ET CISO.in
From The Economic Times

Seqrite reveals critical insights into Google salesforce breach by UNC6040 threat group

Seqrite uncovered a vishing-extortion campaign by UNC6040 (linked to ShinyHunters) that breached Google's Salesforce, exposing SMB client data. The attackers used social engineering, OAuth abuse, and anonymization to gain access and exfiltrate data. This campaign affected major global brands and is linked to "The Com," a cybercriminal collective involved in various illicit activities.

Seqrite, the enterprise arm of Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has unveiled comprehensive insights into the sophisticated vishing-extortion campaign that compromised Google's corporate Salesforce instance in June 2025, exposing small and medium-sized business client data to cybercriminals. The attack was orchestrated by the threat group UNC6040 (linked to ShinyHunters), showing an alarming evolution in social engineering tactics that successfully bypassed Google's security measures through a combination of voice phishing, OAuth abuse, and advanced anonymization techniques.

The threat research, conducted by the team at Seqrite Labs, India's largest malware analysis facility, reveals that the breach involved a calculated multi-vector approach where attackers impersonated IT staff through convincing phone calls, persuading a Google employee to approve a malicious application connected to Salesforce. Once inside, criminals deployed custom Python scripts that emulated Salesforce's DataLoader functionality, enabling automated bulk exports of business names, email addresses, phone numbers and related client notes. Throughout the operation, attackers maintained anonymity through Mullvad VPN-initiated calls followed by TOR-based data exfiltration, effectively masking their true location.

Seqrite's investigation reveals this incident as part of a broader campaign affecting major global brands including Adidas, Qantas, Allianz Life, LVMH brands, Chanel, AT&T, Santander, Starbucks Singapore, Cisco, Pandora, and dozens of others. The parallel UNC6395 attack on Salesloft Drift represents one of 2025's most significant cyber incidents, compromising hundreds of Salesforce customers through OAuth token theft that enabled unauthorized SOQL queries across cases, accounts, users and opportunities databases.

The threat attribution analysis connects UNC6040 and UNC6240 to a chaotic cybercriminal collective known as "The Com" - short for "The Community" - comprising over 1,000 members primarily aged 11-25 across Canada, the United States and the United Kingdom. This sociopathic subculture engages in SIM swapping, cryptocurrency theft, swatting, sextortion and even extreme coercion, with members recruited through social media and gaming platforms before being coerced into increasingly serious crimes.

Technical indicators of compromise documented by Seqrite include specific IP addresses, malicious domains like ticket-dior.com and ticket-nike.com, and email addresses used for communications. The research reveals consistent use of TOR exit nodes hosted primarily in Netherlands, Poland and Germany, with attackers blending TOR traffic with legitimate OAuth sessions to obscure their origins and complicate detection efforts.

The investigation by researchers at Seqrite Labs exposes critical vulnerabilities in cloud SaaS environments where even traditionally "low-sensitivity" data can be weaponized for targeted phishing and extortion schemes. Seqrite warns that the ShinyHunters group is hinting at a potential pivot toward ransomware-as-a-service operations branded as "ShinySP1D3R," suggesting the threat

landscape will continue evolving with increasingly sophisticated attack methodologies.

Seqrite Threat Intel platform provides specific detection guidance including monitoring for suspicious LOGIN events from unfamiliar IP ranges, maintaining dynamic OAuth app registries with mandatory admin approval workflows, implementing caller-ID verification systems, and deploying voice analytics modules that detect key phrases associated with social engineering attempts. The company points out that behavioral analytics will become indispensable as attribution difficulty increases due to continued VPN and TOR usage.