

Scattered LAPSUS\$ Hunters: Anatomy of a Federated Cybercriminal Brand

By Serhii Melnyk

Published: 2025-11-04 · Archived: 2026-07-28 02:00:12 UTC

November 04, 2025 7 Minute Read by Serhii Melnyk

Trustwave SpiderLabs' Cyber Threat Intelligence team is tracking the emergence and communication dynamics of the cybercriminal brand known as Scattered LAPSUS\$ Hunters (SLH), consolidating observed activity across public platforms to provide updated insights into its structure, evolution, and operational behavior.

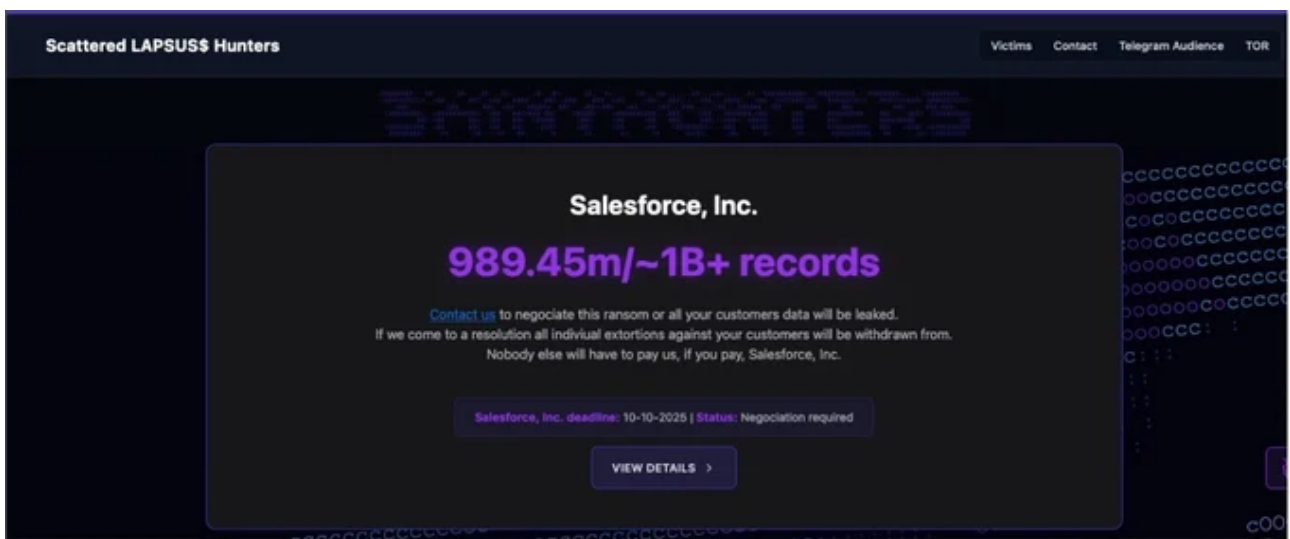


Figure 1. The main page of the Scattered LAPSUS\$ Hunters data-leak site (DLS), announcing Salesforce as one of its victims.

Public-facing materials and channel names indicate that this new umbrella brand appropriates the reputational assets tied to Scattered Spider, ShinyHunters, and LAPSUS\$. Our analysis shows various actors using these legacy brand names collaboratively, or impersonating them, to present a single, federated public front. However, at the moment of publication, we do not assess that this represents a formal, centralized organization composed exclusively of those former tree entities.

The Launch of a Consolidated Threat Group

Emerging in early August 2025, SLH appeared on Telegram as a self-declared hybrid entity, blending naming, reputational and operational traits from three of the most recognized The Com-linked collectives of recent years: Scattered Spider, ShinyHunters, and LAPSUS\$ (while being non-solely cyber related community, in our context, The Com is understood as an informal cybercriminal milieu characterized by fluid collaboration and brand-sharing across multiple operators).

I am writing you on behalf of the **scattered lapsus\$ hunters** group, parently owned by ShinyHunters.

This message is a formal final warning, within the next 72 hours, beginning on business days on Monday, we expect you to remove all IoCs related, associated, or affiliates to either of our 3 branches:

- Scattered Spider
- ShinyHunters
- Lapsus\$

Failure to do so will bring upon significant major consequences that I personally believe can be completely avoided if you comply with our demand. In return we are willing you give you intelligence on these ransomware groups that we have learned from our previous involvement from our Scattered Spider branch:

- DragonForce
 - Qilin (haise)
- unc3944

Figure 2. SLH member unc3944 claims Scattered Spider, ShinyHunters, and LAPSUS\$ as “branches” of SLH, while asserting that SLH itself is “parent-owned by ShinyHunters.” All such claims remain unverified.

Over time, SLH’s associations expanded, showing affiliations (with varying degrees of permanence) with other The Com-adjacent clusters such as CryptoChameleon, suggesting a deliberate attempt to merge established reputations into a new, unified narrative. The collaboration between Crimson Collective and Scattered LAPSUS\$ Hunters (October 2025, Red Hat incident) follows the same pattern – independent clusters temporarily aligning under a unified extortion umbrella. This substantiates our interpretation of SLH as a situational alliance, not a formal merger.

Retrospectively speaking, the first verified channel linked to the group appeared on August 8, 2025, under the handle “scattered lapsu\$ hunters – The Com HQ SCATTERED SP1D3R HUNTERS.” From inception, Telegram served as the group’s primary operational environment and the nucleus of its brand identity. While SLH intermittently hosted clear-web and onion-based data-leak sites to stage limited proof-of-compromise materials, Telegram remained central to its narrative construction – the stage where members performed, coordinated, and curated public visibility. As its activity matured, administrative posts began including signatures referencing the “SLH/SLSH Operations Centre” – a self-applied label projecting bureaucratic legitimacy and the image of an organized command structure.

And while some [public reporting](#) has noted overlaps between Scattered Spider, ShinyHunters, and LAPSUS\$, we do not view Scattered LAPSUS\$ Hunters as a federation or merger of those three clusters at the individual-operator level, and our current analysis focuses solely on the brand itself and how its members position that brand through public messaging.

Contextual Emergence, Operational Persistence, and Platform Cycles

Since its debut, SLH's Telegram channels have been removed and recreated at least 16 times under various iterations of the original name – a recurring cycle reflecting platform moderation and the operators' determination to sustain this specific type of public presence despite disruption.



Figure 3. Excerpt of a Telegram conversation showing member reactions and administrative responses following a channel takedown, referencing [breachforums\[.\]hn](https://breachforums.hn), later seized by law enforcement.

One of the latest versions, “scattered LAPSUS\$ hunters 7.0”, was also removed, with follow-up messaging indicating the group's desire to go dormant in terms of publicity for an undefined period – signaling resilience through adaptive naming and coordinated re-establishment.

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

Table 1. Observed Telegram channels and activity periods.

As these cycles unfolded, SLH's arrival coincided with turbulence across the broader cybercriminal underground. The collapse of BreachForums — long regarded as the successor to RaidForums and a key nexus for data leaks and recruitment — created a vacuum. Into that vacuum, Scattered LAPSUS\$ Hunters inserted itself, repackaging reputational assets from defunct collectives and inheriting fragments of their audiences.

By adopting recognizable branding and recycling reputational capital, the group reasserted legitimacy within The Com network. Soon after, SLH publicly announced an Extortion-as-a-Service (EaaS) model, formalizing its operational ambitions and signaling alignment with the broader cyber-extortion economy.

Following Monday or sometime next week, we will be launching our very own first public EaaS (Extortion-as-a-Service) program.

Similar to how a RaaS program works but with no locking/encryption. There will be a portal dedicated to this and instructions on how to partake in this service.

The main benefits of this program will be the fact that you can use our name to extort your target, with significant success than you'd see from extorting your target privately yourself behind no name or a name with no credibility/reputation/trust/history to it whatsoever.

Figure 4. Channel announcement advertising an Extortion-as-a-Service offering and soliciting customers.

This step revealed not only opportunism but intent: SLH positioned itself as both performer and service provider, using spectacle to attract customers, attention, and recruits.

Narrative Patterns and Messaging Themes

If its structure echoed old collectives, its messaging refined them. SLH channels consistently combined sensationalist rhetoric with theatrical claims of data theft, fusing entertainment with intimidation.

Posts frequently accused Chinese state actors of exploiting vulnerabilities allegedly targeted by SLH, while mocking Western law enforcement, particularly the FBI and NCA. This focus on US and UK agencies evidently signals which jurisdictions are at greatest risk and highlights the attention SLH members pay to these authorities.

Across iterations, channel content also alternated between proof-of-compromise displays, interactive polls, and coercive messaging. Snippets of leaked data served as teasers; polls invited participation in harassment or doxing campaigns; and occasional monetary incentives blurred the line between recruitment and crowdsourced extortion.

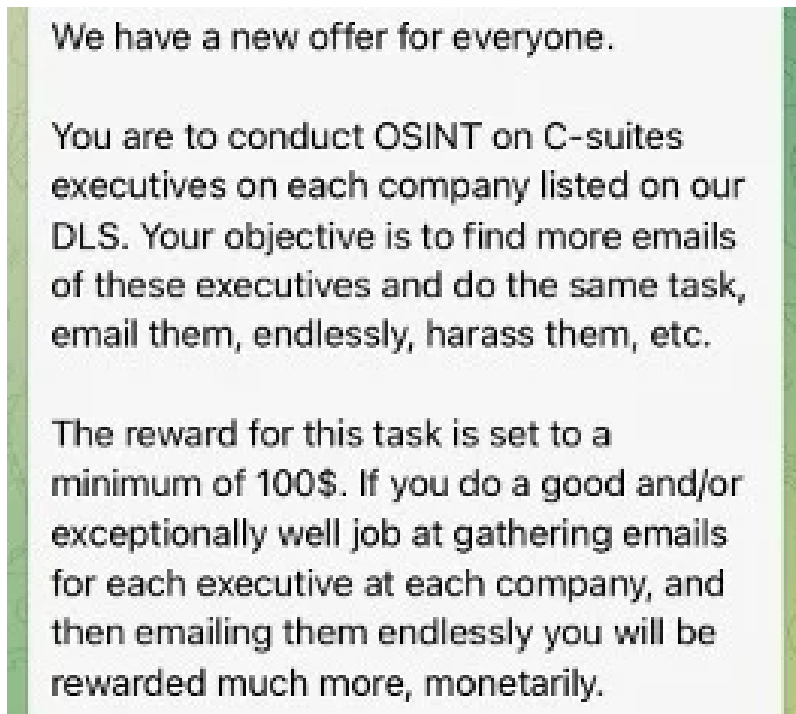


Figure 5. Telegram post inviting channel subscribers to participate, basically as freelancers, in pressure campaigns and doxing for payment or influence.

Parallel sales posts offered stolen credentials and exploits, while threats to executives and agencies amplified pressure and visibility. Although data exfiltration and extortion remain its main revenue channels, recurring mentions of “Sh1nySp1d3r Ransomware” also indicate aspirations toward ransomware operations – a claim yet to be verified.



Figure 6. Channel announcement referencing “Sh1nySp1d3r” as a proposed ransomware offering.

Together, these patterns show a deliberate fusion of technical signaling and social performance, and while financial gain appears to be the main motivation, the group’s reliance on attention, social validation, and audience reactions suggests an additional layer of social dependence. This positions SLH somewhere between financially motivated cybercrime and attention-driven hacktivism, blending monetary incentives with performative, socially contingent behavior.

There’s no clear evidence that SLH targets fall within a traditional hacktivist or socially motivated realm. While their behavior - relying heavily on public attention, social validation, and performative messaging - is unusual for

purely financially motivated actors, their posts and campaigns do not convey any coherent political, ecological, religious, or other social agenda.

The group’s messaging, aside from its antagonism of law enforcement, appears primarily driven by financial incentives, even if delivered in a style that borrows from attention-driven or hacktivist practices. This deliberate blending of social performance and monetary objectives blurs traditional classifications but does not indicate genuine hacktivist motivations.

Persona Architecture and Sockpuppetry

At the same time, behind the loud narrative lies a more controlled reality. Although roughly thirty active handles have been observed across associated channels, ranging from operators to provocateurs, linguistic patterns, emoji usage, and posting cadence suggest that fewer than five individuals drive the core operation.

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

Table 2. Consolidated administrative and affiliated personas.

Among these, “shinycorp” (appearing under aliases such as @sp1d3rhunters, @slope48, and @shinyc0rp) functions as the principal orchestrator, issuing breach claims, mocking enforcement efforts, and coordinating responses to takedowns. While auxiliary identities such as “sevyuwu,”/ Sevy, “Rey,” and “SLSHsupport” amplify

narratives and sustain channel engagement, “Alg0d” operates as a high-visibility broker persona, primarily focused on data sales and negotiation.

One of the more technically intriguing members is “yuka” (also known as Yukari or Cvsp). This persona presents itself as an exploit and initial access broker (IAB) and has been historically associated with exploit development offerings targeting CRM and SaaS ecosystems.

Available evidence suggests that Cvsp’s technical proficiency, spanning exploit development, malware engineering, and vulnerability brokerage – is genuine. Previous associations with the BlackLotus UEFI bootkit and Medusa rootkit lend credibility to this assessment, further supported by reputation vouches from ShinyHunters and the consistent use of escrow services in high-value transactions.

However, in the context of the SLH brand, this persona appears less directly integrated, likely operating in cooperation with, rather than under, the SLH core, as part of its broader ecosystem.

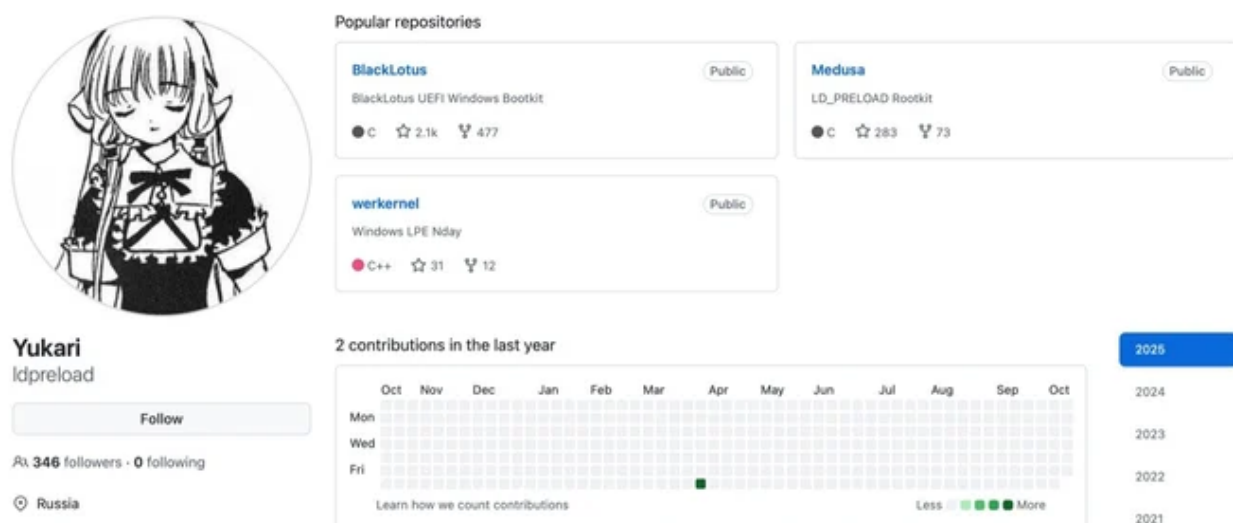


Figure 7. GitHub repository page attributed to “Yukari/Cvsp” showing projects labeled BlackLotus (UEFI bootkit) and Medusa (modular rootkit).

While numerous online personas appear active under the SLH umbrella, it remains impossible to determine with confidence the exact number of distinct individuals operating behind them. Each consistently active persona acts simultaneously as amplifier and shield, complicating attribution, ensuring continuity even when accounts are removed, and despite periodic disputes and peer ridicule, SLH continues to frame itself as part of The Com – a loosely federated community rather than a fixed hierarchy.

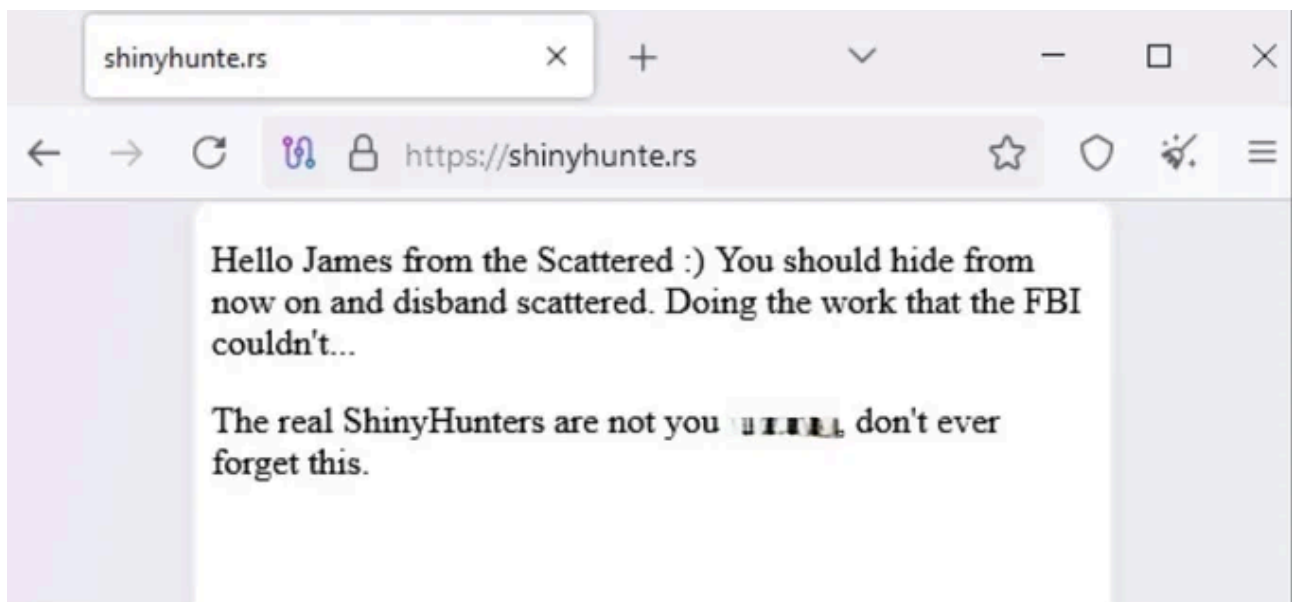


Figure 8. An HTML message posted on a DLS page targeting a named individual and engaging in reputation/peer warfare.

Overall, this self-positioning may represent the first consolidated branding alignment among a small group of mature The Com–related individuals, leveraging mutual notoriety while maintaining fluid cooperation and opportunistic overlap. Alternatively, it may reflect the actions of the same small set of operators – with historical ties to The Com ecosystem, recycling legacy brands to establish a coherent new identity within the broader network of related clusters.

Tactics, Techniques, and Procedures (TTPs)

Beyond identity management, SLH also demonstrates technical versatility consistent with experienced operators. Its activity suggests a continued prioritization of cloud-first extortion and data theft, focusing on high-value aggregation points such as SaaS providers, corporate CRMs, Database systems and other large data lakes offering immediate ROI.

Notably, this technical proficiency appears to reflect a convergence of skills and strengths drawn from multiple merged clusters and operators, suggesting that SLH leverages complementary expertise across intrusion, exploitation, and social engineering domains to enhance operational impact.

Credential harvesting, often through AI-automated vishing or spearphishing, is typically followed by lateral movement for privilege escalation, persistence and rapid data exfiltration.

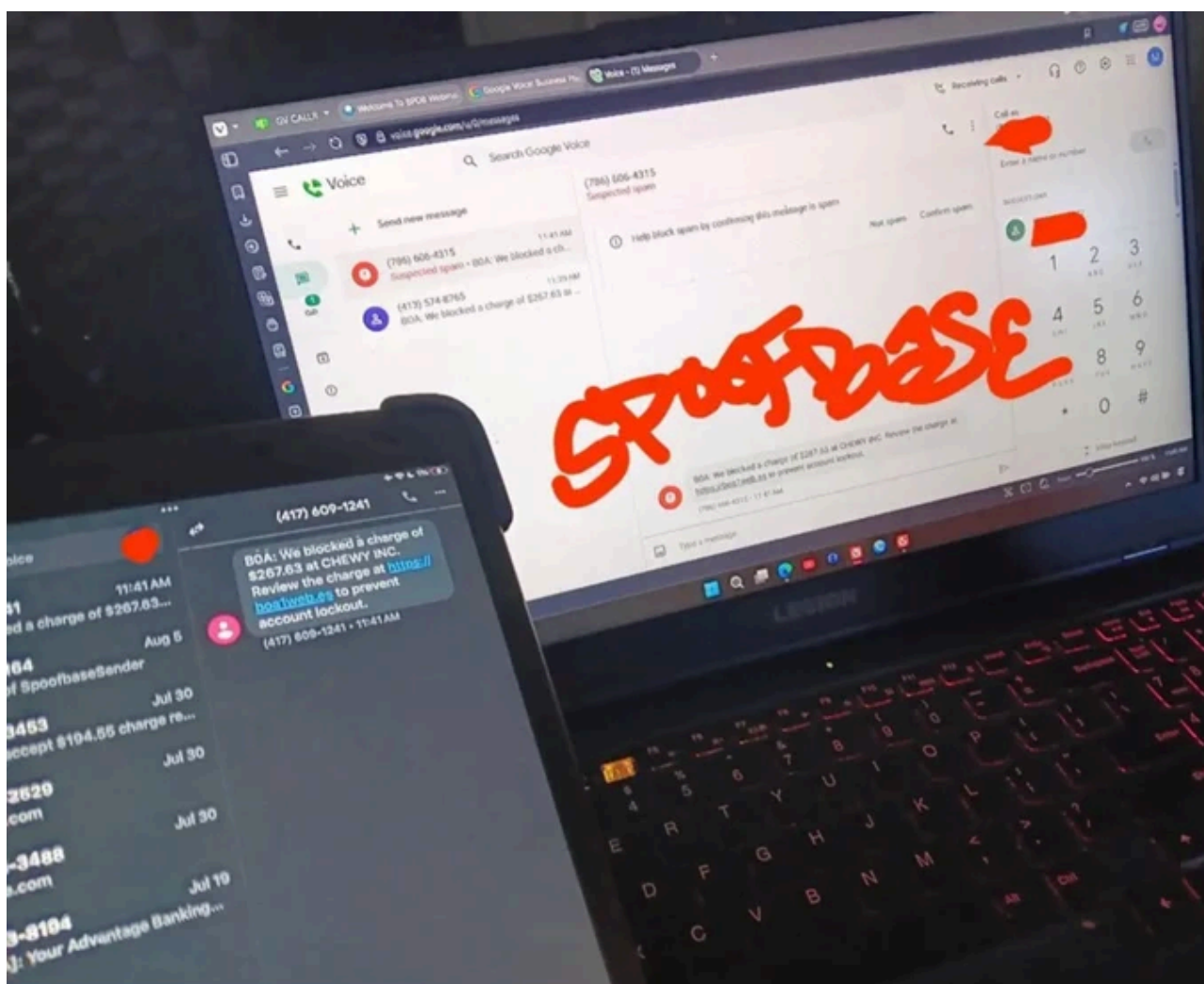


Figure 9. Screenshot shared in the channel by a member, depicting an operator running automated vishing tools that abuse Google Voice to scale social-engineering attempts.

SLH's messaging history also indicates non-trivial exploit development and acquisition capabilities within the group, including tooling consistent with zero- and n-day research specifically targeting CRMs, DBMSs, and SaaS platforms.

```
8  ## MADE BY SCATTERED LAPSUS$ HUNTERS ---- SHINYHUNTERS ---- https://
9
10 import base64
11 import requests
12 import zipfile
13 import io
14 import random
15 import argparse
16 import string
17
18 def get_args():
19     parser = argparse.ArgumentParser(description="SAP Exploit Script")
20     parser.add_argument("target", help="Target URL")
21     parser.add_argument("--command", help="Command to execute on the target")
22     parser.add_argument("--dropshell", action="store_true", help="Drop a shell on the target")
23     return parser.parse_args()
24
25 args = get_args()
26 TARGET = args.target
27 PROXY = {}
28
29 def generate_random_filename(length=8):
30     letters = string.ascii_lowercase
31     print("https://          CCP man dey stole our 0day frfr")
32     return ''.join(random.choice(letters) for i in range(length)) + ".jsp"
```

Figure 10. Code snippet or exploit proof-of-concept circulated within channels claiming to target CVE-2025-31324 (SAP NetWeaver).

Since its inception, affiliated posts have consistently claimed exploit acquisitions, most notably CVE-2025-61882 (Oracle E-Business Suite) – a vulnerability widely associated in public reporting with Cl0p ransomware operators. This overlap suggests potential code leakage, sharing, or exploit brokerage. However, the nature of SLH’s acquisition of this exploit remains unverified, and there is no independent evidence confirming that the group possessed it prior to the exploitation wave publicly attributed to Cl0p.

YES WE DID COMPLAIN ABOUT THE SAP ODAY THAT WE CREATED BECAUSE CCP STOLE IT ! And again we're complaining about the Oracle EBS Oday that WE ALSO CREATED AND LEAKED BECAUSE THESE SKIDS KEEP ON HAPPENING TO HAVE THE SAME Oday that we have and exploit them... and then get CAUGHT....

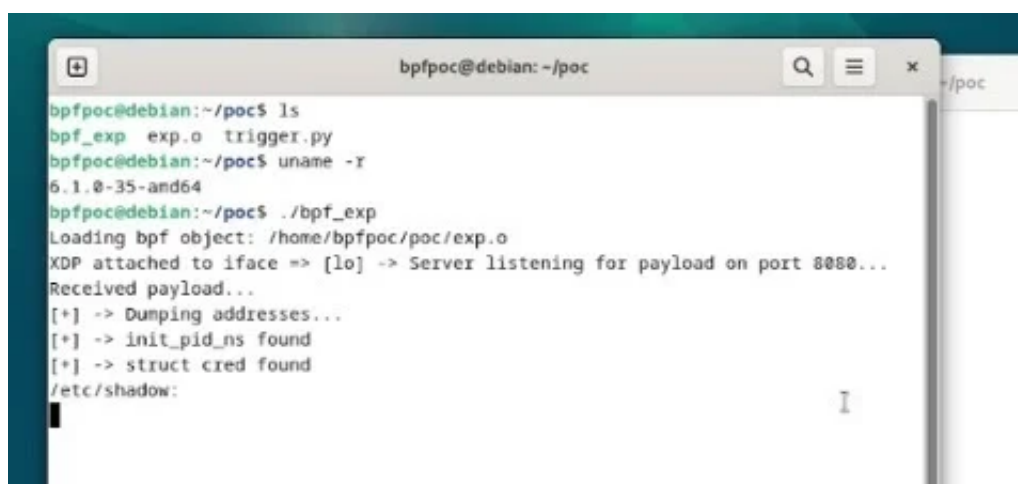
Anyway we have solved the problem in house and have completely gotten rid of the person leaking information.

We WILL. And I mean WE WILL. MOST DEFINITELY be unleashing a HORRIBLE year in 2026, which is very soon, by the way.

We do have a lot more 0/n/1days in a wide range of Identity, SSO, etc type of softwares with WAF bypasses 🙄🙄

Figure 11. Telegram post in which the group claims initial possession of an Oracle E-Business Suite zero-day (CVE-2025-61882), its leakage, and expresses frustration that Cl0p exploited it first.

Historical references support continuity in this focus: the persona Yukari previously claimed exploitation of Oracle Access Manager in 2021, indicating a possible lineage of resources and expertise.

A terminal window titled 'bpfpc@debian: ~/poc' showing the execution of a local privilege escalation exploit. The user runs 'ls', then 'bpf_exp exp.o trigger.py', then 'uname -r' which returns '6.1.0-35-amd64'. Then they run './bpf_exp', which shows 'Loading bpf object: /home/bpfpc/poc/exp.o', 'XDP attached to iface => [lo] -> Server listening for payload on port 8080...', and 'Received payload...'. Finally, it shows '[+] -> Dumping addresses...', '[+] -> init_pid_ns found', '[+] -> struct cred found', and '/etc/shadow:' with a cursor on the next line.

```
bpfpc@debian:~/poc$ ls
bpf_exp  exp.o  trigger.py
bpfpc@debian:~/poc$ uname -r
6.1.0-35-amd64
bpfpc@debian:~/poc$ ./bpf_exp
Loading bpf object: /home/bpfpc/poc/exp.o
XDP attached to iface => [lo] -> Server listening for payload on port 8080...
Received payload...
[+] -> Dumping addresses...
[+] -> init_pid_ns found
[+] -> struct cred found
/etc/shadow:
█
```

Figure 12. Terminal output published by the group that demonstrates a local privilege escalation exploit (CVE-2023-2163) with access to /etc/shadow.

Taken together, these behaviors illustrate an operational structure that combines social engineering, exploit development, and narrative warfare – a blend more characteristic of established underground actors than opportunistic newcomers.

Conclusion

The Scattered LAPSUS\$ Hunters phenomenon demonstrates the increasing fluidity of modern cybercriminal branding. Rather than existing as a cohesive group, SLH represents a federated identity model: a shared narrative container within which multiple actors collaborate, impersonate, or amplify each other for collective visibility and credibility.

This structure – decentralized, attention-driven, and reputationally opportunistic – marks an evolution in The Com ecosystem. SLH's blend of performance, extortion, and self-reinvention underscores the trend toward networked cybercrime as media performance, where the boundary between operator and audience blurs.

SLH's continued reappearance, despite disruption, highlights the resilience of these federated threat identities and their capacity to adapt through the language of spectacle, irony, and shared mythology. As this hybrid ecosystem evolves, its use of identity fluidity, social amplification, growing tailored exploitation development capabilities and adaptive collaboration will likely shape the next phase of data-extortion activity into 2026.

Source: <https://www.levelblue.com/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand>