

# Weekly Intelligence Summary

Report Date: 01.12.2025

Intelligence Cut-off Date: 28.11.2025

## Weekly Focus: Scattered Lapsus\$ Hunters exploit pre-existing trust boundaries.

**A large cyber security company employee allegedly leaks internal information to Scattered Lapsus\$ Hunters in malicious insider incident, as Zendesk users face social engineering attempts.**

A leading cybersecurity provider has disclosed an insider threat involving a now-terminated employee who allegedly shared internal system information with the Scattered Lapsus\$ Hunters (SLH) threat collective. The insider reportedly shared screenshots of internal dashboards, including an Okta single sign-on (SSO) panel used to access corporate applications. These images were later published on SLH's Telegram channel. Details of the motivation of this insider are not known; however, there are individuals within SLH who are well-resourced, and it is almost certain that they have the means and intent to purchase access to high-value organisations. This comes as researchers identify several typo squat domains registered on infrastructure with very similar attributes to the previous SLH infrastructure, masquerading as Zendesk. It is almost certain that this infrastructure was intended to (or was) utilised in social engineering attempts, seeking to undermine the relationship between users and their help desk.

### Why It Matters...

SLH, and similar actors target the trust boundaries between organisations and their information systems. Compromising legitimate authentication material for pre-trusted SaaS services is an efficient way to extort many different companies, particularly as services are inherently trusted, but also offshored, which can make malign activity difficult to rapidly detect and mitigate. Staff (and insiders - such as helpdesk operators) are also inherently trusted by an organisation and, if compromised or malign, can cause great damage. Orpheus frequently observe insiders' recruitment efforts in deep and dark web forums, by criminals who are adept and well-resourced; however, they are seldom publicly reported on.

The key takeaways organisations should take from these events are:

1. Threat Actors will seek to undermine entities with which there is inherent trust. Whether this is pre-trusted applications or pre-cleared humans.
2. Even with a malicious insider, the threat actors were interested in authentication process for corporate applications. Particularly as we move to cloud (SaaS) infrastructure, identity is the new network perimeter.
3. As long as technology is insufficient to mitigate human-centric threats, actors will continue to utilise social-engineering TTPs.

### Intelligence Overview

#### Vulnerabilities

CISA has added CVE-2025-61757 (OVSS: 90 | CVSS: 9.8), a critical vulnerability in Oracle's Identity Manager, to its list of Known Exploited Vulnerabilities. Although exploitation is confirmed but limited, recent Clop activity indicates broader targeting of Oracle services across enterprises.

#### Novel Techniques

A phishing campaign has been observed in which threat actors are employing a subtle typosquatting technique, replacing the letter 'm' with 'r' and 'n' in the domain rnicrosoft[.]com.

A new ClickFix campaign that conceals malware in PNG images and uses fake Windows Update interfaces to execute attacker-supplied PowerShell commands has been identified.

#### Nation State

A potential collaboration between Russia-aligned and North Korean state-sponsored APT groups has been uncovered, with evidence that the threat actors may be operating on shared infrastructure.

#### Cybercrime

CIoP ransomware added 39 alleged victims to the group's data leak site, including Mazda, Michelin, Grupo Bimbo, and Broadcom.

A threat actor claims to have stolen the complete source code for Mall Logistics, the Android application used by AVM Lojistik to manage deliveries, shipments and wider retail-mall logistics operations.