

3CX Confirms Supply Chain Attack as Researchers Uncover Mac Component



Business communication solutions provider 3CX has confirmed that it's investigating a security breach, as the cybersecurity community is sharing more information on what appears to be a sophisticated supply chain attack.

The attack seems to impact 3CXDesktopApp, an enterprise voice and video conferencing software. 3CX claims on its website that its products are used by more than 600,000 companies, including major brands such as Coca Cola, Ikea, PwC and several carmakers, airlines and hotel chains.

The incident came to light after 3CX customers started complaining on the company's forum that various cybersecurity products had started flagging and even removing the 3CXDesktopApp software due to suspicious behavior.

It was initially suggested that the detections were false

positives, but several cybersecurity firms confirmed on Wednesday that the 3CX product was indeed compromised.

An analysis of the attack and indicators of compromise (IoCs) were published by CrowdStrike, SentinelOne and Sophos. At this point in the investigation, evidence collected by CrowdStrike suggests that North Korean threat actor Labyrinth Chollima, a subgroup of the notorious Lazarus Group, is behind the hack.

The attack, dubbed Smooth Operator by SentinelOne, involved the delivery of trojanized 3CXDesktopApp installers. The malware is signed with a code signing certificate and its goal appears to be the deployment of an information stealer.

This multi-stage supply chain attack also involved pulling files from a GitHub repository that has since been shut down.

3CX published a security alert late on Wednesday, informing customers and partners that it has launched an investigation into a 'security issue' related to its Electron Windows App shipped in Update 7, specifically version numbers 18.12.407 and 18.12.416.

"The issue appears to be one of the bundled libraries that we compiled into the Windows Electron App via GIT," said Pierre Jourdan, CISO at 3CX.

"Worth mentioning – this appears to have been a targeted attack from an Advanced Persistent Threat, perhaps even state sponsored, that ran a complex supply chain attack and picked who would be downloading the next stages of their malware. The vast majority of systems, although they had the files dormant, were in fact never infected," the CISO added.

The company has instructed customers to uninstall the affected application and use the PWA client until a new Windows app is developed. Jourdan claimed that the shutdown of the GitHub repository used by the attackers has rendered the compromised library harmless.

[Watch on Demand: Supply Chain & Third-Party Risk Summit Sessions]

3CX's statement focuses on the Windows application and SentinelOne also said it could not confirm that the Mac installer is also trojanized. However, CrowdStrike said it had seen activity on both Windows and macOS systems.

CrowdStrike has shared a sample with Apple security expert Patrick Wardle, whose analysis confirmed that a trojanized macOS application was also used in the Smooth Operator attack.

The researcher found that the malware had been notarized by Apple – which indicates that the tech giant checked it for malicious elements and failed to find any. However, during Wardle's analysis, Apple apparently took action and users are now being warned before installing the trojanized app.

The Mac application is nearly 400 Mb in size, which made it more difficult to analyze, but Wardle was able to confirm suspicious behavior. The malware is apparently designed to download a second-stage payload, but the researcher could not obtain a copy of that payload for analysis.

Wardle has also shared IoCs to help defenders detect the macOS variant of the malware.

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

3CX Confirms Supply Chain Attack as Researchers Uncover Mac Component