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

DarkGate惡意程式已轉向濫用PDF附件檔

2023 年 10 月 31 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

我們在今年 8 月發布有關 DarkGate 惡意程式的最新資訊，這是一種基於 Windows 的惡意軟體，具有廣泛的功能，兼具竊密惡意程式和遠端存取木馬的功能，透過惡意廣告和購買搜尋引擎廣告排名 (SEO) 進行傳播，上個月被稱為 TA577 的駭客組織，同時也是前 Qakbot 的聯盟夥伴公司被發現透過其惡意電子郵件行動傳播 DarkGate，深入拆解其攻擊鏈發現其是複雜精密的工具與手法的組合。

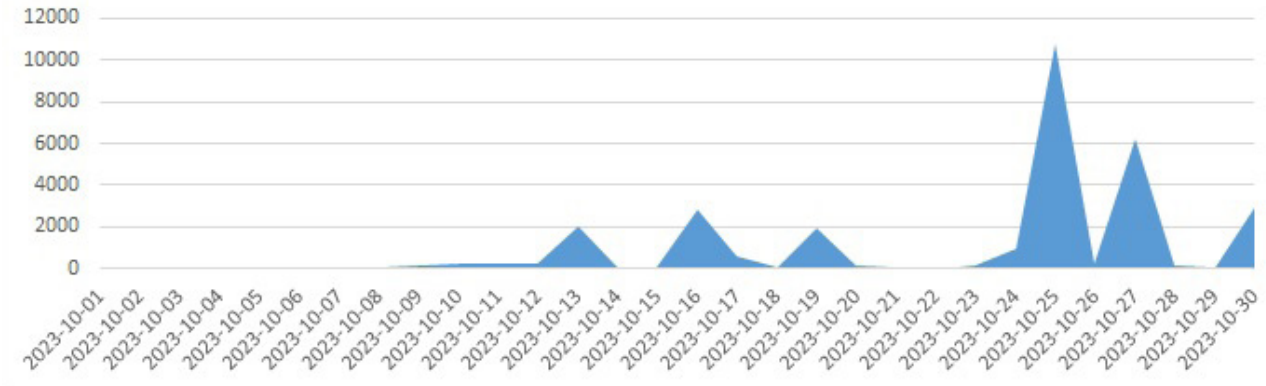
最近，DarkGate 已轉向濫用 PDF 附件檔。在某些情況下，檔案名稱僅包含一兩個字母長度，以及在檔案內容中掃描的惡意連結。在這些情況下，該連結會下載一個 ZIP 壓縮檔，其內容包含惡意 VBS 或 MSI 檔案，第二階段的有效籌載是包含實際 DarkGate 惡意軟體程式碼的 AutoIT 腳本。

也觀察到第三種與 PDF 相關的感染事件。透過這些附加的 PDF 檔案內 (大多數檔名較長) 的連結會下載一個網頁 (URL) 捷徑，該捷徑連接到攻擊者控制的 WebDav 伺服器，以便執行惡意 VBS、JS 或 MSI 檔案。

- PDF > URL > .URL 捷徑 > MSI/JS/VBS > AutoIT > DarkGate

我們的情資大數據遙測系統報告，這項最新攻擊行動於 10 月 13 日正式開始，並在 10 月 25 日出現高峰，隨後在 10 月 27 日出現較少的回報。

賽門鐵克攔截到 DarkGate 的時序分析表



賽門鐵克已經於第一時間提供多種有效保護**(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**。以下說明為 Symantec 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen1
- Scr.DLHeur!gen6
- Scr.DLHeur!gen7
- Trojan.DLHeur!gen5

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
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。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。

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**。