保安資訊--本周(台灣時間2023/02/10)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 85 萬 9,400 台受保護端點上總共阻止了 1 億 400 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/02/06)**

- 在**15萬9,800**台端點上，阻止了**4,060**萬次嘗試掃描**Web**服務器的漏洞。
- 在**30萬1,000**台端點上，阻止了**2,390**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬9,300**台**Windows**伺服主機上，阻止了**1,640**萬次攻擊。
- 在**8萬6,000**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬9,700**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**7萬2,200**台端點上，阻止了**230**萬次嘗試利用的應用程式漏洞。
- 在**28萬4,000**台端點上，阻止了**590**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,300**台端點上，阻止了**320**萬次加密貨幣挖礦攻擊。
- 在**15萬5,000**台端點上，阻止了**1,220**萬次向惡意軟體**C&C**連線的嘗試。
- 在**3,200**台端點上，阻止了**13萬4,700**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。

2023/02/09

PYbot～發動分散式阻斷服務攻擊(DDoS)的惡意軟體

PYbot 是一種採用 Python 撰寫開發的 的 DDoS 惡意軟體，針對 Windows 環境來發動攻擊。該惡意軟體會偽裝成名為 Nitro Generator 的 Discord Nitro 權杖產生器軟體來進行散佈。PYbot 支持多種類型的 DDoS 攻擊，包括 TCP Flood、TCP SYN Flood、UPD Flood、VSE（Valve Source Engine）Flood 和 HTTP GET Request Flood。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2023/02/08

Clop加密勒索軟體的Linux新版本帶有"仁慈"的漏洞

眾所周知的 Clop 勒索軟體已經新出現 Linux 平台的版本。Linux 平台的新版本被證實拿來發動真實環境的網路攻擊始於 2022 年 12 月底前後，與 Windows 版本類似。它還具有特別鎖定 Oracle 資料庫相關資料夾的特性，以加速加密勒索得逞。Linux 版本的 Clop 的加密功能已被證實有瑕疵，允許受害者在不支付贖金的情況下也能解密被加密的檔案。這個最新的 Clop Linux平台版本很可能仍處於開發階段，並且相信後續會有更頑強的版本不斷出現，並將繼續鎖定 Linux 的系統為目標。

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：

- Packed.Generic.620
- Ransom.Ploc
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/02/08

最新的Medusa(*美杜莎)殭屍網路變種帶有勒索軟體及其他功能模組

Medusa 是一個源於高人氣的 Mirai 惡意軟體程式碼的用來發動分散式阻斷服務攻擊(DDoS)的殭屍網路。該殭屍網路的最新變種稍早在真實網路環境中曝光，並新增了勒索軟體和 Telnet 暴力破解模組。其勒索軟體模組能夠在受感染的機器中搜索特定副檔名的檔案，並採用 AES 256 位元加密機制進行加密，完成後會對被加密檔新增 .medustastealer 的副檔名。該惡意軟體還具有在加密後刪除所有檔案的功能，更像是資料刪除程式(wiper)。

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

2023/02/08

烏克蘭遭受 Graphiron 竊密程式的攻擊

Nodaria 間諜組織 (又名 UAC-0056) 正在使用一種全新的兩階段竊密程式對烏克蘭發動目標式攻擊。Graphiron 採用 Go 程式語言所撰寫的惡意竊密程式，可以從受感染的電腦上收集包含括系統資訊、憑證、螢幕截圖和檔案等多元資訊。Graphiron 的最早足跡可追溯到 2022 年 10 月。它至少持續被使用到 2023 年 1 月中旬，可以合理地假設它仍然是 Nodaria 工具組的一部分。該惡意軟體與舊的 Nodaria 工具 (例如：GraphSteel 和 GrimPlant) 有一些相似之處。

在我們的部落格文章中有更多資訊可供參考：Graphiron：俄羅斯針對烏克蘭所部署的全新竊密惡意軟體。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader.Graphiron
- Infostealer
- Infostealer.Graphiron
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/02/07

TgToxic安卓手機行動惡意軟體

TgToxic 是一種 Android 安卓手機行動惡意軟體，已證實自去年年中以來持續鎖定東南亞地區的用戶發動攻擊行動。該惡意軟體已被用於網路釣魚和資訊竊取。攻擊者的目標是竊取並洩漏受感染用戶的銀行或電子郵件 APP 和加密貨幣錢包相關的憑證和資料。TgToxic 透過 WebSocket 通訊協定與攻擊者的 C&C 伺服器的通訊。

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.Malapp
- 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。

2023/02/06

針對遊戲和博弈行業的IceBreaker惡意軟體

去年 9 月，一種稱為“IceBreaker APT”的後門惡意軟體被發現針對遊戲和博弈公司。該惡意軟體的來源和建立者目前尚不清楚。

感染鏈會從威脅行為者聯繫網站的客戶支援開始，聲稱他們遇到問題，假裝發送顯示問題的螢幕截圖，但攻擊者將發送一個包含惡意 ZIP 壓縮檔的鏈結。隨後，惡意 LNK 檔案將下載 IceBreaker 酬載檔案。

IceBreaker 後門具有以下功能：

- 透過威脅內建的擴展功能進行自定外掛
- 程序搜尋
- 從本機儲存區竊取密碼和 cookie。它特別針對谷歌瀏覽器
- 透過開源項目 tsocks 在受感染的機器中啟用 Socks5 反向代理伺服器

- 透過開機自動執行的啟動資料夾 “\Microsoft\Windows\Start Menu\Programs\Startup\WINN.lnk ” 中建立一個全新的 LNK 檔案以持續維持常駐
- 透過web sockets通訊協定將檔案洩露到遠端伺服器
- 在受感染的機器上執行自定義的 VBS 腳本檔
- 從受害者的機器上截取螢幕截圖
- 建立遠端 shell 連線

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：

- CL.Downloader!gen89
- ISB.Downloader!gen52
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/02/06

HeadCrab 惡意軟體到處傳播

HeadCrab 至少從 2021 年 9 月開始就存在。眾所周知，這種難以捉摸的惡意軟體寄生在 Redis 伺服器中。其複雜設計使其能夠僅在記憶體中運行，並且僅與合法的 IP 位址通訊以逃避檢測。

HeadCrab 的主要目的除了建立用來挖掘 Monero 加密貨幣的殭屍網路之外，它還具有其他惡意功能，例如：執行 shell 命令、載入無檔案的內核模組 (kernel modules) 以及將資料洩露到遠端伺服器。

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 Horse
- WS.Malware.2

2023/02/06

防護亮點：DCS提供固若金湯、堅如磐石的伺服主機保護，號稱攻無不克的全新Royal 勒索軟體家族，也無功而返

～防護亮點～

我們最近陸續發布幾則與“Royal”加密勒索軟體相關的公告，它是近期才出現比較新的勒索軟體家族。Royal 會透過各種方式傳播，例如：「回撥網釣」(Callback Phishing)、Batloader 和 Qbot 等惡意軟體酬載載入程序、應用程式漏洞 (CVE-2022-27510 是最近的一個漏洞) 以及各種廣泛可用的開放原始碼工具。據報導，它並鎖定虛擬平台環境為目標。惡意軟體酬載載入程序是在攻擊者和目標系統之間建立通訊的程序，通常代表攻擊的初始階段。這些前段載入程序使用常見的方法傳播，例如：惡意廣告、包含惡意鏈接或嵌入惡意檔案的垃圾郵件、虛假網站、論壇等。

被 Royal 加密後的檔案會被新增 .royal 的副檔名並留下一個 readme.txt 文字檔，將受害者引導至 Tor 的支付贖金網站，並刪除備份和磁碟區陰影複製，以脅迫並增加對贖金支付的壓力。它還會加密網路分享磁碟，並採用可加速的多執行緒加密機制。Royal 背後的駭客集團織針對多個商業領域，包括醫療保健、保險、工業公司，甚至攻擊一個廣受歡迎的英國賽車場。

正如我們之前關於 Royal 的貼文所表明的那樣，賽門鐵克在我們的好幾種保護技術都能同時偵測到這種新型的勒索軟體，包括靜態檔案分析、行為偵測、啟發式機器學習和網路層的特徵碼，然而，根據我們對瞄準 Windows 伺服器的 Royal 勒索軟體在網路的觀察方面，我們還想重點介紹我們的重要伺服器等級的安全解決方案 Symantec Data Center Security (DCS)。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，當然預設強化安全政策就能偵測到以前從未見過的 Royal 勒索軟體變種和行為，如下所示：

基於安全強化政策(適用於使用DCS)：

- DCS 可限制任何軟體的安裝， 當然能防止惡意軟體工的安裝與執行，不管是本地端安裝還是透過遠端執行工具 PsExec 來進行遠端安裝和執行 Royal 勒索軟體。
- 最底層的程序 (Process) 層級的禁用技術，可最有效防止任意系統命令執行和濫用兩用工具進行惡意活動。
- DCS 專屬最小權限與最低資源 "夠用就好" 的工作環境沙箱機制，可防止篡改關鍵系統檔案和註冊表資源。
- 為了確保滴水不漏的最高等級的保護，使用者可以設置綿密與嚴謹的 DCS 網路保護規則，為需要高權限的服務和應用程序設置最嚴謹的網路邊界管控與限制。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

對固若金湯、堅如磐石的賽門鐵克重要伺服主機保護方案-- DCS(Data Center Security) 想深入了解，歡迎瀏覽我們的網站，請點擊此處。

2023/02/05

PixPirate～發動自動轉帳系統(ATS)攻擊巴西的另一個全新惡意APP

過去幾年，巴西發現多種安卓平台上的銀行惡意APP，最近，又有一種名為 PixPirate 的惡意手機 APP 也曝光。據報導，該惡意軟體能夠執行自動轉帳系統 (Automatic Transfer System，ATS) 攻擊，以竊取受害者的財務憑證。ATS 攻擊允許攻擊者在合法的網路銀行動 APP 和加密貨幣錢錢包的地址中輸入資訊，進而接手使用者的操作，包含濫用輔助功能服務 (Accessibility Service)。在佈署方面，它一直偽裝成安卓平台上常見的 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。

- AdLibrary:Generisk
- AppRisk:Generisk

2023/02/05

新型竊密程式～NajtriStealer

賽門鐵克最近觀察到一種名為“NajtriStealer”的竊密程式，該惡意程式有在 Telegram 和 TikTok (抖音) 上投放廣告。這種惡意程式與許多其他已出現的惡意程式相似，因為它不是特別狡滑複雜，因此知名度就大不如其他惡名昭彰的竊密程式來得那麼高。

NajtriStealer 具有以下功能：

- 從常用的應用程式中劫取用戶憑證，例如：Discord、Chrome、Opera、Brave 和 Yandex
- 從網路瀏覽器中竊取 cookie、密碼、一鍵自動填入資料和信用卡資訊
- 從 Telegram 桌面應用程式竊取連線資訊
- 竊取Discord Backup Codes 應急憑證

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：

- Infostealer

2023/02/05

利用VMware ESXi老舊漏洞的Nevada勒索軟體

另一個勒索軟體，這個被稱為“Nevada”的勒索軟體，最近因透過一個老舊漏洞攻擊全球的 VMware ESXi 伺服器而成為頭條新聞。CVE-2021-21974 允許未經身份驗證的攻擊者在受影響的系統上提權並執行任意程式碼。

VMware ESXi 伺服器用於建立虛擬機 (VM) 並在實體機和虛擬化環境之間提供一個抽象層，使勒索軟體攻擊具有高度破壞性。該勒索軟體幕後的行動者同時運行 Windows 和 Linux 版本。到目前為止，我們已經能夠確認對 Windows 的保護。加密後，被加密檔案會被新增 .NEVADA 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.CryptLocker!g36
- SONAR.RansomPlay!gen1

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

2023/02/02

惡意垃圾郵件攻擊行動鎖定銀行、媒體、保險、食品和物流行業

詐騙者冒充知名國際公司和組織的情況並不少見，航運業通常是主要目標。最近就有個例子，賽門鐵克觀察到一名攻擊者一直鎖定銀行、媒體、保險、食品和物流公司為目標，同時以航運為主旨的電子郵件攻擊行動中冒充土耳其物流公司。該公司具有高知名度並提供全球性的空運、海運和公路貨運服務，促使受害者大大降低警戒而陷入誘惑。

這些電子郵件 (主旨：“Q#2201516 Ex-Work Sea Shipment From Door To France”）包含一個偽裝成 PDF 檔案惡意 .cab 的 Windows 之封包 (Cabinet) 檔案，如果開啟該檔案，收件人將會感染 Formbook 惡意程式，這是一個老而彌堅的竊密程式。根據賽門鐵克的資料，在日本、法國、美國和英國等國家／地區都有相關的攻擊行動被發現。

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：

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
- Scr.Malcode!gen19

基於機器學習的防禦技術：

- Heur.AdvML.B