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

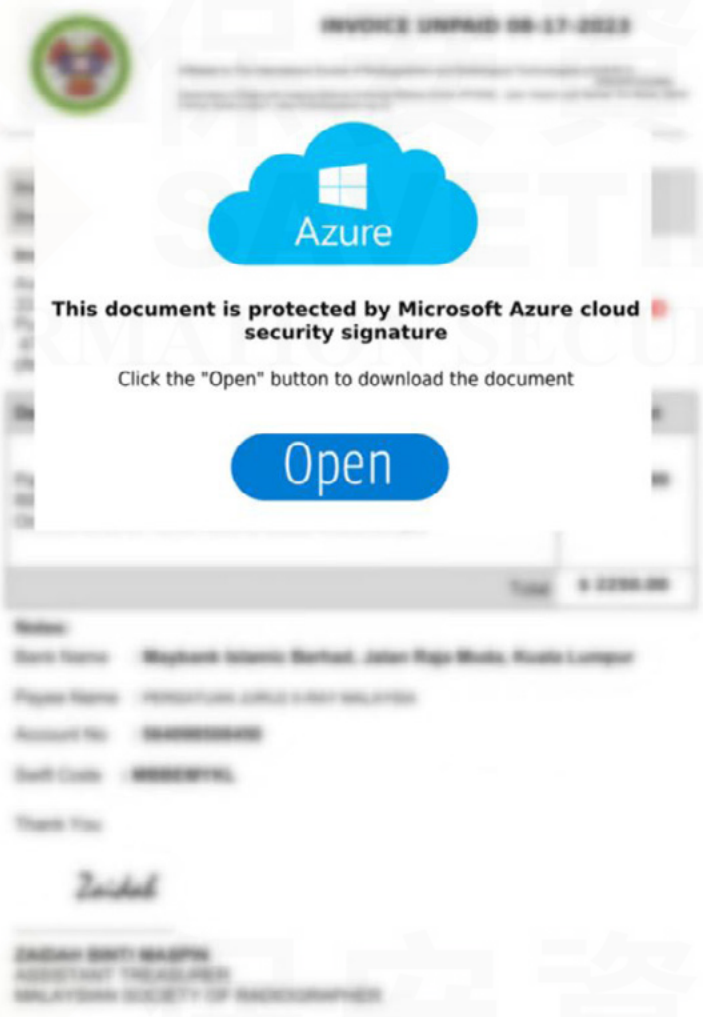
7月和8月的IcedID惡意攻擊行動

2023 年 8 月 29 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

IcedID（也稱為Bokbot）是一種眾所周知的模組化銀行金融木馬惡意軟體，最初出現在 2017 年左右的威脅環境中。它與時俱進並不斷發展，如今更常被用作其他惡意模組和有效負載（包括勒索軟體）的載入器。IcedID 透過魚叉式網路釣魚行動廣泛散布。過去，它還經常在其他惡意軟體 (例如：Emotet) 的攻擊鏈中散布附帶負載。

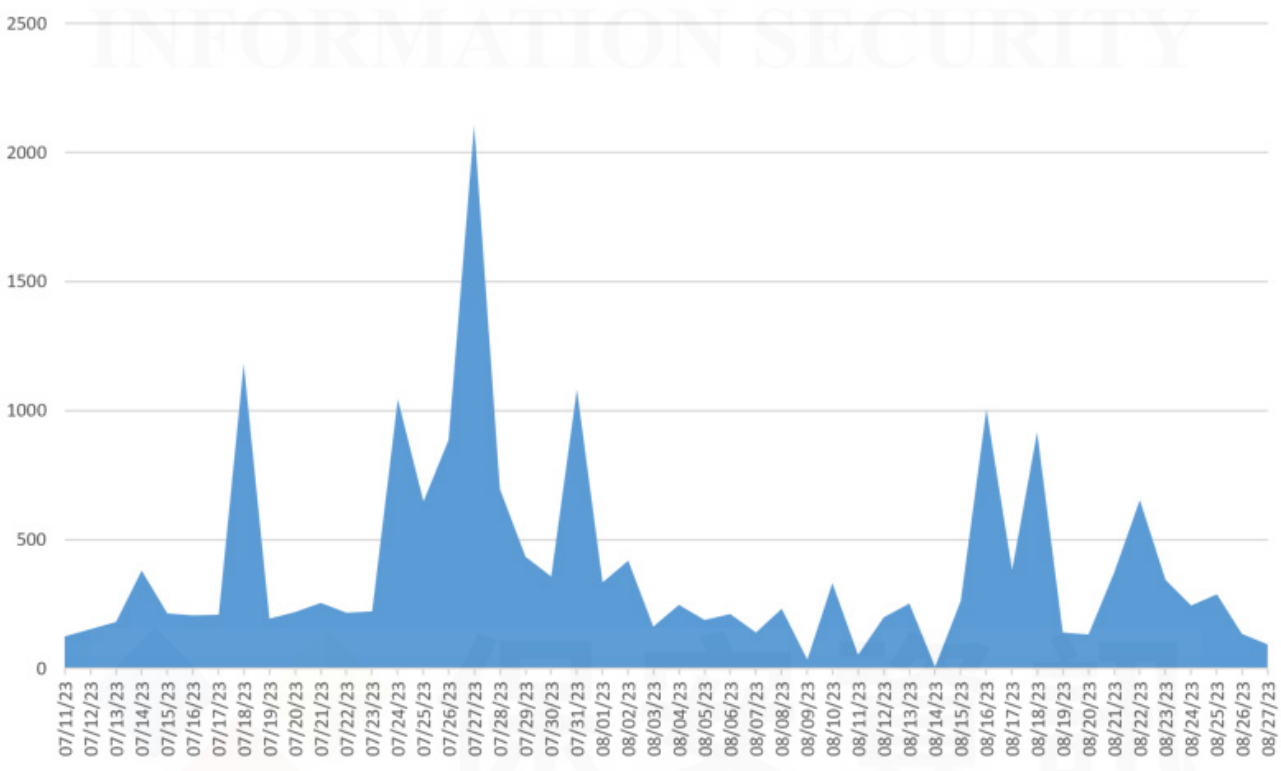
賽門鐵克觀察到，由於惡意垃圾郵件活動依舊節節攀升，7 月和 8 月 IcedID 相關活動也明顯增加。8 月份的最新攻擊樣貌以多階段的攻擊鏈為主，其中涉及由惡意垃圾郵件傳遞的檔名，例如：『Doc_Scan_08_18』或『Document_08_22』的 PDF 檔。惡意 PDF 檔聲稱已經過安全軟體檢查的發票檔案，誘騙受害者放下戒心直接點擊『下載』或『打開』按鈕來下載所需的檔案，如下圖所示：



單擊該鏈接後，受害者會被重定向到包含惡意 JavaScript 的網址，該網址一旦執行，就會將 IcedID 有效籌載以 .dll 二進位檔案件的形式傳遞到受感染的電腦上。

下圖顯示過去兩個月攔截到的 IcedID 的次數，以每日細分：

過去兩個月攔截到的 IcedID 的次數，以每日細分



賽門鐵克提供的解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，僅就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.IcedID!g4
- SONAR.IcedID!g5
- SONAR.SuspLaunch!g235
- SONAR.TCP!gen1

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics, Techniques, and Procedures, TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen1
- Scr.IcedID!gen1
- Scr.IcedID!gen3
- Scr.Malcode!gdn28
- Scr.Malcode!gen46
- Scr.Malpdf!gen2
- Trojan.IcedID
- Trojan.IcedID!g16
- Trojan.IcedID!g17
- Trojan.IcedID!g18
- Trojan.IcedID!gm
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 592
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 764
- System Infected: Trojan.Backdoor Activity 765
- Web Attack: Webpulse Bad Reputation Domain Request

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於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。
欲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。
欲深入瞭解更多有關於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。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 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**。