

Scattered LAPSUS\$ Hunters: 2025's Most Dangerous Cybercrime Supergroup

By Picus Labs

Published: 2025-10-17 · Archived: 2026-07-28 02:00:37 UTC

In 2025, the cybersecurity world witnessed the sudden emergence of a new threat actor alliance dubbed Scattered Lapsus\$ Hunters—a group that unites elements of three well-known cybercrime entities: Scattered Spider, LAPSUS\$, and ShinyHunters. This convergence reflects an escalation in both ambition and coordination: rather than isolated attacks, victims are now confronted with an integrated, multi-phase assault combining social engineering, data exfiltration, and public extortion.

At its core, Scattered Lapsus\$ Hunters operates as a "supergroup" — leveraging the strengths and tactics of its constituent parts. From Scattered Spider, the alliance acquires expertise in initial access and help-desk engineering; from LAPSUS\$, notoriety in insider recruitment and source code theft; and from ShinyHunters, refined capability in large-scale data harvesting and extortion. Together, they have orchestrated high-impact campaigns targeting high-value enterprise environments, especially SaaS platforms like Salesforce, as well as major brands in retail, fashion, aviation, and insurance.

In the following sections, we will detail the known aliases (AKAs) of the individual groups comprising the Scattered Lapsus\$ Hunters supergroup, followed by the historical and major events associated with them, their tactics, techniques, and procedures (TTPs), and finally, a section on how Picus simulates Scattered Spider, LAPSUS\$, and ShinyHunters attacks.

[Simulate APT Attacks with 14-Day Free Trial of Picus Platform](#)

History & Major Activities of Scattered Lapsus\$ Hunters Group

- Late 2024 - Attackers leveraged social engineering—mainly through phone-based "vishing" attacks—to infiltrate corporate Salesforce systems. They deceived employees with access to install a fake integration, which granted the attackers API-level access to the Salesforce environment. This allowed them to exfiltrate data from numerous major companies, including Google and Cisco [1].
- March – June 2025 - The threat actor gained access to Salesloft's GitHub repositories, downloading content, adding a guest account, and setting up workflows. During this time, they conducted reconnaissance across both the Salesloft and Drift environments. The actor then moved on to compromise Drift's AWS environment, where they obtained OAuth tokens linked to customer technology integrations. Using these tokens, they were able to access data through the Drift integrations [1].
- 5 June 2025 - Google [releases a report](#) explaining that the group employs social engineering via phone calls, impersonating IT support or other authorized personnel to access Salesforce data through malicious

integrations. A similar tactic, or the data obtained from such an attack, likely led to the compromise of the initial GitHub credentials for Salesloft.

- 8 August 2025 - A new Telegram channel emerged claiming to bring together members and brands from Scattered Spider, LAPSUS\$, and ShinyHunters. The channel rapidly became a central point for coordinated threats, fabricated data leaks, and the promotion of a forthcoming Ransomware-as-a-Service (RaaS) platform dubbed "shinysp1d3r." Although Telegram later took it down, the channel had already played a significant role in driving multiple large-scale campaigns.
- 12 Sep 2025 - FBI dropped a [FLASH alert](#) connecting a string of Salesforce breaches to two hacker groups: UNC6040, which Google's Threat Analysis Group links to ShinyHunters, and UNC6395, known to share ties with Scattered Spider. Both appear to be part of the broader "Scattered Lapsus\$ Hunters" operation. Google later confirmed that the attackers didn't exploit any Salesforce vulnerabilities — instead, they relied purely on social engineering tricks like vishing and OAuth manipulation to gain access.
- 17 Sep 2025 - The hacker group Scattered Lapsus\$ Hunters announced that they were "going dark" and would be halting their operations. Despite this claim, cybersecurity experts continued to observe ongoing activity, particularly targeting Salesforce-related data [1].
- 3 Oct 2025 - Scattered Lapsus\$ Hunters launched their "extortionware" portal, publicly threatening Salesforce and other organizations affected by social engineering attacks or the Salesloft Drift breach. The portal warned that unless the demanded payment was made, the compromised data would be exposed, setting a deadline of October 10 [1].

ATT&CK Mapping (TTPs) of Scattered Lapsus\$ Hunters Group

Tactic: Resource Development

T1650 Acquire Access

Adversaries often seek to gain an advantage by purchasing or otherwise acquiring existing access to target systems or networks. On August 31, 2025, the Telegram channel "scattered LAPSUS\$ hunters 4.0," operated by the well-known hacking group ShinyHunters, exemplified this tactic by posting a recruitment message aimed at insiders within enterprise organizations. The group specifically sought individuals who could provide access to critical platforms such as Okta, Microsoft SSO, Citrix VPN, and Git-based version control systems like GitHub or GitLab. This incident highlights the growing trend of cybercriminals leveraging insider threats to bypass external defenses and infiltrate high-value corporate infrastructures.

Below is the Telegram message that was sent on August 31, 2025 [4]:

scattered LAPSUS\$ hunters 4.0

IF YOU HAVE OKTA OR MS SSO OR CITRIX ACCESSES MESSAGE

@shinyc0rp YOU WILL BE PAID NICELY!!!!

SECTORS OF INTEREST:

credit bureaus, insurance, finance/banking, aviation/travel agencies, car companies/motor (bmw, rr, audi, etc), retail companies, fastfood/restraunt, hotels, telecoms, gasoline companies like shell, investment companies (blackrock, vangaurd) and etc along these lines

Tactic: Initial Access

T1190 Exploit Public-Facing Application

Scattered Spider Group exploited CVE-2021-35464 to compromise a ForgeRock OpenAM application server. This platform often serves as the gateway for web applications and remote access solutions across a wide range of organizations, making this vulnerability particularly concerning.

T1566.004 Phishing: Spearphishing Voice

Targeted voice-phishing (vishing) campaigns were the opening gambit for recent Salesforce intrusions: attackers posed as IT/help-desk staff and placed convincing calls that persuaded employees and contractors to perform sensitive actions rather than exploiting platform bugs.

They usually open the call with a calm, believable explanation of an IT problem and gently steer the conversation until the person agrees to reset MFA tokens, install remote-management software, or click through to Salesforce's /setup/connect page to approve a rogue app.

Distinctive of this group, the use of AI-driven voice agents enables automated calls, adaptive responses to recipients' reactions, and realistic accent generation, allowing vishing to scale to thousands of targets with minimal additional effort.

Tactic: Credential Access

T1003.003 OS Credential Dumping: NTDS

Once attackers obtain domain administrator access—or an equivalent level of privilege—the LAPSUS\$ group has been known to leverage the built-in ntdsutil utility to extract the Active Directory database [3].

This critical file, NTDS.dit, is stored by default in the %SystemRoot%\NTDS\NTDS.dit path on a domain controller, making it a prime target for those seeking to access sensitive directory information.

```
ntdsutil
```

```
activate instance ntds
```

```
ifm
```

```
create full C:\AD_Dump_Folder
```

```
quit
```

```
quit
```

This sequence launches ntdsutil, selects the NTDS (Active Directory) instance, enters the IFM(Install From Media) mode, and creates a full set of AD database files and supporting metadata in C:\AD_Dump_Folder for seeding new domain controllers or performing authorized recovery.

Attackers who obtain those files could extract credentials or other sensitive information from the AD database.

Scattered Spider Group leveraged a different method for exfiltrating the Active Directory database, ntds.dit. This technique requires privileged access to VMware vCenter—the centralized heart of virtualized infrastructure [5]. The tactic involves creating an unauthorized, unmanaged Virtual Machine (VM) and then attaching the disk of a Domain Controller (DC) to it, completely bypassing the operating system's security controls. This grants them access to the ntds.dit file, enabling the subsequent dumping of hashed credentials and highly sensitive Active Directory information.

T1552.005 Unsecured Credentials: Cloud Instance Metadata API

Following an initial compromise of the web server (likely through an exploit granting access as the tomcat user), Scattered Spider Group executed the well-known reconnaissance script, linpeas.sh. The primary objective of this script was to discover potential privilege escalation paths. Crucially, it targeted the EC2 Instance Metadata Service (169.254.169.254) to steal the temporary AWS IAM Role credentials assigned to the instance. The successful theft of these credentials means the adversary has escalated their access from a limited local user to a powerful cloud identity, enabling lateral movement and potential resource abuse across the AWS environment. Below is the log file that attackers left behind [2]:

Source Process User: tomcat | Source Process Command Line: curl -s -f -H

X-aws-ec2-metadata-token: <redacted>=== http://169.254.169.254/latest/meta-data/iam/security-credentials/<redacted>InstanceRole-<redacted> | Source Process Parent Process: sh linpeas.sh | Source Process Parent Process Start Time: 2022-10-XXTXX:XX:XXZ | Event Type: IP Connect | Source Process Start Time: 2022-10-XXTXX:XX:XXZ | Destination IP: <redacted> | Target file Path:

T1555.003 Credentials from Password Stores: Credentials from Web Browsers

LAPSUS\$ used the RedLine password stealer to harvest passwords and session tokens from compromised systems.

RedLine, sold on underground forums, is information-harvesting malware that exfiltrates saved credentials, autofill data and payment cards from Chromium- and Gecko-based browsers, and also targets FTP clients, messaging apps, crypto wallets and local VPN config files (e.g., %USERPROFILE%\AppData\Local\NordVPN\user.config).

T1621 Multi-Factor Authentication Request Generation

Rather than brute-forcing second factors, Scattered LAPSUS\$ Hunters Group weaponizes MFA flows: they generate or coerce MFA prompts and trick targets into approving them (or reset MFA), effectively bypassing multi-factor protections through social engineering.

In the Salesforce incidents, adversaries combined vishing with prompts to authorize connected apps or to complete OAuth consent screens—moves that convert human interaction into credential and token access.

Tactic: Discovery

T1046 Network Service Discovery

Scattered Spider employed RustScan to probe ESXi appliances for open ports [2], highlighting their approach to identifying potential network entry points.

```
rustscan -a <ESXi_IP_or_CIDR> -r 1-65535 -- -sV -A
```

This command scans the target for open TCP ports across 1–65535 as a fast discovery step, then performs service/version detection and aggressive probing on the ports found.

T1087 Account Discovery

The Scattered Spider Group has been observed conducting thorough Active Directory (AD) reconnaissance on on-premises systems, a critical initial step in their attack chain [5].

This reconnaissance is executed using specialized tools like ADEplorer, the script ADRecon.ps1, and the native PowerShell cmdlet Get-ADUser to efficiently obtain a listing of all domain accounts.

By enumerating domain accounts and their associated privileges, adversaries can strategically target high-value accounts for subsequent malicious activities.

Tactic: Collection

T1114.003 Email Collection: Email Forwarding Rule

Adversaries can exploit email forwarding rules to secretly monitor a victim's communications, exfiltrate sensitive information, and gather intelligence that can support further attacks. Such rules may also enable persistent access to a victim's emails, even after compromised credentials have been reset by administrators.

In a notable case, the LAPSUS\$ group configured an **Office 365 tenant-level mail transport rule** to redirect all incoming and outgoing emails from the targeted organization to an account under their control [3]. This highlights how email infrastructure can be weaponized to maintain long-term access and surveillance.

Tactic: Command and Control

T1219 Remote Access Tools

Adversaries can leverage legitimate remote access tools to establish interactive command-and-control channels, using either graphical interfaces or command-line sessions between trusted hosts. Scattered Spider, for example, has been observed deploying and repurposing commercial Remote Monitoring and Management (RMM) products—such as ScreenConnect, TeamViewer, Splashtop, **and** Pulseway—that are integral to enterprise IT operations

and commonly permitted by security policies. By exploiting this necessary trust relationship, the group is able to maintain robust, often undetected, remote access within compromised networks.

Tactic: Impact

T1657 Financial Theft

Once access was gained, the campaign's monetization followed familiar cybercrime patterns: exfiltrated customer and corporate data were weaponized for extortion, public leaks, or sale on criminal channels and Telegram leak sites. The Scattered LAPSUS\$ Hunters Group maintained an extortionware portal on the TOR Onion network, where they listed affected Salesforce customers and the amount of data they claimed to have stolen, using the site to pressure victims and extract financial gain. Below is the partial content of their site:

Scattered LAPSUS\$ Hunters

Salesforce, Inc.

989.45m/~1B+ records

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.

Salesforce, Inc. deadline: 10-10-2025 | Status: Negotiation required

For: Salesforce customers

<REDACTED-COMPANY-NAME>

DATA-THEFT

Breach Date: 01-05-2025

Data Volume: 64GB

Deadline: 10-10-2025

Countries Data Incl.: INTERNATIONAL

Revenue: \$326.24b+

Status: Active

<REDACTED-COMPANY-NAME>

DATA-THEFT

Breach Date: 31-08-2025

Data Volume: 1.1TB

Deadline: 10-10-2025

Countries Data Incl.: INTERNATIONAL

Revenue: €89b+

Status: Active

<REDACTED-COMPANY-NAME>

DATA-THEFT

Breach Date: 01-05-2025

Data Volume: 36GB

Deadline: 10-10-2025

Countries Data Incl.: INTERNATIONAL

Revenue: \$94.53b+

Status: Active

How Picus Simulates Scattered Spider, LAPSUS\$, and ShinyHunters Attacks?

We also strongly suggest simulating Scattered Spider, LAPSUS\$, and ShinyHunters Attacks to test the effectiveness of your security controls against real-life cyber attacks using the Picus Security Validation Platform. You can also test your defenses against hundreds of other threat groups within minutes with [a 14-day free trial of the Picus Platform](#).

[Picus Threat Library](#) includes the following threats for **Scattered Spider, LAPSUS\$, and ShinyHunters**:

Threat ID	Threat Name	Attack Module
98798	Scattered Spider Threat Group Campaign Malware Email Threat	Network Infiltration
42054	Scattered Spider Threat Group Campaign Malware Download Threat	Network Infiltration
45493	Lapsus Threat Group Campaign Malware Download Threat	Network Infiltration
35139	Lapsus Threat Group Campaign Malware Email Threat	Network Infiltration

Start simulating emerging threats today and get actionable mitigation insights with a [14-day free trial of the Picus Security Validation Platform](#).

Aliases of Scattered Lapsus\$ Hunters Group

Scattered Spider is also known as: Roasted Oktapus, Octo Tempest, Storm-0875, UNC3944, Muddled Libra, Oktapus, Scattered Swine, Scatter Swine, Oktapus, Storm-0971, DEV-0971, Starfraud.

LAPSUS\$ is also known as: DEV-0537, Strawberry Tempest.

ShinyHunters is also known as: UNC6040.

References

- [1] "Salesforce Extortion Accelerates With New Leak Site" Available: <https://www.upguard.com/blog/salesforce-leak-extortion-scattered-lapsus-hunters> [Accessed: Oct. 8, 2025]
- [2] "Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies" Available: <https://www.crowdstrike.com/en-us/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/> [Accessed: Oct. 9, 2025]
- [3] "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction" Available: <https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/> [Accessed: Oct. 9, 2025]
- [4] "ShinyHunters Calling: Financially Motivated Data Extortion Group Targeting Enterprise Cloud Applications" Available: <https://blog.eclecticiq.com/shinyhunters-calling-financially-motivated-data-extortion-group-targeting-enterprise-cloud-applications> [Accessed: Oct. 10, 2025]
- [5] "CrowdStrike Services Observes SCATTERED SPIDER Escalate Attacks Across Industries" Available: <https://www.crowdstrike.com/en-us/blog/crowdstrike-services-observes-scattered-spider-escalate-attacks/> [Accessed: Oct. 10, 2025]

Source: <https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup>