Carderbee APT 集團針對香港機構發動濫用合法軟體的供應鏈攻擊

2023 年 8 月 22 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

這不是 Cobra DocGuard 軟體被網路駭客開採利用發動供應鏈攻擊的首例

一個前所未見的進階持續性滲透攻擊 (APT) 駭客集團利用合法的 Cobra DocGuard (檔案加解密) 軟體發動供應鏈攻擊，目的是將 Korplug 後門程式 (又名 PlugX) 部署到受害者的電腦上。

在這次攻擊中，攻擊者使用帶有合法 Microsoft 憑證的惡意軟體。該行動中的大多數受害者都位於香港，另有一些受害者位於亞洲其他地區。

已知有多個 APT 駭客集團使用這個 Korplug 後門程式，但我們無法將此活動與已知的網路駭客關聯起來，因此我們為此這次攻擊的幕後黑手取了一個新名字--Carderbee。

Cobra DocGuard (檔案加解密) 軟體和先前的活動

Cobra DocGuard Client 是由中國的 EsafeNet 公司所設計生產的軟體，是用於保護、加密和解密檔案的資安軟體。EsafeNet 是中國資安公司：NSFOCUS 轄下的公司。

根據資安公司 ESET 的一份報告中，在 2022 年 9 月，該軟體 (Cobra DocGuard) 的一個「被動過手腳的更新程式」被用來入侵香港的一家博弈公司。同一家公司在 2021 年 9 月也曾遭 Budworm (又名 LuckyMouse，APT27) 採用相同的伎倆入侵，這使 ESET 將 2022 年 9 月的攻擊也歸因於 Budworm。在那次攻擊中，還發現 Korplug 惡意軟體的新變種。當時，它使用耐人尋味的表頭『ESET』，表明它可能已被修改過以試圖繞過 ESET 資安產品的偵測。

Broadcom 旗下的企業安全部門～Symantec 威脅獵手團隊調查的活動中也發現帶有 Korplug 簽署的版本被使用。該活動始於 2023 年 4 月。然而，我們並未發現任何其他證據表明這次攻擊是由 Budworm 所進行。Korplug 後門，已知被多個 APT 駭客集團利用過，包括 APT41 和 Budworm。我們沒有任何關於最近活動中受攻擊目標公司所屬行業別的標示，只有它們的地理位置。

因此，無法確定地將此活動與已知的駭客集團關聯起來，這也就是為什麼我們將其歸因於一個全新駭客集團：Carderbee。

攻擊鏈

在受影響的組織中，大約有 100 台電腦出現惡意活動；然而，安裝 Cobra DocGuard 軟體的電腦大約有 2,000 台，這凸顯攻擊者可能會選擇性地將有效籌載派送給特定的受害者。

惡意軟體被派送到遭入侵電腦的以下位置，這表明攻擊者是透過供應鏈攻擊或與 Cobra DocGuard 的惡意組態有關的方式入侵目標電腦：

"csidl_system_drive\program files\safenet\cobra docguard client\update"

在 2023 年的前幾個月內，觀察到多個不同的惡意軟體家族採用這種方法被部署。在一個有趣的案例中，攻擊者部署的下載程式具有來自 Microsoft 的數位簽章憑證，名稱是 Microsoft Windows Hardware Compatibility Publisher。這個下載器被用來在目標系統上安裝 Korplug 後門。下載器嘗試從以下位置下載名為 *http://cdn.stream-amazon[.]com/update.zip*。

update.zip 是一個 zlib 格式的壓縮檔。它解壓並執行一個名為 content.dll 的檔案。該檔案不會保存在磁碟上。它是惡意植入程式，包含 x64 和 x86 的驅動程式，這些驅動程式會根據系統環境的不同而被植入。驅動程式會建立服務和登錄表項目。被植入的驅動程式從登錄表中讀取加密資料，解密後將其注入 svchost.exe。注入的有效籌載就是 Korplug 後門。

從被下載的 Korplug 樣本中發現它能夠：

- 採用命令提示字元 (cmd) 執行命令
- 列舉檔案
- 檢查執行中的處理程序
- 下載檔案
- 開啟防火牆通訊埠
- 充當鍵盤側錄器

Microsoft 憑證濫用

使用 Microsoft 數位簽章的惡意軟體是一個已知問題。2022 年 12 月，Mandiant 發現一個使用 Microsoft Windows 硬體相容性授權碼憑證的 POORTRY 驅動程式樣本。最近，在 2023 年 7 月，趨勢科技公司表示發現一個使用 Microsoft 簽章的 rootkit，該 rootkit 似乎通過 Windows Hardware Quality Labs(WHQL) 測試簽章計畫獲得有效的簽章。微軟承認這一問題，並表示微軟的 Windows Hardware Developer Program(MWHDP) 計畫所認證的硬體驅動程式正被惡意用於後期滲透攻擊活動。

趨勢科技表示已對該問題進行調查，『確定該活動僅限於濫用幾個開發者計畫帳戶，沒有發現微軟帳戶洩露的情況』。使用看似合法憑證簽章的惡意軟體，會使安全防護軟體更難檢測到。

供應鏈攻擊和憑證濫用

很明顯，這一活動背後的攻擊者都是有耐心且技術嫻熟的行動者。他們利用供應鏈攻擊和具有簽章的惡意軟體來進行他們的活動，試圖掩人耳目。他們似乎只在獲得存取權限的少數電

腦上部署有效籌載，這一事實也顯示幕後攻擊者進行了相當程度的策劃和偵察。軟體供應鏈攻擊仍然是所有行業組織面臨的主要問題，在過去 12 個月中發生多起備受矚目的供應鏈攻擊事件，包括 MOVEit、X_Trader 和 3CX 攻擊事件。

關於 Carderbee 的活動仍存在一些未解之謎，例如：該集團的活動目標是哪些行業，以及 Carderbee 與 Budworm 等其他集團之間是否存有任何關係。

賽門鐵克研究人員將繼續跟蹤這一活動，並在下文中分享入侵指標，以便我們的資安社群同好也能這樣做。

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。

SHA256 file hashes:

96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622
19a6a404605be964ab87905d59402e2890460709a1d9038c66b3fbeedc1a2343
1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d
2400d8e66c652f4f8a13c99a5ffb67cb5c0510144b30e93122b1809b58614936
2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4
47b660bbaacb2a602640b5e2c589a3adc620a0bfc9f0ecfb8d813a803d7b75e2
5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7
7e6d0f14302662f52e4379eb5b69a3749d8597e8f61266aeda74611258972a3d
85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af
8bd40da84c8fa5f6f8e058ae7e36e1023aca1b9a9c8379704934a077080da76f
8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f
9e96f70ce312f2638a99cfbd3820e85798c0103c7dc06fe0182523e3bf1e2805
9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c
b5159f8ae16deda7aa5d55100a0eac6e5dacd1f6502689b543513a742353d1ea
b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510
b84f68ab098ce43f9cb363d0a20a2267e7130078d3d2d8408bfb32bbca95ca37
f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97

Remote IP addresses:

45.76.179[.]209

104.238.151[.]104

URLs:

http://111.231.100[.]228:8888/CDGServer3/UpgradeService2

http://103.151.28[.]11:8090/CDGServer3/UpgradeService2

Domains:

cdn.stream-amazon[.]com

cdn.ofo[.]ac

gobay[.]info

tjj.active-microsoft[.]com

githubassets.akamaixed[.]net

ms-g9-sites-prod-cdn.akamaixed[.]net

ms-f7-sites-prod-cdn.akamaixed[.]net

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/carderbee-software-supply-chain-certificate-abuse
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。2023/8

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**。