保安資訊--本周(台灣時間2022/02/18)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 130 萬個受保護端點上總共阻止了 1.3 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/02/13)**

- 在**23萬5,400**台端點上，阻止了**1.016億**次嘗試掃描**Web**服務器的漏洞。
- 在**50萬9,200**台端點上，阻止了**4,440萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬6,900**台**Windows**伺服主機上，阻止了**2,520萬**次攻擊。
- 在**17萬9,200**端點上，阻止了**1,020萬**次嘗試掃描伺服器漏洞。
- 在**10萬4,000**台端點上，阻止了**480萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬3,900**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**47萬4,700**台端點上，阻止了**1,320萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,200**台端點上，阻止了**390萬**次加密貨幣挖礦攻擊。
- 在**13萬1,800**台端點上，阻止了**520萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,700**台端點上，阻止了**27萬1,400**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。

2022/02/17

最新正在散布的LockBit 勒索軟體行動

在真實環境陸續發現一個散布 Lockbit 勒索軟體的新行動。散布方法包含 (但不限於) 透過垃圾郵件夾帶內藏二進位勒索軟體檔的 .zip 壓縮。這些惡意電子郵件多為假冒與求職申請或侵犯版權通知相關的郵件。一旦被執行，惡意軟體將刪除現有磁碟上的磁卷陰影複製，停用多個系統程序並開始加密用戶資料，同時將加密後的檔案重命名為帶有 .lockbit 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Lockbit
- Ransom.Lockbit!g2
- Ransom.Lockbit!gen3
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- Ransom.Lockbit!gm1
- SONAR.RansomLckbit!g3
- SONAR.SuspBeh!gen82

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：

- Attack: Ransom.Lockbit Activity
- Attack: Ransom.Lockbit Activity 2
- Attack: Ransom.Lockbit Activity 3

2022/02/17

Kraken--Golang 撰寫的殭屍網路

根據最近發布的報告，去年被發現的 Kraken 殭屍網路，該經營者仍然持續增強其威力與功能。Kraken 具有各種功能，可以竊取加密錢包並收集有關受感染系統的資訊。該惡意軟體還可能下載並執行任意有效籌載。在觀察到的幾個散布行動中，Kraken 殭屍網路的二進位檔案已在藉助 SmokeLoader 惡意軟體的狀況下攻城掠地，勢不可擋。

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

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.RGC!g510
- SONAR.SuspPE!gen19

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2022/02/17

破壞力兇猛：Trickbot 殭屍網路攻擊

殭屍網路的兩大梟雄：Trickbot 與 Emotet 的持續狼狽為奸，助長針對主要位於美國的金融、加密貨幣和技術公司的大規模攻擊。惡名昭彰的 Trickbot 是一種模組化惡意軟體，能夠竊取憑證，隨後為其作者提供存取權限，並允許他們從受害者那裡獲取敏感資料。

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.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已於第一時間收錄於不安全分類列表中。

2022/02/17

Quantum (*量子)勒索軟體：惦惦吃三碗公的蠶食戰略，不容小覷

另一種值得關注的勒索軟體，即 Quantum (*量子) 勒索軟體，繼續在百家爭鳴的勒索軟體江湖中走跳。這些攻擊者使用運行良好的勒索軟體雙重勒索方案和其他經驗豐富的勒索軟體攻擊者所使用的感染媒介，看似泛泛之輩卻惦惦吃三碗公的蠶食戰略，不容小覷。

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!g75
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g33

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Quantum
- Ransom.Quantum!gm1

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 56 - Ransom Note

2022/02/16

好工具也能成為壞凶器：Eagle Monitor RAT

Eagle Monitor RAT 是發佈在熱門的網際網路託管平台上，用於軟體開發和版本控制的眾多遠端存取工具之一。它也在地下論壇和各種駭客網站上得到回應，這意味著不僅有經驗的網路犯罪分子可以輕鬆免費存取 Eagle Monitor RAT，而且有樣學樣的腳本小子 (script kiddies) 也渴望開始他們的網路犯罪生涯或提升駭客功力的知識庫和武器庫。

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.BC.Cryptlk!g4

檔案型(基於回應式樣本的病毒定義檔)防護：

- SMG.Heur!gen
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/02/16

Nanocore (*納米核心)，屹立不搖的老木馬

遠端存取特洛伊木馬 (也稱為 RAT) 已屢見不鮮，但它們仍然佔據與安全相關的新聞標題相當的版面。這些惡意軟體通常用於針對性和非針對性攻擊，是網路犯罪集團和個人駭客所偏愛的熱門工具--無論是經濟利益、間諜活動還是更令人毛骨悚然的事情。Nanocore 就是這樣一種已經存在多年的 RAT，並且至今仍在使用。洩露和破解的版本在網際網路上各種地下論壇和其他公共平台上免費提供。賽門鐵克不斷觀察導致 Nanocore 垃圾郵件和順道下載攻擊。

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!gen25
- SONAR.SuspDataRun

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.Nancrat

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/02/16

TA2541 駭客集團是攻擊航空和運輸業的元兇

根據最近針對航空、國防和運輸等多個行業公司多項攻擊行動與被稱為 TA2541 駭客集團有所關聯的報告。該駭客集團活動史至少可以追溯到 2017 年，並顯示攻擊者利用各種可購得的商品化 RAT (遠端存取木馬)，例如：AsyncRAT、STRRAT 或 WSH RAT。該駭客集團通常使用魚叉式網路釣魚電子郵件作為初始感染媒介。這些電子郵件試圖讓收件者下載通常託管於雲端硬碟服務商上有效籌載檔案。

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
- Infostealer
- Trojan Horse

- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- VBS.Downloader.Trojan
- 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已於第一時間收錄於不安全分類列表中。

2022/02/16

Allcome Clipbanker 鎖定電子商務網站結帳網頁的付款表單和加密錢包

Allcome Clipbanker 是在地下論壇上出售的變種惡意軟體。該惡意軟體功能包括以攻擊者的地址替換加密貨幣錢包地址。該惡意軟體可以對各種其他支付形式 (例如：PayPal 電子郵件地址) 執行相同的操作。

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
- WS.Malware.1

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已於第一時間收錄於不安全分類列表中。

2022/02/15

Medusa (*美杜莎)行動惡意軟體，濫用簡訊騙局 (Flubot) 伎倆散布

根據最近發布的報告，Medusa (*美杜莎) 行動惡意軟體最近透過之前用於簡訊騙局 (Flubot) 惡意軟體 (又名 Cabassous) 行動的相同散布架構模式進行傳播。Medusa 惡意軟體包括各種功能，例如：鍵盤側錄、通話錄音或簡訊攔截等。Android 系統的輔助服務功能 (Accessibility Services) 濫用，允許 Medusa 攻擊者在受感染裝置上對正在執行的任何應用程式 APP 執行附加命令。

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。

- AdLibrary:Generisk
- Android.Reputation.1
- 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已於第一時間收錄於不安全分類列表中。

2022/02/15

BitRAT 惡意軟體，濫用 NFT 誘餌檔案傳播

BitRAT 惡意軟體透過偽裝成包含 NFT 相關資訊的惡意 Excel 檔案進行傳播。在最近這些行動中散布的 BitRAT 變種利用隱藏 VNC (HVNC)，為攻擊者提供對受感染主機遠端存取。一旦部署，惡意軟體將嘗試竊取任何本地儲存的憑證、挖掘加密貨幣、記錄擊鍵或將其他任意檔案下載到機器上。

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：

- CL.Downloader!gen7
- Trojan Horse
- Trojan.Mdropper

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。

2022/02/14

FBI 網路安全公告示警--針對企業的 BlackByte 勒索軟體

賽門鐵克安全機制應變中心團隊獲悉最新 FBI 網路安全公告，該公告涉及最近一波針對企業 BlackByte 勒索軟體攻擊。BlackByte 是一種勒索軟體即服務 (RaaS) 惡意軟體，可同時加密實體機和虛擬機伺服主機的檔案。在一些較早 BlackByte 攻擊中，已經看到該惡意軟體幕後的主使者利用 MS Exchange Server 漏洞來入侵目標網路。

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
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/02/11

ModifiedElephant (*改良大象) 進階持續威脅 (APT) 集團

根據最近發布的一份報告，被稱為 ModifiedElephant (*改良大象) APT 組織至少自 2012 年以來一直積極針對印度的人權運動人士、記者、學者和律師為對象進行活動。該組織一直在利用魚叉式網路釣魚和惡意檔案來傳遞各種惡意軟體籌載，例如：Netwire 或 DarkComet。

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
- MSIL.Downloader!gen9
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Klovbot
- Trojan.Mdropper
- W32.Extrat
- W32.Ramnit.B!inf

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。

2022/02/11

Squibldoo 傳播 Qbot 和 Lokibot 等木馬

最近觀察到一些威脅攻擊者選擇使用一種稱為“Squibldoo”的舊技術，使用 regsvr32 透過 Microsoft Office 檔案散布 Qbot 和 Lokibot 等木馬。Squiblydoo 是一種用於散布惡意軟體已知的傳統攻擊媒介，這種方法濫用 Regsvr32（regsvr32 是控制項命令工具，可註冊或取消控制項檔案。）來繞過對執行腳本的限制並規避應用程式白名單保護，不然就結束整個攻擊鏈。

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.Gen.NPE
- Trojan.Mdropper
- WS.Malware.1
- W97M.Downloader