保安資訊--本周(台灣時間2024/10/25)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 43 萬 1,900 台受保護端點上總共阻止了 4,780 萬次攻擊。這些攻擊中有 80.5% 在感染階段前就被有效阻止：**(2024/10/23)**

- 在**9萬3,600**台端點上，阻止了**1,390**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬5,200**台端點上，阻止了**890**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬9,800**台**Windows**伺服主機上，阻止了**7萬7,000**次攻擊。
- 在**5萬9,300**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬600**台端點上，阻止了**69萬8,800**次嘗試掃描在**CMS**漏洞。
- 在**5萬5,000**台端點上，阻止了**280**萬次嘗試利用的應用程式漏洞。
- 在**13萬100**台端點上，阻止了**270**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬800**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬6,100**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**528**台端點上，阻止了**8萬4,800**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 18 萬 5,700 個受保護端點上阻止了總計 760 萬次攻擊。**(2024/10/23)**

- 使用網頁信譽情資，在 **176.3K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **22.3K** 個端點上 **292K** 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 **8.7K** 個端點上攔截 **141.2K** 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 **494** 個端點上攔截 **6.9K** 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。

2024/10/24
與時俱進的Prometei殭屍網路活動

據報導，網路上出現新的 Prometei 殭屍網路活動。該殭屍網路過去主要被用於門羅幣 (Monero) 的加密貨幣挖礦劫持作業，但與時俱進，其背後的攻擊者更新殭屍網路功能，以進行更複雜的攻擊，允許完全控制受感染的機器以及額外的任意有效酬載部署。Prometei 傳播行動通常會利用先前已揭露的 RDP 或 SMB 漏洞、使用網域生成演算法 (DGA) 機制進行 C&C 通訊，以及在攻擊鏈中部署 webshell。

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

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：

- Infostealer!im
- Scr.Malcode!gdn32
- Trojan Horse
- WS.Malware.1
- 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

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 File SMB 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。

2024/10/24

DarkComet～功能強大的遠端存取特洛伊木馬(RAT)

DarkComet 是一款功能強大的遠端存取特洛伊木馬 (RAT)，由於其隱蔽的作業方式和全面的功能，至今仍是一個重大威脅。它能讓攻擊者遠端控制受感染的裝置、滲透敏感資料，並部署進一步的惡意軟體。它可以透過改變檔案屬性、竄改登錄機碼和提升權限來逃避偵測。此外，它還能與命令與控制 (C&C) 伺服器通訊，以執行各種指令，包括擷取按鍵和控制顯示裝置。

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.Ps-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- 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：

- Hacktool.Gen
- Hacktool.Keylogger
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan Horse
- W32.Zorex
- W97M.Downloader
- WS,Malware.1

基於機器學習的防禦技術：

- 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: Backdoor.Graybird 5
- System Infected: Bad Reputation Application Connecting to Cloud Storage

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。

2024/10/23

WarmCookie惡意軟體廣受惡意攻擊者青睞，已涉入多起不同的攻擊行動

WarmCookie 惡意軟體，已被觀察到透過各種行動被散佈，包括惡意電子郵件。此惡意軟體提供初始存取權限給受攻擊的受害者，並用於建立持久性／常駐能力。與 WarmCookie 相關的其他功能包括遠端指令執行、檔案系統操控和有效酬載傳遞等。思科 (Cisco) 旗下的威脅情報組織 Talos 最近一份報告提供技術分析以及資料，以支持將惡意軟體歸屬於 TA866 駭客組織的論述。

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

- ACM.Rd32-TskReg!g1
- ACM.Untrst-TskReg!g1
- ACM.Wscr-Ps!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：

- JS.Downloader
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Coinminer
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malscript
- Trojan.Warmcookie!gen1
- W32.Silly!gen
- 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。

2024/10/23

「Hybrid」不止是油電混合車～Crystal Rans0m：以Rust語言撰寫同時兼具加密勒索與資料竊取「Hybrid」的惡意程式

Crystal Rans0m 是一款以 Rust 語言撰寫同時兼具加密勒索與資料竊取混合 (Hybrid) 的惡意程式，同時結合檔案加密與資料竊取功能，已發現其以義大利和俄羅斯為目標。該惡意軟體可以竊取瀏覽器資料、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密)、Steam 檔案、Riot Games 等數位遊戲平台的用戶端資料，並利用 Discord webhooks 進行資料外洩。它還運用偵測虛擬環境 (anti-VM) 和防偵錯技術。贖金要求以加密貨幣：門羅幣 (Monero) 來支付，並提供一個 Session ID 用於通訊。

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-Mshta!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.Stealer!gen1
- SONAR.Ransom!gen14
- SONAR.Ransomware!g6

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.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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 656
- System Infected: Trojan.Backdoor Activity 721

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。

2024/10/23

防護亮點：Apache OFBiz 存在的多個漏洞已遭開採濫用發動攻擊，賽門鐵克用戶可高枕無憂

Apache OFBiz 是一套開放原始碼的企業資源規劃 (ERP) 系統和商業應用程式。它提供一套企業應用軟體系統，可將企業許多業務流程整合並自動化，協助您營運整個企業。Apache OFBiz 可以多種方式用於自動化和整合業務流程，例如：供應鏈管理、庫存管理、客戶關係管理、電子商務、專案管理、人力資源等。

由於 Apache OFBiz 廣泛用於企業環境中，對於覬覦在企業環境中建立灘頭堡的攻擊者來說，它是一個具有吸引力的目標。更糟糕的是，Apache OFBiz 已被發現多個漏洞。這些漏洞主要屬於路徑／目錄遍歷漏洞和遠端程式碼執行漏洞類型。

路徑／目錄遍歷(原文Path／Directory Traversal Vulnerability也有人稱跨越／穿越)漏洞

路徑遍歷漏洞，也稱為目錄遍歷漏洞，是網頁應用程式中的安全弱點，會讓攻擊者存取網頁伺服器根目錄以外受限制檔案和目錄。我們之前已討論過這類漏洞及其影響。

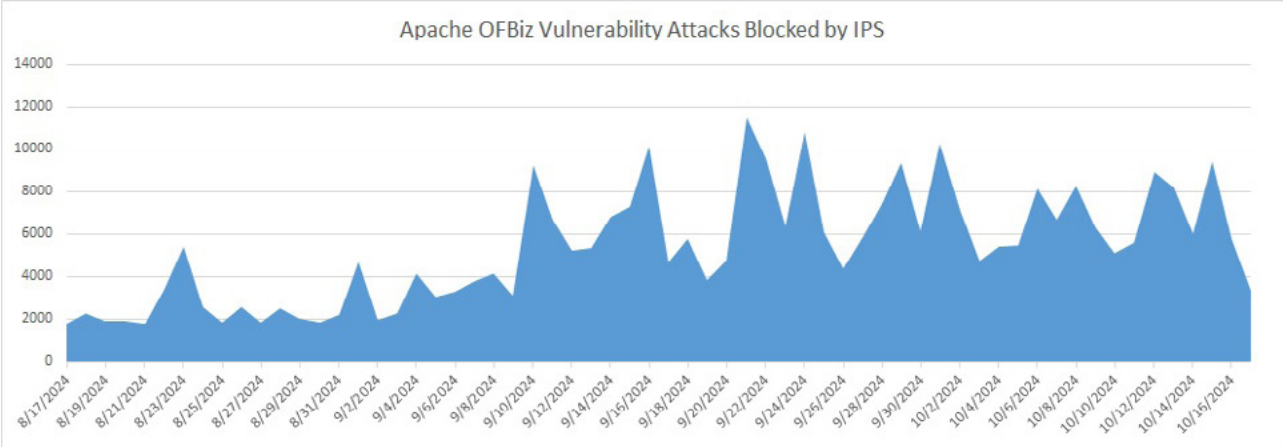
1. **CVE-2024-32113**：是存在 Apache OFBiz 的嚴重風險 (CVSS風險評分為9.1) 路徑遍歷漏洞。如果成功開採濫用此漏洞，可能會在受影響的服務帳戶導入參數執行遠端程式碼。Apache OFBiz 18.12.13 以上的版本已修補此漏洞。此漏洞也已被美國網路安全暨基礎設施安全局 (CISA)列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。
2. **CVE-2024-36104**：此漏洞再次被判定為嚴重風險 (CVSS風險評分為9.1) 路徑遍歷漏洞。此問題影響 18.12.14 之前的 Apache OFBiz。如果遭成功開採濫用，可讓遠端攻擊者存取未經授權的機敏檔案或目錄，並可能導致遠端執行程式碼。此漏洞是先前揭露 CVE-2024-32113 的修補程式繞過漏洞。
3. **CVE-2024-45195**：是一個高度風險 (CVSS風險評分為7.5) 的路徑遍歷漏洞，由於繞過先前 CVE-2024-32113、CVE-2024-36104 的修補程式而產生。如果遭成功開採濫用，將允許遠端攻擊者在伺服器上執行惡意程式碼，可能導致系統完全受損。此問題會影響 Apache OFBiz 18.12.16 之前的版本。

遠端程式碼執行漏洞(RCE)

遠端程式碼執行是一種允許遠端攻擊者在遠端機器上執行任意程式碼的漏洞。RCE 漏洞會危及使用者的敏感資料，讓攻擊者執行惡意程式碼或惡意軟體，並接管受影響的系統。

1. **CVE-2024-38856**：是嚴重風險等級 (CVSS風險評分為9.8) 的預先驗證 (Pre-Authentication) 遠端程式碼執行漏洞，影響 Apache OFBiz 18.12.14 之前的版本。此漏洞源自覆寫檢視功能的缺陷。一旦遭成功開採濫用，未經驗證的攻擊者可透過精心製作的請求遠端執行程式碼。應用程式供應商已釋出修補程式，在 18.12.15 或更新版本的產品中已修補此漏洞。此漏洞透過 Mirai 殭屍網路佈署。此漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

賽門鐵克的網路防護技術入侵防護系統 (IPS) 會阻止這些漏洞利用嘗試，以防止系統受到感染/損害。攻擊會在初始階段就被攔截，而確保不會有惡意的有效負載被注入到系統上。到目前為止，IPS 已在超過 1 萬9,000 台機器上阻擋超過近 33 萬次利用這些漏洞的嘗試。



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 RCE Vulnerability CVE-2024-38856
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-45195
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104 2
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113 2
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113 3

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。
欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

2024/10/22

CVE-2024-28987--SolarWinds服務臺系統Web Help Desk(WHD)存在寫死密碼憑證(Hardcoded)漏洞

CVE-2024-28987 是最近被揭露的一個影響 SolarWinds 服務臺系統 Web Help Desk(WHD) 存在寫死密碼憑證 (Hardcoded) 漏洞。該漏洞被被判定為嚴重風險 (CVSS風險評分為9.1)，如果被成功開採濫用，遠端未認證攻擊者可存取內部軟體功能並修改資料。此漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，顯示在真實網路情境中有活躍的攻擊報告。軟體供應商已針對此漏洞釋出 WHD 應用程式的修補版本--12.8.3 HF2。

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: SolarWinds Web Help Desk CVE-2024-28987

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，預設鎖定政策就可保護底層伺服器免受此漏洞影響，包括防止執行任意指令和限制讀取關鍵作業系統檔案。
- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。
- DCS 的監控政策能夠監控和標記未經認證的使用者活動。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/22

威脅份子濫用開放原始碼網路釣魚框架來傳送遠端存取木馬(RATS)

網路威脅聯盟 (Cyber Threat Alliance，CTA) 會員思科 (Cisco) 旗下的威脅情報組織 Talos 最近一份報告揭露一項新的網路釣魚攻擊行動，濫用名為「Gophish」的開放源碼網路釣魚攻擊演練評估框架來部署兩種攻擊鏈中其中之一。第一個攻擊鏈使用遭 Pidief 感染的 Office 文件來部署新發現 PowerShell RAT，稱為「PowerRAT」；第二個攻擊鏈使用惡意 HTML 檔案和 GOLoader 來部署 DCRAT。

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.MBT
- Trojan.Pidief
- Trojan.Pidief
- JS.Downloader
- Backdoor.Cobalt

基於機器學習的防禦技術：

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

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2024/10/22

IcePeony：與中國有關的進階持續威脅(APT)駭客組織鎖定東南亞政府組織

最近發現一個與中國有關的進階持續威脅 (APT) 駭客組織，名為 IcePeony，針對印度、模里西斯和越南等國家的政府機關和機構發動惡意軟體攻擊行動。該組織的攻擊手法通常與 SQL 注入有關，導致透過 web shells 和後門入侵，利用「IceCache」等自訂惡意軟體滲入網路。

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.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.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。

2024/10/21

透過假的的「CAPTCHA」驗證系統傳播Lumma惡意竊密軟體

研究人員正在監控一項持續進行中的網路釣魚行動，攻擊者似乎已將他們策略從傳統網路釣魚提升到使用假的辨認人類與機器人之「CAPTCHA」驗證系統和利用合法軟體。其目的是最終引誘使用者執行一個名為 Lumma Stealer 的惡意竊密軟體有效酬載。此惡意竊密軟體以惡意軟體即服務 (MaaS：Malware-as-a-Service) 的模式運作，可竊取密碼和加密貨幣資訊等敏感資料。

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)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspLaunch!g221
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32

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

2024/10/21

網路釣魚誘餌暗藏資料刪除程式(Wiper)惡意軟體

研究人員最近觀察到一場攻擊行動，威脅份子假冒某家防毒軟體廠商，向以色列的組織發動目標攻擊，並發送網路釣魚電子郵件，示警來自國家級駭客的威脅。這些電子郵件包含一個假程式的連結，該程式會下載稱為 Wiper 的惡意軟體，目的是刪除資料。

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：

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
- 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

2024/10/21

利用Quasar遠端存取木馬(RAT)針對Meta Ads專業人員進行網路釣魚攻擊

據報導，有針對求職者和數位行銷專業人員的惡意軟體攻擊行動。此行動特別針對 Meta Ads 專業人員，據信是由越南的威脅份子所發起。初始攻擊啟於一封包含壓縮檔附件的釣魚電子郵件，該壓縮檔將惡意 .LNK 檔案偽裝成 PDF。當開啟時，LNK 檔案會觸發 PowerShell 指令，然後下載和執行其他腳本，最終傳送 Quasar 遠端存取木馬 (RAT) 有效酬載。這樣攻擊者就能完全控制受攻擊的系統，進行資料竊取、監視和散佈更多惡意軟體等活動。此惡意軟體具備虛擬環境認知和反偵錯功能，並透過隱藏在系統目錄中來建立持久性／常駐能力。

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-CPE!g2
- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!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。

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：

- Scr.Mallnk!gen13
- Trojan.Gen.NPE.C
- WS.Reputation.1
- WS.SecurityRisk.4

2024/10/18

新興「ClickFix」社交工程伎倆的惡意程式攻擊行動：也出現在針對Google Meet使用者的情境

自 2024 年 6 月以來，已有多起惡意軟體攻擊行動採用新興「ClickFix」社交工程伎倆：利用假冒的驗證碼網頁引誘使用者執行惡意腳本，進而下載不同的惡意竊密程式來竊取憑證等重要資訊。其中一種透過假 Google Meet (主流的視訊通訊服務之一) 頁面散播惡意竊密程式的行動

。使用者會收到看似合法 Google Meet 邀請函的電子郵件，邀請他們參加工作會議、討論或其他重要活動。一旦被誘騙，他們就會被導向一個假的頁面，顯示一個關於技術問題的彈出視窗。按一下此彈出式視窗就會啟動感染程序，進而傳送惡意竊密程式的有效酬載，例如：Stealc、Rhadamanthys 或 AMOS(視作業系統而定)。

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：

- CL.Downloader!gen92
- OSX.Trojan.Gen
- Trojan.Gen.MBT
- 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。

2024/10/18

近期UAT-5647威脅群組所發動的惡意活動

根據 Cisco Talos 發佈的報告，UAT-5647 駭客組織最近鎖定烏克蘭和波蘭的組織機構。這些威脅份子散佈兩種不同的下載器新變種，稱為 RustyClaw 和 MeltingClaw、一種新的 RomCom 惡意軟體變種，稱為 SingleCamper，以及 DustyHammock 和 ShadyHammock 後門。這一波攻擊自 2023 年底開始持續進行，重點在於資料外洩和建立對受攻擊環境的長期存取權。

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.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

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。

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求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。