保安資訊--本周(台灣時間2021/12/10)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 140 萬個受保護端點上總共阻止了 1.733 億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2021/12/06)**

- 在**23萬2,900**台端點上，阻止了**5,960萬**次嘗試掃描**Web**服務器的漏洞。
- 在**58萬2,900**台端點上，阻止了**5,150萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬3,100**台**Windows**伺服主機上，阻止了**2,250萬**次攻擊。
- 在**18萬2,700**端點上，阻止了**1,280萬**次嘗試掃描伺服器漏洞。
- 在**10萬4,000**台端點上，阻止了**560萬**次嘗試掃描在**CMS**漏洞。
- 在**13萬8,300**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**48萬6,000**台端點上，阻止了**1,420萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,100**台端點上，阻止了**400萬**次加密貨幣挖礦攻擊。
- 在**5萬3,700**台端點上，阻止了**570萬**次向惡意軟體**C&C**連線的嘗試。
- 在**8,900**台端點上，阻止了**27萬2,000**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。

2021/12/09

新的「Ceeloader」惡意軟體

疑似俄羅斯所支持的 APT 組織，稱為 Nobelium，利用被識別為「Ceeloader」的新型惡意軟體，來攻擊全球的政府和企業網路。這種新型、高度混淆的自定義惡意軟體是用 C 語言所設計，能夠直接在記憶體內執行程式碼注入 (shell-code) 籌載。它在大量垃圾程式碼中混合對 Windows API 的有意義的呼叫，以隱藏真正的呼叫，來躲避安全軟體的檢測。「Ceeloader」會利用 HTTP 與 C&C 伺服器通訊，並且響應在 CBC 模式下使用 AES256 進行解密。

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：

- Malicious Site: Malicious Domain Request 59

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。

2021/12/09

Cerber 勒索軟體鎖定「Atlassian Confluence」和「Gitlab」遠端程式碼執行漏洞

新勒索軟體變種，採用舊名稱「Cerber」(在 ID Ransomware 網站上被命名為 CerberImposter) 及其支付贖金的說明檔案和 TOR (洋蔥路由器) 支付站點。更新後程式碼使用較新版本的加密函式庫並發布了 Linux 變種，而舊的 Cerber 版本只有 Windows 編譯變種。新版本建立支付贖金的說明檔名為 _$$RECOVERY_README$$_.html，並將 .locked 副檔名附加到用戶被加密的檔案。

在該組織看到的新活動中，攻擊者的目標是公開披露的 Atlassian Confluence (CVE-2021-26084) 和 GitLab (CVE-2021-22205) 的遠端程式碼執行漏洞，以在無需身份驗證情況下獲得遠端存取。這兩個漏洞修補程式都已推出，我們建議用戶更新讓系統處於最新狀態。

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：

- Downloader.Trojan
- Trojan.Gen.2
- 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已於第一時間收錄於不安全分類列表中。

2021/12/08

STOP (又名DJVU) 勒索軟體，活動仍然持續

STOP 勒索軟體（也稱為 DJVU）幕後的威脅參與者已經活躍好幾年，並在全球各地繼續觀察到危害消費者和企業用戶的行為。STOP 勒索軟體主要利用破解軟體和偷渡式下載分發，但與一些更惡名昭彰的勒索軟體不同，它沒有使用雙重勒索戰術。有趣的是，最近報告和分析結果表示，如果受害者位於以下國家／地區，則該威脅將不會執行其加密程序：俄羅斯、白俄羅斯、烏克蘭、亞塞拜然、亞美尼亞、塔吉克、哈薩克、吉爾吉斯、烏茲別克和敘利亞。

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(Snoar)的防護：

- SONAR.Ransomstop!gen7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.620
- Trojan.Gen.MBT
- Ransom.Pots
- Ransom.Pots!gen2

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
- System Infected: Trojan.Ransomware Activity 58

2021/12/08

Emotet 直接植入 Cobalt Strike Beacon訊號發送器 (Stager)

Emotet 威脅發動者似乎已經改進他們的經典感染策略之一，顯著變化是現在可以直接安裝 Cobalt Strike Beacon 訊號發送器 (Stager)，並且不再需要像 Trickbot 或 Qakbot 這樣的中繼木馬下載器 (它隨後使用 RegSvr32 載入特定的 DLL)。以這種方式縮短了攻擊鏈，可以讓威脅發動者迅速進入攻擊下一個階段，例如：在受感染的網路上安裝勒索軟體。

由於 Emotet 現在支持更多指令，攻擊者可通過更多方式在受感染機器上植入、下載 Cobalt Strike 和其他威脅。

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 Horse
- Trojan.Gen.MBT
- WS.Malware.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。

2021/12/07

惡意垃圾郵件行動，趁機植入Matanbuchus 和 Qbot 惡意軟體

今年稍早，研究人員報告名為「Matanbuchus」的惡意軟體即服務領域，新的下載器，在該惡意軟體開發者「BelialDemon」所屬的地下論壇上做廣告。

最近，有人觀察到有惡意垃圾郵件活動利用「Matanbuchus」傳送內含巨集物件的 XLSB 文件，作為隨後呼叫其他 Qakbot (Qbot) 惡意軟體的一種媒介。此活動隨後將導致垃圾郵件殭屍 (機器人) 和 Cobalt Strike 滲透測試工具攻擊。

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：

- Downloader.Trojan
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- W97M.Downloader

基於機器學習的防禦技術：

- 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。

2021/12/07

古巴勒索軟體集團，最新行動 (10月及11月)

最近美國聯邦調查局 (FBI) 發表聲明指稱，截至 2021 年 11 月初，古巴勒索軟體對五個關鍵基礎設施部門的 49 個實體單位進行攻擊。行業包括但不限於金融、政府、醫療保健、製造和資訊技術。

據報導，古巴勒索軟體集團仍與 Hancitor 惡意軟體垃圾郵件運營商合作，以獲取對受感染網路的存取權限。Hancitor 以使用網路釣魚電子郵件、Microsoft Exchange 漏洞和被入侵的憑證建立對受害者網路的初始存取聞名。隨後，古巴勒索軟體攻擊者使用合法的 Windows 服務，例如：PowerShell、PsExec 和其他未指定的服務，利用 Windows 管理員權限遠端執行他們的勒索軟體和其他程序。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- 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。

2021/12/06

駭客組織 TA551， 正在透過惡意垃圾郵件分發 IcedID 金融竊密木馬程式

駭客組織 TA551 也稱為 Shathak，在過去幾年中散布了許多不同家族的惡意軟體，包括 Ursnif、Valak、BazarLoader 和 Trickbot。這些初始媒介通常會導致進一步的 Cobalt Strike 感染。最近的攻擊始於惡意垃圾郵件欺騙，對包含受密碼保護的 zip 附件先前有效電子郵件的回覆。密碼包含在電子郵件本文中，Microsoft Office 文件包含在 zip 壓縮檔中。打開文件並啟動巨集會利用 IcedID (Bokbot) 感染裝置。

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 Horse
- Trojan.Gen.2
- Trojan.Malscript
- W97M.Downloader

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)。

2021/12/05

RedLine 資訊竊取木馬透過惡意 XLL 附加元件散布

一組研究人員最近披露了一項廣泛存在的惡意軟體行動，該行動透過惡意 Excel 附加元件 (XLL) 傳播 RedLine 資訊竊取木馬。用於尋求用戶參與的誘餌各式各樣，包括付款報告、節日禮物指南和網站促銷，並且可以在隨機網站的聯絡人表格、文章評論和論壇中找到，這些誘餌包含在託管惡意 XLL 文件的 Google Drive 鏈接中。

RedLine 是一種資訊竊取木馬，同時也是一種下載程式。它可以執行命令來下載額外的惡意軟體以進一步擴展攻擊。

XLL (.xll) 是 Excel 所特有，且內建的任何編譯器都支援建立 DLL (動態連結文件庫) 。它們不需要安裝或註冊。XLL 附加元件也包含包含使用者定義命令和函數的 DLL。

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：

- Downloader
- 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.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 611(33088)

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。

2021/12/05

Tor2Mine 挖礦惡意軟體仍然處於活躍的狀態，觀察到新的變種

Tor2Mine 是一種挖掘門羅幣 (Monero) 加密貨幣惡意軟體，並且能夠竊取管理員憑證，以便在受感染的環境中透過網路進行傳播。這種威脅已經存在幾年了，並且在當今的威脅環境中仍然活躍。正如最近報告所表明，已經發現了新的變種。

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(Snoar)的防護：

- SONAR.LoadPoint!gen5

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- ISB.Downloader!gen*
- ISB.Heuristic!gen*
- Trojan.Gen.NPE
- Trojan.Gen.6
- Trojan horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

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: Powershell Base64 Script Execution 02
- System Infected: Malicious PowerShell Script Download 24
- System Infected: Trojan.Backdoor Activity 618
- Web Attack: Malicious HTA File Download 3

2021/12/03

留意那些掛羊頭賣狗肉的：偽裝成虛假安裝程式的資訊竊取程式

已經觀察到惡意軟體散布行動，可能經由線上廣告散布，試圖誘騙使用者執行虛假軟體安裝程式。虛假安裝程程式可以充當多種角色，包括尋找系統上任何憑證的資訊竊取程式、通過隱匿的 RDP 連線進行遠端存取的後門程式以及包含鍵盤側錄程式和其他資訊竊取程式行為的惡意 Chrome 瀏覽器擴充程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.DriverPack
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- VBS.Downloader.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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已於第一時間收錄於不安全分類列表中。

2021/12/03

披露未修補完全的 CVE-2021-41379 變種

11 月下旬，一位研究人員發布了有關 Windows 安裝程式 (Installer) 的特權提升漏洞 (CVE-2021-41379) 變種的詳細資訊，其中包括概念驗證程式碼。微軟在 2021 年 11 月的安全更新發布期間修補了原始漏洞，但報告研究人員發現這並不是一個完整的修復程序。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Bloodhound.Exploit.843
- Trojan Horse

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS (Symantec Data Center Security) 為 Windows Installer EOP 漏洞提供 0 天保護。特別是DCS Windows強化政策攔截了 POC／exploit 覆蓋 Windows 服務二進製檔案和 MSI 檔案的嘗試。

2021/12/02

Emotet 找到新的詭計來誘騙用戶

已觀察到最近的 Emotet 惡意垃圾郵件行動濫用 Windows 應用程式(App)安裝包以進行傳播。惡意垃圾郵件包含轉向欺騙檔案共享頁面的鏈接或惡意 Office 文件，提示用戶安裝偽造的 Adobe 閱讀器 PDF 元件以存取檔案。

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：

- CL.Downloader!gen69
- Scr.MalMacro!gen1
- Trojan.Gen
- VBA.Downloader.Gen

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) 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保護 (威脅不落地)。