Forensic Triage of a Windows System running the Backdoored 3CX Desktop App

cadosecurity.com/forensic-triage-of-a-windows-system-running-the-backdoored-3cx-desktop-app/

March 30, 2023

Blog

March 30, 2023

As you've seen there have been a number of reports (Crowdstrike, SentinelOne, Trend Micro, Symantec, Volexity, Huntress) of a supply chain compromise of 3CX, which produces VOIP phone software.

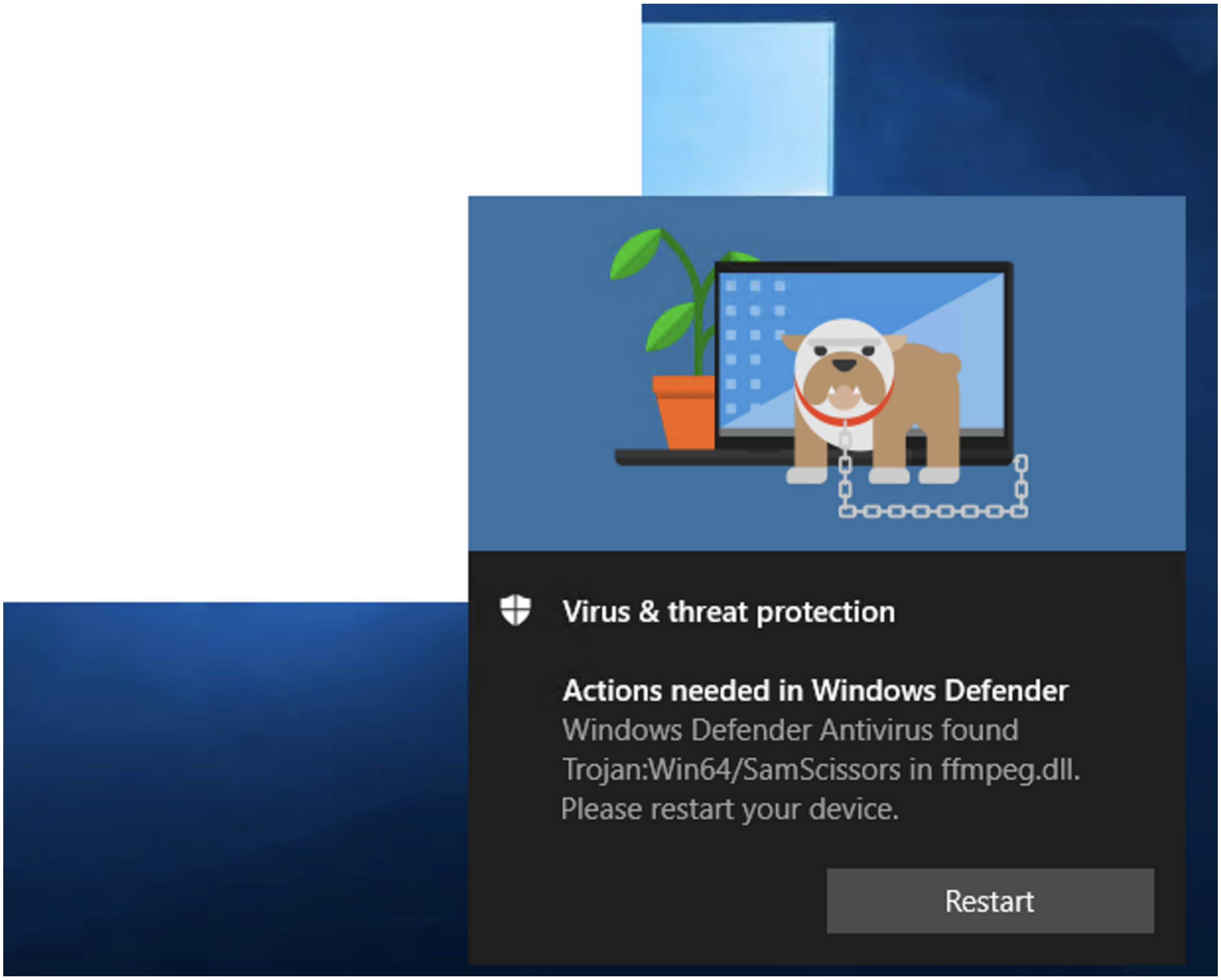
Below we have performed a quick triage forensic investigation of a system we have installed the backdoored installer on. We have also supplied Yara rules for the components under a friendly Apache License (at the bottom) to help you hunt for compromised systems.

Note that our data-set will be missing data you will find on a real compromised system, as the download chain (from Github) is now broken due to a successful taken down request. We deployed the final stage credential theft tool (d3dcompiler_47.dll) manually via rundll32 calling each available exported module. There is also a sleep function to delay the secondary payload. So results may vary a bit from what you will find on a real system!

We have performed the analysis of the system using Cado Response but the results and approach should be transferable.

Installing 3CX

We installed a known-compromised version of 3CX (3CXDesktopApp-18.12.416.msi). After the installation completed successfully, Windows defender detected a malicious component (ffmpeg.dll) as Win64/SamScissors:

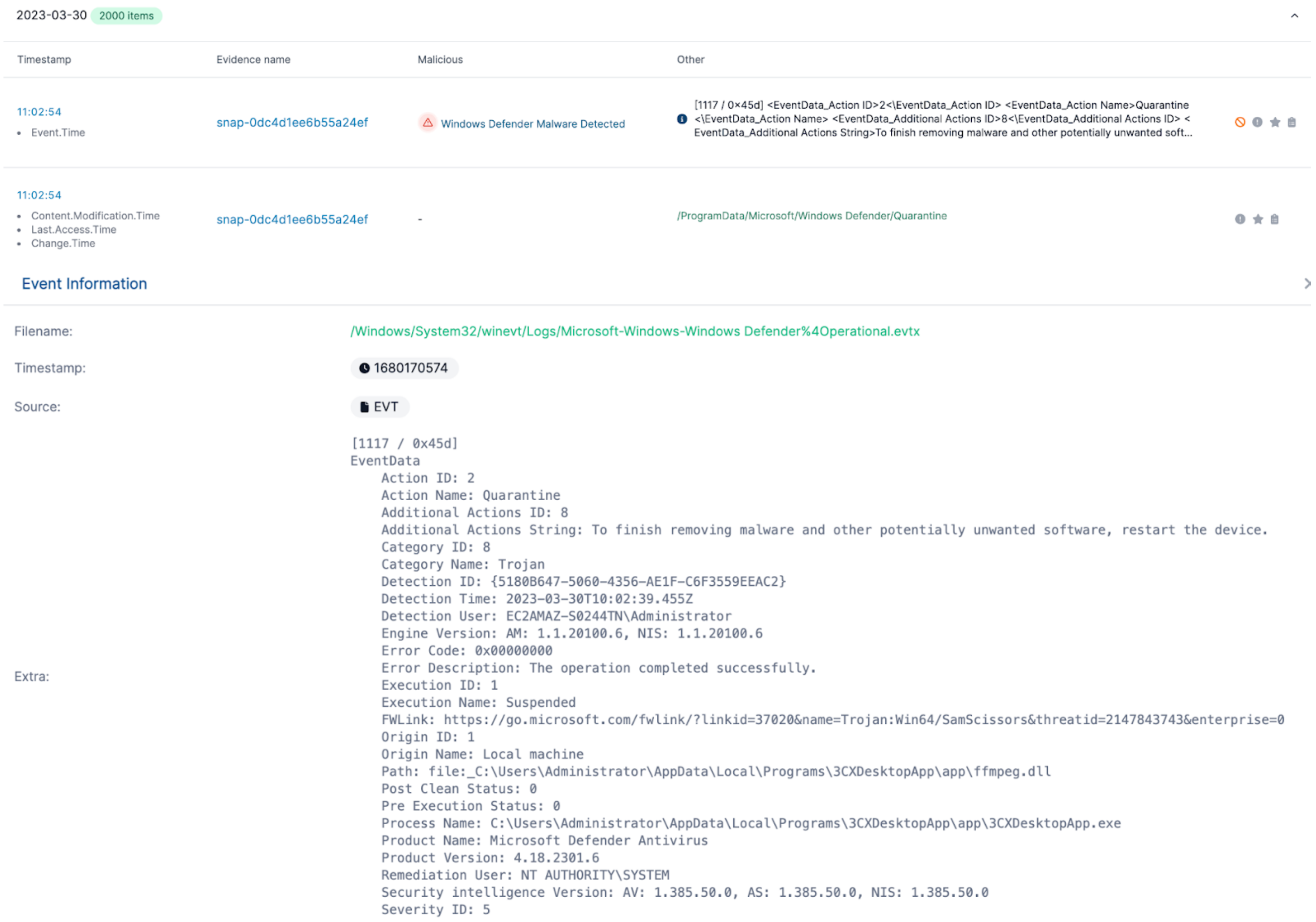


Virus & threat protection

Actions needed in Windows Defender

Windows Defender Antivirus found Trojan:Win64/SamScissors in ffmpeg.dll. Please restart your device.

Which you can see in the Windows Defender event logs as expected:



2023-03-30 2000 items

Timestamp	Evidence name	Malicious	Other
11:02:54 - Event.Time	snap-0dc4d1ee6b55a24ef	Windows Defender Malware Detected	[1117 / 0×45d] <EventData_Action ID>2<\EventData_Action ID> <EventData_Action Name>Quarantine <\EventData_Action Name> <EventData_Additional Actions ID>8<\EventData_Additional Actions ID> < EventData_Additional Actions String>To finish removing malware and other potentially unwanted soft...
11:02:54 - Content.Modification.Time - Last.Access.Time - Change.Time	snap-0dc4d1ee6b55a24ef	-	/ProgramData/Microsoft/Windows Defender/Quarantine

Event Information

Filename: /Windows/System32/winevt/Logs/Microsoft-Windows-Windows Defender%4Operational.evtx

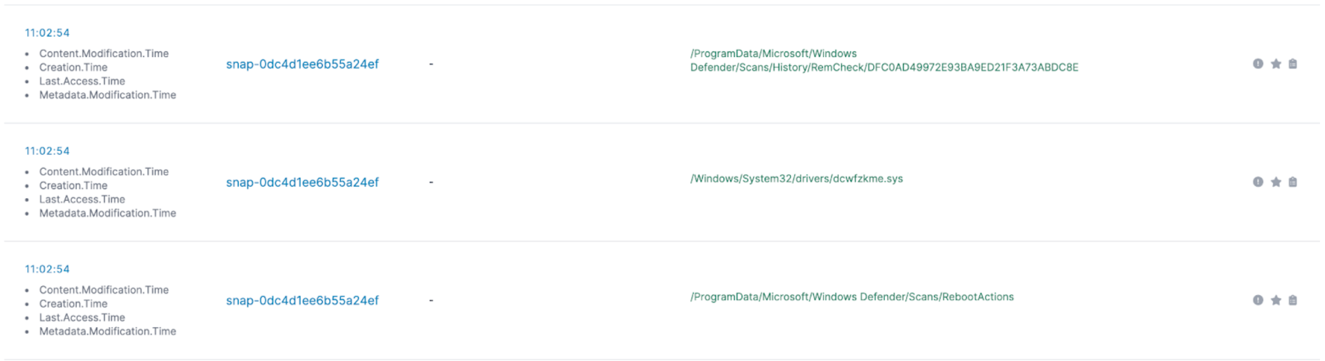
Timestamp: 1680170574

Source: EVT

Extra:

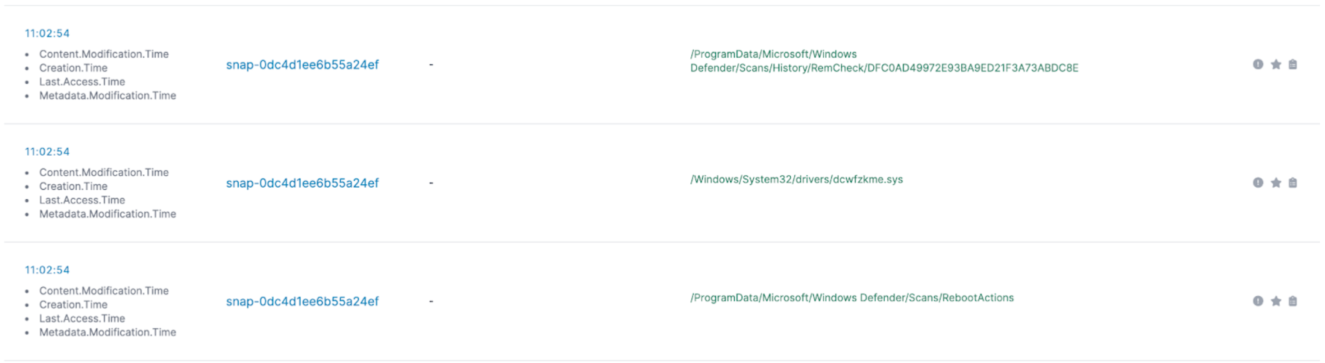
```
[1117 / 0x45d]
EventData
    Action ID: 2
    Action Name: Quarantine
    Additional Actions ID: 8
    Additional Actions String: To finish removing malware and other potentially unwanted software, restart the device.
    Category ID: 8
    Category Name: Trojan
    Detection ID: {5180B647-5060-4356-AE1F-C6F3559EEAC2}
    Detection Time: 2023-03-30T10:02:39.455Z
    Detection User: EC2AMAZ-S0244TN\Administrator
    Engine Version: AM: 1.1.20100.6, NIS: 1.1.20100.6
    Error Code: 0x00000000
    Error Description: The operation completed successfully.
    Execution ID: 1
    Execution Name: Suspended
    FWLink: https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/SamScissors&threatid=2147843743&enterprise=0
    Origin ID: 1
    Origin Name: Local machine
    Path: file:_C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\ffmpeg.dll
    Post Clean Status: 0
    Pre Execution Status: 0
    Process Name: C:\Users\Administrator\AppData\Local\Programs\3CXDesktopApp\app\3CXDesktopApp.exe
    Product Name: Microsoft Defender Antivirus
    Product Version: 4.18.2301.6
    Remediation User: NT AUTHORITY\SYSTEM
    Security intelligence Version: AV: 1.385.50.0, AS: 1.385.50.0, NIS: 1.385.50.0
    Severity ID: 5
```

Looking down in the timeline, we see a suspicious file being created on disk (dcwfzkme.sys)



11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/ProgramData/Microsoft/Windows Defender/Scans/History/RemCheck/DFC0AD49972E93BA9ED21F3A73ABDC8E
11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/Windows/System32/drivers/dcwfzkme.sys
11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/ProgramData/Microsoft/Windows Defender/Scans/RebootActions

Which we can see on disk:



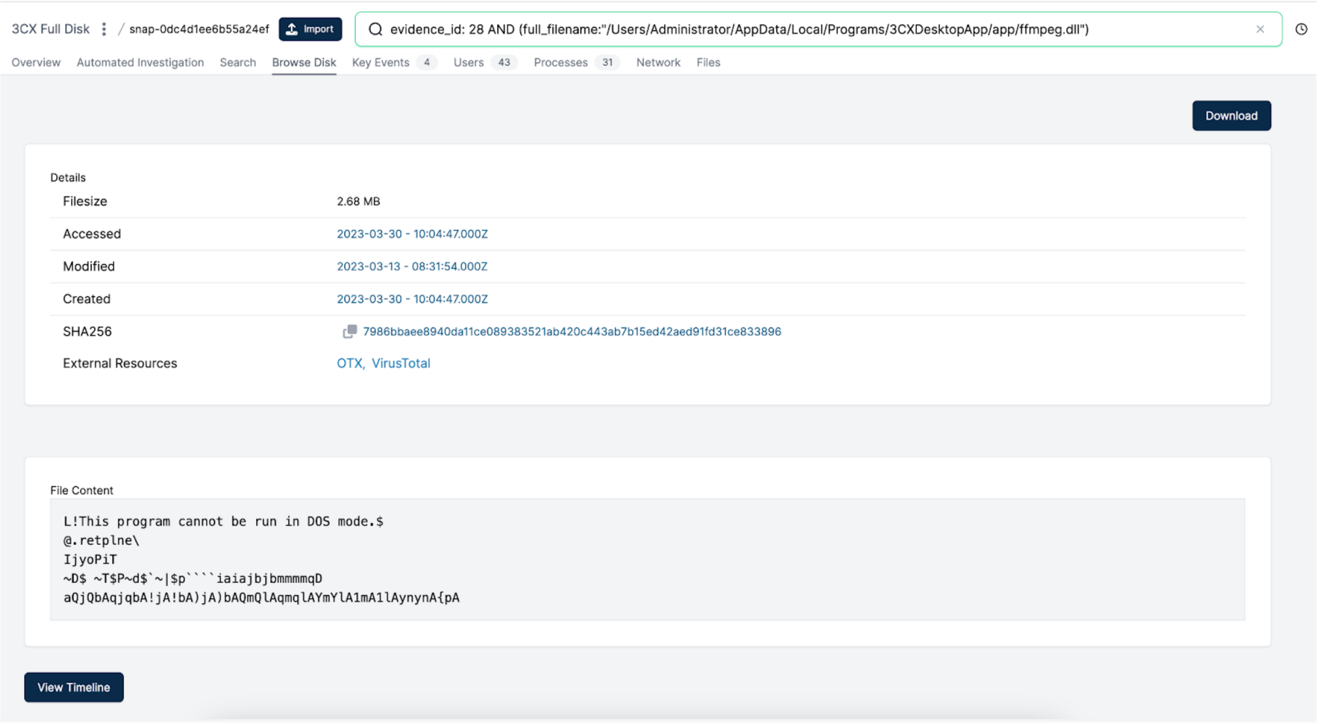
11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/ProgramData/Microsoft/Windows Defender/Scans/History/RemCheck/DFC0AD49972E93BA9ED21F3A73ABDC8E
11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/Windows/System32/drivers/dcwfzkme.sys
11:02:54 - Content.Modification.Time - Creation.Time - Last.Access.Time - Metadata.Modification.Time	snap-0dc4d1ee6b55a24ef	-	/ProgramData/Microsoft/Windows Defender/Scans/RebootActions

However, looking up the hash shows that this is actually a part of Windows Defender's legitimate execution – this is just part of how Microsoft's Boot Time Removal Tool (btr.sys) operates and is a random name. So – let's ignore that one!

So – let's disable Defender and reinstall…

Post Installation

One obvious thing is ffmpeg.dll as discussed and identified already, now viewable on disk:



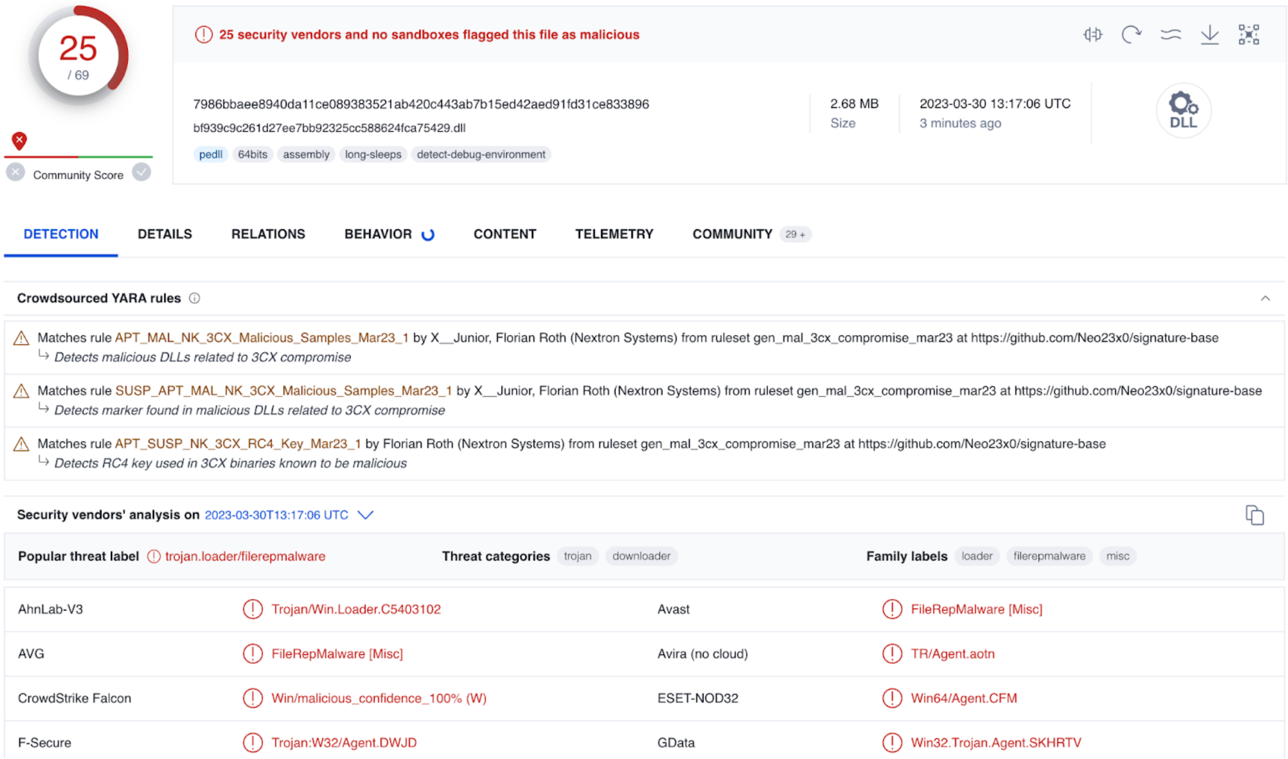
evidence_id: 28 AND (full_filename:"/Users/Administrator/AppData/Local/Programs/3CXDesktopApp/app/ffmpeg.dll")

Details

Filesize	2.68 MB
Accessed	2023-03-30 - 10:04:47.000Z
Modified	2023-03-13 - 08:31:54.000Z
Created	2023-03-30 - 10:04:47.000Z
SHA256	7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
External Resources	OTX, VirusTotal

File Content

```
L!This program cannot be run in DOS mode.$
@.retplne\
IjyoPiT
~D$ ~T$P~d$`~|$p````iaiajbjbmmmmqD
aQjQbAqjqbA!jA!bA)jA)bAQmQlAqmqlAYmYlA1mA1lAynynA{pA
```



25 security vendors and no sandboxes flagged this file as malicious

7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
bf939c9c261d27ee7bb92325cc588624fca75429.dll
pedll 64bits assembly long-sleeps detect-debug-environment

2.68 MB
Size

2023-03-30 13:17:06 UTC
3 minutes ago

Crowdsourced YARA rules

Matches rule APT_MAL_NK_3CX_Malicious_Samples_Mar23_1 by X__Junior, Florian Roth (Nextron Systems) from ruleset gen_mal_3cx_compromise_mar23 at https://github.com/Neo23x0/signature-base
↳ *Detects malicious DLLs related to 3CX compromise*

Matches rule SUSP_APT_MAL_NK_3CX_Malicious_Samples_Mar23_1 by X__Junior, Florian Roth (Nextron Systems) from ruleset gen_mal_3cx_compromise_mar23 at https://github.com/Neo23x0/signature-base
↳ *Detects marker found in malicious DLLs related to 3CX compromise*

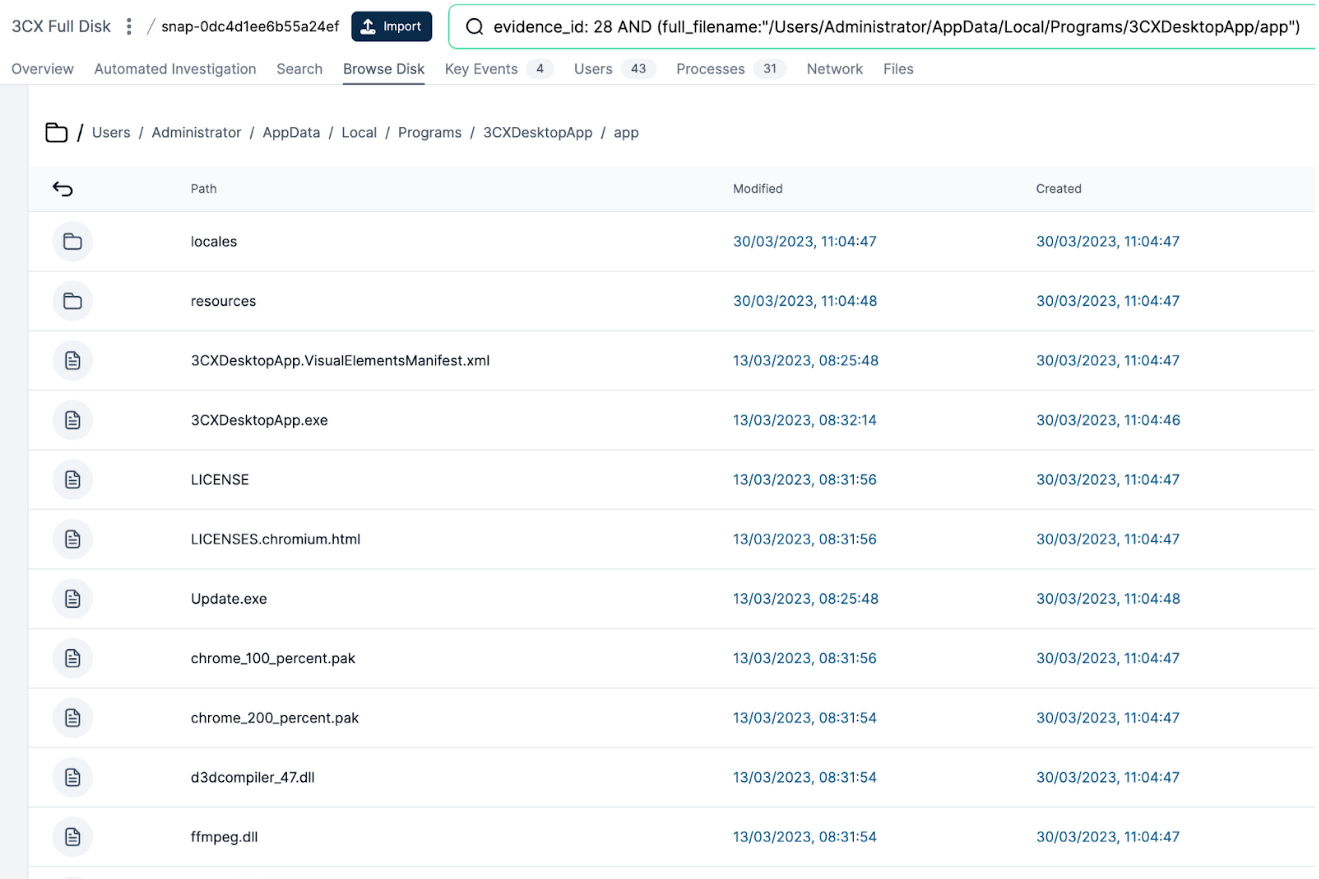
Matches rule APT_SUSP_NK_3CX_RC4_Key_Mar23_1 by Florian Roth (Nextron Systems) from ruleset gen_mal_3cx_compromise_mar23 at https://github.com/Neo23x0/signature-base
↳ *Detects RC4 key used in 3CX binaries known to be malicious*

Security vendors' analysis on 2023-03-30T13:17:06 UTC

Popular threat label trojan.loader/filerepmalware · Threat categories trojan downloader · Family labels loader filerepmalware misc

AhnLab-V3	Trojan/Win.Loader.C5403102	Avast	FileRepMalware [Misc]
AVG	FileRepMalware [Misc]	Avira (no cloud)	TR/Agent.aotn
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	ESET-NOD32	Win64/Agent.CFM
F-Secure	Trojan:W32/Agent.DWJD	GData	Win32.Trojan.Agent.SKHRTV

Browsing to the folder level of ffmpeg.dll, we see a few other key files:

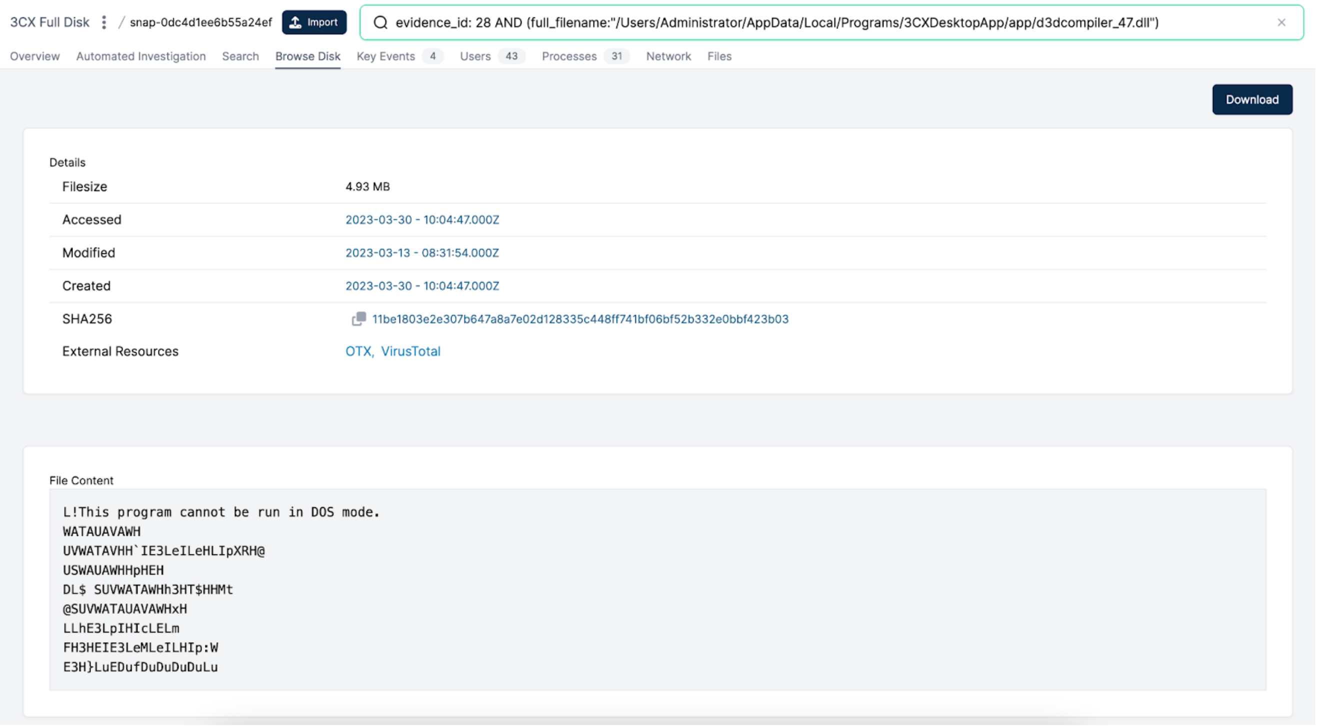


evidence_id: 28 AND (full_filename:"/Users/Administrator/AppData/Local/Programs/3CXDesktopApp/app")

/ Users / Administrator / AppData / Local / Programs / 3CXDesktopApp / app

Path	Modified	Created
locales	30/03/2023, 11:04:47	30/03/2023, 11:04:47
resources	30/03/2023, 11:04:48	30/03/2023, 11:04:47
3CXDesktopApp.VisualElementsManifest.xml	13/03/2023, 08:25:48	30/03/2023, 11:04:47
3CXDesktopApp.exe	13/03/2023, 08:32:14	30/03/2023, 11:04:46
LICENSE	13/03/2023, 08:31:56	30/03/2023, 11:04:47
LICENSES.chromium.html	13/03/2023, 08:31:56	30/03/2023, 11:04:47
Update.exe	13/03/2023, 08:25:48	30/03/2023, 11:04:48
chrome_100_percent.pak	13/03/2023, 08:31:56	30/03/2023, 11:04:47
chrome_200_percent.pak	13/03/2023, 08:31:54	30/03/2023, 11:04:47
d3dcompiler_47.dll	13/03/2023, 08:31:54	30/03/2023, 11:04:47
ffmpeg.dll	13/03/2023, 08:31:54	30/03/2023, 11:04:47

Ffmpeg.dll we have spoken about and is used to side-load encoded data from the other file in the folder – d3dcompiler_47.dll.



evidence_id: 28 AND (full_filename:"/Users/Administrator/AppData/Local/Programs/3CXDesktopApp/app/d3dcompiler_47.dll")

Details

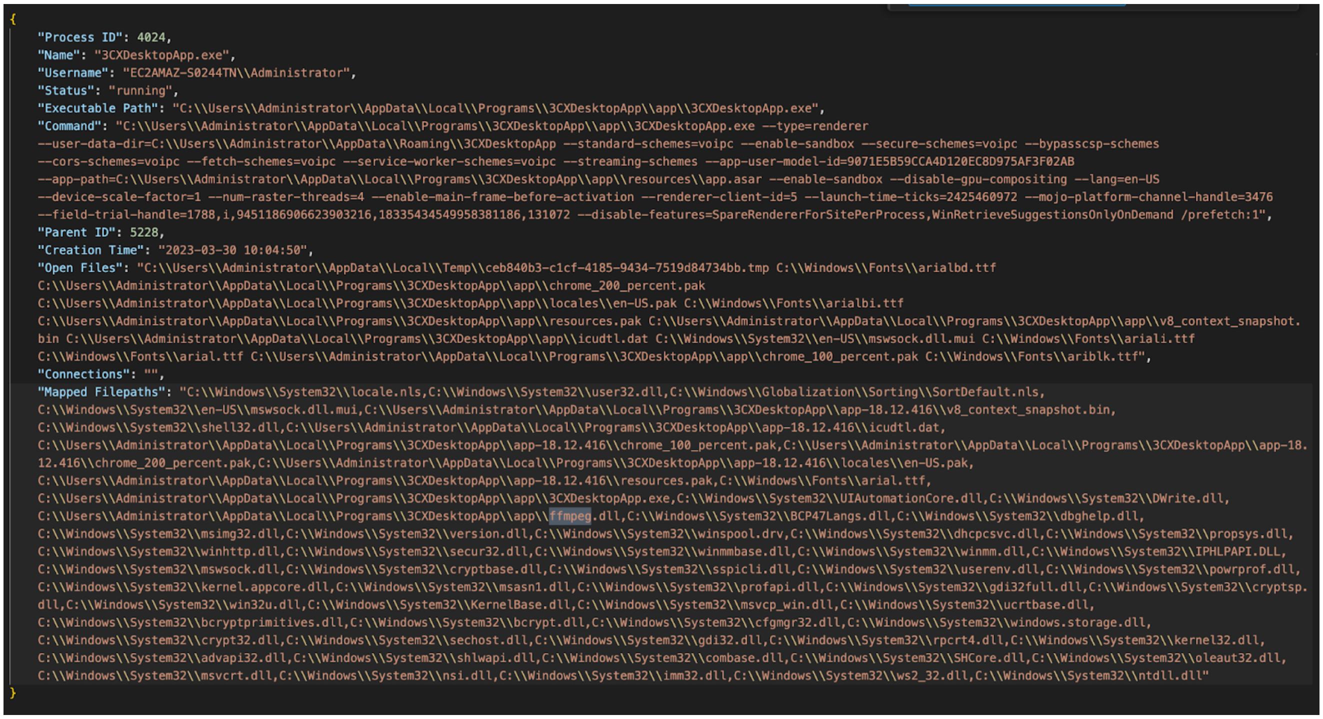
Filesize	4.93 MB
Accessed	2023-03-30 - 10:04:47.000Z
Modified	2023-03-13 - 08:31:54.000Z
Created	2023-03-30 - 10:04:47.000Z
SHA256	11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03
External Resources	OTX, VirusTotal

File Content

```
L!This program cannot be run in DOS mode.
WATAUAVAWH
UVWATAVHH`IE3LeILeHLIpXRH@
USWAUAWHHpHEH
DL$ SUVWATAWHh3HT$HHMt
@SUVWATAUAVAWHxH
LLhE3LpIHIcLELm
FH3HEIE3LeMLeILHIp:W
E3H}LuEDufDuDuDuDuLu
```

Update.exe is used to update the application, and has been seen pulling down the compromised version.

Whilst the analysis above has been performed on a dead disk (in this case for speed an isolated EC2 system) we can also perform a live collection which shows the open files for the 3CX application at the time of collection:



```
{
    "Process ID": 4024,
    "Name": "3CXDesktopApp.exe",
    "Username": "EC2AMAZ-S0244TN\\Administrator",
    "Status": "running",
    "Executable Path": "C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\3CXDesktopApp.exe",
    "Command": "C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\3CXDesktopApp.exe --type=renderer
    --user-data-dir=C:\\Users\\Administrator\\AppData\\Roaming\\3CXDesktopApp --standard-schemes=voipc --enable-sandbox --secure-schemes=voipc --bypasscsp-schemes
    --cors-schemes=voipc --fetch-schemes=voipc --service-worker-schemes=voipc --streaming-schemes --app-user-model-id=9071E5B59CCA4D120EC8D975AF3F02AB
    --app-path=C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\resources\\app.asar --enable-sandbox --disable-gpu-compositing --lang=en-US
    --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=5 --launch-time-ticks=2425460972 --mojo-platform-channel-handle=3476
    --field-trial-handle=1788,i,9451186906623903216,18335434549958381186,131072 --disable-features=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:1",
    "Parent ID": 5228,
    "Creation Time": "2023-03-30 10:04:50",
    "Open Files": "C:\\Users\\Administrator\\AppData\\Local\\Temp\\ceb840b3-c1cf-4185-9434-7519d84734bb.tmp C:\\Windows\\Fonts\\arialbd.ttf
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\chrome_200_percent.pak
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\locales\\en-US.pak C:\\Windows\\Fonts\\arialbi.ttf
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\resources.pak C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\v8_context_snapshot.
    bin C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\icudtl.dat C:\\Windows\\System32\\en-US\\mswsock.dll.mui C:\\Windows\\Fonts\\ariali.ttf
    C:\\Windows\\Fonts\\arial.ttf C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\chrome_100_percent.pak C:\\Windows\\Fonts\\ariblk.ttf",
    "Connections": "",
    "Mapped Filepaths": "C:\\Windows\\System32\\locale.nls,C:\\Windows\\System32\\user32.dll,C:\\Windows\\Globalization\\Sorting\\SortDefault.nls,
    C:\\Windows\\System32\\en-US\\mswsock.dll.mui,C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.12.416\\v8_context_snapshot.bin,
    C:\\Windows\\System32\\shell32.dll,C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.12.416\\icudtl.dat,
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.12.416\\chrome_100_percent.pak,C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.
    12.416\\chrome_200_percent.pak,C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.12.416\\locales\\en-US.pak,
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app-18.12.416\\resources.pak,C:\\Windows\\Fonts\\arial.ttf,
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\3CXDesktopApp.exe,C:\\Windows\\System32\\UIAutomationCore.dll,C:\\Windows\\System32\\DWrite.dll,
    C:\\Users\\Administrator\\AppData\\Local\\Programs\\3CXDesktopApp\\app\\ffmpeg.dll,C:\\Windows\\System32\\BCP47Langs.dll,C:\\Windows\\System32\\dbghelp.dll,
    C:\\Windows\\System32\\msimg32.dll,C:\\Windows\\System32\\version.dll,C:\\Windows\\System32\\winspool.drv,C:\\Windows\\System32\\dhcpcsvc.dll,C:\\Windows\\System32\\propsys.dll,
    C:\\Windows\\System32\\winhttp.dll,C:\\Windows\\System32\\secur32.dll,C:\\Windows\\System32\\winmmbase.dll,C:\\Windows\\System32\\winmm.dll,C:\\Windows\\System32\\IPHLPAPI.DLL,
    C:\\Windows\\System32\\mswsock.dll,C:\\Windows\\System32\\cryptbase.dll,C:\\Windows\\System32\\sspicli.dll,C:\\Windows\\System32\\userenv.dll,C:\\Windows\\System32\\powrprof.dll,
    C:\\Windows\\System32\\kernel.appcore.dll,C:\\Windows\\System32\\msasn1.dll,C:\\Windows\\System32\\profapi.dll,C:\\Windows\\System32\\gdi32full.dll,C:\\Windows\\System32\\cryptsp.
    dll,C:\\Windows\\System32\\win32u.dll,C:\\Windows\\System32\\KernelBase.dll,C:\\Windows\\System32\\msvcp_win.dll,C:\\Windows\\System32\\ucrtbase.dll,
    C:\\Windows\\System32\\bcryptprimitives.dll,C:\\Windows\\System32\\bcrypt.dll,C:\\Windows\\System32\\cfgmgr32.dll,C:\\Windows\\System32\\windows.storage.dll,
    C:\\Windows\\System32\\crypt32.dll,C:\\Windows\\System32\\sechost.dll,C:\\Windows\\System32\\gdi32.dll,C:\\Windows\\System32\\rpcrt4.dll,C:\\Windows\\System32\\kernel32.dll,
    C:\\Windows\\System32\\advapi32.dll,C:\\Windows\\System32\\shlwapi.dll,C:\\Windows\\System32\\combase.dll,C:\\Windows\\System32\\SHCore.dll,C:\\Windows\\System32\\oleaut32.dll,
    C:\\Windows\\System32\\msvcrt.dll,C:\\Windows\\System32\\nsi.dll,C:\\Windows\\System32\\imm32.dll,C:\\Windows\\System32\\ws2_32.dll,C:\\Windows\\System32\\ntdll.dll"
}
```

For now that's it – I was hoping to show the forensic artefacts showing the credential stealing but it hasn't been executed in this environment.

If you'd like to follow along…

If you'd like to try out Cado Response, you can get a free trial here.

Indicators of Compromise and Yara Rules

```
rule APT_Trojan_Win_3CX {
    meta:
        description = "Detects malicious ffmpeg dll used in 3CX supply chain attack"
        author = "[email protected]"
        date = "2023-03-30"
        license = "Apache License 2.0"
        hash1 = "7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896"
        hash2 = "c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02"
    strings:
        $rout1 = { 4C 8D 4C 24 48 4C 89 F1 4C 89 EA 41 B8 40 00 00 00 FF 15 9C 3E 24
00 85 C0 74 22 4C 89 F0 FF 15 27 8E 3B 00 4C 8D 4C 24 48 45 8B 01 4C 89 F1 4C 89 EA
FF 15 7B 3E 24 00 EB 03 45 31 F6 }
        $rout2 = { 48 8B 05 E2 EA 24 00 48 31 E0 48 89 44 24 28 48 C7 44 24 20 00 00
00 00 81 FA BE FF FF 7F 0F 87 A2 00 00 00 89 D6 48 89 CF 8D 56 40 48 8D 4C 24 20 E8
B3 94 01 00 }
        $rout3 = { 44 0F B6 CD 46 8A 8C 0C 50 03 00 00 45 30 0C 0E 48 FF C1 48 39 C8
}
        $xor = { 33 6A 42 28 32 62 73 47 23 40 63 37 00 }
    condition:
        pe.characteristics & pe.DLL
        and all of them
        and filesize < 3MB
}
```

About Cado Security

Cado Security is *the* cloud investigation and response automation company. The Cado platform leverages the scale, speed and automation of the cloud to effortlessly deliver forensic-level detail into cloud, container and serverless environments. Only Cado empowers security teams to investigate and respond at cloud speed.

Prev Post Next Post