

Elastic users protected from SUDDENICON's supply chain attack

 elastic.co/security-labs/elastic-users-protected-from-suddenicon-supply-chain-attack

Elastic alert telemetry has observed protection events related to the supply chain attacks targeting the 3CXDesktopApp update process.

By

[Daniel Stepanic,](#)

[Remco Sprooten,](#)

[Joe Desimone,](#)

[Samir Bousseaden,](#)

[Devon Kerr](#)

30 March 2023

English



Key takeaways

-
- Elastic users are protected from supply chain attacks targeting the 3CX users
 - How the execution flow operates is actively being investigated by Elastic Security Labs and other research teams
 - Irrespective of the anti-malware technology you are using, shellcode and process injection alerts for 3CX should not be added to exception lists

Preamble

On March 29, 2023, CrowdStrike reported a potential supply-chain compromise affecting 3CX VOIP softphone users [as detailed in a Reddit post](#). Elastic Security Labs continues to monitor telemetry for evidence of threat activity and will provide updates as more evidence becomes available. The earliest period of potentially malicious activity is currently understood to be on or around March 22, 2023 [as reported by Todyl](#).

[3CX states](#) it is used by over 600,000 companies and over 12,000,000 users, so Elastic Security Labs is releasing a triage analysis to assist 3CX customers in the initial detection of SUDDENICON, with follow-on malware and intrusion analysis to be released at a later date.

In this informational update, Elastic Security Labs provides the following:

- Potential malicious domains associated with malware activity
- File hashes for 3CX Windows and MacOS clients which may be impacted
- Elastic queries and prebuilt protections which may be relevant to this activity
- YARA rules to identify the SUDDENICON malware

SUDDENICON triage analysis

The 3CXDesktopApp [installer MSI](#) appears to contain malicious code which waits seven days post-installation before downloading additional files from [GitHub](#) and communicating with malicious command-and-control domains. The client application writes **ffmpeg.dll** and **d3dcompiler_47.dll** to disk, the latter of which contains a payload we refer to as SUDDENICON. Both libraries in our sampling appear to have been backdoored. It should be noted that **ffmpeg.dll** and **d3dcompiler_47.dll** are both legitimate file names and rules should not be created on them alone.

00007FF98D12DF63	45:31C9	xor r9d,r9d	
00007FF98D12DF66	FF15 043E2400	call qword ptr ds:[<&CreateFilew>]	
00007FF98D12DF6C	48:83F8 FF	cmp rax,FFFFFFFFFFFFFFFF	rax:L"d3dcompiler_47.dll"
00007FF98D12DF70	0F84 A7020000	jbe ffmpeg.7FF98D12E21D	rax:L"d3dcompiler_47.dll"
00007FF98D12DF76	48:89C7	mov rdi,rax	
00007FF98D12DF79	45:31F6	xor r14d,r14d	
00007FF98D12DF7C	48:89C1	mov rcx,rax	rcx:L"C:\\Users\\user\\AppData\\Local\\Programs\\3CXDesktopApp\\ap
00007FF98D12DF7F	31D2	xor edx,edx	
00007FF98D12DF81	FF15 D93E2400	call qword ptr ds:[<&GetFileSize>]	
00007FF98D12DF87	89C5	mov ebp,eax	
00007FF98D12DF89	89C1	mov ecx,eax	
00007FF98D12DF8B	E8 44970800	call ffmpeg.7FF98D1B76D4	rax:L"d3dcompiler_47.dll"
00007FF98D12DF90	48:89C3	mov rbx,rax	
00007FF98D12DF93	48:C74424 20 00000000	mov qword ptr ss:[rsp+20],0	
00007FF98D12DF9C	4C:8D7C24 4C	lea r15,qword ptr ss:[rsp+4C]	
00007FF98D12DFA1	48:89F9	mov rcx,r15	rcx:L"C:\\Users\\user\\AppData\\Local\\Programs\\3CXDesktopApp\\ap
00007FF98D12DFA4	48:89C2	mov rdx,rax	rax:L"d3dcompiler_47.dll"
00007FF98D12DFA7	41:89E8	mov r8d,ebp	
00007FF98D12DFAA	4D:89F9	mov r9,r15	
00007FF98D12DFAD	FF15 05402400	call qword ptr ds:[<&ReadFile>]	
00007FF98D12DFB3	41:833F 00	cmp dword ptr ds:[r15],0	

ffmpeg.dll referencing the d3dcompiler_47.dll file

The **ffmpeg.dll** binary extracts SUDDENICON from **d3dcompiler_47.dll** by seeking the FEEDFACE byte sequence and decrypting using a static RC4 key (**3jB(2bsG#@c7)**). The resulting payload is then loaded in memory as the second-stage payload. A shellcode stub prepended to the payload used to map it into memory shares similarities with APPLEJEUS loader stubs, which have been associated with DPRK. Upon successfully executing, this shellcode stub writes a new file (**manifest**) to disk with a timestamp 7 days in the future, used to implement a timer after which the malware connects to the C2 infrastructure.

00007FF98D12E029	31C0	xor eax,eax	
00007FF98D12E02B	41:807C00 FD FE	cmp byte ptr ds:[r8+rax-3],FE	
00007FF98D12E031	75 17	jne ffmpeg.7FF98D12E04A	ffmpeg.dll
00007FF98D12E033	41:807C00 FE ED	cmp byte ptr ds:[r8+rax-2],ED	
00007FF98D12E039	75 0F	jne ffmpeg.7FF98D12E04A	ffmpeg.dll
00007FF98D12E03B	41:807C00 FF FA	cmp byte ptr ds:[r8+rax-1],FA	
00007FF98D12E041	75 07	jne ffmpeg.7FF98D12E04A	ffmpeg.dll
00007FF98D12E043	41:803C00 CE	cmp byte ptr ds:[r8+rax],CE	
00007FF98D12E048	74 0D	je ffmpeg.7FF98D12E057	
00007FF98D12E04A	4B:55C0	inc rax	

loading the d3dcompiler_47.dll file

C2 domains are retrieved by downloading and base64-decoding the trailing bytes appended to icon files staged in the [IconStorages Github repository](#). (this repository has been removed by Github). This repo was created by GitHub ID **120072117** on December 8, 2022, and most recently updated on March 16, 2023. After initially connecting to an active C2 server, the malware performs a POST containing a machine identifier. It then downloads and decrypts a new executable.

<pre> .g e -4f11-94d4-d3e90a4931df ows NT 10.0; Win64; x64) AppleWebKit/537.36 pApp/18.11.1197 Chrome/102.0.5005.167 </pre>	<pre> response Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Content-Type: application/json 3 Date: Thu, 30 Mar 2023 01:15:34 GMT 4 Server: LiteSpeed 5 Alt-Svc: h3="443"; ma=2592000, h3-29="443"; ma=2592000, h3-Q050="443"; ma=2592000, h3-Q046="443"; ma=2592000, h3-Q043="443"; ma=2592000, quic="443"; ma=2592000; v="43,46" 6 7 { "url": "", "description": "", "meta": "vyoAAL4DT8aYNEVNT0oU5DVQR+6y1v10BhGRQsSuzEJWdwtRdn2nGm9gl/b5PmA0u9 NJKcTCD29bxgrm9u/1AMofiqdGMzNR8yhE1rPTAkiquGEVvme9+Etac2ztH6yNs5Fq3QME4t uwB4xcD3pUG279H31+T/eR0zAAqXh36MI9HJj9bt8LlmiNAwbQAAEJZnHlovDj1wo/FP+ Fr1k4Y1AdSChwWQ53Q91vjNQWBU/ReN+UWw039Uitntmny1wTx8CWBmG2sDRD55/dnnLo1 +CmyfJrWgLBeYkGvpw0jJP2E6tfYmwEcpnT1QfEaImzgyGG0iccQ9GNwCoVECYFQODBlzY GgoySma+Mf8aN4unSmIocG6hLz1ipYUadraIbw2k4LjWY/+4C1xpKl9e2zf82+Z0nyOID gzZATTS2fEdXD121RdAqH5qNeGdjRdCLnPNbOLx1xjWViZRTAHhbQ1ivg72/RjqTYL6E y5kksy5B1Dncw9h6i1FplezEf/V4NGHLWlnXD1GpljUZhTpWY3qcY8nTCoA3QCFCsJfDx bag4DjMAepyNoGGoWamsRbn7fpS4GsmoDjqpX2MBQBA5/GXeM2LOBHOaj941eb14hbML6o MuVvksjvbnGeC+RQne417H7n7daHSXyebMwWqTVHBqUWw+dbQyOXAM0YqzC3RTYaCXW0soq hxUSNURDLRRdRlVkwOar9/GnMkrd/2AN+AiOdAezRtirAMV+fYabM1MTDTWFGmfCxB5A </pre>
---	---

SUDDENICON downloading a new executable

Initial analysis of the new executable appears to be an information stealer. We'll release an update once the analysis has been completed.

The CEO of 3CX has recommended uninstalling the software; a small number of community forum posts outline how security tooling is reacting to potential malware behaviors, and CrowdStrike and SentinelOne have published initial information. It appears likely that the threat was able to introduce adversary-created malicious software via update channels, overwriting otherwise benign components of the 3CXDesktopApp. Users may accidentally self-infect, as well.

Detection logic

Prevention

- Memory Threat Detection Alert: Shellcode injection
- Windows.Trojan.SuddenIcon

Memory Threat Detection Alert: Shellcode Injection

Mar 29, 2023 @ 14:44:32.243

[Overview](#) [Threat Intel](#) 0 [Table](#) [JSON](#)

Status	Severity	Risk Score	Rule
Open ⌵ ⊕ ⊖ ⋮	● Critical	99	Memory Shellcod

Alert reason

malware , intrusion_detection event with process 3CXDesktopApp.exe , parent process 3CXDesktopApp.exe , by user on DESKTOP-M created critical alert Memory Threat Detection Alert: Shellcode Injection .

Highlighted fields

Field	Value
host.name	DESKTOP-
Agent status	Healthy
user.name	user
Rule type	query
process.name	3CXDesktopApp.exe
Target.process.executable	C:\Users\user\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe
Memory_protection.unique_key_v1	49cb559c4982ff2d367bfab67ce6f02629b82e10a54c2ebe8b6980f4e024d5f1

Memory Threat Detection Alert: Shellcode injection

Hunting queries

The events for both KQL and EQL are provided with the Elastic Agent using the Elastic Defend integration. Hunting queries could return high signals or false positives. These queries are used to identify potentially suspicious behavior, but an investigation is required to validate the findings.

KQL queries

The following KQL query can be used to identify 3CX-signed software performing name resolution of raw.githubusercontent.com, where malicious applications related to this threat have been staged:

```
process.name : "3CXDesktopApp.exe" and dns.question.name :  
"raw.githubusercontent.com"
```

The following KQL query can be used to identify several host-based indicators of this activity:

```
dll.hash.sha256 :  
"7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896" or  
dll.hash.sha256 :  
"c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02"
```

EQL queries

Using the Timeline section of the Security Solution in Kibana under the "Correlation" tab, you can use the below EQL queries to hunt for behaviors similar

The following EQL query can be used to profile 3CX software and child software:

```
any where process.code_signature.subject_name == "3CX Ltd" or  
process.parent.code_signature.subject_name == "3CX Ltd"
```

The following EQL query can be used to identify 3CX-signed software performing name resolution of raw.githubusercontent.com, where malicious applications related to this threat have been staged:

```
network where process.code_signature.subject_name == "3CX Ltd" and dns.question.name  
== "raw.githubusercontent.com"
```

The following EQL query can be used to identify files written by the 3CXDesktopApp client:

```
file where event.type == "creation" and (host.os.type == "windows" and file.path :  
"*:\\Users\\*\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\*" and file.name :  
("manifest")) or (host.os.type == "macos" and file.path : "*/Library/Application  
Support/3CX Desktop App/" and file.name : ("UpdateAgent", ".main_storage",  
".session-lock"))
```

The following EQL query can be used to identify several host-based indicators of this activity:

```
sequence by host.name, process.entity_id
[process where process.code_signature.subject_name:"3CX Ltd"]
[library where
dll.hash.sha256:"c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02", "7
[network where dns.question.name:"raw.githubusercontent.com"]
```

The following EQL query can be used to identify this activity if the DLL is updated:

```
library where process.code_signature.subject_name : "3CX Ltd" and not
dll.code_signature.trusted == true and not startswith~(dll.name, process.name) and
/* DLL loaded from the process.executable directory */ endswith~(substring(dll.path,
0, length(dll.path) - (length(dll.name) + 1)), substring(process.executable, 0,
length(process.executable) - (length(process.name) + 1)))
```

YARA

Elastic Security Labs has released [two YARA signatures](#) for the malicious shellcode, which we refer to as SUDDENICON.

Defensive recommendations

Elastic Endgame and Elastic Endpoint customers with shellcode protections enabled in prevention mode blocked the execution of SUDDENICON, though any compromised client software may need to be removed. Due to the delayed shellcode retrieval and injection, 3CXDesktopApp users may not see alerts until the sleep interval passes (approximately 7 days). Customers who are using shellcode protections in detect-only mode should enable prevention to mitigate the risk of infection. Do not create exceptions for these alerts.

Type Memory threat	Operating system Windows, Mac, Linux	<input checked="" type="checkbox"/> Memory threat protections enabled
Protection level		
<input type="radio"/> Detect <input checked="" type="radio"/> Prevent		
User notification <i>Agent version 7.15+</i>		
<input checked="" type="checkbox"/> Notify user		
Customize notification message ?		
<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">Elastic Security {action} {rule}</div>		

Enabling the Memory threat protection feature in Prevent mode

Indicators

Potentially malicious domains

Bold domains indicate that they were observed in our analysis.

- 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**

Potentially impacted 3CXDesktopApp versions and hashes

Client hash:

dde03348075512796241389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc

OS: Windows

Installer hash:

aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868

Installer filename: **3cxdesktopapp-18.12.407.msi**

Client hash:

fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405

OS: Windows

Installer hash:

59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983

Installer filename: **3cxdesktopapp-18.12.416.msi**

Client hash:

92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61

OS: macOS

Installer hash:

5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290

Installer filename: **3CXDesktopApp-18.11.1213.dmg**

Client hash:

b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb

OS: macOS

Installer hash:

e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec

Installer filename: **3cxdesktopapp-latest.dmg**



Related content

[See all top stories](#)



Unpacking ICEDID

ICEDID is known to pack its payloads using custom file formats and a custom encryption scheme. We are releasing a set of tools to automate the unpacking process and help analysts and the community respond to ICEDID.



Elastic Security Labs discovers the LOBSHOT malware

Elastic Security Labs is naming a new malware family, LOBSHOT. LOBSHOT propagates and infiltrates targeted networks through Google Ads and hVNC sessions to deploy backdoors masquerading as legitimate application installers.



2023 Elastic Global Threat Report - Spring

Elastic publishes 2023 Global Threat Report Spring Edition

This week, we're publishing a new version of this report that's online and interactive, which includes additional data covering the remainder of 2022, written using Elastic technologies.