保安資訊--本周(台灣時間2024/07/26)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 48 萬 5,600 台受保護端點上總共阻止了 4,900 萬次攻擊。這些攻擊中有 80.6% 在感染階段前就被有效阻止：**(2024/07/22)**

- 在**8萬9,900**台端點上，阻止了**1,230**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬7,900**台端點上，阻止了**910**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬3,100**台**Windows**伺服主機上，阻止了**89**萬次攻擊。
- 在**5萬6,400**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬900**台端點上，阻止了**71萬300**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,900**台端點上，阻止了**360**萬次嘗試利用的應用程式漏洞。
- 在**15萬6,700**台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬3,300**台端點上，阻止了**130**萬次加密貨幣挖礦攻擊。
- 在**10萬6,400**台端點上，阻止了**830**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**639**台端點上，阻止了**9萬3,800**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 4,800 個受保護端點上阻止了總計 340 萬次攻擊。**(2024/07/22)**

- 使用網頁信譽情資，在 **96.3K** 個端點上阻止 **300** 萬次攻擊。
- 攔截 **19.3K** 個端點上 **340.1K** 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 **6K** 個端點上攔截 **66.8K** 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 **220** 個端點上攔截 **6.3K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

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。

2024/07/26
已有駭客組織開採濫用MSHTML漏洞來散佈Atlantida惡意竊密軟體

據報導，由名為 Void Banshee 的駭客組織所發動的惡意軟體攻擊行動，散佈 Atlantida 惡意竊密軟體。此攻擊開採濫用 CVE-2024-38112 (MSHTML 漏洞)，駭客使用特製的網路捷徑檔案(.URL) 觸發漏洞來停用 Internet Explorer。使用者會被檔案中包含 PDF 電子書所引誘，這些 PDF 書籍會透過各種公共平台 (例如：線上圖書館、Discord 伺服器……等) 散佈。一旦受到攻擊，受害者會被誘騙執行 Atlantida 惡意竊密軟體，這有助於從 Telegram、Steam 等應用程式、多個離線加密貨幣錢包和瀏覽器儲存的資料中滲透登入資訊。

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：

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：

- ISB.Downloader!gen544
- ISB.Downloader!gen285
- Trojan Horse
- Web.Reputation.1
- WS.Malware.2

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 對 Microsoft Internet Explorer 的預設強化提供針對 CVE-2024-38112 零時差防護。預設強化政策會封鎖所有向外連線。適用於 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。

2024/07/26

SeleniumGreed加密挖礦活動

SeleniumGreed 是最近在真實網路情境觀察到的加密挖礦行動。Selenium Grid 是 Selenium 開源自動化框架中的一個元件，用於測試 Web 應用程式。這些活動背後的威脅份子一直在濫用 Selenium WebDriver API 來執行反向 shell，以交付加密挖礦籌載。部署的酬載是修改過的，用於挖掘門羅幣 (Monero) 或比特幣 (BTC) 等加密貨幣的開源挖礦程式：XMRig。

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：

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.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。

2024/07/26

Zilla勒索軟體--源於Crysis的後繼最新變種

Zilla 是在威脅環境中觀察到的最新 Crysis／Dharma 勒索軟體的後繼新變種。該惡意軟體會加密使用者資料，並在加密檔案中冠上 .ZILLA 副檔名。除了這個自訂的副檔名之外，還會加上獨特的 ID 和威脅者的電子郵件地址。加密過程完成後，惡意軟體會以 ZILLA-INFO.txt 文字檔發送贖金支付說明通知，要求受害者支付贖金。Zilla 具備刪除被攻擊端點上卷影複本的功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomCrys!g2

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：

- 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

2024/07/26

Smishing Triad駭客集團發動針對印度使用者的網路釣魚行動

Fortinet 研究人員報告最近針對印度行動使用者的網路釣魚行動。這次攻擊是由一個名為 Smishing Triad 的駭客集團所為，該駭客集團之前曾針對全球多個國家發動類似的網路釣魚行動。攻擊者利用假冒為來自印度郵政的誘餌，假藉有待交付的包裹。傳送文字訊息包含短網址，將受害者引導至詐騙網站。攻擊者所使用的大量惡意網域名稱與印度郵政的官方網域名稱十分相似，其目的顯然是讓收件人相信所收到的訊息是合法。一旦受害者造訪詐騙網站，攻擊者就會試圖收集銀行資料或其他敏感資訊，這些資訊之後可能會用於其他詐騙或網路釣魚作業。

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：

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的域名。

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。

2024/07/26

歸咎於Stonefly APT駭客集團的持續間諜活動

賽門鐵克安全應變中心 (Symantec Security Response) 得知 CISA、FBI 及其他合作夥伴最近針對 Stonefly APT 駭客集團 (亦稱為 Andariel 或 DarkSeoul) 最近所進行的多項目標式攻擊活動發出聯合警示。眾所周知，該駭客集團以各行各業為目標，目的是獲取機密資訊和智慧財產。Stonefly 常常利用已經公開揭露的漏洞進行攻擊，並散佈各式各樣的有效酬載，包括後門、商品化的惡意軟體、各種遠端存取木馬 (RAT) 和勒索軟體等等。最近觀察到的網路間諜活動歸咎於此駭客集團，其目標是國防、航太、核能和工程部門。

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
- ACM.Ps-Schtsk!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper!gen2
- SONAR.MalTraffic!gen1
- SONAR.Mimikatz!gen26
- SONAR.SuspBeh!gen25
- SONAR.SuspDrop!gen1
- SONAR.TCP!gen1
- SONAR.TCP!gen6

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：

- Backdoor.Atharvan
- Backdoor.Preft
- Backdoor.Trojan
- Hacktool.Mimikatz
- Infostealer.Gampass
- ISB.Downloader!gen68
- Linux.Trojan
- Ransom.Maui
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.2

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

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: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 200
- 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。

2024/07/26

惡意軟體攻擊行動採用SEO中毒手法(搜尋引擎中毒、購買關鍵字排行)來瞄準W2表的尋求者

據報導，有惡意軟體行動採用 SEO 中毒手法 (搜尋引擎中毒、購買關鍵字排行)，針對搜尋 W2 表格的使用者進行攻擊。受害者會被重定向到偽造的 IRS 網站，在那裡他們會被引誘下載一個偽裝成 W2 表格的 JS 檔案。當執行時，JS 檔會下載並執行 MSI 套件，然後安裝包含 Brute Ratel Badger 的 DLL。這最終導致 Latrodectus 惡意軟體的部署。

網路知識：W2 表是美國國稅局使用的一種稅表，用於報告支付給員工的工資以及從他們預扣的稅款。

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!g

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.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：

- Audit: Rundll32 Suspicious Network 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。

2024/07/26

與俄羅斯有關的惡意軟體攻擊印度政治組織

據報導，一個據信是由與俄羅斯有關聯的威脅份子所策劃之惡意軟體攻擊行動，目標是對印度政治事務有興趣的組織。受害者會被偽裝成真正 Office 文件檔的 .LNK 檔案誘騙。點擊這些檔案會部署 .NET 惡意程式載入器，載入以 Go 寫成最終遠端存取木馬 (RAT) 的有效酬載。該有效酬載使用隱寫技術隱藏在 PNG 檔案中。解壓縮之後，它會使用異步程序呼叫 (APC) 注入方法注入 PowerShell 程序。該 RAT 還具備部署其他惡意軟體有效酬載 (包括勒索軟體) 的能力。

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!g

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.Reputation.1
- 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：

- 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。

2024/07/25

RADAR勒索軟體

另一個採用雙重勒索戰術的勒索軟體集團已在本來就高手如雲的勒索軟體生態圈嶄露頭角。該勒索軟體集團自稱為 RADAR，入侵機器後加密檔案，並冠上 .[隨機的 8 個字元] 的副檔名。在贖金支付說明文字檔 (README_FOR_DECRYPT.txt) 中，攻擊者告知受害者他們的資料已被外洩，檔案已被加密。他們建議受害者不要與第三方聯繫，並購買他們的解密器，否則會面臨資料在該組織的網站上被公開或出售。為了進一步迫使受害者支付贖金，他們會提供之前不乖乖就範的受害者例子。

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.SuspLaunch!g250
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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。

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，其出廠就內建的強化政策可針對此勒索軟體提供零時差的防護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/25

日本簡訊釣魚正流行--假冒公用事業、金融服務和航運業最容易讓人上鉤

由於行動裝置的廣泛使用，以及簡訊 (SMS) 的開啟率普遍高於電子郵件，因此簡訊釣魚越來越成為網路罪犯青睞的戰術。簡訊釣魚行動持續在全球各地擴散，在某些國家 (例如：日本) 更以成倍的速度成長，犯罪者最常假冒公用事業、金融服務和航運業，最容易讓人上鉤。

雖然日本大部分的簡訊釣魚都是以竊取敏感資訊來進行財務和身分盜竊為目的，但也有網路罪犯試圖以虛假帳單詐騙使用者，或誘使他們在行動裝置上安裝惡意 APP。

本月觀察到的惡意簡訊範例包括：

- [銀行名稱] 重要通知，詳情請見此處。[惡意網址]
- [停電前通知] 上個月的電費未付，但現已完全恢復。[惡意網址]
- 我們今天試圖送達您的包裹，但因無法與您會合，只好折返。[惡意網址]
- [重要通知] 感謝您使用[銀行名稱]卡。我們想通知您有一筆交易需要確認客戶身份，因此我們決定限制您使用我們的部分服務。如果您在一段時間內沒有確認您的帳戶，您的帳戶交易將會受到限制。

消費者和企業都面臨風險。對消費者而言，最直接的威脅是個人資訊被盜用和財務損失。企業則會面臨額外的危險--員工在連線至企業網路的工作或個人裝置上收到簡訊釣魚的訊息，可能會使公司遭受資料外洩和財務詐騙。

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的域名。

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。

2024/07/25

Stargazer Goblin駭客組織也開始散佈Atlantida惡意竊密程式

Atlantida 惡意竊密程式已被確定為最近在惡意軟體散佈行動中散佈的多個惡意軟體有效酬載之一，該惡意軟體散佈行動歸咎於被稱為 Stargazer Goblin 的駭客組織。其他透過這個被稱為 Stargazers Ghost Network 的惡意軟體傳送服務散播有效酬載，包括 RedLine、Lumma Stealer、Rhadamanthys 和 RisePro。根據 Checkpoint 研究人員的報告，負責此行動攻擊者利用受攻擊的 Github 資源庫和 Wordpress 網站散佈包含惡意二進位檔案的壓縮檔。

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-Msbuild!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Rgasm-Lnch!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g5
- SONAR.SuspBeh!gen825
- SONAR.SuspOpen!gen11
- SONAR.TCP!gen1

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：

- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.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。

2024/07/25

AI成為資安威脅幫兇的威脅日益增加

使用大型語言模型 (LLM) 人工智慧 (AI) 來產生惡意程式碼的網路攻擊越來越多。賽門鐵克團隊觀察到在網路釣魚行動中，LLM 產生的腳本會下載有害之有效酬載，例如：Rhadamanthys、NetSupport、CleanUpLoader (Broomstick、Oyster)、ModiLoader (DBatLoader)、LokiBot 和 Dunihi (H-Worm)。這突顯 LLM 在網路犯罪中遭濫用情況。

我們部落格文章有更深入的說明：AI 成為資安威脅幫兇的威脅日益增加。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.RegRun-TWscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-FlPst!g1
- ACM.Wscr-RgPst!g1
- ACM.Wscr-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g221
- SONAR.SuspOpen!gen11
- SONAR.SuspPE!gen32
- SONAR.SuspScript!g44
- SONAR.SuspStart!gen14
- 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：

- Backdoor.Trojan
- CL.Downloader!gen1
- CL.Downloader!gen9
- CL.Suspexec!gen168
- ISB.Downloader!gen52
- ISB.Downloader!gen53

- ISB.Downloader!gen68
- ISB.Dropper!gen1
- ISB.Heuristic!gen108
- ISB.Suspexec!gen49
- JS.Downloader
- Scr.Malcode!gen
- Scr.Malscript!gen16
- Scr.Phish!gen7
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan.Malscript
- Trojan.Modiloader!gen2
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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

2024/07/24

PicassoLoader惡意程式載入器

最近由 UAC-0057 (也稱為 GhostWriter) 駭客組織所發動的網路攻擊活動激增。在其行動中，攻擊者散佈內嵌巨集的 Word 文件檔，目的是啟動一個名為 PicassoLoader 的惡意程式載入器。此惡意程式載入器能夠在受害者的電腦上部署滲透測試工具 Cobalt Strike的Beacon。滲透測試工具 Cobalt Strike 被用於攻擊的情況，可說是日益頻繁。

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.Exl-CPE!g1
- ACM.Exl-Rgsvr!g1
- ACM.Ps-Rgsvr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MSExcel!g4
- SONAR.MSExcel!g11

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：

- ISB.Downloader!gen433
- WS.Reputation.1

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: Github Cloud Service Connect Attempt
- 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。

2024/07/24

新的Linux Play勒索軟體以ESXi伺服器為目標

趨勢科技的研究人員最近報導，觀察到惡名昭彰的 Play 勒索軟體有新的 Linux 變種並以 ESXi 伺服器為目標。在運行之前，惡意軟體會執行檢查以確認它是在 ESXi 環境中執行。Play 勒索軟體也會先嘗試關閉所有執行中的 ESXi 虛擬機器，然後再繼續加密程序。.PLAY 副檔名被冠上到加密的檔案，而勒索軟體支付說明文字檔則被存放在虛擬機器的根目錄中。此 Linux Play 變種所使用的部分網路基礎架構，先前已在稱為 Prolific Puma 的威脅程式攻擊中被觀察到。

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
- 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。

2024/07/24

LummaC2惡意竊密程式濫用Steam遊戲平台為其C&C網域

我們觀察到 LummaC2 的後繼新變種濫用「Steam」遊戲平台。此新變種現在可依需求取得動態 C2 網域，與之前將 C2 詳細資訊嵌入樣本本身的技術不同。惡意程式會將 Steam 網頁 (特別是 Steam 帳戶資料頁) 儲存為可執行程式碼。在存取此頁面時，它會解析特定的 <tag> 來擷取一個字串，然後將其解密以顯示 C&C 網域。

此惡意軟體利用 SEO 中毒 (搜尋引擎中毒、購買關鍵字排行) 方式散佈，將自己偽裝成 Slack 和 Capcut 等熱門應用程式的首頁。惡意軟體能夠竊取加密錢包、電子郵件用戶端、瀏覽器資料、已安裝的訊息應用程式、FTP 程式等相關資訊。收集到的資料會滲出到威脅者操控 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

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：

- Infostealer.Lumma
- 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。

2024/07/24

在真實網路情境上發現到Jellyfish(*水母)惡意程式載入器的後繼新變種

在真實網路情境上發現基於 .NET 的Jellyfish(*水母) 惡意程式載入器的後繼新變種。據報導，該惡意軟體是透過執行惡意 .LNK 檔案散佈。該 LNK 檔案被偽裝成 .pdf 文件檔，包含在 .zip 壓縮檔中--可能是在惡意垃圾郵件攻擊中傳播。Jellyfish Loader 具備從受害者電腦收集系統資訊的初始功能。之後惡意軟體會啟動與攻擊者 C&C 基礎架構的通訊，以便下載惡意 shellcode 並執行任意指令。據報導，此後繼新變種所採用的技術和部分程式碼特徵，與已知的 Olympic Destroyer 2018 惡意軟體攻擊相似。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- CL.Downloader!gen203
- CL.Downloader!gen241
- Trojan Horse
- Trojan.Gen.9
- Trojan.Gen.NPE
- WS.Malware.1
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/07/24

CVE-2024-4879--ServiceNow Jelly樣板注入漏洞

CVE-2024-4879 是最近被揭露的重大範本注入漏洞 (CVSS 風險評分：9.3)，會影響 ServiceNow，ServiceNow 是數位企業轉型的流行平台。成功開採濫用此漏洞可能會讓未經認證的遠端攻擊者取得存取權限，並在 Now 平台的情境中執行任意程式碼。此漏洞已在原廠發佈的修補軟體版本中解決。

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: ServiceNow Jelly Template Injection CVE-2024-4879

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，針對 Servicenow 的賽門鐵克 DCS 自訂沙箱具有強化規則，可保護關鍵組態檔案，並可設定 Servicenow 啟動任何 shell，以防止利用此漏洞所報告的惡意程式碼注入和未授權執行。
- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，其出廠就內建的系統鎖定政策，可以防止在相關程序伺服器上被部署可疑的 web shell。
- DCS 強化政策主要在防範此漏洞。該政策將攔截與 webdev 伺服器的對外連接，以防止下載 LNK 檔。即使將 LNK 檔下載或複製到機器上也無法啟動 PowerShell，進而在初始階段有效阻止這種攻擊。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/24

BianLian勒索軟體改變策略

BianLian 是自 2022 年中開始活躍的勒索軟體威脅者，特別針對美國和澳洲的基礎建設領域。作為其攻擊媒介的一部分，威脅者通常會利用透過第三方或網路釣魚取得的 RDP 認證來取得初始存取權。他們部署以 Go 程式語言寫成的自訂惡意軟體，並利用 AnyDesk、Atera Agent、TeamViewer 等遠端管理與存取軟體來持續進行攻擊。

最近，BianLian 透過開發一個基於 Go 的後門將其策略轉向資料竊取和勒索。此後門可作為下載和執行其他惡意有效載荷的載入器。它會與攻擊者的指揮與控制 (C2) 伺服器建立連線，以接收持續指令並確保持久性。

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：

- Backdoor.Trojan
- Trojan.Gen.9
- WS.Reputation.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.A!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。

2024/07/23

威脅者持續開採濫用：CVE-2024-21412漏洞

威脅者持續開採濫用：CVE-2024-21412 漏洞，此為 Microsoft Windows SmartScreen 中的安全繞過漏洞，已於 2024 年 2 月通報並以提供修補。

最近發現有人開採濫用 CVE-2024-21412 漏洞，來下載惡意的可執行檔案。這個多階段的攻擊鏈一開始是引誘受害者點擊一個偽裝的網址，再轉向到另一個網頁檔案。此網頁檔案會引導至 LNK 檔案，隨後執行 HTA 指令碼。執行後，HTA 指令碼會下載惡意 shell 程式碼注入器，目的是透過注入合法程序來載入最後的惡意竊密程式。惡意竊密程式會被用來擷取受害者的資料，並將竊取的資訊滲透到攻擊者之命令與控制 (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.Mshta-Cmd!g1
- ACM.Mshta-CPE!g1
- ACM.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MSHta!g1
- SONAR.SuspScript!g5

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Reputation.1
- WS.SecurityRisk.4

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.A!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 強化政策主要在防範此漏洞。該政策將封鎖外寄連線，並防止下載 LNK 檔案。即使 LNK 或 HTA 檔案被下載或另外複製到機器上，也無法啟動 PowerShell，進而在初始階段有效阻止這種攻擊。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。

2024/07/23

災難事件往往衍生更多詐騙事件～透過惡意Word文件檔傳送Daolpu惡意竊密程式

最近全球各地執行微軟作業系統的電腦都受到中斷影響，駭客／攻擊者不斷利用這次事件，引誘使用者存取惡意連結或啟動載有惡意軟體的檔案。與此事件相關所滋生的新攻擊已被發現，涉及一個內嵌巨集的 Word 文件檔，該文件會執行並下載一個名為 Daolpu 的不明竊取程式。

該文件偽裝成微軟的復原手冊，目標對象是受中斷影響而急於修復的人。一旦執行，Daolpu 就能終止「chrome.exe」等程序，並擷取憑證，包括 Chrome 和 Mozilla 瀏覽器的登入資料和 cookies。

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：

- CL.Downloader!gen106
- Scr.Malcode!gen
- Trojan.Gen.MBT
- Web.Reputation.1
- 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。

2024/07/23
防護亮點：賽門鐵克新增掃描／封鎖電子郵件相關的釣魚網頁先進技術：ScriptNN

網路釣魚，簡單但有效的攻擊

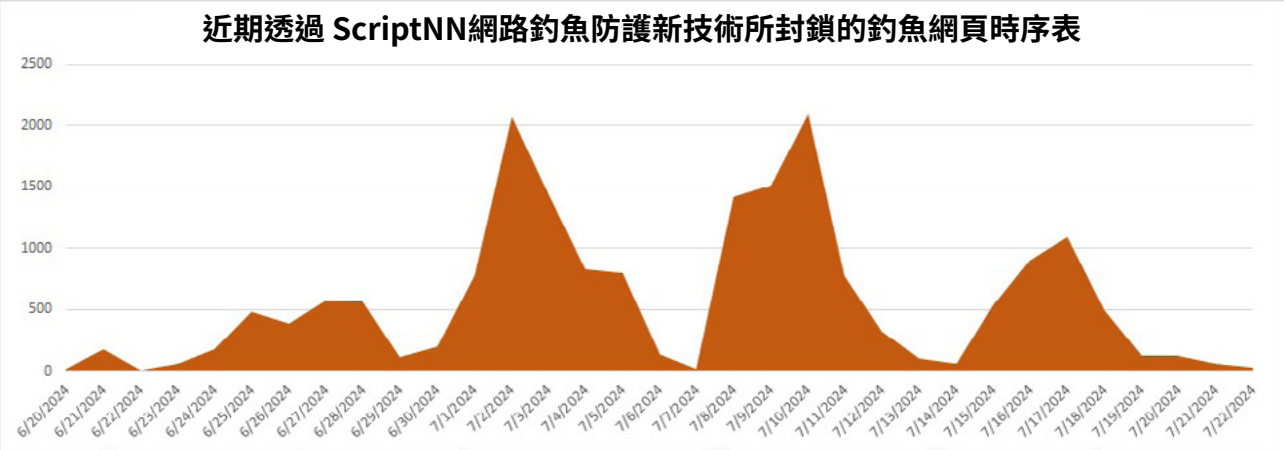
網路釣魚是一種非常常見的社交工程攻擊類型，通常透過電子郵件或簡訊 (SMS) 傳送看似來自合法來源的詐騙通訊，試圖竊取使用者資料。網路釣魚主要在惡意軟體攻擊的第一階段使用，不論最終目的是偵查或入侵。惡意軟體作者製作的網頁看起來與毫無戒心的使用者通常會需要輸入個人或敏感資訊 (通常稱為「PII」或「個人識別資訊」)，例如：電子郵件地址、使用者名稱、密碼、信用卡號碼等的網頁類似或甚至相同。一旦這些資訊被竊取，就很容易潛入使用者的機器甚至企業網路，並根據攻擊的性質和目的，呼叫或導入後續的惡意軟體、滲出資料或造成損害。賽門鐵克不斷創新，以保護我們企業電子郵件客戶免受惡意攻擊者的攻擊，而最常使用的傳播釣魚網頁方式就是透過電子郵件，作為賽門鐵克不斷創新的一部分，我們啟用一項新的先進技術，我們稱之為 ScriptNNto 來掃描電子郵件並封鎖這些釣魚網頁。

先進的網路釣魚偵測技術介紹

ScriptNN 是「HTML 與 JavaScript 神經網路模型」的縮寫，它會掃描電子郵件附件中的 HTML 與 JavaScript，並使用以深度神經網路為基礎的機器學習 (ML) 模型，該模型經過訓練，可透過分析數百萬個乾淨網頁以及已識別釣魚企圖的網頁，區分釣魚企圖與合法網頁。該模型會不斷更新，以便能夠識別零時差攻擊，同時避免誤攔有效的電子郵件。ScriptNN 模型採用最先進的技術架構，在磁碟和記憶體上佔用空間極小，並採用極快的掃描和偵測模式 (每次掃描只需微秒)，確保我們的電子郵件伺服器和電子郵件終端使用者，不會因為這項技術的導入而感受到任何明顯的延遲與效能耗損。

ScriptNN 的優點與風險

根據學習階段所收集的資料，我們預期 ScriptNN 初期每天可在我們的電子郵件防護空間中封鎖超過一千封的釣魚郵件。下圖顯示的是初步版本的實際現場攔截情況，隨著分析資料的增加，下圖也將不斷更新和改進。



ScriptNN 在識別通用檢測遺漏方面有很大幫助，而隨後的通用檢測改進實際上是第二層保護。舉例來說，最近的 Telegram Bot API 網路釣魚攻擊就被 ScriptNN 偵測到，並建立和釋出通用特徵來阻擋這些攻擊--補足現有的防護措施。另一方面，HTML 和 Javascript 是用來建立網路釣魚攻擊的主要運算語言，這兩種語言都因未使用強大的程式設計標準而聲名狼籍。這兩種語言也在不斷演進，所以在這個範疇與領域中幾乎不可能有百分之百零失誤的技術。因此，我們不會吹捧 ScriptNN 可以提供 100% 的涵蓋率，不過我們可以據實陳述，在我們廣泛的測試過程中，很少發生錯誤的判斷。即便極少發生的漏攔或誤攔的情況時，我們會有專門的團隊立即進行修正更新，並對引擎採取永久性的補救措施，以避免這些事件再次發生。

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。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。

2024/07/23

Braodo：基於Python的全新惡意竊密軟體竄出頭

有人觀察到一種名為 Braodo 的新全新惡意竊密軟體，在不斷演變的威脅環境中竄出頭。它透過包含 .BAT 批次檔的壓縮檔散佈。當執行時，此 BAT 檔案會連線至 GitHub 下載第二個 BAT 檔案和 ZIP 壓縮檔，其中包含 Braodo 惡意竊密軟體的最終有效酬載。以 Python 開發的 Braodo 能夠擷取範圍廣泛的個人資訊，包括使用者瀏覽器資料、cookie、密碼、系統資訊、憑證、銀行詳細資料等。一旦收集完成，竊取的資料會壓縮成 ZIP 檔案，並使用 Telegram API bots 傳送至威脅份子的 Telegram 頻道。

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-CPE!g2
- ACM.Ps-FlPst!g1
- ACM.Ps-Http!g2
- ACM.Word-Ps!g1

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
- WS.Malware.2
- WS.Reputation.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：

- Audit: Github Cloud Service Connect Attempt
- Audit: PowerShell Process Accessing Github
- Audit: Untrusted Telegram API Connection

2024/07/23

Daggerfly駭客組織大翻新其駭客工具組

Daggerfly 駭客組織 (也稱為 Evasive Panda, Bronze Highland) 駭客組織，活躍至少有十年之久，他們大翻新其駭客工具組。賽門鐵克的威脅獵手 (Threat Hunter) 團隊發表一份報告，提供有關 Daggerfly 駭客工具組的詳細資訊，例如：模組化惡意軟體框架 MgBot、模組化 macOS 後端程式 Macma，以及最近觀察到的多階段後端程式 Suzafk。

請參閱我們的部落格文章： Daggerfly：間諜組織正對其工具集進行重大更新。

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：

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：

- OSX.Macma
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Suzafk

- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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。

2024/07/23

駭客組織FIN7擁有多樣化的攻擊武器庫

駭客組織 FIN7 (也以 Carbon Spider、Carbanak 和 Sangria Tempest 等名稱被追蹤) 以精通複雜的行動和工程攻擊而聞名，以取得對企業網路的初始存取權。這個駭客組織的武器庫包括 AvNeutralizer、Core Impact、Diceloader、Powertrash 等工具，以及一個以 SSH 為基礎的後門。每種工具都支援入侵期間進行的各種攻擊階段。工具與技術的持續演進與創新，讓該組織能夠巧妙地進行滲透、利用、持續攻擊並逃避偵測。

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.Ps-SvcReg!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Heuristic!gen5
- Packed.Generic.700
- Trojan.Coinminer
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

- Trojan.KillAV
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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。

2024/07/23

BlackSuit勒索軟體以假冒的防毒軟體安裝程式為幌子

在真實網路情境發現 BlackSuit 勒索軟體的全新變種，已採用欺敵戰術來逃避偵測。最近，它們假冒奇虎 360 防毒軟體安裝程式來引誘受害者。一旦安裝，惡意軟體會加密使用者檔案，並冠上 .blacksuit 副檔名。為了避免被偵測到，惡意程式會存放一則名為 readme.blacksuit.txt 的贖金支付說明文字檔，其中包含加密的文字，以及與威脅者的通訊連結。最新版本包含新增功能，例如：強制 ID 參數和自我刪除技術。

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
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Blacksuit
- WS.Reputation.1
- WS.SecurityRisk.4

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

2024/07/23

CyberVolk勒索軟體

據報導，一種被稱為 CyberVolk 的全新勒索軟體已被揭露。此勒索軟體是以 C/C++ 程式撰寫，並採用完全由該惡意軟體幕後駭客集團所開發的獨特加密演算法。被加密的檔案會被冠上『.cvenc』的副檔名。該駭客集團採用持續的加密程序，直到受害者支付並收到解密金鑰為止。

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.RansomCybrVk!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.CyberVolk!gen1
- Trojan.Gen.MBT
- WS.Malware.1
- W32.Silly!gen

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/07/22

RA World勒索軟體駭客集團

Palo Alto Networks 研究人員提供 RA World 勒索軟體駭客集團的分析。該組織自 2023 年開始活躍，目標受害者遍及全球多個行業。該駭客集團透過加密檔案和外洩資料勒索兩種方式進行多重勒索作業。該駭客集團的攻擊通常包括以下步驟：

1. 透過面向網際網路的伺服器進行初始存取
2. 擷取憑證以進行進一步存取
3. 橫向移動以增加部署並存取更多資料
4. 多階段感染鏈以傳送 Babuk 勒索軟體有效酬載

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：

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：

- AGR.Terminate!g2
- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g7
- SONAR.SuspLaunch!g1

- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!gen4
- 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
- Ransom.Babuk

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

2024/07/22

假冒的安卓手機上APP釀成大禍：韓國金融機構的行動使用者成為目標

最近幾週，韓國幾家主要金融機構的客戶成為安卓手機平台上假冒 APP／假冒銀行詐騙攻擊的目標。攻擊者將他們的惡意軟體偽裝成假的應用程式，聲稱是來自知名合作銀行、政府擁有的資產管理公司、最大的商業銀行之一，或是以儲蓄為主的商品。此行動對消費者和企業都構成重大風險。

一旦安裝在行動裝置上，惡意軟體就會宣告安卓系統無障礙服務 (Accessibility Service)，允許它在未經使用者同意的情況下安裝外部惡意應用程式。這項 Android 功能目的在透過自動化任務和提供替代的互動方式來協助殘障使用者，然而它卻被全球各種 Android 惡意軟體濫用。

駭客在假冒的 APP 中嵌入 HTML 和惡意程式，以竊取使用者資料--這種技術通常用來呈現偽造的登入頁面，看起來就像銀行等合法網站，以竊取憑證。此外，惡意指令碼可擷取按鍵或攔截輸入表單的資料，在使用者與裝置互動時即時竊取資料。

雖然這種威脅的一般功能使其成為相當一般 Android 惡意軟體，但它卻使用 Virbox Protector 進行混淆，希望讓安全研究人員和防毒軟體難以分析與偵測它。Virbox Protector 是一款專為加強行動應用程式和軟體開發套件 (SDK) 安全性而設計的工具。

作案手法尚待證實。雖然我們相信惡意應用程式很可能是透過惡意簡訊傳播，但也不排除其他手法。

惡意 APP 所在網址如下範例：

- hxxps[:]//alkwiaw07[.]qznw9t[.]online/[companyname][.]apk
- hxxps[:]//ladiuoaw033[.]7tzne9[.]online/[companyname][.]apk
- hxxps[:]//laiakw9wf037[.]4422cg[.]online/[companyname][.]apk
- hxxps[:]//playstore022[.]k5clll[.]online/[companyname][.]apk
- hxxps[:]//playstore022[.]s0vv7[.]online/[companyname][.]apk
- hxxps[:]//playstore023[.]2bdt4[.]online/[companyname][.]apk
- hxxps[:]//playstore032[.]os3kn[.]online/[companyname][.]apk

- hxxps[:]//playstore045[.]07sed[.]online/[companyname][.]apk
- hxxps[:]//playstore045[.]0oaifp[.]online/[companyname][.]apk
- hxxps[:]//playstore045[.]esn9ds[.]online/[companyname][.]apk

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。

2024/07/22

Bugsleep：由Seedworm涉入垃圾郵件行動中散播全新的後門程式

最近進階持續威脅 (APT) 駭客組織：Seedworm 被觀察到部署一個先前未被記錄的 Bugsleep 後門軟體，主要是針對中東地區組織的網路釣魚行動，使用含有惡意連結的 PDF。一旦部署這個新的後門，攻擊者就可以執行遠端指令，並將檔案滲透到 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g43
- SONAR.ProcHijack!g45
- SONAR.ProcHijack!g47
- SONAR.SuspInject!gen5
- 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 Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malmsi

- 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

2024/07/22

Tag-100：開採濫用裝置漏洞的新興網路駭客組織

據報導，有一個新興網路駭客組織：Tag-100。以全球各地的政府和民營機構為攻擊目標。此駭客組織開採濫用裝置中的漏洞發動攻擊，並已觀察到其利用 Citrix NetScaler 等裝置中的已知漏洞。Tag-100 也利用 Pantegana Go 後門和 SparkRAT 等開放原始碼工具來進行持續攻擊和進一步開發。

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

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。

2024/07/22

Copybara：安卓平台上的惡意軟體

Copybara 是一種影響安卓 (Android) 行動裝置的銀行特洛伊木馬程式，已被觀察到以義大利使用者為目標。威脅者利用先前取得的聯絡資料，將自己偽裝成銀行員工，透過網路簡訊釣魚和語音釣魚，對受害者進行社交工程，使其下載惡意 APP。如果受害者下載 APP 並手動同意給予其存取權限，惡意軟體就會使用 MQTT(訊息佇列遠端偵測傳輸) 與其命令和控制伺服器通訊。

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：

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

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。

2024/07/22

全新NullBulge駭客組織，濫用人工智慧與遊戲領域的程式碼儲存庫

有報導指出，針對利用 AI 與遊戲企業中安全漏洞的威脅行為者，成立一個名為 NullBulge 的全新駭客組織。這個駭客組織透過操控 GitHub 和 Hugging Face 等平台上的程式碼儲存庫，肆無忌憚地瞄準這些領域。他們散佈偽裝的程式庫或 mod 套件，誘騙開發人員在遊戲或 AI 模型工作時，不知不覺地匯入惡意程式碼。作為攻擊策略的一部分，NullBulge 部署 Lockbit 有效酬載，利用 Async RAT 或 Xworm 等工具作為入侵系統和網路的中間步驟。

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
- ACM.Ps-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen821
- SONAR.Ransom!gen113

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Lockbit!g6
- Ransom.Lockbit!g7
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.2

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。

2024/07/21

匈牙利健康保險基金 (NEAK) 遭到 Lokibot 惡意軟體攻擊

最近一份報告顯示，位於匈牙利的國家健康保險基金 (NEAK) 成為攻擊者目標，他們目的是部署 Lokibot 惡意軟體。攻擊鏈由包含有害附件的惡意電子郵件開始，當打開這些附件時，就會將 Lokibot 載入受害者的電腦。Lokibot 以竊取使用者憑證、密碼和銀行資訊等敏感資料而聞名。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Rgsvc-Lnch!g
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g5
- SONAR.SuspOpen!gen11

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.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
- 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。

2024/07/19

Grayfly駭客組織正針對多個行業發動攻擊和破壞

在過去幾個星期內，與中國有關聯的進階持續威脅 (APT) 駭客組織：Grayfly(又稱 APT41) 發起多項攻擊行動。該駭客組織已針對航運與物流、媒體、技術和汽車等領域的多個行業發動攻擊，並成功入侵這些組織。攻擊媒介包括幾個用來執行 DUSTPAN 惡意程式下載器的 web shell，該惡意程式下載器會將後門 BEACON 載入記憶體，以便進行命令與控制通訊 (C&C)。Grayfly 利用 DUSTTRAP 這個多階段架構，提供攻擊者鍵盤側錄、shell 操作、檔案管理及系統程序操控等功能。作為其攻擊活動的一部分，Grayfly 已利用多個公開可用的命令列工具，例如：PineGrove 和 SQLULDR2，從 Oracle 資料庫竊取資料上傳至 Microsoft OneDrive。

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/07/19

BeaverTail惡意軟體的新變種以求職者為目標

有報告指出 BeaverTail 惡意軟體的新變種，透過模仿合法視訊通話服務 MiroTalk 的 macOS DMG 檔案散佈。此行動與以求職者為目標的北韓駭客有關。更新後的惡意軟體是原生的 Mach-O 可執行檔，能夠從網頁瀏覽器和加密貨幣錢包中竊取敏感資料。它還會提供額外的有效酬載，例如：基於 Python 的後台門戶 InvisibleFerret。該行動也涉及惡意的 npm 套件，突顯出與朝鮮有關的網路間諜行為不斷演進之策略。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2024/07/19

駭客組織APT17：發動散播9002遠端存取木馬(RAT)最新變種的網路攻擊行動，以義大利政府單位為目標

據報導，APT17 駭客組織發動惡意軟體攻擊行動，散佈 9002 遠端存取木馬 (RAT) 最新變種。該行動特別針對義大利政府單位和公司行號。使用者會被誘騙至偽裝的義大利政府網域連結，據傳會下載 Skype 安裝程式。一旦使用者被誘騙，安裝程式會在安裝合法軟體的同時啟動 jar 執行。jar 檔案會執行 shellcode，負責啟動 9002 RAT，提供遠端存取受害者的系統。9002 RAT 具備擷取螢幕截圖、與命令與控制 (C&C) 伺服器建立連線以取得額外指令等功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Wscr-Msiexec!g1
- ACM.Ps-Wscr!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：

- Packed.Generic.374
- Trojan.Mdropper
- Web.Reputation.1
- WS.Malware.2

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。

2024/07/18

針對烏克蘭的UAC-0180網路釣魚行動

研究人員最近觀察到針對烏克蘭國防工業的網路釣魚行動，主旨是無人飛行載具 (Unmanned Aerial Vehicle，UAV) 的採購。散佈的電子郵件包含一個 PDF 檔案的 ZIP 附件，其中有一個惡意連結。按下連結就會下載一個名為「adobe_acrobat_fonts_pack.exe」的檔案，這是一個以 Go 為基礎的惡意軟體，名為 GLUEEGG。GLUEEGG 會解密並啟動 DROPCLUE 惡意程式載入器，然後會下載一個誘餌 PDF 和一個 EXE 檔案。EXE 最終會安裝：ATERA，這是一個合法的遠端控制程式應用程式／平台，可讓攻擊者在未經授權情況下存取受害者的電腦。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- 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: Atera Client Activity
- Audit: TLS v1 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。

2024/07/18

合法工具RDP Wrapper和Tailscale在最近的惡意垃圾郵件行動中遭濫用

研究人員發現一個多階段的網路攻擊活動，首先是一個包含 .lnk 捷徑檔案的惡意壓縮檔，很可能是透過網路釣魚電子郵件散佈。執行後，.lnk 檔案會下載 PowerShell 指令碼，讓威脅者能夠透過 RDP 進行存取。為了欺騙使用者，在其後會出現一個有關加密貨幣交易的誘餌 PDF。該攻擊包括 PowerShell 指令碼、批次檔案、基於 Go 的二進位檔，以及利用具有弱點的 Terminator 驅動程式檔案發起自帶驅動程式攻擊 (BYOVD：Bring Your Own Vulnerable Driver)。合法的工具例如：RDP Wrapper 和 Tailscale VPN 用於遠端存取和網路連線，重點是建立與受害者的反向連線。

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-CPE!g2
- ACM.Ps-Http!g2
- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen9
- CL.Downloader!gen12
- PUA.Gen.2
- Trojan.Gen.MBT
- Scr.Malcode!gen
- Scr.Mallnk!gen10
- Scr.Mallnk!gen13
- Scr.Heuristic!gen20
- WS.Malware.1
- WS.SecurityRisk.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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：

- Suspicious Process Accessing Lets Encrypt Certified Site
- Webpulse Bad Reputation Domain Request

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**。