Backdoored 3CXDesktopApp Installer Used in Active Threat Campaign

rapid7.com/blog/post/2023/03/30/backdoored-3cxdesktopapp-installer-used-in-active-threat-campaign/

Rapid7 March 30, 2023

Last updated at Mon, 03 Apr 2023 21:12:33 GMT

Emergent threats evolve quickly. We will update this blog with new information as it comes to light and we are able to verify it. Erick Galinkin, Ted Samuels, Zach Dayton, Eoin Miller, Caitlin Condon, Stephen Fewer, Spencer McIntyre, and Christiaan Beek all contributed to this blog.

On Wednesday, March 29, 2023, multiple security firms issued warnings about malicious activity coming from a legitimate, signed binary from communications technology company 3CX. The binary, 3CXDesktopApp, is popular video-conferencing software available for download on all major platforms. Several analyses have attributed the threat campaign to state-sponsored threat actors, and security firms have observed malicious activity in both Windows and Mac environments.

Rapid7's threat research teams analyzed the 3CXDesktopApp Windows binary and confirmed that the 3CX MSI installer drops the following files: `3CXDesktopApp.exe`, a benign file that loads the backdoored `ffmpeg.dll`, which reads an RC4-encrypted blob after the hexadecimal demarcation of `fe ed fa ce` in `d3dcompiler.dll`. The RC4-encrypted blob in `d3dcompiler.dll` is executable code that is reflectively loaded and retrieves `.ico` files with appended Base64-encoded strings from GitHub. The encoded strings appear to be command-and-control (C2) communications. There is a non-exhaustive list of indicators of compromise (IOCs) at the end of this blog.

Rapid7 reached out to GitHub's security team the evening of March 29 about the GitHub repository being used as adversary infrastructure in this campaign. As of 9:40 PM ET, the malicious user has been suspended and the repository is no longer available.

Rapid7 Managed Detection and Response (MDR) has observed the backdoored 3CX installer and components in several customer environments as of March 29, 2023. Rapid7 MDR is in contact with customers that we believe may be impacted.

Mitigation Guidance

Official guidance from 3CX confirms that the following clients and versions are affected:

- Electron Windows App (shipped in Update 7) versions 18.12.407 and 18.12.416
- Electron Mac App versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416

As of March 30 at 11 AM ET, 3CX has not confirmed which versions of the 3CXDesktopApp are *definitively unaffected*.

Update March 31: 3CX has released new versions of their Windows and Mac Electron app as of March 31. Their update included the following statement:

"The Electron App update that we are releasing today is considered to be secure but there is no guarantee given that we only had 24 hours to make the necessary adjustments."

Rapid7 is continuing to advise customers to pursue a conservative mitigation strategy of **uninstalling 3CXDesktopApp on all platforms** and removing any artifacts left behind. Users should retroactively hunt for indicators of compromise and block known-bad domains. There is a non-exhaustive list of known-bad domains and malicious file hashes at the end of this blog.

3CX has a browser-based Progressive Web App (PWA) that does not require the user to download an executable file. Users should leverage this PWA for the time being instead of downloadable clients. 3CX is intermittently issuing updated guidance here.

Rapid7 customers

The following new rules have been added for Rapid7 InsightIDR and Managed Detection & Response (MDR) customers and will alert on known-bad hashes and file versions of the backdoored executable, as well as known-bad domains in WEB_PROXY and DNS logs:

- Suspicious Web Request - 3CX Desktop Supply Chain Compromise
- Suspicious DNS Request - 3CX Desktop Supply Chain Compromise
- Suspicious Process - 3CX Desktop Supply Chain Compromise

InsightVM and Nexpose customers can use Query Builder (`asset.software.product CONTAINS '3CX Desktop App'`) or a Filtered Asset Search (`Software Name contains 3CX Desktop App`) to find assets in their environment with 3CX installed. The March 30 content release also contains a check that will report any installed version of 3CX Desktop App as vulnerable. This check may be refined as new information regarding vulnerable versions comes to light.

A Velociraptor artifact is available here.

Indicators of compromise

A non-exhaustive list of known-bad domains is below. We advise blocking these immediately:

```
akamaicontainer[.]com
akamaitechcloudservices[.]com
azuredeploystore[.]com
azureonlinecloud[.]com
azureonlinestorage[.]com
convieneonline[.]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
Soyoungjun[.]com
visualstudiofactory[.]com
zacharryblogs[.]com
```

More granular URLs our team has decrypted from C2 communications include:

```
hxxps[://]akamaitechcloudservices[.]com/v2/storage
hxxps[://]azuredeploystore[.]com/cloud/services
hxxps[://]azureonlinestorage[.]com/azure/storage
hxxps[://]glcloudservice[.]com/v1/console
hxxps[://]msedgepackageinfo[.]com/microsoft-edge
hxxps[://]msedgeupdate[.]net/Windows
hxxps[://]msstorageazure[.]com/window
hxxps[://]msstorageboxes[.]com/office
hxxps[://]officeaddons[.]com/technologies
hxxps[://]officestoragebox[.]com/api/session
hxxps[://]pbxcloudeservices[.]com/phonesystem
hxxps[://]pbxphonenetwork[.]com/voip
hxxps[://]pbxsources[.]com/exchange
hxxps[://]sourceslabs[.]com/downloads
hxxps[://]visualstudiofactory[.]com/workload
hxxps[://]www[.]3cx[.]com/blog/event-trainings/
hxxps[://]zacharryblogs[.]com/feed
```

File hashes:

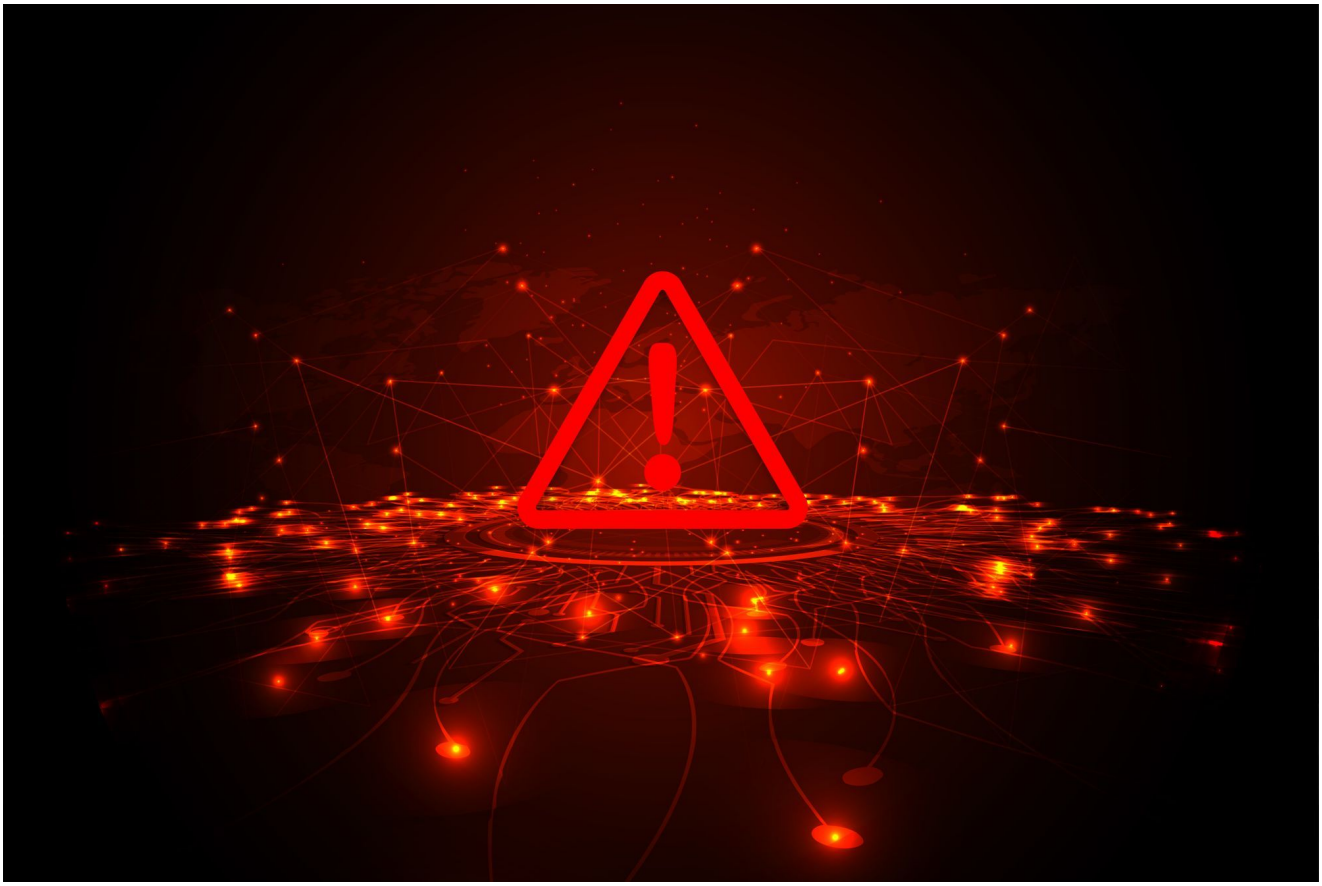
```
Compromised MSI: aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868

3CXDesktopApp.exe: fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405
ffmpeg.dll: 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
d3dcompiler_47.dll: 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03
```

The following file hashes have been reported as related and malicious by the community but not independently verified by Rapid7 analysts:

```
dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb
```

Updates

April 3, 2023: CVE-2023-29059 has been assigned to this issue.



Never miss a blog

Get the latest stories, expertise, and news about security today.