

# Mandiant Investigating 3CX Hack as Evidence Shows Attackers Had Access for Months

## 3CX Supply Chain Hack: Information and Tools for Defenders

Google-owned cybersecurity firm Mandiant has been called in to investigate the supply chain attack that hit business communication solutions provider 3CX, as evidence suggests that the attackers had access to the company's systems for several months before the breach was detected.

3CX's VoIP IPBX software is used by more than 600,000 companies worldwide, including dozens of major brands.

The incident came to light on March 22, after the products of several major cybersecurity firms started flagging 3CXDesktopApp for malicious behavior. An investigation revealed that hackers – possibly a North Korean state-sponsored threat actor – compromised the Windows and Mac versions of the application, leading to many 3CX customers downloading a trojanized version of the app.

The campaign, dubbed SmoothOperator, could impact thousands or even hundreds of thousands of users.

According to threat detection and response firm Huntress, there are more than 240,000 3CX phone management systems that are exposed to the internet. The company has detected over 2,700 instances of malicious 3CXDesktopApp binaries.

The malware delivered by the attackers was apparently designed

to harvest data from compromised systems, including browser data.

However, cybersecurity company Todyl believes “the campaign was in the early, information gathering stage when identified, with the threat group setting up for future malicious activity including extortion and leveraging collected credentials from browsers”.

While 3CX initially claimed that only the Windows app was impacted, it has now confirmed that the Mac version of the app is also affected. The company has advised customers to uninstall the Electron app for Mac and Windows and use the web app (PWA) version until a clean app is developed.

The company initially suggested that an FFmpeg multimedia library was actually compromised rather than 3CX itself. However, FFmpeg has denied these claims and ReversingLabs noted that the malicious FFmpeg files were signed with a legitimate certificate issued to 3CX.

“Our analysis of the malicious update points either to a compromise of the 3CX development pipeline that resulted in malicious code being added during the build, or the possibility of a malicious dependency being served by a package repository,” ReversingLabs said, noting that its researchers believe the incident was caused by “the compromise of the repository from which the Electron application binaries were fetched during the build process”.

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

Evidence collected to date suggests that the attackers had access to 3CX systems for months before the attack was discovered.

Incident response firm Volexity has analyzed the infrastructure used in the supply chain attack and found that

the hackers likely had access to 3CX systems since at least December 2022, possibly even as early as November 2022.

### **3CX criticized for how it handled the incident**

Many 3CX customers are unhappy with the way the company has handled the incident. It initially insisted that the malware detections were false positives, and some users claimed they were instructed by 3CX staff to pay for a support ticket to get help in addressing the issue.

3CX CEO Nick Galea said the company initially thought this was a false positive after none of the antivirus engines on VirusTotal flagged the file as being suspicious or malware. However, some customers believe the firm should have done more to check the file than just uploading it to VirusTotal.

Galea told CyberScoop in an interview that they should have acted sooner, but argued that false positives happen “quite frequently” due to the way VoIP apps work, which is why the antimalware detections were not initially taken seriously.

However, ReversingLabs noted, “The attack on 3CX – though sophisticated – had clear indicators that could have tipped off 3CX to the breach before customer systems were affected.”

Kevin Beaumont, a reputable security researcher, has criticized the company for how it handles security issues in general. The expert noted that last year he deleted some tweets describing a potentially serious 3CX vulnerability after the vendor “took little responsibility, didn’t fix it, and started arguing on Twitter basically.”

### **Resources for defenders**

Several cybersecurity companies have published blog posts, advisories and tools to help organizations that may have been hit by the 3CX supply chain attack:

Huntress blog post with analysis of the attack, Yara rules for

detecting malicious files, and a script that detects compromised 3CX instances

Reversing Labs blog post with IoCs and analysis of how the 3CX application was compromised

Volexity analysis with details on a possible timeline and a detailed technical description of each attack stage.

Toddl malware analysis

CISA alert advising organizations to hunt for IoCs

Blog posts containing IoCs and information that can be useful to their own customers have also been published by Symantec, ReliaQuest, CrowdStrike, Rapid7, Trend Micro, Sophos and SentinelOne.

**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

*Mandiant Investigating 3CX Hack as Evidence Shows Attackers Had Access for Months*