


# 韓國正遭受登錄註冊檔濫用的惡意郵件攻擊

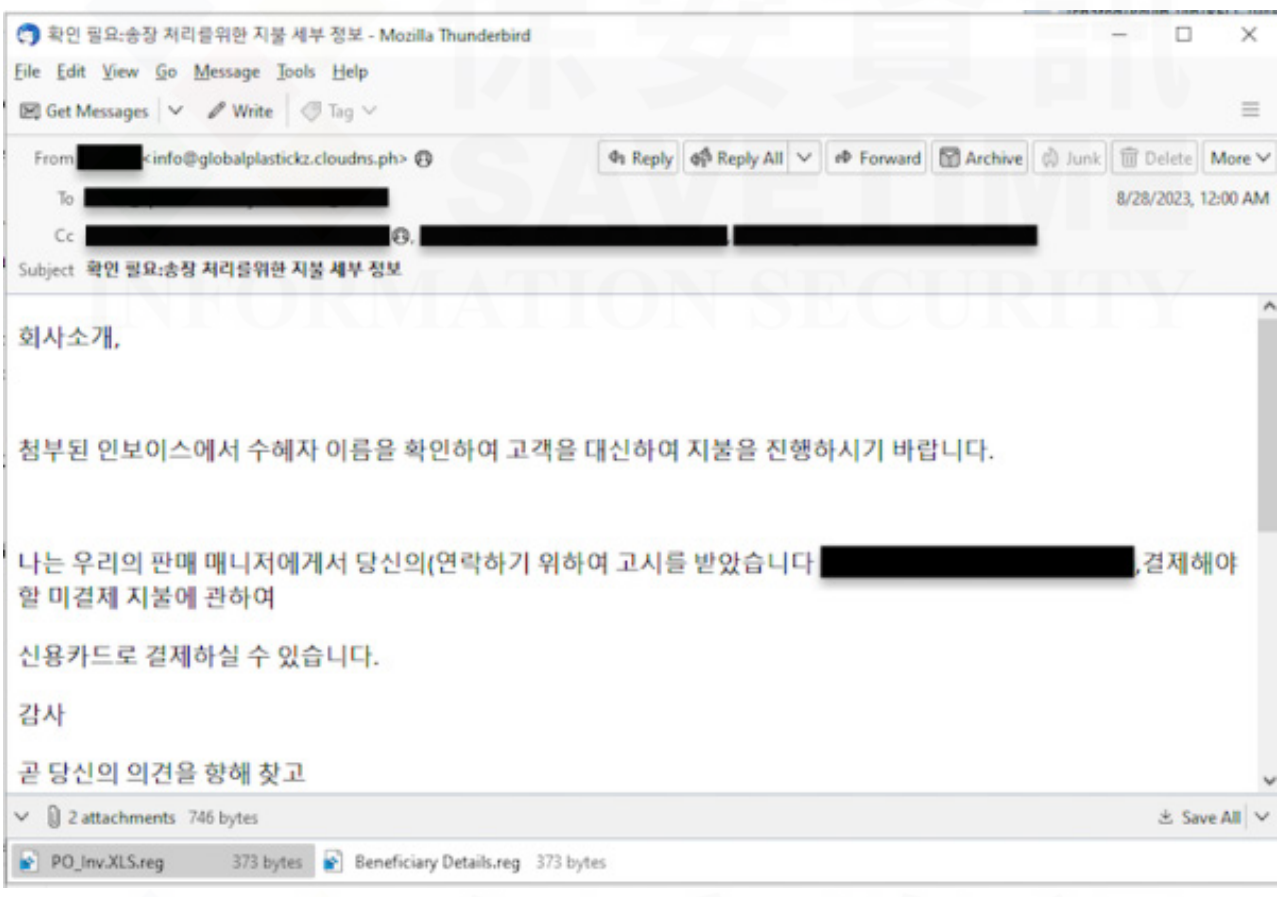
2023 年 9 月 5 日發布



.reg 登錄註冊檔是 Microsoft Windows 作業系統中用於新增、修改或刪除登錄子機碼和值的文字格式的登錄檔的腳本檔，而登錄檔是 Microsoft Windows 操作系統和其應用程式中的一個重要的層次型資料庫，用於儲存作業系統、硬體、軟體以及使用者喜好設定等資訊。

雖然 .reg 檔案通常用於合法目的，它的特性也讓網路犯罪分子可以在受害者的系統上下載和執行惡意軟體。在當今的威脅形勢下，雖然它們並不普遍，但它們仍然被世界各地的特定駭客組織和個人在其攻擊鏈中積極運用。

最近，賽門鐵克觀察到針對韓國機構組織(本地和跨國)的惡意垃圾郵件行動。惡意電子郵件（主旨：“**확인 필요: 송장 처리를 위한 지불 세부 정보**”）夾帶兩個惡意 .reg 檔案『PO_Inv.XLS.reg』和『Beneficiary Details.reg』。如果執行成功，後續將會下載惡意 PowerShell 腳本和 bat 批次檔。




該批次檔 (ld.bat) 將執行 PowerShell 腳本檔 (ld.ps1)，隨後，PowerShell 腳本將嘗試修改電腦的註冊表和隱藏的 %APPDATA% 檔案夾，使其豁免 Windows Defender 的掃描。它還會下載一個冒充 PuTTY（是個開源的Telnet／SSH 安全遠端連線程式）的竊密程式。所有下載的檔案將存儲在%APPDATA%資料夾中。

這個基於 Python 的竊密程式名為『REG STEALER 2023』，經過高度混淆和加密。它與各種 Discord 和 Telegram 竊密程式有許多相似之處。經過分析，我們認為該竊密程式很可能源於 Blank Grabber 的原始碼，該原始碼已發佈在熱門的版本控制和協作軟體開發平台上的網站。以下是它可以從受感染的電腦擷取並透過 Discord Webhooks 和 Telegram 機器人發送的一些資料。

- 瀏覽器密碼、cookie、自動填寫 (autofills) 機制的帳密和網頁瀏覽記錄
- Discord (一款在諸多系統上都可執行且功能完備的社交應用程式) 的 Token 憑證
- 已保存的WIFI密碼
- 系統資訊
- 螢幕截圖
- Telegram 連線
- Common files檔案資料夾
- 加密錢包
- 擷取鏡頭影像
- 各種遊戲和遊戲平台的 cookie 和連線

賽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 偵測到的惡意程式名稱及有效對應的防護機制：

**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：**

- Downloader
- Trojan Horse
- Trojan.Regsteal
- Web.Reputation.1

**基於機器學習的防禦技術：**

- Heur.AdvML.B

**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。

## 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**。