保安資訊--本周(台灣時間2022/09/23)
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 萬受保護端點上總共阻止了1.33億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/09/19)**

- 在**19萬600**台端點上，阻止了**5,700**萬次嘗試掃描**Web**服務器的漏洞。
- 在**35萬9,000**台端點上，阻止了**2,690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬3,000**台**Windows**伺服主機上，阻止了**1,830**萬次攻擊。
- 在**12萬4,400**端點上，阻止了**560**萬次嘗試掃描伺服器漏洞。
- 在**5萬400**台端點上，阻止了**250**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬8,300**台端點上，阻止了**280**萬次嘗試利用的應用程式漏洞。
- 在**33萬7,800**台端點上，阻止了**780**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8萬6,000**台端點上，阻止了**320**萬次加密貨幣挖礦攻擊。
- 在**5萬800**台端點上，阻止了**550**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,800**台端點上，阻止了**18萬6,100**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。

2022/09/22

由 Scarlet Mimic APT 組織散播的 MobileOrder 安卓間諜軟體

在網路上觀察到一波新的惡意活動，這些活動是由被稱為 Scarlet Mimic 的 APT 組織發起，目標是維吾爾族社群。攻擊者繼續利用被稱為 MobileOrder 手機行動惡意軟體，該軟體最早於 2015 年被發現。根據最近一份報告，該惡意軟體很可能是透過各種社交工程行動散播，利用偽裝成 pdf 檔、文件檔、圖片或音訊資料的惡意應用程式。MobileOrder 可以竊取儲存在受感染設備上的資料及拍攝照片、撥打電話或操控通話記錄和簡訊。

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：

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
- Spyware:MobileSpy

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。

2022/09/22

Noberus 勒索軟體以新的戰術、工具和程序 (TTPs) 繼續攻擊

Noberus (又名BlackCat、ALPHV) 被廣泛認為是 Darkside 和 BlackMatter 勒索軟體家族的後續有效籌載。最近幾個月，部署 Noberus 勒索軟體的攻擊者一直在使用新的戰術、工具和程序 (TTPs)，使這種威脅比以往任何時候都更加危險。其中更引人注目的發展是使用新版本的 Exmatter 資料滲透工具及使用 Eamfo，這是一種資訊竊取的竊密惡意軟體，主要在竊取 Veeam 備份軟體儲存的憑證。

在我們的部落格閱讀更多訊息：Noberus 勒索軟體：Darkside 和 BlackMatter 繼任者繼續改進其策略

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.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Eamfo

- Ransom.Noberus
- Trojan.Exmatter
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2022/09/21

觀察到新的大黃蜂攻擊運動

大黃蜂是一種普遍存在的載入程式，已迅速成為各種網路犯罪攻擊的關鍵元件，似乎已經取代一些舊的載入程式。它與一些勒索軟體行動有關聯，包括 Conti、Quantum 和 Mountlocker。

已經觀察到一個新的大黃蜂惡意軟體活動，其攻擊鏈以虛擬硬碟 (VHD) 容器為承載。它再次使用惡名昭張的 ISO 容器內含一個受密碼保護的 ZIP 檔。如果用戶被成功誘導解壓縮 ZIP 和 ISO，然後執行執行 powerhell 腳本的惡意連結檔，就會觸發該攻擊鏈的其他部分。

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.Mallnk
- Scr.Malarchive!gen1

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。

2022/09/21

RAT 惡意軟體透過偽造的 Telegram 網站傳播

一個新的惡意活動已經被發現，攻擊者試圖透過一個偽裝成合法 Telegram 網站的網頁來傳播一個遠端存取木馬 (RAT) 惡意軟體。該惡意軟體是透過MSI安裝包傳播的，一旦執行就會側載一個名為 mpclient.dll 的惡意 .dll 二進位檔案。這個 .dll 檔的名稱故意與 MS Windows 系統中的合法系統檔相似。RAT 有效籌載一旦成功安裝，就會等待來自攻擊者 C&C 伺服器的進一步命令。惡意軟體代碼顯示，它具有停用執行程序、刪除各種應用程式和瀏覽器的資料以及下載額外的

任意有效籌載的功能。

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

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／IP位址已於第一時間收錄於不安全分類列表中。

2022/09/20

Colibri Loader 和 Warzone RAT 被部署在最新的 UAC-0113 APT 攻擊活動中

已觀察到屬於 UAC-0113 威脅組織的新活動，其中攻擊者使用偽裝成烏克蘭電信公司的動態 DNS 網域，試圖將惡意軟體傳播到烏克蘭組織的網路上。所採用的攻擊使用與軍事行動、管理通知、報告等相關的各種誘餌文件。威脅組織正利用惡意 ISO 檔案，這些檔案提供部署 Colibri Loader 和 Warzone RAT（又名 AveMaria）有效負載的可執行檔。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen25
- SONAR.SuspLaunch!g12

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Avecma
- Infostealer
- Packed.Generic.516
- Packed.Generic.526
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

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 446

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。

2022/09/16

針對日本 NTT DOCOMO 使用者的行動惡意軟體

一個針對日本 NTT DOCOMO 用戶的全新惡意行動攻擊已經有到處爆發的跡象。該惡意軟體透過上架在 Google Play 商店假冒成行動安全應用程式散播。該惡意軟體利用收集到的使用者密碼，針對 NTT DOCOMO 行動支付服務，進行支付欺詐。

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
- Android.Reputation.2
- AppRisk:Generisk

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。