A Comprehensive Analysis of the 3CX Attack

blog.cyble.com/2023/03/31/a-comprehensive-analysis-of-the-3cx-attack

March 31, 2023

InfoStealer Deployed in a Massive Supply Chain Attack

An ongoing supply chain attack has been reported, targeting customers of 3CX, a VoIP IPBX software development company. This attack has been attributed to North Korean Threat Actors (TAs). Currently, the 3CX DesktopApp can be accessed on various platforms, including Windows, macOS, Linux, and mobile.

However, reports have indicated that the ongoing activity related to the supply chain attack has been detected on both Windows and macOS operating systems. The attack involves a Trojanized version of the 3CX, a Voice Over Internet Protocol (VOIP) desktop client, which has been digitally signed. 3CX's Phone System is utilized by over 600,000 companies globally and has over 12 million daily users.

The highlights of the incident are as follows:

- On March 29, a significant number of EDR providers and antivirus solutions began to identify and signal a warning for the legitimate 3CXDesktopApp.exe binary, which was signed.
- This binary had initiated an update procedure that ultimately led to malicious activity and communication with Command-and-Control servers.
- The 3CX download that was accessible on the official public website was infected with malware. Systems that had already been installed would undergo updates that would ultimately result in the download of this malware.
- The attack involves a multi-stage process that starts with the 3CX desktop application.
- The process of retrieving malicious payloads from GitHub involves a delay of 7 days before the download takes place. This delay could be an attempt to evade detection by security systems monitoring suspicious activities.

- As per reports, the last stage of the attack involves stealing information. This malware can gather system data and take control of data and login credentials stored in user profiles on various web browsers, including Chrome, Edge, Brave, and Firefox.
- Both the Windows and macOS installers for 3CX have been impacted.
- As per researchers, the evidence from GitHub indicates that the infrastructure utilized by the Windows variant was activated on December 7, 2022.
- Additionally, the domains and web infrastructure utilized in the attacks were registered as early as November 2022.

The 3CX Phone Management System can be implemented on-premises. Upon further investigation, we found that over 240,000 publicly exposed instances of this application.

The figure below shows the Shodan search results.

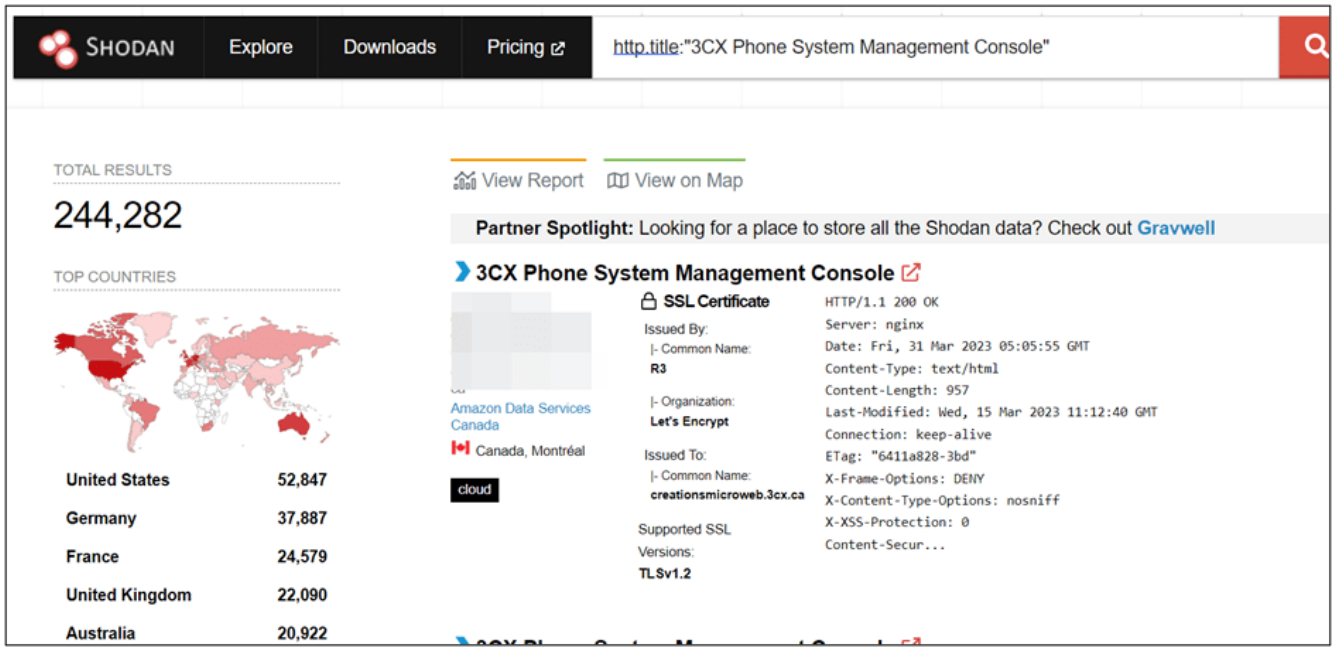

Figure 1 – Exposed Instances

We also came across a Reddit post where a user reported suspicious activity that occurred after updating the 3CX desktop on March 24, 2023. According to the user, the 3cxdesktopapp.exe program accessed browser caches, as revealed by EDR file history data.

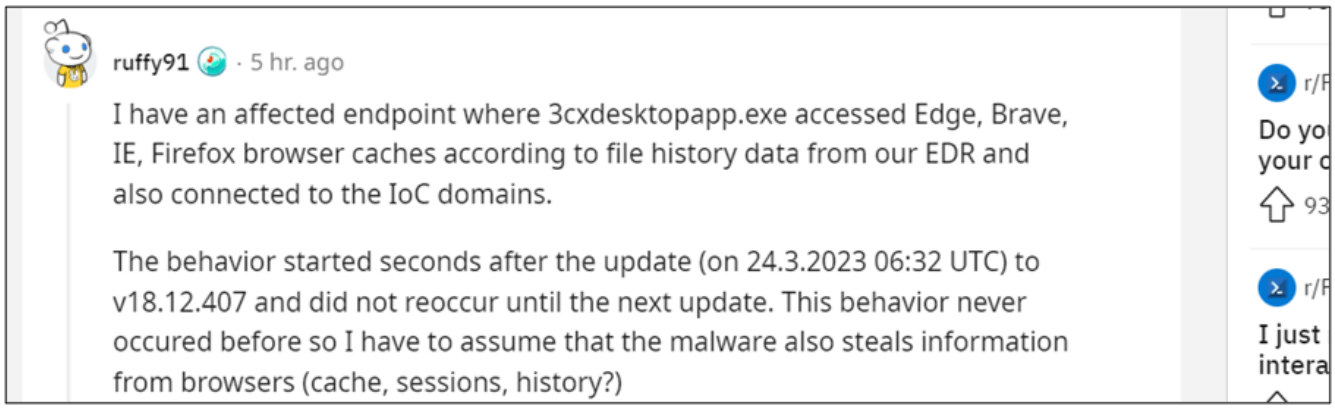

Figure 2 – Reddit Post

According to 3CX, the recent attack was a result of infected bundled libraries that were compiled into the Windows Electron App through GIT. The vendor has also stated, “Electron Windows App shipped in Update 7, version numbers 18.12.407 & 18.12.416, includes a security issue. Anti-Virus vendors have flagged the executable 3CXDesktopApp.exe and in many cases uninstalled it. Electron Mac App version numbers 18.11.1213, 18.12.402, 18.12.407 & 18.12.416 are also affected.”

The .msi file, when executed, drops two malicious files – “ffmpeg.dll” and “d3dcompiler_47.dll” – in the location *C:\Users[user_name]\AppData\Local\Programs\3CXDesktopApp\app*.

The infection begins when the benign file “3CXDesktopApp.exe” loads “ffmpeg.dll”. Then, “ffmpeg.dll” decrypts the encrypted code from “d3dcompiler_47.dll”, which seems to be a shellcode.

This shellcode loads another DLL file that tries to access the IconStorages GitHub page to find an .ico file containing the encrypted Command-and-Control (C&C) server. After locating the C&C server, the backdoor establishes a connection to retrieve the potential final payload.

The figure below shows the infection flow.

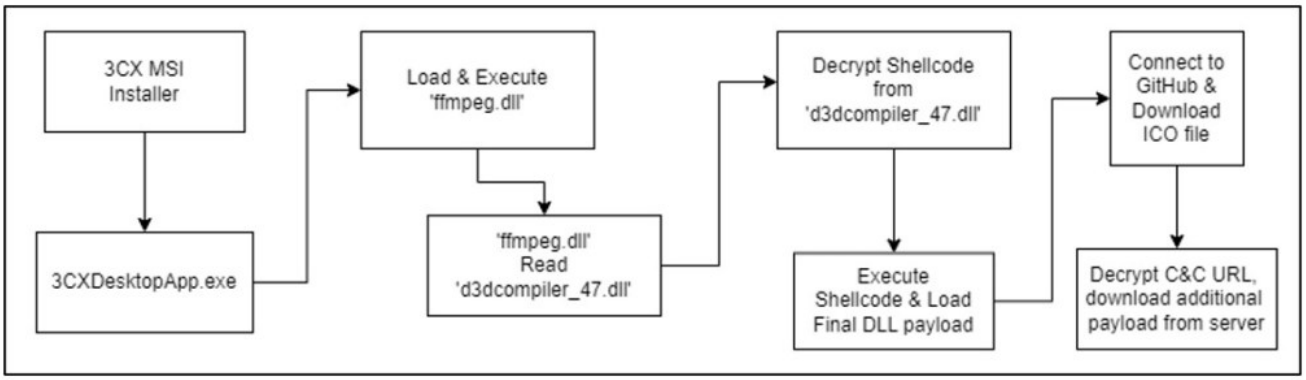

Figure 3 – Infection chain

Technical Analysis

The MSI package installer that has been compromised has a digital signature, and its appearance resembles that of a legitimate file, as shown below.

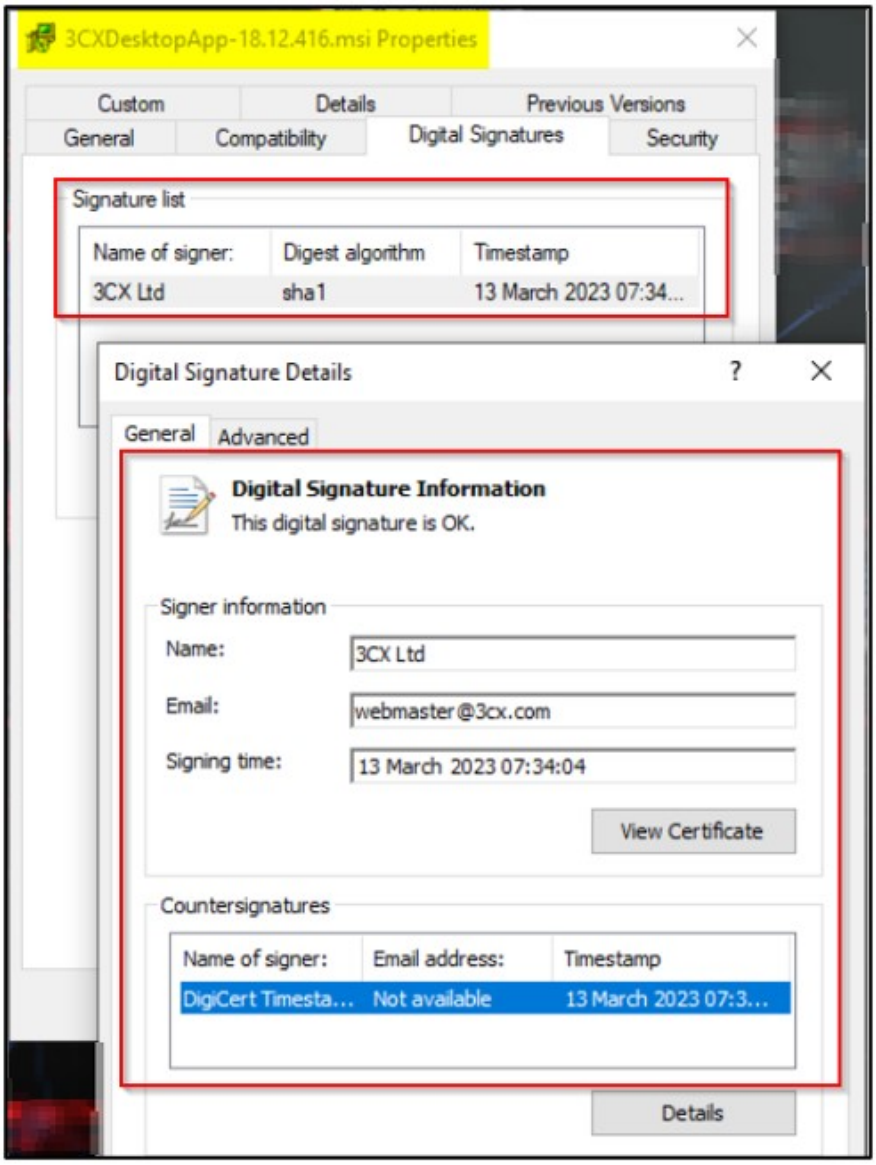

Figure 4 – Digitally signed MSI installer

Upon installation, the MSI package installer drops files such as “3CXDesktopApp.exe”, “ffmpeg.dll”, and “d3dcompiler_47.dll” in the *%LocalAppData%* directory of the system.

%LocalAppData%\Programs\3CXDesktopApp\app

These files are associated with malicious behavior and are accompanied by other supporting files.

The figure below displays the directory where the “3CXDesktopApp” application has been installed.

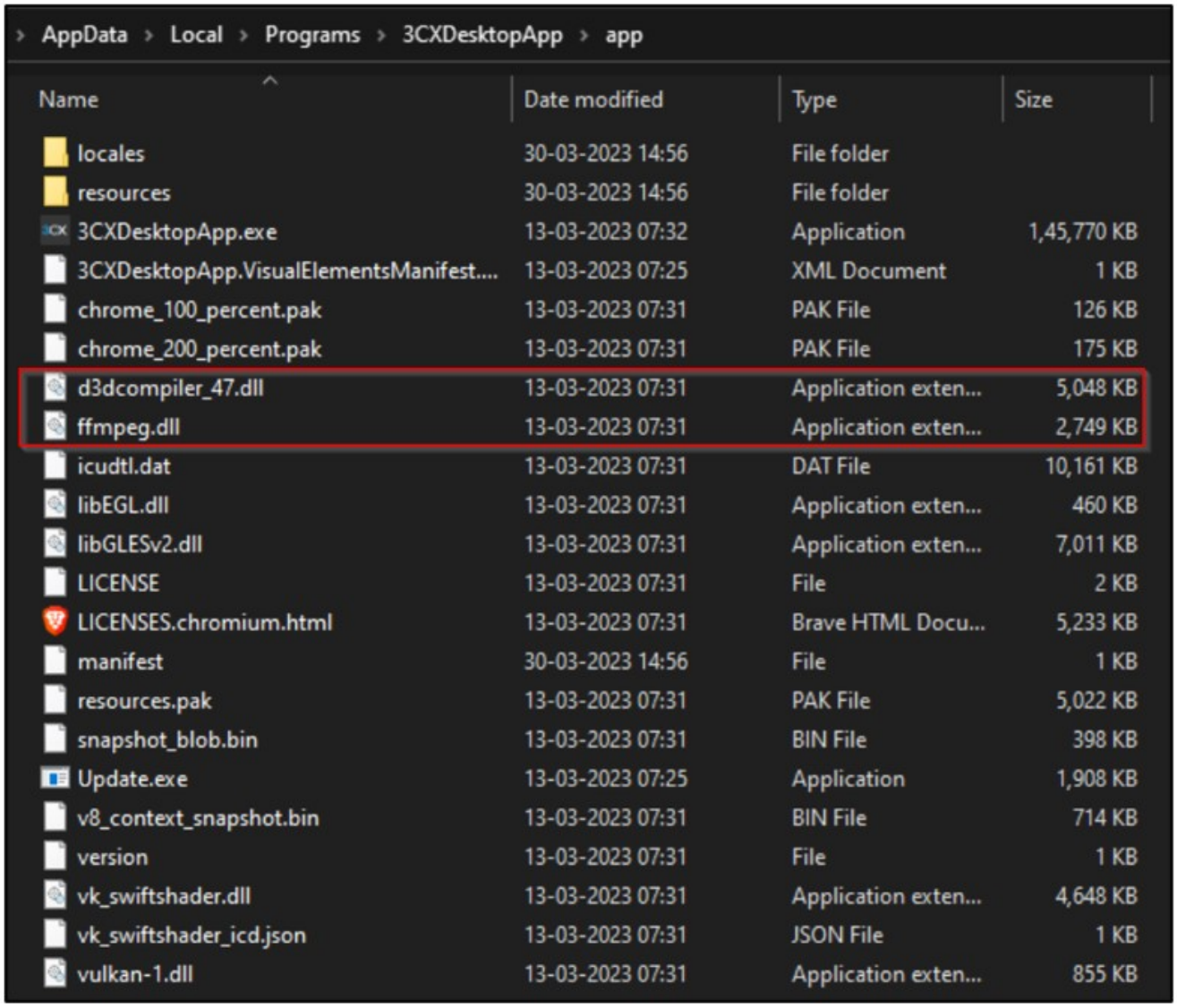

Figure 5 – 3CXDesktop installation folder

After installation, the “3CXDesktopApp.exe” file is executed, which is usually benign but can be utilized to load the malicious DLL, as shown below.

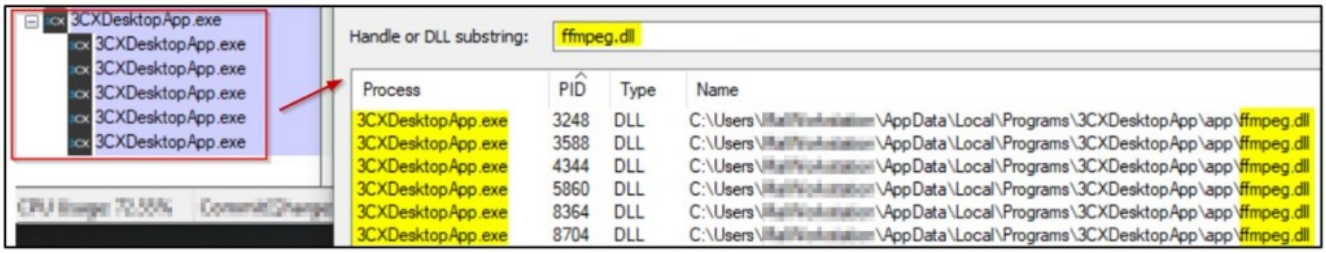

Figure 6 – 3CXDesktop.exe loading ffmpeg.dll file

The figure below illustrates the process tree of the “3CXDesktopApp” application.

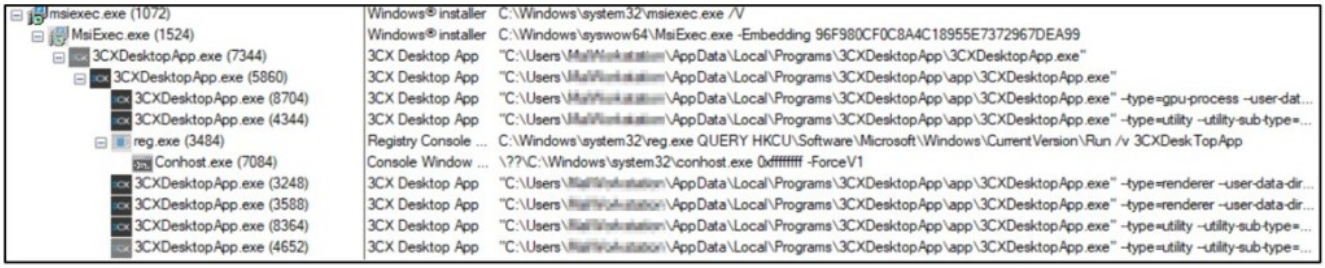

Figure 7 – Process tree

The “3CXDesktopApp.exe” loads the “ffmpeg.dll” file, which is a malicious DLL that has been specifically designed to read, load, and execute harmful shellcode from the “d3dcompiler_47.dll” file.

When executed, the “ffmpeg.dll” creates a new event, “*AVMonitorRefreshEvent*“, identifies the current file path, and searches for the next file in the sequence, which is “d3dcompiler_47.dll”. Once identified, the “ffmpeg.dll” loads the “d3dcompiler_47.dll” file into memory, as illustrated in the assembly code shown below.

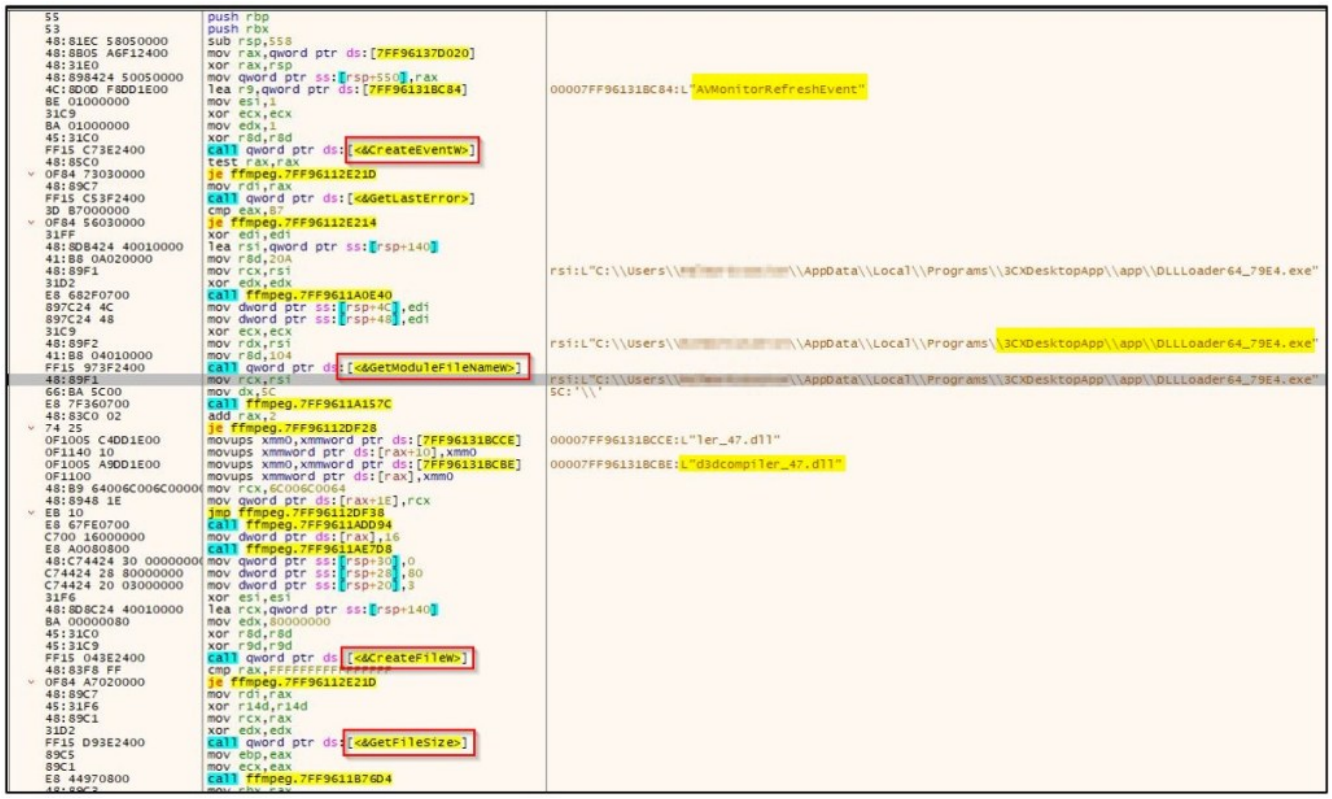

Figure 8 – ffmpeg.dll file is loading d3dcompiler_47.dll

Although the loaded “d3dcompiler_47.dll” is signed by Microsoft, it has an encrypted payload embedded within it. The “ffmpeg.dll” file now identifies the encrypted payload indicated by a particular marker, ‘0xCEFAEDFE’, as shown below.

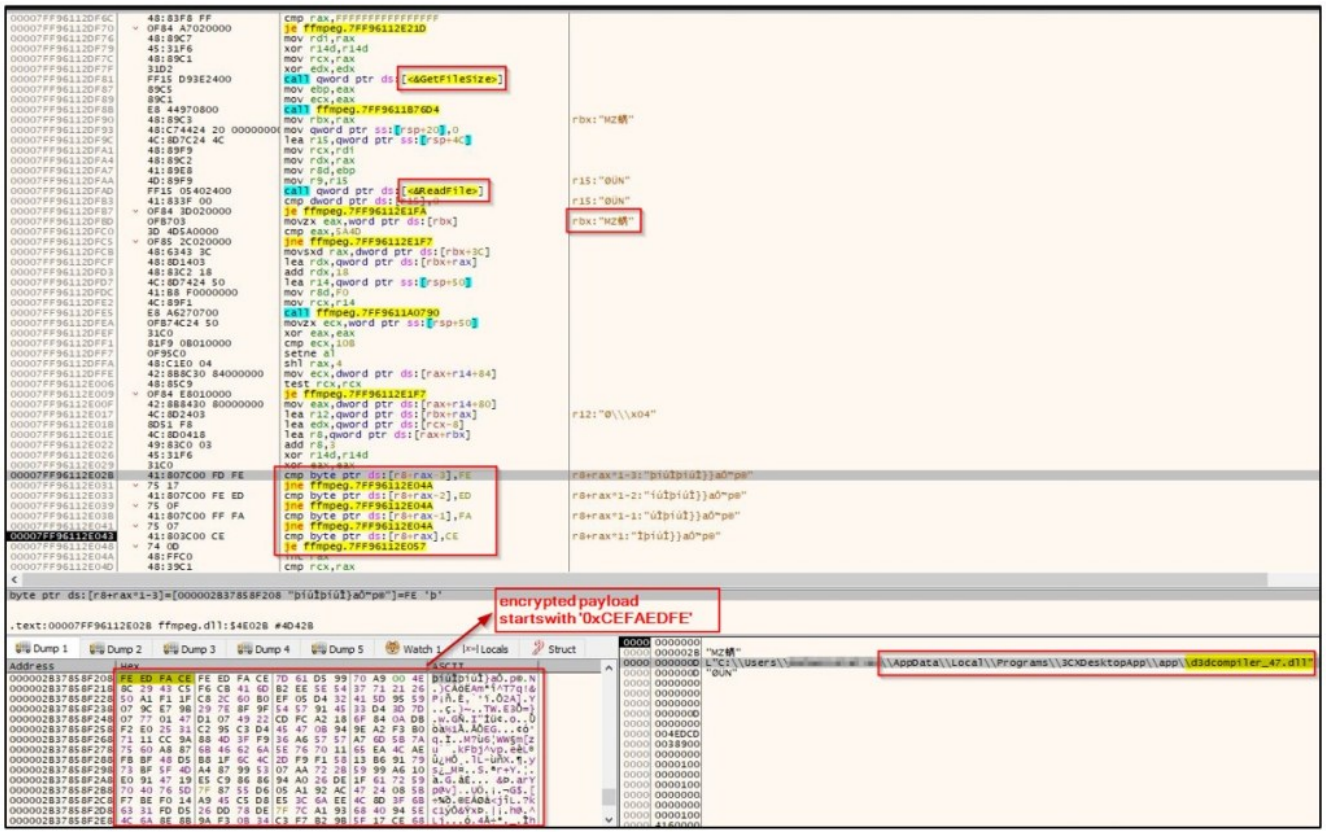

Figure 9 – Identifying encrypted payload in “d3dcompiler_47.dl”l

Once the encrypted payload has been identified, the “ffmpeg.dll” proceeds to decrypt the RC4 stream using the key “*3jB(2bsG#@c7*“. This decryption process results in a shellcode which is then executed by the DLL file.

The figure below shows the RC4 loop and decrypted shellcode function.

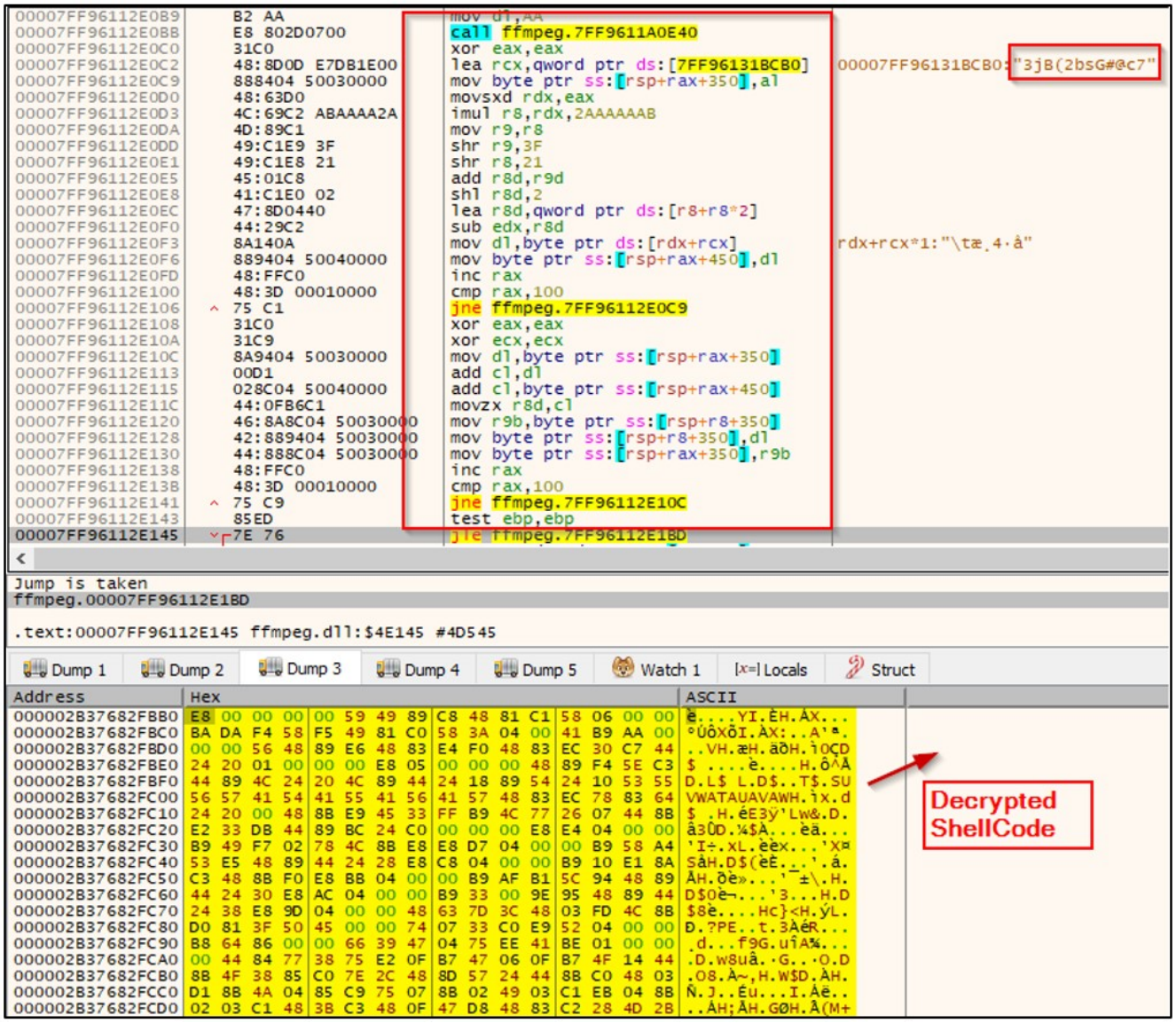

Figure 10 – RC4 loop and decrypted shellcode

After decryption, the “ffmpeg.dll” file employs the *VirtualProtect()* function to alter the memory access permissions of the shellcode. Once the permissions have been changed, the malware proceeds to execute the payload.

An embedded DLL file is present within the decrypted shellcode, as shown in the below figure, which appears to be functioning as a loader for another PE file.

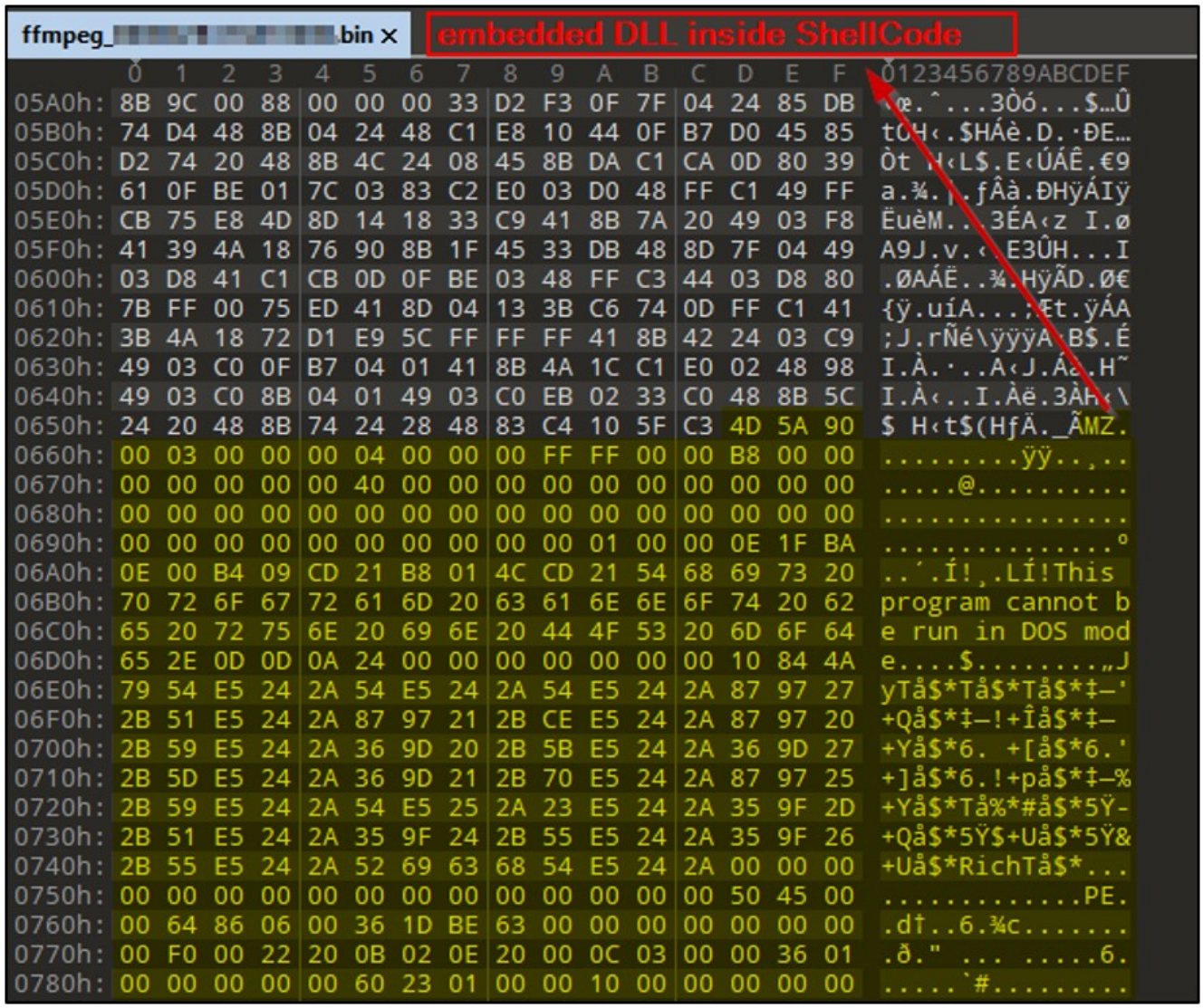

Figure 11 – Embedded DLL file inside Shellcode

After being loaded and executed, the embedded DLL file in the shellcode initiates a sleep state of 7 days before trying to establish communication with Command and Control (C&C) servers. Subsequently, the DLL will attempt to access a GitHub repository that contains an .ICO file.

Figure 12 – Hardcoded GitHub link to download the .ICO file

This ICO file comprises the encrypted C&C strings, which are encoded using Base64 and encrypted with AES & GCM encryption. The Base64 contents are located at the end of the ICO image file, as shown below.

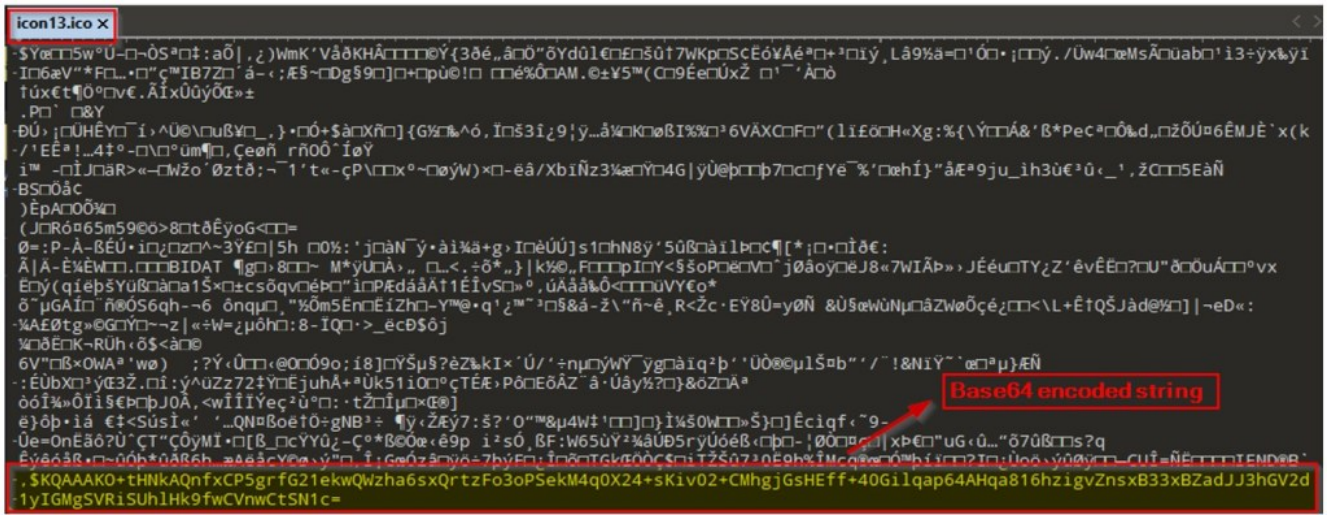

Figure 13 – Base64-encoded string at the end of ICO file

Upon execution, the DLL file decrypts the C&C URLs from the ICO files for downloading additional payloads from the remote server. To obtain distinct C&C URLs, the malware randomly selects an ICO file from a GitHub repository. Unfortunately, we were unable to verify the specific characteristics of these payloads as the corresponding GitHub repository was taken down prior to this analysis.

Researchers discovered that the final stage of malware is a stealer, which can extract system information and steal sensitive information from popular web browsers, such as Chrome, Edge, Brave, and Firefox.

Conclusion

The potential damage caused by the 3CXDesktopApp supply chain attack is significant, including the theft of sensitive user data. Organizations affected by this attack should immediately take steps to prevent it from causing widespread harm. The current investigation suggests that the threat actor behind this attack is skilled and persistent.

The consequences of such an attack, such as financial loss, reputational impact, and the loss of customer trust, are severe. It is crucial that organizations remain vigilant and take proactive measures to secure their supply chains to prevent similar attacks in the future.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Thoroughly investigate all systems to determine the scope and extent of the attack, including identifying all affected systems and data.
- Conduct regular security audits of your supply chain to ensure that all third-party software and components are trustworthy and secure.
- Monitor your network regularly for any suspicious activity or behavior indicating a security breach, such as unauthorized access attempts or data exfiltration.
- Stay up-to-date with the latest threat intelligence and security news to stay informed about emerging threats and vulnerabilities. This will help to mitigate risks proactively and respond quickly in the event of an attack.

- Using a reputed antivirus and internet security software package is recommended on connected devices, including PCs, laptops, and mobile devices.
- Block URLs that could be leveraged to spread malware.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1195	Supply Chain Compromise
Execution	T1204.002	User Execution: Malicious File
Defense Evasion	T1140 T1027 T1574.002 T1497.003	Deobfuscate/Decode Files or Information Obfuscated Files or Information Hijack Execution Flow: DLL Side-Loading Virtualization/Sandbox Evasion: Time-Based Evasion
Credential Access	T1555 T1539	Credentials from Password Stores Steal Web Session Cookie
Command and Control	T1071	Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
f3d4144860ca10ba60f7ef4d176cc736 bea77d1e59cf18dce22ad9a2fad52948fd7a9efa aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868	MD5 SHA1 SHA256	3CX Windows Installer
0eeb1c0133eb4d571178b2d9d14ce3e9 bfecb8ce89a312d2ef4afc64a63847ae11c6f69e 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983	MD5 SHA1 SHA256	3CX Windows Installer
5729fb29e3a7a90d2528e3357bd15a4b 19f4036f5cd91c5fc411afc4359e32f90caddaac 5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290	MD5 SHA1 SHA256	3CX macOS Installer File
d5101c3b86d973a848ab7ed79cd11e5a 3dc840d32ce86cebf657b17cef62814646ba8e98 e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec	MD5 SHA1 SHA256	3CX macOS Installer File
82187ad3f0c6c225e2fba0c867280cc9 20d554a80d759c50d6537dd7097fed84dd258b3e 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03	MD5 SHA1 SHA256	Malicious DLL
74bc2d0b6680faa1a5a76b27e5479cbc bf939c9c261d27ee7bb92325cc588624fca75429 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896	MD5 SHA1 SHA256	Malicious DLL
cad1120d91b812acafef7175f949dd1b09c6c21a	SHA1	Stealer Payload

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 github[.]com/IconStorages/images azureonlinestorage.com convieneonline[.]com Soyoungjun[.]com	URL	Malicious URL
3bb80e9fbeac5383b313084775c80d11 9c943baad621654cc0a0495262b6175276a0a9fb 210c9882eba94198274ebc787fe8c88311af24932832a7fe1f1ca0261f815c3d	MD5 SHA1 SHA256	Malicious ICO File
644f63f869e2b0a9e5d1aa32823956cc 96910a3dbc194a7bf9a452afe8a35eceb904b6e4 a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c	MD5 SHA1 SHA256	Malicious ICO File
8875568b90bb03ff54d63d3bd1187063 0d890267ec8d6d2aaf43eaca727c1fbba6acd16e d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090	MD5 SHA1 SHA256	Malicious ICO File
1640f48cc05c58f4cc077503a5361cea b1dee3ebcffad01a51ff31ff495fef1d40fdfaa0 d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a	MD5 SHA1 SHA256	Malicious ICO File
71d5b9bfd6bf37ff5aa9752b2b6d5af1 64ab912d0af35c01355430d85dd4181f25e88838 4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f	MD5 SHA1 SHA256	Malicious ICO File
da667174c2d145a4d9b3b39387fbd7dd 8377fb40c76aa3ba3efae3d284fa51aa7748e010 8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d	MD5 SHA1 SHA256	Malicious ICO File
69455ba3bfd2d8e3ade5081368934945 11ae67704ea0b930b2cc966e6d07f8b898f1a7d2 f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3	MD5 SHA1 SHA256	Malicious ICO File
848bc8e5917db1f735029fc51952002d ffccc3a29d1582989430e9b6c6d2bff1e3a3bb14 2c9957ea04d033d68b769f333a48e228c32bcf26bd98e51310efd48e80c1789f	MD5 SHA1 SHA256	Malicious ICO File

aafa584176d9aec7912b4bc3476acc1a 89827af650640c7042077be64dc643230d1f7482 268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca	MD5 SHA1 SHA256	Malicious ICO File
4d112603466ac9c57a669445374c1fb5 b5de30a83084d6f27d902b96dd12e15c77d1f90b c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd	MD5 SHA1 SHA256	Malicious ICO File
d232fa2eabc03123517a78936a18448b 3992dbe9e0b23e0d4ca487faffeb004bcfe9ecc8 c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396	MD5 SHA1 SHA256	Malicious ICO File
aff5911f6c211cde147a0d6aa3a7a423 caa77bcd0a1a6629ba1f3ce8d1fc5451d83d0352 f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182	MD5 SHA1 SHA256	Malicious ICO File
4942dc3c0e9808544b068854cf1351e0 57a9f3d5d1592a0769886493f566930d8f32a0fc 2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de	MD5 SHA1 SHA256	Malicious ICO File
3eb70db2f6bffbe29970f759747e07bd f533bea1c0558f73f6a3930343c16945fb75b20f e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c	MD5 SHA1 SHA256	Malicious ICO File
14b79d2f81d1c0a9c3769f7bb83e443d 31d775ab577f3cc88991d90e9ae58501dbe1f0da d0f1984b4fe896d0024533510ce22d71e05b20bad74d53fae158dc752a65782e	MD5 SHA1 SHA256	Malicious ICO File

Yara Rules

Reference:

https://www.3cx.com/blog/news/desktopapp-security-alert/