保安資訊--本周(台灣時間2022/07/01)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1.811億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/06/27)**

- 在**21萬600**台端點上，阻止了**8,590萬**次嘗試掃描**Web**服務器的漏洞。
- 在**41萬7,100**台端點上，阻止了**4,020萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬6,500**台**Windows**伺服主機上，阻止了**2,000萬**次攻擊。
- 在**14萬4,200**端點上，阻止了**800萬**次嘗試掃描伺服器漏洞。
- 在**7萬1,100**台端點上，阻止了**340萬**次嘗試掃描在**CMS**漏洞。
- 在**10萬9,100**台端點上，阻止了**310萬**次嘗試利用的應用程式漏洞。
- 在**31萬3,300**台端點上，阻止了**790萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9萬5,000**台端點上，阻止了**370萬**次加密貨幣挖礦攻擊。
- 在**10萬700**台端點上，阻止了**600萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,100**台端點上，阻止了**26萬6,200**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。

2022/06/30

SessionManager IIS 後門

SessionManager IIS 後門已被用於針對世界各地的政府、軍事和工業實體的各種 2022 年攻擊行動中。根據最近一份報告，SessionManager 已被部署到上述部門 20 多個不同組織。由於使用另一個被稱為 OwlProxy 的惡意軟體變種，利用 SessionManager 的攻擊被歸結為名為 Gelsemium 威脅集團。SessionManager 後門的作用是在被入侵主機上執行任意的二進位檔案，以及存取並操弄其他被入侵的內部網路端點。

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.Owprox
- Trojan.Owprox!gen1
- WS.Malware.1

2022/06/30

GlowSand -- 針對烏克蘭發動的惡意行動

根據最近的一份報告，在真實網路環境觀察到多起針對烏克蘭組織的新威脅活動。被稱為 GlowSand 的攻擊行動，利用夾雜許多類型的附件中偽裝成薪資資料的惡意MS Office XML檔案。惡意軟體有效籌載從遠端伺服器分發，並設定為只允許從烏克蘭 IP 位址才能下載。這些攻擊的目的似乎是要在被入侵的網路上建立一個立足點，收集資訊並下載更多的有效籌載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen203
- ISB.Downloader!gen53
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Mdropper
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/06/29

ZuoRAT 遠端存取木馬劫持 SOHO (小型的家庭辦公室) 路由器

自 2020 年以來，一個被稱為 ZuoRAT 的極隱蔽遠端存取木馬 (RAT) 一直在入侵 SOHO 的路由器。

由於近年來的疫情大爆發，居家辦公的比例非常高，也為威脅者提供一個利用 SOHO 路由器的漏洞機會，因為 SOHO 不像企業網路能獲得系統管理員的嚴格管控。

在這次行動中展示的能力，包括取得對不同品牌和型號 SOHO 設備的操弄權限、收集主機和區域網路資訊以協助確定目標、採樣和劫持網路通信以獲得對內部設備的潛在持續存取，以及利用許多散布各地的路由器建構相互通信的隱秘 C&C 基礎設施。

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.ProcHijack!g43
- SONAR.ProcHijack!g45
- SONAR.ProcHijack!g47
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm5
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.2

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 235
- System Infected: Trojan.Backdoor Activity 612
- Web Attack: Webpulse Bad Reputation Domain Request(29565)

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。

2022/06/29

發現新的變種 AstraLocker 勒索軟體在網路上亂竄

AstraLocker 2.0 變種已在真實網路上被發現。該惡意軟體主要是透過濫用惡意 MS Word 文件的惡意垃圾郵件行動來傳播。據報導，新的變種 AstraLocker 主要是基於 2021 年被洩露給公眾的 Babuk 勒索軟體程式碼。AstraLocker 採用幾種規避策略，並對虛擬環境是否存在進行各種檢查。該勒索軟體對使用者檔案進行加密，並對其附加多種不同的副檔名，例如：.babuk、.astralocker 或 .astra。

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.Babuk
- Trojan Horse
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/06/29

Revive -- Android (*安卓) 平台上的網路銀行惡意軟體

最近被曝光的 Revive 是一個普通安卓平台上的網路銀行惡意軟體，具有間諜軟體功能。據報導，這個威脅的程式碼顯示與 TearDroid 相似，其原始程式碼已向公眾開放。能夠收集憑證和攔截簡訊，使威脅者能夠接管受害者的金融帳戶。

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

2022/06/28

RecordStealer (*記錄竊取程式)--新型竊密程式透過破解版軟體的掩飾來傳播

被稱為 RecordStealer 新型竊密惡意軟體已在網路上到處亂竄。該惡意軟體將自己偽裝成軟體破解包或軟體安裝程式。RecordStealer 的目標是儲存在瀏覽器、cookies、加密貨幣錢包、已儲存的憑證等機敏資料。據報導，RecordStealer 所使用一些 C&C 通信伺服器也與另一個被稱為 Clipbanker 竊密惡意軟體共用。

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：

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。

2022/06/28

Bumblebee (*大黃蜂) 載入程式在威脅領域日益嶄露頭角

Bumblebee (*大黃蜂) 是最近開發的惡意軟體載入程式，已經迅速成為各種網路犯罪攻擊中的關鍵元件，並似乎已經取代一些過時的載入程式，這表明它已被既有威脅者所採用，並是預先有計畫地轉移到 Bumblebee。透過對分析最近涉及 Bumblebee 攻擊中使用的其他三個工具，賽門鐵克的威脅獵手團隊 (隸屬於博通軟體的企業安全部門) 已經將這個工具與一些勒索軟體的幕後集團產生關聯，包括 Conti、Quantum 和 Mountlocker。在這些較早的攻擊中使用的攻擊手法、技術與過程 (TTPs) 支持這樣假設：Bumblebee 可能是作為 Trickbot 和 BazarLoader 的替代載入程式推出，因為最近涉及 Bumblebee 活動和與這些載入程式有關的較早攻擊之間存在一些重疊之處。

在我們的部落格文章中有更多資訊可供參考：Bumblebee (*大黃蜂)：新的載入程式迅速成為網路犯罪生態系統中的運作中樞。

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.Dropper
- SONAR.Module!gen3
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g13

- SONAR.RansomGen!gen1
- SONAR.RansomQuantm!g1
- SONAR.SuspLoad!g12
- SONAR.SuspOpen!gen7
- SONAR.SuspOpen!gen8
- SONAR.SuspStart!gen12
- SONAR.WMIC!gen10
- SONAR.WMIC!gen13

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Ransom.Quantum
- Ransom.Quantum!gm1
- Trojan Horse
- Trojan.Bumblebee
- Trojan.Bumblebee!g1
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT

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: Meterpreter Reverse HTTPS
- Audit: ADFind Tool Activity
- System Infected: Trojan.Backdoor Activity 373

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機保護方案--DCS的政策強化功能可有效阻止BumbleBee載入程式的活動和Quantum勒索軟體的活動，如檔案的寫入/讀取、網路活動、WMI查詢等。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／IP位址已於第一時間收錄於不安全分類列表中。

2022/06/27

烏克蘭電信營運商成為 UAC-0113 駭客集團的目標

烏克蘭的電信營運商已經成為 UAC-0113 也稱為 Sandworm 進階持續威脅 (APT) 駭客組織的網路釣魚攻擊目標。攻擊從一封聲稱是關於法律援助的釣魚郵件開始，該郵件有一個受密碼保護的 RAR 壓縮檔附件。附件解壓縮後的 Excel 檔內嵌巨集會植入 DarkCrystal 遠端存取木馬 (RAT)，該 RAT 能夠存取網路資源、竊取資料和執行程式碼。本月上旬觀察到某次針對烏克蘭媒體組織也有類似的攻擊方式。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Trafic2.RGC!g10

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Mdropper
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/06/24

Bronze Starlight 駭客組織利用 HUI 載入程式來部署勒索軟體的有效籌載

據報導，被稱為 "Bronze Starlight" 的駭客組織，在目標網路上散佈勒索軟體，以作為誘餌來分散組織對其活動目的的注意力，其真正目的即有可能竊取機敏資訊。攻擊者一直在利用 HUI 載入程式來大量部署，包括 LockFile、AtomSilo、Rook、Night Sky 和 Pandora 等勒索軟體的有效籌載。這個威脅行為者已知和另一個名為 Bronze Riverside 的駭客組織密切相關的使用各種現成工具，例如：Sodamaster 遠端存取木馬、PlugX 和 Cobalt Strike 來竊取機敏資訊。

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：

基於行為偵測技術(Snoar)的防護：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Packed.Generic.663
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.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。