Okta links vishing cluster tied to ShinyHunters to new INCEPTION leak site



Okta's threat intelligence team says a vishing cluster linked to ShinyHunters may have rebranded as INCEPTION. The group tricks targets into entering credentials on phishing pages and approving access.

- Okta Threat Intelligence tracks the cluster as O-UNC-053.
- The cluster was previously assessed as affiliated with the ShinyHunters extortion crew.
- It may have rebranded and continued operating under the name INCEPTION.
- Its main technique is voice phishing (vishing) that leads victims to enter credentials on phishing pages and approve access.
- The report links the group to a new data leak site.

Okta's Threat Intelligence team reports that a threat cluster it tracks as O-UNC-053 may have rebranded and continued operating under a new name, INCEPTION. The cluster had earlier been assessed as affiliated with the ShinyHunters extortion crew, and Okta now ties it to a new data leak site.

What is known

The cluster relies on voice phishing, commonly called vishing. Attackers contact targets by phone and persuade them to enter their credentials on phishing pages and to approve access requests. The source excerpt does not give further detail on victims, scale or the data allegedly leaked, so those points should not be assumed.

Why it matters for regulated institutions

This kind of attack targets people and help-desk style processes rather than software flaws, so technical patching does not address it. A rebrand also means indicators and group names may change while the tradecraft stays the same. Teams that track threats by name alone may miss continuity.

Practical next steps

Treat phone-based social engineering as a standing identity risk. Review how staff verify callers, how approvals for sign-in prompts are handled, and whether users know they should never approve a request they did not initiate. Follow Okta's original publication for indicators and updates as they are released.

What to do now

1. Brief staff and help-desk teams on vishing, including callers who push users to enter credentials on a link or approve a prompt.
2. Require call-back verification through a known number before any credential reset or access change requested by phone.
3. Instruct users never to approve MFA or sign-in requests they did not initiate, and to report them at once.
4. Add O-UNC-053 and INCEPTION to threat-intelligence tracking, alongside ShinyHunters, and monitor Okta's publication for indicators.
5. Review identity and SSO logs for unusual sign-in approvals or new device enrolments.