保安資訊--本周(台灣時間2023/04/28)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 6,500 台受保護端點上總共阻止了 8,920 萬次攻擊。這些攻擊中有 91% 在感染階段前就被有效阻止：**(2023/04/24)**

- 在**14萬9,800**台端點上，阻止了**3,710**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**1,810**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬3,400**台**Windows**伺服主機上，阻止了**1,390**萬次攻擊。
- 在**8萬800**台端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,600**台端點上，阻止了**99萬6,400**次嘗試掃描在**CMS**漏洞。
- 在**6萬1,700**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**25萬9,200**台端點上，阻止了**470**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬4,800**台端點上，阻止了**250**萬次加密貨幣挖礦攻擊。
- 在**15萬2,000**台端點上，阻止了**1,130**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,400**台端點上，阻止了**10萬1,300**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。

2023/04/27

神不知、鬼不覺～LOBSHOT惡意軟體內建HVNC(隱藏虛擬網路連線)模組

LOBSHOT 是一種新發現的惡意軟體，具有竊密程式和銀行木馬的功能。該惡意軟體透過濫用 Google Ads 平台傳播，並偽裝成合法軟體安裝程式。LOBSHOT 包括一個 HVNC（隱藏虛擬網路連線）模組，可讓攻擊者在遭駭電腦上建立隱藏的桌面，進而為他們提供直接和不被發現的遠端操作。

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.SuspBeh!gen633

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- 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.B!100

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：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22

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。

2023/04/27

Educated Manticore進階持續威脅(APT)駭客組織部署PowerLess注入程式新變種

根據觀察，Educated Manticore 駭客組織已經發動對以色列境內的新一波攻擊。據信該進階持續威脅 (APT) 駭客組織與另一個名為 APT35（又名 Charming Kitten 或 Phosphorus）的 APT 駭客組織有密切關聯。在初始攻擊階段，攻擊者一直在利用夾帶 ISO 檔的網路釣魚郵件。最新攻擊行動中最終有效籌載是 PowerLess 注入程式的最新變種。之前在 APT35 駭客集團所發起攻擊中發現相同的惡意軟體家族。PowerLess 具有鍵盤側錄程式或竊密程式的功能，可以從系統瀏覽器收集資料或下載其他惡意模組。

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.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Gen
- Trojan Horse
- Trojan.Gen.NPE.C
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/04/26

駭客集團同時搭配PingPull 和Sword2033惡意軟體以攻擊Linux系統

在真實網路上觀察到一種被命名為 Alloy Taurus（又名 GALLIUM）的 APT (進階持續威脅)駭客集團新活動。已知該駭客集團以歐洲、非洲和東南亞許多國家的電信、政府和金融行業為攻擊目標。在這次最新的行動中，攻擊者一直在利用 PingPull 惡意軟體的新變種以及另一個名為 Sword2033 的後門。PingPull 惡意軟體具有對檔案和資料夾的讀／寫／刪除的能力、也可以執行指令等，而 Sword2033 是一個相對基本的後門程式，允許檔案上傳／下載和執行指令。

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.Trojan
- 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。

2023/04/26

Tomiris駭客組織使用各種惡意軟體工具

我們過去曾討論過 Tomiris 駭客組織自己的工具，在最近的攻擊行動顯示，該駭客組織在他們的網站上使用各種工具及技術（Rust、Python、Golang 等）和不同的攻擊方式（DNS 劫持、Telegram 中的 C&C）的攻擊行動。不變是他們鎖定的目標還是在獨立國協 (CIS)。與該駭客組織有關的一些工具是 Topinambour、JLORAT、Tunnus、Roopy、Telemiris。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Burtopinam
- WS.Malware.*

基於機器學習的防禦技術：

- Heur.AdvML,*

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 654
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 564
- Web Attack: Webpulse Bad Reputation Domain Request

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。

2023/04/26

不會更改檔名的勒索軟體：Uniza

Uniza 是眾多威脅型態中觀察到的另一種普通勒索軟體。該惡意軟體會加密用戶檔案，但不會修改任何檔名或將任何特定副檔名新增到被加密檔。該惡意軟體在彈出的命令列視窗中顯示勒索贖金說明，並要求以比特幣 (BTC) 支付贖金。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/04/25

RokRAT惡意軟體透過ISO影像檔和LNK捷徑檔傳播

最近在真實網路環境發現一種利用 ISO 影像檔和 LNK 捷徑檔，來傳播 RokRAT 惡意軟體的全新攻擊行動。當攻擊鏈被觸發後植入的 LNK 捷徑檔，會再呼叫惡意 Powershell 腳本，後續程序包含透過 Google One drive 的 API 下載有效籌載。RokRAT 是一種惡意遠端存取木馬，被普遍認為是出於 APT37（又名 ScarCruft）駭客組織，並且已知濫用各種公有雲端硬碟以協作 C&C 目的。該惡意軟體的功能允許攻擊者從遭駭入電腦收集資料、鍵盤側錄和下載／執行其他任意檔案。

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
- Trojan.Gen.2
- Trojan.Gen.NPE.C
- WS.Malware.1

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：

- System Infected: Trojan.Backdoor Activity 634

2023/04/25

CryptNet以勒索軟體即服務(RaaS)助長網路犯罪

CryptNet 是一種全新的 RaaS（勒索軟體即服務）勒索軟體，於本月出現在威脅領域。該惡意軟體使用 .NET 撰寫，使用 AES 算法進行加密，並具有停用備份服務和刪除卷影副本的功能。成功加密後，CryptNet 會將被加密的檔案新增隨機的副檔名，並以 .txt 文字檔的形式存放贖金支付說明，並變更受感染電腦上的佈景主題 (桌布)。該勒索軟體背後的攻擊者，還建立一個資料竊取網站，他們會在該網站上公布受害者的詳細資訊。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/04/24

防護亮點：SEP提供行動裝置的中間人(MITM)攻擊防護

～防護亮點～

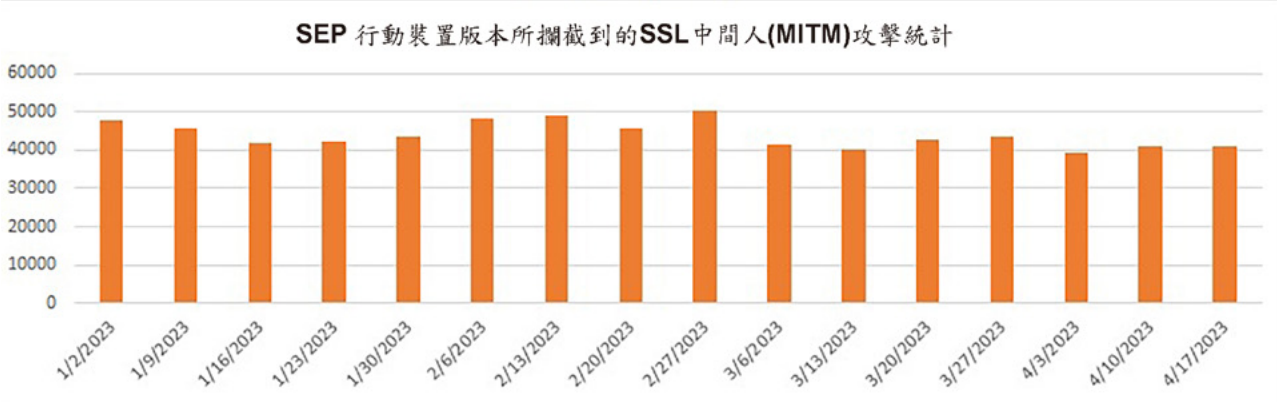
中間人 (MITM) 攻擊是近期熱門的網路攻擊模式之一，通訊雙方之間的通訊被攔截並可能被竄改，同時使其看起來好像正在進行正常的訊息交換。MITM 攻擊通常主要在竊取資訊，但也可能有其他意圖，例如：監視受害者、破壞通訊或破壞資料。

隨著越來越多的人使用行動裝置進行銀行、購物和存取敏感資料等線上活動，行動裝置上的 SSL MITM 攻擊變得越來越猖獗。公共 Wi-Fi 網路的廣泛使用更是助長這些攻擊，這些網路通常不安全且容易被攔截，駭客經常利用未經修補被廣泛運用於保護傳輸安全的 SSL／TLS 網路加密協議進行攻擊。

簡而言之，行動裝置上的 SSL 中間人 (MITM) 攻擊的工作原理如下：

* 攻擊者設置一個假的 Wi-Fi 熱點或一個惡意模仿合法熱點的熱點
* 受害者連接到假熱點並開始瀏覽網際網路或存取線上服務
* 當受害者存取安全網站時，攻擊者攔截 SSL／TLS 流量並與受害者行動裝置建立假的 SSL／TLS 連接
* 攻擊者充當受害者設備和伺服器之間的代理，攔截和解密加密流量
* 攻擊者現在可以讀取和修改受害者裝置和伺服器之間的流量
* 攻擊者可以竊取敏感訊息，例如登錄憑證、信用卡號或個人資料
* 攻擊者可以竄改流量並將惡意程式碼或惡意軟體注入通訊流，進一步駭入受害者的裝置

下圖顯示今年以來 SEP 行動裝置版本所攔截到 SSL 中間人 (MITM) 攻擊的走勢。



SEP 行動裝置版本透過以下防護技術有效防護中間人(MITM)攻擊：

- 主動蜜罐誘捕技術徹底分析端到端的網路連接以確保通訊安全
- 當 SEP 行動裝置版本檢測到 MITM 網路攻擊時，會同時發生兩件事：
  - 我們的自動網路保護回應啟動，包括從行動裝置透過安全的 VPN 連線或阻止行動裝置存取敏感的公司資源（電子郵件、營運類應用程式）等機制
  - 資安管理員和終端使用者都會收到有關威脅的警報，警報包括攻擊中涉及的證書和網路事件的詳細資訊

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版 (SESC)內 含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

2023/04/24

Decoy Dog惡意軟體工具套件包

Decoy Dog 是一種新發現的惡意軟體工具套件包，攻擊者使用它來逃避安全軟體偵測。據報導，Decoy Dog 背後的攻擊者使用 domain aging 或 DNS 查詢混淆等伎倆，以便在後續進行惡意操作之前建立良好的網域信譽。與 Decoy Dog 相關的基礎設施顯示使用稱為 Pupy RAT 的遠端存取木馬連接。Pupy 是一種開放原始碼的後脅迫 (Post-Exploitation) 工具，允許攻擊者遠端控制、執行指令和竊取憑證等。

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.NPE
- WS.Malware.1

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。

2023/04/24

EvilExtractor惡意軟體

EvilExtractor 是一個模組化攻擊工具套件包，最初於 2022 年發布，目前針對 Windows 的系統仍在網路上銷售。EvilExtractor 在最近的網路釣魚行動中被發現偽裝成 PDF 或 Dropbox 檔案來進行傳播。該惡意軟體目的主要是竊取資料／文件檔並側錄遭駭電腦上的鍵擊。EvilExtractor 還有一個勒索軟體模組（稱為 Kodex Ransomware），它濫用 7-Zip 應用程序以建立受密碼保護的壓縮檔，其中包含在遭駭電腦上收集的受害者檔案。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Powershell!g20
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

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

2023/04/21

AuKill--型態惡意後門程式具有安全軟體規避的能力

發現被命名為 AuKill 的新型態惡意後門程式具有安全軟體規避的能力。根據研究人員的說法，該工具是源於開放原始碼工具 Backstab 的修改版本，專門針對 EDR 用戶端。

Backstab 是一種能夠透過經由 Microsoft 簽章的舊版 Sysinternal Process Explorer 驅動程式來停用防毒軟體的程序工具。

自 2021 年 6 月中旬首次發布以來，該工具已被各種勒索軟體攻擊者積極使用。

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.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Rootkit
- Trojan.Gen.MBT
- Trojan Horse
- Trojan.KillAV
- 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.B!100

2023/04/21

X_Trader供應鏈攻擊

在最近一份報告發現，被植入木馬的 X_Trader 軟體是 3CX 遭駭的原因。更進一步調查發現，與 3CX 相比，受 X_Trader 軟體供應鏈攻擊影響的組織更多。迄今為止，賽門鐵克威脅獵手團隊的一項調查發現，受害者中有兩家能源產業的關鍵基礎設施組織，一家在美國，另一家在歐洲。除此之外，另外兩個金融交易相關的組織也遭到入侵。

在我們的部落格文章中有更多資訊可供參考：嚴重影響美國和歐洲關鍵基礎設施的X_Trader供應鏈攻擊

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- FastReverseProxy
- Packed.Generic.553
- Trojan Horse
- Trojan.Dropper
- Trojan.Samsis

基於機器學習的防禦技術：

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