Hundreds of companies potentially hit by Okta hack

23 March

REUTERS

Hundreds of organisations that rely on Okta to provide access to their networks may have been affected by a cyber-attack on the company.

Okta said the "worst case" was 366 of its clients had been affected and their "data may have been viewed or acted upon" – its shares fell 9% on the news.

It says it has more than 15,000 clients – from big companies, including FedEx, to smaller organisations, such as Thanet District Council, in Kent.

Cyber-gang Lapsus$ is behind the hack.

March 22, 2022 • 17 min read

DEV-0537 criminal actor targeting organizations for data exfiltration and destruction

Microsoft Threat Intelligence Center (MSTIC)
Detection and Response Team (DART)
Microsoft Defender Threat Intelligence

Share ⌄

March 24, 2022 update – *As Microsoft continues to track DEV-0537's activities, tactics, and tools, we're sharing new detection, hunting, and mitigation information to give you additional insights on remaining vigilant against these attacks.*

In recent weeks, Microsoft Security teams have been actively tracking a large-scale social engineering and extortion campaign against multiple organizations with some seeing evidence of destructive elements. As this campaign has accelerated, our teams have been focused on detection, customer notifications, threat intelligence briefings, and sharing with our industry collaboration partners to understand the actor's tactics and targets. Over time, we have improved

Dark Reading

August 2016