New Report on Okta Hack Reveals the Entire Episode LAPSUS$ Attack

By The Hacker News

Published: 2022-03-29 · Archived: 2026-04-05 15:53:14 UTC

An independent security researcher has shared what's a detailed timeline of events that transpired as the notorious LAPSUS$ extortion gang broke into a third-party provider linked to the cyber incident at Okta in late January 2022.

In a set of screenshots posted on Twitter, Bill Demirkapi published a two-page "intrusion timeline" allegedly prepared by Mandiant, the cybersecurity firm hired by Sitel to investigate the security breach. Sitel, through its acquisition of Sykes Enterprises in September 2021, is the third-party service provider that provides customer support on behalf of Okta.

The authentication services provider revealed last week that on January 20, it was alerted to a new factor that was added to a Sitel customer support engineer's Okta account, an attempt that it said was successful and blocked.

The incident only came to light two months later after LAPSUS$ posted screenshots on their Telegram channel as evidence of the breach on March 22.

The malicious activities, which gave the threat actor access to nearly 366 Okta customers, occurred over a five-day window between January 16 and 21, during which the hackers carried out different phases of the attack, including privilege escalation after gaining an initial foothold, maintaining persistence, lateral movement, and internal reconnaissance of the network.

Intrusion Timeline

Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle.**

Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01 19:47:58	UserProfileSvcEop.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:28	Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:55:29	C:\Windows\System32\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:55:41	C:\sam.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:56:00	C:\system.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:57:17	C:\Users\[ACCOUNT NAME REDACTED]\Documents\mimikatz_trunk\x64\hash.txt	Escalate Privileges
2022-01-20 18:58:05	hxxps://pastebin.com/7E3Q24r by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 19:06:43	RDP logon by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] from [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 19:53:31	Bing search for Process Hacker by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 19:55:37	Process Hacker downloaded from hxxps://objects.githubusercontent.com	Establish Foothold
2022-01-20 19:55:58	Bing search for Mimikatz by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 19:57:07	Mimikatz downloaded from hxxps://github.com by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 20:58:31	RDP disconnect from [SYSTEM NAME REDACTED] by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Move Laterally
2022-01-20 23:02:41	First malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Initial Compromise
2022-01-21 00:05:15	[ACCOUNT NAME REDACTED]@sykes[.]com accessed hxxps://[INTERNAL URL REDACTED]/personal/[INTERNAL USER NAME REDACTED]/Documents/Projects/ryk/DomAdmins-LastPass.xlsx via SecureLink	Internal Recon
2022-01-21 05:29:50	[ACCOUNT NAME REDACTED] account created by [ACCOUNT NAME REDACTED]@sykes[.]com	Maintain Presence
2022-01-21 05:29:51	[ACCOUNT NAME REDACTED] added to TenantAdmins group by [ACCOUNT NAME REDACTED]@sykes[.]com	Maintain Presence
2022-01-21 05:39:11	Malicious Email Transport rule to forward to BCC all mail to the accounts [ACCOUNT NAME REDACTED]@sykes[.]com and [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-21 14:11:38	Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Complete Mission

Okta claimed that it had shared indicators of compromise with Sitel on January 21 and that it received a summary report about the incident from Sitel only on March 17. Subsequently, on March 22, the same day the criminal group shared the screenshots, it said it obtained a copy of the complete investigation report.

Subsequently, on March 22, the same day the criminal group shared the screenshots, it obtained a copy of the complete investigation report.

"Even when Okta received the Mandiant report in March explicitly detailing the attack, they continued to ignore the obvious signs that their environment was breached until LAPSUS$ shined a spotlight on their inaction," Demirkapi wrote in a tweet thread.

The San Francisco-based company, in a detailed FAQ posted on March 25, acknowledged that its failure to notify its users about the breach in January was a "mistake."

"In light of the evidence that we have gathered in the last week, it is clear that we would have made a different decision if we had been in possession of all of the facts that we have today," Okta said, adding it "should have more actively and forcefully compelled information from Sitel."

Sitel, for its part, said it's "cooperating with law enforcement" on the incident and has clarified that the breach affected "a portion of the legacy Sykes network only," adding it "took swift action to contain the attack and to notify and protect any potentially impacted clients who were serviced by the legacy organization."

The development comes as the City of London Police told The Hacker News last week that seven people connected to the LAPSUS$ gang were arrested and subsequently released under investigation. "Our enquiries remain ongoing," the agency added.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
