保安資訊--今日最新(台灣時間2023/04/20)
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)。

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 600 台受保護端點上總共阻止了 9,110 萬次攻擊。這些攻擊中有 91% 在感染階段前就被有效阻止：**(2023/04/17)**

- 在**15**萬**2,500**台端點上，阻止了**3,720**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26**萬**9,800**台端點上，阻止了**1,950**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5**萬**5,300**台**Windows**伺服主機上，阻止了**1,440**萬次攻擊。
- 在**8**萬**3,500**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**9,000**台端點上，阻止了**100**萬次嘗試掃描在**CMS**漏洞。
- 在**6**萬**2,800**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**26**萬**2,700**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6**萬**2,000**台端點上，阻止了**220**萬次加密貨幣挖礦攻擊。
- 在**15**萬**2,600**台端點上，阻止了**1,170**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,600**台端點上，阻止了**9**萬**6,900**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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2023/04/18

防不勝防～macOS平台也出現Lockbit勒索軟體

已發現一種針對 macOS 平台的新 Lockbit 勒索軟體。該 macOS 勒索軟體案例似乎是同源於 Lockbit 的 Linux 加密技術，並且已彙整的紀錄中，幾乎都是設定不周延脆弱的 macOS 環境。該惡意軟體似乎仍在開發中，尚無部署到所有不同版本的 macOS上的能耐。鑑於 Lockbit 的加密技術已經在多種不同作業系統 (包括 Windows、Linux、ESXi) 上攻城掠地，在真實網路上的 macOS 環境擴張版圖，也只是時間早晚的問題。

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：
- OSX.Ransom.Lockbit
- Trojan Horse

2023/04/18

變種更是棘手～BlackBit勒索軟體

BlackBit 是 LokiLocker 勒索軟體家族的變種，具有許多相同的特徵。BlackBit 偽裝成 svchost.exe 系統檔案 (SVCHOST.EXE 是從動態連結程式庫 (DLL) 執行之服務的一般性主處理程序名稱，由於這個程序是開啟 Windows 服務的重要檔案，因此之前也曾有疾風等多種病毒，會利用SVCHOST.EXE 來達到入侵或破壞等目的，並加密用戶的檔案，而被加密的檔案會被新增 .blackbit 副檔名。與 LokiLocker 類似，該惡意軟體具有在受感染電腦上常駐的特性、停用 Windows Defender 安全軟體、停止各種系統服務和程序以及刪除磁碟陰影複製 (Volume Shadow Copy) 的功能。成功加密後，BlackBit 隨後置放贖金支付說明，建議受害者通過電子郵件聯繫威脅者。

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(SONAR)的防護：
- AGR.Terminate!g2
- SONAR.Cryptolocker!g42
- SONAR.SuspBeh!gen93
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g21
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：
- Downloader
- Trojan Horse
- Trojan.Gen.MBT

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：
- Attack: Ransom.Lockbit Activity
- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 595
- System Infected: Trojan.Backdoor Activity 634
- 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。

2023/04/10

防護亮點：賽門鐵克網路層入侵預防(IPS)技術有效封鎖端點上的SMB攻擊

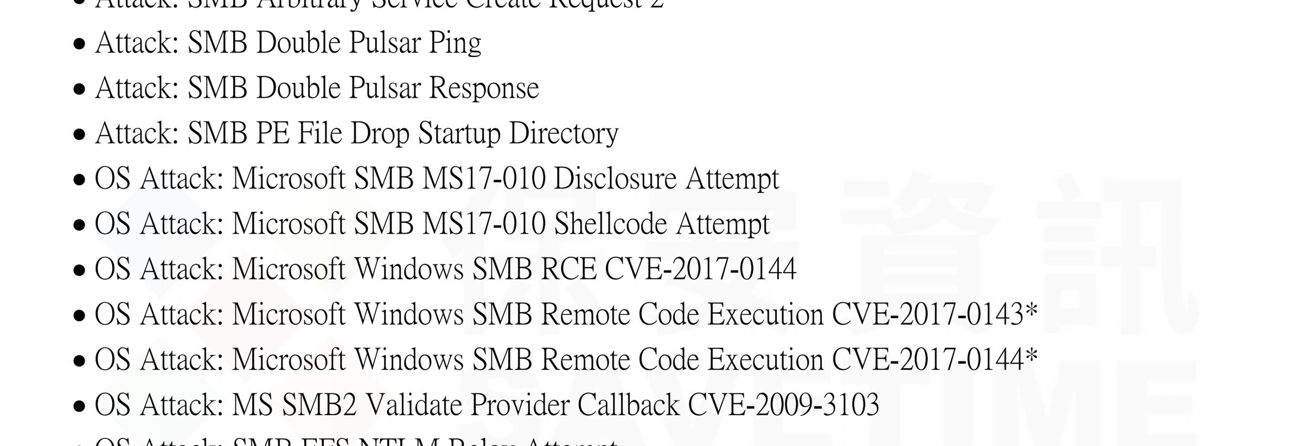
～防護亮點～

伺服器訊息區塊 (SMB:Server Message Block) 一種用戶端 (Client)--伺服器 (Server) 應用層網路傳輸協定，主要由 Windows 作業系統使用，但也在 Linux 和 macOS 電腦上使用，主要功能是讓網路上的機器能夠共享檔案、印表機、串列埠及通訊等資源。由 IBM 早在 1980 年代早期就開發出來，隨即備受網路工程師矚目並廣受應用，其通訊是透過使用 TCP 139 和 445 埠號。直到今天，SMB 仍然是工作場所共享檔案的最常見方法之一。但是，儘管多年來該協議已多次更新以滿足不斷變化的網路要求，但許多設備仍在運行較舊、安全性較低的版本，這不可避免地使其成為網路犯罪分子的主要目標。

SMB 攻擊是一種網路攻擊，其目標是 SMB 傳輸協定中的漏洞，以便獲得對網路未經授權的存取權限，再進展到內網的橫向移動（橫向移動是攻擊者用來推進攻擊鏈從初始入口點進入網路的伎倆）獲得對其他網路資源的存取權限。兩個舉世皆知的 SMB 攻擊--包括 2017 年的“永恆之藍”漏洞利用 (CVE-2017-0144)，同樣惡名昭彰“WannaCry”勒索軟體利用它產生巨大影響，以及最近 SolarWinds 發動供應鏈攻擊，也利用 SMB 協議中的漏洞。

常見的 SMB 攻擊包括：

* SMB 暴力攻擊：暴力攻擊是一種反覆試驗不同帳號與密碼以獲取存取目標電腦的方法。可以手動完成 ，也可以透過自動化工具完成。
* SMB 中繼攻擊：一種中間人 (MITM) 攻擊，攻擊者攔截兩台機器之間的 SMB 流量，再將流量中繼到攻擊者操控的第三方電腦。這允許攻擊者無需有效憑證即可存取目標系統。
* SMB 蠕蟲化攻擊：這些攻擊使用通過利用 SMB 協議中的漏洞，在網路中傳播惡意軟體。一旦惡意軟體感染了一個系統，它就可以傳播到網路上的其他系統。
* SMB 阻斷服務攻擊：此類攻擊涉及用大量 SMB 請求讓目標系統無法負荷，導致系統崩潰或影響其可用性。



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 **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

網路層攔截防護技術的特徵檔名稱：
- Attack: Bluwimps SMB Activity
- Attack: Fake SMB Server Response
- Attack: SMB Arbitrary Service Create Request 2
- Attack: SMB Double Pulsar Ping
- Attack: SMB Double Pulsar Response
- Attack: SMB PE File Drop Startup Directory
- OS Attack: Microsoft SMB MS17-010 Disclosure Attempt
- OS Attack: Microsoft SMB MS17-010 Shellcode Attempt
- OS Attack: Microsoft Windows SMB RCE CVE-2017-0144
- OS Attack: Microsoft Windows SMB Remote Code Execution CVE-2017-0143*
- OS Attack: Microsoft Windows SMB Remote Code Execution CVE-2017-0144*
- OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3103
- OS Attack: SMB EFS NTLM Relay Attempt
- OS Attack: SMB Validate Provider Callback CVE-2009-3103
- OS Attack: Windows SMBv3 CVE-2020-1206
- System Infected: Bad Reputation File SMB Request

網路層稽核管理技術的特徵檔名稱：**
- Audit: Bad Reputation File SMB Request
- Audit: Microsoft Compressed SMB Packet
- Audit: SMB Admin Share Connect Request
- Audit: SMB Bruteforce Attempt
- Audit: SMB Exchange Server WebShell Access Attempt
- Audit: SMB Request From External Host
- Audit: SMB Suspicious DLL Create Attempt
- Audit: SMB Suspicious Folder File Creation
- Audit: SMB Unimplemented Trans2 Subcommand
- Audit: SMB Windows Print Spooler RpcAddPrinterDriverEx Attempt
- Audit: SMBv1 NTLM Authentication Attempt
- Audit: SMBv1 Traffic Request
- Audit: SMBv2 NTLM Authentication Attempt
- Audit: Suspicious SMB Client Activity
- Audit: Suspicious SMB Client Request*
- Audit: Suspicious SMB Server Response

* *這表示存在多個類似名稱的檢測，例如：Audit: Suspicious SMB Client Request2、Audit: Suspicious SMB Client Request3……等。*

** *SEP 的稽核特徵檔旨在提高對網路中可能不需要的流量認識。預設情況下，它們不會攔截。管理員可以查看網路中 IPS 事件日誌所記錄這些稽核事件，並決定是否配置相應的稽核特徵檔來攔截流量。*

要了解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

2023/04/17

Domino後門程式暗助Project Nemesis竊密程式暗度陳倉

在真實網路環境發現一種名為 Domino 的全新惡意後門程式。該惡意軟體與 FIN7 駭客集團有關，並在最近一個利用 Dave 惡意軟體載入程式的行動中傳播。根據最新報告，Domino 顯示一些與 Lizar 工具包（也稱為 DiceLoader）的程式碼重疊。該後門程式會收集遭駭系統的基本資訊，連接到預先設定好的 C&C 伺服器來下載攻擊鏈最後階段所需的惡意酬載，在這一次案件裡是基於 .NET 被命名為 Project Nemesis 的竊密程式。這種竊密程式的惡意酬載可以從網路瀏覽器、VPN 應用程式、聊天應用程式或加密貨幣錢包收集各種資訊的功能。

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：

基於行為偵測技術(SONAR)的防護：
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：
- Heur.AdvML.A
- 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: Trojan.Backdoor Activity 634
- 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。

2023/04/17

參閱說明書(RTM：Read The Manual)加密勒索軟體

RTM (參閱說明書) 加密勒索軟體是最近在威脅環境下觀察到的另一種勒索軟體即服務 (RaaS) 之惡意軟體。該勒索軟體採用多執行序加密技術，能夠刪除磁碟陰影複製 (Volume Shadow Copy)，還可以停止／禁用某些系統程序 (process) 和服務 (Service)。檔案被加密完成，將會置放贖金支付說明檔並更改受感染電腦的佈景主題 (桌布)，來示意受害者已經遭駭並建議他們聯繫攻擊者。最終，該勒索軟體在刪除遭感染電腦的日誌檔之前，還會先清空所有日誌內容，讓事後調查更困難。

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(SONAR)的防護：
- SONAR.CryptoLocker!g35
- SONAR.CryptoLocker!g36
- SONAR.Ransomware!g7
- SONAR.Ransomware!g16

檔案型(基於回應式樣本的病毒定義檔)防護：
- Ransom.Generic.1

基於機器學習的防禦技術：
- Heur.AdvML.B

2023/04/17

Kadavro Vector勒索軟體

Kadavro Vector 是與 NoCry 勒索軟體家族相關的全新索軟體。被該勒索軟體加密後檔案會被新增 .vector_ 的附檔名，並要求以門羅幣 (Monero，XMR) 來支付贖金。Kadavro Vector 透過偽造成 Tor 加密瀏覽器的安裝程式檔來散播感染。

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(SONAR)的防護：
- AGR.Terminate!g2
- SONAR.Ransomware!g34
- SONAR.SuspBeh!gen752
- SONAR.SuspBeh!gen93
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：
- Scr.Malcode!gdn32
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：
- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!200

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: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 634

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。

2023/04/14

Remcos遠端存取木馬(RAT)以美國所得稅納稅申報日為幌子發動惡意行動

最近 Remcos 遠端存取木馬 (RAT) 在威脅環境中相當活耀，據報導觀察到它分佈在美國與稅收相關的惡意電子郵件中。隨著美國稅收季節接近尾聲，攻擊者試圖透過客戶提供有關稅務文件的訊息來吸引從事報稅和金融服務的公司。網路釣魚電子郵件包含偽裝成 .pdf 檔案的捷徑檔，這些檔案在執行時會啟動後續感染鏈並最終安裝 Remcos 遠端存取木馬 (RAT) 的有效籌載。

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：

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：
- Trojan Horse
- Trojan.Gen.MBT

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。

2023/04/14

Legion--採用Python撰寫的身分驗證資料搜集工具

Legion 是一種採用 Python 撰寫的身分驗證資料搜集工具，並在 Telegram 平台上銷售。這種駭客工具的主要功能是從各種網路服務和配置錯誤的網路伺服器中檢索身分驗證資料，可用於發動大規模惡意垃圾郵件行動。Legion 以各種網路服務為目標，包括 AWS、雲端通訊平臺 Twilio、Nexmo 雲端平台、SES、電子郵件 API 服務供應商 Mailgun 等。該駭客工具還具有列舉易受某種漏洞攻擊的 SMTP 伺服器、遠端程式碼執行或開採利用有漏洞的 Apache 版本功能。

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：
- Hacktool
- WS.Malware.2

2023/04/14

具有停用安全機制的--Chameleon全新行動金融木馬程式

Chameleon 是今年出現在威脅領域的全新行動金融木馬程式。該惡意軟體已經針對澳大利亞和波蘭的安卓手機平台用戶發動惡意行動，惡意軟體安裝檔分別偽裝成名為 Coinspot 的加密貨幣APP 或名為 IKO 的銀行 APP。Chameleon 功能包括鍵盤側錄、擷取簡訊內容、竊取 cookie 等等。該惡意軟體還採用「反模擬」（anti-emulator）技術，並能夠在受感染的 Android 裝置上停用 Google Play Protect 安全功能。

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：

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.Reputation.2
- AppRisk:Generisk

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。