保安資訊--本周(台灣時間2025/01/24)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 37 萬 300 台受保護端點上總共阻止了 4,140 萬次攻擊。這些攻擊中有 78.8% 在感染階段前就被有效阻止：**(2025/01/20)**

- 在**7萬9,300**台端點上，阻止了**1280萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬4,800**台端點上，阻止了**680萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,300**台**Windows**伺服主機上，阻止了**5萬7,000**次攻擊。
- 在**4萬8,500**台端點上，阻止了**160萬**次嘗試掃描伺服器漏洞。
- 在**1萬300**台端點上，阻止了**69萬7,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬400**台端點上，阻止了**230萬**次嘗試利用的應用程式漏洞。
- 在**9萬1,700**台端點上，阻止了**190萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,900**台端點上，阻止了**93萬3,200**次加密貨幣挖礦攻擊。
- 在**11萬400**台端點上，阻止了**800萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**512**台端點上，阻止了**8萬8,400**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。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 16 萬 3,300 個受保護端點上阻止了總計 690 萬次攻擊。**(2025/01/20)**

- 使用網頁信譽情資，在 **156.4K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **17.4K** 個端點上 **284.8K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **7.2K** 個端點上攔截 **144K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **193** 個端點上攔截 **4.3K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2025/01/23

Murdoc殭屍網路～源於知名Mirai殭屍網路的後繼新變種

Murdoc 殭屍網路～源於知名 Mirai 殭屍網路的後繼新變種，已被發現涉入近期的網路攻擊行動。該行動利用 ELF 二進位檔和 shell scripts 攻擊各種基於 *nix 的系統，例如：IoT 裝置和 IP 攝影機等。shell scripts 部署到設備上，從 C&C 伺服器下載並執行 Murdoc 殭屍網路的有效酬載。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen277
- Linux.Mirai
- Linux.Mirai!g2
- Scr.Malcode!gen107
- Trojan.Gen.NPE
- 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。

2025/01/22

司空見慣的伎倆，還是許多人上當：駭客組織使用電子郵件炸彈和釣魚攻擊攻擊

研究人員發現兩個惡意軟體駭客組織，其背後牽涉到電子郵件炸彈以及濫用 Microsoft Teams 通訊和遠端控制工具。這些攻擊從目標電子郵件炸彈攻擊行動開始，攻擊者會冒充 IT 人員透過 Teams 與受害者連絡。然後，告訴受害者可以使用 Teams 螢幕分享選項或「快速協助」來解決最近的垃圾郵件問題。一旦建立遠端存取權限後，攻擊團體就會採取不同的策略，其中一個利用 Java／Python 威脅來進一步感染，而另一個則採用側載 DLL。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- 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。

2025/01/22

Nnice勒索軟體

Nnice 是最近在真實網路上發現的全新勒索軟體。該惡意軟體會加密使用者資料，並在加密檔案中冠上「.xdddd」副檔名。除了以「Readme.txt 」文字檔的形式注入勒索 (贖金支付) 說明之外，該勒索軟體還會變更桌面背景，以顯示使用者的檔案已被加密，並向受害者索取贖金。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/01/22

全新駭客組織Silent Lynx：以鎖定吉爾吉斯政府和金融單位闖出名號

一個名為 Silent Lynx 的全新駭客組織被發現以吉爾吉斯及鄰近國家的組織為目標。該駭客組織採用一系列技術，例如：惡意電子郵件附件、誘騙文件和常駐機制以維持對受攻擊系統的存取權。Silent Lynx 使用高明的多階段攻擊方法，包括 ISO 檔案、C++ 載入器、PowerShell 腳本和 Golang 類型的植入程式，主要以政府單位、銀行和外交部門動為目標，同時利用聯合國主題為誘餌和員工獎金方案來欺騙受害者。Silent Lynx 濫用 Telegram 機器人作為指揮與控制 (C&C) 以及資料外洩的媒介。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!300

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2025/01/21

以MintsLoader惡意軟體載入程式主導的網路攻擊行動，搭配StealC和BOINC型態的惡意軟體鎖定能源產業

MintsLoader 是一種複雜的惡意軟體載入程式，它採用先進的技術來逃避偵測，並提高其營運績效。受影響的行業包括美國和歐洲的電力、天然氣和石油行業，以及律師事務所和法律服務行業。當受害者點擊釣魚電子郵件中的連結時，惡意的 JScript 檔案就會被下載，並開始部署 StealC 和柏克萊開放式網路計算平台 (Berkeley Open Infrastructure for Network Computing--簡稱 BOINC) 用戶端等下一階段的有效酬載。這些有效酬載的組合會擷取瀏覽器、應用程式、加密錢包的敏感資料，然後外洩到 C&C 伺服器。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!aat171
- Trojan.Gen.MBT
- Trojan Horse
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2025/01/21

防護亮點：駭客想搭便車，門都沒有--賽門鐵克持續領先的SONAR行為防護技術有效偵測和封鎖惡意程序注入與程序挖空

程序注入與程序挖空伎倆

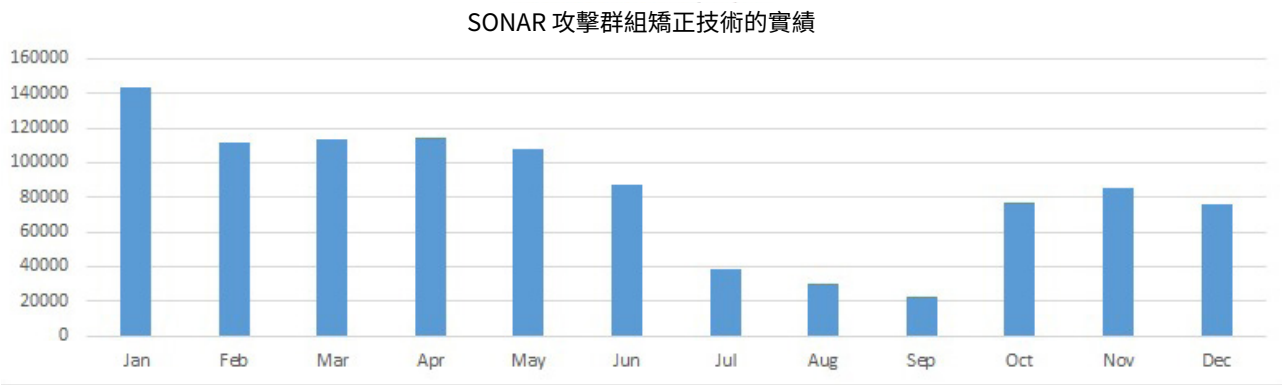
就像最近在 DarkGate 惡意木馬病毒程式攻擊事件中看到，駭客通常會加入一個元件，利用受信任的程序來推進攻擊鏈或傳送有效酬載。程序注入和程序挖空是用來攻擊受信任程序和逃避偵測的兩種伎倆。即使偵測並移除明顯的惡意程序，這些「遭入侵」程序仍可在背景中繼續惡意軟體攻擊。

SONAR(Symantec Online Network for Advanced Responce--前瞻回應線上網路) 是賽門鐵克的一種行為偵測的技術，可以在建立病毒定義檔及間諜軟體偵測定義檔前，阻止惡意程式碼侵入。行為防護會持續監控所有程序，無論是否受信任。行為分析這種即時防護可在電腦上執行應用程式時偵測潛在惡意的行為。行為分析使用啟發式技術及信譽資料來偵測新出現和不明威脅。行為分析提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測惡意行為，從而解決威脅。我們的安全回應工程師持續專注地研究駭客為了在您的網路立足而使用的最新技術。最新的啟發式技術和防護內容會透過線上自動更新機制 (Live Update) 每週傳送 4 次。

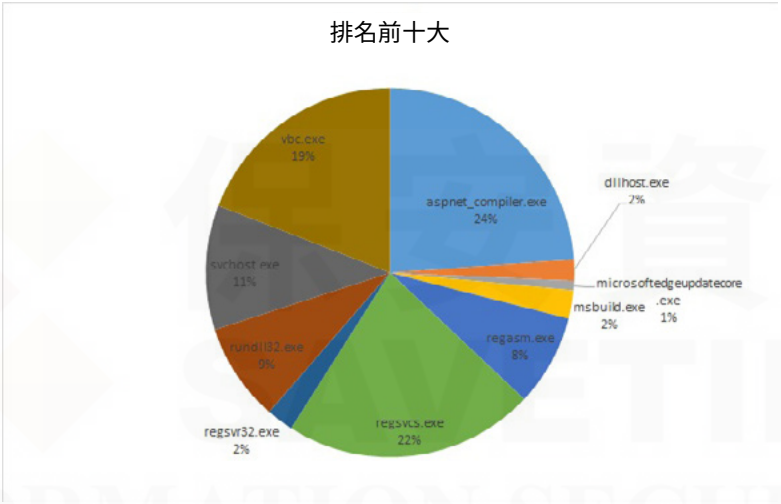
下面圖表顯示 2024 年的資料，證明 SONAR 在偵測和封鎖這些程序注入和程序挖空攻擊方面卓有成效。一旦偵測到「受攻擊」的程序並阻擋惡意行為，SONAR 攻擊群組矯正技術 (Attack Group Remediation--AGR) 就會自動啟動，確保整個攻擊鏈被瓦解。

攔截程序注入與挖空的數量

SONAR攻擊群組矯正技術(Attack Group Remediation-AGR)有效解除程序注入或程序挖空的可信任程序



最常遭受程序注入與程序挖空伎倆攻擊的受信任程序



欲了解何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？請點擊此處。
欲了解如何管理行為分析 (SONAR)，請點擊此處。

2025/01/21

DoNot Team威脅組織推出安卓平台全新惡意軟體：Tanzeem

以安卓平台的 Tanzeem 手機／行動裝置惡意軟體闖出名號的 DoNot Team 威脅組織，正當紅。此惡意 APP 主要利用 OneSignal，OneSignal 是企業用來傳送推送通知、電子郵件、應用程式內訊息和簡訊的熱門客戶參與平臺。惡意 APP 安裝後，會顯示一個假的聊天畫面，提示受害者點擊一個「Start Chat」的按鈕。這樣做會觸發一則訊息，指示受害者授予存取 API 服務權限，進而允許其執行各種惡意行動。此進一步存取有助於收集新增的敏感資訊，例如：通話記錄、聯絡人、簡訊內容、精確位置、帳戶資訊以及外部儲存中的檔案。其他功能包括擷取螢幕錄影以及與 C&C 伺服器建立連線。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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

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。

2025/01/21

弱肉強食、適者生存：Redtail挖礦惡意軟體以幹掉競爭對手而出名

Redtail 是一種應變性很強的惡意軟體，它會利用先進的策略隱蔽地安裝在遭入侵的系統上，以持續利用系統進行未經授權的加密貨幣挖礦。它利用兩個額外的腳本，能夠在各種 CPU 架構上執行：一個腳本識別受害者系統的 CPU 架構，確保惡意軟體的相容性；第二個腳本移除遭入侵系統上可能已經存在的任何其他競爭挖礦軟體。這種雙管齊下的策略可維持其常駐能力，並有效躲避偵測。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

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。

2025/01/20

駭客組織採用PNGPlug惡意程式載入器來發動ValleyRAT惡意程式散佈行動

據報導，在真實網路情境上有新的 ValleyRAT 惡意軟體散佈行動。在觀察到的攻擊鏈中，攻擊者利用一種新的多階段惡意程式載入器，稱為 PNGPlug。部署的 ValleyRAT 有效酬載具有執行部署的 shellcode、下載其他任意元件等功能。此攻擊行動已被歸因於名為：Silver Fox 的進階持續威脅 (APT) 駭客集團，並觀察到其目標針對多個中文地區的各種公司。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2025/01/20

AIRASHI--新出現的大型分散式阻斷服務(DDoS)殭屍網路

Airashi 是去年在真實網路情境上被發現到 Aisiru 殭屍網路的後繼變種。該殭屍網路已知會透過以揭露的漏洞以及利用不嚴謹的 Telnet 認證進行傳播。攻擊者可利用 Airashi 進行各式各樣的分散式阻斷服務 (DDoS) 攻擊。殭屍網路的幾個二進位檔也支援其他功能，例如：指令執行或代理服務。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2025/01/16

威脅份子一再使用合法的政府文件來傳送惡意軟體

一項鎖定中亞國家資料收集的惡意軟體攻擊行動與國家級駭客組織有關。這些攻擊利用合法的政府文件為誘餌來傳遞惡意軟體。一旦惡意的 Word 文件檔被開啟，它會請求接收者啟用並運行嵌入的惡意巨集，自此開啟感染鏈來進行後續進一步的感染計畫，以便建立持久性 (常駐) 並允許與 C&C 進行通訊。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan.Malscript
- Trojan.Mdropper
- WS.Malware.1
- WS.Malware.2

2024/05/01

DarkGate惡意程式載入器仍在大肆傳播

去年，DarkGate 惡意程式載入器的傳播非常氾濫。許多電子郵件攻擊行動利用各種攻擊鏈來傳播 DarkGate 有效酬載。據觀察，有的電子郵件包含直接下載連結，有的則可能使用附件 (PDF、ZIP 等) 來進行傳遞。

最近發現到一個攻擊行動初始階段是透過 XLSX 或 HTML 附件來傳遞 DarkGate。這兩種感染途徑都會透過 XLSX 中的巨集或 HTML 中的 Internet 捷徑檔下載下一階段的腳本。後續的腳本執行最終會衍生 DarkGate 惡意軟體有效酬載。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!g1

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
- ISB.Downloader!gen48
- ISB.Heuristic!gen107
- Phish.Html
- Scr.Malcode!gen136
- Trojan Horse
- Trojan.Darkgate

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。