Okta confirms 2.5% customers impacted by hack in January

By Ionut Ilascu

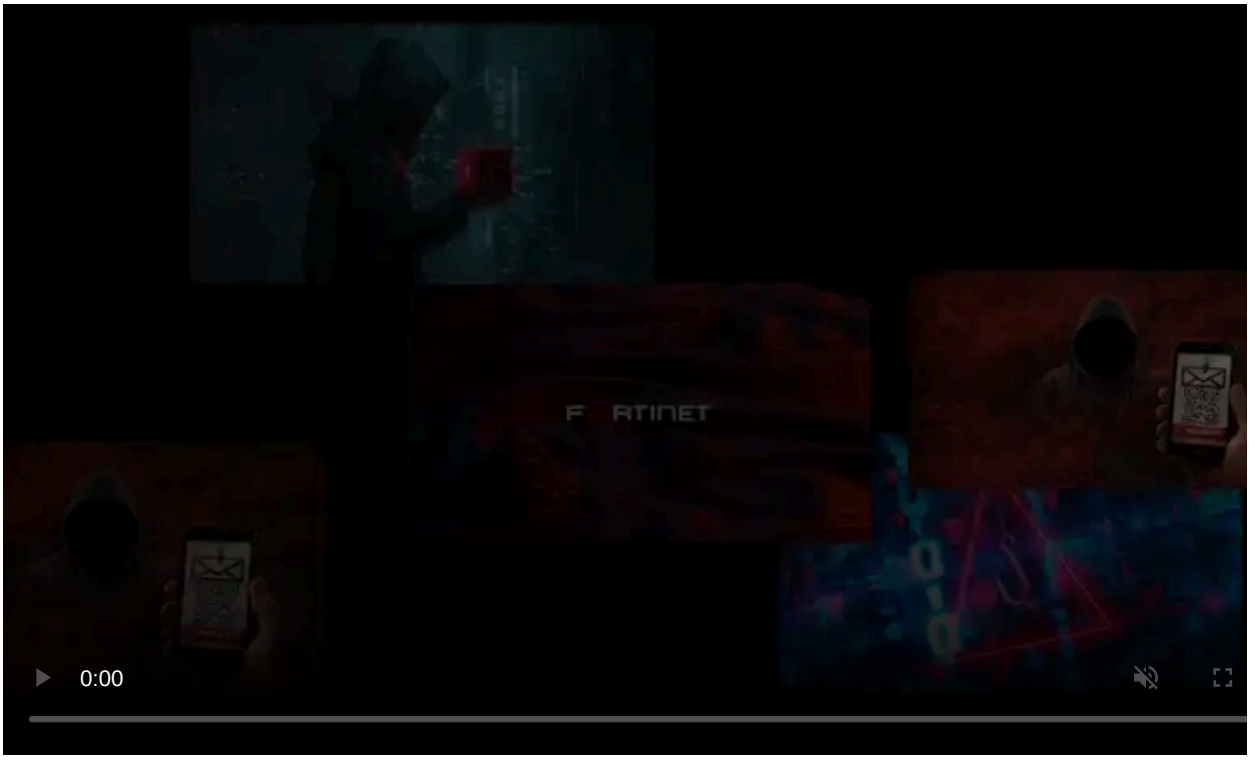
Published: 2022-03-22 · Archived: 2026-04-06 03:11:07 UTC

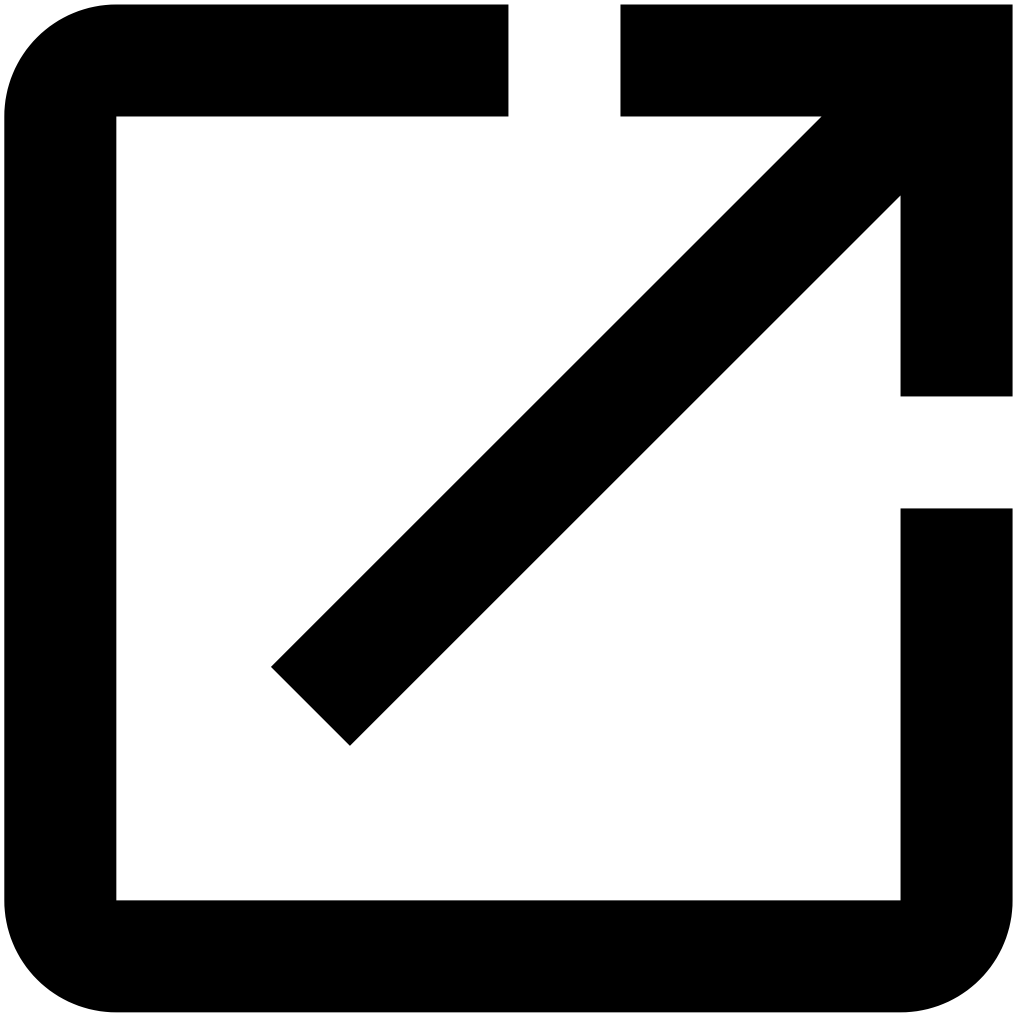
Okta, a major provider of access management systems, says that 2.5%, or approximately 375 customers, were impacted by a cyberattack claimed by the Lapsus$ data extortion group.

The company announced its conclusion today, saying that there are no corrective actions that its customers should take.

Five-day opportunity window

Okta confirmed today they suffered a security incident in January when hackers compromised a laptop of one of its support engineers that could initiate password resets for customers.


F RTINET
0:00



An investigation into the breach showed that the threat actors had access to the laptop for five days, during which they were able to access Okta's customer support panel and the company's Slack server.

“The report highlighted that there was a five-day window of time between January 16-21, 2022, where an attacker had access to a support engineer’s laptop. This is consistent with the screenshots that we became aware of yesterday,” Okta says in an updated statement on the incident.

Screenshots published by the Lapsus$ group show an email address of an Okta employee that appeared to have 'superuser' privileges that allowed them to list users, reset passwords, reset MFA, and access support tickets.

However, the company explains that if successful, such a compromise would be limited to the amount of access that support engineers have, which prevents creating or deleting users, or downloading customer databases.

“Support engineers do have access to limited data - for example, Jira tickets and lists of users - that were seen in the screenshots. Support engineers are also able to facilitate the resetting of passwords and multi-factor authentication [MFA] factors for users, but are unable to obtain those passwords” - Okta

In a later update Tuesday evening, Okta is now stating that approximately 2.5% of its customers were affected by the Lapsus$ cyberattack.

As Okta has over 15,000 customers, this means that approximately 375 organizations may have had accounts that were compromised in some manner.

"We have identified those customers and are contacting them directly. If you are an Okta customer and were impacted, we have already reached out directly by email," explains Okta's Tuesday evening update.

Cloudflare reacts to Okta's breach

In the screenshots from Lapsus$ there is also an email address of a Cloudflare employee whose password was about to be reset by hackers that compromised the account of an Okta employee.

In a report today, web infrastructure and security company Cloudflare revealed that the company email account present in the Lapsus$ screenshots was suspended about 90 minutes after its Security Incident Response Team (SIRT) received the first notification of a potential problem, in the early morning of March 22 (03:30 UTC).

“In a screenshot shared on social media, a Cloudflare employee’s email address was visible, along with a popup indicating the hacker was posing as an Okta employee and could have initiated a password reset” - Cloudflare

Cloudflare notes that Okta services are used internally for employee identity integrated in the authentication stack and that its customers have nothing to worry about, “unless they themselves use Okta.”

To eliminate any chance of unauthorized access to its employee accounts, Cloudflare checked all password resets or modified MFA since December 1, 2021. In total, 144 accounts fit the bill and the company forced a password reset on all of them.

Okta learned of the breach attempt after detecting “an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider.”

The company notified the provider of the issue at the same time terminating the compromised user’s active sessions and suspending their account.

Lapsus$ responds

In response to Okta’s statements today, the Lapsus$ group shared their part of the story saying that they did not compromise an Okta employee’s laptop but their thin client (low-performance system that connects remotely into a virtual environment to carry out tasks).

The hackers dispute Okta's affirmation that the compromise was unsuccessful by claiming that they "logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients."

Lapsus$ is known mostly for leaking proprietary data stolen from big companies like Samsung, NVIDIA, and Mercado Libre. The group has also claims to have breached Microsoft's internal Azure DevOps server and leaked 37 GB of source code allegedly for Bing, Cortana, and other Microsoft projects.

Another breach the group claims is on LG Electronics, bragging that it's the second time in a year they hacked the company's systems.

Source: https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/