The Cost of a Call: From Voice Phishing to Data Extortion

By Google Threat Intelligence Group

Published: 2025-06-04 · Archived: 2026-04-05 13:57:49 UTC

Update (August 8): Google has completed its email notifications to those affected by this incident.

Update (August 8): Emails are actively being sent to those affected by this incident. Another update will be posted here once these alerts have been issued.

Update (August 5)

In June, one of Google's corporate Salesforce instances was impacted by similar UNC6040 activity described in this post. Google responded to the activity, performed an impact analysis and began mitigations. The instance was used to store contact information and related notes for small and medium businesses. Analysis revealed that data was retrieved by the threat actor during a small window of time before the access was cut off. The data retrieved by the threat actor was confined to basic and largely publicly available business information, such as business names and contact details.

UNC6240

Google Threat Intelligence Group (GTIG) tracks the extortion activities following UNC6040 intrusions, sometimes several months after the initial data theft, as UNC6240. The extortion involves calls or emails to employees of the victim organization demanding payment in bitcoin within 72 hours. During these communications, UNC6240 has consistently claimed to be the threat group ShinyHunters.

In addition, we believe threat actors using the 'ShinyHunters' brand may be preparing to escalate their extortion tactics by launching a data leak site (DLS). These new tactics are likely intended to increase pressure on victims, including those associated with the recent UNC6040 Salesforce-related data breaches. We continue to monitor this actor and will provide updates as appropriate.

UNC6240 Extortion Email Sender Addresses

- `shinycorp@tuta[.]com`
- `shinygroup@tuta[.]com`

UNC6040 (Evolving TTPs)

GTIG has observed an evolution in UNC6040's TTPs. While the group initially relied on the Salesforce Dataloader application, they have since shifted to using custom applications. These custom applications are typically Python scripts that perform a similar function to the Dataloader app. The updated attack chain involves a voice call to enroll a victim, which the threat actor initiates while using Mullvad VPN IPs or TOR. Following this initial engagement, the data collection is automated and through TOR IPs, a change that further complicates

attribution and tracking efforts. GTIG observed that the threat actor shifted from creating Salesforce trial accounts using webmail emails to using compromised accounts from unrelated organizations to initially register their malicious applications.

A Google Threat Intelligence (GTI) collection of related Indicators of Compromise (IOCs) is available.

Introduction

Google Threat Intelligence Group (GTIG) is tracking UNC6040, a financially motivated threat cluster that specializes in voice phishing (vishing) campaigns specifically designed to compromise organizations' Salesforce instances for large-scale data theft and subsequent extortion. Over the past several months, UNC6040 has demonstrated repeated success in breaching networks by having its operators impersonate IT support personnel in convincing telephone-based social engineering engagements. This approach has proven particularly effective in tricking employees, often within English-speaking branches of multinational corporations, into actions that grant the attackers access or lead to the sharing of sensitive credentials, ultimately facilitating the theft of organization’s Salesforce data. In all observed cases, attackers relied on manipulating end users, not exploiting any vulnerability inherent to Salesforce.

A prevalent tactic in UNC6040's operations involves deceiving victims into authorizing a malicious connected app to their organization's Salesforce portal. This application is often a modified version of Salesforce’s Data Loader, not authorized by Salesforce. During a vishing call, the actor guides the victim to visit Salesforce's connected app setup page to approve a version of the Data Loader app with a name or branding that differs from the legitimate version. This step inadvertently grants UNC6040 significant capabilities to access, query, and exfiltrate sensitive information directly from the compromised Salesforce customer environments. This methodology of abusing Data Loader functionalities via malicious connected apps is consistent with recent observations detailed by Salesforce in their guidance on protecting Salesforce environments from such threats.

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. 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.

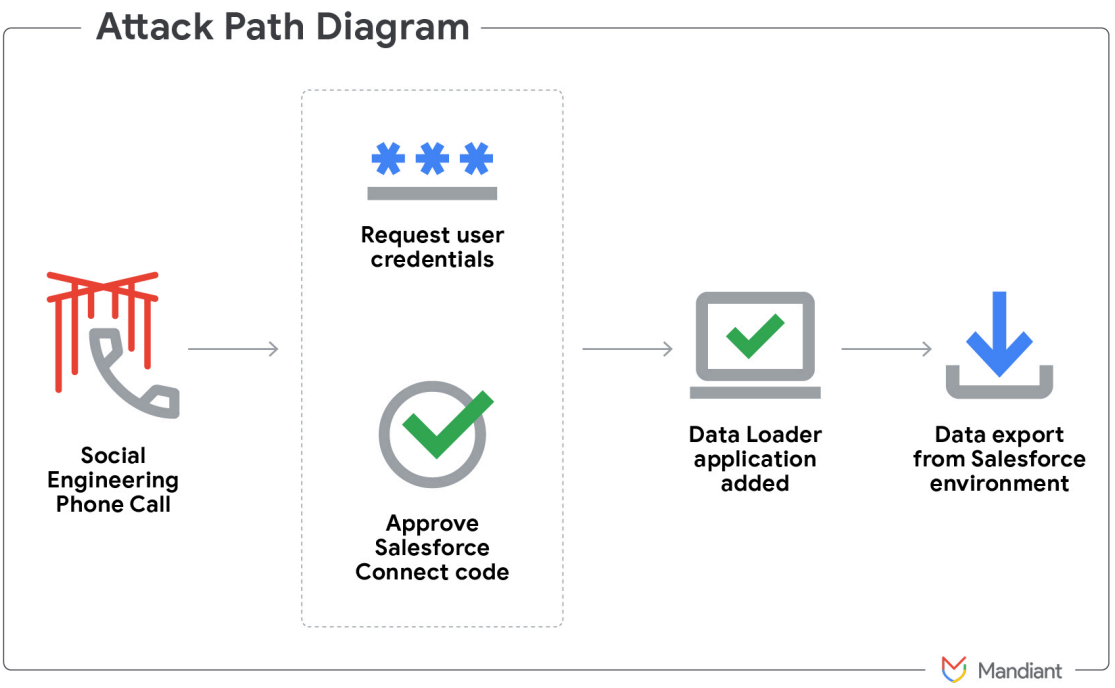

Figure 1: Data Loader attack flow

UNC6040

GTIG is currently tracking a significant portion of the investigated activity as UNC6040. UNC6040 is a financially motivated threat cluster that accesses victim networks by voice phishing social engineering. 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 leveraging end-user credentials obtained through credential harvesting or vishing to move laterally through victim networks, accessing and exfiltrating data from the victim's accounts on other cloud platforms such as Okta and Microsoft 365.

Attacker Infrastructure

UNC6040 utilized infrastructure to access Salesforce applications that also hosted an Okta phishing panel. This panel was used to trick victims into visiting it from their mobile phones or work computers during the social engineering calls. In these interactions, UNC6040 also directly requested user credentials and multifactor authentication codes to authenticate and add the Salesforce Data Loader application, facilitating data exfiltration.

Alongside the phishing infrastructure, UNC6040 primarily used Mullvad VPN IP addresses to access and perform the data exfiltration on the victim's Salesforce environments and other services of the victim's network.

Overlap with Groups Linked to "The Com"

GTIG has observed infrastructure across various intrusions that shares characteristics with elements previously linked to UNC6040 and threat groups suspected of ties to the broader, loosely organized collective known as "The Com". We've also observed overlapping tactics, techniques, and procedures (TTPs), including social engineering

via IT support, the targeting of Okta credentials, and an initial focus on English-speaking users at multinational companies. It's plausible that these similarities stem from associated actors operating within the same communities, rather than indicating a direct operational relationship between the threat actors.

Data Loader

Data Loader is an application developed by Salesforce, designed for the efficient import, export, and update of large data volumes within the Salesforce platform. It offers both a user interface and a command-line component, the latter providing extensive customization and automation capabilities. The application supports OAuth and allows for direct "app" integration via the "connected apps" functionality in Salesforce. 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.

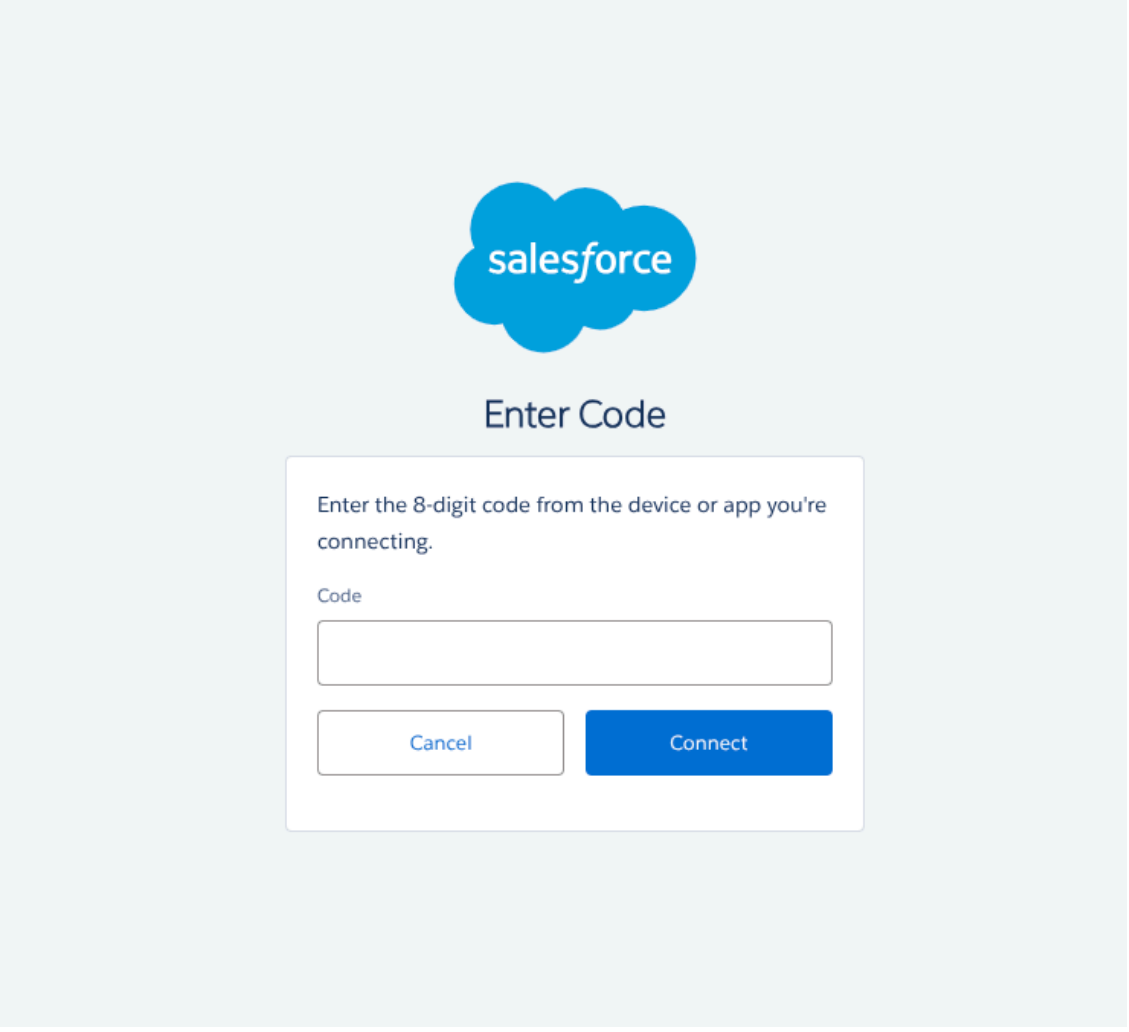

Figure 2: The victim needs to enter a code to connect the threat actor controlled Data Loader

Modifications

In some of the intrusions using Data Loader, threat actors utilized modified versions of Data Loader to exfiltrate Salesforce data from victim organizations. The proficiency with the tool and capabilities by executed queries seems to differ from one intrusion to another.

In one instance, a threat actor used small chunk sizes for data exfiltration from Salesforce but was only able to retrieve approximately 10% of the data before detection and access revocation. In another case, numerous test queries were made with small chunk sizes initially. Once sufficient information was gathered, the actor rapidly increased the exfiltration volume to extract entire tables.

There were also cases where the threat actors configured their Data Loader application with the name "My Ticket Portal", aligning the tool's appearance with the social engineering pretext used during the vishing calls.

Outlook & Implications

Voice phishing (vishing) as a social engineering method is not, in itself, a novel or innovative technique; it has been widely adopted by numerous financially motivated threat groups over recent years with varied results. However, this campaign by UNC6040 is particularly notable due to its focus on exfiltrating data specifically from Salesforce environments. Furthermore, this activity underscores a broader and concerning trend: threat actors are increasingly targeting IT support personnel as a primary vector for gaining initial access, exploiting their roles to compromise valuable enterprise data.

The success of campaigns like UNC6040's, leveraging these refined vishing tactics, demonstrates that this approach remains an effective threat vector for financially motivated groups seeking to breach organizational defenses.

Given the extended time frame between initial compromise and extortion, it is possible that multiple victim organizations and potentially downstream victims could face extortion demands in the coming weeks or months.

Readiness, Mitigations, and Hardening

This campaign underscores the importance of a shared responsibility model for cloud security. While platforms like Salesforce provide robust, enterprise-grade security controls, it’s essential for customers to configure and manage access, permissions, and user training according to best practices.

To defend against social engineering threats, particularly those abusing tools like Data Loader for data exfiltration, organizations should implement a defense-in-depth strategy. GTIG recommends the following key mitigations and hardening steps:

- **Adhere to the Principle of Least Privilege, Especially for Data Access Tools:** Grant users only the permissions essential for their roles—no more, no less. Specifically for tools like Data Loader, which often require the "API Enabled" permission for full functionality, limit its assignment strictly. This permission allows broad data export capabilities; therefore, its assignment must be carefully controlled. Per Salesforce's guidance, review and configure Data Loader access to restrict the number of users who can perform mass data operations, and regularly audit profiles and permission sets to ensure appropriate access levels.

- **Manage Access to Connected Applications Rigorously:** Control how external applications, including Data Loader, interact with your Salesforce environment. Diligently manage access to your connected apps, specifying which users, profiles, or permission sets can use them and from where. Critically, restrict powerful permissions such as "Customize Application" and "Manage Connected Apps"—which allow

users to authorize or install new connected applications—only to essential and trusted administrative personnel. Consider developing a process to review and approve connected apps, potentially allowlisting known safe applications to prevent the unauthorized introduction of malicious ones, such as modified Data Loader instances.

- **Enforce IP-Based Access Restrictions:** To counter unauthorized access attempts, including those from threat actors using commercial VPNs, implement IP address restrictions. Set login ranges and trusted IPs, thereby restricting access to your defined enterprise and VPN networks. Define permitted IP ranges for user profiles and, where applicable, for connected app policies to ensure that logins and app authorizations from unexpected or non-trusted IP addresses are denied or appropriately challenged.
- **Leverage Advanced Security Monitoring and Policy Enforcement with Salesforce Shield:** For enhanced alerting, visibility, and automated response capabilities, utilize tools within Salesforce Shield. Transaction Security Policies allow you to monitor activities like large data downloads (a common sign of Data Loader abuse) and automatically trigger alerts or block these actions. Complement this with "Event Monitoring" to gain deep visibility into user behavior, data access patterns (e.g., who viewed what data and when), API usage, and other critical activities, helping to detect anomalies indicative of compromise. These logs can also be ingested into your internal security tools for broader analysis.
- **Enforce Multi-Factor Authentication (MFA) Universally:** While the social engineering tactics described may involve tricking users into satisfying an MFA prompt (e.g., for authorizing a malicious connected app), MFA remains a foundational security control. Salesforce states that "MFA is an essential, effective tool to enhance protection against unauthorized account access" and requires it for direct logins. Ensure MFA is robustly implemented across your organization and that users are educated on MFA fatigue tactics and social engineering attempts designed to circumvent this critical protection.

By implementing these measures, organizations can significantly strengthen their security posture against the types of vishing and the UNC6040 data exfiltration campaign detailed in this report. Regularly review Salesforce’s security documentation, including the Salesforce Security Guide for additional detailed guidance.

Read our vishing technical analysis for more details on the vishing threat, and strategic recommendations and best practices to stay ahead of it.

Posted in

- Threat Intelligence

Source: https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion