與北韓有關聯的間諜行動繼續瞄準高價值目標

2022 年 4 月 27 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

間諜組織重點專注在獲取具有民用和軍用的機密或敏感智慧財產。

與北韓有關的 Stonefly (*石蠅) 駭客集團正繼續對高度專業的工程公司發動間諜攻擊，目的可能是為了獲得敏感的智慧財產。

Stonefly 擅長針對審慎選擇後的目標發起針對性攻擊，這些目標具有價值連城的智慧財產，以協助能源、航太和軍備等有助戰略發展的行業。幾乎所有它感興趣的技術都具有軍事和民用用途，其中一些可以應用於發展先進武器。

前科累累的攻擊史

Stonefly（又名 DarkSeoul、BlackMine、Operation Troy 和 Silent Chollima）於 2009 年 7 月首次引起注意，當時它對一些南韓、美國政府和金融網站發起分散式拒絕服務 (DDoS) 攻擊。

它於 2011 年再次出現，當時發動更多 DDoS 攻擊，但當發現它對選定目標使用複雜的後門木馬 (Backdoor.Prioxer) 時，也暴露其攻擊的間諜盤算。

2013 年 3 月，該組織與針對多家韓國銀行和廣播公司的 Jokra (Tojan.Jokra) 磁碟刪除攻擊有關。三個月後，該組織參與針對韓國政府網站一系列 DDoS 攻擊。

近年來，該組織的功力顯著增強，至少自 2019 年以來，賽門鐵克已發現其重點轉移到鎖定特定高價值目標的間諜活動上。現在似乎專門針對擁有高機密或高度敏感資訊或智慧財產的組織。Stonefly 的行動似乎是一系列北韓贊助更廣泛的竊取資訊和智慧財產行動，而另一個知名的「Dream Job* 夢想工作」行動，則是由另一個北韓組織 Pompilus 進行跨越多個部門更廣泛情報獵捕拖網行動。

最新目標

賽門鐵克 (現為全球網通晶片巨擘博通--Broadcom 的企業安全部門，美國股市代號：AVGO，全世界網際網路流量有 99.9% 都經過博通的晶片設備) 最近發現的攻擊是針對一家從事能源和軍事領域工作的工程公司。攻擊者於 2022 年 2 月入侵該組織，很可能是透過利用面向公眾的 VMware View 伺服器上 Log4j 漏洞 (CVE-2021-44228) 做攻擊。攻擊者隨後進行橫向移動並入侵另外 18 台電腦。

17 小時後：在突破第一台主機後後不久，攻擊者安裝 Stonefly 更新版 Backdoor.Preft 惡意軟體 (又名 Dtrack、Valefor)。攻擊者隨後使用偽裝為檔名：pvhost.exe 的 PuTTY 之 PSCP 命令列應用程式，推測是為了從受感染的電腦中竊取資料。PSCP 執行後不久，偽裝成檔名 pl.exe 憑證轉儲工具 Mimikatz 被執行。

第 2 天：惡意活動在 3proxy tiny proxy server 執行時重新啟動，這是一個公開可用的代理工具 (檔名：svhost.exe)。在接下來四天裡持續使用這個工具。這四天的兩天內安裝了第二個可疑代理工具 (檔名：tapi.exe)。幾個小時後，安裝 Preft 後門 (檔名：svchost.exe) 副本。兩天後，使用 WinSCP，一個開放原始碼 SSH 檔案傳輸工具，大概是為將資料洩露或上傳到被入侵的電腦上。

第 3 天：入侵的下一階段在第二天開始，當時執行 Preft，攻擊者開始在該組織的網路中橫向移動，使用 Invoke-TheHash，一個公開 PowerShell 傳遞雜湊工具 (檔名：rev.ps1) 以及 wmiexec.py，一個公開可用的 Impacket 工具，用於執行 WMI 命令(檔名：notepad.exe)。

更新版的 Preft 後門

攻擊者使用 Stonefly 更新版本，且自定義 Preft 後門。對該後門分析後證明它是一個多階段工具：

階段 1 是主要的二進位檔案。此階段使用 python 腳本用於解壓縮二進位檔案和 shellcode。

第 2 階段是 shellcode。它執行以下操作：

- 休眠 19,999 秒，可能是為了逃避沙箱偵測。
- 打開一個 mutex，其名稱在 Stage 3 shellcode 中指定。
- 它不載入可執行檔，而是啟動 Internet Explorer (iexplore.exe) 或 explorer.exe 並將 Stage 3 shellcode 注入其中之一。它設定一個具名管道（“.pipepipe”）進行通訊。主二進位檔案的檔案名稱通過管道發送。

第 3 階段是更多的 shellcode。

第 4 階段是有效籌載。它是一個 HTTP 遠端存取工具 (RAT)，支援各種命令，包括：

1. 下載（下載檔案並儲存在本地端）
2. 上傳（上傳檔案到 C&C 伺服器）
3. 設定間隔（更改 C&C 伺服器查詢間隔 - 以分鐘為單位）
4. Shell Execute（在shell中執行命令）
5. 下載外掛程式
6. 更新（下載新版本並替換）
7. Info（傳回目前感染相關的偵錯資訊）
8. 反安裝移除
9. 下載可執行檔案

該惡意軟體可以支援四種不同類型的外掛程式：可執行檔案、VBS、BAT 和 shellcode。它支援三種不同的持續模式：啟動時的捷徑、服務、登錄檔和程式排程。

客製化的竊密程式

除了 Preft 後門，Stonefly 還部署一個似乎是客製開發的竊密程式 (infostealer)。對該惡意軟體分析顯示，它是一個三階段威脅。主二進位檔案使用修改後 RC4 演算法提取和解密該加密的 shellcode。

第 2 階段是 shellcode，它搜索有效籌載並使用相同的修改後 RC4 演算法對其進行解密。解密後的有效籌載是一個載入到記憶體中的可執行檔案。目的在使用預先設定的參數在受感染的電腦上搜尋檔案。然後將它們複製到暫存檔案中，隨後複製到單一 .zip 檔案中，並刪除暫存檔案。ZIP 檔案路徑為 %TEMP/~[XXXXXXXX].tmp，其中 XXXXXXXX 是電腦名稱的簡單雜湊值（八個大寫十六進制數字）。

奇怪的是這個 ZIP 檔案不會自動外洩。有可能是程式碼移除外洩功能，並且攻擊者計劃使用另一種外洩手段。

高價值目標

雖然 Stonefly 的工具和戰術不斷發展，但最近的活動與之前的攻擊之間存在一些共同點，例如：其正在開發 Preft 後門和非常依賴開放原始碼工具。

該組織的能力及其對獲取敏感資訊的專注程度，使其成為當今最強大的北韓網路威脅行為者之一。

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)

我們的威脅獵手團隊持續偵測與分析相關 IOC，並隨時保持 Symantec Endpoint 產品能偵測到並攔截最新的惡意 IOC。

SHA256	Description	File name(s)
3b779a84c17a3a2b588241676ec372c543b592473dae9d6b14db0d0d33522f34	3proxy tiny proxy server	svhost.exe
7ab3f076e70350f06ad19863fdd9e794648020f621c0b1bd20ad4d80f0745142	Backdoor.Preft	mf.exe, mp_updt.exe
537dee22d8bc4867f45deddfa26c6d08a12c09e4fb5b539422e9b4d8fb0dff4a	Backdoor.Preft	svchost.exe
586f30907c3849c363145bfdcdabe3e2e4688cbd5688ff968e984b201b474730	Backdoor.Preft	svchost.exe
453014da94a1382f9f11535b3d90a44d67f43c02ffe8688465956a3ed7e71743	Backdoor.Preft	svchost.exe
d824eb45247f9b8e0266dc739425d80af4145062687d7e825e03adfac1b7e03b	Backdoor.Preft	svchost.exe
414ed95d14964477bebf86dced0306714c497cde14dede67b0c1425ce451d3d7	Backdoor.Preft	credit.exe, credits.exe
30cd61f13d64562a41eb5e8a3d30cd46d8678acd9eef4c73386c3ea4adb50101	Infostealer	mf.exe
8637a4286d87a4fa3b6a102446f437058812be0d4ebb361ac8827ea4f186df23	Infostealer	mf.exe
551653deddb8d9a78c1a239cc2da99ea403ce203c5843384c986149d4c17f26c	Infostealer	mf.exe
b3458b3d0bb80029de30f41ffc8e318176cca650d76b75549089b8a436e8862a	Infostealer	mp_updt.exe
9ca9f414b689fc903afb31401615581488596 6b0e30b21b642819d53ba94533c	Invoke-TheHash	rev.ps1
07b1b9d46a926084019c9e1a22ef724d7dd20fd85d144012dd4855ca66ad96fe	Mimikatz	pl.exe
68d8f895135aab32f0b0f2520f1dd3ea791a0e0fec3e4e21d94040015bbbf096	Mimikatz	pl.exe
5a73fdd0c4d0deea80fa13121503b477597761d82cf2cfb0e9d8df469357e3f8	PuTTY PSCP	pvhost.exe
28d0e945f0648bed7b7b2a2139f2b9bf1901feec39ff4f6c0315fa58e054f44e	Real VNC Bypass Authentication Scanner	vnc.exe, aa.exe
1a0e33a0e434e22e25a17b5d40fbef4fe900f075fcfa0dadd473010d03185e4a	Runasuser privilege escalation tool	sepm.exe
b4a85ef01b5d8058cf94f3e96c48d86ce89b20295e8d1125dc3fc1c799a75789	Suspected proxy tool	tapi.exe
0e20819e5584a31f00d242782c2071734d7e2377306e9ebd20dd435ce9c7d43a	Keylogger	avg.exe, wkeylogger.exe
147187d4ca823187724205a7dbd6502a9409674e6602363d796218503c960e2f	Suspected SOCKS proxy tool	svhost.exe
5e62d4851596e3fb939525fa4437c553ab5c6b9d12920af7740a3473102ccd1a	Unknown file	protect.exe
7399605f47be3d8ed021c9189b6b102461d5dd98a9d9082c71ff368e13cf8541	Unknown file	wax4315.tmp
cb6769bd80d5a234387bdaa907857ae478e2e693a157f29d97b8ce2db07856c1	Unknown file	N/A
dda85ee1e0b4916ebd2eb7cbaeaa969843a19e7b8a9bb5d360a4bbc0bad91877	Unknown file	smssvc.exe
bfa7adeda4597b70bf74a9f2032df2f87e07f2dbb46e85cb7c091b83161d6b0a	WinRAR (old version)	ra.exe
b7de7187f0f0281c17ae349b692f70892689ddf27b6b418142c809b41dfe3ce7	WinSCP	winscp.com
de00c0111a561e88d62fd84f425a6febc72e01e2e927fb76d01603319a34b4b3	WinSCP	winscp.exe
14f0c4ce32821a7d25ea5e016ea26067d6615e3336c3baa854ea37a290a462a8	wmiexec.py	notepad.exe
tecnojournals[.]com	Domain	N/A
semiconductboard[.]com	Domain	N/A
cyancow[.]com	Domain	N/A
bluedragon[.]com	Domain	N/A
hxxps://tecnojournals[.]com/review	Domain	N/A
hxxps://tecnojournals[.]com/general	Domain	N/A
hxxps://semiconductboard[.]com/xml	Domain	N/A
hxxps://semiconductboard[.]com/xcror	Domain	N/A
hxxp://cyancow[.]com/find	Domain	N/A
hxxps://bluedragon[.]com/login	Domain	N/A

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage

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