保安資訊--本周(台灣時間2023/01/27)
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 84 萬 6,100 台受保護端點上總共阻止了 1.018 億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/01/22)**

- 在**15**萬台端點上，阻止了**4,200**萬次嘗試掃描**Web**服務器的漏洞。
- 在**27**萬**2,800**台端點上，阻止了**2,100**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6**萬**100**台**Windows**伺服主機上，阻止了**1,800**萬次攻擊。
- 在**9**萬**1,100**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**120**萬次嘗試掃描在**CMS**漏洞。
- 在**6**萬**6,500**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**30**萬**300**台端點上，阻止了**660**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1**萬**6,500**台端點上，阻止了**250**萬次加密貨幣挖礦攻擊。
- 在**13**萬**1,500**台端點上，阻止了**114**萬次向惡意軟體**C&C**連線的嘗試。
- 在**3,700**台端點上，阻止了**14**萬**5,900**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。

2023/01/27
ManageEngine遠端程式碼執行(RCE)漏洞：CVE-2022-47966已在真實網路環境上被開採利用

CVE-2022-47966 是一個未經身份驗證的遠端程式碼執行(RCE)漏洞，影響二十多個 Zoho ManageEngine 產品，例如：ADManager Plus、ADSelfService Plus、ServiceDesk Plus、Password Manager Pro、Remote Access Plus…等。如果 RCE 漏洞被成功利用，遠端攻擊者可以在易受攻擊的伺服器上執行任意指令。雖然原廠已經為受影響的產品釋出一系列更新修補，但據報導該漏洞已被廣泛開採利用。

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：

- Web Attack: Zoho Manageengine RCE Vulnerability CVE-2022-47966

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS(data Center Security) 內建的強化策略就能針對利用 CVE-2022-47966 的威脅提供零時差保護。預設最小權限與最低資源機制的沙箱運行環境可防止安裝 webshell 和惡意軟體工具、並可完全阻絕任意應用程式、系統命令的執行。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2023/01/27
十八般武藝都有～Mimic勒索軟體

Mimic 是一種在真實網路環境上發現的全新勒索軟體。該惡意軟體濫用運行在 Windows 環境名為“Everything”的第 3 方檔案名稱搜尋引擎公用程式的 API。該惡意軟體利用 Everything32.dll 查詢受感染電腦上的檔案，再由惡意軟體加密目標檔案。Mimic 包括各種功能，例如：收集系統資訊、停用 Windows Defender 防護、繞過 UAC、終止系統程序和刪除陰影複製 (shadow copies) 等。Mimic 勒索軟體利用多執行緒加密並將 .quietplace 副檔名附加到被加密檔案。

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
- Trojan.Gen.2
- 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

2023/01/27

加密貨幣剪貼簿竊密器：Stickman，覬覦加密錢包

在過去幾週裡，賽門鐵克在威脅環境發現另一個加密貨幣剪貼簿竊密器 (Clipper)。它的真名尚不清楚，但我們暫時稱它為“Stickman the Clipper”，因為它的 C&C 登錄頁面有一個攜帶錢包的火柴人。這種威脅背後參與者主要透過偷渡式下載將其作假冒軟體和駭客工具進行散佈。如今，加密貨幣剪貼簿竊密器 (Clipper) 非常普遍，因為它們趁勢利用加密貨幣日益增長的使用和價值，即使加密貨幣圈已因主要的加密貨幣交易所突然一夕之間面臨倒閉破產而風聲鶴唳。

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.Banclip
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/26

以自動感應酒精消毒機、自動感應免按壓皂液器為誘餌的攻擊行動，讓竊密惡意軟體Agent Tesla，在全世界橫行無阻

隨著全世界繼續對 COVID-19 疫情的關注，世界各地的許多組織和企業都增加預算，以應對工作場所的病毒。至少某些組織已經實施的一項措施是使用自動感應酒精消毒機、自動感應免按壓皂液器，以促進手部衛生並幫助減少病毒的傳播。

在過去兩年中，網路犯罪分子利用這一點。在最近的一個例子中，賽門鐵克觀察到一個聲稱來自這些自動感應酒精消毒機、自動感應免按壓皂液器公司的攻擊者，在以訂單為主題的惡意電子郵件行動中，針對世界各地的組織，包括日本、香港、新加坡、中國、以色列、美國、印度和英國。如果成功引誘受害者，他們最終將受到惡名昭章的 Agent Tesla 惡意軟體之危害。

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.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/26

假冒SMBC(三井住友銀行)的網路釣魚行動瞄準日本企業和消費者

SMBC (三井住友銀行) 是日本的一家主要銀行，它成為經常性網路釣魚詐騙的主要目標。賽門鐵克最近發現一個網路釣魚電子郵件攻擊行動 (主旨：【三井住友】カード株式會社からの急のご連接)，歹徒冒充 SMBC 並使用類似於 SMBC Vpass 的虛假登錄網站來竊取用戶的財務資訊。此攻擊行動勢必對個人客戶和企業造成嚴重後果。這些釣魚網站的一些例子是：

- sqrmnwae[.]cf
- glutfgua[.]ga
- vmkikuxe[.]ga

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/01/26

STOP／DJVU 勒索軟體仍在真實網路環境上傳出災情

STOP 勒索軟體 (也稱為 DJVU) 在過去幾年中一直很活躍，並且這種惡意軟體的新變種不斷在真實網路環境上被發現，危害消費者和企業用戶。眾所周知，STOP 勒索軟體主要透過破解軟體和偷渡式下載進行散佈。該惡意軟體將四個字母的副檔名附加到被加密檔案。最近發現的此勒索軟體變種使用的一些副檔名包括：.zoqw、.zouu、.poqw、.mzqw、.mzop 和 .mztu。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Packed.Generic.528
- Ransom.Pots
- Trojan.Gen.2
- 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.B!100
- 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: Ransom.DJVU Activity 4
- System Infected: Trojan.Backdoor Activity 634

2023/01/25

惡意軟體透過Google Ads廣告投放，來擴大散佈

最近幾週，透過濫用 Google Ads 廣告投放平台傳播的不同惡意軟體變種數量顯著增加。感染鏈通常非常簡單直接--用戶在搜尋要下載的特定軟體時，當點擊 Google 搜尋廣告，會將他們帶到假冒的合法的下載網站。攻擊者將惡意可執行檔偽裝成已知合法應用程式或工具的安裝程式，例如：Zoom、LibreOffice、Rufus、7-Zip、WinRaR、VLC-Player、Notepad++……等。最近攻擊行動一直在以這種方式大範圍分發此惡意軟體家族。僅舉幾個最近觀察到的惡意軟體：Rhadamanthys Stealer、BatLoader、Ursnif、IcedID、Redline Stealer、Vidar Stealer 等。

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
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

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：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22
- Malicious Site: Malicious Domain Request 114

- System Infected: Trojan.Backdoor Activity 592
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 735

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。

2023/01/25

Realtek SDK 2021漏洞仍被用於惡意軟體散佈

Realtek Jungle SDK (CVE-2021-35394) 是一個於 2021 年 8 月被揭露的遠端程式碼執行 (RCE) 漏洞。如果成功被開採利用，攻擊者可以完全控制受感染的設備，利用它們進行 DDoS 攻擊或遠端程式碼執行(RCE)。雖然該漏洞已被揭露超過 1.5 年，但據報導，它仍在真實網路環境上被利用來傳播各種惡意軟體，包括 Mirai、Gafgyt、Mozi 和稱為 RedGoBot 的 DDoS 殭屍網路。

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：

- Linux.Lightaidra
- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

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: Realtek Jungle SDK RCE CVE-2021-35394

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。

2023/01/24

Vice Society駭客集團最近所發動的勒索軟體散佈行動

Vice Society (又名 DEV-0832) 勒索軟體集團在威脅領域仍然很活躍，他們的攻擊主要集中在醫療保健、教育和製造業領域。眾所周知，這個駭客集團會部署各種勒索軟體有效籌載，包括 Zeppelin、HelloKitty、RedAlert 或其最新變種 PolyVice。Vice Society 還在入侵初期 (Initial Access)、橫向移動或資料滲出階段使用不同的工具。其中一些工具包括 Cobalt Strike、Mimikatz、Rubeus 或 Kape。根據最新報告，Vice Society 駭客集團最近發起的勒索軟體散佈行動主要鎖定巴西、阿根廷、瑞士和以色列的組織。

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：

- AGR.Terminate!g2
- SONAR.Cryptlocker!g42
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gm5
- Downloader
- Hacktool.Mimikatz
- Hacktool.Rubeus!gen1
- Ransom.Zeppelin
- Trojan Horse
- Trojan.Gen.2
- 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

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。

2023/01/23

Magniber勒索軟體攻擊行動鎖定歐洲國家

根據最新報導，在最近針對多個歐洲國家用戶的攻擊中發現 Magniber 勒索軟體。攻擊者利用惡意廣告作為主要散佈手段。潛在受害者會被引導下載包含偽裝成安全更新或軟體更新修補的惡意 .msi 檔案的 .zip 壓縮檔。僅在去年，Magniber 勒索軟體就透過各種不同的檔案格式傳播，包括已簽章的 .appx 檔案、.msi 和 .js/.jse 檔等。

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.SuspLaunch!g193

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Magniber

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/23

Royal依舊是最多產的勒索軟體變種之一

Royal 是 2022 年初問世的惡意軟體家族，時至今日仍然是最多產的勒索軟體變種之一。Royal 幕後的駭客集團鎖定包括醫療保健在內的各個行業。Royal 的感染鏈以利用廣泛的技術和工具而聞名，包括目標式「回撥網釣」(Callback Phishing) 攻擊、各種啟動器和開放原始碼工具或用於多階段攻擊的額外有效籌載。Royal 勒索軟體具有刪除備份和磁碟陰影複製 (Volume Shadow Copy) 的功能，並且採用多執行緒來提高加密效能。據報導，最新的 2023 Royal 散佈行動利用 Citrix 漏洞 CVE-2022-27510 作為勒索軟體攻擊的初始訪問階段的破口。

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.RansomRoyal!g1
- SONAR.RansomRoyl!gen1
- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.gen!g4
- Ransom.Royal
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

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.Gen Activity 47

2023/01/23

Gigabud安卓手機行動遠端存取木馬(RAT)

Gigabud 是最近被發現 Android 安卓手機行動遠端存取木馬 (RAT)。該惡意軟體具有多種功能，例如：收集受感染設備的相關資料、竊取銀行憑證、濫用輔助服務 (Accessibility Services) 和螢幕錄製……等。Gigabud 最初出現在 2022 年 7 月針對泰國用戶的攻擊中。後來它的使用範圍擴大到許多其他國家／地區。該惡意軟體偽裝成知名銀行或公認的政府單位相關的手機應用程式 APP 進行散佈。

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.1
- Android.Reputation.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／IP位址已於第一時間收錄於不安全分類列表中。