保安資訊--本周(台灣時間2024/02/09)
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 60 萬台受保護端點上總共阻止了 5,719 萬次攻擊。這些攻擊中有 84.6% 在感染階段前就被有效阻止：**(2024/02/06)**

- 在**11萬3,000**台端點上，阻止了**1,960**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**15萬100**台端點上，阻止了**1,320**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬800**台**Windows**伺服主機上，阻止了**1,070**萬次攻擊。
- 在**6萬7,400**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,300**台端點上，阻止了**95萬3,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬8,900**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**22萬2,300**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,800**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**11萬2,400**台端點上，阻止了**780**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**642**台端點上，阻止了**10萬600**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 15.81 萬個受保護端點上阻止了總計 640 萬次攻擊。**(2024/02/06)**

- 使用網頁信譽情資，在 **141.9K** 個端點上阻止 **560** 萬次攻擊。
- 攔截 **33.6K** 個端點上 **623.4K** 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 **13K** 個端點上攔截 **135.7K** 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 **498** 個端點上攔截 **51.9K** 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。

2024/02/08

Troll(*巨魔)惡意竊密程式

Troll 是一款採用 Go 語言撰寫的全新惡意竊密程式，偽裝成一家韓國公司的安全軟體安裝程式而被識破。它使用合法憑證簽章，以逃避安裝過程中的安全檢查機制。與典型的惡意竊密程式如出一轍，Troll 能夠從遭入侵系統中擷取各種資料，例如：SSH 憑證、FileZilla 資訊、檔案／目錄、瀏覽器資料、系統詳細資訊和螢幕截圖。隨後，遭竊取的資料會被外傳到攻擊者所操控的命令與控制 (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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/02/08
Zardoor後門程式

最近，在以伊斯蘭組織為目標的攻擊行動中發現一種涉入其中的 Zardoor 全新後門程式。在這場曠日持久的攻擊中，幕後黑手採用被歸類為就地取材攻擊的二進位檔案 (LoLBins) 和反向代理工具的多重攻擊鏈。據報告稱，攻擊者還定制開源工具，並能夠常駐多年保持對受害者網路的存取權限。目前，初始入侵媒介仍然未知。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- ProxyVenom
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse

2024/02/08
Ov3r惡意竊密程式

最近發現 Ov3r 惡意竊密程式，透過 Facebook 上的詐騙人力招聘資訊進行傳播，通常以招募管理職為幌子。受害者會被引導到一個 Discord 連結，PowerShell 腳本會從 GitHub 儲存庫中下載惡意軟體有效籌載。Ov3r 惡意竊密程式經過精心設計，可以從加密貨幣錢包、網路瀏覽器、瀏覽器擴展、Discord、FileZilla 等各種應用程式中竊取資料。此外，它還會仔細檢查 Windows 註冊表中的系統服務配置，進而鎖定其他目標。

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：

- ISB.Heuristic!gen39
- ISB.Heuristic!gen43
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- 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。

2024/02/08

Mispadu惡意竊密程式

Mispadu 惡意竊密程式於 2019 年首次被發現，已知會透過多階段攻擊傳播。最近，這種惡意軟體的最新變種被用於針對拉丁美洲和加勒比海地區 (尤其是墨西哥) 的網路攻擊行動中。Mispadu 主要在竊取與加密貨幣相關的一系列機構、交易所或企業的財務資訊。

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：

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：

- 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。

2024/02/08

KV-Botnet殭屍網路

KV-Botnet 是 Volt Typhoon 進階持續威脅 (APT) 駭客集團 (又稱 Bronze Silhouette) 所維運的殭屍網路。在該駭客集團所發動的網路攻擊行動中，此殭屍網路主要用來透過被入侵的小型辦公室／家庭辦公室 (SOHO) 設備操控惡意攻擊流量。至少從 2022 年 2 月開始，KV-Botnet 就持續涉入多起攻擊行動，直到 2023 年 12 月被聯邦調查局摧毀。被摧毀後不久，攻擊者試圖重新控制並恢復殭屍網路。雖然據報導這些努力無功而返，但該殭屍網路的活動有可能在未來重現江湖。

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
- Downloader
- Trojan Horse
- Trojan.Gen.NPE
- 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。

2024/02/08

XPhase剪貼簿挾持軟體(Clipper)

發現全新的 XPhase 剪貼簿挾持軟體 (Clipper)，已涉入鎖定加密貨幣用戶的網路攻擊行動。該有效籌載透過冒充熱門加密貨幣錢包或交易平臺 (例如：Metamask、WazirX、Cryptonotify 或 Luno App) 的釣魚網站傳播。這種剪貼簿挾持軟體具有攔截加密貨幣交易的功能，它將受害者錢包位址替換成攻擊者操控的位址。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Reg!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen60
- Trojan.Gen.MBT
- Web.Reputation.1
- 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：

- 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。

2024/02/07

跨平台網管軟體：ManageEngine OpManager，存在路徑遍歷漏洞：CVE-2023-47211

CVE-2023-47211 是最近被揭露的嚴重等級路徑遍歷漏洞，CVSS 風險評分：9.1。它影響 ManageEngine OpManager 的 uploadMib 功能。攻擊者若成功開採濫用該漏洞可修改 MIB 瀏覽器工具中預設安裝目錄以外的檔案路徑，可能導致透過精心製作的 HTTP 請求建立任意檔案。

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：

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: ManageEngine OpManager Path Traversal CVE-2023-47211

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，可以防止在預設 MiBs 檔的位置目錄之外建立檔案，從進而保護底層伺服器免受此漏洞的影響。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/02/06

2023Lock勒索軟體

2023Lock 是一個勒索軟體駭客集團，最近涉入多家企業的加密勒索的攻擊行動。目前，他們似乎不會竊取資料，也不會以公開資料來脅迫被害者就範，而只是專注於加密勒索。加密成功後，檔案會被冠上 .2023Lock 的副檔名。勒索贖金支付說明檔 (README.html 和 README.txt) 很簡單，為使用者提供大多數勒索軟體常見的內容。建議受害者透過指定 Onion 加密網站與攻擊者進行連線和對話。

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.RansomPlay!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

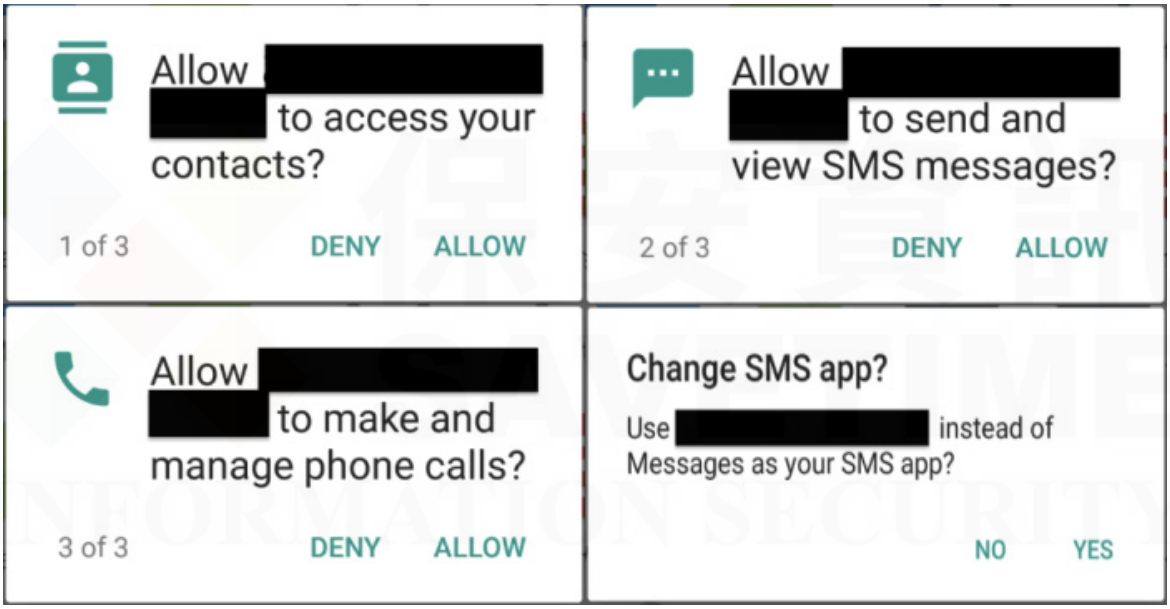
- Ransom.Gen

2024/02/06
防護亮點：正在光顧日本手機／行動裝置的惡意竊密程式：FakeCop

FakeCop 惡意竊密程式，它以手機／行動裝置為目標，蒐集各種類型的資料，包括裝置資訊、連絡人清單和簡訊內容。一旦收集到這些資料，它們就會被轉發到攻擊者所操控的 C&C 伺服器上。作者採用 XOR 加密技術，試圖躲避靜態檢測方法，但還是無法逃脫賽門鐵克端點防護行動裝置版本 (SEP mobile) 先進偵測技術的法眼。

在過去幾年裡，FakeCop 一而再、再而三地困擾著日本的手機／行動裝置用戶。其幕後的主使者一直沒有改變他們的作案手法，繼續濫用惡意簡訊和社交工程傳播他們的 APP，並在這一過程中假借盜用日本知名電信公司的名義。

賽門鐵克最近發現另一波偽裝成日本電信公司 APP 安裝檔--檔名 ([公司名]2024.apk) 的 FakeCop。如果使用者不疑有他在其安卓手機／行動裝置上部署該惡意程式，它會要求使用者授予執行任務所需的相關權限。



然後，它會試圖更改預設的簡訊 APP，並提示使用者卸載特定的防毒應用程式，這些防毒應用程式的清單是預先寫在其程式碼中。

成功入侵後，惡意應用程式很可能會傳播到受害者的連絡人中，還可能導致被盜資料在黑市上出售，進而造成經濟損失，甚至可能導致身份被盜。它還可能被用來進行有針對性的攻擊。

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：

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

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

2024/02/06
Mesmerised勒索軟體

Mesmerised 是 Chaos 勒索軟體家族的後繼新變種，已在真實網路情境上發現它的蹤跡。目前已發現該勒索軟體的多個流通版本。該惡意軟體會加密使用者檔案，並冠上 .mesmerised 的副檔名。在成功入侵並加密檔案後，一個檔名為 READ-ME.txt 的勒索贖金支付說明檔，會被存放到受害者的電腦上，並說明如何使用比特幣或萊特幣支付贖金以獲得解密工具。贖金支付說明包括電子郵件帳號和加密聊天軟體 uTox 的 ID 等詳細聯繫資訊。值得注意的是，該惡意軟體可以停止各種系統程序和服務，並刪除卷影副本磁碟備份。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- 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

2024/02/06
BlackHunt勒索軟體家族活動沒有減緩的跡象

BlackHunt 是採用 C++ 撰寫的勒索軟體，最初發現於 2022 年。該惡意軟體仍然活躍，最近還被用來攻擊巴拉圭的組織。BlackHunt 會加密用戶檔案，並冠上副檔名，最新變種的副檔名是『.Hunt2』。該惡意軟體會避開特定副檔名的檔案及其配置和系統檔。就其功能，該勒索軟體可以刪除受感染機器上的備份資料和磁碟備份，並停用受感染系統的系統還原功能。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Schtsk!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RunSys!g1

- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1
- AGR.Terminate!g2
- SONAR.Ransom!gen14
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g340
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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

2024/02/06
macOS上的PureLand惡意竊密程式

PureLand 是一款只針對 macOS 平臺的惡意竊密程式。該惡意竊密程式最初於 2023 年初被發現，與針對 Windows 平台的 Redline 惡意竊密程式一起傳播。PureLand 具有從各種瀏覽器錢包擴展或加密錢包應用程式中收集主機資訊、cookie、提取資料……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
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- WS.Malware.1

2024/02/06
FritzFrog殭屍網路出現新變種

據報導，FritzFrog 殭屍網路的一個新變種開採濫用 2021 Log4Shell 漏洞。該惡意軟體以提供網際網路服務的伺服器為攻擊目標，透過暴力破解薄弱的 SSH 憑證並針對易受攻擊的 Java 應用程式進行感染。此外，該惡意軟體還整合一個模組，用於開採濫用存在 Linux 的 Polkit 元件的 CVE-2021-4034 提權漏洞，該漏洞允許惡意軟體在易受攻擊的伺服器上以 root 身份運行。

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：

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
- 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。

2024/02/05

影音串流媒體帳號在黑市受歡迎，助長更多網路釣魚和簡訊釣魚的認證資料詐欺

影音串流媒體服務在全球擁有動輒數百萬甚至數億個用戶，必然會成為網路犯罪分子覬覦的目標。龐大的用戶群為攻擊者提供廣泛的潛在受害者，增加網路釣魚成功的機率。此外，被盜影音串流媒體服務的帳號在黑市也很值錢。網路犯罪分子可以將這些帳號用於各種目的，包括未經授權欣賞高資費節目、在地下論壇上轉售 (價格比官方月租費便宜)，甚至濫用更有價值的使用者帳戶內已登錄的資訊。

這些網路釣魚攻擊大多透過電子郵件發動，但有越來越多改採 SMS(簡訊服務) 進行網路釣魚攻擊 (俗稱『簡訊釣魚』)，這可能是由於以下幾個因素，使這種方法對網路犯罪分子具有吸引力：智慧型手機的普及；簡訊的急迫性高於電子郵件，因此大家對簡訊的警戒心較低，因此簡訊的閱讀率高於電子郵件。

賽門鐵克最近發現有網路釣客試圖假借與帳號相關未付款的問題為誘餌，竊取手機／平板用戶的認證資料。如果用戶不疑有他落入這種社交工程伎倆並點擊所提供的網址，就會被引導到一個模仿正牌影音串流媒體服務平臺的虛假登錄頁面。在一個案例中，該釣客還在其惡意網站上加入驗證碼，讓它看起來更像正牌的網站。

觀察到簡訊內容樣本：

- [流媒體服務商名稱]：您的最近一期帳單尚未繳清。單尚未繳可能導致我們停止服務。請參閱此處：[惡意網址]
- [流媒體服務商名稱] 帳戶擱置。請確認您的詳細資訊，以免被取消：[惡意網址]
- [流媒體服務商名稱]：Votre dernier préIèvement a été refusé. Vos services prendront fin automatiquement le 03/02/2024：[惡意網址]
- [流媒體服務商名稱]: votre compte sera suspendu d'ici 24H, veuiIIez confirmer vos informations afin de profiter de nos services：[惡意網址]
- [流媒體服務商名稱] 支付方式暫停。請更新您的帳單資訊，以免帳戶被取消：[惡意網址]

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：

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。WebPulse 已知道此次活動中使用假冒的假域名。

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。

2024/02/05

隨身碟惡意程式又來了～UNC4990駭客組織以大家熟悉的USB裝置圖示為掩護，來鬆懈戒心發動網路攻擊

UNC4990 是一個以濫用 USB 裝置作為初始感染媒介而聞名的駭客組織，最近發現它正在透過存放在外部網站與雲端儲存空間的被加料檔案，充當惡意酬載的來源來擴展其能力。使用者會被誘騙開啟 USB 裝置上的 Powershell 腳本，該腳本會以大家熟悉的圖示為掩護，來鬆懈戒心而點擊並觸發攻擊鏈及呼叫下一階段攻擊所需的惡意軟體。

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：

- Downloader
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

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

2024/02/04

EverSpy(*超級間諜)遠端存取木馬(RAT)

手機與行動裝置生態到處充斥著無數的遠端存取木馬 (RAT)，許多木馬被出售給不同的駭客集團和個體戶。還有一些木馬被破解並免費傳播給更多的惡意行為者。本公告探討其中一種稱為 EverSpy 的 RAT，它在 2023 一整年都在各種平臺上做廣告，而且還被破解公開。在過去的一年裡，賽門鐵克發現大量與該 RAT 相關的測試活動，但我們也觀察到以 APP 偽裝和偷渡式下載為形式的實際惡意活動。EverSpy 具有大多數安卓平台 RAT 所具備的常見功能。以下是其部分功能：

- 來電轉接和歷史記錄
- 簡訊內容轉發與發送簡訊
- 收集連絡人
- 鎖定設備
- 刪除APP
- 鍵盤側錄
- 螢幕截圖
- 照片竊取
- 自行啟動 APP

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

2024/02/02

「天乾物燥，小心火燭」V.S「報稅季節，小心木馬」

研究人員最近觀察到 TA576 駭客集團又回來了，TA576 自 2018 年以來一直使用電子郵件垃圾郵件和其他惡意軟體傳輸技術發動攻擊。今年年初，出現針對北美會計和金融機構的新的稅務相關威脅攻擊。這些攻擊行動濫用尋求報稅協助的電子郵件發送遠端存取木馬 (RAT)。攻擊鏈利用主機上的現有腳本和服務發動惡意活動，並在執行最終有效籌載之前將多個 PowerShell 腳本串聯一起。

每年的報稅孳生的網路攻擊行動屢創新高，隨著今年報稅季節的到來，勢必能會出現類似的網路攻擊行動。

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：

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：

- Trojan Horse

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!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。

2024/02/02

全新的AsukaStealer惡意竊密程式

有人發現一款新上市的惡意竊密程式廣告。該惡意軟體名稱為 AsukaStealer，被定位為以惡意軟體即服務的營運模式。這種新型惡意套裝軟體含常見的資訊竊取功能，例如：竊取瀏覽器和加密貨幣錢包的資料和憑證、Discord 權杖、收集系統資訊和畫面截圖功能。

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：

- Infostealer
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2024/02/02

正在鎖定烏克蘭瘋狂散播的PurpleFox(又名 DirtyMoe)惡意軟體

據報導，被稱為 DirtyMoe 或 PurpleFox 的惡意軟體正在鎖定烏克蘭瘋狂散播。DirtyMoe 採用模組化架構，並帶有 rootkit 元件。該惡意軟體具有後門功能，可用於遠端存取、下載更多額外的惡意有效籌載，甚至可用於發動 DDoS 攻擊。感染鏈包括初始階段的惡意 .MSI 安裝程式，以及後期攻擊階段透過暴力嘗試和漏洞利用進行的惡意軟體自我傳播機制。

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：

- ACM.Ps-Rd32!g1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Hacktool.Rootkit
- Infostealer
- Trojan Horse

- Trojan.Gen.MBT
- Trojan.Kewgad
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- 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。

2024/02/02

使用手機請小心～VajraSpy安卓手機／行動裝置上的惡意程式涉入最近的網路攻擊行動

VajraSpy 是一款可依需打造的安卓手機／行動裝置上的惡意程式，歸屬於 Patchwork 進階持續威脅 (APT) 駭客組織。在真實網路情境觀察到新發動的傳播這種惡意軟體的網路攻擊行動。一些隱藏 VajraSpy 惡意有效籌載荷的惡意 APP 上架在 Google Play 商店中。VajraSpy 主要用於發動有針對性的間諜活動。該惡意軟體能夠擷取使用者資料、按鍵紀錄、通話記錄、存儲的檔案、簡訊、WhatsApp 和 Signal 訊息，還能啟動通話錄音和拍照。

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.Malapp
- Android.Reputation.2
- AppRisk:Generisk

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。

2024/02/02

DX31勒索軟體

Dx31 是 Phobos 勒索軟體家族的另一個後繼新變種，最近剛剛在真實網路情境被發現。該惡意軟體會加密使用者資料，並冠上 .dx31 的副檔名，在副檔名前也會冠上不同專屬的英文字母與數字命名的受害者編號和開發者的電子郵寄地址。加密完成後，被害者的電腦上會出現一個勒索贖金支付說明的文字檔。該惡意軟體具有停用本機防火牆和刪除端點上卷陰影副本備份的功能。

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：

基於行為偵測技術(SONAR)的防護：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Phobos!gm1

基於機器學習的防禦技術：

- Heur.AdvML.B

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: Ransom.Crysis Activity 3

2024/02/02

GreenBean(*綠豆)～安卓手機／行動裝置銀行木馬

GreenBean 是一種全新的安卓手機／行動裝置上的銀行木馬。該惡意軟體主要針對電子商務支付系統、銀行業務和加密貨幣相關的應用程式。GreenBean 濫用安卓系統無障礙服務來獲取目標應用程式的憑證。C&C 伺服器通訊是借助開源的簡單即時伺服器 (SRS) 專案所建立的。GreenBean 還利用主流的媒體串流技術 webRTC 進行螢幕畫面分享和啟動鏡頭錄影功能。

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：

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
- Android.Reputation.2
- AppRisk:Generisk

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。