Suspected DPRK Supply Chain Intrusion Distributed via Trojanized Version of 3CXDesktopApp

Cyber Crime (CC) | Cyber Espionage (CE)

Fusion (FS) | Operational (OP)

March 30, 2023 04:15:07 AM, 23-00005486, Version: 1

Executive Summary

- A campaign is distributing malware via a trojanized version of 3XC's Desktop Client "3CXDesktopApp." This trojanized software runs a downloader and retrieves a subsequent payload from GitHub.
- This activity has some overlaps with previous suspected North Korean activity, but analysis is ongoing to determine motivation and attribution.
- Analysis is ongoing and will be updated as we identify additional details.
- Technical details including indicators of compromise, MITRE ATT&CK mapping, and YARA and Snort rules are in the Technical Annex.

Threat Detail

Mandiant is investigating a suspected DPRK campaign apparently delivering malware via trojanized versions of 3XC's "3XCDesktopApp" client, 482c22[.]msi (MD5: 0eeb1c0133eb4d571178b2d9d14ce3e9). When successfully executed, this trojanized version would run a downloader that then downloads a third stage hosted on GitHub. Analysis of this activity is ongoing, and preliminary technical details are below. This activity has been publicly reported by CrowdStrike and Sentinel One.

- 3XC is a software company specializing in phone and video conferencing software. Its 3XCDDesktopApp software allows users to conduct video and phone calls from their desktop.
- As of 8:30 p.m. EST on March 29, the Windows version available for download from 3XC's website continued to be the trojanized version.
- CrowdStrike has also reported that the MacOS version was tojanized; however, Mandiant has not been able to confirm that at the time of writing.

Attribution and Related Activity

Limited technical artifacts present in this campaign overlap with previously observed North Korea-sponsored cyber activity, but we are continuing to investigate this and are not able to conclusively link this campaign to a tracked group. Some of the artifacts present in the malware used for the supply chain operation have been used in earlier activities.

- The RC4 key 3jB(2bsG#@c7 appears to have been used on multiple occasions.
- The use of the bytes 0xFEEDFACEFEEDFACE to identify a notable part of a file is likely distinctive.

Outlook and Implications

While preliminary indications tie this campaign to North Korea, Mandiant has not uncovered evidence identifying a motive. In addition to traditional espionage, North Korean groups have conducted extensive financially motivated operations, often seeking to steal cryptocurrencies. The wide scope of this campaign could be used for multiple purposes. We will update as we uncover additional information.

Technical Annex

Trojanized 3CXDesktopApp Execution

482c22[.]msi (MD5: 0eeb1c0133eb4d571178b2d9d14ce3e9)

- Windows Installer Package
- Creation date: 2023-03-13 06:33:26Z
- Downloaded from:
  - hxxps://1270[.]3cx[.]cloud/webclient/api/app/windows
- Contains:
  - MD5 74bc2d0b6680faa1a5a76b27e5479cbc
  - MD5 82187ad3f0c6c225e2fba0c867280cc9

_ffmpeg[.]dll_cd92cfbf_289b_424b_89a1_5894463050db (MD5: 74bc2d0b6680faa1a5a76b27e5479cbc)

- Creation date: 2022-11-12 04:12:14Z
- Contains an RC4 key 3jB(2bsG#@c7

_d3dcompiler_47[.]dll_a673e78c_fc6a_4133_b2d9_b6447cfbc1c3 (MD5: 82187ad3f0c6c225e2fba0c867280cc9)

- Creation date: 1981-01-19 07:15:57Z
- Contains an encrypted payload after the bytes 0xFEEDFACEFEEDFACE
- Payload is decrypted with RC4 key from MD5 74bc2d0b6680faa1a5a76b27e5479cbc
  - Decrypts to MD5 6426fe4dc604c7f1784ed1d48ab4ffc8
  - Decrypted payload contains trailing configuration data
    - Configuration is passed as arguments to MD5 6426fe4dc604c7f1784ed1d48ab4ffc8

Figure 1: d3dcompiler_47[.]dll, embedded payload

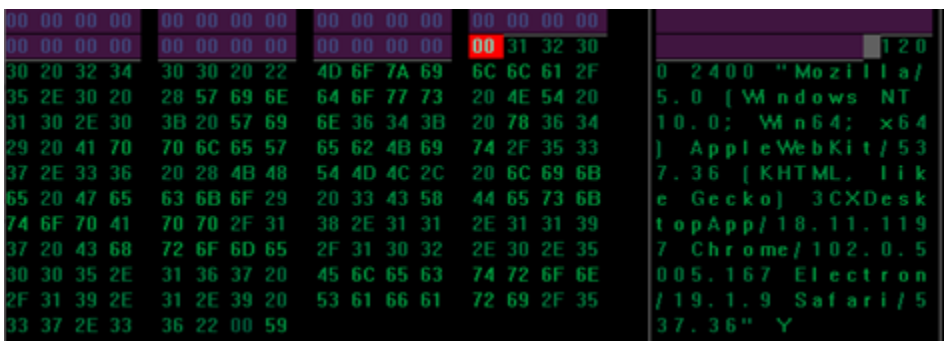

Figure 2: d3dcompiler_47[.]dll, decoded configuration

trololo[.]dll (MD5: 6426fe4dc604c7f1784ed1d48ab4ffc8)

- Creation date: 2023-01-11 02:21:42Z
- Expects command line arguments
  - 1: network request sleep algorithm variable 1
  - 2: network request sleep algorithm variable 2
  - 3: network request User-Agent
- Retrieves an .ico file from the C&C server
  - hxxps://raw[.]githubusercontent[.]com/IconStorages/images/main/icon<NUM>[.]ico
    - An example payload was identified as MD5: 8875568b90bb03ff54d63d3bd1187063
- The .ico file contains an encoded C&C server appended at the bottom
- Retrieves a payload from the decoded C&C server
  - Decryption of the C&C server is on-going
- Decrypts the payload and loads it into memory before executing

Icon10[.]ico (MD5: 8875568b90bb03ff54d63d3bd1187063)

- Example downloaded icon<NUM>.ico

Related Intelligence

Files Also Dropping MD5 74bc2d0b6680faa1a5a76b27e5479cbc

5b2e29[.]msi (MD5: f3d4144860ca10ba60f7ef4d176cc736)

- Windows Installer Package

Files Also Containing the Key 3jB(2bsG#@c7

ffmpeg[.]dll (MD5: 27b134af30f4a86f177db2f2555fe01d)

- Creation date: 2022-11-12 04:12:14Z

Suspected Malicious MacOS 3CXDesktopApp

3CXDesktopApp-18[.]12[.]416[.]dmg (MD5: d5101c3b86d973a848ab7ed79cd11e5a)

- Apple disk image

MITRE ATT&CK Techniques

ID	Technique
T1012	Query Registry

T1027	Obfuscated Files or Information
T1036.001	Invalid Code Signature
T1055	Process Injection
T1071.001	Web Protocols
T1083	File and Directory Discovery
T1140	Deobfuscate/Decode Files or Information
T1497.001	System Checks

Table 1: MITRE ATT&CK techniques

YARA Rules

```
rule M_Hunting_3CXDesktopApp_Key {
  meta:
    disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    description = "Detects a key found in a malicious 3CXDesktopApp file"
    md5 = "74bc2d0b6680faa1a5a76b27e5479cbc"
    date = "2023/03/29"
    version = "1"
  strings:
    $key = "3jB(2bsG#@c7" wide ascii
  condition:
    $key
}
```

Snort Rules

Disclaimer: These rules are meant for hunting and have not been tested to run in a production environment.

alert tcp any any -> any any (msg:"Possible malicious 3CXDesktopApp Identified"; content:"raw[.]githubusercontent[.]com/IconStorages/images/main/"; threshold:type limit, track by_src, count 1, seconds 3600; sid: 99999999;)

First Version Publish Date

March 30, 2023 04:15:07 AM

Threat Intelligence Tags

Affected Systems

- Enterprise/Application Layer

Intended Effects

- Military Advantage
- Political Advantage
- Financial Theft

Motivations

- Military/Security/Diplomatic
- Financial or Economic

Source Geographies

- North Korea

Tactics, Techniques And Procedures (TTPs)

- Hardware/Supply Chain Compromise

Target Geographies

- Global

Technical Indicators & Warnings

Identifier	Attacker
Network Type	url
Port	443
Protocol	https
URL	hxxps://1270[.]3cx[.]cloud/webclient/api/app/windows

Identifier	Attacker
File Size	47754
File Name	images-main/icon10[.]ico
MD5	8875568b90bb03ff54d63d3bd1187063
SHA1	0d890267ec8d6d2aaf43eaca727c1fbba6acd16e
SHA256	d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090
Type	image/vnd[.]microsoft[.]icon

Identifier	Attacker
File Size	2824448
File Name	c:\users\j[.]hart\appdata\local\programs\3cxdesktopapp\app\ffmpeg[.]dll
MD5	27b134af30f4a86f177db2f2555fe01d
SHA1	188754814b37927badc988b45b7c7f7d6b4c8dd3
SHA256	c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02
Type	application/x-dosexec

Identifier	Attacker
File Size	2814976
File Name	c:\users\user\appdata\local\programs\3cxdesktopapp\app-18.12.416\ffmpeg[.]dll
MD5	74bc2d0b6680faa1a5a76b27e5479cbc
SHA1	bf939c9c261d27ee7bb92325cc588624fca75429
SHA256	7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
Type	application/x-dosexec

Identifier	Attacker
File Size	102555648
File Name	3cxdesktopapp-18[.]12[.]416[.]msi
MD5	0eeb1c0133eb4d571178b2d9d14ce3e9

SHA1	bfecb8ce89a312d2ef4afc64a63847ae11c6f69e
SHA256	59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983
Type	application/x-msi
Identifier	Attacker
File Size	5168344
File Name	d3dcompiler_47[.]dll
MD5	82187ad3f0c6c225e2fba0c867280cc9
SHA1	20d554a80d759c50d6537dd7097fed84dd258b3e
SHA256	11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03
Type	application/x-dosexec
Identifier	Attacker
File Size	172150545
File Name	3cxdesktopapp-18[.]12[.]416[.]dmg
MD5	d5101c3b86d973a848ab7ed79cd11e5a
SHA1	3dc840d32ce86cebf657b17cef62814646ba8e98
SHA256	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
Type	application/octet-stream
Identifier	Attacker
File Size	275456
File Name	trololo[.]dll
MD5	6426fe4dc604c7f1784ed1d48ab4ffc8
SHA1	3b88cda62cdd918b62ef5aa8c5a73a46f176d18b
SHA256	aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973
Type	application/x-dosexec
Identifier	Attacker
File Size	102522880
File Name	c:\windows\installer\5a8b52[.]msi
MD5	f3d4144860ca10ba60f7ef4d176cc736
SHA1	bea77d1e59cf18dce22ad9a2fad52948fd7a9efa
SHA256	aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868
Type	application/x-msi

Version Information

Version:1, March 30, 2023 04:15:07 AM