保安資訊--本周(台灣時間2024/12/20)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 38 萬 4,300 台受保護端點上總共阻止了 4,380 萬次攻擊。這些攻擊中有 76.9% 在感染階段前就被有效阻止：**(2024/12/16)**

- 在**8萬3,500**台端點上，阻止了**1260**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬8,400**台端點上，阻止了**760**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,800**台**Windows**伺服主機上，阻止了**6萬4,000**次攻擊。
- 在**4萬8,500**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬200**台端點上，阻止了**73萬8,500**次嘗試掃描在**CMS**漏洞。
- 在**3萬9,500**台端點上，阻止了**230**萬次嘗試利用的應用程式漏洞。
- 在**8萬5,000**台端點上，阻止了**160**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,600**台端點上，阻止了**93萬6,200**次加密貨幣挖礦攻擊。
- 在**10萬3,600**台端點上，阻止了**940**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**484**台端點上，阻止了**8萬1,500**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 1,500 個受保護端點上阻止了總計 690 萬次攻擊。**(2024/12/16)**

- 使用網頁信譽情資，在 **182.3K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **19.6K** 個端點上 **250.9K** 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 **8.2K** 個端點上攔截 **170.1K** 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 **250** 個端點上攔截 **6.1K** 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。

2024/12/19
Bitter駭客集團正在使用MiyaRAT惡意軟體發動攻擊

駭客集團「Bitter」被發現到正在使用 MiyaRAT 惡意軟體，針對土耳其的國防單位進行攻擊。初始攻擊啟於一封含有外國投資專案的誘餌電子郵件，並夾帶一個包含偽裝 PDF 檔案的 RAR 壓縮檔。開啟偽裝檔案會觸發執行隱藏的 PowerShell 程式碼，並執行惡意的 curl 指令來下載額外的有效酬載、執行網路偵測或竊取資料。

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：

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

- 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.B
- Heur.AdvML.B!200
- Heur.AdvML.C
- Heur.AdvML.D

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：

- System Infected: Trojan.Backdoor Activity 634

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。

2024/12/19

進階持續威脅(APT)駭客集團：Fritillary發動惡意RDP攻擊

Fritillary 進階持續威脅 (APT) 駭客集團 (又稱 Earth Koshchei、APT29、Nobelium) 一直以來擅於利用惡意 RDP(Remote Desktop Protocol，遠端桌面協定) 二進位檔案從事惡意活動，以獲得未經授權存取的目標環境。這次攻擊行動最初是在 2024 年 10 月底左右被發現。威脅者利用魚叉式網路釣魚電子郵件散佈惡意 RDP 檔案，並啟動受害者連線至攻擊者控制的 RDP 中繼站。以這種方式取得受害者環境的存取權，可讓攻擊者收集和滲透敏感的使用者資料。

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：

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：

- Infostealer
- Trojan Horse
- Trojan.Gen.MBT

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。

2024/12/19

使用虛擬化程式碼自我保護的全新惡意程式載入器：RiseLoader

RiseLoader 是在真實網路情境中發現的全新惡意程式載入器。它與另一個稱為 RisePro 惡意軟體家族在通訊協定的使用上有某些相似之處。入侵目標端點後，RiseLoaders 主要功能是下載和執行第二階段的任意有效酬載。此惡意軟體使用虛擬化程式碼的防盜版軟體保護程式：VMProtect 進行混淆，據報導會散佈各種有效酬載，例如：Lumma、Vidar、StealC……等惡意竊密程式或 XMRig 挖礦程式。

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-Sc!g1
- ACM.Rgasm-Lnch!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen803
- SONAR.SuspBeh!gen804
- SONAR.SuspDriver!gen1
- SONAR.SuspLaunch!g221
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- 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!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
- 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。

2024/12/18

DXL～新秀雖不亮眼，但惡意竊密軟體該有的功能一樣也沒少

DXL Stealer 是一款在真實網路情境中被新發現的尋常惡意竊密軟體。其初始有效酬載以 PyInstaller 可執行檔的形式出現，並具有從受攻擊的端點收集和滲出各種使用者資料的進階功能。所收集的資訊包括憑證、儲存的 Wifi 密碼、加密貨幣錢包、cookies、瀏覽器歷史和自動填寫資料、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密)、來自各種第三方應用程式 (Steam、Uplay、Telegram) 的會話檔案 (Session files) 等。其他功能可讓惡意軟體收集剪貼簿資料、擷取螢幕截圖或從網路攝影機拍攝影像。攻擊者可借助 Telegram 機器人或透過 Discord webhooks 擷取竊取的資料。

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.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：

- Scr.Malcode!gen129
- 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。

2024/12/18

Cleo軟體漏洞CVE-2024-50623 & CVE-2024-55956遭威脅份子利用進行零時差攻擊

最近披露的兩個漏洞 CVE-2024-50623 和 CVE-2024-55956 已遭威脅者開採濫用於系列的零時差攻擊，包括一些由 Clop 勒索軟體駭客集團發動的攻擊。這些漏洞影響數個 Cleo 軟體解決方案，包括 Cleo Harmony、Cleo VLTrader 和 Cleo LexiCom。CVE-2024-50623 和 CVE-2024-55956 都是未經認證的檔案寫入漏洞。如果成功開採濫用此漏洞，可能導致遠端程式碼執行，並將惡意的有效酬載傳送至受攻擊的機器。CVE-2024-50623 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: Cleo Software CVE-2024-50623

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，DCS 的網路規則政策可設定為，將 Cleo 應用程式限制為受信任的用戶端。
- DCS 預防政策可防止任何 JAR webshell 的下載和執行。這主要是透過控制可以寫入檔案的位置，以及可以在 java scripts 執行的沙箱上強制限縮執行哪些指令來達成。

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。

2024/12/18

全新型惡意軟體載入程式：PSLoramyra

PSLoramyra 是一款新發現的進階惡意軟體載入程式。PSLoramyra 可利用各種腳本 (PS1、VBS、BAT) 將惡意有效酬載注入受攻擊的系統，並直接在記憶體中執行。該惡意軟體還能夠利用 Windows 的工作排程，在系統上建立持久性／常駐能力。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!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：

- Scr.Malcode!gen
- Trojan Horse
- 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。

2024/12/18

Remcos遠端存取木馬(RAT)出現新變種

Remcos 本來是用於遠端控制和監控的良善商業軟體 (Remcos來自於 Remote Control and Surveillance 的縮寫)，因為功能強大，被不安好心的有心份子武器化後，成為惡名昭彰的遠端存取木馬 (RAT) 代名詞，多年來一直相對活躍。最近，有兩款不同的 Remcos RAT 最新變種以獨特創新的傳送和執行方式，讓他們一躍成為威脅生態圈的當紅炸子雞。此惡意軟體透過釣魚電子郵件和惡意附件傳送，讓攻擊者能夠遠端控制受感染的機器、竊取資料並進行間諜活動。第一個變種透過包含惡意 Microsoft Office Open XML (DOCX) 附件的垃圾郵件傳播，濫用老舊的遠端程式碼執行漏洞 (CVE-2017-11882)。第二個變種會執行 VBS 檔案，觸發高度混淆的 PowerShell 指令碼，從 C&C 伺服器下載多個檔案，並將惡意程式碼注入合法的 Microsoft 可執行檔。兩個變種都有幾個共同的特徵。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g20
- SONAR.Powershell!g85
- SONAR.PsEmpire!gen8

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：

- Bloodhound.RTF.*
- CL.Downloader!gen11
- CL.Downloader!aat171
- Exp.CVE-2017-11882!g*
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Scr.Malcode!gen*
- 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

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。

2024/12/17
防護亮點：賽門鐵克EDR，有效應對日益增多的安全軟體殺手工具 (AV/EDR Killers)

駭客瞄準含有漏洞的的系統驅動程式

資安防護軟體可防止敵人執行惡意動作來達成他們的目標。但現在，攻擊者無所不用其極地妨礙資安防禦機制，通常是採取濫用含有漏洞的驅動程式來取得核心層級 (kernel level) 的存取權限。攻擊者在系統中植入含有漏洞的易受攻擊的驅動程式，然後利用它來移除或停用資安防護軟體，以便在不被中斷或被偵測到的情況下進行惡意動作。越來越多浮上檯面的開放原始碼工具都是利用這樣的技術，導致人們對其使用和影響的意識提高。

這種威脅態勢也突顯出這類工具日益老練狡猾，從勒索軟體調查中獲得的證據顯示，濫用常用應用程式中已經被公開揭露的已知漏洞，是目前嘗試滲透客戶環境的勒索軟體攻擊的主要媒介。勒索軟體攻擊者部署的工具數量持續增加，利用「自帶含有漏洞的驅動程式」(bring-your-own-vulnerable-driver，簡稱 BYOVD) 伎倆的工具目前在駭客圈廣受歡迎。

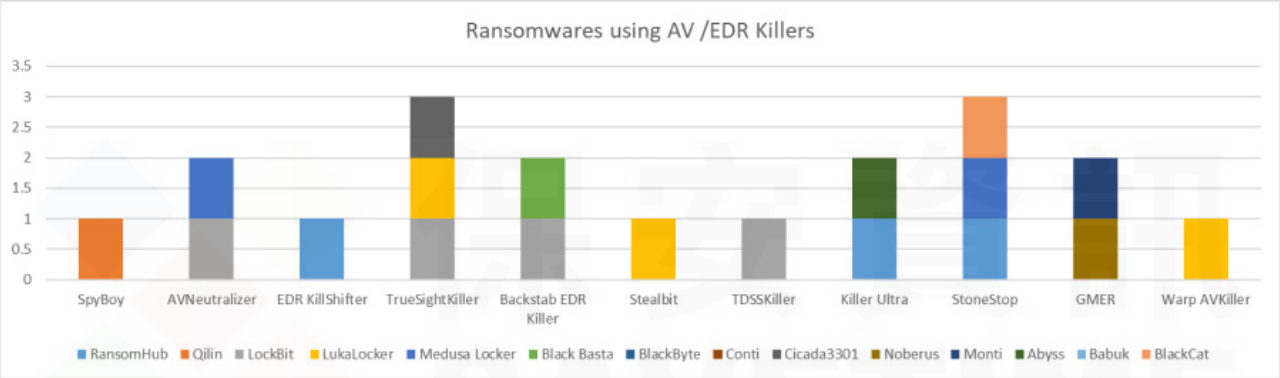
使用安全軟體殺手工具(AV／EDR Killers)癱瘓防禦能力的案例激增

威脅者濫用 BYOVD 攻擊技術，部署合法簽署且可成功載入 Windows 系統的驅動程式。這些易受攻擊的驅動程式賦予攻擊者從特權位置在核心情境中執行攻擊者提供程式碼的能力。

以下是常見的安全軟體殺手工具 (AV／EDR Killers)：

- AV-Neutralizer／AUKill：此工具濫用老舊版本的 Process Explorer 驅動程式。
- EDR KillShifter：此工具會執行自備脆弱驅動程式 (BYOVD) 攻擊。
- Terminator EDR Killer (SpyBoy) and Killer Ultra：這些工具開採濫用 CVE-2024-1853 漏洞，透過使用易受攻擊的 Zemana AntiLogger 驅動程式來停用目標系統上的安全解決方案。
- TDSSKiller：這是卡巴斯基的合法工具，用於嘗試停用目標系統上的端點偵測與回應(EDR)服務。
- StoneStop：此工具使用惡意的 PoorTry 核心模式的 Windows 驅動程式。
- StealBit：與勒索軟體攻擊鏈相關的自訂資料外洩工具。
- GMER：這是一款相對較舊的 rootkit 掃描程式，駭客可利用它來停用執行緒。
- Warp AVKiller：此工具利用易受攻擊的 Avira 的 anti-rootkit 驅動程式來停用安全產品。

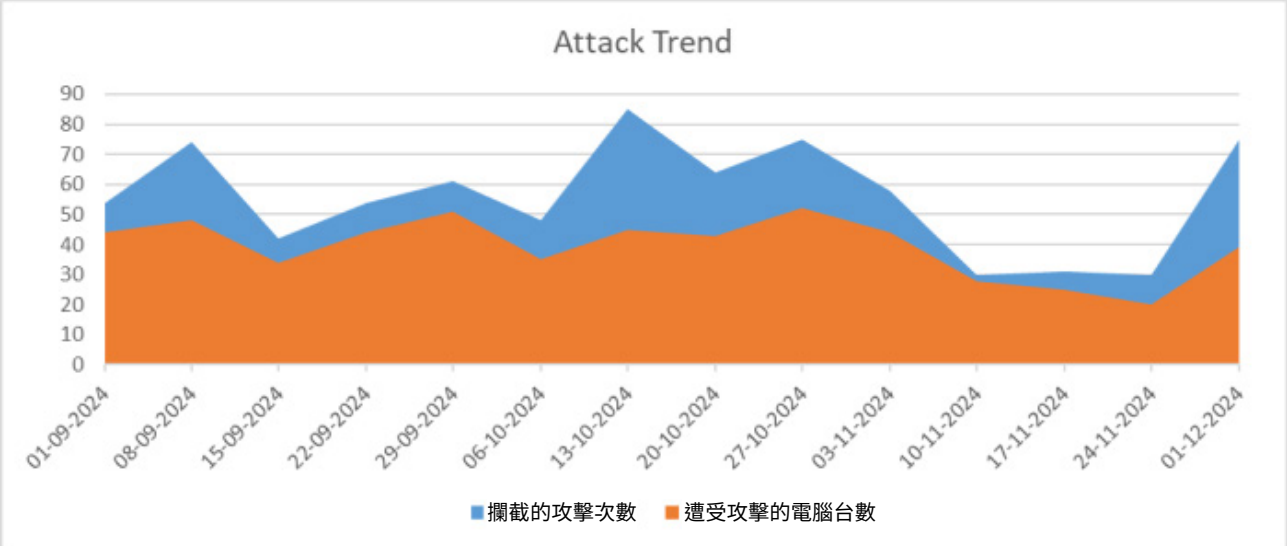
已有許多安全軟體殺手工具(AV/EDR Killers)涉入勒索軟體攻擊鏈



力抗安全軟體殺手工具(AV/EDR Killers)只是賽門鐵克端點偵測與回應(EDR)的效益之一

賽門鐵克端點偵測與回應 (EDR) 能力抗安全軟體殺手工具 (AV／EDR Killers)，保護客戶免受威脅，並在建立事件的同時產生警示。賽門鐵克 EDR 使用機器學習和行為分析來偵測和揭露可疑的網路活動。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以快速進行分類處理，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。

使用安全軟體殺手工具(AV/EDR Killers)癱瘓防禦能力的案日益增多



威脅獵捕查詢

請點擊此處，以檢視 GitHub 上 Symantec EDR 相關的威脅獵捕查詢。
欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

2024/12/17

全新惡意竊密程式：Bizfum，已在真實網路情境造成干擾

Bizfum 是在真實網路情境發現一款採用 C 語言撰寫的全新惡意竊密程式。此惡意軟體目標是從受感染的端點滲出各種資料。竊取的資料可能包括憑證、網頁瀏覽器中的檔案、cookie、瀏覽歷史紀錄、剪貼簿資料、使用者檔案、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密) 等。得力於 Telegram 殭屍的協助下，收集到的資料會被壓縮並滲出回傳給攻擊者。

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.Stealer!gen1
- SONAR.MalTraffic!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：

- Infostealer

基於機器學習的防禦技術：

- 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：

- System Infected: Trojan.Backdoor Activity 654
- System Infected: Trojan.Backdoor Activity 721
- System Infected: Trojan.Backdoor Activity 753

2024/12/13

印度出現一種全新安卓平台上的手機／行動裝置上的銀行金融木馬程式

一種全新安卓平台上的手機／行動裝置上的銀行金融木馬程式，會偽裝成基本服務，例如：公用事業 (如瓦斯或電力) 或銀行 APP，以竊取受害者的財務資料。此詐騙一開始是以公用事業相關訊息 (例如：瓦斯服務將中斷的警告等) 的形式進行，使訊息接收者感到驚慌，進而引誘

受害者立即採取行動，安裝惡意安中套件 (.APK)。此惡意程式會偽裝允許使用者支付帳單，同時竊取敏感的財務資訊，例如：卡片詳細資料或銀行帳戶資訊。

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：

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。

2024/12/13

Shuckworm駭客組織散布安卓平台上的手機／行動裝置惡意軟體：BoneSpy和PlainGnome

駭客組織 Shuckworm (亦稱 Gamaredon) 已被觀察到在最近的網路攻擊行動中，散佈兩個安卓平台上的手機／行動裝置惡意軟體。BoneSpy 和 PlainGnome 是針對從 Android 裝置收集和滲透各種資料的監控惡意軟體類型。這些惡意軟體會收集簡訊、地理位置資訊、聯絡人名單、通話記錄、瀏覽歷史、相機照片等資訊。據報導，BoneSpy 是以獨立應用程式的形式散佈，而 PlainGnome 則是第二階段有效酬載的植入程式。

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。

2024/12/12

專用於人類的釣餌：社交工程～南非的報稅季，想當然耳：偽造南非稅務局(SARS)電子郵件掀起網路釣魚浪潮

在南非，納稅人必須向南非稅務局 (SARS) 報稅。雖然每年稅季的確切時間略有不同，但一般都在年中至秋末冬初之間。全世界都一樣，只要是報稅季節，利用稅務相關社交工程的網路

犯罪活動明顯增加。賽門鐵克最近觀察到在南非營運的公司被數個威脅者當成目標。以下是一些最近的範例：

攻擊行動 #1：

惡意電子郵件 (主旨：「LETTER OF FINAL DEMAND SARS STATEMENT (COURT ORDER)」) 冒充南非稅務局 (SARS)。它使用不相關的寄件者位址，偽冒 Limpopo 衛生部，並使用「最終要求」和「法院命令」等驚人詞彙。該電子郵件包含一個惡意的 PDF 附件，檔名為 ACTION SARS SUMMONS LETTER (RSAE3ET).pdf。

該 PDF 檔模仿 SARS 的官方文件維妙維肖，除有 SARS 的標誌外，還有看起來合法的格式。它聲稱是一份「最終催款」通知，迫使收件人採取緊急行動，以避免被列入「不良紀錄和法院傳票」。該文件包含一個連結，可將使用者導向一個上架在 HiDrive Share 上的惡意 HTML 檔案。當執行時，此 HTML 檔案會顯示一個偽造的登入頁面，目的是存取詐騙的「SARS 文件」以竊取憑證。

攻擊行動 #2：

惡意電子郵件 (主題：「APPROVEMENT NOTE HERE」) 冒充南非獨立選舉委員會 (IEC)。附件是一個惡意 PDF 檔案，檔名為 OPEN DEMAND LETTER.pdf。

該 PDF 模仿 SARS 的官方通知，使用其標誌並包含一個標有「OPEN DEMAND LETTER HERE」的按鈕，如果點擊該按鈕，會將使用者重導向到上架在 JioTransfer 上的惡意 HTML 頁面。此 HTML 頁面會開啟一個釣魚網站，其目的在於竊取電子郵件憑證，並以存取假冒的「已核准的採購訂單文件」來詐騙受害者。

攻擊行動 #3：

一封惡意電子郵件 (主題："Important Notification *重要通知") 冒充南非稅務局 (SARS)。該電子郵件使用令人不安的語言和緊急情況向收件人施壓，並包含一個擋名為 DUE ON 11 DECEMBER 2024.pdf 的詐騙 PDF 附件。

PDF 本身並未顯示惡意行為，例如：網頁重導向。相反地，它模仿 SARS 的官方文件，標題為『Outstanding Tax Debt*逾期未繳稅金』，有 SARS 的標誌，版面設計也很專業，看起來很合法。它聲稱收件者有 1,500.00 盧比的逾期未繳稅金 (在撰寫本報告時價值為 97.50 美元)，必須立即繳清以避免罰款或法律問題。

在此攻擊行動中，攻擊者可能試圖引發對電子郵件的回應，以進一步進行社交工程。這些行為可能包含付款詐騙、提供網路釣魚網頁或傳送惡意軟體。

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：

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。

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**。