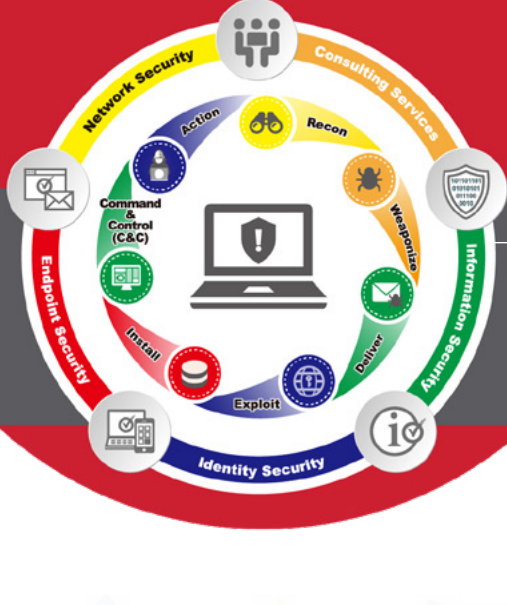




保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克有效應對，以TGZ附件來陳倉暗度GuLoader惡意軟體下載器的電子郵件攻擊

2024 年 11 月 12 日發布

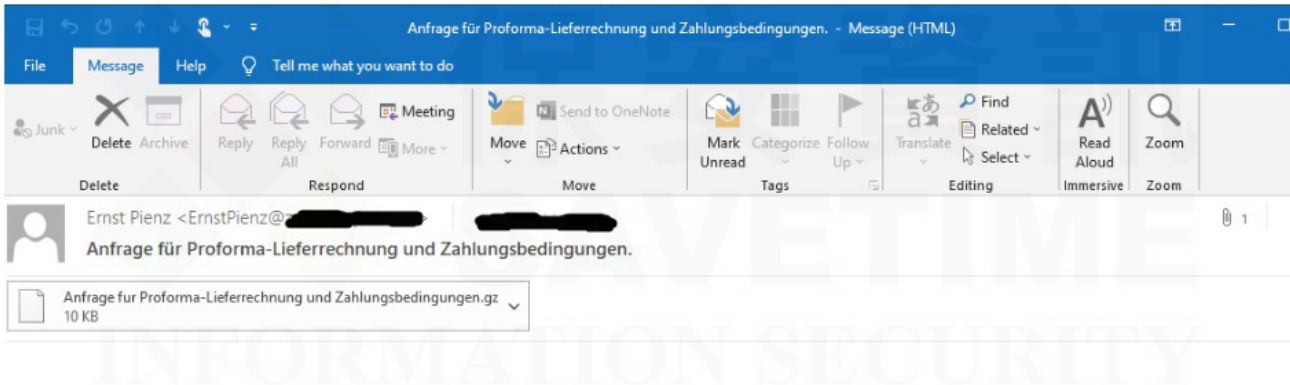
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

GuLoader 也稱為 GuLoad，是一種知名的惡意軟體下載器，自 2019 年出現以來一直困擾著電腦系統的資安威脅。多年來，此惡意軟體經過多年的開發和測試已經展現重大的轉變，可以根據最新的情況不斷調整適應以逃避偵測並利用新的漏洞。

最近幾週，我們在遙測資料中觀察到與 GuLoader 的電子郵件有關的流量變明顯，每天偵測到的數量高達數百封。這些電子郵件通常在本文中包含一則訊息，目的是引誘收件者打開附件並執行其中檔案。值得注意的是，GZ 附件檔案名稱比之前執行的 GuLoader 更長，範例包括：

- Anfrage fur Proforma-Lieferrechnung und Zahlungsbedingungen.gz
- Aqua & Clean LTD - Order Inquiry.Pricing and Shipping Costs - 11524.gz
- Draft_Shipping_documents_0020331110111.gz
- Advice Copy-\$72,000-114571_.pdf.gz
- Anfrage fur Proforma-Lieferrechn
- Anmodning om levering af proformafaktura og betalingsstilstand.gz
- Baratti & Milano S.R.L Cooperation 10_24_2024.gz
- CR-FEDEX_TN-779454699153_DT-MRN_CD-20241023_CT-1934.gz
- Draft_Shipping_documents_0020331110111.gz
- EuroStar Machinery -14240 - PPD 221-29-10-2024.gz
- Kemilab - 291024 Updated price list.gz
- PO 25367 for Seacole - ORD ACK 216668.gz
- Upit W.D. Concord West d.o.o. nr.10072024.gz
- oferta urgente CAF Mexico NCR NCR 6927 09022024.gz
- DHL Documentos De Envo 0020331110114.gz
- DHL Shipping DOC_BG468545215485_.pdf.gz
- Dringende Bestellung 10_24_2024.gz
- Hitna ponuda LUKINTEHNIK, d.o.o. 10242024.gz
- NUEVO_ORDEN_DE_COMPRA_3010202400012709.gz
- Odhad IMP3816 pro vyvoz v poslednim ctvrtleti.gz
- PO 25367 for Seacole - ORD ACK 216668.gz
- SBR & Co-14240 - PPD 221-29-10-2024.gz
- Stima IMP87654 per l'esportazione dell'ultimo trimestre.gz
- Urgent ORDER -Nesma And Partners - SICIM JV.gz

這些電子郵件使用社交工程技術引誘使用者開啟附件。這些技術包括待處理的包裹、不存在的訂單更新，或因尚未收到貨款而寄倉的訂單。



這些老套的社交工程技倆已經流行好多年了，但不知情的使用者仍會上當。隨著年終假期即將來臨，我們預期這些手法會增加，因為網路購物已經增加。

攻擊者可能選擇 TGZ／GZIP 這種較不常見的壓縮檔案格式，以降低被安全軟體偵測到的風險。TGZ／GZIP 格式也提供較佳的壓縮效果，讓附件檔可以更小。

在 .GZ 附件中，有一個與 .GZ 本身名稱相同的惡意 .VBS 檔案。



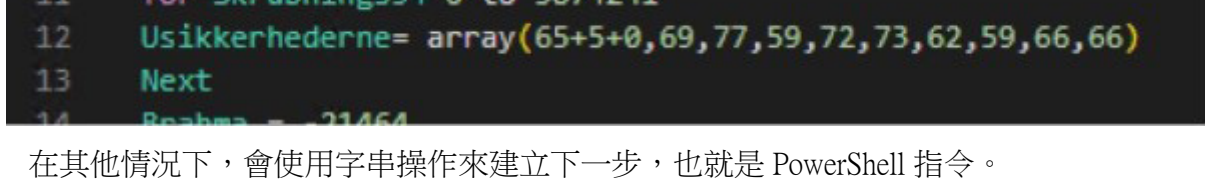
在這起 GuLoader 攻擊中，我們觀察到壓縮檔內的 VBS 檔案有各種版本，使用多種技術來逃避模擬並隱藏程式碼的意圖，同時在檔案中填入大量註解，試圖使其看起來合法。



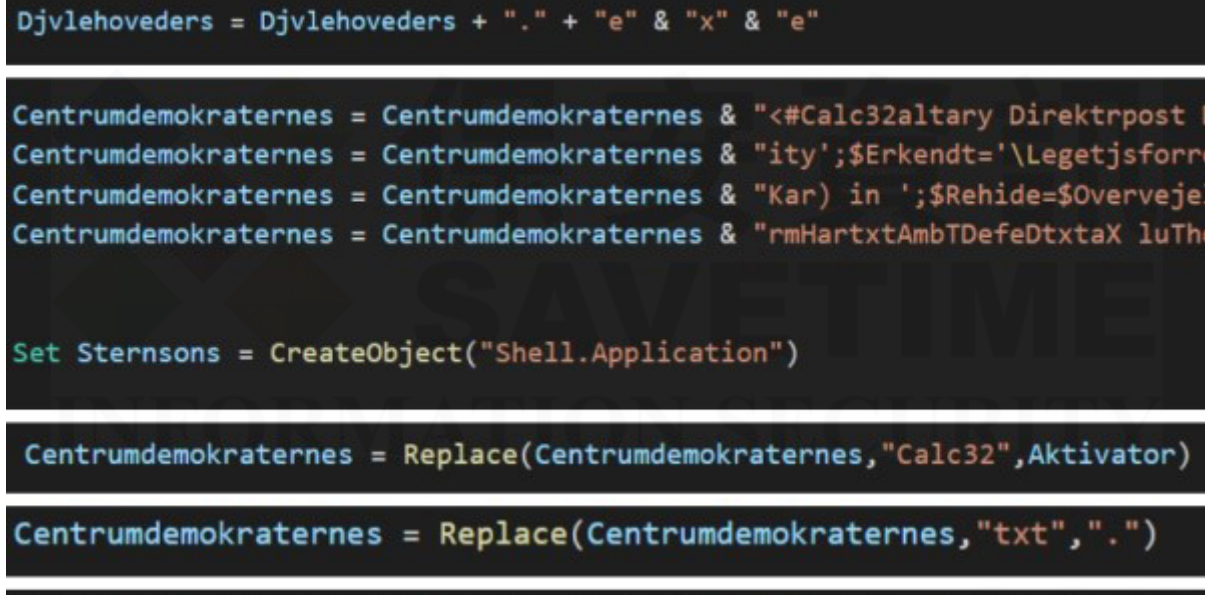
也經常可以看到非常多的變數自我串接。



在 VBS 檔案中使用大型循環可以用來迴避，例如：讓一個陣列被指定給一個變數超過 387 萬次的重複。



在其他情況下，會使用字串操作來建立下一步，也就是 PowerShell 指令。



賽門鐵克的防護技術涵蓋多個層級，包括在電子郵件傳送的初始階段封鎖攻擊。此外，還採取行為和適應性防護 (Adaptive Protection) 措施。為了提供強大的涵蓋範圍，以檔案為基礎的偵測也涵蓋惡意 VBS 檔案。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g111

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.Guloader!gen*
- ISB.Heuristic!gen*
- Scr.Heuristic!gen*
- Trojan Horse
- Web.Reputation.1

賽門鐵克提供三種常見情境的端點安全解決方案：SEP／SESE／SESC，請點擊此處了解解決方案的全貌以及您的企業適合選用哪一種方案。

要了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 Symantec Endpoint Security 的 Adaptive Protection，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。



Symantec
A Division of Broadcom

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有效的解決方案，近三年 Symantec 很少出現在由公開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踐，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。



保安資訊
KEEPSAFE
INFORMATION SECURITY

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 年起就全心全力專注在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，以及基於比原廠更熟悉用戶使用情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。許多顧客樂意與我們建立起長期的友誼，把我們的意圖可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助諮詢對象。

保安資訊連絡電話：0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500 | +886 4 23815000 | http://www.savetime.com.tw