保安資訊--本周(台灣時間2023/02/03)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 77 萬 7,200 台受保護端點上總共阻止了 9,280 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/01/29)**

- 在**14萬4,100**台端點上，阻止了**3,650**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬5,100**台端點上，阻止了**1,940**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬6,500**台**Windows**伺服主機上，阻止了**1,630**萬次攻擊。
- 在**9萬200**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,200**台端點上，阻止了**100**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬3,200**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**27萬4,900**台端點上，阻止了**560**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬9,000**台端點上，阻止了**360**萬次加密貨幣挖礦攻擊。
- 在**12萬1,400**台端點上，阻止了**1,080**萬次向惡意軟體**C&C**連線的嘗試。
- 在**3,400**台端點上，阻止了**13萬900**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。

2023/02/02

Lockbit勒索軟體集團採用全新"LockBit Green"的加密程式

Lockbit 勒索軟體幕後的駭客集團已經開始採用源於被洩露 Conti 勒索軟體原始碼的全新加密程式。該駭客集團採用的加密程式經歷好幾次反覆修正，但當前版本被命名為 Lockbit Green，以區別於仍在使用的其他變種 Lockbit Black（又名 Lockbit 3.0）。

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.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/02/02

觀察到Qakbot殭屍網路使用OneNote檔案所發動的全新攻擊行動

Qakbot 殭屍網路是威脅領域、駭客圈最流行的銀行金融惡意軟體之一，並且已經觀察到一個全新的攻擊行動。在此行動中，垃圾郵件攻擊者利用 OneNote 檔案下載惡意 HTA 檔。如果成功引誘受害，該惡意 HTA 將觸發由 CURL + Rundll32 所引導的接續攻擊鏈來下載 Qakbot。

攻擊鏈：

電子郵件 > 內含網址(url) > .zip（無密碼）> .one 檔案 > 內含嵌入惡意程式元件 .hta > 執行 curl + Rundll32 > 執行 Qakbot .dll

電子郵件 >內含附件檔 > 內含嵌入惡意程式元件 .hta > 運行 curl + Rundll32 > 執行 Qakbot .dll

保安補充說明(引用網路資訊)：檔案副檔名 HTA 是一種由 Microsoft 開發的 HTML Application。HTA 檔案是一種可以從 HTML 檔案執行的程式，或者說是一種包含超文字語法的可執行檔，可以透過將 HTM 檔案的副檔名更改為 HTA 副檔名來建立。

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.MSHta!g17

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
- Trojan Horse
- Trojan.Malscript
- Trojan.Mdropper
- W32.Qakbot
- 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。

2023/02/01

TZW勒索軟體鎖定韓國用戶

TZW 勒索軟體已經在韓國到處流竄。經該勒索軟體加密後，會將 .TZW 的副檔名新增到原始副檔名中。它以系統訊息應用程式可執行檔的形式出現，因此它可以顯示與開機相關的正常程序檔案。在已散布的可執行檔中發現它是在 .NET 環境開發，並具有啟動程式和勒索軟體的功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Cryptolocker
- Scr.Malcode!gdn30
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/30

防護亮點：IPS Chrome 瀏覽器延伸

～防護亮點～

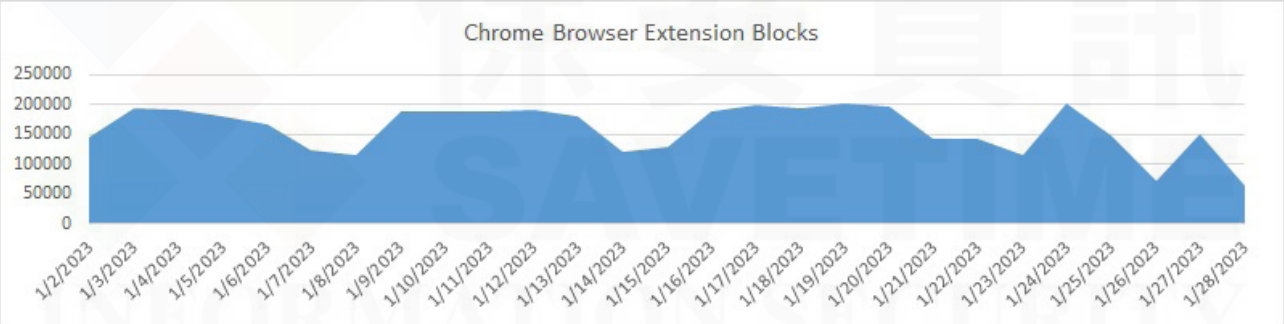
透過我們例行的『在端點啟用賽門鐵克入侵預防系統(IPS) 的好處~上週IPS 的防護效益』公告系列，我們試圖傳達 IPS（入侵防禦系統）是對抗惡意軟體（包括惡意程式和惡意網路流量）的關鍵保護層。單 IPS 技術就能阻止 70% 的惡意軟體--遠遠超過傳統的檔案型掃描技術。在這 70% 中，接近 95% 是所謂“感染前”阻止，這意味著這些攻擊根本無法進入企業環境，即便其他多種保護技術的整合也無法像 IPS 一樣，監控及攔截內網及外網的網路通訊。

這種離埠攔截也是一種重要的保護機制，因為它可以阻止下載額外的惡意軟體 (可能是實際有效負載)、與攻擊者命令和控制伺服器的通訊 (即背景連線通訊：phoning home) 以及公司資料的洩露。如果您的 SEP 沒有啟用入侵防禦 (IPS)，可能會使您的組織面臨嚴重的威脅防護損失。

一些人可能不知道一個非常有用的 IPS 相關功能是 Chrome 瀏覽器延伸。瀏覽器延伸是將功能和特性新增至 Web 瀏覽器的外掛程式。Symantec Endpoint Protection (SEP) 14.3 RU2 和更新版本會安裝 Google Chrome 延伸，讓用戶端電腦無法存取惡意網站。Chrome 瀏覽器延伸會監控進出 Web 瀏覽器的 HTTP 和 HTTPS 流量，並在用戶端確定 URL 是惡意 URL 時攔截該流量。SEP 不需要使用瀏覽器延伸，即可保護存取 Mozilla Firefox 和 Microsoft Internet Explorer 的用戶端使用者。相反地，SEP 會根據用戶端使用的用戶端入侵偵測系統 (CIDS) 引擎版本來支援這些瀏覽器。

所有 Web 瀏覽器都會使用下列技術來識別和保護惡意 URL：

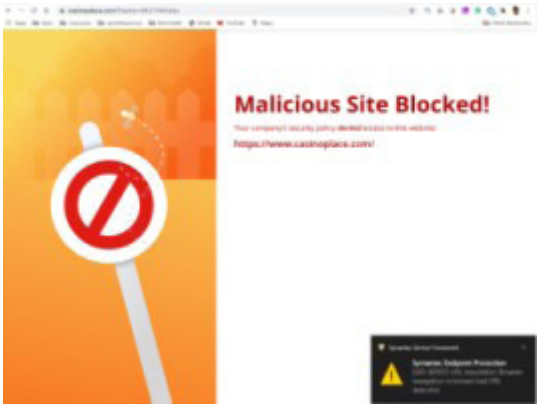
- **瀏覽器入侵防禦** 會將 IPS Web 瀏覽器特徵套用至用戶端上的入埠和離埠瀏覽器流量。請參閱：預期的瀏覽器入侵防禦行為
- **URL 信譽** 可識別來自網域和 URL 的威脅，這些網域和 URL 可以託管惡意程式、詐騙、網路釣魚和垃圾郵件這類惡意內容。URL 信譽接著會攔截識別為惡意內容之已知來源的網址存取權。請參閱：SEP URL 信譽常見問答集



突增的峰值代表與惡意網域和相關網路流量相關聯的每週攻擊行動。

賽門鐵克針對這種惡意網路流量採取了適當的保護措施，其辨識如下：

- 如果 Chrome Web 瀏覽器偵測到 URL 是惡意的，則用戶端會將使用者重新導向到下列預設登陸頁面：



欲了解整合瀏覽器延伸與 Symantec Endpoint Protection 以防禦惡意網站的更多訊息，請點擊此處。

2023/01/30

SwiftSlicer--在烏克蘭發現的全新資料刪除程式(Wiper)

在烏克蘭發現一種被歸屬於 Sandwork APT 駭客集團所擁有的全新資料刪除程式 (Wiper) 攻擊。這種全新的惡意軟體稱為“SwiftSlicer”。這種功能豐富多變的惡意程式具有極強的破壞力，例如：刪除備份和損壞／刪除 Windows 系統檔案的能力。

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：

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.C