保安資訊--本周(台灣時間2024/09/27)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 5,200 台受保護端點上總共阻止了 4,660 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2024/09/23)**

- 在**8萬4,700**台端點上，阻止了**1,170**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬2,800**台端點上，阻止了**830**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬200**台**Windows**伺服主機上，阻止了**7萬3,000**次攻擊。
- 在**5萬2,700**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬700**台端點上，阻止了**63萬500**次嘗試掃描在**CMS**漏洞。
- 在**5萬1,700**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**13萬6,800**台端點上，阻止了**560**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬7,900**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**9萬7,300**台端點上，阻止了**750**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**529**台端點上，阻止了**6萬9,100**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 13 萬 7,900 個受保護端點上阻止了總計 400 萬次攻擊。**(2024/09/23)**

- 使用網頁信譽情資，在 **129.1K** 個端點上阻止 **370** 萬次攻擊。
- 攔截 **19.4K** 個端點上 **253.4K** 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 **7.9K** 個端點上攔截 **66.7K** 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 **310** 個端點上攔截 **7.3K** 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。

2024/09/26

針對運輸業的濫發垃圾郵件攻擊行動

研究人員最近揭露一項針對運輸業組織的濫發垃圾郵件攻擊行動。此攻擊來自已遭入侵挾持的郵件帳戶，並利用垃圾郵件中夾帶 .url 副檔名的附件檔案或可下載 .url 副檔名的網址，如果開啟這些 .URL 檔案，受害者的電腦會啟動外部微軟伺服器訊息區塊 (Server Message Block，SMB) 連線，以下載並執行遠端惡意可執行檔。

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
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspLaunch!g221
- SONAR.SuspOpen!gen11

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Guloader!gen3
- Scr.Malcode!gen102

- Trojan.Gen.MBT
- Web.Reputation.1
- W32.Silly!gen

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。

2024/09/26

SloppyLemming駭客組織涉入針對南亞和東亞組織的網路釣魚行動

報告指出，一個名為 SloppyLemming 的駭客組織一直積極針對南亞和東亞的組織，尤其是巴基斯坦和孟加拉。這個駭客組織使用開放原始碼的「敵我模擬扮演」框架，例如：Cobalt Strike 和 Havoc。攻擊鏈從釣魚電子郵件開始，通常包含緊急行動呼籲，促使受害者點擊連結，透過登入假冒 CloudFlare Worker 主控的入口網站。在最近一次事件中，該駭客組織利用 Dropbox 來上傳包含 WinRAR 已知漏洞 (CVE-2023-38831) 開採濫用攻擊的 RAR 檔案。該壓縮檔案內含一個作為誘餌的 PDF 檔案、一個偽裝成 PDF 的 EXE 檔案以及一個用於由可執行檔進行側載的 DLL 檔。

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!g
- ACM.Rd32-CPE!g1
- ACM.Rd32-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.Gen.MBT
- 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。

2024/09/26

修改自LockBit、Conti兩大勒索軟體的全新勒索軟體：DragonForce，正在鎖定全球的產業

已發現被稱為 DragonForce 全新勒索軟體，特色源於兩大勒索軟體家族：LockBit 和 Conti 的修改版本，目標是全球的製造業、房地產和運輸業。DragonForce 以勒索軟體即服務 (Ransomware-as-a-Service) 的營運模式，提供駭客圈雨露均霑的分潤分工計畫和各種攻擊管理工具。該組織使用 SystemBC 後門進行持久化 (取得常駐的能力)，並使用 Mimikatz 和 Cobalt Strike 等駭客工具，進行憑證收集和橫向移動。

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
- ACM.RegRun-TPs!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30

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.Cobalt
- 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

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。

2024/09/26

「Twelve-十二」攻擊組織志在摧毀與破獲而非金錢利益

成立於 2023 年的「Twelve-十二」攻擊組織，是為了回應俄羅斯與烏克蘭之間的衝突，據觀察所得，該組織目標是俄羅斯的政府組織，其策略包括透過勒索軟體加密檔案、透過抹除程式刪除檔案／系統以及滲出敏感資料等。根據最近發表報告所提供的分析，該組織的目標著重於破壞而非財務收益。

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

- Hacktool.Mimikatz
- Packed.Freeze!gen1
- Ransom.Lockbit!g6
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Webshell
- WS.Malware.1
- WS.Malware.2

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。

2024/09/25

KLogExe鍵盤側錄軟體和FPSpy後門程式，雙雙推出新版本

Sparkling Pisces(又名 Kimsuky、THALLIUM、Velvet Chollima) 威脅組織已導入最新版鍵盤側錄軟體：KLogExe 和後門程式：FPSpy。這進階持續威脅 (APT) 駭客組織以精密的網路間諜行動和先進的魚叉式網路釣魚攻擊而聞名。Sparkling Pisces 會引誘受害者下載並執行惡意程式的有效酬載。包括使用全新、前所未見的惡意軟體。KLogExe 會收集系統運行的資料 (執行中的應用程式、鍵盤按擊和滑鼠點擊) 並從遭入侵的機器中滲出。FPSpy 除具有鍵盤側錄功能之外，還進一步新增許多進階功能，例如：收集組態資料、系統資訊、下載／執行附加模組以及執行指令。

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-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。

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
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

2024/09/25

Foxtrot勒索軟體--源於MedusaLocker勒索軟體家族的後繼新變種

Foxtrot 是源於 MedusaLocker 勒索軟體家族的後繼新變種。該惡意軟體會加密使用者檔案，並冠上 .foxtrot70 副檔名。勒索 (贖金支付) 說明是以 .html 檔案的形式提供，檔案名稱為「How_to_back_files.html」。Foxtrot 具備刪除受感染機器上的磁碟陰影複製 (Volume Shadow Copy) 和 Windows 備份的功能。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen107
- SONAR.RansomLckbit!g3
- SONAR.SuspLaunch!g18

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.MedusaLocker
- 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

2024/09/24

PDiddySploit木馬惡意程式，假借名人醜聞文章散布

美國嘻哈大亨「吹牛老爹」Sean 'Diddy' Combs(P.Diddy) 近期成為多項嚴重指控的焦點，最近一項調查研究顯示，圍繞 Sean 'Diddy' Combs(又稱 P. Diddy) 的醜聞已被利用。攻擊者經常利用大眾對高知名度醜聞的興趣來散播惡意軟體，利用此話題誘騙毫無戒心的使用者下載惡意檔案。

這次涉入的木馬程式稱為 PDiddySploit，是源於開放原始碼的 PySilon 遠端存取木馬 (RAT) 的後繼新變種，以竊取敏感資訊和執行遠端指令而聞名。

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：

自適應防護技術(包含於SESC)：

- 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.Gen.MBT
- WS.Malware.1

2024/09/24

土耳其和保加利亞正遭受Remcos遠端存取木馬(RAT)的目標式攻擊

賽門鐵克最近發現到兩起正在進行中 Remcos 遠端存取木馬 (RAT) 涉入的目標式攻擊行動，這兩個攻擊行動來自同一個威脅發動者，目標是保加利亞和土耳其的公司。在保加利亞的攻擊行動中，他們使用歷久彌堅的發票社交工程伎倆 (電子郵件主旨：Плащане на фактура) 來引誘使用者，而在土耳其攻擊活動中，他們則使用跨境匯款的 SWIFT 轉帳社交工程伎倆 (電子郵件主旨：Gelen Swift Mesaj)。雖然社交工程手法不同，但作案手法相同：他們利用惡意的 .docx 檔案，濫用開採陳年老舊的漏洞 (CVE-2017-0199) 來注入遠端存取木馬程式。

CVE-2017-0199 是 Microsoft Office 和 WordPad 中陳年老舊漏洞，攻擊者可透過特製的 .docx 檔案執行遠端程式碼。這些檔案包含內嵌 OLE 物件，可連結至遠端惡意指令碼，例如：HTA 檔案。當受害者開啟文件時，連結的指令碼會自動下載並執行。

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：

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.Malcode.S!gen
- Web.Reputation.1

2024/09/24

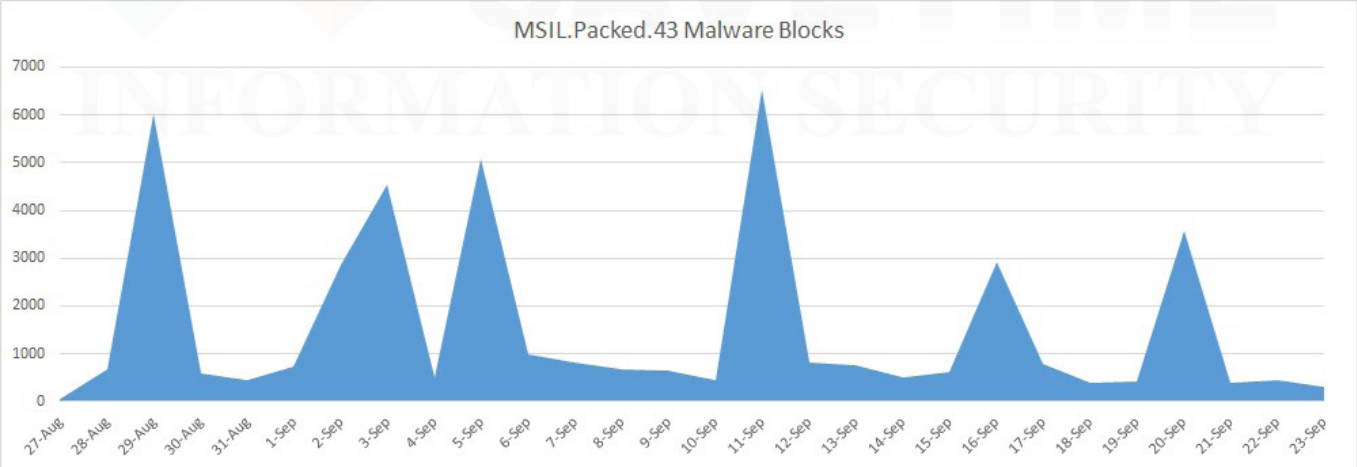
防護亮點：與時俱進的賽門鐵克靜態資料掃描器之.NET模擬器，再老練的駭客也討不到便宜

在現今快速演進的威脅環境中，網路攻擊已變得越來越複雜。Snake Keylogger、Formbook 和 Lokibot 等惡意軟體最近變種活動更加頻繁，並採用各種傳送方式，例如：釣魚電子郵件、惡意附件和偷渡式下載。這些技術最終會部署惡意的 .NET 有效酬荷，對組織造成重大風險。

.Net 是微軟在 2000 年代初推出的軟體開發框架，主要是為了讓程式設計更容易。支援 C#、VB.NET 等多種語言，.NET 程式會編譯成 Microsoft Intermediate Language (MSIL：中繼語言有時也稱為通用中間語言 (CIL))。執行時，即時編譯器 (JIT) 會將 MSIL 轉譯為機器程式碼。雖然 .NET 架構的設計初衷是為了幫助軟體工程師，但網路罪犯很快就找到濫用其功能以謀取自身利益的方法，他們通常使用特殊工具來混淆 .NET 應用程式的原始程式碼，以增加理解逆向工程和分析程式碼的挑戰性。

我們在 2024 年 5 月的公告中討論過賽門鐵克靜態資料掃描技術：SDS--Symantec Static Data Scanner，其中包含模擬器，是它主要功能之一。SDS 實際上包含好幾個模擬器，其中一個是進階的 .NET 模擬器，專門用來有效偵測並解除這些隱藏的威脅。它可發現隱藏在合法功能中的惡意程式碼，發現不尋常的修改或新增內容。它會模擬應用程式的執行，識別標準方法 (例如：Application.Run) 內的異常情況。最後它會在威脅發生時偵測並解除威脅，將潛在損害降到最低。

賽門鐵克持續成功阻擋數以千計以「MSIL」開頭的 .NET 惡意軟體攻擊。以下是上述 Snake、Formbook 和 Lokibot 攻擊的最新範例。



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。

欲深入瞭解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

欲深入瞭解賽門鐵克的端點多層次防護解決方案中「檔案檢測技術」如何保護裝置，請點擊此處。

2024/09/23

Nanocore遠端存取木馬(RAT)以發票為幌子透過惡意.xls檔案進行散播

Nanocore 遠端存取木馬 (RAT) 在前幾年非常盛行，現在已大幅減少，但仍有一些團體和個人，繼續在他們的網路攻擊行動中利用此遠端存取特洛伊木馬。最近一個案例是一個偽造發票的惡意垃圾郵件散播行動，其中作者發送一個惡意的 .XLS(invoice.xls)，被開啟後會從 Discord 伺服器擷取 Nanocore 的二進位檔案。

此遠端存取木馬 (RAT) 可讓攻擊者遠端控制受感染的系統、竊取檔案、按鍵記錄、竊取憑證，甚至啟動網路攝影機和麥克風進行監控。它的模組化設計可讓攻擊者透過外掛程式增強其功能，使其適用於各種惡意活動。

Nanocore 遠端存取木馬 (RAT) 的破解和遭洩露分享，助長其在網路犯罪活動中持續被濫用。這些版本經常在駭客論壇、網站，甚至社群媒體平台上分享和討論，讓更多人可以輕易取得。

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.Nancrat!gen4

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!gen173
- Trojan.Nancrat

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/09/24

SnipBot--源於RomCom惡意軟體的後繼新變種

Palo Alto 的研究人員報告 RomCom 惡意軟體的新變種：SnipBot。此惡意軟體允許攻擊者在受感染的端點上執行命令列指令，以及下載額外的任意模組。SnipBot 新導入一些混淆和新的反分析技術。雖然 RomCom 背後的威脅團體過去曾從事勒索軟體和資料滲出攻擊，但相信這個新變種主要是用於間諜活動。

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

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
- Web.Reputation.1
- Web.Reputation.3
- W32.Silly!gen
- 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。

2024/09/24

在真實情境手機／行動裝置上發現安卓平台上的Octo惡意軟體家族後繼新變種

在真實情境的手機／行動裝置上發現安卓平台上 Octo 惡意軟體家族的後繼新變種稱為 Octo2。此惡意軟體透過針對歐洲國家行動用戶的惡意攻擊行動散播。攻擊者一直偽裝成熱門 APP(例如：NordVPN 或 Google Chrome) 來傳送 Octo2 的二進制檔案。這個最新變種還導入規避和防分析技術、增強的程式碼混淆以及用於 C&C 通訊的 DGA(網域生成算法) 來提升網路攻擊戰力。

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：

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
- Android.Reputation.2
- AppRisk:Generisk

2024/09/24

SectopRAT惡意軟體，偽裝成Notion安裝程式大肆傳播

在真實網路情境上新發現一個傳播 SectopRAT 惡意軟體的網路攻擊行動。該行動將惡意軟體二進位檔偽裝成已知生產力軟體 Notion 的安裝程式檔案。這些偽造的安裝程式也從偽裝成 Notion 軟體下載入口的惡意網站散佈。SectopRAT 有效籌載具有執行攻擊者遠端指令以及從受感染系統收集資料 (包括憑證、cookie、加密貨幣錢包等) 的功能。

網路上的知識：Notion 作為一款功能強大的工作與生活協作工具，憑藉其靈活的操作方式和高度自定義的功能，已經成為全球許多專業人士的首選。無論你是個人用戶還是團隊協作，Notion 將使你的工作流程更加順暢自然。

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.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：

- 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。

2024/09/24

安卓平台出現全新：Necro木馬程式

最新版本 Necro 木馬程式已感染多種熱門的 APP，包括 Google Play 上遊戲修改程式，影響超過 1100 萬部 Android 裝置。此版本採用混淆技術逃避偵測，並使用隱藏技術隱藏其有效酬載。該木馬程式可在隱形視窗中顯示廣告、下載並執行任意的 DEX 檔案、安裝已下載的 APP、開啟隱藏連結、執行 JavaScript、建立穿透受害者裝置的通道，並可能會讓使用者訂閱付費服務。

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.Gen.MBT
- WS.Malware.1

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.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。

2024/09/23

Earth Baxia駭客集團：藉由GeoServer已知漏洞瞄準亞太地區

根據趨勢科技最近一份報告指出，Earth Baxia 駭客集團透過魚叉式網路釣魚電子郵件和利用地理位置資訊伺服器 GeoServer 已知漏洞 CVE-2024-36401 攻擊亞太地區的政府、電信和能源組織。此遠端程式碼執行漏洞 (RCE) 讓行動者可下載或複製惡意元件。Earth Baxia 利用 GrimResource 和 AppDomainManager 注入技術部署額外的有效酬載，包括 Cobalt Strike 和稱為 EAGLEDOOR 的新後門程式。

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-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：

- ISB.Suspexec!gen50
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.4

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。

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: GeoServer RCE Vulnerability CVE-2024-36401
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 2

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，DCS 強化保護政策會封鎖所有對外連線，可防止惡意軟體從網際網路下載或經由 Linux 的 scp 指令在不同 Linux 主機之間複製檔，正如一些公開概念驗證 (POC) 文件中提到的一樣。預設強化政策會封鎖所有向外連線，僅允許已建立的相關連線，以及僅允許 DNS、HTTP 和 HTTPS 等必要的出站流量。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。

2024/09/23

以義大利使用者為目標的SambaSpy惡意軟體

SambaSpy 遠端存取木馬 (RAT) 已在針對義大利使用者的新一波網路攻擊行動被大肆散佈。此惡意攻擊行動的感染鏈有數個階段，並根據觀察到的情況，也會利用惡意軟體下載器或植入程式。攻擊者還會使用 OneDrive 或 MediaFire 等公共檔案儲存庫來上架感染鏈中使用的部分惡意檔案。最終有效酬載 SambaSpy 遠端存取木馬 (RAT) 具有多種功能，包括竊取憑證、鍵盤側錄、遠端桌面管理、遠端 shell 執行、下載／上傳檔案、執行外掛程式、視訊鏡頭控制等。

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：

- Java.Portudrop!gen1
- Scr.Maljava!gen1
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Pidief
- Web.Reputation.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。

2024/09/23

Go Injector涉入部署Lumma惡意竊密程式的攻擊行動

研究人員發現一個使用 Go Injector 部署 Lumma 惡意竊密程式的攻擊行動，Lumma 是專門用來竊取敏感資訊的惡意竊密程式。當使用者造訪一個顯示虛假驗證碼的有害網站時，攻擊就會開始，誘使使用者複製並執行一個指令。這個指令會下載一個 zip 檔案，其中包含看似合法的檔案和 Go Injector。然後，注入器會安裝 Lumma 並將竊取的資料解密並傳送給攻擊者。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g221
- SONAR.SuspOpen!gen11

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

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**。