OKTA Breach

Background

UPDATE: March 23, 2022, 12:30pm EDT
Okta released another update at 11:50am EDT. This update includes a timeline of events highlighting primary milestones of their investigation.

UPDATE: March 23, 2022, 10:00am EDT
Okta released an update Tuesday evening stating that approximately 2.5% of customers were impacted by the breach that occurred in January 2022. Okta has contacted all affected customers by email. The company's service is fully operational. Okta's Chief Security Officer, David Bradbury, wrote, "there are no corrective actions our customers need to take."

March 22, 2022
The Lapsus$ group has released screenshots claiming to be of Okta's internal systems, indicating a potential network breach. The threat group claims to have had admin access to Okta's systems for multiple months. Lapsus$ claimed their focus was on Okta's customers. Okta has over 15,000 customers. Okta has acknowledged this incident, noted that they believe they have remediated the attack in January 2022 and, have not found any evidence of an ongoing attack. They have released an official statement: https://sec.okta.com/articles/2022/03/official-okta-statement-lapsus-claims

Impact

An incident affecting Okta's internal systems has put thousands of businesses on high alert. The impact to individual organizations is currently unknown, however, we suspect Lapsus$ most likely targeted high-profile organizations, Fortune 500.

Recommendations

General MFA Recommendations/Guidance

For any MFA, including Okta, we recommend the following:

- Immediately capture any logs from OKTA that have:
  - User logins
  - User configuration/maintenance of their own MFA accounts (adding devices, removing devices, etc.)
  - Administrator activity (setting up new accounts, adding devices to a user manually, sending MFA codes to a user device, etc.)
- Logging all MFA logs to a SIEM or data lake

Create SIEM detections to help identify unusual or anomalous activity. Note that many organizations utilize MFA differently, so not all rules you may find may be high fidelity or applicable to the way your organization manages MFA. There are a lot of suggestions on the internet for MFA rules, however, to start with, we recommend prioritizing the following:

- An MFA device is being used for more than one account (unnecessary if this control is enforced already)
- A user is presented with a push notification they did not generate (this alert assumes the MFA provider has a means for users to submit "fraudulent" pushes)
- New MFA administrators being created
- MFA device manually being created for an account (depending on how your organization operates, this may not be viable/high fidelity)

The following detection rules have not been tested by SRA, but some of them may be valuable for your organization:

- Detection rules have been made available by Elastic
- SigmaHQ released Sigma rules for OKTA detections

Indicators of Compromise

No IOCs are currently available. We will post an update as soon as any IOCs are known.

References

- https://www.bleepingcomputer.com/news/security/okta-investigating-claims-of-customer-data-breach-from-lapsus-group/
- https://techcrunch.com/2022/03/22/okta-january-hack-breach/
- https://twitter.com/toddmckinnon/status/1506184721922859010
- https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/okta
- https://github.com/elastic/detection-rules/tree/main/rules/integrations/okta

Report Version: v3