保安資訊--本周(台灣時間2023/06/23)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 75 萬 6,100 台受保護端點上總共阻止了 9,390 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/06/18)**

- 在**14萬8,100**台端點上，阻止了**4,140**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬2,500**台端點上，阻止了**1,940**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬4,000**台**Windows**伺服主機上，阻止了**1,350**萬次攻擊。
- 在**8萬1,700**台端點上，阻止了**250**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,200**台端點上，阻止了**81萬5,600**次嘗試掃描在**CMS**漏洞。
- 在**6萬2,200**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**24萬6,000**台端點上，阻止了**610**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,000**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**18萬3,100**台端點上，阻止了**990**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**9萬4,000**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。

2023/06/22

RedEnergy(*紅能)--竊密型勒索軟體

報導指出一種名為 RedEnergy 新型勒索軟體，透過搜尋引擎最佳化中毒 (SEO Poisoning) 手法和偽裝成瀏覽器更新的惡意電子郵件進行傳播。RedEnergy 能夠擷取敏感資料，包括密碼、信用卡號和檔案。此外還具有勒索軟體功能，被加密後的檔案會被冠上 .FACKOFF！副檔名。歹徒採用此兼具竊密與加密勒索功能的惡意程式，使其更容易發動雙重勒索手段或從被盜資料中獲利。

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(SONAR)的防護：

- AGR.Terminate!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2023/06/21

DcRAT遠端存取木馬偽裝成搶眼的OnlyFans情色平台內容

Onlyfans (OF) 是全球知名的情色平台，又被稱為成人版 Instagram。隨著 OnlyFans 受歡迎程度持續上升，吸引不斷尋找趨勢並利用社交工程伎倆加以利用的各種駭客團體和個人的注意力。據報導，為了滿足被害者好奇心，歹徒一直試圖透過以著名女優為主角的免費 OnlyFans 內容來引誘受害者，並使用順道下載作為感染媒介。如果受害者在下載的存檔中執行惡意 VBS 腳本，他們實際上最終會感染名為 DcRAT 的遠端存取木馬。目前，這種威脅正在透過惡意垃圾郵件和偷渡式下載行動在全球大規模傳播。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g284

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/06/21

Flea駭客組織利用Graphican全新後門程式，攻擊美洲國家外交部

Flea（又名 APT15、Nickel）進階持續威脅 (APT) 組織在最近一次從 2022 年底到 2023 年初的攻擊活動中繼續關注美洲國家外交部，其中利用一個名為 Backdoor.Graphican 的全新後門。博通旗下賽門鐵克的威脅追踪團隊觀察到此次行動主要焦點似乎是美洲外交部。

Flea 在這次行動中使用大量的工具。除了新的 Graphican 後門之外，攻擊者還利用各種就地取材攻擊的工具，以及之前與 Flea 相關的工具。

在我們的部落格文章有更詳細內容，歡迎參考：Graphican：Flea 利用新的後門攻擊外交部門

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.Graphican
- Backdoor.Hadmad
- Backdoor.Ketrican
- HackTool.LaZagne!gen1
- Hacktool
- Hacktool.Mimikatz
- Hacktool.Safetykatz
- PHP.Backdoor.Trojan
- Pwdump
- Trojan.Gen
- Trojan.Gen.NPE

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g1
- SONAR.TCP!gen1
- SONAR.TCP!gen6

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。

2023/06/21

Condi殭屍網路：透過TP-Link路由器的公開漏洞發動DDoS攻擊

Condi 是一個分散式阻斷服務 (DDoS) 即服務的殭屍網路，其用戶可以直接購買代碼或租用殭屍網路來發動 DDoS 攻擊。該殭屍網路本身最近透過濫用 TP-Link 路由器系列上已公布的漏洞 (CVE-2023-1389) 進行傳播。該漏洞的修補程式已經正是釋出，因此 Condi 背後的組織只是利用那些尚未修補且可透過網際網路存取的路由器。

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：

- Linux.Mirai
- Trojan.Gen.NPE
- WS.Malware.1

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: TP-Link Router Remote Code Execution Vulnerability CVE-2023-1389

2023/06/19

防護亮點：星際檔案系統(IPFS)網路釣魚行動呈上升趨勢

~ 防護亮點 ~

IPFS 是星際檔案系統 (InterPlanetary File System) 的縮寫，是一個分散式點對點超媒體傳輸協議，目的是要建立分散式共用檔案的網路協定。IPFS 不像基於位置的集中式系統那樣使用檔案路徑，而是使用基於檔案的雜奏 (hash) 值產生的唯一內容辨識碼 (content identifier，CID)，檔案分散在與 IPFS 共享用戶的電腦上。以這種方式共享的檔案是直接從該電腦下載，因此稱為“分散式”。IPFS 有效地取代慣用的 HTTP 和 HTTPS 協定（超文字傳輸通訊協定／超文字傳輸安全通訊協定）作為瀏覽全球資訊網的不同方式。

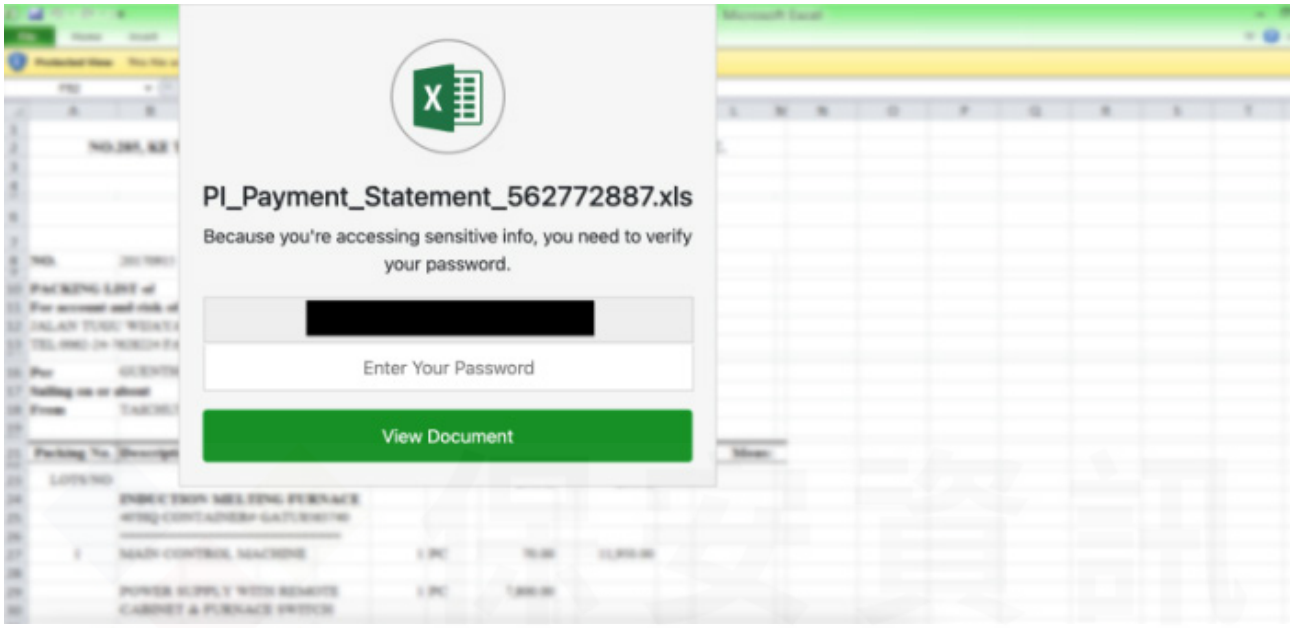
IPFS 網路釣魚攻擊與傳統透過集中式網路進行的網路釣魚攻擊相似，攻擊者使用社交工程伎倆、電子郵件和訊息發送平台以及虛假網站來冒充合法品牌，以竊取您的憑證和／或獲取網路存取權限。使用唯一 IPFS 位址，任何人都可以存取在 IPFS 網路上發布的內容，然後他們可以在自己的節點上重新發布它，進而使攻擊者可以輕鬆建立永久且無法追踪的網路釣魚站台，即使在原始站台被下線後這些站台仍保持活動狀態。

為了便於攻擊，歹徒可能會採用以下方法之一：

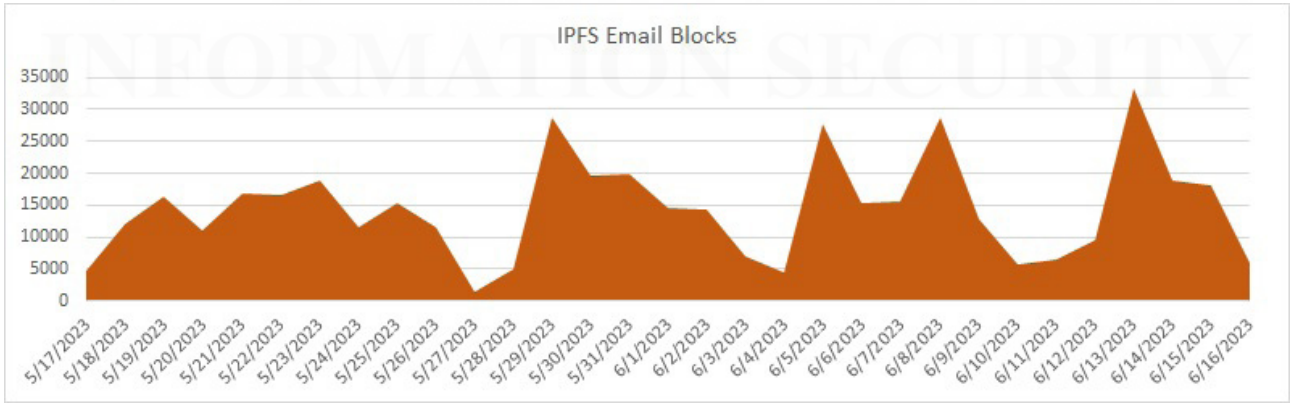
- 惡意網址：釣魚簡訊、電子郵件、直接互相傳訊、彈跳視窗或其他誘騙用戶點擊指向惡意 IPFS 網址的鏈接方式。

- DNS (網域名稱系統) 欺騙：建立一個虛假的 DNS 伺服主機，重定向到上架在虛假網站的惡意 IPFS 網址。
- SSL（安全通訊協定）證書：偽造的 SSL 證書使用戶相信他們正在瀏覽合法站點。

這是一個看起來像 excel 文件的網路釣魚頁面範例，提示用戶輸入密碼才能開啟它。



IPFS 與集中式檔案共享相比具有多項優勢，但多年來它也已成為網路犯罪分子的一個有吸引力的平台。賽門鐵克每月觀察到數以萬計的 IPFS 網路釣魚電子郵件。



賽門鐵克攔截到 IPFS 網路釣魚郵件

另外，在過去 30 天裡，賽門鐵克的網路安全服務標記數千個唯一內容辨識碼 (CID) 子域，包括 11,789 個唯一主機、19,071 個唯一完整 URL 和 55,164 個 CID 路徑。

賽門鐵克針對 IPFS 攻擊提供完整的零時差保護，具體說明如下：

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)。

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。

更詳細資訊有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
更詳細資訊有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請單擊此處。

2023/06/18

Big Head(*大頭)勒索軟體

有報導指出一種名為 Big Head 的全新勒索軟體已經出現。與其他勒索軟體（Sorry、Qinynore、ScorpionLocker 等）一樣，這個勒索軟體似乎是使用開放原始碼專案：Hidden Tear 所開發。在執行時，觀察到 Big Head 透過顯示虛假的 Windows 更新畫面來隱瞞用戶，同時在背景加密用戶的檔案，然後是置放贖金支付通知。攻擊者要求受害者透過電子郵件或 Telegram 頻道與他們聯繫。

在我們持續監控和加強針對該勒索軟體家族保護的同時，我們建議定期備份任何重要檔案，並套用最新的產品定義來抵禦勒索軟體威脅。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransom!gen25
- SONAR.SuspBeh!gen6
- SONAR.SuspBeh!gen625
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1
- Ransom.Sorry
- Scr.Malcode!gdn14
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/06/16

全新安卓平台上：GravityRAT惡意軟體

在真實網路情境發現一個被稱為 GravityRAT 的全新安卓手機惡意軟體。該惡意軟體藉由一支被植入木馬被稱作 BingeChat 的安全即時通訊 APP 來擴散傳播 (採用 XMPP 加密協定的 OMEMO 擴充程式)。在過去的攻擊行動中，GravityRAT 已經被偽裝成類似的訊息 APP，例如：Chatico。此類型的惡意 APP 通常不在 GooglePlay 上架，而是透過標榜免費解決方案的惡意下載網站散播。全新 GravityRAT 還增加刪除受感染裝置上檔案的功能，以及蒐集 WhatsApp 備份檔案的能力。

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

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。