Google: Hackers target Salesforce accounts in data extortion attacks

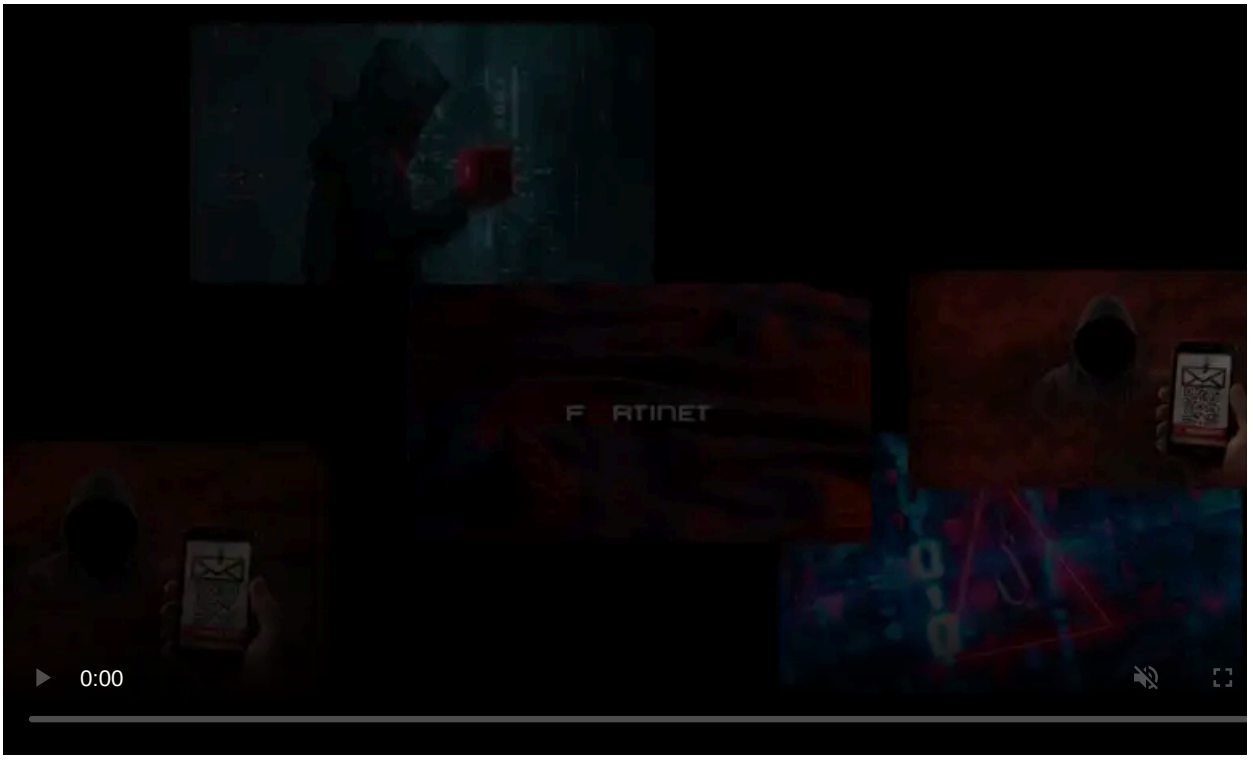
By Bill Toulas

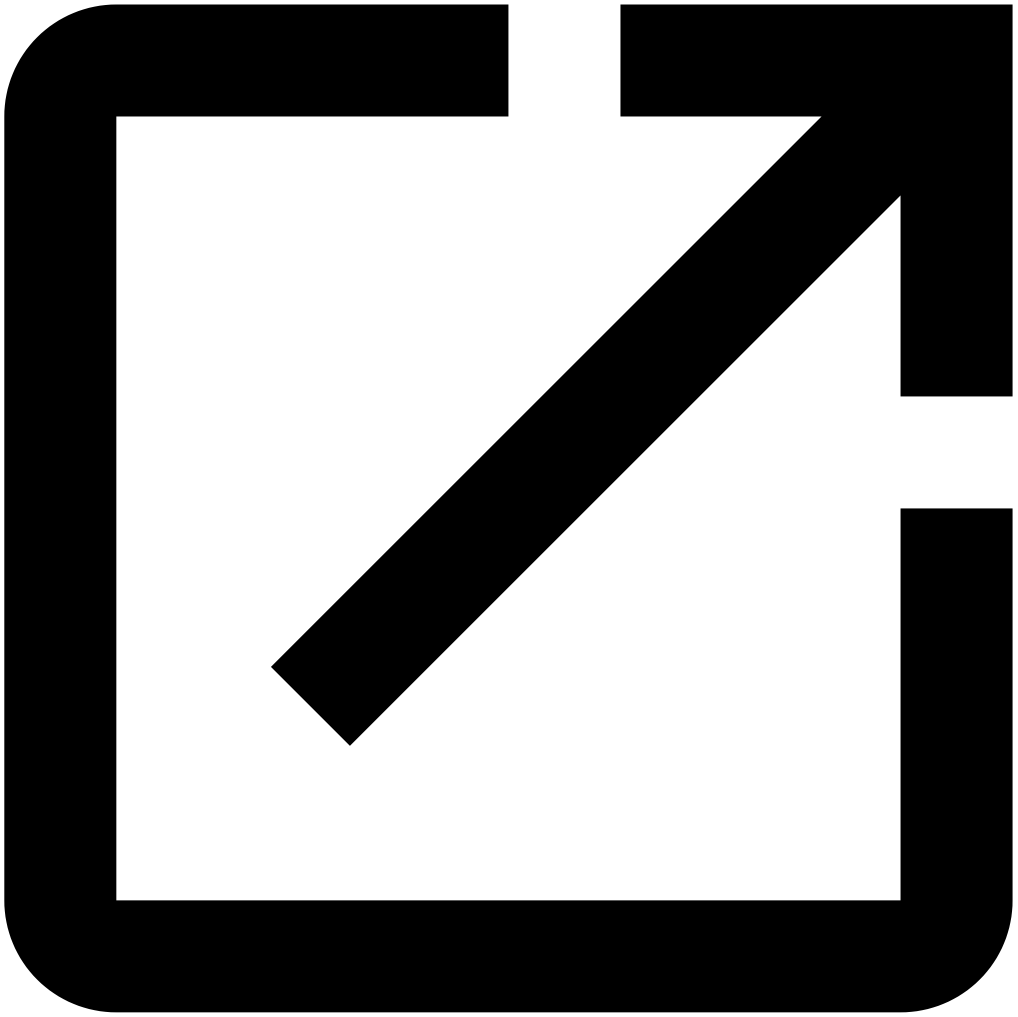
Published: 2025-06-04 · Archived: 2026-04-06 03:23:09 UTC

Google has observed hackers claiming to be the ShinyHunters extortion group conducting social engineering attacks against multi-national companies to steal data from organizations' Salesforce platforms.

According to Google's Threat Intelligence Group (GTIG), which tracks the threat cluster as 'UNC6040,' the attacks target English-speaking employees with voice phishing attacks to trick them into connecting a modified version of Salesforce's Data Loader application.

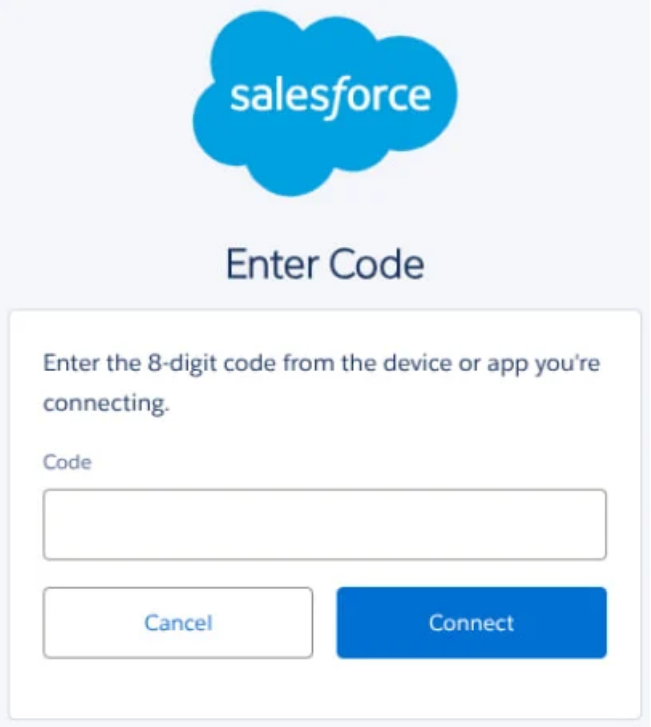
The attackers impersonate IT support personnel, requesting the target employee to accept a connection to Salesforce Data Loader, a client application that allows users to import, export, update, or delete data within Salesforce environments.


F RTINET
0:00



"The application supports OAuth and allows for direct "app" integration via the "connected apps" functionality in Salesforce," explains the researchers.

"Threat actors abuse this by persuading a victim over the phone to open the Salesforce connect setup page and enter a "connection code," thereby linking the actor-controlled Data Loader to the victim's environment.



Prompt to enter connection code
Source: Google

The target organizations already use the Salesforce cloud-based customer relationship management (CRM) platform, so the malicious request to install the tool appears legitimate within the attack's workflow.

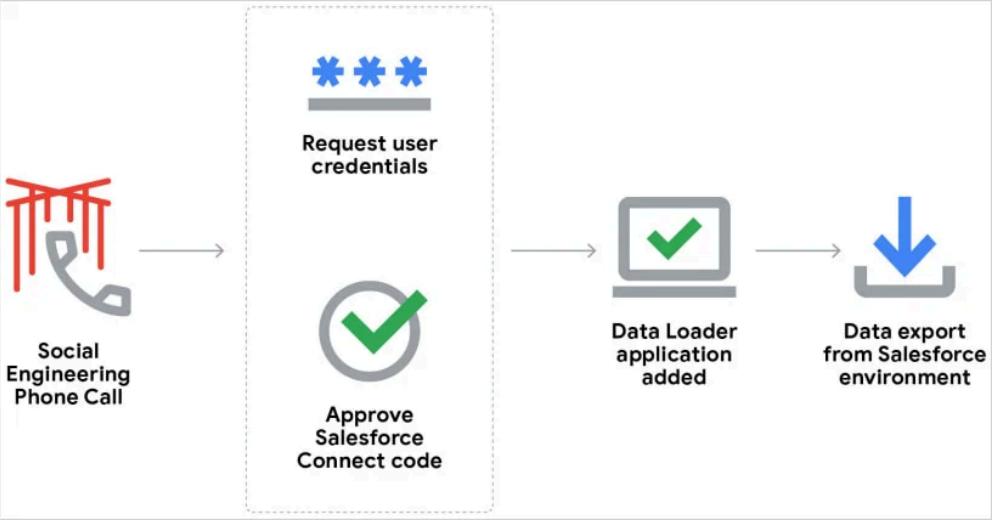
In the UNC6040 attacks, the app is used to export data stored in Salesforce instances and then use the access to move laterally through connected platforms such as Okta, Microsoft 365, and Workplace.

Accessing these additional cloud platforms allows the threat actors to access more sensitive information stored on those platforms, including sensitive communications, authorization tokens, documents, and more.

"UNC6040 is a financially motivated threat cluster that accesses victim networks by voice phishing social engineering," describes the GTIG report.

"Upon obtaining access, UNC6040 has been observed immediately exfiltrating data from the victim's Salesforce environment using Salesforce's Data Loader application."

"Following this initial data theft, UNC6040 was observed moving laterally through the victim's network, accessing and exfiltrating data from other platforms such as Okta, Workplace, and Microsoft 365."



Overview of the UNC6040 attack

Source: Google

In some cases, the data exfiltration process was stopped prematurely, as protection systems that detected unauthorized activity intervened to revoke access. The threat actors appeared to be aware of this risk, experimenting with various packet sizes before escalating their attack.

UNC6040 also used modified versions of the Salesforce Data Loader appropriately named to fit the social engineering context. For example, renaming it to "My Ticket Portal" and tricking victims into installing the app on their systems during an alleged support phone call.

GTIG reports the threat actors use Mullvad VPN IPs when exfiltrating the Salesforce data to obfuscate the activity.

Google says that attacks used phishing pages impersonating Okta, linking them to threat actors associated with the "The Com" or Scattered Spider tactics.

For organizations using Salesforce, Google recommends restricting "API Enabled" permissions, limiting app installation authorization, and blocking access from commercial VPNs like Mullvad.

More information on protecting Salesforce from social engineering attacks is available here.

After publishing our story, Salesforce confirmed to BleepingComputer that accounts are not breached through a vulnerability attack but rather via social engineering attacks.

"Salesforce has enterprise-grade security built into every part of our platform, and there’s no indication the issue described stems from any vulnerability inherent to our services," Salesforce told BleepingComputer

"Attacks like voice phishing are targeted social engineering scams designed to exploit gaps in individual users’ cybersecurity awareness and best practices.

"Security is a shared responsibility, and we provide customers with tools, guidance, and security features like Multi-Factor Authentication and IP restrictions to help defend against evolving threats. For full details, please see our blog on how customers can protect their Salesforce environments from social engineering: https://www.salesforce.com/blog/protect-against-social-engineering/."

Hackers claim to be part of ShinyHunters

In the attacks observed by Google, the threat actors will eventually attempt to extort the company into paying a ransom not to leak the data. Google says these extortion demands can come months later, claiming to be from the infamous ShinyHunters extortion group.

"In some instances, extortion activities haven't been observed until several months after the initial UNC6040 intrusion activity, which could suggest that UNC6040 has partnered with a second threat actor that monetizes access to the stolen

data," explains Google.

"During these extortion attempts, the actor has claimed affiliation with the well-known hacking group ShinyHunters, likely as a method to increase pressure on their victims."

ShinyHunters is a well-known hacking group that has long been associated with data theft attacks that extort companies into paying a ransom.

Threat actors associated with the group have been behind numerous high-profile attacks, including the SnowFlake data theft attacks and the PowerSchool data breach that impacted 62 million students.

Source: https://www.bleepingcomputer.com/news/security/google-hackers-target-salesforce-accounts-in-data-extortion-attacks/