保安資訊--本周(台灣時間2022/07/15)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 100 萬個受保護端點上總共阻止了1.819 億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/07/11)**

- 在**20萬7,300**台端點上，阻止了**8,970**萬次嘗試掃描**Web**服務器的漏洞。
- 在**38萬5,800**台端點上，阻止了**3,690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬6,400**台**Windows**伺服主機上，阻止了**2,090**萬次攻擊。
- 在**13萬9,000**端點上，阻止了**830**萬次嘗試掃描伺服器漏洞。
- 在**6萬8,500**台端點上，阻止了**340**萬次嘗試掃描在**CMS**漏洞。
- 在**10萬7,600**台端點上，阻止了**320**萬次嘗試利用的應用程式漏洞。
- 在**30萬3,600**台端點上，阻止了**790**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬6,400**台端點上，阻止了**440**萬次加密貨幣挖礦攻擊。
- 在**46萬7,000**台端點上，阻止了**640**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,700**台端點上，阻止了**20萬8,700**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。

2022/07/14

NjRAT 遠端存取木馬的危害仍然層出不窮

NjRAT (也被稱為 Bladabindi 或 Ratenjay) 是過去十年中最被廣泛使用的遠端存取木馬 (RATs) 之一。賽門鐵克至今仍然持續監視這個惡意軟體家族的活動。NjRAT 被用於從入侵的端點竊取資料，這包括鍵盤側錄、儲存的憑證、瀏覽網頁的歷史記錄……等。一些較新的 NjRAT 變種也針對加密貨幣錢包。這個遠端存取木馬 (RAT) 還允許攻擊者透過遠端 shell 發送指令、修改登錄表機碼以及下載整個攻擊鏈所需的檔案。

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：

- Backdoor.Ratenjay
- Backdoor.Ratenjay!gen2
- Backdoor.Ratenjay!gen3
- Downloader
- MSIL.Trojan!gen2
- Packed.Generic.619
- Scr.Malcode!gdn14
- Trojan Horse

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：

- System Infected: Backdoor.Ratenjay RAT Activity
- System Infected: Trojan.Backdoor Activity 555
- System Infected: Trojan.Backdoor Activity 634

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。

2022/07/14

Transparent Tribe (*透明部落) 高階駭客組織針對印度教育單位及其學生

Transparent Tribe 高階駭客組織最新行動針對印度，特別是教育單位及其學生。最初的感染媒介是魚叉式網路釣魚電子郵件，其中包含惡意檔案附件或一個可下載惡意檔案的網頁連結。如果該檔案被開啟並執行內嵌巨集，該電腦將被 CrimsonRAT 遠端存取木馬所感染。

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：

- MSIL.KillAV!gen1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Mdropper
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2022/07/13

Paradies (*天主教徒) 加密貨幣剪貼簿竊密器鎖定加密貨幣錢包

加密貨幣剪貼簿竊密器 (Clipper) 是一種新興威脅，其主要目的是將受害者加密貨幣錢包位址與威脅者擁有的位址進行交換。儘管目前加密貨幣市場出現動盪，但相關的威脅活動並沒有減少，賽門鐵克繼續監視這種類型的惡意軟體。最近在威脅領域觀察到一種名為 Paradies 的加密貨幣剪貼簿竊密器，它冒充破解軟體和駭客工具，例如：Spotify 檢查軟體。截至目前，它主要針對的是消費者。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/07/13

Lilith (*莉莉絲) 勒索軟體

最近出現一種新的勒索軟體，名為 Lilith，用 C/C++ 編寫。這種勒索軟體採用雙重勒索攻擊技術，威脅者先竊取敏感性資料並隨後加密檔案。被加密的檔將被附加 .lilith 的副檔名，而隨附的贖金說明檔案的檔名是 "Restore_Your_Files.txt "。

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.Ransomware!g1
- SONAR.Ransomware!g7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Lilith
- Trojan.Gen.MBT
- WS.Malware.1

2022/07/13

AIRAVAT 行動遠端存取木馬 (RAT) 具有勒索軟體功能

AIRAVAT 是一個多功能的行動遠端存取木馬 (RAT) 性質的惡意軟體，已知在地下論壇或最近甚至直接透過 Telegram 頻道銷售。該惡意軟體帶有一個圖形化的網路管理操作介面並允許在被攻擊的裝置上進行各種資訊竊取和鍵盤側錄活動。AIRAVAT 能夠從攻擊者控制的 C&C 伺服器上接收額外的命令，這些命令可能包括典型的勒索軟體活動--加密檔案並透過裝置的通知顯示如何支付贖金的說明。

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

2022/07/13

紛至沓來的 ChromeLoader 惡意軟體行動

ChromeLoader（也被稱為 Choziosi Loader）是一種瀏覽器劫持惡意軟體，它會變更瀏覽器的配置，目的是將使用者的流量重新轉向到廣告網站。該惡意軟體最初在 2022 年 1 月左右出現，在接下來的幾個月裡，它的多個變種已經出現在幾個攻擊行動中。由於 Windows 和 MacOS 平臺都存在不同的變種，該惡意軟體也同樣具有針對 Chrome 或 Safari 瀏覽器的破壞能力。

Chromeloader 的惡意瀏覽器外掛，大多具有廣告軟體的功能，但在某些情況下，它們也具有竊密程式的功能，例如：透過攔截用戶的搜尋引擎查詢並將其轉發到攻擊者的 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：

- Downloader.Chromesten
- OSX.Trojan.Gen
- PUA.Downloader
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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：

- System Infected: Trojan.Backdoor Activity 634
- Web Attack: Malicious Javascript Website 42
- Web Attack: Malicious Website Request 10
- Web Attack: Malicious Website Request 11

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。

2022/07/12

ToddyCat：一個新進的進階持續威脅駭客組織 (APT)

ToddyCat 是一個相對較新的 APT，自 2020 年 12 月以來，攻擊歐洲和亞洲知名的政府和軍事部門。目前還沒有證據顯示 ToddyCat 幕後的威脅者與其他已知的 APT 威脅者有關聯。

ToddyCat 採用 Samurai 後門和 Ninja 木馬，這是兩個精密複雜的網路間諜工具，目的在深入目標網路並保持不被發現的隱匿性。

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

基於安全強化政策(適用於使用DCS)：

Symantec 的 DCS 內建的強化政策即能針對該威脅提供零時差攻擊保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2022/07/12

MikuBot -- 大辣辣地在地下論壇及黑市銷售

在網路黑社會並不缺乏機器人／傀儡／殭屍電腦。賽門鐵克全天候監視全世界的殭屍網路的即時動態，新的殭屍網路在黑市和社交媒體上一夕爆紅的的情況屢見不鮮。這份防護公告介紹了另一個被稱為 MikuBot（以日本動漫人物初音未來命名）的典型機器人，它是 TinyNuke 的變種，目前正在地下論壇和 Telegram 頻道上銷售。必須指出的是，這種惡意軟體也與熱門的 Discord 多用途機器人有相同的名字。在新的廣告出現後不久，賽門鐵克同時觀察到測試階段以及實際網路犯罪有關的行動。截至目前，該殭屍網路背後的威脅者正透過瀏覽網頁時順道下載攻擊作為主要的感染媒介。在其中一項觀察到的活動中，MikuBot 被偽裝成 Vim---一種免費、開放原始碼、基於螢幕的文字編輯器程式--並託管在 Mega 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：

- AGR.Terminate!g2
- SONAR.Heur.Dropper

- SONAR.SuspBeh!gen609

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Tinukebot!gm

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: System Process Suspicious Activity 21
- System Infected: Trojan.Backdoor Activity 634
- Web Attack: Malicious Website Activity 52

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/07/12

Lockbit 勒索軟體以新的 3.0 別名 Lockbit Black 變種重新登臺亮相

2022 年 6 月底左右，惡名昭彰的 Lockbit 勒索軟體一個新的 3.0 變種已經被發佈。這個新版本也被稱為 Lockbit Black，因為其主要程式碼與 BlackMatter／Darkside 勒索軟體變種相似。Lockbit Black 要求在執行時提供一個--pass參數。這又與 BlackCat（又名 Noberus）勒索軟體相似，後者也需要一個特定的存取權杖。Lockbit 3.0 可以刪除一些預先定義的服務並終止某些程序。這個新版本的圖示、桌布和勒索訊息、贖金說明也與前一個版本不一樣。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/07/11

HavanaCrypt 勒索軟體

最近在網路上有一個新的勒索軟體家族在亂竄，名為 HavanaCrypt，它將自己偽裝成一個谷歌軟體更新應用程式。該勒索軟體利用微軟網路託管服務的 IP 位址，作為其命令和控制（C&C）伺服器以逃避檢測，並且還利用 KeePass Password Safe 的優勢來生成加密金鑰。受感染的檔案將被附加上 .Havana 作為其新的副檔名。

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：

- Ransom.Havana
- Trojan.Gen.MBT
- Trojan Horse
- 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已於第一時間收錄於不安全分類列表中。

2022/07/08

OrBit -- 一個新的 Linux 惡意軟體

OrBit 是一個新發現的 Linux 惡意軟體變種，它利用先進的規避技術。OrBit 可以為攻擊者提供對被攻擊主機的遠端存取，但也可以用來獲取用戶的憑證。該惡意軟體能夠感染所有執行中的程序並在受害者的電腦上建立長期立足點。OrBit 的形式是一個植入程式，最初為惡意軟體的執行尋找目標，隨後安裝一個有效籌載二進位檔案。

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：

- Trojan Horse
- WS.Malware.2