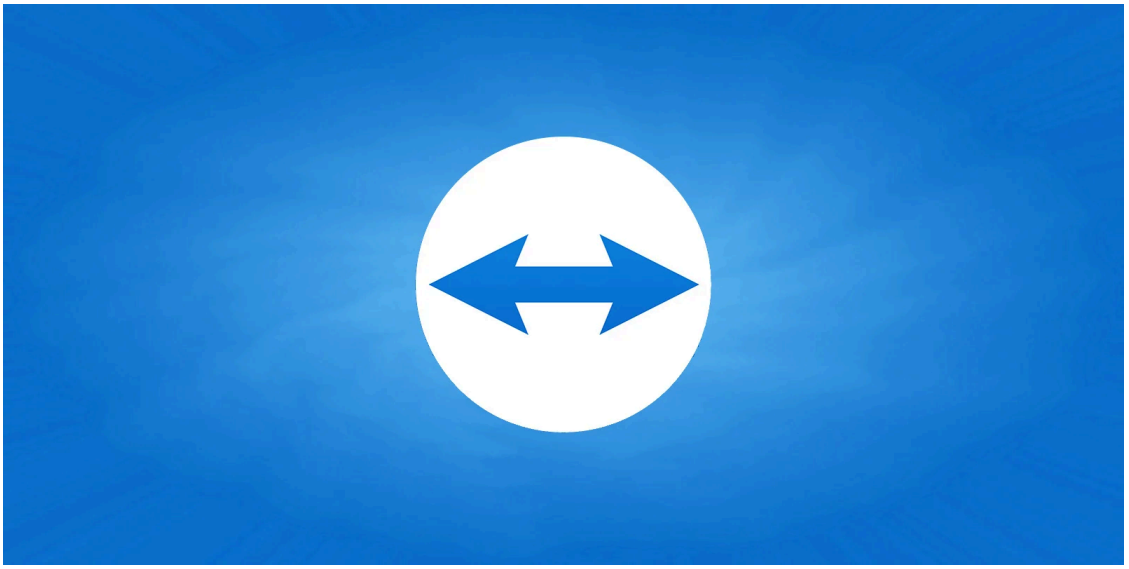
TeamViewer's corporate network was breached in alleged APT hack

By Lawrence Abrams

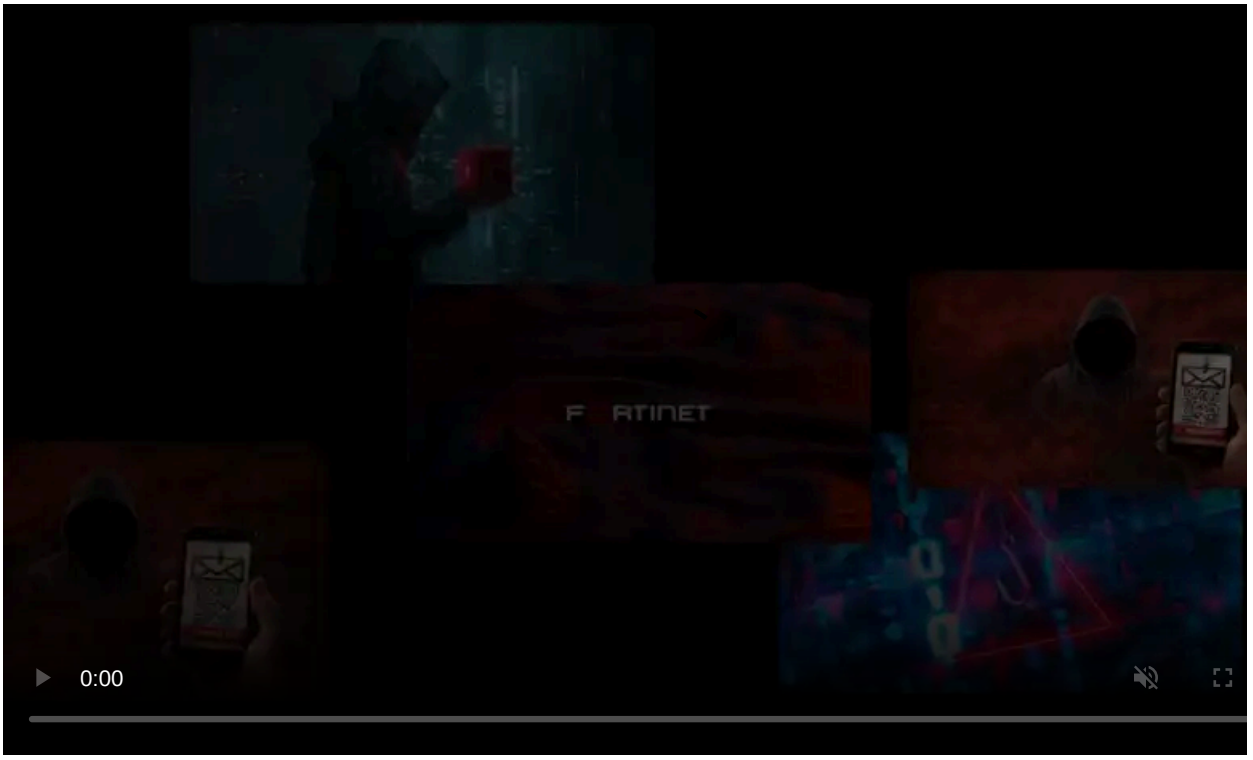
Published: 2024-06-27 · Archived: 2026-04-05 20:34:56 UTC

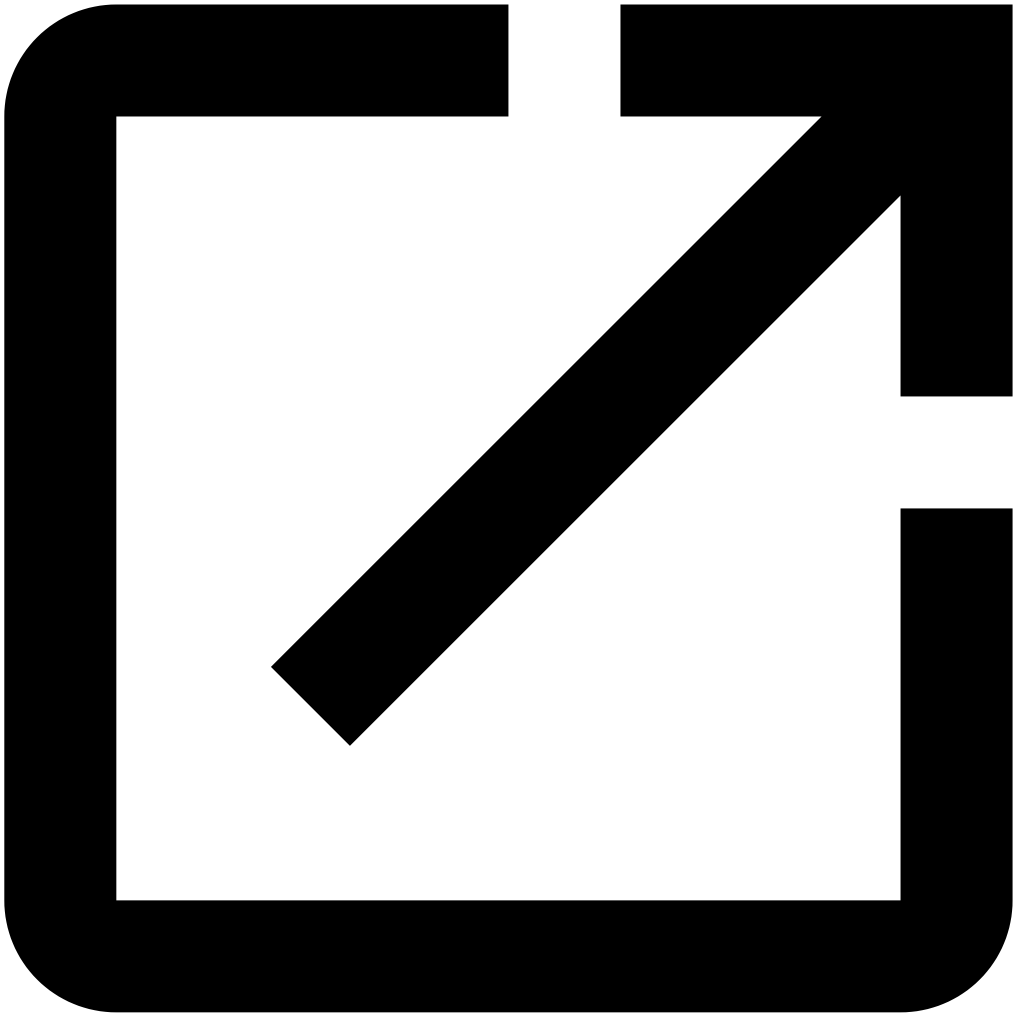


Update: TeamViewer is now attributing the attack to the Russian state-sponsored hacking group known as Midnight Blizzard. Further updates added below.

The remote access software company TeamViewer is warning that its corporate environment was breached in a cyberattack yesterday, with a cybersecurity firm claiming it was by an APT hacking group.

"On Wednesday, 26 June 2024, our security team detected an irregularity in TeamViewer’s internal corporate IT environment," TeamViewer said in a post to its Trust Center.


F RTINET
0:00



"We immediately activated our response team and procedures, started investigations together with a team of globally renowned cyber security experts and implemented necessary remediation measures."

"TeamViewer's internal corporate IT environment is completely independent from the product environment. There is no evidence to suggest that the product environment or customer data is affected. Investigations are ongoing and our primary focus remains to ensure the integrity of our systems."

The company says that it plans to be transparent about the breach and will continuously update the status of its investigation as more information becomes available.

However, though they say they aim to be transparent, the "TeamViewer IT security update" page contains a `<meta name="robots" content="noindex">` HTML tag, which prevents the document from being indexed by search engines and thus hard to find.

TeamViewer is a very popular remote access software that allows users to remotely control a computer and use it as if they were sitting in front of the device. The company says its product is currently used by over 640,000 customers worldwide and has been installed on over 2.5 billion devices since the company launched.

While TeamViewer states there is no evidence that its product environment or customer data has been breached, its massive use in both consumer and corporate environments makes any breach a significant concern as it would provide full access to internal networks.

In 2019, TeamViewer confirmed a 2016 breach linked to Chinese threat actors due to their use of the Winnti backdoor. The company said they did not disclose the breach at the time as data was not stolen in the attack.

Alleged APT group behind attack

News of the breach was first reported on Mastodon by IT security professional Jeffrey, who shared portions of an alert shared on the Dutch Digital Trust Center, a web portal used by the government, security experts, and Dutch corporations to share information about cybersecurity threats.

"The NCC Group Global Threat Intelligence team has been made aware of significant compromise of the TeamViewer remote access and support platform by an APT group," warns an alert from the IT security firm NCC Group.

"Due to the widespread usage of this software the following alert is being circulated securely to our customers."

An alert from Health-ISAC, a community for healthcare professionals to share threat intelligence, also warned today that TeamViewer services were allegedly being actively targeted by the Russian hacking group APT29, also known as Cozy Bear, NOBELIUM, and Midnight Blizzard.

"On June 27, 2024, Health-ISAC received information from a trusted intelligence partner that APT29 is actively exploiting Teamviewer," reads the Health-ISAC alert shared by Jeffrey.

"Health-ISAC recommends reviewing logs for any unusual remote desktop traffic. Threat actors have been observed leveraging remote access tools. Teamviewer has been observed being exploited by threat actors associated with APT29."

APT29 is a Russian advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The hacking group is known for its cyberespionage abilities and has been linked to numerous attacks over the years, including attacks on Western diplomats and a recent breach of Microsoft's corporate email environment.

While the alerts from both companies come today, just as TeamViewer disclosed the incident, it is unclear if they are linked as TeamViewer's and NCC's alerts address the corporate breach, while the Health-ISAC alert focuses more on targeting TeamViewer connections.

BleepingComputer also contacted TeamViewer with questions about the attack but was told no further information would be shared as they investigated the incident.

Update 6/27/24: NCC Group told BleepingComputer that they had nothing further to add when contacted for more information.

"As part of our Threat Intelligence service to our clients, we issue alerts on a regular basis based on a variety of sources and intelligence," NCC Group told BleepingComputer.

"At this time, we do not have anything further to add to the alert that was sent to our clients."

Update 6/28/24: TeamViewer has told BleepingComputer that they have removed the noindex tag from their Trust Center and that it should be indexed soon by search engines.

Source: https://www.bleepingcomputer.com/news/security/teamviewers-corporate-network-was-breached-in-alleged-apt-hack/