保安資訊--本周(台灣時間2022/11/25)
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 99 萬 2,500 台受保護端點上總共阻止了1.271億次攻擊。這些攻擊中有 91% 在感染階段前就被有效阻止：**(2022/11/21)**

- 在**17萬4,400**台端點上，阻止了**5,000**萬次嘗試掃描**Web**服務器的漏洞。
- 在**34萬9,000**台端點上，阻止了**2,640**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬6,900**台**Windows**伺服主機上，阻止了**1,870**萬次攻擊。
- 在**11萬6,100**端點上，阻止了**380**萬次嘗試掃描伺服器漏洞。
- 在**3萬3,300**台端點上，阻止了**160**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬7,300**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**36萬8,300**台端點上，阻止了**880**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬4,300**台端點上，阻止了**540**萬次加密貨幣挖礦攻擊。
- 在**5萬3,800**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,000**台端點上，阻止了**17萬4,300**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。

2022/11/24

人性是資安的最大破口～FIFA世界杯惡意垃圾郵件活動呈上升趨勢

包括 SolarMarker 和 Parrot TDS 在內的不同惡意軟體家族，一直在利用 FIFA 世界杯活動來瞄準用戶，威脅發動者使用 FIFA 遊戲破解版等策略來散佈惡意 PDF，或通知用戶下載重要的瀏覽器更新程式。

研究人員觀察到假冒的串流媒體網站和使用新註冊域名提供世界杯門票的網站有所增加。

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 Horse
- JS.Cryxos!inf
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A!500

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。

- 惡意來源／惡意網路
- 網路釣魚

2022/11/24

留意您使用中的瀏覽器外掛～透過瀏覽器外掛的ViperSoftX竊密程式攻擊行動有所增加

ViperSoftX 竊密程式最初是在 2020 年首次被報導。此後幾乎達到脫胎換骨的蛻變，現在被部署為隱藏在大型系統日誌檔案中的小型 PowerShell 腳本。最近，據報導 ViperSoftX 以瀏覽外掛的形式散佈另一支 VenomSoftX 的竊密程式。ViperSoftX 和 VenonSoftX 都專注於竊取加密貨幣、剪貼板交換和主機指紋識別，以及下載惡意籌載並在受感染的電腦上執行。眾所周知，竊密程式是透過使用破解的軟體透過世界各地的種子 (torrents) 和軟體共享站台進行傳播。

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
- Trojan Horse

2022/11/23

叫得出名字的都有兩把刷子～D0nut 勒索軟體

Donut 是最近嶄露頭角的勒索軟體，在多如過江之鯽的勒索軟體威脅環境中能出名都有兩把刷子。D0nut 的勒索軟體採用雙重勒索戰術。被其加密後，檔案的副檔名會新增為 .D0nut。勒索後的贖金說明包含一張使用 Ascii 編碼的甜甜圈圖片，以及如何使用 Tox 聊天聯繫作者的指南。

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!g12

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

2022/11/23

功力再提升～RobinBot殭屍電腦發動多重DDoS攻擊

RobinBot 是另一個基於惡名昭彰的 Mirai 惡意軟體的殭屍電腦 (機器人)，據報導，它目前正在透過已知漏洞在基於 Linux 的設備上傳播。該惡意軟體的早期版本是用 C 語言撰寫，但最近的版本是用 Java 撰寫。該殭屍網路幕後的攻擊者能夠發起 HTTP 和 OVH Flood 攻擊、針對 Roblox 的 DDoS 攻擊以及來自受感染裝置的基於 Bootstrap 的 DDoS 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE

2022/11/21

傷口撒鹽～Hornet(*大黃蜂)勒索軟體，嘲弄受害者

某些勒索軟體威脅者在勒索贖金說明中可能對他們的受害者相當粗魯，大黃蜂勒索軟體就是其中的代表，大辣辣地稱他的受害者為“白痴”，嘲弄他們笨到允許自己被感染。這個大言不慚的威脅集團一直採用普通的勒索軟體來鎖定消費者和小型企業，被其加密後的檔案將使用隨機的 8 個字元重新命名。沒有採用雙重勒索戰術。

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!gen25
- SONAR.SuspBeh!gen626

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/11/21

Earth Preta(又名Mustang Panda)惡意垃圾郵件活動持續發威

最近，另一項 Mustang Panda（也稱為 Earth Preta）活動被曝光--攻擊者針對包括政府在內的各種組織以及研究和學術機構開展的攻擊行動。據報導，該攻擊行動是由帶有網址 (URL) 的電子郵件帶頭，該 URL 會將用戶重新導到到存放在 Google 雲端硬碟上的惡意檔案套件包，該惡意檔案套件包中，有三個惡意二進位檔案分別為 TONEINS、TONESHELL 和 PUBLOAD。

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：

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/11/21

有效避免小事釀成大禍～防護亮點：Hive勒索軟體踢到賽門鐵克的64位元零時差攻擊防護技術的鐵板

Hive 是一種特別頑強的勒索軟體，首次出現於 2021 年 6 月，並且截至 2022 年 11 月仍然是最流行的勒索軟體之一，據了解迄今為止已經影響了數百個組織。根據最近發布的網路安全通報 (Cybersecurity Advisory，CSA)，全球有 1,300 多名受害者和超過 1 億美元的贖金損失。

已知透過各種方式進入受害者的網路，包括易受攻擊的 RDP 伺服器、遭入侵的 VPN 憑證和網路釣魚電子郵件，一旦入侵網路，它就會部署遠端存取軟體 (例如：AnyDesk 或 ScreenConnect) 以維持網路內的持久性，利用合法的遠端命令執行工具，例如：PSExec、WMI 和 BITSAdmin 等方便發動就地取材攻擊 (LOLBins) 的常用公用／管理程式組合，以在網路中橫向傳播。

雖然 Hive 最早先的版本是用 Goland 撰寫，但後來被移植到 Rust 程式語言，這使得攻擊者可以擴展到 Linux 的作業系統，包括 VMWare ESXi 虛擬機和伺服器。與許多其他勒索軟體家族一樣，Hive 採用雙重勒索戰術，這意味著它不僅在本地加密受害者的檔案，還將它們洩露到遠端存儲位址，並脅迫不支付贖金就將機敏資料公開。

然而，最近新 Hive 變種發現自己踢到**賽門鐵克的 64 位元機器學習技術**的鐵板，並在每個攻擊鏈中無法招架。更明確證據，這是一種 AI 驅動的主動型防禦技術，分析全球的威脅情資庫所包含的上數兆個良好檔案和無效檔案的範例。無需被動式特徵檔技術的更新就能在執行前攔截新惡意軟體變種。

賽門鐵克已經提供有效對應的零時差攻擊保護，詳細說明如下：

基於機器學習的防禦技術：

- Heur.AdvML.B

要詳細了解 Symantec Endpoint Protection 如何使用進階機器學習，請點擊此處。

2022/11/21

不會改變副檔名的加密勒索軟體～AXLocker並具有竊密功能

AXLocker 是一種針對 Windows 環境的全新勒索軟體變種。該勒索軟體利用 AES 演算算法對檔案進行加密，並且加密後不會變更原來的副檔名，因此很難從檔名發現已被加密。該惡意軟體還會收集該台電腦的各種資訊，並將其洩漏上傳到攻擊者的 C&C 命令與控制主機。該惡意軟體還將嘗試竊取 Discord 權杖並將其洩露給威脅攻擊者。

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.MBT
- Trojan.Gen.2
- WS.Malware.1

基於機器學習的防禦技術：

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

2022/11/21

近期在拉丁美洲出現的全新勒索軟體～ARCrypter

ARCrypter 是一種全新的勒索軟體，在撰寫本文時與以前的勒索軟體家族或威脅參與者沒有已知的聯繫。最近在拉丁美洲報告的入侵事件中也看到它的蹤跡。勒索軟體已知會加密檔案並將其副檔名變更為 .crypt 。研究人員發現，該惡意軟體現在也在拉丁美洲以外的地區引起災情。

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

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen678
- SONAR.TCP!gen6

基於機器學習的防禦技術：

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

2022/11/18

HZ遠端存取木馬(RAT)

HZ 是一種遠端存取木馬 (RAT) ，通常嵌入在可自我解壓的 .zip 壓縮檔或附加到惡意垃圾郵件的 .rtf 檔案中散佈。已知使用 .rtf 附件的散佈鏈利用一個相對較舊的在舊版 Office 上用於文件插入及編輯 Equation Editor 編輯器的記憶體毀損漏洞--CVE-2017-11882。HZ 的功能在很大程度上取決於從攻擊者的 C&C 伺服器接收到的命令集。HZ 遠端存取木馬 (RAT) 案例中使用特定互斥值來判斷以防止在同一端點上進行多次安裝。已經發現，相同的互斥值也與一些已知的 Cobalt Strike stager 樣本共享。

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：

- Backdoor.Cobalt!gen9
- Backdoor.Meciv
- Exp.CVE-2017-11882
- 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

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。

2022/11/18

精益求精～LodaRAT遠端存木馬，依舊保持活躍狀態並持續新增功能

LodaRAT 是一種遠端存取木馬，最初於 2020 年被發現。該惡意軟體在 2022 年的許多攻擊行動中仍然搶盡風頭，在這些攻擊行動它要麼經由其他惡意軟體（例如：VenomRAT）植入，要麼與 Redline 竊密程式 或 Neshta 的其他有效籌載一起被散佈。LodaRAT 是用 AutoIt 程式語言所撰寫，最新版本包含搜尋任何插入在電腦上的可攜式儲存裝置並自動將惡意軟體檔案複製到其中的功能。

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(Snoar)的防護：

- SONAR.SuspDataRun
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan Horse
- W32.Neshuta
- 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。

2022/11/17

Linux 作業系統依舊是最令人垂涎的挖礦攻擊目標

雖然加密貨幣市場因多家加密貨幣交易所的倒閉而風雨飄搖，但企業、團體和個人繼續使用知名與不知名的挖礦程式來進行加密貨幣挖礦開採。雖然這些加密貨幣挖礦開採作業大多是合法，但多年來相關的軟體已經被警示為具有被濫用的潛在風險，賽門鐵克長期以來一直對其進行檢測。大多數挖礦活動都是在 Windows 和 Linux 作業系統上觀察到，最近我們在許多 Linux 平台上發現與以往不太一樣的樣貌。

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：

- Miner.XMrig
- Trojan.Gen.NPE