保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

應對GitHub屢遭惡意濫用 --賽門鐵克的防護機制

2024 年 8 月 6 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

隨著世界變得越來越數位化，科技也變得更令人興奮和方便。軟體開發人員可以使用大量的線上工具來增進他們的技能、管理他們的程式碼以及形塑他們的想法。其中最受歡迎的應用程式之一是 **Git**，這是一套開放原始碼的版本控制軟體，可讓多位開發人員同時對各自的專案進行修改。開發人員也可以使用 **GitHub**，這是一個網頁型應用程式，可讓開發人員輕鬆地與其他開發人員分享檔案和進行協作。但不幸的是，這種便利性也有缺點。越來越多威脅份子濫用 GitHub 服務來寄生和散播垃圾郵件與惡意軟體。到目前為止，我們的防護公報中提到 GitHub 寄存或協助散播惡意軟體不下 44 次。平心而論，這類濫用絕非 GitHub 所獨有，但同樣令人擔心。

以下是一些濫用 GitHub 發動的攻擊鏈、惡意軟體原始碼/廣告、駭客工具，以及軟體和硬體漏洞的方式：

- **惡意軟體原始碼**：攻擊者可以在 GitHub 上傳並分享惡意軟體的原始碼，讓其他人可以存取，並將其用於惡意目的或進行修改。
- **惡意軟體散佈**：GitHub 儲存庫可用來寄存惡意檔案或腳本，然後透過網路釣魚電子郵件或其他方式散佈給受害者。
- **指揮與控制 (C&C)**：某些進階惡意軟體使用 GitHub 作為指揮與控制的平台，將與受感染機器的通訊隱藏在看似良性的資源庫活動中。
- **惡意軟體廣告**：GitHub 可以用來宣傳或展示惡意軟體的功能，將惡意軟體出售或與其他惡意行為者分享。
- **漏洞開採濫用**：GitHub 上公開分享的程式碼可能包含漏洞。攻擊者可以搜尋這些弱點，並利用它們進行廣泛的攻擊。
- **網路釣魚行動**：攻擊者可利用 GitHub 是知名且廣受信任的平台，在網路釣魚電子郵件中使用 GitHub 網頁，使其看起來像是合法的。

在本公告中，我們將介紹這些威脅所濫用的兩種常見攻擊媒介。

主題 1 攻擊媒介：惡意網頁

電子郵件被偽裝成政府組織的稅務相關通知，例如：美國國稅局 (Internal Revenue Service；縮寫 IRS) 和英國稅務海關總署 (His Majesty's Revenue and Customs，HMRC) 。

電子郵件本文要求收件人檢閱稅務相關文件，並在需要採取行動時作出回應。它們通常遵循以下模式：

- 電子郵件以正式的語氣撰寫，並在郵件內容中插入惡意的 GitHub 專案 (Project) 網頁。由於 GitHub 專案儲存庫頁面上的壓縮檔受密碼保護，因此電子郵件中也會提供簡短的密碼或 PIN。
- 點擊該網址會下載檔案，收件者會被提示輸入電子郵件內容中提供的密碼。加入這一步驟是為了向收件者保證一切都是合法的，沒有任何可疑的地方需要擔心。
- 在擷取壓縮檔內容之後，有效負載會有 .bat 到 .exe 不同的副檔名，以啟動一連串的事件，導致惡意感染和敏感資料的潛在損失。

攻擊鏈

- 電子郵件包含 github.com 專案內的網頁和密碼 → 重導向至專案頁面並包含密碼保護的壓縮檔 → DLL → .exe → 最終有效酬載

惡意網頁結構範例：

- hxxps[:]//github[.]com/[user_project]/[repo_name]/files/[file_id]/2023[.]COMPLETE[.]TAX[.]ORGANIZER[.]pdf[.]zip

圖 1：內嵌 GitHub 專案儲存庫網址的電子郵件預覽

主題 2 攻擊媒介與手法： 附件

電子郵件被偽裝成有關法律團隊發出西班牙文的訴訟相關通知。

- 電子郵件本文部分的內容非常簡潔，使用正式的語氣和簡短的密碼，並有一個假冒的「.svg」檔案。
- 電子郵件收件人會被引誘下載「.pdf.svg」或「.docx.svg」副檔名檔案，其中包含內嵌的 github.com 專案儲存庫網址。
- github.com 專案儲存庫網址會為收件者提供受密碼保護的壓縮檔。
- 使用電子郵件中提供的密碼擷取出檔案後，有效籌載會有從 .bat 到 .exe 等各種副檔名，準備啟動一連串事件，導致惡意感染和敏感資料的潛在損失。

攻擊鏈

- 電子郵件包含附加的 .svg 檔案和密碼 → 重導向至 github.com 專案頁面，其中包含密碼保護的壓縮檔 → DLL → .exe → 最終有效酬載

圖 2：附有「.pdf.svg」副檔名檔案的電子郵件預覽

此類型的惡意垃圾郵件攻擊行動可能特別針對特定的電子郵件使用者群組，也可能針對較大的非目標群組，視攻擊行動特定目標而定。最終有效酬載各不相同，包括許多惡名昭章的威脅，例如：Remcos、AsyncRAT 和 Agent Tesla。

賽門鐵克防護機制

賽門鐵克的**郵件安全雲端服務 (Cloud Email Security Service) 和郵件安全閘道 (虛擬) 硬體裝置(Messaging Gateway)** 可發揮封鎖作用，這都歸功於一整套完整的先進技術，專門用於保護組織免受此類威脅。

- **反垃圾郵件過濾系統**：頻率近乎即時的各種網頁屬性的資料庫更新、檔案附件和其他電子郵件功能的系統，以跟上快速演進的電子郵件威脅環境變化。
- **模擬器和啟發式特徵**：我們的解決方案採用先進的模擬器和啟發式特徵碼來識別隱藏在電子郵件中的惡意元素。透過模擬程式碼執行和分析行為模式，我們可以在潛在威脅對組織造成影響之前，先行偵測並解除威脅。
- **透過 WebPulse 技術建立網頁信譽**：以雲端為基礎的架構，專以利用使用者導向行為的力量，並將使用者的回報轉換為全球網路情報和網路威脅情報。
- **連結追蹤**：賽門鐵克的專利技術，可掃描超連結，以判斷它們是否被用於垃圾郵件、網路釣魚或惡意目的。持續進行更新，以更好地識別 GitHub 儲存庫和網頁中的濫用情況。
- **賽門鐵克資料外洩防護(Data Loss Prevention)**：透過與我們的電子郵件安全解決方案無縫整合，協助對抗資料竊取情況。

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲深入瞭解鐵克資料外洩防護 (DLP) 的更多訊息，請點擊此處。
可以透過以下網址回報垃圾郵件、惡意軟體或濫用 GitHub 服務：
https://docs.github.com/en/communities/maintaining-your-safety-on-github/reporting-abuse-or-spam

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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。
保安資訊連絡電話：**0800-381-500**。