1Password

OCTOBER 19, 2023

Security incident report

Last updated October 27th

Executive summary

On September 29, 2023, a member of the IT team received an unexpected email notification suggesting they had initiated an Okta report containing a list of admins.

They recognized that they hadn't initiated the admin report and alerted our security incident response team. Preliminary investigations revealed activity in our Okta environment was sourced by a suspicious IP address and was later confirmed that a threat actor had accessed our Okta tenant with administrative privileges.

Corroborating with Okta support, it was established that this incident shares similarities of a known campaign where threat actors will compromise super admin accounts, then attempt to manipulate authentication flows and establish a secondary identity provider to impersonate users within the affected organization.

Based on our initial assessment, we have no evidence that proves the actor accessed any systems outside of Okta. The activity that we saw suggested they conducted initial reconnaissance with the intent to remain undetected for the purpose of gathering information for a more sophisticated attack.

While immediate measures have mitigated the risks associated with this event, it highlights a number of security improvements we will be prioritizing.

Technical overview

A member of the IT team was engaged with Okta support, and at their request, created a HAR file from the Chrome Dev Tools and uploaded it to the Okta Support Portal.

This HAR file contains a record of all traffic between the browser and the Okta servers, including sensitive information such as session cookies. In the early morning hours of Friday, Sept. 29th, an unknown actor used the same Okta session that was used to create the HAR file to access the Okta administrative portal, and performed the following logged actions:

- Attempted to access the IT team member’s user dashboard, but was blocked by Okta.
- Updated an existing IDP tied to our production Google environment.
- Activated the IDP.
- Requested a report of administrative users.

The final action in that list resulted in an email being sent to the member of the IT team, and alerted them to this event. At this point it is known that the unknown actor performed other less sensitive actions (such as viewing groups) that did not result in log entries; Okta is working to pull log entries for these actions for us to review.

It is not known how the actor gained access to this session, though it has been confirmed that the generated HAR file contained the necessary information for an attacker to hijack the user's session. This was confirmed by IT creating a HAR file, and Security using Burp Suite to force the browser to use the session cookies captured in the HAR file to reproduce the events of the incident.

Based on the activity logs provided by Okta for their Support Portal, the HAR file had not been accessed by their support engineer until after the events of the incident. Security confirmed that the act of downloading the file would be captured in the activity logs by downloading the file from the support case. This eliminated the possibility that the Okta support engineer or administrative user had accessed the file before the incident to perform the events of the incident.

There has been no indication of this actor accessing any other systems, based on the indicators available.

The HAR file was created on the team member’s macOS laptop and uploaded via hotel provided WiFi, as this event occurred at the end of a company event. Based on an analysis of how the file was created and uploaded, Okta’s use of TLS and HSTS, and the prior use of the same browser to access Okta, it is believed that there was no window in which this data could have been exposed to the WiFi network, or otherwise subject to interception.

The IT team member’s macOS laptop that was used is currently offline, and was scanned with the free version of Malwarebytes, which reported no findings. At this point, malware or some other compromise of this device is the leading theory for how this session data was exposed; though this is complicated by the fact that no other unusual activity tied to this team member’s accounts have been identified.

The IT team member's credentials for all systems were rotated, switched to only using a Yubikey for MFA, and additional restrictions have been implemented related to their Okta account.

During the weekend, a number of changes were made to the Okta configuration, including denying logins from non-Okta IDPs, reducing session times for administrative users, tighter rules on MFA for administrative users, and the number of super administrators was reduced. Datadog was updated with additional alerts to reduce the time to detection for such events, as well as alerts related to specific actor indicators. Sessions were cleared, and credentials rotated for Okta administrative users.

In the early morning hours of Monday, Oct. 2nd, the actor returned and attempted to use the Google IDP that they had enabled, though this failed as the IDP had been removed. In both cases, the actor accessed Okta via a server hosted by LeaseWeb in the US, and used a very similar and older version of Chrome (though different operating systems). It is unknown if the actor possesses valid Google account credentials that would have allowed them to complete a login via this IDP.

Addendums

Oct 21, 2023: Okta confirmed publicly that their internal support systems were compromised. This answers how the HAR file was accessed by the attacker and confirms that the initial compromise was not through the employee's laptop.

Oct 25, 2023: During the early phase of our investigation, Okta provided an initial set of logs of access to our IT administrator's HAR file which did not show any unauthorized activity. That led us to focus our investigation on the theory of endpoint malware as indicated in the incident report above.

On October 20th, Okta confirmed an attack on their customer support system and provided 1Password with additional logs. Those logs showed that a compromised service account on Okta's customer support system had indeed accessed the HAR file. This activity was not evident in the initial set of logs given to Okta by the support vendor, and subsequently to 1Password. On further investigation the HAR file existed under two distinct object IDs on the support vendor's system, and the first analysis that was sent to us only covered entries for one of these identifiers. The access timestamps from these additional logs showed that the attacker accessed the HAR file prior to the activity we detected in our Okta instance. This confirmed that the activity stemmed from Okta's security incident.

We would like to reiterate that no 1Password user data or sensitive information was accessed as a result of the attack on Okta's support systems. This activity was confined to our Okta instance and the attacker was not able to create a new Google identity provider or access our Google instance. They modified and re-enabled a connection to our own production Google instance within Okta, which we deleted prior to the attacker's unsuccessful attempt to access it on October 2nd.

October 27, 2023: While Malwarebytes was called out specifically in the Incident Report, it was used as an additional signal within the investigation and does not constitute the entirety of our Endpoint Detection and Response (EDR) strategy.

Our endpoint security strategy is multi-layered, and incorporates various tools, protocols, and best practices. One component of our endpoint security strategy is our mobile device management (MDM) platform, which is used to deploy hardening standards to endpoints. Hardening measures enforced using MDM include, among other things, local disk encryption, user account password requirements, secure configuration of applications, and update enforcement (software and operating system). It also enforces the use of built-in operating system security features.