保安資訊--本周(台灣時間2022/04/22)
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 1.949 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/04/18)**

- 在**22萬1,000**台端點上，阻止了**1.026億**次嘗試掃描**Web**服務器的漏洞。
- 在**47萬5,500**台端點上，阻止了**3,630萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬7,300**台**Windows**伺服主機上，阻止了**2,440萬**次攻擊。
- 在**16萬7,400**端點上，阻止了**990萬**次嘗試掃描伺服器漏洞。
- 在**8萬9,900**台端點上，阻止了**430萬**次嘗試掃描在**CMS**漏洞。
- 在**12萬7,900**台端點上，阻止了**360萬**次嘗試利用的應用程式漏洞。
- 在**38萬4,800**台端點上，阻止了**1,090萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,000**台端點上，阻止了**330萬**次加密貨幣挖礦攻擊。
- 在**12萬3,800**台端點上，阻止了**560萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,700**台端點上，阻止了**24萬5,800**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。

2022/04/21

利用 Spring4Shell 的 CVE-2022-22965 漏洞散布挖礦行動

在真實環境觀察到利用 Spring4Shell 漏洞 (CVE-2022-22965) 散布挖礦惡意程式的新行動。在行動的分配階段，攻擊者確定目標的作業系統，並依 Windows 或 Linux 的系統提供惡意軟體籌載。被植入的挖礦惡意程式具有停用防火牆並刪除任何已知與它有競爭關係的挖礦程序（如果發現）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：

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.NPE

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：

- Audit: Spring Framework CVE-2022-22965 Scanning
- Web Attack: Spring Framework CVE-2022-22965
- Web Attack: Spring Framework CVE-2022-22965 2

基於安全強化政策(適用於使用DCS)：

賽門鐵克 Data Center Security (DCS) 入侵預防 (IPS) 內建的安全政策，早就能預防 Spring4Shell 的漏洞利用並提供零時差攻擊提供保護。

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。

2022/04/20

Oski 竊密程式繼續瞄準企業和消費者

Oski Stealer 是一支竊密程式，專注於從 Web 瀏覽器中竊取機敏資訊，包括用戶憑證和加密貨幣錢包等。這種惡意軟體並非新鮮玩意，首次被觀察到於 2019 年底和 2020 年初在地下論壇上銷售。多年來，它一直活躍在威脅領域，儘管它曾經並且仍然不如其他惡名昭彰的竊密程式那麼普遍。

由於它被多個團體和個人使用，賽門鐵克會定期觀察針對企業和消費者的活動 (透過惡意電子郵件和瀏覽網頁時的順道下載)，但其他網路罪分子也可能成為目標。最近幾天，一名攻擊者甚至試圖透過將 Oski 偽裝成惡意加密軟體 (Alien*外星人) 和 Mars 竊密程式的建構器 (Builder) 來引誘和感染網路罪分子--但往往是弄巧成拙、偷雞不成蝕把米。

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.AM.E!g11
- SONAR.AM.E!g13
- SONAR.SuspBeh!gen609

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：

- Packed.Generic.548
- Scr.Malcode!gdn30
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

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

2022/04/20

新的 BotenaGo 惡意軟體變種

BotenaGo 是一種用 Golang 程式語言編寫的惡意軟體變種，早在去年就被發現。最初，BotenaGo 包含 30 多種不同的漏洞利用，並針對各種路由器和物聯網設備。根據最近一份報導，這種惡意軟體的一個新變種，已經去除大部分的漏洞利用，目前專門針對 Lilin DVR 設備。與 BotenaGo 攻擊相關的後期階段，還看到來自 Mirai 家族的其他惡意軟體也被部署到受感染的裝置上。

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：

- Hacktool
- Linux.Lightaidra
- Trojan.Gen.NPE

2022/04/20

Shuckworm 高階駭客集團，持續對烏克蘭發動網路攻擊行動

與俄羅斯有聯繫的 Shuckworm 間諜組織（又名 Gamaredon、Armageddon）正在持續對烏克蘭的組織發起激烈網路攻擊。自 2014 年首次出現以來，Shuckworm 幾乎將其業務集中在烏克蘭。自俄羅斯入侵該國，這些攻擊一直有增無減。該組織近期活動的標誌之一是在目標電腦上部署多個惡意軟體有效籌載。這些有效籌載通常是同一惡意軟體 (Backdoor.Pterodo) 的不同變種，目的在執行類似的任務。

在我們的部落格文章可中閱讀更多內容：Shuckworm (*蚱蜢)：間諜組織繼續針對烏克蘭發動激烈攻擊行動。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!g39

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Pterodo.B
- Backdoor.Pterodo.C
- Backdoor.Pterodo.D
- Backdoor.Pterodo.E
- Trojan Horse
- Trojan.Certbypass
- Trojan.Dropper
- Trojan.Gen.MBT

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：

- 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。

2022/04/19

PYSA 勒索軟體集團依然活躍

PYSA（Protect Your System Amigo--保護您的系統Amigo）勒索軟體集團，也稱為 Mespinoza，自 2020 年以來一直活躍，主要針對教育和醫療保健行業。PYSA 的攻擊會洩露機敏和關鍵資料，加密受害者檔案並要求贖金。他們的攻擊通常透過網路釣魚電子郵件來濫用 RDP 漏洞，並高度依賴現成的工具，包括 Cobalt Strike、Empire、WinSCP 和 Cloud Storage 服務。在最近的攻擊中，使用 Chisel (*鑿子) 通道工具，並透過 PowerShell 腳本為目標環境預做準備。

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.Ransom!gen57
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Gen
- Ransom.Hermes!gen2
- Ransom.Mespinoza
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/04/19

安卓平台上：VajraSpy 惡意程式

VajraSpy 是一種RAT（遠端存取木馬）變種，它使用 Google 雲端硬碟從 Android 使用者那裡收集被盜資料。VajraSpy 被歸咎於一個駭客集團：APT-Q-43，積極針對巴基斯坦軍事人員。該惡意軟體主要在收集有關受感染設備的詳細資訊以及使用者資料，包括：簡訊、WhatsApp 和 Signal 訊息以及通話記錄等。

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：

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

2022/04/18

近期的 Qakbot (Qbot) 惡意垃圾郵件行動

觀察到最近 Qakbot 垃圾郵件行動夾帶內建巨集的Excel XLSB檔案。啟用巨集會導致下載 Qakbot DLL 檔，這些檔案用於啟動與 Qakbot 專用 C&C 伺服器的通信。觀察到與 DarkVNC 和 Cobalt Strike 相關的惡意流量。

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.C
- WS.Malware.2
- W97M.Downloader

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。

2022/04/18

打死不退的 Andoid 惡意程式：Joker

Joker 是惡名昭彰的 Android 惡意軟體，它一直能夠潛入 Google Play 商店，截至今天，幾乎每天都有關於新 Joker 變種的報導。這種行動惡意軟體試圖透過攔截簡訊來模擬點擊，並為受害者訂閱頂級服務。

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

2022/04/15

在針對烏克蘭組織的攻擊中發現 IcedID 受到濫用

據報導，IcedID 惡意軟體被濫用於針對烏克蘭各種組織的攻擊。一場被認為是「UAC-0041」威脅組織發起的網路攻擊，利用名為“Mobilization Register.xls”並內嵌巨集的 Excel 試算表檔案。一旦開啟並啟動巨集就會被感染 GzipLoader 惡意軟體，該惡意軟體又會將 IcedID 有效籌下載到受感染的電腦上。IcedID 惡意軟體至少從 2017 年就已為人所知，直到今天，它仍然是威脅版圖上繼續發光的頂級銀行木馬之一。

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：

- ISB.Downloader!gen60
- ISB.Downloader!gen68
- ISB.Downloader!gen433
- Trojan Horse
- Trojan.Mdropper
- Trojan.Gen.NPE.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。

2022/04/15

TinyFluff 後門由 OldGremlin 威脅組織散布

根據最新報導，一個名為 OldGremlin 的威脅組織，最近至少活躍在兩個不同的垃圾郵件行動中，這些行動被用來散布名為 TinyFluff 後門惡意軟體。TinyFluff 主要用於偵察目的和收集有關受感染系統的資訊。攻擊的最後階段，包括以稱為 TinyCryptor 勒索軟體變種形式提供的最終有效籌載。

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.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader

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。