保安資訊--本周(台灣時間2022/05/06)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 120 萬個受保護端點上總共阻止了2.015 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/05/02)**

- 在**21萬9,300**台端點上，阻止了**1億800萬**次嘗試掃描**Web**服務器的漏洞。
- 在**46萬2,600**台端點上，阻止了**3,730萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬2,800**台**Windows**伺服主機上，阻止了**2,400萬**次攻擊。
- 在**16萬2,700**端點上，阻止了**1,000萬**次嘗試掃描伺服器漏洞。
- 在**8萬4,800**台端點上，阻止了**420萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬4,200**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**36萬8,600**台端點上，阻止了**1,000萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,710**台端點上，阻止了**390萬**次加密貨幣挖礦攻擊。
- 在**11萬5,400**台端點上，阻止了**560萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,200**台端點上，阻止了**21萬2,900**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。

2022/05/05

假冒 Instander (*旁觀者) 安卓 APP 竊取 Instagram 用戶憑證

雖然 Instagram 處於一個競爭激烈的領域，但截至目前，它仍然非常受歡迎，對許多人來說是賺錢的途徑。當涉及到人氣、名氣和金錢時，總是會有網路犯罪。多年來，已經有許多人試圖透過惡意軟體、網路釣魚和單純的社交工程來竊取 Instagram 使用者的憑證 (帳密)。

最近幾天報導，有一個覬覦 Instagram 使用者憑證的 Android 惡意軟體。在這個行動中，威脅者將他們惡意軟體偽裝成 Instander，這是一個 Instagram 平台的修改版，它提供超越正統 Instagram 平台權限的受歡迎 MOD 功能，以提高使用者體驗。

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：

- AdLibrary:Generisk

2022/05/05

Mustang Panda 進階持續威脅 (APT) 攻擊中最近散佈 PlugX 惡意軟體

Mustang Panda（又名 Bronze President* 青銅總統）是一個來自中國的駭客組織，在過去 10 年中積極攻擊對象是世界各地的政府和非政府組織。這個 APT 組織最近活動的目標集中在歐洲，並在利用各種政治主題作為誘餌的惡意郵件活動中，散佈 PlugX 惡意軟體變種。Mustang Panda APT 還更新使用的散佈戰術，威脅者開始利用二進位檔案下載器，而不是像早期活動中所看到那樣載入對應的惡意軟體 DLLs。

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.Cobalt!gen16
- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Backdoor.Korplug
- Backdoor.Rozena
- Downloader.Trojan
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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：

- 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。

2022/05/05

Remcos RAT 在最近的惡意軟體行動中再次出現

Remcos RAT 已經在最近的惡意郵件行動中，利用受密碼保護的 .xls 檔案來散佈。聲稱來自城市國民銀行（CNB）的惡意電子郵件包含一個名為“CNB Payment Advice.xls”附件檔。該試算表包含惡意的巨集，執行後會生成 Remcos RAT 有效籌載。Remcos 是一個著名的商業遠端存取木馬（RAT），可以讓攻擊者遠端控制受感染的電腦，並有能力竊取機密資料。

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：

- Downloader
- Trojan Horse
- WS.Malware.2
- 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。

2022/05/04

BluStealer 惡意軟體以新變種重出江湖

BluStealer 是一種惡意軟體，最初於 2021 年被發現，並在惡意垃圾郵件行動期間以惡意郵件附件或網址鏈結 URL 的形式傳遞。根據一份最新報告，BluStealer 幕後的攻擊者仍在開發這種惡意軟體的更新變種。惡意軟體感染經歷三個階段，載入程式以 NSIS（Nullsoft 腳本化安裝系統）安裝程式的形式啟動整個攻擊鏈。BluStealer的功用可從各種 Web 瀏覽器中竊取使用者憑證，從郵件應用程式中讀取資料或提取多種類型的加密貨幣錢包的密鑰。

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

基於機器學習的防禦技術：

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

2022/05/03

Magniber 勒索軟體，透過假 Windows 更新散布

據觀察，Magniber 勒索軟體是透過偽造 Windows 10 安全或累積更新來散布。該 msi 檔有各種名稱，但都聲稱是某種更新。下載內容存放在 warez 和破解網站上，因此最安全的方法是僅從受信任的 Microsoft 網站下載 Windows 更新。該行動主要針對學生和消費者，贖金要求並不高約只要 2,500 美元。

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

2022/05/02

Emotet 利用惡意 .LNK 檔傳播攻擊行動

Emotet 殭屍網路在最近攻擊行動中開始將 .LNK 檔作為初始的傳遞機制。.LNK 檔是透過夾帶 .zip 附件的惡意郵件傳播。一旦解壓縮並執行 .LNK 檔，將執行 Powershell 命令，從遠端 URL 下載 Emotet 有效酬載。

Emotet 駭客集團對戰術、技術和程序 (TTPs) 的改弦易轍是企圖再次規避偵測機制--就在最近，也有報導稱 Emotet 模組已升版為 64 位元。在 Emotet 散布階段不只有 .LNK 檔，因為賽門鐵克繼續觀察到 LNK 和 XLS Emote 行動在同一時間運行。

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：

- CL.Downloader!gen20
- CL.Downloader!gen260
- CL.Downloader!gen261
- CL.Downloader!gen262
- CL.Downloader!gen263
- CL.Suspexec!gen128
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Scr.Malcode!gen
- Scr.Mallnk!gen1
- Scr.Mallnk!gen2
- Scr.MalMacro!gen1
- Trojan.Gen.2
- Trojan.Gen.NPE.C
- Trojan.Mdropper
- XLM.Downloader!gen1
- XLM.Downloader!gen2

基於行為偵測技術(Snoar)的防護：

- SONAR.MSExcel!g2
- SONAR.MSExcel!g4
- SONAR.MSExcel!g9

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已於第一時間收錄於不安全分類列表中。

2022/05/02

REvil 勒索軟體，死灰復燃

早在 2021 年 10 月，俄羅斯當局就成功取締 REvil 勒索軟體集團的營運。然而，在上個月，該集團被觀察到在 TOR 網路上的活動，似乎該集團可能已經死灰復燃。

最近出現一個樣本，經過拆解、分析該感染鏈的細部，如：舊網站、舊基礎設施和勒索信說明，似乎證實這個懷疑，確認與 REvil 相關聯。但新樣本未如預期進行加密，這可能表示它實際上只是由該集團的現有成員使用以前的原始程式碼，來進行新瓶裝舊酒的改名勒索軟體。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/29

APT29 駭客集團 (也稱Nobelium) 在 2022 年行動中運用全新的惡意軟體變種

APT29 駭客集團也被稱 Nobelium，一直利用兩個新惡意軟體家族--BEATDROP和BOOMMIC發動 2022 年攻擊行動。攻擊者一直鎖定外交和政府組織為目標，發動一系列網路釣魚活動，當然少不了利用惡意軟體下載程式。與 2021 年一些舊的傳播行動類似，已知威脅行動者濫用合法網路服務，如：Trello、Dropbox 或 Firebase，既能方便傳播惡意軟體，同時也能逃避任何檢測。

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：

- Meterpreter
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/04/29

Earth Berberoka 濫用 PuppetLoader 以及 oRAT 等惡意軟體發動跨平台攻擊

一個被稱為 Earth Berberoka (又名 GamblingPuppet) 新進階威脅 (APT) 組織被發現。據報導，該組織在最新一系列惡意行動中針對賭博網站。該威脅組織利用 Windows、Linux 和 MacOS 平臺的惡意軟體。除使用已知的惡意軟體家族，如：PlugX 和 Gh0stRAT，攻擊者還發佈一個名為 PuppetLoader 新變種。在針對 MacOS 平臺的攻擊中，使用另一個與眾不同稱為 oRAT 惡意軟體變種。

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.Dofloo
- Linux.Mirai
- OSX.Trojan.Gen
- Trojan Horse
- Trojan!gm
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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。

2022/04/29

SaintStealer：另一個普通的竊密程式

另一個被稱為 SaintStealer 普通的竊密程式變種被觀察正在各地流竄。該惡意軟體針對各種使用者的資料、憑證、銀行資訊、VPN 資料、Discord 權杖等，並將收集的資訊提取到攻擊者控制 Telegram 頻道。據報導，SaintStealer 使用 C2 基礎設施與其他幾個惡意軟體家族共用，如：QuasarRAT 或 EchelonStealer 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
- WS.Malware.1

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。

2022/04/29

泰國通行證 (Thailand Pass) 成為 AsyncRAT 遠端存取木馬的攻擊目標

已觀察到鎖定申辦線上泰國旅遊登記 (Thailand Pass) 使用者 AsyncRAT 遠端存取木馬的攻擊。透過垃圾訊息或惡意網址 URL 來引誘受害者打開 HTML 檔案。打開該檔案會自動投放一個 ISO 檔，內容包含一個經混淆的 Visual Basic 腳本，在檢查目前所使用的防毒軟體之後，該腳本會用 AsyncRAT 來感染電腦。

*註(非原稿)：自 2021 年 11 月 1 日起，以空運入境泰國須辦理泰國旅遊登記 Thailand Pass。

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：

- JS.Downloader.D
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B