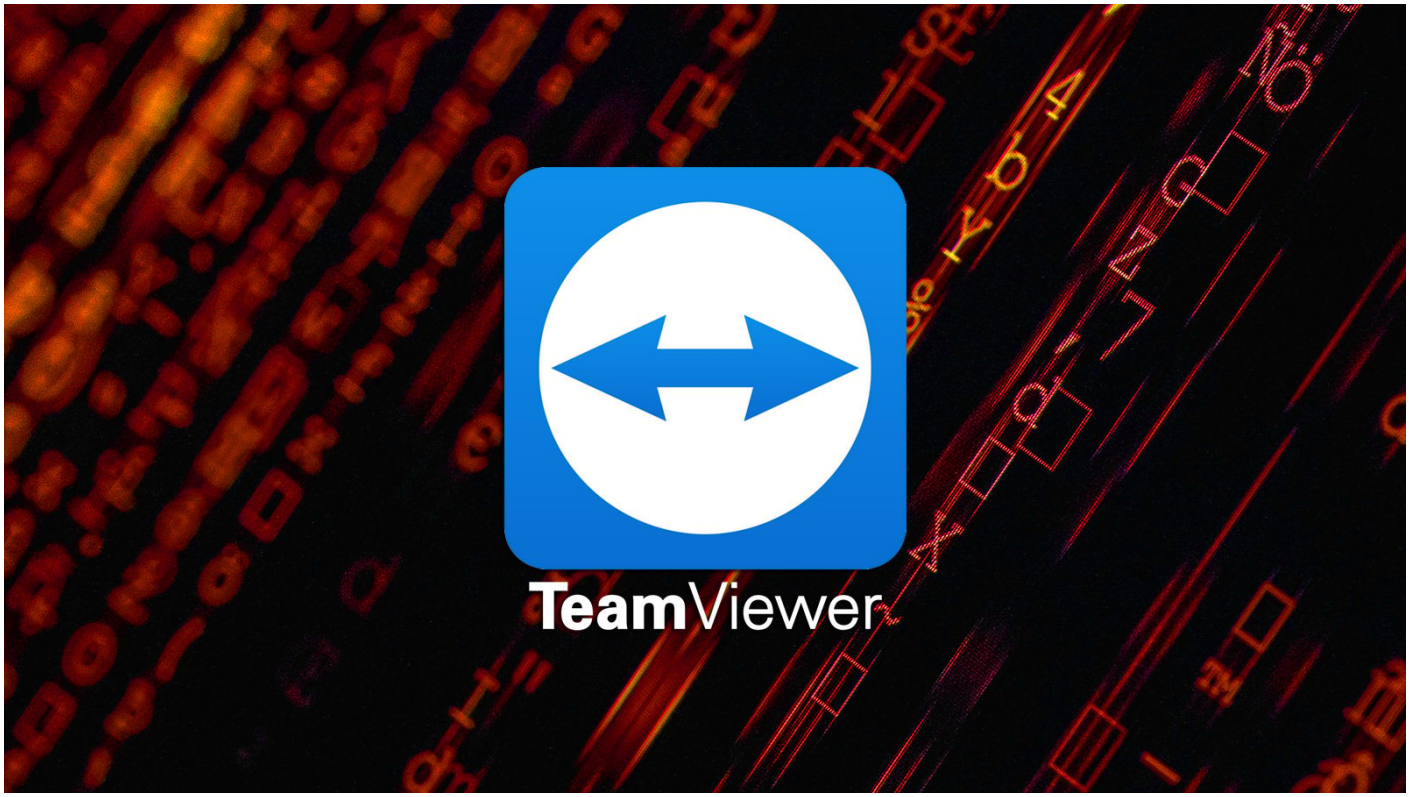
TeamViewer links corporate cyberattack to Russian state hackers

Lawrence Abrams ⋮⋮ 6/28/2024



RMM software developer TeamViewer says a Russian state-sponsored hacking group known as Midnight Blizzard is believed to be behind a breach of their corporate network this week.

Yesterday, BleepingComputer reported that TeamViewer had been breached and that cybersecurity experts and healthcare organizations had begun warning customers and organizations to monitor their connections.

TeamViewer is widely used by enterprises and consumers for remote monitoring and management (RMM) of devices on internal networks. As the scope of the cybersecurity incident was not known, experts began warning stakeholders to monitor for suspicious connections that could indicate threat actors attempting to use the TeamViewer breach to gain access to further networks.

Today, TeamViewer has shared an updated statement with BleepingComputer, stating that they attribute the attack to Midnight Blizzard (APT29, Nobelium, Cozy Bear).

TeamViewer says they believe their internal corporate network, not their production environment, was breached on Wednesday, June 26, using an employee's credentials.

"Current findings of the investigation point to an attack on Wednesday, June 26, tied to credentials of a standard employee account within our Corporate IT environment," reads the updated TeamViewer statement.

"Based on continuous security monitoring, our teams identified suspicious behavior of this account and immediately put incident response measures into action. Together with our external incident response support, we currently attribute this activity to the threat actor known as APT29 / Midnight Blizzard."

The company stressed that their investigation has shown no indication that the production environment or customer data was accessed in the attack and that they keep their corporate network and product environment isolated from each other.

"Following best-practice architecture, we have a strong segregation of the Corporate IT, the production environment, and the TeamViewer connectivity platform in place," continues TeamViewer's statement.

"This means we keep all servers, networks, and accounts strictly separate to help prevent unauthorized access and lateral movement between the different environments. This segregation is one of multiple layers of protection in our 'defense in-depth' approach."

While this is reassuring to TeamViewer customers, it is common in incidents like this for more information to come out later as the investigation progresses. This is especially true for a threat actor as advanced as Midnight Blizzard.

Therefore, it is recommended that all TeamViewer customers enable multi-factor authentication, set up an allow and block list so only authorized users can make connections, and monitor their network connections and TeamViewer logs.

BleepingComputer contacted TeamViewer with further questions about who is assisting with the investigation and how the employee credentials were compromised but has not received a response at this time.

Midnight Blizzard

Midnight Blizzard (aka Cozy Bear, Nobelium, and APT29) is an advanced state-sponsored hacking group believed to be associated with Russia's Foreign Intelligence Service (SVR).

The threat actors have been linked to a wide variety of attacks, primarily associated with cyber espionage, in which they breach government and corporate networks to silently steal data and monitor communications.

The US government linked the hacking group to the infamous SolarWinds supply chain attack in 2020, where the threat actors breached the company to gain access to its developer environment. From there, they added a malicious backdoor to a Windows DLL file that was then pushed down to SolarWinds customers in a supply chain attack via an automatic update platform.

This DLL allowed the threat actors to monitor for high-value targets, breach networks, and steal data from their environments.

More recently, Midnight Blizzard turned their attention to Microsoft in a series of successful cyberattacks.

In 2023, the threat actors breached Microsoft's corporate Exchange Online accounts to monitor and steal emails from the company's leadership, cybersecurity, and legal teams. Of particular interest, Microsoft says that they initially targeted email accounts to find information related to themselves.

In March 2024, Microsoft said the threat actors once again breached their systems using secrets found in the emails that were stolen in the previous incident.

Midnight Blizzard accessed some of its internal systems and source code repositories as part of this breach.

In both incidents, the threat actors used password spray attacks to breach corporate accounts and then used those accounts as a springboard to other accounts and devices in targeted systems.

Microsoft had previously shared guidance for responding and investigating attacks by Midnight Blizzard.