保安資訊--本周(台灣時間2024/03/15)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 55 萬 5,800 台受保護端點上總共阻止了 5,700 萬次攻擊。這些攻擊中有 84.4% 在感染階段前就被有效阻止：**(2024/03/11)**

- 在**11萬3,300**台端點上，阻止了**1,890萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬8,900**台端點上，阻止了**1,200萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,000**台**Windows**伺服主機上，阻止了**9,400萬**次攻擊。
- 在**6萬5,400**台端點上，阻止了**200萬**次嘗試掃描伺服器漏洞。
- 在**1萬4,900**台端點上，阻止了**90萬5,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬6,400**台端點上，阻止了**140萬**次嘗試利用的應用程式漏洞。
- 在**21萬2,100**台端點上，阻止了**480萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6萬8,000**台端點上，阻止了**130萬**次加密貨幣挖礦攻擊。
- 在**10萬5,800**台端點上，阻止了**760萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**590**台端點上，阻止了**6萬1,200**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。

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 15.39 萬個受保護端點上阻止了總計 620 萬次攻擊。**(2024/03/11)**

- 使用網頁信譽情資，在 **138.1K** 個端點上阻止 **540** 萬次攻擊。
- 攔截 **33K** 個端點上 **608.1K** 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 **12.4K** 個端點上攔截 **121.4K** 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 **450** 個端點上攔截 **30.9K** 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。

2024/03/14

FakeBat惡意軟體正透過惡意廣告傳播

最近，一個惡意廣告行動借助 MSIX 安裝檔傳播 FakeBat 惡意軟體。他們冒充各種知名品牌的軟體，例如：Notion、Trello、Braavos 或 OneNote，誘使受害者下載惡意安裝檔。其中一些惡意廣告使用短網址的偽裝來隱藏惡意網域，以便向潛在受害者傳遞惡意網域。傳送給用戶的 MSIX 檔包含經過混淆的 PowerShell 腳本，進而導致惡意軟體感染。

保安補充:MSIX 是一種 Windows 應用程式套件格式，結合了 MSI、.appx、App-V 和 ClickOnce 的最佳功能，以提供現代化且可靠的封裝體驗。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- 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.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。

2024/03/13

假冒Adobe Reader安裝程式的惡意竊密程式

近期一份報告詳細描述攻擊者是如何在傳送 PDF 檔時，提示用戶下載並執行 Adobe Reader 安裝程式以讀取 PDF 內容。實際上，受害者會在不知情的情況下安裝一個惡意竊密程式。

惡意竊密程式的目的在從受害者機器上收集敏感性資料和系統資訊，並將其轉發回攻擊者的 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Pidief
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/03/13

Payuranson／Payuransom--Skynet(*天網)勒索軟體的最新變種

Payuranson／Payuransom 是 Skynet 勒索軟體家族的最新變種。該惡意軟體會加密使用者檔案，並冠上 .payuranson 或 .payuransom 副檔名。被攻擊的機器上會出現一個勒索贖金支付說明檔，通常檔名為 SkynetData.txt 或 ReadMeForDecrypt.txt。勒索者要求用比特幣支付，並以電子郵件和 Telegram 即時通訊等方式提供詳細聯繫資訊。該勒索軟體具有刪除受感染端點的磁碟備份功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspDrop!gen1

- SONAR.TCP!gen1

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

2024/03/13

CVE-2024-1071--WordPress Ultimate Member外掛程式漏洞

CVE-2024-1071 是一個最近披露的 SQL 注入漏洞，影響 WordPress Ultimate Member Plugin 2.1.3 至 2.8.2 版本。若成功開採濫用該漏洞可讓未經認證的攻擊者在現有的 SQL 查詢中附加額外的 SQL 查詢，進而可能導致從資料庫中擷取敏感性資料。該漏洞已被證實在真實網路情境被開採濫用，供應商已發佈 2.8.3 修補版本以降低風險。

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：

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: WordPress Ultimate Member Plugin CVE-2024-1071

2024/03/13

Agent Tesla惡意竊密程式行動著眼於法國、西班牙、土耳其和北非

Agent Tesla(一種基於 .NET 的惡意竊密程式) 正被多個攻擊者傳播到全球各地的企業，這些攻擊者的目地各不相同，包括經濟利益、商業間諜、勒索軟體要脅等。我們每天都會攔截到一些網路攻擊行動，例如：一個針對法國和北非公司的行動。犯罪者假扮成摩洛哥一家專門從事服裝製造和出口的公司。

惡意郵件的主旨是『AVIS DE VIREMENT』，包含一個 .BZ 壓縮檔(Avis_Virement1502002024.bz)。在此檔中，Agent Tesla 將自己偽裝成一份假冒檔案或資金轉帳通知(Avis_Virement1502002024.exe)。這是一種常見的社交工程伎倆，已經行之多年，但仍然有效。

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)。

基於行為偵測技術(SONAR)的防護：

- SONAR.Trafic2.RGC!g16

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

2024/03/12

Meow(*喵)勒索軟體

Meow勒索軟體，早在 2022 年就被報導過，它是源於同年遭洩露的 Conti 勒索軟體原始程式碼的後繼改良版本。該勒索軟體幕後的威脅者在沉寂幾個月後於今年再捲土重來，據報導，迄今為止共有九名受害者。

該勒索軟體會加密各種類型的檔案，並冠上 .MEOW 的副檔名。攻擊者習慣讓受害者透過電子郵件或 Telegram 與檔名為『readme.txt』的贖金支付說明中提到的帳號來進行互動溝通。

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.RansomPlay!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Conti!gen4
- Ransom.Conti!gen10
- Ransom.Conti!gen12
- Ransom.Generic.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

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

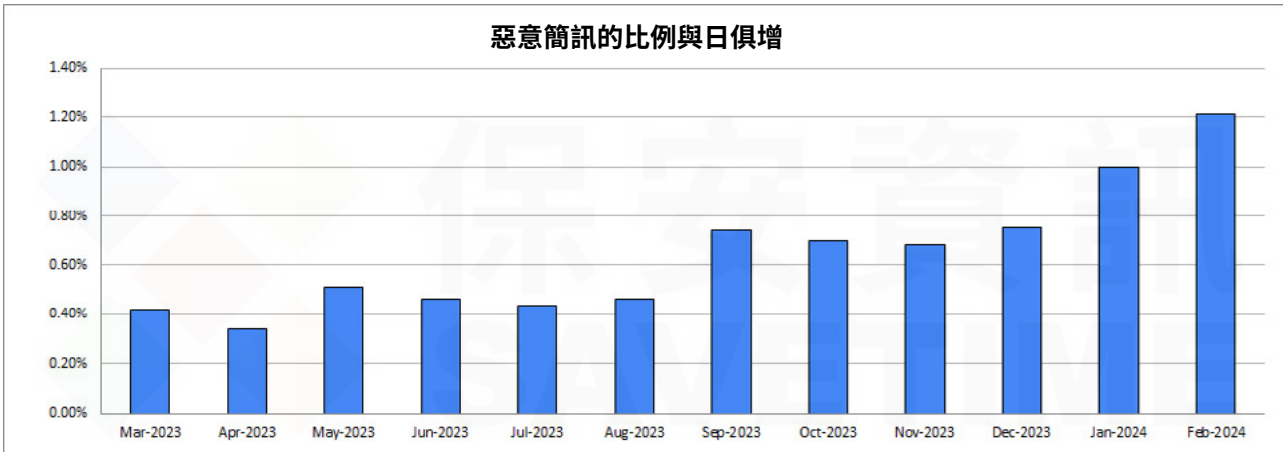
2024/03/12
防護亮點：行動裝置網路釣魚攻擊持續上升

行動裝置網路釣魚攻擊:上升趨勢和當務之急的解決方案

在當前的威脅環境中，行動裝置防護一直以來就是資安領域關注的焦點之一。儘管業界做出努力，但簡訊網路釣魚攻擊仍在繼續擴散。聯邦通訊委員會和 T-Mobile 等運商，最近在 2024 年打擊詐騙簡訊的行動顯然還不夠。我們的分析顯示一個令人擔憂的趨勢：惡意簡訊網路釣魚攻擊不僅普遍存在，而且呈上升趨勢。

驚悚的數字

2024 年 2 月，我們對數以百萬計的簡訊進行細緻分析，特別關注潛在的惡意網址 (URL)。令人震驚的是，每 1,000 則簡訊中就有 12 條 (1.21%) 被歸類為惡意簡訊釣魚攻擊。這比前一年增加了 105%，比 2024 年 1 月增加了 22%，增幅驚人。



令人擔憂的現實

行動裝置的使用環境面臨著持續進化的威脅：攻擊者現在透過建立幾可亂真的假冒身份驗證網站來誘騙員工。他們的目標是什麼？騙取有價值的憑證和多重身份驗證 (MFA) 的驗證碼。攻擊鏈通常由發送到員工行動裝置的簡訊釣魚資訊開始。該資訊包含一個導向 Okta 驗證登錄頁面的連結，誘使使用者輸入他們的帳戶憑證和 MFA 驗證碼。

我們的觀察結果顯示，有多種攻擊以組織內的使用者為目標。我們主動掃描簡訊中的惡意網址，並及時提醒使用者注意潛在的有害內容。此外，我們還發現透過像 WhatsApp 等其他傳播管道進行的憑證釣魚詐騙攻擊。

解決方案建議：Symantec Mobile Threat Defense(簡稱MTD：賽門鐵克行動裝置威脅防禦)

當企業行動管理 (EMM) 本身存在不足時，Symantec Mobile Threat Defense 系統就會介入。根據賽門鐵克透過 WebPulse 的威脅情資嚴格檢查簡訊中發現的網址，MTD 可提供及時、強大的保護，有效攔截使用者在行動裝置上瀏覽釣魚網站。MTD 行動果斷，從一開始就阻斷攻擊鏈，使用戶免受這些惡意簡訊釣魚企圖的攻擊。

欲深入瞭解有關賽門鐵克更多有關惡意簡訊偵測和防護的資訊，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。
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。

2024/03/12

CryptoWire 勒索軟體

CryptoWire 是一種勒索軟體，最初在 2018 年被發現。雖然該勒索軟體在過去幾年中並不特別活躍，但就在最近，在真實網路情境觀察到一起全新的傳播行動。該惡意軟體具有加密本機和網路磁碟、USB 隨身碟或任何外部連接磁碟上的檔案的功能。CryptoWire 會在被加密檔中添加『.encrypted』字串，並以快顯視窗顯示贖金支付說明。對於這類惡意軟體來說，非常不尋常是，報告中的變種會將解密金鑰設置在送回 C&C 伺服器的流量中或使用的自動操作 Windows 應用程式的 Autoit 腳本中。

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-Schtsk!g1
- ACM.Untrst-Rgpst!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransom!gen14
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g340
- SONAR.SuspReg!gen49

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Cryptolocker
- Scr.Malcode!gen
- Trojan.Gen.9
- Trojan.Gen.MBT
- Web.Reputation.1
- 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

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：

- Audit: Bad Reputation Application Activity
- 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。

2024/03/12

NarniaRAT遠端存取木馬和Fenix殭屍網路，在針對拉丁美洲的網路攻擊行動中傳播

在最近一次針對拉丁美洲用戶的網路攻擊行動中，NarniaRAT 遠端存取木馬和 Fenix 殭屍網路作為兩個單獨的有效籌載被傳播。該行動傳播偽裝成合法工具的惡意 .zip 壓縮檔。注入有效籌載可用於資訊竊取、鍵盤側錄和資料萃取 (Data extraction)，大多是圍繞著銀行相關資料。該惡意軟體目標是外洩與在拉丁美洲國家營運的多家知名銀行相關資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

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.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。

2024/03/12

打死不退的Swallowtail(*燕尾服)進階持續威脅(APT)駭客組織

Swallowtail (也稱Fancy Bear、Forrest Blizzard 或 ITG05) 是一支國家支援的進階持續威脅 (APT) 駭客組織，以攻擊全球政府和非政府組織而聞名。最近由 Swallowtail 發起的網路攻擊行動濫用 Masepie 和 OceanMap 後門以及基於 Powershell 惡意竊密程式：SteelHook。所有叫得出名的惡意軟體都曾被該駭客組織使用過。初始攻擊採用各個領域的熱門話題為誘餌的網路釣魚。據觀察，該駭客組織還濫用免費託管平臺來上架管惡意有效籌載，並在攻擊中利用 WebDAV 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.Untrst-FlPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!500

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。

2024/03/12

漏洞開採濫用成為勒索軟體的主要攻擊媒介

勒索軟體業者不斷發展戰術，以因應惡意軟體傳播管道遭執法單位的中斷。博通公司旗下的賽門鐵克威脅獵手團隊匯整有關從殭屍網路到漏洞開採濫用作為主要感染途徑明顯變化的詳細資訊。最近觀察到針對影響 Exchange 伺服器、IT 客服支援軟體、VPN 和應用服務傳遞控制器 (Application Delivery Controller，ADC) 的漏洞的攻擊。

在我們的部落格文章有更詳細內容：「勒索軟體攻擊持續增加：威脅業者不斷因應反制中斷，隨機應變。」

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

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Trojan.Gen.MBT
- Trojan.Stealbit

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

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: Citrix NetScaler CVE-2023-4966
- Web Attack: Zoho Manageengine RCE Vulnerability CVE-2022-47966

2024/03/12

在羅馬尼亞和莫爾達瓦發現Remcos遠端存取木馬(RAT)

Remcos 遠端存取木馬 (RAT) 似乎無處不在，幾乎在常見的網路攻擊行動中都可以發現它的跡象。在本公報中，我們將介紹一個案例，該案例中的攻擊者鎖定在羅馬尼亞、莫爾達瓦和周邊國家。最近這次行動的幕後黑手將自己塑造是一家羅馬尼亞的專門生產機台的工業設備供應商。

向該地區公司行號發送的惡意電子郵件 (主旨：Comandă nouă) 利用『產品訂單』社交工程伎倆。附件是一個 ZIP 壓縮檔 (Noua lista de comenzi.zip)，其中包含冒充命令列表的 Remcos 二進位檔案 (Noua lista de comenzi.exe)。

Remcos 遠端存取木馬 (RAT) 的功能強大，包含資料盜竊、系統入侵、營運中斷、間諜活動、信譽受損以及法律和合規問題，進而嚴重影響公司。它能夠遠端存取被入侵的系統，使攻擊者能夠進行各種惡意活動，導致經濟損失、營運中斷、法律後果和信譽受損。

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)。

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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：

- Audit: Bad Reputation Application Activity

2024/03/11

Magnet Goblin駭客組織鎖定Ivanti公司旗下的Connect Secure VPN使用者為目標

據報導，Magnet Goblin 駭客組織鎖定 Ivanti 公司旗下的Connect Secure VPN 使用者為目標，發起一場惡意軟體攻勢。該行動部署基於 Linux 的惡意軟體 NerbianRAT 遠端存取木馬和 WARPWIRE 惡意竊密程式。Magnet Goblin 專門利用提供網際網路服務電腦中的一日漏洞 (1-day: 漏洞被揭露的當天還來不及安裝修補程式就發動攻擊)，這次他們利用 Ivanti Connect Secure Web 元件中的命令注入漏洞 (CVE-2024-21887)。

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：

- Hacktool.Ligolo
- Trojan.Gen.NPE
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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：

- Web Attack: Ivanti ICS CVE-2023-46805
- Web Attack: Ivanti ICS CVE-2024-21887

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。

2024/03/11

個人隱私的勒索威脅：假冒的約會APP以法國和土耳其使用者為目標

長期以來，遠端存取木馬 (RAT) 一直被認為是網路犯罪份子彈藥庫中威力強大的工具，經常被用來發動金融盜竊和間諜活動。然而，它們的應用範圍並不僅僅局限於金錢利益。近來，許多攻擊者利用 RAT 精心策劃複雜的勒索活動，利用個人隱私中的漏洞進行勒索。

賽門鐵克發現一個從二月中旬開始的網路攻擊行動，在這個行動中，攻擊者試圖用一個模仿鮮為人知的約會服務的假約會 APP 來引誘法國和土耳其的手機／行動裝置用戶。該惡意應用程式沒有上架在 Google Play 上，而是上架在一個惡意網站上，該網站的站名與被冒充的正統約會服務名稱相似，但使用不同的頂級網域 (TLD)。使用者會透過網路搜尋或點擊簡訊內文的網址

進入惡意網站和下載 APP。他們最終看到的不是約會 APP，而是 SpyNote，這是一種惡名昭章的遠端存取木馬，被全球多個駭客團體和個體戶所侵人使用。

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：

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 已知道此次攻擊行動中使用假冒或誤植的域名。

- 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。

2024/03/11

Duralock勒索軟體

DuraLock 是又一個進入勒索軟體威脅領域的攻擊者。根據被投放的贖金支付說明 (HOW_TO_BACK_FILES.html)，他們採用雙重勒索戰術。他們要脅受害者在 72 小時內支付贖金，否則將提高價格；如果不支付贖金，他們還威脅要洩露或轉售竊取的資料。成功入侵後，被加密檔將被冠上 .duralock05 副檔名。

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.SuspReg!gen47
- SONAR.SuspReg!gen48

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2024/03/10

FakeBank安卓惡意軟體：鎖定設有國外分行的伊朗銀行為目標

FakeBank 是安卓平台常見的惡意軟體，目的在竊取行動裝置使用者與金融機構相關的敏感性資料。其技術包括偽造登入畫面、來電轉接 (又稱語音釣魚攻擊) 和簡訊窺探。這些惡意軟體已在行動威脅領域存在多年，其猖獗程度可見一般。

在最近的一個案例中，賽門鐵克觀察到一個假冒銀行的駭客以伊朗最大的商業銀行的客戶為目標，該銀行在歐洲、中東和中亞等地都設有國際分行。惡意 APP(可能透過惡意簡訊傳送) 被

偽裝成受害銀行的官方 APP。它被上架在惡意網站上，駭客申請與正牌網站很相似的網站名稱 (如誤植或拼字錯誤)，讓用戶不疑有他就上鉤了。

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 已知道此次攻擊行動中使用假冒或誤植的域名。

- AppRisk:Generisk

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。

2024/03/10

偽造由美國最大加密貨幣交易平臺Coinbase所發行的電子錢包APP，爽撈憑證

賽門鐵克最近觀察到，有網路惡棍用安卓平台上的惡意 APP(CoinbaseWallet.apk) 冒充事由美國最大加密貨幣交易平臺 -- Coinbase 所發行的 app，以 Coinbase 的使用者為目標，詐騙他們的憑證。

如果受害者被成功誘騙下載並在設備上安裝偽造的 APP，系統就會提示他們登錄，這時 APP 就會收集他們的憑證。

該惡意軟體上架在一個仿效 Coinbase 的網站上，其網站名稱與著名的加密貨幣交換平臺相似。雖然未經證實，但我們認為用戶是透過惡意簡訊被重導向到該網站。

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。WebPulse 已知道此次攻擊行動中使用假冒或誤植的域名。

- 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。

2024/03/10

Zarik勒索軟體：要求透過Boosty平台支付20美元作為解密的贖金

另一個勒索軟體攻擊者一直使用各種 Chaos 勒索軟體後繼新變種來鎖定個別電腦。不幸被加密後，投放的贖金支付說明會建議受害者在俄羅斯內容訂閱平臺 Boosty 上支付 20 美元以作為解密的贖金。在俄羅斯、荷蘭和烏克蘭都發現此類活動。瀏覽網頁的偷渡式下載是主要的感染途徑，其惡意二進位檔案被偽裝成 Photoshop 等破解軟體。

保安網路知識補充：Boosty 是一個創意平台，受歡迎的作家、遊戲玩家、博主、音樂家、作家、藝術家、主播和其他創意人士可以在這裡與他們的粉絲分享獨特的內容。在 Boosty 上，您可以找到流媒體廣播的錄音、來自博主和遊戲玩家的內容、藝術家作品集、音樂家的作品和作家的部落客。發現來自流行作者的獨家內容和同人圈！

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-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

2024/03/10

偽裝成 Dork 工具的CyberGate 遠端存取木馬(RAT)

最近一個攻擊者將遠端存取木馬偽裝成可下載 Dork 轉換器工具的網址，鎖定安全研究人員、滲透測試人員和網路犯罪分子為目標。這個遠端存取木馬就是 CyberGate，它已經活躍多年。

在網路安全領域，『Dorks』是網路安全專家和駭客用來搜尋脆弱性網站、敏感資訊和惡意軟體的特殊搜索查詢工具。它們有助於發現安全性漏洞、暴露的資料 (例如：密碼或財務資訊) 以及惡意軟體的位置。網路安全研究人員使用它們進行研究、測試和防範威脅。不過，它們也可能被駭客濫用於非法活動。

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-RgPst!g1

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：

- W32.Spyrat

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2024/03/08

CVE-2024-27199：JetBrains TeamCity中的身份驗證繞過漏洞

CVE-2024-27199 是由 JetBrains 公司所開發的構建管理和持續整合伺服器 TeamCity 的 Web 元件中的身份驗證繞過漏洞。該漏洞由路徑遍歷／遊走問題所引起。成功開採濫用該漏洞的未經認證攻擊者可透過 HTTP(S) 瀏覽 TeamCity 伺服器，繞過身份驗證檢查，獲得對 TeamCity 伺服器的管理控制權並修改系統，包括使用惡意憑證替換 HTTPS 憑證。賽門鐵克的網路防護技術入侵防護系統 (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: JetBrains TeamCity Authentication Bypass CVE-2024-27199

2024/03/08

Planet(*星球)惡意竊密軟體

Planet Stealer 是最近發現的一種惡意竊密軟體。這種基於 Go 語言的惡意軟體已在地下論壇上販售。Planet Stealer 的目標是從遭入侵的端點竊取各種資料，包括使用者憑證、瀏覽器 cookie、加密貨幣電子錢包、連線資料、各種通訊程式和軟體啟動器的設定檔等。收集到的資料透過 Telegram webhooks 外洩。

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.Stealer!gen1

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.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：

- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/03/08

駭客組織繼續利用DDoSia駭客工具套件發動攻擊

DDosia 是一種 DDoS 殭屍網路駭客工具套件，屬於名為 NoName057(16) 的威脅組織。該威脅組織主要針對支持烏克蘭的歐洲機構和企業發動攻擊。雖然 DDosia 已經支援多種架構和作業系統，但去年年底又出現一個新變種，增加對 FreeBSD 作業系統的支援。自今年年初以來，在真實網路情境上觀察到的持續性行動中，DDosia 工具包仍在被利用。

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：

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：

- Hacktool
- Linux.Mirai
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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!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。

2024/03/08

針對Linux網頁伺服器的全新惡意軟體攻擊行動

最近檢測到一個惡意軟體攻擊行動部署多個新型的 Golang 類型的惡意軟體有效籌載，目標是攻擊提供網頁服務的伺服主機，例如：Apache Hadoop、Docker、Redis 和 Confluence。該行動背後的攻擊者正在利用這些有效籌載，利用執行這些錯誤配置的服務伺服器，最終部署惡意挖礦

程式。這些有效籌載利用一系列技術，包括通訊埠掃描、HTTP 請求和 shell 命令來開採濫用已知漏洞，並在被入侵系統上執行惡意程式碼。

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：

- Hacktool
- Trojan Horse
- 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。

2024/03/07

DoNex勒索軟體

一個自稱為『DoNex』的新勒索軟體攻擊者在真實網路情境上出現。他們最近在自己的 Onion 加密網站上宣傳有好幾家企業成為受害者，其中包括美國和歐洲的公司。該組織採用雙重勒索策略，通常包括檔案加密（冠上.VictimID 副檔名）和資料洩露。

遭入侵的公司會收到勒索熟金支付說明檔案（Readme.VictimID.txt），建議他們透過加密的 Tox messenger 與該組織聯繫。目前，他們入侵公司的作案手法尚不清楚，進一步的監控和調查正在進行中。

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.Darkrace

基於機器學習的防禦技術：

- Heur.AdvML.B!200

2024/03/07

透過惡意XLS檔開展的Matanbuchus惡意程式載入器攻擊行動

Matanbuchus 是一種惡意程式載入器即服務 (loader-as-a-service)，出現在威脅環境中已有幾年時間，至今仍很活躍。該威脅主要透過電子郵件散佈，已觀察到各種攻擊鏈。它作為初始感染，主要在下載其他惡意軟體並將其安裝到遭入侵的機器上。目前已有報告稱出現一種新的網路攻擊行動，在該行動中，駭客利用惡意 XLS 檔來呼叫 JS 檔，而 JS 檔件又會導致惡意 DLL。

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)。

自適應防護技術(包含於SESC) ：

- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.MBT
- Trojan.Mdropper

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/03/07

zgRAT涉入的惡意活動呈上升趨勢

在過去的兩個月中，我們觀察到 zgRAT 涉入的惡意活動持續增加，其中大部分是直接透過惡意電子郵件或透過其他威脅 (例如：惡意程式載入器和惡意竊密程式) 傳播。這種威脅是一種典型的遠端存取木馬 (RAT)，允許操作者遠端控制遭入侵的機器、執行鍵盤側錄、竊取敏感性資料，還能上傳／執行其他威脅。特別值得一提的，zgRAT 還能透過 USB 隨身碟傳播。

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)。

自適應防護技術(包含於SESC) ：

- ACM.Ps-RgPst!g1
- ACM.RegRun-TPs!g1
- ACM.Ps-Msbuild!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.B