嚴重影響美國和歐洲關鍵基礎設施的 X_Trader 供應鏈攻擊

2023 年 4 月 21 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

除了 3CX 供應鏈攻擊外，這起與北韓有關的網路攻擊行動影響更多組織，包括兩個能源領域的關鍵基礎設施部門

X_Trader 軟體供應鏈攻擊比 3CX 軟體供應鏈攻擊影響更多的組織。賽門鐵克威脅獵手 (Threat Hunter) 團隊的初步調查發現，迄今為止，受害者中包括能源領域的兩個關鍵基礎設施組織，一個在美國，另一個在歐洲。除此之外，還包含兩個金融交易的組織也遭入侵。

正如 Mandiant 昨天的報導，被植入惡意木馬的 X_Trader 軟體是上個月發現 3CX 軟體供應鏈攻擊的原因。由於這一漏洞，3CX 軟體遭入侵並植入惡意程式，許多用戶無意中下載該公司語音和視訊通話軟體 DesktopApp 的惡意版本。除了受害者更多之外，賽門鐵克還發現了更多的入侵指標，列舉如下。

看起來 X_Trader 供應鏈攻擊很可能是出於獲取金錢利益上的動機，因為 X_Trader 軟體的開發商：Trading Technologies 促進期貨交易便利性，包含能源期貨。然而，對關鍵基礎設施目標的破壞是一個令人擔憂的原因。眾所周知，北韓支持的威脅攻擊者既從事間諜活動，也發動獲取金錢利益動機的攻擊，不能排除在獲取金錢利益行動中，遭入侵的組織多具有相當高的戰略意義，會成為進一步侵入的目標。

惡意安裝程式

初始感染鏈從檔名為 X_TRADER_r7.17.90p608.exe（SHA256 ：900b63ff9b06e0890bf642bdfcbfcc6ab7887c7a3c057c8e3fd6fba5ffc8e5d6 ）的被植入木馬的惡意安裝程式開始，此程式是由 "Trading Technologies International, Inc." 簽章，包含一個名為 Setup.exe 惡意執行程式。我們對這個可執行檔案的一個版本（SHA256：aa318070ad1bf90ed459ac34dc5254acc178baff3202d2ea7f49aaf5a055dd43）分析後發現，當執行時，它檢查名為 X_TRADER-ja.mst 的檔案（也包含在安裝程式中），是否在寫死的程式碼中 offset 0x167000 處有以下標記字串 (marker bytes)：

- 5E DA F3 76

如果標記字串存在，它就會建立一個資料夾，名為：

- C:\Programdata\TPM

然後，它將檔案 C:\Windows\Sysnative\immersivetpmvscmgrsvr.exe 複製到新檔案夾中，路徑為 C:\Programdata\TPM\TpmVscMgrSvr.exe。

接下來，它將植入兩個惡意的DLL ：

- C:\Programdata\TPM\winscard.dll (SHA256: cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2)
- C:\Programdata\TPM\msvcr100.dll (SHA256: d937e19ccb3fd1dddeea3eaaf72645e8cd64083228a0df69c60820289b1aa3c0)

該植入檔案的內容是採用以下密鑰的 XOR 演算法，並對前面提到的檔案 X_TRADER-ja.mst 區塊進行解密產生的：

- 74 F2 39 DA E5 CF

為了在受害者的系統上能夠常駐，該惡意軟體呼叫 CLSID_TaskScheduler COM 物件，可能是為了建立一個定期執行的排程任務，定期執行以下檔案：

- C:\Programdata\TPM\TpmVscMgrSvr.exe

然後 Setup.exe 會注入一個名為 X_TRADER.exe 的檔案，該檔也包含在安裝程式中。該檔案內容是採用 XOR 演算法，從它自己一個可移植、可執行資源中解密，從寫死在程式碼中的 offset 0x1CB40 開始，並使用以下金鑰：

- 74 F2 39 DA E5 CF

安裝過程將執行 X_Trader.exe，然後自我刪除。

安裝後門

一旦安裝後，合法 X_Trader 可執行檔案會側載安裝程式植入的兩個惡意 DLL。首先 winscard.dll 會被載入，隨後將載入和執行第二個 (msvcr100. dll) 有效籌載。msvcr100. dll 檔案包含一個附加到該檔案的加密 blob。該 blob 以十六進制的值 FEEDFACE 為起始字串，載入程式使用該值來尋找 blob。

有效籌載的安裝過程幾乎與被植入惡意木馬的 3CX 應用程式過程相同，其中兩個側載的 DLL 被用來從加密的 blob 中提取有效籌載。

在這次攻擊中，提取的有效籌載是一個名為 Veiledsignal(SHA256：e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345)的模組化後門程式。Veiledsignal包含另一個 DLL(SHA256：19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae)，這是一個處理序插入模組。它可以被插入到 Chrome 、Firefox 或 Edge 網頁瀏覽器中。該模組包含第二個 DLL(SHA256：f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce)，這是一個命令和控制 (C & C) 模組。它連接到以下 C&C 的網址：

- https://www.tradingtechnologies.com/trading/order-management

類比海德拉 (Hydra)：九頭蛇的複雜刁鑽攻擊行動

發現 3CX 被另一次早期的供應鏈攻擊入侵後，很有可能會有更多組織受到此行動的影響，現在還發現此行動的範圍比原來認為要廣泛得多。這些成功入侵幕後的攻擊者，顯然有一個成功的軟體供應鏈攻擊範本，故不能排除未來會有進一步的類似攻擊。

保安註解說明：海德拉(Hydra)--為希臘傳說中的九頭蛇，據說若將其中一個頭砍，就會又長出兩個新的頭來。

防護方案／緩解措施

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)。

入侵指標 (IOCs)

如果 IOC 是惡意的並且我們可以取得該檔案，賽門鐵克端點安全系列解決方案就能偵測並阻止該檔案。入侵指標 (IOC) 如下所述：

900b63ff9b06e0890bf642bdfcbfcc6ab7887c7a3c057c8e3fd6fba5ffc8e5d6－被植入惡意木馬程式的安裝程式 (X_TRADER_r7.17.90p608.exe)

6e989462acf2321ff671eaf91b4e3933b77dab6ab51cd1403a7fe056bf4763ba－可能有被植入惡意木馬程式的安裝程式

aa318070ad1bf90ed459ac34dc5254acc178baff3202d2ea7f49aaf5a055dd43－被植入惡意木馬程式的安裝程式的部分惡意元件(setup.exe)

6e11c02485ddd5a3798bf0f77206f2be37487ba04d3119e2d5ce12501178b378－被植入惡意木馬程式的安裝程式的部分惡意元件(setup.exe)

47a8e3b20405a23f7634fa296f148cab39a7f5f84248c6afcfabf5201374d1d1－隨作業系統啟動的惡意測載程式(tpmvscmgrsvr.exe)

cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2－載入程序(winscard.dll)

277119738f4bdafa1cde9790ec82ce1e46e04cebf6c43c0e100246f681ba184e－載入程序(devobj.dll)

cb374af8990c5f47b627596c74e2308fbf39ba33d08d862a2bea46631409539f－惡意DLL檔 (msvcr100.dll)

d937e19ccb3fd1dddeea3eaaf72645e8cd64083228a0df69c60820289b1aa3c0－惡意DLL檔 (msvcr100.dll)

e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345－Veiledsignal 主要元件

19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae－Veiledsignal 程序注入模組

f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce－Veiledsignal 通訊模組

https://www.tradingtechnologies[.]com/trading/order-management－Veiledsignal C&C 伺服主機

\\.\pipe\gecko.nativeMessaging.in.foo8bc16e6288f2a－Veiledsignal 程序的雙向 named pipe

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 Edg/95.0.1020.40－Veiledsignal 用戶端程式

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。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/4

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。