保安資訊--本周(台灣時間2024/06/21)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 50 萬 6,500 台受保護端點上總共阻止了 5,600 萬次攻擊。這些攻擊中有 83.1% 在感染階段前就被有效阻止：**(2024/06/18)**

- 在**10萬3,100**台端點上，阻止了**1,640**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬1,700**台端點上，阻止了**1,040**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬4,100**台**Windows**伺服主機上，阻止了**850**萬次攻擊。
- 在**6萬1,000**台端點上，阻止了**220**萬次嘗試掃描伺服器漏洞。
- 在**1萬3,400**台端點上，阻止了**92萬7,100**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,600**台端點上，阻止了**320**萬次嘗試利用的應用程式漏洞。
- 在**16萬8,000**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**7,700**台端點上，阻止了**130**萬次加密貨幣挖礦攻擊。
- 在**10萬1,900**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**657**台端點上，阻止了**18萬6,200**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 17 萬 2,300 個受保護端點上阻止了總計 810 萬次攻擊。**(2024/06/18)**

- 使用網頁信譽情資，在 **160.5K** 個端點上阻止 **760** 萬次攻擊。
- 攔截 **27.5K** 個端點上 **409K** 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 **9.5K** 個端點上攔截 **87.6K** 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 **351** 個端點上攔截 **10.7K** 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。

2024/06/20

SquidLoader--威脅領域的全新惡意程式載入器

據報導，一種名為 SquidLoader 的新型惡意程式載入器，正利用網路釣魚行動來鎖定中文使用者大肆傳播。該惡意軟體採用各種規避和誘餌技術，以保持低調，避免被發現。在最近的行動中，發現該惡意程式載入器會發送 Cobalt Strike beacon。在啟動 C&C 通訊後，遞交的有效酬載將擷取遭入侵機器的相關資訊回傳給攻擊者，並等待進一步的命令。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- 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：

- Backdoor.Cobalt
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- 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。

2024/06/20

假冒人力資源部(人資：HR)的員工考核報告，出現在新一波網路釣魚行動中

威脅行動者繼續偽裝成人力資源部 (人資：HR) 的同仁，大肆傳播新一波的網路釣魚電子郵件。在賽門鐵克最近觀察到的一次網路釣魚行動中，含有網路釣魚的網址並偽裝成『員工考核』報告的電子郵件被發送給目標收件人。電子郵件主旨包含『重要』關鍵字--這是引誘收件人打開電子郵件的常用伎倆，而電子郵件本文則包含考核報告中特別強調的描述。為了瀏覽考核報告，收件人需要點擊會被安裝有竊取憑證的釣魚網址。

電子郵件主旨：

- 主旨：2024 年組織和員工評估調查-重要 (2024 Organization and Employee Evaluation survey -Important)
- 寄件者：人力資源部 <偽造的電子郵寄地址

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。

2024/06/20

亞洲國家電信公司成為中國間諜工具覬覦的目標

在一份最新發佈的報告中，賽門鐵克威脅獵手團隊對觀察到影響特定亞洲國家電信業者的網路攻擊行動進行分析。在一場可能早在 2020 年就開始的持續行動中，發現與中國攻擊組織有關的定制型間諜工具。攻擊中使用 Coolclient、Quickheal 和 Rainyday 等後門程式，以及其他用於竊取憑證、鍵盤側錄和通訊埠掃描的工具。

我們部落格文章中有更詳細的內容：利用中國間諜工具持續攻擊電信公司的網路攻擊行動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Coolclient
- Backdoor.Healquick
- Backdoor.Rainyday
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Malload!gen1
- 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。

2024/06/19

TA571駭客組織利用剪貼簿植入惡意腳本

最近觀察到 TA571 駭客組織在惡意垃圾郵件行動中利用惡意 HTML 檔案。這些檔案一旦被打開，就會複製一個惡意 PowerShell 腳本到用戶的剪貼簿，同時顯示一張圖片，說明所附文件已損壞，使用者需要按照指示的步驟操作。這些步驟要求使用者打開 PowerShell，貼上之後就會執行惡意腳本，進而部署第二階段的感染酬載。

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：

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：

- ISB.Heuristic!gen106
- ISB.Heuristic!gen107
- Phish.Html
- Trojan Horse
- Trojan.Malscript

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。

2024/06/19

Fickle(*善變的)惡意竊密程式

Fickle 惡意竊密程式是最近觀察到的一種用 Rust 撰寫的惡意軟體。攻擊者利用多階段攻擊鏈中的多種途徑與方法來發送惡意有效酬載。攻擊可能會以 Word 文件檔、網址鏈結檔或可執行檔來觸發，這些檔案會被注入或下載 PowerShell 腳本以繼續入侵。竊取的標的包羅萬象，包括加密錢包、瀏覽器和瀏覽器外掛程式相關敏感性資料、多種檔案類型以及許多通訊應用程式等。Fortinet 有發佈一份有關該惡意軟體更多的活動技術報告。

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：

- Infostealer
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mallnk
- Trojan.Malmsi
- Trojan.Mdropper

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2024/06/19

AzzaSec勒索軟體

AzzaSec 是另一種在真實網路情境上傳播的一般性勒索軟體。該勒索軟體會加密檔案並冠上 .AzzaSec 副檔名。該勒索軟體幕後的攻擊者會留下勒索贖金支付說明檔案，要求被害人採用比特幣支付檔案解密的贖金。

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：

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

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!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 568

2024/06/19

Diamorphine Linux rootkit出現新變種

一種名為 Diamorphine 的開源 LKM(可載入內核模組) rootkit 的新變種，在真實網路情境上被發現。該 rootkit 被威脅者用來隱藏惡意程序或在被入侵機器的權限提升。Diamorphine 利用特殊格式的資料包 (俗稱魔術包；Magic Packet) 在受感染的端點上執行任何指令。這個最新變種還新增退出功能，可以從記憶體中卸載 rootkit 內核模組。

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.NPE
- 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：

- Web Attack: Webpulse Bad Reputation Domain Request

於安全強化政策(適用於使用DCS)：

賽門鐵克重要主機防護系統：DCS～Data Center Security，針對此漏洞提供如下的多層級保護：

- Symantec Data Center Security 的預設鎖定政策可保護底層 UNIX 伺服器免受 rootkit 的攻擊，包括防止執行任意命令和限制對主要作業系統檔的讀取權限。
- DCS UNIX 強化政策預設情況下會鎖定 root 帳戶，以防止濫用管理存取權限。此外，還可以配置政策中的 DCS 網路規則，以限制伺服器與網際網路的接觸。

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。

2024/06/19

惡意廣告行動利用假冒軟體安裝程式引誘受害者

有人發現一個惡意廣告行動，引誘被害者下載偽裝成 Google Chrome和Microsoft Teams 等熱門軟體的安裝程式。受害者在搜尋引擎上搜索這些軟體關鍵字後，就會被引誘到網域名稱誤植 (typo-squatting) 的網站。這些安裝程式會部署一個名為 Oyster(也稱為 Broomstick) 的後門程式。Oyster 可用來收集遭入侵系統的資訊，管理與命令控制 (C&C) 伺服器的通訊，並具有遠端程式碼執行能力。

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-Rd32!g1
- ACM.Ps-Rgsvr!g1
- ACM.Rd32-Schtsk!g1

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.B
- 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: Rundll32 Suspicious Network Activity

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。

2024/06/19

惡意軟體載入工具：HijackLoader和Vidar惡意竊密程式鎖定Cisco Webex視訊會議和線上會議軟體的用戶

最近報告影響拉丁美洲和亞太地區使用者的惡意軟體行動。這些行動以思科 Webex Meetings App 等熱門商務軟體的使用者為目標，誘使他們下載受密碼保護且含木馬軟體的壓縮檔。在解壓並執行後，一個名為 Hijack Loader 的隱蔽惡意軟體載入器就會被啟動。然後，Hijack Loader 會替換閘道設定，使用 AutoIt 腳本部署 Vidar 惡意竊密程式。Vidar 惡意竊密程式的設計目的是收集憑證和敏感性資料，並將其滲出攻擊者所操控的命令與控制 (C&C) 伺服器。此外，該惡意竊密程式還能下載用於啟動 XMRig 挖礦程式的 Amadey Loader 等有效酬載，以及將加密貨幣交易重導向到攻擊者控制的錢包剪貼簿挾持軟體 (Clipper)。

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.Ps-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDrop!gen1

- SONAR.SuspBeh.C!gen18

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
- 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。

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。

2024/06/18

Rogue Raticate網路犯罪集團發起惡意垃圾郵件行動：惡意PDF導致NetSupport遠端存取木馬(RAT)

Rogue Raticate(又名 RATicate) 網路犯罪集團已活躍數年，因使用惡意電子郵件和遠端存取木馬攻擊企業而聞名。本周觀察到他們的另一起攻擊行動。惡意電子郵件的附件是一個內嵌惡意網址的 PDF 檔案 (例如：unpaid-7985652547.pdf、Paper-2445311685.pdf)。攻擊者使用兩種社交工程伎倆為誘餌--OneDrive 和 Adobe。如果用戶被成功誘騙點擊該惡意網址，他們將透過惡意流量導向系統 (Traffic Direction System，TDS) 進入其他通道，最終在其電腦上部署 NetSupport 遠端存取工具。

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

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.DLHeur!gen7
- Scr.DLHeur!gen10

2024/06/18
防護亮點：固若金湯的IPS防護技術，提供目錄遍歷攻擊堅若磐石的保護

目錄遍歷(Path Traversal)／路徑跨越(path traversal)漏洞

目錄遍歷漏洞又稱路徑跨越漏洞，是網路應用程式中的一個安全性漏洞，允許攻擊者存取網頁伺服器根目錄之外受限制存取的檔案和目錄。

目錄遍歷攻擊操弄網頁應用程式中引用檔案路徑的變數。攻擊者修改路徑變數，以便在目錄結構中向上移動或瀏覽到不同的目錄。通常會使用特定的序列來完成，例如：在 Unix 和 Windows 系統中分別使用『.../』或『...\』。攻擊者可能會在網址或輸入欄位中使用這些序列，試圖誘騙伺服器從文件的根目錄之外傳回檔案。

目錄遍歷漏洞是對使用者輸入的過濾／驗證不足造成的。目錄遍歷漏洞可能存在於網頁伺服器軟體和檔案中，也可能存在於伺服器上執行的應用程式碼中。

目錄遍歷在 CWE 前 25 個最危險軟體弱點清單和前 25 個頑固弱點列表中排名第 8。美國網路安全暨基礎設施安全局 CISA 在「已知成功利用漏洞列表(the Known Exploited Vulnerabilities Catalog-KEV)」目錄中列出 50 多個目錄遍歷漏洞。因此，目錄遍歷漏洞仍然是軟體產品中長期存在的一項缺陷。

目錄遍歷攻擊的危害程度

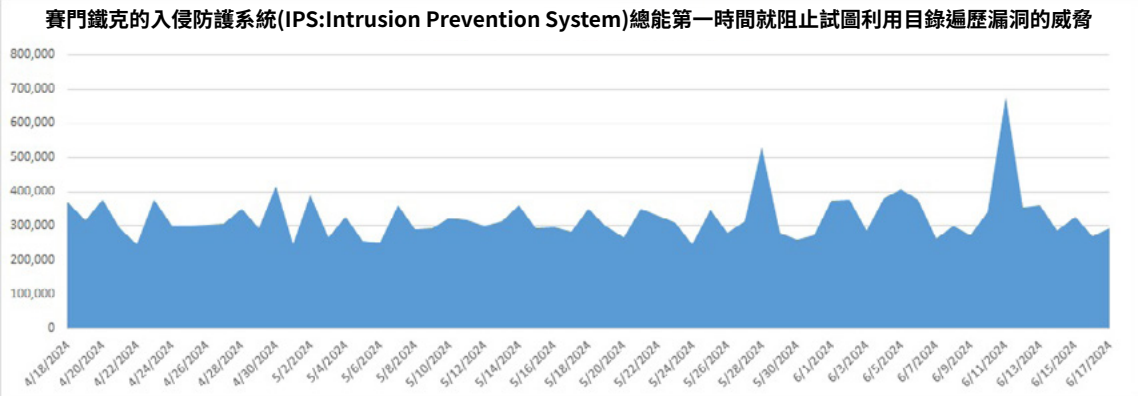
目錄遍歷攻擊對網頁伺服器和應用程式的安全性和完整性構成重大威脅：

- 目錄遍歷可導致未經授權存取儲存在網頁根目錄以外檔案中的敏感資訊。這可能包括系統檔案、設定檔甚至使用者資料。未經授權存取機密資料是對隱私的直接侵犯，並可能導致資訊失竊。
- 攻擊者可以讀取、修改或刪除關鍵檔，造成嚴重的系統故障或服務中斷。可能導致嚴重的停機、生產力損失甚至經濟損失。
- 成功的目錄遍歷攻擊可為攻擊者提供實施破壞性攻擊的能力。例如：存取某些系統檔可以提供有關伺服器結構、配置和安全措施的寶貴資訊。綜合來看，這些資訊可用在未來建立更複雜的攻擊。

目錄遍歷是一種嚴重的安全風險，會導致網頁伺服器和應用程式的隱私性、完整性和可用性嚴重受損。

賽門鐵克的網路層的防護技術

賽門鐵克的入侵防護系統 (IPS：Intrusion Prevention System) 總能第一時間阻止試圖利用目錄遍歷漏洞的威脅。IPS 平均每天可攔截超過 1 萬 3,000 台電腦，共高達 34 萬次的目錄遍歷攻擊。



賽門鐵克與時俱進的創新多層次零時差防護技術經證實可以有效防禦這些攻擊，包括但不限於以下措施：

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: Generic Directory Traversal 5
- Attack: Generic Directory Traversal 2
- Web Attack: Directory Traversal Exploitation Attempt
- Web Attack: Adobe Coldfusion Directory Traversal Vulnerability
- Attack: HTTP Apache Tomcat UTF-8 Dir Traversal CVE-2008-2938
- Web Attack: Adobe ColdFusion Directory Traversal Vulnerability CVE-2013-0629
- Web Attack: Apache Tomcat Directory Traversal CVE-2000-1210
- Web Attack: SCO Skunkware ViewSrc Directory Traversal CVE-1999-0174
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Web Attack: IBM Tivoli Directory Server Directory Traversal Vulnerability CVE-2004-2526

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。

2024/06/18

被惡意加料的Vortax虛擬會議軟體安裝檔：重創MacOS環境的用戶

最近一個利用開採濫用 macOS 漏洞的惡意竊密程式涉入一起攻擊行動。幕後的主使者是 markopolo 駭客集團，正肆無忌憚地瞄準加密貨幣用戶。他們利用一款名為 Vortax 的虛擬會議軟體被惡意加料後的二進位檔案，一旦下載並安裝，就會部署 Rhadamanthys、Stealc 和 Atomic macOS Stealer 等惡意竊密程式。

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：

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

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

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。

2024/06/18

開採濫用Docker引擎漏洞的挖礦劫持攻擊(Cryptojacking)行動

據觀察，一起全新的挖礦劫持攻擊 (Cryptojacking) 行動，以公開暴露的 Docker 引擎主機為目標。據推測，這與之前出現的 Spinning YARN 惡意軟體攻擊行動之幕後主使者有關聯。攻擊途徑與手法從掃描開放的通訊埠 2375 開始，並部署一個 Alpine Linux 容器。該容器透過綁定 Docker 主機的根目錄，授予攻擊者完全的系統存取權限。隨後，攻擊者透過建立取得並執行惡意 shell 腳本的 cron 作業來建立常駐能力。這些腳本會下載附加工具和有效酬載，使安全防護機制失效、資訊外洩、利用 SSH 協議進行橫向移動，並可能安裝挖礦劫持惡意軟體。

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：

- Linux.Trojan
- PUA.Gen.2
- 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。

2024/06/17

Rapax 勒索軟體

Rapax 勒索軟體，其二進位檔案最近被提交到一個公共惡意軟體分析和檢測平臺。在遭入侵機器上發現的勒索 (贖金支付) 說明檔的內容 (instruction.txt) 顯示，作者只專注於加密檔案，而不是採用資料滲出和雙重勒索戰術，要脅以支付等值於 5000 美元的比特幣為贖金才能解密。加密成功後，檔案會被冠上 .rapax 副檔名。根據檔名 (例如：inquiryfdp.exe)，這些惡意二進位檔案的幕後黑手似乎試圖將它們偽裝成與業務查詢相關的 PDF 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.Untrst-FlPst!g1
- ACM.Wmic-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g341
- SONAR.SuspLaunch!g340
- SONAR.SuspLaunch!g195
- SONAR.RansomGen!gen5

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.B!100

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。

2024/06/17
鎖定ESXi伺服器：Limpopo勒索軟體

據 Fortinet 報導，Limpopo 是一種全新的勒索軟體，主要針對易受攻擊的 ESXi 伺服器。該惡意軟體被公認是從被洩露的 Babuk 勒索軟體原始程式碼演生出來，並與 Socotra 和 Formosa 等其他勒索軟體有相關聯。據觀察，Limpopo 在傳播行動中影響拉丁美洲和泰國。該勒索軟體會加密使用者檔案並冠上 .Limpopo 副檔名。

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：

- Ransom.Babuk
- Trojan Horse
- WS.Malware.2

2024/06/17

SolarWinds Serv-U存在高風險弱點：CVE-2024-28995目錄遍歷漏洞

CVE-2024-28995 是最近被揭露的目錄遍歷漏洞，影響 SolarWinds Serv-U 受管的檔案傳輸 (MFT) 伺服器解決方案。如果成功開採濫用該漏洞，攻擊者就可以讀取受影響主機上的敏感資訊。雖然目前還沒有關於網路上被利用的報告，但原廠已經在產品 15.4.2 Hotfix 2 版本中修補被揭露的漏洞。

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：

- Attack: SolarWinds Serv-U Directory Traversal CVE-2024-28995

2024/06/16

Brain Cipher勒索軟體

投入勒索軟體的不法業者前仆後繼，在本防護公告中，我們將簡要地討論最近出現在威脅環境中一個使用 Lockbit 變種的勒索軟體。該組織在其勒索贖金支付說明檔案 ([randomID].README.txt) 中自稱為『Brain Cipher勒索軟體』，似乎在實施雙重勒索--滲出敏感性資料並對其進行加密。受害者可在該組織的 Onion 網站上使用加密 ID 與他們取得聯繫。

目前，他們所採用的策略、技術和程序 (TTPs) 仍不清楚，不過他們很可能會利用已知的攻擊策略進行初始存取，包括透過初始存取代理 (IAB)、網路釣魚、利用網際網路上應用程式中的漏洞或竄改遠端桌面協議 (RDP) 的設定。

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：

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!g6

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。

2024/06/16

狐假虎威：採用Chaos勒索軟體作怪的小嘍囉，冒名最活躍的勒索軟體集團 Lockbit

賽門鐵克最近觀察到一款 Chaos 勒索軟體後繼版本，正在四處流竄--加密單一台電腦，並在留下的勒索贖金支付說明檔 (readme.txt) 中聲稱自己是『Lockbit』。在此個案中，他們要求向指定加密錢包支付價值 180 美元的比特幣。

基於不同策略考量，小嘍囉等級的駭客團體和個體戶冒充知名駭客集團相當普遍。令人聞風喪膽的大惡霸可以促使更快地支付贖金。這種方法也會增加受害者的心理壓力，他們可能會認為來自像 Lockbit 這樣知名組織的威脅更嚴重，進而增加花錢消災的可能性。此外，不那麼老練的犯罪分子，通常會使用知名的名字來提高他們可信度和贖金行動的成功率。

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.HiddenTear!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。

2024/06/14

DISGOMOJI：在Discord上針對政府組織的惡意軟體行動

一種新出現的創新惡意軟體行動出現了，它利用 Discord 來進行命令和控制 (C&C) 操作，並採用表情符號 (emoji-based) 的協定，威脅行為者透過命令通道中的表情符號向惡意軟體傳達指令。該惡意軟體被命名為 DISGOMOJI，是一個用 Golang 編寫並以 UPX 封裝的 ELF2。它在 ELF 中包含預先寫入程式碼的身份驗證權杖和伺服器 ID，可存取 Discord 伺服器。

該行動幕後的主使者是 UTA0137 駭客集團，主要鎖定印度的政府組織。UTA0137 利用 Zenity 工具顯示惡意對話框塊，主要透過社交工程伎倆引誘使用者洩露密碼。與許多其他攻擊者一樣，UTA0137 在入侵後使用開源工具，包括 Nmap、Chisel 和 Ligolo。

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
- 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。

2024/06/13

OPIX勒索軟體

OPIX 是一種新發現的勒索軟體新變種，通常透過社交工程手法來傳播，例如：釣魚郵件和偷渡式下載。使用者被加密後的檔案名稱是以隨機字串，並冠上『.OPIX』副檔名來命名。例如：名為『test.txt』檔案會變成類似『B532D3Q9.OPIX』檔案。受害者會發現勒索軟體所留下的勒索贖金支付說明，通常檔名為『#OPIX-Help.txt』，指示他們在 48 小時內透過提供的電子郵件或 Telegram 聯繫攻擊者，否則他們被盜的資料將被出售給競爭對手並公佈在暗網上。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen16
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g340
- SONAR.SuspLaunch!gen4

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

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。

2024/06/13

傳播Koi惡意程式載入器／Koi惡意竊密程式的垃圾郵件行動

最近惡意郵件攻擊行動中，攻擊者似乎改變戰術，以避免被發現。在此個案中，他們不再採用典型直接發送帶有惡意連結的電子郵件方法，而是先發送討論隨機場景的良性電子郵件。如果收件人回覆並參與，攻擊者就會趁勝追擊並發送惡意連結。點擊該連結將進入特定的惡意網頁，並下載一個包含 Windows 捷徑檔 (.LNK) 的 ZIP 壓縮檔。該捷徑隨後將載入 Koi 惡意程式載入器／Koi 惡意竊密程式的有效酬載，來竊取 cookie、歷史記錄和登錄資訊等敏感性資料。

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.Ps-TJs!g1
- ACM.Ps-Schtsk!g1
- ACM.Schtsk-TJs!g1
- ACM.Wscr-Ps!g1
- ACM.Ps-Http!g2
- ACM.Wscr-Wscr!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g367

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：

- Scr.Mallnk!gen3
- Trojan.Malscript

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。