保安資訊--今日最新(台灣時間2022/01/18)
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23萬0,700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。

點擊此處獲取--關於賽門鐵克原廠防護週報

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交互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。

2022/01/13
Coinbase 用戶面臨網路釣魚活動激增的風險

隨著加密貨幣對世界的開放程度越來越高，加密貨幣的受歡迎程度不斷提高，現在主要經紀人之客戶成為覬覦的對象。最近幾週，試圖竊取 Coinbase（用於購買、出售、轉移和存儲加密貨幣的線上平台）用戶憑證的網路釣魚攻擊有所增加。這些行動幕後的黑手已經建立了多個虛假的 Coinbase 網站，其中許多網站使用一種被稱為域名仿冒的技術。賽門鐵克觀察到惡意電子郵件和簡訊都被用作初始感染媒介，如果成功引誘，會將用戶重新轉導向到這些虛假網站。

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)。

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：

- Malicious Phishing Site: Phishing Suspicious Request 2

賽門鐵克的端點防護行動裝置版本 (IOS/Android)：

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) 重要來源之一的 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。

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。

2022/01/13
OceanLotus (*海蓮花) 使用網頁封存檔散布後門

已觀察到 OceanLotus 組織（也稱為 APT32 或 SealLotus）使用 MHT 和 MHTML 等網頁封存檔來散布後門惡意軟體。該組織正試圖透過使用這些較不起眼的檔案類型來躲避檢測。初始感染媒介是一個 rar 壓縮檔案，其中包含網頁封存檔案，然後擴展具有惡意 VBA 巨集的 Office 文件，這些文件再利用後門感染系統。

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.NPE
- W97M.Downloader
- WS.Malware.1

2022/01/13
MuddyWater APT 組織對中東組織的網路攻擊

根據美國網路司令部最近一份報告，被稱為 MuddyWater (又名 Seedworm) 的 APT 組織一直在利用各種工具和技術在世界各地進行攻擊。至少從 2017 年 2 月開始活躍，主要針對中東的組織，但也包括歐洲和北美的企業。據觀察，該組織將攻擊重點放在能源、政府和電信部門。該組織最近使用的工具包括 PowGoop 加載程序惡意軟體、Mori 後門、各種隧道和 JavaScript 工具。

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：

- Hacktool
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2022/01/13
惡意垃圾郵件行動中的 RAT Nanocore、Netwire 和 AsyncRAT

2021 年 10 月，一個研究團隊發現一個惡意垃圾郵件行動，總共出現了三個遠端存取木馬(RAT)，分別名為 nanocore、netwire 和 asyncRAT。報告中的詳細資訊顯示，大多數受害者位於美國、義大利和新加坡。有人提到，攻擊者的 C&C 伺服器正在濫用 Microsoft Azure 和 Amazon Web Services 的雲端服務，以降低行動成本，並使防禦者更難追踪其運作。

帶有惡意 ZIP 附件的網路釣魚電子郵件將成為其初始攻擊媒介，在該壓縮檔中是包含惡意 JS、VBS 和批次檔腳本載入程式的 ISO 映像檔。載入程序將幫助建立 C&C 通信以獲取 RAT 有效籌載，目的是從受感染的機器或設備中竊取資料。

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：

基於行為偵測技術 (Snoar) 的防護：

- SONAR.SuspDataRun
- SONAR.Zbot!gen8

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Infostealer
- ISB.Downloader!gen
- ISB.Downloader!gen52
- ISB.Downloader!gen53
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan.Gen.NPE
- Trojan Horse
- Trojan.Nancrat
- Trojan.Nancrat!g1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

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: Backdoor.Ratenjay.C/D Activity
- System Infected: JS.Downloader Activity 34
- System Infected: Netweird.B Activity 2
- System Infected: Trojan.Backdoor Activity 629
- System Infected: Trojan.Nancrat Activity 2
- System Infected: Trojan.Revetrat Activity 2

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。

2022/01/13
網路釣魚導致資料竊取--韓國知名入口網站也遭殃

韓國一家網際網路公司 Kakao Corp，最近遭受具有破壞憑證和提供惡意下載雙重功能的嚴重網路釣魚攻擊。如果用戶點擊電子郵件中的鏈接，他們將首先看到一個相似頁面，以引誘輸入他們的帳戶憑證。此時，如果用戶提供他們的憑證，則該帳戶將被盜用。

此外，如果用戶從該網路釣魚站瀏覽網頁，則會下載一個看起來像是來自另一個韓國入口網站：Naver 提供的保護工具。如果運行此程序，電腦將感染竊密惡意程式，該竊密惡意程式將長駐在電腦中，從系統和用戶操作中收集詳盡的資訊。

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 Horse

基於行為偵測技術 (Snoar) 的防護：

- SONAR.SuspBeh!gen657

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/12
Kuzuluy 網路釣魚變種，鎖定 PayPal 憑證

網際網路上有無數可供公眾使用的網路釣魚工具包，並且多年來一直在進行純粹的網路釣魚活動。這種形式的網路犯罪很容易被吸收，以至於惡意投入者的數量比惡意軟體大得多。多年來，最令人垂涎的憑證之一是 PayPal。在最近一個例子中，據報導，在歐洲發現了一種名為 Kuzuluy 的舊網路釣魚工具包的變種。攻擊者試圖通過這些工具包生成的虛假 PayPal 網站來使受害者輸入其 PayPal 憑證。

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。

2022/01/12
TellYouThePass 被發現用 Golang 編寫用於跨平臺勒索

TellYouThePass 勒索軟體已被發現利用最近 Log4Shell 的漏洞做有效載荷。已部署的最新版本是用 Golang 編寫，並且已經觀察到 Windows 和 Linux 跨平臺變種。這個新版本還試圖透過其內部核心功能的隨機化來避免檢測和分析。

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.Cryptlocker!g75

檔案型(基於回應式樣本的病毒定義檔)防護：

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

2022/01/12
發現新型的多平臺後門 SysJoker

一種被稱為 SysJoker 的新型多平臺後門已經在網路上被觀察到。該惡意軟體針對 Windows、Linux 和 macOS 平臺偽裝成系統更新套件。一旦進入受感染的系統，SysJoker 將收到來自攻擊者的 C&C 伺服器的指令。根據那些資料，它可能會下載並執行其他惡意軟體有效載荷。

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

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。

業界公認 **保安資訊**--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost
服務電話：0800-381500｜+886 4 23815000｜http://www.savetime.com.tw