Okta, Lastpass, Cisco, Twilio:

Lessons Learned from Recent Attacks

BEYOND IDENTITY

Eighty-six. That's the number of "significant cyber incidents" Center for Strategic and International Studies (CSIS) lists so far for 2022. And that only includes government agencies, defense and high tech companies, and economic crimes with losses of more than a million dollars. If you count attacks on small businesses, attacks that didn't include major financial losses, and phishing scams, the number skyrockets.

Legacy security solutions are no longer enough. The only way to protect your organization is to update your security processes. That means getting rid of passwords and other phishable vulnerable credentials. It's time to implement zero trust authentication that uses unphishable MFA, device trust, continuous authentication, and eliminates passwords. These recent attacks show how basic MFA and older security procedures aren't enough.

LastPass source code theft

In August, Karim Toubba, the CEO of LastPass, released a statement about a major breach, and it wasn't their first.

Touba stated, "We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information."

What we know:

- Bad actors gained access to the development environment through a developer account.
- LastPass states their development environment is physically separated from their production environment. The attackers had no access to customer information.
- While there is "no evidence that this incident involved any access to customer data or encrypted password vaults," repeated successful attacks show vulnerabilities exist and are being used to infiltrate LastPass' systems.
- LastPass saw "no evidence of attempts of code-poisoning or malicious code injection" during an inspection of their system.

Cisco hacked by ransomware gang

Ransomware attacks also continue to escalate. In May 2022, attackers breached Cisco's network and threatened to leak stolen files online if the company didn't meet their demands.

What we know:

- Access was achieved through an employee's stolen credentials.
- The employee accepted multi-factor authentication (MFA) push notifications after that attacker utilized MFA fatigue and voice phishing attacks.
- The attackers infiltrated the employee's personal Google account, which contained passwords synced from their Chrome browser.
- Once the attackers gained access to the company's network, they moved laterally to attack Citrix servers and domain controllers.

Twilio's employees and customers hacked

In August 2022, attackers accessed Twilio customer accounts using a "sophisticated social engineering attack designed to steal employee credentials." Twilio was also impacted in 2021 by the Codecov supply-chain attack.

What we know:

- The attackers stole multiple employee credentials in an SMS phishing attack.
- Attackers impersonated Twilio's IT department. They told users passwords had expired or were scheduled to be changed.
- The phishing attack asked users to click legitimate looking URLs containing "Twilio," "Okta," and "SSO." The links redirected them to a Twilio sign-in page clone that harvested the user credentials.
- They used the stolen credentials to breach internal systems and access customer data.

0ctopus phishing campaign goes after Okta

Simple phishing schemes can lead to just as much damage as social engineering attacks. Group-IB researchers reported a large-scale supply chain attack, codenamed 0ktapus, that impacted over 130 organizations using simple phishing kits available online.

What we know:

- According to Group-IB, the attackers wanted to "obtain Okta identity credentials and two-factor authentication (2FA) codes from users of the targeted organizations."
- Attackers could then use these Okta credentials to gain access to any enterprise resource available to the user The attackers were able to use "low-skill methods" to compromise well-known organizations.
- The researchers detected 169 unique domains involved in the attack.
- Most of the attacked companies provide IT, software development, and cloud services.

AiTM targeting Google Workspace (G Suite)

Attackers launched a large-scale adversary-in-the-middle (AiTM) attack against Google G Suite users. According to ThreatLabz, "This campaign specifically targeted chief executives and other senior members of various organizations which use G Suite."

What we know:

- The attack bypassed Gmail's MFA.
- The same group launched a similar attack on Microsoft enterprise accounts earlier in the month.
- The attackers used proxy servers set up between the target user and the website the user was trying to visit.
- Using the proxy servers, the attackers captured the target's password and the session cookie.
- Using the captured credentials attackers accessed user mailboxes and used them to launch further attacks.

Uber breach using contractor account

An attacker, likely affiliated with a hacking group called Lapsus$, was able to access Uber's network using a purchased password, social engineering, and notification fatigue. Lapsus$ has used similar techniques to target other technology companies. The same attacker claims to be behind the recent Rockstar Games breach.

What we know:

- An attacker was able to compromise an external contractor's account.
- The attacker may have been able to purchase the account password on the dark web after malware on the contractor's personal device collected the credentials.
- Lapsus$ often purchases session cookies or authentication tokens from those credential marketplaces.
- The attacker repeatedly tried to log into the account, resulting in multiple two-factor login requests.
- Eventually the contractor accepted one of the requests and the attacker gained access.
- The attacker then accessed other employee accounts, gaining permissions to other tools, posted to a company-wide Slack channel, and reconfigured Uber's OpenDNS to display a graphic image on internal sites.

All of these attacks highlight the weakness of password-based MFA and the ease at which hackers can bypass legacy solutions. These attacks will continue to happen as long as these tools are in use. If you'd like to see how Beyond Identity can provide your organization with phishing resistant, zero trust authentication to keep hackers at bay and protect your organization, book a demo today.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.