新的間諜行動瞄準東南亞

2021 年 10 月 20 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

未知攻擊者使用無過往紀錄可查的工具組，瞄準國防、醫療保健和資通 (ICT) 行業。

使用無過往紀錄可查的工具組進行的間諜行動，已對東南亞的一系列組織為目標。已被證實的目標包括國防、醫療保健以及資通 (ICT) 行業的組織。該行動似乎早在 2020 年 9 月就開始，並至少持續到 2021 年 5 月。

攻擊者使用的工具組包括下載器、模組化的後門程式、鍵盤側錄程式和被設計來濫用雲儲存服務 Dropbox 的滲漏工具。

攻擊者工具箱

攻擊者採用的初始感染媒介仍然未知。嘗試入侵的最早跡象是一個載入器，它從 .dat 檔案解密並載入。.dat 檔案至少有兩個不同的檔案名稱：sdc-integrity.dat 和 scs-integrity.dat。載入器還從解密的有效籌載中呼叫 DumpAnalyze 輸出。

有效籌載 (payload) 尚未被定義（名稱），但幾乎可肯定是模組化的後門。這可從已識別的模組中推斷出來。這個「Orchestrator」模組指出一個單獨存在的 DLL 模組，該模組公開至少 16 個函數，及存在一個由 Orchestrator 使用但單獨實現的自定義二進制之命令和控制 (C&C) 協議。

該模組似乎是後門的核心元件。它是以 Windows 服務執行，其大部分功能從註冊表掛載到個別的 DLL 中 (位於 HKEY_CLASSES_ROOT\.z\OpenWithProgidsEx\<value_name_resolved_at_runtime>)。

該模組預計將導出以下功能：

- Construct
- ConnectHost1
- ForceCloseSocket
- Accept
- Recv
- RecvEx
- Send
- SendEx
- BindShell
- TransmitData_htran

- KillChildenProcessTree (sic)
- ExtractIPToConnect
- ExtractIPToConnect1
- GetDeviceInfoString1
- GetPseudoSocketInfo
- Decrypt_ByteToByte

該模組從檔案 (CSIDL_COMMON_APPDATA\Microsoft\Crypto\RSA\Keys.dat) 或註冊表 (HKEY_CLASSES_ROOT\.z\OpenWithProgidsEx\CONFIG) 引入配置。該配置已加密。該模組使用來自單獨 DLL 的函數 Decrypt_ByteToByte 來解密配置。該配置包含以下選項（以 XML 格式儲存）：

- FLAG
- Ip
- Dns
- CntPort
- LstPort
- Blog
- DropboxBlog
- SvcName
- SvcDisp
- SvcDesc
- SvcDll
- OlPass
- OlTime
- SelfDestroy

該模組還使用硬編碼的互斥鎖 (hardcoded mutex) 名稱：GlobalQVomit4。

行動中使用的其他工具，包括鍵盤側錄器，它顯示出由同一開發人員撰寫的跡象，與其他工具和字串混淆技術共用特定的字串。攻擊者也使用了 7zr，這是一種合法工具，它是 7-Zip 壓縮程式的輕量化版本，此外還有一種將竊取的資料發送到 Dropbox 的資料洩露工具。

可能採用聲東擊西的「偽旗」戰術

目標的性質和使用的工具具有間諜活動的所有特徵。賽門鐵克尚未將攻擊歸類為已知的攻擊者，而且攻擊者似乎採取了一些措施來使歸類變得愈加複雜。例如：目前尚不清楚該組織使用什麼語言，並且發現的後門模組樣本中包含的字串似乎是西里爾文和烏爾都語腳本。

迄今為止發現的唯一潛在線索是，其中同一時期被攻擊的組織之一也被中國相關 Leafhopper 集團 (又名 APT30) 使用的工具所攻擊。但是，目前還沒有證據表明該工具與該活動有相關聯。

保護／緩解措施

有關最新的防護更新，請訪問賽門鐵克防護公告。

感染指標 (IOC:Indicators of Compromise)

Hash	說 明
ac4b50727c69ca7cc3c0a926bb1b75418a8a0eabd369a4f7118bb9bba880e06	載入器
b04be710feba6a070107ff276e1e17e348f534eb9be142271e1ea2fcffa1ef9b	載入器
b25f3e8d1b7fcef6a54fc959d7e82c6a4e2da3836e98766ae4a157484da0b9b1	載入器
1af5252cadbe8cef16b4d73d4c4886ee9cecddd3625e28a59b59773f5a2a9f7f	協調管理(Orchestrator)模組
a6f75af45c331a3fac8d2ce010969f4954e8480cbe9f9ea19ce3c51c44d17e98	協調管理(Orchestrator)模組
d1ff2ded43e2d9c2e6e07e71f0e3adb815ea0eef7ca391ee272b874807add4a	協調管理(Orchestrator)模組
7904ce020b55a6343005db5a5dad7d841db8300fb270c78e8585903e1de13e2	滲漏工具
a15eda7c75cf4aa14182c3d44dc492957e9a9569e2d318881e5705da2b882324	鍵盤側錄器
967e8063bd9925c2c8dd80d86a6b01deb5af54e44825547a60c48528fb5f896d	鍵盤側錄器
64f036f98aad41185163cb328636788a8c6b4e1082ae336dad42b79617e4813d	未知檔案
91b3022e776d1ffb350e550911d08f10d30678bcb4c17d9c0ae5088f5e63146e	未知檔案
c3aee1f79e27af6ddc8ded38bfdfab004ad489c8f81f7928cfea5c05a3605338	可疑的載入器
37d0c0afaa77c7363b6515eff9590eba546cce2a751a454d5200a25b7c24dfef	未知檔案

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/espionage-campaign-south-east-asia

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