間諜團體重新將美國組織作為攻擊目標

2022 年 10 月 13 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

該團體最近的攻擊橫跨各大洲，包括近年來首次被確認針對美國的攻擊。

Budworm間諜組織在過去六個月裡對一些具有戰略意義的目標發動了攻擊，包括一個中東國家的政府、一家跨國電子製造商和一個美國州議會。後期的攻擊是賽門鐵克多年來第一次看到budworm病毒以美國實體為目標。除上述高價值目標外，該組織還對東南亞的一家醫院進行攻擊。

目前的工具集

在最近的攻擊中，Budworm利用Log4j漏洞（CVE-2021-44228和CVE-2021-45105）來破壞伺服器上的Apache Tomcat服務，以便安裝網路殼層。攻擊者使用代管在Vultr和Telstra的虛擬私人伺服器（VPS）作為命令和控制（C&C）伺服務器。

Budworm的主要有效載荷仍然是HyperBro惡意軟體系列，它經常使用一種被稱為動態連結檔（DLL）側面加載的技術。這涉及到攻擊者將一個惡意的DLL放置在一個預計會合法使用DLL的目錄中。然後，攻擊者執行合法的應用程式（自己安裝了它）。然後合法的應用程式執行並載入有效載荷。

在最近的攻擊中，Budworm使用端點權限管理軟體CyberArk Viewfinity來執行側面加載。該二進製檔案的預設檔名為vf_host.exe，通常會被攻擊者重新命名，以偽裝成一個看似更無害的檔案。偽裝的名稱包括securityhealthservice.exe、secu.exe、vfhost.exe、vxhost.exe、vx.exe和v.exe。

在某些情況下，HyperBro後門被加載其自己的HyperBro加載器（檔案名：peloader.exe，12.exe）。它被設計用來加載惡意的DLLs和加密有效載荷。雖然HyperBro被頻繁使用，但攻擊者有時也使用PlugX／Korplug木馬作為有效載荷。

最近的攻擊中使用的其他工具包括：

- Cobalt Strike：一種現成的工具，可用於在受害者機器上加載殼層的程式碼。它是合法的滲透測試工具軟體，但經常被惡意行為者利用。
- LaZagne：一個公開可用的憑證傾印工具。
- IOX：一個公開可用的代理和通訊埠轉發工具。
- Fast Reverse Proxy (FRP)：一個反向代理工具。
- Fscan：一個公開可用的內網掃描工具。

結論

Budworm以對高價值目標發動雄心勃勃的攻擊而聞名。雖然六到八年前經常有關於Budworm針對美國組織的報告，但在最近幾年，該組織的活動似乎主要集中在亞洲、中東和歐洲。然而，這是近幾個月來，Budworm第二次與針對美國目標的攻擊有關。最近CISA關於多個攻擊國防部門組織的APT團體的報告提到了Budworm的工具集。恢復對美國目標的攻擊可能意味著該組織的重點發生了變化。

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，且該檔可供我們比對，賽門鐵克端點產品將檢測並阻止該檔案。入侵指標 (IOC) 如下述：

5aecbb6c073b0cf1ad1c6803fa1bfaa6eca2ec4311e165f25d5f7f0b3fe001db — Credential Dumper

779ae012ede492b321fd86df70f7c9da94251440ebe5ec3efee84a432f432478 — FSCAN

ab949af896b6a6d986aed6096c36c4f323f650ccccfc7ea49004ba919d1bfa46 — HyperBro launcher

bebce37572ea2856663383215a013f8115c1f81da0f2bf1233c959955c494032 — HyperBro launcher

6e493ce8dccabf172d818453cc9d4e5bf4b1969ff9690c51b8cb538346e8e00e — HyperBro launcher

8b2e7924f5038473736705b5c3dc3efa918fb7ffe2cc19ce48e4554658d33fe6 — HyperBro launcher

cda8f76ce72759324e11c8af17736d685ca95954c0a09a682834b92a033bb11a — HyperBro launcher

25da610be6acecfd71bbe3a4e88c09f31ad07bdd252eb30feeef9debd9667c51 — HyperBro launcher

90eb92db757dc1ab4ca55b18b604350ecd84b7cd1d9a2555d789432f8c9a430b — HyperBro launcher

6398876f73cd0157a7681de4b2326a0a313dc7f9cb2bee3001894137da41c1f0 — HyperBro launcher

c53b6a2ec48647121a3e8816636b34ee2cdd6846d6d05efd9539d17a1c021da0 — HyperBro launcher

c3213937c194246d29dd5fb39d8e7ef3671df58e3f01353784a06a075f21cfc5 — HyperBro launcher

386c9079d65bdd7e3f7b8872024a80992b5d5c6a3c8b971c47d1ef439b9e2671 — HyperBro loader

bfffc43d948d1787622bcde524e51c932a2a1fdc761539f60e777e21ef16e83d — HyperBro loader

018d3a957aa0eaa7a621b52d15f4a1ed18b0f81c477e6023cd80313d83f7dbc0 — HyperBro loader

d4776939dcf78f5f7491b9938480423956ac10a3c576028dec307511c586a124 — HyperBro loader

27c2a9608ce80a443c87a0a2947864df7d4491cfa85608c6a6b6680ec0277f9d — HyperBro loader

42b603fffd4766fa22f6e10884e7fa43f449d515cfa20a18f0d07a6d4c370962 — IOX

0d46907320ab55d98966389f41441aa0341a7db829cd166748d8929d466c9fba — IOX

714d0101039bfd7d3db4dfe8307bc1657b7266ff2528b5e852b752879ebe7113 — IOX

0129c9c7b55a6f514a9fa8c38ce59d8939efda6ece67b90c6be13aec40f1bdab — Viewfinity side-load

df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 — Viewfinity side-load

620e401b2b7727a6c7ebc37ee1f7d8e1742d7121c1f4ea350a43d460ef9bdc4c — Viewfinity side-load

c8aea84abb476ab536198a36df53b37be3d987a9ce58cb06e93cac7d2bfb3703 — Viewfinity side-load

233bb85dbeba6923153340850169769 5a66b7790e751925231d64bddf80bbf91 — Cobalt Strike

d610547c718fcca7c5c7e02c6821e9909333daf6376a1096edf21f9355754f29 — FRP

5c2d05bfc9b6d4fc7aea32312c62180564fac9f65b0867e824d81051e5fc34fd — Korplug

ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56 — Lazagne

61deb3a206cc203252418b431f6556e3f7efd9556fc685eeda7281d9baf89851 — Lazagne

892663bb4f3080c3f2f1915734897cab1c9ee955a77bb8541b417ec2b03cd4ef — Lazagne

3d7dc77ded4022a92a32db9e10dbc67fbcc80854a281c3cc0f00b6cbd2bfd112 — Trojan Horse

48e81b1c5cc0005cc58b99cefe1b6087c841e952bb06db5a5a6441e92e40bed6 — Trojan.Dropper

5cba27d29c89caf0c8a8d28b42a8f977f86c92c803d1e2c7386d60c0d8641285 — Trojan.Dropper

139.180.146[.]101 — C&C VPS

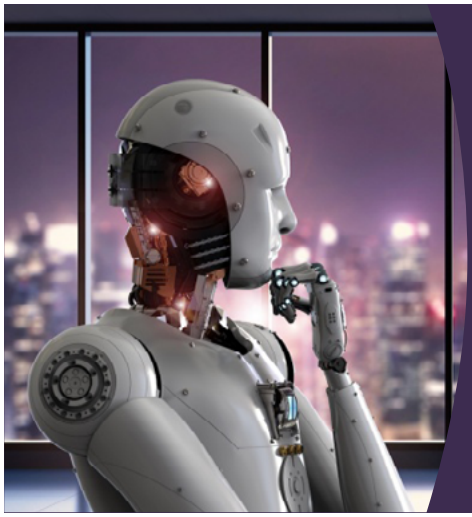
45.77.46[.]54 — C&C VPS

139.168.200[.].123 — C&C VPS

207.148.76[.]235 — C&C VPS

setting.101888gg[.]com/jquery-3.3.1.min.js — C&C

207.148.76[.]235/jquery-3.3.1.min.js — C&C



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/budworm-espionage-us-state
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。2022/10

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)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588