保安資訊--本周(台灣時間2024/09/20)
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 46 萬 8,600 台受保護端點上總共阻止了 4,810 萬次攻擊。這些攻擊中有 81% 在感染階段前就被有效阻止：**(2024/09/16)**

- 在**8萬6,200**台端點上，阻止了**1,170**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬2,900**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**3萬500**台**Windows**伺服主機上，阻止了**7萬3,000**次攻擊。
- 在**5萬3,700**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,700**台端點上，阻止了**62萬6,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,800**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**13萬6,900**台端點上，阻止了**540**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,700**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**10萬7,900**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**563**台端點上，阻止了**8萬8,600**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 12 萬 6,800 個受保護端點上阻止了總計 330 萬次攻擊。**(2024/09/16)**

- 使用網頁信譽情資，在 **118.2K** 個端點上阻止 **300** 萬次攻擊。
- 攔截 **18.3K** 個端點上 **255.2K** 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 **7.6K** 個端點上攔截 **63.3K** 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 **227** 個端點上攔截 **6.5K** 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。

2024/09/19

北韓駭客組織：Appleworm透過武器化的Python套件傳送遠端存取木馬：PondRAT

據報導，一個如火如荼進行中的網路攻擊行動，涉及提供 Linux 和 macOS 後端程式的武器化 Python 套件，稱為 PondRAT。此攻擊行動據信是由北韓駭客組織：Appleworm(又稱為 AppleJeus、Citrine Sleet、Gleaming Pisces) 所發動。作為其攻擊媒介的一部分，惡意套件會上載至 PyPI，目的是取得供應鏈供應商及其客戶的存取權限。感染鏈涉及執行編碼程式的多個階段，最終導致下載和執行 PondRAT 惡意程式，該惡意程式與已知的 macOS 遠端管理工具 POOLRAT 有相似之處。

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：

- Downloader
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse

- WS.Malware.1
- 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。

2024/09/19

新發現鎖定GitHub使用者以散播Lumma惡意竊密程式的網路釣魚行動

CERT-AGID (義大利類似 TWCERT／CC 台灣電腦網路危機處理暨協調中心) 報告 Lumma 惡意竊密程式所新涉入的網路攻擊行動。在此網路攻擊行動中，GitHub 用戶會收到聲稱來自「GitHub 安全團隊」、主旨為『IMPORTANT！Security Vulnerability Detected in Your Repository (Issue #1)』的網路釣魚郵件。這些電子郵件以虛構的安全漏洞警告收件者，並引誘他們點擊一個可疑的連結。點選連結後會出現執行惡意 PowerShell 程式碼的欺騙性警告，導致下載並執行 Lumma 惡意竊密程式。此惡意軟體會竊取使用者的敏感資訊，包括登入憑證和個人資料。

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.Rgasm-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspOpen!gen11

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：

- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

2024/09/18

在真實網路情境上發現Gomorrah惡意竊密程式的最新變種

在真實網路情境上已經發現 Gomorrah 惡意竊密程式的最新變種。Gomorrah 以惡意軟體即服務 (Malware-as-a-Service：MaaS) 模式出售。該惡意軟體的設計者也還在積極開發，並已宣佈即將推出最新 5.5 版本。Gomorrah 具有從遭入侵的端點擷取敏感資訊的功能。目標資料包括儲存在網頁瀏覽器、加密貨幣錢包、系統資訊、憑證、組態檔案、FTP 用戶端資料、授權金鑰等的資訊。

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-RgPst!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- 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 634

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。

2024/09/17
防護亮點：賽門鐵克的行為分析技術(SONAR)徹底拆解BatCloak混淆技術!

批次檔淪為混淆化惡意程式的自動化載入工具

批次檔 (通常簡稱為 “.BAT” 檔) 是一種簡單的純文字檔，它包含一系列命令，用於在 Windows 作業系統上按順序來自動執行程式和應用程式，而無須逐一手動操作。它們已經存在很長時間，與許多其他常見作業系統工具一樣，也可以用於惡意目的。有越來越多的 BAT 檔被濫用於載入攻擊鏈不同階段的惡意程式。

BatCloak 惡意軟體混淆引擎，以高明手法掩護惡意軟體躲避安全軟體的偵測(FUD)

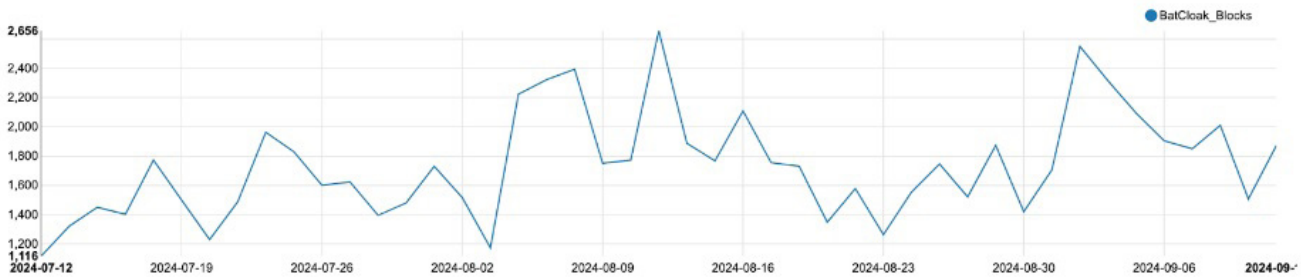
BatCloak 就是這樣一種惡意工具，用來繞過安全軟體、滲入電腦網路並傳遞各種惡意軟體。BatCloak 產生的批次檔案會混合使用壓縮、加密、多型 (polymorphism) 等手法進行高度混淆，以躲避檔案掃描和模擬引擎的偵測。在安全產業中，這些惡意軟體通常被稱為「完全無法被偵測有異的惡意軟體」或 FUD(Fully Undetectable)， (請勿與該縮寫的另一種用法混淆，該縮寫用於描述目的在散佈恐懼 (Fear)、不確定性 (Uncertainty) 和懷疑 (Doubt) 的可疑資訊)，但必須說這些惡意軟體顯然並非完全無法偵測，它們只是期望不被偵測到而已。這些批次檔案接著會利用 LOTL(就地取材) 攻擊鏈 (LOTL 或「Living Off The Land」攻擊是一種網路攻擊，利用被入侵系統上已有的合法工具) 來載入並執行各種有效酬載。BatCloak 已在多個攻擊行動中被用來傳送各種惡意軟體，包括各大家族的惡意竊密程式和遠端存取木馬 (RAT)，例如：AgentTesla、AsyncRAT 和 Snake Keylogger。

賽門鐵克端點防護／安全上的行為分析技術(SONAR)

SONAR 是賽門鐵克安全防護中，多掃毒引擎之一也是不可或缺的一層，非常適合偵測和攔截具有攻擊性混淆的惡意軟體。SONAR 會追蹤並分析所有程序的行為，包括作業系統的行為。透過檔案掃描和模擬很難偵測到的 LOTL 攻擊和惡意軟體，可以在早期階段透過行為方式偵測，並在有效酬載執行之前加以攔截。

Symantec 透過下列偵測成功阻擋數以千計的 BatCloak 攻擊：

- SONAR.BatCloak!gen1
- SONAR.BatCloak!gen2



欲瞭解有關賽門鐵克端點防護／安全上的多掃毒引擎之一的行為分析技術 (SONAR：Symantec Online Network for Advanced Response)？請點擊此處。

欲瞭解管理行為分析 (SONAR)，請點擊此處。

欲瞭解 SONAR 如何與賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 整合，請點擊此處。

2024/09/16

Fireant(APT31)駭客組織導入新工具發動對亞太地區政府單位的網路攻擊行動

與中國有關聯的駭客組織 Fireant(也稱為 Mustang Panda 或 APT31) 最近被觀察到在針對亞太地區政府單位的間諜攻擊中使用新工具，包括 PUBLOAD、FDMTP 和 PTSOCKET。這些工具透過 HIUPAN 蠕蟲變種部署，從遭入侵的電腦收集和滲出相關檔案 (.DOC、.DOCX、.XLS、.XLSX、.PDF、.PPT 和 .PPTX)。該駭客組織還濫用網址附件進行魚叉式網路釣魚行動，傳送 DOWNBAIT 等惡意下載工具，隨後再部署 PULLBAIT 和 CBROVER 等惡意軟體。

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-Rd32!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。

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.Cobalt
- 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
- 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

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。

2024/09/16

手機／行動裝置銀行木馬程式：Ajina

Ajina 是最近發現的機／行動裝置銀行木馬程式，主要針對中亞地區。該惡意程式專門竊取使用者包括銀行在內的機密資料，也會攔截雙因子認證 (2FA) 資訊。Ajina 惡意程式會偽裝成銀行、線上付款、宅配等各種合法 APP 散佈。散佈此惡意軟體的行動至少從 2023 年 11 月開始一直活躍至今。此惡意軟體的已知傳播媒介之一，是透過大量新建立 Telegram 帳戶傳送精心製作的訊息和惡意連結給毫無戒心的受害者。

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：

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
- 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。

2024/09/16

隱匿式惡意軟體鎖定美台國防工業會議與會者為目標

據報導，有惡意軟體涉入的網路攻擊行動，鎖定即將舉行美台國防工業會議有關的單位進行攻擊。受害者被偽裝成合法報名表 PDF 的 .ZIP 壓縮檔案和 .LNK 捷徑檔所誘騙。一旦開啟，LNK 檔案會執行指令，將誘餌的 PDF 檔案和可執行檔置於啟動資料夾中以達到常駐目的。可執行檔隨後會下載並在記憶體中執行其他內容，以避免被安全偵測到。惡意軟體透過與一般流量混合的網路請求，將敏感資料滲出到攻擊者操控的伺服器，使其更難被偵測到。

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：

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：

- CL.Suspexec!gen157
- Scr.Malcode!gdn14
- Scr.Mallnk!gen4
- Trojan Horse
- Trojan.Gen.9
- WS.Malware.1

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。

2024/09/13

在Gecko Assault網路攻擊行動中，散佈Mekotio和Mispadu惡意軟體

SCILabs 研究人員報告一個名為 Gecko Assault 的全新惡意行動。威脅份子散佈歸屬於 URSA／Mispadu 和 Mekotio 惡意軟體家族的兩種不同有效酬載。散佈有效酬載具有滲出銀行資訊、竊取瀏覽器儲存資料以及各種憑證的功能。在攻擊鏈中，威脅者開採濫用各種漏洞、惡意 AutoIt 腳本以及 DLL 劫持技術，其中合法的 GoToMeeting 應用程式可執行檔會被用來注入惡意 DLL 檔案。此行動主要鎖定拉丁美洲地區的使用者。

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-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.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mekotio
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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。

2024/09/13

狼狽為奸：AutoIt類型的憑證刷新程式與StealC惡意竊密程式攜手合作

在真實網路情境上發現到一個散播 StealC 惡意竊密程式的全新網路攻擊行動。攻擊的初始階段使用 Amadey 惡意軟體將該惡意竊密程式載入目標端點。在傳送 StealC 有效酬載的同時，攻擊者還會使用一個 AutoIt 類型的憑證刷新程式惡意軟體。憑證刷新程式的功能是在 kiosk 模式 (沒有任何明顯介面的瀏覽器全螢幕模式) 下啟動一個獨立的瀏覽器視窗，提示受害者輸入憑證。如果使用者上當，輸入的憑證就會被 StealC 惡意竊密程式竊取。

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-TskReg!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!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。

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.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: Bad Reputation Application Activity
- System Infected: Bad Reputation Application Network Activity
- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/09/13

Hadooken--以Weblogic伺服器為目標的Linux平台上全新惡意軟體

Hadooken 是針對 Oracle Weblogic 伺服器的新 Linux 惡意軟體。在攻擊鏈的初始階段，威脅者會開採濫用已知的漏洞、伺服器配置錯誤，或使用脆弱或其他已被外洩的憑證，來存取目標環境。在易受攻擊的伺服器上執行時，Hadooken 會注入兩個不同的有效酬載--Tsunami 惡意軟體和另一個用於挖掘加密貨幣的二進位檔案。

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
- Scr.Malcode!gdn14
- 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.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

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，可防止惡意軟體在系統上植入或執行。DCS 可以保護 Linux 伺服器防止從暫存檔案或其他可寫入位置執行惡意軟體，這是惡意軟體中使用的一種技術。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。

2024/09/13

ShrinkLocker勒索軟體：利用BitLocker進行加密和系統破壞

ShrinkLocker 是最近發現的勒索軟體，它利用 BitLocker (一種合法的 Windows 功能) 來加密資料，並將使用者鎖在系統之外。與傳統勒索軟體不同，ShrinkLocker 利用 BitLocker 的安全開機分割區，使解密變得極為困難。惡意軟體首先會識別並鎖定適合的作業系統。它會修改與 Remote Desktop Protocol (RDP) 和 Trusted Platform Module (TPM) 相關的關鍵系統登錄設定。ShrinkLocker 接著會將非開機磁碟分割縮小 100MB、格式化這些磁碟分割，並重新設定開機檔，可能會破壞系統的穩定性並使其無法修復。此外，它還會將資料滲出到命令控制伺服器 (C&C)，並刪除日誌、防火牆規則和排程工具，以掩蓋其行蹤。

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

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.ShrinkLocker
- Scr.ShrinkLocker!g1
- Web.Reputation.1
- WS.Malware.1

2024/09/13

影片剪輯軟體CapCut(剪映)被利用成為網路釣魚行動的誘餌

熱門影片剪輯軟體：CapCut 遭利用成為網路釣魚行動的誘餌。涉入最新攻擊行動的惡意套件，內含合法的 CapCut 應用程式、JamPlus 建立工具和有害的「.lua」腳本。執行應用程式會觸發 JamPlus 執行腳本，然後從遠端伺服器下載並執行最終的有效酬載。

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-Http!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen205
- ISB.Downloader!gen221
- Trojan Horse

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。

2024/09/12

Veaty和Spearal：近期針對伊拉克政府的新興惡意軟體

據 CTA 會員 Check Point 報告，一個全新惡意軟體家族 Veaty 和 Spearal 涉入針對伊拉克政府基礎設施的攻擊行動。此惡意軟體採用多種技術，包括被動模式的 IIS 後門、DNS 通道，以及透過遭入侵的電子郵件帳戶進行命令與控制 (C&C) 通訊。被動模式的 IIS 後端門似乎是賽門鐵克先前發現 GreenBug APT 集團較新的後門變種。初始攻擊鏈包含一系列具有雙重副檔名的檔案，目的是偽裝成合法的文件附件。這些檔案會觸發 PowerShell 或 PyInstaller 腳本的執行，最終部署基於 .NET 的後端惡意軟體 Veaty 或 Spearal 作為最終的有效酬載。

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-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-FlPst!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：

- Backdoor.Trojan
- 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.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。

2024/09/12

Yet Another Silly Stealer(YASS)惡意竊密程式

有觀察到一種新的資訊竊取程式，被稱為「Yet Another Silly Stealer」(YASS)。雖然 YASS 與 CryptBot 有某些相同之處，但 YASS 也有其獨特之處。該研究將 YASS 與 CryptBot 作比較，強調 YASS 獨特的程式碼，並透過稱為 MustardSandwich 的多階段下載器傳送。此下載程式透過 .LNK 的 Windows 捷徑檔案執行，包含兩個 JScript 階段和兩個 PowerShell 階段，其中第一個 PowerShell 指令碼透過 ActiveXObject 執行。下載程式的最後階段負責擷取多重有效酬載或單一有效酬載，以便在目標機器上執行。

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-Http!g2
- ACM.Ps-Mshta!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!gen111
- Trojan.Gen.MBT
- WS.Malware.1
- 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。

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**。