The purported Mandiant timeline starts on January 16, with the initial compromise of Sitel. That’s in contrast to the [timeline](https://www.okta.com/blog/2022/03/oktas-investigation-of-the-january-2022-compromise/) provided by Okta, which starts on January 20 and does not include any details about what happened [prior](https://venturebeat.com/2022/03/23/okta-and-the-lapsus-breach-5-big-questions/) to that point.

Lapsus$ did not begin investigating the compromised system until January 19, according to the timeline posted by Demirkapi.

On that day, the threat actor did a Bing search for privilege escalation tools on GitHub, the purported Mandiant timeline says. “With little regard for OPSEC, LAPSUS$ searched for a CVE-2021-34484 bypass on their compromised host and downloaded the pre-built version from GitHub,” Demirkapi said in a [tweet](https://twitter.com/BillDemirkapi/status/1508527492285575172).

The threat actor “bypassed the FireEye endpoint agent by simply terminating it,” then “simply downloaded the official version of Mimikatz (a popular credential dumping utility) directly from its repository,” Demirkapi said.

The attacker created backdoor users within Sitel’s environment and “finished off their attack by creating a malicious ’email transport rule’ to forward all mail within Sitel’s environment to their own accounts,” Demirkapi wrote in a tweet.

A top question for Okta is, “You knew that the machine of one of your customer support members was compromised back in January. Why didn’t you investigate it? Having the capability to detect an attack is useless if you aren’t willing to respond,” Demirkapi said on Twitter.