← Blog

Ivan Pisarev
Technical Head, META

Victor Belov
Senior Malware Analyst

36gate: supply chain attack

What is known about the 3CX supply chain incident and how to defend against it?

March 31, 2023 · min to read · Threat Landscape Overview

3CX Malware analysis Managed XDR Threat Intelligence

What is known so far?

On the 29th of March, 2023 SentinelOne, Crowdstrike, and IBM Sophos reported malicious activity of a trojanized version of the **3CX Desktop App**, a client used to make VoIP calls.

One day later, on March 30th, it was found that the malicious application was not specially crafted, but was in fact legitimate software published and signed by a certificate belonging to 3CX, a phone system software provider, whose customers include Wilson, Mercedes-Benz, Coca Cola, and many other large enterprises, according to the company's website. The full consequences of this supply chain incident are yet to be seen.

That same day, the company's CEO issued an advisory and recommended using 3CX's PAW client until a new build is released:

As part of the attack, the malicious installer deploys legitimate software with malicious libraries. Once the application is launched, a malicious code sleeps and then attempts to download and execute a payload. The payload is unknown at the moment.

According to the 3CX statement, the malicious code was injected via a library: “The issue appears to be one of the bundled libraries that we compiled into the Windows Electron App via GIT”.

If you are using 3CX VoIP in your organisation, it is recommended to check your infrastructure immediately for the signs of intrusion and take the appropriate mitigation measures described in this blog post.

Technical analysis

According to the most recent 3CX statement, versions 18.12.407 & 18.12.416 of its Electron Windows App and versions 18.11.1213, 18.12.402, 18.12.407 & 18.12.416 of the Electron Mac App have been infected.

The following samples, obtained via VirusTotal, were analyzed by Group-IB Threat Intelligence team:

3CXDesktopApp-18.12.416.dmg
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec

3CXDesktopApp-18.12.416.msi
59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983

As it has been discovered, the Windows installer deploys **ffmpeg.dll** signed by **3CX Ltd** with a valid digital signature:

The **DllEntryPoint** leads to the main malicious function, which is responsible for reading the **d3dcompiler_47.dll** file that has to be located in the same directory as the executable file. This file contains an encrypted shellcode responsible for unpacking and executing the next stage, which is a downloader. It is important to note, that before extracting the shellcode the infected DLL creates an event with the name **AVMonitorRefreshEvent**. The shellcode itself is located in the second DLL after **FEEDFACE** bytes:

The code that searches for the start of the shellcode

The encrypted version of the shellcode in d3dcompiler_47.dll

It is worth noting that **d3dcompiler_47.dll** also has a digital signature, but it is non-valid in this case:

The shellcode decryption key is **3jB(2bsG#@c7**. The goal of the shellcode is to load an embedded payload, which is a downloader. The first stage, **ffmpeg.dll**, also passes the following arguments to the next stage:

```
1200 2400 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
```

The downloader is also a DLL file with one export function: **DllGetClassObject** — it contains all malicious functionality (DllEntryPoint does not perform any activity). First of all, the downloader attempts to open the **manifest** file which contains 4 bytes representing the time in seconds when the application should launch. This time is generated using the following method:

sleep_time = rand() % 1800000 + first_running_time + 604800;

It is important to note that the range of the rand() function in this case is [0;32767], so the application maximum sleep time is 7.4 days. The file will be created during the first run of the application.

The C2 list is located in .ico-files that are available at: **hxxps://raw.githubusercontent[.]com/IconStorages/images/main/icon[1;15].ico**. At the time of writing, this GitHub repository was unavailable, however, we managed to find a VirusTotal archive and found this repository in the Wayback machine:

Because of the logic implemented in the downloader, the icon0.ico will never be used. It is possible that the threat actor used this .ico-file during the testing:

for (i = rand() % 15 + 1; ; i = 0)

The archive itself contains the following images:

Each image contains C2, encoded in base64 and encrypted:

The encoded data is preceded by the **$** Symbol. The Group-IB Threat Intelligence team managed to decrypt the .ico-files:

Icon name	SHA1	C2
icon1.ico	96910a3dbc194a7bf9a452afe8a35eceb904b6e4	hxxps://msstorageazure[.]com/wind
icon2.ico	ffccc3a29d1582989430e9b6c6d2bff1e3a3bb14	hxxps://officestoragebox[.]com/api/
icon3.ico	89827af650640c7042077be64dc643230d1f7482	hxxps://visualstudiofactory[.]com/w
icon4.ico	b5de30a83084d6f27d902b96dd12e15c77d1f90b	hxxps://azuredeploystore[.]com/clo

icon5.ico	3992dbe9e0b23e0d4ca487faffeb004bcfe9ecc8	hxxps://msstorageboxes[.]com/offic
icon6.ico	caa77bcd0a1a6629ba1f3ce8d1fc5451d83d0352	hxxps://officeaddons[.]com/techno
icon7.ico	57a9f3d5d1592a0769886493f566930d8f32a0fc	hxxps://sourceslabs[.]com/downloa

Also the repository contained a file named **web.pack**, but its purpose is unknown. We suppose that this file is encrypted and could be used in a kill chain.

The sequence of bytes highlighted above appears frequently in the file, but it hasn't been encrypted at the time of writing.

One of the notable features of the downloader is how it fills a header of the request:

```
accept: */*
accept-language: en-US,en;q=0.9
accept-encoding: gzip, deflate, br
content-type: text/plain
```

And it can also optionally add the cookie field:

cookie: %data%=%data%

A payload will be executed in the context of the infected process.

Malicious 3CX app for MacOS

Compared to the Windows version of the 3CX app, its Mac OS version has a slightly different logic. The application contains libffmpeg.dylib with two sublibs inside: for arm64 and x86_64 code. The malicious code is implemented under _run_avcodec() which can be found only in x86_64 sublib. ARM64 version doesn't contain the malicious code. URLs of the next stage are hardcoded into the library XORed with 0x7A.

The following headers are used when sending requests to C2:
z3cx_auth_id=%s;3cx_auth_token_content=%s;__tutma=true

C2s of the MacOS version:

- 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
- msedgepackageinfo[.]com/ms-webview
- glcloudservice[.]com/v1/status
- pbxsources[.]com/queue

Domain	Registrar	Date
msstorageazure[.]com	NAMECHEAP	2022-11-17
officestoragebox[.]com	NAMECHEAP	2022-11-17
visualstudiofactory[.]com	NAMECHEAP	2022-11-17

azuredeploystore[.]com	NameSilo	2022-12-07
msstorageboxes[.]com	NAMECHEAP	2022-12-09
officeaddons[.]com	PublicDomainRegistry.com	2022-12-09
sourceslabs[.]com	ENOM	2022-12-09
zacharryblogs[.]com	NAMECHEAP	2022-12-13

Crowdstrike and other cybersecurity companies reported additional domain names, but we cannot confirm their usage.

At the moment of writing, Group-IB didn't find or retrieve the payload.

Am I in danger? The to do list

According to the 3CX security alert Electron Windows App versions numbers 18.12.407 & 18.12.416 and Electron Mac App version numbers 18.11.1213, 18.12.402, 18.12.407 & 18.12.416 are malicious. MITRE has assigned the CVE-2023-29059 identifier to the supply chain attack and linked it to the CWE-506 weakness described as 'Embedded Malicious Code.'

Recommendations for 3CX customers:

1. Identify any employees using affected versions of the 3CX app
2. Ensure you have the latest update installed. The updated version 18.12.422 of the Windows desktop app and the Mac desktop app has been released by 3CX.

If your employees have used the desktop app, the best option is to uninstall the software (the detailed guide can be found here). Incident response should be conducted in order to identify malicious activities and proper remediation should be carried out.

You can follow these simple steps to understand if a compromised version of the 3CX application is/was present in your infrastructure to identify malicious activity:

1. Check for the presence of files that match the hashes provided in the IoC section.

2. If you have an [EMX]DR solution, search for connections to the identified URLs and domain names.
   Sigma and YARA rules also can be used for DNS event searching.
3. On MacOS check for .session-lock , .main-storage and UpdateAgent files. Presence of such files in the 3CX application directory with high probability indicates that the second stage of malware was executed. You can use simple bash script suggested by anschluss.

```
for f in $(find /Users -type d -maxdepth 1 -mindepth 1); \
do \
  test -d $f/Library/Application\ Support/3CX\ Desktop\ App && echo "$f: found 3CX app us
  test -f $f/Library/Application\ Support/3CX\ Desktop\ App/UpdateAgent && echo "$f: foun
  test -f $f/Library/Application\ Support/3CX\ Desktop\ App/.main_storage && echo "$f: fo
  test -f $f/Library/Application\ Support/3CX\ Desktop\ App/.session-locks && echo "$f: f
done
```

4. You can use YARA rules by Florian Roth to search for malicious signs.
5. In order to perform threat hunting if you don't have automated detections implemented, you can utilize your EDR telemetry to search for the following traces:

look for DLL loading events by 3CXDesktopApp (ffmpeg.dll and d3dcompiler_47.dll are known to be trojanized, but other yet unknown DLL names may be considered); test found files against Virustotal or aforementioned yara rules;

look for DNS events produced by 3CXDesktopApp; it is currently known that the payload connects to github.com, but any other cloud-based service should be considered as being abused by the threat actor for the same goal;

monitor for hands-on attacker's activity; expect basic reconnaissance commands executed by 3CXDesktopApp seen in process creation telemetry and files created by 3CXDesktopApp in file creation telemetry;

monitor for hands-on attacker's activity; expect basic reconnaissance commands executed by 3CXDesktopApp seen in process creation telemetry and files created by 3CXDesktopApp in file creation telemetry.

Attribution

HTTPS beacon structure and encryption key match those observed by CrowdStrike in a March 7, 2023 campaign attributed with high confidence to DPRK-nexus threat actor LABYRINTH CHOLLIMA (aka Lazarus) — CrowdStrike reports.

According to Sophos researchers, they “cannot verify this attribution with a high degree of certainty.” Volexity has described the second stage of the payload. However they mentioned that they cannot currently map the disclosed activity to any threat actor, so it will be tracked under UTA0040.

The Twitter thread also reveals some similarities with the activity of North Korean threat actors, however the pieces of evidence are still not strong enough to confirm the link.

Group-IB researchers also do not yet see obvious links with existing threat clusters. We will provide an update if more information becomes available.

How Group-IB technologies can help

Group-IB Managed Extended Detection and Response (MXDR) detects and automatically blocks malicious 3CX executables as of March 30, 2023. Below you can find how Group-IB’s Malware Detonation Platform (part of MXDR) detects this threat:

1. The alerts triggered during an analysis in Group-IB Malware Detonation Platform

Group-IB EDR solution is capable of providing comprehensive telemetry data that can be used to search for trojanized DLL files:

For organisations that have a mature cybersecurity program, we suggest taking a closer look at our **Threat Intelligence** solution.

Threat description available to the users of Group-IB Threat Intelligence platform

Indicators of compromise

Below you can find a list of Indicators of compromise linked to the 3CX supply chain incident, collected by Group-IB Threat Intelligence unit and other industry researchers. This section will be constantly updated as new data becomes available.

FS objects

event “AVMonitorRefreshEvent”

~/Library/Application Support/3CX Desktop App/UpdateAgent
~/Library/Application Support/3CX Desktop App/.main_storage
~/Library/Application Support/3CX Desktop App/.session-locks

MD5	SHA1	S
ca8c0385ce2b8bdd19423c8b98a5924b	**f3487a1324f4c11b35504751a5527bc60eb95382**	I
27b134af30f4a86f177db2f2555fe01d	**188754814b37927badc988b45b7c7f7d6b4c8dd3**	c
5729fb29e3a7a90d2528e3357bd15a4b	**19f4036f5cd91c5fc411afc4359e32f90caddaac**	5
d5101c3b86d973a848ab7ed79cd11e5a	**3dc840d32ce86cebf657b17cef62814646ba8e98**	c
0eeb1c0133eb4d571178b2d9d14ce3e9	**bfecb8ce89a312d2ef4afc64a63847ae11c6f69e**	5
3703770e32820397c6e7e1e1221e6d0d	**5d833bcc679db38a45111269e727ec58b75c8d31**	9
2fdf61fdfd649f8bbf5730307a0ab5d1	**b2a89eebb5be61939f5458a024c929b169b4dc85**	1
bb915073385dd16a846dfa318afa3c19	**6285ffb5f98d35cd98e78d48b63a05af6e4e4dea**	c
9833a4779b69b38e3e51f04e395674c6	**8433a94aedb6380ac8d4610af643fb0e5220c5cb**	1

Bold hashes indicate that they were observed in our analysis, other files were taken from reports Volexity, SentinelOne and @dodo_sec.

Network indicators

Bold domains indicate that they were observed in our analysis, other files were taken from reports Volexity, SentinelOne and CrowdStrike.

msstorageazure[.]com/window
officestoragebox[.]com/api/session
visualstudiofactory[.]com/workload
azuredeploystore[.]com/cloud/services
msstorageboxes[.]com/office
officeaddons[.]com/technologies
sourceslabs[.]com/downloads
zacharryblogs[.]com/feed
pbxcloudeservices[.]com/phonesystem
akamaitechcloudservices[.]com/v2/storage
azureonlinestorage[.]com/azure/storage
msedgepackageinfo[.]com/microsoft-edge
glcloudservice[.]com/v1/console
pbxsources[.]com/exchange
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
sbmsa[.]wiki/blog/_insert
www.journalide[.]org
dunamistrd[.]com
azureonlinecloud[.]com
akamaicontainer[.]com
qwepoi123098[.]com

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Contact

Subscription plans

Services

Resource Center

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends