THREAT ALERT

cybereason

THREAT ALERT: 3CXDesktopApp Supply Chain Attack

The Cybereason Global Security Operations Center (SOC) issues Cybereason Threat Alerts to inform customers of emerging impacting threats. The Alerts summarize these threats and provide practical recommendations for protecting against them.

WHAT'S HAPPENING?

The Cybereason team is investigating a recent campaign using 3CXDesktopApp in a supply chain attack. 3CXDesktopApp, is an application developed by 3CX allowing users to make calls, video conferences, and check voicemails. Supply chain attacks are a type of cyber attack that targets vulnerabilities in a company's supply chain. They involve exploiting weak links in the chain, such as third-party vendors, suppliers, or contractors.

The threat actor trojanized this application to add an installer that communicates with various command-and-control (C&C) servers to retrieve the final payload. The trojanized 3CXDesktopApp is the first stage of the supply chain attack that pulls the ICO file from GitHub and leads to a third stage of the attack. It was reported that the payload, once unpacked, downloads an infostealer on the victim machines which can lead to credential theft and data exfiltration.

KEY OBSERVATIONS

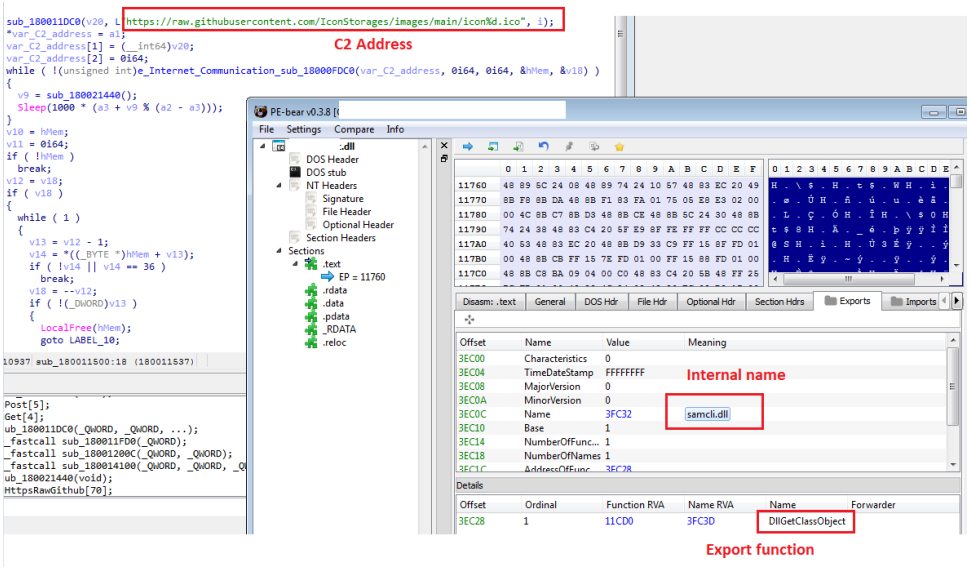
- **State-sponsored adversary** : Using a supply chain attack, threat actors, suspected to be state-sponsored and operating out of North Korea, were able to infiltrate a malicious version of one of the modules connected to the application 3CXDesktopApp.
- **Trojanized for a week** : Earlier abuse of this application has been identified starting March 22, 2023 from the 3CX forum supporting the desktop application.
- **Browser information stealer final stage:** The final payload targets web browsers and may lead to sensitive data exposure and exfiltration. This content includes browsing history, cookies, cached data and images, bookmarks, auto-fill forms, and user logins.

- **Available Indicators of Compromise (IoCs)** : Cybereason has added the indicators of compromise (IOC) to our Global Threat Intelligence server to automatically detect the presence of these exploits.
- **Detected by Cybereason:** Using our Global Threat Intelligence server, Cybereason detects this attack. Using our VPP (Variant Payload Protection) module, Cybereason prevents this attack.

ANALYSIS

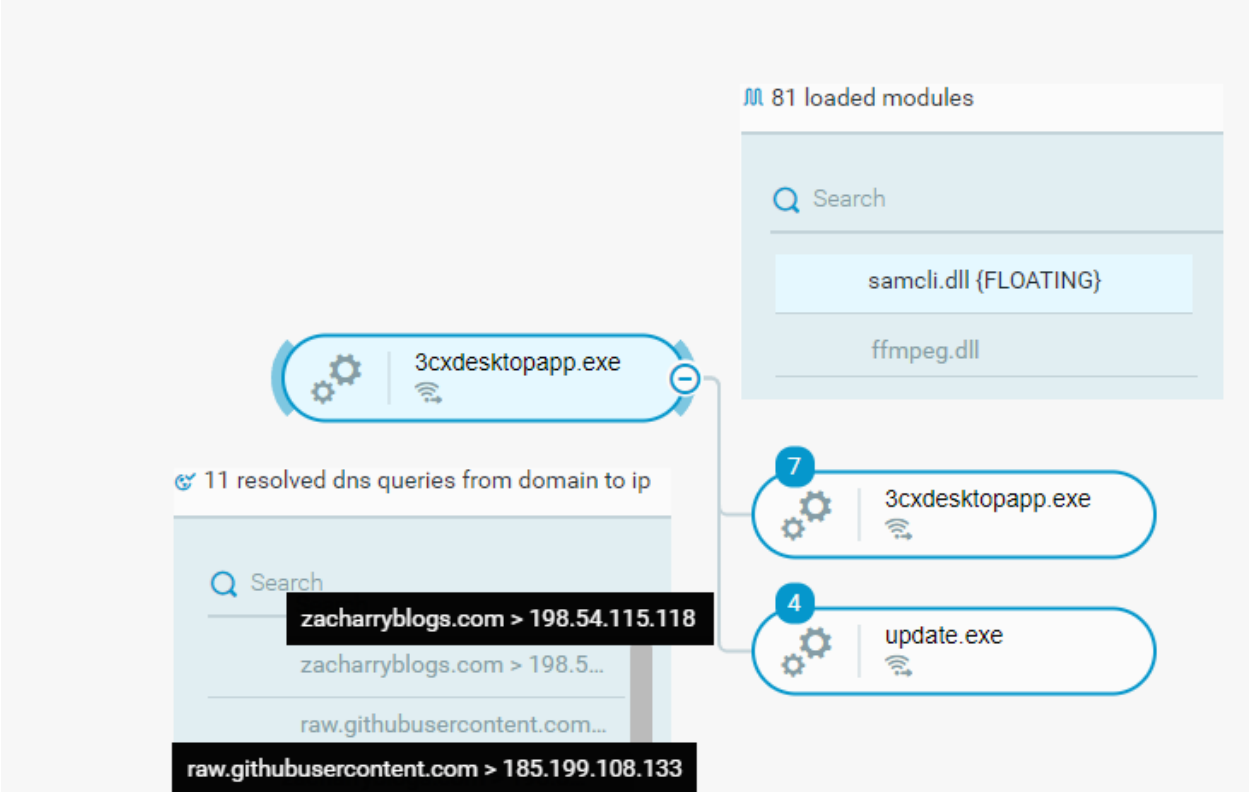
This attack is a clear example of how threat actors are using advanced techniques to exploit vulnerabilities in supply chains. In this section, we analyze a trojanized sample of the 3CXDesktopApp Windows client.

The compromised 3CXDesktopApp is the first stage in the attack chain and uses the DLL side-loading technique to load a rogue DLL (*ffmpeg.dll*). *Ffmpeg.dll* loads *d3dcompiler_47.dll* to its memory and decodes it with the RC4 algorithm, which reveals a shellcode and another binary. The shellcode allocates memory by using the VirtualAlloc function and writes the binary, named *samcli.dll* into the allocated memory.



Extraction of the Github-related URL from the binary analysis

Then, the payload tries to access the IconStorages GitHub page to pull an ICO file containing the encrypted command-and-control servers. The payload uses this file to communicate with the C&C server and retrieve the final stage of the attack.



3xcdesktopapp.exe trojanized application process tree

The GitHub page used in this attack, *raw.githubusercontent[.]com/IconStorages/images/main/*, has been taken down as of the time of writing.

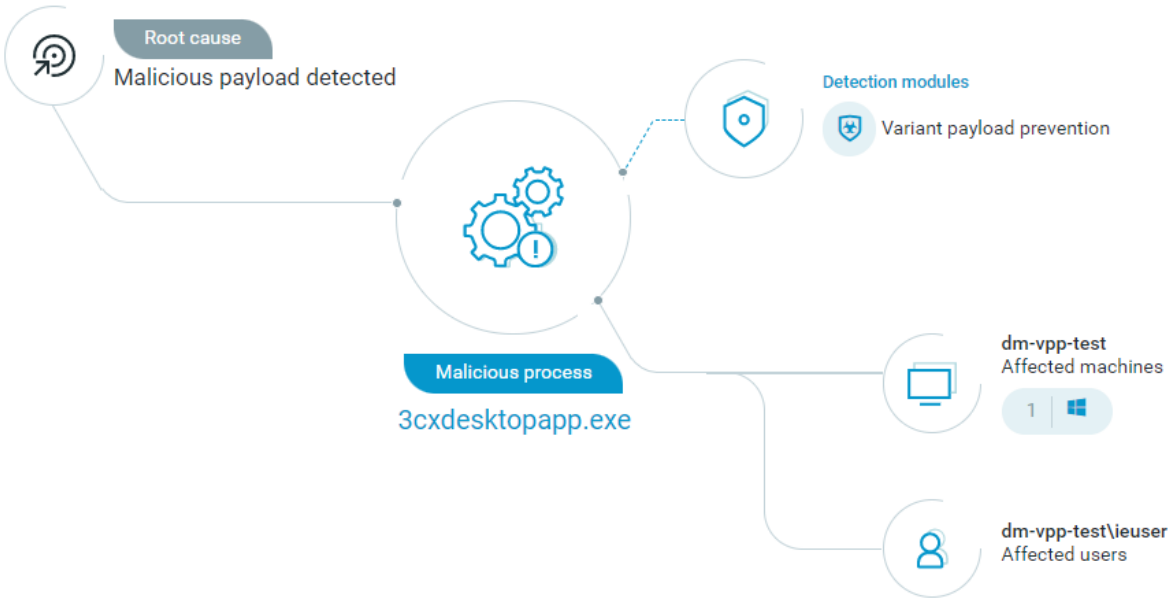
According to 3CX, the issue appears to be one of the bundled libraries they compiled into the Windows Electron App via GIT.

The 3CXDesktopApp supply chain attack is a sobering reminder of the evolving nature of cyber threats and the need for constant vigilance. In conclusion, this attack highlights the importance of taking a comprehensive approach to cybersecurity that includes monitoring and securing supply chains.

DETECTION

Variant Payload Prevention (VPP)

Cybereason Variant Payload Protection (VPP) **detects and prevents** the shellcode associated with the exploitation of the application from the beginning of the attack.

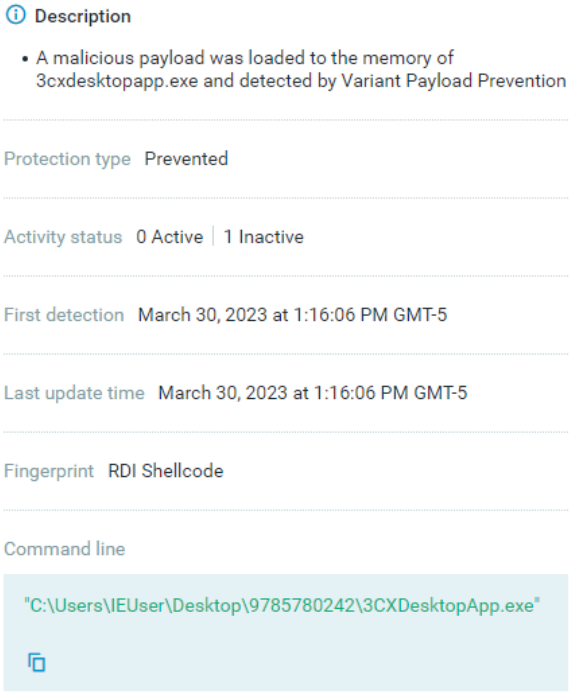


MalOp created after the execution of the trojanized 3xcdesktopapp.exe application

Process (1)

Name	Protection type	First execution time	Last execution time
3cxdesktopapp.exe	Prevented	March 30, 2023 at 1:...	March 30, 2023 at 1:...

Trojanized 3xcdesktopapp.exe process prevent



Process prevention of the trojanized application

MDR / Proactive Threat Hunting

Cybereason GSOC is notifying our Managed Detection and Response (**MDR**) customers in the scope of ***Proactive Threat Hunting*** service that helps our customers uncover exploitation of zero day vulnerabilities and other Advanced Persistent Threat actor activities.

CYBEREASON RECOMMENDATIONS

Cybereason recommends the following:

- Ensure the Cybereason sensor is deployed to applicable systems.
- Enable Cybereason Endpoint Prevention and NGAV in Prevent mode via your Security Policies for the affected machines.
    - Enable Variant Payload Protection (VPP) in your Cybereason sensor policy (Requires version 21.2.160 and above)
- Locate the presence of 3CXDesktopApp software in your environment by using the queries outlined in the Hunting Query section.
- Fully remove 3CX software from all endpoints in your environment.
- Add mentioned SHA1 hashes IOCs to your Cybereason custom reputation list with Detect and Prevent reputation and make sure that the Endpoint Prevention component - AppControl enabled in all your security policies.
- Block communication to the domains in this IOCs List in your organization's firewall, proxy, mail filtering, and web filtering.
- Add the IOC domains to your Cybereason custom reputation list with Detect reputation.

Indicators of Compromise (IOCs)

Below are listed the published indicators of compromise related to this threat alert:

Type	Value	Comment
Sha1	bea77d1e59cf18dce22ad9a2fad52948fd7a9efa 8433a94aedb6380ac8d4610af643fb0e5220c5cb bfecb8ce89a312d2ef4afc64a63847ae11c6f69e	3CXDesktopApp
Sha1	19f4036f5cd91c5fc411afc4359e32f90caddaac 3dc840d32ce86cebf657b17cef62814646ba8e98	3CXDesktopApp (DMG)
Sha1	F3487a1324f4c11b35504751a5527bc60eb95382 5d833bcc679db38a45111269e727ec58b75c8d31	3CXDesktopApp (Mach-O)
Sha1	188754814b37927badc988b45b7c7f7d6b4c8dd3 bf939c9c261d27ee7bb92325cc588624fca75429	ffmpeg.dll
Sha1	20d554a80d759c50d6537dd7097fed84dd258b3e	d3dcompiler_47.dll
Sha1	79ae52b1088742202351460ff3562fdc1797f04d	Malicious second stage
URL	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	C&C domains