前所未見的駭客組織：Grayling，鎖定多個台灣組織為攻擊目標

2023 年 10 月 10 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

攻擊行動的動機很可能是針對多個產業別、領域的情報收集

一個前所未見的進階持續性威脅 (APT) 駭客組織使用客製化的惡意軟體和多種可公開取得的駭客工具，對台灣製造業、IT 和生醫等相關產業與機構組織發動網路攻擊。

於太平洋的該島國的一個政府機構以及越南和美國的一些組織似乎也在這次活動中受到攻擊。這項活動從 2023 年 2 月開始，至少持續到 2023 年 5 月。

博通公司旗下的企業安全部門：賽門鐵克威脅獵手團隊將這項活動歸咎於一個內部稱為 Grayling 的新駭客組織。該活動非常顯眼的原因是由於 Grayling 使用獨特的 DLL 側載技術，並使用自訂解密器來部署有效籌載。這項活動的幕後動機似乎是情報收集。

攻擊方的活動

有跡象顯示，Grayling 可能會利用面向公眾的基礎設施的漏洞對受害者電腦發動初步存取攻擊。在 DLL 測載活動發生之前，有在一些受害者電腦上觀察到 Web shell 的部署。DLL 測載用於加載各種有效籌載，包括 Cobalt Strike、NetSpy 和 Havoc 框架。

攻擊者在獲得受害者電腦的初始存取權限後會採取各種行動，包括提權、網路掃描和使用下載器。

攻擊者使用攻擊策略、技術及程序 (Tactics, Techniques and Procedures，TTPs) 包括：

- **Havoc**：攻擊者在 2023 年初開始使用的開放原始碼漏洞命令列控制框架，似乎是 Cobalt Strike 和類似工具的替代品。Havoc 能夠執行各種活動，包括執行命令、管理執行緒、下載附加有效載荷、操縱 Windows 權杖和執行 shellcode。Havoc 還具有跨平臺的特點。
- **Cobalt Strike**：一種現成的工具，可用於執行命令、注入其他執行緒、提升當前執行緒或假冒其他執行緒，以及上傳和下載檔案。它表面上作為滲透測試工具有合法用途，但總是被惡意行為者利用。
- **NetSpy**：一種公開可用的間諜軟體工具。
- 對 **CVE-2019-0803** 漏洞的開採利用：當 Win32k 元件無法正確處理記憶體中的物件時，Windows 中存在權限提升漏洞。

- **Active Directory discovery**：用於查詢 AD 目錄並對應網路路徑。
- **Mimikatz**：公開可用的憑證傾印工具。
- **中止執行緒**。
- **下載程式**。
- 從 imfsb.ini 下載的**未知有效載荷**。

該活動的典型攻擊鏈似乎是通過匯出 API SbieDll_Hook 進行 DLL 側載。這將導致載入各種入侵工具，包含先是 Cobalt Strike Stager，進而下載 Cobalt Strike Beacon、Havoc 框架和 NetSpy。攻擊者還從 imfsb.ini 中載入並解密一個未知的有效籌載。在此過程中還使用 CVE-2019-0803 的漏洞利用工具組，同時還下載並執行 shellcode。

這些攻擊者隨後進行的入侵活動包括使用 kill 指令中止名為 processlist.txt 檔案中列出的所有執行緒，以及下載公開可用的憑證傾印工具 Mimikatz。

動機

雖然我們沒有看到有資料從受害者機器中外洩，但我們看到的活動和部署的工具都顯示，這種活動背後的動機是情報收集。受害者所處的行業--製造業、IT、生醫和政府機構--也是最有可能成為情報收集目標的行業，很顯然不是出於經濟的因素。

整合使用客製化技術與可公開取得的駭客工具是我們最近從 APT 組織中看到的典型活動，威脅者經常使用公開可取得或就地取材〈寄生攻擊〉的工具，嘗試繞過安全軟體，使他們的活動不被防禦機制偵測得到。Havoc 和 Cobalt Strike 等工具由於功能廣泛，也經常被攻擊者使用。對於老練的攻擊者來說，使用現成的此類工具往往比自己開發具有類似功能的客製化工具要容易得多。使用公開可取得的駭客工具也會使調查人員更難確定活動的來龍去脈。攻擊者所採取的手法，如中止執行緒等，也表明他們優先考慮的是隱藏活動歷程語軌跡。

我們尚無法明確地將 Grayling 與某一特定地域聯繫起來，但其行為特別大量針對臺灣的組織確實顯示，他們的源頭可能是對臺灣戰略利益有興趣的地域。

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／感染指標 (IOC:ndicators of Compromise)

如果 IOC 是惡意的並且我們可以取得該檔案，賽門鐵克端點解決方案將檢測並攔截阻止該檔案。

檔案類型指標

sha256 雜湊值：

da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9 - Havoc framework
79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17 - Downloader
bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec - Downloader
c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3 - Cobalt Strike Beacon
667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c - Exploit for CVE-2019-0803
87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8 - Downloader
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0 - Loader
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2 - Cobalt Strike Stager
d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c - NetSpy
4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba - DLL file
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739 - NetSpy
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b - Downloader
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9 - Downloader
23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae - Downloader
6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50 - Downloader
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581 - Downloader 12924d7371310c4
9b1a215019621597926ef3c0b4649352e032a884750fab746 - Windump
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f
c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e
245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa
4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9
e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3
f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31
971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f
f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0
c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5
af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889
1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce
7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f
30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6
74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87
752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea
6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721
7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2
a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe
de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c
1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91
ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf
1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9
dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548
d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29
b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba
6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068
3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b
5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

網路類型指標

網域

d3ktcnc1w6pd1f.cloudfront[.]net

IP位址

172.245.92[.]207
3.0.93[.]185

網址

http://45.148.120[.]23:91/version.dll
http://45.148.120[.]23:91/vmtools.exe

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/grayling-taiwan-cyber-attacks
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。2023/10

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**。