保安資訊--本周(台灣時間2023/11/17)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 1,900 台受保護端點上總共阻止了 7,000 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2023/11/12)**

- 在**10萬3,700**台端點上，阻止了**2,440**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**18萬500**台端點上，阻止了**1,510**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬300**台**Windows**伺服主機上，阻止了**1,230**萬次攻擊。
- 在**6萬1,300**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,000**台端點上，阻止了**88萬2,400**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,800**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**22萬8,500**台端點上，阻止了**430**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,900**台端點上，阻止了**350**萬次加密貨幣挖礦攻擊。
- 在**11萬7,500**台端點上，阻止了**960**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**840**台端點上，阻止了**6萬5,000**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。

2023/11/17

Stately Taurus(*莊嚴的金牛座)頑強駭客集團(APT)針對菲律賓展開攻擊行動

據觀察，Stately Taurus 頑強駭客集團 (APT)(又名 Mustang Panda) 最近的攻擊行動可追溯到 8 月份，目標鎖定南太平洋地區的機構，包括菲律賓政府。攻擊者一直在濫用合法軟體來側載惡意二進位檔案。被濫用的應用程式包括 Solid PDF Creator 應用程式和 SmadavProtect 防毒軟體。該威脅組織還試圖將惡意 C&C 連線偽裝成合法的微軟連線。

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.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

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。

2023/11/17

直接撕票，連付贖金的機會也沒有～WannaDie(*想死) 勒索軟體

WannaDie 是最近在真實網路情境所觀察到的另一個源於 Chaos 勒索軟體的新變種。在加密使用者資料後，該惡意軟體會以檔名為『info[隨機數字].txt』的 .txt 文字檔的形式發送一份英語和德語的勒索 (贖金支付) 說明。由於該說明並沒有提供任何聯繫方式，也沒有要求支付任何贖金，因此攻擊者目前可能更側重在將該惡意軟體用作破壞性資料清除程式 (Wiper)，而不是典型的勒索軟體。WannaDie 還能刪除受感染機器的磁卷陰影複製 (volume 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：

- SONAR.SuspBeh!gen625

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

2023/11/17

SystemBC(也稱為 Coroxy)的威力持續危害網路安全

SystemBC (也稱為 Coroxy) 是一個眾所周知的代理機器人，多年來一直被駭客組織用於下載和執行惡意籌載。它具有攻擊鏈許多階段所需的威脅能力，包括從遭入侵系統中收集資料、建立持久性 (常駐)、為惡意流量隧道設置 SOCKS5 代理以及下載和執行包括勒索軟體在內的附加任意有效籌載。據瞭解，SystemBC 多在黑市交易，通常由惡意垃圾郵件行動中的惡意載入程式來傳播。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.SystemBC
- Backdoor.SystemBC!g1
- Backdoor.SystemBC!g2
- Backdoor.SystemBC!g3
- Trojan Horse
- 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.A!400
- Heur.AdvML.A!500
- 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 597
- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 721
- 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。

2023/11/16

神也拼不過愚蠢～阿爾卑斯銀行(Alpine bank)用戶憑證遭受網路釣魚攻擊風險

賽門鐵克最近觀察到鎖定美國科羅拉多州社區型銀行：阿爾卑斯銀行 (Alpine Bank) 存戶的網路釣魚行動。該銀行在該州多個鄉鎮設有據點，以注重社區參與和客戶服務而聞名，攻擊者覬覦他們的銀行憑證／帳密。

這次攻擊幕後的個體戶或組織向銀行用戶發送惡意簡訊，告知他們的轉帳卡 (debit card) 因可疑活動而被鎖定，並邀請他們點擊所提供的網址。雖然這種社交工程伎倆在全世界都很普遍，但老練的威脅者通常會濫用網域名稱相似的打錯字或記錯網址手法來提高用戶上鉤的機會。但在本例中，建立的圈套域名與該銀行域名明顯不像，可見很多人還是缺乏基本的資安概念。

觀察到的簡訊內容：

- 由於最近的活動，我們暫時鎖定您的轉帳卡 (debit card)，請造訪 hxxps[:]//aquamed[.]com[.]pe/c/Alphine/e 立即驗證。

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 已知此活動中使用的虛假網域。

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。

2023/11/16

塞爾維亞農業食品出口商被冒名針對該國多個組織的網路詐騙行動

賽門鐵克最近觀察到塞爾維亞最大的農業食品出口商之一被冒名針對該國多個組織的網路詐騙行動。這些惡意電子郵件以塞爾維亞語撰寫 (主題：Састанак за заказивање)，並以邀請安排業務約訪為由。

電子郵件中還附有一個惡意 .Z 壓縮檔 (Писмо састанка о именовању docx.z)--使用的是 Lempel-Ziv-Welch (LZW) 壓縮演算法。雖然這種演算法在過去很常用，但現在基本上已被 .zip、.gzip 和 .tar.gz 等更高壓縮比的技術所取代。儘管如此，賽門鐵克仍發現某些駭客集團和個體戶還有使用這種壓縮檔。

如果使用者被這種社交工程伎倆成功引誘並執行壓縮檔中的惡意二進位檔案 (Писмо састанка о именовању.docx.exe)，他們最終將運行一個 NullSoft 腳本檔類型的安裝程式，該程式將部署一個載入器和 Agent Tesla 的加密有效籌載。

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)。

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g21
- SONAR.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Atesla

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2023/11/16

又是Chaos的新變種～Shanova勒索軟體

Shanova 是近期在威脅環境中發現源於 Chaos 勒索軟體的全新變種。該惡意軟體會加密使用者檔案，並冠上 .shanova 副檔名。勒索 (贖金支付) 說明以檔名為『read_it.txt』的文字檔形式提供，威脅者要求受害者透過提供的電子郵寄地址與他們聯繫，以獲取如何解密的進一步說明。Shanova 還具有磁卷陰影複製 (volume shadow copies) 的破壞力。

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：

- SONAR.SuspBeh!gen625
- SONAR.SuspLaunch!g22
- SONAR.SuspLaunch!g266

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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2023/11/15

TA402頑強駭客(APT)組織散播全新的惡意程式下載器：IronWind

據報導，TA402 頑強駭客 (APT) 組織最近在針對中東政府實體的網路釣魚行動中散播全新惡意程式下載器：IronWind。該初始攻擊途徑始於一封包含 XLL 或 RAR 檔附件的網路釣魚電子郵件。開啟這些附件後，就會下載和並側載惡意軟體 DLL。

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
- 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。

2023/11/15

Dark Pink(*深粉紅色)頑強駭客(APT)組織的最新活動

眾所周知，Dark Pink 是一個頑強駭客 (APT) 組織，主要鎖定的目標多集中在亞太地區。Dark Pink 擅於進行商業間諜活動、資訊／資料盜竊和滲漏等。該組織濫用各種惡意軟體和定制工具組。其中包括 Cucky 竊密程式、Ctealer 惡意軟體、TelePowerBot 和 KamiKakaBot 等各種殭屍電腦。從被入侵端點收集的資料會透過公共雲服務、HTTP 協定或各種網頁掛勾服務 (Webhooks) 流出。

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：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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。

2023/11/15

編號CVE-2023-46604的Apache ActiveMQ遠端程式碼執行(RCE)漏洞，已被勒索軟體開採利用

CVE-2023-4660 是最近揭露的 Apache ActiveMQ 上的嚴重等級 (CVSS 評分：10) 遠端程式碼執行 (RCE) 漏洞。該漏洞如被開採利用，未經認證的遠端攻擊者可在遭入侵的系統上運行任意 shell 命令。Apache 已於上月底釋出相對應的安全更新。與此同時，該漏洞已被某些威脅者大肆濫用於散播開源木馬程式 SparkRAT 以及 TellYouThePass 、HelloKitty 等勒索軟體的攻擊行動上。

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.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

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

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

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：其預設就啟用的系統鎖定功能，保護底層作業系統免受此漏洞遭開採利用。政策集的網路規則可設定只讓特定版本的 ActiveMQ

應用程式信任限定的用戶端。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。

2023/11/15

新一波的GuLoader垃圾郵件攻擊行動

GuLoader 是一種先進的基於 shellcode 的惡意程式載入器，它使用各種反分析技術來試圖躲避檢測並增加逆向工程的難度，目的是傳播一大堆惡意軟體，包括但不限於勒索軟體、竊密程式、銀行金融木馬、遠端存取木馬 (RAT) 和代理伺服器。

誠如我們在先前的防護公報中提及的，GuLoader 今年確實很活躍。最近，我們又再次觀察到相關的垃圾郵件活動，導致我們的遙測系統在 11 月 8 日報告一個顯著的峰值，其兩側的峰值較小。在這一特定的行動中，觀察到的有效酬載之一被命名為『TAROM - Romanian Air Transport P.O. 4500106584 11082023.vbs』。

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：

- Scr.Guloader!gen1
- Scr.Malcode!gen
- Trojan Horse
- Web.Reputation.1

2023/11/14

SysAid公司所開發的IT服務管理軟體零時差漏洞在真實網路情境已被開採利用

據報導，有人濫用 SysAid 公司所開發的 IT 服務管理軟體中的零時差漏洞發起一場全新的攻擊行動。Lace Tempest 駭客組織與這些有目標式攻擊有關。該漏洞已被收納並編號為 CVE-2023-47246 漏洞，屬於路徑穿越 (Path Traversal) 類型的漏洞，能夠在內部安裝的系統中執行程式碼。開採利用該漏洞後，威脅者利用遭入侵的 SysAid 軟體發佈命令，以利後續 Gracewire 惡意軟體的惡意酬載順利佈署。

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
- WS.Malware.1

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。

2023/11/14

攻擊者偽造知名網站WindowsReport.com來傳播惡意軟體

WindowsReport.com 是一個線上 Windows 出版平臺，主要提供與 PC 相關的新聞、秘笈和建議。該網站分享科技業相關的最新消息，使用者還可以下載實用軟體。

谷歌廣告被濫用來誘使受害者瀏覽一個與 WindowsReport 網站完全相同但卻是偽造的網站，該網站上有一個被植入木馬的『CPU-Z』的熱門免費工具軟體的加料版本。CPU-Z 安裝檔內藏一個名為『FakeBat』的 PowerShell 載入程式，它隨後會進一步連結 RedLine Stealer--一個能夠收集敏感個人資訊和加密貨幣錢包資料的惡意軟體。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.NPE.C
- Trojan.RedLineStealer
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- 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。

2023/11/14

幣安(Binance)在日本開疆闢土也助長簡訊網路釣魚詐騙

全球最大加密貨幣交易平臺幣安 (Binance)，提供購買、出售和交易多種數位貨幣的平臺。該公司的服務遍及全球許多國家，但由於監管方面的考量因素，某些服務和功能的提供可能因不同國家而有所差異。

2023 年 8 月，Binance 在日本上線，為日本居民提供現貨交易和 Earn 產品。已在全球 Binance 平臺註冊的日本用戶被要求將其帳戶轉移日本 Binance 平臺，如果他們想在日本生活期間繼續使用其服務的話，務必在 11 月底前完成轉移到日本專屬平台，未完成轉移的全球帳戶將在 2023 年 12 月之後才能提供提款服務。

網路犯罪分子很快就利用 Binance 向日本擴點和帳號轉移過程的好機會。賽門鐵克發現一個針對日本手機用戶的惡意簡訊釣魚行動，企圖誘使他們瀏覽假冒 Binance 網站來進行帳號轉移。

觀察到惡意簡訊內容 (簡訊內容的日文明顯不符合母語水準)：

- 日本の住民はサイト移転を行う必要があり、そうしないと 11 月 30 日以降使用できない binanc-jp[.]com
- 日本居民必須帳號轉移，否則 11 月 30 日後將無法使用 binanc-jp[.]com

這次攻擊行動中假冒的網站域名是採用眾所周知的域名誤植或打字錯誤 (typosquatting) 之伎倆，網路犯罪分子透過常見的拼寫錯誤或註冊與合法域名相似的域名。賽門鐵克從這個域名註冊商發現其他也正在對 Binance 發動域名誤植或打字錯誤 (typosquatting) 伎倆的域名。有些域名中含有國家代碼，這表明它們是用來針對這些國家的用戶 (例如：binance-my[.]com、binance-tw[.]com、binance-au[.]com、binance-ch[.]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的假冒 Binance Japan 功能變數名稱以及已發現的其他功能變數名稱。

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。

2023/11/14

逃不出～NoEscape勒索軟體～的手掌心？

NoEscape 勒索軟體是一種按需付費的『勒索軟體即服務』(Ransomware-as-a-Service)，最初出現在 2023 年上半年。NoEscape 活動軌跡遍及全球，主要集中在北美和歐洲，受害者也遍佈各行各業，包括零售、政府和製造業等。利用 NoEscape 所發動攻擊表現出典型的勒索軟體行為，例如：檔案加密、程序 (process) 終止、資料滲漏以及要脅不就範就要將資料公諸於世的心理壓力來進行敲詐勒索。

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.SuspLaunch!g189
- SONAR.SuspLaunch!g193
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.NoEscape

- Trojan Horse
- 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

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：

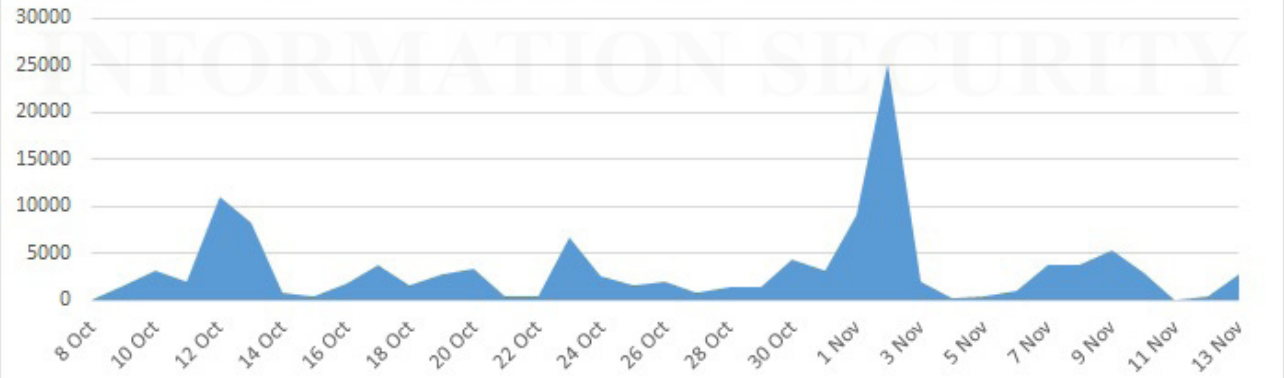
- Attack: Ransom.Gen Activity 46

2023/11/14

防護亮點：濫用Cloudflare物件儲存服務R2的網路釣魚威脅

長期以來，發動網路釣魚的惡棍，無論是個人還是團體，都在持續嘗試各種可能的方法實施網路釣魚行動。星際檔案系統 (IPFS) 和 Cloudflare 物件儲存服務 R2 等內容存儲網路 (CDN) 是被濫用最多的網路釣魚網頁主機。我們最近發佈一份有關單個活動的防護公告，但在過去 30 天內，我們在全球觀察到更多的實例，主要是試圖竊取企業使用者的電子郵件憑據／帳密。

賽門鐵克所攔截到的上架在 Cloudflare R2 的網路釣魚郵件時序統計圖



我們可以認為，CloudFlare R2 日益被網路釣魚威脅者濫用的主要原因是其免費、易用性、良好聲譽和遍及全球的影響力。所有這些因素結合在一起，為他們提供一個強大的平臺來操弄社交工程伎倆，以達到一定程度的規避、韌性和匿名性來進行非法的勾當。

如前所述，所觀察到的大多數網路釣魚行動都以誘騙電子郵件憑證／帳密為目標，透過與帳戶相關問題 (密碼問題、終止、未讀郵件等)、帳單、警方警告和其他社交工程伎倆等相關的電子郵件來引誘使用者。這些電子郵件包含一個引導至網路釣魚頁面的惡意網頁鏈結，網頁鏈接的尾部是使用者的電子郵寄地址。因此，如果用戶被成功誘騙點擊 URL，假冒的登錄頁面就會在登錄欄位中顯示使用者的電子郵寄地址，使登錄過程看起來更加可信。

以下是一些惡意網頁鏈結的最新實例，這些惡意網頁鏈結會引導至上線在 CloudFlare R2 代

管的釣魚網頁：

- hxxp[:]//pub-733372c603ef451496fbd54cfcb41576[.]r2[.]dev/93306DHI[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-be898b69352444c28d68f43e8725f2d1[.]r2[.]dev/godisalive[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-f4d1302dafbf4beeaf3e5e773e67edc4[.]r2[.]dev/allupdate[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-ad5b0662c2a54e5884a831384bd99913[.]r2[.]dev/pagefem345[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-ad60cadbed8e448499578f472c0a3183[.]r2[.]dev/af[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-a8906372f15e4c3c9eeedea91a48a923[.]r2[.]dev/index[.]html#[使用者的電子郵寄地址]

賽門鐵克的多重防護技術已經於第一時間提供最有效的保護(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。

2023/11/13

荷蘭稅務與海關管理局(Belastingdienst)被冒名發動金融詐騙的惡意簡訊攻擊行動

賽門鐵克最近發現針對荷蘭行動電話用戶的惡意簡訊釣魚行動。該惡意行動的幕後黑手冒充荷蘭稅務與海關管理局 (Belastingdienst)，目的是詐騙荷蘭居民。簡訊通知當事人有一筆未償還債務需要支付。如果有人被成功誘騙，他們就會登入一個假冒的 Belastingdienst 網站，網站上引導透過 iDEAL(一種荷蘭流行的線上支付方式) 支付的金額。

觀察到的惡意簡訊內容：

- Uw openstaande schuld van: €451,65 is tot op heden niet betaald. Betaal dit nog voor 11-11-2023 via: hxxps[:]//aanmaning-herinnering[.]net/belastingdienst/BD7893409/

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的假冒荷蘭稅務與海關管理局 (Belastingdienst) 網站。

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。

2023/11/13

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 1.857 萬個受保護端點上阻止了總計 710 萬次攻擊。

- 使用網頁信譽情資，在 1.659 萬個端點上阻止 610 萬次攻擊。
- 攔截 36.2K 個端點上 731.5K 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 15.4K 個端點上攔截 213.2K 次瀏覽器通知詐騙攻擊。
- 在 805 個端點上攔截 66.2K 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 1.6K 個端點上阻止 2.7K 次技術支援詐騙攻擊。
- 在 251 個端點上阻止 655 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。

2023/11/13

繼Linux平台之後，BiBi破壞性資料清除程式(Wiper)推出Windows的版本

繼在 Linux 平台發現全新名為 BiBi 的破壞性資料清除程式 (Wiper) 後不久，一個研究小組又發現其 Windows 平台上的版本。到目前為止，感染媒介尚不清楚，但與 Linux 的版本類似，『破壞性資料清除程式 (Wiper)』會用亂七八糟的內容覆蓋寫入目標檔案。至於在 Windows 中的具體行為，該資料清除程式確實會將副檔名更改為 BiBi[編號]，它不會更改 exe、DLL 和類似檔，以免在觸碰系統檔後無法運行，並刪除任何可能的磁碟陰影複製 (Volume Shadow Copy)。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/11/10

基於Python的BlazeStealer竊密惡意軟體

BlazeStealer 是一種竊密惡意軟體，它借助偽裝成合法混淆工具的惡意 Python 套裝軟體，在最近觀察到的網路攻擊行動中傳播。第一個使用 Python 套裝軟體名為『pyobftoexe』，早在 1 月份已在真實網路情境觀察到，而最近一個名為『pyobfgood 』套裝軟體則在上個月發現。一旦感染機器，BlazeStealer 惡意軟體就會運行一個 Discord 機器人，其功能包括收集主機資訊、從系統瀏覽器中竊取憑證、鍵盤側錄、螢幕截圖、啟動鏡頭錄影、使用者檔案收集、遠端命令執行等。

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：

- Downloader
- Infostealer
- 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。

2023/11/10

全新手機／行動間諜軟體：Kamran

Kamran 是一種全新發現的安卓平台上的間諜軟體。它在最近的利用水坑式伎倆的攻擊行動中被傳播，據報導，它專門針對巴基斯坦吉爾吉特--巴爾蒂斯坦地區講烏爾都語的用戶。Kamran 功能包括收集手機上的連絡人、通話記錄、簡訊內容和裝置上存儲的檔案等。收集到的資訊會被轉發到保管在 Firebase 上、由攻擊者所操控的 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：

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

2023/11/10

BlueNoroff駭客組織部署MacOS平台上的ObjCShellz惡意軟體

在真實網路情境發現一個歸屬於 BlueNoroff 進階持續威脅 (APT) 駭客組織全新 macOS 平台上的惡意軟體。這款名為 ObjCShellz 惡意軟體與同一駭客組織在早期行動中部署名為 RustBucket 的惡意軟體有一些共同特徵。從功能上看，該惡意軟體充當遠端 shell，執行從攻擊者那裡接收到的命令。

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：

郵檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Nukesped
- Trojan Horse
- 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。