保安資訊--本周(台灣時間2023/08/18)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 75 萬 8,400 台受保護端點上總共阻止了 3,401 萬次攻擊。這些攻擊中有 98.3% 在感染階段前就被有效阻止：**(2023/08/14)**

- 在**13萬5,500**台端點上，阻止了**3,080**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**22萬2,600**台端點上，阻止了**1,690**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬9,100**台**Windows**伺服主機上，阻止了**1,240**萬次攻擊。
- 在**8萬9,800**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,300**台端點上，阻止了**94萬7,300**次嘗試掃描在**CMS**漏洞。
- 在**6萬7,400**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**23萬4,900**台端點上，阻止了**550**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,500**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**22萬3,800**台端點上，阻止了**26萬9,400**台次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**9萬100**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。

2023/08/17

Gozi的最新攻擊行動鎖定銀行和加密貨幣領域

Gozi (又名 Ursnif、Snifula) 屹立不搖至今超過 15 年，目前在威脅領域依舊是排名很前面的銀行金融木馬家族。該惡意軟體可以從遭入侵的端點竊取登錄憑證／帳密、雙因素身份驗證碼、銀行詳細資訊和其他機敏資訊。最新觀察到的 Gozi 的傳播行動主要針對銀行業以及與加密貨幣行業相關的公司，例如：交易所和區塊鏈服務商。

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(SONAR)的防護：

- SONAR.SuspScript!g20

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2023/08/16

最新改版的KmsdBot殭屍電腦持續造成物聯網的災難

最新改版的 KmsdBot 殭屍電腦已經出現在真實網路世界。KmsdBot 是採用 Golang 語言撰寫的殭屍網路惡意軟體，支持各種 CPU 架構。眾所周知，該殭屍網路以鎖定有提供服務並採用出廠預設或弱帳密登入的低安全性物聯網系統為目標，主要被用利用於發動 DDoS 攻擊以及加密貨幣挖礦活動。最新改版的 KmsdBot 程式檔案是 kmsdx，會先進行 telnet 掃瞄、軟體更新並增加對其他 CPU 架構的支援。

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

2023/08/16

Raccoon(*浣熊)惡意竊密程式v2.3.0

沉寂 6 個月後，在地下論壇上又看到一篇帖文在宣傳最新的 Raccoon 惡意竊密程式 v2.3.0 版本。該惡意竊密程式較之前的版本進行了許多強化及新增功能，例如：新版的快速搜索工具可以輕鬆瀏覽被盜資料、自動攔截機器人和顯示面板、透過爬蟲檢測和阻止 IP (防止威脅研究人員) 的報表系統以及新的日誌統計面板。

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
- ISB.Downloader!gen483
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- 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)：

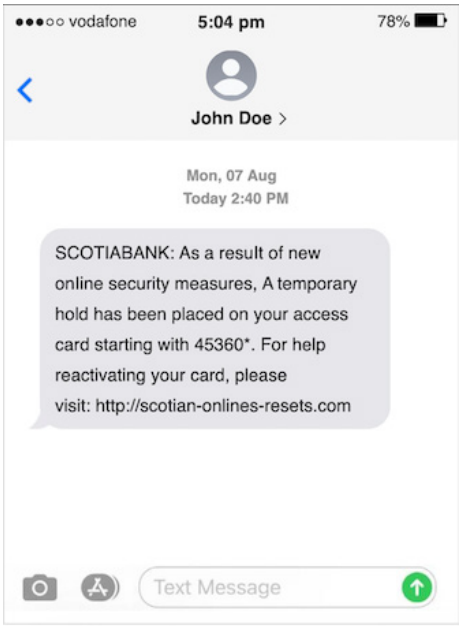
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/08/15

防護亮點：賽門鐵克有效防護網路釣魚簡訊，以近期的加拿大為例

賽門鐵克全天候監控全球範圍內可能會引爆網路詐騙、網路釣魚和惡意軟體的惡意簡訊 (也稱為簡訊詐騙)。儘管這早已不是什麼新聞，但每下愈況，而且許多都冒充知名金融機構，讓人誤以為真。近期的加拿大的銀行和金融科技公司就是一個例子，賽門鐵克最近幾週阻止其中的多起詐騙行動。

在這些網路攻擊行動中，消費者是主要的目標，但由於越來越多企業公發智慧型手機給員工和『自帶設備（Bring Your Own Device，BYOD）』 趨勢，企業用戶也一樣面臨風險。這些網路釣魚攻擊的影響和後果對這兩個群體來說都是嚴重的。誤信簡訊內容的用戶會被重導向模仿銀行的網路釣魚網站，其目的是竊取機敏資訊敏感訊息，最終導致金錢損失、身份盜竊、帳戶被盜、情緒困擾等。



惡意簡訊示例（按原樣 - 包括拼寫或打字錯誤）：

- RBC CANADA Security Alert：Your Client Card 4519**** has been temporarily locked due to unusual activity. To Regain Access Visit hxxps[:]//royal-banking-casecurity-verifcationonline[.]com～謊稱你的帳戶有異常，被暫停服務， 用簡訊誤導你登入假冒的網站以解鎖
- SCOTIABANK：As a resuIt of new onIine security measures, A temporary hold has been placed on your access card starting with 45360*. For help reactivating your card, please visit: hxxp[:]//scotian-[.]com～謊稱銀行提升安全認證機制，用簡訊誤導你登入假冒的網站以重新登入
- Info RBC：Vous avez recu (2) message important. Voir hxxps[:]//royalbank-messages[.]com～謊稱銀行重要通知，用簡訊誤導你瀏覽詳細資訊
- RBC：A temporary hold has been placed on your access card starting with 4519**. To reactivate your online access, please visit: hxxps[:]//rbc-profile[.]com～謊稱門禁卡被暫時停用，用簡訊誤導你登入假冒的網站以重新啟用
- CIBC SECURITY ALERT As a resuIt of new onIine security measures, A temporary hold has been placed on your access card starting with 45064*. For help reactivating your card, please visit: hxxps[:]//cibcreset[.]info～謊稱銀行提升安全認證機制，用簡訊誤導你登入假冒的網站以重新登入
- INTERAC e-Transfer：Canada Revenue Agency has issued you a refund on 20/03/2023 after making calculation errors on your last T4 return. Remember to deposit your interac E-transfer of 583.18$ CAD at: hxxps[:]//etransfer-interacdeposit[.]com/～謊稱報稅經修正後還可以退稅已匯入你的銀行帳戶，用簡訊誤導你登入假冒的網站以確認
- INTERAC e-Transfer：Canada Revenue Agency has sent you money. See hxxps[:]//secure-e-transfer-acceptonline-cra[.]com～謊稱退稅已匯入你的銀行帳戶，用簡訊誤導你登入假冒的網站以確認

賽門鐵克的多重防護技術已經於第一時間提供最有效的保護(**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。

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。

此外，為了有效降低網路釣魚攻擊的風險，使用簡訊服務時必須保持警惕，不回應不請自來的簡訊，避免點擊簡訊內嵌的可疑網址，並使用官方聯繫方式直接與銀行確認相關事宜。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。
欲瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲瞭解有關賽門鐵克全球情報網路 (GIN) 的更多訊息，請點擊此處。

2023/08/15

Linux平台上的新版Monti加密勒索軟體已開始大肆傳播

在真實網路情境已發現 Linux 平台上的新版 Monti 加密勒索軟體的蹤跡。Monti 是一個勒索軟體家族，最初於 2022 年 6 月發現，最初是源於令人聞風喪膽的 Conti 勒索軟體被洩漏公開的程式碼。Monti 同時具有支持 Windows 和 Linux 系統的兩個版本。最新 Linux 版本與以前版本的差異，主要是不再深深地依賴 Conti 原始碼，並且引入更先進的加密技術。該惡意軟體利用 AES-256-CTR 加密方法，而舊版本則使用 Salsa20 演算法。被其加密後的檔案會被冠上 .monti 的副檔名，並在每個被加密檔的目錄中存放『readme.txt』文字檔的勒索贖金支付說明。

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.NPE
- WS.Malware.1

2023/08/15

QwixxRAT遠端存取木馬

最近在真實網路情境上發現利用全新 QwixxRAT 遠端存取木馬所發動的網路攻擊行動。據報導，該惡意軟體透過 Telegram 和 Discord 平台傳播。QwixxRAT 遠端存取木馬具有允許攻擊者遠程控制遭入侵的電腦、啟動任意命令或收集用戶機敏資訊的功能。透過 Telegram 機器人 API 將竊取的資料傳送給攻擊者所操控的 C&C 伺服主機。

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(SONAR)的防護：

- SONAR.Dropper

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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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。

2023/08/15

全新變種的LummaC竊密惡意程式，在真實網路情境被用於發動網路攻擊

LummaC 竊密惡意程式，自 2022 年 8 月起在地下論壇上進行廣告和銷售。一直以來，被透過各種伎倆傳播，包括偽裝成合法軟體來源的網路釣魚網站和魚叉式網路釣魚電子郵件。該惡意軟體可以從 Chromium 和 Mozilla 的瀏覽器中擷取各種資訊，包括加密錢包的詳細資訊以及受害者電腦上安裝的雙因素身份驗證 (2FA) 擴展功能。一旦完成資訊收集並加密，然後轉發到歹徒所操控的 C&C 伺服器。

該惡意軟體一直持續發展，最新版本能夠將額外的惡意軟體引入受感染的系統。在觀察到的該行動的具體實例中，LummaC 竊密惡意程式被用來獲取和設置 Amadey 殭屍網路機器人，該機器人因其在系統評估、竊取資訊取和傳遞額外有害有效籌載等攻擊鏈中不同階段都有作用而聞名。隨後，Amadey 殭屍網路機器人被執行以取得 SectopRAT，這是一種基於 .NET 框架建立的遠端存取木馬。SectopRAT 以其多方面的功能而聞名，包括各種躲避偵測的技術，突顯網路威脅日益複雜的情況。

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：

- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

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：

- System Infected: Infostealer Lumma Activity 3
- System Infected: Trojan.Backdoor Activity 611

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。

2023/08/14

Cyclops勒索軟體家族的全新變種～Knight(*騎士)勒索軟體

Knight 勒索軟體是 Cyclops 勒索軟體家族的新變種。該惡意軟體會加密被害者的檔案，並冠上 .knight_l 的副檔名，並留下名為『How To Restore Your Files.txt』的文字檔的勒索贖金支付說明檔案。Knight 勒索軟體最近以偽裝成 TripAdvisor 投訴通知的惡意垃圾郵件散佈行動中廣為傳播。惡意垃圾郵件大辣辣包含惡意軟體執行檔的壓縮附件，或者包含重定向用戶下載 Excel .xll 檔案的 .htm 附件，從而導致感染。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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：

- System Infected: Trojan.Backdoor Activity 721

2023/08/14

瀏覽網頁來的～Statc(*靜態)竊密程式

威脅研究人員已公布名為 Statc (*靜態) 的全新竊密程式。這種竊密程式會感染 Windows 平台並竊取受害者的許多資訊。Statc (*靜態) 竊密程式還支援檔名差異檢查，以逃避沙箱檢測。

初始攻擊是使用 Google Chrome 類的瀏覽器點擊惡意廣告開始引爆，該惡意廣告會下載惡意檔案。觸發惡意檔案再導引 PDF 誘餌和惡意下載器程式 (downloader) 檔案。該檔案隨後將透過 PowerShell 腳本下載 Statc 竊密程式。受害者被擷取的資訊將被加密並隨後傳輸到歹徒所操控的 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：

- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2
- W32.Qakbot

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2023/08/14

注意Mac也有不少惡意軟體～AdLoad惡意軟體在不斷針對macOS系統

許多人還是存在 Mac 不會中毒或很少中毒的老舊錯誤觀念，只要有利可圖的地方就會有不軌。AdLoad 是一種被廣泛傳播的惡意軟體載入程式／序 (Loader)，在過去幾年中出現在威脅領域。眾所周知，AdLoad 發起針對 macOS 系統的攻擊行動，它提供各種有效籌載，包括廣告軟體、捆綁軟體、後門等。最近觀察到的 AdLoad 攻擊行動一直在提供能夠將遭入侵系統轉變為代理機器人的代理應用程式／序。此類殭屍網路稍後可能會被歹徒用於其他惡意攻擊行動或濫發垃圾郵件等目的。

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.AdLoad
- OSX.AdLoad!g1
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2023/08/11

青出於藍～改編的全新JanelaRAT惡意遠端存取木馬

JanelaRAT 是由 BX RAT 遠端存取木馬改編的全新變種。JanelaRAT 常見於針對拉丁美洲地區銀行用戶的網路攻擊行動中的散佈階段。為了避免安全軟體的檢測，其利用 DLL 側載到合法可執行檔的技術。JanelaRAT 功能包括滑鼠／鍵盤側錄和螢幕截圖等。惡意軟體透自定義通訊協定與預定義的 C&C 伺服器通訊，並將擷取的資訊傳輸給攻擊者。

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：

- Infostealer.Eynice
- ISB.Downloader!gen62
- ISB.Houdini!gen7
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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。