3CX supply chain attack analysis

zscaler.com/security-research/3CX-supply-chain-attack-analysis-march-2023

On March 29th 2023, CrowdStrike published a blog outlining a supply chain attack leveraging the 3CXDesktopApp - a softphone application from 3CX. The ThreatLabz Team immediately started hunting for IoCs on the Zscaler Cloud.

We observed infections dating back to **February 2023** for both the Windows as well as the MacOS variant of the Trojanized 3CXDesktopApp installers.

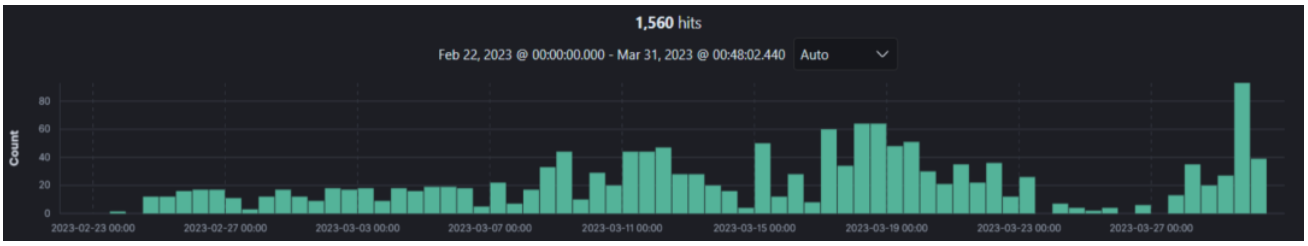

Fig.1 - Infections dating back to February 2023 in Zscaler Cloud

In this case the Threat Actors targeted various industry verticals such as:

- Technology
- Services
- Manufacturing and more

Further let's analyze the Infection Chain for the 3CX Supply Chain Attack:

Infection Chain:

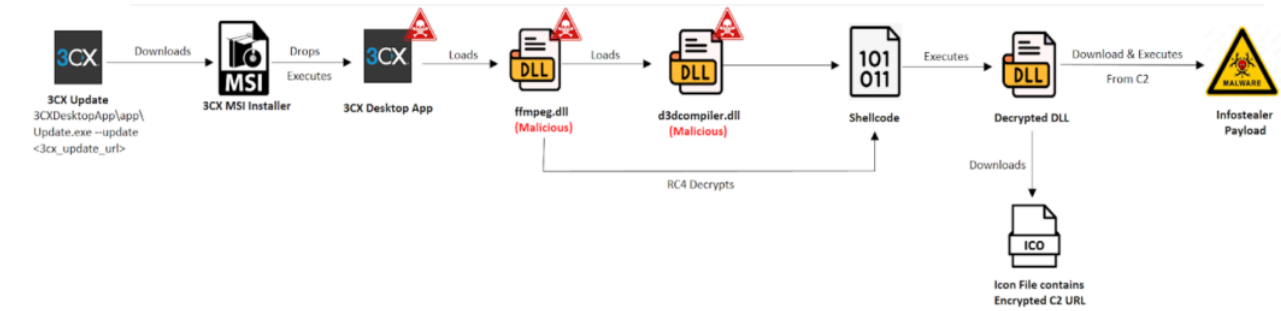

Fig.2 - Infection Chain

The Infection chain begins with the software update routine where the 3CXDesktopApp calls the “Update.exe --update <3cx_update_url>” 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.

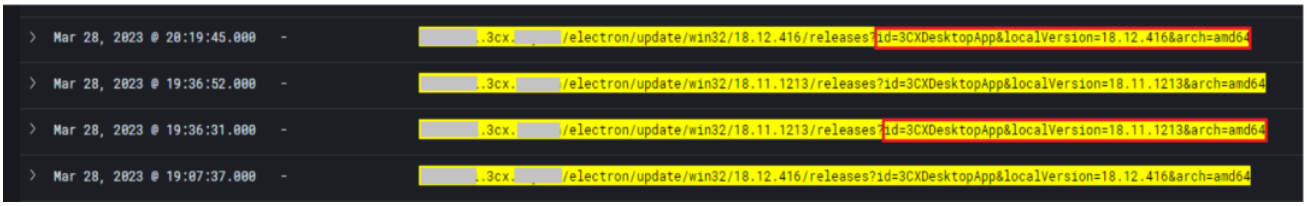

Fig.3 - Requests to 3CX domain to download the Affected 3CX MSI installer v18.12.416 & 3CX Mac App v18.12.416 as an Update Package

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.

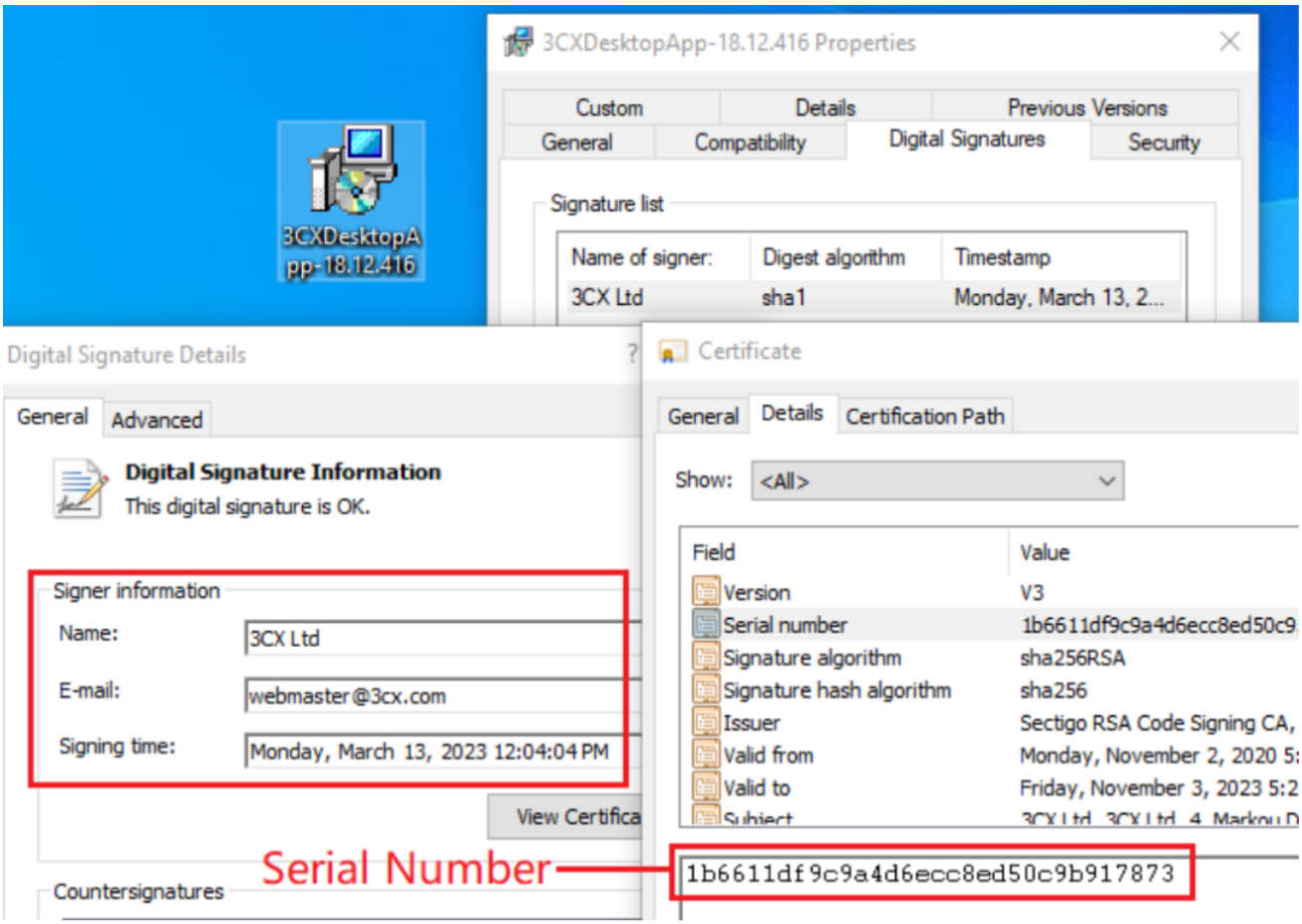

Fig.4 - Signed 3CX MSI Installer

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.

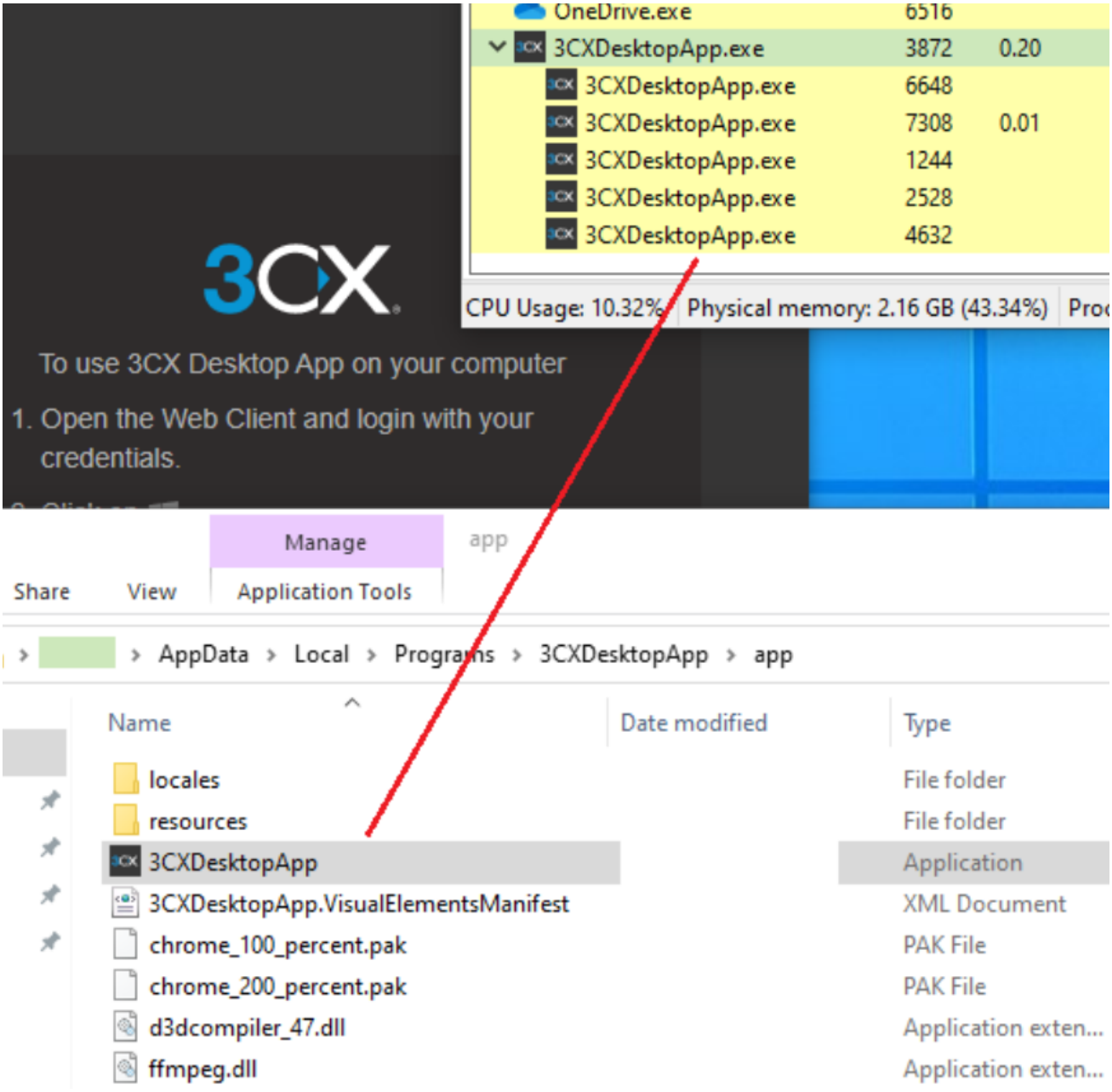

Fig.5 - Execution of 3CXDesktopApp

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.

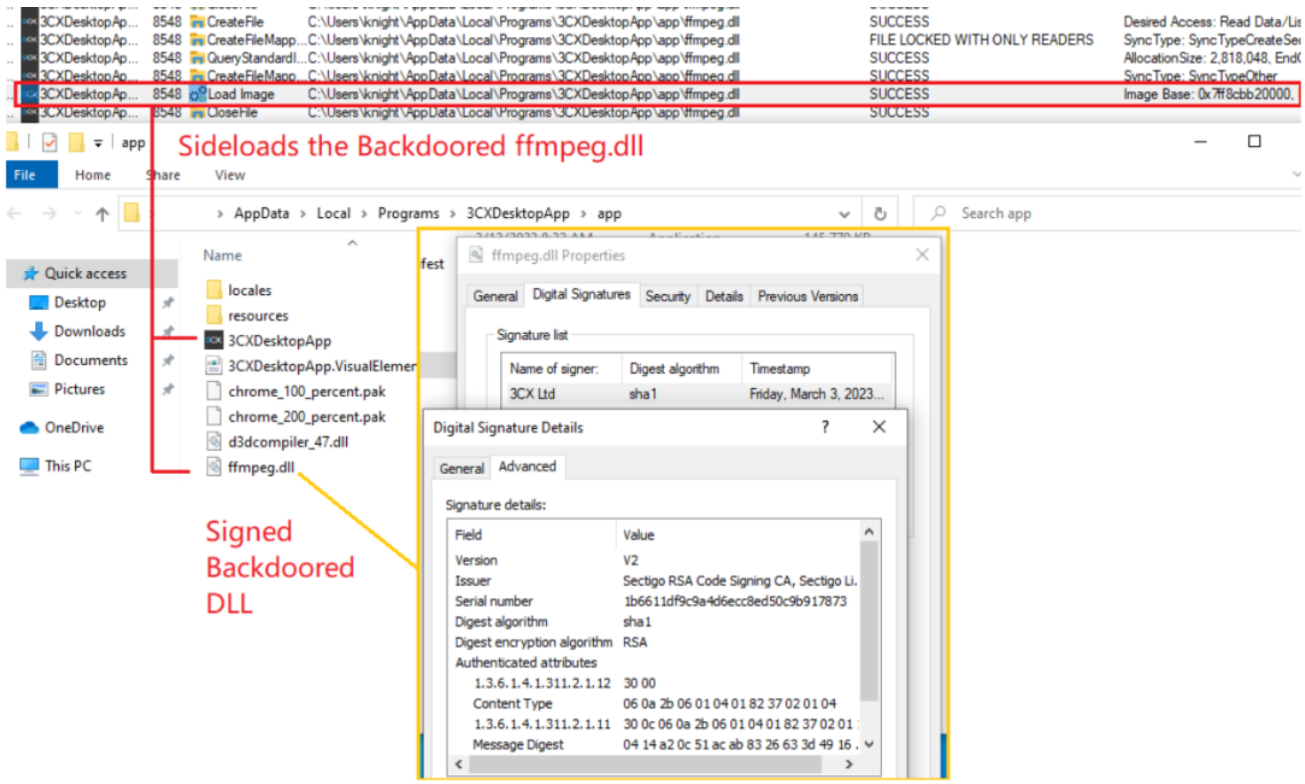

*Fig.6 - 3CXDesktopApp sideloads the Backdoored **"ffmpeg.dll"***

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.

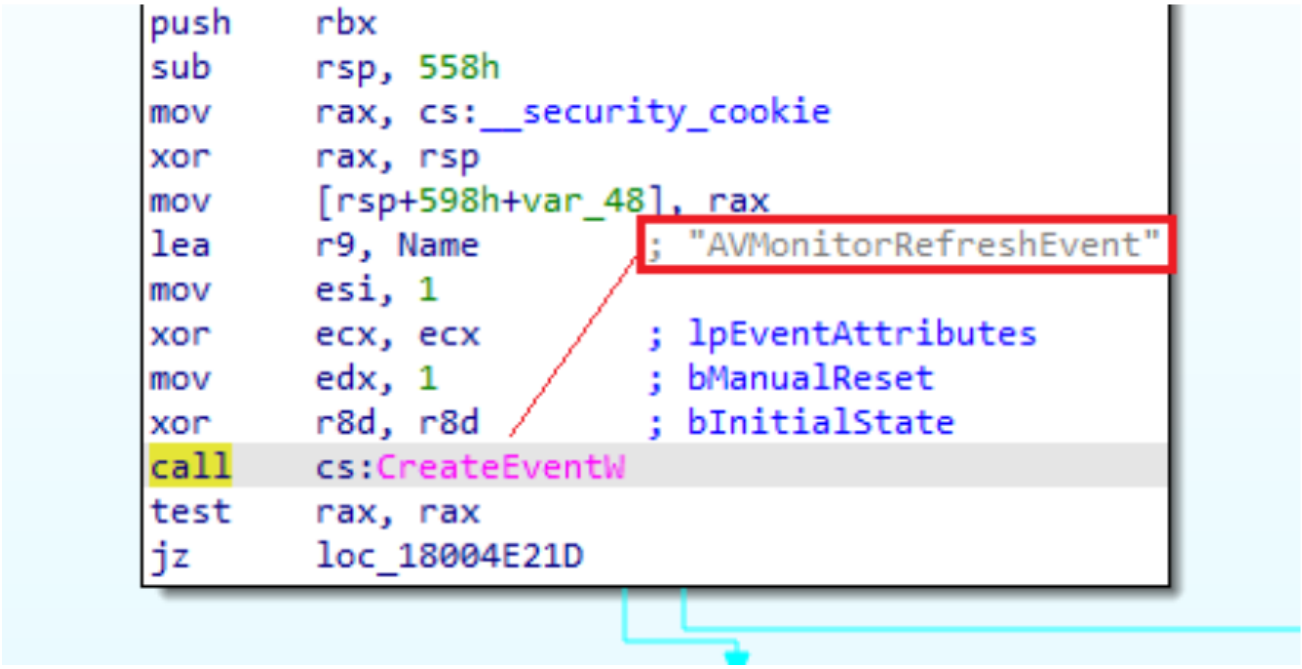

Fig.7 - Main function of ffmpeg.dll

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.

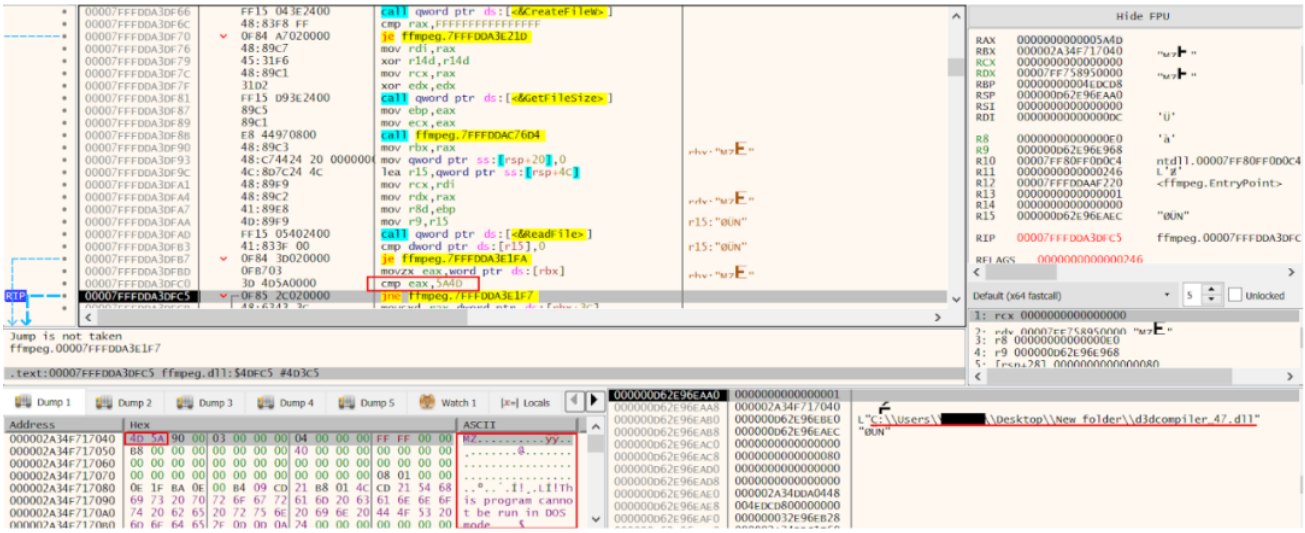

Fig.8 - Load d3dcompiler_47.dll and check for starting byte of DLL

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.

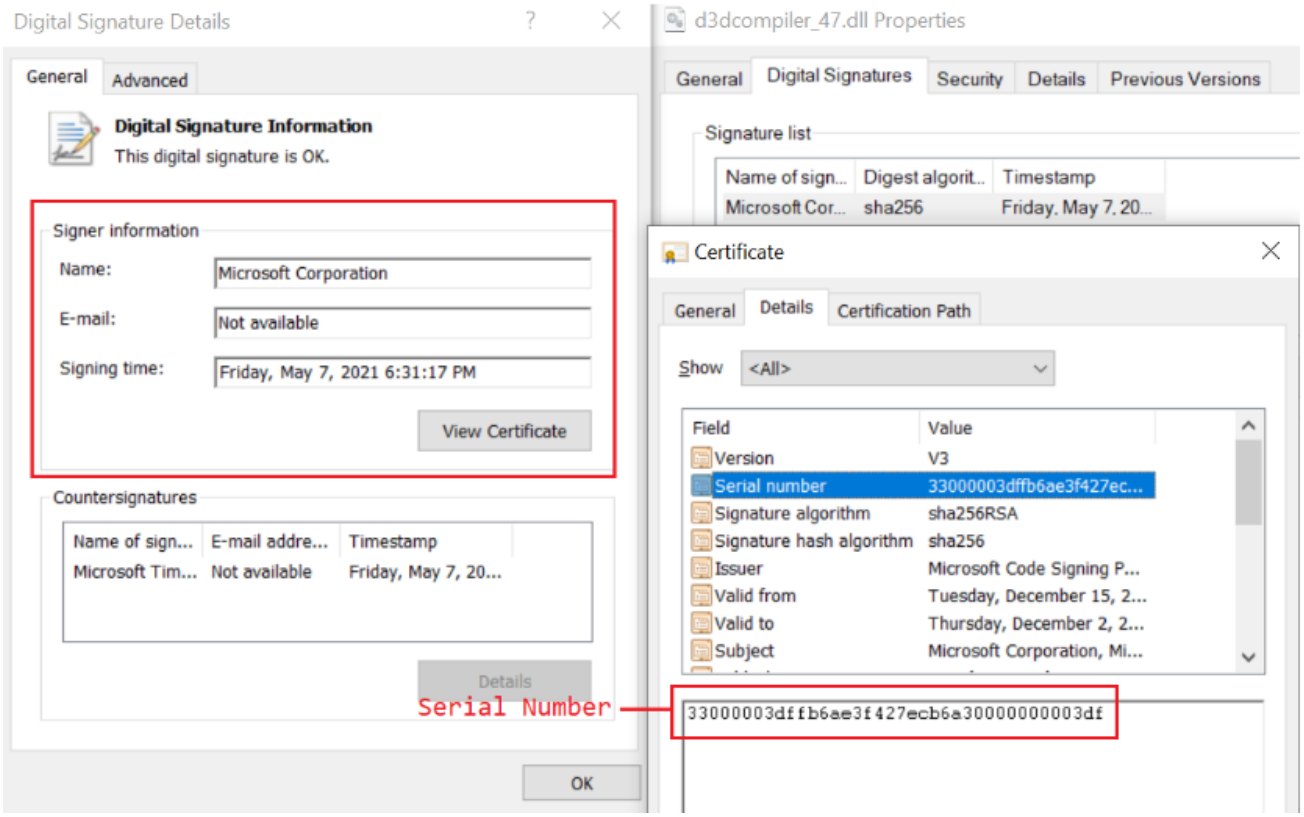

Fig.9 - Microsoft signed d3dcompiler_47.dll

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

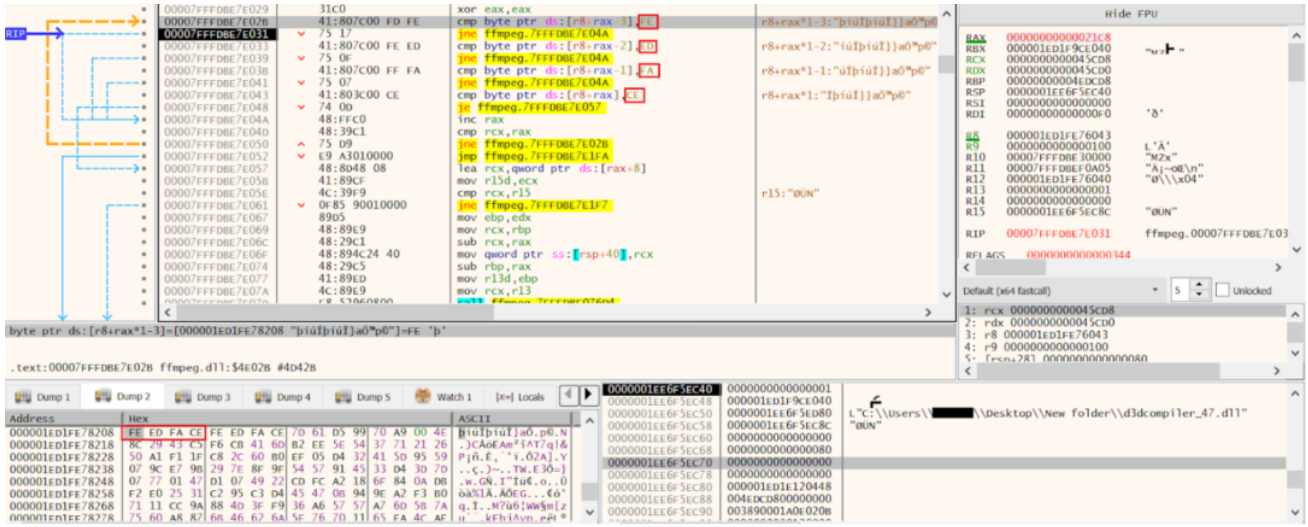

Fig.10 - Look for specific hex byte (FE ED FA CE) in loaded d3dcompiler_47.dll

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.

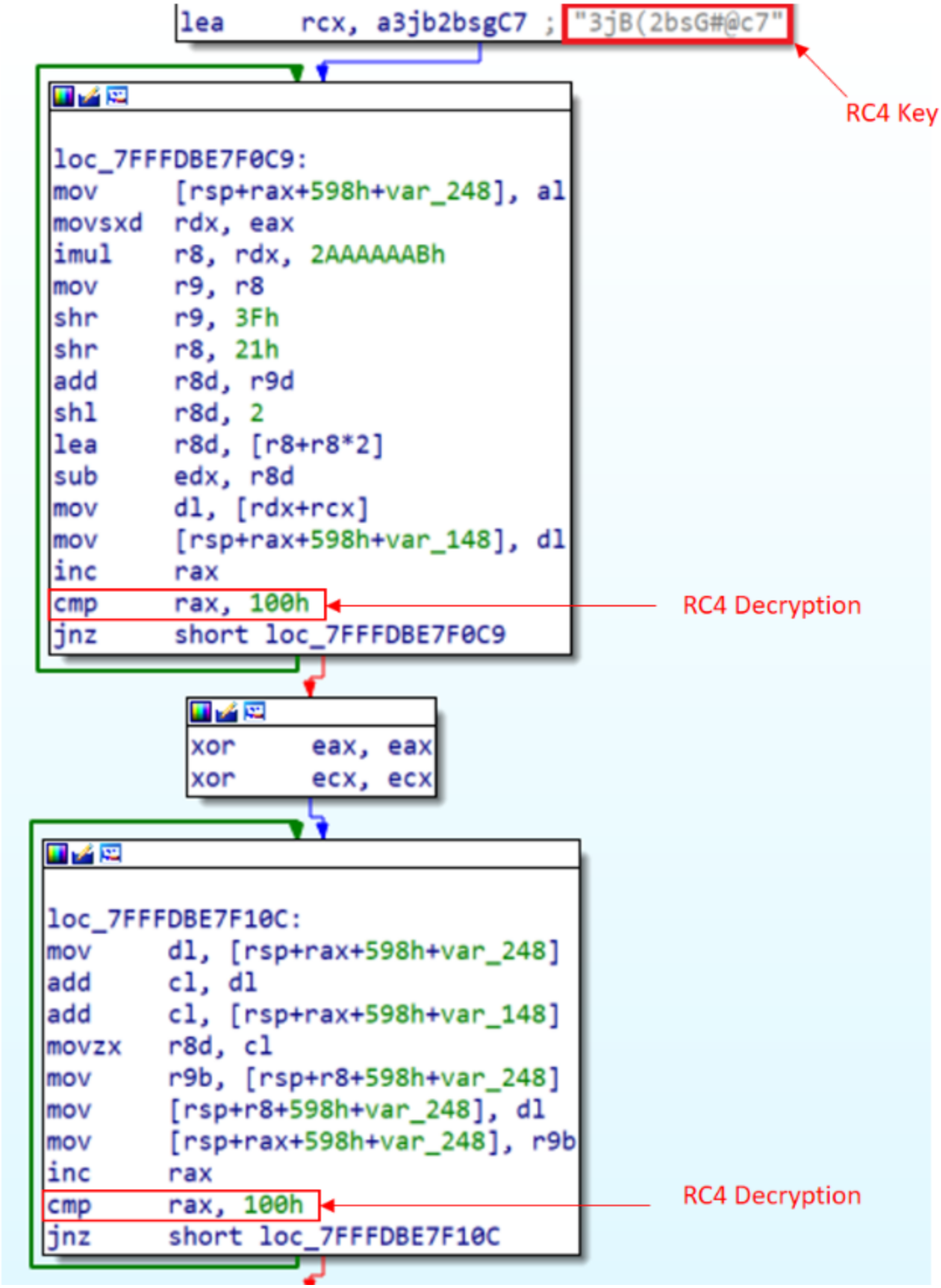

Fig.11 - Decryption of second stage payload

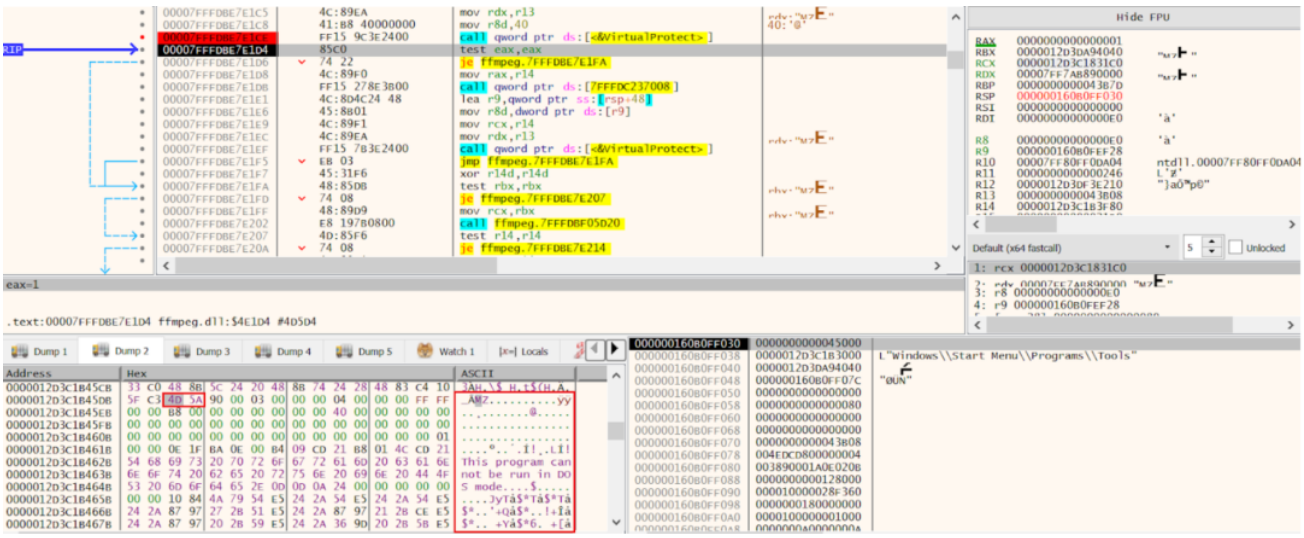

Fig.12 - Decrypted second stage payload

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.

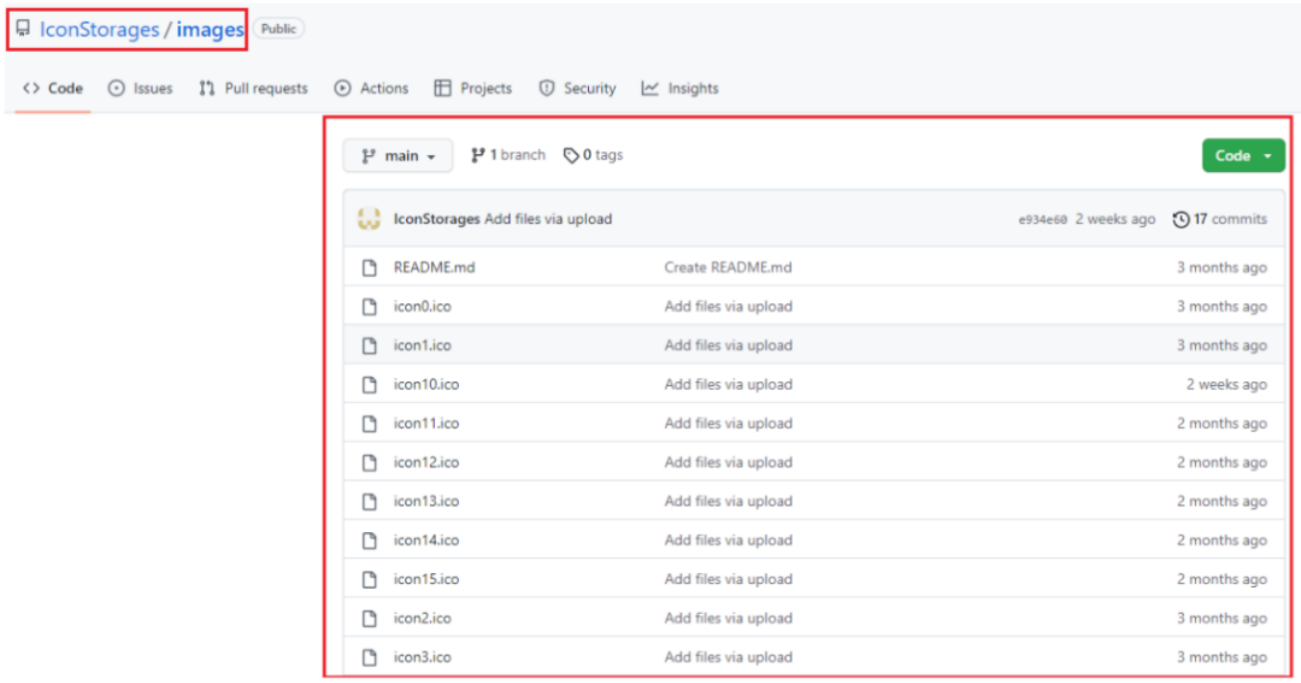

Fig.14 - Github Repository hosting multiple icon files.

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.

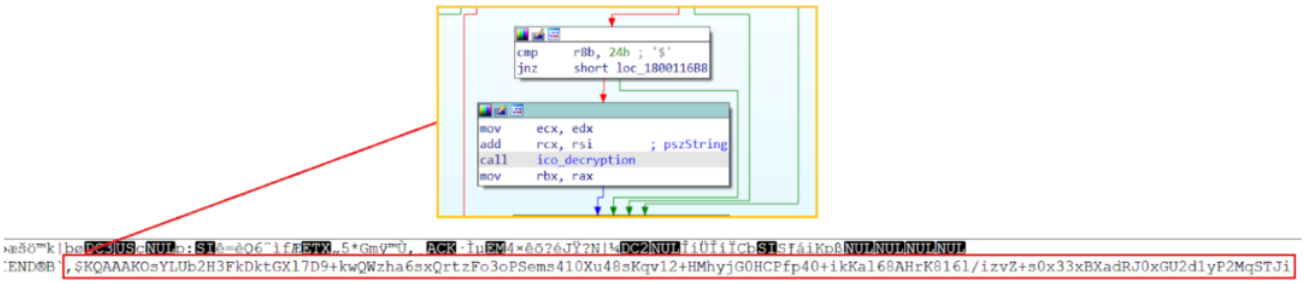

Fig.15 - Parsing of the Encrypted string in the ICON File

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**

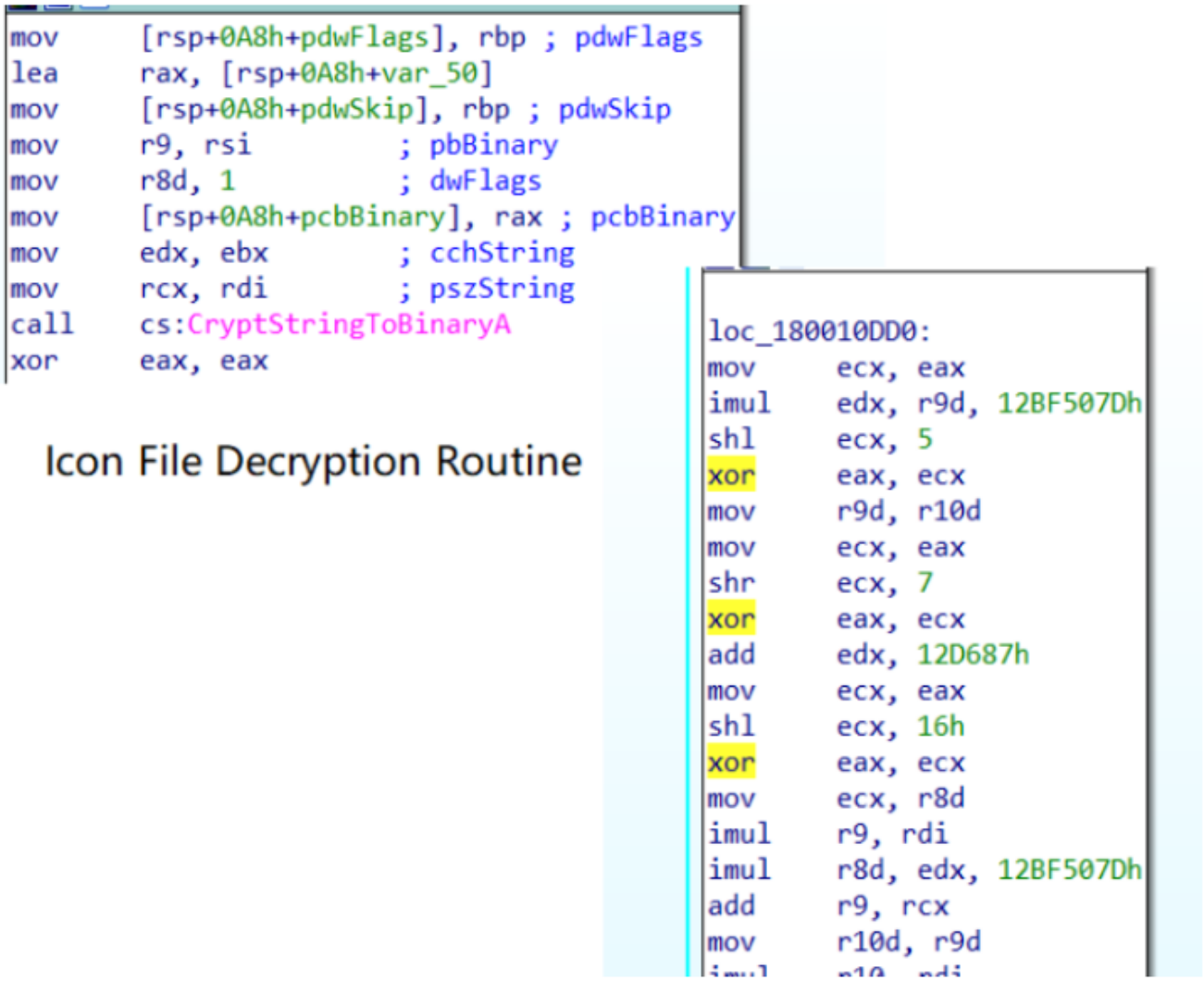

Fig.16 - Decryption of C2 URL from the encrypted string parsed via the ICON File

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

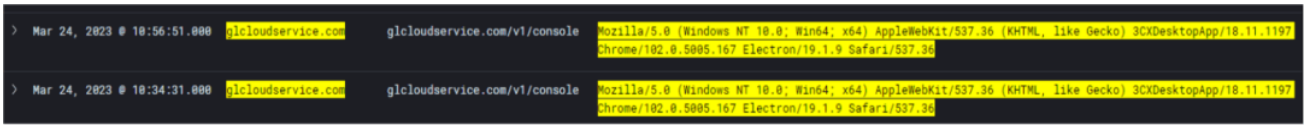

Fig.17 - HTTPS Requests to the C2 URL seen in the Zscaler Cloud

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

Affected 3CX Versions:

Following are the affected versions announced by 3CX:

Affected 3CX Electron Windows App Versions:

- 18.12.416
- 18.12.407

Affected Electron Mac App versions:

- 18.11.1213
- 18.12.402
- 18.12.407
- 18.12.416

IoCs:

File Name	Md5
3CXDesktopApp-18.12.416.msi	0eeb1c0133eb4d571178b2d9d14ce3e9
3CXDesktopApp.exe	704db9184700481a56e5100fb56496ce
ffmpeg.dll	cb01ff4809638410a531400a66376fa3
d3dcompiler_47.dll	82187ad3f0c6c225e2fba0c867280cc9

C2 Domains:

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

msedgeupdate[.]net