

Weekly Intelligence Summary

Report Date: 23.02.2026

Intelligence Cut-off Date: 20.02.2026

Weekly Focus: New ShinyHunters Data Leak Site (DLS) lists major organisations across sectors

Campaigns target financial, technology, retail, education and food services sectors and reportedly originate from the recent Okta SSO credential theft campaign.

In late January 2026, the prolific ransomware collective ShinyHunters, affiliated with Scattered Lapsus Hunters (SLH), resurfaced with a new dark web DLS. A variety of high-profile organisations have been listed, including Canada Goose, Harvard University, Match Group, SoundCloud, Betterment, Crunchbase and Figure Technology Solutions. Most enterprises have confirmed a compromise, although it cannot be definitively linked to ShinyHunters activity.

Data from several of these recent breaches was reportedly exfiltrated via the recently disclosed Okta single-sign-on (SSO) credential theft campaign, which was claimed by ShinyHunters in late January 2026. In this voice phishing (vishing)-based campaign, threat actors posed as IT staff during phone calls to employees and lured them into logging into phishing pages and completing MFA challenges in real time, effectively controlling the authentication flow. Notably, in November 2025, a CrowdStrike employee illicitly shared an internal Okta SSO dashboard used to access corporate applications with SLH, although these two incidents have not been linked.

Why It Matters...

Shiny Hunters and the SLH franchise are known to victimise high-value organisations, typically targeting SaaS and Cloud environments and supply chain compromise for mass data exfiltration. Infection from the collective revolves around sophisticated social engineering and increasingly vishing. The group focuses on credential theft and OAuth token compromise rather than system vulnerabilities, targeting users with privileged access to internal tools and systems to maximise impact.

The group strategically leverages the reputational, operational and potential legal damages experienced by targeted organisations to bolster its own brand as a disruptive and capable extortion group. They reinforce perceptions of operational capability and persistence, effectively strengthening their coercive leverage in future campaigns.

The repeated seizure and reactivation of Shiny Hunters and SLH DLS and operations indicate loose structuring and direction, and operational resilience. Their extortion campaigns remain disruptive and scalable, requiring proper securitisation through the review of SSO and OAuth access, third-party access pathway restrictions and enhanced detection and response of social engineering, particularly vishing techniques.

Intelligence Overview

Data Breaches

The WorldLeaks extortion group has targeted the UK Thames Valley Chamber of Commerce in a breach, which includes data from the Bank of England.

North Korea-linked Lapsus\$ group lists Adidas on Breach Forums, claiming 815,000 records of exfiltrated data.

Vulnerabilities

A critical remote code execution vulnerability in Google Chrome, CVE-2026-2441 (OVSS: 72 | CVSS: 8.8), has been identified as actively exploited and has been added to CISA's

Known	Exploited
-------	-----------

 Vulnerabilities catalogue.

A critical remote code execution vulnerability, tracked as CVE-2025-15556 (OVSS: 74 | CVSS: 7.5), has been identified in Notepad++.

Exploitation was confirmed for a pre-authentication remote code execution (RCE) vulnerability affecting BeyondTrust, tracked as CVE-2026-1731 (CVSS: 9.9 | OVSS: 64), leading to VShell and SparkRAT malware deployment.

Novel Techniques

Researchers observed a new variant of the ClickFix tactic that leverages DNS lookup to deliver ModeloRAT.

Threat actor using the moniker w1kkid claimed the exfiltration of 662,752 Substack account records, including email addresses, phone numbers, Stripe IDs and other metadata. Substack confirmed the intrusion.