

3CX supply chain attack analysis | ThreatLabz

By Rohit Hegde, Niraj Shिवtarkar, Meghraj Nandanwar

Published: 2023-03-31 · Archived: 2026-04-05 20:33:42 UTC

Infection Chain

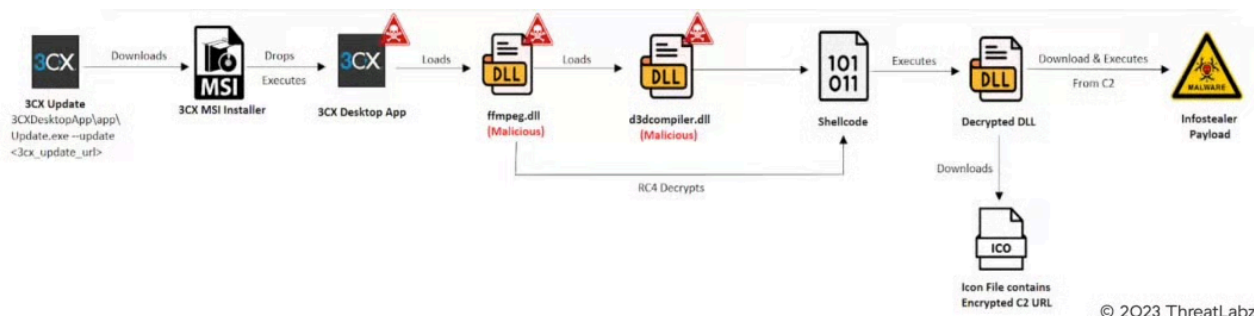


Fig.2 - Infection Chain

The Infection chain begins with the software update routine where the 3CXDesktopApp calls the “Update.exe --update ” from its bundle to fetch the updates. This then downloads the valid signed Malicious 3CX MSI installer and the Affected 3CX MAC Application as required in the form of an update package on the victim's machine as shown in the screenshot below.

```
© 2023 ThreatLabz
> Mar 28, 2023 @ 20:19:45.000 - .3cx. /electron/update/win32/18.12.416/releases?id=3CXDesktopApp&localVersion=18.12.416&arch=amd64
> Mar 28, 2023 @ 19:36:52.000 - .3cx. /electron/update/win32/18.11.1213/releases?id=3CXDesktopApp&localVersion=18.11.1213&arch=amd64
> Mar 28, 2023 @ 19:36:31.000 - .3cx. /electron/update/win32/18.11.1213/releases?id=3CXDesktopApp&localVersion=18.11.1213&arch=amd64
> Mar 28, 2023 @ 19:07:37.000 - .3cx. /electron/update/win32/18.12.416/releases?id=3CXDesktopApp&localVersion=18.12.416&arch=amd64
```

Fig.3 - Requests to 3CX domain to download the Affected 3CX MSI installer v18.12.416 & 3CX Mac App v18.12.416 as an Update Package

In this blog, we will take a look at the affected valid signed 3CX MSI Installer version 18.12.416 named “3CXDesktopApp-18.12.416.msi” which is signed on March 13, 2023.

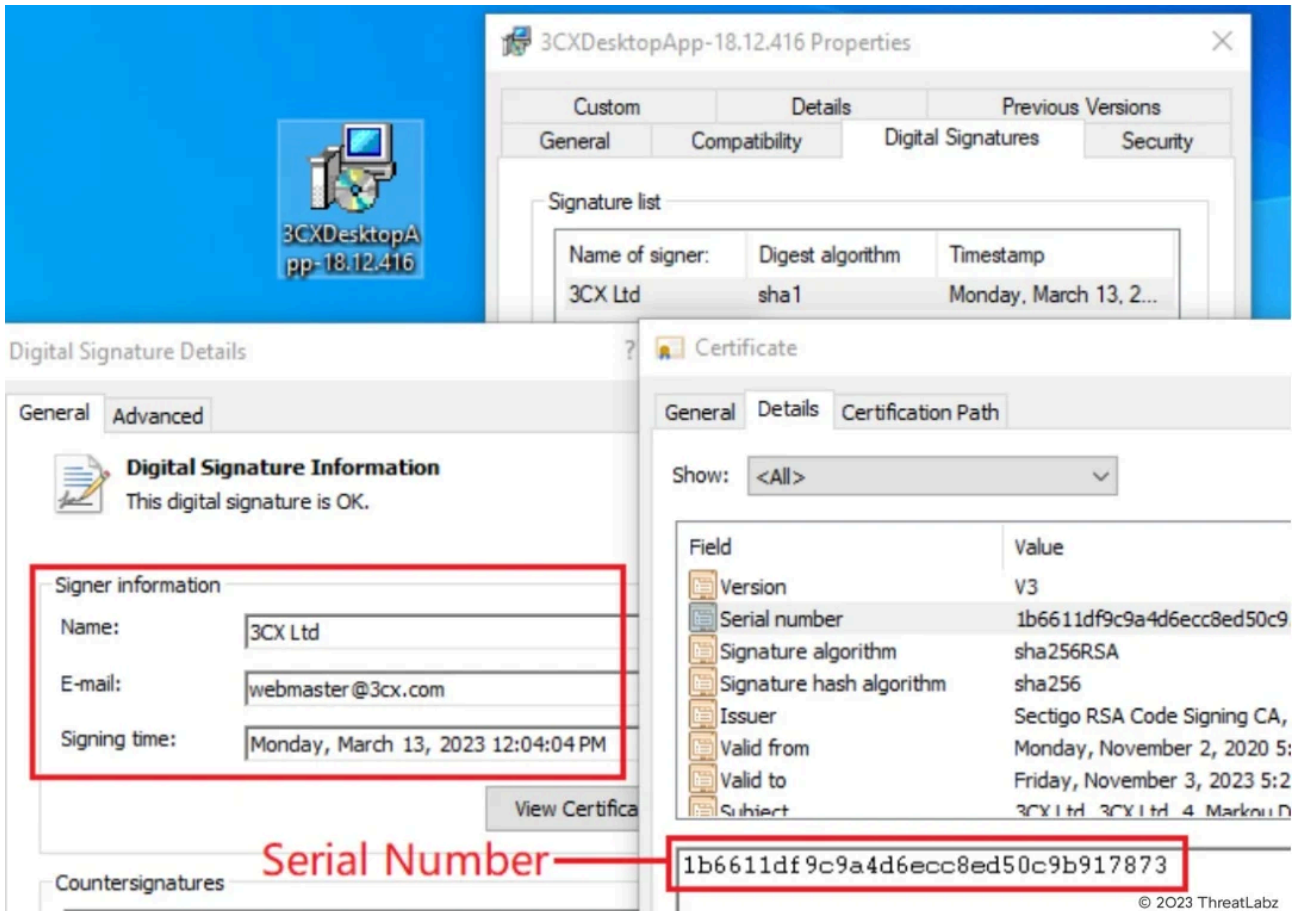


Fig.4 - Signed 3CX MSI Installer

Upon execution the 3CX MSI installer extracts multiple files in the “AppData\Local\Programs\3CXDesktopApp” and then executes the valid signed **3CXDesktopApp.exe** as shown below in the screenshot.

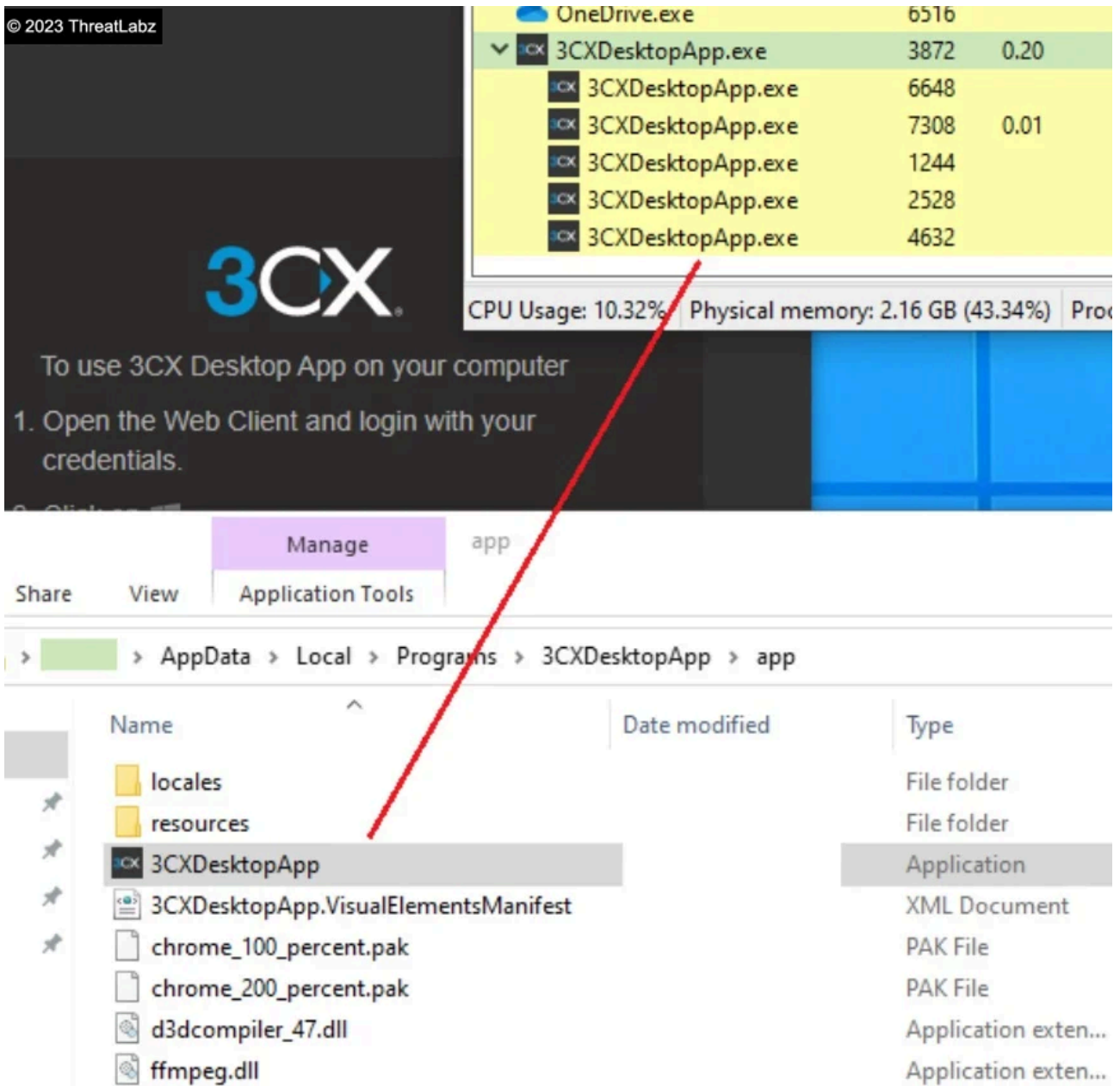
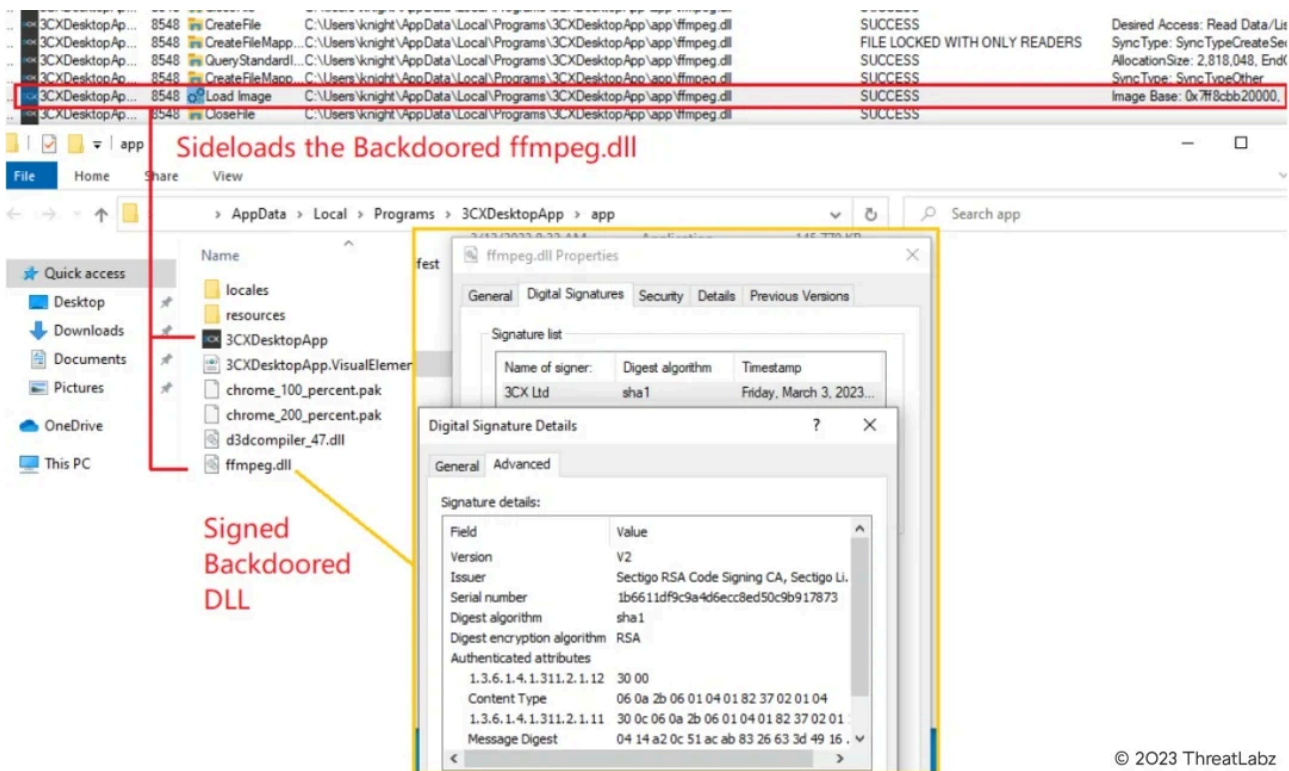


Fig.5 - Execution of 3CXDesktopApp

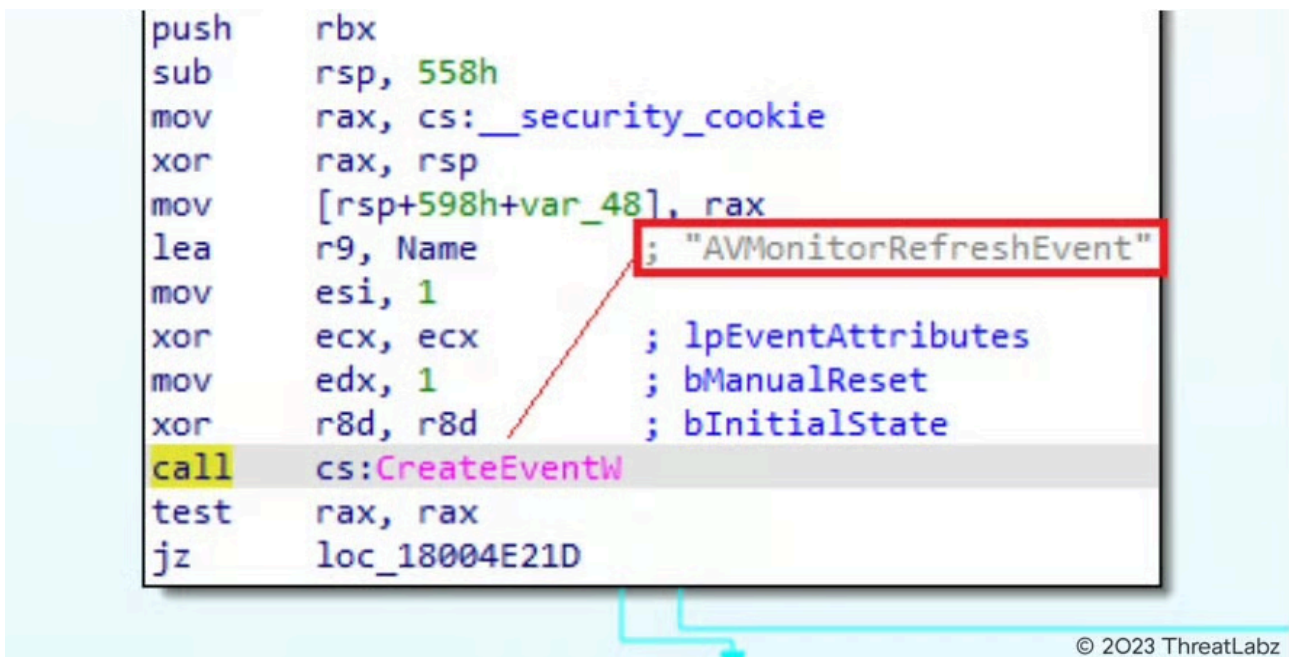
Further the 3CXDesktopApp.exe side loads the Backdoored signed DLL named “ffmpeg.dll” as based on the DLL search order mechanism if the DLL is present in the applications directory the DLL is loaded from there as shown in the screenshot.



© 2023 ThreatLabz

Fig.6 - 3CXDesktopApp sideloads the Backdoored “ffmpeg.dll”

Based on reports, the ffmpeg.dll was backdoored by the Threat Actors via manipulating the source code leading to the Supply Chain Attack. Once loaded into the virtual memory, the malicious “ffmpeg.dll” is commissioned to load the **d3dcompiler_47.dll** which contains the encrypted second stage payload. Initially the main function creates an event called "AVMonitorRefreshEvent" and checks if it already exists. If it does, it exits.



© 2023 ThreatLabz

Fig.7 - Main function of ffmpeg.dll

After that it checks the current path in order to load the d3dcompiler_47.dll into memory and further loads the DLL into memory and checks if the DLL loaded correctly by comparing the starting byte of DLL.

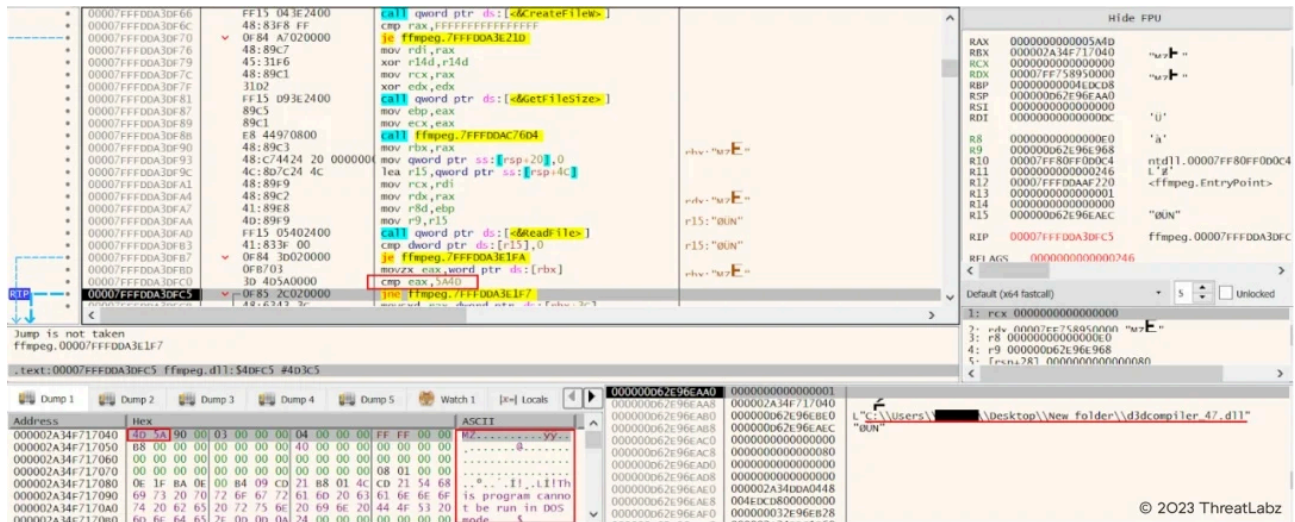


Fig.8 - Load d3dcompiler_47.dll and check for starting byte of DLL

In this case the d3dcompiler_47.dll consisting of the RC4 encrypted shellcode and embedded DLL is valid signed by the Microsoft Digital certificate as shown in the screenshot below.

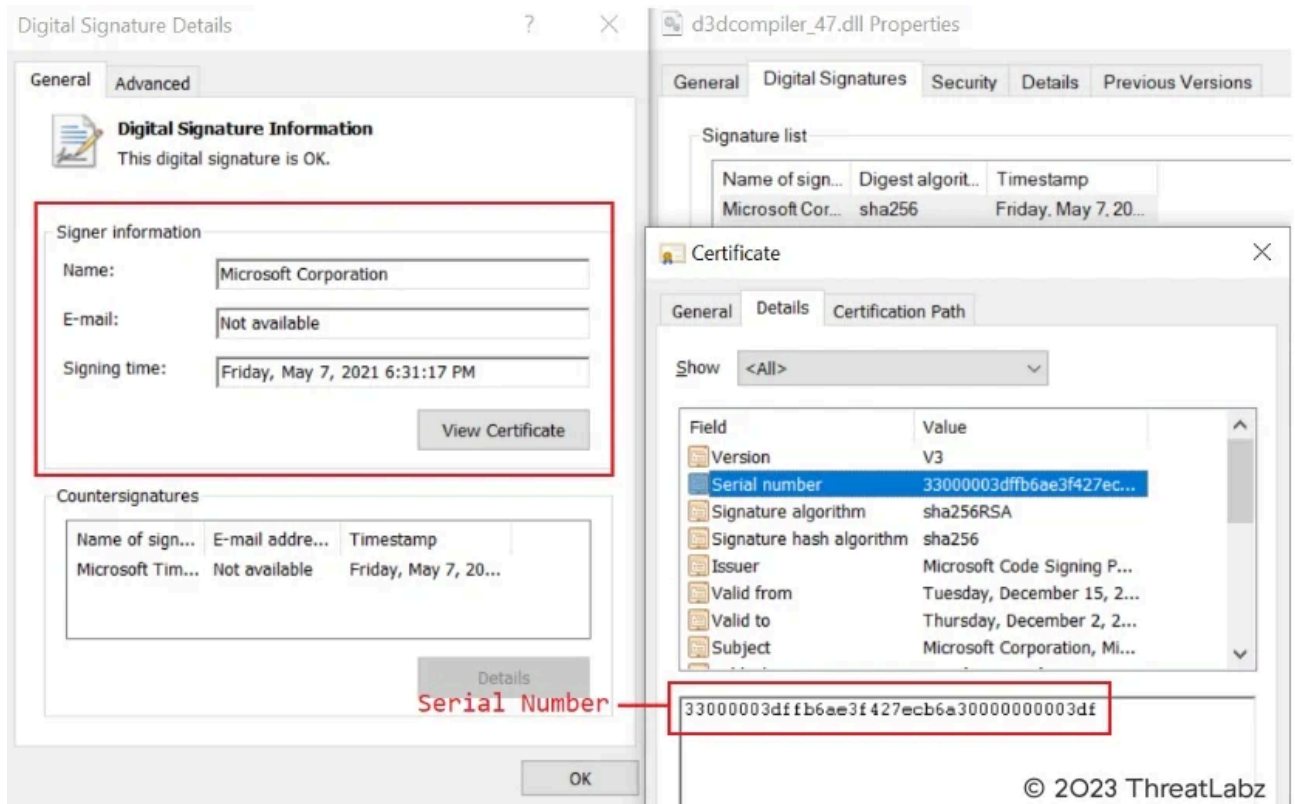


Fig.9 - Microsoft signed d3dcompiler_47.dll

Further in the infection chain, the ffmpeg.dll looks for the specific hex byte (FE ED FA CE) in the loaded d3dcompiler_47.dll which contains a second stage encrypted payload.

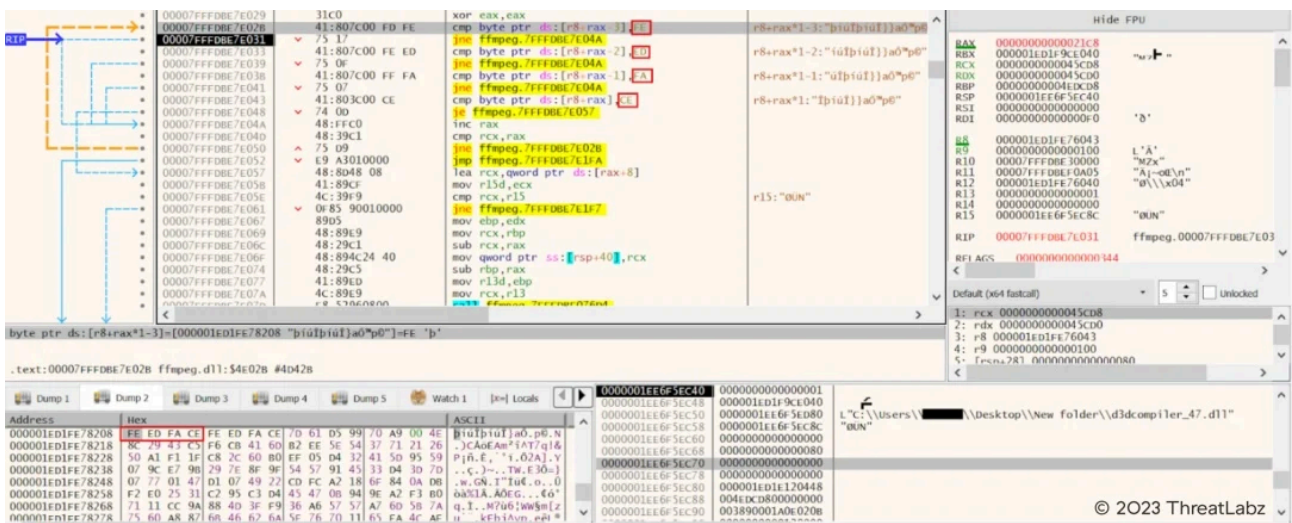


Fig.10 - Look for specific hex byte (FE ED FA CE) in loaded d3dcompiler_47.dll

After it locates the specific hex in loaded d3dcompiler_47.dll, it uses the RC4 decryption with the key “3jB(2bsG#@c7” to decrypt the second stage payload which is a shellcode with embedded DLL. The shellcode is responsible for calling the export function “DllGetClassObject” of the second stage DLL to execute and download further stage payload.

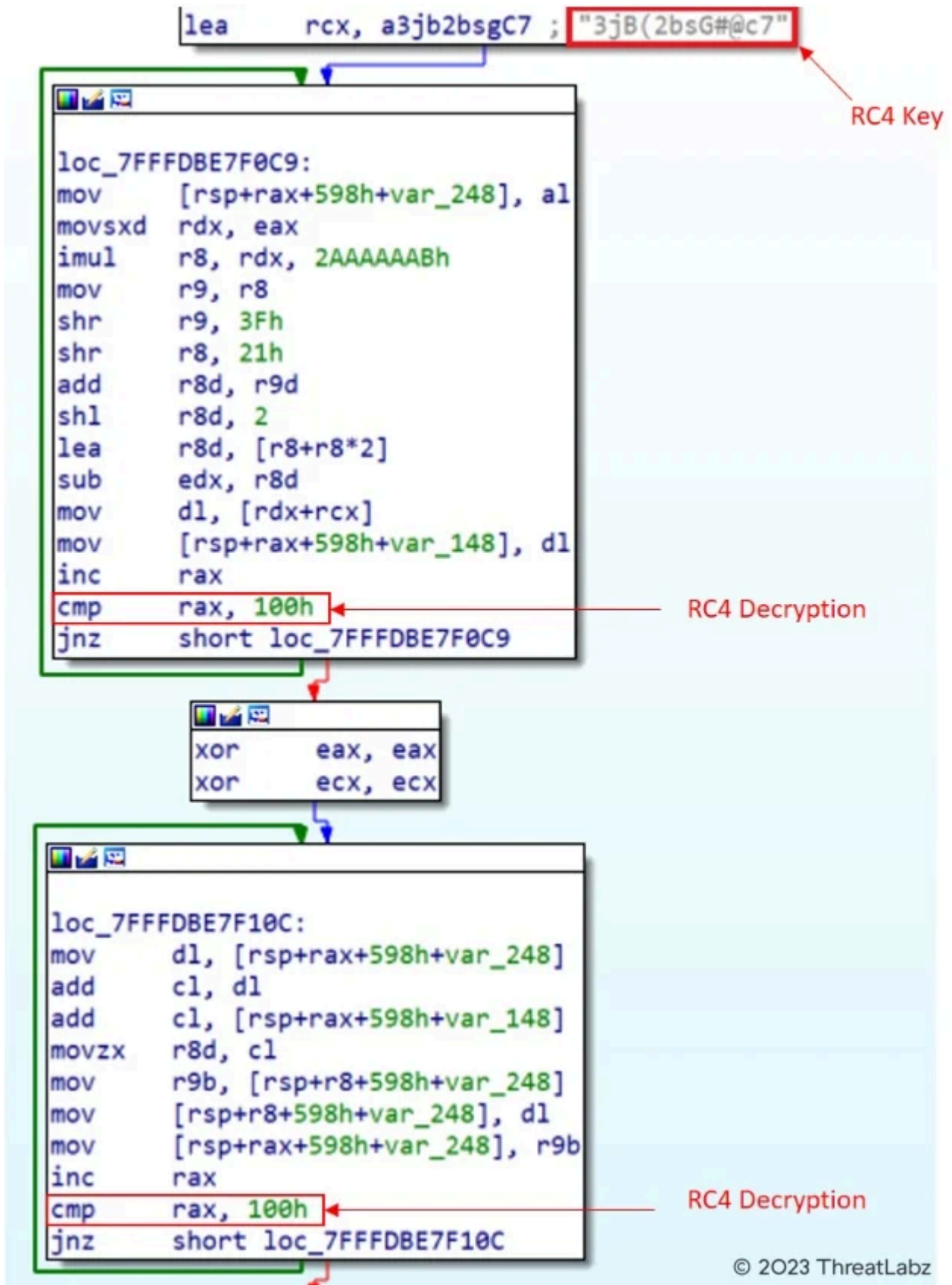


Fig.11 - Decryption of second stage payload

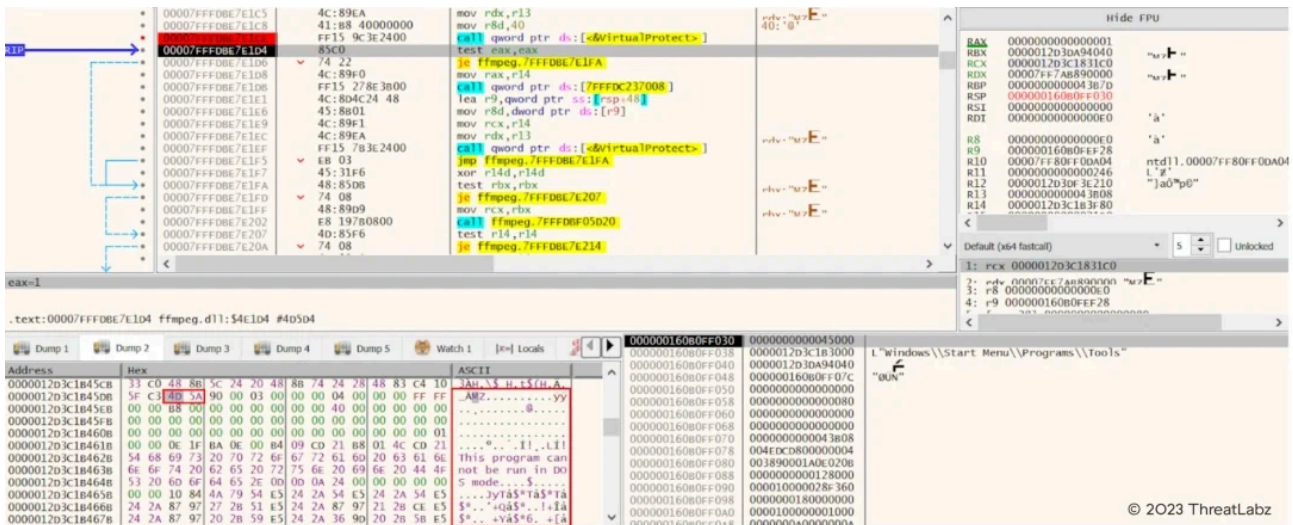


Fig.12 - Decrypted second stage payload

The Stage-2 DLL further downloads the Icon file from the following Github repository as shown below. We observed in some cases that the second stage decrypted DLL would sleep for more than 7 days before communicating with the C2 server.

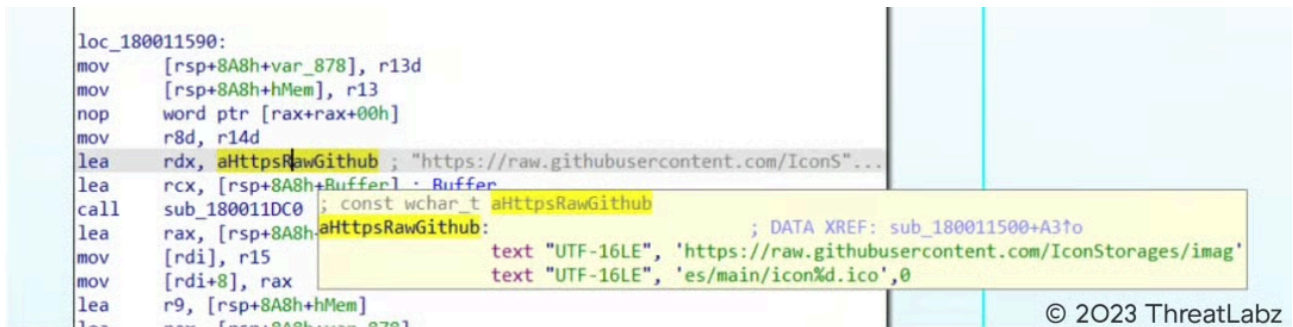
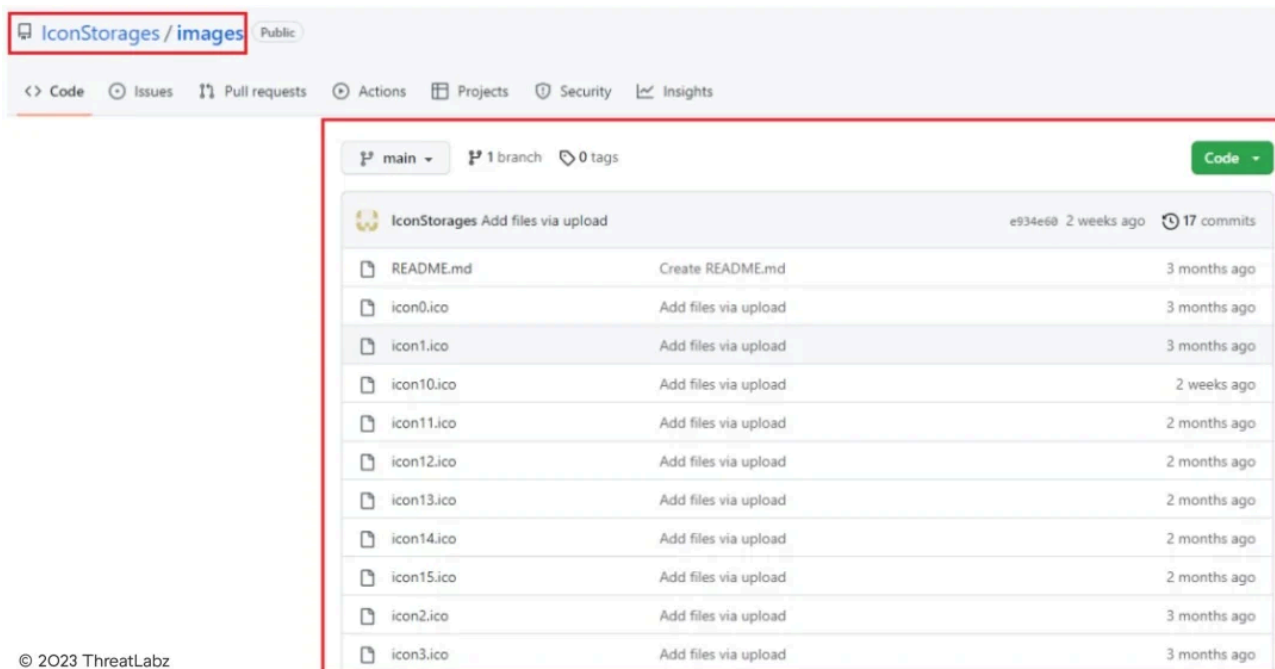


Fig.13 - Second Stage payload downloads icon files from GitHub Repository

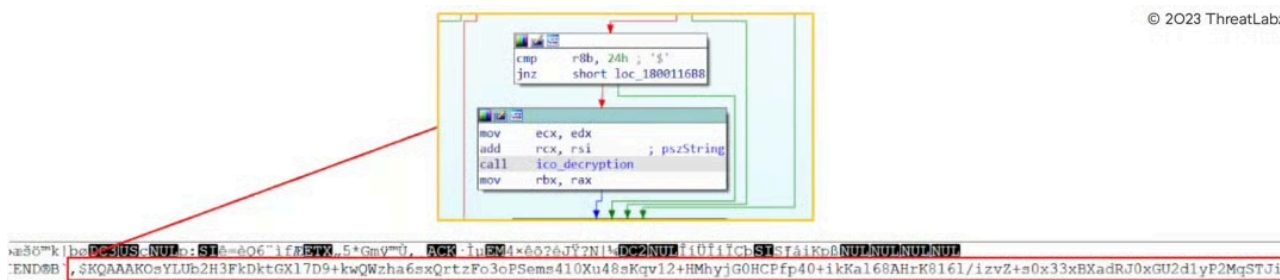
The github repository consists of multiple icon files as shown below. These icons are been downloaded by the Stage-2 DLL.



© 2023 ThreatLabz

Fig.14 - Github Repository hosting multiple icon files.

Further the Stage-2 DLL reads the icon file and parses the encrypted string present at the end of the downloaded icon file and passes it to the ico_decryption() function.



© 2023 ThreatLabz

Fig.15 - Parsing of the Encrypted string in the ICON File

The encrypted string from the icon file is base64 decoded and then passed to a decryption routine as shown below in the screenshot. The decrypted string in this case is the C2 URL: **https[:]//glcloudservice[.]com/v1/console**

```

mov     [rsp+0A8h+pdwFlags], rbp ; pdwFlags
lea     rax, [rsp+0A8h+var_50]
mov     [rsp+0A8h+pdwSkip], rbp ; pdwSkip
mov     r9, rsi           ; pbBinary
mov     r8d, 1           ; dwFlags
mov     [rsp+0A8h+pcbBinary], rax ; pcbBinary
mov     edx, ebx         ; cchString
mov     rcx, rdi         ; pszString
call    cs:CryptStringToBinaryA
xor     eax, eax

loc_180010DD0:
mov     ecx, eax
imul   edx, r9d, 12BF507Dh
shl    ecx, 5
xor    eax, ecx
mov    r9d, r10d
mov    ecx, eax
shr    ecx, 7
xor    eax, ecx
add    edx, 12D687h
mov    ecx, eax
shl    ecx, 16h
xor    eax, ecx
mov    ecx, r8d
imul   r9, rdi
imul   r8d, edx, 12BF507Dh
add    r9, rcx
mov    r10d, r9d

```

Icon File Decryption Routine

© 2023 ThreatLabz

Fig.16 - Decryption of C2 URL from the encrypted string parsed via the ICON File

Further the malware performs HTTPS requests to the C2 URL as shown in the screenshot below from the Zscaler Cloud.

```

> Mar 24, 2023 @ 10:56:51.000 glcloudservice.com glcloudservice.com/v1/console Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 3CXDesktopApp/18.11.1197
Chrome/102.0.5005.167 Electron/19.1.9 Safari/537.36
> Mar 24, 2023 @ 10:34:31.000 glcloudservice.com glcloudservice.com/v1/console Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 3CXDesktopApp/18.11.1197
Chrome/102.0.5005.167 Electron/19.1.9 Safari/537.36

```

© 2023 ThreatLabz

Fig.17 - HTTPS Requests to the C2 URL seen in the Zscaler Cloud

At the time of analysis the C2 Domains were down. The expected response would be in JSON format consisting of encrypted data which is then decrypted by the decryption routine before the final payload is executed on the infected machine.

Based on the [blog](#) published by Sentinel One, the final payload delivered on the target machines in the supply chain attack was an Infostealer with capabilities such as collecting system information and browser information such as saved credentials from the Brave, Chrome, Edge, and Firefox

Source: <https://www.zscaler.com/security-research/3CX-supply-chain-attack-analysis-march-2023>