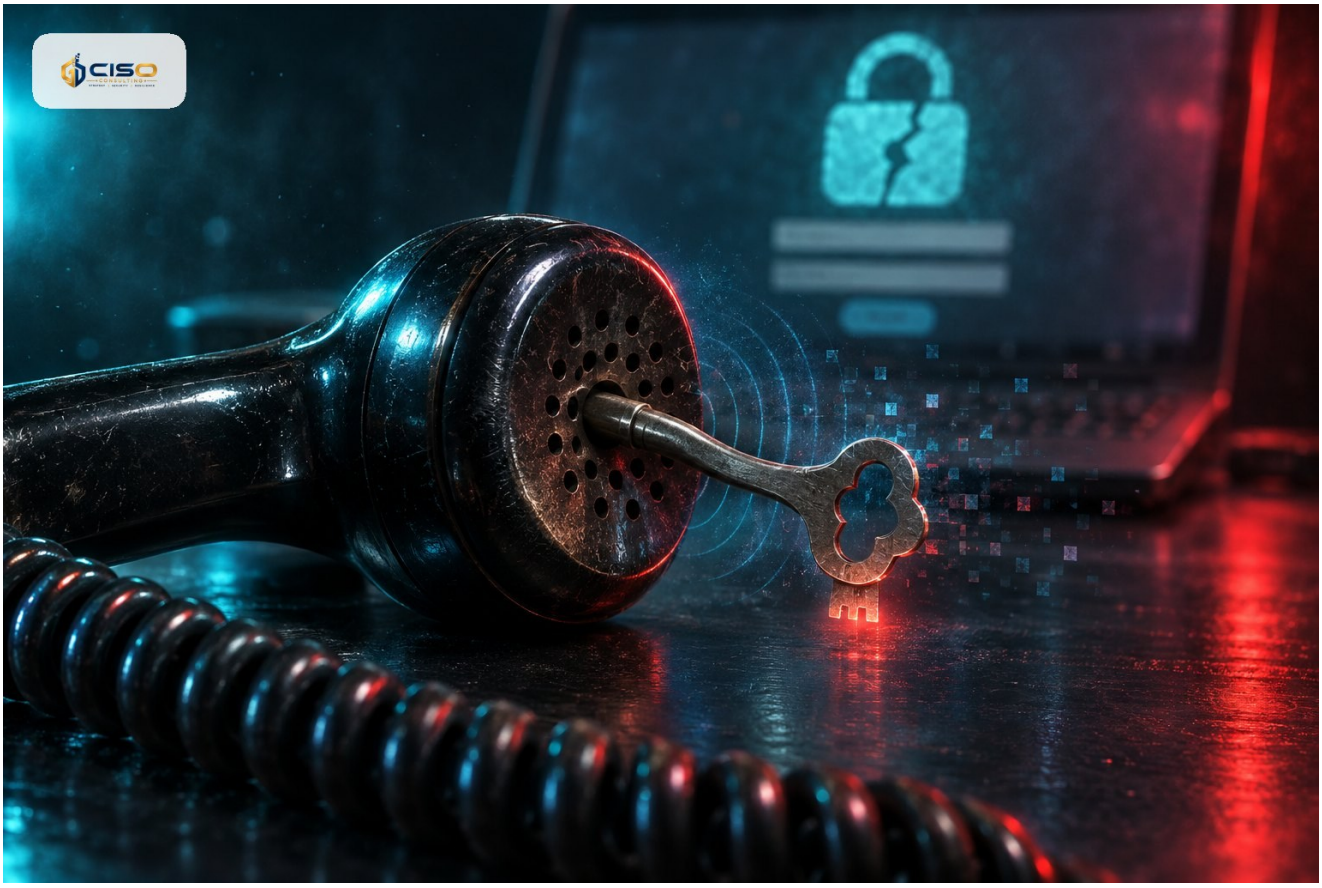
Inception extortion gang runs vishing campaign aimed at SSO credentials



A new extortion group, Inception, is using phone-based social engineering and fake Okta-style login sites to steal SSO credentials. Okta links it to a cluster tied to ShinyHunters; the group denies this.

- Inception appeared on November 17 and listed seven claimed victims; none has publicly confirmed a breach.
- ReversingLabs says activity began in late October and found 21 SSO phishing domains, 41 suspected infrastructure domains and 4 other suspicious ones.
- The campaign relies on phone-based social engineering and legal-themed sites imitating Okta and NetIQ/OpenText Access Manager.
- Okta assesses the cluster O-UNC-053, previously tied to ShinyHunters, has very likely rebranded;

Inception denies any affiliation.

- Recommended defences: phishing-resistant authentication, stronger help desk verification and log review back to October 21, 2026.

A newly formed data extortion group calling itself Inception has been linked to a large-scale campaign aimed at single sign-on (SSO) credentials of companies around the world. The group surfaced on November 17 and named seven alleged victims on its extortion site. None of them has publicly confirmed a breach.

What is known

ReversingLabs, which has tracked the group, says activity started in late October. It confirmed 21 domains used for SSO phishing, 41 believed to support campaign infrastructure and 4 more with suspected use. The infrastructure impersonates dozens of well-known brands, but the existence of these domains does not show that those firms were targeted or breached.

The campaign appears to depend on phone-based social engineering rather than email phishing, closely resembling tactics associated with ShinyHunters. Inception uses legal-themed websites that imitate corporate authentication services, mainly Okta and also NetIQ/OpenText Access Manager.

Attribution is disputed

Okta has linked Inception to O-UNC-053, a cluster it earlier associated with ShinyHunters. Okta says the cluster kept registering phishing domains after law enforcement disrupted ShinyHunters, launched the legal-themed campaign in late October, and that the Inception leak site went live in mid-November. Because infrastructure and techniques stayed consistent, Okta assesses a very likely change of brand.

Inception rejects this. It says it operates independently, that overlapping targets and shared registration and CDN services prove nothing, and that private tooling circulates among independent actors.

Why it matters

SSO credentials open many systems at once, and voice-based pretexting targets staff and help desks rather than mail filters. Institutions using Okta or similar identity providers should treat this as a prompt to review identity controls, whatever the final attribution.

What to do now

1. Enforce phishing-resistant authentication such as FIDO2 security keys or passkeys for SSO, starting with privileged and help desk accounts.
2. Tighten help desk identity verification for password and MFA resets, and require call-back or other independent confirmation.

3. Review DNS, proxy and identity provider logs back to October 21, 2026 for suspicious activity and lookalike login domains.
4. Brief staff and support teams on phone-based pretexting that references login or legal notices.
5. Prepare an incident response path for suspected SSO compromise, including session revocation and regulator notification checks.