保安資訊--本周(台灣時間2024/10/18)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 45 萬 100 台受保護端點上總共阻止了 4,770 萬次攻擊。這些攻擊中有 81.1% 在感染階段前就被有效阻止：**(2024/10/14)**

- 在**9萬2,900**台端點上，阻止了**1,420萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬600**台端點上，阻止了**870萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬**台**Windows**伺服主機上，阻止了**7萬1,000**次攻擊。
- 在**6萬200**台端點上，阻止了**190萬**次嘗試掃描伺服器漏洞。
- 在**1萬600**台端點上，阻止了**72萬9,300**次嘗試掃描在**CMS**漏洞。
- 在**5萬300**台端點上，阻止了**260萬**次嘗試利用的應用程式漏洞。
- 在**14萬1,500**台端點上，阻止了**290萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,000**台端點上，阻止了**100萬**次加密貨幣挖礦攻擊。
- 在**10萬4,600**台端點上，阻止了**810萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**529**台端點上，阻止了**9萬900**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 18 萬 7,000 個受保護端點上阻止了總計 750 萬次攻擊。**(2024/10/14)**

- 使用網頁信譽情資，在 **177.6K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **22.2K** 個端點上 **278K** 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 **8.8K** 個端點上攔截 **116.8K** 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 **454** 個端點上攔截 **9.7K** 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。

2024/10/17

新興惡意竊密程式如雨後春筍般湧現：活蹦亂跳的Divulge、DedSec和Duck等新興惡意竊密程式

在駭客論壇、GitHub 和 Telegram 上發現有多種新興惡意竊密程式正在做廣告，這些新興惡意竊密程式都是由同一個單位開發和推廣。值得注意這些變種包括 Divulge(Umbral 的副本)、DedSec(以 Doenerium為基礎) 和 Duck(AZStealer 的衍生出來的版本)。這些變種主要以 Discord 資料、瀏覽器資訊、加密貨幣錢包為目標，並採用反分析技術以逃避偵測，並在背景中有效運作。

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

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.MBT
- 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

2024/10/17

新版TrickMo手機惡意程式，針對Android使用者提供假的螢幕鎖定畫面

安全研究人員最近揭露 TrickMo 的後繼新變種，這是一種針對 Android 和 iOS 使用者的行動銀行木馬程式。這個新變種除了原有的功能外，還增加一些新功能，例如：螢幕錄製、遠端控制和權限授予。現在 TrickMo 包含從受感染的裝置中竊取螢幕解鎖編碼和唯一裝置識別碼的功能。當惡意 APP 執行時，它會顯示一個模仿標準鎖定螢幕設計的全螢幕網頁，如果使用者輸入他們的螢幕解鎖代碼，該代碼就會透過 PHP 外洩給攻擊者以供後續攻擊使用。

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。

2024/10/17

狐假虎威～假裝Lockbit勒索軟體的網路攻擊行動，針對macOS和Windows環境進行資料竊取

據報導，在真實網路情境上出現一個假裝大尾勒索軟體：Lockbit 的網路攻擊行動。此惡意軟體是以 GO 語言撰寫，並鎖定 macOS 和 Windows 使用者為目標，試圖加密和竊取機密資料。被竊取的資訊會上傳到由攻擊者控制的 Amazon AWS S3 雲端儲存貯體。惡意軟體會加密使用者檔案、刪除受感染機器上的陰影複本，並在被加密的檔案上冠上 .abcd 副檔名。然後，勒索惡意軟體會將桌面背景變更為從 Lockbit 2.0 攻擊複製而來的背景。此舉顯然是向受害者施壓，迫使其乖乖就範，支付所要求的贖金。

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：

- AGR.Terminate!g2
- SONAR.Patchbrowse!g1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!gen9
- SONAR.SuspLaunch!g18
- SONAR.TCP!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：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/10/17

存在微軟Windows核心的競爭危害(Race Condition)型態的漏洞：CVE-2024-30088

CVE-2024-30088 是存在微軟 Windows 核心中被稱為 Time-of-Check to time-of-use(TOCTOU)，屬於競爭危害 (Race Condition) 型態的漏洞。當資源的狀態在驗證 (檢查) 與實際使用之間被修改時會產生此漏洞，攻擊者可利用此漏洞提升權限。當成功開採濫用此漏洞時，攻擊者可在受影響的系統上以提升的權限執行程式碼。此漏洞已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，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

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)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 入侵防護系統 (IPS) 中的 Exchange 工作負載政策會封鎖所有在 exchange 伺服器上初始存取以防止被植入 web shell。
- DCS 網域控制器和 Exchange 工作負載政策 (IPS) 可提供零時差保護，防止從 Microsoft Exchange 伺服器和網域控制器竊取憑證。
- DCS 預設政策將阻止在機器上注入和載入密碼過濾政策 DLL(psgfilter.dll)。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/16

Leafperforator進階持續威脅(APT)駭客集團揮軍進擊中東和非洲地區

Leafperforator (也稱為 SideWinder) 進階持續威脅 (APT) 駭客集團主要針對軍事和政府單位。據觀察，該駭客集團已將其攻擊行動擴展至中東和非洲。攻擊鏈通常從魚叉式網路釣魚電子郵件開始，其中包含惡意 Microsoft Office 文件檔或含有 .LNK 檔案的 ZIP 壓縮檔。這些文件通常使用來自公開網站的資訊，以合法性為幌子引誘受害者開啟這些文件。此外，一個名為「StealerBot」的後滲透 (Post-exploitation) 工具組已被確認為涉入此攻擊行動。

網路上的知識：後滲透 (Post-exploitation) 是網路攻擊的後期階段，發生在成功入侵目標系統或網路之後。在這一階段，重點是進行一系列後續操作，目的是加強攻擊者在系統中的地位、擴大存取範圍、竊取敏感資料、植入後門，或為未來的攻擊活動做準備。後滲透的活動可能包括提權、橫向移動、存取敏感資料、維持存取權限等，與初步入侵階段不同，後滲透更側重於利用已經獲得存取權限來達成攻擊者的目標。

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.Mshta-Http!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-SvcReg!g1
- ACM.Ps-RgPst!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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- CL.Downloader!gen128
- Trojan.Mdropper
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Reputation.1

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。

2024/10/16

Meduza惡意竊密程式

研究人員最近針對 Telegram 帳戶「@reserveplusbot」發佈警告，該帳戶與特定應用程式相連，並作為技術支援的聯絡人。這些可疑訊息引誘使用者安裝一個包含惡意軟體的 ZIP 壓縮檔案。裡面可執行檔案是 Meduza 惡意竊密程式，它會竊取檔案，並透過修改 Microsoft Defender 設定來規避偵測。

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-Base64!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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：

- 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.B
- 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。

2024/10/16

自動櫃員機(ATM)／收銀機(PoS)的車手～發現FASTCash惡意軟體在Linux平台上的新變種

FASTCash 惡意軟體 (美國網路安全暨基礎設施安全局 (CISA)) 認為是北韓製造的駭客工具在 Linux 平台上的新變種已被發現。FASTCash 會植入受攻擊的網路，並利用此惡意軟體執行未經授權的銀行交易。此惡意軟體會攔截交易訊息，並產生詐騙回應，會攔截、操縱自動櫃員機 (ATM)／收銀機 (PoS) 等支付卡及信用卡交易訊息。

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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2024/10/16

CVE-2024-44849--存在Qualitor特定版本的遠端執行程式碼(RCE)漏洞

CVE-2024-44849 是 Qualitor 的一個重要 (CVSS：9.8) 遠端執行程式碼 (RCE) 漏洞，Qualitor 是一個管理客戶服務流程和集中化服務的平台。在 8.24 之前的 Qualitor 版本中，此漏洞可透過任意檔案上傳遠端執行程式碼 (RCE)。若遭開採濫用，此漏洞可能會讓遠端攻擊者控制主機系統，可能導致系統完全被接管。賽門鐵克的網路防護技術入侵防禦系統 (IPS) 會阻止這些漏洞利用嘗試，以防止系統受到進一步感染／損害。

網路上的知識：Qualitor 是專注在提供 IT 服務管理 (ITSM) 的 B2B 公司。

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: Qualitor RCE Vulnerability CVE-2024-44849

2024/10/16

ThunderKitty惡意軟體

ThunderKitty 是一種源於開放原始碼採用 GO 語言撰寫的惡意竊密程式，已經在真實網路情境中出沒。該惡意軟體具有從遭感染的電腦收集各種資訊的功能，包括銀行詳細資訊、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密)、Cookie、瀏覽器歷史紀錄和瀏覽器中存儲的其他資料等。ThunderKitty 建置諸多逃避和反分析技術，包括偵測虛擬機器環境和偵錯程式 (Debugger) 的存在，並具有持久性／常駐能力的機制。

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-Reg!g1
- ACM.Untrst-Csc!g1
- ACM.Untrst-RunSys!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：

- Infostealer
- ISB.Malscript!gen9
- Trojan Horse

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

2024/10/16

CVE-2024-45519--存在Zimbra Collaboration Suite(ZCS)的遠端程式碼執行(RCE)漏洞

CVE-2024-45519 是最近被揭露存在 Zimbra Collaboration Suite(ZCS) 的遠端程式碼執行 (RCE) 漏洞，影響 8.8.15 Patch 46 之前的版本、9.0.0 Patch 41 之前的版本、10.0.9 之前的版本，以及 10.1.1 之前的版本。此漏洞源於使用者輸入認證失敗，如果成功利用此漏洞，未經認證的攻擊者可能會在受影響的 Zimbra 安裝過程中執行任意程式碼。

網路上的知識：Zimbra Collaboration Suite 為企業級的協作軟體，可用來管理電子郵件、行事曆、聯絡人、任務或文件共享。

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: Zimbra Collaboration Suite CVE-2024-45519

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，其出廠就內建的 sym_unix_protection_sbp 強化政策已內建的最少權限、最低資源限縮的沙箱運行環境，可以防止未經授權的指令執行。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/15

INTERLOCK勒索軟體

最近在威脅領域中出現一個全新的勒索軟體駭客組織，被稱為 INTERLOCK。該駭客組織似乎採取雙重勒索策略。成功入侵後，加密檔案會被冠上「.interlock」的副檔名。

留置的勒索贖金支付說明告誡受害者，他們的組織已遭受重大的資安危害。重要檔案已被加密，敏感資料已被竊取。勒索贖金支付說明提供使用唯一的公司 ID，透過 TOR 網路上的安全匿名平台與威脅者聯繫的指示。警告受害者不要更改檔案、使用復原軟體或重新開機系統，因為這些行為可能會導致後續無法逆轉的損害。

該說明咄咄逼人、苦苦相逼：在 96 小時內，被竊資料會公諸於世包含競爭對手和監管機構，可能會造成嚴重的財務損失和聲譽損失，倍增乖乖就範的壓力。

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。

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g7
- SONAR.Ransomware!g16

檔案型(基於回應式樣本的病毒定義檔)防護：

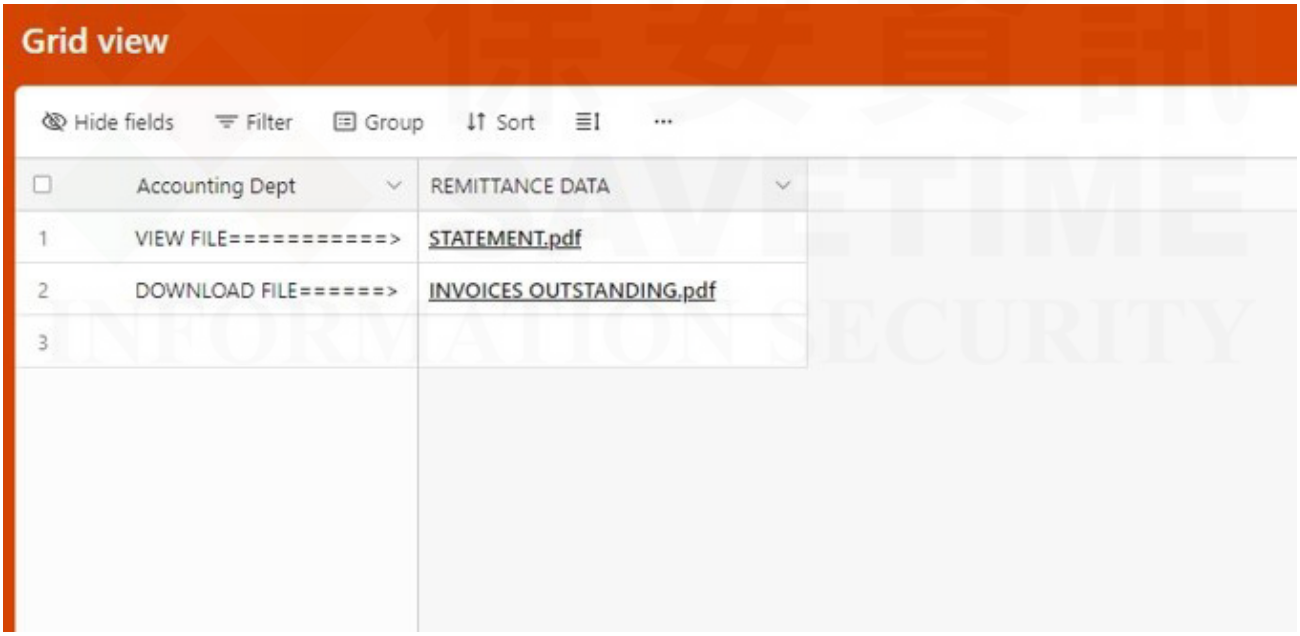
- Trojan.Gen.MBT

2024/10/15

防護亮點：賽門鐵克的網頁生態即時分類系統--WebPulse持續偵測到唯妙唯肖的釣魚、詐騙網站

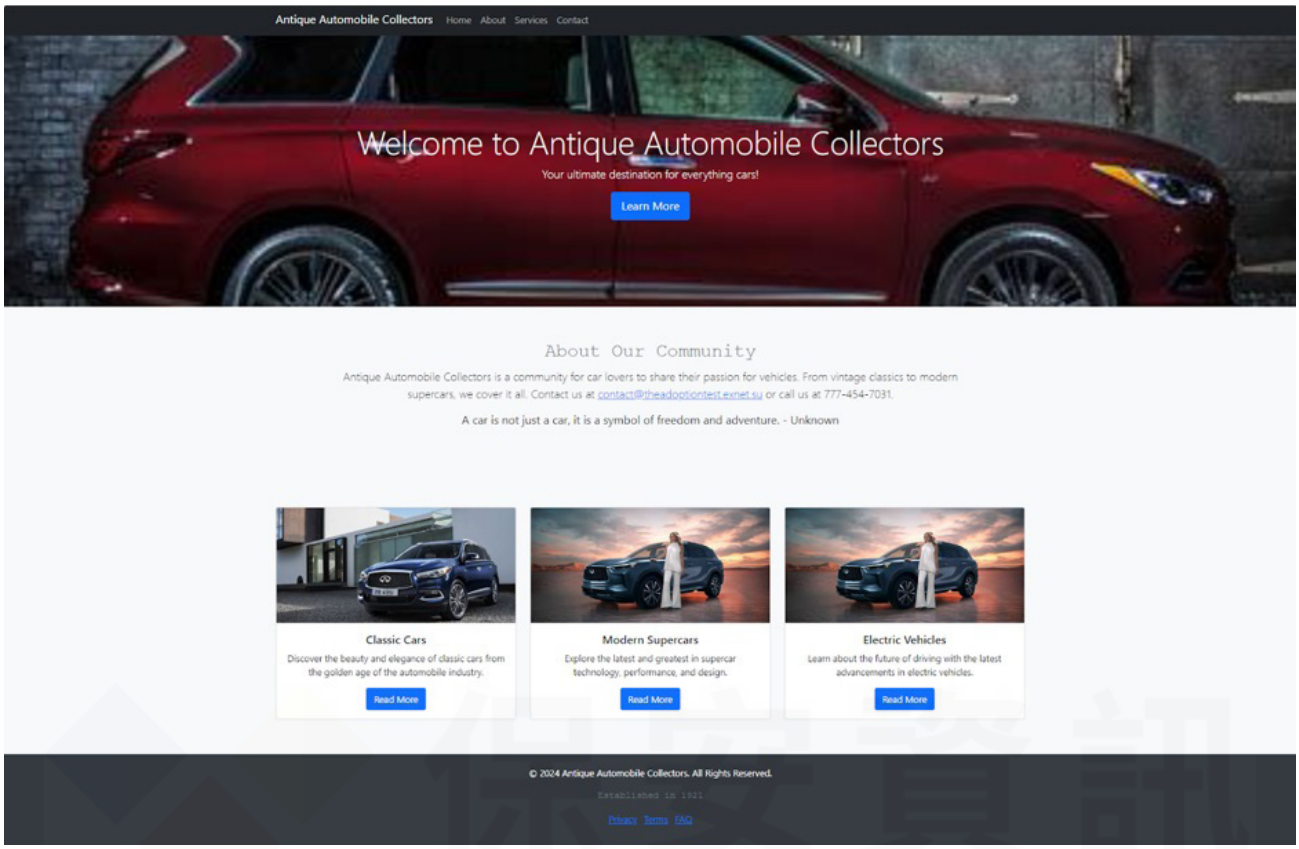
賽門鐵克的網頁生態即時分類系統--WebPulse 持續偵測到可能來自俄羅斯 Microsoft Outlook 主題網路釣魚活動的內容。惡意網域名稱及遭濫用網際網路服務上的某些子網域 (例如：page[.]dev 和r2[.]dev) 傳回的內容包含指向其他網域的連接，這些網域傳回 Microsoft Outlook 的偽裝內容，然後該內容被有關汽車收藏的引誘內容所取代。

例如：hxxps://airtable[.]com/appCFZIhXR4xkRsBW/shrBlLd0rIPEHc6VC/tblHMgIOgYgGhRnt2 傳回以下內容：

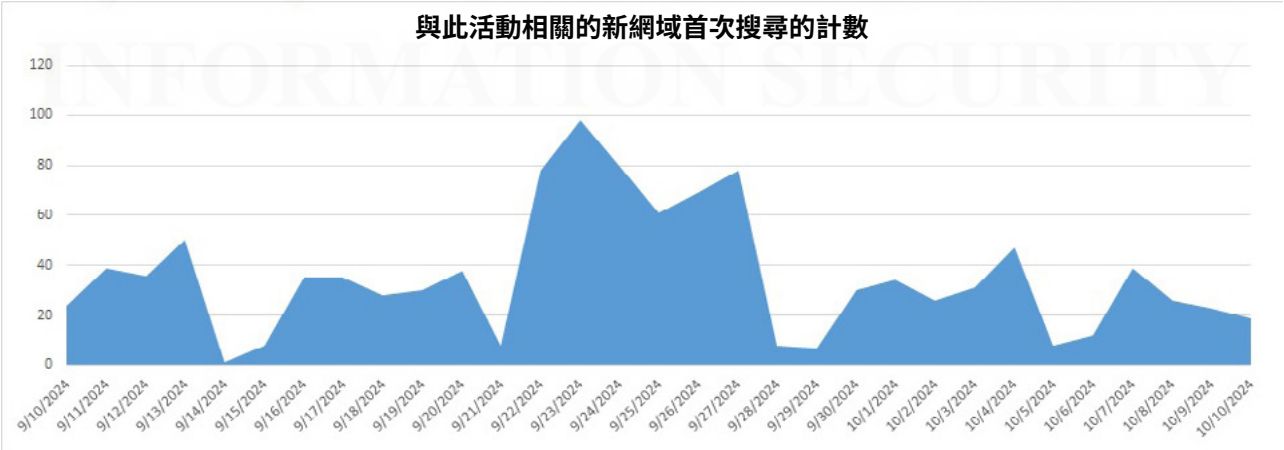


兩個 .pdf 檔名都會連結到 hxxps://shopzingr[.]bir[.]ru/eXgHl/，該鏈結隱藏在 CLOUDFLARE 的「CAPTCHA」辨認人類與機器人的驗證系統驗證碼複選框後面。勾選該方塊後，會短暫顯示此 Microsoft Outlook 圖示：

然後它會被一個有關汽車收藏的詐騙網站所取代。在此範例中，詐騙網站的標題是『Antique Automobile Collectors*古董車收藏網站』並顯示以下內容：



WebPulse 偵測到此活動並即時回應到 WebPulse 的網頁分類平台並歸為釣魚網頁。自 2024 年 9 月 10 日到 10 月 10 日，WebPulse 偵測到 1,106 個獨立網域。下圖顯示與此活動相關的新網域首次搜尋的計數：



獨立的網域使用以下 TLD／ccTLD (註：頂級網域／國家或地區的頂級網域)：

- .ru (520)
- .com (102) (註：包括 sa[.]com 和 za[.]com 上託管的許多子網域)
- .dev (86) (註：主要被濫用的pages[.]dev 和r2[.]dev 服務)
- .site (72)
- .pl (69)
- .de (58)
- .id (32)

- .shop (25)
- .moscow (25)
- .su (24) (註：莫斯科地區的網域名稱)
- .pro (22)
- .sbs (13)
- .uk (12)
- .top (10)
- .buzz (8)
- .cyou (7)
- .online (6)
- .store (4)
- .space (3)
- .ua (2)
- .me (2)
- .art (2)
- .hu (1)
- .cfd (1)

偵測到的網域範例包括：

Domains／網域

- 0700ihrenummer[.]msk[.]ru
- 1349653976[.]my[.]id
- bytevault[.]com[.]de
- bytevault[.]ru
- cloudcogmputing[.]ru
- digitalbuzztechmo[.]ru
- digitalgroovetechieno[.]shop
- enterlifegrooved[.]com[.]pl
- entertaintechtrendsro[.]ru
- fggiggle[.]site
- gadgetgroovees[.]shop
- payment-to-your-bank-urska-zupanc-lasic-hidrotehnik-si[.]dynamictooilngsolutionsinc[.]com
- pulsesagego[.]top
- quickbooksboose[.]ru
- techlifegrooveeo[.]ru
- trenddigitalgadgetcx[.]ru

遭濫用服務的子網域

- 11299onedrive84899nhfhjke3hdhhdd[.]pages[.]dev
- accessdocumentfile[.]pages[.]dev

- aldkdlkdkdkdkdldlkdljdkskdjsdjsnmdkskddskdkekdksdk[.]pages[.]dev
- fsafacbcvbcxbdsfafafsf[.]pages[.]dev
- graves-construction-llc[.]pages[.]dev
- lively-crystal-reward[.]glitch[.]me
- pagemicrorofimicrsftonininecheckverf-portal-secure-logon[.]us-east-1[.]linodeobjects[.]com
- pub-80ebf6b7d8e54c738b0717427e3e131c[.]r2[.]dev
- pub-e0deb07b5eea4ed5b7ab525b4d87d2a8[.]r2[.]dev
- sharepointrickdirkse[.]pages[.]dev
- sj84848383voicena0mprdooooprodoutlookcommmailpppprotection[.]pages[.]dev

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)。

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路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2024/10/15

使用SHTML格式的附件檔發動網路釣魚行動，方興未艾

賽門鐵克最近發現一種新的網路釣魚行動，使用偽裝成進口報單或付款表單 SHTML 格式的附件檔。這些訊息試圖引誘使用者開啟附件檔案，以解決進口或帳單問題。如果收件者打開附件檔，就會出現偽造的「DHL」登入頁面，並將輸入的憑證滲出到私人 Telegram 頻道，供攻擊者稍後使用。

附件檔名範例

- Original Delivery Document & payment receipt.(7.3KB).(9.3KB).shtml *原始交貨文件及付款收據.(7.3KB).(9.3KB).shtml
- Import Declaration form.(9.3KB).shtml *進口申報表.(9.3KB).shtml
- [recpient address]-swift-inv002133.html [*收件人地址]-swift-inv002133.html

網路上的知識：shtml 是一種用於 SSI(Server Side Include，包含服務器端) 技術的文件，是 WEB 在服務器提供的一種功能，並且在服務器端執行。

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：

- Phish.ScrTgHtml!gen1
- Phish.ScrTgHtml!gen3

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)。

2024/10/15

MiyaRat：來自Bitter進階持續威脅(APT)駭客集團的最新駭客工具

Bitter 進階持續威脅 (APT) 駭客集團因針對東亞和南亞進行複雜的網路間諜活動而聞名，據觀察，該駭客集團部署一種名為 MiyaRat 的全新型惡意軟體。此惡意軟體能夠收集系統資訊、擷取螢幕截圖、執行檔案上傳與下載，並將資料滲出到其指揮與控制 (C&C)，以等待後續進一步的指示。

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：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.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.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.D

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。

2024/10/15

開源網路性能和故障管理框架：Cacti存在CVE-2024-43363遠端程式碼執行(RCE)漏洞

CVE-2024-43363 是開源網路性能和故障管理框架：Cacti 存在的遠端程式碼執行 (RCE) 漏洞。成功開採濫用此漏洞的方法是在受影響實例上進行日誌中毒。此漏洞最終可讓攻擊者執行任意指令。此漏洞已在 1.2.28 或更新的版本的中已修補。

網路上的知識：日誌中毒是一種網路攻擊，威脅份子利用系統的日誌檔來掩蓋其活動或執行惡意程式碼。

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: Cacti RCE Vulnerability CVE-2024-43363

2024/10/15

拆解部署Lumma Stealer惡意竊密程式的攻擊行動中，發現HijackLoader惡意程式載入器居然帶有合法的簽章

一起惡意軟體行動被觀察到採用 HijackLoader 來部署 Lumma Stealer 惡意竊密程式。攻擊手段使用「偽造的 CAPTCHA」來引誘使用者執行 PowerShell 類型的有效酬載來下載包含 DLL 或具簽章的 HijackLoader 的 .ZIP 壓縮檔。然後透過 DLL側載來載入此二進位檔案，最終安裝 Lumma Stealer 惡意竊密程式。惡意軟體濫用多個憑證公司簽發的憑證，這些憑證都是從不同的憑證簽發單位取得，這些機關基本上都是自動化，只需要一個有效的公司註冊號碼和聯絡人。

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-Java!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A

- 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。

2024/10/15

CoreWarrior惡意軟體

研究人員調查一款名為 CoreWarrior 的惡意軟體，發現此變種透過建立無數複本、連線至各個 IP 位址、開啟多個後門存取點，以及截取 Windows UI 元件以達到監控目的，大肆進行傳播。

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：

- Hacktool.Flooder
- SMG.Heur!gen
- 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

2024/10/15

Core Werewolf駭客集團採用新的駭客工具：AutoIt類型惡意程式載入器和Telegram發動網路攻擊

主要針對俄羅斯國防產業和關鍵基礎設施的 Core Werewolf 進階持續威脅 (APT) 駭客集團，已被發現到採用新的駭客工具，包括 AutoIt 腳本語言類型的惡意程式載入器，並透過 Telegram 傳送惡意檔案。作為攻擊鏈的一部分，他們利用包含 SFX 可執行檔的 RAR 壓縮檔來部署經混淆 AutoIt 腳本、合法的 AutoIt 解譯器和誘騙 PDF 文件檔。該惡意程式載入器會收集系統資訊、加密和傳輸檔案，並與指令控制伺服器 (C&C) 通訊以進行資料外洩。為了逃避偵測，攻擊者使用與誘餌文件內容相符的欺騙性檔案名稱。

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.SuspLaunch!g444

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：

- Trojan Horse
- Trojan.Gen.MBT
- 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。

2024/10/14

ErrorFather：安卓平台上的手機／行動裝置木馬程式

Cerberus 是在 2019 年曝光安卓平台上的手機／行動裝置木馬程式，其後繼新變種利用多階段植入程式來部署其有效酬載，並可透過遠端攻擊、鍵盤側錄和覆蓋策略來執行金融詐騙。ErrorFather 出現突顯出重新改造惡意軟體的威脅持續存在，因為網路罪犯在最初 Cerberus 惡意軟體問世的多年後，仍持續重新改造遭洩漏的原始碼。

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：

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

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

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。

2024/10/14

Demodex惡意軟體持續涉入針對美國電信供應商的網路攻擊

根據報導，進階持續威脅 (APT) 駭客組織--「Squash」正在利用 Demodex 惡意軟體，針對美國電信供應商，發動網路攻擊。Demodex 是一種用來建立持久性／常駐能力的 rootkit，再用帶有虛假檔案標頭 (已發現到 PNG、JPEG 和 WAV) 的檔案來協助躲避偵測，並用來建立 C&C 通訊。

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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

2024/10/14

CVE-2024-43573--存在微軟視窗環境的MSHTML平臺欺騙漏洞

CVE-2024-43573 是存在微軟視窗環境的 MSHTML 平臺欺騙漏洞，最近被披露並已在微軟發布的 10 月例行更新 (Patch Tuesday) 中推出修補程式。此漏洞會影響 Microsoft Windows MSHTML 平台。此漏洞的 CVSS 風險評分 6.5 (中度)，攻擊者可在運行受影響應用程式的情境中執行任意程式碼。CVE-2024-43573 漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，之前也曾有報告指出有人在真實網路情境上大肆開採濫用此漏洞。

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：

- Web Attack: Windows MSHTML Platform CVE-2024-43573

基於安全強化政策(適用於使用DCS)：

針對此漏洞提供如下的多層級保護：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，可以對 Microsoft Internet

Explorer 的預設強化提供針對 CVE-2024-43573 的零時差防護。在預設強化政策中，所有向外連線都會被封鎖。

- 套用於 Microsoft IE 的 DCS 沙箱可防止下載任何惡意有效酬載或執行任意程序。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/14

全新Pronsis惡意程式載入器，涉入傳遞Lumma惡意竊密程式和Latrodectus有效酬載荷的網路攻擊行動中嶄露頭角

全新 Pronsis 惡意程式載入器，最近在涉入傳遞 Lumma 惡意竊密程式和 Latrodectus 有效酬載荷的網路攻擊行動中嶄露頭角。Pronsis 是採用 JPHP 程式語言編譯的可執行檔，這是 PHP 的 Java 實作。已發現的攻擊事件中發現，Pronsis 也使用 Nullsoft Scriptable Install System (NSIS) 來部署。該惡意軟體具有多種偵測規避技術，例如：從 Windows Defender 掃描中排除使用者設定檔目錄路徑。

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-FlPst!g1
- ACM.Ps-Java!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspRename!g4
- SONAR.TCP!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：

- Trojan Horse
- MSIL.Downloader!gen8
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Startpage
- W32.Silly!gen
- 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：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/10/11

LemonDuck：越來越大尾的多平臺挖礦惡意軟體

LemonDuck 是一款知名的挖掘惡意軟體，已演變成多平台威脅，且被發現到利用 SMB 漏洞作為其攻擊媒介的一部分，尤其是 EternalBlue，以取得網路存取權限。該惡意軟體採用的技術包括暴力攻擊、建立隱藏的管理共用，以及透過批次檔案和 PowerShell 腳本執行惡意動作。LemonDuck 具備建立排程任務、停用 Windows Defender，以及利用反偵測機制持續作業的能力。它會偽裝成合法的系統服務，操控防火牆設定，此外還會使用密碼提取工具：Mimikatz 來盜取憑證。

網路上的知識：EternalBlue 是一個 Windows Server Message Block(SMB) 協議中的漏洞，該漏洞允許攻擊者在無需用戶交互的情況下，遠端執行任意代碼。開採濫用 EternalBlue 漏洞，攻擊者可以輕鬆地在未修補的 Windows 系統上植入惡意程式碼，並進一步擴散到網路中其他設備。

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.Wscr-Cmd!g1
- ACM.Wscr-Ps!g1
- ACM.Wscr-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g393

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
- Remacc.Remadmin
- CL.Downloader!gen9
- WS.Malware.2

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: Impacket Tool Activity
- Audit: RADMIN Tool Activity
- Audit: Powershell Base64 Script Execution 02

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。

2024/10/11

CVE-2024-7954--存在SPIP Porte Plume外掛程式的遠端執行程式碼漏洞

CVE-2024-7954 是存在 SPIP 4.30-alpha2、4.2.13 及 4.1.16 之前版本所使用 porte_plume 外掛程式中的遠端執行程式碼 (RCE) 嚴重等級 (CVSS 風險評分：9.8) 的漏洞。SPIP 是用於發布內容管理系統 (CMS) 網站的免費軟體。此漏洞可能會允許未認證的遠端攻擊者傳送特製 HTTP 請求，並以 SPIP 使用者身份執行任意 PHP 程式碼。此攻擊可完全入侵伺服器以竊取機密資訊，並轉向內部網路。賽門鐵克端點防護的多層防護技術之一網路層防護技術的入侵防護系統 (IPS) 可阻止這些漏洞利用嘗試，以防止系統受到進一步感染／損害。

網路上的知識：SPIP 是一種用於網際網路的發佈系統，非常重視協作工作、多語言環境以及網頁作者的簡易使用。它是自由軟體，根據 GNU／GPL 許可證分發。

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: SPIP Porte Plume Plugin RCE Vulnerability CVE-2024-7954

2024/10/11

Lynx勒索軟體--讓人毛骨悚然的網路勒索威脅

Palo Alto Networks Unit 42 發表最新研究指出，被稱為 Lynx 勒索軟體最新變種與 INC 勒索軟體共用大部分的原始碼。Lynx 營運商已積極鎖定美國和英國的各行各業 (建築、房地產、零售和金融／環境服務) 的組織為目標。此勒索軟體採勒索軟體即服務 (RaaS) 的營運模式，並透過各種攻擊媒介 (欺騙性的釣魚郵件、感染使用者系統的惡意下載以及駭客論壇等) 散播。一旦感染 Lynx 勒索軟體，受害者的資料會在加密前先被滲出，然後採用雙重勒索的戰術來脅迫受害者以提高就範率。

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.RansomPlay!gen1
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.Ransomware!g38
- SONAR.Ransom!gen14
- SONAR.Ransom!gen98

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：

- Trojan.Gen.MBT
- Ransom.Gen
- Ransom.Inc
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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

- 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。

2024/10/11

CVE-2024-43572--存在微軟Windows管理主控臺(MMC)的遠端執行程式碼(RCE)類型的漏洞

CVE-2024-43572 是存在微軟 Windows 管理主控臺 (MMC) 遠端執行程式碼 (RCE) 類型的漏洞，最近被披露並已在微軟發布的 10 月例行更新 (Patch Tuesday) 中推出修補程式。此漏洞可透過執行特製的惡意 Microsoft Saved Console (MSC) 檔案利用。成功開採濫用此漏洞可讓攻擊者在執行應用程式的情境執行任意程式碼。CVE-2024-43572 漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中 ，之前也曾有報告指出有人在真實網路情境上大肆開採濫用此漏洞。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLoad!g65

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Suspexec!gen50
- Trojan Horse

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。

2024/10/11

Apache RocketMQ的已知漏洞CVE-2023-33246，已被Perfctl惡意軟體開採濫用以攻擊全球Linux伺服器

已發現到針對全球數百萬台 Linux 伺服器的 Perfctl 惡意軟體攻擊行動。該行動開採濫用分散式訊息串流資料平臺 Apache RocketMQ 的已知漏洞 CVE-2023-33246。該惡意軟體利用 rootkits 進行隱身和程序偽裝，並利用洋蔥路由器加密通訊 (TOR) 與命令和控制 (C&C) 伺服器通訊。最終有效酬載，是部署挖礦程式和代理劫持軟體。此外，惡意軟體利用暫存目錄和修改過的系統公用程式來逃避偵測。

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：

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：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- PUA.Gen.2
- WS.Malware.2

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: RocketMQ RCE CVE-2023-33246

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。

2024/10/11

偽裝成《Honkai：Star Rail／*崩壞：星穹鐵道》的安裝程式～Kransom勒索軟體以遊戲玩家為目標

有報告指出，一款名為 Kransom 的全新勒索軟體正在利用《Honkai: Star Rail／*崩壞：星穹鐵道》這款受歡迎的多平台銀河冒險角色扮演遊戲。該勒索軟體透過隨機下載行動進行傳播，將惡意的二進位檔偽裝成合法的 Star Rail 遊戲安裝程式，且使用有效的數位憑證，進而誘騙受害者。執行時，惡意 DLL 會使用動態連結庫 (DLL) 側載技術載入，啟動勒索軟體的加密程序。

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：

- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1
- WS.Reputation.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.B
- 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。

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**。