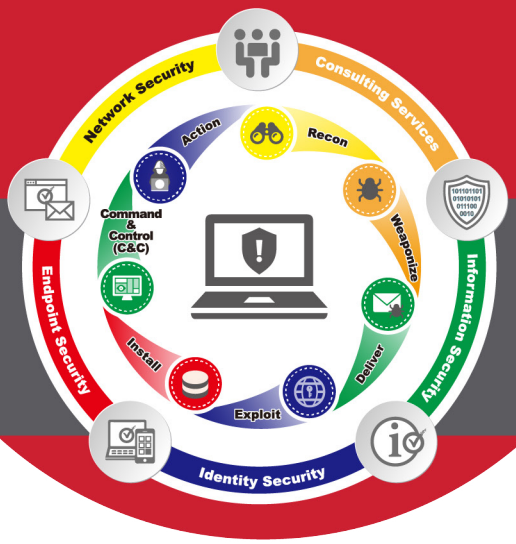


保安資訊--本周(台灣時間2024/11/01)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 43 萬 7,600 台受保護端點上總共阻止了 4,990 萬次攻擊。這些攻擊中有 80.3% 在感染階段前就被有效阻止：**(2024/10/28)**

- 在**9萬5,100**台端點上，阻止了**1,440萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬5,400**台端點上，阻止了**860萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬9,200**台**Windows**伺服主機上，阻止了**8萬5,000**次攻擊。
- 在**6萬2,100**台端點上，阻止了**180萬**次嘗試掃描伺服器漏洞。
- 在**1萬1,300**台端點上，阻止了**75萬2,500**次嘗試掃描在**CMS**漏洞。
- 在**6萬300**台端點上，阻止了**340萬**次嘗試利用的應用程式漏洞。
- 在**13萬3,800**台端點上，阻止了**280萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬7,000**台端點上，阻止了**120萬**次加密貨幣挖礦攻擊。
- 在**10萬9,000**台端點上，阻止了**870萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**543**台端點上，阻止了**9萬9,000**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 19 萬 1,100 個受保護端點上阻止了總計 830 萬次攻擊。**(2024/10/28)**

- 使用網頁信譽情資，在 **181.7K** 個端點上阻止 **780** 萬次攻擊。
- 攔截 **22.6K** 個端點上 **312.5K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **9.1K** 個端點上攔截 **143.2K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **509** 個端點上攔截 **9.3K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2024/10/31

安卓手機／行動裝置平台上的FakeCall惡意軟體出現新變種

有人在真實網路情境中發現到安卓手機／行動裝置平台上的 FakeCall 惡意軟體出現新變種。此惡意軟體背後的攻擊者使用語音釣魚 (vishing) 伎倆，誘騙受害者透露敏感資訊，例如：憑證或銀行資訊。在濫用 Android 平台上的輔助服務 (Accessibility Service) 的同時，FakeCall 可讓攻擊者對受感染裝置進行相當程度的遠端控制，允許他們模擬使用者動作、攔截來電或撥出電話、操控裝置的攝影機等。FakeCall 也允許從被攻擊的裝置收集使用者聯絡人、通話記錄或簡訊訊息。收集到的資料會轉送到攻擊者控制的 C&C 伺服器。

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：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.2
- AppRisk:Generisk

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。

2024/10/31

Sauron--在真實網路情境中出現的全新勒索軟體

Sauron 是最近在真實網路情境中發現的全新勒索軟體。此惡意軟體會在被加密的檔案中冠上「.sauron」副檔名。勒索贖金支付通知會以檔名為「#HowToRecover.txt」的文字檔形式存放在受害電腦上。攻擊者要求透過提供的電子郵件帳號與他們聯繫，並要求以彼特幣 (Bitcoin) 來支付贖金。惡意軟體還能夠更改桌面背景，示警受害者檔案已被加密。Sauron 具備刪除受感染電腦的磁碟區陰影複本 (Volume Shadow Copies) 功能，讓受害者無法復原資料。

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-Schtsk!g1
- ACM.Untrst-RunSys!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomGen!gen3
- SONAR.Ransom!gen14
- SONAR.Ransomware!g20
- SONAR.Ransomware!g38
- SONAR.SuspLaunch!g193

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

2024/10/30

UNC5812駭客組織利用Android和Windows惡意軟體對烏克蘭進行攻擊

最近一份報告凸顯一個名為 UNC5812 疑似俄羅斯駭客組織所展開的攻擊活動。該活動涉及散佈針對烏克蘭新兵的 Android 和 Windows 惡意軟體。該活動目的不僅是從事間諜活動，還試圖對親烏克蘭軍隊的支持造成負面影響。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Downloader!gen8
- Trojan.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- Android.Reputation.2
- Spyware:MobileSpy

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。

2024/10/30

Bumblebee(*大黃蜂)惡意程式載入器很可能再次捲土重來

據報導，本月發現新一起傳送 Bumblebee(*大黃蜂) 惡意程式載入器的網路攻擊行動。Bumblebee 是一種非常老練複雜的惡意程式載入器，最早是在 2022 年被發現。該惡意軟體已涉入許多惡意攻擊行動，並用於傳送和執行各種有效酬載，例如：Cobalt Strike、勒索軟體等。自從歐洲刑警組織在 2024 年 5 月進行名為「Operation Endgame」的殭屍網路瓦解行動後，Bumblebee 直到現在才又被發現。新 Bumblebee 感染鏈包含惡意的 .zip 壓縮檔、PowerShell 指令、.lnk 和 .msi 檔案，這些手法都會讓部署 .dll 二進位檔形式的有效酬載變得更難被偵測。

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-Http!g2
- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.Malcode!gen
- Scr.Mallnk!gen2
- Scr.Mallnk!gen15
- Trojan Horse
- Trojan.Bumblebee
- Trojan.BumbleBee!g13
- Trojan.BumbleBee!g14
- Trojan.Dropper
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Web.Reputation.1
- 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

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。

2024/10/30

CVE-2024-40711--Veeam的Backup and Replication備份解決方案存在不安全的反序列化漏洞已被駭客開採濫用

CVE-2024-40711 是最近被揭露存在 Veeam 的 Backup and Replication 備份解決方案存在不安全的反序列化漏洞，CVSS 風險評分為 9.8，屬於非常嚴重等級，會影響版本 12.1.2.172 或更舊的版本。如果成功開採濫用此漏洞，未經驗證的攻擊者可能會在遭入侵的系統上遠端執行程式碼 (RCE)。據報導，此漏洞已被 Akira 和 Fog 勒索軟體組織開採濫用。繼此報告後，CVE-2024-40711 也被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

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：

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：

- Web Attack: Malicious Payload Download 36

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，預設防護政策透過封鎖所有入埠和離埠連線，防止攻擊者存取有漏洞的系統。
- 某些勒索軟體駭客組織已知會利用此漏洞作為第二階段的攻擊，以建立新的本機管理員並進行橫向移動。DCS 預設政策會在第零天阻止這些惡意嘗試。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/30

養成使用手機的好習慣：安裝APP還是由官網下載～惡意的「Lounge Pass」手機APP，覬覦印度的航空旅客

有人觀察到一起名為「Lounge Pass」惡意 Android 手機 APP 涉入的攻擊行動，目標是針對印度機場的航空旅客。該 APP 透過造假的站台散佈，會從受害者的裝置攔截並轉發簡訊給網路罪犯，導致重大財務損失。網路騙徒利用暴露的 Firebase 端點來儲存竊取的簡訊。為了防止資料被盜用，建議僅從官方商店下載 APP 式，並避免授予旅遊或休息室 APP，存取簡訊的權限。

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：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.2
- AppRisk:Generisk

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。

2024/10/29

惡意廣告行動透過假「CAPTCHA」驗證系統傳播Lumma、Amadey等惡意軟體

威脅份子日益增加透過假的用來辨認人類與機器人「CAPTCHA」驗證系統作為攻擊鏈的初始攻擊。最近廣告軟體攻擊行動以線上使用者為目標，向他們提供假 CAPTCHA 或更新提示。攻擊者利用廣告網路，將受害者重導向到託管這些社交工程誘餌的受攻擊網站。一旦被誘騙，受害者就會觸發 PowerShell 指令，部署竊取憑證的惡意軟體，例如：收集加密貨幣錢包、密碼和瀏覽器資料的 Lumma ，或收集憑證並部署 Remcos RAT 的 Amadey。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen2
- SONAR.SuspOpen!gen11

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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：

- Audit: Bad Reputation Application Activity
- System Infected: Bad Reputation Process Request 4
- Web Attack: Webpulse Bad Reputation Domain Request

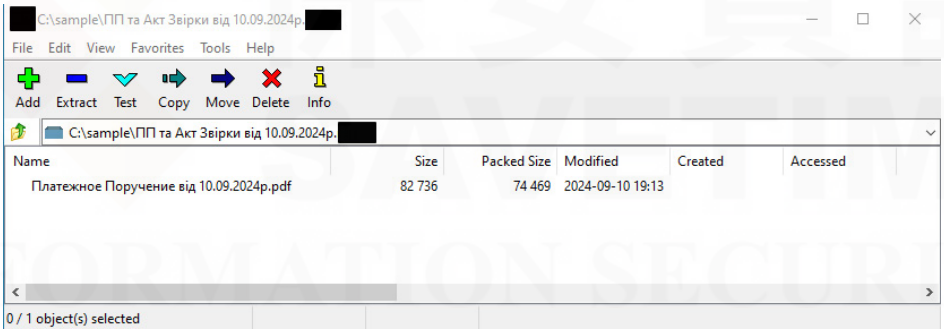
2024/10/29
防護亮點：賽門鐵克的用戶～免驚！特定資料壓縮軟體的使用者成為駭客利用異常ZIP壓縮檔發動攻擊的目標

ZIP 資料壓縮格式於 1989 年首次推出，是一種廣泛使用於各種作業系統的壓縮檔格式，許多人每天都要使用它。它主要用於將一個或多個檔案合併到單一位置，通常使用壓縮來減少檔案大小。可節省儲存空間，並加快檔案傳輸速度。接收者可以解壓縮 (英文常用 extract 或 unzip) ZIP 檔案，然後以原始格式使用檔案。目前有多種資料壓縮軟體可處理 ZIP 檔案 (例如：RAR/7z)，但它們的行為可能有很大差異，尤其是在處理異常的壓縮檔時。

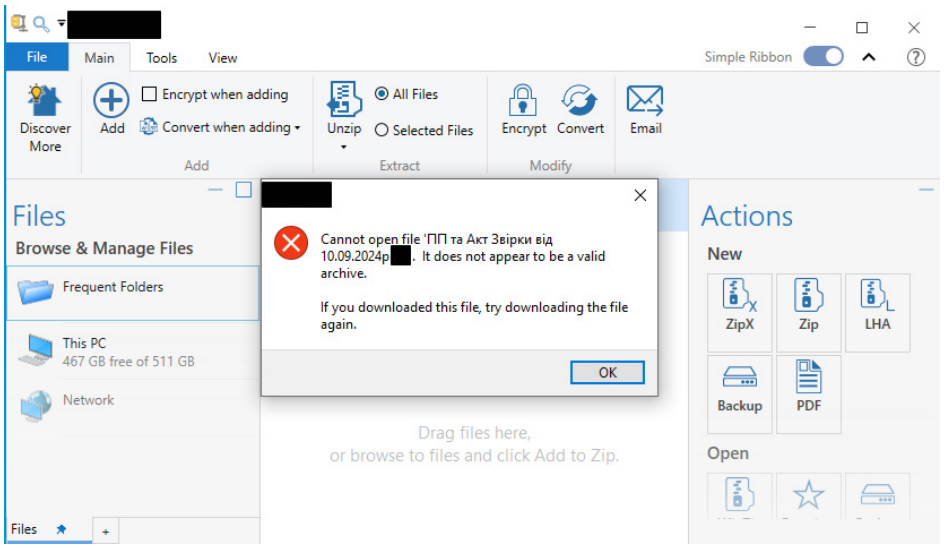
如果要將兩個或更多 ZIP 壓縮檔合併為單一檔案 (此過程稱為拚接--concatenation)，該如何處理？不同的資料壓縮軟體有不同的回應方式。大多數資料壓縮軟體只能存取第一個壓縮檔中的檔案，或將拚接檔案回報為已損毀。然而，有一個特定的資料壓縮軟體會特別地允許存取拚接序列中最後一個壓縮檔中的檔案。

最近，有人觀察到攻擊者利用這個不一致，針對特定資料壓縮軟體的使用者，使用後門程式：Smokeloader 家族的 JavaScript 惡意程式下載器。他們刻意使用通常與該資料壓縮軟體相關的副檔名來拚接 ZIP 壓縮檔。

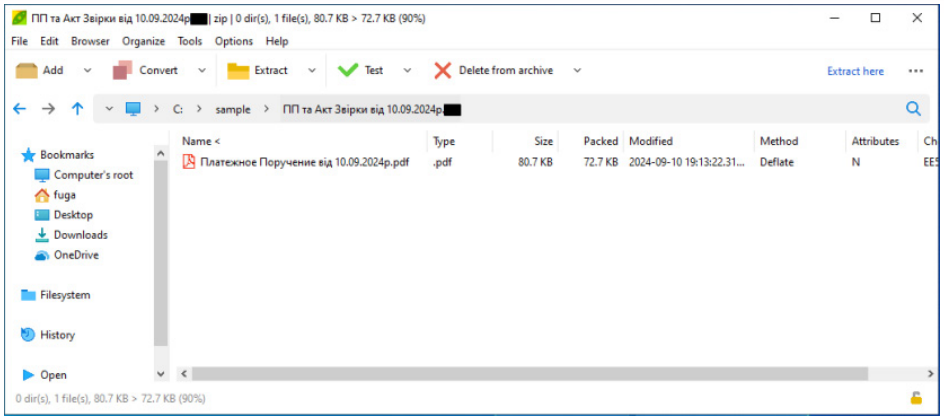
攻擊者將兩個 ZIP 檔案連結在一起。第一個壓縮檔包含一個無害的 PDF 檔案，而第二個壓縮檔則包含兩個具有相同有效酬載的 JavaScript 下載程式--兩個程式都是用來下載和執行 Smokeloader 惡意軟體。以下是截圖，顯示各種資料壓縮軟體如何處理此畸形 ZIP 壓縮檔。



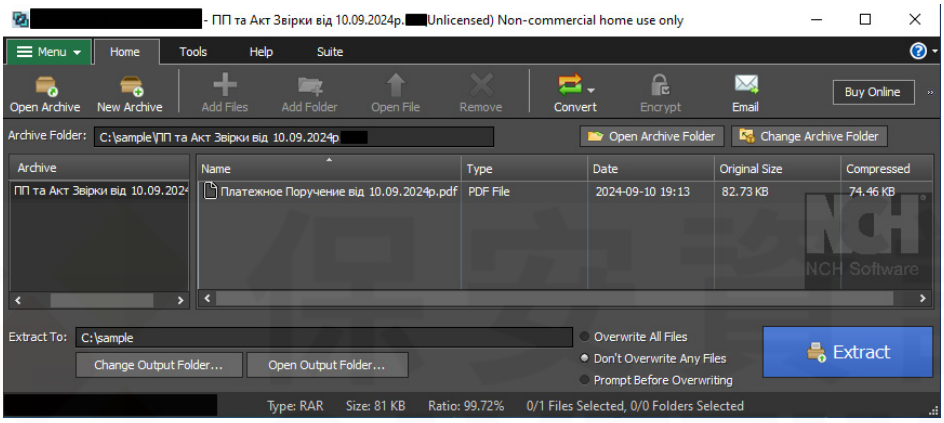
資料壓縮軟體 #1，只能存取第一個壓縮檔中的 PDF 檔案。



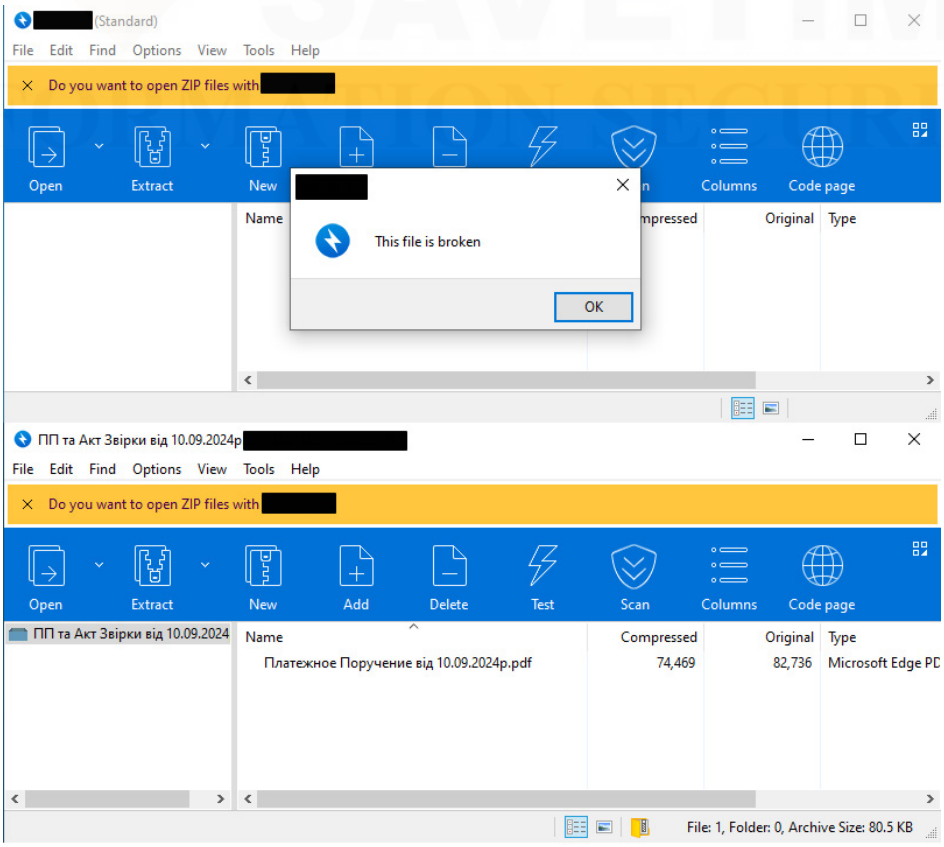
資料壓縮軟體 #2 ，回報拚接的壓縮檔已損毀。



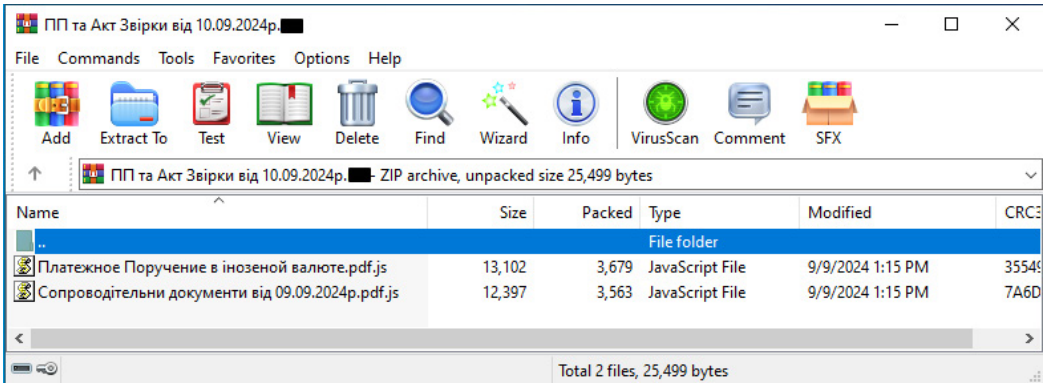
資料壓縮軟體 #3，只能從第一個壓縮檔存取 PDF 檔案。



資料壓縮軟體 #4，只能從第一個壓縮檔存取 PDF 檔案。



資料壓縮軟體 #5 ，回報拚接壓縮檔已損毀，並顯示第一個壓縮檔中的 PDF 檔案。



只有資料壓縮軟體 #6 ，有顯示出第二個壓縮檔中的 JavaScript 檔案。

此伎倆可確保安裝特定資料壓縮軟體的使用者能夠存取第二個壓縮檔中的惡意 JavaScript 檔案。然而，並非所有安全軟體都能有效處理這種畸形的 ZIP 壓縮檔，因此難以擷取和偵測惡意 JavaScript 檔案。這種手法大大增加惡意軟體成功傳送的成功率。

賽門鐵克靜態資料掃描 (Static Data Scanner：SDS) 的進階剖析技術是專為掌管此類異常現象而設計。它可以準確剖析拚接的 ZIP 檔案，確保提取並有效偵測惡意檔案，例如：Smokeloader 攻擊中使用的 JavaScript 惡意程式下載器。

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.Malarchive!gen9
- Scr.Malcode!gen164
- Trojan.Smokeloader!g1

欲深入瞭解更完整的的賽門鐵克端點／重要主機／郵件安全/網頁安全解決方案，請點擊此處。
欲深入瞭解更多關於賽門鐵克先進的防護技術在真實網路情境的優異防護能力，請點擊此處。

2024/10/29

駭客組織TeamTNT發動以雲端原生環境為目標的新一波挖礦劫持攻擊行動

據報導，駭客組織 TeamTNT 發起新的攻擊行動，目標是在雲端原生環境中進行「挖礦劫持」並轉售已遭劫持的伺服器。他們利用暴露的 Docker daemon 來部署 Sliver 惡意程式、網路蠕蟲和加密挖礦程式，透過暴露的 Docker 連接埠取得存取權限，並使用受遭入侵的 Docker Hub 帳戶散佈惡意程式和出租受害者的運算能力。

網路上的知識：

- 「挖礦劫持」又被稱為「挖礦綁架」或「惡意挖礦」。駭客在使用者未察覺的狀態下，於使用者的手機、筆電、桌上型電腦，甚至是網路伺服器上安裝加密貨幣挖礦程式，利用受害者的硬體資源進行挖礦，但獲利的卻是駭客。這些挖礦程式可能會耗用受害者的處理器資源、記憶體資源、增加使用者的電費，還會縮短裝置壽命。
- 雲端原生一詞指建置和執行應用程式的概念，以利用雲端交付模型所提供的分散式運算功能。雲端原生應用程式的設計和建置目的，是要利用雲端所提供的規模、彈性、復甦力和彈性。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Rootkit
- Trojan Horse
- Trojan.Gen.NPE

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。

2024/10/29

發現可能針對TradingView社群使用者的 Rekoobe 惡意軟體

Rekoobe 惡意軟體被發現託管在一個開放目錄 (open directory)，其目的可能是針對 TradingView 使用者以及其他網路間諜行動。Rekoobe 是 APT31 駭客組織和其他從事網路間諜及資料竊取對手之前部署的多功能後門。該惡意軟體部分以公開的 Tiny SHell 為基礎，並已進化為結合增強的加密技術和獨特命令與控制配置，使得分析和偵測變得更加困難。

網路上的知識：TradingView 提供免費／付費線上金融圖表、行情報價，是活躍交易員與投資人的專屬社群。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Trojan
- Trojan.Gen.NPE
- WS.Malware.1

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。

2024/10/29

Daggerfly駭客組織特別針台灣的企業與組織機構，推出全新CloudScout駭客工具集

據報導，與中國有關連的駭客組織：Daggerfly (也被稱為 Evasive Panda) ，已經鎖定台灣一家政府單位和一家宗教組織，使用先前未聞的侵入後 (Post-Compromise) 駭客工具集：CloudScout。此駭客工具集可利用竊取的網路會話 cookies 從各種雲端服務擷取資料。此外，CloudScout 可與 Evasive Panda 的簽名式惡意軟體框架 MgBot 無縫整合。

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-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mgbot!gen1
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- 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。

2024/10/28

散佈XWorm遠端存取木馬(RAT)的網路釣魚行動

研究人員最近發現一個惡意行動，透過冒充軟體與服務公司：Namirial(專注在電子簽章與數位憑證) 官方通訊的偽造電子郵件散佈 XWorm 遠端存取木馬 (RAT)。這些電子郵件會提示使用者開啟一個有密碼保護的 PDF 檔案，如果開啟失敗，就會引導使用者到一個 Dropbox 連結，下載一個包含惡意網址的 .ZIP 壓縮檔，這個惡意網址會連接到攻擊者的伺服器，並下載額外的惡意腳本，進而控制受害者的機器。

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-CPE!g2
- ACM.Ps-Http!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Web.Reputation.1

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。

2024/10/27

HeptaX駭客組織發動的網路攻擊行動

研究人員最近發現針對醫療保健產業發動的多階段網路攻擊行動，該攻擊是透過一個包含惡意捷徑 (.lnk) 檔案的 .ZIP 壓縮檔案所觸發，很可能是透過網路釣魚電子郵件散佈。當執行時，.LNK 檔案會執行 PowerShell 指令，從遠端伺服器下載其他有效酬載，包括指令碼和 .BAT 批次檔。這些腳本會建立新的有管理者權限之帳戶，並變更 RDP 設定以降低驗證要求，讓攻擊者取得遠端存取權，以進一步進行惡意行動，例如：竊取資料和安裝惡意軟體。

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-Enc!g1
- ACM.Ps-Net!g1
- ACM.Ps-Reg!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政

策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen241
- ISB.Downloader!gen294
- Scr.Heuristic!gen20
- Scr.Mallnk!gen6
- Scr.Mallnk!gen10
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

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。

2024/10/25

多個漏洞影響Palo Alto Networks Expedition (第三方廠商組態轉移至Palo Alto工具)

本月揭露多個影響 Palo Alto Networks Expedition (第三方廠商組態轉移至 Palo Alto 工具) 的漏洞。所報告的漏洞 (CVE-2024-9463、CVE-2024-9464、CVE-2024-9465、CVE-2024-9466、CVE-2024-9467) CVSS 風險評分介於 7.0 與 9.9 之間，包含命令注入、跨站腳本 (XSS)、敏感資訊的明文儲存、誤失身份驗證和 SQL 注入漏洞。如果被開採濫用，攻擊者除了可將任意檔案寫入受攻擊系統的暫存位置外，還可以讀取資料庫內容。原廠已在 1.2.96(含) 之後的版本修正這些漏洞。

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：

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：

- Attack: Palo Alto Expedition OS Command Injection CVE-2024-9463
- Attack: Palo Alto Expedition SQL Injection CVE-2024-9465

2024/10/25

CVE-2024-47575--存在Fortinet FortiManager的誤失身份驗證漏洞

CVE-2024-47575 是一個影響 Fortinet FortiManager 的零時差漏洞，本月份剛被揭露。此漏洞的 CVSS 風險評分為 9.8。如果被成功開採濫用，它可能允許遠端未認證之攻擊者透過特定的請求執行任意程式碼。有報告指出至少從 2024 年 6 月起，該漏洞已在真實網路情境中被開採濫用發動攻擊。在這些報告之後，它也在本週被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

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：

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，政策建議封鎖 fgfmd daemon 用於存取敏感資料或執行任意指令。其主要是透過在 Fortinet 應用程式執行的沙箱中，控制可寫入檔案的位置以及可透過此 daemon 執行的指令。
- DCS 的 UNIX 預設的強化沙箱和應用程式自訂沙箱，可保護底層作業系統資源不受受影響的應用程式所影響，並防止攻擊者使用多種技術實現常駐和執行任意程式碼。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2024/10/25

Parano惡意竊密程式

Parano 惡意竊密程式是最近在真實網路情境中被發現的另一種「普通」惡意竊密程式之新變種。這個以 Python 為基礎的惡意軟體具有從受攻擊的端點收集和滲出各種資訊的功能，包括：憑證、cookie、儲存在網頁瀏覽器中的雜項資料、加密貨幣錢包、系統資訊或來自 Steam、Telegram 或 Discord 等各種第三方應用程式的資料。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.NPE
- WS.Malware.1

2024/10/25

Liberium遠端存取木馬(RAT)惡意軟體

Liberium 遠端存取木馬 (RAT)(也稱為 ShadowRoot) 是最近在駭客論壇上出售的惡意軟體新變種。該惡意軟體具有允許攻擊者遠端存取易受攻擊的端點、進行檔案管理操作、竄改登錄檔 (registry) 以及竊取系統相關資訊和其他機密資料的功能。

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-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse
- WS.Malware.2

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

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。

2024/10/24

CVE-2024-38094--存在Microsoft SharePoint的反序列化漏洞(Deserialization)出現實際漏洞利用攻擊行動

CVE-2024-38094 是存在 Microsoft SharePoint 的反序列化漏洞 (Deserialization)，最初於 2024 年 7 月揭露並已修補。該漏洞的 CVSS 風險評分為 7.2，是由於產品在沒有充分驗證所產生的資料輸出是否有效的情況下進行資料反序列化所引起。成功開採濫用此漏洞可讓攻擊者在有漏洞的應用程式中注入並執行任意程式碼。繼公開報導此漏洞在真實網路情境中被開採濫用之後，此漏洞也在本週被美國網路安全暨基礎設施安全局(CISA) 列入「已遭成功利用的高風險漏洞名單(the Known Exploited Vulnerabilities Catalog-KEV)」中。

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：

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，針對此漏洞提供如下的多層級保護：

- 賽門鐵克 Data Center Security(DCS) IPS 政策可以控制哪些程式可以在自訂的 EM7 沙箱中執行。它還可以控制哪些資源可以寫入或讀取。
- DCS 還可防止執行任意指令，並限制讀取作業系統主要檔案的存取權限。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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，以及基於比原廠更孰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，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。