保安資訊--本周(台灣時間2024/02/16)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 54 萬 4,900 台受保護端點上總共阻止了 5,230 萬次攻擊。這些攻擊中有 84.6% 在感染階段前就被有效阻止：**(2024/02/12)**

- 在**10萬8,100**台端點上，阻止了**1,730**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬700**台端點上，阻止了**1,100**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,700**台**Windows**伺服主機上，阻止了**9,300**萬次攻擊。
- 在**6萬5,300**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,400**台端點上，阻止了**86萬9,600**次嘗試掃描在**CMS**漏洞。
- 在**5萬900**台端點上，阻止了**120**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**460**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,600**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**9萬9,400**台端點上，阻止了**690**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**538**台端點上，阻止了**9萬6,700**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 15.07 萬個受保護端點上阻止了總計 610 萬次攻擊。**(2024/02/12)**

- 使用網頁信譽情資，在 **135K** 個端點上阻止 **540** 萬次攻擊。
- 攔截 **32.6K** 個端點上 **562.8K** 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 **12.4K** 個端點上攔截 **129.5K** 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 **447** 個端點上攔截 **37.3K** 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。

2024/02/15

全新後門程式：TinyTurla-NG(TTNG)

全新後門程式：TinyTurla-NG (TTNG) 據證實是由俄羅斯駭客集團：Turla APT 所擁有及負責維運。Turla APT 利用遭入侵的 WordPress 網站作為該後門的 C&C 端點。TTNG 會在受害者受感染的機器上執行任意命令，以竊取與熱門密碼管理軟體憑證相關的關鍵資訊。

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-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A

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。

2024/02/15

TicTacToe(井字遊戲／圈圈叉叉遊戲)惡意軟體植入程式(Dropper)

TicTacToe 惡意軟體植入程式 (Dropper)，最近因涉入網路攻擊行動而被發現。該程式通常利用惡意 .iso 附件透過垃圾郵件傳播。一旦進入遭入侵的電腦，TicTacToe 可能會發送包括 AgentTesla、SnakeLogger、Remcos、LokiBot 等多種惡意軟體的有效籌載。據信，這種惡意軟體植入程式 (Dropper) 被多個威脅組織使用，並可能以惡意軟體即服務模式的形式擴散。

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.Stealer!gen1
- SONAR.SuspBeh!gen752
- SONAR.SuspLaunch!g310

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen8
- MSIL.Packed.38
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- 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。

2024/02/15

JKwerlo勒索軟體

JKwerlo 是一種新發現的採用 Go 程式語言撰寫的勒索軟體。該惡意軟體最近涉入針對西班牙語和法語用戶的網路攻擊行動。初始攻擊階段是透過垃圾郵件向用戶發送惡意 .html 檔案附件。勒索軟體的有效籌載透過 .zip 壓縮檔附件傳遞，或從 Dropbox 雲端空間下載。被 JKwerlo 加密過的檔案不會再冠上任何副檔名。該惡意軟體具有刪除卷影副本、停用 Windows 防火牆和恢復模式等功能。在某些情況下，還能觀察到該勒索軟體會下載一個名為 Rubeus 的額外後滲透 (post-exploitation) 工具，威脅者可能利用該工具獲取受感染機器的管理員權限。

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：

- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen523
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2024/02/14
安卓平台上的惡意鎖定程式(Locker)偽裝成文件檔

當勒索軟體持續在桌機／筆電環境中肆虐時，賽門鐵克繼續發現安全平台上的惡意鎖定程式 (Locker) 以手機／行動裝置用戶為目標，儘管其流行程度遠不如幾年前。在最近一個案例中，我們觀察到馬來西亞的網路惡棍，將他們的惡意鎖定程式 APP 的安裝檔偽裝文件檔 (DOC-[日期]-[隨機字元].apk)。除了能鎖定安卓手機螢幕外，它還能收集敏感性資料，例如：設備資訊、簡訊內容、連絡人和相機資料。受害者會收到網路惡棍設置的新桌布提示，透過 Telegram 連接並支付贖金以換取解鎖密碼。

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

2024/02/14
新一波鎖定Microsoft Azure雲端平台的網路釣魚行動

最近觀察到有人在微軟 Azure 雲端平台中接管用戶帳號。擁有高權限的使用者或掌握機密商業資訊的個人最有可能成為鎖定目標。這種攻擊採用各種伎倆，例如：在電子郵件中嵌入假冒共享檔案鏈結來收集用戶憑證、接管帳號、滲出資料並發動新的網路釣魚攻擊。

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。

2024/02/14
全新木馬惡意軟體：Coyote

全新木馬惡意軟體：Coyote，一直以巴西金融機構的用戶為目標。該惡意軟體利用各種先進技術 (例如：Squirrel 安裝程式) 進行感染，然後與其 C&C 伺服器建立連線。一旦連線接並通過驗證，收集到的資訊 (例如：截圖、憑證……等) 就會從遭感染的機器中滲出。

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：

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.B
- Heur.AdvML.A!300
- 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。

2024/02/14

Glupteba惡意軟體透過UEFI引導工具包不斷翻新

在最近的網路攻擊行動中，發現 Glupteba 惡意軟體部署一個統一可延伸韌體介面 (UEFI) 引導工具安裝程式二進位檔案，偽裝成合法的 Windows 二進位檔案。這些網路攻擊行動幕後的駭客，採用越來越受歡迎的按每安裝付費 (PPI) 計價服務助長大規模的感染。UEFI 引導工具包具有干預和控制作業系統啟動過程的能力，進而使 Glupteba 能夠有效地隱藏其存在。這凸顯駭客戰術和技術的不斷演變。

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.Glupteba!gen2
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Efiguard
- Trojan.Glupteba
- 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

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 (33246)

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。

2024/02/14

Ivanti旗下多項產品被揭露存在：CVE-2024-21893伺服器端請求偽造(SSRF)的資安漏洞

CVE-2024-21893 是 Ivanti 旗下多項產品，最近被揭露一個伺服器端請求偽造 (SSRF) 漏洞，CVSS 風險評分為：8.2。該漏洞影響多個 Ivanti 旗下產品的安全性聲明標記語言 (SAML) 元件，例如：Ivanti Connect Secure (9.x、22.x)、Ivanti Policy Secure (9.x、22.x) 和 Ivanti Neurons for ZTA。被成功開採濫用該漏洞會讓攻擊者在未進行身份驗證的情況下存取某些受限資源。據報告，該漏洞已在真實網路情境上被開採濫用。

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：

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 SSRF Vulnerability CVE-2024-21893
- Web Attack: Ivanti SSRF Vulnerability CVE-2024-21893 2

2024/02/14

macOS後門程式引發勒索軟體攻擊

最近發現一個 macOS 後門程式。這個全新後門程式偽裝成 Visual Studio 更新，已經發現 3 個不同版本的變種，都是採用 Rust 撰寫。安裝後，後門會嘗試假冒常見的軟體通知，以獲取管理員密碼。一旦獲得密碼，它就會開始常駐並竊取資料，隨後用以脅迫受害者。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- OSX.Trojan.Gen
- OSX.Trojan.Gen.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：

- 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。

2024/02/13
防護亮點：Apache ActiveMQ漏洞(CVE-2023-46604)仍被大肆開採濫用

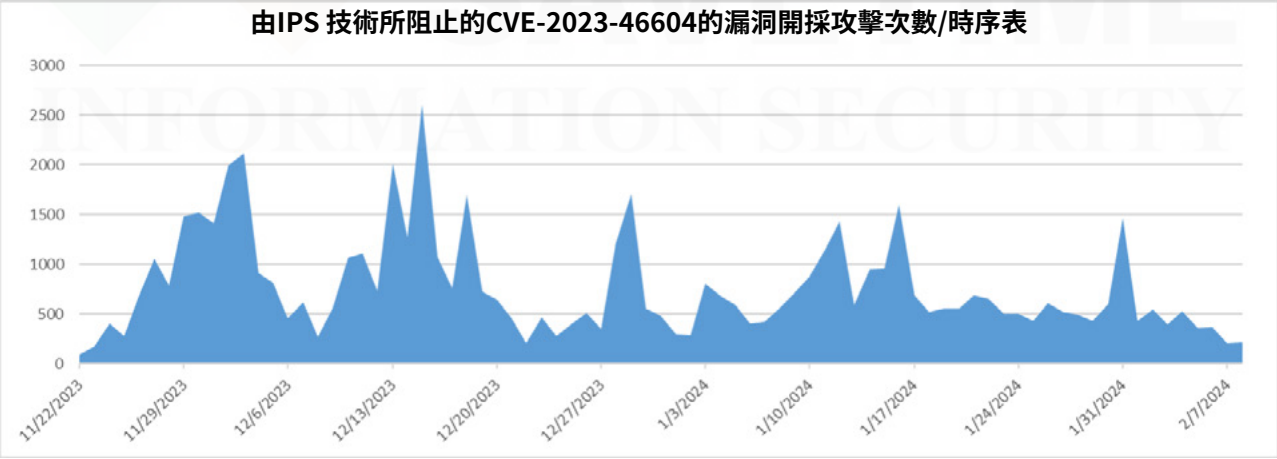
Apache ActiveMQ 是一個用 Java 撰寫的開源訊息代理程式。可促進不同的企業級應用程式、服務和系統之間的訊息傳遞提供高可用性、可擴展性、可靠性、性能和安全性。

CVE-2023-46604 是一個存在 Apache ActiveMQ 的嚴重等級 (CVSS 風險評分：10) 遠端程式碼執行 (REC) 漏洞。如果被成功開採濫用，未經認證的遠端攻擊者，可在有機可趁的系統上執行任意 shell 命令。由於該漏洞很容易被開採濫用，攻擊者可以很快將其整合到他們攻擊手法中，以入侵企業環境並傳播各種惡意軟體有效籌載。

賽門鐵克已觀察到攻擊者成功開採濫用該漏洞後，傳遞以下惡意軟體的有效載荷：

- Linux 惡意軟體讓攻擊者操控遭入侵的 Linux 機器。
- 惡意挖礦程式，可在遭入侵的 Linux 和 Windows 機器上暗中執行挖礦程式。
- 反向 shell 有效籌載，可以獲取遭入侵機器的後門存取權限。
- Kinsing 惡意軟體，執行挖礦程式，並試圖將自身傳播到環境中的其他系統。
- Paradise、TellYouThePass 和 HelloKitty 等多種勒索軟體變來加密系統中的檔案，破壞其可用性。
- Shellbot 用於入侵伺服器，然後發動 DDoS 攻擊並傳遞惡意挖礦程式。

賽門鐵克的網路層防護技術：入侵預防禦系統 (IPS) 可有效阻止這些漏洞利用嘗試，防止系統受到感染／入侵。攻擊在初始階段就會被阻止，進而確保沒有惡意有效籌載駭入系統。迄今為止，IPS 技術已阻止超過 60K 次意圖開採濫用該漏洞的網路攻擊。



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: Apache ActiveMQ RCE CVE-2023-46604
- System Infected: Bad Reputation Process Request
- Web Attack: Malicious Java Payload Download

基於行為偵測技術(SONAR)的防護：

- SONAR.Cryptolocker!g75
- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Malscript!g1
- Ransom.HelloKitty
- Ransom.Tellyouthepass
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- Ransom.Paradise
- Linux.Kaiten
- Scr.Malcode!gen
- IRC.Backdoor.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.B
- 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其出廠就內建的系統鎖定政策，可以保護底層的作業系統免受此漏洞的侵擾。DCS 的網路規則政策可設定為，將 ActiveMQ 應用程式限制為受信任的用戶端。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。

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。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
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。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2024/02/13

qBit惡意竊密程式

qBit 是由 qBit 勒索軟體集團採用 Golang 語言開發的惡意竊密程式。該惡意軟體的原始程式碼最近被公佈在地下論壇上遭大量濫用。該惡意軟體具有收集敏感使用者資料和系統資訊的功能，然後將這些資料和資訊轉傳至雲端儲存服務商 MEGA 的雲端空間。此外，該惡意軟體還採用反偵錯和反虛擬化技術來提高安全軟體的規避能力。

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：

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：

- 可疑程序執行：預防政策可防止惡意軟體在系統中被注入或執行。
- 網路控制：在這種情況下，預防政策會阻止與網際網路 (Mega[.]nz) 的對外連接。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/02/12

Raspberry Robin惡意軟體不斷翻新

據觀察，手腳俐落的 Raspberry Robin 惡意軟體開採濫用兩個當天剛揭露的 (1-day) LPE(本機提權：Local Privilege Escalation) 漏洞，最近一個是 CVE-2023-36802，這是一個微軟串流媒體代理服務漏洞，可以進行提權。Raspberry Robin 也持續不斷發展，採用更先進的防禦規避技術，包括規避系統關機、驗證遠端桌面和檢查 UWF(整合寫入篩選器) 篩選器驅動程式。此外，它還利用新的部署方法更新攻擊途徑，例如：偽裝成合法的 Windows 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：

- Packed.Generic.553
- Trojan Horse
- Trojan.Emotet
- 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
- 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。

2024/02/12

Nightingale(*夜鶯)惡意竊密程式

Nightingale 是另一款具有常見功能的惡意竊密程式，最近在各種平臺上都能看到它的宣傳廣告，而且還被用於網路犯罪攻擊 (透過瀏覽網頁的偷渡式下載)。如果有人被成功誘騙執行此惡意竊密程式，它常被發現於收集資料，包括瀏覽器、加密錢包和系統規格。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

2024/02/12

專挑軟式子～攻擊者持續開採濫用陳年老漏洞

攻擊者仍然持續開採濫用陳年老漏洞來傳送惡意有效籌載。我們持續發現到 Word、Excel 和 RTF 等文件檔案，試圖開採濫用 CVE-2017-0199 或 CVE-2017-11882 等 Microsoft Office 的陳年老漏洞。這些檔案通常以社交工程郵件附件的形式被接收，並利用它們進一步傳播惡意軟體，例如：遠端存取木馬 (RAT) 或銀行金融木馬等有效籌載。

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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-0199*
- Exp.CVE-2017-11882*
- ISB.Downloader!gen217

- ISB.Downloader!gen48
- ISB.Downloader!gen60
- ISB.Downloader!gen63
- Scr.Malcode!gen125
- Scr.Malcode!gen29

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。

2024/02/12

jRAT遠端存取木馬：偽裝成薪資管理系統

網路犯罪分子繼續將其惡意軟體偽裝成小型企業常用的薪資管理軟體，主要在竊取敏感資訊，例如：員工詳細資訊和財務記錄，目的是透過資料盜竊或詐騙以獲取經濟利益。

最近一個案例中，攻擊者將其 jRAT(也稱為 JacksBot) 二進位檔案偽裝成一個名為『EzPayroll』的軟體，很可能是透過瀏覽網頁時的偷渡式下載傳播。JRAT 由來已久，多年來在全球眾多類型的攻擊中都發現其後繼版本。

雖然從功能上看，它是一款普通的遠端存取木馬，但基於 Java 是其顯著特點之一，這也是其跨平臺相容性的原因之一。只要目標設備安裝了 Java Runtime Environment (JRE)，它就能在 Windows、Mac OS、Linux 甚至 Android 等不同平台上成功運行。

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.Untrst-RunSys!g1
- ACM.Ps-CPE!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Maljava

2024/02/12

Pony(*小馬)惡意竊密程式

Pony又稱 Siplog 或 Fareit，同時具有惡意程式載入器和惡意竊密程式的功能，遭感染後可被操控為殭屍網路的成員。它可以隨時購買，並被用於針對歐洲和美國用戶的特定攻擊。它透過網路釣魚行動、漏洞利用工具包和偽造程式等手法來引誘受害者。一旦受害者的機器被感染，它就會竊取敏感性資料，包括瀏覽器資料、FTP 憑證和電子郵件用戶端資訊。該惡意軟體採用反沙箱和反虛擬機器技術來逃避檢測，同時將自身注入合法程序以執行其惡意程式碼。此外，它還會生成額外的檔案，以確保其存在並實現自我刪除，進而提高其隱藏能力，並可以常駐在遭入侵的系統中。

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)：

- AGR.Terminate!g2

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen650
- SONAR.SuspStart!gen14
- SONAR.TCP!gen1
- Trojan.Fareit!gm

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader.Ponik
- Downloader.Ponik!gm
- Infostealer!im
- Scr.Malcode!gdn20
- SMG.Heur!gen
- Packed.Generic.459
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.3

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

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)

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。