保安資訊--本周(台灣時間2023/02/17)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 83 萬 700 台受保護端點上總共阻止了 1 億 150 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/02/13)**

- 在**15萬6,900**台端點上，阻止了**4,210**萬次嘗試掃描**Web**服務器的漏洞。
- 在**29萬1,400**台端點上，阻止了**2,280**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬8,000**台**Windows**伺服主機上，阻止了**1,570**萬次攻擊。
- 在**8萬5,600**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬8,800**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬8,600**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**27萬9,500**台端點上，阻止了**570**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,700**台端點上，阻止了**220**萬次加密貨幣挖礦攻擊。
- 在**14萬6,700**台端點上，阻止了**1,170**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,900**台端點上，阻止了**14萬8,000**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。

2023/02/16

被命名為V3G4的全新Mirai殭屍網路變種，已經在真實網路環境釀成禍害

被命名為V3G4 全新 Mirai 殭屍網路變種，已經在真實網路環境釀成禍害。攻擊者利用幾個不同的漏洞來進行散佈。感染 V3G4 後，漏洞未修補的易受攻擊的設備將成為 Mirai 殭屍網路的一部分，允許攻擊者經由遠端操控。該惡意軟體將嘗試終止在受感染主機上運行的其他殭屍網路或不同分支的 Mirai 變種的相關程序。V3G4 殭屍網路可能會進一步用於發動分散式阻斷服務 (DDoS) 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan.Gen.NPE
- WS.Malware.1

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: Airspan AirSpot RCE CVE-2022-36267
- Web Attack: Atlassian OGNL Injection CVE-2022-26134
- Web Attack: Draytek Routers CVE-2020-8515
- Web Attack: Webmin Remote Code Execution CVE-2019-15107

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。

2023/02/16

採用Golang程式語言撰寫的全新勒索軟體～DarkBit勒索軟體

DarkBit 是一種採用 Golang 程式語言撰寫的全新勒索軟體，最近已經被證實在真實網路環境開始發動攻擊。該勒索軟體利用多執行緒加密機制，也包含檔案／資料夾排外清單，被其加密後檔案將被新增 .darkbit 的副檔名，同時留下贖金支付說明的檔案名稱為 "RECOVERY_DARKBIT.txt" 的文字檔。Darkbit 也會刪除受感染電腦上的刪除陰影複製 (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：

- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.SuspLaunch!gen4
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Darkbit
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A

2023/02/16

攻擊台灣：Frebniis惡意軟體，濫用微軟IIS的功能來建立後門

賽門鐵克發現一種全新的惡意軟體，它濫用 Microsoft 的網際網路資訊服務 (Internet Information Services--IIS) 的一項功能，在目標系統上部署後門。這種被稱為 Frebniis 的惡意軟體被一個目前未知的威脅者用來攻擊台灣的目標。Frebniis 使用的駭客技術包含注入惡意程式碼至與 IIS 功能相關的 DLL 檔案 (iisfreb.dll) 記憶體中，該 IIS 的模組功能用是用於對失敗的網頁請求進行故障排除和分析。這允許惡意軟體偷偷監視所有 HTTP 請求並識別攻擊者發送的特殊格式的 HTTP 請求，從而允許遠端程式碼執行。

在我們的部落格文章中有更多資訊可供參考：Frebniis：全新惡意軟體濫用 Microsoft IIS 功能建立後門

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：

- Backdoor.Frebniis
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/02/15

MortalKombat--源於Xorist勒索軟體的新變種

MortalKombat 是一種源於 Xorist 的全新勒索軟體，最近與採用 Go 語言撰寫的 Laplas Clipper 惡意軟體一起在攻擊鏈中同時被散播。這些攻擊主要集中在美國、英國、土耳其和菲律賓的個人和組織。MortalKombat 會感染電腦上的各種類型檔案，包括應用程式、備份或資料庫等相關的檔案。由於沒有硬編碼排除項，勒索軟體還以加密各種系統相關的資料夾和檔案，進而導致整台電腦系統損壞。檔案被加密後，MortalKombat 將留下贖金支付說明並更改電腦上的桌面背景圖片。

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!gen93
- SONAR.SuspBeh!gen616
- SONAR.SuspTempRun
- SONAR.SuspTempRun2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.CryptoTorLocker
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

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。

2023/02/14

不會向被害人獅子大開口的Dodo勒索軟體，現在偽裝成Mercurial版本控制系統(VCS)

最近，另一種名為 Dodo 的勒索軟體正在流行。這個勒索軟體與其他勒索軟體的不同之處在於它只索價少少的 15 美元的比特幣 (Bitcoin) 或門羅幣 (XMR)。檔案被加密後，將被新增 .dodov2 的副檔名，並留下贖金支付說明文字檔 (dodov2_readit.txt)。Dodo 勒索軟體已在多個國家／地區偵測到，包括菲律賓、法國、英國、比利時、德國、瑞典、愛沙尼亞和土耳其，在這些國家／地區，它偽裝成稱為 Mercurial 的分散式版本控制系統 (VCS)，通常用於管理軟體開發專案。與其他 VCS 類似，Mercurial 支援多個使用者在共享程式碼儲存庫上進行共同協作，追踪程式碼異動並允許在必要時恢復以前的版本。

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.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/02/14

真實網路世界依舊傳出VoidCrypt勒索軟體的災情

VoidCrypt 是 2020 年問世的勒索軟體。雖然流行程度遠低於當前威脅領域的其他勒索軟體，但這種威脅的新變種仍然在不斷湧現。VoidCrypt 會停用系統服務和程序及從受感染端點刪除備份或卷冊陰影本的功能。被加密的檔案會依不同的攻擊行動而新增不同的副檔名。最近發現的災情所看到的副檔名樣本包括：.gogo、.MrWhite、.pay、.rykcrypt、.sunjn、.sunjun、.zendaya。

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!g18
- SONAR.SuspLaunch!g21

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.2
- 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
- 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 634

2023/02/14

向墨西哥用戶傳播銀行惡意軟體的Red Appaloosa攻擊行動

Red Appaloosa 是一起針對墨西哥用戶全新攻擊行動，攻擊鏈包含各種銀行惡意軟體。攻擊者利用偽裝成聯邦電力委員會 (CFE--Comisión Federal de Electricidad) 付款發票的網路釣魚電子郵件。傳送的電子郵件包含 .pdf 或 .html 的附件案，這些惡意附件檔會將受害者轉導向到攻擊者控制的網站並觸發下載包含惡意執行檔的 .zip 壓縮。一旦惡意軟體被安裝在受害者的電腦上，它就會伺機當用戶瀏覽其中一個被觀察到的銀行網站，以試圖竊取用戶的銀行資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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。

2023/02/13

Puspa勒索軟體(也稱為Chaos 500)

Puspa勒索軟體 (也稱為 Chaos 500) 在威脅領域並不陌生，幸運是它的蹤跡偶而才被觀察到，它也不像許多惡名昭彰的同類惡意軟體那樣具有破壞性。根據他們最近的活動，幕後的攻擊者只會感染單台電腦並要求支付 500 美元的比特幣贖金。

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：

- SONAR.SuspDrop!gen1

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

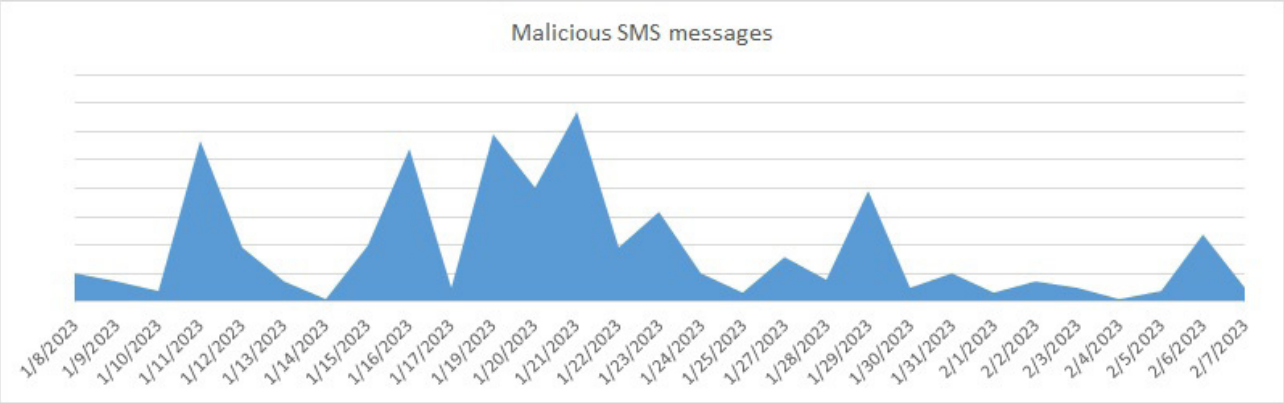
2023/02/13

SEP-NOVILE防護亮點：手機行動惡意軟體以日本為目標

～防護亮點～

在過去的幾個月裡，針對日本手機用戶實施 (包括消費者和企業) 攻擊行動不斷，其中含針對安卓 (Android) 的惡意軟體和針對 iPhone 的網路釣魚。

攻擊行動的方法保持不變，攻擊者繼續使用惡意簡訊作為感染手段，並利用免費的動態 DNS 代管服務 Duck DNS 使用子網域。被這些簡訊引誘的安卓用戶會被重導向假冒的 Softbank 和 KDDI 網站，並被提示下載假冒的手機安全 APP。iPhone 用戶被重導向到一個虛假的電子帳單系統網站。下面是過去一個月的攻擊模式，每個峰值代表一個新的活動。



在這兩種平台 (Android 和 iPhone)，重新轉導向到的最終的網域會有所不同，顯然該攻擊行動比想像的更複雜。以下是常見的接收到的詐騙簡訊內容的樣本：

* 【国税庁】重要なお知らせ、必ずお読みください
* 【国税庁 18:30】未払い税金お支払いのお願い。詳細はこちら【TT499】
* 【重要なお知らせ】未払い税金お支払いのお願い。ご確認ください【TQ177】
* 【重要なお知らせ HD474】SoftBank未払い料金お支払いのお願い
* 【12月6日利用停止予告】SoftBank未払い料金お支払いのお願い
* 【要確認】SoftBank重要なお知らせ、必ずお読みください
* 【ソフトバンク】お支払期限を過ぎた利用料金があります〔12月9日〕
* 【利用停止予告】KDDI未払い料金お支払いのお願い

本月初所發起的新一輪攻擊涉及 757 個使用 [10randomletters][.]duckdns[.]org 規則組合的 Duck DNS 子網域。偽裝成來自 Softbank 和 KDDI 的安全軟體的 Android 惡意軟體具有以下功能：

- 更改內定的簡訊APP
- 收集聯絡人、已安裝的APP、電話號碼和簡訊並將它們轉發送到遠端伺服器
- 未經用戶同意發送簡訊
- 如果偵測到特定組合規則的網域，則修改或刪除簡訊內容

從本質上來講，這種惡意軟體能夠操控受害者的手機使其成為魁儡／機器人，也能夠進一步傳播感染源和／或發動以受害者手機電話簿上的聯絡人及其他收集到的電話號碼來進行詐騙行動。此外，歹徒還可以存取透過簡訊發送的機敏雙重驗證／兩步驟驗證 (2FA) 驗證碼。這對消費者和企業都有極大的風險。

日本是擁有大量智慧型手機用戶的科技先進國家，當然也是網路駭客認為最有利益可圖的目標，歹徒企圖入侵行動手機裝置以竊取敏感資訊並進一步傳播他們的惡意軟體。這些類型的攻擊只會日益增加。

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
- 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。

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。

2023/02/13

近期TA866駭客集團相關的新活動

最近幾個月觀察到與 TA866 駭客集團相關的新活動。威脅者一直鎖定美國和德國的組織為目標，使用各種商品化和自定義惡意軟體變種。攻擊鏈通常與內嵌惡意巨集的 Microsoft Publisher (.pub) 檔案附件的網路釣魚電子郵件，或包含帶有惡意 Javascript 的 PDF 檔案之網頁連結有關聯。WasabiSeed、Screenshotter 以及 AHK Bot 和 Rhadamanthys 竊密程式都是 TA866 駭客集團組織最近散佈的惡意軟體系列。

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.Malmsi

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。

2023/02/13

Sunloginclient的CVE-2022-10270漏洞利用攻擊還是時有耳聞

Sunloginclient 是一個具有遠端遙控功能的軟體，多用於監控和操控 IT 環境中的各種設備。Sunloginclient 存在可導致執行任意程式碼的漏洞 (CVE-2022-10270)。原廠已發布修補程式來解決該漏洞。與此同時，賽門鐵克也持續觀察到攻擊者目前利用該漏洞散佈各種惡意軟體，也包括惡意挖礦程式。

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：

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: Sunlogin RCE Vulnerability

2023/02/12

針對日本GMO Aozora Net Bank網路銀行用戶的網路釣魚攻擊

最近，賽門鐵克發現一個針對 GMO Aozora Net Bank 網路銀行用戶的網路釣魚行動，目的是竊取他們的金融憑證。GMO Aozora Net Bank 是 GMO Financial Group 的子公司，是日本的一家網路銀行，主要向日本客戶提供一系列金融服務，包括儲蓄帳戶、貸款和信用卡。該行動背後的參與者已向企業和零售客戶發送主旨為“【GMOあおらネット銀行】から重要なお知らせ”的電子郵件。

如果用戶被這些虛假的“重要通知”引誘，電子郵件中的網址 會將他們重定導向到一個模仿 GMO Aozora Net Bank 網站的假冒登錄頁面。攻擊者還使用常見的的不慎輸入鍵盤周圍鍵的誤植伎倆來讓受害者更容易掉入他們的陷阱。這種手法有人稱為網址劫持或網域名稱詐騙，歹徒會去申請與合法網站相似但拼寫略有不同或域名略有變化的域名 (例如：使用不同的頂級域名)。

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：

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。

2023/02/12

Garsomware以及Rakkun：兩個源於Chaos的加密勒索軟體正在危害全世界

隨著世界各地的駭客集團和個體戶越來越多接納開放原始碼，我們現在對於源於 Chaos 的全新勒索軟體變種已經司空見慣。Garsomware 和 Rakkun 就是最近被發現的兩個全新變種，它們都索價 0.1473766 BTC--在撰寫本文時相當於 3207.53 美元。大多數 Chaos 的變種都不會大範圍爆發，並且以單機模式的電腦為目標，而不是在基礎設施中橫向移動並感染其他電腦。此外，少有採用雙重勒索戰術，也就是先竊取機敏資料，勒索不成會公開機敏資料作為威脅。

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.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/02/10

請留意老舊Intel驅動程式漏洞～Enigma竊密程式利用驅動程式漏洞，將目光聚焦在加密貨幣行業

Enigma 竊密程式是源於舊版 Stealerium 竊密程式。最近觀察到利用此惡意軟體的攻擊一直以加密貨幣行業為目標，使用包含假的面試或工作機會誘餌的網路釣魚電子郵件。攻擊者還一直在使用較舊 Intel 驅動程式漏洞 (CVE-2015-2291) 在受害者的端點上安裝惡意程式。Enigma 竊密程式收集儲存在各種瀏覽器和其他幾個應用程式(例如：Telegram、Signal 或 VPN 程序) 中的用戶資訊、密碼和資料。

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：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- 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：

- 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。

2023/02/09

小心線上訂票系統類的網路釣魚～日本鐵路集團已發生真實案例

Eki-net 是日本鐵路集團 (也稱為 JR 集團) 採用的鐵路車票預訂和管理系統。這項服務被廣泛使用，因為每天有數百萬人乘坐 JR 列車出遊。它提供一種便捷高效的方式來計劃鐵路旅行、進行預訂和線上購票。

網路罪犯者充分意識到 Eki-net 的流行，並在網路釣魚活動中利用它來獲取敏感的財務訊息。最近的報告顯示，針對 Eki-net 用戶的新網路釣魚活動，電子郵件 (主題：【重要】会員情報変更および退会に関するお知らせ）聲稱是關於帳戶更改和提款的。如果受害者上當受騙並點擊電子郵件中的網址 URL，他們將被重導向到假的 Eki-net 登錄頁面。

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。