保安資訊--本周(台灣時間2022/09/02)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 100 萬受保護端點上總共阻止了1.503億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/08/28)**

- 在**20萬1,900**台端點上，阻止了**7,290**萬次嘗試掃描**Web**服務器的漏洞。
- 在**36萬5,600**台端點上，阻止了**2,820**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬2,000**台**Windows**伺服主機上，阻止了**1,910**萬次攻擊。
- 在**12萬7,400**端點上，阻止了**600**萬次嘗試掃描伺服器漏洞。
- 在**5萬5,200**台端點上，阻止了**260**萬次嘗試掃描在**CMS**漏洞。
- 在**9萬4,000**台端點上，阻止了**300**萬次嘗試利用的應用程式漏洞。
- 在**33萬4,700**台端點上，阻止了**770**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,700**台端點上，阻止了**380**萬次加密貨幣挖礦攻擊。
- 在**4萬8,000**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**7,000**台端點上，阻止了**18萬8,000**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。

2022/09/01

Agenda (*議程)--採用 GO 語言開發的目標式勒索軟體

據報導，一個被稱為 Agenda 的新型勒索軟體變種以亞洲和非洲企業為目標。這種採用 GO 語言開發的 (Golang-based) 惡意軟體針對 Windows 環境。該勒索軟體是有針對性，並可以為每個目標受害者客製化。據報導，負責 Agenda 傳播的攻擊者一直在利用面向公眾的 Citrix 伺服器作為初始入侵點。Agenda 勒索軟體具有終止特定系統程序和服務以及刪除受感染主機上的磁碟區陰影複製 (shadow volume) 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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18

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.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：

- Attack: Ransom.Gen Activity 46

2022/09/01

Asbit -- 一個全新的新興遠端存取木馬 (RAT)

Asbit 是一個全新的新興遠端存取木馬 (RAT)，由其開發者直接提供銷售。Asbit 最早在 2021 年被注意到，並透過安裝套件包散佈提供。在一些較新的 2022 年網路攻擊行動中，惡意軟體的安裝檔已經透過 Discord 隱藏在 .pif 檔案來傳播。該惡意軟體從植入一個載入程式的模組開始，並導引核心模組的進一步下載。Asbit 的功能包括遠端桌面控制、命令執行和按鍵注入等。Asbit 也利用 TightVNC 的遠端桌面功能。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

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。

2022/09/01

Formbook 竊密程式相關的網路攻擊行動鎖定波蘭境內的組織

Formbook 竊密程式相關的活動從未減少過，衍生的網路攻擊也在全世界造成很大禍害，是被公認的頂級竊密程式。最近賽門鐵克觀察到一個主要針對波蘭組織的 Formbook 網路攻擊行動，但也在其他周邊國家出現。威脅者自稱是義大利和羅馬尼亞的塑膠／泡沫製造公司，發送虛假的訂單郵件 (主旨：Zamówienie nr_DOC_0080962946)，其中包含一個惡意的 IMG 格式檔案作為附件。如果用戶沒有戒心而被成功引誘，他們最終會執行偽裝成虛假訂單的 Formbook 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：

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.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/08/31

利用 ModernLoader 載入程式所發動的攻擊行動，散佈一系列的惡意軟體

最近觀察到散佈 ModernLoader 載入程式作為最終的有效籌載攻擊行動。ModernLoader 載入程式是一個可以收集系統資訊的遠端存取木馬 (RAT)，同時可以部署各種威脅模組，包括加密貨幣挖礦劫持的惡意軟體。這些攻擊似乎是透過被入侵的網站針對東歐用戶的，並使用偽裝成偽造的亞馬遜禮品卡的檔案來傳遞威脅。

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：

- ISB.Downloader!gen281

- ISB.Heuristic!gen5
- Trojan Horse
- Trojan.Dropper!g6
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan.Whispergate

2022/08/31

GO#WEBBFUSCATOR 攻擊行動利用隱寫術和惡意巨集程式

一個被稱為 GO#WEBBFUSCATOR 的新型惡意攻擊行動在真實網路環境爆發。攻擊者正在利用包含帶有內嵌惡意巨集的 MS Word 文件的惡意郵件。一旦執行，一個以詹姆斯--韋伯望遠鏡所拍攝的 JPG 格式太空畫面影像檔的圖片檔會被下載，隨後被解碼為一個用 Golang 程式設計語言編寫的惡意可執行檔。該惡意軟體建立與攻擊者 C&C 伺服器的 DNS 網路連線，並開始發送加密查詢。根據報告，已經觀察到該惡意軟體運行任意的列舉命令，這是標準的第一步偵察。

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：

- ISB.Downloader!gen433
- Trojan Horse
- Trojan.Gen.MBT
- W97M.Downloader
- WS.Malware.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。

2022/08/31

最新的間諜行動中散佈 ScanBox 漏洞利用框架

在最近由名為 TA423 或 Red Ladon 的進階持續威脅 (APT) 組織所發動的間諜行動中，發現 ScanBox 漏洞利用框架已經被散佈。在整個行動中，攻擊者一直在利用聲稱來自澳洲多個媒體單位的魚叉式網路釣魚郵件。ScanBox 漏洞利用框架允許攻擊者對受害者的網路進行偵察，並進一步向選定目標投遞額外的有效籌載。據報導，相關攻擊行動主要針對澳洲政府機構、澳洲新聞媒體機構和在南中國海地區有生產基地的幾個重工業製造商。

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：

- Infostealer

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。

2022/08/31

被入侵網站上的虛假 DDoS 提示，誘騙安裝 NetSupport 遠端存取木馬(RAT)

隨著新的重大漏洞被揭露並幾乎每隔一天就會出現在新聞中，像社交工程這樣的惡意軟體散佈行動往往會被掩飾隱藏到檯面下，或是讓它自然被淡忘。社交工程仍然是向毫無戒心的使用者提供惡意軟體的最有效方式之一。賽門鐵克瞭解到有報告指出，在被入侵的網站上顯示的虛假 DDoS 提示正在引誘用戶下載偽裝成安全工具安裝程式的惡意軟體。攻擊者在被入侵的網站上注入一小段 javascript 程式碼，顯示虛假的 DDoS 提示。DDoS 提示欺騙用戶，使其相信瀏覽該網站需要一個驗證碼，而這個驗證碼可以透過下載和執行安全工具安裝程式獲得。安全工具安裝程式實際上是一個惡意軟體，它安裝 NetSupport RAT，能夠對受害者的機器進行後門存取。攻擊者可以利用這個後門存取權來安裝額外的惡意軟體或執行任何其他惡意活動。

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.Dropper
- Trojan.Mallnk
- NetSupportManager!conf

網路層防護：

賽門鐵克的網路層防護技術:入侵預防系統(IPS)，入侵預防會自動偵測和攔截網路攻擊。在 Windows 電腦上，入侵預防還會偵測和攔截對於受支援瀏覽器的瀏覽器攻擊。入侵預防是繼防火牆之後用於保護用戶端電腦的另一層防護。入侵預防會截取網路層中的資料。它使用特徵掃描封包或封包串流。透過尋找與網路攻擊或瀏覽器攻擊對應的模式，入侵預防可以個別掃描各個封包。入侵預防會偵測作業系統元件和應用程序層的攻擊：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22
- Web Attack: Mass Injection Website 96

2022/08/30

Nitrokod：全新的加密貨幣挖礦劫持攻擊行動

據報導，一個被稱為 Nitrokod 的全新加密貨幣挖礦劫持攻擊行動已經感染全球 11 個國家的機器。該惡意軟體透過多個分享站點提供免費軟體進行傳播。其中一個應用程式是 "Google Translate Desktop--谷歌翻譯桌面版"，一旦安裝，就會啟動一個延遲的多階段感染過程，最終下載並執行 XMRig 加密貨幣挖礦劫持有效籌載。

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.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2022/08/29

另一個基於 .NET 新型勒索軟體：Moishage

Moisha 是一個全新基於 .NET 的勒索軟體變種。8 月中旬首次出現，該惡意軟體在攻擊過程中採用雙重勒索戰術，也就是先竊取機敏資料，勒索不成會公開機敏資料作為威脅。Moisha 具有停止某些系統服務的功能，並能強制結束目標主機上運行特定應用程式的程序。該惡意軟體不會對加密後的檔案附加任何副檔名，贖金說明以簡單易懂：閱讀以恢復你的資料 ("!!!READ TO RECOVER YOUR DATA!!!.txt") 文字檔形式發佈。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/08/26

利用光碟映像檔 .ISO …等附件來散佈 AgentTesla 竊密程式的惡意攻擊行動

8月中旬，發現一個新的散佈 AgentTesla 竊密程式的惡意攻擊行動。該惡意軟體透過包含光碟映像檔 .ISO 附件的惡意郵件傳播，這些附件包含導致感染的惡意 chm 檔案--一種“Compiled HTML Help File--已編譯的html檔案”。AgentTesla 是一個熱門的竊密程式，在過去幾年來一直在網路黑社會嶄露頭角、為非作歹。它從使用者的電腦、存儲在瀏覽器、電子郵件和 VPN 用戶端的密碼中偷竊機密資訊。它還可能導致在受感染的主機上植入額外的有效籌載。

以下補充說明節錄自 WiKI，非 Symantec 原廠的本文：微軟 HTML 幫助集，即已編譯的 HTML 說明檔案，是微軟繼承早先 WinHelp 發展的一種檔案格式，用來提供線上幫助，是一種應用較廣泛的檔案格式。因為 CHM 檔案如一本書一樣，可以提供內容目錄、索引和搜尋等功能，所以也常被用來製作電子書。實際上，微軟閱讀器的 .lit 就是由 CHM 擴充而成。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen272
- JS.Downloader
- 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。