保安資訊--本周(台灣時間2023/11/10)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 59 萬 800 台受保護端點上總共阻止了 7,390 萬次攻擊。這些攻擊中有 84.6% 在感染階段前就被有效阻止：**(2023/11/06)**

- 在**10萬4,400**台端點上，阻止了**2,820**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**17萬3,600**台端點上，阻止了**1,500**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬1,100**台**Windows**伺服主機上，阻止了**1,330**萬次攻擊。
- 在**6萬1,300**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,600**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬5,300**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**22萬8,300**台端點上，阻止了**460**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,800**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**11萬3,200**台端點上，阻止了**940**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**844**台端點上，阻止了**6萬6,200**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。

2023/11/09

又是全新變種勒索軟體～GoTiS勒索軟體

GoTiS 是最近在威脅環境中發現的全新 Xorist 勒索軟體變種。該惡意軟體會加密使用者檔案後並冠上 .GoTiS 副檔名。勒索 (贖金支付) 說明以名為『HOW TO DECRYPT FILES.txt 』的文字檔形式提供，威脅者要求受害者以比特幣支付贖金，並建議受害者透過所提供的電子郵寄地址聯繫他們，以便在支付贖金後獲得進一步說明。

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：

- Ransom.CryptoTorLocker
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.B

2023/11/09

以退款通知為幌子，瑞典電信服務商TELE2遭冒名發送釣魚郵件

瑞典電信服務商 TELE2 也是一家知名的跨國行動網路供應商，成立於 1993 年，總部位於瑞典斯德哥爾摩。最近，賽門鐵克發現有釣魚網站冒充 Tele2，誘使用戶打開虛假的退款通知電子郵件。這些釣魚郵件試圖誘使用戶打開並點擊釣魚網頁。

- 原文電子郵件主旨：Bekräfta din återbetalning från Tele2
- 電子郵件主題 (已翻譯)：確認您從 Tele2 收到的退款

點擊電子郵件內容中顯示的釣魚網頁後，受害者會看到登入憑據／帳密的網頁。

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。

2023/11/09

CVE-2023-46747：F5 BIG-IP遠端程式碼執行(Remote Code Execution，RCE)漏洞～原廠已釋出修補

CVE-2023-46747 是最近披露的一個影響應用交付控制器系統 BIG-IP 嚴重等級(CVSS 評分：9.8) 遠端程式碼執行 (Remote Code Execution，RCE) 漏洞。如果成功開採利用該漏洞，未經身份驗證的攻擊者可透過 BIG-IP 系統網路存取權限執行任意系統命令。應用程式交付平臺供應商 F5 已經修補該漏洞，但也表示該漏洞已在真實網路情境被各種威脅行動者開採利用，這些威脅行動者還將該漏洞與另一個 BIG-IP 漏洞 CVE-2023-46748 結合起來利用。

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：

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：

- Attack: F5 BIG-IP RCE CVE-2023-46747

2023/11/08

竊『蛇』出洞～全新Serpent(*蛇)竊密惡意程式已造成災難

Serpent 竊密惡意程式是一款基於 .NET 的新型複雜惡意軟體。它透過地下論壇傳播，可以從大多數網路瀏覽器和程式中收集資料，並收集一些登錄憑證／帳密。已發現的 Serpent 竊密惡意程式足跡，顯示其使用各種技術躲避防毒軟體以及偵錯工具和虛擬機器等惡意軟體工具的檢測，並能繞過 Windows 用戶帳戶控制 (UAC)。透過濫用 Discord 掛勾 (webhook) 將所收集的資料洩漏出去。

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.TCP!gen1

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.MBT
- Trojan.horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300

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

2023/11/08

SideCopy頑強駭客組織(APT)：在最近攻擊行動中散布Linux平台上的Ares遠端存取木馬(RAT)及其他多種惡意酬載

與 SideCopy 頑強駭客組織 (APT) 有關連的最新攻擊行動中散布包含 Linux 平台上的 Ares 遠端存取木馬 (RAT) 及其他多種惡意酬載。據報導，威脅分子利用 WinRAR 漏洞 CVE-2023-38831 散布多種遠端存取木馬 (RAT) 變種，例如：Allakore、DRAT、Key RAT 或 Ares RAT 的 Linux 變種。據瞭解，攻擊者還利用釣魚連結指向誘餌 .pdf 檔案，並下載惡意 LNK 和 HTA 檔，主要目的就是將最終有效籌載下載到受攻擊的系統上。上述惡意有效籌載之一的 Ares 惡意軟體是一種基於 Python 的開源 RAT，能夠執行 shell 命令、截圖和下載其他檔案等功能。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen203
- CL.Downloader!gen241
- Infostealer.Eynice
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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。

2023/11/08

請關切～激增的Jupyter竊密惡意程式相關活動

最近觀察到 Jupyter 竊密惡意程式相關聯的活動明顯增加。Jupyter 最初發現於 2020 年，已知可透過一般常見的攻擊媒介 (例如：偷渡式下載、網路釣魚電子郵件或惡意軟體) 傳播。該惡意軟體的功能是攫取存儲在各種網路瀏覽器中的憑證／帳密和資料，然後將收集到的資訊洩露到攻擊者控制的 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 Horse
- Trojan.Gen.MBT
- WS.Malware.1
- Ws.Malware.2
- WS.Reputation.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。

2023/11/08

Socks5Systemz代理殭屍網路

在真實網路情境發現一個名為 Socks5Systemz 的全新代理殭屍網路。據觀察，該殭屍網路透過兩個熱門的惡意程式載入器 PrivateLoader 和 Amadey 來感染。

該殭屍網路背後的威脅者開發一種綜合代理服務，允許使用者訂閱、管理現有訂閱並存取當前可用代理清單。此外，他們還涉及出售被入侵的帳戶和代理存取權限。

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.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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 558

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。

2023/11/07

Trap Stealer(*設圈套的小偷)惡意竊密程式

Trap Stealer 是一款新觀察到的開源惡意竊密程式。該惡意竊密程式具有許多功能，包括但不限於以下內容：

- 從瀏覽器中竊取 cookie、自動填表資訊、密碼和搜索歷史記錄
- 根據關鍵字收集系統資訊並竊取敏感檔案
- 竊取與 Discord 和 WhatsApp 相關的內容

Trap Stealer 透過濫用 Discord 掛勾 (webhook) 將所收集的資料洩漏出去。

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：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g269
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- WS.Malware.1

2023/11/07

防護亮點：濫用JavaScript的惡意廣告

JavaScript 是一種常用於動態網頁內容的腳本程式語言。維基百科告訴我們，截至 2023 年，98.7% 的網站都在用戶端使用 JavaScript 進行網頁瀏覽。因此，如果你正在瀏覽一個網頁，它的程式碼中很可能包含 JavaScript。

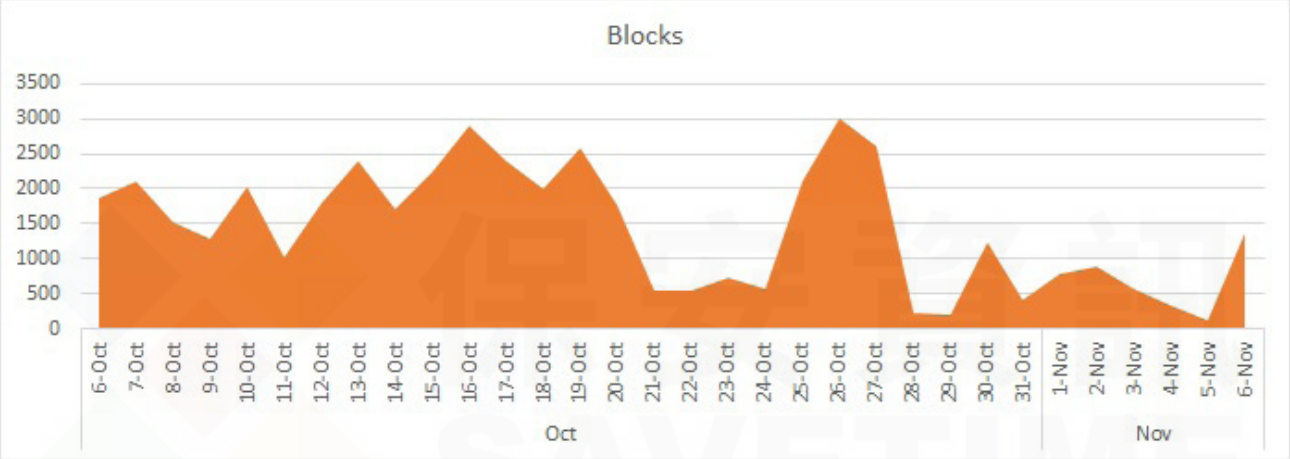
惡意廣告的定義是利用線上廣告傳播惡意軟體，通常是在合法的線上廣告網路和網頁中注入惡意或含有惡意軟體的廣告。這些廣告包含惡意程式碼（可能使用 JavaScript 編寫，也可能不使用 JavaScript 編寫），可能直接連結到惡意軟體，也可能最終將用戶重定向到另一個網站（甚至是一連串網站），最終載入的有效籌載可能是漏洞開採利用工具包、網路釣魚網頁、勒索軟體等。

惡意 JavaScript 很難被發現，因為它本質上只是純文字。當它被偷偷注入網站時，有時會在網頁上停留數月甚至數年，包括在非常熱門、知名和完全合法的網站上。當人們瀏覽這樣的網

站時，他們的安全軟體會突然彈跳出一個可怕的視窗，顯示該網站已被感染，他們可能會認為安全軟體搞錯了，這肯定是一個『誤判』檢測，因為該網站畢竟是大家高度信任的網站。

大約一年前，賽門鐵克收到類似的詢問--瀏覽一個可信網站時產生檢測結果，一個指腳本檔被發送到隔離區，這合理嗎？當時的分析表明該檔確實很糟糕，是一個惡意 JavaScript 轉導向。幾天前，我們又收到同樣的詢問，同樣的檔，但這次是在不同網站上。再次審查證實最初的判斷--惡意網頁。

幸運是這種情況並不常見，但也沒有什麼特別之處。有趣是我們在 VirusTotal 上查找 JavaScript 的檔案，看看它影響層面有多大。除了賽門鐵克以外，只有另一家資安公司有進行攔截。儘管這種惡意腳本檔多年來在網路上流傳數千個實例，顯然感染大量網站，而且可能有大量用戶瀏覽這些網站。



這證明威脅行動者是多麼狡猾，以及他們在不遺餘力地破壞您和您的寶貴資訊時所使用的一些伎倆是多麼難以察覺。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Wonode

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

2023/11/07

全新的AsyncRAT遠端存取木馬的感染鏈

AsyncRAT 遠端存取木馬感染鏈行動始於垃圾郵件中嵌入的惡意網頁鏈接，該網頁鏈接會導致惡意 HTML 檔案下載。多個程序被啟動以執行 C&C 通訊。該惡意軟體具有多種功能，如竊取憑證、鍵盤側錄、瀏覽器資料截取等。所有收集到的資料都會洩漏到 AsyncRAT 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：

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：

- Backdoor.ASync!gm
- CL.Downloader!gen
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/11/07

SecuriDropper手機行動平台上的惡意軟體

SecuriDropper是一種全新的手機行動平台上的惡意軟體，以『惡意植入程式即服務』(DaaS) 模式出售。該惡意軟體具有繞過安卓13 中推出的『受限制的設定』安全功能，該功能負責對授予側載應用程式的許可權設置某些限制。據觀察，一些濫用 SecuriDropper 最新攻擊行動將 SpyNote RAT 或 Ermac 銀行木馬作為最終有效籌載。

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

2023/11/07

2023年假日季節以假的年終休假郵件拉開序幕

時值假日季節，威脅分子又在他們的武器庫增加一個新主題。在最近的一次網路釣魚活動中，有人向收件人發送包含釣魚網頁並偽裝成年終或年假通知的電子郵件。電子郵件主旨包含收件人的網域名稱和時間戳記。這樣做是為了增加個人化的感受，引誘使用者打開電子郵件。電子郵件正文內容簡短，『寄件者』欄位顯示收件人的域名＋人力資源部門。

電子郵件標題：

- 主旨： [收件人的域名] 2023 年年終年假
- 寄件者 "[收件人的域名] 人力資源部" <已修改的電子郵件位址>

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。

2023/11/07

冒名Colisimo(*科利西莫)的簡訊釣魚攻擊行動，正在危害法國

Colissimo 是由法國國家郵政局 La Poste 運營的包裹遞送服務。它為個人和企業提供國內和國際航運解決方案。Colissimo 一直以來常被冒名用於社交工程攻擊，以詐騙使用者和／或竊取他們的憑證和其他敏感資訊，如地址、姓名、信用卡等。世界各地每天都能看到這些非法的攻擊行動，主要是透過惡意電子郵件和簡訊來發動的。

最近，賽門鐵克在法國發現了一個網路釣魚行動，壞蛋冒充 Colissimo 公司～一家由法國國家郵政局 La Poste 運營的包裹遞送服務商，在法國佔有重要地位。

在這一起攻擊行動中，主使者試圖欺騙手機用戶，聲稱他們的包裹運送出狀況，並建議他們點擊一個網頁鏈結進行驗證。這些主使者推出模仿正統 Colissimo 的網站，申請多個與正統合法 Colissimo 類似的網域名稱。這種伎倆利用人們在輸入網址時不免會輸入錯誤。針對 Colissimo 公司這個個案而言，這是一種有效的伎倆，因為人們經常登入這些網站來跟蹤包裹、查看運送狀態或尋求客戶支援。

收到的簡訊內容：

- Colissimo：您的包裹 CH7013262652FR 在運輸途中遇到問題。請瀏覽以下鏈結：colissimo-parceltrack[.]

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。

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。

2023/11/06

駭客濫用Cloudflare R2物件儲存服務代管釣魚網頁

網頁郵件服務經常被網路釣客冒充 (網頁郵件是一種透過網頁瀏覽器，而非 email 用戶端，發送 email 的方式)，試圖竊取企業電子郵件的憑據／帳密。賽門鐵克每天都在觀察這些攻擊。在最近一個案例中，我們發現一個假冒 Roundcube 的網路攻擊行動，Roundcube 是一種熱門的開源 Webmail 應用程式，以友善的使用者介面而著稱。

在此起攻擊行動中，攻擊者正在發送主旨為『[公司名稱] 警告！！！停用警告』的郵件。如果受害者被這些電子郵件誘騙並點擊惡意網頁鏈結，他們將被重定向到一個代管在 Cloudflare R2 上的假冒 Roundcube 登錄釣魚頁面。

出現過的網頁鏈結：hxxps://pub-[removed][.]r2[.]dev/RWMAIL[.]html#John[.]Doe@JohnDoe[.]com

Cloudflare 的 R2 是 Cloudflare 提供一項免費代管服務，允許使用者快速部署靜態網站。不幸是此類服務提供便利和易用性也可能吸引做壞事的人，包括發動網路釣魚的主使者。

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：

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。

2023/11/06

Vector(*向量)竊密惡意程式

Vector 是典型的竊取程式，今年初首次在網路安全社群受到關注，此後便不時出現在威脅環境中，無論是與測試相關還是實際的惡意攻擊行動。賽門鐵克最近觀察到的樣本似乎是透過瀏覽網頁時的順道下載的方式傳播，並使用.NET應用程式的虛擬化保護程式 KoiVM 進行保護／混淆。

一旦該惡意軟體被執行，它就會擷取各種電腦資訊，包括 MAC 位址、使用者名稱、機器名稱、作業系統、目錄、安裝的防毒軟體、IP 位址和作業系統平臺 (x64 或 x86)。接下來，它會試圖從以下應用程式中獲取敏感資訊或檔案：

- 郵件用戶端 Outlook、ThunderBird、FoxMail
- 各種瀏覽器的 Cookie 和cards
- 聊天應用程式 Discord 和 Telegram
- 冷加密錢包 Exodus、Electrum
- FTP 應用程式 FileZilla、WinSCP

它還會嘗試攫取可能被認為敏感的 .doc、.docx、.pdf、.rdp 和 .txt 檔案。任務完成後，它會將竊取資料存檔並發送到作者的 Telegram(一種跨平台的即時通訊軟體) 帳號。

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.SuspBeh!gen313

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/11/06

網路陷阱十面埋伏～近期濫用金融業的拼字錯誤域名(域名誤植)網路陷阱明顯增加

賽門鐵克最近發現多個針對金融機構的網路釣魚主機。網路壞蛋發送自稱來自金融機構的電郵，並在連結中使用仿冒網頁而不是實際的公司連結。在過去的兩個月中，已經發現數百個個別的拼字錯誤主機，其中一些主機來自相同 IP 位址。

例子包括：

- <銀行域名>-iaccessweb[.]com
- <銀行域名>-iauth[.]com
- <銀行域名>-safetyupdated[.]com
- <銀行域名>secure-access[.]com

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。

2023/11/06

有憑有據！SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點 (桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 1.872 萬個受保護端點上阻止了總計 700 萬次攻擊。

- 使用網頁信譽情資，在 1.676 萬個端點上阻止 590 萬次攻擊。
- 攔截 36.5K 個端點上 736.1K 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 15.5K 個端點上攔截 216.9K 次瀏覽器通知詐騙攻擊。
- 在 797 個端點上攔截 70.3K 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 2.1K 個端點上阻止 4K 次技術支援詐騙攻擊。
- 在 239 個端點上阻止 467 次加密劫持嘗試。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2023/11/06

命名的靈感來自千年一擊：千年一成，一擊而解嗎？居然有遠端存取木馬命名為Millenium(*千年)

Millenium RAT (遠端存取木馬) 是一種 Windows 平臺上的惡意軟體，允許攻擊者透過 Telegram 進行遠端控制。該惡意軟體具有廣泛的資訊竊取功能，包括鍵盤側錄、螢幕截圖、瀏覽器內存儲資料收集 (cookie、憑證、銀行資訊等) 以及遠端命令執行和下載附加有效籌載。攻擊者利用 Telegram API 進行惡意軟體通信和檔案／資料擷取。

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：

- AGR.Terminate!g2

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

2023/11/06

針對MySQL伺服器的Ddostf DDoS殭屍網路

Ddostf 惡意軟體是另一種針對易受攻擊／漏洞未補的 MySQL 伺服器之 DDoS 殭屍網路。雖然它相對是較老的惡意軟體，最初發現於 2016 年，但至今仍被用於惡意網路攻擊行動中。該惡意軟體會掃描 MySQL 伺服器使用的開放埠 3306／TCP，並對易受攻擊／漏洞未補的系統進行暴力或字典攻擊。感染後，Ddostf 會聯繫預定義的 C&C 伺服器，將受感染系統的基本資訊上傳給攻擊者，最後接收執行 DDoS 攻擊或下載附加任意有效籌載的命令。

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
- SMG.Heur!gen
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2023/11/05

安卓平台上WhatsApp模組出現暗藏惡意軟體向阿拉伯語系使用者傳播

最近在真實網路情境發現向阿拉伯語系的使用者，傳播安卓平台上惡意軟體的新一波網路攻擊行動，這些惡意軟體偽裝成 WhatsApp 模組的 APP。這些非官方的 WhatsApp 模組 APP，大多透過第三方應用程式商店和 Telegram 頻道傳播，此外還有各種專門用於修改 WhatsApp 的可疑網站。

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：

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
- AppRisk:Generisk
- Android.Reputation.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／IP 位址已於第一時間收錄於不安全分類列表中。

2023/11/05

以色列成為MuddyWater頑強駭客(APT)組織最近一波網路攻擊行動的目標

根據最近一份報告，觀察到名為 MuddyWater 的頑強駭客 (APT) 組織以以色列實體為目標。MuddyWater 至少從 2017 年 2 月以來一直活躍，主要針對中東地區的政府和民間機構。在最近的網路攻擊行動中，該威脅行動者一直在利用一種全新的主機代管服務和一種新的遠端系統管理工具。攻擊途徑始於一封釣魚電子郵件，其中包含一個帶有鏈結捷徑的壓縮附件檔，該壓縮附件檔會啟動攻擊鏈，導致遠端系統管理工具的執行。

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：

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。

2023/11/03

瞄準金融業的惡意垃圾郵件網路攻擊行動散布Zorex惡意程式

賽門鐵克最近發現一個惡意垃圾郵件網路攻擊行動，散布感染 W32.Zorex 的 IMG 檔案，目標對象包括銀行／金融、醫藥和飯店業等不同產業。Zorex 一旦被執行，就會試圖感染受害者機器上的 XLS、XLSX 和 XLSM 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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen633
- SONAR.SuspBeh!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- W32.Zorex

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

2023/11/03

網路攻擊行動濫用社交媒體惡意廣告散布NodeStealer惡意竊密軟體

最近觀察到濫用社交媒體惡意廣告散布 NodeStealer 惡意軟體的網路攻擊行動。攻擊者一直在劫持 Facebook 企業帳戶以提供惡意廣告。點擊該廣告會觸發惡意可執行檔的下載，進而感染最終有效籌載。NodeStealer 是今年初首次出現的一種竊密惡意軟體。論其功能，它可以劫持各種網路瀏覽器的 cookie session，還可以竊取加密貨幣錢包、其他應用程式的資料或下載額外的相關有效籌載。

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
- WS.Malware.2
- WS.Reputation.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。

2023/11/03

傳播KANDYKORN惡意軟體的網路攻擊行動，正在鎖定macOS使用者

據報導，在真實網路情境發現到一起名為 REF7001 網路供行動，正在鎖定 macOS使用者。該攻擊鏈可拆解為多個階段，包括透過 Python 腳本進行初始入侵、發送 SugarLoader 和 HLoader 惡意軟體以及最終感染 KandyKorn 有效籌載。KandyKorn 惡意軟體具有從受感染端點收集和洩漏資料的功能。惡意軟體還可能執行從攻擊者操控 C&C 伺服器接收的其他任意命令或有效籌載。

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
- OSX.Trojan.Gen
- 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。