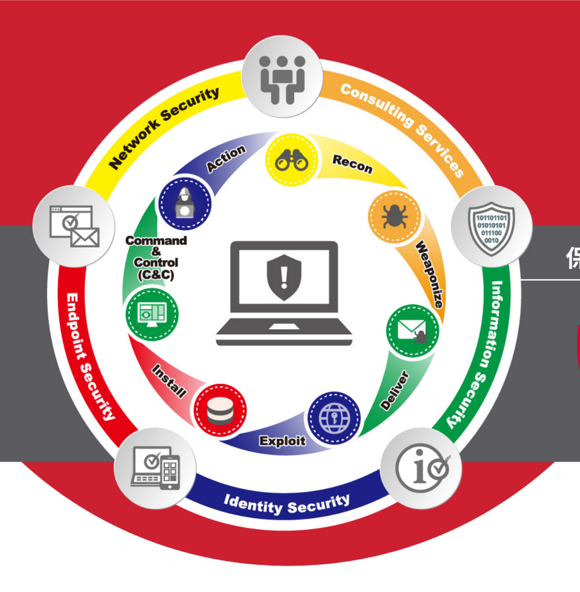


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

濫用惡意PDF檔案的網路攻擊持續上升

2024 年 2 月 20 日發布

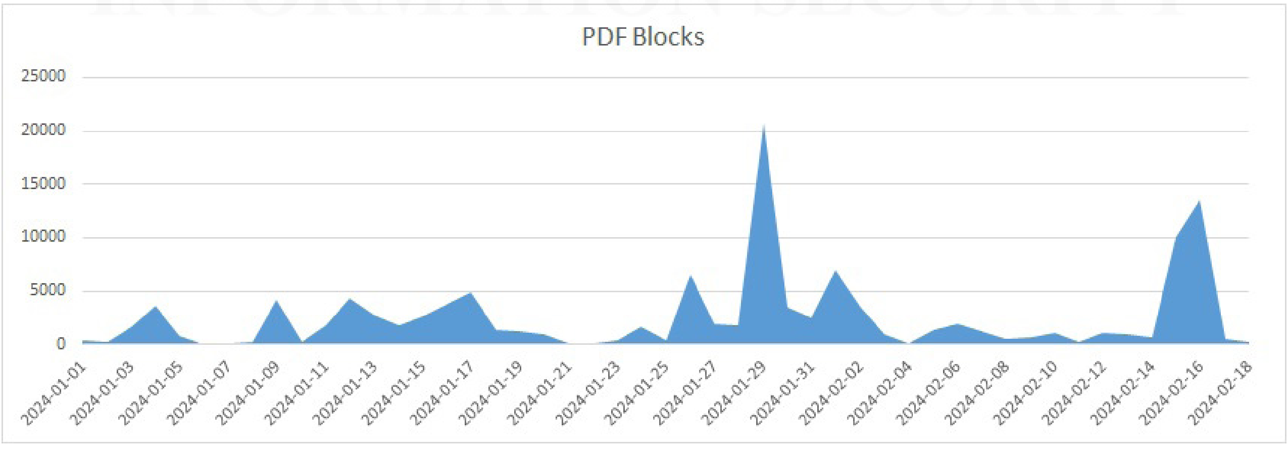
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在過去幾個月中，我們發現濫用惡意 PDF 檔案的郵件攻擊激增。為了應對這些攻擊，賽門鐵克創新的 PDF 啟發式解決方案利用先進的啟發式和機器學習技術。事實證明，這種主動式防護技術非常有效，成功阻止大量攻擊，包括由 TA544、TA577 和 RogueRadicate……等惡名昭彰的駭客組織所策動的網路攻擊。

以下是我們的啟發式解決方案在 1 月和 2 月期間阻止的一些垃圾郵件攻擊行動，涉入的駭客正試圖在其攻擊鏈中濫用惡意 PDF 檔案：

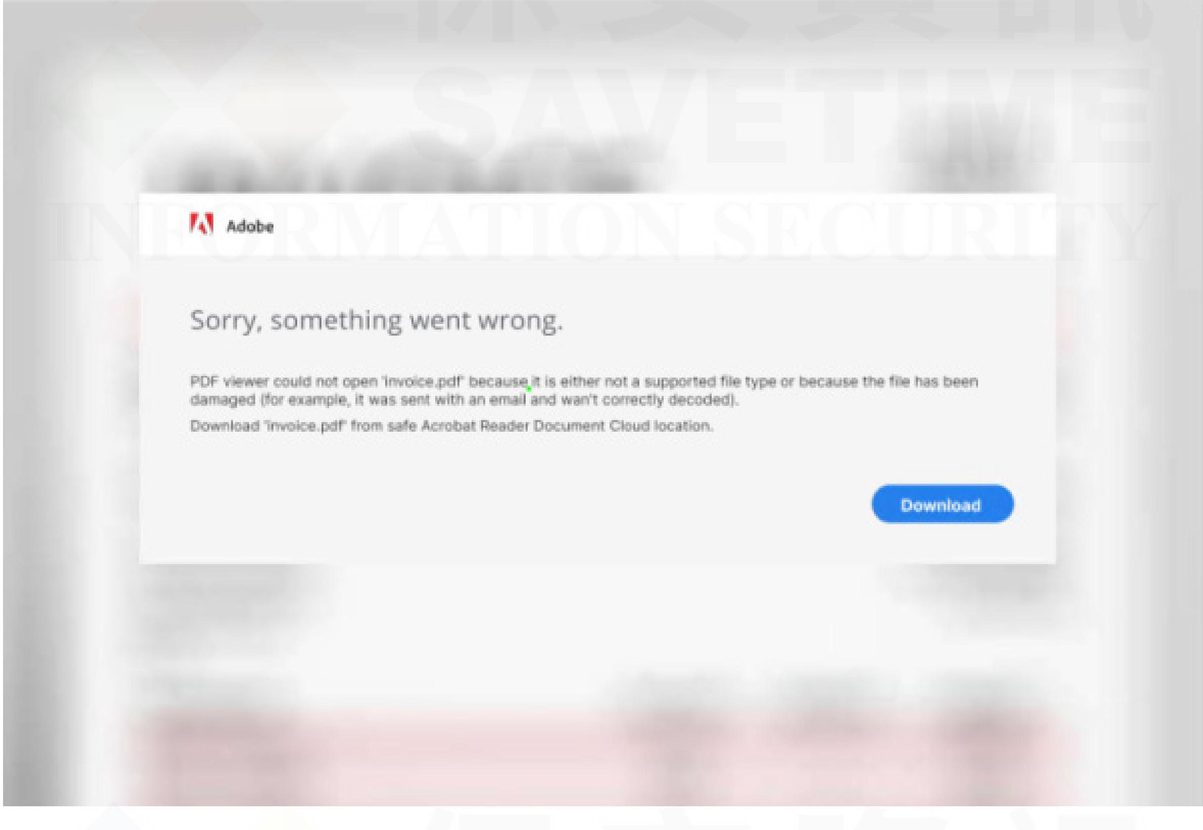
- 1 月 9 日～利用 PDF 附件傳遞 Netsupport 遠端存取木馬 (RAT) 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 16 日～利用 PDF 附件傳遞 Lokibot 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 16 日、24 日和 2 月 1 日、2 日～利用 PDF 附件傳遞 DBatLoader 和 Remcos 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 17 日、31 日～利用 PDF 附件傳遞 Wikiloader 最終有效酬載的垃圾郵件攻擊行動。
- 1 月 24 日、25 日、26 日、29 日和 2 月 12 日、13 日～利用 PDF 附件傳遞 Darkgate 最終有效酬載的垃圾郵件攻擊行動。

暗藏惡意程式碼的 PDF 網路攻擊在 1 月下旬和 2 月中旬出現明顯的高峰。



NetSupport 遠端存取木馬(RAT)

據觀察，最近傳遞 NetSupport 遠端存取木馬 (RAT) 網路攻擊行動與去年 11 月 Darkgate 行動使用類似的 PDF。因此，我們認為它們是由同一個攻擊者 RogueRadicate 所發送。當使用者點擊 PDF 中的下載連結時，會傳遞惡意有效酬載。



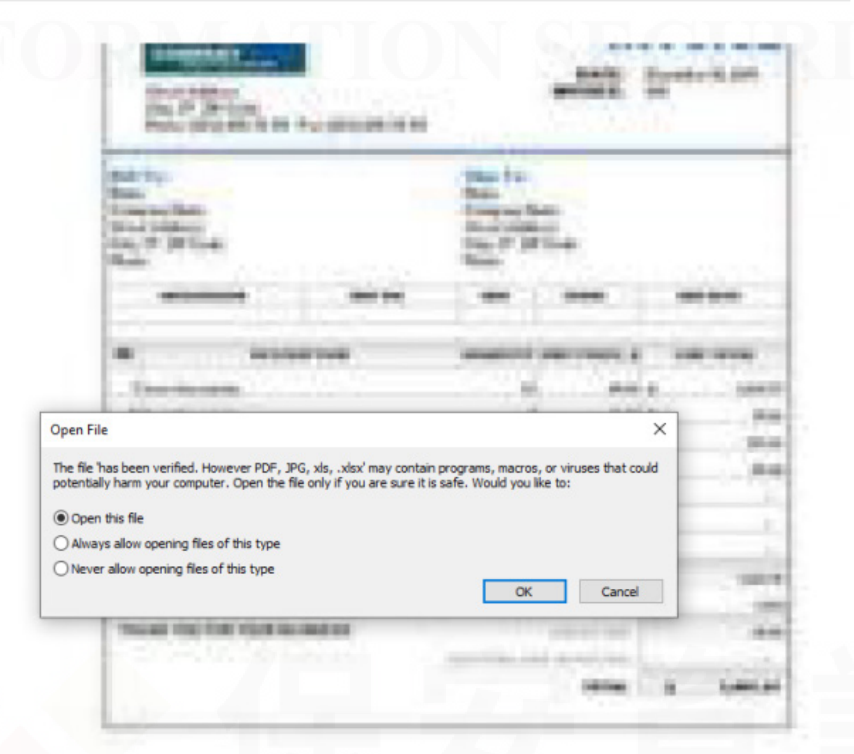
Sorry, something went wrong.

PDF viewer could not open 'invoice.pdf' because it is either not a supported file type or because the file has been damaged (for example, it was sent with an email and wasn't correctly decoded).

Download 'invoice.pdf' from safe Acrobat Reader Document Cloud location.

木馬程式LokiBot

值得關注的趨勢是，越來越多的惡意竊密程式選擇透過 PDF 垃圾郵件進行傳播。我們在今年 1 月破獲一波 Lokibot 寄生惡意 PDF 的網路攻擊行動，使用者打開 PDF 附件時會被注入一個 Office 檔案。最終的有效酬載通常會濫用眾所周知的陳年老漏洞 (例如：CVE-2017-11882 或 CVE-2017-0199) 下載並執行。

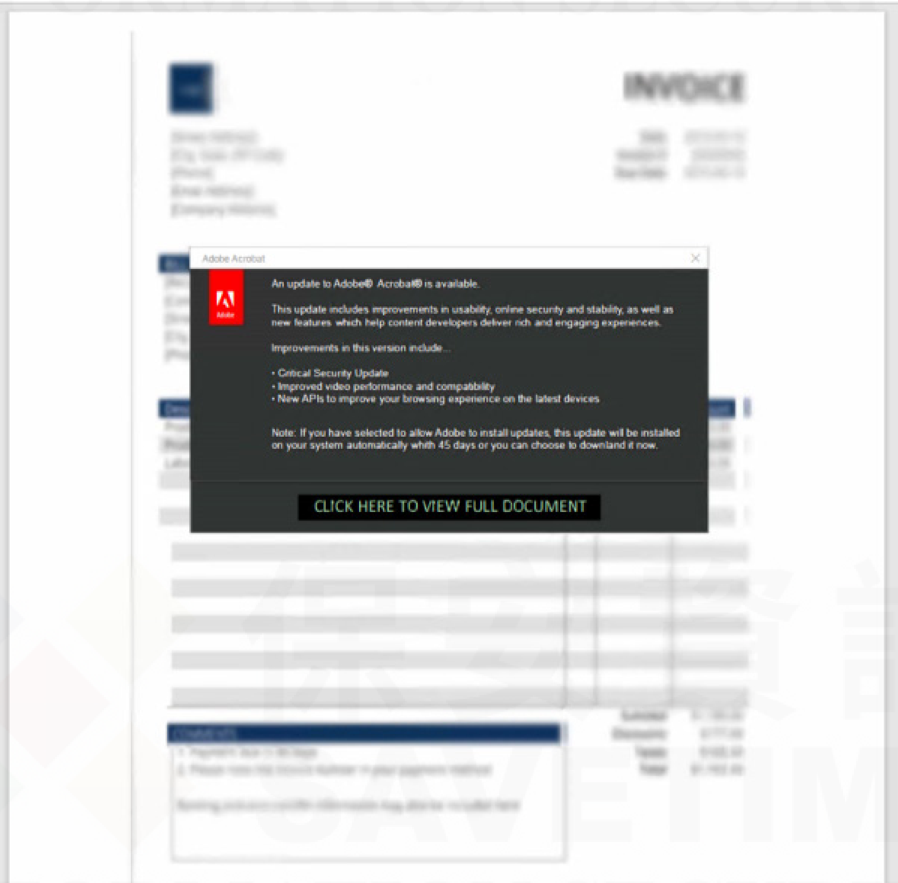


The file 'has been verified. However PDF, JPG, xls, .xlsx' may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to:

- ● Open this file
- ○ Always allow opening files of this type
- ○ Never allow opening files of this type

惡意軟體載入器DBatLoader和Remcos遠端存取木馬(RAT)

我們最近還觀察到某些 PDF 垃圾郵件攻擊行動間歇性地將 DBatLoader 和 Remcos 作為其最終有效酬載。該電子郵件偽裝成出貨單／發票，但要求使用者更新 Adobe Acrobat 軟體才能查看完整文件。如果使用者點擊更新連結，該威脅將下載惡意有效酬載，而不是軟體更新。



An update to Adobe® Acrobat® is available.

This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

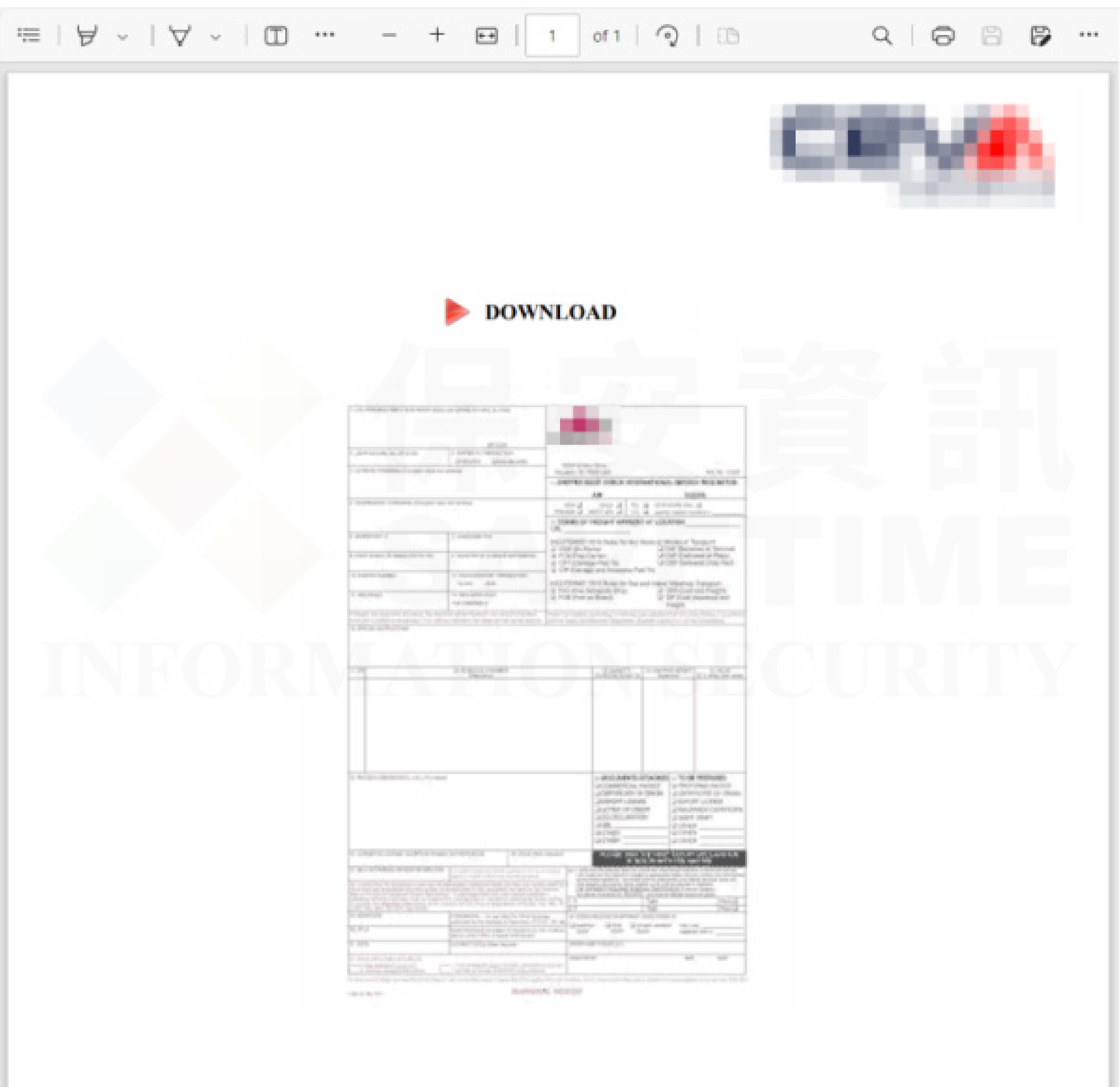
Improvements in this version include...

- Critical Security Update
- Improved video performance and compatibility
- New APIs to improve your browsing experience on the latest devices

Note: If you have selected to allow Adobe to install updates, this update will be installed on your system automatically whith 45 days or you can choose to download it now.

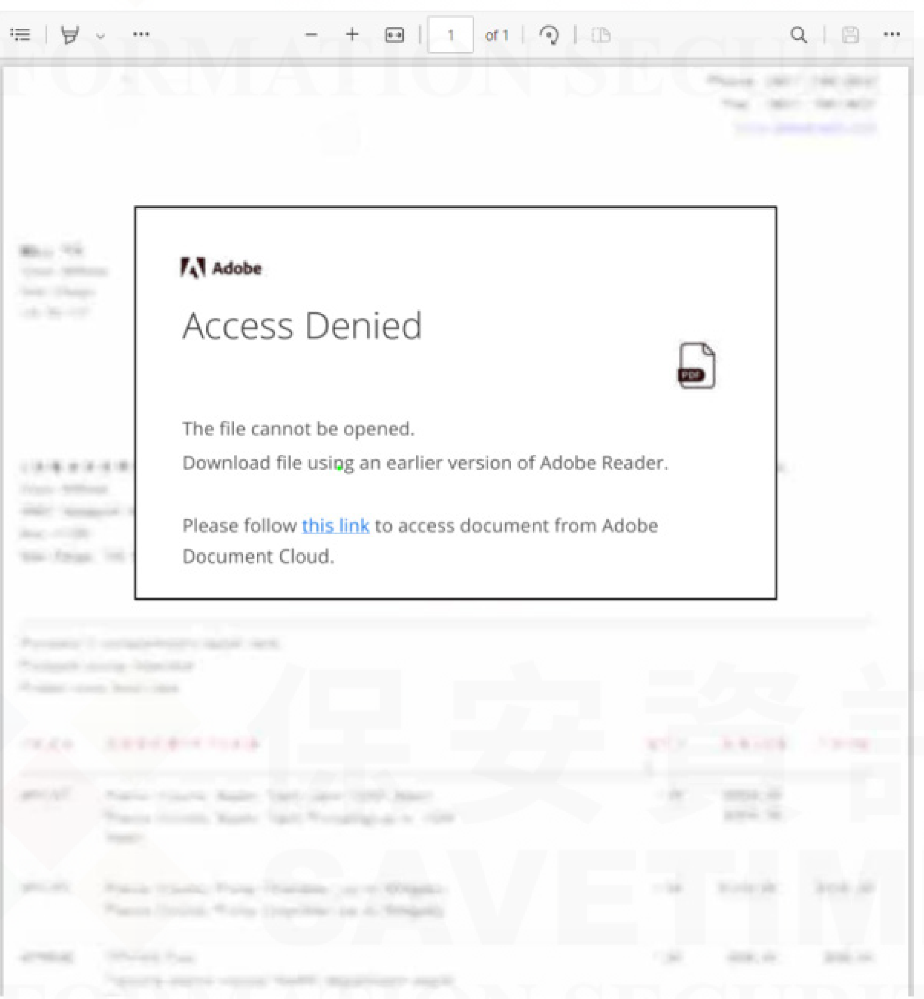
WikiLoader 惡意程式載入器

我們在之前的『防護亮點』中報導今年傳播 Wikiloader 垃圾郵件行動的強勢回歸。垃圾郵件中使用的 PDF 偽裝成一家物流公司的發票下載。點選連結後，用戶將被被重導向到一個網站，且會被注入惡意有效酬載。



惡意程式載入工具：DarkGate(*黑暗之門)

Darkgate 在去年 10 月至 11 月期間相當活躍。在 12 月份相對沉寂一段時間後，他們在 1 月份再次出現。他們在垃圾郵件中使用的 PDF 檔會顯示『存取拒絕』或『檔案顯示不正確』……等警告，目的是說服使用者點選連結進行所謂的 Adobe Reader 更新或下載檔案進行離線查看。與其他連結一樣，該連結會將使用者轉導向到另一個網站，並注入惡意有效酬載。有關 2024 年 1 月『Darkgate』活動更多資訊，請參閱先前的《防護公告：惡意程式載入工具DarkGate(*黑暗之門)涉入的網路攻擊行動中，藏身在PDF附件陷阱越來越多)》。



Access Denied

The file cannot be opened.

Download file using an earlier version of Adobe Reader.

Please follow this link to access document from Adobe Document Cloud.

值得一提的還有……

除了減輕上述一波波垃圾郵件的攻擊，PDF 啟發式防護技術還能有效阻止透過電子郵件附件或連結傳送的網路釣魚 PDF，這些網路釣魚主要在竊取使用者的機密資訊，例如：信用卡詳細資訊、銀行帳戶憑證或電子郵件帳戶登錄資訊。

賽門鐵克可保護您免受這些 PDF 相關的威脅(**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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen1
- Scr.DLHeur!gen2
- Scr.DLHeur!gen3
- Scr.DLHeur!gen5
- Scr.DLHeur!gen6
- Scr.DLHeur!gen7
- Scr.DLHeur!gen8
- Scr.DLHeur!gen9
- Scr.DLHeur!gen10
- Scr.DLHeur!gen13
- Scr.DLHeur!gen14
- Scr.DLHeur!gen15
- Trojan.DLHeur!gen2
- Trojan.DLHeur!gen3
- Trojan.DLHeur!gen4
- Trojan.DLHeur!gen5
- Phish.Pdf!gen2
- Phish.Pdf!gen3
- Phish.Pdf!gen4
- Phish.Pdf!gen5
- Phish.Pdf!gen6
- Phish.Pdf!gen7
- Phish.Pdf!gen8
- Scr.Qbot!gen12
- Scr.Qbot!gen14
- Scr.Qbot!gen19

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)。

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。

關於賽門鐵克 (Symantec)

Symantec
A Division of Broadcom

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
KEEPSAFE
INFORMATION SECURITY

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**。

2024/01/25

惡意程式載入工具DarkGate(*黑暗之門)涉入的網路攻擊行動中，藏身在PDF附件陷阱越來越多

DarkGate 是一種惡意遠端存取木馬 (RAT)，自 2018 年以來一直到處傳播。這種『惡意軟體即服務』(MaaS) 類型的惡意軟體發展迅速，就在去年 10 月，我們曾撰文報導 DarkGate 將 PDF 附件納入其網路攻擊行動的武器，以此來提高其行動的成功率。

最近，發現一種 Darkgate 藏身在惡意 PDF 檔所涉入的網路攻擊行動，其感染鏈如下：

- 網址 > 短網址 1 > 短網址2 > ZIP壓縮檔 > MSI 安裝檔 > DLL 測載 > Autoit3.exe 以及 Autoit script > DarkGate

感染鏈的複雜性顯示作者為逃避檢測的本領 (**目前除賽門鐵克外，沒有其他供應商在 VirusTotal 上顯示檢測結果，因此他們在某種程度上是成功的**)，但我們的啟發式引擎還是偵測到它。

MSI 會安裝一個名為 ItuneHelper.exe 的合法 EXE 執行檔，攻擊者使用 DLL 側載的伎倆。這種技術結合合法應用程式和惡意 DLL，在本例中，惡意 DLL 被命名為『CoreFoundation.dll』。它冒用 EXE 檔中真正 DLL 元件的名稱。

在執行過程中，CoreFoundation.dll 會從 sqlite3.dll 檔案中呼叫 Autoit3.exe 和一個名為 script.au3 的惡意檔。Autoit3.exe 是合法的 EXE 檔，它會執行 script.au3 來解密和載入最終有效籌載--一個 DarkGate 二進位檔案。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen7

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)。