Malware Hunters Spot Supply Chain Attack Hitting 3CX Desktop App

Threat hunters at CrowdStrike and Sentinel One are tracking what is believed to be an active supply chain attack hitting businesses using a desktop app distributed by video conferencing software firm 3CX.

CrowdStrike threat intelligence team sounded the alarm on Wednesday after observing unexpected malicious activity from a legitimate, signed version of the 3CXDesktopApp.

“The malicious activity includes beaconing to actor-controlled infrastructure, deployment of second-stage payloads, and, in a small number of cases, hands-on-keyboard activity,” the company warned.

“At time of writing, activity has been observed on both Windows and macOS,” CrowdStrike said.

The 3CXDesktopApp, available for Windows, macOS, Linux and mobile, is used by 3CX customers to make calls, view the status of colleagues, chat, schedule a video conference and check voicemails from the desktop software.

CrowdStrike believes the attacks are the work of a North Korean government hacker group and urged 3CX customers to immediately start hunting for signs of infections.

3CX has not yet publicly acknowledged the issue but CrowdStrike says it has been in touch with the VOIP software company to share its findings.

On the 3CX users forums, customers are reporting warnings from both CrowdStrike and SentinelOne anti-malware products about command execution and code injection attacks targeting the 3CX product.

Editor's Note: *This is a developing story. We will provide updates as new information becomes available.*

Related: Microsoft: No-Interaction Outlook Zero Day Exploited Since Last April

Related: Mandiant Catches Another North Korean Gov Hacker Group

Related: Supply Chain Attack Targets Customer Engagement Firm Comm100

Malware Hunters Spot Supply Chain Attack Hitting 3CX Desktop App