HYPR Info Brief

Securing Okta Better Than Okta

Background

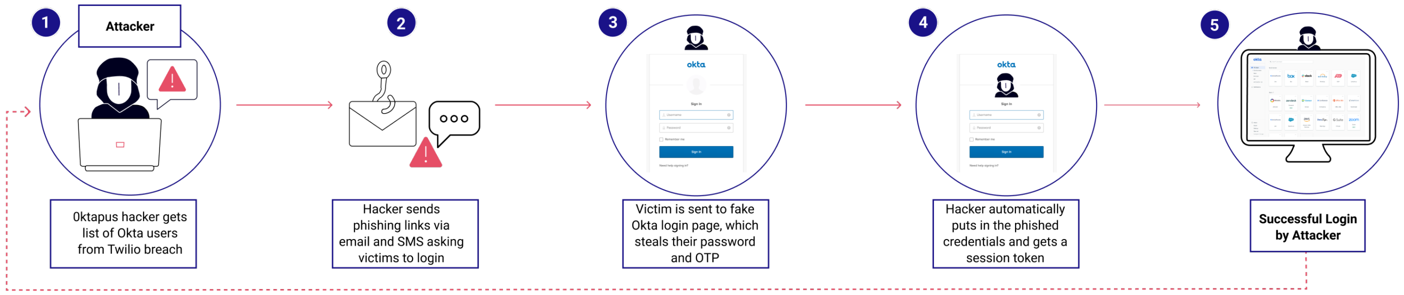
Over the last month through various news outlets, the world has learned that both Twilio and Okta have been hacked. Specifically, the threat actors behind the Twilio hack used their access to steal one-time passwords (OTPs) delivered over SMS from customers of Okta. Okta provides its customers with multiple forms of authentication for services, including temporary codes delivered over SMS through Twilio or via authenticator apps.

Security Impact

To date, this current news event has impacted over 140 companies with more appearing every day. In the following days and weeks, this number will undoubtedly continue to grow. This highly publicized and ongoing incident makes it clear that the authentication methods Okta uses, even their "more secure" MFA, is inherently insecure as it relies on passwords and one-time passwords. Specifically, as an SSO provider that is predicated on tying all accounts to a "single sign-on," Okta-provided authentication places organizations at serious risk, creating a single point of security failure.

The Cyber Killchain

The following represents how the Oktapus Attacks Hacked 10k+ Accounts Across 140+ Organizations.



1 Attacker

Oktapus hacker gets list of Okta users from Twilio breach

2 Hacker sends phishing links via email and SMS asking victims to login

3 Victim is sent to fake Okta login page, which steals their password and OTP

4 Hacker automatically puts in the phished credentials and gets a session token

5 **Successful Login by Attacker**

Recommended Immediate Actions

There are several actions HYPR recommends that organizations immediately execute:

- If the organization currently uses traditional multi-factor authentication (MFA), disable SMS.
- Use phishing resistant MFA. This rules out using Okta Verify, Duo Mobile, Microsoft Authenticator, Google Authenticator, or anything else that relies on OTPs and/or shared secrets.

How to Secure Okta

SSOs Are Based on Passwords

Okta relies on passwords, leaving organizations highly vulnerable. HYPR passwordless MFA eliminates passwords and shared secrets while streamlining the login process. HYPR works in conjunction with SSOs like Okta so your employees gain a consumer-like, frictionless experience and your organization gains the authentication security it needs.

Phishing-Resistant MFA Is Critical

Multi-factor authentication using SMS, OTPs or push notification is easily phished, intercepted and bypassed — allowing attackers to take over employee SSO accounts and gain access to your systems and data. Regulatory agencies and security experts recommend phishing-resistant MFA based on FIDO standards. HYPR's phishing-resistant passwordless authentication prevents MFA bypass and is FIDO Certified across all solution components.

90%
Of MFA solutions are phishable[1]

33%
YOY increase in MFA push attacks[2]

$2.19M
Average cost of an authentication-related breach[3]

Desktop to Cloud Protection

SSOs do not protect the desktop, leaving a critical attack entry point open. Attackers that gain access to the endpoint device can access password managers, browser-stored passwords and other sensitive resources. HYPR provides phishing-resistant, passwordless MFA that begins with initial endpoint login and carries through to Okta and all downstream resources.

Take Action

Please reach out to your direct sales representative or channel partner today.

[1] Roger A. Grimes, Hacking Multifactor Authentication, Wiley, 2021
[2] The State of Passwordless Security 2022, HYPR
[3] The State of Authentication in the Finance Industry 2022, HYPR

THE PASSWORDLESS COMPANY

Phone: 1-866-GET-HYPR [US]
Email: info@hypr.com
Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.