Microsoft and Okta disclosed breaches this week involving Lapsus$, a cybercrime group that has made headlines multiple times in recent months for attacks against corporations including NVIDIA, Ubisoft, Samsung, and Vodafone. The group specializes in stealing and extorting data in exchange for a ransom payment. Lapsus$ is known to leverage low-tech but high-impact methods to gain access to organizations. Lapsus$ has used tactics such as social engineering, SIM swapping, and paying employees and business partners for access to credentials and multifactor authentication approvals. The first known extortion attempt by Lapsus$ included the Brazil Health Ministry in December of 2021.

What happened in the Okta attack?

According to a blog penned by the Okta CISO, here's what happened:

- On January 20 2022, a third-party customer support engineer working for Okta had their account compromised by Lapsus$.
- Lapsus$ was seeking information on Okta customers, not Okta directly.
- The threat actor compromised information from up to 366 Okta customers. Per Okta, the data that was accessible in this breach was very limited — though it's worth noting that Lapsus$ refuted this statement, claiming the ability to reset passwords and MFA factors.
- Per Okta, the incident was mitigated within hours of the initial compromise and is no longer a security risk.
- On March 22, 2022, Lapsus$ posted screenshots of their compromise to Telegram.

Zscaler's cloud is not at risk:

After a thorough investigation, ThreatLabz determined that Zscaler has not been impacted by the Okta breach. While Zscaler does use Okta internally for employees as an Identity Provider (IDP), all access to our production environments requires multiple additional factors including hardware tokens not provided by Okta. You can read the ThreatLabz trust post here.

Additionally, the Zscaler platform is built on a holistic zero trust architecture that offers defense-in-depth against supply chain and compromised user attacks, mitigating incidents such as this in the following ways:

- Eliminates lateral movement: Zscaler connects users directly to apps, not the network, to limit the blast radius of a potential incident.
- Shuts down compromised users and insider threats: If an attacker gains access to your identity system, we can prevent private app exploit attempts with in-line inspection and detect the most sophisticated attackers with integrated deception.
- Stops data loss: Zscaler inspects data-in-motion and data-at-rest to prevent potential data theft from an active attacker.

ThreatLabz' SOC playbook for Okta:

The Zscaler Security team has developed a Security Operations Center (SOC) playbook for identity (IDP) providers, giving our security analysts and researchers fast track access to threat identification and remediation at the user level. Suspicious behaviors trigger a security action workflow: for example, moving a user to a higher-access security group, changing multi-factor authentication methods, or other anomalous and potentially dangerous user behaviors.

A review of IDP logs for indicators of compromise associated with this attack should include the following steps:

- Review Okta admin/super admin account audit logs.
- Review cloud admin/super admin account audit logs.
- Review all executive accounts including MFA method changes.
- Review new Okta account creations and compare against employee onboarding.
- Review full Okta config to check for API access, logging configs, etc.
- Identify Okta accounts where MFA was disabled from January 1, 2022 to March 22, 2022. Identify the user and root cause of the disablement. Re-enable MFA for those accounts.
- Reset password for Okta admins.
- Reset 2-factor authentication for Okta superadmins.
- Rotate Okta-generated API tokens.
- Verify Okta Support access is disabled.
- Verify Directory Debugger access is disabled.
- Review all critical users' access levels.

SOC Detection Rules for Okta

The process to enable Threat Detection for Okta using a SOC Playbook should be well-defined with specific workflows and actions. Okta has pre-built log ingestion modules for many of the common SIEM solutions. Once events are ingested, a number of queries can be created and easily leveraged for signs of a potential compromise or other suspicious activities. While they are not a comprehensive set of queries, they serve as a solid starting point for a security investigation.

Detection Name	Detection Query
MFA Deactivation Attempt	event.dataset:okta.system and event.action:user.mfa.factor.deactivate
MFA Reset Attempt	event.dataset:okta.system and event.action:user.mfa.factor.reset_all
MFA Push Brute Force Attempt	sequence by user.email with maxspan=10m [any where event.module == "okta" and event.action == "user.mfa.okta_verify.deny_push"] [any where event.module == "okta" and event.action == "user.mfa.okta_verify.deny_push"] [any where event.module == "okta" and event.action == "user.authentication.sso"]
MFA Bypass Attempt	event.dataset:okta.system and event.action:user.mfa.attempt_bypass
Account Login Brute Force Attempt	event.dataset:okta.system and event.action:user.account.lock
User Session Impersonation	event.dataset:okta.system and event.action:user.session.impersonation.initiate
Group Administrative Privilege Assignment	event.dataset:okta.system and event.action:group.privilege.grant
User Administrative Privilege Assignment	event.dataset:okta.system and event.action:user.account.privilege.grant
Policy Rule Modification	event.dataset:okta.system and event.action:policy.rule.update
Policy Rule Deletion	event.dataset:okta.system and event.action:policy.rule.delete
Policy Rule Deactivation	event.dataset:okta.system and event.action:policy.rule.deactivate

Guidance and Best Practices

If you are an Okta customer, we encourage you to take the following steps to protect your business:

- Contact Okta to ensure your organization’s data wasn’t compromised.
- Rotate all credentials and ensure MFA is enabled for all users. Consider MFA methods not facilitated by Okta for critical systems including hardware-based tokens.
- Review logs in your Okta tenant from January to March of 2022 to look for suspicious activity, including password & MFA resets, user account email updates, admin privileges within your IDP tenant, and configuration changes.
- Continually review policies and procedures with any organization involved in your supply chain. Many organizations were potentially impacted by this incident.
- Run security incident preparedness exercises for incidents just like this (a primary Identity Provider compromise) to understand how to respond and what to communicate to whom and when.

Learn more: join a live ThreatLabz briefing on Tuesday, March 22 and 9:30am PT for updated information on the Lapsus$ attack on Okta, a walkthrough of our SOC playbook, and zero trust strategies for preventing and mitigating damage from similar compromises in the future. Register now.

- Security Research
- Insights and Research
-

Authors

Deepen Desai

Dhaval Parekh

Recommended for You

Midas Ransomware : Tracing the Evolution of Thanos Ransomware Variants

Domain Fronting, Abuse and Hiding

Analysis of Adobe Acrobat Pro DC Solid Framework Heap-based Buffer Overflow Vulnerability (CVE-2021-44708)

Speeding Deal Velocity for Healthcare M&A