Pegasus(又稱飛馬、天馬)間諜軟體風雲再起

2021 年 9 月23 日發布｜威脅情報

凱文・沃特金斯
安全研究員

賽門鐵克解決方案可幫助偵測、過濾和阻止威脅

最近的 iOS 14.8 更新修復了一個影響每個 iOS 行動裝置的漏洞的零時差、零點擊漏洞。這個被稱為 FORCEDENTRY (CVE-2021-30860) 的漏洞存在於 Apple 的 iMessage 中，根據公民實驗室的一份報告，它被利用來將 NSO Group 的 Pegasus 間諜軟體推送到 iOS 行動裝置，時間可以追溯到 2021 年 2 月。

Pegasus 商品化間諜軟體，已經問世好多年了，但最近在公民實驗室和國際特赦組織相繼揭露關於該間諜軟體針對記者、活動人士和其他人的報導後，重新成為人們關注的焦點。

FORCEDENTRY 的主要問題之一是它可以用於所謂的**「零點擊」攻擊**，這意味著**用戶不需點擊連結或打開文件就會讓手機／平板被感染**。利用該漏洞的攻擊者只需要該裝置的 Apple ID 就可以無聲無息地破壞它。

這篇部落格文章將介紹目前已知的 Pegasus 威脅、它有多普遍以及賽門鐵克（目前為博通公司--Broadcom 美國股市代碼：AVGO 的企業安全部門）如何保護其客戶免受間諜軟體的侵害。

飛馬威脅

Pegasus 由以色列網路武器公司 NSO Group 所開發，是一種複雜且難以捉摸的行動間諜軟體，迄今已存在多年。Pegasus 能夠閱讀訊息、跟踪通話、跟踪裝置位置、收集密碼以及存取目標裝置的麥克風和相機/視訊鏡頭。

據 NSO Group 稱，Pegasus 被出售給民族國家和執法部門，以幫助打擊犯罪和恐怖主義，並維護公共安全。儘管有此聲明，這個多年來引人注目的軟體遭濫用，賽門鐵克長期以來一直有能力對其進行檢測。

最近的一份報告揭露了利用 Apple iMessage 服務中的漏洞來安裝 Pegasus 的攻擊。攻擊只需要 Apple ID（電子郵件或電話號碼）即可感染目標行動裝置。

攻擊籌載使用對用戶「隱藏」的 iMessage 欄位；事實上，如果 iMessage 文字欄位是空白，則根本不會顯示任何警報或通知。這種類型的 iMessage 零點擊攻擊可以追溯到 iOS 11 和 Google Project Zero 團隊所做的研究。

酬載利用 iMessage 框架中的漏洞，例如：利用發送惡意的 PDF 來呼叫 PDF 處理器以執行駭客所預藏的任意代碼（在 iOS 14.8 更新中已修復）。此外，攻擊執行完全在 iMessage 框架的沙箱程序內進行，並在裝置重啟時被清除。

威脅有多普遍？

只能說，評估 Pegasus 威脅的範圍非常具有挑戰性。FORCEDENTRY 攻擊留下的最好線索是它在嘗試下載 Pegasus 間諜軟體框架文件時所生成的 Web 流量。

國際特赦組織的報告列出了已知的 Pegasus 感染的網址(URL)。我們的Symantec Endpoint Protection Mobile--賽門鐵克端點防護行動裝置版本，幕後所使用的 WebPulse 網頁分類與安全技術平台，已包含相關的情資資料庫，可以以識別和阻止可疑的網頁流量。我們發現近 150,000 台 iOS 裝置中就有 1 台試圖存取已知的 Pegasus 所感染的網頁。雖然這個數字可能看起來很低，但這只是攻擊狙殺鏈的一冰山一角。

無論如何，賽門鐵克的 WebPulse 網頁分類與安全技術平台，總也能在第一時間識別潛在風險或惡意網頁，並能阻止任何階段的攻擊進而制敵機先、瓦解攻擊狙殺鏈， 即使它包含零日漏洞和「零點擊」攻擊--也無所遁形。

賽門鐵克如何解決問題？

Symantec Endpoint Protection Mobile--賽門鐵克端點防護行動裝置版本，分析簡訊內容中所包含的鏈接，通過針對 Symantec WebPulse（賽門鐵克全球情報網路的一部分）中的威脅情報檢查網頁鏈結（甚至可能對用戶隱藏的 URL）來保護用戶免受攻擊。

Symantec Endpoint Protection Mobile--賽門鐵克端點防護行動裝置版本，提供針對網路內容威脅的保護、過濾和阻止與 Pegasus 活動中使用的已知命令和控制服務器的通信（相同的 WebPulse 全局 URL 情報訊息嵌入在我們的 Windows 和 Mac Symantec Endpoint Protection 代理中）。它還可以識別和保護易受攻擊的 iOS 和 Android 裝置。有關覆蓋範圍的更多詳細訊息，請參閱賽門鐵克安全中心的 Pegasus 間諜軟體防護公告。

FORCEDENTRY 修補程式適用於 macOS、iOS、iPadOS 和 watchOS，建議使用者盡快更新這些修補程式。

結論

Apple 通過其 iOS 14.8 更新修補迅速解決了 FORCEDENTRY 漏洞。然而，隨著 iMessage 框架越來越成為威脅追踪者鎖定的目標，我們預期會有更多修補會被釋出。我們還預期針對 iOS 裝置的攻擊數量將遵循 Pegasus 使用的類似攻擊模式。不幸的是，由於對攻擊有效籌載和殺傷鏈的的瞭解非常有限，攻擊者知道他們可以輕鬆逃避檢測。

所有這些都凸顯了將行動端點保護作為多層次網路防禦政策的一部分，以防止針對行動裝置的已知和未知（零日）攻擊的重要性。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/pegasus-forcedentry-protection

關於作者

凱文 • 沃特金斯

安全研究員

凱文 是賽門鐵克現代作業系統安全 (MOS) 部門的一名安全研究員。他一直在研究創新的新技術來自動發現會衝擊行動用戶的威脅。

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