3CX: Supply Chain Attack Affects Thousands of Users Worldwide

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3cx-supply-chain-attack

Threat Hunter TeamSymantec

UPDATE March 31 2023 14:26 UTC: *Our blog has been updated with a Yara rule to detect the final infostealer payload.*

UPDATE March 30 2023 17:39 UTC: *Our blog has been updated with technical analysis of the macOS versions.*

UPDATE March 30 2023 14:17 UTC: *Our blog has been updated with additional IOCs*

UPDATE March 30 2023 12:47 UTC: *Our blog has been updated with additional IOCs and protection information.*

UPDATE March 30 2023 9:07 UTC: *Our blog has been updated with technical analysis of the malware used.*

Attackers believed to be linked to North Korea have Trojanized 3CX's DesktopApp, a widely-used voice and video calling desktop client. In an attack reminiscent of SolarWinds, installers for several recent Windows and Mac versions of the software were compromised and modified by the attackers in order to deliver additional information stealing malware to the user's computer. The information gathered by this malware presumably allowed the attackers to gauge if the victim was a candidate for further compromise.

Attack chain

The attackers compromised installer files for at least two Windows versions (18.12.407 and 18.12.416) and two Mac versions (8.11.1213 and latest) of 3CX DesktopApp. The installers contained clean versions of the app along with malicious DLLs. The app was used to sideload the malicious DLLs, which then installed information-stealing malware on the computer.

In two variants analyzed by Symantec (SHA256: aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868 and 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983), the clean executable was used to load a malicious DLL named ffmpeg.dll (SHA256: 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896)

This DLL contains code that will load and execute a payload from a second DLL named d3dcompiler_47.dll. (SHA256: 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03)

D3dcompiler_47.dll contains an encrypted blob appended to the file, suggesting that it is possibly a Trojanized version of a legitimate file. The blob starts with the hex value "FEEDFACE" which the loader uses to find the blob. The decrypted blob contains shellcode and a third DLL (SHA256: aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973).

The shellcode loads and executes this third DLL, export DLLGetClassObject with parameters:

- 1200 2400 "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"

It will then attempt to download an ICO file from the following GitHub repository:

> https://raw.githubusercontent[].com/IconStorages/images/main/icon%d.ico

Mac versions

At last two macOS versions of the affected software were compromised in a similar fashion. In this case a dynamic library named libffmpeg.dylib was Trojanized. There are at least two variants of this file (SHA256: a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67 and fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7) and they seem to relate to different versions of the software.

The malicious code is in the InitFunc_0 function of libffmpeg.dylib, it calls _run_avcodec which starts a thread, in this thread it decodes some shellcode with XOR key 0x7A and then will make a http request.

It attempts to download a payload from:

- URL: https://msstorageazure[.]com/analysis
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.128 Safari/537.36

The following URLs were embedded in analyzed variants:

- 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

Mitigation

3CX is aware of the compromise and is advising users to immediately uninstall the app. It said that it is working on an update to the software that will be released within hours. It advised users to consider using its PWA client as an alternative until a clean version of DesktopApp is released.

Protection

File-based

- Infostealer
- Trojan Horse
- Trojan.Dropper
- Trojan.Malfilter
- WS.Malware.2
- OSX.Samsis
- Trojan.Samsis

Machine Learning-based

- Heur.AdvML.A
- Heur.AdvML.B

Network-based

- Malicious Site: Malicious Domains Request
- Malicious Site: Malicious Domain Request 59
- Web Attack: WebPulse Bad Reputation Domain Request

For the latest protection updates, please visit the Symantec Protection Bulletin.

Yara Rule to detect final infostealer payload

```
rule icon_3cx_stealer {

    meta:

        copyright = "Symantec"

        description = "Infostealer component used in 3CX supply chain attack"

    strings:

        $a1 = "******************************** %s ********************************" wide fullword

        $a2 = "\\3CXDesktopApp\\config.json" wide fullword

        $a3 = { 7B 00 22 00 48 00 6F 00 73 00 74 00 4E 00 61 00 6D 00 65 00 22 00 3A 00 20 00 22 00 25 00 73 00 22 00 2C 00 20 00 22 00 44 00 6F 00 6D 00 61 00 69 00 6E 00 4E 00 61 00 6D 00 65 00 22 00 3A 00 20 00 22 00 25 00 73 00 22 00 2C 00 20 00 22 00 4F 00 73 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 22 00 3A 00 20 00 22 00 25 00 64 00 2E 00 25 00 64 00 2E 00 25 00 64 00 22 00 7D }

        $b1 = "HostName: %s" wide fullword

        $b2 = "DomainName: %s" wide fullword
```

```
        $b3 = "OsVersion: %d.%d.%d" wide fullword

        $b4 = "%s.old" wide fullword

    condition:

        3 of ($a*) and 2 of ($b*)

}
```

For more information on scanning SEP client computers using custom Yara rules, read this knowledge base article.

Indicators of Compromise

dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc – Windows app

aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868 – Windows installer

fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405 – Windows app

59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983 – Windows installer

92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61 – macOS app

5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290 – macOS installer

b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb – macOS app

e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec – macOS installer

11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03 – Infostealer (d3dcompiler_47.dll)

7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896 - Infostealer (ffmpeg.dll)

aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973 - Infostealer

c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02 - Infostealer (ffmpeg.dll)

fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7 - Malicious macOS library (libffmpeg.dylib)

a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67 - Malicious macOS library (libffmpeg.dylib)

210c9882eba94198274ebc787fe8c88311af24932832a7fe1f1ca0261f815c3d – Malicious ICO file (icon0.ico)

a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c – Malicious ICO file (icon1.ico)

d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090 – Malicious ICO file (icon10.ico)

d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090 – Malicious ICO file (icon11.ico)

d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a – Malicious ICO file (icon12.ico)

4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f – Malicious ICO file (icon13.ico)

8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d – Malicious ICO file (icon14.ico)

f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3 – Malicious ICO file (icon15.ico)

2c9957ea04d033d68b769f333a48e228c32bcf26bd98e51310efd48e80c1789f – Malicious ICO file (icon2.ico)

268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca – Malicious ICO file (icon3.ico)

c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd – Malicious ICO file (icon4.ico)

c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396 – Malicious ICO file (icon5.ico)

f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182 – Malicious ICO file (icon6.ico)

2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de – Malicious ICO file (icon7.ico)

e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c – Malicious ICO file (icon8.ico)

d0f1984b4fe896d0024533510ce22d71e05b20bad74d53fae158dc752a65782e – Malicious ICO file (icon9.ico)

akamaicontainer[.]com
akamaitechcloudservices[.]com
azuredeploystore[.]com
azureonlinecloud[.]com
azureonlinestorage[.]com
dunamistrd[.]com
glcloudservice[.]com
journalide[.]org
msedgepackageinfo[.]com
msstorageazure[.]com
msstorageboxes[.]com
officeaddons[.]com
officestoragebox[.]com
pbxcloudeservices[.]com
pbxphonenetwork[.]com
pbxsources[.]com
qwepoi123098[.]com
sbmsa[.]wiki
sourceslabs[.]com
visualstudiofactory[.]com
zacharryblogs[.]com
raw.githubusercontent[.]com/IconStorages/images/main/

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.