保安資訊--本周(台灣時間2024/09/06)
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 47 萬 3,300 台受保護端點上總共阻止了 4,820 萬次攻擊。這些攻擊中有 81.2% 在感染階段前就被有效阻止：**(2024/09/02)**

- 在**8萬5,900**台端點上，阻止了**1,190**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬9,100**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**72**萬次攻擊。
- 在**5萬3,500**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**82萬1,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,600**台端點上，阻止了**240**萬次嘗試利用的應用程式漏洞。
- 在**13萬3,200**台端點上，阻止了**520**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5萬8,000**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬2,900**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**615**台端點上，阻止了**9萬1,700**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 11 萬 9,900 個受保護端點上阻止了總計 340 萬次攻擊。**(2024/09/02)**

- 使用網頁信譽情資，在 **111.3K** 個端點上阻止 **310** 萬次攻擊。
- 攔截 **18.8K** 個端點上 **279K** 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 **6.9K** 個端點上攔截 **72.8K** 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 **219** 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。

2024/09/05

Acab惡意竊密程式

Acab 是最近在真實網路情境上發現的一種採用 Python 撰寫的惡意竊密程式。此惡意軟體的程式碼與另一種稱為 1312 的惡意竊密程式有一些相似之處。Acab 具備從受感染端點擷取各種機密資訊的功能，包括憑證、銀行資訊、加密錢包資料、應用程式資料／權杖 (tokens)、儲存在網頁瀏覽器中的各種資訊等。

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：

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.Acab
- WS.SecurityRisk.4

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。

2024/09/05

WordPress網站的捐贈外掛程式(Plugin)GiveWP：存在CVE-2024-5932安全性漏洞

CVE-2024-5932 是最近被揭露，會影響 WordPress 網站的捐贈外掛程式 (Plugin)：GiveWP，這是 WordPress 的捐款與募款平台外掛程式。此漏洞允許在 3.14.1 或以下受影響版本的外掛惡意注入。成功開採濫用此漏洞，未經認證的攻擊者可注入任意 PHP 物件，進一步導致在受攻擊應用程式的上下文中執行任意程式碼。外掛程式的修補版本 3.14.2 已經發佈。

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: WordPress GiveWP CVE-2024-5932

2024/09/05

有效酬載生成框架：MacroPack所產出有效酬載在最新的行動中大肆被散佈

Cisco Talos 的資安研究人員最近觀察到，在一系列惡意活動中，有人利用稱為 MacroPack 的有效酬載生成框架來建立各種有效酬載。攻擊者一直在使用 Word、Excel 或 PowerPoint 誘餌，一旦打開就會執行惡意 MacroPack VBA 程式碼，最終導致有效酬載的傳送和執行。散佈的有效酬載包括 Brute Ratel 和 Havoc 後期攻擊工具，以及 PhantomCore RAT 的最新變種。

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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- 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。

2024/09/05

Funnelweb進階持續威脅(APT)駭客組織，濫用KTLVdoor後門來發動攻擊

趨勢科技的研究人員發現一個全新的基於 Golang 的後門軟體，稱為 KTLVdoor。此惡意軟體是由 unnelweb 進階持續威脅 (APT) 駭客組織 (也稱為 Earth Lusca) 所持有。KTLVdoor 是一款高度混淆的惡意軟體，有多個變種，同時支援 Windows 和 Linux 平台。功能方面，該惡意軟體能夠執行從 C&C 伺服器接收的指令和 shellcode，並在受感染的機器上執行各種檔案和目錄操作，包括檔案下載／上傳等。

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-Rd32!g1
- ACM.Ps-Sc!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
- Trojan.Gen.NPE
- Trojan.Gen.NPE.2
- 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。

2024/09/04

網路攻擊行動：SLOW#TEMPEST，針對中國的機構組織

最近發現一個被命名為 SLOW#TEMPEST 的惡意軟體攻擊行動，目標對象是中國的機構組織。攻擊鏈由 .zip 壓縮檔案形式的惡意垃圾郵件附件觸發，除 dll／exe 檔案外，還捆綁一個快捷列 .lnk 檔案。成功執行內附的內容可在目標環境中建立據點。透過這個據點，攻擊者可以執行進一步的策略、技術和程序 (TTPs) 來達到他們的目標 (例如：憑證收集、橫向移動、常駐和提權)。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- 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：

- Hacktool
- Hacktool.Iox
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2024/09/04

下載程式 Latrodectus 1.4 出現新版本：具備更進階的功能

最新版本 Latrodectus 下載程式已被觀察到，其特徵包括新的字串解混淆方法、經修訂的 C&C 端點，以及兩個額外的後門指令。感染鏈從嚴重混淆的 JavaScript 檔案開始，該檔案使用大量註解來增大檔案大小和複雜性，使分析變得複雜。惡意軟體隨後會擷取並執行隱藏程式碼，然後從遠端伺服器下載並安裝 MSI 檔案。此 MSI 檔案會載入混淆的 DLL 來執行惡意任務。

Latrodectus 於 2023 年 10 月首次被發現，主要透過 TA577 和 TA578 等威脅份子的垃圾郵件傳送。它能夠下載和執行額外的有效酬載、收集系統資訊並傳送至其 C&C 伺服器，以及終止程序等惡意活動。

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：

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.SuspBeh!gen609
- SONAR.SuspRename!g4

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!gen195
- Trojan.Gen.MBT
- W32.Silly!gen
- 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

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。

2024/09/04

Emansrepo惡意竊密程式

Fortinet 的研究人員報告一個新的 Python--based 惡意竊密程式，稱為 Emansrepo。此惡意軟體透過偽裝成採購發票或訂單的網路釣魚行動散布。最初的攻擊鏈初期階段依不同的攻擊行動而有所不同，可能會利用不同的附件，例如：.html 或 .7z。植入 Emansrepo 有效籌載具有從受攻擊的端點收集各種機密資料的功能，包括憑證、銀行資訊、加密錢包、瀏覽器和下載歷史、自動填寫資料，以及從各種磁碟位置滲出文字／文件檔案。

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：

自適應防護技術(包含於SESC)：

- ACM.Btsad-Lnch!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- 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：

- CL.Downloader!gen92
- Infostealer
- ISB.Dropper!gen1
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- ISB.Downloader!gen523
- Scr.Heuristic!gen21
- Scr.Malarchive!gen1
- Scr.Malcode!gen
- Scr.Malcode!gen160

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Malscript
- 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.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。

2024/09/04

Zharkbot 惡意軟體

Zharkbot 是一種基於 C++ 的惡意程式載入器，最近觀察到一些攻擊行動中，它經由 Amadey 木馬程式來植入。Zharkbot 採用多種反分析、反 VM 和沙箱偵測／逃避技術。一旦進入被攻擊的機器，惡意軟體會嘗試將其自身複製到暫存資料夾，並設定執行排程任務，以建立常駐的能力。Zharkbot 具備在受感染端點下載和執行任意有效酬載的功能。

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

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspBeh!gen667
- 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.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：

- Audit: Bad Reputation Application Activity
- 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。

2024/09/04

Traccar 5存在CVE-2024-24809及CVE-2024-31214安全性漏洞

CVE-2024-24809 和 CVE-2024-31214 是最近被揭露的安全性漏洞，會影響 Traccar 5(一個開放源碼 GPS 追蹤系統)。這兩個漏洞的 CVSS 風險評分分別為 8.5 和 9.7。成功開採濫用有受影響的產品版本 5.1 至 5.12，可讓未認證的攻擊者進行路徑遍歷和不受限制地上傳任意檔案。此漏洞可能導致進一步的攻擊，例如：在受影響的實體上執行遠端程式碼。產品供應商已在產品 6.0 版本中發佈修補程式解決該漏洞。

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: Traccar Arbitrary File Upload Vulnerability CVE-2024-31214
- Web Attack: Traccar Path Traversal Vulnerability CVE-2024-24809

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，針對此漏洞提供如下的多層級保護 Windows 和 Linux 伺服器：

- 預防政策可防止任意檔案／惡意軟體在系統上植入或執行。
- 賽門鐵克 DCS 阻擋攻擊者利用的各種 RCE 方法。一些範例包括：
  - 上傳 Crontab 檔案：被 DCS 封鎖
  - 上傳核心模組：被 DCS 封鎖
  - 建立 udevd 規則 : 被 DCS 封鎖
  - 上傳 Windows 捷徑檔案 : 被 DCS 封鎖

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/04

CVE-2024-22319--存在IBM Operational Decision Manager中的JNDI注入漏洞

CVE-2024-22319 是 IBM Operational Decision Manager 中嚴重等級(CVSS 風險評分：9.8) JNDI 注入漏洞。IBM ODM 是一套全面決策自動化解決方案，可協助組織自動化及最佳化決策流程。攻擊者可透過 JNDI (Java Naming and Directory Interface) 將惡意程式碼注入傳送至特定 API 的未檢查參數，從而開採濫用此漏洞。透過在應用程式的輸入欄位注入惡意 LDAP 陳述，攻擊者可在未經授權的情況下存取敏感資料，甚至在目標系統上執行任意程式碼。此漏洞影響 IBM Operational Decision Manager 版本 8.10.3 至 8.12.0.1。賽門鐵克的網路防護技術入侵防禦系統 (IPS) 可阻止這些漏洞利用嘗試，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: IBM ODM JNDI Injection Vulnerability CVE-2024-22319

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 對於封鎖 JNDI 用於存取敏感資料或執行任意指令的政策建議。這主要是透過在 java 應用程式執行的沙盒中，控制可寫入檔案的位置以及可透過 java 執行的指令。。
- 基於對外連線的預防：DCS IPS 有能力封鎖到公共網際網路的外向連線，並將伺服器工作負載和容器化應用程式所需的 LDAP、HTTP 和其他流量限制到內部可信賴系統。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/03
防護亮點：賽門鐵克雲端沙箱，瓦解新興惡意程式的「零日」威脅

在安全領域中，建立立足點是惡意威脅者在鎖定目標組織中窺探和竊取資訊、執行搜尋和進行橫向移動最重要的第一步。我們經常看見組織收到惡意連結、可執行檔案、Office 文件檔、腳本，包含各種威脅的壓縮檔案或者其中一個作為起點導致另一個的組合，然後在整個威脅鏈中發動隱蔽攻擊，進而入侵目標組織的資訊環境，而目標組織發現時，常常為時已晚，已經造成嚴重的資安事故了。

經矇混程式碼的 VB 腳本

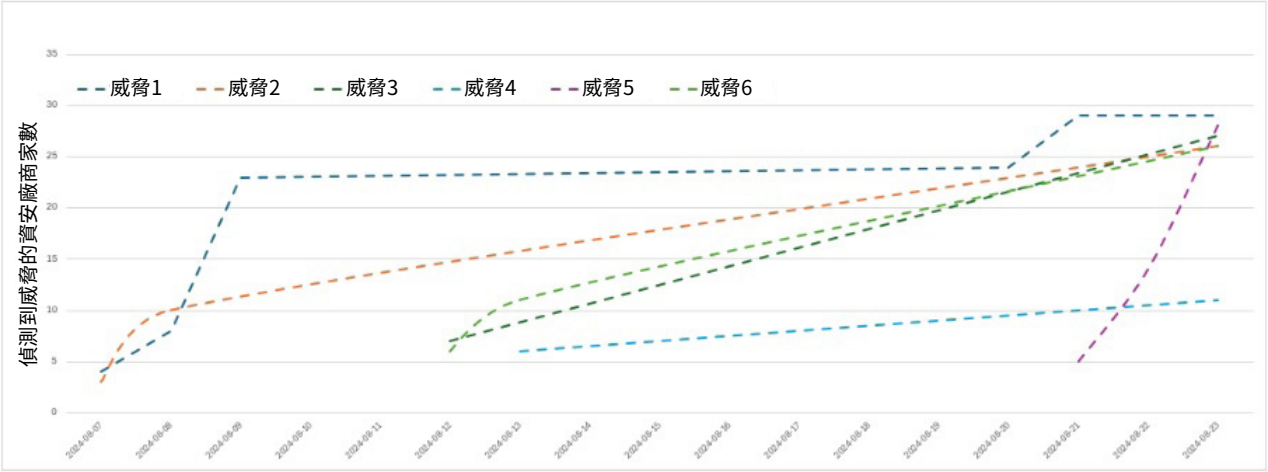
最近，Visual Basic Scripts (VBScript 檔案) 是這種威脅的常見例子。我們觀察到 VBS 和 VBE (已編碼的 VBScript 檔案) 被打包在檔案中，並傳送給不知情的使用者，這些檔案看起來像是圖片檔 (IMG-50012-3067.7z)、文件檔 (Docu_720001.7z)、預訂確認函／收據 (Reservations_00206PDF.7z、Booking_No1162808.rar) 或其他取名為需要使用者開啟和確認的有益無害的檔案。一旦開啟，這些腳本會解密、解壓縮並將較小的有效酬載傳送至本機，或從攻擊者控制的遠端伺服器下載惡意有效酬載。傳統的防毒軟體 (AV) 掃描一直在努力跟上這些攻擊，但由於這些腳本是文字格式，且被 IT 部門廣泛用於日常的業務運作，因此攻擊者可以濫用這些腳本所執行的機器資源來進行掩護、混淆，或使分析變得非常複雜且耗費大量資源。

賽門鐵克雲端沙箱：提供「零日」防護

賽門鐵克雲端沙箱透過利用投入密集的資源的靜態掃描～這是遠超乎運行在端點上模擬偵測技術、頂尖的行為監控和偵測技術 (可關聯所有可用的中繼資料，以偵測此類惡意軟體)，針對上述攻擊提供「零日」防護。這些 VBS／VBE 腳本不斷演進，以躲避包含經混淆的網址和傳統防毒解決方案；然而賽門鐵克雲端沙箱提供更全面的防護，可偵測從混淆機制和可疑技術，到躲避靜態層和被檢測威脅行為的網路物件。在長時間追蹤各種 VB 下載程式後，我們發現賽門鐵克雲端沙箱可提供針對此惡意軟體的「零日」防護 (通常是在檔案建立後幾分鐘內首次出現)，比社群獲得針對這些下載程式的強大防護還要早許多天。

根據「資安術語」的定義： 所謂「day zero(零日)」是指前所未見的惡意軟體發佈到真實網路情境上的那一天，因此對資安產品來說完全未知。相對於「zero-day(零時差)」(也稱為 0-day)一詞，「零時差」是指軟體或硬體中的漏洞，廠商通常不知道該漏洞，也沒有修補程式或其他修復方法。廠商有「零」天的時間準備修補程式，因為該漏洞已被描述或被開採濫用。

偵測到威脅的資安廠商數量



一旦在賽門鐵克雲端沙箱中偵測到特定的檔案，所有沙箱客戶都會立即受惠於已知的處理方式，而所有賽門鐵克客戶則會在幾分鐘內受益於已知的處理方式，因為所有賽門鐵克產品都會參照使用到我們的全球情報網路 (GIN)。

欲瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲瞭解更多有關賽門鐵克郵件安全雲端安全服務(Email Security.Cloud)的電子郵件掃描順序，請點擊此處。
欲瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全完整版(SESC)的端點偵測和回應(EDR)功能，請點擊此處。
欲瞭解更多有關賽門鐵克郵件安全雲端服務的(Email Security.Cloud)與資料外洩防護(DLP)的整合功能，請點擊此處。

2024/09/03

Stone Wolf威脅攻擊者發動～Meduza Stealer惡意軟體涉入針對俄羅斯公司的網路攻擊行動

據報導，Stone Wolf 威脅攻擊者針對俄羅斯公司進行惡意攻擊行動。攻擊者使用冒充合法工業自動化供應商的釣魚電子郵件來傳送 Meduza Stealer 惡意軟體。攻擊媒介包括含有合法文件的壓縮檔，以及下載和執行 Stealer 有效酬載的惡意連結。此惡意軟體會從受攻擊的系統收集和滲出憑證、系統資訊和應用程式資料。

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.Mshta-Http!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!g1
- ACM.Wscr-Mshta!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g285

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：

- CL.Downloader!gen55
- CL.Downloader!gen111
- Scr.Heuristic!gen20
- Scr.Malcode!gen147
- Scr.Mallnk!gen13
- Trojan Horse
- WS.SecurityRisk.4
- 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

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。

2024/09/03

WailingCrab：假冒VPN騙局的WikiLoader惡意程式後繼新變種

Palo Alto 最近一份報告顯示，WailingCrab 是 WikiLoader 惡意程式後繼新變種，透過搜尋引擎中毒(SEO)／購買搜尋排名和假冒的 GlobalProtect VPN 軟體散佈。此行動主要針對美國高等教育和運輸業。攻擊途徑與手法涉可拆解成多個階段，例如：DLL sideloading、shellcode injection，以及使用 MQTT 進行命令與控制。攻擊者採用各種迴避技術，例如：偽造錯誤訊息、程序檢查及加密。惡意載入程式的進階策略還利用受攻擊的 WordPress 網站和雲端 Git 儲存庫作為基礎架構。

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

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.IcedID

- Trojan.Wikiloader!gen2
- 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。

2024/09/03

Luxy惡意竊密程式

Luxy 是最近新發現的惡意軟體，同時具有惡意竊密程式和勒索軟體的功能。Luxy 會從受感染的機器中收集各種機密資訊，包括憑證、瀏覽器資料、cookie、加密貨幣錢包等。勒索軟體模組使用 AES256 演算法來加密受感染端點上的檔案。加密完成後，勒索通知會要求受害者支付贖金，並讓受害者透過 Discord 與攻擊者聯絡。

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.C

2024/09/02

網路罪犯利用SpyNote攻擊馬來西亞的數位生活方式

在世界各地，電子商務 (購物)、服務導向 (外送、叫車……等按需要服務)、數位支付和交易平台等安卓平台 APP 廣受歡迎。它們已經成為數位生活方式不可或缺的一部分，滿足了各個市場對便利、具成本效益服務不斷增長的需求。這些 APP 滿足了消費者對效率、便利性和省錢的需求，使其成為日常生活中不可或缺的工具。

由於這些 APP 在全球大受歡迎，越來越多的網路罪犯利用這些平台作為社交工程的門戶，以擴大他們的行動規模，讓他們能夠將影響、收益和覆蓋範圍最大化。

在最近的一個例子中，賽門鐵克在馬來西亞觀察到一個行動--快速數位化的國家之一--其中一種名為 SpyNote 的遠端存取特洛伊木馬／間諜軟體變種正在散播，並偽裝成虛假的 APP (例如：promo.apk、promotion.apk、discounts.apk、cod.apk 和 delivery.apk)。目前還不清楚這些 APP 的傳播方式，不過很可能是透過惡意網站重新轉導向和／或簡訊。

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。

- AppRisk:Generisk

2024/09/02

CVE-2024-7593--Ivanti Virtual Traffic Manager(vTM)應用程式交付系統存在身分驗證繞過漏洞

CVE-2024-7593 是存在 Ivanti Virtual Traffic Manager (vTM) 的關鍵等級 (CVSS 風險評分：9.8 分) XML 身分驗證繞過漏洞。成功開採濫用此漏洞可讓攻擊者繞過認證並建立新的管理使用者。此漏洞可能導致在受影響的應用程式中執行任意程式碼。開發商已在更新的軟體版本中發佈修補程式，解決此漏洞。

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: Ivanti vTM CVE-2024-7593

2024/09/02

RAZR勒索加密軟體～採用雙重勒索戰術

RAZR 是最近發現的勒索軟體變種，濫用名為 PythonAnywhere 網路託管服務來上架惡意的二進位檔案。該惡意軟體使用 AES-256 演算法進行加密，並冠上 .raz 的副檔名。隨附的勒索贖金支付說明文字檔：README.txt 的內容，還威脅說，機密檔案不僅被加密，還會被洩漏。

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-Bcdedit!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g45
- SONAR.Ransomware!g34
- SONAR.SuspLaunch!g195
- 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
- Ransom.Raz
- 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 634
- System Infected: Trojan.Backdoor Activity 721
- 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。

2024/08/30

Corona：Mirai後繼新變種透過漏洞開採濫用進行散佈

Mirai 惡意軟體的後繼新變種：Corona 最近透過開採濫用 AVTECH IP 攝影機裝置的指令注入漏洞 (CVE-2024-7029) 傳播。該殭屍網路還試圖利用一些較舊的漏洞，包括華為路由器中的 CVE-2017-17215 和影響 Realtek 的 CVE-2014-8361。殭屍網路部署完成後，會嘗試透過開啟的 Telnet 連接埠連接其他主機。經注入的有效酬載可能會被攻擊者用於各種 DDoS 攻擊或在受影響的設備上執行指令。

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-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：

- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

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: Huawei Router RCE CVE-2017-17215
- Web Attack: Realtek SDK RCE CVE-2014-8361

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。

2024/08/30

LummaC2惡意竊密程式後繼新變種，透過PowerShell的執行來散佈

據報導，LummaC2 惡意竊密程式在最近的網路攻擊行動中利用混淆的 PowerShell 指令散佈。LummaC2 是基於 C 的惡意竊密程式，通常以惡意軟體即服務 (MaaS) 模式銷售。此惡意軟體的主要功能是從受感染的端點竊取機密資料，並將其滲出到攻擊者控制的 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.Stealer!gen2
- 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。

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：

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

2024/08/30

資安鐵律：下載程式還是從原廠網站下載～中東地區成為使用偽造Palo Alto VPN惡意軟體的攻擊目標

據報導，有針對中東地區組織的惡意軟體攻擊行動，攻擊者利用偽造 Palo Alto GlobalProtect VPN 用戶端欺騙使用者。此惡意軟體採用先進的技術，包括巧妙偽裝的命令與控制 (C&C) 架構，以及 Interactsh 等工具，來與特定主機名稱通訊並監控感染進度。它可以執行 PowerShell 指令、管理程序和加密資料。此外，它還結合複雜的迴避技術來繞過沙箱並避免偵測。

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
- 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
- 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。

2024/08/30

具有先進且複雜的功能，並持續精益求精：X-FILES惡意竊密程式，將會令人不寒而慄

X-FILES 是一款以 C 語言寫成的惡意竊密程式，在地下論壇積極宣傳，並持續精益求精。與許多其他惡意竊密程式一樣，它的目的是從受感染的系統中竊取並滲出敏感資訊，包括瀏覽器資料、cookie、密碼、自動填寫資料、信用卡資訊和加密貨幣錢包的詳細資訊。該惡意軟體包括自訂記錄系統、Telegram 通知和自動更新等功能，以及針對獨立國協的地理封鎖和定期清理相關記錄以逃避偵測等安全措施。此外，即將推出的 VNC 設定收集和自動密碼解密等功能顯示其仍在持續開發中，因此 X-FILES 對組織而言是一項重大威脅。

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.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.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: TLS v1 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。

2024/08/30

CVE-2024-38653--存在Ivanti Avalanche中的XXE漏洞

CVE-2024-38653 是一個高度嚴重 (CVSS 風險評分：7.5 分) 的 XML External Entity (XXE) 漏洞，會影響 Ivanti Avalanche 的 SmartDeviceServer。成功開採濫用此漏洞可讓未經驗證的遠端攻擊者讀取伺服器上的任意檔案。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: XML External Entity Attack

2024/08/30

伊朗駭客集團：Elfin部署「Tickler」後門程式

伊朗駭客集團：Elfin (也稱為 APT33，Peach Sandstorm) 已被發現到部署一個全新的客製化多階段後門程式，稱為 Tickler。此惡意軟體已針對美國和阿拉伯聯合大公國 (UAE) 的政府、國防、衛星、石油與天然氣部門。該惡意程式針對數以千計的組織進行密碼潑灑 (password spray) 攻擊，並利用 Microsoft Azure 基礎架構進行命令與控制 (C&C)，透過詐騙、攻擊者控制的 Azure 訂閱來運作。

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-Reg!g1
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1
- WS.Reputation.1

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。

2024/08/29

針對日本工會工人的網路釣魚行動

有人發現到針對日本工會員工的網路釣魚行動。網路犯罪份子冒充労働金庫 (R ō d ō Kinko)，俗稱 Rokin，以及全国労働金庫協会 (National Association of Labour Banks or Zenkoku R ō d ō Kinko Ky ō kai)，這兩個組織是日本獨特金融體系的一部分，主要在服務勞工的金融需求。該電子郵件 (主旨：労働金庫】【要返信】お客様の直近の取引における重要な確認について）警告可疑交易，並催促收件人透過詐騙連結來驗證他們的帳戶--意圖竊取個人資訊的企圖。

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)。

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**。