保安資訊--本周(台灣時間2024/03/08)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 59 萬 9,000 台受保護端點上總共阻止了 6,240 萬次攻擊。這些攻擊中有 84.5% 在感染階段前就被有效阻止：**(2024/03/04)**

- 在**11萬4,000**台端點上，阻止了**2,100**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**15萬2,800**台端點上，阻止了**1,260**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,300**台**Windows**伺服主機上，阻止了**9,500**萬次攻擊。
- 在**6萬8,700**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,800**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬7,200**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**21萬6,500**台端點上，阻止了**490**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5萬7,000**台端點上，阻止了**150**萬次加密貨幣挖礦攻擊。
- 在**13萬8,200**台端點上，阻止了**830**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**584**台端點上，阻止了**6萬900**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 16.39 萬個受保護端點上阻止了總計 630 萬次攻擊。**(2024/03/04)**

- 使用網頁信譽情資，在 **147.5K** 個端點上阻止 **550** 萬次攻擊。
- 攔截 **34.5K** 個端點上 **656.5K** 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 **12.5K** 個端點上攔截 **127.4K** 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 **443** 個端點上攔截 **34.8K** 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。

2024/03/07

加密不是為了贖金，而是搞壞你的電腦系統～破壞性惡意軟體Windestroye

最近在真實網路情境上發現一種名為 Windestroyer 全新破壞性惡意軟體。Windestroyer 會感染並加密所有可執行檔，導致目標系統無法運作、可以重新載入 DLL 和 發動 API hammering 攻擊來規避安全軟體的檢查，並具有開機惡意啟動程式 (Bootkit) 功能和透過修改機碼來常駐。一旦在遭入侵的系統上被執行，它還能橫向移動，搜尋網路分享，然後感染所有搜尋到的檔案。

攻擊者可能來自俄羅斯，但沒有留下勒索贖金支付說明檔案或索取贖金的要求，這顯示是某種『激進駭客』攻擊，很可能不是出於經濟動機。

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

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.B!100
- Heur.AdvML.B
- Heur.AdvML.B!200
- Heur.AdvML.C

2024/03/07

以俄羅斯法律文件為誘餌的SapphireStealer惡意竊密程式散播活動

據觀察，最近報導一個網路攻擊行動試圖從一個假冒的俄羅斯政府網站上傳播 SapphireStealer 惡意竊密程式。在執行下載的有效籌載時，受害者會看到一份偽造的法律文件，同時惡意竊密程式會在後臺執行活動。竊取的資料隨後會外傳到攻擊者所操控的命令和控制 (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!gen1
- SONAR.TCP!gen1

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

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。

2024/03/06

全新GhostLocker 2.0勒索軟體即服務

據報導，GhostSec 駭客組織已推出全新的 GhostLocker 2.0 勒索軟體即服務。這個新變種是採用 Golang 程式語言所撰寫，並且已被用於對多個國家的組織實施雙重勒索攻擊。此外，該公司還推出了幾款新工具，包括一款名為『GhostSecDeepScanToolset』的網站掃描工具，用於對目標網站進行深度掃描，以及『GhostPresser』專用於探測和接管 WordPress 類型網站的工具。

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.Untrst-FlPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.IcedID
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2024/03/06

留意MS Outlook中的MonikerLink漏洞--CVE-2024-21413

CVE-2024-21413 也被稱為 MonikerLink 漏洞，是最近被揭露存在多個版本的 Microsoft Outlook 個人資訊管理系統軟體上的嚴重安全性漏洞。若被成功開採濫用該漏洞會讓未經認證的攻擊者繞過 Office 保護檢視模式 (Protected View) 安全機制，其保護檢視模式可在用戶於開放網際網路、不安全地點 (例如：公司網路外) 開啟文件，或是開啟 Outlook 郵件附檔時，在沙箱環境下以唯讀方式開啟。本漏洞可能導致本地 NTLM(NT LAN Manage) 憑證暴露並允許遠端程式碼執行 (RCE)。據報導，早在微軟發佈二月份例行修補之前，該漏洞早就是在真實網路情境中被開採濫用的零時差漏洞。

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：

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)。

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: Microsoft Outlook RCE CVE-2024-21413

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 內建的預設強化政策，即能保護 MS Office 應用程式。
- DCS 可防止 MS Office 應用程式將命令直譯器 (包括 cmd.exe、powershell.exe 或 winrar.exe／winzip.exe 作為子程序) 啟動。
- DCS 預設政策會阻止任何 SMB 連接。
- DCS 預設政策也會阻止任何惡意軟體在系統中被注入或執行。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/03/06
CVE-2024-23334 aiohttp中的目錄遍歷漏洞

CVE-2024-23334 是 aiohttp 中的目錄遍歷漏洞，aiohttp 是 asyncio 和 Python 的非同步 HTTP 用戶端／伺服器框架。如果被成功開採濫用該漏洞，未經認證的遠端攻擊者可從伺服器檔案系統上的任何檔案讀取敏感資訊。賽門鐵克的網路層防護技術入侵防禦系統 (IPS) 會阻止漏洞的攻擊嘗試，以防止系統受到進一步感染或入侵。

保安網路知識：aiohttp 是基於 asyncio 非同步 HTTP 用戶端／伺服端套件，能夠非同步的發送請求 (request) 及執行非同步的程式碼，所以非常適合用來開發 Python 非同步的網頁爬蟲，提升執行的效率。

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：

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: Passwd File Download Attempt

2024/03/06
勒索軟體攻擊利用「兩用工具」進行資料洩露

檔案被加密同時又遭到洩露的雙重蹂躪是勒索軟體受害者最無助的遭遇。博通公司旗下的企業安全部門：賽門鐵克威脅獵手團隊公開一份報告，內容指出惡意工具和合法工具被用作資料洩露的嚴重程度雙雙增加，這些幫兇工具提供攻擊者所需的資料洩露功能。該報告指出，Rclone、AnyDesk 和 ScreenConnect 等合法使用的工具以及 Cobalt Strike 等惡意工具被多個勒索軟體攻擊者使用。

在我們的布落格文章中有更多內容可供參閱：資料洩露：勒索軟體攻擊者利用的工具越來越多。

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：

- AGR.Terminate!g2
- AGR.Terminate!g10
- AGR.Terminate!g5
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gen1
- Backdoor.Cobalt!gen7
- Backdoor.Cobalt!gm1
- Backdoor.Cobalt!gm5
- Hacktool
- Hacktool.Chisel
- Hacktool.Gen
- Trojan Horse
- Trojan.Gen.9
- Trojan.Gen.MBT
- 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!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：

- Web Attack: Webpulse Bad Reputation Domain Request (29565)

2024/03/05

SupermanMiner(*超人礦工)挖礦木馬一直在持續演變

最近，SupermanMiner挖礦木馬引起了人們的關注，這是一種自 2021 年以來一直活躍在威脅環境中的惡意挖礦木馬。該惡意軟體由多個元件組成，報告顯示目前至少有八個變種在流竄。SupermanMiner 是一個用 Go 程式設計語言撰寫的門羅幣(Monero,XMR)挖礦木馬，它利用Google Sites協作平台來上架自訂網頁以傳播惡意軟體。一如過往， SupermanMiner 聯盟成員採用了各種技術來發動攻擊，如漏洞利用、SSH 強制和 web shell 注入。

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：

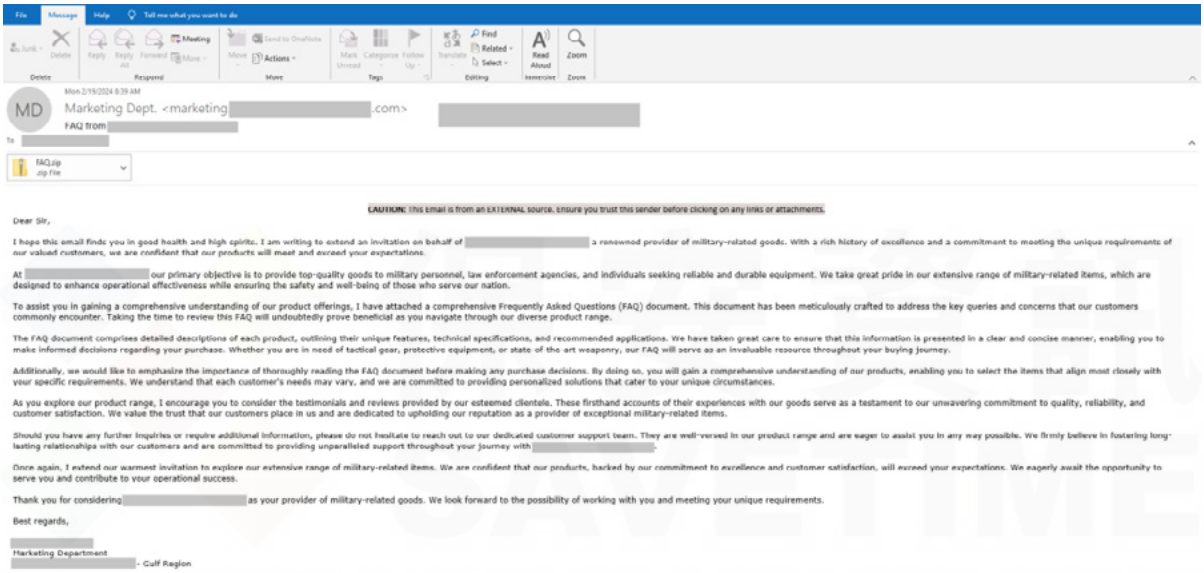
檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

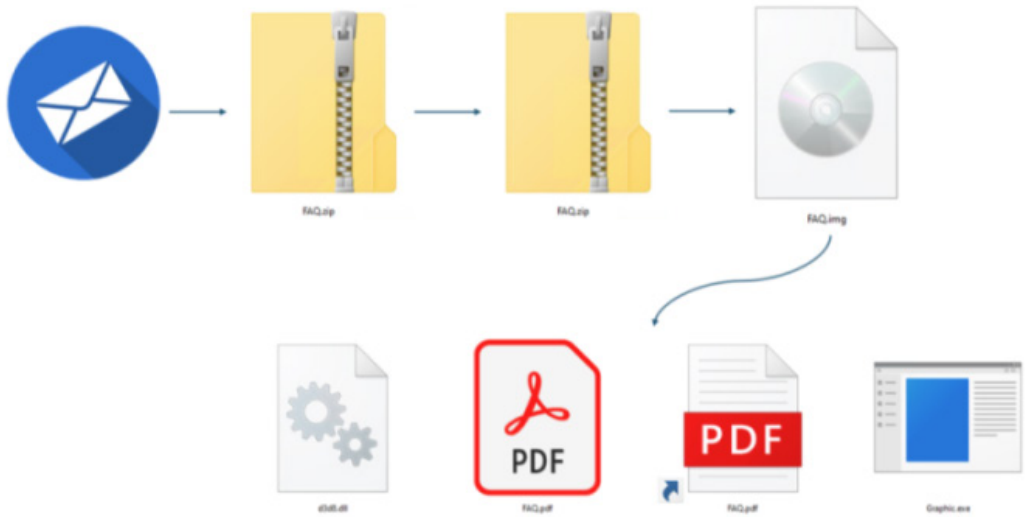
2024/03/06
防護亮點：針對中東各國政府的網路攻擊

在東歐和中東持續不斷的衝突中，一個網路惡棍一直在策劃針對中東各國政府的網路間諜行動。這些網路威脅行動利用該地區因長期衝突而加劇的恐懼和緊張局勢。這些惡意行動只會加劇對受影響政府及其人民的干擾，對該地區的穩定和安全構成更大的威脅。

攻擊行動是透過精心設計過的魚叉式網路釣魚電子郵件發起，攻擊者冒充一家信譽良好的美國航太和國防公司。這些精心製作的電子郵件大多以軍事和執法勤務裝備機具為主要誘餌。實際上，攻擊者誘使用戶存取他們偽造的常見問題 (FAQ) 檔案。在該檔案中，除了提供每種產品的獨特屬性、技術規格和推薦應用外，還提供詳細的說明。



如果用戶不疑有他被誘騙開啟所附的 ZIP 檔 (FAQ.zip)，就會遇到另一個同名的 ZIP 檔 (FAQ.zip)，其中包含一個 IMG 壓縮檔 (FAQ.img)。第二個壓縮檔包含一個 PDF 誘餌 (FAQ.pdf)，以及惡意捷徑檔 .LNK (FAQ.pdf.lnk)、EXE (Graphic.exe) 和 DLL (d3d8.dll) 等檔案。



執行後，惡意 .LNK 捷徑檔將啟動 PDF 誘餌，同時在後臺執行 EXE 檔。此外，DLL(d3d8.dll)會使用搜尋序劫持技術載入。然後，該 DLL 會載入解密後的後門程式碼，進而啟動系統指紋識別，並開始對主機進行 C&C 註冊，分配亂數 ID，這些 ID 處於待機狀態，以接收和執行進一步命令。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Backdoor Trojan

基於機器學習的防禦技術：

- Heur.AdvML.C

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)。

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 內建的預設強化政策，即能保護 MS Office 應用程式。
- DCS 可防止 MS Office 應用程式將命令直譯器(包括 cmd.exe、powershell.exe 或 winrar.exe / winzip.exe 作為子程續)啟動。
- DCS 將阻止任何可執行檔在該威脅的攻擊鏈上進一步執行。
- 為了提供更進一步的保護，客戶可以設定 DCS 網路規則，為特權服務和應用程式設置網路存取權限。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲深入瞭賽門鐵克端點安全完整版的調適型防護 (Adaptive Protection) 功能，請點擊此處。
欲深入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。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

2024/03/05
Waterbug(*水蟲)威脅組織(又名 Turla)部署新的封裝程式

Waterbug 威脅組織 (又名 Turla) 是一個可追溯到 2004 年的進階持續威脅 (APT) 駭客組織，它已開始使用一種被稱為 Pelmeni(*俄國餃子) 的 wrapper(建立包裝函式、 包裝應用程式的打包工具)。它在遭入侵的系統中偽裝成合法的 DLL 以側載方式出現。一旦合法軟體呼叫這個詐騙的 DLL ，它就會接續第二階段的攻擊鏈，下載後門木馬 Kazuar。利用 Kazuar，攻擊者可以從遭入侵的機器中竊取資料。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.9
- Trojan.Gen.MBT
- W32.Qakbot
- WS.Malware.1
- WS.SecurityRisk.3

基於機器學習的防禦技術：

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

2024/03/05
Rhadamanthys惡意竊密程式繼續透過惡意廣告傳播

據了解，Rhadamanthys 是一種主要透過惡意垃圾郵件或惡意廣告傳播的惡意竊密程式。最近觀察到傳播該惡意軟體的行動，是利用惡意廣告和偽裝成下載熱門的生產力應用程式之誘餌網站。在該行動中，攻擊者試圖同時傳播針對 macOS 和 Windows 使用者的惡意軟體。基於 macOS 有效籌載是一個源於Atomic 惡意竊密程式的變種，而 Windows 二進位檔案則最終部署 Rhadamanthys 有效籌載。惡意竊密程式具有從各種應用程式和電子郵件程式中竊取憑證的威脅能力。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- OSX.Trojan.Gen
- Trojan Horse

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

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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
- 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。

2024/03/05

全新銀行金融木馬：Chavecloak

一個名為 Chavecloak 的全新銀行金融木馬，被證實是針對南美使用者所發動覬覦金錢為動機的垃圾郵件行動所傳播的惡意程式有效籌載。惡意電子郵件包含一個 PDF 附件，開啟後會提示下載一個壓縮檔。解壓縮該壓縮檔會利用 DLL 側載技術觸發 Chavecloak 的執行。該惡意軟體具有按鍵記錄、顯示詐騙性快顯視窗以及監控金融和加密貨幣交易等功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Pidief
- WS.Malware.1

基於機器學習的防禦技術：

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

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。

2024/03/04

全新Linux後門程式：GTPDOOR

據報導，有一種名為 GTPDOOR 全新 Linux 後門程式已經出現在真實網路情境。該惡意軟體專門針對電信網路所量身打造，被懷疑與 Mystrium 駭客組織 (又稱 LightBasin) 有關。GTPDOOR 利用 GPRS Tunnelling Protocol Control Plane(GTP-C)-GPRS 隧道協議建立隱秘的命令和控制 (C&C) 通訊，使其能夠在合法的網路流量中偽裝其非法活動。

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：

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

2024/03/04

近期傳播Agent Tesla惡意軟體的垃圾郵件行動明顯增加

我們最近發現，由於惡意軟體攻擊行動持續不斷，偵測到 Agent Tesla 惡意軟體相關的次數激增。攻擊由帶有惡意附件或連結的釣魚電子郵件發起，通常偽裝成合法來源。賽門鐵克的進階機器學習技術 (AML) 已經主動阻止這個發現的行動。

Agent Tesla 是一種用 .NET 撰寫的遠端存取木馬 (RAT)，自 2014 年起開始活躍。該惡意軟體功能多樣，具有鍵盤側錄、螢幕截圖、資料竊取和遠端存取控制等功能，會定期更新和突變，使檢測成為一項持續的挑戰。

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-Sc!g1
- ACM.Ps-RgPst!g1
- ACM.Rgsvc-Lnch!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen24
- SONAR.SuspBeh!gen526
- SONAR.SuspBeh!gen530
- SONAR.SuspBeh!gen752
- SONAR.SuspLaunch!g310
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen8
- CL.Suspexec!gen168
- Scr.Malcode!gdn33
- Scr.Malcode!gdn34
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

2024/03/04

GuLoader惡意軟體下載器被發現藏身在SVG圖檔暗渡惡意ZIP壓縮檔

最近發現一個散播 Guloader 惡意軟體下載器的垃圾郵件行動，在其附加的 SVG(Scalable Vector Graphics，可縮放向量圖形) 圖檔中偷渡惡意 ZIP 壓縮檔。這些 SVG 檔暗藏 JavaScript 程式碼，開啟檔後會自動產生惡意 ZIP 檔，並自動顯示下載提示。ZIP 檔包含一個 WSF(Windows Script File：Windows指令碼檔案) 檔，可下載最終感染有效籌載。

電子郵件主旨範例 (主要還是透過社交工程伎倆)：

- INVOICE-INVOICE#RVBSA09SGSA(出貨單／發票單據明細)
- Payment Confirmation(付款確認)
- Solicitud de Cotización #PO-SJ005182824013710(訂單編號通知)
- Please confirm Payment(付款通知)

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.IcedID!gen2
- Scr.Guloader!gen3
- Scr.Malcode!gen
- VBS.Downloader.Trojan

2024/03/04

惡意後門程式：XRed

XRed 惡意後門程式具有許多破壞力，它會收集系統資料資訊，並使用 SMTP 將資料傳輸到電子郵件位址。該後門程式還具有顯著的常駐能力，靠得就是使用隱藏目錄和機碼裡的 Run 值，同時試圖隱藏在木馬軟體中。此外，它還能透過 USB 隨身碟進行蠕蟲式傳播。

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-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspPE!gen32
- SONAR.Dropper

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Graybird
- Backdoor.Trojan
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mdropper
- W32.Changeup
- W32.Fixflo.B!inf
- W32.Zorex
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.A!300
- 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。

2024/03/04

Frea勒索軟體

Frea 是最近在真實網路情境所發現另一個源於 Chaos 勒索軟體的新變種。該惡意軟體會加密使用者檔案並冠上 .frea 副檔名。它還會更改受感染電腦的桌面背景。勒索 (贖金支付) 說明以『oku.txt』的文字檔形式提供，會向受害者提供攻擊者的電子郵件位址作為後續聯繫之用。

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
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/03/04

利用PDF附件傳播Agent Tesla惡意軟體的網路攻擊行動正在流行

據報導，目前流行一種透過 PDF 附件傳播 Agent Tesla 惡意軟體的魚叉式網路釣魚電子郵件行動。該行動專門鎖定常在網訂票的遊客，提供假冒來自某知名旅行社的預訂發票。打開 PDF 附件後，會觸發一個 JavaScript 有效籌載，該籌載會呼叫並執行一個 PowerShell 腳本，最終導致安裝 Agent Tesla 惡意軟體。該惡意軟體能夠從常用網路瀏覽器中擷取個人資料和憑證，並透過攻擊者的 Telegram 頻道將這些資訊外洩。

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-Wscr!g1
- ACM.Wscr-Ps!g1
- ACM.Rgsvc-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g318

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen572
- JS.Downloader
- Scr.DLHeur!gen17

- Scr.Malcode!gen
- Trojan Horse
- Trojan.Pidief

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：

- 34479 Audit: Suspicious Process Accessing bitbucket.org
- 33337 Audit: PowerShell Process Accessing bitbucket.org

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。

2024/03/01

Blind Eagle(*盲鷹)駭客組織利用Ande Loader惡意載入程式發動網路釣魚

APT-C-36 駭客組織 (又名 Blind Eagle) 於 2018 年首次被發現，自 2021 年以來一直被觀察到在散播遠端存取木馬 (RAT)。該駭客組織被認定來自南美洲，已被觀察到以哥倫比亞和該地區其他國家的製造業為目標。在最新的攻擊中，受害者會收到一封帶有惡意連結的釣魚郵件，點擊連結後會下載包含惡意 VBS(Visual Basic 腳本) 的 RAR 和 BZ2 壓縮檔案。然後，Ande Loader 就會被用來發送 Remcos RAT 和 NjRAT 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Ratenjay
- Backdoor.Ratenjay!gen3
- ISB.Heuristic!gen62
- Scr.Malcode!gdn14
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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
- Heur.AdvML.C

2024/03/01

ConnectWise ScreenConnect存在的CVE-2024-1709和CVE-2024-1709漏洞已遭勒索軟體威脅組織開採濫用

CVE-2024-1709 和 CVE-2024-1709 是最近被披露的兩個存在 ConnectWise ScreenConnect 伺服器的漏洞。第一個漏洞--CVE-2024-1708 是一個高優先目錄遍歷漏洞，可能允許未經身份驗證的攻擊者存取受限檔案和目錄，導致資訊洩露。第二個漏洞--CVE-2024-1709 是一個重要的身份驗證繞過漏洞，允許攻擊者存取易受攻擊的系統，並可能執行惡意程式碼。據報導，包括 Lockbit、Black Basta 和 Bl00dy Ransomware 在內的多個勒索軟體威脅組織都在利用這些漏洞。ConnectWise 原廠已經發佈 23.9.8 安全修復版本，以解決被公開的漏洞。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen82
- SONAR.Ransom!gen113
- SONAR.SuspDataRun
- SONAR.SuspLaunch!g193
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gen19
- ISB.Downloader!gen173
- Packed.Generic.700
- Scr.Malcode!gdn14
- Scr.Malcode!gdn20
- 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.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 721
- Web Attack: ConnectWise ScreenConnect CVE-2024-1708
- Web Attack: ConnectWise ScreenConnect CVE-2024-1709
- 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。

2024/03/01

CVE-2024-20931-Oracle WebLogic Server的T3／IIOP協議之遠端程式碼執行(RCE)漏洞

代號為 CVE-2024-20931 漏洞是位於 Oracle WebLogic Server 的 T3／IIOP 協議的遠端程式碼執行 (RCE) 漏洞，一經開採可在無需驗證用戶身份及密碼情況下，遠端在 WebLogic 伺服器軟體在應用程式的上下文內執行任意程式碼，以及不受限制存取遭入侵的 Oracle WebLogic Server 上重要資料。原廠已為此漏洞釋出修補程式。

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：

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: Oracle Weblogic Server CVE-2024-20931

2024/03/01

WordPress新款編輯器：「Bricks Builder」存有CVE-2024-25600的遠端程式碼執行(RCE)漏洞

CVE-2024-25600 是存在 WordPress 的 Bricks Builder 外掛編輯器的嚴重等級 (CVSS 風險評分：9.8) 遠端程式碼執行 (RCE) 漏洞。成功被開採濫用此漏洞可讓未經認證的攻擊者，在有此漏洞的 WordPress 網站上遠端執行任意 PHP 程式碼。據報告，該漏洞已被惡意開採濫用，包括在受影響之伺服器上安裝 PHP 的惡意 webshell。解決此漏洞的更新程式已在 Bricks Builder 1.9.6.1 或更新的版本中釋出。

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: WordPress Bricks Builder Theme RCE CVE-2024-25600