On March 22, 2022, nearly 24 hours ago, a number of screenshots were published online that were taken from a computer used by one of Okta’s third-party customer support engineers. The sharing of these screenshots is embarrassing for myself and the whole Okta team.

In this post, I want to provide a timeline and my perspective on what has transpired, and where we are today with this investigation. I hope that it will illuminate why I am confident in our conclusions that the Okta service has not been breached and there are no corrective actions that need to be taken by our customers.

By way of background, like many SaaS providers, Okta uses several companies (“sub-processors”) to expand our workforce. These entities help us to deliver for our customers and make them successful with our products. Sitel, through its acquisition of Sykes, is an Okta sub-processor that provides Okta with contract workers for our Customer Support organisation.

On January 20, 2022, the Okta Security team was alerted that a new factor was added to a Sitel customer support engineer’s Okta account. This factor was a password. Although that individual attempt was unsuccessful, out of an abundance of caution, we reset the account and notified Sitel who engaged a leading forensic firm to perform an investigation.

The following timeline outlines the key milestones:

Timeline (times in UTC)

* January 20, 2022, 23:18 - Okta Security received an alert that a new factor was added to a Sitel employee’s Okta account from a new location. The target did not accept an MFA challenge, preventing access to the Okta account.
* January 20, 2022, at 23:46 - Okta Security investigated the alert and escalated it to a security incident.
* January 21, 2022, at 00:18 - The Okta Service Desk was added to the incident to assist with containing the user’s account.
* January 21, 2022, at 00:28 - The Okta Service Desk terminated the user’s Okta sessions and suspended the account until the root cause of suspicious activity could be identified and remediated.
* January 21, 2022, at 18:00 - Okta Security shared indicators of compromise with Sitel. Sitel informed us that they retained outside support from a leading forensic firm.
* January 21, 2022, to March 10, 2022 - The forensic firm’s investigation and analysis of the incident was conducted until February 28, 2022, with its report to Sitel dated March 10, 2022.
* March 17, 2022 - Okta received a summary report about the incident from Sitel
* March 22, 2022, at 03:30 - Screenshots shared online by LAPSUS$
* March 22, 2022, at 05:00 - Okta Security determined that the screenshots were related to the January incident at Sitel
* March 22, 2022, at 12:27 - Okta received the complete investigation report from Sitel

I am greatly disappointed by the long period of time that transpired between our notification to Sitel and the issuance of the complete investigation report. Upon reflection, once we received the Sitel summary report we should have moved more swiftly to understand its implications.

Our investigation determined that the screenshots, which were not contained in the Sitel summary report, were taken from a Sitel support engineer’s computer upon which an attacker had obtained remote access using RDP. This device was owned and managed by Sitel. The scenario here is analogous to walking away from your computer at a coffee shop, whereby a stranger has (virtually in this case) sat down at your machine and is using the mouse and keyboard. So while the attacker never gained access to the Okta service via account takeover, a machine that was logged into Okta was compromised and they were able to obtain screenshots and control the machine through the RDP session.

It’s important to understand that the access that a support engineer has is limited to basic duties in handling inbound support queries. Support engineers use a number of customer support tools to get their job done including Okta’s instances of Jira, Slack, Splunk, RingCentral, and support tickets through Salesforce. The majority of support engineering tasks are performed using an internally-built application called SuperUser or SU for short, which is used to perform basic management functions of Okta customer tenants. This does not provide “god-like access” to all its users. This is an application built with least privilege in mind to ensure that support engineers are granted only the specific access they require to perform their roles. They are unable to create or delete users. They cannot download customer databases. They cannot access our source code repositories.

The report from the forensic firm highlighted that there was a five-day window of time between January 16-21, 2022 when the threat actor had access to the Sitel environment, which we validated with our own analysis.

In trying to scope the blast radius for this incident, our team assumed the worst-case scenario and examined all of the access performed by all Sitel employees to the SuperUser application for the five-day period in question. Over the past 24 hours we have analysed more than 125,000 log entries to ascertain what actions were performed by Sitel during the relevant period. We have determined that the maximum potential impact is 366 (approximately 2.5% of) customers whose Okta tenant was accessed by Sitel.

Because of the access that the support engineers had, the information and the actions were constrained. While it is not a necessary step for customers, we fully expect they may want to complete their own analysis. For transparency, these customers will receive a report that shows the actions performed on their Okta tenant by Sitel during that period of time. We think this is the best way to let customers assess the situation for themselves.

As with all security incidents, there are many opportunities for us to improve our processes and our communications. I’m confident that we are moving in the right direction and this incident will only serve to strengthen our commitment to security.