保安資訊--本周(台灣時間2022/03/04)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 130 萬個受保護端點上總共阻止了 2.0463 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/02/27)**

- 在**23萬7,800**台端點上，阻止了**1.068億**次嘗試掃描**Web**服務器的漏洞。
- 在**51萬6,200**台端點上，阻止了**4,580萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬6,500**台**Windows**伺服主機上，阻止了**2,660萬**次攻擊。
- 在**18萬5,000**端點上，阻止了**1,030萬**次嘗試掃描伺服器漏洞。
- 在**10萬800**台端點上，阻止了**510萬**次嘗試掃描在**CMS**漏洞。
- 在**15萬3,400**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**44萬7,800**台端點上，阻止了**1,330萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,800**台端點上，阻止了**490萬**次加密貨幣挖礦攻擊。
- 在**13萬2,700**台端點上，阻止了**560萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,500**台端點上，阻止了**28萬940**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。

2022/03/03

TeaBot 行動惡意軟體透過新的傳播行動捲土重來

TeaBot 是在 2021 年初首次發現的行動銀行惡意軟體。在過去，該惡意軟體主要是透過偽裝成 DHL 或 UPS 快遞通知的釣魚資訊進行傳播。也有少數情況是透過 Google Play 商店上架的 Apps傳播。根據最近發佈的一份報告，最新的 TeaBot 行動正是回歸到這種傳播方式，透過在 Google Play 商店發佈的 Apps 傳播惡意軟體。TeaBot 更新的竊密功能，針對銀行和保險 Apps及加密貨幣交易所／錢包Apps。

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.1
- Android.Reputation.2
- AppRisk:Generisk

2022/03/02

Lampion 銀行木馬鎖定葡萄牙語國家

Lampion 惡意軟體仍然是針對葡萄牙語國家很活躍的銀行木馬之一。Lampion 在最近的行動中透過惡意 .vbs 檔案傳遞。為了繞過檢測機制，攻擊者透過添加大量垃圾資料，將這些 VBS 載入程式的檔案大小增加到大約 56 MB。Lampion 以使用者的銀行資訊為目標，重點鎖定最知名的巴西和葡萄牙銀行組織。

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.C

2022/03/02

在安卓平台上的新銀行木馬：Xenomorph

Xenomorph 與另一個惡名昭彰的銀行木馬“Alien”有關，因為它的程式碼相似、類別名稱和有趣的字串。然而，雖然它可能與 Alien 功能密切相關，但 Xenomorph 確實有差異，並且充滿許多未啟用的功能，顯示這個變種可能仍在進行中。

Xenomorph 最新版本能夠濫用輔助功能服務、竊取未知受害者的個人識別資訊 (PII)、防止被移除並截取 SMS。

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.MBT
- WS.Malware.1

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已於第一時間收錄於不安全分類列表中。

2022/03/01

濫用 Formbook 竊密程式的行動，正在全世界亂竄

眾所周知，許多熱門的竊密程式被多團體和個人所濫用，Formbook 就是其中之一，這使得它在威脅領域中炙手可熱、歷久不衰。賽門鐵克繼續觀察許多 Formbook 行動，其規模和存活時間各不相同。在過去 30 天裡，一名參與者使用常用的社交工程誘餌，如：航運、報價和環球銀行金融電信協會(SWIFT)支付系統，並聲稱自己是知名的國際銀行和石油公司，發動一波又一波的大規模垃圾郵件行動。沒有特定的目標，全球各個行業都收到垃圾郵件。

觀察到的電子郵件主旨：

- CHARTERER REQUISITION
- Quotation
- Bank SWIFT Advice generated on 29.02.2022
- Bank Generated Swift message HSBC

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!g21

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.Gen.2
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/03/01

OutSteel 和 SaintBot 惡意軟體被用於針對烏克蘭能源部門的攻擊中

被稱為 UAC-0056 (又名 TA471 或 SaintBear) 的威脅集團，與 2 月初針對烏克蘭能源組織的攻擊活動有關。根據最近發佈的一份報告，攻擊者一直在利用 Word 附加檔案的魚叉式網路釣魚資訊。這些附加檔案包含惡意的 Javascript 檔，下載 SaintBot 下載程式和 OutSteel 竊密程式等有效籌載。這個惡意軟體具有雙重角色既可滲透機密資料，也能下載額外有效籌載到受感染的電腦。該威脅集團一直在使用 Discord 內容遞送網路 (Content Delivery Network，CDN) 架構來託管惡意軟體的有效籌載。

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：

- Bloodhound.RTF.20
- CL.Downloader!gen10
- Downloader
- Infostealer
- ISB.Downloader!gen69
- ISB.Downloader!gen80
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- Scr.Malcode!gdn30
- W97M.Downloader

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：

- Audit: PowerShell Process Accessing discordapp[.]com
- Malicious Site: Malicious Domain Request 59
- 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。

2022/03/01

Jester 竊密程式--威脅版圖中的另一個竊密程式

一個被稱為 Jester 竊密程式的新變種已在真實環境中被觀察到。Jester 主要針對用戶的登錄憑證、瀏覽器 cookies、加密貨幣錢包資料和銀行資訊。雖然這種惡意軟體的最初版本早在 2021 年 7 月就已經在各種地下論壇上提供銷售，但最近報告顯示，Jester 仍在不斷發展，經反覆修正最近也具備額外的反沙箱和反虛擬機器功能。

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.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/02/28

利用烏克蘭和俄羅斯衝突有關的社交工程攻擊越來越多！

賽門鐵克已經開始觀察利用烏克蘭和俄羅斯衝突的社交工程攻擊。最近的例子，一個參與者一直試圖透過惡意電子郵件和通訊軟體，來引誘受害者，呼籲利用加密貨幣捐款幫助烏克蘭，使用的電子郵件主題是：與烏克蘭站在一起--你可以透過這種方式捐款。與烏克蘭站在一起--這裡是你可以捐款的方式。這位肆無忌憚的參與者，還在郵件中加入一條類似 2 月 27 日從烏克蘭官方推特帳戶發出的推文。如果成功引誘，受害者最後將進入 Formbook，這是一個已經存在多年著名的竊密爬蟲。它仍然是威脅領域的頂尖竊密程式，被許多集團和個人所使用。

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：

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：

- Scr.MalPbs!gen1

2022/02/28

Daxin (*大新)，精密且隱秘的後門程式

賽門鐵克發現一種高度精密的惡意軟體，該惡意軟體被與中國有關聯的威脅行為者使用。這種隱形後門被稱為 Daxin (*大新)，已被用於針對特定政府和其他關鍵基礎設施目標的間諜活動。有關此惡意軟體和活動的更多資訊，請參閱此處：

Daxin (*大新)：一支專為攻擊安全強化的網路環境而設計隱秘的後門程式

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：

- Backdoor.Daxin
- Backdoor.Trojan
- Backdoor.Zala
- Trojan Horse
- Trojan.Emulov
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

DCS 內建的強化安全政策能預防惡意驅動程式被植入 Windows 作業系統。

2022/02/25

MuddyWater (*混沌的水)威脅集團所使用的惡意軟體和工具

根據美國和英國當局發佈的聯合公告，被稱為 Small Sieve (*小篩子)的惡意軟體已被 Seedworm (又名MuddyWater) 駭客集團用於針對全球關鍵基礎設施的攻擊。Small Sieve (*小篩子) 是一個用 Python 撰寫的後門程式，威脅者主要是使其在被攻擊的目標上持續存在。該組織利用的其他惡意軟體變種包括：PowGoop 載入器、Canopy (又名StarWhale)、Mori 後門、PowerStats 和一個新發現用於加密命令和控制 (C&C) 通信管道的 PowerShell 後門…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：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mdropper
- VBS.Downloader.Trojan
- 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：

- 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。