SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack

sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

March 29, 2023

By Juan Andres Guerrero-Saade, Asaf Gilboa, David Acs, James Haughom & SentinelLabs

Executive Summary

- As of Mar 22, 2023 SentinelOne began to see a spike in behavioral detections of the 3CXDesktopApp, a popular voice and video conferencing software product categorized as a Private Automatic Branch Exchange (PABX) platform.
- Behavioral detections prevented these trojanized installers from running and led to immediate default quarantine.
- The trojanized 3CXDesktopApp is the first stage in a multi-stage attack chain that pulls ICO files appended with base64 data from Github and ultimately leads to a 3rd stage infostealer DLL still being analyzed as of the time of writing.
- The compromise includes a code signing certificate used to sign the trojanized binaries.
- Our investigation into the threat actor behind this supply chain is ongoing. The threat actor has registered a sprawling set of infrastructure starting as early as February 2022, but we don't yet see obvious connections to existing threat clusters.
- March 30th, 2023: We have updated our IOCs with contributions from the research community.
- March 30th, 2023: We can confirm that the MacOS installer is trojanized, as reported by Patrick Wardle. We have identified the limited deployment of a second-stage payload for Mac infections. We have updated our IOCs to reflect MacOS components. Our telemetry now sets the earliest infection attempt as March 8th, 2023.

Background

3CXDesktopApp is a voice and video conferencing Private Automatic Branch Exchange (PABX) enterprise call routing software developed by 3CX, a business communications software company. The company website claims that 3CX has 600,000 customer companies with 12 million daily users. 3CX lists customer organizations in the following sectors:

- Automotive
- Food & Beverage
- Hospitality
- Managed Information Technology Service Provider (MSP)
- Manufacturing

The 3CX PBX client is available for Windows, macOS, and Linux; there are also mobile versions for Android and iOS, as well as a Chrome extension and a Progressive Web App (PWA) browser-based version of the client.

PBX software makes an attractive supply chain target for actors; in addition to monitoring an organization's communications, actors can modify call routing or broker connections into voice services from the outside. There have been other instances where actors use PBX and VOIP software to deploy additional payloads, including a 2020 campaign against Digium VOIP phones using a vulnerable PBX library, FreePBX.

Campaign Overview

As others have noted, SentinelOne began automatically detecting and blocking the activity over the span of the week, prior to our active investigation of the campaign.

> Seems like this has progressed into “3cx desktop app is compromised and the prevailing theory is that its the wannacry people who are behind it”? So that’s something to keep an eye on I guess… pic.twitter.com/vkVnXtRDd5
>
> — patrick (@ggstoneforge) March 29, 2023

As we actively analyze the malicious installer, we see an interesting multi-stage attack chain unfolding. The 3CXDesktopApp application serves as a shellcode loader with shellcode executed from heap space. The shellcode reflectively loads a DLL, removing the “MZ” at the start. That DLL is in turn called via a named export ‘DllGetClassObject’ with the following arguments:

```
1200 2400 "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”
```

as well as the size of this User-Agent string.

This stage will in turn download icon files from a dedicated Github repository:

```
https://github[.]com/IconStorages/images
```

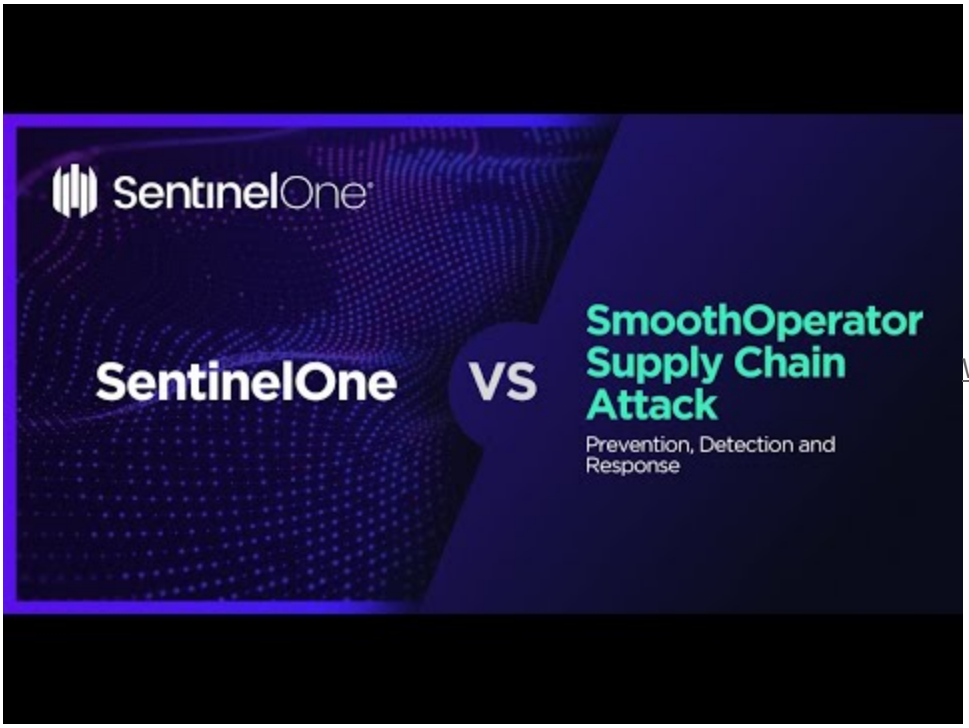
These ICO files have Base64 data appended at the end. That data is then decoded and used to download another stage. At this time, the DLL appears to be a previously unknown infostealer meant to interface with browser data, likely in an attempt to enable future operations as the attackers sift through the mass of infected downstream customers. We have issued a takedown request for this repository.

The final stage (cad1120d91b812acafef7175f949dd1b09c6c21a) implements infostealer functionality, including gathering system information and browser information from Chrome, Edge, Brave, and Firefox browsers. That includes querying browsing history and data from the Places table for Firefox-based browsers and the History table for Chrome-based browsers.

```
text "UTF-16LE", 'AppData\Local\Google\Chrome\User Data',0
align 10h
:                       ; DATA XREF: .data:0000000180113008↓o
text "UTF-16LE", 'AppData\Local\Microsoft\Edge\User Data',0
align 20h
:                       ; DATA XREF: .data:0000000180113010↓o
text "UTF-16LE", 'AppData\Local\BraveSoftware\Brave-Browser\User Data'
text "UTF-16LE", 0
align 10h
:                       ; DATA XREF: .data:0000000180113018↓o
text "UTF-16LE", 'AppData\Roaming\Mozilla\Firefox\Profiles',0
align 8
                        ; DATA XREF: .data:0000000180113020↓o
                        ; .data:0000000180113028↓o ...
text "UTF-16LE", 'History',0
                        ; DATA XREF: .data:0000000180113038↓o
text "UTF-16LE", 'places.sqlite',0
align 8
                        ; DATA XREF: .data:off_180113040↓o
text "UTF-16LE", 'Chrome',0
align 8
                        ; DATA XREF: .data:0000000180113048↓o
text "UTF-16LE", 'Edge',0
align 8
                        ; DATA XREF: .data:0000000180113050↓o
text "UTF-16LE", 'Brave',0
align 8
```

Infostealer strings used to query for History and Places tables

SentinelOne Protects Against SmoothOperator



Watch Video At:

https://youtu.be/jbIGuCG7fyA

Recommendations

For SentinelOne customers, no action is needed. We've provided technical indicators to benefit all potential victims in hunting for the SmoothOperator campaign.

Indicators of Compromise

Note: we have removed soyoungjun[.]com and convieneonline[.]com as they were linked based on inaccurate information from a passive DNS provider. Thank you to Daniel Gordon for the tip.

We have also added the full list of URIs decrypted from the ICO files previously referenced. Thanks to Johann Aydinbas for the excellent work!

URL	github[.]com/IconStorages/images
Email	[.]me
Email	[.]me
SHA-1	cad1120d91b812acafef7175f949dd1b09c6c21a
SHA-1	bf939c9c261d27ee7bb92325cc588624fca75429
SHA-1	20d554a80d759c50d6537dd7097fed84dd258b3e
URI	https://www.3cx[.]com/blog/event-trainings/
URI	https://akamaitechcloudservices[.]com/v2/storage
URI	https://azureonlinestorage[.]com/azure/storage
URI	https://msedgepackageinfo[.]com/microsoft-edge
URI	https://glcloudservice[.]com/v1/console
URI	https://pbxsources[.]com/exchange
URI	https://msstorageazure[.]com/window
URI	https://officestoragebox[.]com/api/session
URI	https://visualstudiofactory[.]com/workload
URI	https://azuredeploystore[.]com/cloud/services
URI	https://msstorageboxes[.]com/office
URI	https://officeaddons[.]com/technologies
URI	https://sourceslabs[.]com/downloads

URI	https://zacharryblogs[.]com/feed
URI	https://pbxcloudeservices[.]com/phonesystem
URI	https://pbxphonenetwork[.]com/voip
URI	https://msedgeupdate[.]net/Windows

Additional Mac Indicators

SHA-1	libffmpeg.dylib 769383fc65d1386dd141c960c9970114547da0c2
SHA-1	3CXDesktopApp-18.12.416.dmg 3dc840d32ce86cebf657b17cef62814646ba8e98
SHA-1	UpdateAgent 9e9a5f8d86356796162cee881c843cde9eaedfb3
URI	https://sbmsa[.]wiki/blog/_insert