保安資訊--本周(台灣時間2022/04/29)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 1.916 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/04/25)**

- 在**21萬7,500**台端點上，阻止了**9,880萬**次嘗試掃描**Web**服務器的漏洞。
- 在**46萬2,000**台端點上，阻止了**3,820萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬6,000**台**Windows**伺服主機上，阻止了**2,380萬**次攻擊。
- 在**15萬6,600**端點上，阻止了**950萬**次嘗試掃描伺服器漏洞。
- 在**8萬2,000**台端點上，阻止了**400萬**次嘗試掃描在**CMS**漏洞。
- 在**11萬7,900**台端點上，阻止了**340萬**次嘗試利用的應用程式漏洞。
- 在**37萬1,300**台端點上，阻止了**1,030萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,040**台端點上，阻止了**340萬**次加密貨幣挖礦攻擊。
- 在**11萬4,000**台端點上，阻止了**580萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,200**台端點上，阻止了**24萬3,400**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。

2022/04/28

Black Basta (*黑色巴斯塔) 勒索軟體，危害多個機構

據報導，一種名為 Black Basta 的新型勒索軟體變種，最近危害多個機構。Black Basta 幕後的攻擊者採用雙重勒索戰術，在加密之前先竊取機密資料，並威脅不就範就會公開發布該資訊。Black Basta 惡意軟體會加密使用者的檔案，並將加密後的檔案以 .basta 附檔名重新命名，甚至還會顯示自定義的圖示 (icon)。

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.Basta
- Ransom.Basta!gm
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/27

被稱為 Bumblebee (*大黃蜂) 的新惡意軟體

今年3月，一名研究人員發現一個利用名為 Bumblebee 全新惡意軟體的網路釣魚行動。它由一個熟悉的感染鏈組成，其中 ISO 檔會植入一個攜帶 Bumblebee 作為其最終有效籌載的 DLL。散布 Cobalt-Strike 框架似乎也是目標之一。

Bumblebee 使用 Conti 勒索軟體集團中的一個威脅載入器而與此集團有所關聯，並且由於某些方法的相似性，它也與 Trickbot 作者相關聯，但目前這部分仍未得到證實。

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
- Trojan.Gen.2
- Trojan Horse
- Trojan.Trickybot
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/27

Stonefly (*石蠅) 進階威脅 (APT) 集團，繼續瞄準高價值目標

與北韓有關的 Stonefly 駭客集團，繼續對高度專業的工程公司發動間諜攻擊，其目標可能是獲得敏感的智慧財產。最近發現的攻擊是針對一家從事能源和軍事領域工作的工程公司。攻擊者於 2022 年 2 月入侵該組織，最有可能是利用面向公眾 VMware View 伺服器上的 Log4j 漏洞 (CVE-2021-44228) 漏洞。攻擊者使用更新版的 Stonefly 自訂 Preft 後門。除了 Preft 後門，Stonefly 還部署似乎是客製化開發的竊密程式。

在我們的部落格文章中可閱讀更多內容：與北韓有關的間諜行動繼續瞄準高價值目標。

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：

- Backdoor.Prorat
- Hacktool
- ISB.Malscript!gen7
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Seaduke

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

基於機器學習的防禦技術：

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

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: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 3
- Attack: Log4j2 RCE CVE-2021-44228 4
- Attack: Log4j2 RCE CVE-2021-44228 5
- Attack: Log4j2 RCE CVE-2021-44228 6
- Attack: Log4j2 RCE CVE-2021-44228 7

基於安全強化政策(適用於使用DCS)：

賽門鐵克 Data Center Security (DCS) 內建的入侵防禦 (IPS) 系統，能有效防禦 VMWare Horizon 伺服器 Log4Shell 漏洞攻擊並提供零時差保護。也可以防禦 Stonefly 在攻擊過程中的惡意程式植入嘗試。

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。

2022/04/26

Qakbot 殭屍網路攻擊，一波未平，一波又起

由 Qakbot 殭屍網路發送的惡意軟體已經存在很長時間，並且隨著賽門鐵克持續觀察針對全球各種組織反覆出現的垃圾郵件攻擊行動，並沒有停止的跡象。雖然初始的感染媒介沒有改變（基本的惡意電子郵件和線程竊取），但攻擊鏈本身一直在循環，有時還包括新技術。

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.Module!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen128
- Scr.MalMacro!gen3
- Trojan.Gen.NPE.C
- XLM.Downloader!gen1
- XLM.Downloader!gen2
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2022/04/26

DarkWatchman 遠端存取木馬 (RAT) 散布給東歐的預定目標對象

賽門鐵克安全機制應變中心團隊瞭解到，最近有一項源於俄語系國家針對東歐多個部門組織的攻擊行動。該行動偽裝成來自俄羅斯政府聯邦警局的電子郵件通信，試圖將名為 DarkWatchman 遠端存取特洛伊木馬的有效籌載傳遞給預定目標對象。

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

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。

2022/04/26

Serpent (*大毒蛇) 後門瞄準法國的組織

據報導，被稱為 Serpent 後門惡意軟體針對法國政府機構和組織。該惡意軟體透過包含帶有惡意巨集的 MS Word 文件檔之垃圾郵件傳播。在惡意軟體散布階段，攻擊者利用圖像隱碼技術暗助下的隱藏 .jpg 影像檔中之惡意 Powershell 腳本。該後門可能授予攻擊者對受感染系統的存取權限，以進行資料盜竊或派送其他任意有效籌載。

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

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。

2022/04/25

Venom Spider (*毒液蜘蛛)駭客集團散布 More_Eggs (*更多蛋) 惡意軟體

Venom Spider 駭客集團在一項新的惡意行動中重出江湖，散布被稱為 More_eggs 的惡意軟體。散布行動依賴假冒成應徵者的求職申請信的魚叉式網路釣魚電子郵件，目標是美國和加拿大的幾家公司負責招募員工的人資部門。惡意郵件包含 .zip 附件，其中包含惡意.lnk檔。這些 .lnk 檔用於執行感染過程中存在的各種惡意軟體模組。More_eggs 惡意軟體用於收集機密資料、使用者憑證或銀行相關資訊，並將其洩露給攻擊者擁有的遠端伺服器。

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：

- CL.Downloader!gen222
- MSH.Downloader
- Trojan Horse
- Trojan.Gen.NPE

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。

2022/04/25

LemonDuck 殭屍網路以 Docker 實例為目標進行加密挖礦

據報導，LemonDuck 殭屍網路針對暴露在雲端的 Docker 實例進行加密貨幣挖掘。殭屍網路幕後的攻擊者最近在一系列針對 Windows 和 Linux 平臺的行動中利用多個 C&C 伺服器，採用至少五個不同的植入程式變種。在針對 Docker 的攻擊中部署的 LemonDuck 惡意軟體能夠檢測和刪除已知競爭對手的加密採礦殭屍網路的可執行檔，並刪除正在執行中的程序並切斷屬於其他挖礦集團的 C&C 伺服器的網路連線。

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：

- Downloader
- ISB.Downloader!gen76
- ISB.Downloader!gen77
- ISB.Downloader!gen462
- ISB.Heuristic!gen39
- ISB.Heuristic!gen43
- ISB.Lemonduck!gen2
- ISB.Lemonduck!gen7
- Trojan Horse
- Trojan.Gen.NPE

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。

2022/04/22

Prynt Stealer--新發現的竊密軟體，還具有鍵盤側錄功能

一種被稱為 Prynt Stealer 的新型竊密程式和鍵盤側錄軟體，被發現在各種地下論壇上進行廣告銷售。Prynt Stealer 具有從各種瀏覽器（包括 MS Edge、Chromium 和 Firefox 的瀏覽器）竊取各種資訊的功能。該惡意軟體針對自動填入的資訊、登錄憑證和 cookie 等。除了針對網頁瀏覽器外，Prynt 還可以從多個訊息應用程式（例如：Discord 或 Telegram、FTP 或 VPN 應用程式和加密錢包）中竊取資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/22

BlackCat (也稱為 Noberus) 勒索軟體正在危害全球各地的組織

賽門鐵克安全機制應變中心團隊瞭解到，近期聯邦調查局發出關於被稱為 BlackCat (也稱為Noberus) 的勒索軟體，正在危害全球各地組織的警戒報告。BlackCat 是一種勒索軟體即服務 (RaaS) 惡意軟體，它既可以加密用戶的檔案，又可以在加密之前竊取機密資訊。已知攻擊者利用 PowerShell 和批次處理腳本進行初始勒索軟體部署，並進一步破壞目標網路中的其他主機。

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.Module!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gen9
- Hacktool
- Hacktool.Gen
- Hacktool.Mimikatz
- Ransom.Noberus
- Ransom.Noberus!gen1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE

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.Gen Activity 43

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。

2022/04/22

假的MetaMask--加密貨幣錢包 Apps， 鎖定行動裝置用戶

根據最近一份報告，假的 MetaMask 行動應用程式APP，正在透過一系列模仿真實網頁的網路釣魚網站進行散布。MetaMask 是一個允許用戶與以太坊區塊鏈互動的加密貨幣錢包。假的行動應用程式 APP 幕後的威脅組織，試圖入侵受害者 Metamask 帳戶並從錢包中竊取加密貨幣。

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.2

2022/04/21

Nokoyawa 和 Karma 勒索軟體的相似之處

早在 3 月份就認為 Nokoyawa 可能與 Hive 有聯繫，因為他們的攻擊鏈中有一些相似之處，但經過進一步調查，似乎 Nokoyawa 實際上是一種進化的 Karma (Nemty) 勒索軟體。Nokoyawa 和 Karma 在結構和程式碼有一些相似之處，但 Nokoyama 仍然不是一個完整的副本，因為 Nokoyawa 的勒索說明信中缺少洋蔥洩漏頁面，這與 Karma 提供的內容形成鮮明對比。這可能是刻意隱瞞攻擊者的行為，以混淆歸屬。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Gen
- Ransom.Karma!gen1
- Ransom.Karma!gm1
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B