保安資訊--本周(台灣時間2023/01/13)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 79 萬 5,900 台受保護端點上總共阻止了 9,990 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/01/09)**

- 在**15萬1,200**台端點上，阻止了**4,000**萬次嘗試掃描**Web**服務器的漏洞。
- 在**27萬5,200**台端點上，阻止了**2,210**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬9,600**台**Windows**伺服主機上，阻止了**1,750**萬次攻擊。
- 在**8萬9,100**台端點上，阻止了**290**萬次嘗試掃描伺服器漏洞。
- 在**2萬900**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬8,300**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**25萬7,100**台端點上，阻止了**640**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬8,300**台端點上，阻止了**250**萬次加密貨幣挖礦攻擊。
- 在**4萬8,200**台端點上，阻止了**470**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,000**台端點上，阻止了**13萬4,400**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。

2023/01/12

OriginLogger雙效惡意軟體在最近的惡意垃圾郵件攻擊行動中聲名大噪

OriginLogger 惡意軟體最近偽裝成付款發票的惡意 .iso 附件檔的惡意垃圾郵件攻擊行動中傳播。發送的郵件主旨為“銀行付款通知”的電子郵件據稱來自銀行機構。在執行該 .iso 檔中包含的可執檔後，整個感染鏈由觸發惡意軟體載入程式開始，後續會將惡意酬載傳送到受害者的電腦。OriginLogger 是一種兼具竊密程式與鍵盤側錄的惡意軟體，與 AgentTesla 惡意軟體有許多相似之處。

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.NPE
- WS.Malware.2

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。

2023/01/11

Apple揭露並提供修補MacOS CVE-2022-46689漏洞

Apple 最近發布針對 macOS 版本 13.1、12.6.2 和 11.7.2 中的漏洞 (CVE-2022-46689) 的修補，這些漏洞可能允許本地經過身份驗證的攻擊者獲得系統的權限提升。此漏洞是由 macOS 的核心中出現競爭條件所引起，經過身份驗證的攻擊者可以透過特製請求 (例如：透應用程序) 利用核心權限執行任意程式碼。最近在用於軟體開發和版本控制的 Internet 代管服務上分享此漏洞的概念證明，可用於攻擊含有漏洞的 MacOS 版本。

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：

- Exp.CVE-2022-46689

2023/01/11
新出爐的勒索軟體：Upsilon(*厄普西隆)

要求支付價值 500 美元比特幣作為贖金的全新勒索軟體已被發現。一旦受害者的檔案被加密，會被新增“.upsil0n”的副檔名，並且留下檔名為“Upsilon.txt”勒索贖金說明在受影響的電腦上。此 Upsilon 勒索軟體活動背後的歹徒並未使用雙重勒索伎倆，但他們要脅如果 3 天內未支付贖金則會增加贖金來向受害者施壓。

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.Heur.Dropper
- SONAR.SuspBeh!gen625
- SONAR.SuspBeh!gen676
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!gen250
- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/01/11
NeedleDropper惡意程式植入工具

NeedleDropper 是全新的惡意軟體植入程式，在駭客論壇上進行宣傳和銷售，用於植入惡意籌載。NeedleDropper 以自解壓縮 (SFX) 檔的形式出現，其中包含多個二進位檔案和用於惡意軟體執行的其他設定檔案。NeedleDropper 傳播方法非常多元，可能包括透過 Discord 或 OneDrive 鏈接發送惡意垃圾郵件或直接分享惡意檔案。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.681
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.2

2023/01/10

假冒Tele2電信公司的網路釣魚攻擊行動，瞄準荷蘭和比利時的用戶

賽門鐵克每天都會偵測到，歹徒冒充世界各地知名的電信公司的網路釣魚攻擊行動。網路犯罪分子經常在網路釣魚攻擊中這樣偽裝，因為這些知名的電信公司擁有大量客戶，人們可能會信任來自他們的通訊。

賽門鐵克最近發現針對荷蘭和比利時的消費者和企業的 Tele2 網路釣魚攻擊行動。歹徒偽裝成服務暫停的緊急通知惡意電子郵件來引誘用戶落入圈套，同時內含轉向假冒 Tele2 登錄網站的鏈接。以下是觀察到的電子郵件主旨樣本：

- Herinnering: Uw toegang wordt als ongeautoriseerd verklaard
- Uw toegang wordt geweigerd

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)。

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。

2023/01/10

網路犯罪商腦筋：只要有利可圖，安卓手機平台上的帳單詐欺惡意軟體就會是永遠的好生意

安卓手機平台上的帳單欺詐惡意軟體仍然很氾濫，因它是網路犯罪集團可日進斗金、一夜致富的可能。惡意軟體開發商可以輕鬆開發和散播惡意手機 APP，這些 APP 是專為竊取個人資訊並向受害者榨取不需要或未經授權的服務費用而設計。智慧型手機及行動裝置的普及和惡意 APP 可以輕易經由 APP 商店和其他線上平台取得，這樣蓬勃發展的生態系，助長歹徒的覬覦。

Joker 和 Harly 是安卓平台上最常見的帳單詐欺惡意軟體之二，即便每天都會發現全新的惡意 APP。它們主要透過 Google Play 商店傳播，將自己隱藏在看似合法的 APP 中。這些惡意軟體對消費者和企業都構成重大風險。消費者可能讓自己的行動裝置成為目標，而當員工使用已被感染的公司的行動裝置時，企業可能會受到攻擊。

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

2023/01/09

LummaC2 竊密程式

LummaC2 是一種在地下論壇上宣傳和銷售的竊密程式惡意軟體。該惡意軟體從基於 Chromium 和 Mozilla 的瀏覽器中擷取各種資訊。LummaC2 還針對安裝在受害者機器上的各種加密錢包和任何雙因素身份驗證 (2FA) 的應用機制。一旦資訊被截取，就會被加密後轉傳至攻擊者所操控的 C&C 伺服器。

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：

- OTrojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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。

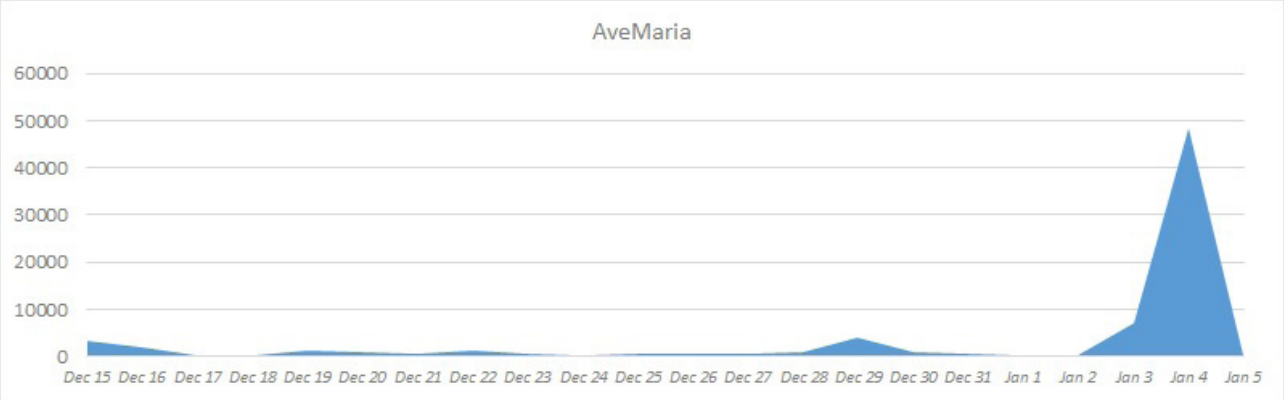
2023/01/06

防護亮點：賽門鐵克多層次防護機制讓 AveMaria RAT 落荒而逃

～防護亮點～

AveMaria (也稱為 Warzone RAT) 是一種遠端存取木馬 (RAT)，首次出現於 2018 年底前後，它具有從受害者那裡竊取資訊的能力，儘管某些變種還具有其他功能，例如：遠端桌面存取、提升用戶權限和啟動相機。它通常透過包含惡意附件的垃圾郵件“網路釣魚”行動傳播，或者在某些情況下鏈接到代管在合法雲端服務和檔案共享平台上的惡意檔案。相對於其他一些 RAT，AveMaria 沒有很流行，但它持續定期針對廣泛的商業部門發動垃圾郵件攻擊，雖然它似乎主要集中在 EMEA (歐洲、中東及非洲) 地區，但也包括在美國、中東和亞太地區的企業組織。

賽門鐵克安全機制應變中心，每天都會收到警報並調查涉及多種威脅的不同程度的威脅活動，但在 1 月 4 日至少有三種不同類型的防護技術同時偵測到，提醒我們留意 AveMaria 涉及的網路攻擊大幅增加。我們的 .NET 模擬器將其識別為 MSIL.Downloader!gen8，我們的機器學習技術將該攻擊識別為 Heur.AdvML.B，並且我們的一個啟發式技術權重機制將其歸類為 Scr.Malcode!gdn32。



值得注意的是，這種特殊的攻擊採用雙重副檔名伎倆，惡意郵件附件內含 “.pdf.exe" 之.gz 格式的自解壓縮檔附件。

賽門鐵克擁有領先業界的 **零時差** 保護技術，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!gen8
- Scr.Malcode!gdn32

基於機器學習的防禦技術：

- Heur.AdvML.B

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)。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，請點擊此處下載我們型錄及簡報檔。

要了解有關賽門鐵克安全 (SEP/SESE/SESC) 的更多資訊，請點擊此處下載我們型錄及簡報檔。

2023/01/06

macOS平台上的ThiefQuest勒索軟體在真實環境仍然活躍

ThiefQues (也稱為 EvilQuest) 是一種針對 macOS 平台的勒索軟體變種。除具有典型的勒索軟體該有的特徵外，該惡意軟體的一些變種還表現出鍵盤側錄、資訊竊取和後門功能……等額外功能。ThiefQuest 能夠執行多項檢查，驗證設備的 MAC 位址前 3 個字元的組織唯一識別碼 (Organizationally Unique Identifier，OUI) 是其中一項，也包含虛擬環境感知功能。該惡意軟體還會停用裝置上已安裝的安全軟體，以避免被安全軟體偵測到。雖然 ThiefQuest 已經問世好幾年，但僅在上個月才有在真實網際網路環境中發現許多全新變種。

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：

- OSX.RansomThiefQuest
- OSX.RansomThiefQue!g1
- OSX.Trojan.Gen
- WS.Malware.1

2023/01/06

鎖定Linux平台的Monti勒索軟體

Monti 是一種由惡名昭彰 Conti 勒索軟體被洩露原始程式碼所改編的後繼變種。該惡意軟體以 Linux 作業系統平台為目標，感染後被其加密的檔案會新增 .puuuk 的副檔名。該勒索軟體變種背後的威脅參與者運營著一個洋蔥網路 (Tor) 的資料洩露網站。被加密後，勒索軟體會留下 README.txt 這個文字檔的贖金說明，另外還會留下另一個 result.txt 的文字檔來說明被加密檔案清單及所有檔案大小。

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.Conti
- Trojan.Gen.NPE
- WS.Malware.1