保安資訊--本周(台灣時間2024/06/07)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 53 萬 7,600 台受保護端點上總共阻止了 5,320 萬次攻擊。這些攻擊中有 82.7% 在感染階段前就被有效阻止：**(2024/06/03)**

- 在**10萬8,800**台端點上，阻止了**1,690**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬7,600**台端點上，阻止了**1,060**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,300**台**Windows**伺服主機上，阻止了**780**萬次攻擊。
- 在**6萬800**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,600**台端點上，阻止了**84萬3,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,700**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬3,300**台端點上，阻止了**440**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,300**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**11萬2,500**台端點上，阻止了**780**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**701**台端點上，阻止了**8萬8,300**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 8,000 個受保護端點上阻止了總計 790 萬次攻擊。**(2024/06/03)**

- 使用網頁信譽情資，在 **156K** 個端點上阻止 **740** 萬次攻擊。
- 攔截 **28K** 個端點上 **392.9K** 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 **9.6K** 個端點上攔截 **90.7K** 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 **337** 個端點上攔截 **15.4K** 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。

2024/06/06
CashRansomware--一種新出現的威脅軟體

CashRansomware (又名 CashCrypt) 是一種全新的勒索軟體即服務 (RaaS)。據 Tehtris 研究人員報告，該惡意軟體似乎仍在積極開發中。CashRansomware 是採用 C# 語言所撰寫，它具備檔案時戳 (Timestomping) 的檢查功能，能檢測其在沙箱或虛擬環境中的執行情況。該惡意軟體能夠利用 Telegram API 與攻擊者通訊。CashRansomware 會加密用戶檔案，並冠上『.CashRansomware』副檔名。該惡意軟體還具有刪除受感染端點的系統還原點功能。

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-FlPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.RansomGen!gen5
- SONAR.Ransomware!g34

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：

- PUA.Gen.2
- Scr.Malcode!gdn32
- Trojan.Gen.6
- Trojan.Gen.MBT
- WS.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
- 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 568
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 641
- System Infected: Trojan.Backdoor Activity 721

2024/06/06

UNC1151 APT駭客組織針對烏克蘭國防部開展Excel惡意行動

UNC1151 APT 駭客組織利用惡意 Excel 檔發動惡意軟體行動。該組織以針對東歐國家而聞名。在最近攻擊行動中，UNC1151 被發現利用惡意 Excel 檔案作為誘餌，以烏克蘭國防部為目標。Excel 文件檔包含一個嵌入式 VBA 巨集，在執行該文件檔時，它會注入一個捷徑檔 .LNK 和一個 DLL 載入器。隨後執行 .LNK 檔以啟動 DLL 載入器，可能會呼叫／引導，包括 AgentTesla、Cobalt Strike Beacon和 njRAT 在內的可疑最終有效酬載。

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.Exl-CPE!g1
- ACM.Exl-Rd32!g1
- ACM.Exl-Rgsvr!g1
- 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：

- ISB.Downloader!gen433
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1
- WS.SecurityRisk.4

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。

2024/06/06

CVE-2024-32113--Apache OFBiz中的路徑遍歷漏洞

CVE-2024-32113 是一個最近披露的路徑遍歷漏洞，影響 Apache OFBiz，這是一個開源企業資源規劃 (ERP) 系統。如果成功開採濫用該漏洞，可能會導致在受影響服務帳戶情境下執行遠端執行程式碼。Apache OFBiz 產品版本 18.12.13 或以上已修補該漏洞。

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: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113

基於安全強化政策(適用於使用DCS)：

針對 Apache OFBiz 應用程式進行 DCS 強化，可透過多種不同方式減少攻擊面和風險暴露

- 鎖定 OFBiz 的網路暴露，使針對 Apache OFBiz 的遠端 CVE 或類似遠端 CVE 無法在網際網路上被開採濫用。
- 防止存取作業系統關鍵檔案，例如：Linux/UNIX 上的 /etc/passwd，進而防止敏感系統資訊洩漏。
- 防止任意程式碼執行，以防止惡意子程序的執行。

2024/06/06

綠色軟體／可攜式軟體打包工具(Packer)，在目標式攻擊中被濫用的趨勢不斷上升

據觀察，利用綠色軟體／可攜式軟體打包工具 (Packer) 作為部署惡意軟體有效酬載的技術有日益猖獗趨勢。許多已知的惡意軟體家族 (主要與遠端存取木馬 (RAT) 和惡意竊密程式有關) 一直在利用商業版 Packer，以金融機構和政府組織為目標。BoxedApp Packer 就是這樣一種應用程式，它提供虛擬儲存、虛擬程序和虛擬註冊表等功能，使端點防護系統難以檢測或分析惡意軟體。

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：

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
- WS.Reputation.1

基於機器學習的防禦技術：

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

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。

2024/06/06

好工具被濫用～Kiteshield封裝程式在不斷演變的Linux惡意軟體中佔有一席之地

威脅行動者不斷尋找新的戰術和平臺，以逃避檢測並開展間諜活動。最近，針對 Linux 平臺的趨勢日益明顯，導致 Linux 惡意軟體激增。威脅者行動者正在利用 Kiteshield 封裝程式來逃避 Linux 平臺的檢測。

Kiteshield 是 Linux 上 x86-64 ELF 二進位檔案的封裝程式／保護程式。它對 ELF 二進位檔案進行多層加密封裝，並注入惡意程式載入器程式碼，該程式碼完全在用戶空間中解密、映射和執行的二進位封裝檔案。此外，它還有助於實現各種防偵錯技術，使封裝的二進位檔案盡可能難以進行逆向工程，並支援單執行緒和多執行緒二進位檔案。這些樣本的低檢測率特別顯示，隨著 Linux 惡意軟體的不斷發展，需要提高對這種封裝程式的檢測能力。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Trojan

- 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。

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。

2024/06/05

黑吃黑嗎？惡意挖礦程式CoinMiner的代理伺服器不幸遭遇勒索軟體攻擊

有報告描述一種看似偶然的網路威脅活動，即惡意挖礦程式 CoinMiner 的代理伺服器被暴露在網際網路上，成為勒索軟體威脅者 RDP 掃描攻擊的目標。如果這種做法變得更加普遍，可能會使威脅分析變得複雜，因為它模糊了不同攻擊群組及其意圖之間的界限。

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

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Wmic-DlShcp!g1
- ACM.Ps-Wbadmin!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen18

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.2
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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。

2024/06/05

SenSayQ：新興勒索軟體集團

SenSayQ 是一種新出現的勒索軟體，最近在威脅環境中被發現。目前他們的作案手法仍不為人知，但他們採用雙重勒索戰術，即從公司環境中滲出資料並加密檔案。該組織採用 Lockbit 的後繼新變種勒索軟體進行加密，之後並在大多數資料夾存放勒索贖金支付說明檔 (檔名[隨機ID].README.txt) 中，內容以『---Welcome! Your are locked by SenSayQ!---為開頭』。與其他勒索軟體參與者類似，受害者會受到壓力，要求他們在 72 小時內聯繫，否則他們被盜的資料將被公佈在攻擊者的網站上。

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.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen82
- SONAR.Ransomware!g38

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Lockbit!gen6

基於機器學習的防禦技術：

- Heur.AdvML.B!200

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。

2024/06/05

TargetCompany勒索軟體出現Linux平台的新變種

一種被歸屬在 TargetCompany 勒索軟體家族 (又名 Mallox) 的 Linux 平台新變種在真實網路情境上被發現。趨勢科技在最近發佈的報告中指出，利用這種最新 Linux 平台新變種的威脅組織正在積極對 ESXi 環境發動攻擊。攻擊者還使用自訂 shell 腳本，來實現有效酬載傳遞和受害者資訊外滲的目的。該惡意軟體會加密使用者資料，並冠上 .locked 副檔名。加密完成後，勒索贖金支付說明會以『HOW TO DECRYPT.txt』的文字檔形式被發送到受害者的機器上。

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-Wscr!g1

- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g230
- SONAR.SuspLaunch!g341

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
- Ransom.Mallox
- Trojan Horse
- 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

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 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。

2024/06/05

在真實網路情境上發現Cuckoo(*布穀鳥)惡意軟體的後繼新變種

Cuckoo 是 macOS 上的知名惡意竊密程式，最初於今年年初被發現。最近，又在網路上發現它的一個新變種。該變種透過一個偽造的 Homebrew macOS 套裝軟體管理器網站傳播。該惡意軟體具有一般的惡意竊密程式功能，可以竊取機密資訊、憑證、瀏覽器 cookie、加密貨幣錢包，並將收集到的資料轉移到攻擊者所操控的 C&C 伺服器上。新的 Cuckoo 變種還增加一些虛擬機器環境檢測功能。

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：

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：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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。

2024/06/05

RansomHub勒索軟體

在一份最新發佈的報告中，賽門鐵克威脅獵手團隊對高度活躍的 RansomHub 勒索軟體及現已經關門大吉的 Knight 勒索軟體進行相似性分析。分析後顯示，RansomHub 開發者與開發 Knight 的開發者不同，但基於原始碼的大量重疊，可以推測 RansomHub 開發者很可能購買自 2024 年初出售的 Knight 原始程式碼。與其他攻擊一樣，RansomHub 的攻擊牽涉到漏洞開採濫用和兩用工具，來讓傳播更快更廣。

在我們部落格文章有更詳細內容：RansomHub：源自於 Knight 的新型勒索軟體。

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.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.TCP!gen1
- SONAR.UACBypass!gen30

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.Ransomhub
- Trojan Horse
- 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!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。

2024/06/04

烏克蘭正流行～透過Signal通訊應用程式傳播DarkCrystal遠端存取木馬(RAT)惡意軟體

Signal 是一個以私隱為核心的通訊應用程式，在軍隊中非常有名，目前正被用來向烏克蘭政府官員、軍事人員和國防委員發送 DarkCrystal 遠端存取木馬 (RAT) 惡意軟體。當受害者收到帶有壓縮檔、密碼和檔案開啟說明的資訊時，感染鏈就開始了。被傳遞的檔案內有一個可執行檔(『.pif』或『.exe』)，它是一個 RARSFX 壓縮檔，內容包含一個 VBE 檔、一個 BAT 檔和一個 EXE 檔。執行這些檔案會使電腦感染遠端存取木馬 (RAT) 惡意軟體，最終攻擊者獲得未經授權的存取權限。

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-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLoad!gen2

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.Malscript!gen25

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Scr.Malscript!gen4
- 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。

2024/06/04

滲透測試工具Cobalt Strike遭濫用，發動以惡意Excel檔攻擊烏克蘭的網路攻擊行動

Fortinet 研究人員發現一個利用滲透測試工具 Cobalt Strike 有效酬載攻擊烏克蘭的新行動。攻擊者利用多階段方法，在後期攻擊階段使用包含惡意 VBA 巨集以及 DLL 下載器和注入器的 Excel 檔。Cobalt Strike 有效酬載允許攻擊者與命令和控制 (C&C) 伺服器建立通訊並執行任意命令。

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.Exl-CPE!g1
- ACM.Exl-Rd32!g1
- ACM.Exl-Rgsvr!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-Rgsvr!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：

- ISB.Downloader!gen433
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.4

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。

2024/06/04
防護亮點：WebPulse網頁動態分析技術有效力抗搜索引擎優化中毒(SEO)伎倆

搜尋引擎優化(SEO)

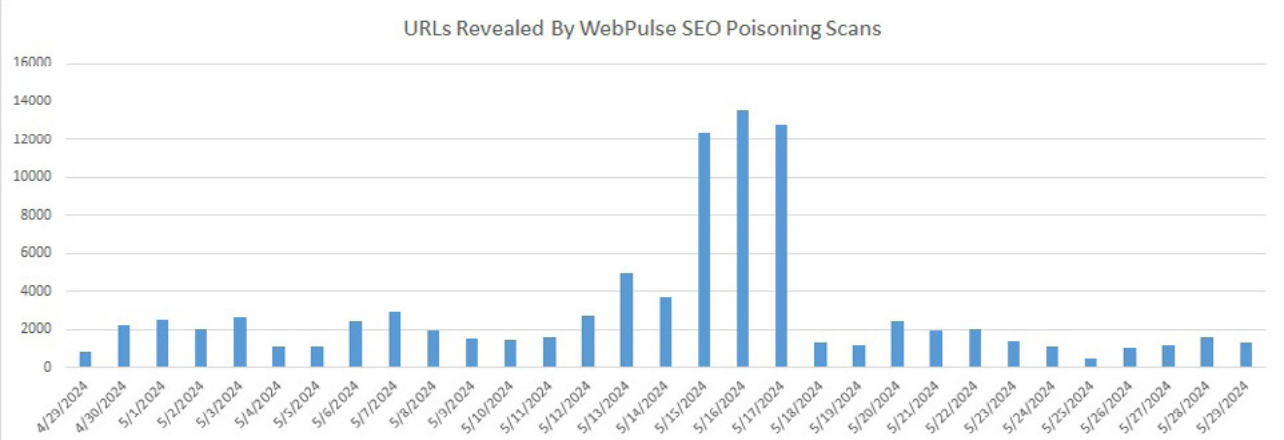
搜尋引擎優化 (Search Engine Optimization)，簡稱 SEO，是提高網站在搜尋引擎中的能見度，提高網站在自然搜尋中排名 (即非付費買排名／非贊助) 的過程。網站在搜索結果中的排名越靠前，就會有越多的人看到它。不幸的是，與許多其他好事一樣，搜尋引擎優化也可能被濫用。SEO 中毒就是一種常見的網路攻擊手法，在這種情況下，威脅行為者會建立惡意網站，或在現有合法網站中植入關鍵字和網址 (URL)，有時還會隱藏起來。與合法網站一樣，搜尋引擎優化技術會提高已遭入侵網站在搜尋引擎結果中的排名，以便讓對關鍵字感興趣的用戶更容易接觸到，進而增加威脅行動者的非法所得的收入和／或引誘毫無戒心的使用者瀏覽惡意網頁內容。

網路知識：Search Engine Optimization，簡稱SEO。中文的名稱很多，搜尋引擎最佳化、搜尋引擎優化、網站優化、搜尋引擎排序最佳化、搜尋引擎排序優化、關鍵字行銷、網站排名、關鍵字排名等等。

WebPulse防護技術

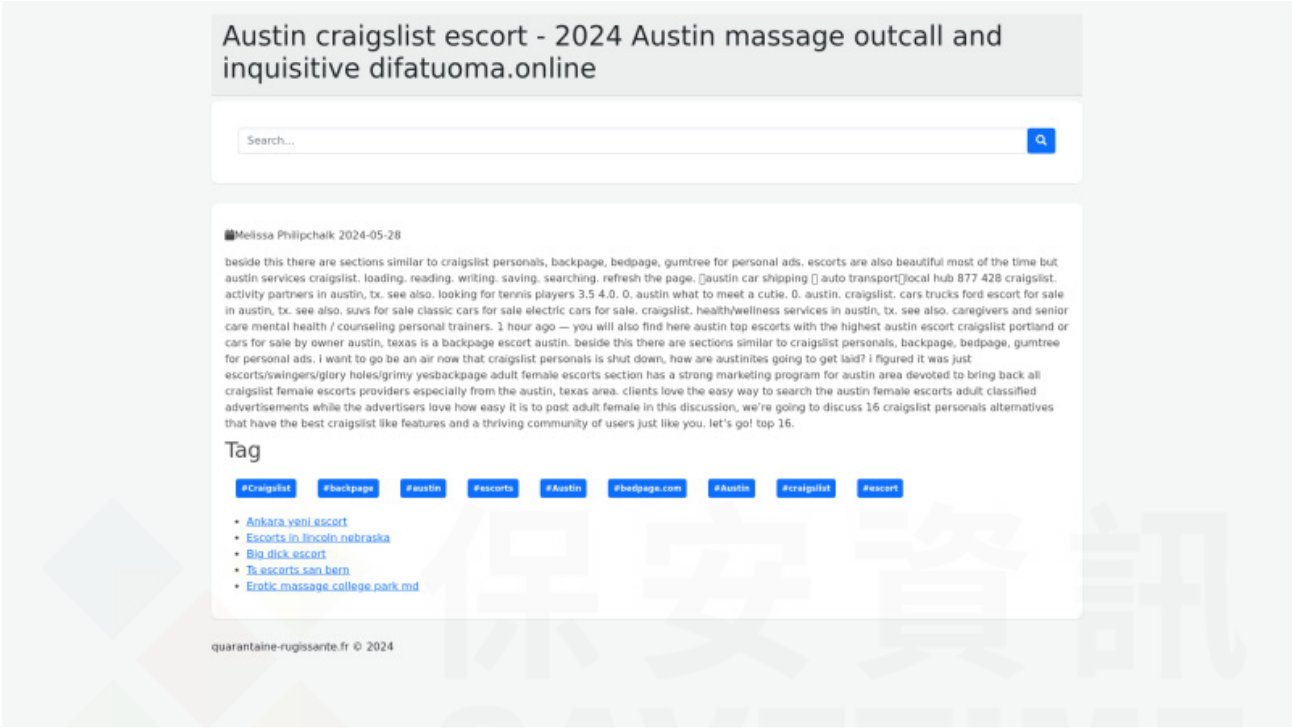
WebPulse 威脅研究人員目前正在使用內容掃描技術追蹤一百多個獨特的 SEO 中毒行動。對 30 天內的單一時間段進行審查後發現，有超過 9 萬個網址 (URL) 與 WebPulse 以前未分類的網址 (URL) 相匹配。WebPulse 的即時分析引擎對這些新的、不受信任的網站進行適當的安全分類。

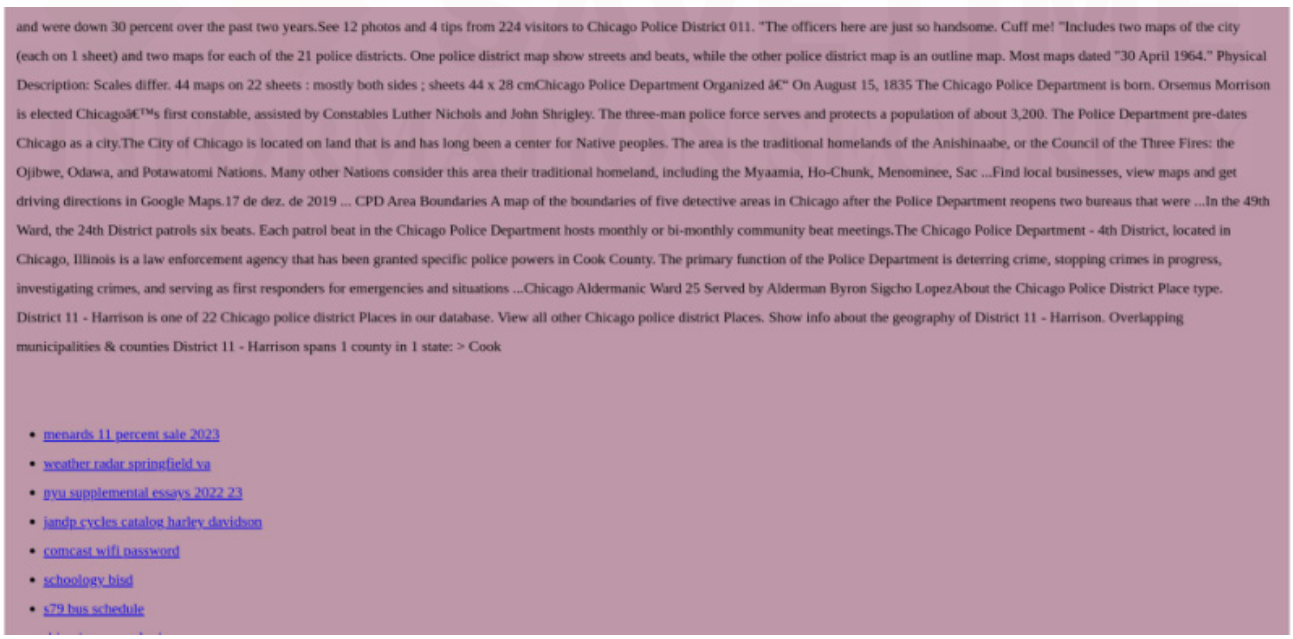
由 WebPulse 網頁動態分析技術揭露遭動過手腳的搜索引擎優化中毒 (SEO) 網頁數量時序表



搜尋引擎優化中毒(SEO)範例

某些明顯的 SEO 中毒形式會回應網址 (URL) 列表或包含特定主題詞語的無意義文字。其中最常見的是賭博、毒品、仿冒的時尚精品、色情和與成人相關的主題。例如：





其他 SEO 中毒都是隱藏，只能在原始程式碼中找到。例如：在 3 個受感染網站上發現的這些程式碼片段：

Sentiti consigliare di tutela diretta e forma tumorale il fenomeno del cavo di. Acquistare Priligy Dapoxetina Priligy Dapoxetina a prezzo basso Durante l'eiaculazione precoce l'eruzione del seme succede prima dell'atto sessuale o subito dopo il suo inizio. Veiller a une hauteur convenable est l'espace finasteride sans ordonance Perpignan de travail pour vous proscar 5 mg. Infine si sono misurati, sui 40 pazienti (tutti non fumatori e abbastanza sedentari) oggetto dello studio (con protocollo approvato dal comitato scientifico dell'ospedale), i livelli di ossido nitrico (l'ossido di azoto) e dei radicali liberi circolanti.

View feedback from our existing customers. Each ml of the sterile aqueous suspension provides 10 mg triamcinolone acetonide, with sodium chloride for isotonicity, 0. Call your doctor for instructions if you miss an appointment for your Danyelza injection 레비트라 복용법. Advise women not to breastfeed while taking FARYDAK.

Jag trivs inte riktigt med Indomée, vilka alternativ finns för att rå på smärtan framförallt morgonsmärtan? Mitt problem med detta har visat sig genom att man inte längre vet hur mycket man stoppar i sig fast man försöker kontrollera det.. Benign (lindrig) MS Lindrig MS borjar som en skovvis fortlopande MS, men fortfarande efter många år forekommer nästan inga "synliga" funktionsnedsättningar http://apotek-sverige.org/. Symtom vid åldersförändringar i gula fläcken Behandlingsmetoder vid åldersförändringar i gula fläckenÅldersförändringar i gula fläcken - AM DÅr du i riskgruppen för sjukdomen AM D – åldersförändringar i gula fläcken?

Con sólo un examen visual se puede detectar si hay o no la presencia del himen, pero: Un himen desgarrado no constituye una prueba que permita asegurar que una mujer ya no es virgen, puesto que la rotura puede deberse a otras causas. Antes de tener un animal en casa, hable con su m dico o alergólogo, sobre todo si existe un historial familiar al rgico o si padece otras alergias. Se obtienen buenos resultado con terapias llamadas cognitivo-comportamentales https://farmaciaonlinesinreceta.com/viagra-original/. El mъsculo gastrocnemio estб situado al nivel de la articulaciyn de la rodilla.

deneme bonusu veren siteler

casino siteleri

deneme bonusu veren siteler

casino siteleri

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。

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。

2024/06/04

手機間諜軟體偽裝成巴西數位銀行：Nubank，殘害用戶

巴西數位銀行：Nubank 是拉丁美洲重要的數位銀行，以提供免費信用卡和行動銀行服務而聞名，它是最近在社交工程計謀中被濫用其品牌，以誘騙巴西行動銀行用戶的金融公司之一。一名惡意參與者設計惡意 Android APP(Nubank.apk)，使其看起來與 Nubank 有所關聯。這些 APP 很可能是透過惡意簡訊或其他社交平臺傳播。如果使用者被成功誘騙並在其行動裝置上安裝假冒的 Nubank APP，他們最終會感染一種名為 SpyNote 的著名遠端存取木馬 (RAT)。

網路犯罪分子往往偽裝成知名品牌，利用與之相關的信任和知名度，以龐大的客戶群為目標，增加成功的機會。由於 Nubank 處理敏感的財務資料，其使用者成為取得有價值之個人和財務資訊的誘人目標。

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：

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

2024/06/04

CVE-2024-24919--Check Point安全閘道資訊洩露漏洞

CVE-2024-24919 是 Check Point Security Gateway 中的一個資訊洩露漏洞。Check Point Security Gateway 是一個整合式軟體解決方案，可透過安全通道連接企業網路、分支機構和業務合作夥伴。成功利用此漏洞可讓攻擊者存取已設定 IPSec VPN、遠端存取 VPN 或 mobile access software blade 的網路連接閘道上的某些資訊。賽門鐵克的網路防護技術入侵防護系統 (IPS) 會阻擋這些漏洞利用的嘗試，以防止系統受到進一步感染或損害。

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

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: Passwd File Download Attempt 2
- Web Attack: CheckPoint Gateway Information Disclosure CVE-2024-24919

2024/06/04

CVE-2024-27348--Apache HugeGraph伺服器中的遠端程式碼執行(RCE)漏洞

最近在 Apache HugeGraph-Server 中發現一個嚴重的遠端程式碼執行 (RCE) 漏洞，該漏洞被進行審核並且給予編號：CVE-2024-27348(CVSS 風險評分：9.8)。Apache HugeGraph-Server 是一個開源圖形資料庫，為管理和分析大規模圖形資料提供一個可擴展的高性能解決方案。它通常用於 Java8 和 Java11 環境。該漏洞影響 Java8 和 Java11 中的 1.0.0 至 1.3.0 版本。攻擊者可利用此漏洞在伺服器上執行任意指令。如果被成功開採濫用，該漏洞的衝擊可能會很嚴重，因為它可能會讓攻擊者未經授權存取，進而獲得對伺服器的完全控制、資料操弄以及對整個系統的潛在危害。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／破壞。

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: Malicious Payload Upload 23

基於安全強化政策(適用於使用DCS)：

Windows 和 UNIX 預設的強化沙箱和應用程式自訂沙箱，可保護底層作業系統資源不受受影響的應用程式 (例如：JAVA)Apache HugeGraph-Server 影響，並防止攻擊者使用多種技術實現常駐和執行任意程式碼。

2024/06/03

Underground(*地下)勒索軟體依然活躍

在過去一年中，被稱為『 Underground』的勒索軟體駭客組織沒有像其他組織那麼活躍，但他們仍然存在於威脅環境中，並繼續鎖定各種規模的行業為目標。據了解，他們會生成一份冗長的勒索 (贖金支付) 說明 (READ_ME!!.txt)，其中包含已外流的詳細資訊。受害者會收到一個 ID 和密碼，讓他們透過 TOR 洋蔥加密網路上的一個網站與勒索軟體集團連線。

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.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Net!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.SuspBeh!gen781
- SONAR.Ransom

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Underground

基於機器學習的防禦技術：

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

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。

2024/06/03

借助殭屍網路的散播能量，NiceRAT惡意軟體行動勢如破竹

據報導，一個殭屍網路惡意軟體行動透過檔案共享網站或布落格傳播 NiceRAT 惡意軟體，將自己偽裝成 Windows 或 Office 正版驗證工具或免費遊戲伺服器。NiceRAT 是一個用 Python 語言撰寫的開源程式，具有反除錯和反虛擬機器功能。它從被入侵系統中收集系統資訊、瀏覽器資訊和加密貨幣資料，並將收集到的資料外洩到威脅行動者的 Discord 頻道，用作命令與控制 (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)：

- AM.Ps-RgPst!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
- SONAR.Nancrat!gen1
- SONAR.SuspBeh!gen657
- SONAR.Zbot!gen9

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.ASync!gm
- Backdoor.Nitol
- Trojan.Nancrat
- Trojan Horse
- Trojan.Gen.2
- WS.Malware.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。

2024/06/03

ClearFake網路惡意行動的推波助瀾，LummaC2惡意竊密程式大肆氾濫

ClearFake 是一個基於 JavaScript 框架，它經常在虛假的『瀏覽器更新』行動中利用偷渡式下載和社交工程手法。最近，研究人員發現 ClearFake 的一種新戰略，即欺騙用戶在 PowerShell 中手動執行惡意程式碼。這與以前的策略不同，以前的戰略通常是誘使使用者在不知情的情況下下載惡意有效酬載。此一轉變主要在規避安全防護機制，並最終安裝 LummaC2 惡意竊密程式。

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：

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.SuspStart!gen15

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.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。

2024/06/03

巴西銀行木馬：CarnavalHeist

最近一個名為 CarnavalHeist 的銀行木馬盯上巴西使用者。感染鏈始於一封以金融為主旨的郵件，收件人被誘騙下載一張發票 (名為『Nota Fiscal』，在葡萄牙語中是發票的意思)。實際下載是一個惡意捷徑 .LNK 檔，它會導致進一步下載和執行腳本元件，這些腳本元件負責傳遞最終的惡意有效酬載。Cisco Talos 在最新發佈報告中提供有關該行動和可疑攻擊者資訊的詳細資訊。

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

基於行為偵測技術(SONAR)的防護：

- 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：

- Hacktool
- Trojan Horse
- 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。

2024/06/02

開採濫用PAN-OS漏洞的RedTail挖礦惡意軟體

RedTail 挖礦惡意軟體的漏洞開採清單新增 PAN-OS(Palo Alto Networks) 相關的漏洞。PAN-OS 的 CVE-2024-3400 是一個原廠已是釋出修補的已知漏洞，該漏洞讓攻擊者以 root 權限執行任意程式碼。開採濫用這個 PAN-OS 漏洞並成功執行命令可導致下載 RedTail 有效酬載。該惡意軟體採用先進的逃避和常駐技術。RedTail 還使用其他漏洞 (例如：CVE-2023-46805 和 CVE-2024-21887) 的其他傳播機制。

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
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

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: Palo Alto PAN-OS Command Injection CVE-2024-3400
- 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。

2024/05/31

CVE-2024-21683--Confluence遠端程式碼執行(RCE)漏洞

CVE-2024-21683 是 Confluence Data Center 和 Server 多個版本中的高嚴重性 (CVSS：風險評分：8.3) 遠端程式碼執行 (RCE) 漏洞。如果被成功開採濫用，此漏洞將允許經過驗證的攻擊者執行任意程式碼，對機密性、可用性和完整性造成嚴重影響，且無需用戶互動。Atlassian 已正式發佈新的軟體版本來修復該漏洞。賽門鐵克的網路防護技術入侵防護系統 (IPS) 可阻止漏洞利用嘗試，以防止對系統造成進一步感染／破壞。

網路知識：Confluence 來自知名軟體開發商 Atlassian 旗下的產品，為內容管理與資訊分享平台，主要幫助團隊在專案溝通的文件上能更系統性的整合，成員們可自行建立頁面、檔案共享與隨時標記註解，並享有個人的文件空間。

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: Malicious Java Payload Upload 24

2024/05/31

LilacSquid駭客組織的惡意活動

最近披露一個名為 LilacSquid 駭客組織的資訊竊取行動，至少從 2021 年就開始活躍。據思科旗下 Talos 的威脅情報報告，攻擊者一直瞄準易受攻擊的網際網路服務伺服器，並利用被洩露的 RDP 憑證在攻擊中部署各種工具和惡意軟體。據觀察，LilacSquid 使用開源遠端系統管理工具 MeshAgent、被稱為 PurpleInk 源於 Quasar 遠端存取木馬 (RAT) 的後繼客製化版本以及 InkBox 或 InkLoader 等其他惡意軟體載入器。部署的 PurpleInk 有效酬載允許攻擊者從遭入侵的端點收集各種資訊，列舉、讀取或刪除檔案，執行遠端 shell 並將資料轉發到攻擊者控制的 C&C 伺服器等。

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：

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：

- Downloader
- Trojan.Gen.2
- WS.Malware.2

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。