保安資訊--本周(台灣時間2023/10/27)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 64 萬 9,000 台受保護端點上總共阻止了 8,020 萬次攻擊。這些攻擊中有 86.4% 在感染階段前就被有效阻止：**(2023/10/23)**

- 在**11萬2,500**台端點上，阻止了**3,130**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**19萬4,200**台端點上，阻止了**1,580**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬4,300**台**Windows**伺服主機上，阻止了**1,510**萬次攻擊。
- 在**6萬6,600**台端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,500**台端點上，阻止了**130**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬2,200**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**24萬8,500**台端點上，阻止了**490**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬5,300**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**11萬5,600**台端點上，阻止了**890**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**870**台端點上，阻止了**6萬100**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。

2023/10/26

RisePro惡意竊密程式仍活躍在駭客圈

RisePro 惡意竊密程式於 2022 年底首次被觀察到，至今一直都有其活動跡象，並且仍然主要透過密碼破解／產生器程式夾帶的 PrivateLoader 載入程式來進行傳播。PrivateLoader 的惡意軟體服務目前是採按安裝次數收費，其具有將惡意酬載下載到受感染系統上的能力。最近幾週，我們觀察到命令和控制伺服器 (C&C) 活動增加。竊取的目標是 cookie、密碼、信用卡和使用瀏覽器擴充的加密錢包等。雖然消費者和小型企業似乎是主要目標，但大中型企業仍然面臨可能使用其他感染媒介的駭客組織和駭客個體戶的風險。

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
- Trojan.Gen.MBT
- 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!100
- Heur.AdvML.B!200

2023/10/26

又是新來的～CATAKA勒索軟體

CATAKA 是一種正在真實網路情境流竄的全新勒索軟體。該惡意軟體會加密使用者的檔案並冠上隨機的副檔名。除勒索贖金支付說明檔是以 readme.txt 檔案存在電腦外，同時也會將桌面背景替換為包含勒索贖金支付說明的圖片。威脅者索取相當於 1500 美元的比特幣加密貨幣作為解鎖檔案費用。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g22
- SONAR.SuspLaunch!g266

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/10/26

小心銀行來的郵件：網路釣魚電子郵件冒充布拉德斯科銀行的忠誠顧客紅利點數兌換系統

巴西布拉德斯科銀行 (Banco Bradesco) 是拉丁美洲最大的私人金融機構之一。它成立於1943年 3月 10 日，總部位於巴西奧薩斯科。最近，賽門鐵克觀察到持續存在的網路釣魚行為，並冒充布拉德斯科銀行的忠誠顧客紅利點數兌換系統竊取憑證／帳密。這些網路釣魚電子郵件通常偽裝成通知訊息，並嘗試引誘使用者開啟並點擊網路釣魚的網頁。

- 電子郵件主旨：Bradesco 訊息：Mais de 359.180 mil pontos para resgate
- 電子郵件主旨：布拉德斯科銀行紅利點數生效通知：超過 293,000 點可兌換

點擊電子郵件內文中顯示的網路釣魚網址鏈接 (URL) 後，受害者就會看到收集憑證/帳密的網頁。

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。

2023/10/25

樹大招風～駭客冒名土耳其大型銀行，發動散布Snake鍵盤側錄程式的網路攻擊行動

賽門鐵克最近觀察到一場冒用土耳其最大、最著名的銀行之一的名義來發送惡意垃圾郵件的網路攻擊行動，主要是散布 Snake 鍵盤側錄惡意程式。犯罪分子試圖透過「帳戶交易」社交工程來引誘受害者。惡意電子郵件（主旨：Hesap hareketleriniz）夾帶 GZ 壓縮附件檔（Hesap hareketleriniz pdf.gz），內含 Snake 鍵盤側錄惡意程式的二進位檔案。在土耳其營運各行各業的本地和跨國企業是此次攻擊行動主要目標。

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：

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.SuspBeh!gen752
- SONAR.SuspLaunch!g310

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/25

KeyLock勒索軟體

賽門鐵克發現一種被稱為 KeyLock 的勒索軟體。如果該惡意軟體成功執行，它將嘗試加密檔案並冠上 .keylock 副檔名。它還會投放勒索贖金說明檔『README-id-（受害者的 ID 號碼）.txt』，建議受害者在 72 小時內透過電子郵件或 Telegram 與他們聯繫。根據勒索贖金說明的內容，犯罪分子似乎採取雙重勒索策略，要脅被害者，除非支付贖金，否則他們將公開敏感資訊。

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.SuspLaunch!g22
- SONAR.SuspLaunch!g266

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/25

Easy(*輕鬆)竊密惡意程式

Easy 竊密惡意程式在 2023 年中首次曝光，此後一直有零星活動。它在俄羅斯地下論壇和 Telegram 上做廣告。到處都有觀察到與惡意活動和似乎正在測試的內容有關的命令和控制面板。在最近的一個案例中，賽門鐵克觀察到了一個全新的 C&C，很可能與測試有關。該竊密惡意程式，雖然功能齊全，但相較於其他更惡名昭彰的竊密惡意程式並無過人之處。它具有通用功能，例如：從網頁瀏覽器和加密錢包、檔案中竊取敏感資料以及載入其他惡意軟體。

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：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/25

Mad Cat(*瘋貓)勒索軟體

據觀察，一種源於 Chaos 的「Mad Cat」勒索軟體會對單一台電腦進行加密，從而影響消費者和企業。觀察到的樣本將加密檔案，然後冠上隨機 4 個字元的副檔名。該勒索軟體幕後的攻擊者索價要 0.02 比特幣 (BTC)，在撰寫本文時相當於 682.33 美元。

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.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

2023/10/25

發動新的網路攻擊行動～BbyStealer 竊密惡意軟體捲土重來

在真實網路情境已經偵測到散布 BbyStealer 竊密惡意軟體的新行動。該幕後的攻擊者一直在利用多個網路釣魚網站宣傳免費下載各種虛擬私人網路 (VPN) 應用程式的 Windows 平台上安裝程式。從其入口網站下載的安裝程式包會衍生 BbyStealer 竊密程式的感染。該惡意軟體具有從目標端點、憑證、瀏覽器中儲存的資料、cookie 和加密錢包擴充功能等擷取機密資訊的功能。收集到的資料隨後被轉發到攻擊者所操控的 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

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。

2023/10/25

駭客組織YoroTrooper鎖定獨立國家國協(CIS)政府機構

最近一份報告提供所觀察到駭客組織 YoroTrooper 涉及活動的相關細節。據報導，該駭客組織的成員來自哈薩克，似乎正在轉向使用更多客製化惡意軟體來針對獨立國家國協 (CIS) 的政府機構。已證實這些地方政府機構以及國有網站已遭到入侵。該駭客組織利用多種駭客工具，以利開啟反向 shell 並從受害者那裡竊取資訊。

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：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Infostealer
- JS.Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mallnk
- VBS.Downloader.Trojan
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- 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: Python Meterpreter Reverse TCP Activity

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。

2023/10/25

SmokeLoader惡意程式越來越常出現在對烏克蘭機構的攻擊行動中

根據烏克蘭國家網路安全協調中心 (NCSCC) 的報告，針對烏克蘭組織和政府機構的網路攻擊活動增加。威脅者至少從今年 5 月起就一直在攻擊行動中濫用 SmokeLoader 惡意軟體。這種模

組化惡意軟體主要透過網路釣魚行動進行傳播，一旦被感染，就會擷取憑證／帳密、機密資訊、收集電子郵件和檔案、鍵擊側錄，還會下載和執行其他多種有效籌載。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.ProHijack!g45
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.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。

2023/10/25

.cfd頂級域名成為傳播網路釣魚電子郵件的新寵

.cfd 是時裝產業，獨立設計師，服裝品牌和服裝製造商的頂級域名，為服裝和時裝設計帶來新的繁榮未來。在最近網路釣魚活動中，.cfd 的頂級域名被各種威脅者嚴重濫用。CFD 代表『服裝、時裝和設計』，可供時裝設計師、服裝品牌、零售商和電子商務商店等使用。賽門鐵克觀察到，在「寄件者」電子郵件地址欄位中使用 .cfd 頂級域名的網路釣魚浪潮持續存在。這些網路釣魚郵件經常偽裝成通知性質的郵件，其主旨包含常見的關鍵字，例如：

- 帳號續訂
- 帳號暫停
- 帳號關閉
- 帳號認證
- 休假規定

有趣的是，日文網路釣魚也具有類似的特徵，並且被觀察到偽裝成受歡迎的服務。由於主旨中的關鍵字會製造真實的急迫感，用戶會被引誘打開此類電子郵件並點擊網路釣魚網頁鏈接

。這些網頁鏈接將受害者引導至憑證收集網頁。與這個特定頂級域名相關的網域大多是可疑，並且註冊時間至少為 1 或 2 年。

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。

2023/10/25

GoPIX惡意軟體，專門鎖定巴西國營PIX Pay的惡意軟體

GoPIX 是另一種針對 PIX Pay 的惡意軟體，PIX Pay 是由巴西金融管理局、巴西中央銀行所營運的即時支付系統。該惡意軟體於去年年底首次出現在威脅領域，主要透過惡意廣告傳播。GoPIX 具有剪貼簿竊取功能，專門針對 PIX Pay 的交易。它還具有利用攻擊者控制的位址，替換加密貨幣錢包位址的加密貨幣剪貼布內容置換器 (clipper) 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
- Trojan.Gen.MBT
- WS.Malware.1

2023/10/24

Formbook網路攻擊行動：假冒德國熱塑性塑膠公司和法國汽車供應商發送惡意電子郵件

有攻擊者最近發起一場惡意電子郵件攻擊行動，透過欺假冒一家德國熱塑性塑膠公司和一家法國全球汽車供應商來針對歐洲公司。這些電子郵件附加惡意文件檔案，這些檔案可以開採利用眾所周知的 CVE-2017-11882 漏洞，然後植入 Formbook 惡意程式。CVE-2017-11882 是指 2017 年發現 Microsoft Office 中的一個漏洞，目前仍被廣泛開採濫用。具體來說，它是 Microsoft Office 可於文件中插入及編輯程式中的遠端執行程式碼漏洞 (RCE)，如果使用者開啟被加料的 Microsoft Office 文件檔案，攻擊者就可以在受害者的系統上執行任意程式碼。

保安網路知識補充：CVE-2017-11882 是個記憶體毀損漏洞，主要是因 Office 未能妥善處理記憶體中的物件，若使用者以管理員權限登入，那麼駭客就能接管整個系統，繼之安裝程式、變更或刪除檔案，也能建立具備完整使用者權限的新帳號。

已發現的案例郵件主旨包括：

- （冒充公司名稱）採購訂單_231023
- （冒用公司名稱）大量採購訂單
- Factura_ 03351

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：

- Exp.CVE-2017-11882!g6

2023/10/24

BlackDream勒索軟體

BlackDream (源於 Babuk 的變種) 是另一個正在真實網路情境流竄的勒索軟體營運商。此時，他們似乎並沒有採取可怕的雙重勒索戰術。最近活動顯示，他們一直將勒索軟體二進位檔案偽裝成虛假的「Windows 安全」安裝程式。成功執行後，將加密檔案並冠上 .BlackDream 的副檔名。投放的勒索 (贖金支付) 說明建議受害者透過 Telegram 或電子郵件聯繫該歹徒，以了解解密檔案需要花費多少費用。

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：

基於行為偵測技術(SONAR)的防護：

- Ransom.Babuk

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

2023/10/24

GuLoader網路攻擊行動：冒充韓國HomeTax

賽門鐵克在韓國偵測到 GuLoader 惡意載入程式網路攻擊行動，其中攻擊者利用國家稅務局 (NTS) 作為社交工程伎倆。HomeTax 被冒充，惡意電子郵件（主題：국세청 홈택스 서비스의 전자세금계산서입니다）試圖使用來自 NTS HomeTax 5 的假稅務發票來欺騙用戶。附件是一個 Zip 壓縮檔案 (NTS_eTaxInvoice.zip)，其中包含惡意 VBS (NTS_eTaxInvoice.vbs)，即是 GuLoader 惡意載入程式。

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

2023/10/24

東歐正在發生的散布ModiLoader惡意載入程式網路攻擊行動

ModiLoader 惡意載入程式仍然是網路安全領域活躍的威脅，主要透過惡意電子郵件在全球傳播。在最近的一個案例中，賽門鐵克發現一項針對匈牙利、克羅埃西亞、俄羅斯、馬其頓、斯洛維尼亞、波士尼亞和黑塞哥維那的本地和國際公司的網路攻擊行動。發動攻擊的犯罪者冒充塞拉耶佛 (Sarajevo) 的電信公司，並採用經典的「訂單」社交工程伎倆。如果成功引誘使用者開啟附加的檔案 (U prilogu je potvrda narudzbe.zip) 並隨後執行 (U prilogu je potvrda narudzbe.exe) 中的二進位檔案，它將觸發 ModiLoader 的執行。

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：

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：

- AGR.Terminate!g5
- SONAR.SuspBeh!gen24
- SONAR.SuspBeh!gen526
- SONAR.SuspBeh!gen530

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

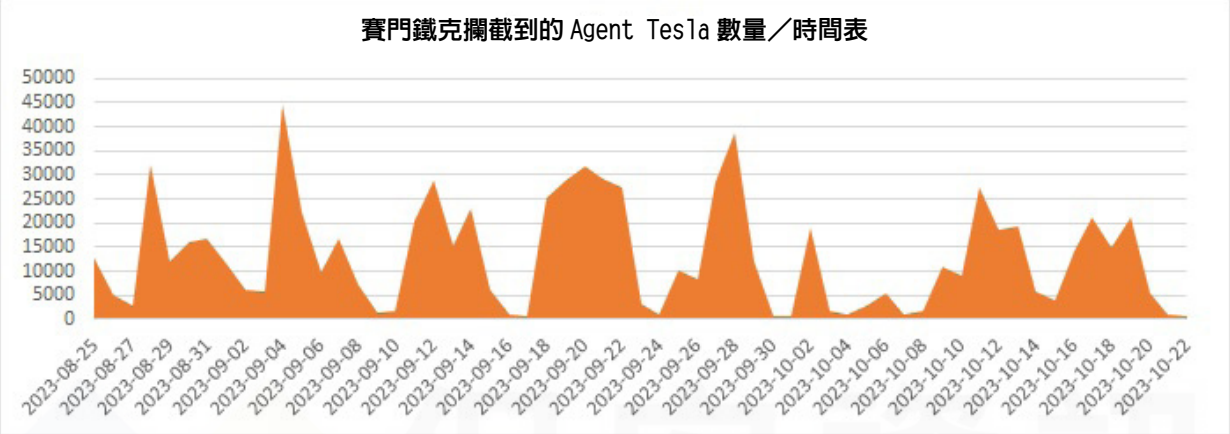
基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/24

防護亮點：Agent Tesla惡意程式轉為濫用CHM和PDF檔案進行傳播

自 2014 年以來，Agent Tesla 竊密程式一直在網路犯罪圈具有很高的影響力，並且沒有任何式微的跡象。這種具有竊密程式和遠端存取功能的惡意程式廣受許多駭客組織和個人青睞，常被用於電子犯罪和發動目標攻擊。Agent Telsa 通常透過 .DOC、.XLS 和 .PPT 檔案進行傳播，但最近 CHM 和 PDF 檔案似乎也已經被納入，在多起攻擊活動中有發現這個跡象。



CHM 檔案來自下載的 PowerShell 腳本，該腳本會釋放一個載入程式 DLL 檔案，該檔案又將 Agent Tesla 載入到名為「RegAsm.exe」的合法 Windows 程序。PDF 檔案使用兩種不同的方法來傳播 Agent Tesla 惡意軟體。首先，開啟 PDF 檔案將觸發 PowerShell 命令來載入 Agent Tesla。其次，將顯示一個虛假的彈出通知，顯示「錯誤：無法載入 PDF 檔案」。如果使用者按一下「重新載入」按鈕，將下載 PPAM 檔案（PowerPoint 外掛程式），則是負責執行隨後下載 Agent Tesla 的 PowerShell 命令。

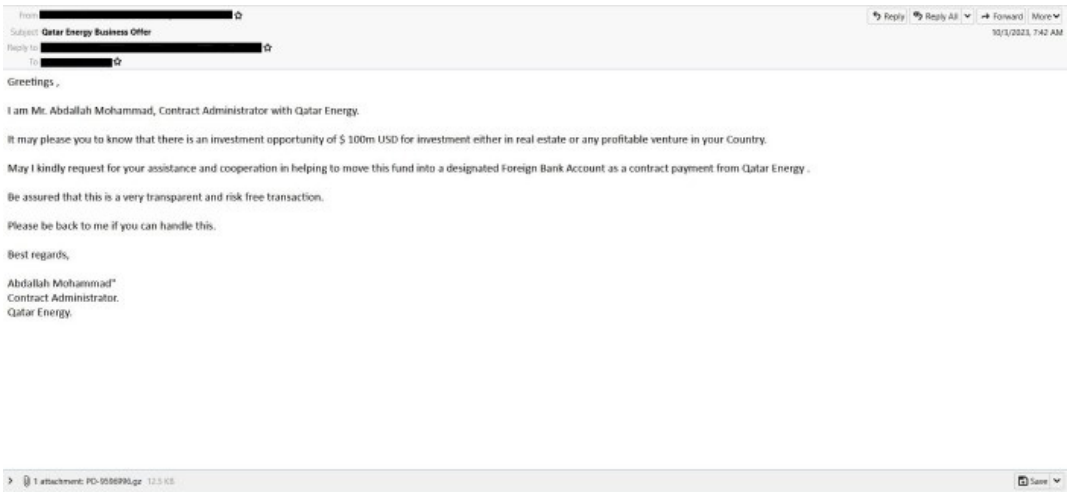
觀察到的郵件主旨樣本：

- 卡達能源業務報價
- 緊急訂購單
- 緊急採購訂單

Gzip 壓縮附件檔名：

- PO-9596996.gz

電子郵件範例：


Subject: Qatar Energy Business Offer

Greetings ,

I am Mr. Abdallah Mohammad, Contract Administrator with Qatar Energy.

It may please you to know that there is an investment opportunity of $ 100m USD for investment either in real estate or any profitable venture in your Country.

May I kindly request for your assistance and cooperation in helping to move this fund into a designated Foreign Bank Account as a contract payment from Qatar Energy .

Be assured that this is a very transparent and risk free transaction.

Please be back to me if you can handle this.

Best regards,

Abdallah Mohammad"
Contract Administrator.
Qatar Energy.

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：

- Downloader
- Scr.Malcode!gen
- Scr.Malcode!gen45
- Trojan.Gen.NPE.C
- Web.Reputation.1
- WS.Malware.1
- W97M.Downloader

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。

2023/10/24

在真實網路情境偵測到新版STRRAT惡意軟體散佈行動

在真實網路情境偵測到新版 STRRAT 惡意軟體散佈行動。該惡意軟體透過偽裝成付款發票的惡意垃圾郵件進行傳播，主題為「RE：待處理的發票付款//INV-2200541/2023/09/21」。這些電子郵件附加雙副檔名 .doc.jar 檔案（『INV-220054120230921.doc.jar』），一旦開啟，就會導致惡意 JavaScript 檔案的執行，進而啟動遠端存取木馬 (RAT) 惡意酬載的感染。與舊版相比，新版 STRRAT 的功能仍然非常雷同，具有憑證竊取、鍵盤側錄、命令執行、控制受感染系統以及下載／安裝其他任意有效籌載等功能。

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：

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：

- ISB.Dropper!gen12
- Scr.Malcode!gen
- Scr.Malcode!gen69
- Trojan.Dropper
- 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。

2023/10/24

Lumar(*盧瑪)竊密程式

Lumar 是一種新發現的竊密惡意程式，在地下論壇上以惡意軟體即服務 (MaaS) 的套裝形式進行銷售廣告。該惡意軟體具有擷取瀏覽器 cookie 和憑證、收集各種使用者檔案、竊取加密貨幣錢包或攔截 Telegram 對話等功能。擷取的資料被轉發到惡意軟體作者所操控的 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.2

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：

- System Infected: Trojan.Backdoor Activity 634

2023/10/24

Pure Clipper(剪貼布內容置換)惡意軟體針對義大利語系的使用者

已觀察到向義大利語系的使用者傳播 Pure Clipper (剪貼布內容置換) 惡意軟體的新行動。該惡意軟體是由名為「Alibaba2044」的威脅組織發起，該組織在利用 PureLogs 惡意軟體的較早攻擊中也針對義大利。在這次最新的行動中，Pure Clipper 透過冒充 Tor 專案 (Tor project) 官方網頁的網路釣魚網站進行傳播。該惡意軟體具有將用戶複製的加密貨幣錢包位址與攻擊者位址交換的功能。

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：

- AGR.Terminate!g2
- SONAR.Powershell!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Limitail
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Scr.Malcode!gen
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- 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。

2023/10/23

日本新一波網路釣魚鎖定個人編號卡(MY NUMBER CARD)持有人

個人編號卡 (My Number Card) 也稱為個人編號卡 (the Individual Number Card)，是由日本市町村政府所發行用於識別身分的證件。它是日本各地公民的身份證件。最近，賽門鐵克觀察到新一波網路釣魚活動利用拼字錯誤的網路釣魚網頁來欺騙 MyNumber Card 服務。電子郵件內容提供一些有關 Minor Points (MyNa Points) 系統的資訊，並誘使持有人點擊網路釣魚網頁以查看當前積分。

- 郵件主旨：【マイナポイント第 2 弾】20,000 円分のポイントプurezento！
- 郵件主旨：【小積分 2nd】價值 20,000 日圓的積分送！
- 網路釣魚的網頁結構：hxxps://mynumber.card [.] jp。[redacted_domain] .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：

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。

2023/10/20

夾帶著仿冒品促銷得新一波雪鞋垃圾／攻擊郵件

網路壞蛋想出一種新伎倆，透過設計和執行新一波的雪鞋行動來淹沒用戶並向用戶發送垃圾郵件。最近，這些雪鞋跑步活動因 sa.com 的濫用而受到關注。Sa.com 是沙烏地阿拉伯王國 .COM 的子網域。1998 年前後網際網路超瘋狂的年代所註冊的隨機網域，在這次特定活動中被濫用。一般來說，雪鞋跑步出現在少量的電子郵件中。相反，在本例中，賽門鐵克觀察到單次爆發的電子郵件數量超過一百萬封，涵蓋各種假冒產品促銷活動。這些偵測到的電子郵件展示網路壞蛋引誘收件人接受此類「好得令人難以置信」的優惠伎倆。電子郵件主旨誘使收件者打開它們並觸發點擊的後續惡意連鎖反應。

以下列出一些觀察到的電子郵件主旨：

- 使用此 WIFI 增強器提高您的網路速度！
- 隨時隨地即時追蹤您的車輛！
- 告別疼痛--立即緩解
- 只需 7 天即可獲得更燦爛的笑容！
- 使用這款智慧手錶追蹤您的健康狀況！
- 您的虛擬禮賓就在這裡！
- 4K 無人機--以低廉價格獲得專業品質的影片！
- 簡單的 7 秒「真菌消失」Ritual 可將指甲清除速度加快 3 倍
- 這款太陽能手電筒可以拯救生命！
- 該設備可即時翻譯 36 種語言！
- 3 天控制血糖--這是可能的！
- 頭髮再生的自然方法！
- 手提式吸塵器，隨身攜帶！
- 與腰痛說再見！
- 您想找到解決方案來反擊潛伏的小偷嗎？

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。

2023/10/19

義大利公共災防警報系統被濫用於部署SpyNote Android惡意軟體

「IT-alert」是一種基於簡訊的公共災防警報系統，這是一項義大利政府提供的服務，旨在向公眾發出有關即將發生或正在進行的自然災害的警告。一份報告顯示，攻擊者利用該服務發出有關可能發生火山爆發的虛假警告。用戶被敦促安裝一個 APP，以隨時了解這些活動的最新情況，但實際上卻無意中安裝能夠竊取銀行、加密貨幣和社交媒體憑證的 SpyNote 惡意軟體。其他功能包括攝影機錄製、GPS 和網路位置追蹤以及電話錄音。

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：

- WS.Malware.1

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

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。