針對中東和亞洲電信組織的間諜行動

2021 年 12 月 14 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

暫定與伊朗支持的 Seedworm 駭客集團有關聯

在過去六個月中，最有可能與伊朗有關的攻擊者，一連串攻擊了中東和亞洲的電信運營商，此外還有一些資訊科技 (IT) 服務組織和一家公用事業公司。

以色列、約旦、科威特、沙烏地阿拉伯、阿拉伯聯合大公國、巴基斯坦、泰國和寮國的電信組織成為該行動的目標，該行動似乎沒有使用自定義惡意軟體，而是依賴合法工具、公開可用的惡意軟體和就地取材的戰術的組合。雖然攻擊者的身份仍未獲得證實，但有一些證據顯示與伊朗的 Seedworm (又名 MuddyWater* 髒水) 組織有聯繫。鎖定的目標和使用戰術與伊朗贊助的攻擊者一致。

攻擊概述

在入侵目標網路後，攻擊者通常會嘗試竊取憑證並在網路中橫向移動。他們似乎對 Exchange Server 特別感興趣，將 Web shell 部署到它們上面。在某些情況下，攻擊者可能會利用受入侵的組織作為其他受害者的跳板。此外，某些目標可能僅為了對其他組織執行供應鏈類型的攻擊而已經遭到入侵。

在大多數攻擊中，感染媒介是未知的。僅在一個目標上發現可能載體的證據。可疑的Screen Connect 安裝程式 MSI 似乎已以名為「特殊折扣計劃.zip」壓縮檔交付，這表明它以魚叉式網路釣魚電子郵件的形式到達。

電信攻擊

在 2021 年 8 月開始的一次針對中東電信公司攻擊中，入侵的第一個證據是建立了一個服務來啟動一個未知的 Windows 腳本檔 (WSF)。然後使用腳本發出各種尋找網域、用戶和遠端服務的指令。

攻擊者使用 PowerShell 下載另一個 WSF 並運行它。Net group 用於查詢「Exchange Trusted Subsystem」網域群組。

攻擊者使用 Certutil 下載可疑的 Ligolo 隧道工具並啟動 WMI，該工具用於獲取遠端電腦執行以下任務：

- 執行 Certutil 以下載未知檔
- 執行 Certutil 以下載未知的 WSF 檔並執行 Wscript 以啟動此腳本
- 執行 PowerShell 以下載和執行內容
- 執行 PowerShell 以將可疑的 Web shell 下載到 Exchange Server

根據程序歷程資料，攻擊者似乎廣泛使用腳本。這些腳本可能是用來收集資訊和下載其他工具的自動腳本。但是，在一個實例中，出現一個 cURL 尋求說明的指令，這顯示攻擊者可能至少進行一些手動鍵盤的操作。

然後，攻擊者使用被認為是eHorus的遠端存取工具執行以下任務：

- 提交並運行可疑的本地安全性授權子系統服務（LSASS）傾印工具
- 提交被認為是 Ligolo 的隧道工具
- 執行 Certutil 以從 Exchange Web Services (EWS) 請求似乎是其他目標組織的網址鏈接 (URL)

針對電信組織的此攻擊的特徵是，攻擊者可能試圖利用連接到其他組織的 Exchange Web 服務（EWS）、另一家電信運營商和同一區域中的一家電子設備公司來轉向其他目標。使用以下命令：

- certutil.exe -urlcache – split [DASH]f hxxps://[REDACTED]/ews/exchange[.]asmx
- certutil.exe -urlcache – split [DASH]f hxxps://webmail.[REDACTED][.]com/ews

目前尚不清楚這些請求的意圖是什麼。攻擊者可能試圖檢查與這些組織的連接。

可能是另一起供應鏈攻擊

一個疑似異常目標是寮國的一家公用事業公司。感染媒介可能是利用對公開服務公眾服務的攻擊，因為第一台似乎受到入侵電腦主機是 IIS Web 伺服器。可疑活動在程序歷程中也有 w3wp.exe。

然後，攻擊者使用 PowerShell 來：

- 下載可疑的 Ligolo 隧道工具
- 下載未知的 PowerShell 腳本
- 下載未知的 XLS 檔

然後，攻擊者使用 PowerShell 連接到泰國一個組織的網路郵件伺服器。他們還試圖連接到屬於泰國另一家公司 IT 相關伺服器。

為了便於竊取憑證，WMI 用於執行 PowerShell 以修改註冊表 (登錄檔)，以明文形式將密碼存儲在記憶體中。除此之外，似乎還部署了公開可用的 CrackMapExec 工具的混淆版本。

工具集

攻擊者大量使用合法工具和公開可用的駭客工具。這些包括：

- ScreenConnect：合法的遠端管理工具
- RemoteUtilities：合法的遠端管理工具
- eHorus：合法的遠端管理工具
- Ligolo：反向通道工具
- Hidec：用於執行隱藏視窗的命令列工具
- Nping：封包生成工具
- LSASS Dumper：從本機安全認證子系統服務（LSASS）程序傾印憑證的工具
- SharpChisel：通道工具
- Password Dumper：密碼傾印工具
- CrackMapExec：公開可用的工具，用於自動執行 Active Directory 環境的安全評估
- ProcDump：Microsoft Sysinternals 工具，用於監視應用程式的 CPU 峰值和生成故障傾印，但也可以用作一般程序傾印程式
- SOCKS5 代理伺服器：通道工具
- Keylogger：檢索瀏覽器憑證
- Mimikatz：公開可用的憑證傾印工具

與 Seedworm(* 種子蟲) 駭客集團有關連嗎？

有證據顯示，這些攻擊可歸咎於伊朗所支持的 Seedworm 駭客集團。此行動中使用的兩個 IP 位址與之前 Seedworm 的活動有所關聯。然而，眾所周知，Seedworm 會定期切換其基礎設施，這意味著無法做出決定性的歸因。

此行動與早期的 Seedworm 行動之間的工具也有一些重疊。ScreenConnect、RemoteUtilities、SharpChisel、Ligolo、ProcDump 和 Password Dumper 都被趨勢科技在 2021 年 3 月關於 Seedworm 活動的部落格中引用。

在兩個工具的情況下--SharpChisel 和 Password Dumper--在本次行動中使用與趨勢科技記載版本相同的版本。

專注特定目標的行動

如果這些攻擊與伊朗有關，這已不是伊朗威脅行為者第一次瞄準電信行業了。2018 年，賽門鐵克揭露了 Chafer 集團已經對中東一家大型電信服務提供者入侵了。

雖然該行動的最終目標尚不清楚，但將焦點集中在電信運營商，彰顯攻擊者正在收集有關該行業的情報，並可能試圖轉向對通信進行間諜活動。

保護／緩解

有關最新的防護更新，請訪問賽門鐵克防護公告。

入侵 (危害／感染) 指標 (IOC:Indicators of Compromise)

ae5d0ad47328b85e4876706c95d785a3c1387a11f9336844c39e75c7504ba365 – Ligolo
e0873e15c7fb848c1be8dc742481b40f9887f8152469908c9d65930e0641aa6b – Ligolo
22e7528e56dffaa26cfe722994655686c90824b13eb51184abfe44d4e95d473f – Hidec
b0b97c630c153bde90ffeefc4ab79e76aaf2f4fd73b8a242db56cc27920c5a27 – Nping
b15dcb62dee1a8499b8ac63064a282a06abf0f7d0302c5e356cdb0c7b78415a9 – LSASS Dumper
61f83466b512eb12fc82441259a5205f076254546a7726a2e3e983011898e4e2 – SharpChisel
ccdddd1ebf3c5de2e68b4dcb8fbc7d4ed32e8f39f6fdf71ac022a7b4d0aa4131 – Password Dumper
facb00c8dc1b7ed209507d7c56d18b2c542c4e0b2986b9bfaf1764d8e252576b – CrackMapExec
1a107c3ece1880cbbdc0a6c0817624b0dd033b02ebaf7fa366306aaca22c103d – ProcDump
916cc8d6bf2282ae0d2db587f4f96780af59e685a1f1a511e0b2b276669dc802 – ProcDump
e2a7a9a803c6a4d2d503bb78a73cd9951e901beb5fb450a2821eaf740fc48496 – ProcDump
f6600e5d5c91ed30d8203ef2bd173ed0bc431453a31c03bc363b89f77e50d4c5 - SOCKS5 proxy server
6d73c0bcdf1274aeb13e5ba85ab83ec00345d3b7f3bb861d1585be1f6ccda0c5 – Keylogger
912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 – Mimikatz
96632f716df30af567da00d3624e245d162d0a05ac4b4e7cbadf63f04ca8d3da – Mimikatz
bee3d0ac0967389571ea8e3a8c0502306b3dbf009e8155f00a2829417ac079fc – Mimikatz
d9770865ea739a8f1702a2651538f4f4de2d92888d188d8ace2c79936f9c2688 - Mimikatz

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-telecoms-asia-middle-east
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。2021/12

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