

Hundreds of companies potentially hit by Okta hack

🕒 23 March



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.

BBC

March 2022

MSRC

March 2022

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




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

8/29/2016
07:30 AM



Alex Campbell
Commentary

 0 COMMENTS
[COMMENT NOW](#)

Critical Infrastructure: The Next Cyber-Attack Target

Power and utilities companies need a risk-centric cybersecurity approach to face coming threats.

The way we think about cyber attacks changed in December 2015, when Ukraine experienced the first recorded power outage caused by a cyber attack. It didn't last long—between one and six hours, depending on the area—but it showed the government, industry, and the public how these attacks could affect the physical world. It's not just personal information and other sensitive data that's at stake. Critical infrastructure is now under threat.

Dark Reading

August 2016