保安資訊--本周(台灣時間2024/01/05)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 49 萬 3,500 台受保護端點上總共阻止了 5,330 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：**(2024/01/02)**

- 在**9萬2,900**台端點上，阻止了**1,580**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬8,000**台端點上，阻止了**1,434**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬8,400**台**Windows**伺服主機上，阻止了**1,020**萬次攻擊。
- 在**5萬7,100**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,800**台端點上，阻止了**80萬500**次嘗試掃描在**CMS**漏洞。
- 在**3萬9,800**台端點上，阻止了**120**萬次嘗試利用的應用程式漏洞。
- 在**17萬7,100**台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,300**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**9萬9,500**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**684**台端點上，阻止了**29**萬次加密勒索嘗試。

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 9.85 萬個受保護端點上阻止了總計 420 萬次攻擊。**(2024/01/03)**

- 使用網頁信譽情資，在 **87.8K** 個端點上阻止 **350** 萬次攻擊。
- 攔截 **23.4K** 個端點上 **554.6K** 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 **8.9K** 個端點上攔截 **146.8K** 次瀏覽器通知詐騙攻擊。
- 在 **337** 個端點上攔截 **18K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **632** 個端點上阻止 **1.7K** 次技術支援詐騙攻擊。
- 在 **133** 個端點上阻止 **452** 次加密劫持嘗試。

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。

2024/01/04

Electronic(*電子)勒索軟體

在真實網路情境觀察到 Electronic 勒索軟體似乎是 BTC 勒索軟體的後繼新變種。它會加密使用者檔案，並冠上 .[Email].[ID].ELECTRONIC 規則及 ELECTRONIC 結尾的附檔名。一旦加密完成，就會存放檔名為『README ELECTRONIC.txt』的勒索 (贖金支付) 說明文字檔，引導如何透過 Telegram 機器人或電子郵件聯繫攻擊者。該惡意軟體會停止各種系統程序和服務，並刪除陰影複製 (shadow copies)。

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：

- Ransom.Gen
- Ransom.Zombie
- Trojan.Gen.MBT
- W32.Neshuta
- 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.A!300

2024/01/04

澳洲聯邦銀行CommBank存戶成為網路釣魚行動覬覦的目標

CommBank 是澳洲聯邦銀行 (Commonwealth Bank of Australia) 的簡稱，是澳洲最大的金融機構之一，也是紐西蘭、美國、英國……等其他幾個國家以及亞洲部分地區舉足輕重的銀行。多年來，人們在電腦和手機上發現無數企圖竊取 CommBank 存戶憑據的網路釣魚行為。後者雖然不太常見，但卻越來越普遍。

在最近的一個網路釣魚行動中，賽門鐵克觀察到網路釣客向澳洲民眾發送釣魚簡訊，假冒銀行並謊稱異常的帳戶活動來引誘存戶。簡訊內容包含一個網址鏈接，該網址的一段字串包含誤植的澳洲聯邦銀行的域名 (Commonwealth Bank of Australia)，以取得信任以利降低心防及戒心。

觀察到簡訊內容：

- CommBank 已檢測到異常交易，請按照網址鏈接提示立即完成驗證：hxxps://www[.]comnebank[.]com

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 CommBank 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。

2024/01/04

UAC-0050駭客集團濫用Remcos遠端存取木馬(RAT)攻擊烏克蘭政府機構

據報導，UAC-0050 駭客集團濫用 Remcos 遠端存取木馬 (RAT) 攻擊烏克蘭政府機構。攻擊通常從偽裝成人力銀行的職缺或建議書的網路釣魚或垃圾郵件所開啟，部署包含 VBS 和 PowerShell 腳本的惡意 .LNK 捷徑檔和 .HTA 網頁格式檔。最終，這個感染鏈會觸發 Remcos 遠端存取木馬 (RAT) 有效籌載的執行，攻擊者主要利用它進行情報搜集和間諜活動。

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：

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!gen111
- ISB.Downloader!gen63
- Scr.Heuristic!gen20
- Scr.Malcode!gen
- Scr.Mallnk!gen13
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.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：

- 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。

2024/01/04

網路釣客假冒墨西哥稅務局採用的電子發票--Comprobantes Fiscales Digitales por Internet(CFDI)格式來發送釣魚郵件

賽門鐵克在最新網路釣魚活動中發現，網路釣客假冒墨西哥稅務局採用的電子發票格式--Comprobantes Fiscales Digitales por Internet (CFDI)，竊取用戶憑據。網路釣魚郵件偽裝成付款通知郵件，要求收件人下載 PDF 或 XML 格式的電子發票。要下載電子發票，收件人必須點擊偽裝成下載網頁的網路釣魚網址。

- 電子郵件主旨：Fw：Error en tu pago cfdi. -([random_numbers])
- 翻譯後的電子郵件主旨： Fw：您的 cfdi 付款出錯。-([隨機的一組數字])

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。

2024/01/04

Shuriken勒索軟體

Shuriken 是在真實網路情境所觀察到的全新勒索軟體。該惡意軟體似乎是 Blackbit(又名 LokiLocker) 勒索軟體家族的後繼新變種。它會加密使用者檔案並冠上 .Shuriken 副檔名。加密完成後，檔名為『READ-ME-SHURKEWIN.txt』的勒索 (贖金支付) 說明文字檔，會被存放在受感染機器上被加密檔案所在的資料夾。該惡意軟體具有停用 Windows 防火牆、刪除卷影副本以及受感染端點的系統備份等功能。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Schtsk!g1
- ACM.Untrst-FlPst!g1
- ACM.Wmic-DlShcp!g1
- AGR.Terminate!g2
- SONAR.RansomGen!gen3
- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen752

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100

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: Bad Reputation Process Request 4

2024/01/04

假借哈薩克國家石油天然氣公司(KazMunayGas)的名義：網路駭客濫用知名竊密惡意程式：Formbook針對世界各地的公司和政府機構發動攻擊

在變幻莫測的網路威脅中，當我們步入 2024 年時，Formbook 仍然是一個歷久不衰的竊密惡意程式。賽門鐵克在新年的頭幾天，一直在持續監控世界各地的網路攻擊行動。以一個正在進行中的攻擊事件為例，一個網路惡棍冒充哈薩克國家石油和天然氣公司 (KazMunayGas) 發送電子郵件。

這些惡意電子郵件 (主旨：КОМЕРЧЕСКИЙ ПОСТАВЩИК) 被發送到德國、英國、加拿大、俄羅斯、土耳其、以色列、日本、模里西斯、匈牙利、福克蘭群島、西班牙、阿聯酋等國的企業組織和政府機構。郵件附件是一個壓縮檔 (КОМЕРЧЕСКИЙ ПОСТАВЩИК.zip)，其中包含偽裝成虛假商業證明文件的惡意 Formbook 二進位檔案 (КОМЕРЧЕСКИЙ ПОСТАВЩИК.exe)。

眾所周知，這種持頑強惡意軟體給企業組織和政府機構構都帶來了巨大風險。其影響包括潛在的資料洩露，導致關鍵資訊外洩、經濟損失、運營中斷和聲譽受損。對於企業組織來說，智慧財產權被盜是一個令人擔憂的問題，而政府機構則面臨著國家安全問題。

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)。

基於行為偵測技術(SONAR)的防護：

- ACM.Untrst-RunSys!g1
- ACM.Rgsvc-Lnch!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Suspexec!gen8
- Scr.Malcode!gdn34
- Trojan.Formbook

基於機器學習的防禦技術：

- 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.Formbook Activity 2
- Web Attack: Webpulse Bad Reputation Domain Request

2024/01/03

好諷刺～STOP不是停止的意思嗎？STOP勒索軟體發動大規模攻擊

STOP 勒索軟體 (又稱 DJVU) 的後繼新變種在真實網路情境大肆氾濫。STOP 勒索軟體主要透過破解盜版軟體和瀏覽網頁的偷渡式下載傳播。一旦觸發，該惡意軟體就會加密使用者檔案，並冠上四個字母的副檔名，例如：.cdqw、.nbzi……等。加密過程結束後，會發現一個名為『_readme.txt』的勒索 (贖金支付) 說明文字檔，要求以比特幣支付贖金。

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：

基於行為偵測技術(SONAR)的防護：

- Ransom.Pots

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.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。

2024/01/03

三井住友銀行(SMBC)存戶遭受到新一波網路釣魚攻擊

三井住友銀行(SMBC)是一家日本跨國銀行，總部位於日本東京千代田區。最近，賽門鐵克發現有釣魚網站冒充三井住友銀行的服務，誘使使用者打開虛假的通知郵件。郵件內文簡短，提及確認 SMBC 卡的使用。這些釣魚郵件試圖誘使用戶開啟並點擊釣魚網址。在這次釣魚電郵攻擊中，網路釣客濫用網域名稱相似的打錯字或記錯網址手法冒充合法的 SMBC 網站網址。

- 電子郵件主旨：【重要なお知らせ】三井カードご利用確認のお願い
- 翻譯後的電子郵件主旨： [重要通知] 請求確認三井卡的使用情況

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。

2024/01/03

在真實網路情境發現Meduza竊密程式的最新版本

最近，人們發現一個宣傳最新版 Meduza 竊密程式的廣告，並且已經注意到它的活動 (透過瀏覽網頁的順道下載感染)。該竊密程式與其他竊密程式基本上相同，有人將其與更惡名昭彰的竊密程式 (例如：AzorUlt、Raccoon 和 RedLine) 相提並論。該威脅針對敏感的瀏覽器資訊、密碼錢包、Discord 和 Telegram 資料、Steam、密碼管理器等。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Msbuild!g1

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
- Heur.AdvML.B!200

2024/01/03

Empire(*帝國)勒索軟體

Empire 是一種在真實網路情境所觀察到的新型勒索軟體。該惡意軟體會加密使用者檔案並冠上 .emp 副檔名。加密完成後，一個名為『HOW-TO-DECRYPT.txt』的勒索 (贖金支付) 說明文字檔就會出現，其中說明如何使用 Telegram 機器人或透過電子郵件與勒索軟體加害者聯繫。該惡意軟體具有刪除受感染機器上的陰影複製 (shadow copies) 和系統備份的功能。

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.Untrst-FlPst!g1
- SONAR.MalTraffic!gen1
- SONAR.Ransomware!g16
- SONAR.SuspWrite!g6

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.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：

- 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。

2024/01/03

烏克蘭政府機關遭俄羅斯駭客APT28鎖定，散布惡意程式Masepie

在針對烏克蘭的新一波網路攻擊行動中，APT28 駭客集團 (又名 Fancy Bear 或 Strontium) 利用釣魚信件誘騙收件人點擊一個鏈結，宣稱有一份重要文件務必閱覽。

點擊這些鏈結會將受害者重新導到惡意的網頁，該網頁的 JavaScript 語法可以自動下載一個 Windows 快捷列檔案 (LNK)，該檔案會啟動 PowerShell 命令，進而觸發另一個名為『MASEPIE』新型 Python 惡意軟體下載器的感染鏈。該惡意軟體的主要作用是在受感染設備上下載其他惡意軟體並竊取資料。

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 Horse
- Trojan.Gen.MBT
- Web.Reputation.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。

2024/01/02

安卓平台上的竊密軟體Ermac--正在誘惑聯安(Allianz)在巴西的客戶

安卓平台上知名竊密軟體 Ermac，至少從 2021 年就開始出現，在過去 3 年中，因其先進的功能和竊取敏感資訊的能力 (尤其是針對銀行和加密貨幣憑證) 而成為頭條新聞。時至今日，這種威脅仍然非常活躍並廣受多個駭客團體和個體戶喜好，對消費者和企業用戶造成嚴重影響。

最近，賽門鐵克觀察到一個網路惡棍，將惡意二進位檔案偽裝成 Allianz Brasil 的安卓 APP (Allianz Brasil.apk)，以巴西的行動用戶為目標。Allianz Brazil 是全球領先的保險和金融服務提供者之一 Allianz SE 的巴西分公司。我們認為，這些網路犯罪分子的目標是安聯客戶，因為他們有可能透過多種途徑管理財富和進行金融交易，因此安聯客戶是網路惡棍垂涎欲滴的目標。

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：

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

2024/01/02

Albaba勒索軟體(又名White Bat*白蝙蝠)

最近幾周，Albabat 勒索軟體 (又名White Bat*白蝙蝠) 被觀察到在針對不同國家 (例如：匈牙利、哈薩克、美國、捷克……等)的企業和消費者四處傳播。根據觀察到的二進位檔案，該組織似乎在使用假冒 Windows 10 數位授權啟用工具來感染使用者。

成功入侵後，除了加密檔案外，該勒索軟體還會更改桌面背景圖案 (黑底白字的蝙蝠徽標) 及置放 HTML 格式的勒索 (贖金支付) 說明的網頁格式檔。

勒索 (贖金支付) 說明中包含關於該組織的詳細資訊、所使用加密方法的說明、聯繫方式 (加密郵件 Proton Mail 帳號) 以及贖金支付說明 (比特幣地址和價格)。在最近的活動中，他們索價 0.0015 比特幣 (撰寫本文時價值 67.87 美元)。他們的贖金說明中沒有明確提到採取雙重勒索手段，只建議受害者有在願意遵守贖金要求的情況下才聯繫他們。

感染 Albaba 勒索軟體的特徵，還包含會生成以下的資料夾和檔案：

- %USERPROFILE%\Albabat\Albabat.ekey
- %USERPROFILE%\Albabat\Albabat_Logs.log
- %USERPROFILE%\Albabat\personal_id.txt
- %USERPROFILE%\Albabat\readme\README.html
- %USERPROFILE%\Albabat\readme\assets\banner.jpg
- %USERPROFILE%\Albabat\readme\assets\script.js
- %USERPROFILE%\Albabat\readme\assets\style.css
- %USERPROFILE%\Albabat\readme\pages\faq.html
- %USERPROFILE%\Albabat\wallpaper_albabat.jpg

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.Vss-DlShcp!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Sc!g1
- ACM.Untrst-RunSys!g1
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!gen4

- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.Cryptlocker!g38

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Ransom.Albabat

2024/01/01

網路購物線上市集(例如：Mercari--日本最大二手交易平台線上市場)年終強強滾，網路釣客也一樣

網路購物線上市集 (例如：Mercari--日本最大二手交易平台線上市場)，通常在年終歲末生意會特別好。許多人都會在年底進行大掃除、整理和重新布置，這往往會導致他們出售不再需要的物品。此外，節慶長假也會促使人們為送禮或為節慶假日開支賺取外快而買賣物品。賽門鐵克發現，每年的這個時候，網路釣魚活動都會明顯增加。

例如：一個網路釣客透通過隨機生成域名的電子郵件，向日本消費者和企業使用者發送惡意電子郵件。郵件主旨為『【メルカリ】一時的な利用停止、ログインして確認してください、』利用典型的恐嚇帳戶被凍結之伎倆，試圖誘使收件人點擊惡意網址並將其重轉向偽造的 Mercari 登錄頁面，以騙取憑證／帳密。

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。

2024/01/01

又是利用Chaos勒索軟體的後繼新變種～Pirat(*皮拉特)勒索軟體集團

據觀察，一個被稱為『Pirat』駭客組織利用 Chaos 勒索軟體的後繼變種，來攻擊企業和消費者的個人電腦。雖然它已在多個國家被發現，但與其他從事多重加密、橫向移動和雙重勒索更邪惡的勒索軟體駭客組織相比，它的流行程度並不高。

成功入侵後，該勒索軟體會加密檔案，並冠上一個隨機的 4 個字元的副檔名。該勒索軟體會留存一個以『HACKED BY PIRAT HACKER GROUP』開頭的勒索 (贖金支付) 說明檔，告知受害者需支付價值 300 美元的比特幣。他們還提供一個加密貨幣錢包位址和聯繫的電子郵件。

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.Untrst-RLsass!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- SONAR.SuspLaunch!g266
- SONAR.Dropper
- SONAR.SuspDrop!gen1
- SONAR.SuspLaunch!g22
- SONAR.SuspBeh!gen676
- SONAR.SuspBeh!gen625
- SONAR.Susp

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

2024/01/01

年終也不得閒：偽造日本電力公司逾期未繳電費通知的網路釣魚行動

日本是一個網路釣魚郵件非常氾濫的國家，即使是在許多人放假休息的年終最後一周和新年第一天也不例外。賽門鐵克發現，目前有一種針對日本企業和消費者逾期未繳電費通知的社交工程網路釣魚行動。

該主使者在電子郵件上動手腳（主旨：【くらしTEPCO】電気料金未払い？即時対応が必要），假冒日本大型電力公司東京電力控股公司（TEPCO）。如果用戶沒有戒心中了圈套並點擊惡意網址，將會被重導向到假冒的東京電力公司登錄頁面。該域名是依附在 XYZ 為頂層網域名之下，其實是採用域名誤植或打字錯誤 (typosquatting) 的伎倆，以進一步欺騙用戶。

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。

2023/12/28

Barracuda電子郵件安全閘道器(ESG)的CVE-2023-7102零日漏洞已被開採濫用

據報導，一個名為 UNC4841 的中國國家級駭客組織開採濫用 Barracuda 電子郵件安全閘道器 (ESG) 的 CVE-2023-7102 零日漏洞。該駭客組織開採濫用名為『Spreadsheet ParseExcel』的第三方 Perl 模組中的任意程式碼執行漏洞 (Arbitrary Code Execution，ACE)，並透過被動過手腳的 Excel 檔案附件來植入惡意程式碼並觸發感染鏈。Barracuda 觀察到在這些 ESG 電子郵件安全閘道器上被傳送 SEASPY 和 SALTWATER 惡意軟體的新變種。

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：

- DDoS.Trojan
- Exp.CVE-2023-2868
- Linux.Trojan
- Trojan Horse
- WS.Malware.2
- WS.SecurityRisk.4

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。