FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

12 September 2025

FLASH Number

FLASH-20250912-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:CLEAR**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

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

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate Indicators of Compromise (IOCs) associated with recent malicious cyber activities by cyber criminal groups UNC6040 and UNC6395, responsible for a rising number of data theft and extortion intrusions. Both groups have recently been observed targeting organizations' Salesforce platforms via different initial access mechanisms. The FBI is releasing this information to maximize awareness and provide IOCs that may be used by recipients for research and network defense.

Technical Details

Initial Access

UNC6040

Since October 2024, UNC6040 threat actors have obtained initial access by leveraging social engineering attacks, in particular voice phishing (vishing), to gain access to organizations' Salesforce accounts. To do so, UNC6040 threat actors commonly call victims' call centers posing as IT support employees addressing enterprise-wide connectivity issues. Under the guise of closing an auto-generated ticket, UNC6040 actors trick customer support employees into taking actions that grant the attackers access or lead to the sharing of employee credentials, allowing them access to targeted companies' Salesforce instances to exfiltrate customer data.

UNC6040 threat actors have utilized phishing panels, directing victims to visit from their mobile phones or work computers during the social engineering calls. After obtaining access, UNC6040 threat actors have then used API queries to exfiltrate large volumes of data in bulk.

UNC6040 threat actors have also directly requested user credentials and multifactor authentication codes to authenticate and add the Salesforce Data Loader application, facilitating data exfiltration.

Salesforce allows organizations to integrate with third-party applications, often called connected apps, using OAuth tokens for authentication after approved by an administrator or sufficiently privileged user. UNC6040 threat actors have deceived victims into authorizing malicious connected apps to their organization's Salesforce portal. This application is often a modified version of Salesforce's Data Loader. During a vishing call, the actor guides the victim to visit Salesforce's connected app setup page, i.e., https://login.salesforce[.]com/setup/connect, to approve the UNC6040 malicious app. This grants UNC6040 threat actors significant capabilities to access, query, and exfiltrate sensitive information directly from the compromised Salesforce customer environments. Authorizing a malicious connected app bypasses many traditional defenses such as MFA, password resets and login monitoring, and because OAuth tokens are issued by Salesforce itself, activity coming from the malicious app can look like it's from a trusted integration.

UNC6040 threat actors have created malicious applications within Salesforce trial accounts, allowing the threat actors the ability to register the connected apps without using a legitimate corporate account, making detection difficult.

Some UNC6040 victims have subsequently received extortion emails allegedly from the ShinyHunters group, demanding payment in cryptocurrency to avoid publication of exfiltrated data. These extortion demands have varied in time following UNC6040 threat actors' access and data exfiltration, ranging from a period of days to months.

UNC6395

The FBI is also warning the public about another widespread data theft campaign targeting Salesforce platforms, designated UNC6395, utilizing a different initial access mechanism than UNC6040. In August of 2025, UNC6395 threat actors exploited compromised OAuth tokens for the Salesloft Drift application, an AI chatbot that can be integrated with Salesforce. Using the

compromised OAuth tokens and third-party app integration, UNC6395 threat actors were able to compromise victims' Salesforce instances and exfiltrate data.

On August 20, 2025, Salesloft, in collaboration with Salesforce, revoked all active access and refresh tokens with the Drift application, terminating any threat actor access to victims' Salesforce platforms from the previously connected Salesloft app.

Indicators

Disclaimer: The FBI recommends organizations investigate and vet indicators prior to taking action, such as blocking.

UNC6040 IOCs:

IP Addresses:			
13.67.175.79	20.190.130.40	20.190.151.38	20.190.157.160
20.190.157.98	23.145.40.165	23.145.40.167	23.145.40.99
23.162.8.66	23.234.69.167	23.94.126.63	31.58.169.85
31.58.169.92	31.58.169.96	34.86.51.128	35.186.181.1
37.19.200.132	37.19.200.141	37.19.200.154	37.19.200.167
37.19.221.179	38.22.104.226	45.83.220.206	51.89.240.10
64.95.11.225	64.95.84.159	66.63.167.122	67.217.228.216
68.235.43.202	68.235.46.22	68.235.46.202	68.235.46.151
68.235.46.208	68.63.167.122	69.246.124.204	72.5.42.72
79.127.217.44	83.147.52.41	87.120.112.134	94.156.167.237
96.44.189.109	96.44.191.141	96.44.191.157	104.223.118.62
104.193.135.221	141.98.252.189	146.70.165.47	146.70.168.239
146.70.173.60	146.70.185.47	146.70.189.47	146.70.189.111
146.70.198.112	146.70.211.55	146.70.211.119	146.70.211.183
147.161.173.90	149.22.81.201	151.242.41.182	151.242.58.76
163.5.149.152	185.141.119.136	185.141.119.138	185.141.119.151
185.141.119.166	185.141.119.168	185.141.119.181	185.141.119.184
185.141.119.185	185.209.199.56	191.96.207.201	198.44.129.56
198.44.129.88	195.54.130.100	196.251.83.162	198.244.224.200
198.54.130.100	198.54.130.108	198.54.133.123	205.234.181.14
206.217.206.14	206.217.206.25	206.217.206.26	206.217.206.64
206.217.206.84	206.217.206.104	206.217.206.124	208.131.130.53
208.131.130.71	208.131.130.91	31.58.169.96	64.94.84.78
64.95.11.225	163.5.149.152	192.198.82.235	

URLs/Links:
Login[.]salesforce[.]com/setup/connect?user_code=aKYF7V5N
Login.salesforce.com/setup/connect?user_code=8KCQGTVU
https://help[victim][.]com
https://login[.]salesforce[.]com/setup/connect
http://64.95.11[.]112/hello.php
91.199.42.164/login

UNC6395 IOCs:

IP Addresses:			
208.68.36.90	44.215.108.109	154.41.95.2	176.65.149.100
179.43.159.198	185.130.47.58	185.207.107.130	185.220.101.133
185.220.101.143	185.220.101.164	185.220.101.167	185.220.101.169
185.220.101.180	185.220.101.185	185.220.101.33	192.42.116.179
192.42.116.20	194.15.36.117	195.47.238.178	195.47.238.83

User-Agent Strings:
Salesforce-Multi-Org-Fetcher/1.0
Salesforce-CLI/1.0
python-requests/2.32.4
Python/3.11 aiohttp/3.12.15

Recommended Mitigations:

The FBI recommends network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by cyber criminals:

Preparing for Cyber Incidents:

- **Train call center employees** to recognize and report phishing attempts.
- **Require phishing-resistant multi-factor authentication (MFA)** for as many services as possible.
- **Implement authentication, authorization, and accounting (AAA) systems** to limit actions users can perform. Apply the Principle of Least Privilege to user accounts and groups, allowing only the performance of authorized actions.
- **Enforce IP-based access restrictions and monitor and detect API usage,** looking for unusual or malicious behavior.

- **Monitor network logs and browser session activity** for anomalous activity, to include indicators of data exfiltration.
- **Review all third-party integrations connecting to third-party software instances.** For each application, rotate API keys, credentials, and/or authentication tokens.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to the FBI Internet Crime Complaint Center at www.ic3.gov or their local FBI field office at www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324). When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

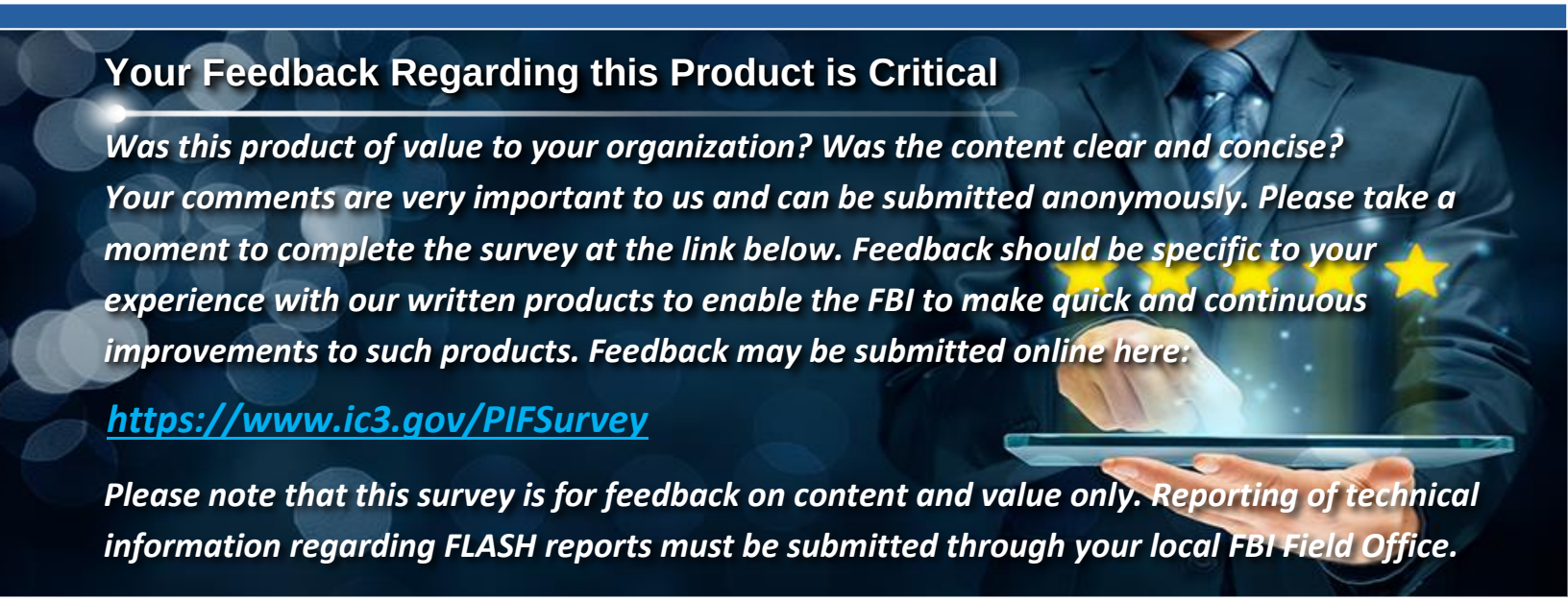
With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Your organization has no obligation to respond or provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided "as is" for informational purposes only. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI.

This product is marked **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.



Your Feedback Regarding this Product is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through your local FBI Field Office.