保安資訊--本周(台灣時間2023/11/24)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 69 萬 1,000 台受保護端點上總共阻止了 5,990 萬次攻擊。這些攻擊中有 80.1% 在感染階段前就被有效阻止：**(2023/11/20)**

- 在**10萬1,200**台端點上，阻止了**2,370**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**17萬2,400**台端點上，阻止了**1,460**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬1,200**台**Windows**伺服主機上，阻止了**1,180**萬次攻擊。
- 在**6萬400**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,500**台端點上，阻止了**85萬800**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,100**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**22萬6,400**台端點上，阻止了**440**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,100**台端點上，阻止了**440**萬次加密貨幣挖礦攻擊。
- 在**11萬3,800**台端點上，阻止了**940**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**788**台端點上，阻止了**4萬6,800**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 1.611 萬個受保護端點上阻止了總計 670 萬次攻擊。**(2023/11/20)**

- 使用網頁信譽情資，在 **1.424** 萬個端點上阻止 **570** 萬次攻擊。
- 攔截 **34.9K** 個端點上 **700.5K** 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 **14.9K** 個端點上攔截 **179.8K** 次瀏覽器通知詐騙攻擊。
- 在 **736** 個端點上攔截 **71K** 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 **1.4**K 個端點上阻止 **2.3K** 次技術支援詐騙攻擊。
- 在 **238** 個端點上阻止 **532** 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。

2023/11/23

可能是駭客圈的明日之星：Persian Remote World(*波斯遠端世界)駭客集團自用也對外銷售自己的駭客工具

最近成立一個名為『波斯遠端世界』(Persian Remote World) 駭客集團，開發自己的駭客工具，在網路上大辣辣地以訂閱模式出售。這些駭客工具涵蓋多種功能，包括負責互相調適連結惡意酬載的載入程式、遠端存取木馬 (RAT)、資訊竊取程式、銀行木馬、螢幕截圖，當然也包含勒索軟體。

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：

- Trojan.Gen.MBT
- Ws.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/11/22

ClearFake攻擊行動向macOS用戶發送原子竊密程式(AMOS)惡意軟體

原子竊密程式 (Atomic Stealer：又名 AMOS) 是一種 macOS 平臺上的惡意軟體，最近在一場被稱為 ClearFake 的惡意攻擊行動中被傳播。攻擊者將惡意二進位檔案偽裝成假冒的 Safari 或 Chrome 瀏覽器之更新檔 DMG 包。據瞭解，AMOS Stealer 可從受感染的 macOS 電腦中滲出各種敏感性資料，包括系統資訊、金鑰密碼、瀏覽器資料和 cookie、信用卡詳細資訊、加密貨幣錢包等。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- 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。

2023/11/22

XWorm惡意軟體在真實網路情境依舊陰魂不散

XWorm 是一種基於 .NET 的商品化遠端存取木馬 (RAT)，在真實網路情境被廣泛操弄。雖然該惡意軟體家族在過去曾多次被發現，但新版本仍在地下論壇上出售，並可能由不同的威脅組織在不同的攻擊行動中大肆傳播。除了典型 RAT 常見的功能外，XWorm 最新變種還具有一些額外的竊密功能，允許攻擊者收集機密的使用者資料、銀行詳細資訊、憑證、cookie 和其他資訊。該惡意軟體還可以從 C&C 伺服器下載其他外掛程式，從而進一步增強其運作能力。

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：

- ACM.Ps-Rd32!g1
- ACM.Untrst-FlPst!g1
- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen752
- SONAR.SuspDataRun
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Xworm!gen1

- Scr.Malcode!gdn14
- Scr.Malcode!gdn30
- 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
- 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 568

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。

2023/11/21

非原廠下載的NetSupport Manager安裝檔被植遠端存取木馬(RAT)

威脅行動者篡改熱門的跨平台、跨設備、多據點的多人桌面遠端管理軟體：NetSupport Manager 真實用途，以執行惡意活動，現在它作為遠端存取木馬 (RAT) 執行。最近報告顯示，使用者透過從上架在遭入侵網站上的捆綁，在虛假瀏覽器更新檔案中下載該工具。

一旦在受害者的機器中建立立足點，攻擊者就會獲得遠端存取控制權，有可能跨越各種連線電腦，最終竊取受害者的敏感資訊並執行一系列的惡意活動。

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.Gen.NPE
- WS.Malware.1
- WS.Reputation.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。

2023/11/21

針對印度的安卓平台垃圾郵件攻擊行動

印度的安卓手機用戶最近經由 WhatsApp 或 Telegram 收到來自一個實體的消息，該實體聲稱自己在銀行、政府服務和公用事業等各種機構工作。目標使用者被要求使用威脅行動者轉發的銀行 APP 安裝檔 ([org name]-bank.apk) 更新他們的永久帳號 (PAN)，如果不更新，他們的銀行帳戶將被凍結。如果目標受害者同意並成功上當安裝惡意 APK 檔，攻擊者就能竊取個人資訊和銀行相關憑證／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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- WS.Malware.2

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

2023/11/21

Remcos遠端存取木馬程式(RAT)--聰明的社交工程，還是糊塗的作者？

無論是否有針對性，大多數惡意垃圾郵件攻擊行動一般都是操弄社交工程手段，綿密編織人性互動相關聯的元素，以讓受害者毫無戒心地上當。然而，確實存在各組成部分無法協調一致百密一疏的必然情況。在這種情況下，攻擊者可能會利用用戶的困惑，誘使一些人出於好奇而點擊，卻對明顯的警訊視若無睹。

最近一起 Remcos 攻擊行動就是一個很好的例子，在該行動中，威脅行動者假冒在布宜諾斯艾利斯、特雷利烏和伊瓜蘇港設有分店的阿根廷連鎖酒店。然後，他們用阿拉伯語發送惡意電子郵件 (主旨為『نخسن ةروتافلا』)，並使用不同員工姓名冒充阿聯酋的一家鋼鐵公司。耐人尋味的是，他們試圖透過聲明他們的新電子郵件域名今後將與鋼鐵公司相關聯來為受害者注入信心，這就可想而知了。

電子郵件附件包含一個 .R10 壓縮檔 (INVOICE0987654570.R10) 和 Remcos 二進位檔案 (INVOICE0987654570.exe)，隨機發送給英國、美國和歐盟的公司，其中一些公司位於阿聯酋。

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

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.Remcos

基於機器學習的防禦技術：

- Heur.AdvML.B!200

2023/11/21

防護亮點：網路釣魚呈上升趨勢，賽門鐵克讓自己更強大

網路釣魚是一種基於社交工程伎倆的網路攻擊，攻擊者發送垃圾郵件 (通常是電子郵件或簡訊，但也越來越多包括社交媒體甚至電話)，目的在欺騙目標對象洩露敏感資訊 (例如：信用卡號或帳號密碼)，或在受害者的裝置上安裝惡意軟體。網路釣魚攻擊日益增多，任何使用電子郵件、簡訊和其他通訊方式的人 (即我們中的大多數人) 都有可能成為受害者。

據統計，全球每天發送的垃圾郵件和簡訊數高達數十億計，有些調查顯示垃圾郵件占所有電子郵件的比例約為 50%，而另一些調查則顯示垃圾郵件比例遠遠超過 80%。可以說這是一個相當大的比例，導致大量未經請求、不受歡迎的資訊。其他與垃圾郵件相關的統計數字包括：有報告稱，超過 80% 的公司每年至少會遭受一次網路釣魚攻擊，而遭受攻擊次數逐年增加的比例也與此類似。據聯邦調查局報告，僅在 2022 年，網路釣魚攻擊就超過 30 萬次。據報導，公司遭受一次典型的網路釣魚攻擊需要花費近 500 萬美元來善後，令人唏噓不已。另一項調查報告顯示，約 90% 的企業資安危害事件是網路釣魚攻擊造成。

組織可能面臨一些最常見的網路釣魚攻擊包括：

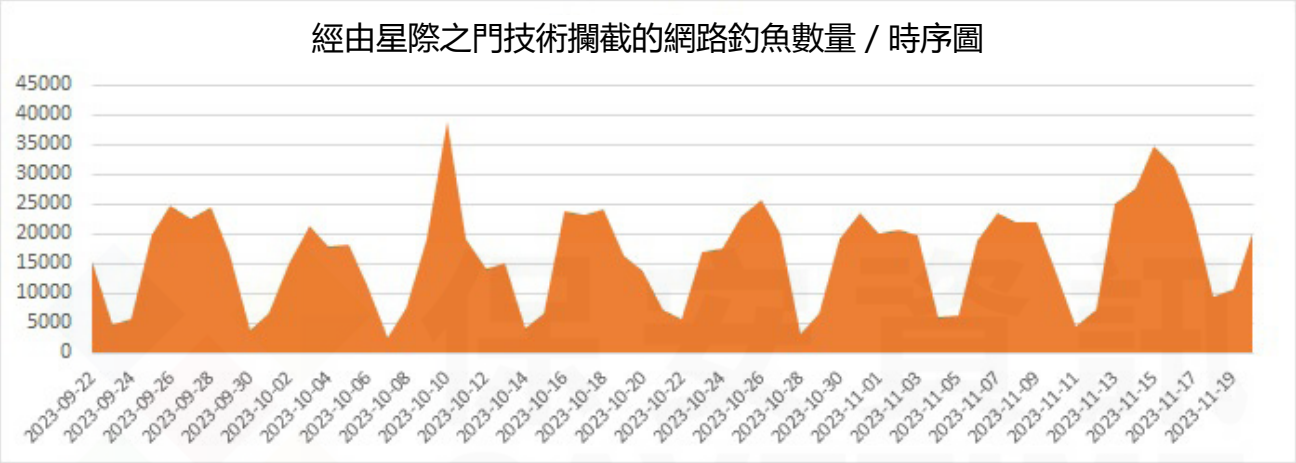
- 電子郵件網路釣魚--這是最常見的網路釣魚形式，攻擊者發送看似來自合法來源的欺騙性電子郵件。
- 魚叉式網路釣魚---一種更有針對性的攻擊形式，攻擊者會對目標進行背景研究，以定制他們的資訊。
- 鯨釣--此類攻擊以公司高階主管知名人士為目標。
- 網址嫁接攻擊 (Pharming)--是一種重新導向 (Re-dircert) 的詐騙技巧，由網路釣魚 (Phishing) 衍生而來，藉由入侵使用者電腦、植入木馬程式 (Trojan)，或者是利用域名伺服器 (Domain Name Server；DNS Server) 的漏洞，將使用者錯誤地引導到偽造的網站中，並伺機竊取重要資料。

常見的偽冒寄件者包括：

- 快遞公司
- 銀行和金融機構

- 網購等電子商務公司
- 政府部門服務
- 人力銀行等招聘服務

去年 12 月，我們發佈關於星際之門 (Stargate) 在『即使採用混淆技術的的網路釣魚攻擊也不是賽門鐵克Stargate(*星際之門)安全引擎的對手』的文章。當時，我們情資大數據的遙測系統平均每天記錄 2,500 個攔截，12 月 5 日出現一個相當大的峰值。相比之下，我們現在平均每天記錄約 17,000 個攔截，峰值超過 30,000 個。雖然沒有出現在下圖中，但 8 月初出現超過 60,000 個攔截的峰值。看來網路釣魚不會很快消失。



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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malscript!gen2

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。

欲深入了解有關賽門鐵克端點安全安全完整版更多資訊，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。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲瞭解有關星際之門安全服務（基於機器學習、雲知識和深度內容檢查的威脅檢測平臺）的更多資訊，請點擊此處聯繫賽門鐵克。

2023/11/21

蝙蝠對病毒的易感性無庸置疑～Batloader在惡意程式的感染鏈也不容小覷

Batloader 惡意程式載入程式常被用於散佈各式各樣的遠端存取木馬 (RAT)、勒索軟體、竊密程式、以及 AgentTesla 間諜程式等各種惡意軟體。無論它的程式碼有何細微變化，其基本方法始終保持驚人的一致性。這一過程的複雜程度可能各不相同，但 Batloader 被用作協調與互相串連多階段攻擊的工具，以確保最終有效籌載確實交付與執行的腳色始終不變。

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.BatCloak!gen2
- SONAR.SuspLaunch!g84

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.Suspexec!gen
- Scr.Malcode!gen108
- Trojan.BatCloak!gen2
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan Horse
- 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。

2023/11/21

Konni遠端存取木馬在最近的網路攻擊行動中被大肆散播

在最近網路攻擊行動中被大肆散播 Konni 的遠端存取木馬 (RAT) 是濫用惡意 Word 檔、批次檔和 DLL 二進位檔案被大肆散播。Konni 遠端存取木馬具有從遭入侵電腦中擷取機密資料和執行遠端命令的功能。Konni 還具有繞過使用者帳戶控制 (UAC) 和與 C&C 伺服器進行加密通訊的功能。

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-Rd32!g1

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
- 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。

2023/11/21

LitterDrifter惡意軟體

LitterDrifter 是一種惡意軟體，歸屬於 Gamaredon(又名 Shuckworm) 駭客集團。LitterDrifter 是一種用 VBS 撰寫的蠕蟲，已知可透過 USB 隨身碟自我傳播。它的主要功能是向其他端點傳播感染，並執行從威脅者操控的 C&C 伺服器接收命令或任意有效籌載。迄今為止，LitterDrifter 主要用於針對烏克蘭目標的攻擊行動，但在美國、越南、智利、波蘭和德國也發現它的感染痕跡。

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.Downloader!gen53
- Trojan Horse
- Trojan.Gen.NPE
- VBS.Downloader.Trojan
- 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。

2023/11/20

觀察到Wikiloader惡意垃圾郵件攻擊行動

有報告稱，在另一場 WikiLoader 攻擊行動，網路惡棍使用帶有惡意網頁鏈結的電子郵件作為攻擊鏈之初始階段。這是一起亂槍打鳥的攻擊行動，不針對特定的組織，也不局限於特定的國家--該惡意電子郵件在世界各地都有出現。WikiLoader 是一種惡意軟體下載器，於 2022 年底首次曝光，與 Ursnif 等多種惡意軟體威脅有關。

觀察到的電子郵件主旨：

- 逾期應收帳款對帳單
- 付款狀態通知單
- 應收帳款對帳單

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.Ps-Wscr!g1
- ACM.Wscr-CPE!g1
- ACM.Ps-Rd32!g1
- ACM.Wscr-Rd32!g1
- SONAR.SuspLaunch!g235

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：

- Audit: Scripting Host Processes Making Network Connections
- Audit: System Process Accessing discordapp.com
- 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。

2023/11/20

駭客發動NjRAT遠端存取木馬攻擊行動：針對西班牙諮詢、醫療保健和能源行業

11 月中旬，賽門鐵克發現有人企圖利用一種著名的遠端存取木馬 (NjRAT) 感染西班牙的企業和組織。惡意電子郵件 (主旨：ENVIO FACTURAS SOLICITAD ENVIO FACTURAS SOLICITADA (Facturas Nº:232683)) 冒充一家德國建築材料製造商 (更具體地說是其西班牙子公司)，啟動帳單相關的社交工程伎倆。

就受害者而言，他們主要針對諮詢、醫療保健和能源相關公司。如果用戶碰巧被誘騙，他們將打開所附的壓縮檔 (FACTURAS.rar)，再打開偽裝成假帳單 NjRAT 二進位檔案 (FACTURAS.exe)。

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-FlPst!g1
- SONAR.SuspBeh!gen625

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

2023/11/20

Fenix剪貼簿挾持軟體(Clipper)

在某些方面，加密錢包剪貼簿挾持軟體 (Clipper) 被認為比挖礦挾持更有利可圖，除非可以營運一個大型殭屍網路。在過去幾年中，許多此類加密錢包剪貼簿挾持軟體 (Clipper) 器都在地下論壇甚至雲端軟體開發及版本控制服務平台上做過廣告。

在本防護公報中，我們將介紹一款名為『Fenix』的程式，它可能不像某些程式那樣普遍，但在威脅環境中也被觀察到，值得注意是它擁有 AS 旁路功能。

它主要透過瀏覽網頁常見的順道下載社交工程伎倆傳播，主要目標是消費者。它的活動時斷時續，只要有人在網站、論壇和社交媒體上新貼文就會出現小高峰。

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-RunSys!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

2023/11/20

加密貨幣主要功能是付勒索贖金嗎?土耳其正遭遇新一波Chaos勒索軟體攻擊，要求透過Metamask(小狐狸)加密貨幣錢包來支付贖金

土耳其的消費者和企業用戶最近正遭受駭客發動新一波 Chaos 勒索軟體攻擊的肆虐。相較於其他一些聲名狼藉的勒索軟體，它們活動影響仍然較小，因為它們不會在內網橫向移動。它們主要針對單台機器，並要求受害者透過 Metamask(小狐狸) 加密貨幣錢包來支付金額等值約為為 10,000 土耳其里拉的勒索贖金。

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：

- ACM.Untrst-RLsass!g1
- SONAR.Dropper
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- SONAR.SuspBeh!gen625
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!gen4
- ACM.Vss-DlShcp!g1
- SONAR.Suspl

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

2023/11/20

8base駭客組織在發動其Phobos勒索軟體的攻擊行動中，濫用SmokeLoader後門木馬

一個全新的 Phobos 勒索軟體變種被認為可能出 8base 駭客組織。該變種是經由 SmokeLoader 後門木馬來載入和執行。與其他勒索惡意軟體一樣，Phobos 具有常駐能力、終止開啟中檔案的程序、停用復原功能、刪除備份和磁卷陰影複製 (volume shadow copies)。被其加密後的檔案通常會被冠上『.8base』副檔名。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspDataRun
- SONAR.SuspLaunch!gen4
- 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：

- Downloader
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Ransom.Phobos!g2
- Ransom.Phobos!gm1
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1
- WS.SecurityRisk.4

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

2023/11/19

SnakeKeylogger多功能竊密惡意程式：冒充俄羅斯醫學物理師協會(AMFR)的網路攻擊正在歐洲及中東流竄

SnakeKeylogger 多功能竊密惡意程式在駭客圈舉足輕重，也受到全球多個駭客組織和個人大量使用。賽門鐵克發現一個始於 11 月 17 日新一波網路攻擊行動，攻擊者冒充俄羅斯醫學物理師協會 (AMFR：Association of Medical Physicists of Russia)，鎖定歐洲和中東的各行各業。這些郵件 (主旨：Договор) 包含一個惡意壓縮檔 (Contract.bz)，其中的 SnakeLogger 二進位檔案 (Contract.exe) 被偽裝成一份合約。雖然這是一支簡單的竊密惡意程式，但如果使用者被成功誘騙，其後果可能包括財務和身份盜竊以及重要資料洩露。

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：

- Scr.Malcode!gdn32

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/11/19

TA557駭客組織重新利用Qakbot曾經用過的域名來傳遞Pikabot模組化木馬程式

TA557 駭客組織在這幾年已經在駭客圈佔有一席之地，因其針對全球各行業和組織的持續性惡意垃圾郵件攻擊行動而惡名昭彰。在目前的攻擊行動中，TA557 部署三種不同的有效籌載：IcedID、Pikabot 和最近推出的 Darkgate。Darkgate 出現是繼幾周前成功接收 Qakbot 之後又一重大突破。

賽門鐵克一直在密切關注該威脅組織的活動 (參考以前的防護公報)。儘管 Qakbot 已從威脅環境中消失，但有跡象表明 TA557 仍在繼續利用以前前者使用過的域名。在最近觀察到 146 個域名中，Pikabot 就占 20 個，這證明 TA557 仍在利用以前使用過的域名來散播最新有效籌載。

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)。

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。

2023/11/19

聲東擊西的Chaos新變種：表象是加密勒索，真相是竊取加密貨幣

每天都有人回報 Chaos 惡意軟體，其中大多數都是以消費者和企業的單台電腦為目標，透過瀏覽網頁的順道下載伎倆，通常冒充各種類型的合法軟體。最近，賽門鐵克發現一個變種，其中威脅者在勒索 (贖金支付) 說明中並沒有提到他們聯繫的方式，也沒有提及解密贖金。該說明指出要找回私密金鑰，他們需要在被害者的電腦上找到一個秘密檔案 (實際上並非如此)。除了加密檔案和更改電腦桌面背景圖案為一些樹木的黑白圖片外，該變種還能監控複製到剪貼簿的內容，並對其進行竄改。如果內容被識別為比特幣位址，就會被替換成另一個位址，最終目的當然是竊取加密貨幣。

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
- AGR.Terminate!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/11/19

Eject(*彈出)勒索加密軟體

目前，一個源於 Phobos 勒索軟體的後繼變種正在土耳其和德國境內流竄。成功感染後，它會在被加密檔冠上『.ID(受害者編號)[亂數].[威脅發動者的電子郵件].eject 』副檔名，並在受害者機器上留下勒索 (贖金支付) 說明。該說明是用土耳其語寫的，並沒有顯示贖金金額，並建議受害者透過電子郵件連同提供的 ID(受害者編號) 與威脅發動者聯繫。

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-RunSys!g1
- ACM.Ps-RgPst!g1
- ACM.Vss-DlShcp!g1
- ACM.Wmic-DlShcp!g1
- ACM.Ps-Wbadmin!g1
- ACM.Wbadmin-DlBckp!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!200