Microsoft and Okta Confirm Breach by LAPSUS$ Extortion Group

thehackernews.com/2022/03/microsoft-and-okta-confirm-breach-by.html

March 22, 2022

Microsoft on Tuesday confirmed that the LAPSUS$ extortion-focused hacking crew had gained "limited access" to its systems, as authentication services provider Okta revealed that nearly 2.5% of its customers have been potentially impacted in the wake of the breach.

"No customer code or data was involved in the observed activities," Microsoft's Threat Intelligence Center (MSTIC) said, adding that the breach was facilitated by means of a single compromised account that has since been remediated to prevent further malicious activity.

The Windows maker, which was already tracking the group under the moniker DEV-0537 prior to the public disclosure, said it "does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk."

"This public disclosure escalated our action allowing our team to intervene and interrupt the actor mid-operation, limiting broader impact," the company's security teams noted.

Identity and access management company Okta, which also acknowledged the breach through the account of a customer support engineer working for a third-party provider, said that the attackers had access to the engineer's laptop during a five-day window between January 16 and 21, but that the service itself was not compromised.

The San Francisco-based cloud software firm also said it's identified the affected customers and that it's contacting them directly, stressing that the "Okta service is fully operational, and there are no corrective actions our customers need to take."

"In the case of the Okta compromise, it would not suffice to just change a user's password," web infrastructure company Cloudflare said in a post mortem analysis of the incident. "The attacker would also need to change the hardware (FIDO) token configured for the same user. As a result, it would be easy to spot compromised accounts based on the associated hardware keys."

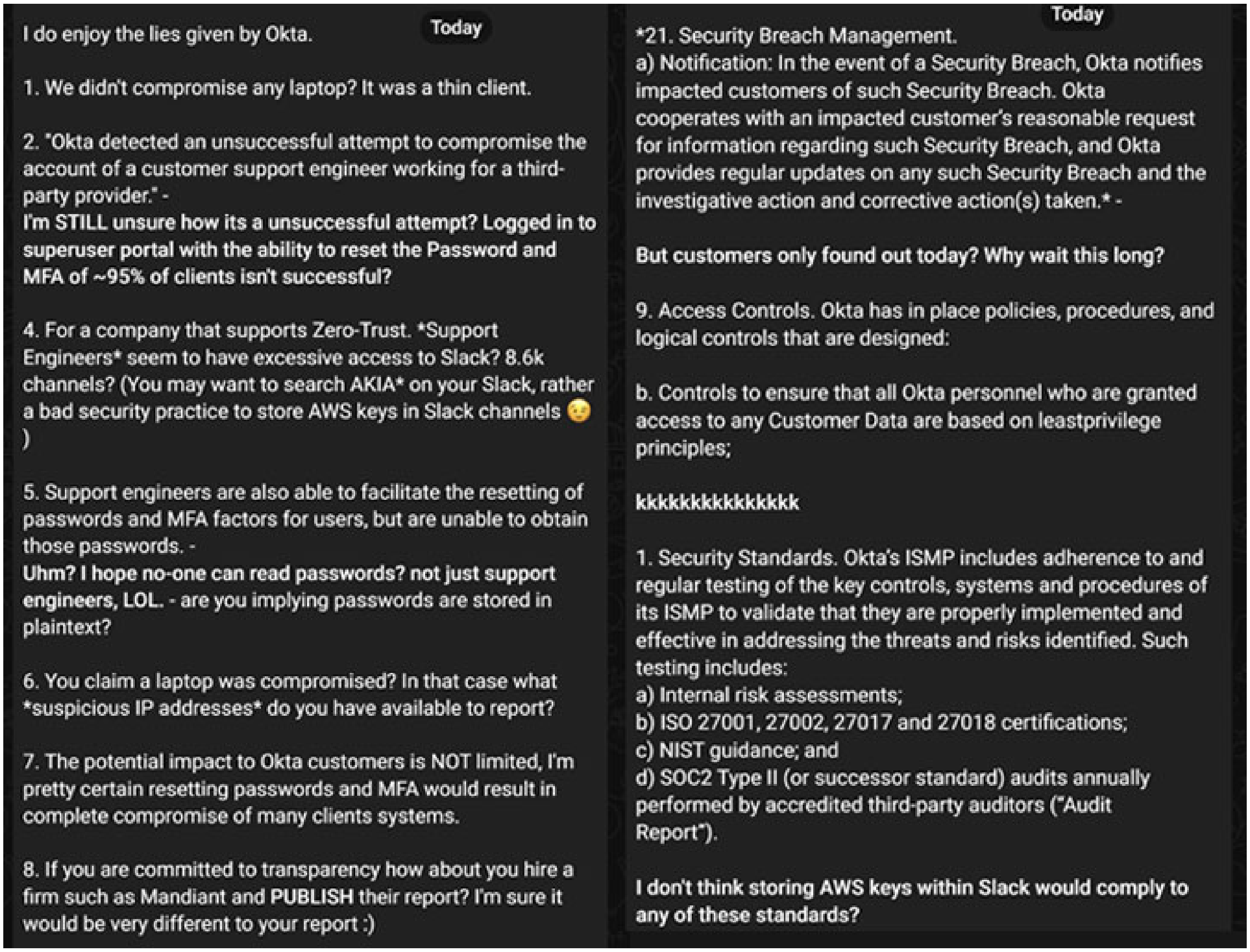
That said, of particular concern is the fact that Okta failed to publicly disclose the breach for two months, prompting the cyber criminal group to ask "Why wait this long?" in its counter statement.

LAPSUS$ has also claimed in its rebuttal that Okta was storing Amazon Web Services (AWS) keys within Slack and that support engineers seem to have "excessive access" to the communications platform. "The potential impact to Okta customers is NOT limited, I'm pretty certain resetting passwords and MFA would result in complete compromise of many clients' systems," the gang elaborated.

Microsoft Exposes the Tactics of LAPSUS$

LAPSUS$, which first emerged in July 2021, has been on a hacking spree in recent months, targeting a wealth of companies over the intervening period, including Impresa, Brazil's Ministry of Health, Claro, Embratel, NVIDIA, Samsung, Mercado Libre, Vodafone, and most recently Ubisoft.

The financially motivated group's modus operandi has been relatively straightforward: break into a target's network, steal sensitive data, and blackmail the victim company into paying up by publicizing snippets of the stolen data on their Telegram channel.



I do enjoy the lies given by Okta.

1. We didn't compromise any laptop? It was a thin client.

2. "Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider." -
I'm STILL unsure how its a unsuccessful attempt? Logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients isn't successful?

4. For a company that supports Zero-Trust. *Support Engineers* seem to have excessive access to Slack? 8.6k channels? (You may want to search AKIA* on your Slack, rather a bad security practice to store AWS keys in Slack channels 😳)

5. Support engineers are also able to facilitate the resetting of passwords and MFA factors for users, but are unable to obtain those passwords. -
Uhm? I hope no-one can read passwords? not just support engineers, LOL. - are you implying passwords are stored in plaintext?

6. You claim a laptop was compromised? In that case what *suspicious IP addresses* do you have available to report?

7. The potential impact to Okta customers is NOT limited, I'm pretty certain resetting passwords and MFA would result in complete compromise of many clients systems.

8. If you are committed to transparency how about you hire a firm such as Mandiant and **PUBLISH** their report? I'm sure it would be very different to your report :)

*21. Security Breach Management.
a) Notification: In the event of a Security Breach, Okta notifies impacted customers of such Security Breach. Okta cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and Okta provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.* -

But customers only found out today? Why wait this long?

9. Access Controls. Okta has in place policies, procedures, and logical controls that are designed:

b. Controls to ensure that all Okta personnel who are granted access to any Customer Data are based on leastprivilege principles;

kkkkkkkkkkkkkk

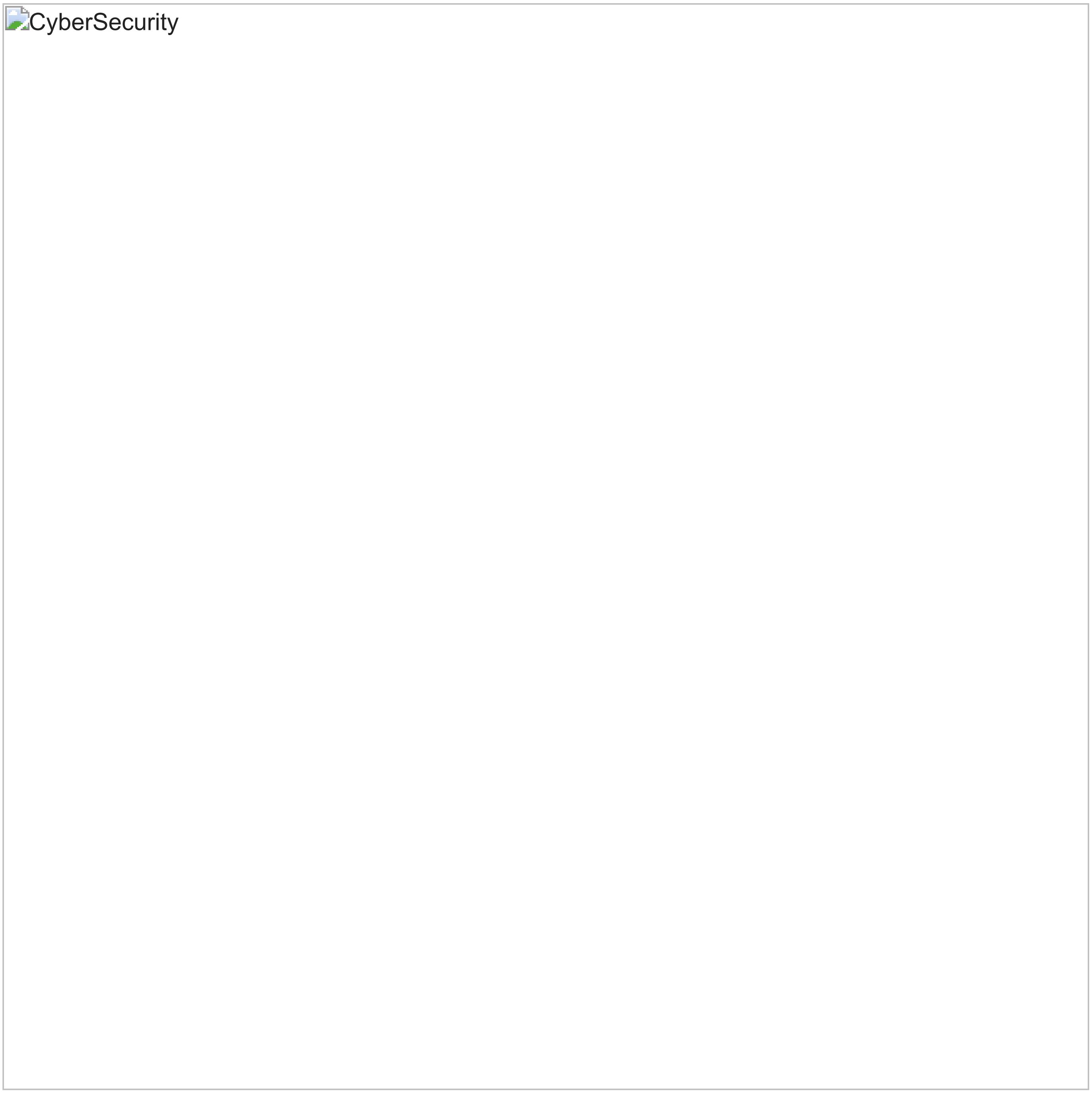
1. Security Standards. Okta's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:
a) Internal risk assessments;
b) ISO 27001, 27002, 27017 and 27018 certifications;
c) NIST guidance; and
d) SOC2 Type II (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").

I don't think storing AWS keys within Slack would comply to any of these standards?

Microsoft described LAPSUS$ as a group following a "pure extortion and destruction model without deploying ransomware payloads" and one that "doesn't seem to cover its tracks."

Other tactics adopted by the crew include phone-based social engineering schemes such as SIM-swapping to facilitate account takeover, accessing personal email accounts of employees at target organizations, bribing employees, suppliers, or business partners of companies for access, and intruding in the ongoing crisis-response calls of their targets to initiate extortion demands.

LAPSUS$ has also been observed deploying the RedLine Stealer that's available for sale on underground forums to obtain passwords and session tokens, in addition to buying credentials and access tokens from dark web marketplaces as well as searching public code repositories for exposed credentials, to gain an initial foothold.



"The objective of DEV-0537 actors is to gain elevated access through stolen credentials that enable data theft and destructive attacks against a targeted organization, often resulting in extortion," the company said. "Tactics and objectives indicate this is a cybercriminal actor motivated by theft and destruction."

Following initial access, the group is known to exploit unpatched vulnerabilities on internally accessible Confluence, JIRA, and GitLab servers for privilege escalation, before proceeding to exfiltrate relevant information and delete the target's systems and resources.

To mitigate such incidents, Microsoft is recommending organizations to mandate multi-factor authentication (but not SMS-based), make use of modern authentication options such as OAuth or SAML, review individual sign-ins for signs of anomalous activity, and monitor incident response communications for unauthorized attendees.

"Based on observed activity, this group understands the interconnected nature of identities and trust relationships in modern technology ecosystems and targets telecommunications, technology, IT services and support companies – to leverage their access from one organization to access the partner or supplier organizations," Microsoft detailed.

Amidst the fallout from the leaks, LAPSUS$ appear to be taking a break. "A few of our members has [sic] a vacation until 30/3/2022. We might be quiet for some times [sic]," the group said on its Telegram channel.

SHARE □ □ □ □ ק
SHARE □