保安資訊--本周(台灣時間2024/07/19)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 48 萬 1,600 台受保護端點上總共阻止了 5,070 萬次攻擊。這些攻擊中有 81.8% 在感染階段前就被有效阻止：**(2024/07/15)**

- 在**9萬700**台端點上，阻止了**1,200**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬7,700**台端點上，阻止了**920**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬4,000**台**Windows**伺服主機上，阻止了**104**萬次攻擊。
- 在**5萬7,600**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬700**台端點上，阻止了**68萬1,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,600**台端點上，阻止了**580**萬次嘗試利用的應用程式漏洞。
- 在**16萬3,400**台端點上，阻止了**430**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,800**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**10萬800**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**600**台端點上，阻止了**8萬7,000**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 10 萬 4,400 個受保護端點上阻止了總計 420 萬次攻擊。**(2024/07/15)**

- 使用網頁信譽情資，在 **95.8K** 個端點上阻止 **370** 萬次攻擊。
- 攔截 **20.1K** 個端點上 **348.4K** 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 **6.3K** 個端點上攔截 **62.1K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **206** 個端點上攔截 **7.2K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2024/07/18

ShadowRoot勒索軟體

威脅研究人員發現一種名為 ShadowRoot 的全新勒索軟體，其目標是土耳其的企業。此攻擊透過來自「internet[.]ru」網域的可疑電子郵件傳送 PDF 附件。如果使用者點擊 PDF 內的嵌入式連結，就會下載可執行的有效酬載，進而加密檔案。被加密檔案的副檔名已變更為「.shadowroot」。此勒索軟體正積極針對全球企業，包括醫療保健和線上零售業。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- 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：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.SmartInst
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!400

- 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。

2024/07/18

針對烏克蘭政府單位的網路釣魚惡意軟體行動與俄羅斯駭客組織：UNC4814有關聯

賽門鐵克發現針對烏克蘭政府單位的網路釣魚惡意軟體攻擊行動。根據攻擊媒介和行為，賽門鐵克認為 UNC4814(一個疑似與俄羅斯有關連的駭客組織) 涉嫌重大。此駭客組織透過傳送附有 HTA 檔案的網路釣魚電子郵件，偽裝成帳單和付款通知來發動攻擊。

觀察到電子郵件主旨：

- Оплата виконана.(*付款完成)
- Переказ вручено.(*轉帳已交付)
- Переказ сплачено.(*轉帳已支付)
- Перерахунок виконано.(*轉帳已完成)
- Перерахунок завершено.(*轉帳已完成)
- Рахунок розраховано.(*帳戶已結清)

開啟這些 HTA 檔案後，會觸發 SMOKELOADER 的下載和執行，這是一種在俄羅斯地下論壇中很熱門的下載工具。SMOKELOADER 主要功能是在受感染的機器上安裝更具破壞性的惡意軟體。此外，SMOKELOADER 還擁有資訊竊取能力，能夠從被廣泛使用的郵件用戶端、FTP 用戶端和其他常用程式中擷取密碼。惡意軟體會將這些竊取的資料傳送到攻擊者控制的命令與控制 (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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Mshta!g1
- ACM.Mshta-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g45

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

- ISB.Downloader!gen48
- ISB.Downloader!gen56
- WS.Malware.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。

2024/07/17

零時差漏洞：Windows平台存在的CVE-2024-38112漏洞已遭惡意.url檔案開採濫用

已觀察到針對 Windows 使用者的持續性攻擊行動。威脅者散佈的釣魚電子郵件包含副檔名為 .url 的 Windows Internet 捷徑檔案。這些檔案利用 MSHTML 的零時差漏洞 (CVE-2024-38112)。這些 .url 檔案偽裝成 PDF 文件的連結，利用「mhtml」手法啟動過時和終止支援的 Internet Explorer (IE) 版本。這個動作會將用戶重導向到由威脅者操控的網址，該網頁被設計用來下載並執行惡意 .hta 檔案。此檔案可能有助於遠端執行程式碼 (RCE)。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，DCS 可以對 Microsoft Internet Explorer 的預設強化提供針對 CVE-2024-38112 的零時差防護。預設強化政策會封鎖所有向外連線。套用於 Microsoft IE 的 DCS 沙箱可防止下載任何惡意有效酬載或執行任意程序。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。

2024/07/18

Killer Ultra(*終極殺手)惡意軟體

研究人員最近發現一種涉入 Qilin 勒索軟體攻擊的駭客工具，稱為「Killer Ultra」。它會停用端點偵測與回應 (EDR) 和防毒 (AV) 工具，並使用 Zemana 驅動程式終止這些工具的程序。此外，Killer Ultra 會清除所有 Windows 事件日誌，以隱藏其行動。該惡意軟體還包括典型後期攻擊工具的隱匿功能，顯示未來可能透過 C&C 通道下載和執行工具。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDrop!g86

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Dropper!g7

基於機器學習的防禦技術：

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

2024/07/17

Noxious(*有害；有毒；敗壞道德)惡意竊密程式

研究人員最近發現一款名為 Noxious 全新惡意竊密程式。這個以 Python 為基礎的開放原始碼工具目前上架在 GitHub 上，擁有多項功能，例如：收集敏感的使用者資料，包括帳單詳細資料、電子郵件、電話號碼、tokens 以及 Cookie、瀏覽歷史和 WiFi 密碼等系統資訊。此外，它還可以收集 IP 位址和地理資料，並具有擷取加密貨幣錢包資訊的能力。此惡意竊密程式似乎仍在進行增強工作，以擴大其功能。

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：

- PUA.Gen.2
- Trojan Horse
- WS.Malware.2
- WS.Reputation.1
- WS.SecurityRisk.3

2024/07/17

精心製作的HTML檔案巧妙地濫用Windows搜尋功能

最近發現有攻擊者濫用 Windows 搜尋功能，將使用者重導向至惡意軟體。此攻擊會先傳送含有精心製作 HTML 檔案的惡意垃圾郵件給目標對象，這些檔案是設計來濫用內建的 Windows 搜尋功能，一旦這些檔案被開啟，就會重新導向到外部託管的網站，下載攻擊者所操弄的惡意軟體。

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：

- Phish.Html
- Scr.Malcode!gen

2024/07/17

Jenkings Script Consolec被利用於加密貨幣挖礦

配置不當的 Jenkins Script Console 實例 (例如：Jenkins Groovy 外掛) 已被攻擊者利用來進行網路犯罪活動，例如：部署加密貨幣挖礦並收集敏感資訊的後門。利用配置錯誤／不當的伺服器和未修補的版本並非新手法。為了防範這類攻擊意圖，一般建議確保正確的組態、執行強大的驗證和授權，以及進行定期稽核。在這種情況下，也建議限制 Jenkins 伺服器從網際網路公開存取。

網路知識：Jenkins 是個（提供）自動化的伺服器，可用來將各種關於 building、測試、發佈、部署軟體的工作自動化。

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：

- PUA.Gen.2
- 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。

2024/07/17
冒充Afrihost ISP服務商的網路釣魚活動

Afrihost 是南非的一家網際網路服務供應商 (ISP)，提供 ADSL 寬頻、無線、行動服務和網站主機等服務。最近，賽門鐵克發現冒充 Afrihost 服務的網路釣魚行動。這些行動涉及偽造的通知郵件，提醒收件人更新付款方式以避免服務中斷。

電子郵件本文提到，用戶需要更新他們的付款方式，以繼續使用 Afrihost 的服務而不會中斷。該電子郵件包括一個偽裝成「更新付款方式」鏈接的釣魚網址，意圖引誘用戶點擊並提交他們的憑證／帳密。

電子郵件主旨：Update Your Payment Method to Avoid Service Disruption
(*更新您的付款方式以避免服務中斷)
電子郵件來自：Afrihost <偽造的郵件地址>

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。

2024/07/17
CVE-2024-36401：GeoServer存在高風險安全漏洞

CVE-2024-36401 (CVSS 風險評分：9.8) 是存在 GeoServer GeoTools 的安全性漏洞，有證據顯示已被大肆開採濫用。GeoServer 是以 Java 撰寫的開放原始碼軟體伺服器，可讓使用者分享及編輯地理位置資料。由於以 XPath 表達式評估屬性名稱不安全，此漏洞可讓未認證使用者透過特定輸入針對預設的 GeoServer 安裝執行遠端程式碼。賽門鐵克端點防護／安全解決方案的網路層防護技術入侵防護系統 (IPS) 可阻止利用此漏洞的嘗試，進而防止系統受到進一步感染或損害。

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: GeoServer RCE Vulnerability CVE-2024-36401
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 2

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，DCS UNIX 強化保護政策可設定成停用反向連線、允許已建立的相關連線，並只允許 DNS、HTTP 和 HTTPS 等必要的出埠流量。客戶也應停用 WFS 請求，直到將 GeoServer 升級至已修補的版本。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/16
偽裝成MS Office破解版的惡意軟體

威脅研究人員發現偽裝成 MS Office 破解版的惡意軟體。它透過下載和 torrent 分享機制進行傳播，使攻擊者能夠透過更新來控制受感染的系統。惡意軟體會根據 V3 安全軟體的存在調整安裝方法。它使用工作排程器以維持常駐功能，確保即使被偵測到也能保持隨時可下手的狀態。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Ps-Masq!g1
- ACM.Ps-Reg!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g303

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen221
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!500

2024/07/16
防護亮點：QR Code詐騙呈上升趨勢，SEP Mobile提供最先進的防護能力

QR Code 已經成為人們的日常生活

根據維基百科解釋，QR 或「Quick-Response」code 是一種二維矩陣條碼，由日本公司 Denso Wave 於 1994 年發明，用於標示汽車零件。儘管 QR Code 的效用顯而易見，但直到 2010 年左右，第一款在智慧型手機平台上所推出 QR Code 掃描器和閱讀器誕生之後，QR Code 才被介紹給普羅大眾，手機的相機讓讀取 QR Code 變得非常方便和容易。但同樣地，儘管 QR Code 很有用，卻很快被冷落了。

新冠疫情推了 QR Code 一把

QR Code 現在已經融入全球許多國家日常生活中，成為不可或缺的一部分。在 COVID-19 大流行期間，QR Code 使用量激增，增進非接觸式交易和資訊分享。以法國為例，QR 碼在以下方面非常普遍：

- **COVID-19 健康通行證**：用於顯示疫苗接種證明或陰性測試結果。
- **餐廳點餐**：數位菜單減少實體接觸。
- **支付系統**：行動支付與銀行交易。
- **公共運輸**：票務與即時資訊。
- **廣告與資訊**：即時存取網站和促銷活動。

新興威脅

QR Code 普遍使用不可避免地導致網路犯罪活動增加。常見的手法包括：

- **釣魚網站**：惡意 QR Code 會將使用者重新導向釣魚網站，以竊取憑證和個人資訊。
- **惡意軟體散佈**：掃描惡意 QR Code 可將惡意軟體下載到使用者的裝置上。
- **付款詐騙**：假冒的 QR Code 會將使用者導向詐騙付款入口網站。
- **收集憑證**：QR Code 會誘導使用者進入假冒的登入頁面以騙取使用者帳號和密碼。

法國執法單位於 2024 年 1 月發表文章，警告讀者提防 QR Code 詐騙，並提到法國有超過 800 宗涉及 QR Code 的刑事訴訟正在進行中。您可以在此閱讀英文版本。

受害者理論與犯罪剖繪

消費者是主要的目標，尤其是遊客。由於不熟悉當地的安全措施、語言障礙以及無法使用常用的安全工具，遊客特別容易受到傷害。他們經常會分心，降低對潛在詐欺的警覺性。例如：我們預期 QR code 詐騙會在巴黎奧運期間激增，因為大型的國際活動會吸引許多遊客，創造一個容易被利用的環境。大量遊客的湧入、數位交易的增加，以及對 QR code 的依賴，為網路罪犯提供更大的攻擊面。

但這個重責大任不只由法國來承擔。美國聯邦貿易委員會 (Federal Trade Commission，FTC) 於去年 12 月發出消費者警示，警告 QR code 詐欺的危險。這個問題也不只限於消費者。由於遠端工作和數位交易的增加，企業使用者也越來越受到影響，擴大網路罪犯的攻擊面。

最有效的防護方案

SEP Mobile 使用者可透過網路防護與行動威脅防護 (MTD) 的多層次防護，抵禦惡意 QR code的攻擊。當使用者被誘騙瀏覽嵌入 QR code 的惡意連結時，網路防護會識別後續衍生的攻擊。與防範簡訊 (SMS) 類的網路釣魚攻擊類似，網路防護使用賽門鐵克 WebPulse 的網頁 (URL) 信譽，可辨識可疑連線並阻斷攻擊鏈。行動威脅防護工具結合弱點管理、異常偵測、行為分析、程式碼模擬、入侵防護、主機防火牆和傳輸安全技術，以防護行動裝置和應用程式受到包括 QR code 詐騙在內的各種進階威脅。

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。
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。

2024/07/16
Android惡意軟體中使用BadPack手法

BadPack 是一種在針對 Android 行動裝置的惡意軟體中觀察到之手法。BadPack 的作者會篡改安卓 APP 安裝套件檔 .APK 檔案格式的標頭資訊，進而有效地破壞檔案，防止手動分析。由於與 APK 檔案格式相關的規則不太嚴格，這種修改不會影響 Android 作業系統，因此惡意軟體可以成功安裝。這種竄改檔案表頭的手法曾在多種 Android 銀行木馬程式中出現。Palo Alto Networks 的研究人員發表一份有關 BadPack 更深入的報告。

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
- AppRisk:Generisk
- Other:Android.Reputation.1

2024/07/15

透過非官方的韓國HTS(Home Trading System)電子交易系統傳播的Quasar遠端存取木馬(RAT)

威脅研究人員發現 Quasar 遠端存取木馬 (RAT) 透過非官方的 Home Trading System(HTS) 散佈，而 Home Trading System 是一種可讓投資人從自己個人電腦進行交易的工具。然而，這些攻擊中使用的 HTS(又名 HPlus) 無法搜尋，其供應商也仍然不明。據推測，攻擊者使用的 HPlus HTS 是透過未經授權的金融投資單位安裝。Quasar RAT 一旦安裝，攻擊者就能遠端控制受攻擊的系統，進行資料竊取和其他惡意活動。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Msbuild!g1
- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.2

基於機器學習的防禦技術：

- Heur.AdvML.B!100
- 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。

2024/07/15
惡意Word文件檔傳播惡意竊密程式

一起持續進行中的攻擊行動，揭露一種初始階段透過 Word 文件檔散佈的惡意竊密程式。此惡意竊密程式會感染電腦、擷取裝置的 IP 位址，然後將使用者的瀏覽器資訊傳送至攻擊者專用的指揮與控制 (C&C) 伺服器，並針對不同國家自訂資料。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- W97M.Downloader
- WS.Malware.1
- WS.Malware.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。

2024/07/15
CVE-2024-36991--Splunk Enterprise中的路徑遍歷漏洞

CVE-2024-36991(CVSS 風險評分：7.5) 是 Splunk Enterprise 中一個路徑遍歷漏洞，Splunk Enterprise 是一個大數據平臺，可簡化收集和管理大量機器產生資料的作業，協助企業從這些資料中獲得可識別的資訊。此問題特別影響安裝在 Windows 上的 Splunk Enterprise 。該漏洞影響 9.2.2、9.1.5 和 9.0.10 以下的所有版本。成功開採濫用該漏洞後，未經認證的遠端攻擊者可從伺服器檔案系統上的任意檔中讀取敏感資訊。賽門鐵克端點防護的網路層防護技術入侵防護系統 (IPS) 可阻止嘗試利用這個漏洞，進而防止系統受到進一步感染或損害。

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: Splunk Enterprise Path Traversal Vulnerability CVE-2024-36991

基於安全強化政策(適用於使用DCS)：

針對 Splunk Enterprise 應用程式的 DCS 強化可透過多種不同方式減少攻擊面和暴露：

- 鎖定 Splunk Enterprise 的網路暴露，使 Splunk Enterprise 的此漏洞或類似遠端漏洞無法透過網際網路被利用。
- 防止存取底層作業系統上的作業系統關鍵檔案，進而防止敏感系統資訊洩漏。
- 防止任意程式碼執行，以防止惡意子程序譜系。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/15

Poco RAT涉入針對西班牙語系使用者的網路釣魚行動

自 2024 年初以來，一個持續進行中的網路釣魚行動，一直以西班牙語系的使用者為目標，傳播一種名為 Poco RAT 新型遠端存取木馬 (RAT)。該惡意軟體主要針對採礦業者、製造業和酒店業。它的反分析、C&C 通訊和檔案執行的功能讓人眼睛一亮。此外，Poco RAT 還能根據地理位置提供具有惡意竊密程式的有效酬載。作為其攻擊媒介的一部分，它採用以金融為主題的網路釣魚電子郵件，並利用 Google Drive 等合法服務來上架惡意軟體有效酬載，企圖逃避檢測。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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
- Machine Learning-based

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

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。

2024/07/14

CRYSTALRAY駭客組織持續利用網路映射工具：SSH-Snake發動攻擊行動

自 2024 年 2 月以來，研究人員一直在追蹤不斷演變的 CRYSTALRAY 駭客組織。據觀察，該駭客組織濫用一種名為 SSH-Snake 的網路映射工具，這是一種可自我修改的蠕蟲惡意軟體，它濫用遭入侵系統上的 SSH 憑證在網路中傳播。CRYSTALRAY 變本加厲，利用各種開源安全工具進行大規模掃描、漏洞開採濫用和部署後門，導致受害者數量不斷增加。

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：

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

2024/07/12

OilAlpha惡意竊密程式以葉門講阿拉伯語的非政府人道主義組織為目標

OilAlpha 持續對講阿拉伯語的單位以及對在葉門運作的人道主義組織和非政府組織感興趣的人為目標。據報導，使用者被誘騙到一個欺騙性的入口網站，該網站模仿 CARE International (國際關懷協會) 和 Norwegian Refugee Council (挪威難民理事會) 等人道主義組織常見的登錄介面，目的是竊取憑證。

潛在用戶似乎是透過 WhatsApp 直接聯繫到他們，並誘使他們下載被注入 SpyMax 等遠端存取木馬的欺騙性安卓 APP。這種惡意軟體能夠存取和收集照片、檔案、位置資料、連絡人、簡訊和通話記錄、管理麥克風、捉取影片和存取 WiFi。

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

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。

2024/07/11

假冒服裝零售商品牌APP的攻擊行動，實則散播Vultur銀行金融惡意軟體

各種類型的品牌不斷被網路犯罪分子濫用，以針對特定人群，而金融機構通常是最多被冒充。然而，其他類型的行業也無一倖免。最近一家名為『Terraces Menswear』的服裝零售商 (專門為男士和青少年設計高檔服裝) 品牌就遭到網路犯罪份子的濫用。

網路犯罪份子將 Vultur 銀行金融惡意軟體偽裝成一個假冒 Terraces Menswear 推出安卓平台的 APP 安裝套件檔 (TerracesMenswear.apk)。該惡意軟體利用堆疊技術，顯示假的堆疊視窗，企圖誘騙使用者輸入銀行憑證。它的目標是數百家銀行和加密貨幣交換平臺。

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。

- AppRisk:Generisk

2024/07/11

全新惡意程式載入器：DodgeBox正幫MoonWalk後門程式，推波助瀾

威脅研究人員最近發現一個名為 DodgeBox 的全新惡意程式載入器。該惡意程式載入器與 StealthVector 有顯著的共同特徵，後者與中國進階持續威脅 (APT) 駭客組織 APT41／Earth Baku 有關。DodgeBox 被用於載入全新後門程式：MoonWalk ，該後門程式採用諸如堆疊欺騙、DLL 側載 (sideloading)、DLL 挖空 (hollowing) 和環境護欄 (environmental guardrails) 等規避技術，與 DodgeBox 類似，它也利用 Google Drive 進行 C&C 操作。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Coinminer
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/07/11

輕信稅務相關誘餌，烏茲別克共和國的手機／行動裝置使用者正遭受安卓平台上的惡意軟體侵擾

稅務相關的誘餌很容易讓受害者上鉤，在世界各地稅務相關的詐騙 (包括消費者和企業) 一直以來總是名列前茅的社交工程伎倆，初始在其機器上部署惡意軟體、後續會陷入商務郵件詐騙 (BEC) 的圈套並向釣魚網站輸入敏感性資料等。

賽門鐵克在最近一個案例 (眾多案例中的一個) 中發現，一個惡意團體或個人針對烏茲別克共和國的手機／行動裝置使用者發佈與稅務相關的虛假 APP 安裝套建檔 (例如：ИловасиСолик.apk、ЯнгиСолик.apk、СоликЗудлик.apk 等)，這些 APP 可能宣稱用於為烏茲別克的個人和企業報稅、檢查稅務狀況、繳稅或瀏覽查閱稅務相關資訊。實際上，用戶最終安裝的 APP 主要用於竊取簡訊和其他敏感資訊的安卓惡意軟體。

一種以簡訊為目標的安卓惡意軟體，可攔截銀行的一次性密碼和驗證碼，導致未經授權的帳戶被存取和交易，進而造成嚴重的金融詐騙。還可能導致身份盜用、機密通訊洩露以及各種服務的驗證過程中斷。

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。

- AppRisk:Generisk

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。