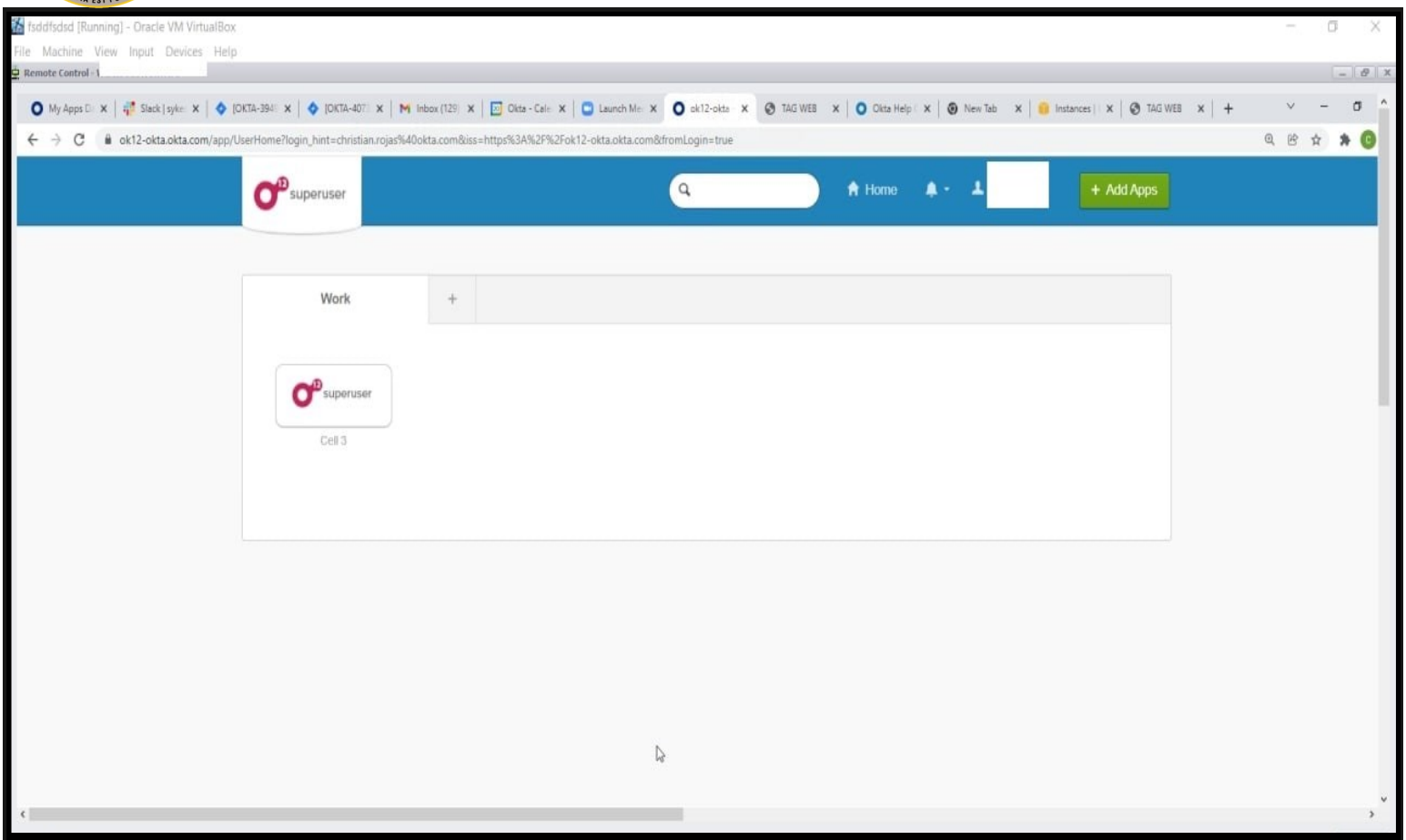
(U) VFC Cyber Link #22-02

03/25/2022 Tracked by: HSEC-1.8, VFC/NVRIC SIN# 1

(U) Okta Single Sign-On Breach



UNCLASSIFIED

(U) Above picture shows superuser access to the Okta platform, allowing Lapsus to access many Okta internal services.

(U) Executive Summary

- (U) Okta, an identity and access management platform that provides Single Sign-on (SSO) services to over 15 thousand customers, has experienced a data breach.
- (U) Malicious actors from the ransomware group Lapsu$ gained access to an Okta platform administrator account, allowing them to access enterprise portal settings and information for Okta employees, customers, and user accounts.
- (U) From the portal, Lapsu$ actors captured photographic proof of the attack and their ability to reset passwords for individual user accounts on the Okta platform, using an account from Cloudflare, a major internet safety and security organization, as illustration.
- (U) Lapsu$ released evidence of an Okta breach on March 22, 2022, but it is believed actors gained access on January 21, 2022.
- (U) During Okta's investigation into the breach, they claimed to have found no evidence of an ongoing attack, suspecting the pictures to be related to the account-compromise incident that occurred in January 21, 2022.
- (U) The Lapsu$ group claims to have had access to Okta for several months, targeting customers of the platform specifically.
- (U) Organizations which use Okta's services should consider password resets on potentially impacted users.

(U) Please direct any questions related to this Cyber Link to vfc@vfc.vsp.virginia.gov.

(U) VFC Cyber Link #22-02

02/18/2022 Tracked by: HSEC-1.8, VFC/NVRIC SIN# 1

(U) Okta Single Sign-On Breach

(U) Okta Data breach — On March 22, 2022 at 1 AM (EST) the Virginia Fusion Center was notified that a ransomware group called Lapsu$ (Lapsus) had gained access to Okta's platform administrator account. To verify the security breach the Lapsus Group posted several pictures containing sensitive information and interactions from Okta employees, including internal communication channels, VPN configurations, customer information and security status.

(U) **Okta's Investigation** — Okta has launched an investigation into the incident to identify more information. At this time, their investigation indicates the information released may have been from a breach in January of 2022, which is in line with Lapsus Ransomware Group's claim that they had gained access.

(U) Level Of Access — Okta authenticates users for access to several services, including email and cybersecurity tools. Lapsus actors can reset login credentials through the Okta Admin portal, allowing them to easily gain access to sensitive tools and information within your organization through privileged accounts. Such a high level of access can possibly lead to secondary incidents, such as ransomware infections or data theft.

(U) Mitigation Steps — If your entity uses Okta for identity services / Single Sign-On, it is possible that user accounts within your organization have been tampered with while the actors had access to the Okta administrator account. If possible, please consider taking the following actions, in addition to any actions defined in your organization's policies and procedures for handling account compromise:

1) A password reset for all Okta users.
If not possible, a password reset for all Okta users whose password changed in the last four months.

2) Password reset for any accounts bound to Okta through custom or official connections.

3) Enable Multifactor Authentication on all applicable accounts.

4) Analyze prior logging information for any suspicious activity such as excessive or foreign sign-on attempts.

5) Continue monitoring for suspicious activity.

(U) Cloudflare — A major internet service provider that delivers safety, security, and trust services for internet-facing entities was mentioned in the breach, with the actors showing Cloudflare's Okta account information in multiple screenshots, including one showing a possible user password reset conducted by the platform administrator.

(U) Cloudflare has not found any evidence of a compromise having occurred on their network, but they continue to investigate to rule out the possibility of a successful attack.

(U) Cloudflare has issued a password reset for any employee whose password has changed in the last four months as a precautionary step.

(U) If your organization is a customer of Cloudflare, be alert for any suspicious activity on your account and continue to seek information from Cloudflare as they investigate.

(U) Please direct any questions related to this Cyber Link to vfc@vfc.vsp.virginia.gov.