保安資訊--本周(台灣時間2022/06/24)
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 100 萬個受保護端點上總共阻止了1.921億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/06/19)**

- 在**20萬8,600**台端點上，阻止了**9,350萬次**嘗試掃描**Web**服務器的漏洞。
- 在**41萬3,100**台端點上，阻止了**4,020萬次**嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬6,700**台**Windows**伺服主機上，阻止了**1,980萬次**攻擊。
- 在**14萬9,300**端點上，阻止了**860萬次**嘗試掃描伺服器漏洞。
- 在**7萬4,300**台端點上，阻止了**350萬次**嘗試掃描在**CMS**漏洞。
- 在**11萬500**台端點上，阻止了**330萬次**嘗試利用的應用程式漏洞。
- 在**30萬6,700**台端點上，阻止了**820萬次**試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,200**台端點上，阻止了**390萬次**加密貨幣挖礦攻擊。
- 在**10萬4,500**台端點上，阻止了**600萬次**向惡意軟體**C&C**連線的嘗試。
- 在**6,600**台端點上，阻止了**28萬1,300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。

2022/06/23

中國駭客組織 Tropic Trooper 利用全新的 Nimbda 載入程式來發動攻擊

由中國駭客組織 Tropic Trooper 所發起新的惡意攻擊行動，使用一個被稱為 Nimbda 的新型載入程式和來自 Yahoyah 木馬家族一個全新的惡意軟體。Nimbda 惡意軟體附帶一個 "SMS Bomber"，這是一個可對指定電話號碼發送大量文字訊息的阻斷服務攻擊 (DoS) 類型攻擊的工具。Yahoyah木馬是一個以前被 Tropic Trooperl 濫用的惡意軟體，而這個最新的變種被用來收集本地無線網路的資訊。透過使用圖像隱碼術 (Steganography)，Yahoyah 還植入稱為：TClient 後門是該攻擊行動最終有效籌載。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLoad!gen2

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

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。

2022/06/22

APT28 駭客組織對烏克蘭發動的最新攻擊行動中傳播 CredoMap 惡意軟體

APT28 駭客組織被觀察到在他們最新的行動中，向烏克蘭的目標散佈 CredoMap 惡意軟體。威脅者在攻擊中一直在利用惡意的 .rtf 檔案和濫用 MSDT CVE-2022-30190，也被稱為 Follina 的漏洞。CredoMap 惡意軟體能夠從各種網頁瀏覽器中竊取憑證和 cookie。該惡意軟體使用 IMAP 電子郵件協定進行資料竊取。

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
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

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: MSDT Remote Code Execution CVE-2022-30190
- Web Attack: Webpulse Bad Reputation Domain Request

基於安全強化政策(適用於使用DCS)：

DCS (Data Center Security) 預設的安全政策強化 MS Office 應用程式。DCS 防止 MS Office 應用程式啟動命令直譯器，包括 cmd.exe、powerhell.exe 和其他子程序。此外，對應這個安全漏洞，可以透過將 *\msdt.exe 新增到沙箱執行控制 "Microsoft Office不可執行的程式" 中，來防止遠端程式碼執行 (RCE) 漏洞。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。

2022/06/21

Search Marquis (*搜索侯爵) 仍然讓 MacOS 用戶不堪其擾

瀏覽器劫持是一種老掉牙的威脅伎倆，但賽門鐵克繼續觀察到一些惡意軟體和廣告軟體，它們未經允許就擅自修改用戶的瀏覽器設定，將他們重新轉向到非預期的網頁。Search Marquis (也被稱為Search Baron 和 OfferDeal) 就是其中之一，它已經存在幾年，並繼續針對 MacOS 用戶。

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.OfferDeal

2022/06/21

小心您的捷徑檔 (LNK) 檔案，最近惡意捷徑檔 (LNK) 有增多的趨勢

最近的資料顯示，使用微軟本地檔案捷徑的副檔名 (LNK) 檔案，透過電子郵件發送惡意軟體的情況越來越多。觀察到的惡意軟體家族包括 Qakbot (在早期 6 月防護公報中提到過)、Emotet、IcedID、BumbleBee Loader 和其他。這些威脅行動正在利用多種不同的機制，將有效籌載的交付和執行合併在一起。其中包括使用 ISO、zip 和 html 檔來傳遞 LNK 檔，而 LNK 檔又可以啟動 Powershell、CMD、curl 和 regsvr32 等應用程式來完成攻擊鏈。

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：

- CL.Downloader!gen111
- CL.Downloader!gen260
- CL.Downloader!gen261
- Downloader
- ISB.Downloader!gen347
- Trojan Horse

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。

2022/06/21

AvosLocker 勒索軟體在真實網路世界蠢蠢欲動

最近報導，AvosLocker 勒索軟體仍然在真實網路世界蠢蠢欲動。散佈這種勒索軟體的最新行動之一顯示，攻擊者正在積極利用各種不同的工具，包括：Mimikatz、Cobalt Strike 和 Sliver 工具。威脅者繼續利用 Log4Shell 漏洞來部署勒索軟體。在其他一些觀察到 AvosLocker 行動中，如最近在防護公報中所報告，勒索軟體也是透過利用 Atlassian Confluence 漏洞進行傳播。

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!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Mimikatz
- Ransom.AvosLocker
- Ransom.AvosLocker!gen2
- Trojan Horse
- Trojan.Vilers!gen1

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：

- Attack: Ransom.AvosLocker Activity 3
- Web Attack: Malicious Java Payload Upload 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。

2022/06/20

Blackguard 竊密程式視遊戲玩家為目標

Blackguard 是一個普通的竊密程式，被多個駭客組織和個體使用。在過去的幾個月裡，它主要是透過瀏覽網頁時的順道下載 (drive-by-download) 來針對消費者發動威脅。最近一個威脅者把目光投向遊戲玩家，他試圖透過把它偽裝成 CounterStrike 修補程式 (補丁) 來引誘他們安裝這款惡意軟體，該修補程式 (補丁) 已被張貼在遊戲論壇和 Discord 頻道。

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.Gen.MBT
- Trojan Horse

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/06/20

BRATA 行動惡意軟體具有新的資訊竊取能力

據報導，被稱為 BRATA 的行動惡意軟體的最新變種已經大大進化，其中包括一個全新的資訊竊取模組。在最近的威脅活動中，BRATA 主要針對的是金融機構，現在該惡意軟體假冒一個模仿目標銀行登錄頁面的網路釣魚頁面。這些變化顯示，BRATA 幕後的威脅者大大改變他們的攻擊方法，並開始從事更多類似進階持續威脅 (APT) 類型的行動。

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。

2022/06/20

利用猴痘病毒新聞，誘騙微軟憑證

網路犯罪分子傾向於利用世界新聞來助長他們的網路釣魚和惡意軟體威脅行動--特別是產生恐懼和好奇心的全世界事件，將永遠是一種強大的社交工程戰術。許多國家都出現猴痘病例，並在全球新聞中引起回響，也有報導稱攻擊者利用猴痘作為社交工程的誘餌，透過惡意郵件來釣取微軟的憑證。

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／IP位址已於第一時間收錄於不安全分類列表中。

2022/06/19

新版 CopperStealer 竊密程式在網路上出現

CopperStealer 是一個相對較新的竊密程式，今年初人們第一次在那些存放假的破解軟體的網站上看到它。這個普通的竊密程式幕後的作者持續優化它，新的版本已經在網路上被發現。在過去的幾週裡，其作案伎倆沒有改變，繼續將消費者作為主要目標。

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.Gen.MBT
- Trojan Horse

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 564
- System Infected: Trojan.Backdoor Activity 634

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/06/19

最近的 Matanbuchus 行動植入 Cobalt Strike 有效載荷

一份有關新的 Matanbuchus 惡意軟體即服務 (MaaS) 專案的報告在 2021 年的最初幾個月首次曝光。幾天前一個全新的網路釣魚行動被發現利用同樣的 MaaS，最終植入一個 Cobalt Strike 信標，用來增加後續的潛在利用價值。

之前關於 Matanbuchus 的保護公告在這裡看到：惡意垃圾郵件行動，趁機植入 Matanbuchus 和 Qbot 惡意軟體。

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：

- ISB.Downloader!gen520
- Trojan Horse
- Trojan.Malscript
- Trojan.Gen.NPE
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.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。

2022/06/19

赫米特 (Hermit) 間諜軟體

Hermit 是一個複雜的手機間諜軟體，已經存在好幾年。據了解它是由 RCS 實驗室和 Tykelab Srl 所建立，並被出售給民族國家和執法部門，以幫助打擊犯罪和恐怖主義並維護公共安全。儘管如此，多年來該軟體的潛在濫用已經被議論紛紛，賽門鐵克對其進行長期的檢測。最近在哈薩克觀察到這種威脅可能是透過簡訊傳播。它經常被視為偽裝成與電信和智慧型手機行業有關的應用程式 APP。

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

Symantec Endpoint Protection Mobile 還能够分析簡訊中包含的連結。它透過對照賽門鐵克全球情報網（GIN）旗下的賽門鐵克 WebPulse 中的威脅情報檢查簡訊中的 URL，並在連結可疑時提醒用戶，進而保護用戶免受簡訊釣魚攻擊。

SEP Mobile 針對網路內容威脅提供保護，過濾和封鎖與 Hermit 行動中使用的已知 C&C 伺服器的通訊。它還可以識別和保護易受攻擊的 iOS 和 Android 設備。

2022/06/17

浣熊竊密程式 (Raccoon Stealer) 以最新的變種強勢回歸

在網路上發現一個惡明昭章的浣熊竊密程式 (Raccoon Stealer) 的最新版本。正如地下論壇上所宣傳的那樣，浣熊竊密程式 2.0 是用 C++ 撰寫，並聲稱比早期版本在性能和規避檢測方面有一些改進。據報導，最新的惡意軟體已經透過破解的套裝軟體散佈。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.AM.E!g37
- SONAR.ProcHijack!g21
- SONAR.SuspLaunch!g12
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- Packed.Generic.525
- Packed.Generic.620
- Scr.Malcode!gdn30
- Scr.Malcode!gdn33
- Scr.Mallnk!gen1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

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：

- System Infected: Trojan.Backdoor Activity 632
- System Infected: Trojan.Backdoor Activity 634

2022/06/17

Panchan 殭屍網路以 Linux 執行個體進行加密貨幣開採 (挖礦)

最近發現一個全新的點對點僵屍網路，稱為 Panchan。Panchan 是用 Golang 撰寫，針對 Linux 伺服器進行加密挖礦。該殭屍網路繼承 SSH 蠕蟲的典型功能，例如：進行字典攻擊或收集用於橫向移動 SSH 金鑰的能力。該惡意軟體部署兩個不同的加密貨幣礦工--xmrig 和 nbhash，可以直接在記憶體中執行。據報導，最近的 Panchan 傳播活動主要針對教育部門。

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.Gen.NPE
- WS.Malware.1

2022/06/17

Leafperforator (又名Sidewinder) 在南亞和東亞發動的 Android 平台威脅行動

被稱為 LeaftPerforator (又名Sidewinder 與 Rattlesnake) 的進階持續威脅 (APT) 組織至少自 2012 年以來一直活躍，並持續在南亞和東亞展開威脅行動。已知他們使用帶有惡意檔案／連結的電子郵件來對感興趣的目標發動攻擊或釣魚行為。所使用的誘餌是包含可能與目標相關的內容所特定制的。最近，他們針對巴基斯坦的一次行動被揭露。攻擊者偽裝成 VPN、宗教和手機清理等相關應用 APP，在 Google Play 上植入 Android 惡意軟體。

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。

- AdLibrary:Generisk
- AppRisk:Generisk

2021/12/07

惡意垃圾郵件行動，趁機植入Matanbuchus 和 Qbot 惡意軟體

今年稍早，研究人員報告名為「Matanbuchus」的惡意軟體即服務領域，新的下載器，在該惡意軟體開發者「BelialDemon」所屬的地下論壇上做廣告。

最近，有人觀察到有惡意垃圾郵件活動利用「Matanbuchus」傳送內含巨集物件的 XLSB 文件，作為隨後呼叫其他 Qakbot (Qbot) 惡意軟體的一種媒介。此活動隨後將導致垃圾郵件殭屍 (機器人) 和 Cobalt Strike 滲透測試工具攻擊。

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：

- Downloader.Trojan
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- W97M.Downloader

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。