保安資訊--本周(台灣時間2024/01/26)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 57 萬 6,200 台受保護端點上總共阻止了 5,880 萬次攻擊。這些攻擊中有 83% 在感染階段前就被有效阻止：**(2024/01/22)**

- 在**10萬2,200**台端點上，阻止了**1,820**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**16萬500**台端點上，阻止了**1,360**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**1,060**萬次攻擊。
- 在**6萬2,100**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,600**台端點上，阻止了**84萬2,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,100**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**23萬700**台端點上，阻止了**500**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬4,400**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**11萬2,400**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**750**台端點上，阻止了**29萬4,100**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。

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 15.82 萬個受保護端點上阻止了總計 630 萬次攻擊。**(2024/01/22)**

- 使用網頁信譽情資，在 **142.6K** 個端點上阻止 **550** 萬次攻擊。
- 攔截 **33.1K** 個端點上 **655.5K** 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 **12.2K** 個端點上攔截 **154.4K** 次瀏覽器通知詐騙攻擊。
- 在 **562** 個端點上攔截 **52.4K** 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 **795** 個端點上阻止 **1.2K** 次技術支援詐騙攻擊。
- 在 **219** 個端點上阻止 **506** 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。

2024/01/25

P2PInfect惡意軟體

P2PInfect 惡意軟體是採用 Rust 語言開發，是一種跨平臺的蠕蟲病毒，它使用各種傳播方式在各種架構和平臺上進行感染。該惡意軟體利用 Redis 資料庫的漏洞，能夠在不依賴 C&C 伺服器的情況下執行點對點 (P2P) 通訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 能為 Windows 和 Linux 伺服器提供多層次保護。
- 賽門鐵克重要主機防護系統：DCS～Data Center Security 其出廠就內建的強化政策，可防止惡意軟體在系統上植入或執行。DCS 可以保護 Linux 伺服器防止從暫存檔案或其他可寫入

位置執行惡意軟體，這是惡意軟體中使用的一種技術。

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 其出廠就內建的強化政策，採用基於最小權限、最低資源的自訂沙箱來限縮 Redis 伺服器執行環境，可防止這些類型的惡意軟體。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2024/01/25

透過BYOVD『自帶易受攻擊驅動程式』(BYOVD)伎倆傳播的Kasseika勒索軟體

Kasseika 是最近在真實網路情境上觀察到值得關注的勒索軟體，與目前威脅環境中的其他一些勒索軟體類似，Kasseika 也採用所謂的『自帶易受攻擊驅動程式』(BYOVD) 伎倆。在這種情況下，攻擊者利用易受攻擊的驅動程式 Martini.sys 來停用受害者端點上的各種安全軟體。一旦入侵後，惡意軟體將終止機器上運行的多個系統進程和服務，然後開始加密過程。完成檔加密後，勒索軟體會在每個加密目錄中留下勒索 (贖金支付) 說明 .txt 文字檔，並更改桌面背景。

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.RansomBlkMat!g2
- SONAR.RansomPlay!gen1
- SONAR.Ransom!gen98
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Ransom.Kasseika
- Trojan.Killfiles
- Trojan.Malscript
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

2024/01/25
利用Muieblackcat漏洞掃描的攻擊者

Muieblackcat 是一款用於網路伺服器的漏洞掃描產品。遠端攻擊者可以使用 Muieblackcat 檢測目標伺服器上的漏洞，並從易受攻擊的系統中獲取敏感資訊。入侵預防系統 (IPS) 根據威脅狀況監測結果進行掃描，顯示該工具的使用率最近有所上升。賽門鐵克的網路保護技術入侵預防系統 (IPS) 會阻止來自該工具的掃描活動，以防止對系統造成進一步感染／破壞。

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：

- Web Attack: Muieblackcat Scanner Request

2024/01/25
Parrot(*鸚鵡)惡意網頁導向服務--持續助長網頁式攻擊的氾濫

至少自 2019 年以來，Parrot(*鸚鵡) 惡意網頁導向服務 (Traffic Direction System--TDS) 一直持續助長網頁式攻擊的氾濫而聲名大噪。這種 TDS 背後的攻擊者一直以 WordPress 或 Joomla 等安全性較差的內容管理系統 (CMS) 網頁服務平台為目標，使用 JavaScript 程式碼將受害者重導向到惡意的網址。涉入攻擊的兩個腳本元件--一個是負責分析目標的登陸腳本，另一個是用於將受害者重定向到惡意內容的有效酬載腳本。據觀察，Parrot TDS 涉入的攻擊行動以全球各行各業為目標。據瞭解，這些攻擊者還會在攻擊中開採濫用已知的漏洞。

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：

- JS.Cryxos!inf
- JS.Malscript!g1
- JS.Redirector
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Malscript
- Web.Reputation.1
- WS.Malware.2

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: Mass Injection Website 90
- Web Attack: Mass Injection Website 95

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。

2024/01/25

CVE-2024-0204：GoAnywhere MFT(Managed File Transfer)軟體檔案傳輸服務解決方案存有認證旁路(Authentication Bypass)漏洞

CVE-2024-0204 是 GoAnywhere MFT(Managed File Transfer) 軟體檔案傳輸服務解決方案存有認證旁路 (Authentication Bypass) 漏洞。如果被成功被開採濫用，該漏洞允許未經授權的攻擊者透過管理頁面建立管理員帳戶，這足以讓攻擊者部署惡意軟體、瀏覽敏感性資料，並可能在網路內發起進一步攻擊。賽門鐵克的網路防護技術入侵預防系統 (IPS) 可阻止這些漏洞利用嘗試，防止系統受到進一步感染／入侵。

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：

- Web Attack: Nginx Improper Path Normalization

2024/01/24

小心惡意捷徑檔(.LNK 檔案)～發現被加料的捷徑檔以Word檔為幌子，最終是在傳遞AsyncRAT遠端存取木馬

駭客圈正在大肆利用駭客工具來產出有加料的惡意捷徑檔 (.LNK 檔案) 最終就是要傳遞有效籌載。最近的報告顯示，發現專門用來下載 AsyncRAT 遠端存取木馬 (又名 VenomRAT) 的惡意捷徑檔。為了將惡意捷徑檔 (.LNK 檔案) 以合法的 Word 文件檔來掩護，它會藏身在一起打包在壓縮檔中。涉入攻擊鏈中被濫用的可執行檔偽裝成一家韓國公司憑證。使用者在不知情的情況下點擊這些檔案，就會危及系統安全，並面臨敏感資訊被盜的風險。

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：

- CL.Suspexec!gen162
- ISB.Downloader!gen285
- ISB.Downloader!gen544
- ISB.Heuristic!gen66
- ISB.Heuristic!gen5
- MSH.Downloader
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

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。

2024/01/24

MetaStealer惡意軟體涉入鎖定尋求美國庇護者為目標的網路攻擊行動

MetaStealer 惡意軟體在最近一次鎖定尋求美國庇護者為目標的網路攻擊行動被大肆散播。據了解，該行動是透過垃圾郵件發起的，郵件內包含一個指向惡意 .zip 壓縮檔的下載連結。解壓縮後，受害者會收到一個偽裝成 PDF 檔案的惡意 .lnk檔 (捷徑檔)，進而在遭入侵的端點上啟動感染鏈。當惡意軟體在背景執行時，一個誘餌檔案『I-589 表格--申請庇護和暫緩遣返』表格的 PDF 文件檔會顯示給受害者。MetaStealer 惡意軟體就是該網路攻擊行動的最終有效籌載荷，具有從受遭入侵電腦中竊取機密資訊的功能。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Rd32!g1
- ACM.Rd32-CPE!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen241
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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：

- 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。

2024/01/23

發現Chaes惡意竊密程式的後繼新版本

據報導，Chaes 惡意竊密程式的後繼新版本正在大肆瘋傳。攻擊由含有惡意網址的釣魚電子郵件所引爆，該惡意網址偽裝成與法律案件有關的緊急通知，並用葡萄牙語編寫。點擊鏈結後，受害者會被重導向到一個冒充 TotalAV 的詐騙網站，網站會提示使用者輸入密碼以下載文件。此動作會觸發 MSI 安裝程式的發送。一旦被安裝的惡意軟體成功啟動後，遭竊的資料會被發送到駭客的 C&C 伺服器，然後透過 Chaes 幕後主謀團隊控制頁面登錄進行存取。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen89
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

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。

2024/01/23

電子郵件夾帶附件PDF檔中內嵌RogueRaticate虛假瀏覽器更新程式鏈結

賽門鐵克最近發現，2023 年首次發現的惡意威脅『瀏覽器更新』RogueRaticate 透過惡意 PDF 檔案發送。這些訊息慫恿收件人開啟附件的惡意 PDF 檔。

觀察到的郵件主旨包括：

- Bill for Conference Sign-Up Costs
- Client Presentation #28277
- Client Presentation #718481
- Data Analysis #8989
- Feedback Request #2698
- Invoice for Conference Registration Fees
- Journey Expense Billing
- Mockups for the Design #4617

- Next Week Meeting Agenda #14873
- Outline for the Proposal #425145
- Presentation for the Client #47133
- Project Updated Timeline #9233
- Training Feedback #79655
- Travel Cost Bill Submission
- Travel Expense Invoice Submission
- Upcoming Meeting Agenda #142354

一旦該檔案被開啟後，收件人會被建議點擊一個連結，該連結會引導使用者下載一個網頁檔，最終導致 RogueRaticate 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：

- Scr.DLHeur!gen7

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：

- WS.SecurityRisk.4

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)。

2024/01/23
防護亮點：又見WikiLoader惡意程式載入器強勢回歸

WikiLoader 是早在 2022 年就被發現的惡意程式載入器，可以下載並植入惡意軟體在目標電腦上。它採用多種規避安全軟體偵測的伎倆和客製化的程式碼，與兩個主要的駭客組織 TA544 和 TA551 有所關連。

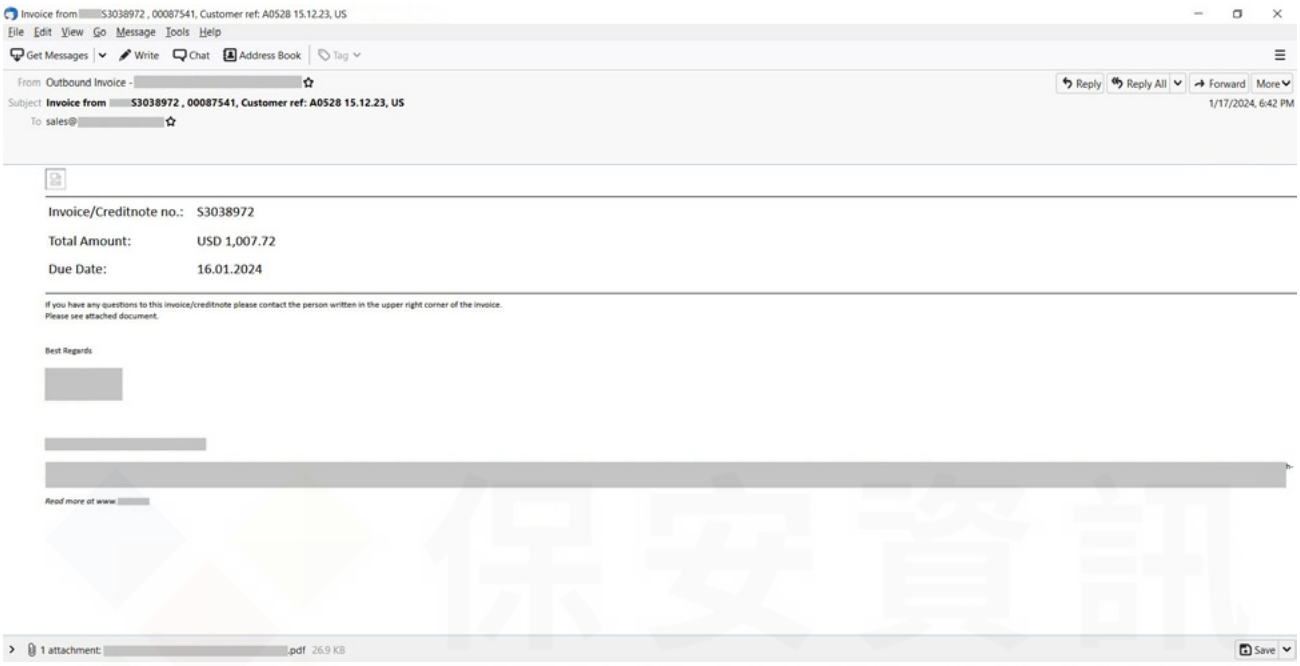
它之所以被命名為 WikiLoader，是因為最初的版本會向維基百科網站發出 Https 的連線請求，這很可能是為了檢查它是否有網際網路連接的能力，並且沒有在虛擬機器或隔離環境中運行，這可能顯示它正在被安全研究人員或某種類型的自動分析系統分析以規避安全軟體的偵測。

WikiLoader 的典型初始感染鏈始於一封包含 PDF 附件的電子郵件。在 PDF 檔中，會有一個連結，如果點擊該連結，就會下載一個壓縮的 JavaScript 檔，進而下載最終有效籌載。值得注意的是，開發者在腳本混淆方面下了很大的功夫。在超過 7 MB 的原始檔和 4383 行的程式碼中，大約 99.8% 是混淆的程式碼 (即垃圾程式碼)，目的是試圖隱藏其餘的一小部分核心惡意程式載入器的脈絡。鑒於 WikiLoader 的主要目的--提供惡意軟體散播服務--最終有效籌載可能是包羅萬象，但迄今為止較常見的是銀行金融惡意軟體，例如：Ursnif 或其他類型的惡意竊密程式。

觀察到的電子郵件主旨：

- Invoice from [company name]S7354534 , 01070875, Customer ref: A0627 15.12.23, US
- Invoice from [company name] S8786164 , 04725130, Customer ref: A0703 15.12.23, US

電子郵件範例：



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.DLHeur!gen8
- Scr.Malcode!gen
- Web.Reputation.1
- WS.SecurityRisk.4

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：

- [33403] Audit: System Process Accessing discordapp.com

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。

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。
欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入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。

2024/01/23

少見的BianLian勒索軟體集團：專門鎖定醫療保健和製造業的資料竊取而非檔案加密

BianLian 勒索軟體集團是當今比較活躍的駭客集團。他們鎖定的目標遍及各行各業，主要的受害產業還是以醫療保健業和製造業為大宗。雖然該駭客集團的大部分的活動都在美國進行，但其勢力範圍也遍及全球。該駭客集團目前的作案手法主要是竊取資料以勒索受害者，罕見地不採用最常見的檔案加密策略。

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(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：

- Ransom.Bianlian
- Ransom.Bianlian!gm
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/01/23

破解版的macOS應用程式內藏加密貨幣竊取惡意程式

在真實網路情境上演一起向 macOS 用戶散播加密貨幣竊取惡意程式的網路攻擊行動。透過熱門應用程式的破解，啟動工具掩護來安裝惡意軟體。經證實，該工具可在 MacOS 13.6 Ventura 或更新的版本上順利運行，這顯示攻擊者的目標是最新作業系統版本的使用者。攻擊行動的最終有效籌載是一個加密貨幣竊取惡意程式，目標是儲存在 Exodus 和 Bitcoin Core 加密錢包中的加密貨幣。

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.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。

2024/01/23
Frivinho勒索軟體

Frivinho 是一種全新的勒索軟體，它會在被加密檔冠上『.Frivinho0>v』的副檔名。加密完成後，會有『PLS_READ_ME.txt』的加密勒索 (贖金支付) 說明檔被存放在遭入侵的裝置上，引導受害者支付比特幣以取得解密金鑰。值得注意的是，該惡意軟體能夠刪除遭入侵端點上的磁碟陰影複製 (Volume Shadow Copy) 備份。

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：

- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/01/23
濫用ClearFake惡意框架的網路攻擊行動，正在散播Amadey惡意竊取程式

最近的濫用 ClearFake 惡意框架的網路攻擊行動，正在散播 Amadey 惡意竊取程式。該攻擊行動利用社交工程伎倆，透過偽造的瀏覽器更新向受害者發送惡意軟體。惡意 JavaScript 程式碼會注入到遭入侵的網站，並在受害者瀏覽頁面時被觸發。這讓惡意軟體有效載荷以瀏覽器更新的形式下載。據觀察，ClearFake 幕後的主謀還採用一種名為 EtherHiding 的新技術，利用 Binance 智慧鏈向潛在目標傳遞惡意的 JavaScript。

ClearFake 是一種部署在遭入侵網站上的惡意 JavaScript 框架，採用瀏覽網頁常見的偷渡式下載伎倆傳播更多惡意軟體。該惡意軟體利用社交工程手段誘騙受害者進行虛假的瀏覽器版本更新。

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：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- SONAR.Dropper
- SONAR.TCP!gen1

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

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

2024/01/22

LockBit勒索軟體採取寄生Word文件檔的伎倆

以『勒索軟體即服務』(RaaS) 而名噪一時的 LockBit 勒索軟體，一躍成為 2023 年當紅的勒索軟體之一。最近報告顯示，LockBit 幕後的主謀一直在利用 Word 檔作為傳播方式，這與他們過去的策略如出一轍。主要方法是在 Word 文件檔中嵌入惡意巨集。打開這些文件檔時，惡意巨集會觸發從外部網址下載衍生的惡意程式碼，進而導致 LockBit 勒索軟體的執行。這些惡意 Word 文件檔的檔案名，通常模仿與工作應用程式相關的常見名稱或文字。

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
- Ransom.Blackmatter!gm1
- SONAR.MSWord!g6

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：

- CL.Downloader!gen20
- ISB.Downloader!gen69
- Scr.Malcode!gen
- Trojan.Mdropper
- W97M.Downloader
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.A!300
- 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：

- Web Attack: Webpulse Bad Reputation Domain Request (29565)

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。

2024/01/22

Zloader惡意軟體在新一波網路攻擊行動中捲土重來

Zloader (又名 DELoader 或 Terdot) 是一種源於遭於洩露的 Zeus 惡意軟體原始程式碼的模組化木馬的後繼變種，於 2015 年左右首次出現在威脅環境中。在 2022 年 4 月的大執法掃蕩行動之後，Zloader 在將近兩年的時間裡都處於休養生息的狀態。現在，在網路上又發現新一波傳播 Zloader 的網路攻擊行動。該惡意程式載入器最新變種具有新增的強化功能，例如：支援 64 位版本的 Windows、導入動態網域產生演算法 (DGA) 或為網路通訊增加 RSA 加密功能。

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：

- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gen20
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A

- 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。

2024/01/21

鎖定Coinbase 用戶的網路釣魚行動

隨著加密貨幣不斷成為主流，賽門鐵克發現在電子郵件和行動領域，相關的網路釣魚行動都在穩定增加。

本篇防護公告論及一場正在進行中的主要在騙取美國 Coinbase 用戶的行動手機登入憑證的網路攻擊行動。Coinbase 是全球最受歡迎的加密貨幣交易所之一。

該簡訊試圖以虛構的無人認領獎金為誘餌引誘受害者，並提供一個惡意網址來申請獎金。如果用戶點擊該網址，就會進入一個偽造的 Coinbase 登錄頁面，該頁面只有在透過手機 APP 的瀏覽器瀏覽時才會出現。

觀察到惡意簡訊：

- Coinbase--您的帳戶上有 60 美元獎金無人認領。要領取獎金，請瀏覽我們的網站：hxxps[:]//id38-coinbase[.]com/connect

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。WebPulse 已知道此次活動中使用假冒的 Coinbase 域名。

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。

2024/01/21

GuLoader惡意程式載入器涉入的惡意電子郵件攻擊行動，最終會傳播Remcos遠端存取木馬(RAT)

最近觀察到一個 GuLoader 惡意程式載入器涉入的全球性惡意電子郵件攻擊行動，最終會傳播 Remcos 遠端存取木馬 (RAT)。拆解其攻擊鏈發現初始攻擊是以 zip 檔的電子郵件附件的形式傳送開始。壓縮檔內是第一階段的 GuLoader 腳本，並會執行第二階段的 Powershell 腳本。這反過來又會在第三階段啟動額外的 shell 程式碼。最終階段是下載 Remcos 遠端存取木馬 (RAT) 有效籌載並將其注入合法的 Windows 程序。

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.Guloader!gen1
- Trojan Horse
- Trojan.Gen.NPE

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。

2024/01/21

冒牌的Google Play商店上的APP助長Hydra惡意軟體的傳播

Hydra 的惡意活動屢見不鮮，它是安卓平台上熱門的銀行金融惡意軟體，近年來一直是行動裝置上相當棘手的全球性資安威脅。最近，賽門鐵克發現有人將 Hydra 偽裝成假冒的 Google Play 商店上的 APP 安裝檔 (Play_Store.apk)，其中大部分是透過偷渡式下載社交工程傳播。他們利用惡意網站進行傳播，但也有濫用 Discord 的情況。

Google Play 商店是一個廣受 Android 用戶信任的下載和安裝 APP 的平臺。透過將惡意軟體偽裝成官方商店，攻擊者利用用戶對合法來源的信任，使他們更有可能安裝惡意 APP。作為安卓生態系統的一個基本元件，使用者通常不會卸載或禁用它。透過將惡意軟體偽裝成這一重要元件，駭客的目的是在設備上持續常駐。

與大多數同類惡意軟體一樣，這款銀行金融惡意軟體透過注入和覆蓋來進行金融盜竊，但也能收集其他敏感性資料，例如：簡訊、連絡人和裝置資訊。

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。

- AdLibrary:Generisk
- Android.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。

2024/01/19

Brimstone(*硫磺)：俄羅斯間諜組織導入全新惡意軟體

國家級的俄羅斯 Brimstone 間諜組織 (又名 Coldriver、Callisto、TA446、Star Blizzard) 提高對烏克蘭和北大西洋公約組織國家的針對式攻擊。Brimstone 擴大攻擊的策略、技術和程序 (TTPs)，現在正採用 PDF 檔案內嵌 Spica 惡意軟體向目標投遞誘餌。Spica 是一個用 Rust 撰寫的後門程

式，當受害者要求取得被加密檔案的解鎖金鑰時該後門就會被發送。它隨後會常駐在受害者電腦上，並可以執行任意命令、下載檔案和外洩資料。

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：

- ACM.Untrst-RLsass!g1

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 Horse
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

2024/01/19

Dharma(*達摩)(又名 Crysis)勒索軟體活動仍在繼續鎖而不捨

Dharma 是 Crysis 惡意軟體家族中的勒索軟體，最初發現於 2016 年。雖然該惡意軟體家族相對比較久遠，但至今仍有新的變種在真實網路上危害。已知感染媒介通常是惡意垃圾郵件或濫用曝險的 RDP 伺服器。該惡意軟體會加密使用者的檔案，並根據不同勒索軟體變種冠上各種不同的副檔名。最近發現勒索軟體變種冠上的副檔名包括 .shiel、.avan、.AeR、.data、.intel、.tutu。

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：

- ACM.Ps-RgPst!g1
- ACM.Vss-DlShcp!g1
- SONAR.RansomCrys!g1
- SONAR.RansomCrys!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Crysis
- Ransom.Crysis!gm
- 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

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: Ransom.Crysis Activity 3

2024/01/19

Zephyr惡意挖礦軟體

最近觀察到一個傳播 Zephyr 惡意挖礦軟體的網路攻擊行動。該惡意軟體透過一個檔名為『WINDOWS_PY_M3U_EXPLOIT_2024』的 .7z 壓縮檔傳播。該壓縮檔內含惡意軟體的二進位檔案，並宣稱已竊得存有漏洞的 Windows 原始程式碼為幌子。壓縮檔包括一個 NSIS 安裝程式系統 (Nullsoft 可腳本安裝系統) 的安裝檔和兩個 JavaScript 檔。執行 .js 檔會觸發 AutoIt 的腳本，最後會部署最終的惡意挖礦程式。

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：

- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Schtsk!g1
- ACM.Wscr-Wscr!g1
- AGR.Terminate!g2
- SONAR.SuspDrop!g36
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen202
- 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.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：

- Web Attack: Webpulse Bad Reputation Domain Request

2024/01/19

Mimo惡意挖礦程式和Mimus勒索軟體在近期網路攻擊行動中相當活耀

Mimo (又名 Hezb) 惡意軟體是最近一些惡意挖礦攻擊行動的最終有效酬載。據報導，該惡意軟體的幕後主使者還在其他場合傳播過 Mimus 勒索軟體 (源於 MauriCrypt 原始程式碼)。眾所周知，Mimo 幕後主使者在其攻擊行動中廣泛開採濫用各種漏洞。他們開採濫用的漏洞包括 Log4Shell 漏洞 CVE-2021-44228、Atlassian Confluence 漏洞 CVE-2022-26134、WSO2 漏洞 CVE-2022-29464、Papercut 漏洞 CVE-2023-27350 以及最近的 Apache ActiveMQ 漏洞 CVE-2023-46604。

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：

- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!g1
- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader.Trojan
- ISB.Downloader!gen205
- Ransom.Crysis
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- 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
- 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：

- Attack: Apache ActiveMQ RCE CVE-2023-46604

- Attack: Log4j2 RCE CVE-2021-44228*
- Attack: WSO2 Unrestricted File Upload Vulnerability CVE-2022-29464
- Audit: Papercut NG CVE-2023-27350
- Web Attack: Atlassian OGNL Injection CVE-2022-26134
- Web Attack: Papercut NG CVE-2023-27350 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。

2024/01/19

伊朗駭客Sandstorm鎖定研究人員所發動的全新魚叉式網路釣魚行動

據報導，伊朗駭客 Sandstorm 最近鎖定研究人員和多所大學發動新一波的魚叉式網路釣魚攻擊行動。攻擊者接管或劫持遭入侵的真實電子郵件帳戶誘騙受害者下載惡意檔案，目的是竊取敏感性資料。值得注意的是，已觀察到一個被命名為 MediaPI 的全新客製化後門程式。該後門偽裝成 Windows Media Player 執行時會與 Sandstorm 所操控的命令與控制 (C&C) 伺服器進行加密連線，並取得 C&C 資訊並執行加密功能。

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 Horse
- Trojan.Gen.MBT
- 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。