



# Cisco Talos Blog<sup>1</sup>



## Threat Advisory: 3CX Softphone Supply Chain Compromise<sup>3</sup>

By Cisco Talos<sup>4</sup>

THURSDAY, MARCH 30, 2023 18:29<sup>5</sup>

THREAT ADVISORY<sup>6</sup>

- Cisco Talos is tracking and actively responding to a supply chain attack involving the 3CX<sup>7</sup> Desktop Softphone application.



- This is a multi-stage attack that involves sideloading DLLs, seven-day sleep routines, and additional payloads dependent on a now-removed GitHub repository for Windows-based systems.
- MacOS systems used a different infection chain leveraging a hardcoded C2 domain, as opposed to the GitHub repo.
- This is just the latest supply chain attack threatening users, after the [SolarWinds incident in 2020](#) and the [REvil ransomware group exploiting Kaseya VSA in 2021](#).

## Summary<sup>2</sup>

Cisco Talos recently became aware of a [supply chain attack](#) affecting Windows and MacOS users of the 3CX software-based phone application. This attack leveraged the legitimate update functionality of the 3CX application to deliver a set of malicious payloads to 3CX users.

The infection chain consists of several stages and involves sideloading DLLs along with a seven-day sleep cycle before the malware attempts to retrieve additional malicious artifacts from a now-removed GitHub repository for the Windows based infection. The GitHub repository hosted a series of icon files with encrypted data appended to the end of the files. These encrypted strings, once decrypted, contained the C2 domains for additional malicious artifacts.

The MacOS version used a hard coded C2 domain. These second-stage payloads are information stealers that attempt to obtain system information and the latest browsing history records, indicating this information may be used as a filtering mechanism to identify and discard some victims while maintaining unauthorized access to others.

During our investigation we were able to see file activity dating back to February 3, 2023. However, the GitHub repository has been active since December 2022. The full scope of the attack is uncertain at this point. The [3CX website](#) claims to have over 600,000 customers and 12 million daily users. It's unclear how many are users of the 3CX Desktop App versus the web app option that was not affected. 3CX is [currently asking users](#) to use the web app while they work to release an update.

## Preparing since February 2022<sup>7</sup>

Based on Cisco Talos investigation, it appears the infrastructure that supported this attack was being prepared as early as February 2022 when the domains were first registered. A second cluster of activity happened toward the end of 2022 when the GitHub repository was created, along with a few other domains. The sbmsa[.]wiki domain was also created on Feb. 9, 2023, which was found to be used by the second stage of the MacOS version.

The timeline below illustrates these clusters of activity. <sup>1</sup>



*Timeline of domain registration activity.*

Coverage

	Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)	<sup>2</sup>
		N/A	N/A		
	Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)	
					

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#). <sup>3</sup>

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#). <sup>4</sup>

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat. <sup>5</sup>

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device. <sup>6</sup>

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products. <sup>7</sup>

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#). <sup>8</sup>

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them. <sup>9</sup>

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center. <sup>10</sup>

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network. <sup>11</sup>

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#). <sup>12</sup>

Talos created the following coverage for this: <sup>13</sup>

Snort SIDs: <sup>14</sup>

Snort 3: 300480,300481 <sup>15</sup>

Snort 2: 61550-61553



## Orbital Queries<sup>1</sup>

Cisco Secure Endpoint users can use [Orbital Advanced Search](#) to run complex OSqueries to see if <sup>2</sup> their endpoints are infected with this specific threat. For specific OSqueries on this threat, Cisco Secure Endpoint customers need to make sure that "%3CX%" is entered into the program field under the "Installed Program Search" for Windows and ".\*3CX.\*" under "Installed Applications Monitoring" for MacOS in Orbital.

Additionally, the users can access the OSqueries directly on GitHub for both [Windows](#) and <sup>3</sup> [MacOS](#).

## Indicators of Compromise (IOCs)<sup>4</sup>

Indicators of compromise (IOCs) associated with ongoing activity can be found [here](#).<sup>5</sup>

---

SHARE THIS POST



---

### RELATED CONTENT

ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices<sup>6</sup>

APRIL 24, 2024 11:54<sup>7</sup>

ArcaneDoor is a campaign that is the latest example of state-sponsored actors targeting perimeter <sup>8</sup> network devices from multiple vendors. Coveted by these actors, perimeter network devices are the



perfect intrusion point for espionage-focused campaigns. 1

Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials 2

APRIL 16, 2024 08:00 3

Cisco Talos would like to acknowledge Anna Bennett and Brandon White of Cisco Talos and Phillip Schafer, Mike Moran, and Becca Lynch of the Duo Security Research team for their research that led to the identification of these attacks. Cisco Talos is actively monitoring a global increase in brute-force attacks 4

Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities 5

OCTOBER 16, 2023 11:05 6

Cisco has identified active exploitation of two previously unknown vulnerabilities in the Web User Interface (Web UI) feature of Cisco IOS XE software — CVE-2023-20198 and CVE-2023-20273 — when exposed to the internet or untrusted networks. 7

INTELLIGENCE CENTER

Intelligence Search 10

Email & Spam Trends

VULNERABILITY RESEARCH 13

Vulnerability Reports 14

Microsoft Advisories

INCIDENT RESPONSE 8

Reactive Services 11

Proactive Services

Emergency Support

SECURITY RESOURCES 15

Open Source Security Tools 16

Intelligence Categories Reference

Secure Endpoint Naming Reference

MEDIA 9

Talos Intelligence Blog 12

Threat Source Newsletter

Beers with Talos Podcast

Talos Takes Podcast

Talos Videos

SUPPORT 17

Support Documentation

COMPANY

About Talos

Careers

Cisco Security

FOLLOW US



© 2025 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our [Privacy Policy](#).<sup>2</sup>