保安資訊--本周(台灣時間2022/05/13)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 120 萬個受保護端點上總共阻止了2.015 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/05/09)**

- 在**22萬5,700**台端點上，阻止了**1億1,120萬**次嘗試掃描**Web**服務器的漏洞。
- 在**45萬7,700**台端點上，阻止了**3,120萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬2,400**台**Windows**伺服主機上，阻止了**2,220萬**次攻擊。
- 在**16萬6,000**端點上，阻止了**1,070萬**次嘗試掃描伺服器漏洞。
- 在**9萬1,200**台端點上，阻止了**450萬**次嘗試掃描在**CMS**漏洞。
- 在**13萬2,300**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**33萬7,300**台端點上，阻止了**910萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,630**台端點上，阻止了**330萬**次加密貨幣挖礦攻擊。
- 在**11萬7,700**台端點上，阻止了**480萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,900**台端點上，阻止了**18萬6,100**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。

2022/05/11

新的遠端存取木馬 Nerbian

最近一個惡意軟體活動一直在散佈被稱為 Nerbian 全新隱祕性遠端存取木馬 (RAT)，目標是義大利、西班牙和英國的機構。受害者被引誘打開一個經由電子郵件接收到的附件，該附件冒充世界衛生組織（WHO），聲稱其中有關於 COVID-19 的重要資訊。一旦惡意檔案被開啟，就會執行一系列的程序，包含下載植入程式，執行各種環境檢查的反分析工具，以躲避在部署 Nerbian RAT 之前的各種安全機制檢測。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2022/05/11

Bitter (*苦澀的) 進階持續威脅 (APT) 威脅者

一個被稱為 Bitter 專注於間諜活動，進階持續威脅 (APT) 威脅者已經擴大他們的目標名單，包括孟加拉政府部門（其他含中國、巴基斯坦和沙烏地阿拉伯的能源、工程和政府部門）。引誘受害者的最新主題是帶有惡意附件的魚叉式網路釣魚電子郵件，聲稱與受害者組織的例行公事有關。一旦受害者打開附件，就會從代管伺服器下載木馬 ZxxZ，然後在受害者的電腦上執行。這使得威脅者可以進行遠端程式碼執行，透過安裝其他工具為其他活動另闢蹊徑。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Mdropper

- WS.Malware.1
- WS.Malware.2

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／IP位址已於第一時間收錄於不安全分類列表中。

2022/05/10

APT34 使用被稱為 Saitama 的新後門惡意軟體

自 2014 年以來，APT34 這個伊朗的駭客威脅集團，也被稱為 OilRig／COBALT GYPSY／IRN2／HELIX KITTEN，針對中東金融、政府、能源、化工和電信等相關領域的公司。

去年 4 月，對約旦政府的一次攻擊被發現，看到該老練的駭客集團，利用一種新的後門惡意軟體，稱為 Saitama。Saitama 是用 .Net 編寫，能夠濫用受害者電腦的 DNS 協議進行 C&C 通信，使攻擊者能夠操作進一步的命令，例如：執行遠端預設的命令、自訂命令和植入惡意檔案。

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：

- Scr.Malcode!gen
- Scr.Malcode!gen1
- Trojan.Mdropper
- WS.Malware.1

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已於第一時間收錄於不安全分類列表中。

2022/05/10

REvil 在沉寂數月後重出江湖

新的 REvil 樣本已經被發現，顯示這個勒索軟體即服務在幾個月的關閉後又重啟。新的樣本出現一些硬編碼相關的公開金鑰、配置儲存和關聯追蹤的小變化。

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.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/05/10

Jester (*傑斯特) 竊密程式在烏克蘭大規模傳播

一個如影隨行的惡意軟體行動，正在烏克蘭透過網路釣魚郵件進行大規模傳播。這些郵件的誘餌是一個關於來自俄羅斯化學攻擊的預警通知，並包含一個 XLS 檔案的附件，聲稱有哪些地區可能會受到影響的細節。XLS 檔案實際上包含一些巨集，如果執行成功，將下載 Jester 竊密程式--可以擷取儲存在瀏覽器中的資料，例如：帳號密碼、電子郵件用戶端上的資訊、IM應用程式上的討論和加密貨幣錢包的詳細資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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)。

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/05/09

編號 CVE-2022-1388 漏洞，繞過 F5 的 BIG-IP 系統身分認證程序

F5 報告 BIG-IP 中一個重要的認證繞過漏洞 (CVE-2022-1388)，可能允許攻擊者在受影響的設備上提權以高權限執行命令。根據該公告，“該漏洞可能允許未經認證的攻擊者透過管理埠和／或自我 IP 位址對 BIG-IP 系統進行網路存取，以執行任意系統命令、建立或刪除檔案，或停用服務”。

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：

- [32947] Web Attack: F5 iControl RCE CVE-2021-22986

2022/05/09

暗藏 Joker (*小丑) 木馬的新安卓應用程式APP

安卓惡意軟體“小丑”非新鮮玩意，但它繼續在當今的行動威脅領域找到新的傳播方式。這種威脅經常出現在 Google Play 商店上，狡猾地在審查過程時讓惡意的有效籌載處於休眠狀態而通過審查，待正式上架後該惡意酬載才會被啟動。這種惡意軟體被用於簡訊／帳單欺詐、竊取簡訊和收集聯絡人名單／設備資訊。最新的應用程式與血壓／健康、相機 PDF 掃描器和風格資訊有關。目前，這些應用程式已經從 Google Play 商店中下架，但在其他第三方應用程式提供商那裡可以找到。

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.Malapp

2022/05/08

XFiles 竊密程式活動有所增加

雖然還不到所謂的盛行，但最近幾個月，賽門鐵克觀察到威脅中出現更多 XFiles 竊密程式。這種普通竊密程式可以竊取各種密碼、加密錢包、discord 權杖、文件、機器的資訊，並有螢幕截圖的功能。去年，它被破解並在地下論壇上被洩露，使許多人可輕鬆取得。最近活動中，參與者大多透過標準手段散佈這種惡意軟體，包括惡意的電子郵件和瀏覽網頁時的順道下載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/05/06

散佈 NetDooka 框架的 PrivateLoader 惡意軟體

NetDooka，一個由 PrivateLoader 惡意軟體所散佈的新框架最近被確認。PrivateLoader 是以安裝次數計費（PPI）的惡意程式即服務，而且還因散佈其他惡意軟體家族，包括 Anubis、Raccoon Stealer、Redline、Smokeloader 等而出名。NetDooka 框架包括一個植入程式、載入程式、遠端存取木馬 (RAT) 和其他惡意工具。它處於早期開發階段，除了它自己的 RAT 之外，還可以用來傳遞其他有效籌載，所以應該密切關注。

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：

- Heur.AdvML.B
- Heur.AdvML.C
- Trojan.Gen.2
- W32.Pajetbin

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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: Bad Reputation Process Request 4(31528)
- System Infected: Trojan.Backdoor Activity 634(33246)
- Web Attack: Webpulse Bad Reputation Domain Request(29565)