A Comprehensive Analysis of the 3CX Attack

blog.cyble.com/2023/03/31/a-comprehensive-analysis-of-the-3cx-attack

March 31, 2023



InfoStealer Deployed in a Massive Supply Chain Attack

An ongoing supply chain attack has been <u>reported</u>, targeting customers of 3CX, a VoIP IPBX software development company. This attack has been attributed to North Korean Threat Actors (TAs). Currently, the 3CX DesktopApp can be accessed on various platforms, including Windows, macOS, Linux, and mobile.

However, reports have indicated that the ongoing activity related to the supply chain attack has been detected on both Windows and macOS operating systems. The attack involves a Trojanized version of the 3CX, a Voice Over Internet Protocol (VOIP) desktop client, which has been digitally signed. 3CX's Phone System is utilized by over 600,000 companies globally and has over 12 million daily users.

The highlights of the incident are as follows:

- On March 29, a significant number of EDR providers and antivirus solutions began to identify and signal a warning for the legitimate 3CXDesktopApp.exe binary, which was signed.
- This binary had initiated an update procedure that ultimately led to malicious activity and communication with Command-and-Control servers.
- The 3CX download that was accessible on the official public website was infected with malware. Systems that had already been installed would undergo updates that would ultimately result in the download of this malware.
- The attack involves a multi-stage process that starts with the 3CX desktop application.
- The process of retrieving malicious payloads from GitHub involves a delay of 7 days before the download takes place. This delay could be an attempt to evade detection by security systems monitoring suspicious activities.

- As per reports, the last stage of the attack involves stealing information. This malware can gather system data and take control of data and login credentials stored in user profiles on various web browsers, including Chrome, Edge, Brave, and Firefox.
- Both the Windows and macOS installers for 3CX have been impacted.
- As per researchers, the evidence from GitHub indicates that the infrastructure utilized by the Windows variant was activated on December 7, 2022.
- Additionally, the domains and web infrastructure utilized in the attacks were registered as early as November 2022.

The 3CX Phone Management System can be implemented on-premises. Upon further investigation, we found that over 240,000 publicly exposed instances of this application.

8 Shodan	Explore	Downloads	Pricing 2	http.title:"3CX Phone Sy	/stem Management Console"
TOTAL RESULTS 244,282			錙 View Report 〔 Partner Spotlig	即 View on Map ht: Looking for a place to	o store all the Shodan data? Check out Gravwell
TOP COUNTRIES			> 3CX Phone Sy	ystem Management	Console 🗹
			Amazon Data Services Canada	SSL Certificate Issued By: I- Common Name: R3 I- Organization: Let's Encrypt Issued To:	HTTP/1.1 200 OK Server: nginx Date: Fri, 31 Mar 2023 05:05:55 GMT Content-Type: text/html Content-Length: 957 Last-Modified: Wed, 15 Mar 2023 11:12:40 GMT Connection: keep-alive ETag: "6411a828-3bd"
United States	52,847		cloud	- Common Name: creationsmicroweb.3cx.ca	X-Frame-Options: DENY
Germany	37,887			Supported SSL	X-XSS-Protection: 0
France	24,579			Versions: TLSv1.2	Content-Secur
United Kingdom	22,090				
Australia	20,922				

The figure below shows the Shodan search results.

Figure 1 – Exposed Instances

We also came across a Reddit post where a user reported suspicious activity that occurred after updating the 3CX desktop on March 24, 2023. According to the user, the 3cxdesktopapp.exe program accessed browser caches, as revealed by EDR file history data.

8	ruffy91 🎱 - 5 hr. ago	r/F
	I have an affected endpoint where 3cxdesktopapp.exe accessed Edge, Brave, IE, Firefox browser caches according to file history data from our EDR and also connected to the IoC domains.	Do you your d 2 93
	The behavior started seconds after the update (on 24.3.2023 06:32 UTC) to v18.12.407 and did not reoccur until the next update. This behavior never occured before so I have to assume that the malware also steals information from browsers (cache, sessions, history?)	≥ r/F I just intera

Figure 2 – Reddit Post

According to 3CX, the recent attack was a result of infected bundled libraries that were compiled into the Windows Electron App through GIT. The vendor has also stated, "Electron Windows App shipped in Update 7, version numbers 18.12.407 & 18.12.416, includes a security issue. Anti-Virus vendors have flagged the executable 3CXDesktopApp.exe and in many cases uninstalled it. Electron Mac App version numbers 18.11.1213, 18.12.402, 18.12.407 & 18.12.416 are also affected."

The .msi file, when executed, drops two malicious files – "ffmpeg.dll" and "d3dcompiler_47.dll" – in the location *C:\Users[user_name]\AppData\Local\Programs\3CXDesktopApp\app*.

The infection begins when the benign file "3CXDesktopApp.exe" loads "ffmpeg.dll". Then, "ffmpeg.dll" decrypts the encrypted code from "d3dcompiler_47.dll", which seems to be a shellcode.

This shellcode loads another DLL file that tries to access the IconStorages GitHub page to find an .ico file containing the encrypted Command-and-Control (C&C) server. After locating the C&C server, the backdoor establishes a connection to retrieve the potential final payload.

The figure below shows the infection flow.



Figure 3 – Infection chain

Technical Analysis

The MSI package installer that has been compromised has a digital signature, and its appearance resembles that of a legitimate file, as shown below.

Compatibility ner: Digest sha1 ignature Detai Advanced Digital Sig	Digital S algorithm	ignatures Timestamp 3 March 2023 07	Security :34 ?	×	
ignature Detai	algorithm 1 1 Is nature Inform	îmestamp 3 March 2023 07	:34	×	
ignature Detai	algorithm 1	Timestamp 3 March 2023 07	:34	×	
sha1 ignature Detai Advanced Digital Sig	ls nature Inform	3 March 2023 07	:34 ?	×	
ignature Detai Advanced Digital Sig	s nature Inform		?	×	4
Advanced	nature Inform				
Digital Sig	nature Inform				
This digital s		nation			
	ignature is OK.				
er information				_	Figure 4 – Digitally signed N
me:	3CX Ltd			- 1	
ail:	webmaster @	Sex com		- 1	
ning time:	ha the state	2022404		_	
ing one.	13 March 202	3 07:34:04			
		Vi	ew Certificate	e	
ntersignatures					
		ss: Timesta	np		
ame of signer:	Email addre				
	ner information - me: nail: gning time: untersignatures	ner information ame: 3CX Ltd nail: webmaster@3 gning time: 13 March 202 untersignatures	ner information ame: 3CX Ltd nail: webmaster@3cx.com gning time: 13 March 2023 07:34:04 Vi untersignatures	ner information ame: 3CX Ltd nail: webmaster@3cx.com gning time: 13 March 2023 07:34:04 View Certificat	ner information ame: 3CX Ltd nail: webmaster@3cx.com gning time: 13 March 2023 07:34:04 View Certificate untersignatures

installer

Upon installation, the MSI package installer drops files such as "3CXDesktopApp.exe", "ffmpeg.dll", and "d3dcompiler_47.dll" in the *%LocalAppData%* directory of the system.

%LocalAppData%\Programs\3CXDesktopApp\app\

These files are associated with malicious behavior and are accompanied by other supporting files.

The figure below displays the directory where the "3CXDesktopApp" application has been installed.

» AppData » Local » Programs » 3CXDesktopApp » app						
Name	Date modified	Туре	Size			
	30-03-2023 14:56	File folder				
resources	30-03-2023 14:56	File folder				
🗠 3CXDesktopApp.exe	13-03-2023 07:32	Application	1,45,770 KB			
3CXDesktopApp.VisualElementsManifest	13-03-2023 07:25	XML Document	1 KB			
chrome_100_percent.pak	13-03-2023 07:31	PAK File	126 KB			
chrome_200_percent.pak	13-03-2023 07:31	PAK File	175 KB			
📓 d3dcompiler_47.dll	13-03-2023 07:31	Application exten	5,048 KB			
📓 ffmpeg.dll	13-03-2023 07:31	Application exten	2,749 KB			
icudtl.dat	13-03-2023 07:31	DAT File	10,161 KB			
🗟 libEGL.dll	13-03-2023 07:31	Application exten	460 KB			
IibGLESv2.dll	13-03-2023 07:31	Application exten	7,011 KB			
	13-03-2023 07:31	File	2 KB			
🤯 LICENSES.chromium.html	13-03-2023 07:31	Brave HTML Docu	5,233 KB			
📄 manifest	30-03-2023 14:56	File	1 KB			
resources.pak	13-03-2023 07:31	PAK File	5,022 KB			
snapshot_blob.bin	13-03-2023 07:31	BIN File	398 KB			
💶 Update.exe	13-03-2023 07:25	Application	1,908 KB			
v8_context_snapshot.bin	13-03-2023 07:31	BIN File	714 KB			
version	13-03-2023 07:31	File	1 KB			
🚳 vk_swiftshader.dll	13-03-2023 07:31	Application exten	4,648 KB			
vk_swiftshader_icd.json	13-03-2023 07:31	JSON File	1 KB			
🚳 vulkan-1.dll	13-03-2023 07:31	Application exten	855 KB			

Figure 5 – 3CXDesktop installation folder

After installation, the "3CXDesktopApp.exe" file is executed, which is usually benign but can be utilized to load the malicious DLL, as shown below.

CX 3CXDesktopApp.exe		Handle or DLL substring:	ffmpe	eg.dl	
CX 3CXDesktopApp.exe		Process	PID	Туре	Name
acx 3CXDesktopApp.exe	-	3CXDesktop.App.exe	3248	DLL	C:\Users\\\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dl
icx 3CXDesktopApp.exe		3CXDesktopApp.exe	3588	DLL	C:\Users\
		3CXDesktopApp.exe	4344	DLL	C:\Users\\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dll
	-	 3CXDesktopApp.exe 	5860	DLL	C:\Users\\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dll
CPU Image 72.55% Committe	Stands	3CXDesktopApp.exe	8364	DLL	C:\Users\\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dll
		3CXDesktopApp.exe	8704	DLL	C:\Users\

Figure 6 – 3CXDesktop.exe loading ffmpeg.dll file

The figure below illustrates the process tree of the "3CXDesktopApp" application.

msiexec.exe (1072)	Windows® installer	C:\Windows\system32\msiexec.exe /V
MsiExec.exe (1524)	Windows® installer	C:\Windows\syswow64\MsiExec.exe -Embedding 96F980CF0C8A4C18955E7372967DEA99
SCXDesktopApp.exe (7344)	3CX Desktop App	"C:\Users\Mu!W=kitati=_\AppData\Loca\\Programs\3CXDesktopApp\3CXDesktopApp.exe"
SCXDesktopApp.exe (5860)	3CX Desktop App	"C:\Users\InternationalAppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe"
CX 3CXDesktopApp.exe (8704)	3CX Desktop App	"C:\Users\Marine and AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" -type=gpu-process -user-dat
CX 3CXDesktopApp.exe (4344)	3CX Desktop App	"C:\Users\IIII and AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" -type=utility-utility-sub-type=
🖃 🌆 reg.exe (3484)	Registry Console	C:\Windows\system32\reg.exe QUERY HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v 3CXDeskTopApp
Conhost.exe (7084)	Console Window	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1
CX 3CXDesktopApp.exe (3248)	3CX Desktop App	"C:\Users\Mail_and_mail_and_AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" -type=renderer -user-data-dir
CX 3CXDesktopApp.exe (3588)	3CX Desktop App	"C:\Users\manual_AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe" -type=renderer -user-data-dir
CX 3CXDesktopApp.exe (8364)	3CX Desktop App	"C:\Users\llandstandstandstandstandstandstandstandst
CX 3CXDesktopApp.exe (4652)	3CX Desktop App	"C:\Users\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

Figure 7 – Process tree

The "3CXDesktopApp.exe" loads the "ffmpeg.dll" file, which is a malicious DLL that has been specifically designed to read, load, and execute harmful shellcode from the "d3dcompiler_47.dll" file.

When executed, the "ffmpeg.dll" creates a new event, "*AVMonitorRefreshEvent*", identifies the current file path, and searches for the next file in the sequence, which is "d3dcompiler_47.dll". Once identified, the "ffmpeg.dll" loads the "d3dcompiler_47.dll" file into memory, as illustrated in the assembly code shown below.



Figure 8 – ffmpeg.dll file is loading d3dcompiler_47.dll

Although the loaded "d3dcompiler_47.dll" is signed by Microsoft, it has an encrypted payload embedded within it. The "ffmpeg.dll" file now identifies the encrypted payload indicated by a particular marker, '0xCEFAEDFE', as shown below.



Figure 9 – Identifying encrypted payload in "d3dcompiler_47.dl"I

Once the encrypted payload has been identified, the "ffmpeg.dll" proceeds to decrypt the RC4 stream using the key "3jB(2bsG#@c7". This decryption process results in a shellcode which is then executed by the DLL file.

The figure below shows the RC4 loop and decrypted shellcode function.

0000755961125089			
00000/FF30116E083	B2 AA	MOV dl.AA	
00007EE96112E0BB	E8 802D0700	call ffmpeg.7FE9611A0E40	
0000755961125000	3100	YOF BAY BAY	
0000755961122000	48:8000 57081500	lap new gward ath der [755061210600]	0000755961218680."258(2bc6#8c7"
000077759611220022	40.000 E70BIE00	rea rex, quoru per us. [/ Probisibebuj	0000777901516660. 5]8(2050#607
00007FF96112E0C9	888404 50030000	mov byte ptr ss:[rsp+rax+350],ai	
00007FF96112E0D0	48:63D0	movsxd rdx,eax	
00007FF96112E0D3	4C:69C2 ABAAAA2A	imul r8,rdx,2AAAAAAB	
00007FF96112E0DA	4D:89C1	mov r9.r8	
00007FF96112F0DD	49:C1E9 3E	shr r9.3F	
0000755961125051	49.0168 21	shr rg 21	
0000755061125055	45:0100	add ned nod	
00007FF96112E0ES	45:0108	adu rou, rou	
00007FF96112E0E8	41:C1E0 02	sni rad,2	
00007FF96112E0EC	47:8D0440	lea r8d,qword ptr ds:[r8+r8*2]	
00007FF96112E0F0	44:29C2	sub edx,r8d	
00007FF96112E0F3	8A140A	mov dl.byte ptr ds:[rdx+rcx]	rdx+rcx*1:"\tæ 4·å"
00007FF96112E0F6	889404 50040000	mov byte ptr ss: [rsp+rax+450],d]	
00007EE96112E0ED	48: FEC0	inc rax	
0000755061125100	48:20 00010000	cmp max 100	
00007FF96112E100	48.50 00010000	chip rax,100	
00007FF96112E106	^ /5 C1	jne TTmpeg./FF96112E0C9	
00007FF96112E108	31C0	xor eax,eax	
00007FF96112E10A	31C9	xor ecx,ecx	
00007FF96112E10C	8A9404 50030000	mov dl.byte ptr ss:[rsp+rax+350]	
00007EE96112E113	0001	add cl.dl	
0000755961125115	028004 50040000	add cl byte ntr ss [rsn+ray+450]	
0000755961125116	44:058601	mourse and cl	
00007FF96112E11C	44.UFBOCI		
00007FF96112E120	46:8A8C04 500300	u mov ryb, byte ptr ss: rsp+r8+350	
00007FF96112E128	42:889404 500300	0 mov byte ptr ss: rsp+r8+350,d1	
00007FF96112E130	44:888C04 500300	0 mov byte ptr ss:[rsp+rax+350],r9b	
00007FF96112E138	48: FFC0	inc rax	
00007EE96112E13B	48:3D 00010000	cmp rax,100	
0000755961125141	A 75 C9	ine ffmned 75596112510C	
0000755961125142	REED	test ehn ehn	
00007FF96112E143	35 70	test ebp,ebp	
00007FF96112E145	*F/E /6	Jie Timpeg./FF96112E180	
<			
Jump is taken			
ffmpeg.00007FF961	12E1BD		
and the second se			
.text:00007FF9611	2E145 ffmpeg.dll:\$4E2	45 #4D545	
-000		A0	
Dump 1 Dump 1	Imp 2 Dump 3	Dump 4 Dump 5 Watch 1 [x=] Locale	2 Struct
Dump 1 Dump 1	imp 2 💭 Dump 3 🚛	Dump 4 Ump 5 🛞 Watch 1 🛛 🕬 Locals	Struct
Address	ımp 2 🕊 Dump 3 👹	Dump 4 🕮 Dump 5 💮 Watch 1 [x=] Locals	Struct
Address 000002B37682FBB0	Imp 2 Ump 3 Ump 3 Ump 3 Ump 2 Hex	Dump 4 Dump 5 🐨 Watch 1 [x=] Locals ASCII 89 C8 48 81 C1 58 06 00 00 10YI.ÈH.ÁX.	2 Struct
Address 000002837682FBB0 000002837682FBC0 000002837682FBC0 0000002837682FBC0	Jump 2 Jump 3 Jump 3<	Dump 4 Ump 5 (1) Watch 1 [x=] Locals ASCII 89 C8 48 81 C1 58 06 00 00 20 XI.AXA C0 58 3A 04 00 41 89 AA 00 20 XOT.AXA	2 Struct
Address 000002B37682FBB0 000002B37682FBC0 000002B37682FBC0	Jmp 2 Jmp 3 Jmp 3 Hex E8 00 00 00 00 59 49 BA DA F4 58 F5 49 81 DA F4 58 F5 48 56 48 F5 48 56 48 F4 58 56 48	Dump 4 Dump 5 Image: Constraint of the state of the	2 Struct
Address 000002B37682FBB0 000002B37682FBD0 000002B37682FBD0 000002B37682FBD0	Imp 2 Jump 3 Jump 3 Jump 3 Hex Imp 3 Im	Dump 4 Dump 5 Watch 1 [x=] Locals ASCII ASCII 89 C8 48 S1 C1 58 06 00 0 <td>Struct</td>	Struct
Address 000002837682F880 000002837682F8C0 000002837682F8D0 000002837682F8D0	Imp 2 Imp 2 Imp 3 Imp 3 Hex E8 00 00 00 59 49 BA DA F4 58 F5 49 81 00 00 64 89 E6 48 24 20 01 00 00 E8 24 20 100 00 00 E8 24 20 01 00 00 00 E8 24 20 01 00 00 00 E8 24 20 01 00 00 00 E8 24 20 20 20 00 00 00 E8 24 20 <th>Dump 4 Dump 5 Image: Constraint of the state of the</th> <td>Struct</td>	Dump 4 Dump 5 Image: Constraint of the state of the	Struct
Address 000002837682FB80 000002837682FBC0 000002837682FBC0 000002837682FBE0 000002837682FBE0	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Image: Constraint of the state of the	Struct
Address 00002837682F880 00002837682F8C0 00002837682F8C0 00002837682F8D0 000002837682F8D0 000002837682F8C0	Jump 2 Jump 3 Jump 3 Hex E8 00 00 00 59 49 BA DA F4 58 F5 49 81 00 00 56 48 89 E6 48 24 20 10 00 00 E8 44 89 42 20 42 84 56 57 41 54 41 55 41	Dump 4 Dump 5 Watch 1 [x=l Locals 89 C8 48 S1 C1 58 06 00 $\stackrel{6}{2}$, Y1, ÈH, ÅX, ASCII 89 C8 48 S1 C1 58 06 00 $\stackrel{6}{2}$, Y1, ÈH, ÅX, ASCII 83 E4 F0 48 83 EC 30 C7 44 , VH, æH, aðH, 10 05 00 00 04 89 F4 52 \$, è, H, ô 44 24 18 89 54 24 10 53 50 LL \$L, D\$,, T\$, \$ 56 41 57 48 83 EC 78 83 64 VWATAUAVAWH, 11	Struct
Address 000002837682F880 000002837682F800 000002837682F800 000002837682F800 000002837682F800 000002837682F800 000002837682F00	Jump 2 Jump 3 Jump 3 Hex E8 00 00 00 59 49 BA DA F4 58 F5 49 81 00 00 56 48 89 E6 48 24 20 01 00 00 00 E8 44 89 4C 24 20 4C 89 56 57 41 54 41 55 41 24 20 04 88 E9 45 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 41 54 34 54 34 34 54 34 54 34 54 34 34 54 34 54 34 54	Dump 4 Dump 5 Image: Constraint of the system of the syst	Struct
Address 00002837682F880 00002837682F8C0 00002837682F8C0 00002837682F8D0 00002837682F8D0 00002837682F8D0 00002837682FC00 00002837682FC10	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Watch 1 [x=] Locals 89 C8 48 S1 C1 58 06 00 0	Decrypted ShellCode
Address 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC10	Imp 2 Imp Dump 3 Imp Hex Imp Imp Imp Imp BA DA F4 58 F5 49 81 Imp Imp Imp 00 00 56 48 89 E6 48 89 E7 41 54 41 55 41 54 41 55 41 54 41 55 41 54 24 24 24 24 24 24 24 24 24 80 24 80 24 89 49 25 41 45 41 45 41	Dump 4 Dump 5 Watch 1 [x=] Locals 89 C8 48 C1 58 06 00	Decrypted ShellCode
Address 000002837682F880 000002837682F800 000002837682F800 000002837682F800 000002837682F800 000002837682FC00 000002837682FC10 000002837682FC10 000002837682FC20 000002837682FC30	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Image: Constraint of the state of the	Struct
Address 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC20 000002837682FC30 000002837682FC30	Imp 2 Imp Dump 3 Imp Hex Imp Imp Imp Imp BA DA F4 58 F5 49 81 Imp Imp Imp Imp 00 00 56 48 89 E6 48 E6 48 E6 48 E6 48 Imp Imp 44 89 4C 24 20 4C 89 56 57 41 54 41 55 41 54 41 55 41 S4 41 55 41 S4 42 S2 45 24 20 00 48 88 E9 45 E2 33 DB 44 89 8C 24 S9 49 F7 02 78 4C 88 S3 E5 48 89 44 24 S8 53 E5 48 89 44 24 88 S8 53 E5 48 89 44 24 88 S8 53 E5 48 89 44 24 88 S8 54 85 85 85 85 85 85 85 85 85 85 85 8	Dump 4 Dump 5 Image: Constraint of the state of the	Struct Decrypted ShellCode
Address 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC30 000002837682FC30 000002837682FC40 000002837682FC40	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Image: Constraint of the state of the	Struct
Addr ess 000002837682F880 000002837682F800 000002837682F800 000002837682F800 000002837682F800 000002837682F00 000002837682FC00 000002837682FC30 000002837682FC30 000002837682FC50 000002837682FC50	Jump 2 Jump 3 Jump 3 Hex Image: Constraint of the system of	Dump 4 Dump 5 Watch 1 [x=l Locals ASCII 89 C8 48 S1 C1 58 06 00 00 00 00 00 0. 0. YI. ÉH. ÁX. 00 00 00 0. 0. YI. ÉH. ÁX. 00 00 00 0. 0. YI. ÉH. ÁX. 00 00 00 0. 41 B9 A0 00 00 0. 0. A. 0. 0. 0. 0. A. 00 0. A. 0. 0. 0. A. 0. 0. 0. A. 0. 0. 0. A. 0. 0. 0. 0. 0. A. A. 0. 0. A. 0. 0. A. <	Struct
Addr ess 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC40 000002837682FC50 000002837682FC40 000002837682FC50 000002837682FC60 000002837682FC70	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Image: Constraint of the state of the	Struct Decrypted ShellCode
Www Dump 1 Www Dump 1 Addr ess 000002837682F880 000002837682F8C0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC10 000002837682FC20 000002837682FC20 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC50 000002837682FC50 000002837682FC50 000002837682FC30 000002837682FC30 000002837682FC30	Jump 2 Jump 3 Jump 3 Hex E8 00 00 00 59 49 BA DA F4 58 F5 49 81 00 00 56 48 89 E6 48 24 20 01 00 00 00 E8 24 20 01 00 00 E8 E4 24 20 04 41 54 15 21 24 20 04 48 BE 94 F7 02 78 4C 88 23 45 88 F0 E8 BB 04 24 24 20 86 89 04 44 24	Dump 4 Dump 5 Watch 1 [x=1 Locals 89 C8 48 S1 C1 58 06 00 00 0	Struct DCD DCA SU CD Decrypted ShellCode CD ShellCode
Addr ess 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F00 000002837682FC10 000002837682FC20 000002837682FC30 000002837682FC40 000002837682FC40 000002837682FC40 000002837682FC40 000002837682FC50 000002837682FC70 000002837682FC70 000002837682FC70 000002837682FC70 000002837682FC70 000002837682FC70 000002837682FC70	Imp 2 Imp Dump 3 Imp Hex Imp Imp Imp Imp BA DA F4 58 F5 49 81 Imp Imp Imp 00 00 56 48 89 E6 47 89 E6 48 89 E7 47 89 41 54 11 54 11 54 20 60 48 88 E9 45 E2 33 DB 44 89 BC 24 28 E3 E5 48 80 44 24 28 E3 45 42 24 28 E3 24 24 24	Dump 4 Dump 5 Image: Constraint of the state of the	Struct
Addr ess 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC30 000002837682FC40 000002837682FC50 000002837682FC50 000002837682FC70 000002837682FC30 00000000000000000000000000000000000	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Watch 1 [x=1 Locals 89 C8 48 81 C1 58 06 00 00 0	Struct
Addr ess 000002837682F880 000002837682F800 000002837682F800 000002837682F800 000002837682F800 000002837682F00 000002837682FC00 000002837682FC30 000002837682FC40 000002837682FC40 000002837682FC50 000002837682FC50 000002837682FC50 000002837682FC50 000002837682FC30 00000000000 0000000000000000000000	Imp 2 Imp Dump 3 Imp Hex 00 00 00 59 49 BA DA F4 58 F5 49 81 00 00 66 48 89 E6 48 24 20 01 00 00 00 E8 44 89 4C 24 20 4C 89 55 23 3DB 44 89 BC 24 88 E9 45 24 20 00 48 8B E9 45 E2 33 DB 44 89 BC 24 89 49 F7 02 78 4C 88 E9 45 E3 E4 88 E4 42 88 E4 44 24 30 E8 E4 E5 E4	Dump 4 Dump 5 Watch 1 [x=l Locals Solution 1 [x=l Locals Solution 2 Solutit	Struct
Addr ess 000002837682F8B0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682FC00 000002837682FC10 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC40 000002837682FC50 000002837682FC40	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Watch 1 [x=1 Locals 89 C8 48 C1 58 06 00	Decrypted ShellCode
Www Dump 1 Www Dump 1 Addr ess 000002837682F880 000002837682F8C0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F8D0 000002837682F60 000002837682F8D0 000002837682FC00 000002837682FC20 000002837682FC30 000002837682FC30 000002837682FC30 000002837682FC50 000002837682FC50 000002837682FC50 000002837682FC30 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80 000002837682FC80	Jump 2 Jump 3 Jump 3 Hex	Dump 4 Dump 5 Watch 1 [x=l Locals Solution 1 [x=l Locals Solution 2 Solutit 2 <tr< th=""><td>Struct DCD SA SU CD Decrypted ShellCode ShellCode</td></tr<>	Struct DCD SA SU CD Decrypted ShellCode ShellCode

Figure 10 – RC4 loop and decrypted shellcode

After decryption, the "ffmpeg.dll" file employs the *VirtualProtect()* function to alter the memory access permissions of the shellcode. Once the permissions have been changed, the malware proceeds to execute the payload.

An embedded DLL file is present within the decrypted shellcode, as shown in the below figure, which appears to be functioning as a loader for another PE file.

ffmpeg		1	100			bin ×	ζ.										
	Ŏ	1	2	3	4	5	6	7	8	9	А	В	С	D	E	F	0123456789ABCDEF
05A0h:	8B	9C	00	88	00	00	00	33	D2	F3	0F	7F	04	24	85	DB	💘.^3Òó\$Û
05B0h:	74	D4	48	8B	04	24	48	C1	E8	10	44	0F	B7	DO	45	85	tÔų‹.\$HÁè.D. ĐE…
05C0h:	D2	74	20	48	8B	4C	24	08	45	8B	DA	C1	CA	0D	80	39	Òt \(L\$.E‹ÚÁÊ.€9
05D0h:	61	0F	BE	01	7C	03	83	C2	E0	03	DO	48	FF	C1	49	FF	a.¾. , fÂà.ÐHÿÁIÿ
05E0h:	CB	75	E8	4D	8D	14	18	33	C9	41	8B	7A	20	49	03	F8	ËuèMSÉA∢z I.ø
05F0h:	41	39	4A	18	76	90	8B	1F	45	33	DB	48	8D	7F	04	49	A9J.v. (E3ÜHI
0600h:	03	D8	41	C1	CB	0D	0F	BE	03	48	FF	C3	44	03	D8	80	.ØAÁ˾ HÿÃD.Ø€
0610h:	7B	FF	00	75	ED	41	8D	04	13	3B	C6	74	0D	FF	C1	41	{ÿ.uíA Æt.ÿÅA
0620h:	3B	4A	18	72	D1	E9	5C	FF	FF	FF	41	8B	42	24	03	C9	;J.rŇé\ÿÿÿA <mark>_</mark> B\$.É
0630h:	49	03	C0	0F	B7	04	01	41	8B	4A	1C	C1	E0	02	48	98	I.A. · A (J. A A, H~
0640h:	49	03	C0	8B	04	01	49	03	C0	EB	02	33	C0	48	8B	5C	I.A <i.aë.3ah(\< td=""></i.aë.3ah(\<>
0650h:	24	20	48	8B	74	24	28	48	83	C4	10	5F	C3	4D	5A	90	<pre>\$ H<t\$(hfaamz.< pre=""></t\$(hfaamz.<></pre>
0660h:	00	03	00	00	00	04	00	00	00	FF	FF	00	00	B8	00	00	····.ÿÿ···,··
0670h:	00	00	00	00	00	40	00	00	00	00	00	00	00	00	00	00	@
0680h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0690h:	00	00	00	00	00	00	00	00	00	00	01	00	00	0E	1F	BA	····· ⁰
06A0h:	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	69	73	20	'.I!,.LI!This
06B0h:	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	74	20	62	program cannot b
06C0h:	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	e run in DOS mod
06D0h:	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	10	84	4A	e\$
06E0h:	79	54	E5	24	2A	54	E5	24	2A	54	E5	24	2A	87	97	27	yTá\$*Tá\$*Tá\$*‡–'
06F0h:	2B	51	E5	24	2A	87	97	21	2B	CE	E5	24	2A	87	97	20	+Qa\$*I-!+Ia\$*I-
0700h:	2B	59	E5	24	2A	36	9D	20	2B	5B	E5	24	2A	36	9D	27	+Ya\$*6. +[a\$*6.
0710h:	2B	5D	E5	24	ZA	36	9D	21	2B	70	E5	24	ZA	87	97	25	+]a\$*6.!+pa\$*I-%
0720h:	2B	59	E5	24	2A	54	E5	25	2A	23	E5	24	2A	35	9F	2D	+Ya\$*Ta%*#a\$*5Y-
0730h:	ZB	51	E5	24	ZA	35	9F	24	2B	55	E5	24	ZA	35	9F	26	+Qa\$*5Y\$+Ua\$*5Y&
0740h:	ZB	55	E5	24	ZA	52	69	63	68	54	E5	24	ZA	00	00	00	+Ua\$*Richla\$*
0750h:	00	00	00	00	00	00	00	00	00	00	00	00	00	50	45	00	PE.
0760h:	00	64	86	06	00	36	10	BE	63	00	00	00	00	00	00	00	.dl6.%C
0770h:	00	FO	00	22	20	OB	02	UE	20	00	UC	03	00	00	36	01	.0
0780h:	00	00	00	00	00	60	23	01	00	00	10	00	00	00	00	00	· · · · · # · · · · · · · · ·

Figure 11 – Embedded DLL file inside Shellcode

After being loaded and executed, the embedded DLL file in the shellcode initiates a sleep state of 7 days before trying to establish communication with Command and Control (C&C) servers. Subsequently, the DLL will attempt to access a GitHub repository that contains an .ICO file.

T distant	- C:\Users\
561	And it hands the test in the second second in these of second sec
00058550	CONOTIDS
00059EDD	ChainingModeGCM
00059EFD	ChainingMode
0005AF9D	POST
0005B04D	Software\Microsoft\Cryptography
0005B09D	manifest
0005B0CD	https://raw.githubusercontent.com/IconStorages/images/main/icon%d.ico

Figure 12 – Hardcoded GitHub link to download the .ICO file

This ICO file comprises the encrypted C&C strings, which are encoded using Base64 and encrypted with AES & GCM encryption. The Base64 contents are located at the end of the ICO image file, as shown below.



Figure 13 – Base64-encoded string at the end of ICO file

Upon execution, the DLL file decrypts the C&C URLs from the ICO files for downloading additional payloads from the remote server. To obtain distinct C&C URLs, the malware randomly selects an ICO file from a GitHub repository. Unfortunately, we were unable to verify the specific characteristics of these payloads as the corresponding GitHub repository was taken down prior to this analysis.

Researchers discovered that the final stage of malware is a stealer, which can extract system information and steal sensitive information from popular web browsers, such as Chrome, Edge, Brave, and Firefox.

Conclusion

The potential damage caused by the 3CXDesktopApp supply chain attack is significant, including the theft of sensitive user data. Organizations affected by this attack should immediately take steps to prevent it from causing widespread harm. The current investigation suggests that the threat actor behind this attack is skilled and persistent.

The consequences of such an attack, such as financial loss, reputational impact, and the loss of customer trust, are severe. It is crucial that organizations remain vigilant and take proactive measures to secure their supply chains to prevent similar attacks in the future.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Thoroughly investigate all systems to determine the scope and extent of the attack, including identifying all affected systems and data.
- Conduct regular security audits of your supply chain to ensure that all third-party software and components are trustworthy and secure.
- Monitor your network regularly for any suspicious activity or behavior indicating a security breach, such as unauthorized access attempts or data exfiltration.
- Stay up-to-date with the latest threat intelligence and security news to stay informed about emerging threats and vulnerabilities. This will help to mitigate risks proactively and respond quickly in the event of an attack.

- Using a reputed antivirus and internet security software package is recommended on connected devices, including PCs, laptops, and mobile devices.
- Block URLs that could be leveraged to spread malware.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	<u>T1195</u>	Supply Chain Compromise
Execution	<u>T1204.002</u>	User Execution: Malicious File
Defense Evasion	<u>T1140</u> <u>T1027</u> <u>T1574.002</u> T1497.003	Deobfuscate/Decode Files or Information Obfuscated Files or Information Hijack Execution Flow: DLL Side-Loading Virtualization/Sandbox Evasion: Time-Based Evasion
Credential Access	<u>T1555</u> <u>T1539</u>	Credentials from Password Stores Steal Web Session Cookie
Command and Control	<u>T1071</u>	Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
f3d4144860ca10ba60f7ef4d176cc736 bea77d1e59cf18dce22ad9a2fad52948fd7a9efa aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	MD5 SHA1 SHA256	3CX Windows Installer
0eeb1c0133eb4d571178b2d9d14ce3e9 bfecb8ce89a312d2ef4afc64a63847ae11c6f69e 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983	MD5 SHA1 SHA256	3CX Windows Installer
5729fb29e3a7a90d2528e3357bd15a4b 19f4036f5cd91c5fc411afc4359e32f90caddaac 5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	MD5 SHA1 SHA256	3CX macOS Installer File
d5101c3b86d973a848ab7ed79cd11e5a 3dc840d32ce86cebf657b17cef62814646ba8e98 e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	MD5 SHA1 SHA256	3CX macOS Installer File
82187ad3f0c6c225e2fba0c867280cc9 20d554a80d759c50d6537dd7097fed84dd258b3e 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03	MD5 SHA1 SHA256	Malicious DLL
74bc2d0b6680faa1a5a76b27e5479cbc bf939c9c261d27ee7bb92325cc588624fca75429 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896	MD5 SHA1 SHA256	Malicious DLL
cad1120d91b812acafef7175f949dd1b09c6c21a	SHA1	Stealer Payload

akamaicontainer[.]com akamaitechcloudservices[.]com azuredeploystore[.]com azureonlinecloud[.]com dunamistrd[.]com glcloudservice[.]com journalide[.]org msedgepackageinfo[.]com msstorageazure[.]com officeaddons[.]com officeaddons[.]com officestoragebox[.]com pbxcloudeservices[.]com pbxcloudeservices[.]com pbxsources[.]com gltub[.]com visualstudiofactory[.]com zacharryblogs[.]com github[.]com/lconStorages/images azureonlinestorage.com convieneonline[.]com	URL	Malicious URL
3bb80e9fbeac5383b313084775c80d11 9c943baad621654cc0a0495262b6175276a0a9fb 210c9882eba94198274ebc787fe8c88311af24932832a7fe1f1ca0261f815c3d	MD5 SHA1 SHA256	Malicious ICO File
644f63f869e2b0a9e5d1aa32823956cc 96910a3dbc194a7bf9a452afe8a35eceb904b6e4 a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c	MD5 SHA1 SHA256	Malicious ICO File
8875568b90bb03ff54d63d3bd1187063 0d890267ec8d6d2aaf43eaca727c1fbba6acd16e d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090	MD5 SHA1 SHA256	Malicious ICO File
1640f48cc05c58f4cc077503a5361cea b1dee3ebcffad01a51ff31ff495fef1d40fdfaa0 d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a	MD5 SHA1 SHA256	Malicious ICO File
71d5b9bfd6bf37ff5aa9752b2b6d5af1 64ab912d0af35c01355430d85dd4181f25e88838 4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f	MD5 SHA1 SHA256	Malicious ICO File
da667174c2d145a4d9b3b39387fbd7dd 8377fb40c76aa3ba3efae3d284fa51aa7748e010 8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d	MD5 SHA1 SHA256	Malicious ICO File
69455ba3bfd2d8e3ade5081368934945 11ae67704ea0b930b2cc966e6d07f8b898f1a7d2 f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3	MD5 SHA1 SHA256	Malicious ICO File

aafa584176d9aec7912b4bc3476acc1a 89827af650640c7042077be64dc643230d1f7482 268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca	MD5 SHA1 SHA256	Malicious ICO File
4d112603466ac9c57a669445374c1fb5 b5de30a83084d6f27d902b96dd12e15c77d1f90b c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd	MD5 SHA1 SHA256	Malicious ICO File
d232fa2eabc03123517a78936a18448b 3992dbe9e0b23e0d4ca487faffeb004bcfe9ecc8 c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396	MD5 SHA1 SHA256	Malicious ICO File
aff5911f6c211cde147a0d6aa3a7a423 caa77bcd0a1a6629ba1f3ce8d1fc5451d83d0352 f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182	MD5 SHA1 SHA256	Malicious ICO File
4942dc3c0e9808544b068854cf1351e0 57a9f3d5d1592a0769886493f566930d8f32a0fc 2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de	MD5 SHA1 SHA256	Malicious ICO File
3eb70db2f6bffbe29970f759747e07bd f533bea1c0558f73f6a3930343c16945fb75b20f e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c	MD5 SHA1 SHA256	Malicious ICO File
14b79d2f81d1c0a9c3769f7bb83e443d 31d775ab577f3cc88991d90e9ae58501dbe1f0da d0f1984b4fe896d0024533510ce22d71e05b20bad74d53fae158dc752a65782e	MD5 SHA1 SHA256	Malicious ICO File

Yara Rules

Reference:

https://www.3cx.com/blog/news/desktopapp-security-alert/