Graph：利用 Microsoft API 的威脅數量正在增加

2024 年 5 月 2 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

Graph API 常被利用於對雲端上的指揮與控制伺服器的不顯眼通訊

越來越多的威脅開始利用 Microsoft Graph API，通常是為了便於與托管在 Microsoft 雲端服務上的指揮與控制 (C&C) 基礎設施進行通訊。

這種技術最近被用於針對對烏克蘭一個組織的攻擊，在這次攻擊中，一個以前從未記錄的惡意軟體利用 Graph API 將 Microsoft OneDrive 用於 C&C 目的。

BirdyClient

在烏克蘭發現的惡意軟體似乎被開發者命名為 BirdyClient 或 OneDriveBirdyClient，因為在其程式碼中發現對這兩個名稱的引用。它的檔案名稱--vxdiff.dll--與一個名為 Apoint (apoint.exe) 的應用程式相關的合法 DLL 相同，後者是 Alps 指向裝置的驅動軟體，通常用於筆記型電腦。該惡意軟體是偽裝成合法文件，還是被 Apoint 附帶，目前還不清楚。

對 BirdyClient 惡意軟體 (Trojan.BirdyClient) 的分析表明，它的主要功能是連接到 Microsoft Graph API，並使用 Microsoft OneDrive 作為 C&C 伺服器機制，用來上傳和下載檔案。該樣本也會建立以下日誌檔案：

%AllUsersProfile%/{0134AA2C-03BE-448D-8D28-7FFE94EA3A49}/config/001.temp

迄今為止，尚未發現任何相關工具。目前仍不清楚該威脅的開發者是誰以及他們的動機是什麼。

什麼是 Graph API ？

Graph 是 Microsoft API，旨在允許開發人員存取 Microsoft 雲端服務 (例如：Microsoft 365) 上託管的資源。使用 OAuth 存取權杖進行身份驗證。

Graph 可用於存取各種資料和服務，例如：電子郵件、日曆事件、檔案或裝置。應用程式開發人員可以使用它從一個或多個 Microsoft 服務中提取數據，並將其整合到自己的解決方案中。

率先使用

BirdyClient 是利用 Graph API 的最新威脅。第一個已知的用途是與北韓有聯繫的 Vedalia 間諜組織 (又稱 APT37) 開發 Bluelight，這是一種第二階的有效載荷，可以與多個不同的雲端服務進行通訊，以實現 C&C 目的。據發現 Bluelight 的 Volexity 稱，其分析的變種使用 Graph API 與 OneDrive 進行通訊。

2021 年 10 月，賽門鐵克發現 Harvester 組織，這是一個由國家支持的間諜行動，目標是南亞地區的組織。其工具集包括一個名為 Backdoor.Graphon 的自訂後門，該後門使用 Graph API 與微軟基礎架構通訊，以實現 C&C 目的。

2022 年 1 月，Graphite 惡意軟體被發現，該軟體使用 Graph API 與充當 C&C 伺服器的 OneDrive 帳戶通訊，進一步引起了公眾對該技術的關注。

Graphite 被部署在針對歐洲和亞洲多個政府的攻擊活動中。攻擊始於魚叉式網路釣魚郵件，這些郵件發送一個包含遠端程式碼執行漏洞 (CVE-2021-40444) 的 Excel 下載器。這導致第二階下載器的安裝，隨後是 Graphite 和次級有效載荷--PowerShell Empire。

這項活動最終被認定與俄羅斯Swallowtail間諜組織（又稱 APT28，Fancy Bear）有關。

更廣泛的採用

其他間諜組織似乎很快就從早期用戶那裡學到了經驗，並開始在其工具集中利用 Graph API。2022 年 12 月，Elastic Security 記錄了一起入侵東協成員國外交事務辦公室的事件。部署的工具包括 SiestaGraph，它使用 Graph API 與 OneDrive 和 Microsoft 365 Mail 進行溝通，以實現 C&C 目的。SiestaGraph 似乎還在持續開發中。2023 年 9 月，賽門鐵克發現該惡意軟體的新變種，其中包含的命令識別碼與原本記錄的不同。

2023 年 6 月，賽門鐵克發現了 Backdoor.Graphican，該軟體被Flea（又名 APT15、Nickel）進階持續性威脅（APT）組織使用，於主要針對美洲國家的外交部門開展間諜活動。

Graphican 是 Flea 組織的一套名為 Ketrican 的舊版本後門的進化版，而 Ketrican 本身則是基於先前的一個惡意軟體--BS2005，該惡意軟體也曾被 Flea 使用。Graphican 具有與 Ketrican 相同的功能，但其新功能包括使用 Microsoft Graph API 和 OneDrive 來取得其 C&C 基礎架構。

其他人也正在學習它被使用的方式。例如：滲透測試公司RedSiege 最近宣布開發 GraphStrike，這是一套與 Cobalt Strike 配合使用的工具集，可以讓 Cobalt Strike Beacon 有效載荷使用 Graph API 進行 HTTPS C&C 通訊。

對攻擊者的吸引力

攻擊者與 C&C 伺服器的通訊通常會引起目標組織的警覺。Graph API 之所以受到攻擊者的青睞，可能是因為他們認為，與已知實體 (例如：廣泛使用的雲端服務) 的通訊不太可能引起懷疑。除了看起來不顯眼之外，由於 OneDrive 等服務的基本帳戶是免費，因此對於攻擊者來說，這也是一種廉價且安全的基礎設施來源。

隨著人們對這項手法認識的加深，試圖利用 Graph 的攻擊者數量可能會進一步增加。

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。

afeaf8bd61f70fc51fbde7aa63f5d8ad96964f40b7d7fce1012a0b842c83273e－BirdyClient
5c430e2770b59cceba1f1587b34e686d586d2c8ba1908bb5d066a616466d2cc6－Bluelight
470cd1645d1da5566eef36c6e0b2a8ed510383657c4030180eb0083358813cd3－Graphon
f229a8eb6f5285a1762677c38175c71dead77768f6f5a6ebc320679068293231－Graphite
4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5－Graphican
a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8－Graphican
02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5－Graphican
1a87e1b41341ad042711faa0c601e7b238a47fa647c325f66b1c8c7b313c8bdf－SiestaGraph
fe8f99445ad139160a47b109a8f3291eef9c6a23b4869c48d341380d608ed4cb－SiestaGraph
7fc54a287c08cde70fe860f7c65ff71ade24dfeedafdfea62a8a6ee57cc91950－SiestaGraph

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/graph-api-threats
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。2024/5

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**。