SEPTEMBER 2025

SECURITY BYTES

Data Theft and Extortion: Rising Threats to Cloud Platforms

The growing reliance on cloud-based platforms has created new opportunities for cybercriminals to steal sensitive data and pressure organizations into paying extortion demands. Recent activity reported by the FBI highlights how two threat actor groups—UNC6040 and UNC6395—are exploiting Salesforce environments to compromise data and launch extortion campaigns.

Tactics and Techniques

UNC6040: Social Engineering and Malicious Apps

Since late 2024, UNC6040 actors have used voice phishing (vishing) to impersonate IT support staff and deceive customer service employees. Their tactics include:

- Convincing employees to share login credentials or MFA codes.
- Guiding victims to approve malicious connected apps disguised as Salesforce's Data Loader.
- Exploiting OAuth tokens to exfiltrate data while bypassing traditional defenses such as password resets or MFA.

Once access is established, they issue API queries to steal large amounts of customer data. Victims often later receive extortion emails, sometimes attributed to the ShinyHunters group, threatening public release of the stolen data unless cryptocurrency payments are made.

UNC6395: Exploiting OAuth Tokens

In mid-2025, UNC6395 launched a separate campaign leveraging compromised OAuth tokens from the Salesloft Drift application, an AI chatbot that integrates with Salesforce. Using these tokens, the group infiltrated Salesforce environments and siphoned data. Salesforce and Salesloft responded by revoking all active Drift tokens, cutting off this attack vector.

Impact of Data Theft and Extortion

The consequences of these attacks extend beyond data loss:

- Operational disruption as organizations scramble to investigate breaches.
- Financial losses from potential ransom payments, incident response, and remediation.
- Reputational damage due to leaked customer or business data.
- Regulatory and legal exposure, especially for companies handling sensitive personal or financial information.

Recommended Mitigations

To counter these evolving threats, the FBI advises organizations to strengthen defenses and resilience:

- Employee training: Equip call center and support staff to recognize social engineering attempts.
- Phishing-resistant MFA: Deploy FIDO2/WebAuthn or hardware tokens where possible.
- Principle of Least Privilege: Limit what actions users and apps can perform.
- Monitor integrations: Regularly review and rotate API keys, OAuth tokens, and third-party app connections.
- Network monitoring: Track anomalous logins, API queries, and data exfiltration attempts.
- Incident reporting: Quickly report suspicious activity to the FBI's Internet Crime Complaint Center (IC3) at ic3.gov.

Data theft and extortion campaigns targeting Salesforce and other cloud platforms illustrate the increasing sophistication of cybercriminal groups. By combining social engineering, OAuth abuse, and extortion tactics, attackers are exploiting trust in cloud ecosystems. Proactive defense—through training, strong authentication, continuous monitoring, and rapid reporting—remains the best safeguard against these persistent threats.

Security News

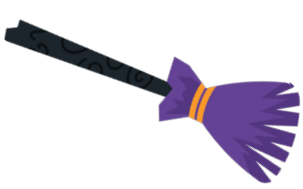
5 trends reshaping IT security today

From market and financial pressures to the rise of AI, CISOs are getting agile with their security outlooks and roadmaps to contend with and keep in front of accelerating risks and disruptions.
Source: CSO

LastPass warns of fake repositories infecting macOS with Atomic Infostealer

LastPass is warning of an ongoing, widespread information stealer campaign targeting Apple macOS users through fake GitHub repositories that distribute malware-laced programs masquerading as legitimate tools.

Source: The Hacker News



Scattered Spider tied to fresh Attacks on financial services

Elements of a notorious cybercrime and ransomware group mashup appear to be carrying on, despite retirement claims.

Source: Bank Info Security

AI-powered phishing scams now use fake captcha pages to evade detection

In an attempt to evade security tools, cybercriminals are now leveraging AI to craft sophisticated phishing campaigns using fake captcha pages.

Source: CSO

2 Clinics notify 700,000 patients of alleged BianLian hacks

Now-Dormant Gang claimed North Carolina, Florida groups on data leak site this year.

Source: Bank Info Security

Hackers steal SonicWall firewall configurations

Hackers accessed backup firewall preference files.

Source: Bank Info Security

European airports continue to crawl after a cyberattack on Collins' MUSE systems

The MUSE software outage has disrupted check-ins and boarding at major European airports, forcing flight cancellations, long queues, and a temporary return to manual operations.

Source: CSO

Microsoft patches critical Entra ID flaw enabling global admin impersonation across tenants

A critical token validation failure in Microsoft Entra ID (previously Azure Active Directory) could have allowed attackers to impersonate any user, including Global Administrators, across any tenant.

Source: The Hacker News

2025 National Insider Threat Awareness Month

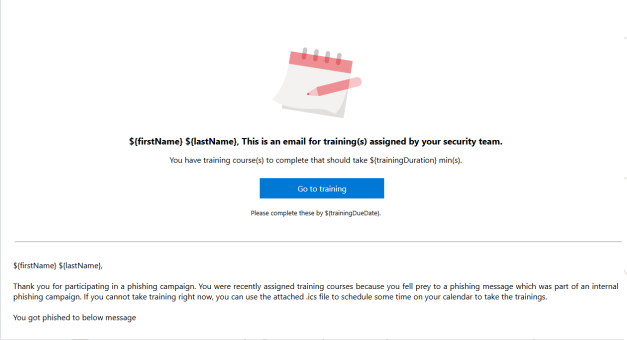
This September, Treasury joins federal partners in recognizing National Insider Threat Awareness Month (NITAM). Protecting our people and information is essential to safeguarding the nation's economic security. This year's theme is Partnering for Progress. Here's what you can do to make Treasury's network, data, and people more secure:

- **Stay Observant:** Insider threats often show warning signs such as unusual information access, unreported foreign travel, compliance issues, sudden affluence, irregular technical activity, or signs of stress and addictive behaviors. If a colleague engages in behaviors that are out of character or concerning, remain alert.
- **Report Concerns Early:** Reporting is not about turning people in—it's about getting them help and protecting the Department. A single behavior may not be significant, but patterns of concerning behavior should be reported to the Insider Risk Management Office (IRMO) at Treasury_ITP@treasury.gov or 202-622-1000, or through the SENTRY portal. Reports can be made anonymously, though providing your name allows IRMO to follow up more effectively. Your identity will remain confidential, except when disclosure is legally required.
- **Understand Your Responsibilities:** Creating a positive culture of security is everyone's responsibility. Please complete the required Treasury Insider Threat Awareness training on your ITM learning platform this month, if you have not already done so this year.

STAY SAFE OUT THERE!

Special Note: Microsoft Defender

For those that have fallen prey to our phish simulation, you will be assigned training that will be due within 30 days. This training is meant to show you tips and tricks on catching future phishing emails.



This email will come from:

Security and Compliance Team <notification@attacksimulationtraining.com>

This is an official email with assigned training!

22ND ANNUAL CYBERSECURITY AWARENESS MONTH OCTOBER 2025

Editorial Information

The Fiscal Service Security Bytes is published bimonthly by Information Security Services, Bureau of the Fiscal Service, Washington, DC 20227.

Editorial Team: David Ambrose, Michael Merrill, Darius Hall, Casey Corbett, Ronald Hall, Douglas Windsor, Patricia Cochran.

Creative Team: Graphics and Printing section, Centralized Services Branch, Administrative and Facilities Services Division.

Contact: David.Ambrose@fiscal.treasury.gov

For feedback, comments, or other suggestions, email them to:

IT Security Training@fiscal.treasury.gov

For this and previous security newsletters, visit our Awareness & Training SharePoint site. Also visit our Cybersecurity Resources page.