Elastic users protected from SUDDENICON's supply chain attack

By Daniel Stepanic, Remco Sprooten, Joe Desimone, Samir Bousseaden, Devon Kerr

Published: 2023-05-05 · Archived: 2026-04-05 21:13:48 UTC

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

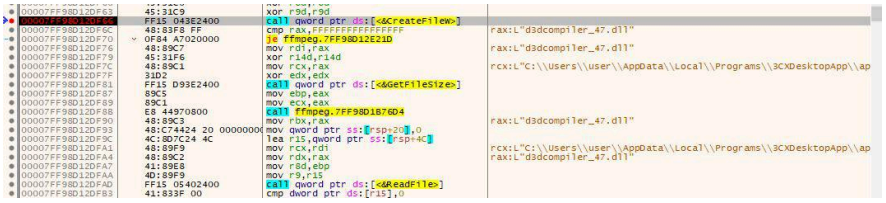
On March 29, 2023, CrowdStrike reported a potential supply-chain compromise affecting 3CX VOIP softphone users as detailed in a Reddit post. Elastic Security Labs continues to monitor telemetry for evidence of threat activity and will provide updates as more evidence becomes available. The earliest period 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

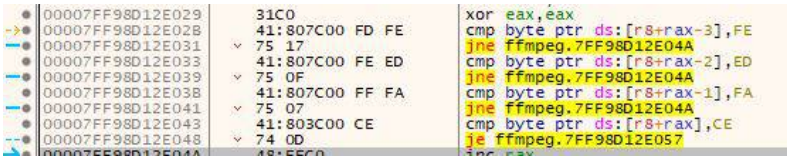
SUDDENICON triage analysis

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.



ffmpeg.dll referencing the d3dcompiler_47.dll file

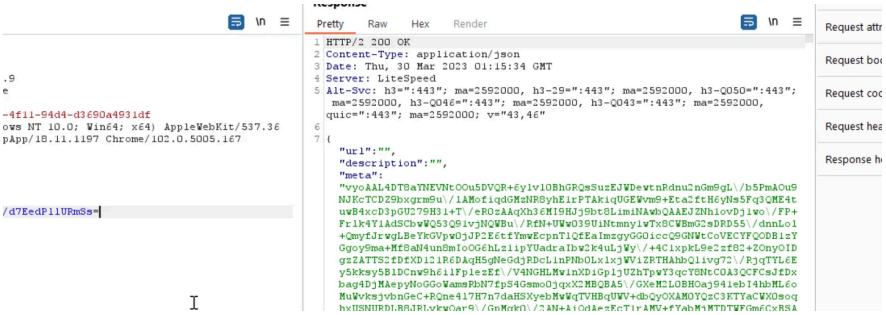
The `ffmpeg.dll` binary extracts SUDDENICON from `d3dcompiler\_47.dll` by seeking the FEEDFACE byte sequence and decrypting using a static RC4 key (`3jB(2bsG#@c7`). The resulting payload is then loaded in memory as the second-stage payload. A shellcode stub prepended to the payload used to map it into 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.



ffmpeg.dll 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.



SUDDENICON downloading a new executable

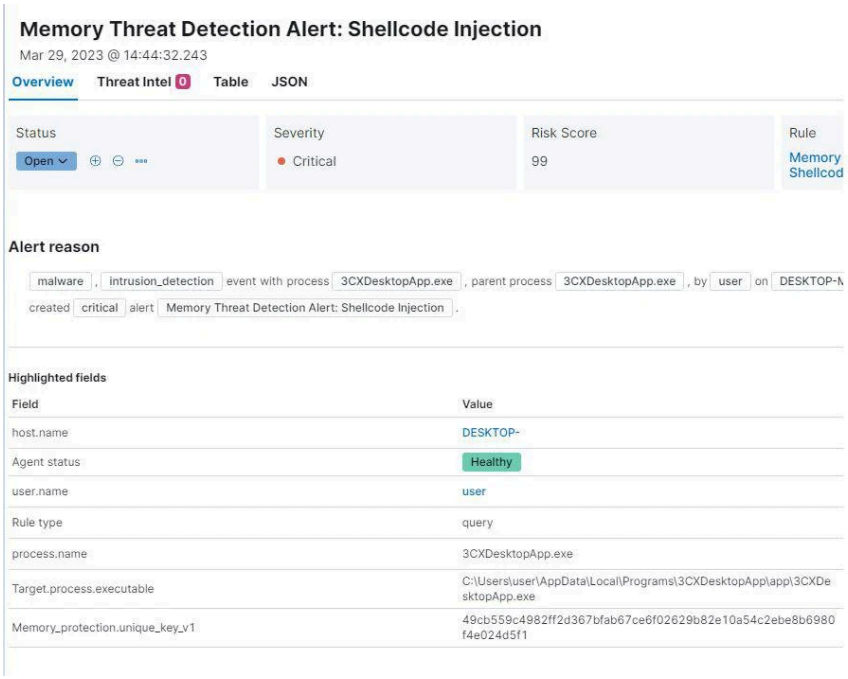
Initial analysis of the new executable appears to be an information stealer. We'll release an update once the analysis has been completed.

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

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 similar behaviors.

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","7986bbaee8940da11ce089383521ab420c443ab7b15ed42a[network where dns.question.name:"raw.githubusercontent.com"]
```

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

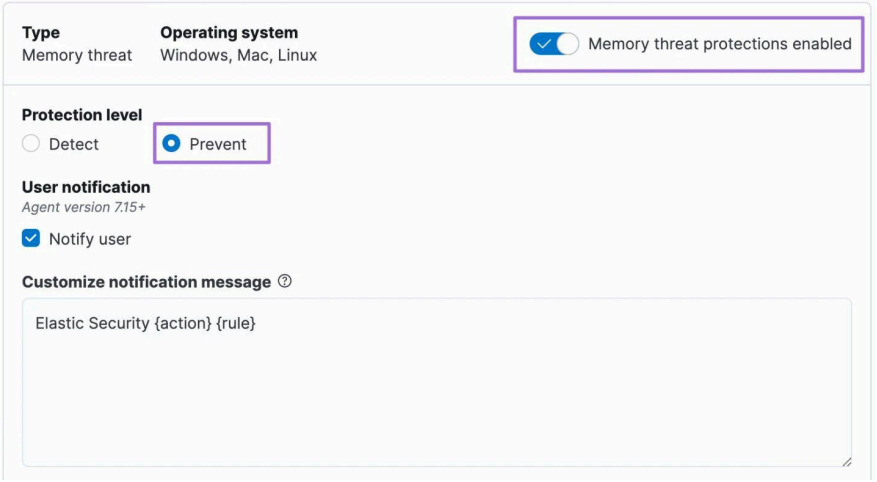
```
library where process.code_signature.subject_name : "3CX Ltd" and not dll.code_signature.trusted == true and not startswith~(dll.name, process.name) and /* DLL loaded from the process.executable directory */ endswith~ (substring(dll.path, 0, length(dll.path) - (length(dll.name) + 1)), substring(process.executable,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



Enabling the Memory threat protection feature in Prevent mode

References

The following were referenced throughout the above research: - https://www.reddit.com/r/crowdstrike/comments/125r3uu/20230329_situational_awareness_crowdstrike/ - https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/ - https://www.todyl.com/blog/post/threat-advisory-3cx-softphone-telephony-campaign

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: `dde0334807551279624l389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc` 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`
