GUIDEPOINT SECURITY

Threat Bulletin: Recent LAPSUS$ Activity Targeting Okta and Microsoft

GuidePoint Research and Intelligence Team (GRIT)

Summary

Between March 20, 2022, and March 21, 2022, the eCrime group known as LAPSUS$ released several screenshots via Telegram indicating that they had successfully breached Okta and Microsoft as part of two separate breach scenarios.

LAPSUS$ Threat Profile

Becoming more visible beginning in December 2021, LAPSUS$ is well-known for targeting victims in the telecommunications and technology sectors, where noteworthy victims of this group include NVIDIA, Samsung, and Ubisoft. The most notable characteristic of this group is they do not perform encryption of files/data for extortion purposes, rather, they target and exfiltrate sensitive data. This stolen information is leveraged to build credibility, extort their victims for money, and/or specific demands, such as the case with Nvidia where they demanded the release of less restrictive firmware. This deviates from the traditional ransomware approach used by other eCrime groups such as Conti, Lockbit, and others, which is why we refer to them as an eCrime group rather than a ransomware group. Another deviation from traditional ransomware groups is their use of Telegram, a free instant messaging service, for communication and extortion purposes, versus the use of a leak site hosted using a TOR service. They are also known for taking unorthodox approaches to initial access into organizations. On March 11, 2022, LAPSUS$ posted a recruiting message on their telegram channel in search of insiders within telecommunications and technology companies that could provide access via VPN, Citrix, or remote access tools such as AnyDesk.

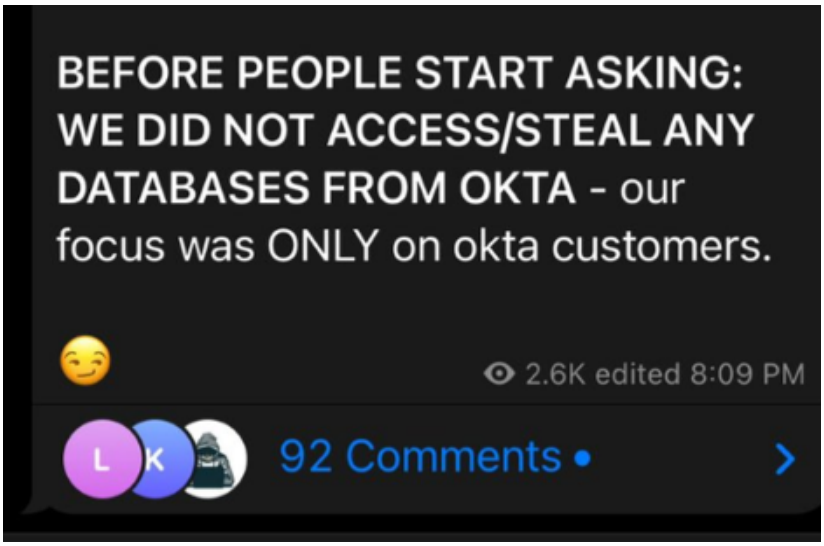
The LAPSUS$ group is suspected to operate out of South America, specifically Brazil, and has been observed communicating in Portuguese and English. Their motivation seems to be more geared towards reputation and influence versus monetary gain.

Suspected Okta Breach

LAPSUS$ released a screenshot on March 21, 2022, indicating there was evidence that they compromised an account that had “Super User” level privileges and was tied to a sub-processor. According to Okta, sub-processors “process Customer Data and assist Okta with respect to the provision of the applicable Service under the Okta Master Subscription Agreement.” This level of access would give an attacker the ability to access to multiple applications within the Okta infrastructure including Slack, Jira, CloudFlare, and other applications tied to Okta’s SSO infrastructure.

The screenshots provided by LAPSUS$ indicate that they were taken on January 21, 2022, and although the group claims to still have access to the environment, the CEO of Okta released a statement via Twitter indicating that they detected the “attempted compromise” of an account tied to a third-party support engineer which was “investigated and contained by the subprocessor.” He went on to indicate that Okta’s stance is that the screenshots released by LAPSUS$ are from the January incident and there is no evidence of on-going malicious activity in their environment.

In LAPSUS$’s screenshots regarding their breach of Okta, they depict access to internal applications such as Slack, Jira, and CloudFlare. However, based on statements released from Telegram, LAPSUS$ indicated that they are most interested in accessing Okta’s customers versus Okta itself.



Although there hasn’t been any public announcement of downstream customer compromise due to the compromised Okta account, this situation is still developing and being investigated.

Suspected Microsoft Breach

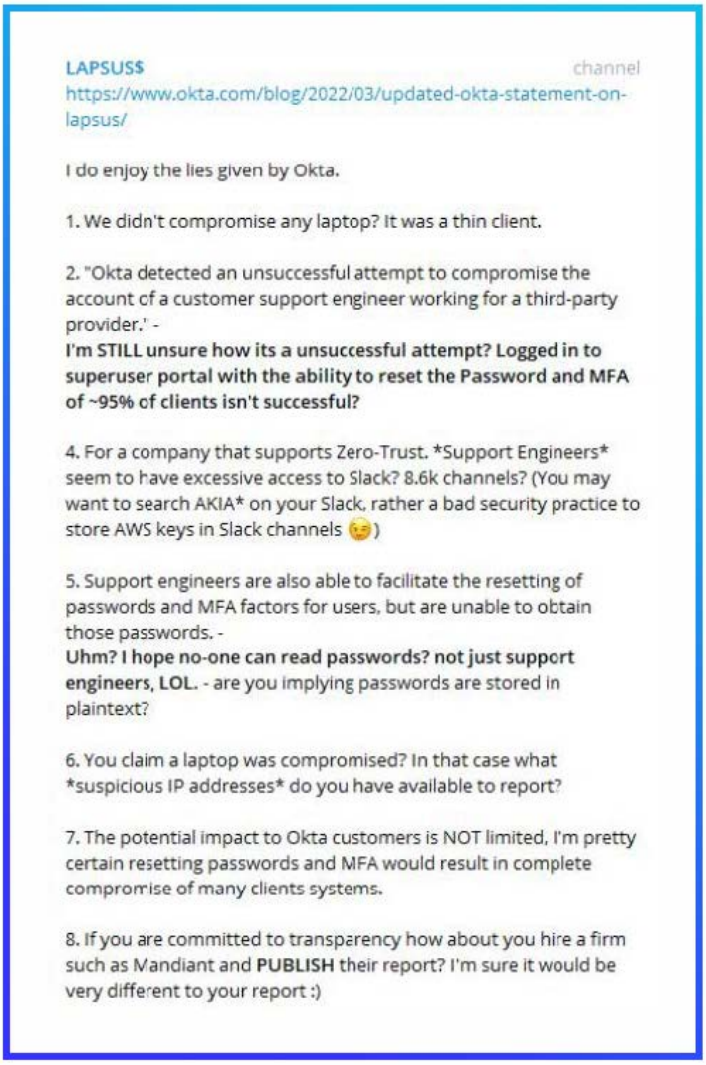
LAPSUS$ also released a screenshot on March 20, 2022, indicating that they had access to a set of internal repositories and suggested that they belonged to Microsoft. The repositories in the screenshot related to Bing and Cortana, amongst other internal applications. On March 21, 2022, LAPSUS$ posted a torrent link to a suspected partial source code leak for the repositories associated with their original screenshot. Microsoft is currently investigating this suspected breach and has not commented publicly at this time.

Updates – March 22, 2022 1800 ET:

Okta

Okta's Chief Security Officer, David Bradbury, released a statement in response to discussions regarding the LAPSUS$ compromise. In his statement, Bradbury reiterated that the compromise took place during a five-day window between January 16, 2022, and January 21, 2022. The statement additionally indicated that the "potential impact to Okta customers is limited to the access that support engineers have" and that "support engineers are unable to create or delete users, or download customer databases." Lastly, the statement also confirmed that, "Support engineers are also able to facilitate the resetting of passwords and multi-factor authentication factors for users, but are unable to obtain those passwords." Okta confirms that there are no impacts to Auth0, HIPAA, or FedRAMP customers.

The Lapsus$ group responded to Okta's published statement via Telegram, a snippet of which can be seen below. Most interestingly, the group confirms that the compromised a thin client system rather than a user's laptop, and makes several critiques of Okta's security posture including access to Slack channels and the storing of AWS keys in Slack channels. The response from LAPSUS$ did not contain new details regarding the compromise.



LAPSUS$ channel

https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

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 :)

Microsoft

Regarding the Microsoft breach, several sources on Twitter have indicated that in addition to source code being leaked, Microsoft has had several code signing certificates released as part of the LAPSUS$ leaks. At least one security researcher has been able to successfully sign code with this certificate. Microsoft has not yet released any public statements regarding LAPSUS$ activity.

Recommendations

GRIT recommends taking the following actions to reduce risk and investigate for potential unauthorized activity related to recent LAPSUS$ activities relating to Okta and Microsoft:

1. Rotate Okta privileged passwords.
2. Review Okta logs for suspicious or unauthorized activity related to elevated privilege accounts.
3. Review log settings for Okta activity and ensure that sufficient logging durations are enabled and stored in a log aggregation tool, if possible.
4. Perform a comprehensive Threat Discovery including all SaaS applications connected to Okta, specifically focusing on anomalous logins and behaviors.
5. Monitor all new executables in your environment, including any signed by Microsoft, until further guidance is available

Detection Opportunities

The following sources are available to aid in the creation of detection capabilities for the LAPSUS$ group:

https://github.com/elastic/detection-rules/tree/main/rules/integrations/okta
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/okta

Need Help?

If you suspect you may be impacted by the LAPSUS$ breach of Okta and Microsoft, contact

GRIT@guidepointsecurity.com

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.

GUIDEPOINT SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132