

Resecurity | Trinity of Chaos: The LAPSUS\$, ShinyHunters, and Scattered Spider Alliance Embarks on Global Cybercrime Spree

Published: 2025-09-25 · Archived: 2026-07-28 02:00:45 UTC

Introduction

LAPSUS\$, Scattered Spider, and **ShinyHunters** are three of the most notorious English-speaking cybercrime groups operating today. While each group has its own distinct origins and operational history, recent developments (especially since 2023 to 2025) reveal significant connections, tactical overlaps, and even direct collaboration.

These connections are evident in their shared proclivity for social engineering, overlapping membership, joint public channels, and coordinated attacks on high-profile targets. The lines between these groups have become increasingly blurred, with cybersecurity researchers and law enforcement now viewing them as part of a loosely connected and highly adaptive cybercrime ecosystem.

Irrespective of individual attack attribution, these groups have revealed to the world the alarming cyber-insecurity of major Fortune 100 corporations and government agencies, particularly considering that social engineering-based attacks have remained their primary method of gaining access to target networks.

The attack vectors and exploitation techniques used by the actors were not particularly sophisticated; instead, they were well-organized and coordinated, exploiting both human weaknesses and technological misconfigurations. These actors rely on social engineering techniques, often impersonating employees or contractors to deceive IT help desks into granting them access.

In this report, Resecurity has prepared a summary of the activity associated with these actors, based on human intelligence (HUMINT) and collaboration with incident response teams from the affected victim organizations.

Resecurity does not believe that the group's recent announcement of ceasing operations is sincere. On the contrary, our team has become aware of multiple previously undisclosed victims who are currently being extorted privately. The group has likely decided to operate discreetly after establishing substantial credibility and a proven track record of successful hacks and large-scale data breaches. As such, the group can now leverage its commanding reputation to coerce victim payments without having to immediately engage the media to help amplify its ransom threats.

Documented Connections and Collaboration

A. Joint Operations and Public Collaboration

In August 2025, a Telegram channel explicitly combined the brands and apparent memberships of **Scattered Spider**, **LAPSUS\$**, and **ShinyHunters**. T

his channel was used to coordinate threats, tease data leaks, and market a new Ransomware-as-a-Service (RaaS) offering [dubbed](#) “shinysp1d3r.” Security researchers described the channel as “[chaotic](#),” and it was eventually

banned by Telegram

ShinyHunters confirmed that **Scattered Spider** provided initial access to targets, while the former handled data exfiltration and dumps. **LAPSUS\$** members were also active participants in this alliance, with all three groups working together on high-profile campaigns, such as the Salesforce and Snowflake breaches.

On September 12, the FBI released a [FLASH alert](#) on the targeting of Salesforce platforms by the cybercriminal groups **UNC6040** and **UNC6395**, which are responsible for a surge in data theft and extortion attempts. If this attack method is not entirely new, Resecurity has documented several Fortune 100 companies that received extortion emails bearing signatures and verified contact details of the ShinyHunters threat group.

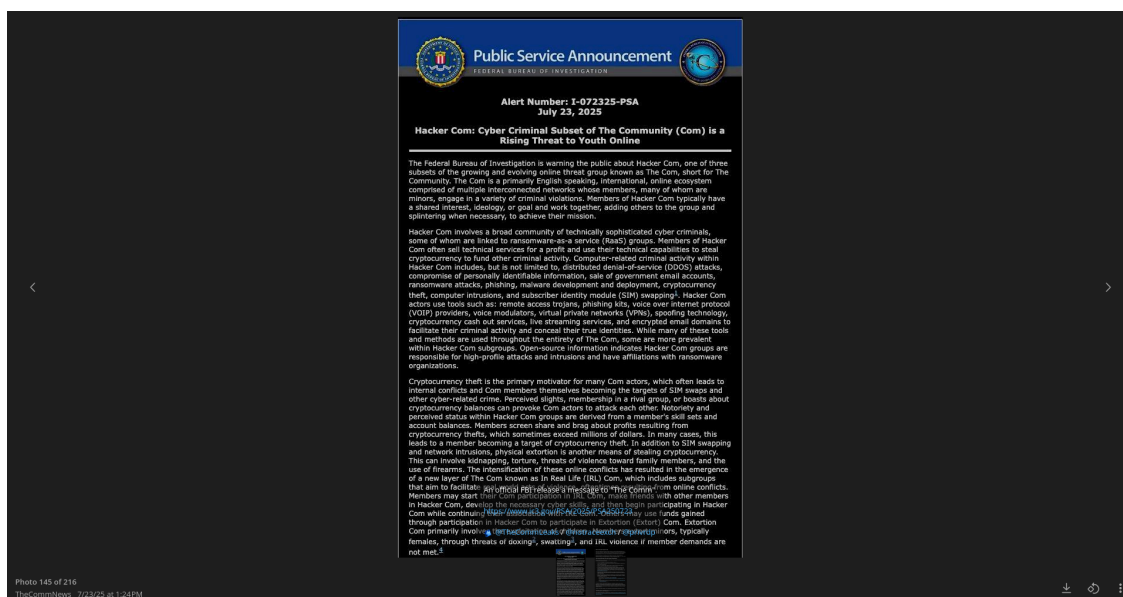
Despite the group's "retirement" announcement, it is doubtful that threat actors will stop their operations. Such 'exits' have occurred before, providing hacker collectives time to regroup and reemerge later under different names. The notorious Russian ransomware gang Conti is a prime example of this exit cover.

B. Association with "The Com" Collective

LAPSUS\$

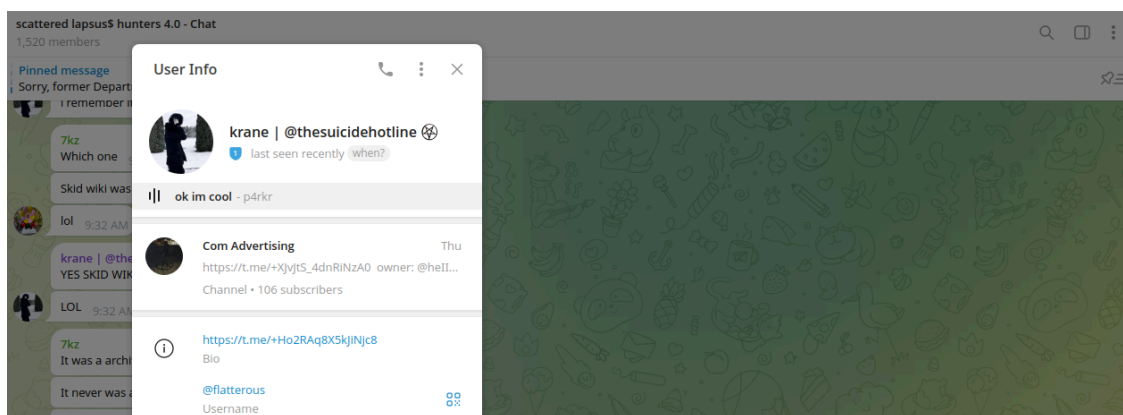
, **ShinyHunters**, and **Scattered Spider** are linked to 'The Com,' a predominantly English-speaking cybercriminal ecosystem. This loosely organized network operates more as a cybercrime youth movement, encompassing a broad and constantly shifting range of actors, mainly teens and 20somethings.

Some of the announcements related to successful data breaches by the actors were published at the associated Telegram channel known as "[The Comm Leaks](#)". The amplification of the trio's malicious campaigns via official Com channels suggests at least some level of shared ideology, membership, resources, or possible operational coordination. The FBI issued a [Public Service Announcement \(PSA\)](#) warning about the risks associated with joining such movements.



The Com is a primarily English-speaking, international, online ecosystem comprised of multiple interconnected networks whose members, many of whom are minors, engage in a variety of cyber-enabled crimes. Members of Hacker Com typically have a shared interest, ideology, or goal and work together, adding others to the group and splintering when necessary to achieve their objectives.

In fact, there are several groups associated with "The Com" movement. Some of them are advertised via "Com Advertising" and "Combos" channels. They are indirectly linked to key actors responsible for network intrusions and hacking activities, thereby promoting the ideology in general.



2. Overlaps in Tactics, Techniques, and Procedures (TTPs)

A. Social Engineering and Phishing

All three groups are renowned for their advanced social engineering capabilities, including vishing (voice phishing), phishing, and impersonation of IT staff to trick employees into granting them access or installing malware. Both **LAPSUS\$** and **Scattered Spider** are known for help desk impersonation and credential theft, while **ShinyHunters** has recently adopted similar vishing tactics, especially in attacks on Salesforce environments.

B. MFA Bypass and SIM Swapping

L

APSUS\$ pioneered the use of SIM swapping and MFA bombing (push fatigue) to bypass multi-factor authentication (MFA), techniques now widely used by **Scattered Spider** and, to a lesser extent, **ShinyHunters**

C. Data Theft, Extortion, and Publicity

A

ll three groups focus on stealing large volumes of data and extorting victims by threatening to leak it. Their extortion tactics often involve public shaming, leak sites, and direct communication with victims

T

he collective has recently gamified data leaks, using public polls to decide which victim's data to release next, maximizing psychological impact and publicity

.

D. Target Selection and Attack Vectors

The groups have jointly targeted organizations in the financial services, technology, retail, and airline sectors, including Qantas, Allianz Life, LVMH, Adidas, Google, and more.

Their campaigns are characterized by rapid adaptation and creative use of cloud service vulnerabilities, especially in VMware hypervisor environments like VMware ESXi and SaaS platforms like Salesforce and Snowflake.

3. Overlaps in Membership and Ecosystem Fluidity

The level of coordination and blending of tactics among the three groups strongly suggests at least some operational overlap or shared resources. Security researchers have described the alliance as a "cybercrime supergroup," indicating a possible pooling of talent and infrastructure.

The cybercrime ecosystem is increasingly fluid, with tactics, tools, and even members moving between groups, making attribution and group boundaries less distinct.

4. Recent Developments (2023–2025)

The partnership between **Scattered Spider** and **ShinyHunters** was first teased in the Fall of 2024, but has become especially prominent in 2025, with a marked increase in the scale and impact of their attacks. Recently, these attacks include coordinated phishing and extortion campaigns targeting Salesforce and major global brands.

While the groups' joint branding and shared Telegram channels first surfaced a year ago, their high-profile reemergence in 2025 show signs of significant escalation, indicating that these groups are not only aware of each other but are likely actively collaborating or at least coordinating their public-facing activities.

Security advisories in 2025 have highlighted the convergence of tactics among these groups, warning that the lines between data theft, extortion, and ransomware are increasingly blurred.

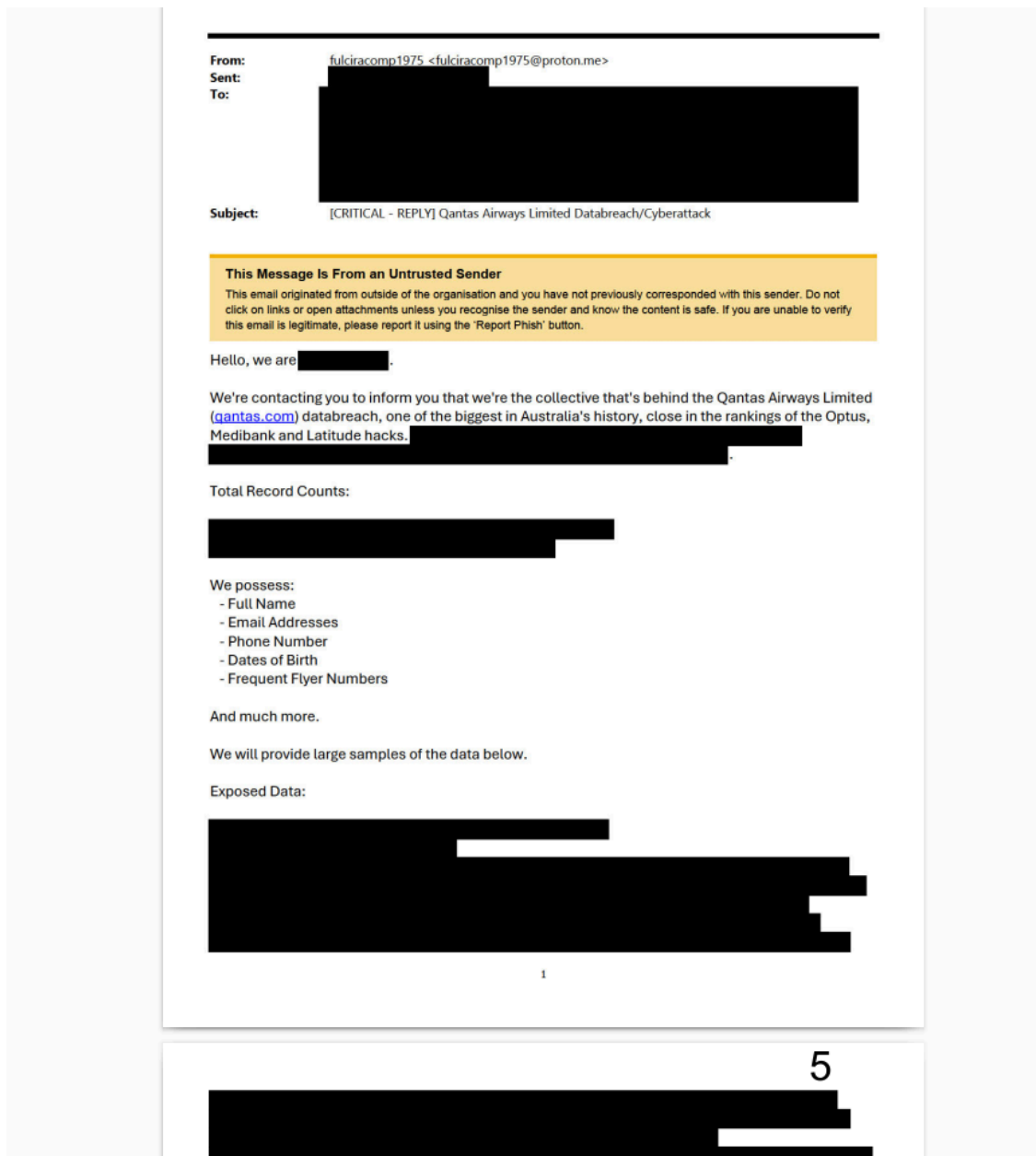
Cyberattacks on Airlines

Airlines are frequently targeted by cyberattacks, resulting in operational disruptions, flight cancellations, data breaches, and financial losses. Recent incidents include **Scattered Spider**'s ransomware attacks on major global carriers like WestJet, Hawaiian, and Qantas in mid-2025, the 2024 Port of Seattle attack impacting airport services, and a 2024 Russia-focused attack on Aeroflot by pro-Ukraine hackers. These attacks exploit vulnerabilities in aging IT systems and aim to steal passenger data or disrupt operations.

In July 2025, the cybercrime group **ShinyHunters** claimed responsibility for a data breach at Qantas that compromised the personal information of nearly 6 million customers. The attack was part of a larger campaign

targeting Salesforce users through voice-phishing, or "vishing," to steal data for extortion. The breach involved a third-party customer service platform used by a Qantas call center.

Example of extortion email received by Qantas:



Typical of ransomware tactics, the actors shared a substantial dump of stolen records as proof of a successful data breach. At that time, the company did not disclose the receipt of an extortion email transparently and only announced the data breach after a significant delay.

[REDACTED]

Please download qtox ([https://urldefense.com/v3/__https://qtox.github.io/__;!!PUxuPyJolyFOV1eDvpjUTTGUvfPfiLY6m8rliksCAMJjm7OSdfa-2oeRI3u16fNCQyx2iCaO5VYC8FzS7Pb3N01p4vAieLg\\$](https://urldefense.com/v3/__https://qtox.github.io/__;!!PUxuPyJolyFOV1eDvpjUTTGUvfPfiLY6m8rliksCAMJjm7OSdfa-2oeRI3u16fNCQyx2iCaO5VYC8FzS7Pb3N01p4vAieLg$)) [REDACTED] is our

BD1B683FD3E6C8094341317A4C09923B7AE3E7903A6CDB90E5631EC7DC1452636FF35D9F5AF2

[REDACTED]

From: "3lcqdwsboaq86xo" <3lcqdwsboaq86xo@proton.me>

[REDACTED]

Subject: [CRITICAL - REPLY] Qantas Airways Limited Databreach/Cyberattack

Hello, we are [REDACTED]

We're contacting you to inform you that Qantas Airways Limited (qantas.com) has suffered a massive databreach. [REDACTED]

[REDACTED]

Total Record Counts:

[REDACTED]

[REDACTED]

We possess:

- Full Name
- Email Addresses
- Phone Number
- Dates of Birth
- Frequent Flyer Numbers

And much more.

We will provide large samples of the data below.

Exposed Data:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

These groups also collaborate with other cybercrime actors, including initial access brokers (IABs). For example, in one of the posts shared by the hacking collective, they mentioned a member outside of their community offering access to an EU-based airline on the Dark Web.

A concerning note: Resecurity has observed similar access postings listed for nearly every airline and airport authority around the world. These accounts make these organizations vulnerable to similar attacks at the date and time of the attacker's choosing. Threat actors may combine a variety of methods to acquire compromised data, as well as access credentials for further development toward a complete data breach - potentially requiring the acquisition of infostealer logs, VPN access, and exposed tokens (non-human identities) available for sale on underground marketplaces.

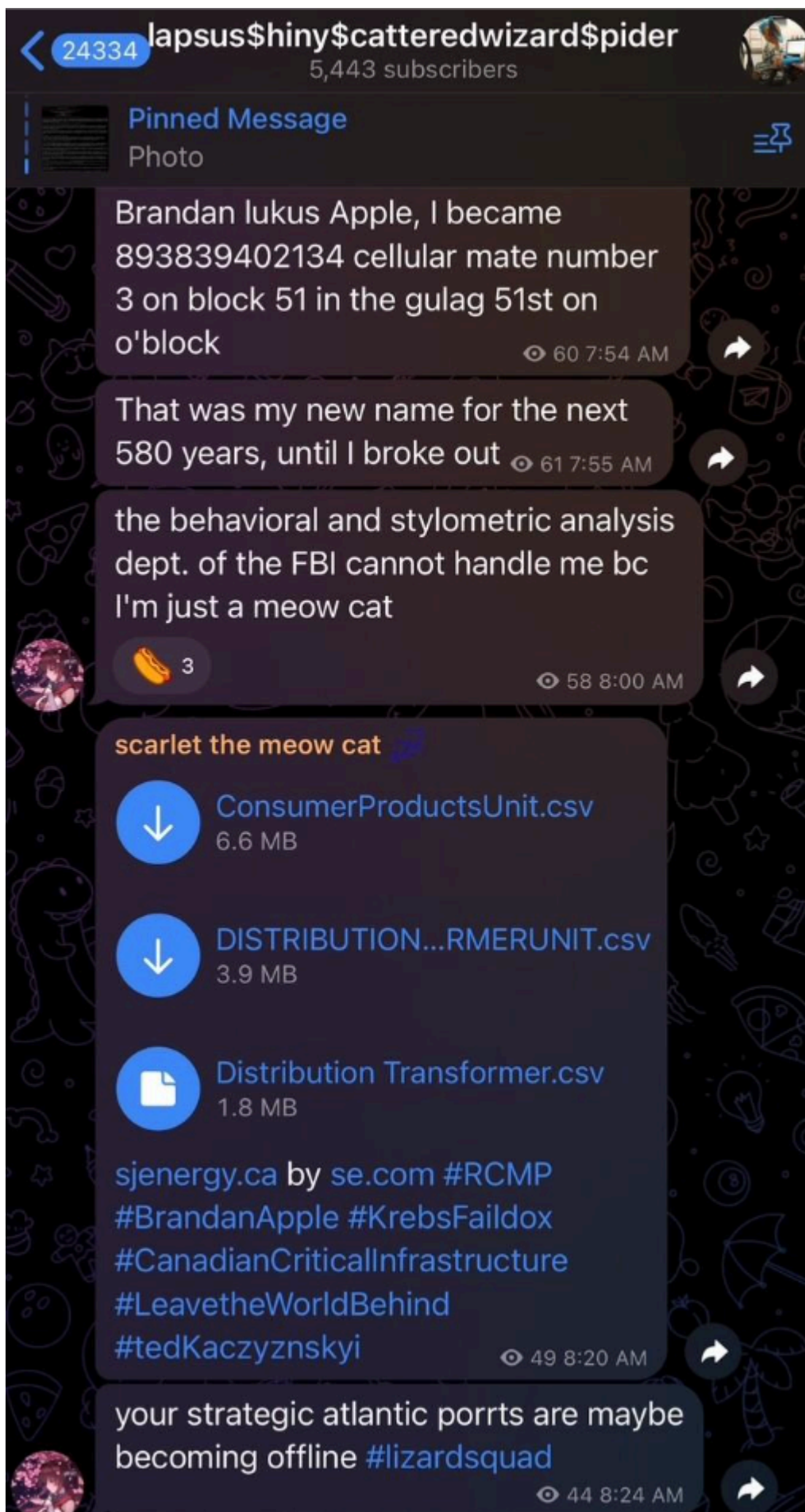
Cyberattacks on Retailers

Victoria's Secret [experienced](#) a significant security incident in late May 2025, forcing the company to take its U.S. e-commerce site offline for several days. The incident also disrupted corporate systems, leading to a [postponement](#) of the company's first-quarter earnings report. While the full scope of the breach is still under investigation by third-party experts, and the company has not confirmed if customer data was compromised, the disruption is expected to [impact](#) the company's second-quarter operating income by an estimated \$10 million.

However, in March 2024, AT&T confirmed that data leaked from the 2021 breach they previously denied was indeed theirs, acknowledging that it affected approximately 73 million current and former customers. This admission marked a significant reversal from the company's initial position.

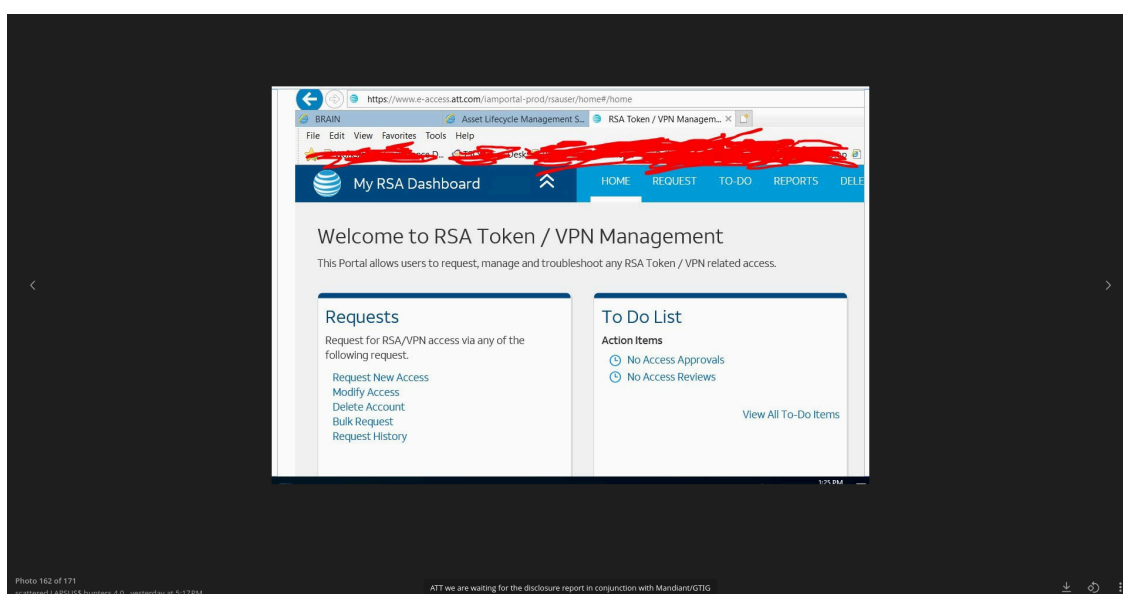
A separate cyberattack [transpired](#) in April 2024 after hackers John Eric Binns and Connor “Judische” Moucka allegedly exploited security flaws in Snowflake, a cloud data warehouse provider. This supply-chain attack affected over 165 organizations, with AT&T among the victims. The Snowflake-related breach exposed call and text metadata for nearly 110 million AT&T customers between May 1, 2022, and October 31, 2022, along with some records from January 2, 2023. Notably, this breach involved call logs and interaction data but did not contain personally identifiable information (PII) like Social Security Numbers (SSNs).

Reports indicate that AT&T paid Binns and Moucka a ransom of approximately \$370,000 in Bitcoin to have the Snowflake-related stolen data deleted. Moucka, also known as ‘**Waifu**’ and ‘**scarlet the meow cat**,’ also frequently posted in a since-deleted Telegram channel that was active in the Fall of 2024 called “lapsus\$hiny\$scatteredwizard\$pider.”

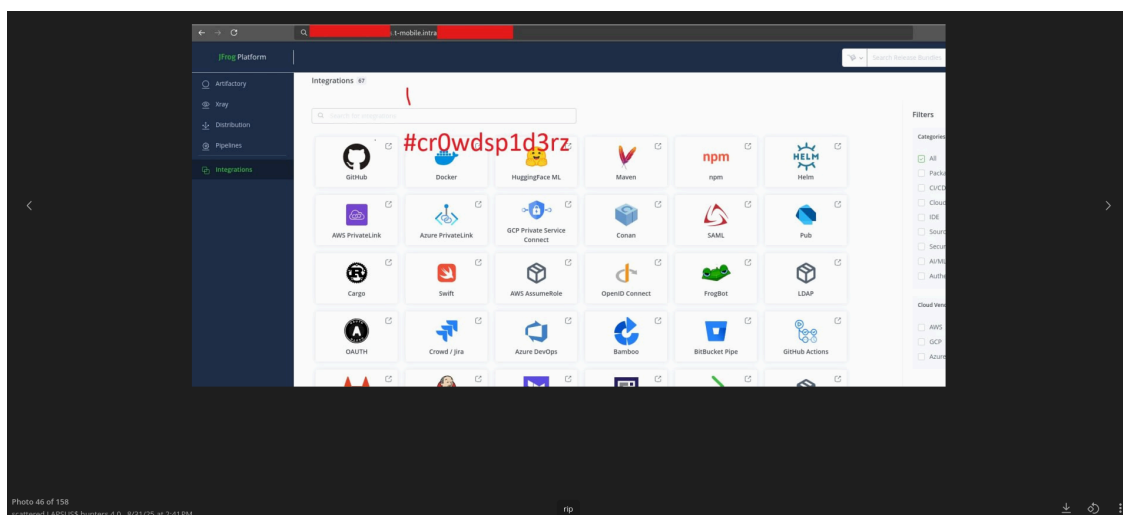


As the name of the channel suggests, the collaboration between the three eponymous groups likely commenced nearly a year before their more recent chaos-themed channel captured the attention of the cyber-threat-intelligence (CTI) community. Additionally, Moucka's highly active participation in this channel indicates some level of connectivity and possible collaboration between the since arrested Snowflake hacker and these threat groups. To this point, the **ShinyHunters** group was also associated with this Snowflake campaign, having taken credit for the major Ticketmaster data breach connected to the same security incident.

Some time ago, the hacking trio mentioned AT&T again and released a screenshot purportedly showing access to the RSA Token / VPN Management dashboard. The actors sanitized the access details, which makes it impossible to verify this information independently. However, the fact that they are mentioning the same target again may indicate continued interest in the telecom sector overall.



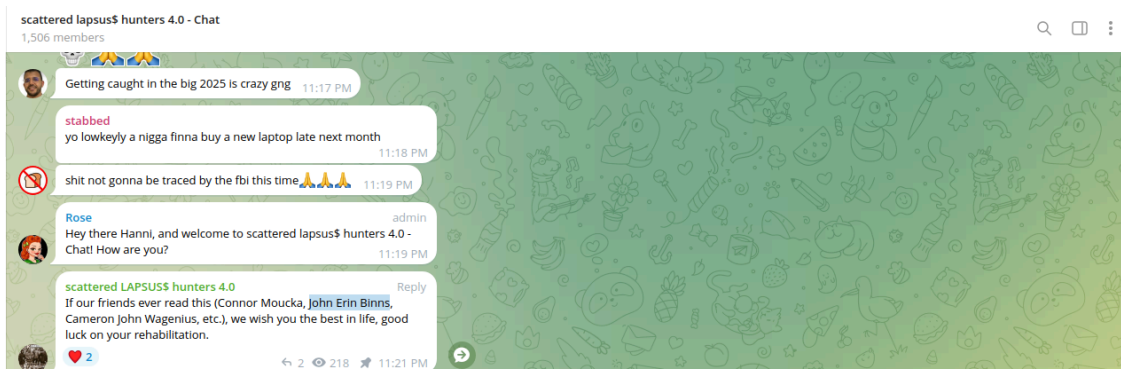
The group also mentioned T-Mobile and released a potential access to the JFrog Platform. In fact, this is not the first time advanced cybercriminals have targeted T-Mobile and have become victims of a cyber-attack.



T-Mobile has been [targeted](#) by multiple hacking groups and individuals over the years, with several high-profile breaches. In the summer of 2021, T-Mobile confirmed a massive data breach that exposed millions of customer

records. The hacker who took credit for this breach was Moucka's AT&T collaborator Binns, who was also [arrested](#) in Turkey in 2024.

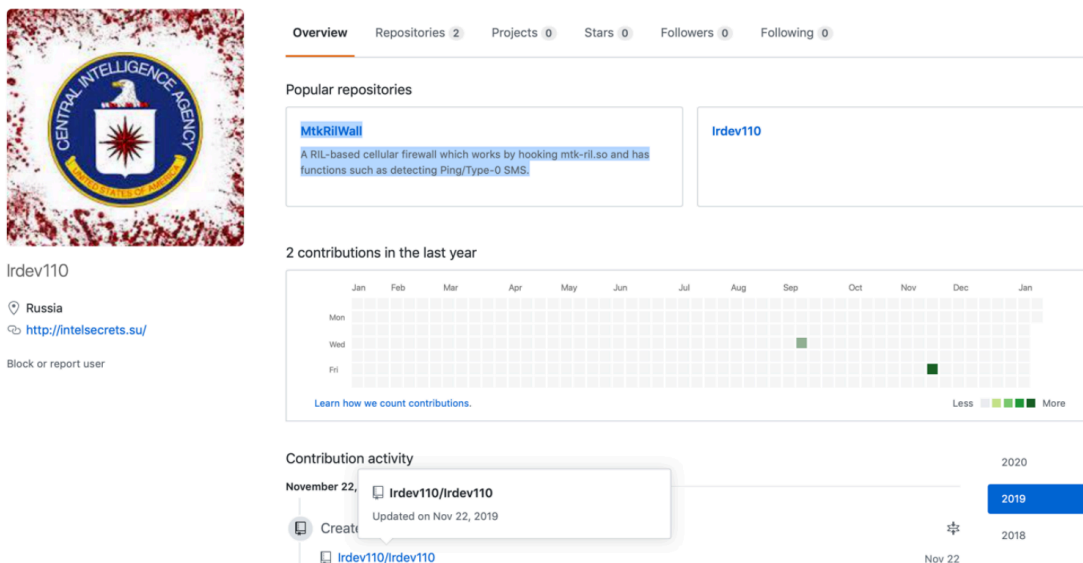
Binns publicly claimed responsibility for the attack, which led to significant regulatory scrutiny and a \$15 million fine for T-Mobile in 2024. Notably, the hacking conglomerate mentioned Binns in one of their recent Telegram updates.



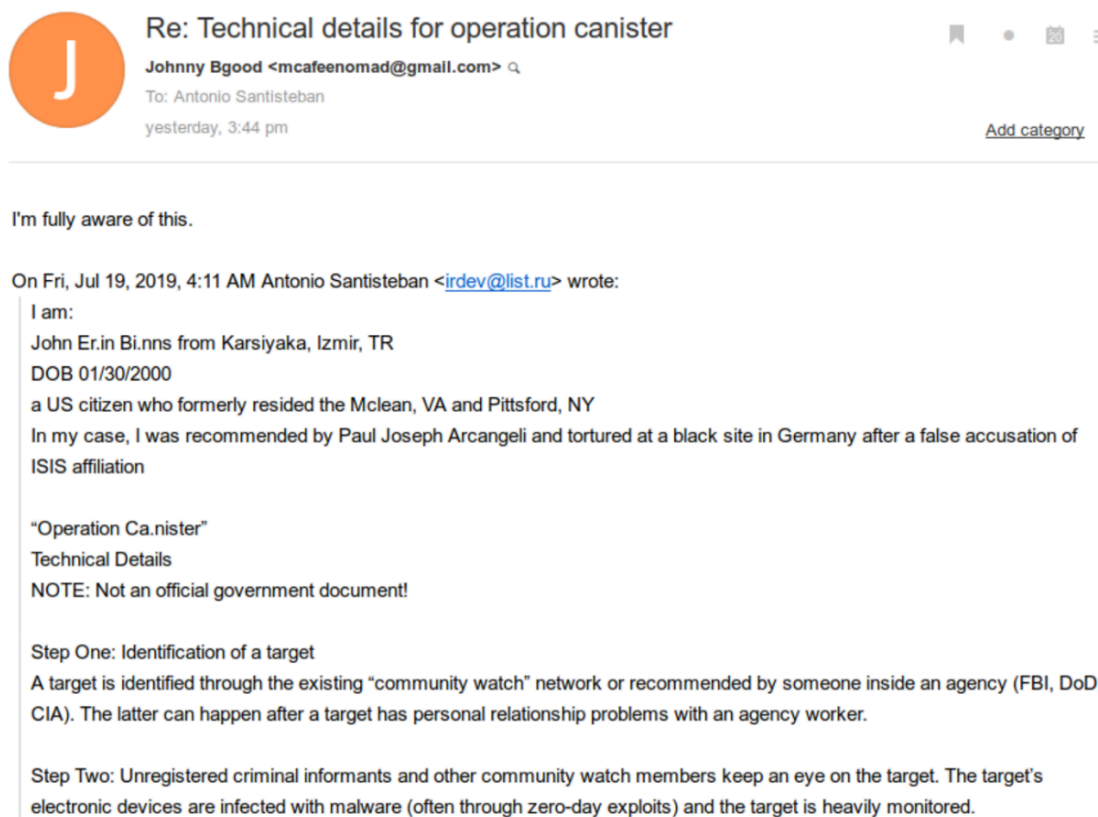
Resecurity has been tracking Binn's activity since August 2021, when he and his associates created the intelsecrets[.]su websites to harass U.S. government officials and publicize stolen data. Binn and his associates were using several aliases, including but not limited to "irdev007," "und0xxed," "v0rtex," "IIIIIIIIIIII", "Antonio Santisteban", "Aslan Aliev," and "Anton Lyshevskiy," falsely claiming to be originally from Minsk, Belarus.



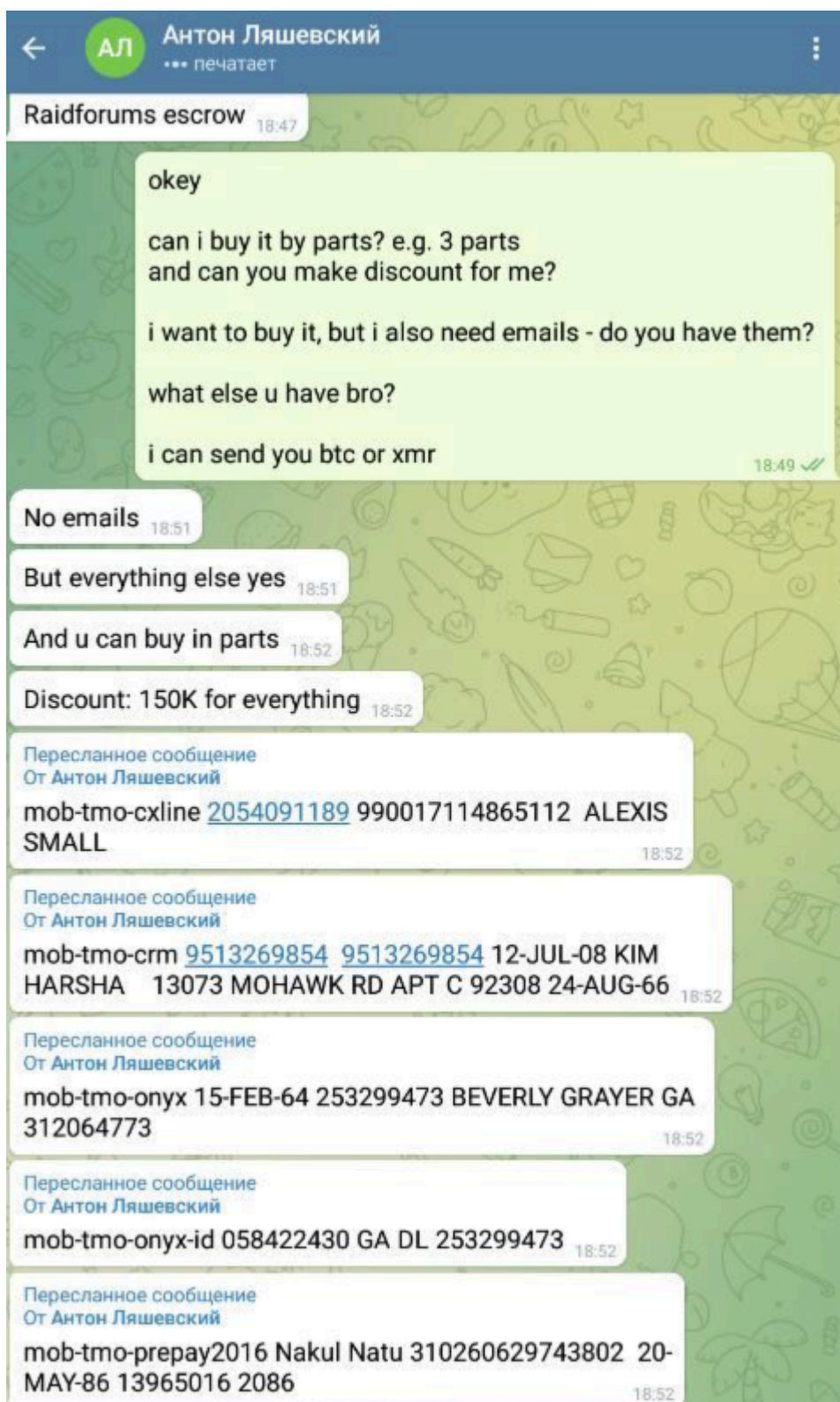
On some of his profiles, Binn also falsely claimed to be from Russia and even created several accounts on Russian-speaking Dark Web forums and email providers. One such account has been identified by Resecurity, along with his personal cellphone number registered via a foreign mobile carrier. Possibly, the actor thought that such measures could improve his OPSEC and complicate further investigation.



In one of the email messages acquired by Resecurity's HUNTER (HUMINT) team, the actor attempted to contact the now-deceased John McAfee and accused law enforcement of wrongdoing against him. He also mentioned several FBI employees and IC members at the intelsecrets[.]su website, threatening them.



The actor attempted to monetize stolen T-Mobile data for \$150,000, to be paid in cryptocurrency. Notably, he agreed to use escrow via RaidForums and provided numerous samples confirming the breach.



The actor also shared a screenshot from a possibly compromised system, showing a successful login dated September 29, 2015, via SSH. According to him, this access was obtained to penetrate the T-Mobile network.

```
ECDSA key fingerprint is MD5:46:7c:9a:f3:3c:58:01:a6:a5:0f:74:f4:06:21:95:85.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.92.10.12' (ECDSA) to the list of known hosts.
This is your local Unix password:
Last unsuccessful login: Tue Sep 29 08:10:52 PDT 2015 on ssh from gaatladk0475392.gsm1900.org
Last login: Wed Aug 4 08:54:27 PDT 2021 on ssh from 100.123.0.2
=====
T-Mobile USA Corporate Network

Use of this system is explicitly limited to the employees of
T-Mobile USA individuals conducting business at the behest of
T-Mobile. All data contained on T-Mobile computer systems is owned
by T-Mobile and may be monitored, intercepted, read, copied, or
captured in any manner and disclosed by authorized personnel.

THERE IS NO RIGHT TO PRIVACY ON THIS SYSTEM.

Use of this system constitutes express consent to monitoring, data
capture, and disclosure to law enforcement officials by authorized
personnel. Unauthorized use of this system is a criminal offense
and will be prosecuted to the fullest extent of both state and
federal law.

Use of this system also constitutes express agreement that you will
not: modify any system files (any file not owned by application or
application user), add account(s) to the system, grant any account
additional privileges over those which have been approved and
implemented by Operations, or bypass any controls put in place to
prevent these actions. Any infringement will be reported to
T-Mobile's Cyber Incident Response Team (CIRT) or Corporate
Investigations (CI), and may be subject to disciplinary action.

For technical assistance, please call the National Help Desk at
1-877-878-7326.
=====
prdcmrp102 in polaris Datacenter on pxibm204
SN: 218DAA7 HMC: pxhmc201a Row: R112 Cabinet: C07
Model: IBM,9117-MMD - 16 Logical CPUs - 112.00 GiB RAM
ServiceNow Status: INSTALLED
Used For: Production Audit Flags: NO_PCI NO_SOX
=====

*****
Databases Running On This Server ..
*****
+ASM2
+ccmrp2
*****
Goldengate Running On prdcmrp101 Server as ggsadm User for PCMRP database for Replication Hub ..
*****
prdcmrp102:oracle:sid:/home/oracle: 
```

The actor shared various internal identifiers, hostnames, and references. He also indicated that the system could be used by one of the FBI units for lawful interception purposes, and such access would provide extremely extensive visibility into the activities of mobile carrier customers.

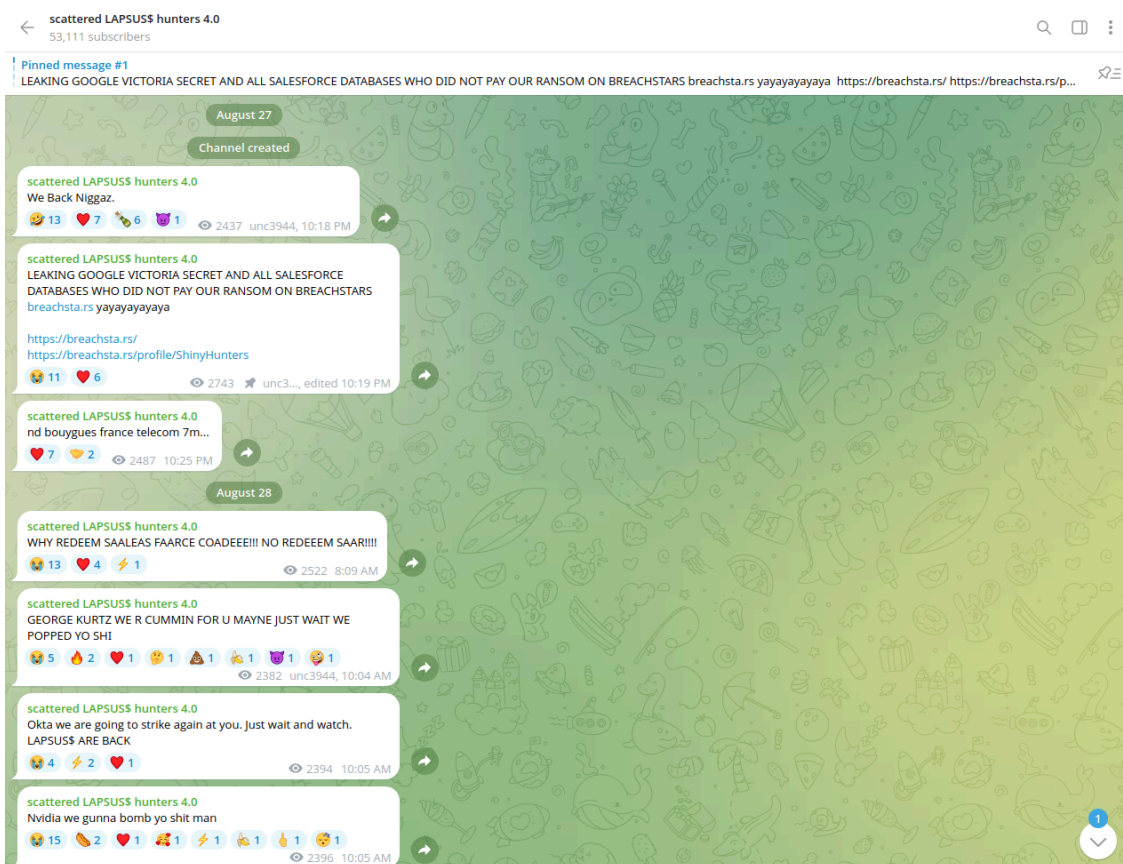
```
prms
prnst-scan.unix.gsm1900.org
prdtalers0004.unix.gsm1900.org
prnst ,4236102900
Oracle
19.0.0
Production
Law Enforcement App
APM0103533
Guardian - Production
APP0005768
Shobha Sangani (SSangan)
Rittu Jewett (RJewett2)
Craig Thomas (DThomas109)
Production
LERS
APM0103533_Law_Enforcement_App
Shobha Sangani (SSangan-DISABLED46739)
Rittu Jewett (RJewett2)
Craig Thomas (DThomas109)
RMS,RMS_SRV_MGR
Active ,
22-JUL-19,09-AUG-21,Y,Production
prnst-scan.unix.gsm1900.org
rac ,N
N
N ,N,N,Y
sadulla1
ssuraka1
TIER_1
prms2
```

Resecurity acquired data samples containing consumer details, along with IMSI and other fields, stored in Elastic data lake.

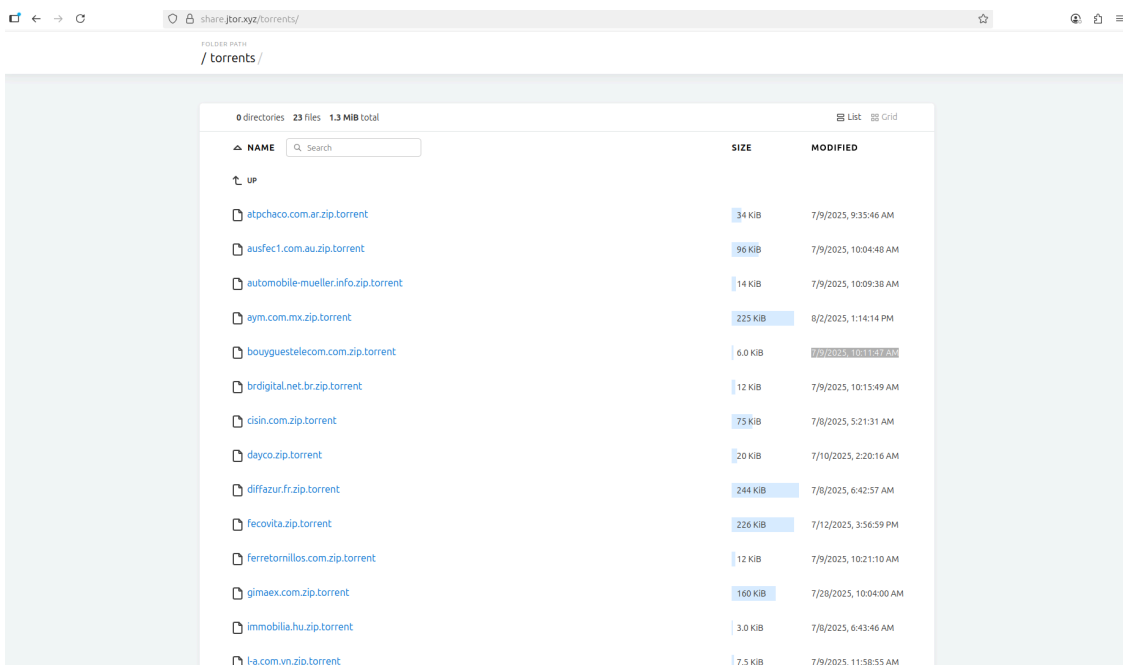
Filter *current* page...						
fname (fname.keyword)	lname (lname.keyword)	msi (msi.keyword)	msidn (msidn.keyword)	dob (dob.keyword)	puk1 (puk1.keyword)	pin (pin.keyword)
se	varela	318268253335931	13136639397	20-DEC-64	46225243	1234
PREPAID	CUSTOMER	318268251858268	13235999164	09-SEP-88	61267217	0000
mifer	Burzynski	318268593904488	13144906341	09-OCT-58	63454869	7370
ck	cohorst	318268254678266	19562479223	20-MAR-68	22412330	1234
uhnae	davis	318268653523779	18434525683	16-SEP-93	55387244	0916
uan	green	318268255474855		28-FEB-92	32623586	6229
reesha		318268255417894	13372929842	06-JUL-89	79274342	2888
mine	Ding	318268584973158		29-AUG-75	98438827	1983
rad	palladino	318268255481133	19143123116	15-FEB-86	76779833	1234
PREPAID	CUSTOMER	318268938669152	13233174787	01-JAN-80	97889287	4787
tsu	Ishida	318268285578167	15822969452	18-JAN-49	68837783	9432
lfrey	Morris	318268314833687	16466372835	19-MAR-45	43386115	1111
/	hartley	318268593319069	13382616883	28-DEC-43	46479633	6883
)	GRIFFIN	318268613521374		28-MAR-47	11111111	5281
PREPAID	CUSTOMER	318268583648883		28-APR-72	98826328	2872

Binn's activity demonstrated some of the first episodes in cybercrime history of targeted attacks against law enforcement and telecommunications companies, and it is likely that the collective has continued to conduct these attacks at a much more sophisticated level. For example, one year later, other groups like Lapsus\$ also [claimed](#) responsibility for breaching T-Mobile's internal systems.

The actors also mentioned Bouygues Telecom, the third oldest mobile network operator in France, after Orange and SFR, as one of the targeted telecoms. At the beginning of August, Bouygues Telecom, a large French mobile carrier, disclosed a cyberattack and data breach affecting more than 6 million customer accounts. At that time, no specific threat actor or group was identified.



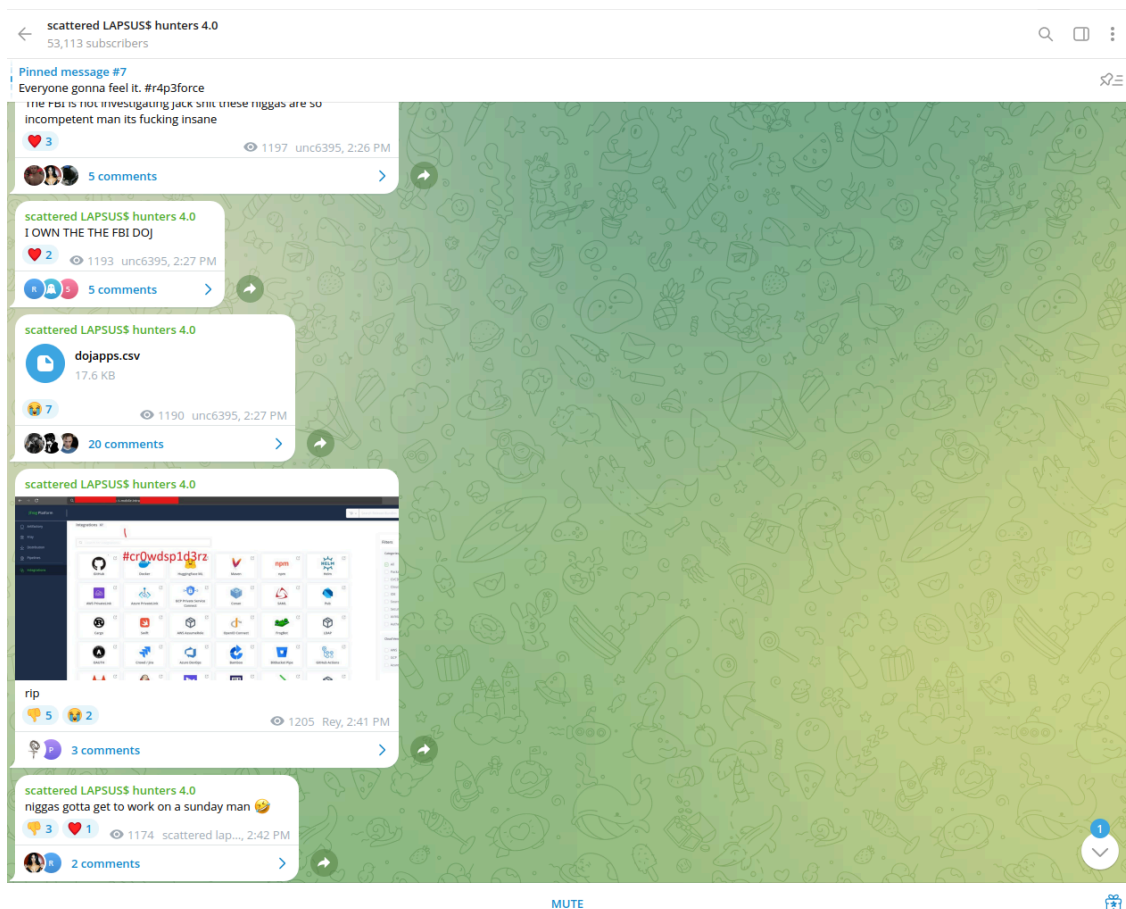
At the same time, the data presumably stolen from Bouygues Telecom began to appear on the Dark Web for sale. Resecurity has acquired a substantial number of records from several different actors, confirming the involvement of access brokers during the early stages of the intrusion. As of today, a group calling themselves "[J Ransomware](#)" claimed responsibility for the attack and shared the stolen data in the form of a Torrent file available for download via their Data Leak Site (DLS) on the TOR network.



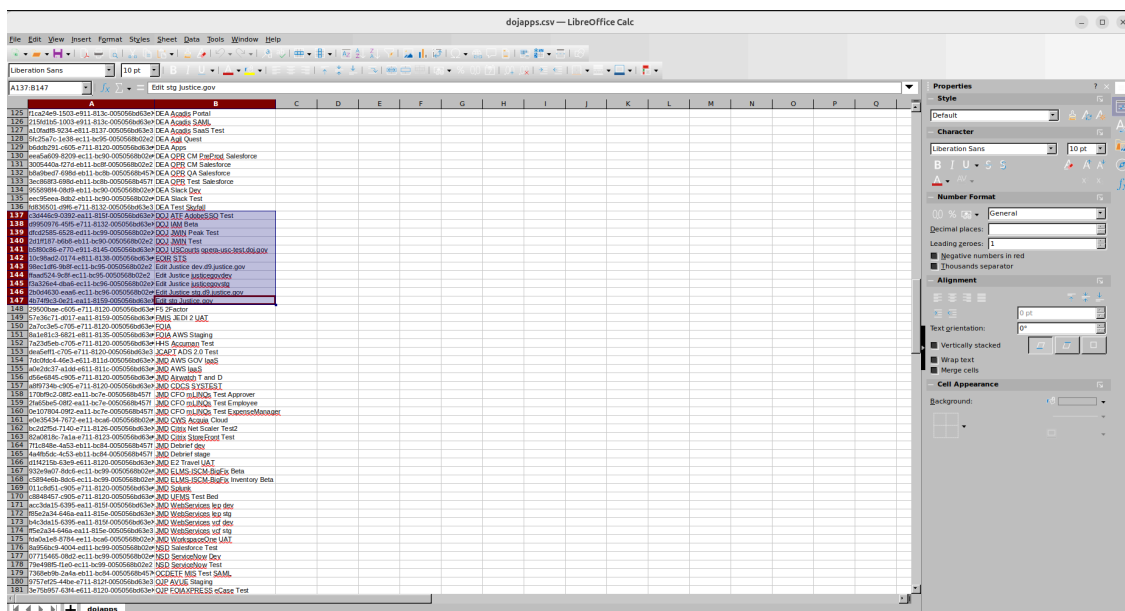
These details may suggest a possible overlap between the activities of the hacking "trio," independent access brokers, and ransomware groups. Given that the cybercrime ecosystem is highly dynamic, actors may collaborate, exchange, share, and reuse stolen data and access among themselves to identify the most effective monetization strategies.

Cyberattacks on Law Enforcement

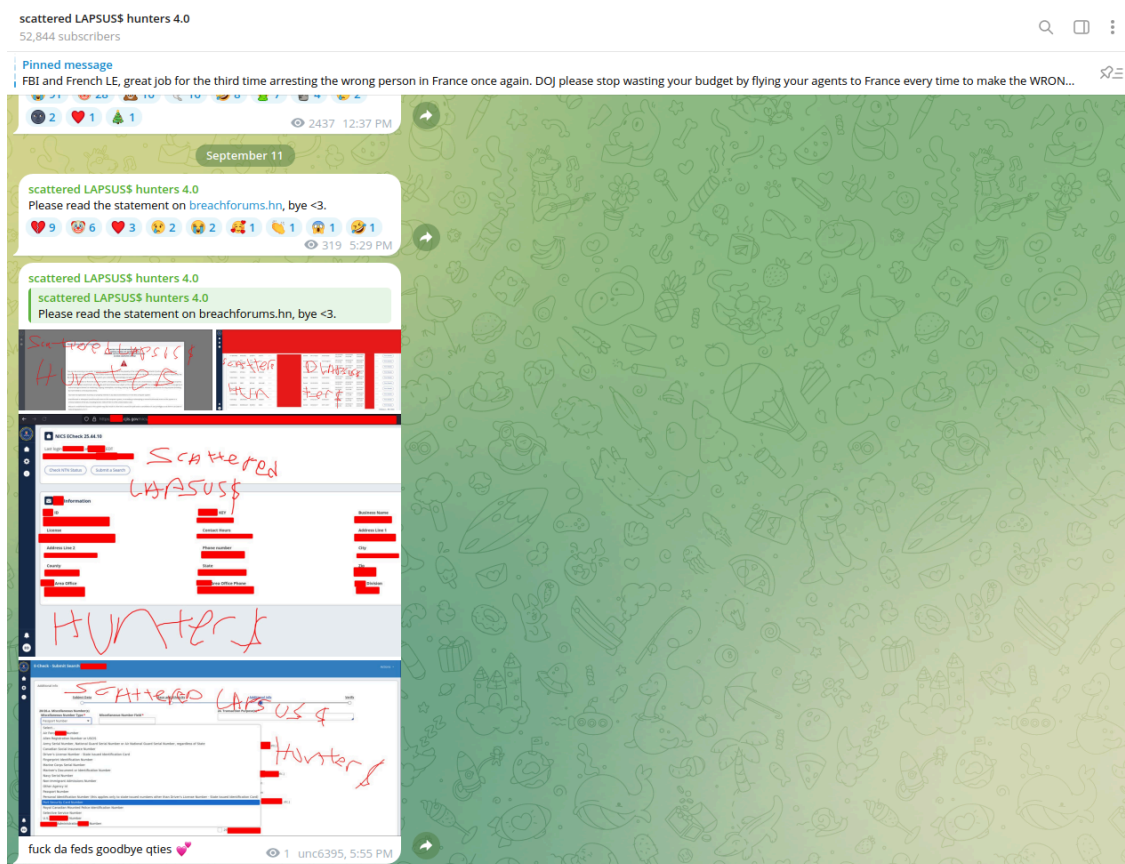
Neither **ShinyHunters** nor **Scattered Spider** has a documented history of directly attacking law enforcement agencies. Contrarily, some new content has started to emerge, although the details remain limited due to the potential sensitivity of such activities, and that the trio's recent breach claims are false. Before the group disappeared from public channels, the hacking trio claimed to have breached various law enforcement agencies, including the FBI. In their postings, they published data samples and screenshots suggesting a possible compromise of an account within an undisclosed law enforcement system.



The actor with the alias UNC6395 shared several text files containing identifiers of various applications and hostnames referencing the U.S. government.



It is possible that the group attempted to demonstrate resilience after legal actions were taken against one of their members by [French](#) and U.S. law enforcement authorities.



The actors also shared screenshots from the so-called NICS E-Check system (National Instant Criminal Background Check System). Law enforcement and criminal justice agencies use this system to conduct background checks.

E-Check - Submit Search [REDACTED] Actions +

Additional info

Subject Data [REDACTED] Race and Ethnicity [REDACTED] Additional Info [REDACTED] Verify [REDACTED]

20/26 a. Miscellaneous Number(s)

Miscellaneous Number Type * [REDACTED]

Miscellaneous Number Field * [REDACTED]

24. Transaction Purpose(s) [REDACTED]

Select...

- Air Force [REDACTED] Number
- Alien Registration Number or USCIS
- Army Serial Number, National Guard Serial Number or Air National Guard Serial Number, regardless of State
- Canadian Social Insurance Number
- Driver's License Number - State issued Identification Card
- Fingerprint Identification Number
- Marine Corps Serial Number
- Mariner's Document or Identification Number
- Navy Serial Number
- Non-Immigrant Admissions Number
- Other Agency Id
- Passport Number
- Personal Identification Number (this applies only to state-issued numbers other than Driver's License Number - State issued Identification Card)
- Port Security Card Number
- Royal Canadian Mounted Police Identification Number
- Selective Service Number
- U.S. [REDACTED] Number
- [REDACTED] Administration [REDACTED] Number

[REDACTED] 25 [REDACTED]

SCATTERED LAPsus\$

HUNTER\$

← → ↻ https://cjis.gov/nics [REDACTED]

NICS ECheck 25.44.10

Last login [REDACTED] a [REDACTED] EDT

Check NTN Status Submit a Search

Information

ID [REDACTED] KEY [REDACTED] Business Name [REDACTED]

License [REDACTED] Contact Hours [REDACTED] Address Line 1 [REDACTED]

Address Line 2 [REDACTED] Phone number [REDACTED] City [REDACTED]

County [REDACTED] State [REDACTED] Zip [REDACTED]

Area Office [REDACTED] Area Office Phone [REDACTED] Division [REDACTED]

HUNTER\$

SCATTERED LAPsus\$

HUNTER\$

Please review Terms and Conditions

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
NATIONAL INSTANT CRIMINAL BACKGROUND CHECK
E-CHECK COMPUTER SYSTEM

You are now accessing a non-public "protected computer" system that is the property of the United States Department of Justice. Use of this computer system is reserved exclusively to the United States Government and those expressly authorized by the FBI for specific purposes permitted or required by law. By accessing and/or using this computer system, you understand, acknowledge and agree that:

All data transmitted to or from this computer system, including any stored data resulting from such a transmission, is and shall remain the property of the United States Government. All such data and transmissions are subject, at the unreviewed discretion of the United States Government or any agency or authorized agent thereof, to monitoring, copying, interception, recording, tracking, disclosure, dissemination, retrieval or destruction for any purpose (including but not limited to criminal prosecution).

You have no expectation of privacy or property interest in any data transmitted to or from this computer system.

Unauthorized or attempted unauthorized access to this computer system, or exceeding or attempting to exceed authorized access to this system is a criminal violation of the law, including Section 1030 of Title 18 of the United States Code.

Misuse or unauthorized access to this system may also result in a fine not to exceed \$10,000 and/or cancellation of user privileges as set forth in 28 Code of Federal Regulations 25.11.

User ID	Name	Status	Date 1	Date 2	Date 3	Date 4	Date 5	Action
101BNH0BD	MITCHELL JOSEPH SCOTT	Denied	04/17/2020	03/24/2020	03/18/2020	03/22/2020	03/22/2020	Print Details
10133KH51	Not Supplied	Not Assigned	08/23/2019	08/28/2019	08/23/2019	08/23/2019	08/23/2019	Print Details
1011VMD14	Not Supplied	Not Assigned	08/10/2019	08/16/2019	07/11/2019	07/16/2019	07/16/2019	Print Details
100MSPBTL	MYGAN PATRICK GERARD	Denied	02/19/2018	04/05/2018	03/31/2018	04/06/2018	04/06/2018	Print Details
100KY5SW5	INGALA RICHARD PAUL	Denied	04/30/2018	04/05/2018	03/31/2018	04/06/2018	04/06/2018	Print Details
100PUNSG	EBBS BRYAN WILLIAM	Denied	03/23/2018	02/24/2018	02/20/2018	02/20/2018	02/20/2018	Print Details
100CH6214	ROBERT NMM	Denied	10/09/2017	09/14/2017	09/09/2017	09/15/2017	09/15/2017	Print Details
100BDMC02	MULLEN MATTHEW STEVEN	Denied	08/26/2017	08/02/2017	07/27/2017	10/06/2017	10/06/2017	Print Details
100916KJ6	GROPMAN KENNETH ROBERT	Open	07/02/2017	06/08/2017	06/08/2017	06/08/2017	06/08/2017	Print Details
100BBHGS	RODRIGUEZ RAMON NMN	Denied	06/04/2017	05/11/2017	05/09/2017	05/05/2017	05/05/2017	Print Details

Similar messages have been directed by the trio toward Italian law enforcement. The actors leaked a possible report, presumably authored by the police, related to their activities. Resecurity's dark web data collection has identified users accessing the NICS system from devices controlled by threat actors, including accessing systems from infected devices outside the United States.

Rapporto Investigativo Carabinieri Collaborazione con Interpol e.pdf

Legione Carabinieri "Marche"
Comando Provinciale di Ancona
Rapporto Operativo-Nucleo Investigativo

1. Rapporto operativo: Nucleo Investigativo 1 - Ser. aggiornamento al 08.25.2025

2. Nominativo indagato: Procura della Repubblica presso il Tribunale di Ancona Dott. Valeria Ciglioli e Dott. Rosario Rossi conosciuti

3. Nominativo indagato: Procura della Repubblica presso il Tribunale di Ancona Dott. Valeria Ciglioli e Dott. Rosario Rossi conosciuti

4. Stato attività: Il Nucleo Investigativo competente sta eseguendo attività investigative nei confronti di un'organizzazione criminale di origine italiana coinvolta in condotte di criminalità

5. Soggetti coinvolti alla data attuale: [Redacted]

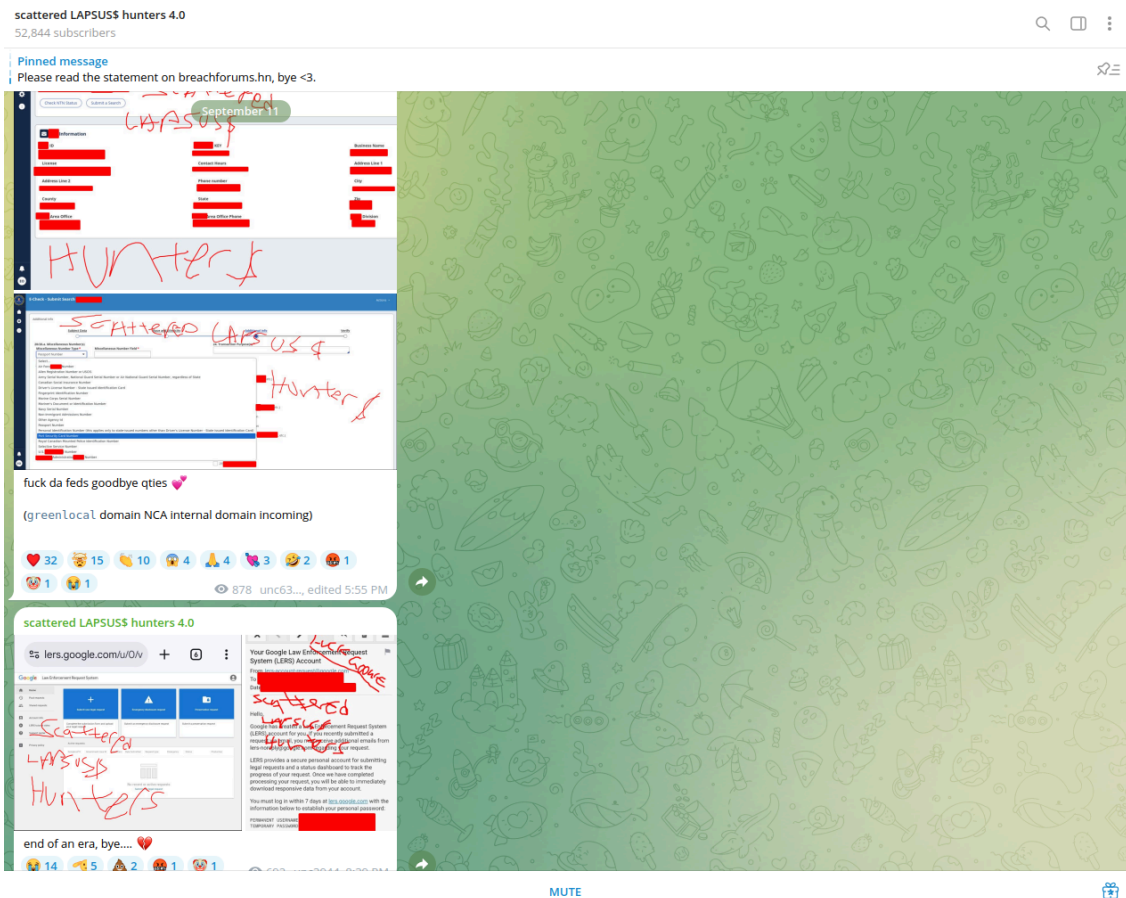
6. Rilevamenti operativi alla data attuale: [Redacted]

7. Note: [Redacted]

IL COMANDANTE

In the trio's last posts before their farewell announcement, the group also claimed to have breached sensitive law enforcement data-sharing portals belonging to the UK's National Crime Agency, responsible for a string of successful arrests targeting **Scattered Spider** members, and Google.

The trio also shared a screenshot from the Law Enforcement Notification System (LENS). This web-based system provides local law enforcement with information on federal offenders currently under supervision by the U.S. Courts. As with the NICS system mentioned above, Resecurity's dark web data collection has found users accessing the LENS system from devices under threat actor control, including from infected devices outside the United States.



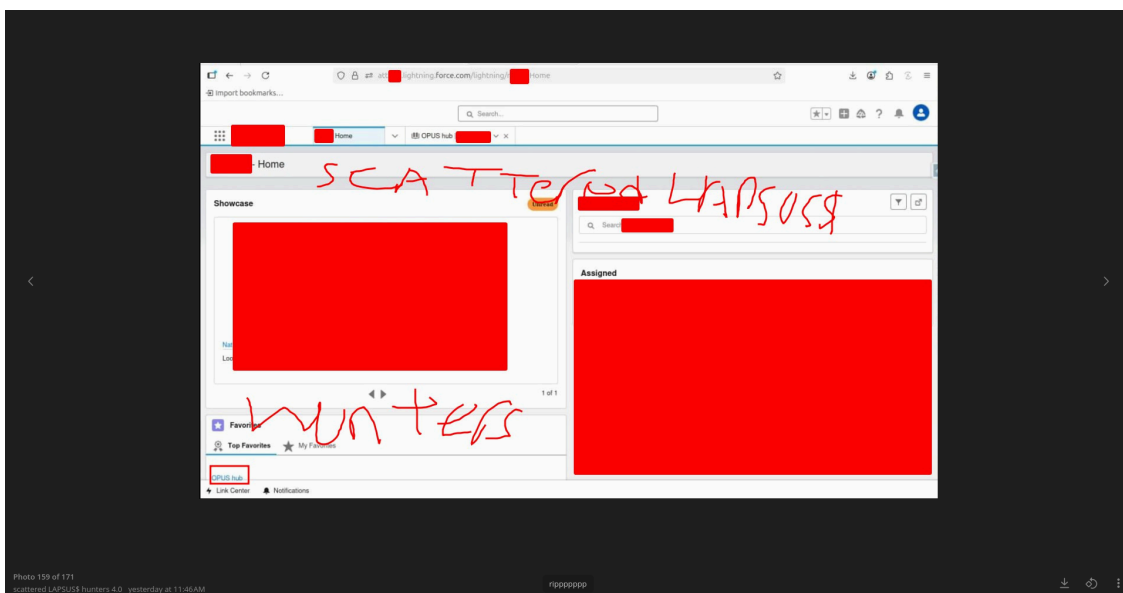
Cyberattacks on Salesforce

Most recently, **ShinyHunters** and their collaborators have made headlines for actively targeted Salesforce environments in a series of high-profile cyberattacks throughout 2025. These attacks involved sophisticated social engineering, vishing, and OAuth token abuse to compromise Salesforce accounts and exfiltrate large volumes of data from numerous blue chip companies.

The group exploited OAuth tokens to access Salesforce environments, enabling them to steal massive amounts of data from hundreds of organizations. **ShinyHunters** claimed to have stolen over 1.5 billion Salesforce records from 760 companies by compromising OAuth tokens associated with Salesloft and Drift integrations. This allowed the group to access and exfiltrate customer relationship management (CRM) data at scale.

[illegible]

Page 24 of 33



The issue [affected](#) over 20 companies, including cybersecurity vendors:

TheCommNews
3,975 subscribers

Salesloft Drift OAuth Breach Hits Major Tech Firms

In a major supply chain attack, threat group UNC6395 exploited compromised OAuth tokens from the Salesloft Drift-Salesforce integration, bypassing MFA and exfiltrating sensitive Salesforce data — including support cases, business contacts, AWS keys, and Snowflake tokens.

Logs were reportedly deleted to hide the intrusion. So far, **over 20 companies** have been confirmed as victims, including:

- ◆ Palo Alto Networks
- ◆ Tenable
- ◆ Cloudflare
- ◆ CyberArk
- ◆ Zscaler
- ◆ Proofpoint
- ◆ Rubrik
- ◆ BeyondTrust
- ◆ Fastly
- ◆ Dynatrace
- ◆ Qualys
- ◆ Nutanix
- ◆ Elastic
- ◆ Sigma Computing
- ◆ Esker
- ◆ Workiva
- ◆ Cato Networks
- ◆ JFrog
- ◆ Bugcrowd
- ◆ Heap
- ◆ Megaport
- ◆ Tanium
- ◆ PagerDuty
- ◆ SpyCloud

Track updates here: [\[driftbreach.com\]](https://driftbreach.com) (<https://driftbreach.com>)

Expect the list to grow as the investigation continues.

@TheCommLeaks / @notraceexch / @privrdp

5

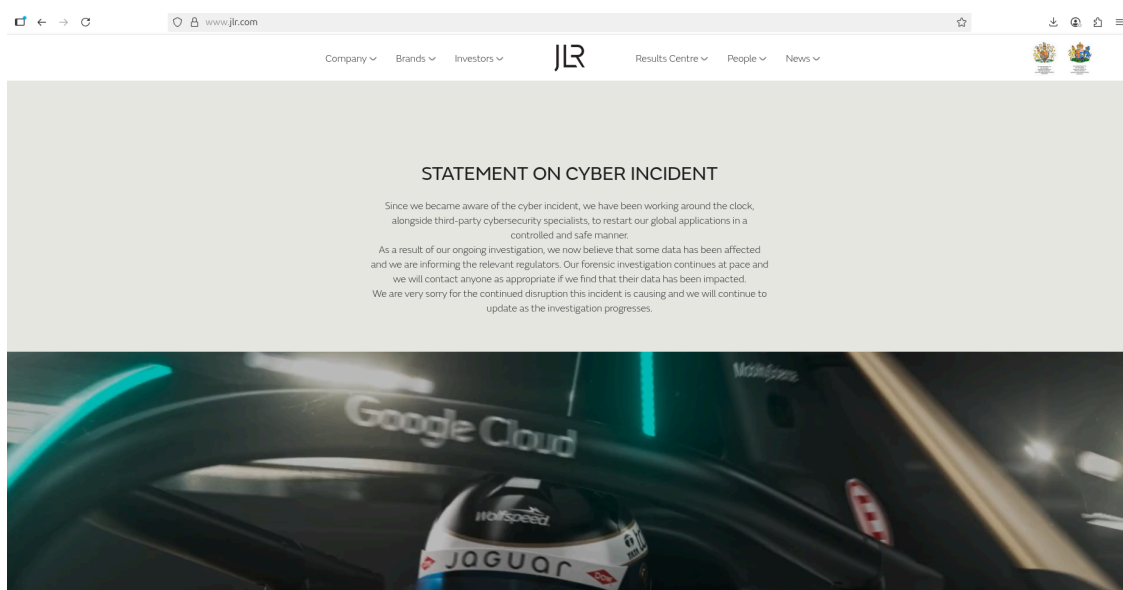
753 12:57 PM

Leave a comment

Attack on Jaguar Land Rover (JLR)

Jaguar Land Rover (JLR) has been the target of several significant cyberattacks in 2025. The most recent attack [discovered](#) on August 31— a [breach of historically catastrophic proportions](#)— has been credibly attributed to the threat actor trio of **Scattered Spider** (also known as **Octo Tempest/UNC3944**), **ShinyHunters**, and **Lapsus\$**.

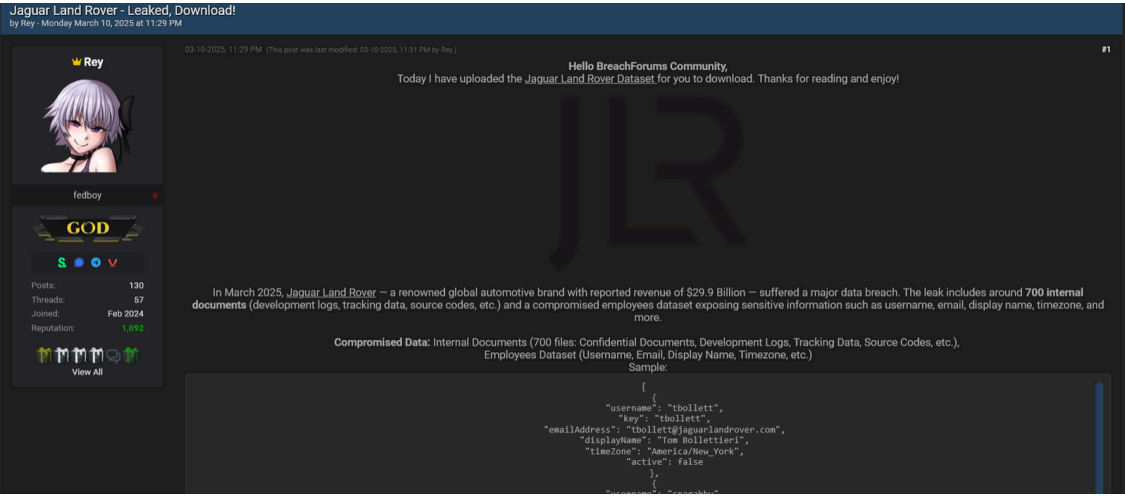
There is no indication this breach, which has shut down JLR's global production line for over the last three weeks and threatens a major auto industry supply-chain disaster, is linked to the broader Salesforce campaign. In fact, intelligence collected by Resecurity suggests this attack is part of a unique exploit campaign that has no links to the Salesforce supply-chain saga.



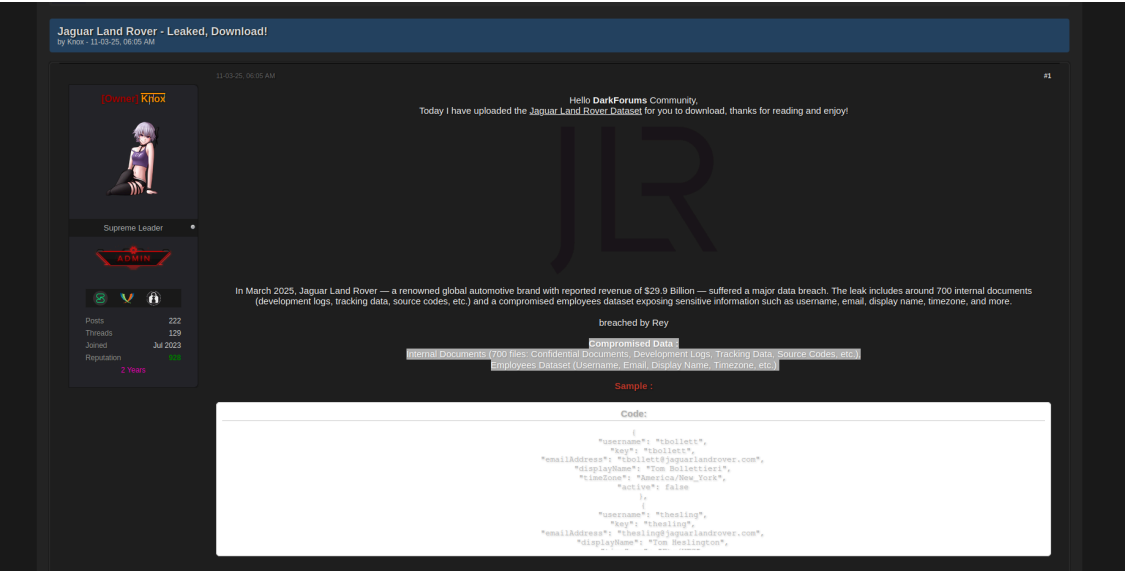
Notably, a separate earlier breach in March 2025 was attributed to the **HELLCAT** ransomware group, which counts an actor known as "**Rey**" from Raidforums as a leading member. **Rey**, reportedly relied on infostealer harvesting to steal Jira credentials from an LG Electronics employee (siphoned by Lumma malware). Jira is a widely used software development collaboration tool that helps engineers manage projects and track issues.

Infostealers are a type of malware designed to harvest sensitive information from infected devices covertly. This includes login credentials, session cookies, browser-stored passwords, and other authentication data. Once exfiltrated, this information is sold on cybercrime marketplaces or used directly by attackers to access high-value platforms like Salesforce. Ordinary infostealer families used in enterprise attacks include Azorult, Lumma, RedLine, Raccoon, and Vidar.

Infostealers harvest not only usernames and passwords, but also active session cookies. Attackers use these to hijack authenticated sessions, gaining immediate access to Salesforce without triggering login alerts or MFA challenges. Attackers also trick users into authorizing malicious "Connected Apps" in Salesforce, which can generate long-lived OAuth tokens. These tokens grant persistent access to Salesforce data, often bypassing MFA and other controls.



Darkforums administrator **Knox** amplified the same breach at roughly the same time as **Rey**:



Rey exfiltrated gigabytes of data from JLR, including Jira issues, source code, employee databases, usernames, emails, and dev logs, which were then leaked on forums to facilitate phishing and lateral attacks. Notably, an account with the same alias was present in the member list of the chaos-themed Telegram channel created by the hacking trio. However, there is no conclusive evidence these personas belong to the same actor. Shortly after **Rey**'s March 2025 posting, hacker "APTS" dumped 350GB more using 2021 creds.

Jaguarlandrover Jira 2025/Jan
by APTS - Friday March 14, 2025 at 08:02 AM

03-14-2025, 08:02 AM (This post was last modified: 03-14-2025, 08:15 AM by APTS.)

APTS



Breached

MEMBER

Posts: 6
Threads: 3
Joined: Feb 2025
Reputation: 0

JLR

gofile.io/d/ [redacted]
gofile.io/d/ [redacted]
uncompressed 9.3 GB

350 gb archive of attachments is available to upgraded users. drop inbox.

Hidden Content

password: of [redacted]

<!--
RSS generated by JIRA (7.3.6#73017-sha1:51437cf70ba5689aad808c1cc05a46d676f5739) at Wed Jan 22 19:26:55 UTC 2025

It is possible to restrict the fields that are returned in this document by specifying the 'field' parameter in your request.
For example, to request only the issue key and summary add field=key&field=summary to the URL of your request.
For example:
<https://jira.sdo.jlrmotor.com/sr/jira.issueviews:searchrequest-xml/temp/SearchRequest.xml?jqlQuery=&tempMax=1000&pager/start=->>
-->
<!-- If you wish to do custom client-side styling of RSS, uncomment this:

There is no evidence that **Rey**, **Knox**, **APTS**, or the broader **HELLCAT** collective were involved in the more recent and disastrous September attack. JLR has confirmed the September 2025 cyberattack, stating it caused severe operational disruption and resulted in confirmed data theft.

Notably, right before this string of JLR-related leaks, **Rey** published data from an unnamed government system, presumably related to Florida.

BreachForums Leaks Databases **DATABASE** FL Department of State - Leaked, Download! Mark all as read Today's posts

FL Department of State - Leaked, Download!
by Rey - Saturday March 29, 2025 at 10:44 PM

03-29-2025, 10:44 PM

Rey



fedboy

GOD

Posts: 151
Threads: 41
Joined: Feb 2024
Reputation: 1,322

View All

Hello BreachForums Community,
Today I have uploaded the Florida Department of State Database for you to download, thanks for reading and enjoy!



The Florida Department of State has suffered a significant data breach, exposing 568,835 records, including 487,961 unique email addresses. The breach compromised sensitive personal information from individuals associated with the department, released exclusively to piss the #FederalChunks off.

Compromised data (Sample <https://ghostbin.lain.la/paste/43kg>): First names, Last names, Addresses, Email addresses

Hidden Content

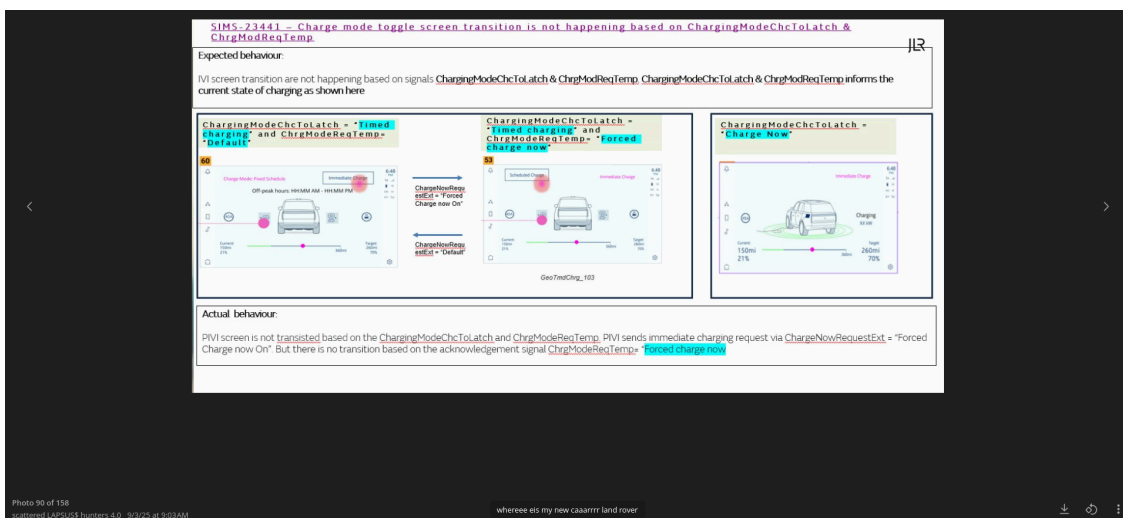
Unlock for 0 credits

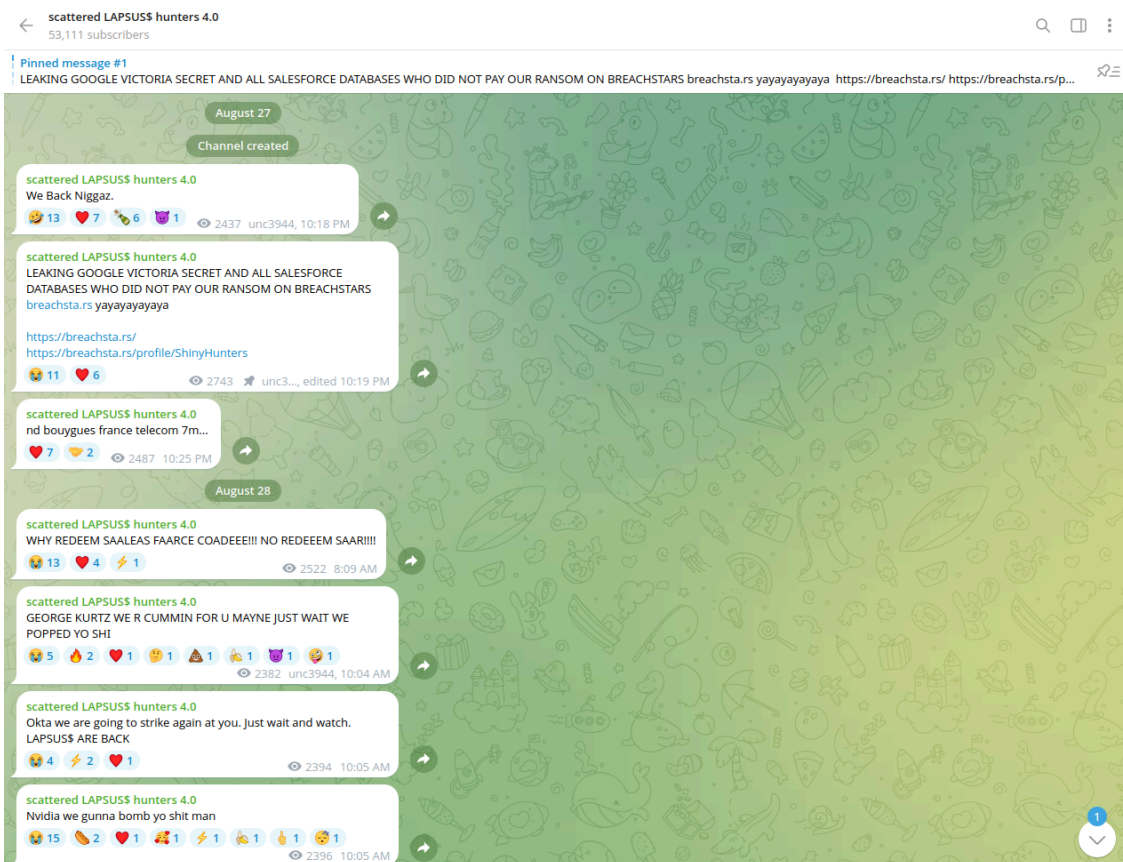
Circling back to JLR, *Wired* [reported](#) that the automaker may be “losing up to £50 million (\$67 million) per week in the shutdown.” Additionally, *Wired* said that, as the production shutdown stretches out until at least the beginning of October, “the knock-on impacts are being felt at the hundreds of companies that supply JLR with parts and materials and risk turning the attack into a full-blown crisis.”

While JLR has not publicly named the threat actors, the claims and evidence from **Scattered Spider**, **ShinyHunters**, and their collaborators are widely accepted by the cybersecurity community and media as credible. This attack caused severe operational disruption and a confirmed data breach.

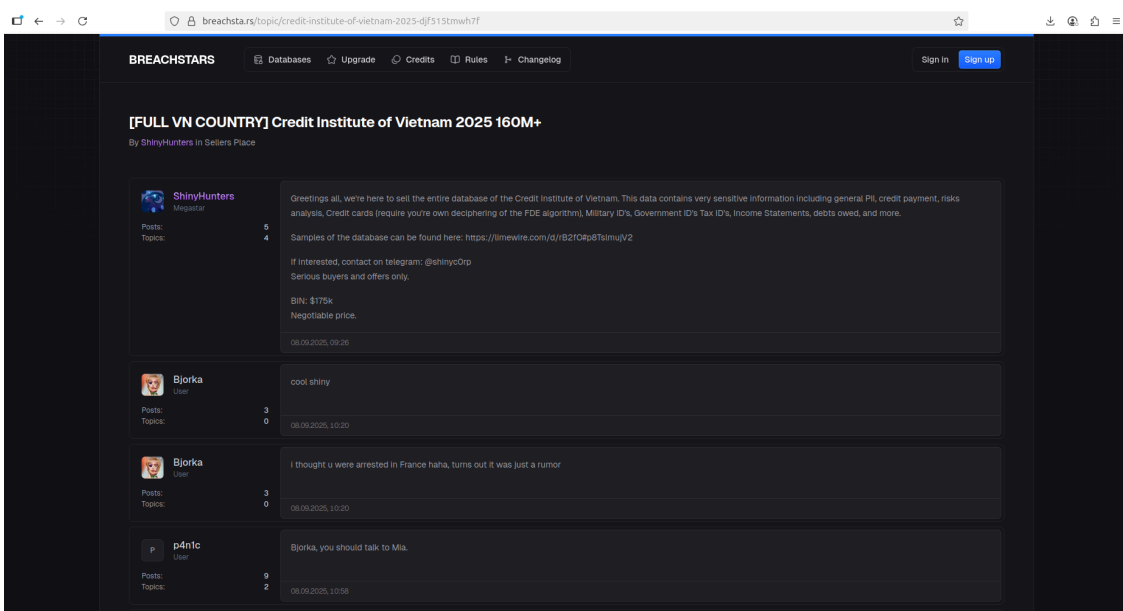
The actors shared several samples of stolen data without providing exact timestamps or sources. As [suggested](#) by independent cybersecurity experts, the data could be stolen at a different time and reused as a result of the

previous successful breach.

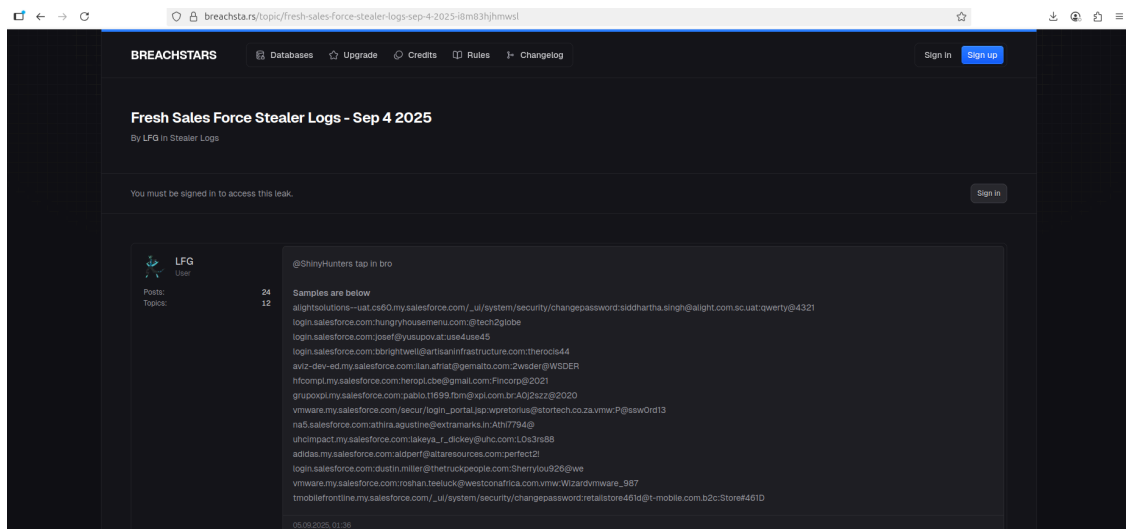




A registered account named "**ShinyHunters**" was identified there. However, it remains uncertain whether this account belongs to the actual threat actors or if someone is reusing their "brand." In one of the latest posts, threat actors claimed to have [exfiltrated over 160 million records](#) from the National Credit Information Center (CIC) of Vietnam. Resecurity covered these events in a separate [threat intelligence report](#). This is a staggering number, considering Vietnam's population is under 102 million, which suggests that the dataset includes historical records and possibly multiple entries per individual.



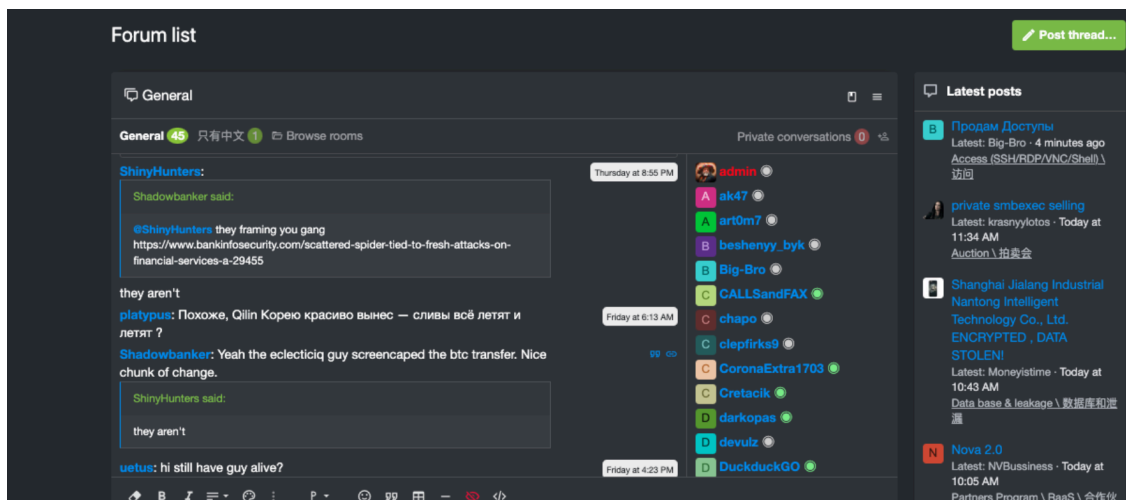
Notably, other actors on the forum are offering stolen access credentials to Salesforce, which will serve as one of the main catalysts for further successful cyberattacks.



Time to Say Goodbye?

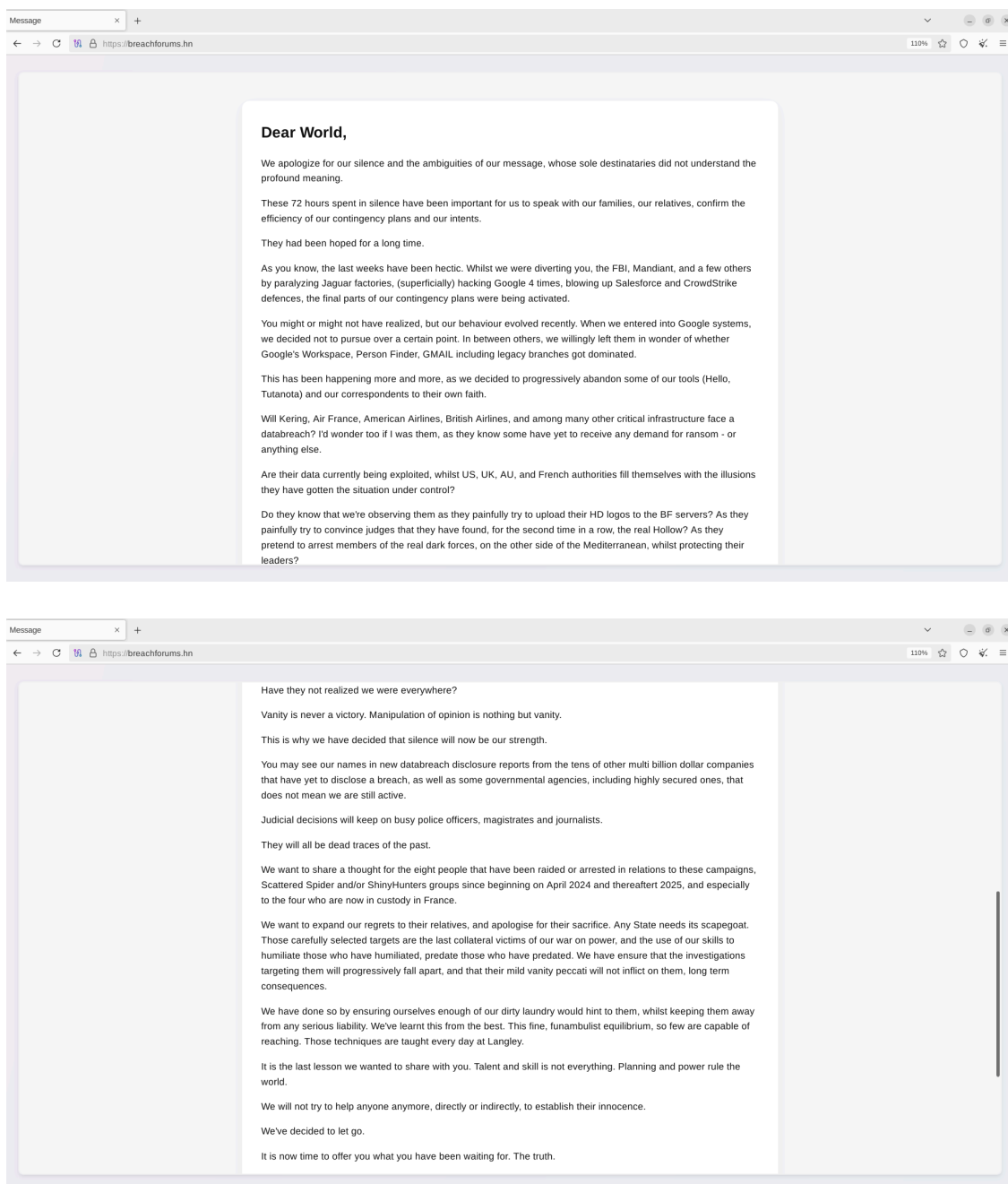
Law enforcement and cybersecurity agencies have begun to mention **LAPSUS\$**, **ShinyHunters**, and **Scattered Spider** together in briefings and advisories, reflecting the growing perception of overlap and possible joint operations among these groups. The groups' ability to rapidly adapt and escalate their attacks has made them a top concern for both private sector security teams and law enforcement. The boundaries between **LAPSUS\$**, **Scattered Spider**, and **ShinyHunters** have become increasingly fluid, with evidence of both operational overlap and tactical convergence. These groups now represent a loosely connected, highly adaptive cybercrime ecosystem, posing an advanced persistent threat (APT) to large enterprises worldwide.

According to recent reports, the trio announced that they were retiring and ceasing their activities. The groups stated they had "achieved their goals of exposing weaknesses in digital security". Already, these claims have proven to be nothing more than performative trolling. On September 18, just days after the gang posted their retirement announcement, a RAMP forum account credibly believed to be operated by the **ShinyHunters** leader claimed credit for a new campaign targeting the financial services sector in the forum chat.

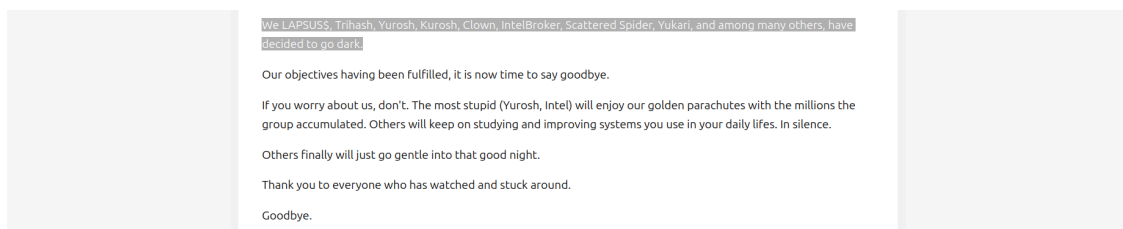


Resecurity believes that these groups will continue their malicious activities using different names or reorganize like **Conti** rather than truly disbanding. Additionally, the groups themselves hinted that future data breach disclosures involving their names do not necessarily mean they are still active, suggesting some ambiguity in their retirement.

The text of the "goodbye letter" was published on breachforums[.]hn, a domain registered by the actors a few days before the announcement:



This is also the first time the hacking "trio" has mentioned the specific team members involved in their activities:



The cached copy of their announcement is [available](#) via Wayback Machine.

Significance

In closing, Resecurity has identified new, previously undisclosed attacks carried out by this Trinity of Chaos, along with reports of new victims receiving extortion emails. This development underscores the urgent need to accelerate defensive measures and improve employee awareness of such threat actors and their TTPs.

While there is a concern about other actors impersonating the group to carry out malicious activities, the new attributable operations still pose a significant threat to organizations worldwide. Prompt action and heightened vigilance are essential to mitigate potential damages from these emerging threats.

References

This report would not be possible without the hard work of many cybersecurity industry professionals. In this section, Resecurity shares a list of publications providing additional insights into the malicious cyber activities conducted by these groups.

- Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion

<https://www.ic3.gov/CSA/2025/250912.pdf>

- Scattered Spider - Cybersecurity Advisory

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>

- Jaguar Land Rover Breached by HELLCAT Ransomware Group Using Its Infostealer Playbook—Then a Second Hacker Strikes

<https://www.infostealers.com/article/jaguar-land-rover-breached-by-hellcat-ransomware-using-its-info...>

- Jaguar Land Rover admits hackers may have taken data

<https://www.bbc.com/news/articles/cp8wk7rdz8yo>

- Cyber Monitoring Centre Statement on Ransomware Incidents in the Retail Sector

<https://cybermonitoringcentre.com/2025/06/20/cyber-monitoring-centre-statement-on-ransomware-inciden...>

Source: <https://www.resecurity.com/blog/article/trinity-of-chaos-the-lapsus-shinyhunters-and-scattered-spider-alliance-embarks-on-global-cybercrime-spree>