More evidence links 3CX supply-chain attack to North Korean hacking group

By Alexander Martin

Published: 2023-03-31 · Archived: 2026-04-05 15:17:13 UTC

The supply-chain attack on the enterprise phone company 3CX used hacking code that “exactly matches” malware previously seen in attacks by a notorious North Korean group, according to new analysis.

Establishing the extent of the damage caused by the hack has been a priority for researchers after a number of cybersecurity businesses went public with reports about the 3CX compromise on Wednesday evening, including SentinelOne, Sophos and CrowdStrike.

At the time CrowdStrike said there was “suspected nation-state involvement” in the attack by a group it calls Labyrinth Chollima and describes as “one of the most prolific” hacking groups based in North Korea. Other researchers refer to it as the Lazarus Group.

Sophos added more evidence Friday to this attribution, saying that a shellcode loader the attacker used has only previously been seen in incidents attributed to Lazarus — a financially motivated hacking organization that the FBI has linked to multiple cyber heists and allegedly is sponsored by the North Korean government.

“The code in this incident is a byte-to-byte match to those previous samples,” said Sophos in an updated blog post on the incident.

Christopher Budd, a senior manager for threat research at Sophos, said in a statement: “Upon further analysis of the attack, it’s clear the perpetrators were able to compromise the installation in a way that users unknowingly downloaded not only the original application but also additional malicious code.”

The attackers were able to manipulate the application “in such a way that users were able to use 3CX without any indication that, in the background, this malicious code was running and executing various malicious commands.”

“In terms of the who is behind the attack, further investigation has found that part of the malicious code in the corrupted app exactly matches — byte by byte — malicious code that has been seen in attacks publicly attributed to Lazarus,” said Budd.

3CX, which says it provides office phone systems to more than 600,000 companies globally, confirmed on Thursday that its desktop apps for Windows and MacOS had been compromised by suspected state-sponsored attackers.

The hackers secretly modified these apps so they executed malicious commands in the background, downloading malware that allowed them to steal sensitive information from the web browsers on users’ computers.

Software providers have been on high alert for these types of supply-chain intrusions since the 2020 attack on SolarWinds, which led to data breaches at multiple organizations — including the U.S. government — after hackers compromised a third-party system used by Microsoft customers.

It is not yet known how many of 3CX's customers have been impacted by the incident.

The company's chief information security officer, Pierre Jourdan, described it as "a complex supply chain attack" and said the attackers "picked who would be downloading the next stages of their malware," in a statement on the 3CX's website.

Brand logos featured on 3CX's promotional materials include Mercedes-Benz, Coca-Cola, American Express and the United Kingdom's National Health Service.

The NHS has issued a cyber alert with a "High" severity ranking warning about the active intrusion campaign, telling healthcare organizations that "legitimate versions of 3CX DesktopApp have been compromised and are being actively exploited."

A spokesperson for Mercedes-Benz declined to comment, while American Express said that despite being listed on 3CX's website they were not a client of the company and did not use 3CX's software.

No previous article

No new articles

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79

Source: https://therecord.media/3cx-attack-north-korea-lazarus-group