保安資訊--本周(台灣時間2022/07/22)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 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：**(2022/07/17)**

- 在**19萬6,600**台端點上，阻止了**8,140萬**次嘗試掃描**Web**服務器的漏洞。
- 在**38萬5,400**台端點上，阻止了**3,560萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬3,600**台**Windows**伺服主機上，阻止了**2,070萬**次攻擊。
- 在**13萬5,300**端點上，阻止了**790萬**次嘗試掃描伺服器漏洞。
- 在**6萬8,700**台端點上，阻止了**330萬**次嘗試掃描在**CMS**漏洞。
- 在**10萬2,900**台端點上，阻止了**310萬**次嘗試利用的應用程式漏洞。
- 在**30萬3,800**台端點上，阻止了**800萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬100**台端點上，阻止了**430萬**次加密貨幣挖礦攻擊。
- 在**42萬8,000**台端點上，阻止了**640萬**次向惡意軟體**C&C**連線的嘗試。
- 在**5,800**台端點上，阻止了**20萬7,100**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。

2022/07/21

Amadey 機器人／殭屍電腦 (BOT) 在 SmokeLoader 惡意軟體的掩護下傳播

一個傳播 Amadey 機器人／殭屍電腦 (BOT) 的新行動已經被發現。根據最近一份報告，該殭屍網路的二進位檔案是在 SmokeLoader 惡意軟體的掩護下安裝，並被偽裝成破解版軟體或軟體啟動序號產生器程式。Amadey 主要被攻擊者用來從被入侵的主機中竊取機密資訊，但它也可以下載和安裝額外的有效籌載。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.RGC!g542
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Amadey
- Trojan.Amadey!g1
- Trojan Horse
- Trojan.Gen.2
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/07/20

CloudMensis -- 一個針對 macOS 的新惡意軟體

一個被稱為 CloudMensis 的新 macOS 後門已在真實網路世界亂竄。該惡意軟體利用公有雲端儲存空間進行 C&C 通信--這包括 Dropbox、pCloud 和 Yandex Disk 服務。CloudMensis 惡意軟體被攻擊者用來竊取各種敏感的使用者資料，包括文件檔案、螢幕截圖、電子郵件資訊和鍵盤紀錄。CloudMensis 還具有繞過 macOS 的 Transparency Consent and Control（TCC）保護機制的能力，這是一個控制應用程式存取某些作業系統功能的 macOS 機制。

～所謂 TCC 是蘋果於 2012 年 macOS Mountain Lion 加入的防護子系統，它維護儲存用戶明顯同意的 App 清單或資料庫。任何 macOS App 若不在 TCC 清單中，就會被拒絕存取用戶敏感資訊。TCC 目的在讓用戶設定 App 隱私，包括 App 是否能存取電腦攝影機、麥克風或定位資訊、行事曆或 iCloud 帳號等。而為保護 TCC，macOS 還加入禁止非授權程式碼執行的功能，並強制執行一項政策，僅允許具有全磁碟存取權限的 App 可以存取 TCC。～節錄自 iThome

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：

- OSX.Trojan.Gen
- WS.Malware.1

2022/07/20

LockBit 威脅行動利用群組原則進行網路傳播

賽門鐵克最近觀察到威脅者將伺服主機作為目標，以便在被入侵的網路中傳播 LockBit 勒索軟體威脅。在特定的攻擊中，收集網域相關資訊後，LockBit 利用群組原則更新，向連線至網域的電腦強行派送惡意軟體。

在我們的部落格文章中可閱讀更多內容：LockBit：專門鎖定伺服主機的勒索軟體。

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.RansomLckbit!g1
- SONAR.RansomLckbit!g3
- SONAR.RansomNokibi!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.LockBit
- Ransom.LockBit!g2
- Ransom.Lockbit!gen3
- Ransom.Lockbit!gm1
- Scr.Malscript!gen1

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：

- Attack: Lockbit Ransomware Binary Copy GPO Config
- Attack: Lockbit Ransomware Enable Share GPO Config
- Attack: Lockbit Ransomware Security Services Taskkill GPO
- Attack: Lockbit Ransomware Services Disable GPO Config

基於安全強化政策(適用於使用DCS)：

賽門鐵克 DCS 的安全強化政策可針對 Windows 伺服器和網域控制器防止 Lockbit 勒索軟體的安裝。預設 DCS 鎖定政策可以防止 Lockbit 勒索軟體在網路上的橫向移動，並保護伺服器免受 Lockbit 執行企圖篡改群組原則和關鍵系統資源。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。

2022/07/19

AsyncRAT 和 LimeRAT 木馬二人組被用於攻擊政府組織

據報導，至少從 2021 年開始，一個利用 AsyncRAT 和 LimeRAT 遠端存取木馬的惡意行動被用來攻擊印度、義大利、波蘭和美國的政府組織。攻擊鏈包含惡意電子郵件，其中包含直接作為附件的惡意 MS Excel 檔案或其 URL 網頁連結。這些檔案一旦被開啟，就會執行嵌入的惡意巨集，進而導致感染上述木馬。攻擊者可以利用 AsyncRAT 和 LimeRAT 竊取使用者的憑證、鍵盤點擊側錄或將受感染的系統被殭屍網路所操控成為殭屍電腦。

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.MSOffice!g23

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1

基於機器學習的防禦技術：

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

2022/07/18

Oski (*奧斯基) 冒充 Avast 防毒軟體安裝程式

Oski 竊密程式繼續在威脅領域中作怪。這種普通的竊密程式被多個團體和個人使用，主要透過瀏覽網頁時的順道下載 (drive-by-download) 來傳播，也有一些是透過惡意郵件行動。該惡意軟體仍由其作者維護中，我們經常看到新版本。最近，賽門鐵克觀察到一個順道下載行動，其中惡意的 Oski 被偽裝成 Avast 防毒軟體安裝程式。

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

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: Vidar Malware Activity 2

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。

2022/07/18

發現 WatchDog (*看門狗) 駭客集團使用圖像隱碼術 (Steganography) 來傳遞惡意軟體

據觀察，WatchDog 駭客集團使用圖像隱碼術來傳遞惡意軟體的有效籌載。影像檔包含嵌入的惡意軟體，以 IEND 為標頭並以標誌檔結尾，這樣可以允許腳本直接呼叫惡意軟體。有效籌載透過 Redis 傳播、大量掃描和安裝 XMRig 加密貨幣挖礦程式。據瞭解，WatchDog 鎖定中國的網路，因使用被入侵的阿里巴巴雲端儲存空間 (Bucket) 和程式碼中有中文註解所以有這種猜測。

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

2022/07/15

Vertex (*頂點) 竊密程式鎖定歌手及製作人

Vertex (*頂點) 是一種普通的竊密程式，至少從2021年就開始出現，雖然它在威脅領域並不特別顯眼，但賽門鐵克確實看到反覆出現的實例。這種惡意軟體被多個團體和個人使用，他們喜歡透過瀏覽網頁時的順道下載 (drive-by-download) 攻擊作為感染的媒介。最近，有一個威脅者將惡意二進位檔案偽裝成 FL Studio--一種數位音樂工作站軟體，被許多知名的嘻哈和電音舞曲音樂 (EDM) 製作人使用，以此來攻擊音樂藝術家。

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

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