Salesforce Data Exfiltration, Campaign C0059

Archived: 2026-04-05 17:06:49 UTC

Enterprise T1020 Automated Exfiltration

During Salesforce Data Exfiltration, threat actors used API queries to automatically exfiltrate large volumes of data.[1]

Enterprise T1671 Cloud Application Integration

During Salesforce Data Exfiltration, threat actors deceived victims into authorizing malicious connected apps to their organization's Salesforce portal.[1][2]

Enterprise T1059 .006 Command and Scripting Interpreter: Python

During Salesforce Data Exfiltration, threat actors used custom applications developed in python.[2]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

During Salesforce Data Exfiltration, threat actors used compromised emails to create Salesforce trial accounts.[2]

Enterprise T1213 .004 Data from Information Repositories: Customer Relationship Management Software

During Salesforce Data Exfiltration, threat actors accessed and exfiltrated sensitive information from compromised Salesforce instances.[2]

Enterprise T1587 .001 Develop Capabilities: Malware

During Salesforce Data Exfiltration, threat actors created malicious applications within Salesforce trial accounts, typically Python scripts with similar function to the Salesforce Data Loader.[1][2]

Enterprise T1585 Establish Accounts

During Salesforce Data Exfiltration, threat actors created Salesforce trial accounts to register their malicious applications.[2]

.002 Email Accounts

During Salesforce Data Exfiltration, threat actors registered emails shinycorp@tuta[.]com and shinygroup@tuta[.]com to send victims extortion demands.[2]

Enterprise T1567 Exfiltration Over Web Service

During Salesforce Data Exfiltration, threat actors exfiltrated data via legitimate Salesforce API communication channels including the Salesforce Data Loader application.[2][1]

Enterprise T1083 File and Directory Discovery

During Salesforce Data Exfiltration, threat actors queried customers' Salesforce environments to identify sensitive information for exfiltration.[1]

Enterprise T1656 Impersonation

During Salesforce Data Exfiltration, threat actors impersonated IT support personnel in voice calls with victims at times claiming to be addressing enterprise-wide connectivity issues.[2][1]

Enterprise T1036 Masquerading

During Salesforce Data Exfiltration, threat actors used voice calls to socially engineer victims into authorizing a modified version of the Salesforce Data Loader app.[2]

Enterprise T1588 .002 Obtain Capabilities: Tool

During Salesforce Data Exfiltration, threat actors initially relied on the legitimate Salesforce Data Loader app for data exfiltration.[2][1]

Enterprise T1598 .004 Phishing for Information: Spearphishing Voice

During Salesforce Data Exfiltration, threat actors initiated voice calls with victims to socially engineer them into authorizing malicious applications or divulging sensitive credentials.[1][2]

Enterprise T1090 Proxy

During Salesforce Data Exfiltration, threat actors used Mullvad VPN IPs to proxy voice phishing calls.[2]

.003 Multi-hop Proxy

During Salesforce Data Exfiltration, threat actors used Tor IPs for voice calls and for the collection of stolen data.[2]

Enterprise T1608 .005 Stage Capabilities: Link Target

During Salesforce Data Exfiltration, threat actors established an Okta phishing panel which victims were tricked into accessing from mobile phones or work computers during social engineering calls.[1][2]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

During Salesforce Data Exfiltration, threat actors used compromised credentials for lateral movement.[1][2]
