保安資訊--本周(台灣時間2022/01/21)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 130 萬個受保護端點上總共阻止了2.156 億次攻擊。這些攻擊中有 96% 在感染階段前就被有效阻止：**(2022/01/17)**

- 在**25萬1,300**台端點上，阻止了**1.135億**次嘗試掃描**Web**服務器的漏洞。
- 在**49萬6,400**台端點上，阻止了**4,260萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬1,200**台**Windows**伺服主機上，阻止了**2,610萬**次攻擊。
- 在**19萬1,500**端點上，阻止了**1,080萬**次嘗試掃描伺服器漏洞。
- 在**10萬7,500**台端點上，阻止了**530萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬9,800**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**49萬9,400**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**4,800**台端點上，阻止了**420萬**次加密貨幣挖礦攻擊。
- 在**5萬**台端點上，阻止了**500萬**次向惡意軟體**C&C**連線的嘗試。
- 在**9,000**台端點上，阻止了**23萬700**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。

2022/01/20

偽裝成美國勞工部 (DoL) 的新網路釣魚行動

一項新的網路釣魚行動透過偽裝成美國勞工部 (DoL)，邀請投標政府標案來引誘收件人。

這些郵件來自新註冊的網域，這些網域被偽裝成有效的，並且包含帶有 PDF 附件的正文內容／格式，該附件看起來也似乎是合法，以增加郵件的可信度。

點擊 PDF 中的“出價”按鈕後，受害者會進入一個與合法網站非常相似的欺騙性網路釣魚網站。該站台專作憑證收集。該站台也故意設置錯誤，以誘騙受害者多次輸入其憑證，然後重新轉向到實際的美國勞工部 (DoL) 站台以避免受害人起疑。

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)。

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。

2022/01/20

WhisperGate -- 偽裝成勒索軟體的磁碟清除程式，目前鎖定烏克蘭組織

被稱為 WhisperGate 新型磁碟清除程式的惡意軟體被發現並針對烏克蘭的多個組織。儘管惡意軟體偽裝成勒索軟體，但攻擊的動機似乎具有破壞性，因為無法恢復被清除磁碟的電腦。一旦執行，惡意軟體將覆蓋主引導記錄 (MBR) 並留下支付贖金的說明。由於惡意軟體會清除 MBR，因此支付贖金的說明只是掩飾攻擊真正目的的誘餌。

在攻擊的進一步階段，一個下載程式啟動了一個功能，它可以獲取一個文件，破壞託管在 Discord 頻道上的惡意軟體。這種破壞性惡意軟體將覆蓋包含任何預先配置副檔名列表所有檔案的內容。

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：

- MSIL.Downloader!gen7
- MSIL.Downloader!gen8
- SMG.Heur!gen
- Trojan Horse

- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Whispergate
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/01/20

Earth Lusca 威脅行動者發動的的惡意活動

一份有關名為 Earth Lusca 威脅參與者透過魚叉式網路釣魚和水坑等傳統社交工程攻擊活動的新報告浮出水面。攻擊者與另一個稱為 Winnti 的 APT 組織（也稱為 APT41、BARIUM 和 Blackfly）共享一些戰術、技巧、程序（TTP）以及其他別名。Earth Lusca 一直在對包括政府、教育和研究機構在內的各個領域以及世界各地的新聞媒體和電信公司進行攻擊。這些攻擊在部署 Cobalt Strike 載入程式和其他惡意軟體有效籌載（如 Winnti、ShadowPad 或 FunnySwitch 等）之前利用其行動中的已知漏洞。

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!gen4
- Hacktool
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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：

- 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。

2022/01/19

散布 Guildma／Astaroth 惡意軟體的惡意垃圾郵件行動

最近，發現另一個針對巴西用戶來散布 Guildma 惡意垃圾郵件行動。Guildma（也稱為 Astaroth）於 2017 年首次在真實環境中被發現，當時它被確定為一種非常普遍的拉丁美洲銀行木馬。該惡意軟體通常是遠端存取木馬 (RAT)、間諜軟體、密碼竊取程式和銀行惡意軟體的組合。如果惡意軟體成功載入到受害者的電腦上，感染範圍可能包括竊取登錄憑證、進行螢幕截圖以及攔截滑鼠和鍵盤點擊，這些點擊可用於進一步下載和執行更多惡意軟體。

郵件主旨的樣本：Referente ao Pedido-6569RWW6A5C - 3NA7P12P92FDTE5I9H13G0FNZIR1I

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!Im.B
- 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已於第一時間收錄於不安全分類列表中。

2022/01/19

隨著在勒索軟體中逐漸佔有一席之地，Noberus開始提供勒索軟體即服務

Noberus，也稱為 BlackCat、AlphaVM 或 AlphaV，是一個相對年輕但已經穩定且不斷增長的勒索軟體即服務參與者。這個惡意軟體是高度可配置的、跨平台的，並且是用 Rust 撰寫的。

Noberus 支援 Windows 和 Linux，通常透過第三方工具或易受攻擊的應用程式遞送。經由其配置，攻擊者可以調整其行為，以秘密破壞、加密和洩露目標資料。

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

基於機器學習的防禦技術：

- Heur.AdvML.*

2022/01/16

威脅警報：賽門鐵克提供對 CVE-2022-21907 的保護

作為一月份例行性修補更新的一部分，微軟最近修補“HTTP協定疊”(CVE-2022-21907) 中的一個關鍵遠端程式碼執行 (RCE) 漏洞，該漏洞是可以進行「蠕蟲繁殖」(Wormable)，感染速度異常快速，這也意味著它可以在沒有使用者互動的網路環境中自我傳播。利用此漏洞，未經身份驗證的攻擊者能夠利用 HTTP 協定疊 (HTTP.sys) 向目標伺服器發送經特殊設計的封包來處理封包。它會影響 Windows 10 和 Windows 11，以及 Server 2019 和 Server 2022，儘管預設情況下它不包括在 Windows Server 2019 和 Windows 10 版本 1809 中。

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：

- OS Attack: HTTP Protocol Stack CVE-2022-21907

2022/01/14

利用 APPX 檔案散布的勒索軟體：Magniber

根據最新報告，已發現 Magniber 勒索軟體利用偽裝成 Chrome 或 Edge 瀏覽器的更新套件 .appx 檔案（Windows 應用程式封裝檔案）散布。這種散布方法與 Magniber 攻擊者以前使用的戰術略有不同，因為這種勒索軟體變種過去主要透過利用 Flash 或 Internet Explorer 漏洞進行散布。

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
- Ransom.Magniber
- Trojan Horse
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3
- SONAR.RansomMgnibr!g2
- SONAR.Ransomware!g19

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：

- 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。

2022/01/14

BlueNoroff 使用偽造的 MetaMask 網頁瀏覽器擴充功能來竊取加密貨幣

BlueNoroff 是一個北韓的 APT 組織，過往以鎖定銀行業發動攻擊而聞名，但去年的報導似乎顯示該組織已經改弦易轍，他們現在瞄準了 MetaMask 等加密貨幣業務。MetaMask 是一個網頁瀏覽器擴充功能，允許用戶透過網頁瀏覽器存取和管理他們的以太坊錢包。該組織有不同的攻擊策略來啟動他們的行動，但觀察到橫向移動場景是利用偽裝加密貨幣交易軟體的一部分，期望它會誘使用戶安裝看起來合法的應用程式，隨後將導致後門攻擊。

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：

- CL.Downloader!gen195
- Downloader.Trojan
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- VBS.Downloader.Trojan
- WS.Malware.1
- WS.Malware.2
- W97M.Downloader

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。