保安資訊--本周(台灣時間2022/03/25)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 120 萬個受保護端點上總共阻止了 2.065 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/03/21)**

- 在**23萬600**台端點上，阻止了**1.039億**次嘗試掃描**Web**服務器的漏洞。
- 在**50萬2,100**台端點上，阻止了**4,410萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬5,300**台**Windows**伺服主機上，阻止了**2,660萬**次攻擊。
- 在**17萬2,300**端點上，阻止了**970萬**次嘗試掃描伺服器漏洞。
- 在**9萬4,500**台端點上，阻止了**470萬**次嘗試掃描在**CMS**漏洞。
- 在**13萬9,900**台端點上，阻止了**390萬**次嘗試利用的應用程式漏洞。
- 在**42萬3,200**台端點上，阻止了**1,210萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,300**台端點上，阻止了**410萬**次加密貨幣挖礦攻擊。
- 在**12萬5,200**台端點上，阻止了**620萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,200**台端點上，阻止了**24萬2,800**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。

2022/03/24

Scarab (*聖甲蟲) 在烏克蘭的活動已被揭露

根據最近報導，一個被稱為 Scarab (又名 UAC-0026) 進階持續威脅 (APT) 駭客組織，被觀察到透過魚叉式網路釣魚郵件針對烏克蘭的活動。這些惡意郵件包含一個附件檔案 (翻譯檔案名：關於保存俄羅斯聯邦軍隊犯罪行為的紀錄影片 錄影.rar)。如果受害者被成功引誘，該檔案內的可執行檔，將建立一個引誘檔案並植入被稱為 HeaderTip 的 Scarab 惡意軟體。

這些參與者至少從 2012 年開始就在發動情報收集行動。據瞭解，他們使用客製化的惡意軟體 (如 Scieron) 和魚叉式網路釣魚作為感染的主要媒介。多年來，他們已經在全球各地的許多國家被發現。

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.SuspBeh!gen650

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse

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。

2022/03/24

GodFather (*教父) 惡意軟體針對 Android 銀行用戶

據報導，GodFather (*教父) 行動裝置銀行惡意軟體在歐洲各地的攻擊中以安卓使用者為目標。該惡意軟體顯示出與 Cerberus 和 Medusa 銀行木馬的顯著相似性。GodFather 的功能包括：獲取被攻擊設備的資訊、存取和發送簡訊、轉接電話以及在 VNC 的協作下接管設備螢幕。

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

2022/03/24

Arid Gopher (*旱地地鼠) -- 源於進階持續威脅 (APT) 駭客組織的間諜程式新變種

最近觀察到一種用 GoLang 編寫的新惡意軟體，並與一個被稱為 Mantis (又名Arid Viper，APT-C-23) 進階持續威脅 (APT) 駭客組織有關。據報導，這是屬於 Micropsia 組織的一個新變種惡意軟體。這個被稱為 Arid Gopher 的新變種在今年初被觀察到。

至少從 2014 年開始，Mantis 就參與以間諜為目的針對性目標式攻擊。據瞭解，他們的目標是政府、軍事、媒體、金融、研究、智庫、教育和能源領域的組織。他們主要針對中東地區的組織和個人；然而，攻擊並不局限於這一地區。眾所周知，為了入侵受害者，Mantis 使用含有惡意附件／連結有針對性的電子郵件，並利用戰略網站入侵。許多歸因於該組織的電子郵件似乎表明他們是以阿拉伯語為母語的人。

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

基於機器學習的防禦技術：

- 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 634

2022/03/23

強震後日本製造業遭受社交工程衝擊

在日本東部發生 7.4 級強震幾天後 (16日星期三晚些時候)，Emotet 開始透過惡意電子郵件瞄準日本製造業。攻擊發動者試圖透過詢問地震是否對供應鏈有任何影響來引誘受害者 (電子郵件主題：緊急！調查日本地震對供應商的影響)。眾所周知，Emotet 垃圾郵件參與者密切關注全球新聞，並迅速將其轉化為社交工程攻擊的誘餌。

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.Module!gen3
- SONAR.MSExcel!g*

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.Trojan
- Trojan.Emotet
- Trojan.Mdropper

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/03/23

烏克蘭公司遭受 DoubleZero 資料刪除工具的攻擊

另一個名為 DoubleZero 破壞性惡意軟體已被識別出來，並正被用於針對烏克蘭企業。在此之前，最近在烏克蘭觀察到了一系列破壞性的資料刪除工具攻擊，包括 CaddyWiper、HermeticWiper 和 WhisperGate。DoubleZero 是用經過混淆技術的 .NET 程式碼編寫，它覆蓋或使用 API 呼叫來清除關鍵系統檔案和登錄機碼。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspWrite!g6

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/03/23

Gimmick (*噱頭) -- 發現中國進階持續威脅 (APT) 駭客組織使用新 macOS 惡意軟體

一種名為 Gimmick 新 macOS 惡意軟體已被發現。眾所周知，Gimmick 是一種多平台威脅。雖然早期 Windows 版本是用 .NET 和 Delphi 編寫，但新 macOS 變種是用 Objective C 編寫。據報導，該惡意軟體在最近由中國間諜威脅組織 Storm Cloud 進行的針對性攻擊中被利用。Gimmick 惡意軟體使用公有雲代管平台進行 C&C 通信。

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.Gimmick
- OSX.Trojan.Gen.2
- Trojan.Gen.2

2022/03/23

Emotet 利用烏克蘭和俄羅斯衝突相關的社交工程

正如我們之前報導，烏克蘭和俄羅斯的衝突已經變成多個駭客集團和個體戶駭客的強大社交工程行動。最近幾天，賽門鐵克觀察到 Emotet 行動利用這場戰爭的最新發展，以吸引受害者並透過惡意的 XLSM 檔部署各種惡意軟體。這些電子郵件並非專門針對烏克蘭或俄羅斯組織，因為參與者一直透過亂槍打鳥的電子郵件，將這些電子郵件發送給不同國家的組織。

觀察到的電子郵件主旨：

- *歐洲國家政府 -- 烏克蘭最新消息*
- *能源組合：俄羅斯襲擊烏克蘭對全球能源部門的影響*
- *幫助烏克蘭*

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.Module!gen3
- SONAR.MSExcel!g*

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：

- DTrojan.Emotet
- Trojan.Mdropper
- W97M.Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/03/23

FaceStealer 惡意竊密程式在 Google Play 商店有超過 10 萬次下載

根據最近報導，在 Google Play 商店中觀察到 Android FaceStealer 的下載量超過 10 萬次。此惡意軟體幕後的參與者已自動執行重新打包處理，並將一小段惡意程式碼注入合法的影像處理應用程式，以繞過 Play 商店審查程序。執行後，受害者將被提示輸入 Facebook 帳密，然後這些帳密將被上傳到惡意軟體參與者的 C2 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：

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

2022/03/22

Avoslocker 勒索軟體 -- 用於攻擊美國關鍵基礎設施部門

賽門鐵克安全機制應變中心團隊瞭解到聯邦調查局發出關於被稱為 AvosLocker 勒索軟體變種活動警戒報告。根據報告，AvosLocker 一直針對美國多個關鍵基礎設施部門的實體，包括政府設施、金融服務和製造業。AvosLocker 是一個 RaaS (勒索軟體即務的變種，同時支援 Linux和 Windows 平臺)。該惡意軟體將加密受害者電腦上檔案，並為被加密後的檔案附加 .avos 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Linux.RansomAvos
- Ransom.Avoslocker
- Ransom.AvosLocker!gm1

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

2022/03/22

BitRAT 遠端存取木馬，透過 Webhards 雲端硬碟平台散佈， 危害韓國用戶

在威脅環境中看到 BitRAT 遠端存取木馬已是司空見慣，因為它的程式碼近年來已被洩露過幾次。這種常見的遠端存取木馬被多個團體和個人用來對付企業用戶和一般消費者。最近，一個發動者試圖透過冒充 Windows 10 授權驗證工具來引誘韓國的受害者。這個假冒工具被存放在韓國的雲端硬碟業者--Webhard 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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/03/21

LokiLocker -- 一種新的勒索軟體即服務（RaaS）家族

在真實環境發現一個被稱為 LokiLocker 新的勒索軟體即服務 (RaaS) 家族。該惡意軟體具有停止系統服務和程序及刪除系統備份和磁卷陰影複製 (shadow copies) 的功能。LokiLocker (如果有勾選這個選項) 還可以在指定時間內未收到贖金，試圖清除 (刪除) 受感染的系統。加密檔的副檔名可能會有所不同，因為這一設置是開放給勒索軟體聯盟附屬機構可自行設定的功能之一。

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.LokiLocker
- Trojan.Gen.2
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen66
- SONAR.SuspBeh!gen93
- SONAR.SuspDataRun
- SONAR.SuspLaunch!g18

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。