利用中國間諜工具持續攻擊電信公司的網路攻擊行動

2024 年 6 月 20 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

攻擊者主要地針對某一個亞洲國家的電信公司

攻擊者使用與中國間諜組織相關的工具，在一場長期間諜行動中入侵亞洲某國的多家電信公司。攻擊者在目標公司的網路上安裝後門，並試圖竊取憑證以利取得後續所需的存取權限。

這些攻擊至少從 2021 年就開始，有證據表明，其中一些活動甚至可以追溯到 2020 年。幾乎所有被攻擊的組織都是電信公司，此外還有一家客戶主要是電信行業的服務公司和亞洲另一個國家的一所大學。

使用的工具

行動中使用與一些與中國有關連的間諜行為者有關的客製化惡意軟體，包括：

Coolclient：與 Fireant 集團 (又名 Mustang Panda、Earth Preta) 有關的後門程式。其功能包括鍵盤側錄、讀取和刪除檔案，以及與命令和控制 (C&C) 伺服器通訊。此次行動中使用的後門程式與 Trend 在 2023 年記錄的後門類似。偽裝成谷歌檔案 (googleupdate.exe) 的合法 VLC 媒體播放程式被用於側載 Coolclient 惡意程式載入器 (檔案名：libvlc.dll)。惡意程式載入器從檔名為 loader.ja 的檔案中讀取加密有效酬載。該有效酬載將反過來從檔名為 goopdate.ja 的檔案中讀取第二個加密有效酬載，並將其注入 winver.exe 執行緒。

Quickheal：一個與 Neeedleminer 駭客組織 (又名 RedFoxtrot、Nomad Panda) 有長期關聯的後門。此次行動中使用 Quickheal 變種是一個名為 RasTls.dll 的 32 位元 DLL，其匯出名為 GetOfficeDatatal。

對該惡意軟體分析顯示，它與 Recorded Future 在 2021 年記錄的 Quickheal 變種幾乎完全相同，唯一區別是編譯程式碼中有新的配置細節和 VMProtect 混淆。

該後門使用 TCP 443 埠與名為 swiftandfast.net 已寫死固定值的 C&C 伺服器通訊。它使用是一種自訂通訊協定，該協定的設計看起來像 SSL 流量，但卻使用了自己的加密技術。

Rainyday：是與 Firefly 駭客組織 (又名 Naikon) 有關的後門程式。行動中使用的大多數 Rainyday 變種都是使用名為 fspmapi.dll 惡意程式載入器執行。該惡意程式載入器使用名為 fsstm.exe 的合法 F-Secure 可執行檔進行側載。載入後，它會截取啟動執行緒的可執行檔的磁碟資料夾路徑，並將其設定為目前的目錄。然後，它會取得可執行檔的記憶體位置，並修補其記憶體映射。這樣做似乎是為了在惡意軟體被某個可執行檔載入時劫持執行流程。如果劫持成功，惡意

程式載入器就會從一個名為 dataresz 的檔案中讀取資料，使用單字節 XOR 金鑰 (0x2D) 解密有效酬載，並將其作為 shellcode 執行。

上述病毒的次要變種包括一個帶有『卡巴斯基實驗室』無效數位簽章的變種，以及另一個其載入器從檔名為 iReports 檔案中讀取加密 shellcode 的變種。

另一個變種使用名為 security.dll 的惡意程式載入器執行。它使用名為 msproxy.exe 可執行檔進行側載，這是一個由 Initex 開發名為 Proxifier 的應用程式。該可執行檔的預設名稱是 ProxyChecker.exe，很可能被重新命名以偽裝成微軟檔案。在這種情況下，惡意程式載入器會從名為 nod193100 檔案中讀取加密的 shellcode。使用 XOR 金鑰也不同：0xF6。

經分析，在 VirusTotal 上發現兩個名稱為 nod193100 的檔案與 Bitdefender 於 2021 年記錄 Rainyday 後門所用的惡意程式載入器相似。

其他 TTPs

除上述客製化後門外，攻擊者還使用其他各種戰略、技巧和程序 (TTPs)：

- 可能是客製化開發的鍵盤側錄惡意軟體
- 通訊埠掃描：至少部署三種不同的埠掃描工具
- 通過傾印登錄檔來竊取憑證
- Responder：是一種可公開取得工具，可用作連結本機群組播名稱解析 (LLMNR) NetBIOS 名稱服務 (NBT-NS) 和廣播 DNS (mDNS) 投毒程式
- 啟用 RDP

與中國間諜組織的關係

此次行動中使用的工具與多個中國組織有密切的關聯，至少有三個客製化後門被認為是中國間諜人員專用。Coolclient 與 Fireant 集團有關，而 Quickheal 則與 Needleminer 集團有關。而 Rainyday 則一直由 Firefly 組織使用。包括賽門鐵克在內的多家安全公司普遍認為，這三個組織都是從中國開始發跡。美國國會成立的獨立諮詢機構美中經濟與安全審查委員會將 Firefly 描述為『可能與在南部戰區司令部責任區 (AOR) 活動的 78020 部隊 (中國人民解放軍) 有關 APT』。

參與當前運動的行為者之間聯繫性質尚不清楚。可能性包括但不限於：

- 多個行動者的攻擊，或彼此獨立行動。
- 單個行動者使用從其他團體獲得或共用的工具和／或人員。
- 多個行為者在單次活動中相互支援協作。

此次入侵行動的最終動機尚不清楚。攻擊者可能在收集該國電信部門的情報。另一種可能是竊聽。另外，攻擊者可能試圖建立針對該國關鍵基礎設施的破壞能力。

防護方案／緩解措施

有關 Alpha 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 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

089809e73354648b3caed7db6bc24dcce4f2ef0f327206fd14f36c6619d9ed30 – Rainyday loader
1906e7d5a745a364c91f5e230e16e1566721ace1183a57e8d25ff437664c7d02 – Quickheal
3aae73ff8ff5973c74af5a7991ca6a57ce797b7b775e1358efd9d76b67b5797b – Rainyday loader
4c136270ca4c17edb77985aca570e291fa77abaaa48761f85e184892089164a6 – Coolclient
6a5fdbe9579b69d4a5e1f6930145debd5adb2a9f93dd052bfb442cbd0141277b – Coolclient
6ad67d7f76986359865667bdd51ba267f6bd7e560270512074448dd7b088bcb7 – Rainyday loader
c348eba51897fbd55ca3ffdaab21259b8f73688e6e008b923ebc597c6272d2d9 – Coolclient
c61daa0df88a33387b94b22bfc0b68d1211a57357aff401613c07832b5192fc0 – Rainyday loader
dc9a12574f8c3b5bed6043b1cd3fd43672779d132c864bb22ae8b0a5dee24576 – Rainyday loader
e32c5e6d70895f0d071f420b7ff28c6fe0eaf2c08eeebe39122b3b1fd1981473 – Rainyday loader
f45dabd683795f099a40553e5d85c9bc8a15bb964c992b45cec48c620ff78fdb – Rainyday loader
103.180.161[.]123
110.34.166[.]198
203.159.95[.]197
115.79.207[.]240
206.189.140[.]171
117.2.82[.]149
113.160.186[.]153
134.209.147[.]60
139.59.35[.]77
134.209.156[.]5
139.84.137[.]139
139.84.130[.]178
139.59.37[.]50
139.84.165[.]248
139.84.166[.]131
139.84.163[.]162
14.161.4[.]152
142.93.223[.]200
146.190.18[.]167

143.110.250[.]11
143.110.244[.]132
159.65.158[.]28
159.89.170[.]164
157.245.107[.]16
38.60.254[.]243
43.152.200[.]62
206.189.136.180
65.20.66[.]128
49.204.77[.]162
65.20.66[.]214
65.20.69[.]80
65.20.70[.]110
65.20.82[.]212
65.20.73[.]72
65.20.76[.]211
swiftandfast[.]net

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/threat-intelligence/telecoms-espionage-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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。