Webworm：間諜攻擊者正在使用並測試較舊版且已客製化的 RATs

2022 年 9 月 15 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

攻擊者正在研究一些有威脅性的惡意軟體，其中一些已經在攻擊中使用，而另一些則處於預先部署或測試階段。

賽門鐵克的威脅獵手團隊 (現為博通 (Broadcom) 軟體事業部的企業資訊安全部門) 正在深入研究一個我們稱之為 Webworm 團體的當前活動。該組織已經開發三個舊版本的已客製化遠端存取木馬 (RAT)，包括 Trochilus、Gh0st RAT 和 9002 RAT。賽門鐵克觀察到至少有一個入侵指標 (IOCs) 被用於攻擊一個在亞洲多國營運的 IT 服務提供商，而其他的似乎處於預先部署或測試階段。

Webworm

賽門鐵克發現 Webworm 與一個被稱為 "Space Pirates" 組織有關聯，此前 Positive Technologies 已在 2022 年 5 月一份報告中記錄這個組織。這兩個組織很可能是同一團隊。據瞭解，Webworm 至少從 2017 年開始活躍，目標是位於俄羅斯、格魯吉亞 (喬治亞)、蒙古和其他一些亞洲國家的政府機構和涉及 IT 服務、航太和電力行業的企業。以前對該組織活動研究發現，它使用隱藏在誘餌檔案後面的自訂載入器和修改過的後門，這些後門已經存在相當長的一段時間。這與賽門鐵克最近觀察到 Webworm 活動相吻合。

Webworm 威脅使用的惡意軟體包括以下的版本：

Trochilus RAT

最早於 2015 年被首次發現，Trochilus 是一個用 C++ 開發的 RAT，其原始程式碼可在 GitHub 上下載。該惡意軟體已被多個團體用於有針對性的威脅行動，其特色是有助於躲避沙箱分析並在網路間諜行動中發揮作用。該 RAT 的功能包括下載、上傳和執行檔案的能力，但不限於可遠端移除檔案管理員的能力。

Trochilus 被發現和已知威脅者的惡意軟體行動有關，威脅者也使用 PlugX 和 9002 RAT 變種惡意軟體。

9002 RAT

9002 RAT 似乎至少從 2009 年被開始使用，並在歷史上一直被國家支援的行為者所使用。該

惡意軟體為攻擊者提供廣泛的資料外流能力。某些 9002 RAT 的變種使用插入記憶體攻擊且不寫入儲存區，此一特徵也與賽門鐵克分析的樣本符合。

該惡意軟體已被一系列行為者用於多個活動中，包括針對位於韓國的幾家大型企業的駭客行動。該 RAT 被用來將其他惡意軟體，包括 PlugX RAT 發送到被攻擊的機器上。它還參與利用零日漏洞的攻擊。

Gh0st RAT

雖然 Gh0st RAT 的原始程式碼已於 2008 年在網路上發佈，但該惡意軟體仍被進階持續威脅 (APT) 組織使用。Gh0st RAT 在 2009 年首次成為頭條新聞，當時一個名為 GhostNet 的網路間諜組織用它來攻擊世界各地的外交、政治、經濟和軍事目標。

已被發現的 Webworm 活動

賽門鐵克觀察到三個由 Webworm 開發的惡意軟體病毒植入程式。

- 6201c604ac7b6093dc8f6f12a92f40161508af1ddffa171946b876442a66927e (Trochilus dropper)
- b9a0602661013d973bc978d64b7abb6bed20cf0498d0def3acb164f0d303b646 (Trochilus Dropper)
- c71e0979336615e67006e20b24baafb19d600db94f93e3bf64181478dfc056a8 (Trochilus Dropper)

對其中一個病毒植入程式的分析顯示，它植入以下檔案。

- [TEMP]\Logger.exe (28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679)
- [TEMP]\sc.cfg (a618b3041935ec3ece269effba5569b610da212b1aa3968e5645f3e37d478536)
- [TEMP]\logexts.dat (a6b9975bfe02432e80c7963147c4011a4f7cdb9baaee4ae8d27aaff7dff79c2b)
- [TEMP]\logexts.dll (a73a4c0aa557241a09e137387537e04ce582c989caa10a6644d4391f00a836ef)
- [TEMP]\logger.dat (10456bc3b5cfd2f1b1ab9c3833022ef52f5e9733d002ab237bdebad09b125024)
- [TEMP]\[RANDOM_DIGITS].doc (d295712185de2e5f8811b0ce7384a04915abdf970ef0f087c294bb00e340afad)

合法的可執行檔 Logger.exe 被用來調用 "LoadLibraryA" API，以載入惡意的 "[TEMP]\logexts.dll" 檔案。

logexts.dll 檔案是一個載入器。一旦執行，它將檢查執行緒的命令列參數。如果命令列是單一參數 "isdf"，它就試圖從 "WINLOGON.EXE" 執行緒中竊取一個安全性權杖。然後，它通透過調用 CreateProcessAsUserW API 啟動以下執行緒。

C:\ProgramData\Logger\Logger.exe mdkv

否則，它將根據自己正在執行的可執行檔建構第二階段的路徑名，其中用硬式編碼的 "dat" 替換最後三個字元 (結果為 "Logger.dat")。然後讀取並執行第二階段的 shellcode。

第二階段 ("Logger.dat") 建構第三階段的路徑名，也是基於它自己正在執行的可執行檔，其中它將目錄部分與硬式編碼的 "logexts.dat" 相結合。最後，它讀取並執行第三階段。

logexts.dat 檔案被混淆處理，包括可繞過幾個用戶帳戶控制 (UAC) 的限制。

它試圖將先前植入的檔案複製到以下新位置：

- [Temp]\Logger.exe to C:\ProgramData\Logger\Logger.exe
- [Temp]\Logger.dat to C:\ProgramData\Logger\logger.dat
- [Temp]\logexts.dll to C:\ProgramData\Logger\logexts.dll
- [Temp]\logexts.dat to C:\ProgramData\Logger\logexts.dat
- [Temp]\sc.cfg to C:\ProgramData\Logger\sc.cfg

然後，該檔案在記憶體中解壓並執行其後門有效載荷，即 Trochilus RAT (e69177e58b65dd21e0bbe4f6caf66604f120e0c835f3ee0d16a45858f5fe9d90) 的變種。

Trochilus 修改包括從檔案中載入其參數的功能，方法是檢查以下任何位置 (按優先順序)：

- C:\ProgramData\Logger\sc.cfg
- C:\ProgramData\resmon.resmoncfg
- C:\ProgramData\appsoft\resmon.resmoncfg

設定檔的內容是用 Lempel-Ziv-Welch (LZW) 演算法解壓縮。

有趣的是，上述位置之一 ("C:\ProgramData\resmon.resmoncfg") 在其它資安廠商以前對 Space Pirates (Webworm) 活動的研究曾被提及並詳細解說。

然後，該惡意軟體向svchost.exe插入以下能力：

- 執行命令
- 下載疑似的惡意檔案

賽門鐵克進一步調查發現，與用來部署被 Webworm 修改 Trochilus RAT 程式版本，其結構相似的植入程式也被用來部署另外兩個修改的 Gh0st RAT 和 9002 RAT版本。對 Trochilus RAT 變種所作的一些程式碼修改，也出現在另外兩個重新調整的 RAT 中。這些額外的 RATs 包括：

Gh0st RAT：

- 1e725f1fe67d1a596c9677df69ef5b1b2c29903e84d7b08284f0a767aedcc097 (Dropper)
- b0a58c6c859833eb6fb1c7d8cb0c5875ab42be727996bcc20b17dd8ad0058ffa (Shellcode loader)
- 1CC32C7F2C90A558BA5FF6BA191E655B20D7C65C10AF0D5D06820A28C2947EFD (Shellcode loader)

9002 RAT：

- 6e46054aa9fd5992a7398e0feee894d5887e70373ca5987fc56cd4c0d28f26a1 (Dropper)
- 37fa5108db1ae73475911a5558fba423ef6eee2cf3132e35d3918b9073aeecc1 (Packed backdoor)

Webworm 對 9002 RAT 這個版本所做的改變顯然是為了逃避檢測。例如：該RAT通訊協定的細節，如加密方法也被威脅者修改。

Gh0st RAT (BH_A006) 活動在協力廠商研究中已被記錄下來，詳細說明以前 Webworm (Space Pirates) 活動。在該研究中，Gh0st RAT 的版本含有多種功能，例如：繞過安全保護的混淆和阻礙分析、網路服務建立、繞過UAC以及在記憶體中解壓和啟動 shellcode 程式碼。其中一些功能也存在於 Webworm 正在準備的 RAT 版本中。

結論

Webworm 使用舊版本，在某些情況下是開放原始碼惡意軟體的客製版本，已知與被稱為 Space Pirates 組織的程式碼相似，這表示他們可能是同一個威脅集團。然而，此類型工具的共同使用和該地區各團體之間的工具交流，可以掩飾不同的威脅團體蹤跡，這可能是採用這種方法的原因之一，另一個原因是成本，因為開發複雜的惡意軟體在金錢和時間上都非常昂貴。

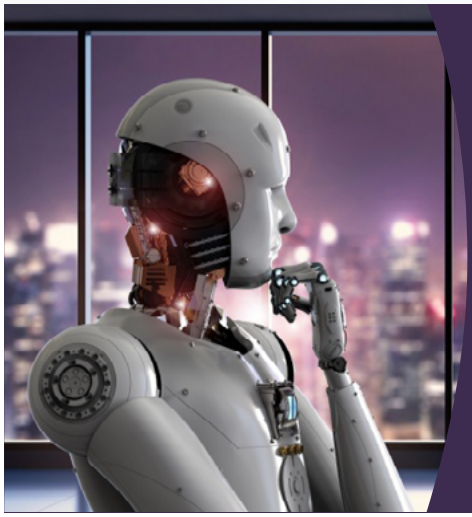
防護方案／緩解措施

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)

c71e0979336615e67006e20b24baafb19d600db94f93e3bf64181478dfc056a8 – Trochilusdropper
28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679 – Logger.exe
a6b9975bfe02432e80c7963147c4011a4f7cdb9baaee4ae8d27aaff7dff79c2b – logexts.dat
a73a4c0aa557241a09e137387537e04ce582c989caa10a6644d4391f00a836ef – logexts.dll
10456bc3b5cfd2f1b1ab9c3833022ef52f5e9733d002ab237bdebad09b125024 – logger.dat
d295712185de2e5f8811b0ce7384a04915abdf970ef0f087c294bb00e340afad – [RANDOM_DIGITS].doc
e69177e58b65dd21e0bbe4f6caf66604f120e0c835f3ee0d16a45858f5fe9d90 – TrochilusRAT
a618b3041935ec3ece269effba5569b610da212b1aa3968e5645f3e37d478536 – Backdoorconfiguration
6201c604ac7b6093dc8f6f12a92f40161508af1ddffa171946b876442a66927e – Trochilusdropper
3629d2ce400ce834b1d4b7764a662757a9dc95c1ef56411a7bf38fb5470efa84 – Backdoorconfiguration
b9a0602661013d973bc978d64b7abb6bed20cf0498d0def3acb164f0d303b646 – Trochilusdropper
824100a64c64f711b481a6f0e25812332cc70a13c98357dd26fb556683f8a7c7 – Packedbackdoor

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats



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