保安資訊--本周(台灣時間2021/12/31)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 2.079 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2021/12/19)**

- 在**31萬7,300**台端點上，阻止了**1億190萬**次嘗試掃描**Web**服務器的漏洞。
- 在**55萬7,400**台端點上，阻止了**4,630萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**10萬9,500**台**Windows**伺服主機上，阻止了**3,290萬**次攻擊。
- 在**18萬8,200**端點上，阻止了**1,190萬**次嘗試掃描伺服器漏洞。
- 在**10萬8,100**台端點上，阻止了**540萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬8,700**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**47萬8,300**台端點上，阻止了**1,340萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,200**台端點上，阻止了**390萬**次加密貨幣挖礦攻擊。
- 在**5萬6,500**台端點上，阻止了**520萬**次向惡意軟體**C&C**連線的嘗試。
- 在**8,700**台端點上，阻止了**24萬9,700**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。

2021/12/29

BlackTech APT 集團，利用的 Flagpro 惡意軟體

據報導，BlackTech APT 集團在針對日本公司的攻擊中利用了一種名為 Flagpro 的新型惡意軟體。Flagpro 是透過魚叉式網路釣魚電子郵件發佈帶有惡意巨集的 MS Excel 壓縮檔案。攻擊者主要在初始攻擊階段使用這種新的惡意軟體，以進行偵察和第二階段的有效籌載下載。

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
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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：

- 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。

2021/12/28

BLISTER 載入程式的惡意軟體行動

根據最近發布的一份報告，一種全新名為 BLISTER 載入程式的惡意軟體，已被廣泛用於派送各種第二階段惡意軟體籌載。攻擊者一直在惡意軟體植入程式上使用有效的程式碼簽章以逃避檢測。CobaltStrike 和 BitRAT 在最近涉及此載入程式的行動中被視為最終有效籌載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- 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: 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。

2021/12/28

巴西使用者不斷成為金融惡意軟體的目標

拉丁美洲不斷受到金融惡意軟體的夾攻，尤其是巴西，這些惡意軟體針對包括電腦和行動裝置在內的各種技術平臺。最近，其中一種威脅被發現針對巴西一家主要銀行的行動用戶和客戶。該行動幕後的參與者建立一個假的銀行 Android 應用程式，聲稱來自這家巴西銀行。如果受害者成功安裝偽造的應用程式，它將能夠使用輔助功能服務執行傳輸攻擊。

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：

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：

- AdLibrary:Generisk

2021/12/27

跳梁「小丑：Joker」潛入 Google Play 商店

Android 惡意軟體「小丑：Joker」並不是新出現，已經存在許多年了。這些年來，它因多次潛入 Google Play 等官方應用商店而惡名昭彰。Joker 仍然處於活動狀態並且沒有停止的跡象，最近在 Google Play 商店上觀察到仍活躍中，這次安裝量超過 50 萬。該威脅能夠竊取裝置資訊、簡訊內容和聯絡人。然後它嘗試模擬點擊，併為受害者訂閱高資費服務。

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：

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：

- AppRisk:Generisk

2021/12/27

Rook 勒索軟體與 Babuk 變種有相似之處

據報導，最近發現的 Rook 勒索軟體是改編自 Babuk 勒索軟體洩露的原始程式碼。Rook 是透過網路釣魚電子郵件或濫用紅隊演練工具 Cobalt Strike 進行有效籌載的行動來傳遞。感染目標系統後，Rook 將嘗試終止特定程序 (Process) 和服務並刪除磁卷陰影複製。Rook 幕後的攻擊者還採用雙重勒索戰術--威脅受害者如果不支付贖金，就會將已竊取的資料公諸於世。

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

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!g18

2021/12/26

TigerDownloader 自定義下載器 和 TigerRAT 遠端存取木馬

一個名為 Stonefly (又名 Silent Chollima 和 Andariel) 的 APT 組織仍然活躍，該組織主要針對韓國各個行業。在最近的金融和網路間諜活動中，該組織一直使用魚叉式網路釣魚和受感染網站，以及自定義下載器 (TigerDownloader) 和遠端存取木馬 (TigerRAT) 作為其初始攻擊媒介。

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：

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.2
- Trojan.Gen.MBT
- Trojan Horse

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。