Europe, North America Most Impacted by 3CX Supply Chain Hack

Organizations in Europe, North America and Australia seem to account for the highest percentage of victims of the supply chain hack that hit business communication company 3CX.

According to data collected by Fortinet, based on the number of devices connecting to attacker-controlled infrastructure, the highest percentage of victims is in Italy, followed by Germany, Austria, the United States, South Africa, Australia, Switzerland, the Netherlands, Canada and the United Kingdom.

Looking at regional data, Europe is at the top of the chart with 60%, followed by North America with 16%.

“This may indicate that the threat actor is mainly targeting enterprises in those regions – however, this is uncertain. This could be indicative of 3CX product’s geographic customer base – including the possibility of various multinational corporations operating inside those regions,” Fortinet noted.

BlackBerry’s security researchers have also seen many apparent victims in Australia, the United States and the United Kingdom, across the healthcare, pharmaceutical, IT, and financial sectors.

3CX’s VoIP software is used by more than 600,000 companies worldwide, including major consumer brands, airlines, carmakers and hotels.

Security firm Huntress noted last week that there are more than 240,000 3CX phone system management consoles that are accessible from the internet, and the company saw over 2,700 instances of compromised binaries on customer systems.

It was previously reported that the attackers likely had access to 3CX systems for months before the breach was

detected. Based on BlackBerry's own analysis, "the initial phase of this operation took place somewhere between the end of summer and the beginning of fall 2022."

[Read: 3CX Supply Chain Hack: Information and Tools for Defenders]

It's still unclear how the attackers gained access to 3CX systems, and whether they exploited any known or unknown vulnerability for initial access, but the new identifier CVE-2023-29059 has been assigned to the 3CXDesktopApp compromise.

Bleeping Computer also reported that the attackers appear to have exploited CVE-2013-3900, a file signature-related vulnerability for which Microsoft released an opt-in fix a decade ago.

Evidence collected to date suggests that the attackers compromised 3CX's development systems and abused them to deliver a piece of malware – including a malicious component designed for data harvesting – to the company's customers. Some believe the attack may have been in an early, information-gathering phase when it was detected.

CrowdStrike said a group linked to the North Korean threat actor Lazarus may have been behind the attack, and Sophos has also found links to the North Korean group.

3CX, which has called in Mandiant to assist with the investigation, said in its latest update, "Initial investigation suggested the incident was carried out by a highly experienced and knowledgeable hacker."

The company has confirmed that both its Windows and Mac applications are affected. The company has advised customers to uninstall the impacted apps and use the PWA web client instead. The Windows app is being rebuilt, but Google has invalidated the vendor's software security certificate.

The vendor has been criticized by many for the way it has responded to the breach, particularly for ignoring customer reports about the application being detected as malware by multiple cybersecurity products.

Some members of the cybersecurity community have created an online tool that can help users determine if they may have been affected by the attack. Users simply have to visit the tool's website to know if they are impacted, based on a list of IP addresses known to have interacted with the attacker's infrastructure.

SecurityWeek has also compiled a list of information and tools that can be useful to defenders.

Related: Over 250 US News Websites Deliver Malware via Supply Chain Attack

Related: Hundreds Infected With 'Wasp' Stealer in Ongoing Supply Chain Attack

Related: Iranian Hackers Deliver New 'Fantasy' Wiper to Diamond Industry via Supply Chain Attack

Europe, North America Most Impacted by 3CX Supply Chain Hack