保安資訊--本周(台灣時間2022/11/04)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 95 萬 700 台受保護端點上總共阻止了 1.333億次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2022/10/31)**

- 在**18萬3,800**台端點上，阻止了**6,260**萬次嘗試掃描**Web**服務器的漏洞。
- 在**32萬2,800**台端點上，阻止了**2,430**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬7,900**台**Windows**伺服主機上，阻止了**2,040**萬次攻擊。
- 在**12萬6,400**端點上，阻止了**470**萬次嘗試掃描伺服器漏洞。
- 在**3萬8,800**台端點上，阻止了**200**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬600**台端點上，阻止了**270**萬次嘗試利用的應用程式漏洞。
- 在**32萬7,900**台端點上，阻止了**800**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬9,500**台端點上，阻止了**480**萬次加密貨幣挖礦攻擊。
- 在**5萬4,300**台端點上，阻止了**570**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,400**台端點上，阻止了**19萬1,500**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。

2022/11/03

沒說要贖金，但還是被加密了～LoveRansomware(*愛的勒索軟體)

另一個被稱為 "LoveRansomware" 的勒索軟體已被發現在真實網路環境四處亂竄。有趣的是，在被加密的電腦上留下的勒索贖金說明中並沒有明載勒索金額。威脅者要求受害者透過電子郵件或 Telegram 與他們聯繫。這是一個簡單又普通的勒索軟體，並沒有特別突出的功能，讓它在威脅領域中脫穎而出。檔案被加密後會被附加 .Love 的副檔名。

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.Ransomnemty!g2
- SONAR.Ransomnokibi!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1

2022/11/03

江山代有才人出，各領風騷數百年～全新Medusa $tealer竊密程式，傷害力不容小覷

竊密程式是網路攻擊鏈的常用工具，後起之秀絡繹不絕。最近有一支全新的 Medusa $tealer 竊密程式，具有資訊竊取、分散式阻斷服務攻擊 (DDoS) 和加密貨幣挖礦劫持的多重破壞力。該威脅幕後的威脅者最近在 Discord、TikTok 和T elegram 上大舉宣傳。截至目前，在真實網路環境並無太多威脅事件回報，但我們評估在不久的將來，隨著駭客組織和個人駭客對它的青睞，會觀察到透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/03

網路攻擊也講究分工～Lockbit Black勒索軟體透過Amadey殭屍電腦來散播

據報導，在最近一些攻擊行動中，AmadeyAmadey 殭屍電腦(機器人)被利用來散播 Lockbit Black 勒索軟體。攻擊鏈中常有惡意的 word 檔案或偽裝成 word 檔案的可執行二進位檔案被發現。Amadey 殭屍電腦是一個能夠進行系統偵察、資訊竊取和載入任意有效籌載的惡意軟體變種。在過去 Amadey 已經被用來傳播各種勒索軟體的有效籌載，其中包括 GandCrab。

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.UACBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Amadey!g1
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1
- WS.SecurityRisk.4

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：

- 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。

2022/11/03

兩情相悅，正在上演中～Vultur和Brunhilda共譜惡意攻擊的愛情故事

Vultur 繼續在手機行動威脅領域被觀察到，並仍然透過惡名昭彰的植入惡意程式即服務 (Dropper-as-a-Service) 的 Brunhilda 惡意軟體服務商來負責。這種安卓手機行動銀行惡意軟體利用惡名昭彰的覆蓋技術--顯示假冒的全螢幕視窗，意圖誘使使用者輸入他們的銀行憑證。它的目標鎖定 190 多家銀行和加密貨幣交換平臺。

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。

- AppRisk:Generisk

2022/11/02

樹大招風～FFDroider竊密程式利用偽造的谷歌瀏覽覽器(Chrome)和Facebook安裝程式

今年年初，一個主要針對社交媒體憑證的竊密程式 (FFDroider) 被揭露。在過去的幾週裡，賽門鐵克發現到與這種威脅有關的全新命令和控制伺服器 (C&C)。這種新活動幕後的威脅者一直在透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播假冒的 Google Chrome 和 Facebook 安裝程式引誘受害者。

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(Snoar)的防護：

- SONAR.WMIC!gen16

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/02

Emotet 捲土重來強勢回歸

在長達數月的沉寂之後，我們觀察到新的攻擊行動透過垃圾郵件傳遞 Emotet 惡意軟體。這些電子郵件包含一個 Excel 附件，負責下載 Emotet。該 Excel 檔案利用社交工程，要求使用者輸入以成功執行惡意內容。

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.MSExcel!g4

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen128
- Scr.Malcode!gen
- Scr.MalMacro!gen1
- XLM.Downloader!gen1
- XLM.Downloader!gen2
- XLM.Downloader!gen4

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: Malicious Payload Download 26
- Web Attack: W97M.Downloader Payload Download

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已於第一時間收錄於不安全分類列表中。

2022/11/02

可以判定正確國家位置的的全新的Sharkbot銀行惡意軟體攻擊行動

在真實網路環境發現一個傳播 Sharkbot 手機銀行惡意軟體 2.29-2.32 版本的新活動。該惡意軟體已透過 Google Play 商店的惡意應用程式 APP 傳播，目標是義大利、英國、德國、西班牙和波蘭等國的網路銀行用戶。Sharkbot 前期誘餌程式一直偽裝成名為 "Codice Fiscale" 的報稅計算應用程式 APP 或一個檔案管理員應用程式 APP。所植入的套裝程式包含檢查SIM卡國家位置的功能，並與指定的目標國家清單進行比對。如果不符合比對條件，該惡意軟體將退出而不執行任何惡意行為。

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.Malapp
- Android.Reputation.2
- AppRisk:Generisk

2022/11/02

鍾愛法語～法語系國家出現Cryptonite勒索軟體

最近在加拿大等法語系國家發現 Cryptonite 勒索軟體。最近這系列活動背後的威脅者，似乎並沒有在遭入侵的環境中進行橫向移動，他們要求 0.51 比特幣來換取解密密鑰。他們更威脅在不付贖金前，會每 24 小時刪除 2 個檔案，直到付款為止，如果 7 天後仍未付贖金，將會提高價格，而不是使用經典的雙重勒索戰術，現在更多惡名昭彰的勒索軟體集團似乎更喜歡這樣做。

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!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/01

故意拼錯嗎？～Pyschedelic(*迷幻)勒索軟體

又一個被稱為 Pyschedelic 的普通勒索軟體已經在真實網路環境有多起威脅事件被揭露。雖然這個惡意軟體的名字似乎拼錯，但威脅者在贖金說明中提供這個名字。該勒索軟體對受害者電腦上的檔案進行加密，並要求受害者透過電子郵件與攻擊者聯繫。Pyschedelic 勒索軟體利用 Windows 內建用來計算雜湊值的工具 "certutil -encode" 指令對檔案進行編碼。

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：

- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/01

情有獨"日"～LODEINFO惡意軟體繼續針對日本的組織進行攻擊

LODEINFO 是一個最初在 2019 年發現的惡意軟體家族，歸屬於 APT10 威脅集團。多年來，該惡意軟體一直以日本的政府和公共部門的組織為目標。根據一份最新報告，該惡意軟體在 2022 年的攻擊行動中仍然活躍，並繼續針對日本的實體。自最初發現以來，LODEINFO 的開發團隊一直在不斷地更新和改進。據報導，最新的變種已經可以支援 64 位元架構，也對 C&C 通信中的功能進行優化與增強。

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!gen411
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W97M.Downloader
- WS.Malware.1

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。

2022/11/01

惡意程式更會與時俱進～Drinik被發現具有全新功能

被稱為 Drinik 的安卓手機行動平台惡意軟體再次被觀察到，透過與報稅有關的社交工程針對印度使用者--這次偽裝成由等同印度國稅局部門所提供的一個應用程式APP。據報導，在這次攻擊行動中，該惡意軟體配備全新的功能，例如：惡名昭彰的覆蓋技術--顯示假冒的全螢幕視窗，誘騙使用者輸入他們的機敏憑證。現在還能透過 CallScreeningService 來阻止來電，並透過 FirebaseCloudMessaging 接收命令。

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。

- AppRisk:Generisk

2022/11/01

加密掛載磁碟和共用的網路分享～請對Surtr勒索軟體，提高警覺

Surtr 是一種勒索軟體服務 (Ransomware-as-a-Service) 至少從2021年底就開始出現，最近在韓國的報告中觀察到。在成功感染後，就像許多勒索軟體一樣，它將試圖刪除陰影複製 (shadow copies) 並加密檔案 (加密後新增.surtr副檔名)。它還能夠加密已掛載的磁碟和共用的網路分享。這種威脅幕後的威脅者採用可怕的雙重勒索戰術，也就是先竊取機敏資料，勒索不成會公開機敏資料作為威脅。

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：

- Ransom.Surtr
- Trojan.Gen.MBT

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 46

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/31

永遠無解！Azov(*阿佐夫)--沒有解密金鑰的勒索軟體

新的勒索軟體名稱 "Azov" 因其為該被加密檔案重新加入該副檔名而命名，其命名又與烏克蘭的 Azov 團體似乎有些關聯。它是透過夾帶在盜版軟體、金鑰或序號產生器軟體和廣告軟體來散佈。根據勒索說明文件所示，它號稱是由已知的安全研究人員所建立，並提供他們的聯繫資訊，但這種說法是錯誤。由於這個勒索說明文件提供虛假的聯繫資訊，並沒有對應的解密金鑰，所以與其說是勒索軟體，不如說是一個破壞性的檔案刪除程式，因為根本無法解密。

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.Ransomware!g7
- SONAR.Ransomware!g20
- SONAR.Ransomware!g3
- SONAR.TCP!gen1
- SONAR.ProcHijack!g45

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- 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

2022/10/30

惡意的MSI檔案，進一步引爆BatLoader的災情

在過去的兩年裡，BatLoader 攻擊行動一直都有，並且時大時小，到今天為止，它仍然在威脅領域中榜上有名。這種威脅在過去的攻擊行動中載入各種竊密程式和遠端存取木馬。賽門鐵克最近觀察到新的命令和控制伺服器 (C&C)，這些伺服器可以提供並散佈多個惡意的 Windows Installer 檔案(*.msi)，如果成功執行，就會部署這種載入程式。最近這一系列攻擊行動背後的威脅者將這些MSI安裝程式偽裝成知名的熱門軟體，例如：Tor、MsOffice、Malwarebyte、Adblock、WinRar、Luminar 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：

- Trojan.Gen.MBT
- Scr.Malscript!gen1
- Ws.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/10/30

貍貓換太子！Laplas剪貼簿竊密器(Clipper)

隨著賽門鐵克繼續觀察到越來越多具有這種破壞力的威脅，竊取加密貨幣錢包是一個日益增長的趨勢，而 Laplas 是另一該典型的威脅代表，目前正在俄語系的地下論壇上做廣告，並有多起在真實網路環境被發現。這種剪貼簿竊密器將把受害者的加密貨幣錢包位址與惡意軟體威脅者擁有的位址進行對調與交換。

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.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/10/28

Cranefly 威脅者在隱秘的攻擊行動中使用前所未見的技術和工具

賽門鐵克發現一個以前沒有記錄的植入程式 (dropper)，它被用來安裝一個新的後門和其他工具，使用的新技術是從看似無害的網際網路資訊服務 (IIS) 日誌中讀取命令。賽門鐵克稱之為 Cranefly (又名UNC3524) 的威脅者正在使用該植入程式 (Trojan.Geppei) 安裝另一個迄今未記錄的惡意軟體 (Trojan.Danfuan) 和其他工具。從 IIS 日誌中讀取命令的技術是賽門鐵克研究人員迄今為止在現實世界的攻擊中沒有看到過的東西。

在我們的部落格文章中有更多資訊可供參考：Cranefly：威脅者在隱秘的活動中使用前所未見的技術和工具

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
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Regeorg
- Trojan.Danfuan
- Trojan.Geppei
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A