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.

Ву

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 <u>as detailed in a Reddit post</u>. 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 <u>as reported by Todyl</u>.

<u>3CX states</u> 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 <u>installer MSI</u> appears to contain malicious code which waits seven days post-installation before downloading additional files from <u>GitHub</u> 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.

```
45:3109
FF15 043E2400
48:8378 FF
0784 A7020000
48:89C7
48:89C1
31D2
FF15 D93E2400
89C5
89C1
89C3
48:89C3
48:89F5
48:89F5
48:89F5
48:89F5
48:89F5
48:89F5
FF15 043E2400
                                                                                              rax:L"d3dcompiler_47.dll"
                                                                                              rcx:L"C:\\Users\\user\\AppData\\Local\\Programs\\3CXDesktopApp\\ap
                                                                                               ax:L"d3dcompiler_47.d11"
                                                                                                cx:L"C:\ \  ax:L"d3dcompiler_47.d11"
```

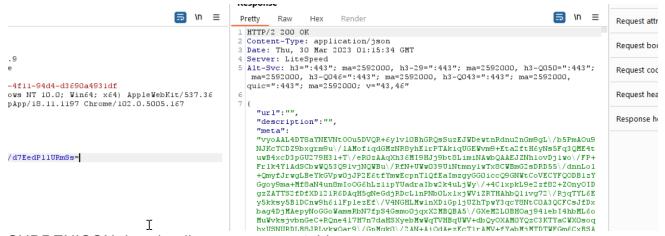
ffmpeg.dll referencing the d3dcompiler 47.dll file

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
                                                  ffmpeg.7FF98D12E04A
                        75 17
00007FF98D12E033
                        41:807C00 FE ED
                                              cmp byte ptr ds:[r8+rax-2],ED
• 00007FF98D12E039
                                                  ffmpeg.7FF98D12E04A
                                                                               ffmpeg.dll
                        75 OF
  00007FF98D12E03B
                                              cmp byte ptr ds:[r8+rax-1],FA
                        41:807C00 FF FA
00007FF98D12E041
                                                  ffmpeg.7FF98D12E04A
                        75 07
                                              cmp byte ptr ds:[r8+rax],CE
  00007FF98D12E043
                        41:803C00 CE
                        74 OD
  0000755080135044
```

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 <u>IconStorages Github repository</u> (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.



SUDDENICON downloading a new executable

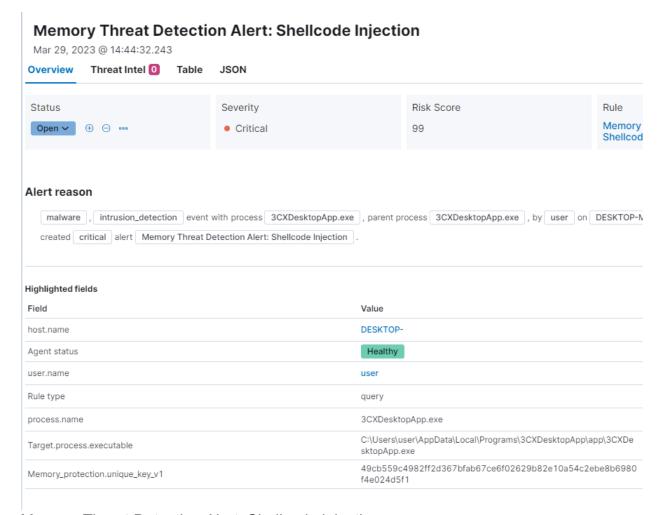
Initial analysis of the new executable appears to be an information stealer. We'll release an update once the analysis has been completed.

The CEO of 3CX has <u>recommended uninstalling the software</u>; a small number of <u>community forum</u> posts outline how security tooling is reacting to potential malware behaviors, and <u>CrowdStrike</u> and <u>SentinelOne</u> 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 <u>self-infect</u>, as well.

Detection logic

Prevention

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



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\\C3XDesktopApp\\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 guery can be used to identify this activity if the DLL is updated:

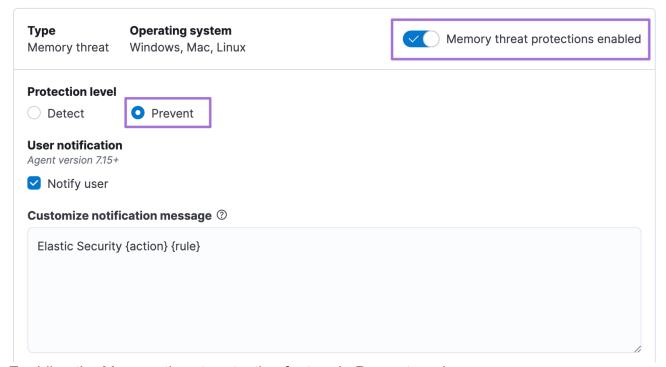
library where process.code_signature.subject_name : "3CX Ltd" and not
dll.code_signature.trusted == true and not startswith~(dll.name, process.name) and
/* DLL loaded from the process.executable directory */ endswith~(substring(dll.path,
0, length(dll.path) - (length(dll.name) + 1)), substring(process.executable,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

YARA

Elastic Security Labs has released <u>two YARA signatures</u> 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.



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.



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.