Oktapus Phishing Campaign Targets Okta Identity Credentials

By Alok Patidar

Published: 2022-09-08 · Archived: 2026-04-02 12:07:29 UTC

Introduction

Though we often hear news about cyberattacks or identity thefts, big brands falling victim to these cyberattacks is quite rare.

A similar incident happened recently where cybersecurity researchers revealed the latest phishing campaign that targeted identity and access management giant Okta.

The phishing campaign, Oktapus, targeted many renowned companies that also became victims of various phishing attempts.

As per the experts, the cybercriminals sent text messages to the company's employees with a link to the phishing sites mimicking the Okta authentication page for their website.

Moreover, the report revealed that once the users landed on the phishing page, they were asked for a 2FA code. And once the user entered their credentials to log in, their credentials were forwarded to the malicious actors that started the attack.

Group-IB, the company that conducted the analysis, also confirmed that once the cybercriminals could pivot and launch various attacks, including supply chain attacks. And this was a clear indicator that these attacks were carefully planned and executed.

As per the report, 169 unique domains were identified involved in the Oktapus phishing campaign. And Group-IB analyzed the resources used by fraudsters to create fake websites.

Furthermore, the targetted organization were majorly from the U.S., followed by the U.K. and Canada. Most of them were I.T. companies offering cloud and software development services, and few were dealing with finance-related work.

The incident portrays the importance of proper cybersecurity training for employees and customers since various cybersecurity best practices are useless if the end-user isn’t aware of the risks.

As per Group-IB, the end users, especially with admin rights, must always double-check the URL of a website where they share their login credentials to ensure maximum security. Moreover, the company officials also advised businesses to invoke the true potential of a FIDO2-compliant security key for MFA.

Also, businesses must identify various loopholes that can help cybercriminals to exploit crucial information about customers and companies. Once the loopholes are identified, the best security practices must be implemented soon.

However, brands need to focus on educating their employees, IT staff, and end users to ensure they're well-prepared for any cybersecurity challenge and can quickly identify phishing attempts.

The right combination of cybersecurity best practices and employee/customer awareness works flawlessly in mitigating the risks associated with data breaches and identity thefts.

Looking for an Okta alternative? Learn more about the highest rated, most secure CIAM technology in the world.
