Cvsp**: exploits and initial access broker (IAB) with real technical expertise in exploit development, malware engineering and vulnerability brokering.

The group also uses **“Rose”, an automated bot** that greets new members by username, scans their profiles and automatically bans non-compliant users. This tool enables rapid vetting of potential insiders and detection of lurkers (passive observers), in line with Trustwave’s analysis of the SLSH distributed trust model.

| Actor / Handle                                | Functional Role      | Additional Notes                                                                                        |
|-----------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------|
| Shinycorp / @sp1d3rhunters / multiple aliases | Coordinator          | Central to narrative, manages brand projection                                                          |
| Rey / @meow31337                              | Coordinator          | Engagement and amplification                                                                            |
| SLSHsupport / @SLSHsupport                    | Coordinator / Claims | Maintains visibility and continuity                                                                     |
| @barbie / @sevyuwu                            | Coordinator          | Attention generation. Multiple accounts (e.g., @tinysexyblonde, @catxduwumeow) were created to mimic it |
| UNC5537                                       | Operational Support  | Persona borrowing from Snowflake campaign                                                               |
| unc3944                                       | Operational Support  | UNC-style persona, likely Scattered Spider connection                                                   |
| Alg0d / @alg0d1337 / @alg0dls                 | Operational Support  | Posts on Google, Victoria’s Secret, LVMH                                                                |
| Yuka / Yukari / Cvsp                          | Exploit / IAB Broker | Multilingual actor, prior ShinyHunters affiliation                                                      |
| bd / @u0001bdk                                | Contributor          | Manages targeting of executives                                                                         |
| UNC6040 / @UNC6040 / @uncc6040                | Contributor          | Limited activity                                                                                        |
| lj / @u900061                                 | Contributor          | Content posting                                                                                         |
| CCP AGENT 99283 / @chinahunterz               | Contributor          | Attention-focused                                                                                       |
| Others                                        | Various              | Multiple sockpuppets, impersonations, attention operations                                              |

Key figures and affiliates of Scattered LAPSUS\$ Hunters – Source: Trustwave SpiderLabs

## The business model: extortion and services

### Systematic double extortion

The group operates according to a proven **double extortion model**: after stealing sensitive data, the attackers encrypt the victim’s systems. The victim is thus faced with a double threat: paying to regain access to his or her systems, and paying again to prevent publication of the stolen data.

This strategy considerably increases the pressure on victims, particularly those operating in regulated sectors such as healthcare, finance or utilities, where disclosure of data can result in massive regulatory sanctions and an irreparable loss of trust.

## Extortion-as-a-service (RaaS)

Scattered LAPSUS\$ Hunters has formalized its offering by proposing an **extortion-as-a-service** model. This approach enables other cybercriminals to use the group's infrastructure, reputation and expertise in return for a share of the profits. This professionalization of crime illustrates the evolution of the cybercriminal underground towards increasingly sophisticated structures.

## Recruiting insiders

A particularly worrying component of their model is the **active recruitment of disgruntled employees**. The group regularly solicits insiders in large companies, offering to share ransom payments in exchange for internal access. This approach turns the insider threat from a latent risk into an active attack strategy.

## Responses from the authorities

### FBI seizures

On October 5, 2025, the FBI announced that it had again seized domains associated with BreachForums, describing the platform as “a major criminal marketplace used by ShinyHunters and others to market stolen data and facilitate extortion”. According to the FBI, *“this seizure removes access to a key hub used by these actors to monetize intrusions, recruit collaborators and target victims across multiple industries”*.

On October 13, 2025, a joint FBI-French authorities operation targeted the platforms used to extort victims of the massive Salesforce breach, including the clearnet breachforums(.)hn domain.

### Arrests in France

French authorities have made several arrests of suspected network members, although precise details remain limited. These actions are part of a coordinated international effort to dismantle the group.

### Advisories and alerts

Several agencies have issued specific alerts:

- **FBI FLASH Alert (September 12, 2025):** alert concerning the targeting of Salesforce platforms by the UNC6040 and UNC6395 groups;
- **CISA:** advisory on Scattered Spider detailing the group's techniques, tactics and procedures.

## The spectacular farewell of September 2025

In mid-September 2025, the group published a farewell letter on Breachforums, announcing that it had “achieved its goals of exposing digital security weaknesses”. This announcement, accompanied by a list of team members, seemed to mark the end of their public operations.

## Immediate return to business

This retreat turned out to be a **pure PR exercise**. As early as September 18, 2025, just a few days after the announcement, a RAMP forum account presumably operated by the leader of ShinyHunters claimed responsibility for a new campaign targeting the financial services sector.

Resecurity researchers believe that **these groups will continue their malicious activities** under different names or reorganize as the Conti group did, rather than truly disbanding. The group itself has suggested that future disclosures of intrusions involving their names would not necessarily mean that they are still active, creating deliberate ambiguity around their status.

## Protection recommendations

### Securing identities and access

In the face of advanced manipulation techniques, securing identities is the first line of defense. Experts recommend **eliminating all direct RDP exposure** on the Internet, and **deploying multi-factor authentication** on all administrative interfaces, with preference for phishing-resistant FIDO2 hardware security keys. The adoption of [Zero Trust](#) principles imposes continuous identity verification, with no default trust. **Strict network segmentation between IT management tools and production systems** limits lateral propagation in the event of compromise.

### Endpoint hardening

Terminal hardening completes these defenses. **Enabling forgery protection** with anti-exploit protection prevents attackers from disabling security solutions, a tactic systematically employed by SLSH. **Password-restricted uninstallation of security agents** makes any attempt visible. **Enabling agent self-defense** makes it possible to resist neutralization, even with elevated privileges. **Deployment of predictive machine learning** proactively detects malicious behavior before it is fully executed.

### Monitoring cloud and SaaS applications

**Scattered LAPSUS\$ Hunters** ' focus on cloud environments means that these ecosystems need to be closely monitored. **Regular audits of connected applications** and authorized OAuth tokens quickly identify malicious applications or excessive authorization. The Salesloft and Gainsight attacks demonstrated that compromised OAuth tokens offer persistent access even after passwords have been reset. **Monitoring for abnormal administrative activity** needs to pay particular attention to critical shares such as NETLOGON. **Strictly restricting access to sensitive shares** and **detecting attacks by vulnerable drivers** complete the package.

### Training and awareness

Since the manipulation of the human factor is the main vector, training is a fundamental defensive investment. **Regular training in phishing and identity theft techniques should be targeted at all staff**, particularly helpdesk personnel. Procedures should impose systematic multi-channel checks for all sensitive requests: callback on verified number, confirmation by direct superior before MFA reset or critical modification. **Establishing escalation protocols** for high-risk changes adds a further level of validation. These protocols require the explicit approval of a manager prior to any high-impact action.

## Implications for the cybersecurity landscape

### The evolution towards malware-free attacks

Scattered LAPSUS\$ Hunters embodies a **major trend: 79% of detections are now malware-free**, up from 40% in 2019. Attackers are deliberately bypassing traditional endpoint- and network-centric security controls by directly targeting applications and services via account takeover.

This trend is rendering many established defenses ineffective:

- Endpoint Detection and Response (EDR) solutions fail to see attacks that take place entirely in the browser;
- network controls fail to detect legitimate traffic from compromised accounts;
- traditional cloud security solutions struggle to encompass all applications and detect malicious actions that blend into normal activity.

Modern attackers are constantly diversifying their attack vectors. Beyond the techniques used by SLISH, other emerging methods such as [ClickFix](#) demonstrate that cybercriminals are continually innovating to bypass traditional defenses and exploit users' trust.

### Identity as the new perimeter

The data converge on an alarming observation:

- **identity-based attacks have jumped by 32%** over the past year;
- **97% of identity attacks are password-based**, fuelled by credential leaks and malware infostealers;
- **credential abuse and phishing combined account for 38% of intrusions**, making identity the main intrusion vector.

### The professionalization of cybercrime

Scattered LAPSUS\$ Hunters illustrates the **growing professionalization of the cybercrime ecosystem**: organized structures, role specialization, service models (RaaS, EaaS), polished brands and identities, strategic public communication. This evolution is transforming cybercrime from an opportunistic activity into a structured industry with global ambitions.

## Conclusion: a persistent and evolving threat

**Scattered LAPSUS\$ Hunters** represent much more than just a cybercriminal group: they are the **symbol of a new era** in the digital threat landscape. Their ability to federate diverse skills, to exploit human rather than technical vulnerabilities, and to rapidly adapt to the defenses in place makes them one of the most formidable adversaries of 2025.

Despite seizures, arrests and retirement announcements, all indicators suggest that **this threat will persist in one form or another**. The Com ecosystem continues to produce new players, proven techniques will be revived and

refined (as demonstrated by [LockBit's resurgence](#) despite dismantling operations), and the financial motivation remains intact.

For organizations, the message is clear: traditional defenses are no longer sufficient. Protection against adversaries like SLISH requires a **holistic approach** combining identity security, behavioral detection, operational resilience and, above all, human vigilance in the face of increasingly sophisticated social engineering techniques.

The year 2025 has shown that the most dangerous attackers are not necessarily the most technical, but the most creative, the most daring and the most persistent. **Scattered LAPSUS\$ Hunters** embodies this disturbing reality and shapes the cybersecurity challenges for years to come.

**Are you a victim of ransomware?** [Contact our 24/7 support team](#). We provide [an exclusive technical response to ransomware incidents](#), to help you recover your data and get back to business quickly.

#### Sources :

**Krebs on Security:** [Meet Rey, the Admin of 'Scattered Lapsus\\$ Hunters'](#)

**Unit 42 (Palo Alto Networks):** [The Golden Scale: 'Tis the Season for Unwanted Gifts](#)

**Push Security:** [Scattered LAPSUS\\$ Hunters](#)

**FalconFeeds:** [Threat Intelligence Briefing: Scattered LAPSUS\\$ Hunters \(SLSH\)](#)

**Trustwave SpiderLabs:** [Scattered LAPSUS\\$ Hunters: Anatomy of a Federated Cybercriminal Brand](#)

**Resecurity:** [Trinity of Chaos: The LAPSUS\\$, ShinyHunters, and Scattered Spider Alliance Embarks on Global Cybercrime Spree](#)

**Reliaquest:** [Is Zendesk Scattered Lapsus\\$ Hunters' Latest Campaign Target?](#)

**BleepingComputer:** [Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters](#)

**BleepingComputer:** [Co-op says it lost \\$107 million after Scattered Spider attack](#)

---

Source: <https://sosransomware.com/en/ransomware-groups/scattered-lapsus-hunters-the-cybercrime-alliance-that-will-shake-global-businesses-in-2025/>