保安資訊--本周(台灣時間2022/04/01)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 120 萬個受保護端點上總共阻止了 2.085 億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/03/27)**

- 在**21萬9,900**台端點上，阻止了**1.048**億次嘗試掃描**Web**服務器的漏洞。
- 在**48萬4,500**台端點上，阻止了**4,470**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬3,600**台**Windows**伺服主機上，阻止了**2,530**萬次攻擊。
- 在**16萬3,200**端點上，阻止了**940**萬次嘗試掃描伺服器漏洞。
- 在**8萬9,900**台端點上，阻止了**460**萬次嘗試掃描在**CMS**漏洞。
- 在**13萬100**台端點上，阻止了**370**萬次嘗試利用的應用程式漏洞。
- 在**42萬800**台端點上，阻止了**1,180**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,100**台端點上，阻止了**580**萬次加密貨幣挖礦攻擊。
- 在**12萬100**台端點上，阻止了**650**萬次向惡意軟體**C&C**連線的嘗試。
- 在**6,900**台端點上，阻止了**23萬4,800**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。

2022/03/31

全新 Blackguard 的竊密程式，大辣辣地在駭客論壇上出售

一個名為 Blackguard 的基於 .Net 全新竊密程式，開發者仍然持續增強其威力與功能中，並在駭客論壇上以賣斷或按月訂閱出售。Blackguard 被發現具有全方位的竊密功能，包括瀏覽器、電子郵件用戶端、聊天室、VPN 軟體和加密錢包。

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

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。

2022/03/31

威脅警報：Spring4Shell （CVE-2022-22965） 漏洞

研究人員發現一個名為 Spring4Shell（CVE-2022-22965）的遠端程式碼執行（RCE）漏洞，該漏洞一直存在 Spring Core Java 框架中。該漏洞允許未經身份驗證的攻擊者，在目標系統上執行任意程式碼。Spring Core 是一個熱門的應用程式框架，允許軟體開發人員輕鬆開發具有企業級功能的 Java 應用程式。然後，可以將此類應用程式部署在具有所有必需要的獨立安裝套件（如 Apache Tomcat）的情境上。

Spring 在其 CVE 報告中證實，該漏洞需要某些先決條件才能被利用。Spring 已經發佈 Spring Framework 版本更新 5.3.18 和 5.2.20，這些更新解決這個漏洞。

賽門鐵克發佈以下部落格文章，其中包含更多詳細資訊：Spring4Shell：Java 框架中發現的新零時差 RCE 漏洞

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：

- Hacktool
- Hacktool.Spring4shell

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: Spring Core Spring4Shell Activity
- Web Attack: Spring Core Spring4Shell Activity 2

基於機器學習的防禦技術：

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

基於安全強化政策(適用於使用DCS)：

DCS 的入侵預防 (IPS) 內建的安全政策早就能預防 Spring4Shell 的漏洞利用並提供零時差攻擊提供保護。

2022/03/31

Transparent Tribe (*透明部落) 進階持續威脅 (APT) 集團發動新的攻擊行動 -- 鎖定印度政府及軍方

在真實環境發現，針對印度政府官員和軍事單位的新惡意攻擊行動。據報導，一個名為 Transparent Tribe (*透明部落)(又名 APT36 或 Mythic Leopard) 的威脅組織應與這些攻擊有關。據說威脅發動者利用正在用 Crimson RAT 惡意軟體搭配初始惡意軟體散佈和植入媒介感染受害者。該集團利用的傳播媒介包括封存和惡意檔案，以及使用偽裝成合法安裝程式的惡意可執行檔。

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
- Trojan.Gen.MBT
- Trojan.Gen.Mdropper

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

基於機器學習的防禦技術：

- 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：

- Malicious Site: Malicious Domains Request
- 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。

2022/03/31

發現大量散佈 Remcos 遠端存取木馬 (RAT) 的最新攻擊行動

據報導，最新利用與銀行帳戶有關誘餌的惡意垃圾郵件攻擊行動，正在大量散佈 Remcos 惡意程式。網路釣魚電子郵件包含檔名為「WFCEO23_Remittance_Advice.xls」惡意附件檔，這些附件檔一被執行就會馬上啟動感染鏈並最終引爆 Remcos RAT 的有效籌載。Remcos 是一種著名的商業遠端存取木馬 (RAT)，多年來一直保持相對活躍，且至今仍是利用垃圾郵件傳播最常見的惡意軟體家族之一。RAT 使攻擊者具有輕鬆就能遠端控制受感染的機器及收集機敏資料的能力。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen81
- ISB.Dropper!gen40
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- W97M.Downloader

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

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。

2022/03/30

Cobalt Strike -- 透過魚叉式網路釣魚行動來散布

一起新的魚叉式網路釣魚行動針對的是反對俄羅斯政府的俄羅斯公民和政府單位。目標會收到各種仿效官方標誌的電子郵件，警告使用即時通訊應用程式、社交網路、VPN 服務和被俄羅斯政府禁止的網站的人，將對他們提出刑事指控。這些消息聲稱來自「聯邦資通信監督局」和「俄羅斯聯邦數位發展、電信和大眾通信部」。受害者被引誘點擊網頁鏈接 (URL) 或打開惡意附件，以了解有關警告的更多資訊，結果卻被 Cobalt Strike 感染。

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：

- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- Trojan.Mdropper
- W97M.Downloader
- 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已於第一時間收錄於不安全分類列表中。

2022/03/30

Google 上的 OpenOffice 廣告被當作 Mars Stealer 的誘餌

Mars Stealer 是一種竊密程式，在 Racoon Stealer 幕後的組織最近退出江湖後，它已經嶄露頭角。該竊密程式基於較舊的 Oski Stealer，並且已在網路上發佈破解版本以及具有錯誤配置選項的說明。由於這種糟糕的配置，攻擊者在測試竊密程式時，會向研究人員洩漏自己的資訊。攻擊者使用付費的 Google 廣告試圖誘騙人們下載惡意軟體並感染自己。此行動中的 Google 廣告針對熱門的開放原始碼專案 OpenOffice，並使用與原始網站幾乎相同的複製網站。

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：

- MSIL.Downloader!gen7
- 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.*

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 59

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。

2022/03/30

SunCrypt 勒索軟體在真實環境仍然活躍

SunCrypt 是勒索軟體即服務 (RaaS) 的變種，於 2019 年首次出現。根據最新報告，該惡意軟體在 2022 年仍然活躍，其最新版本具有新的增強功能。勒索軟體能夠停用系統程序和服務，並清除其執行的任何痕跡。SunCrypt 勒索軟體集團還在其戰術中採用三重勒索--除了檔案加密和在洩漏網站上發佈之外，攻擊者還以潛在的 DDoS 攻擊威脅受害者。

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
- Ransom.Gen
- Ransom.Gen!gm
- Ransom.Suncrypt
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g7

基於機器學習的防禦技術：

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

2022/03/29

謹防使用 PseudoSteel 的網路釣魚攻擊

最近觀察到針對烏克蘭國家當局使用 PseudoSteel 的網路釣魚攻擊。這次攻擊使用聲稱與烏克蘭軍人傷亡有關的檔案。它們安裝 PseudoSteel，可用於搜索和上傳本機檔案和封存檔案。此活動可能與俄羅斯威脅組織 UAC-0010（世界末日）有關。

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：

- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

2022/03/29

Purple Fox (*紫狐)駭客組織在最近的行動中引入了新的感染媒介

據報導，*紫狐駭客組織在最近的攻擊行動中，引入一種新的感染媒介。攻擊者正在利用偽裝成合法安裝程式的特洛伊木馬軟體套件來感染使用者。該組織使用熱門的應用程式名稱，如 Adobe、Chrome 或 Telegram 來隱藏惡意安裝程式。*紫狐最近還更新他們的惡意軟體組合，推出一種名為 FatalRAT 的新型遠端存取木馬 (RAT) 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：

- Trojan Horse
- 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。

2022/03/29

發現手法老練的 Verblecon 惡意載入程式

被稱為 Verblecon 新惡意軟體已被用於最近發現的攻擊，在受感染的電腦上散布挖礦程式。還有一些跡象表明，攻擊者可能正在竊取 Discord 的 Token，並利用這些 Token 來宣傳木馬電子遊戲應用程式。這些應用程式可以進一步作為 Verblecon 額外散布的通路。這種惡意軟體的能力表明，如果在勒索軟體或間諜活動中加以利用，它可能會非常危險。

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.Verblecon
- 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已於第一時間收錄於不安全分類列表中。

2022/03/25

Coper 銀行木馬偽裝成 Google Play 商店安裝程式以感染受害者

Coper 行動惡意軟體的一個新變種，已被觀察到偽裝成 Google Play 商店安裝程式，並針對整個歐洲 Android 使用者。Coper 惡意軟體被認為與較舊的 Exobot 惡意軟體有關。Coper 是模組化，在感染階段採用多階段方法。該惡意軟體的功能包括鎖定裝置螢幕、發送或攔截簡訊，進行鍵盤側錄以及在應用程式上方顯示網路釣魚視窗等。

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：

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

2022/03/25

Hodur：Korplug 惡意軟體的新變種

總部位於中國的進階持續威脅 (APT) 組織 Mustang Panda 與正在進行的網路釣魚和間諜活動有關，該行動針對歐洲外交官的 ISP (網際網路服務提供商)。該活動於 2021 年 8 月首次啟動，並帶有名為 Hodur 新 Korplug 惡意軟體變種。

有關 Korplug 的遠端存取特洛伊木馬 (RAT) 方面的其他命令和功能：

- Ping -- 開始監聽命令
- GetSystemInfo -- 收集和發送系統資訊
- ListenThread -- 啟動新威脅以監聽第二個處理程式的命令
- ResetConnection -- 重置與 C&C 的連接
- Uninstall -- 刪除添加的登錄機碼，刪除所有惡意軟體元件並刪除建立的資料夾
- Stop -- 停用登錄機碼並退出

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.Module!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- 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已於第一時間收錄於不安全分類列表中。