3CX：供應鏈攻擊影響全球數千用戶

2023 年 3 月 30 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

北韓贊助的駭客被認為與對多個 3CX DesktopApp 版本所進行的木馬化攻擊有關

2023/03/31 14:26 UTC 更新：我們的布落格已更新為使用 Yara 規則來檢測最終的訊息竊取器有效負載。

2023/03/30 17:39 UTC 更新：我們的布落格已更新 macOS 版本的技術分析。

2023/03/30 14:17 UTC 更新：我們的布落格已更新額外的 IOC。

2023/03/30 12:47 UTC 更新：我們的布落格已更新額外的 IOC 和防護訊息。

2023/03/30 09:07 UTC 更新：我們的布落格已更新，其中包含對所用惡意軟體的技術分析。

據信與北韓關係匪淺的駭客組織已將 3CX 網路電話系統公司的：3CX DesktopApp 植入惡意木馬程式，這是一種被廣泛使用的影音通話桌面應用程式。讓人再次想起之前針對 SolarWinds 的供應鏈攻擊，該軟體的幾個最新 Windows 和 Mac 版本的安裝程式被駭客入侵並修改植入惡意程式以利後續布署攻擊鏈所需的惡意酬載及竊密程式。該惡意軟體收集的資訊想必是是讓攻擊者可以篩選潛在得進一步攻擊對象。

攻擊鏈

攻擊者至少入侵兩個 3CX DesktopApp 的 Windows 版本（18.12.407 和 18.12.416）和兩個 Mac 版本（8.11.1213 和最新）的安裝檔。安裝檔包含應用程式的乾淨版本以及惡意 DLL。該應用程式用於側載惡意 DLL，然後在電腦上安裝竊密惡意軟體。

在賽門鐵克分析的兩個變種中 (SHA256: aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868 and 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983), 其一乾淨的執行檔用來掛載惡意的 ffmpeg.dll 動態連結檔 (SHA256：7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896)

此 DLL包含會從第二個DLL, d3dcompiler_47.dll 載入並執行的有效籌載程式碼。(SHA256：11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03)

D3dcompiler_47.dll 包含新增加密 blob 副檔名，顯示它可能是合法檔案的木馬化版本。blob 以十六進制值“FEEDFACE”開頭，加載程序使用它來查尋 blob。解密的 blob 包含 shellcode 和第三個 DLL (SHA256：aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973)。

shellcode 加載並執行這第三個 DLL，使用參數匯出 DLLGetClassObject：

- 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”

然後它會嘗試從以下 GitHub 儲存庫下載 ICO 檔：

- https://raw.githubusercontent[].com/IconStorages/images/main/icon%d.ico

Mac 版本

最後，受影響的兩個 macOS 版本軟體以類似的方式遭到破壞。在這種情況下，一個名為 libffmpeg.dylib 的動態庫被植入木馬。該檔至少有兩個變種（SHA256：a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67 和 fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58016c82956c956），它們似乎出現在不同版本上。

惡意程式碼在libffmpeg.dylib的InitFunc_0 函數中，它啟動 calls _run_avcodec 這個執行緒，在這個執行緒中它用 0x7A 的 XOR 金鑰解碼部份 shellcode，然後發出 http 請求。

它嘗試從以下位置下載檔案：

- URL: https://msstorageazure[.]com/analysis
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.128 Safari/537.36

以下網址(URL) 會嵌入到被分析的變種中：

- officestoragebox[.]com/api/biosync
- visualstudiofactory[.]com/groupcore
- azuredeploystore[.]com/cloud/images
- msstorageboxes[.]com/xbox
- officeaddons[.]com/quality
- sourceslabs[.]com/status
- acharryblogs[.]com/xmlquery
- pbxcloudeservices[.]com/network
- pbxphonenetwork[.]com/phone
- akamaitechcloudservices[.]com/v2/fileapi
- azureonlinestorage[.]com/google/storage
- msedgepackageinfo[.]com/ms-webview
- glcloudservice[.]com/v1/status
- pbxsources[.]com/queue

緩解措施

3CX 已獲悉該漏洞並建議用戶立即移除該應用程式。它表示將在數小時內發佈的新的軟體版本進行更新。它建議用戶考慮使用其 PWA 用戶端作為替代方案，直到發佈乾淨版本的 DesktopApp。

防護方案／緩解措施

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- Trojan.Dropper
- Trojan.Malfilter
- WS.Malware.2
- OSX.Samsis
- Trojan.Samsis

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Malicious Site: Malicious Domains Request
- Malicious Site: Malicious Domain Request 59
- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

Yara Rule 檢測最終的信息竊取器負載

```
rule icon_3cx_stealer {
   meta:
      copyright = "Symantec"
      description = "Infostealer component used in 3CX supply chain attack"
   strings:
      $a1 = "******************************** %s ********************************" wide fullword
      $a2 = "\\3CXDesktopApp\\config.json" wide fullword
      $a3 = { 7B 00 22 00 48 00 6F 00 73 00 74 00 4E 00 61 00 6D 00 65 00 22 00 3A 00 20 00 22 00 25 00 73 00 22 00 2C 00 20 00 22 00 44 00 6F 00 6D 00 61 00 69 00 6E 00 4E 00 61 00 6D 00 65 00 22 00 3A 00 20 00 22 00 25 00 73 00 22 00 2C 00 20 00 22 00 4F 00 73 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 22 00 3A 00 20 00 22 00 25 00 64 00 2E 00 25 00 64 00 2E 00 25 00 64 00 22 00 7D }
      $b1 = "HostName: %s" wide fullword
      $b2 = "DomainName: %s" wide fullword
      $b3 = "OsVersion: %d.%d.%d" wide fullword
      $b4 = "%s.old" wide fullword
   condition:
      3 of ($a*) and 2 of ($b*)
}
```

有關使用自定義 Yara 規則掃描 SEP 客戶端電腦的更多訊息，請閱讀此知識庫文章。

入侵指標 (IOCs)

dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc – Windows app
aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868 – Windows installer
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405 – Windows app
59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983 – Windows installer
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61 – macOS app
5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290 – macOS installer
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb – macOS app
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec – macOS installer
11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03 – Infostealer (d3dcompiler_47.dll)
7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896 - Infostealer (ffmpeg.dll)
aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973 - Infostealer
c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02 - Infostealer (ffmpeg.dll)
fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7 - Malicious macOS library (libffmpeg.dylib)
a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67 - Malicious macOS library (libffmpeg.dylib)
210c9882eba94198274ebc787fe8c88311af24932832a7fe1f1ca0261f815c3d – Malicious ICO file (icon0.ico)

a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c – Malicious ICO file (icon1.ico)
d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090 – Malicious ICO file (icon10.ico)
d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090 – Malicious ICO file (icon11.ico)
d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a – Malicious ICO file (icon12.ico)
4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f – Malicious ICO file (icon13.ico)
8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d – Malicious ICO file (icon14.ico)
f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3 – Malicious ICO file (icon15.ico)
2c9957ea04d033d68b769f333a48e228c32bcf26bd98e51310efd48e80c1789f – Malicious ICO file (icon2.ico)
268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca – Malicious ICO file (icon3.ico)
c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd – Malicious ICO file (icon4.ico)
c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396 – Malicious ICO file (icon5.ico)
f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182 – Malicious ICO file (icon6.ico)
2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de – Malicious ICO file (icon7.ico)
e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c – Malicious ICO file (icon8.ico)
d0f1984b4fe896d0024533510ce22d71e05b20bad74d53fae158dc752a65782e – Malicious ICO file (icon9.ico)
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
raw.githubusercontent[.]com/IconStorages/images/main/

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3cx-supply-chain-attack

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588