保安資訊--本周(台灣時間2023/05/12)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 72 萬 8,700 台受保護端點上總共阻止了 8,300 萬次攻擊。這些攻擊中有 91% 在感染階段前就被有效阻止：**(2023/05/07)**

- 在**14萬6,900**台端點上，阻止了**3,380**萬次嘗試掃描**Web**服務器的漏洞。
- 在**24萬9,200**台端點上，阻止了**1,690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬1,900**台**Windows**伺服主機上，阻止了**1,330**萬次攻擊。
- 在**7萬8,000**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,000**台端點上，阻止了**87萬5,600**次嘗試掃描在**CMS**漏洞。
- 在**5萬8,400**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**26萬4,800**台端點上，阻止了**580**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3萬4,000**台端點上，阻止了**200**萬次加密貨幣挖礦攻擊。
- 在**14萬4,100**台端點上，阻止了**1,040**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,300**台端點上，阻止了**9萬8,300**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。

2023/05/11

Rancoz勒索軟體

Rancoz 是最近在網路上發現的勒索軟體。勒索軟體會加密檔案並新增 .rec_rans 的副檔名。該惡意軟體具有刪除受感染電腦上的系統備份、陰影副本和系統日誌的功能。完成加密後，惡意軟體會變更桌布並留下贖金說明，且建議受害者透過電子郵件與攻擊者聯絡。此惡意軟體背後的攻擊者也採用雙重勒索伎倆，透過不支付熟金就要公開洩露入侵的資料來威脅受害者。

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(SONAR)的防護：

- SONAR.Cryptolocker!g42
- SONAR.Ransomware!g38
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.SuspLaunch!gen4
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/05/11

利用Powershell的PowerDash後門

PowerDash 是最近被發現的一個 PowerShell 後門，透過包含惡意 .doc 附件的垃圾郵件進行傳播。附件試圖利用一個已經公布好久的 Microsoft Office／WordPad 遠端程式碼執行 (RCE) 漏洞 CVE-2017-0199 進行傳播。一旦該漏洞被開採利用，就會下載一個 .hta 腳本，然後執行一個 PowerShell stager，作為長駐目的和最終後門檔案的下載。PowerDash 具有收集受感染電腦的系統相關資訊的功能，並轉發到攻擊者所操控的 C&C 伺服器，後續也會等待進一步命令。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Downloader
- Trojan Horse
- Trojan.Gen.NPE.C
- 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：

- Attack: Malicious RTF File CVE-2017-0199

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。

2023/05/11

SpyNote安卓手機平台惡意軟體的最新活動

SpyNote 是一種安卓手機平台惡意軟體，過去幾年在威脅領域頗有人氣，並被各種威脅組織多所採用。該惡意軟體的功能包括從受感染裝置中竊取資料和憑證、鍵擊側錄、Google 身份驗證碼轉發和通話／鏡頭記錄等。惡意軟體通常偽裝成與知名品牌及其公司相關的合法 APP 進行傳播。僅在上個月，就有幾起攻擊行動透過偽裝成日本銀行、7-11、印度鐵路餐飲和旅遊公司 (IRCTC) 之 APP 的 .apk 套件傳播 SpyNote。

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
- 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。

2023/05/10

Umbral惡意竊密程式

Umbral 只是另一個具有 Discord webhooks 功能的普通竊密程式，可供公開使用（發佈在一個流行的 Web 平台上用於版本控制和協作軟體開發），現在也落入一直在進行典型偷渡式下載惡意攻擊者的手中。

在過去幾個星期，賽門鐵克發現有越來越多利用 Umbral 的惡意活動，活動中發現執行擋偽裝成與遊戲相關的安裝程式（例如：Battle.net，一個熱門的遊戲平台）、加密貨幣工具、剪貼簿竊密器 (Clipper) 和駭客工具等。

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 Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/05/10

假冒 Windows更新程式散布Aurora(*極光)竊密程式

賽門鐵克發現惡意廣告攻擊將用戶重導向到假冒的 Windows 安全更新。據報導，攻擊者利用無效的印表機載入器（也稱為“in2al5d p3in4er”）來傳播和植入被稱為“Aurora Stealer”的竊密程式。該竊密程式能夠從受感染的電腦中竊取憑證。

關於 Auror a(*極光) 竊密程式和無效的印表機載入器的防護公告紀錄可以參考以下的文件：

- Aurora (*極光) 竊密程式
- 散布 Aurora 竊密程式的活動明顯增加
- in2al5d p3in4er～惡意程式載入器

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- 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。

2023/05/10

RapperBot 殭屍網路現在能利用被害者電腦的運算資源暗中挖礦

RapperBot 是一個可以發動分散式服務阻斷 (DDoS) 攻擊的殭屍網路，已知自 2022 年年中左右以來就以物聯網裝置為目標。殭屍網路通常利用脆弱的或預設的 SSH／Telnet 憑證並強制存取易受攻擊的裝置，以發起分散式服務阻斷 (DDoS) 攻擊。最近觀察到一些利用 RapperBot 的攻擊行動，在遭入侵的裝置上執行 Monero 加密貨幣挖礦。執行中的挖礦程式可以配置使用多個礦池，其中一些作為挖礦代理託管在 RapperBot 本身的 C&C 伺服器上。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- 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。

2023/05/09

KEKW竊密程式透過PyPI套件傳播

KEKW 竊密程式是最近以 PyPI（Python專案的官方第三方軟體儲存庫 Python Package Index）套件傳播的惡意軟體。KEKW 的功能包括從遭駭的電腦中收集資訊、竊取 cookie 和憑證、擷取瀏覽器資料、執行剪貼簿竊密器 (Clipper) 活動等。收集後，被盜的資料以 JSON 格式並壓縮為 .zip 存檔，然後洩露到攻擊者控制的 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2023/05/08

Dragon Breath進階持續威脅(APT)駭客組織使用雙DLL側載伎倆

根據最近報告，在網路上發現一個利用不同版本的雙 DLL 側載技術全新攻擊行動。據報導，Dragon Breath 又名 APT-27 駭客組織是針對使用中文 Windows 平台來進行網路博弈用戶的攻擊的幕後黑手。攻擊的媒介包括引誘受害者下載和安裝被植入木馬的 Telegram、WhatsApp 和 LetsVPN 等熱門應用程式，以便進行第二階段乾淨的應用程式 DLL 載入，再是惡意軟體 DLL 側載，進而解密最終有效籌載，主要目的從 Chrome 瀏覽器中竊取加密貨幣資產。

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

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。

2023/05/08

惡意竊密程式～“NodeStealer”

NodeStealer 惡意竊密程式由 Javascript 撰寫，透過 Node.js 執行。並偽裝成 PDF 或 Excel 檔的 Windows 可執行檔做傳播。如果被執行，Node.js 的自動啟動模組會新增一個全新的機碼，以便在重啟之間在受害者的電腦常駐。NodeStealer 允許攻擊者竊取瀏覽器 cookie，這些 cookie 可用於跨各種平台（包括 Linux、macOS 和 Windows）劫持 Facebook 帳戶、 Gmail 和其他 outlook 帳戶。

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：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- 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。

2023/05/08

防護亮點：Akira 勒索軟體～鎖定大戶

～防護亮點～

我們賽門鐵克的監控系統最近公開通報一種自稱為“Akira”（攻擊者自己命名）的新勒索軟體變種。然而，它並不完全是原創，看起來是由 Conti 勒索軟體的原始碼來進行修改。

當一台電腦被成功入侵時，資料會被上傳到攻擊者的伺服器，在檔案被加密並附加 .akira 副檔名之前作為威脅受害者之用。隨後是相當冗長的勒索說明，指示受害者安裝 TOR 瀏覽器，以便瀏覽 Akira 聊天室，讓他們可以開始與攻擊者進行談判。

Akira 背後的組織還維護著一個洩密網站，他們在該網站上大辣辣公布某些遭其入侵的金融、建築和房地產等多個受害企業的名稱。

據報導，攻擊者向受害者索價數十萬至數百萬美元不等，這大概取決於該組織認為受害者的支付能力。

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 **零時差**防護技術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(SONAR)的防護：

- SONAR.Ransomware!g*
- SONAR.Ransom!gen98
- SONAR.Ransomconti!g1

基於機器學習的防禦技術：

- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

Symantec Data Center Security (DCS) 預設的強化政策可提供針對 Akira 勒索軟體的零時差保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

*這表示存在多個名稱相似的檢測，例如：SONAR.Ransomware!g1、SONAR.Ransomware!g2 等。

要了解賽門鐵克端點防護(SEP)的進階機器學習防護技術，請點擊此處。

要了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

要了解有關賽門鐵克 DCS：Data Center Security～資料中心安全更多訊息，請單擊此處。

2023/05/08

安卓手機平台惡意軟體～FluHorse

FluHorse 是一種新發現針對東亞地區的安卓手機平台用戶的惡意軟體。FluHorse 是由 Flutter 的開放原始碼框架開發。該惡意軟體透過網路釣魚和社交工程傳播，並偽裝成合法金融機構或收費系統的APP。FluHorse 惡意軟體的目標是竊取憑證、雙因素身份驗證 (2FA) 認證碼和信用卡資訊等。收集後，被竊取的資料將被外洩到攻擊者所操控的 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：

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
- 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。

2023/05/05

SideCopy進階持續威脅(APT)駭客集團最新活動

SideCopy 是一個先進的駭客集團，至少從 2019 年開始就在駭客圈展露頭角。眾所周知，該駭客集團主要鎖定印度、阿富汗的組織和政府機構為目標。最近與該駭客集團有關聯的活動已被發現使用遠端存取木馬 (RAT)，例如：Action RAT 和 AllaKore RAT。據報導，攻擊者還利用名為 SILENTTRINITY 漏洞利用的後滲透攻擊 (Post-Exploitation) 技術開發框架來生成有效籌載。已經被散佈的遠端存取木馬 (RAT) 具有允許攻擊者檢索遭駭入電腦的詳細資訊、執行任意指令或下載更多惡意籌載的功能。

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(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen203
- CL.Downloader!gen241
- Downloader
- ISB.Downloader!gen67
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2022/11/24

Aurora(*極光)竊密程式

Aurora 是另一個以惡意軟體即服務 (Malware-as-a-Service) 的形式銷售的竊密程式。據報導，它於今年初首次被發現，最近在地下網站常見它的廣告。雖然它的曝光度還沒有達到其他更惡名昭彰的竊密程式的水準，但它已經開始被各種駭客組織和個人所採用，這些駭客組織和個人正在進行透過典型瀏覽網頁時的偷渡式下載攻擊活動。Aurora 具有一般竊密程式的常見功能--與其他竊密程式的功能相比並沒有特別顯眼。

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.Dropper
- SONAR.PsDownloader!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Suspicious: Content
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Reputation.1

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.B

2023/05/01

散布Aurora竊密程式的活動明顯增加

Aurora 竊密程式是一種基於 Golang 程式語言的惡意程式，以惡意軟體即服務 (MaaS) 營運模式進行銷售。該惡意軟體於 2022 年首次出現，自發布以來已經多次進行優化與更版。Aurora 具有相當典型的竊密程式功能，它主要在竊取系統資訊、憑證、銀行帳號資訊、加密貨幣錢包、cookie 等。在過去的幾個星期中，賽門鐵克觀察到與散布 Aurora 竊密程式相關的惡意活動有所增加，這可能顯示該惡意軟體家族在威脅環境中越來越受歡迎。

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(SONAR)的防護：

- AGR.Terminate!g2

- SONAR.ProcHijack!g45
- SONAR.Susp.Beh!gen93
- SONAR.SuspLaunch!g52
- SONAR.SuspLaunch!g266
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Infostealer.Aurora!g1
- Packed.Generic.528
- Packed.Generic.616
- 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.B!100
- Heur.AdvML.B!200
- 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: Aurora Infostealer Activity
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 735

2023/04/19

in2al5d p3in4er～惡意程式載入器

許多惡意軟體攻擊者使用載入器 (Loader) 來部署他們的惡意軟體，這是一種提高攻擊有效性和隱蔽性的常用伎倆。Aurora 竊密程式在最近的惡意行動中，採用其中一種稱為“Invalid Printer*無效印表機”(也稱為“in2al5d p3in4er”) 的載入器。據報導，該載入器幕後的駭客組織或個體戶一直在使用 YouTube 為誘餌，將正在搜尋軟體和工具程式的受害者誘騙到假冒的網站。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Suspicious: Content
- Suspicious: Reputation
- WS.Reputation.1