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

有效抵禦複雜攻擊鏈的威脅情資 --STARGate(*星際之門)

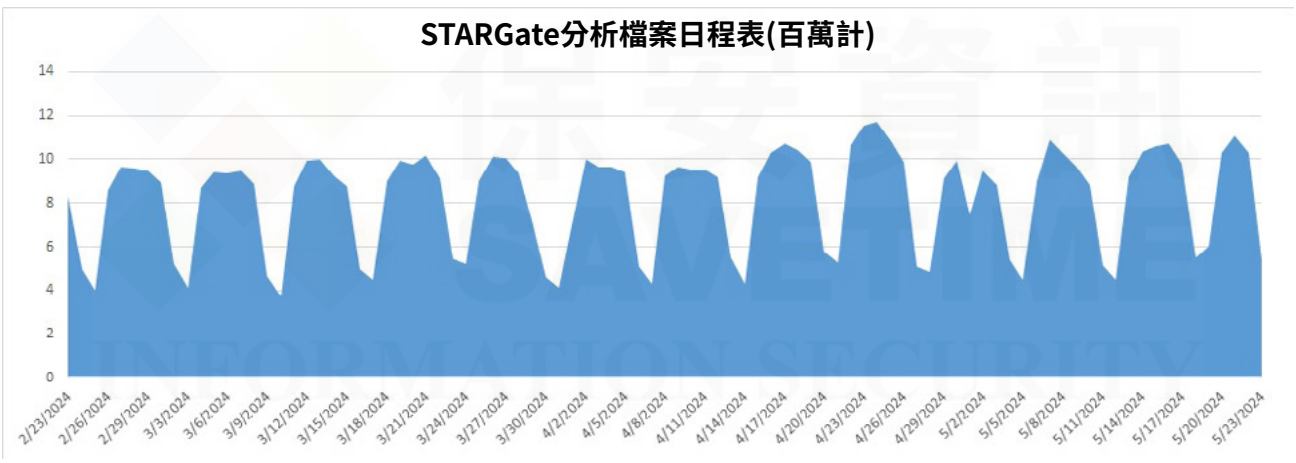
2024 年 5 月 28 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

攻擊者不斷尋找新穎且創新的方法，透過混淆和複雜的多重步驟攻擊鏈來規避安全解決方案。採用多層式的安全方法、跨技術分享事件脈絡、對抗不斷演變的威脅態勢，是積極保護我們的客戶的關鍵。

STARGate

STARGate 提供可根據威脅情況隨時擴充並改變遊戲規則的安全性，它是一種先進的網路防禦平臺，涵蓋廣泛的賽門鐵克企業安全產品，能夠在超過 100 億個檔案中，對靜態內容進行威脅檢測和分析。

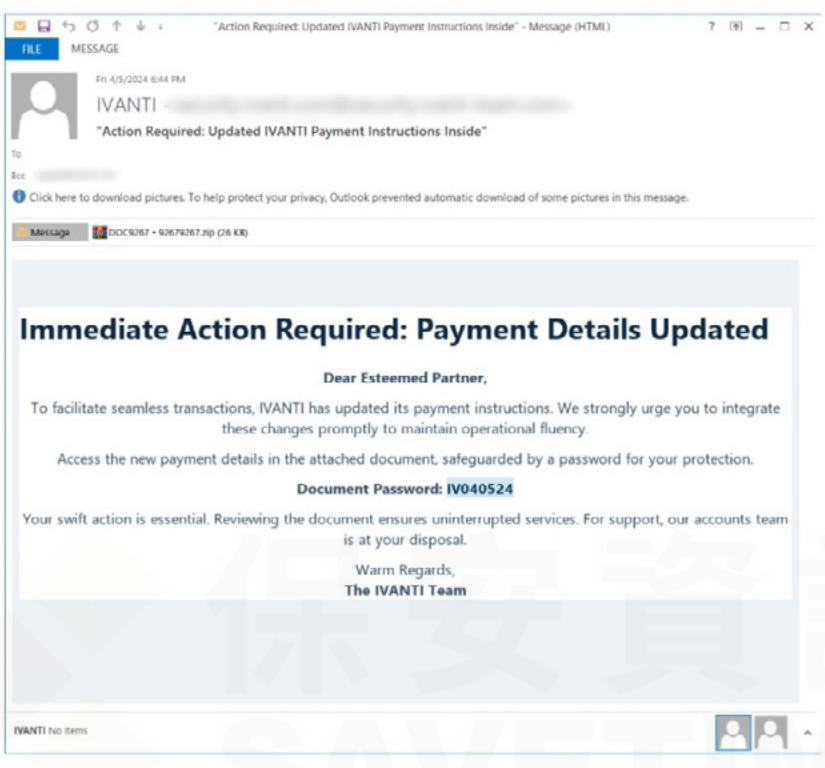


STARGate 利用其先進的技術能量和資料追踪狀態模型，將攻擊鏈各層次的資訊關聯起來。這樣，它就能破解規避技術，識別惡意軟體的意圖，並阻止以下威脅：

- 透過進階機器學習識別可被利用的零時差威脅
- 透過賽門鐵克全球威脅情資網路 (GIN) 發現帶有惡意嵌入網址的可疑檔案
- 使用關聯性的機器學習，發現前所未見的 PE、MSI 和 Android 應用程式 (APK) 攻擊
- 嵌入式命令列中編碼的漏洞，例如：『就地取材』攻擊
- 利用複雜啟發式演算法的情境式威脅
- 使用 VBA 巨集 (例如：AveMaria)、Javascript (例如：Avaddon) 或 VBS (例如：Guloader) 的腳本攻擊
- 混淆惡意軟體的 x86 自訂打包程式 (例如：Lokibot)
- 漏洞利用 (例如：CVE-2017-0199 和 CVE-2017-1182) 的格式錯誤、混淆的 RTF 威脅
- 使用光學字元辨識 (OCR) 和 QRCode 混淆的攻擊

TA547 垃圾郵件攻擊行動

受益於 STARGate 的跨技術分享事件脈絡的運作，有效阻止最近 TA547 垃圾郵件行動的成效是有目共睹。4 月份，一個名為 TA547 垃圾郵件行動透過以下攻擊鏈的變種，針對德國機構發送 Rhadamanthys 惡意竊密程式。向目標群組織發送包含受密碼保護的 ZIP 附件電子郵件。收件者在解壓縮該附件檔會發現一個連結檔。點擊該連結後會下載一個 PowerShell 腳本，該腳本會提供 Rhadamanthys 惡意竊密程式的可執行檔。



PowerShell 腳本似乎是由 LLM (大型語言模型) 生成的：

STARGate 透過關聯分析、交叉比對各層級攻擊鏈的資訊來阻止攻擊。這種跨技術分享事件脈絡，使 STARGate 能夠成功提取加密的 ZIP 附件和電子郵件正文中的嵌入密碼。STARGate 利用其命令列啟發式技術，能夠識別 ZIP 中 LNK 檔的惡意意圖，將其檢測為 CL.Downloader!gen1。此外，在攻擊鏈的變種中，STARGate 將包含由 PowerShell 程式碼載入 Rhadamanthys 惡意竊密程式的 .EXE ，被賽門鐵克進階機器學習檢測為 Heur.AdvML.B。

受益於賽門鐵克持續在人工智慧、模擬和威脅研究方面的不斷創新，STARGate 防護能力領先業界、與時俱進，以下的解決方案也同時受惠於 STARGate 的安全運作機制：

- Email Security Service
- Symantec Messaging Gateway
- Content Analysis Security
- Symantec Web Protection
- Advanced Secure Gateway
- CloudSOC
- Symantec Web Isolation
- Security Analytics
- Symantec Protection Engine for NAS Storage
- Symantec Protection for Sharepoint Services
- Cloud Workload Protection Storage
- Symantec Mail Security for Microsoft Exchange
- Cynic Sandboxing
- Link Following
- Data Center Security Server
- Industrial Control System Protection

欲深入了解更多有關賽門鐵克 STARGate 引擎的詳細資訊，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**。