保安資訊--本周(台灣時間2022/04/15)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 2.074 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/04/11)**

- 在**22萬3,100**台端點上，阻止了**1.079億**次嘗試掃描**Web**服務器的漏洞。
- 在**48萬4,100**台端點上，阻止了**4,070萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬7,100**台**Windows**伺服主機上，阻止了**2,550萬**次攻擊。
- 在**16萬7,700**端點上，阻止了**1,030萬**次嘗試掃描伺服器漏洞。
- 在**9萬300**台端點上，阻止了**460萬**次嘗試掃描在**CMS**漏洞。
- 在**12萬8,400**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**41萬4,300**台端點上，阻止了**1,120萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,800**台端點上，阻止了**380萬**次加密貨幣挖礦攻擊。
- 在**12萬100**台端點上，阻止了**610萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,800**台端點上，阻止了**29萬600**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。

2022/04/14

CryptoClip 劫持 Discord 使用者的加密錢包

挖礦同好經常聚集在熱門的網路即時通話平臺上，如：Discord，網路犯罪分子非常清楚這一點。根據最近報導，一名參與者濫用該平臺來發動偷渡式下載攻擊行動，誘使受害者下載並安裝偽裝成 CryptoClipWatcher（一種監控這些威脅的舊工具）的 CryptoClip 惡意軟體。劫持加密錢包的惡意軟體可能會嚴重影響到受害者，雖然這些惡意軟體主要針對消費者，但它們在企業環境中也被觀察到。

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.SuspBeh!gen66

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

2022/04/14

CVE-2022-26809，遠端程序呼叫 (Remote Procedure Call，RPC) 漏洞

作為例行性四月份週二修補的一部分，微軟修補一個關鍵的 Windows RPC 漏洞 (CVE-2022-26809)，該漏洞允許透過 Microsoft 遠端程序呼叫 (RPC) 通信協定中的漏洞進行未經授權的遠端程式碼執行。微軟建議企業可關閉邊界防火牆 TCP 445 埠來緩解該漏洞。

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：

- Attack: Fake SMB Server Response
- Audit: EFSRPC Bind Attempt
- Audit: Suspicious SMB Client Request 2

2022/04/14

Adload 惡意廣告軟體，仍在世界各地興風作浪

惡名昭彰且老練的廣告軟體：Adload 以及其他熱門，如：Bundlore 廣告軟體，仍然繼續主導整個 MacOS 領域。世界各地的消費者和企業用戶每天都受到 Adload 的威脅攻擊。初始攻擊媒介很少改變，主要透過假冒軟體更新偷渡式下載，因為它仍然是一種相當有效的社交工程手法。

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.Adload*

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Adload*

2022/04/14

近期聲名大噪的 Parrot 惡意流量導向系統 (TDS)

流量導向系統在威脅領域並不是什麼新鮮事，多年來它們已被許多參與者用作發動惡意攻擊行動的媒介，並且最近幾天，另一個名為 Parrot 惡意流量導向系統，因成功利用惡意 Javascript 來入侵數千個網站而聲名大噪，如此大量的網站提供參與者長驅直入的機會，並且能夠將額外有效籌載植入到許多用戶的電腦上。

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：

- Malicious Site: Malicious IP Address Request
- Malicious Site: Malicious Domain Request 22
- Malicious Site: Malicious Domain Request 21
- System Infected: Trojan.Backdoor Activity 669
- Web Attack: Mass Injection Website 90

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。

2022/04/14

全新的竊密惡意軟體：“ZingoStealer”

一個名為 ZingoStealer 全新的竊密惡意軟體，最近被作為犯罪軟體相關威脅參與組織 Haskers Gang 成員的免費產品而嶄露頭角。這種全新的惡意軟體具有從受害者那裡竊取敏感資訊的能力，例如：環境和系統資訊、使用中的網頁瀏覽器儲存的資訊、協作軟體的登入帳密以及與加密貨幣錢包等相關的資訊。它還能夠下載其他惡意軟體來感染系統。

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：

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

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
- System Infected: Redline Stealer Activity 2
- Web Attack: Webpulse Bad Reputation Domain Request

2022/04/14

“TellYouThePass”勒索軟體仍對企業虎視眈眈

據報導，“TellYouThePass”勒索軟體仍在針對企業的積極惡意活動中被散布。該惡意軟體自 2019 年左右以來就已為人所知，並且具有 Windows 和 Linux 加密器版本。眾所周知，早先的 TellYouThePass 散布行動是透過濫用 Log4j 相關的漏洞來發動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Tellyouthepass
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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。

2022/04/14

由 Lazarus (*拉撒路) 進階持續威脅集團發動：Pompilus 間諜行動

據觀察，與北韓有關聯的進階持續威脅組織 (APT)：Lazarus，正在針對化工行業展開間諜行動。該行動似乎是由 Lazarus 發起，被稱為「夢想工作行動」間諜行動的延續，該活動於 2020 年 8 月首次被觀察到。賽門鐵克成立 Pompilus 計畫來追蹤 Lazarus 的子活動。“夢想工作行動”涉及 Lazarus 使用虛假的工作機會，誘使受害者點擊惡意鏈接或打開惡意附件的手段，最終導致安裝用於間諜活動的惡意軟體。

在我們的部落格文章中有更詳細的資訊：Lazarus針對化工行業

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.2
- Trojan.Lazarus!g1

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3

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。

2022/04/13

SpyNote (*間諜筆記)：在義大利橫行的 Android 平台遠端存取木馬 (RAT)

有報導稱，正在肆虐義大利一項網路攻擊行動，其參與者一直試圖用一種名為 SpyNote 的遠端存取木馬（RAT）感染 Android 使用者。該惡意軟體成功偽裝成義大利郵政服務商：Poste Italiane S.p.A的Android 安全應用程式 (APP)，該公司還提供其他服務，如：通信整合、物流、金融和保險。該 RAT 已經存好幾年，具有以下常見的功能：

- 存取檔案、簡訊、電話、聯絡人、位置、帳戶和相機
- 下載並安裝其他 apk
- 鍵盤側錄
- 錄音及錄影

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。

- Trojan.Spymax

2022/04/13

“技術支援詐騙”仍然是一大威脅

大多數人都知道什麼是技術支援詐騙--這些手法已經存在很多年，截至今天，仍然經常用於快速獲得經濟收益。賽門鐵克繼續觀察世界各地的日常詐騙，這些騙局主要針對消費者，但在某些情況下，企業使用者也會遭潑及。雖然經濟利益是主要目標，但如果這些參與者能夠吸引企業用戶並獲得對其電腦的遠端存取權限，他們可能就能夠收集敏感資料，例如：聯絡人、應用程式和文件內容的螢幕截圖，以及記錄在沒有保護措施檔案內的密碼 (是的，還是有不少人仍然這樣做) 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：

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: Fake Tech Support Domains *
- Web Attack: Fake Tech Support Website *
- Web Attack: Fake Scan Webpage *

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。

2022/04/13

在日本層出不窮的假冒“樂天”的網路釣魚行動

在網路釣魚領域，有一些非常受歡迎的服務，在很長一段時間內一直被參與者作為目標。在日本，樂天就是這些服務之一。該公司主要被稱為線上網路電商平台，還提供金融服務等。賽門鐵克每天都會持續觀察針對日本消費者和企業的多個樂天網路釣魚行動，試圖竊取憑證。建立包羅萬象、各種風格，從高品質，幾乎相同的網站到那些充斥著拼寫錯誤和過時範本的網站。

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 Site: Malicious 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。

2022/04/13

鎖定物聯網：Fodcha 殭屍網路活動

據報導，被稱為 Fodcha 的新 DDoS 殭屍網路在網際網路上傳播，主要鎖定易受攻擊的物聯網設備。惡意軟體透過已揭露的漏洞發動攻擊以及暴力破解弱密碼或沒有變更過出廠預設密碼的裝置。Fodcha 鎖定不同的 CPU 架構，包括 mips、mpsl、arm 和 x86。

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
- 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。

2022/04/12

一種名為「Fakecalls*假來電」的銀行木馬

偽裝成韓國銀行應用程式 (APP)，除了平常的間諜軟體的功能外，此 Fakecalls 銀行木馬的一個明顯特徵是它能夠啟動模仿標準銀行問候對話的虛假來電，以便在將來電直接傳遞給攻擊者之前獲得受害者的信任。

除了虛假來電功能外，安裝後會被授予許可權的特洛伊木馬程式將授權攻擊者控制受害者的電話，並且還將授予對聯絡人、麥克風、相機、地理位置和來電處理的存取權限。

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.2
- WS.Malware.2

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

2022/04/12

不分晴天、雨天，幾乎每天都會有新的勒索軟體出現：新勒索軟體 SunnyDay

在真實環境觀察一種名為 SunnyDay (*晴天)的新勒索軟體。該惡意軟體與被稱為 MedusaLocker 或 Keversen 的勒索軟體變種具有幾個共同特徵。SunnyDay 能夠刪除磁碟陰影複製以及停用各種系統服務和程序。該惡意軟體會加密使用者的檔案並將 .sunnyday 副檔名新增至被加密過的檔案。

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：

- Ransom.Gen
- Trojan Horse

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!gen4

2022/04/12

MoqHao 惡意軟體繼續針對歐洲的行動裝置用戶

據報導，MoqHao 惡意軟體（也稱為 Wroba）持續以全球行動裝置用戶為攻擊目標。該惡意軟體與 Roaming Mantis 威脅組織有所關聯。雖然較早散布這種惡意軟體的行動主要針對日本、台灣和美國的受害者，但最近針對歐洲國家的行動日益增多。MoqHao 主要透過簡訊網路釣魚 (smishing) 進行傳播，它同時具有間諜軟體和銀行惡意軟體的多重功能。

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

2022/04/11

SolarMarker 後門程式發動新攻擊行動，強勢回歸

SolarMarker 惡意軟體的新變種已在真實環境被發現。SolarMarker 是一個廣為人知的後門，它透過利用搜尋引擎最佳化中毒（SEO-Poisoning）的攻擊散布。該惡意軟體針對存放於瀏覽器中的使用者資訊，例如：cookie、自動填入欄位的詳細資訊或登錄憑證。這個最新惡意軟體變種的多種變化中，提升規避安全軟體檢測的能力是最明顯。

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。

2022/04/11

EvilNominatus 勒索軟體

據報導，EvilNominatus 勒索軟體在行動中大量散布惡意 .BAT 批次檔。EvilNominatus 勒索軟體變種是在去年首次被發現。它具有刪除磁碟陰影複製和停用受感染主機上防火牆的功能。該惡意軟體會加密用戶的檔案並將 .ink-locked 的副檔名新增至被加密過的檔案。

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.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!g18

基於機器學習的防禦技術：

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

2022/04/11

Casbaneiro 銀行木馬積極針對拉丁美洲

Casbaneiro 銀行木馬也被稱為 Metamorfo，在針對拉丁美洲用戶的惡意垃圾郵件行動中一再出現。該惡意攻擊利用帶有包含 URL 鏈接的 .pdf 附件之網路釣魚電子郵件。如果點擊這些惡意鏈接，則會導致啟動多階段感染過程的惡意 .cmd 腳本。Casbaneiro 木馬攻擊行動目的在覬覦與金融網站相關的用戶資訊和憑證。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

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)。

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2022/04/11

NB65 駭客集團攻擊俄羅斯組織

NB65 駭客集團針對俄羅斯組織使用從洩露 Conti 勒索軟體原始碼衍生的勒索軟體變種。該勒索軟體的感染例程包括更改檔案名稱、被加密過的檔案會新增 .NB65 副檔名，並且還會建立一個名為“R3ADM3.txt”的勒索信或說明。

這是與烏克蘭--俄羅斯衝突有關的網路攻擊，因為勒索信特別提到俄羅斯總統普丁(Vladimir Putin)。

“我們正在密切關注。你的總統不應該犯下戰爭罪。如果你正在尋找對你目前的情況負責的人，看看普丁 (Vladimir Putin) 就知道了”NB65 勒索軟體說明中寫道。

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：

- Downloader
- Ransom.Conti!gen12
- Ransom.Generic.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/10

AveMaria 垃圾郵件行動，攻擊全球各地的組織

在過去的幾個星期，賽門鐵克觀察到一起大型垃圾郵件攻擊行動，攻擊者一直針對世界各地的各種組織，企圖採用一種稱為 AveMaria 的遠端存取木馬 (RAT) 感染它們。這些電子郵件採用社交工程常見的惡意垃圾信件，談不上獨特或巧妙，而是使用一個單詞的電子郵件主旨：“Inquiry* 查詢”。

AveMaria 的攻擊行動屢見不鮮，但自從幾年前首次出現以來，它們的氾濫程度肯定有所下降。該惡意軟體的功能很普通，並不具有使其在駭客圈有鶴立雞群的特殊功能。由於多年來，攻擊者還是利用惡意電子郵件，當成主要的感染媒介一直保持不變。

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：

- Backdoor.Avecma

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：

- Scr.Malcode!gdn30

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/10

Mercurial 爬蟲程式，搜捕 Discord 權杖

雖然主要針對消費者，但企業用戶也會是竊取 Discord 權杖竊密程式的受害者。Discord 權杖是用戶登錄 Discord（一種流行的網路即時通話軟體與數位發行平台）時，建立一系列獨特的數字和字母。Mercurial 爬蟲程式是過去幾個月熱門的竊密程式之一，原因之一是它是一家軟體開發和版本控制（公眾可存取）的熱門網際網路託管商。除了能夠獲取 Discord 權杖之外，它還可以竊取 Roblox cookie 和 Minecraft 的工作階段。除此之外，它還具有其他常見的竊密功能。

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(Snoar)的防護：

- SONAR.SuspTempRun
- SONAR.SuspTempRun2
- SONAR.SuspBeh!gen616

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer

基於機器學習的防禦技術：

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

2022/04/10

另一值得關注的殭屍網路：EnemyBot

Linux 威脅環境中不乏殭屍網路，雖然 Mirai 和其變種是最流行的，但其他具有類似功能的殭屍網路也屢見不鮮。EnemyBot 也算是檯面上的要角，它針對一系列基於 Linux 的系統，例如：工作站、伺服器和物聯網。傳播殭屍網路依賴於與大多數其他網路相同的戰術，掃描環境並尋找易受遠端程式碼有機可趁的脆弱系統。

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：

- Linux.Lightaidra
- WS.Malware.1

2022/04/08

SystemBC (也稱為Coroxy) 代理機器人，仍然在最新的攻擊行動中被濫用

SystemBC（也稱為 Coroxy）是一個眾所周知的代理機器人，多年來一直用於下載和執行惡意籌載。根據最新報導，SystemBC 最近透過 SmokeLoader 和 Emotet 惡意軟體散布。SystemBC 允許攻擊者從受感染的機器上獲取一些基本的系統資訊，下載額外的有效籌載或只是利用機器人作為代理路徑進行持續性攻擊。

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：

- Backdoor.SystemBC
- Packed.Generic.620
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2022/04/08

用於傳遞勒索軟體有效酬載的 Blister 和 SocGholish 載入器

根據最近的一份報告，Blister 和 SocGholish 載入器已經一起被用於提供勒索軟體有效籌載的惡意行動。兩種載入器都以其規避特性而聞名，並且經常被利用以規避有效籌載傳遞期間的任何安全檢測。那些最近報導的活動也一直在使用 Cobalt Strike stagers 並將 Lockbit 作為最終有效籌載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Dropper
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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。

2022/04/08

在美國稅務相關的垃圾郵件中觀察到 Sorillus 遠端存取木馬 (RAT)

最近，Sorillus 遠端存取木馬 (RAT) 在威脅領域的活動有所增加，據報導觀察到在與美國稅務相關的惡意電子郵件中散布。攻擊者試圖誘使受害者從雲端硬碟和檔案託管服務商：Mega，下載偽裝成 PDF 檔案的惡意可執行檔。

這種威脅是一種普通的跨平台遠端存取工具（用 Java 編寫），售價 19.99 美元（終身使用）。據作者介紹，他們正在努力改進，例如：Android 用戶端。駭客論壇上一直在討論這種 RAT，有人呼籲破解它。

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
- Trojan Horse

2022/04/08

Snake(*蛇) 鍵盤側錄程式，在威脅領域還佔有一定的份量

Snake 鍵盤側錄程式在威脅環境中繼續被觀察到，但由於有越來越多更精密竊密程式的競爭讓 Snake 開始走下坡，自 2021 年中以來，其氾濫程度已大不如前。這種普通的竊密程式被各種偏愛惡意電子郵件和網頁順道下載戰術的團體和個人所採用 ，以作為初始感染的媒介。當涉及到惡意垃圾郵件行動時，大多時候都會採用通用的社交工程戰術。以下是我們最近幾天觀察到的電子郵件主旨範例：

- NEW ORDER ENQUIRY_ETS60
- Order list (BERN220819)
- Acknowledge PO
- INVOICE CORRECTION
- PO S1070069415
- PAYMENT ADVICE

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：

- Scr.Malcode!gdn30

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/07

Venom (*毒液) 勒索軟體

最近幾天，一種名為 Venom 勒索軟體的活動有所增加。成功感染後，它將加密檔案並為其新增 .venom[ID] 作為副檔名。根據他們的勒索信，這些參與者還採用可怕的雙重勒索戰術，威脅受害者如果不付款，他們將在黑市上出售他們的遭竊資料。

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：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/07

SharkBot 及其植入程式(droppers)

在行動威脅領域中繼續觀察到相對較新的 Android 惡意軟體：SharkBot，這些惡意軟體由潛入 Google Play 的植入程式（偽裝成假防毒軟體）啟用。正如研究人員所指出，這些植入程式並沒有針對位於中國、印度、羅馬尼亞、俄羅斯、烏克蘭或白俄羅斯的用戶。

雖然這種銀行惡意軟體利用典型的覆蓋技術和使用輔助功能服務 (Accessibility Service) 的「自動轉帳系統（Automatic Transfer System，ATS）」攻擊，但它在使用 DGA（動態網域產生演算法）方面，確實從其他銀行惡意軟體中脫穎而出--攻擊者使用這種技術來產生惡意軟體的命令和控制 (C&C) 伺服器所使用的新網域名稱和 IP 位址。

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