Graphican：Flea 利用新的後門攻擊外交部門

2023 年 6 月 21 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

該後門利用 Microsoft Graph API 進行命令與控制 (C&C) 通訊

在最近的攻擊活動中，Flea (又稱 APT15、Nickel) 進階持續性滲透攻擊 (APT) 組織持續專注於外交部門，此次攻擊活動從 2022 年末持續至 2023 年初，並利用一個名為 Backdoor.Graphican 的新後門。

該攻擊活動主要針對美洲的外交部門，但該組織還攻擊一個位於美洲國家的政府財政部門以及一家在中南美洲銷售產品的公司。還有一個受害者位於歐洲國家，這有點不尋常。該受害者在 2022 年 7 月還曾遭受過一次看似無關的勒索軟體攻擊。然而，Symantec (Broadcom 旗下的威脅獵手團隊) 觀察到這次攻擊活動的主要焦點似乎確實是美洲的外交部門。

Flea 一直都以瞄準政府目標、外交使團和大使館為特點，很可能目的是為了情報收集。

工具

在這次攻擊活動中，Flea 使用大量的工具。除了新 Graphican 後門外，攻擊者還利用各種現成的工具以及與 Flea 相關聯的工具。我們將在本節中詳細介紹這些工具。

Backdoor.Graphican

Graphican 是已知的 Flea 後門 Ketrican 進化版本，而 Ketrican 本身是基於之前由 Flea 使用的惡意軟體 BS2005。Graphican 與 Ketrican 具有相同的基本功能，不同之處在於 Graphican 利用 Microsoft Graph API 和 OneDrive 獲取對基礎設施的命令與控制權 (C&C)。

這種技術曾在俄羅斯政府支持的 APT 組織 Swallowtail (又稱 APT28、Fancy Bear、Sofacy、Strontium) 在 2022 年一次活動中以類似的方式使用過，並在該活動中傳播 Graphite 惡意軟體。在該活動中，Graphite 惡意軟體使用 Microsoft Graph API 和 OneDrive 作為命令與控制伺服器。

觀察到的 Graphican 樣本中並沒有硬編碼的命令與控制伺服器，而是通過 Microsoft Graph API 連接到 OneDrive，從 『Person』 資料夾內的子資料夾獲取加密的命令與控制伺服器位址。然後，惡意軟體解碼資料夾名稱並將其用作惡意軟體的命令與控制伺服器。所有此變種的惡意軟體都使用相同的參數對 Microsoft Graph API 進行身份驗證。我們可以假設它們都有相同的命令與控制伺服器，該伺服器可以由威脅行為者進行動態更改。

Graphicanh 會在電腦上執行以下操作：

- 通過登錄機碼禁用 Internet Explorer 10 的首次執行精靈和歡迎畫面

- 檢查 iexplore.exe 程式是否運行
- 建立一個 IWebBrowser2 COM 總體物件以存取網際網路
- 通過 Microsoft Graph API 進行身份驗證，獲取有效的存取權杖和重新整理權杖
- 使用 Graph API 列舉 OneDrive 中『Person』資料夾內的檔案和子資料夾
- 獲取第一個資料夾的名稱並對其進行解密，以用作命令與控制伺服器
- 基於受感染電腦的主機名稱、本地端 IP、Windows 版本、系統預設安裝語言和受感染電腦的程式位元數 (32 位元或 64 位元)，產生一個機器人識別碼
- 使用從受害者電腦收集的資訊使用特定格式字串『f$$$%s&&&%s&&&%s&&&%d&&&%ld&&&%s』 或 『f@@@%s###%s###%s###%d###%ld###%s』將機器人註冊到命令與控制伺服器
- 向命令與控制伺服器輪詢新的執行命令

Graphican 可執行的命令包括：

- 『C』--建立從命令與控制伺服器控制的互動指令
- 『U』--在遠程電腦上建立檔案
- 『D』--從遠程電腦下載檔案到命令與控制伺服器
- 『N』--建立具有隱藏視窗的新程式
- 『P』--建立具有隱藏視窗的新 PowerShell 程式，並將結果保存在 TEMP 資料夾中的臨時檔案中，然後將結果發送到命令與控制伺服器

此次攻擊活動中，我們還觀察到 Ketrican 的更新版本，該版本具有硬編碼的命令與控制伺服器，僅實現『C』、『U』和『D』命令。我們還看到一個較早版本的 Ketrican (編譯於 2020 年)，該版本僅實現『N』和『P』命令。這表明該組織正在積極開發和調適 Ketrican，以適應其目標。

其他工具

Flea 在最近的活動中使用了其他工具，包括：

- **EWSTEW**--這是一個已知的 Flea 後門，從感染的 Microsoft Exchange 伺服器上擷取發送和接收的電子郵件。我們在這次攻擊活動中看到這個工具的新變種被使用。
- **Mimikatz、Pypykatz、Safetykatz**--Mimikatz 是一個公開可用的憑證傾印工具。它通過利用 Windows 單一登入功能，讓本地端攻擊者能夠從記憶體中傾印金鑰。Pupykatz 和 Safetykatz 是具有相同功能的 Mimikatz 變種。
- **Lazagne**---一個公開可用的開源工具，用於擷取多個應用程式的密碼。
- **Quarks PwDump**--Quarks PwDump 是一個開源工具，可以傾印各種類型的 Windows 憑證：本機使用者、網域使用者帳戶和暫存的網域憑證。據報導，早在 2013 年，卡巴斯基就曾在一場名為 IceFog 的活動中使用過該工具。
- **SharpSecDump**--Impacket 的 secretsdump.py 遠程 SAM 和 LSA Secrets 傾印功能的 .Net 版本。

- **K8Tools**--這是一個公開可用的工具集，具有各種功能，包括特權提升、破解密碼、掃描工具和漏洞利用。它還包含對各種系統中眾多已知漏洞的利用。
- **EHole**--一個公開可用的工具，可以幫助攻擊者識別存在漏洞的系統。
- **Web shells**--攻擊者使用許多公開可用的 Web shell，包括 AntSword、Behinder、China Chopper 和 Godzilla。Web shell 對受害者的電腦提供了後門。其中一些 Web shell，例如：China Chopper 和 Behinder，與中國的威脅行為者有關聯。
- **CVE-2020-1472 的利用**--這是一個特權提升漏洞，該漏洞存在於當攻擊者使用 Netlogon 遠端通訊協定 (NRPC) 與網域控制器建立有缺陷的 Netlogon 安全通道連線時。成功利用此漏洞的攻擊者可以在網路上的設備上執行特定的應用程式。2021 年第一季以後已經有該漏洞的修補程式可用。

Flea 背景

Flea 自 2004 年以來一直在運行。在這段時間內，它的戰術、技術和程序 (TTPs)，以及它的目標，都發生變化和發展。近年來，該組織主要專注於針對政府組織、外交界和非政府組織 (NGOs) 的攻擊，以進行情報收集。最近，該組織似乎更加關注北美和南美地區，這與我們在這次攻擊中觀察到的目標一致。該組織的目標似乎是為了長期存取感興趣的受害者網路，以進行情報收集。在這次攻擊中，它目標是外交部門，這也表明該活動背後可能存在地緣政治動機。

Flea 通常使用電子郵件作為初始傳染途徑，但也有報告稱其利用公眾性的應用程式，以及使用 VPN 來獲得對受害者網路的初始存取權。

微軟在 2021 年 12 月沒收屬於 Flea 的域名。該公司沒收 42 個域名，稱其用於針對美國和其他 28 個國家的組織進行情報收集的行動。Flea 也與 Lookout 在 2022 年 11 月的一份報告中有關聯，該報告揭示該組織長期以來針對中國的維吾爾語網站和社交媒體的攻擊活動。

Flea 被認為是一個規模龐大且資源豐富的組織，而且似乎其活動的曝光，甚至像微軟所詳述的沒收行動，對於阻止該組織的活動並沒有產生顯著影響。

新的後門和值得注意的技術

Flea 使用新的後門顯示出，儘管該組織已經運作多年，但仍在積極開發新的工具。多年來，該組織開發多個自訂工具。Graphican 和已知的 Ketrican 後門之間功能的相似之處可能表明，該組織對被歸因於自己的活動並不太關心。

Graphican 本身最值得注意的是濫用 Microsoft Graph API 和 OneDrive 來獲取其 C&C 伺服器。值得注意的是，一個來自不同地區的與 Flea 無關的 APT 組織 Swallowtail 也使用類似的技術。一旦一個威脅行為者使用某種技術，我們通常會看到其他組織效仿，所以有趣的是看到這種技術是否會被其他 APT 組織和網路罪犯廣泛採用。

Flea 的目標--外交部門--也很有趣；儘管這些目標與該組織過去的活動目標一致。看起來，Flea 的興趣在近年來保持相似，即使它的工具和技術不斷演變。

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)

如果入侵指標 (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
SHA256 file hashes	
4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5	Backdoor.Graphican
a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8	Backdoor.Graphican
02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5	Backdoor.Graphican
617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd	Backdoor.Ketrican
858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253	Backdoor.Ketrican
fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476	Backdoor.Ketrican
177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf	Backdoor.Ketrican
8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b	Backdoor.Ketrican
f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286	Backdoor.Ketrican
865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48	Backdoor.Ketrican
d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30	Backdoor.Ketrican
bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64	EWSTEW
5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6	EWSTEW
f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d	EWSTEW
af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523	EWSTEW
548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc	EWSTEW
9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e	EWSTEW
18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051	Mimikatz
f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db	Mimikatz
df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f	Mimikatz
c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819	Pypykatz
7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d	Pypykatz
17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef	Pypykatz
b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222	Safetykatz

bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8	CVE-2020-1472
ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56	Lazagne
e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f	Pwdump
07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df	Pwdump
42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b	Pwdump
a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86	Pwdump
e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0	Pwdump
617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d	Pwdump
dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b	Pwdump
f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51	Pwdump
65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806	Hadmad
44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf	Hadmad
7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6	AntswordLoader
9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760	BehinderWebshell
f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663	BehinderWebshell
2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660	JSPWebshell
d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337	PHPWebshell
31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203	China Chopper
7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08	Sharpsecdump
2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8	Sharpsecdump
819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301	K8Tools
7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978	EHole

Network Indicators
172.104.244[.]187
50.116.3[.]164
www.beltsymd[.]org
www.cyclophilit[.]com
www.cyprus-villas[.]org
www.perusmartcity[.]com
www.verisims[.]com

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15
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。2023/6

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**。