保安資訊--本周(台灣時間2023/03/03)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 79 萬 7,800 台受保護端點上總共阻止了 9,520 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/02/27)**

- 在**14萬8,100**台端點上，阻止了**3,470**萬次嘗試掃描**Web**服務器的漏洞。
- 在**28萬2,200**台端點上，阻止了**2,240**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬5,900**台**Windows**伺服主機上，阻止了**1,720**萬次攻擊。
- 在**8萬3,600**台端點上，阻止了**280**萬次嘗試掃描伺服器漏洞。
- 在**2萬700**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬6,000**台端點上，阻止了**230**萬次嘗試利用的應用程式漏洞。
- 在**27萬900**台端點上，阻止了**560**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬4,000**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**14萬6,800**台端點上，阻止了**1,210**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,900**台端點上，阻止了**16萬4,100**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。

2023/03/02

Mallox勒索軟體積極鎖定企業及政府組織

Mallox 勒索軟體重出江湖並且高調鎖定企業及政府組織。Mallox (又名 Fargo) 是 TargetCompany 勒索軟體的最新變種，早在 2021 年就已首次出現在威脅領域中。傳播鏈包含一個惡意程式呼叫／下載的有效籌載，該攻擊鏈還被觀察到會下載其他幾個惡意軟體家族，例如：AgentTesla 或 Remcos。Mallox 會加密用戶的檔案並為其新增 .mallox 副檔名。如同已知情況，這種最新版的勒索軟體採用雙重勒索伎倆，從受感染的端點中搜集機密資訊，並脅迫被害者要公開發布被盜資料以迫就範。

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.Cryptlocker!g42
- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g230
- 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：

- Trojan.Gen.2
- Downloader
- MSIL.Downloader!gen7
- MSIL.Downloader!gen8
- Ransom.Mallox
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- SMG.Heur!gen
- Trojan.Gen.NPE
- 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
- 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。

2023/03/01

Parallax 遠端存取木馬鎖定加密貨幣公司

Parallax 遠端存取木馬(RAT)自 2019 年首次出現以來，一直透過惡意垃圾郵件和網路釣魚活動在傳播。一份新的報告顯示，加密貨幣公司最近成為威脅者的首要目標。

該惡意軟體能夠讀取登錄憑證、存取檔案、鍵盤記錄、遠端桌面控制並遠端控制受感染的電腦。Parallax 還具有稱為程序掏空（process-hollowing）的功能，是惡意程式使用的一種技術，目的在於規避檢測，先運行一個合法的程序，將惡意的程序掛到合法程序上，僅將合法程序用作惡意代碼的容器。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g45

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2023/03/01

假冒知名印尼大學學者的惡意電子郵件攻擊行動造成東南亞嚴重網路安全災情

假冒知名大學和學者是全球各地攻擊者在惡意軟體攻擊行動中使用的常見伎倆。賽門鐵克檢測到最近的一起事件，其中一名攻擊者冒充了一位與印尼大學有關的著名印尼經濟學家。該攻擊者利用這種詐騙來針對研究機構、金融、能源、工業以及在東南亞營運的企業集團。此惡意攻擊行動中使用的電子郵件主旨是“Quotation - Universitas Indonesia”，並包含內含一個偽裝成報價檔案(Quotation-Universitas Indonesia_pdf.exe)的 .xz 壓縮檔。以下是此威脅的一些功能：

- 按鍵記錄
- 截圖
- 從網路請求中獲取 HTTP(s) 表單
- 從剪貼簿竊取資料
- 竊取使用者和系統訊息
- 從瀏覽器、電子郵件、IM 和 ftp用戶端等竊取資料

- 關閉／重啟作業系統
- 下載並執行附加檔
- 遠端執行指令

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：

基於行為偵測技術(SONAR)的防護：

- AGR.terminate!g2
- SONAR.heur.dropper
- SONAR.prochijack!g21

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：

- Packed.NSISPacker!g14

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/03/01

RIG漏洞刺探利用工具套件的近期活動

儘管利用漏洞刺探利用工具套件 (Exploit Kit，簡稱 EK) 相關的活動在過去幾年普遍下降，但 RIG EK 仍然在真實網路環境不斷被利用。僅去年一年，由該漏洞刺探利用工具套件引起的攻擊量就呈上升趨勢，這表明該活動將在未來幾年繼續存在，並將繼續對企業構成重大威脅。RIG 仍然會刺探利用包含可追溯到 2012 年的相對較舊的 Internet Explorer 漏洞。最近使用的兩個漏洞是 Microsoft Internet Explorer CVE-2020-0674 和 CVE-2021-26411。之前，RIG EK 曾被用於散佈各種惡意軟體有效籌載，包括 Dridex、SmokeLoader、RaccoonStealer、RedlineStealer、Ursnif、PureCrypter、Royal 勒索軟體等。

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：

- SONAR.ProcHijack!g45
- SONAR.SuspScript!g20

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.528
- Packed.Generic.553

- Packed.Generic.616
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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: Internet Explorer RCE CVE-2021-26411
- Web Attack: Microsoft Internet Explorer CVE-2019-0752
- Web Attack: Microsoft Internet Explorer CVE-2020-0674
- Web Attack: Microsoft VBScript Engine RCE CVE-2018-8174
- Web Attack: RIG Exploit Kit Website
- Web Attack: RIG Exploit Kit Website 3
- Web Attack: RIG Exploit Kit Website 5
- Web Attack: Rig Exploit Kit Website 8
- Web Attack: Rig Exploit Kit Website 14
- Web Attack: Rig Exploit Kit Website 23

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。

2023/02/28

丹麥，也發現冒名Nordea銀行的網路釣魚行動正在進行中

大型金融機構不斷被冒名利用成為發動社交工程攻擊最有效的方法之一，有很高的比例可以引誘受害者登入釣魚網站或執行惡意附件檔案。賽門鐵克每天都在觀察世界各地冒名利用這些大型金融機構的惡意行動。最近，丹麥的消費者和企業也成為了另一場冒名利用 Nordea 的網路釣魚行動的鎖定目標。Nordea 是北歐地區最大的銀行之一，在丹麥、瑞典、芬蘭和挪威開展業務。具有以下主旨的電子郵件意圖將受害者重轉向到虛假的 Nordea 登錄網站：

- Din Nordea-ID er tilbagekaldt e-ticket ref [random ID]
- Opdater dine personlige oplysninger
- Du har et nyt online dokument
- Meddelelse online, handling påkrævet

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已於第一時間收錄於不安全分類列表中。

2023/02/28

SkullLocker 勒索軟體災情頻傳

SkullLocker 是一支較新的勒索軟體家族（源於 chaos 的變種）已經在威脅領域中嶄露頭角。入侵後被成功加密的檔案會新增 .skull 副檔名。在受害者電腦上發現的勒索贖金支付說明是用波蘭語寫成，要求受害者與他們聯繫並在 72 小時內交付贖金。不確定這些攻擊者是否採用可怕的雙重勒索伎倆，但在勒索贖金支付說明中並未提及任何出售或洩露受害者資料的後續手段。

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

2023/02/28

Telegram API(應用程式介面)日益受到網路釣魚歹徒利用

近幾個月來，全球網路釣魚歹徒濫用 Telegram API 呼叫（透過殭屍電腦）的事件激增。他們使用這種方法竊取資訊並將其傳輸到他們的 Telegram 頻道或私人聊天室。Telegram 頻道和群組的匿名性質給試圖找到罪魁禍首的執法機構帶來了挑戰，端到端加密確保透過該平台發送訊息的的安全性。此外，Telegram API 的易用性使其成為攻擊者收集被盜資料的有吸引力的選擇。在這類型的網路釣魚行動中，冒用 Microsoft Office 365 登錄頁面是最常見的網路釣魚行動之一。

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)。

2023/02/28

GoAnywhere檔案傳輸管理模組遠端程式碼執行漏洞在真實網路環境傳出災情

CVE-2023-0669 是檔案傳輸管理解決方案 GoAnywhere MFT (Managed File Transfer) 中的遠端程式碼執行漏洞代碼 (RCE)。成功利用該漏洞可允許遠端攻擊者執行任意程式碼。原廠已發布修補更新程式來解決該漏洞。與此同時，賽門鐵克持續觀察此漏洞是否在真實網路環境傳出災情。

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: GoAnywhere MFT RCE CVE-2023-0669

2023/02/28

歸因於 BlackFly APT 駭客組織的新活動

Blackfly 駭客間諜組織（又名 APT41、Winnti Group、Bronze Atlas）持續對亞洲的目標發動攻擊，最近又針對一家亞洲企業集團的兩家子公司，這兩家子公司都是材料和復合材料領域的廠商，這表明該組織可能試圖竊取知識產權。

在我們的部落格文章中有更詳盡內容：Blackfly 間諜組織瞄準材料科技行業

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
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Winnkit
- Hacktool.Mimikatz
- Spyware.Gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- Heur.AdvML.C

2023/02/27

MetaMask小狐狸加密貨幣錢包的廣受歡迎，當然會引來更多的新興詐騙手法

Metamask 是一種近期非常熱門的透過瀏覽器及外掛就能簡單操作的加密貨幣錢包，允許用戶直接從他們的網路瀏覽器安全地存儲、管理以太坊加密貨幣和去中心化應用程序 (dApp) 並與之互動。多年來，它已成為加密貨幣用戶和 dApp 開發人員的熱門選擇。然而，眾所周知，在網路安全領域，流行總是會引起不必要的關注。

近年來，賽門鐵克發現越來越多的釣魚網站假冒 Metamask，企圖誘騙用戶洩露他們的私鑰、助記詞 (seed phrases) 或其他可用於竊取加密貨幣的機敏資訊。這些網路釣魚行動由世界各地的駭客組織和個體戶所發動，主要透過網路釣魚電子郵件和簡訊來進行。以下是最近偵測到的網路釣魚電子郵件攻擊行動中觀察到的郵件主旨的一些實例：

- MetaMask Quick Identity Verification
- [Important Notice] Request to confirm use of MetaMask
- MetaMask Privacy Policy Update: 21/02/2023
- This email is a service from MetaMask
- MetaMask(メタマスク) クイック本人確認
- 【重要なお知らせ】MetaMask(メタマスク) ご利用確認のお願い
- You have a frozen MetaMask wallet
- Your MetaMask wallet is limited!

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)。

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。

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)：

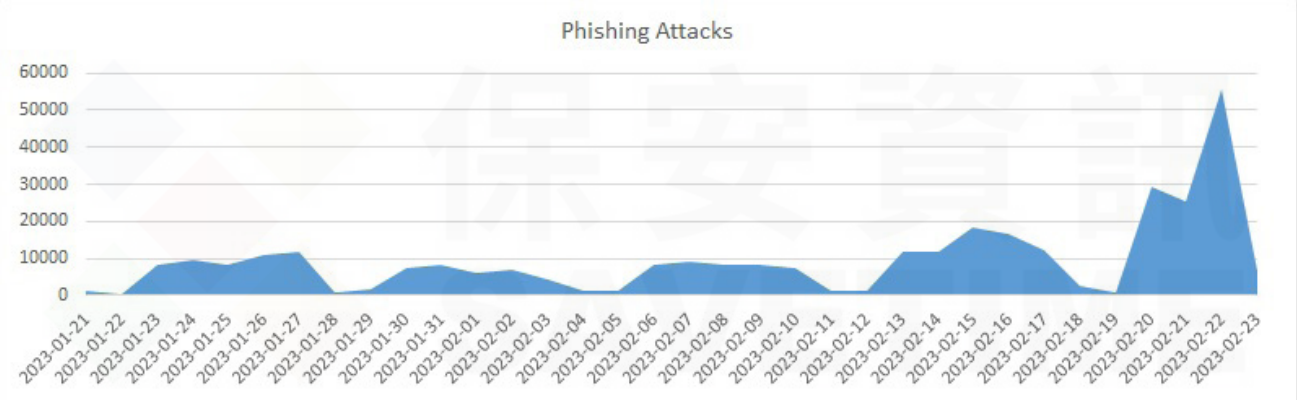
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/02/27

防護亮點：賽門鐵克第一時間就能攔截假冒美商優比速國際股份有限公司(UPS)的網路釣魚行動

～防護亮點～

網路釣魚攻擊是最常見的網路犯罪活動形式之一，到 2022 年會顯著增加，而且到 2023 年的速度似乎也不會放緩。賽門鐵克安全解決方案每天全天候檢測並阻止網路釣魚行動，但惡意軟體偶爾會激增電子郵件流量非常大，足以引起人們的注意，因為它往往表明有人比平時更努力地嘗試竊取某些系統或其他系統的登錄資訊。過去一周，我們的監控系統提醒我們注意一個針對 企圖詐騙UPS 憑證的大規模網路釣魚行動，高峰期有超過 50,000 封電子郵件，請放心，所有這些惡意攻擊行動都被我們的 Stargate 安全引擎（它是我們電子郵件安全服務的基礎）及其先進的啟發式威脅檢測功能主動阻止。



2 月 20 日至 22 日是假冒 UPS 網路釣魚行動的高峰

這些電子郵件包含一個惡意附件檔，開啟該附件會呈現 HTML 格式的網頁內容，該網頁會顯示“UPS Worldwide Saver”的假冒 UPS 登錄頁面，並要求受害者透過提供他們的登錄帳號和密碼來驗證他們的身份，以“證明你是人類”。輸入請求的訊息將導致輸入的憑證等機敏內容將被上傳到攻擊者所操控的伺服器。成功上鉤之後還可能導致登錄的詳細資訊被用於進一步的詐騙攻擊，因為許多資安觀念與認知薄弱的用戶會採用相同的憑證（帳號／密碼）在不同的網路銀行或線上服務。為提升保護自己免受網路釣魚攻擊的免疫力，切勿點擊來路不明的電子郵件和手機簡訊中出現的網址鏈接，切勿回應來路不明或陌生人的請求（無論是通過電話還是網際網路）並嚴禁提供您的個人資訊。

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 **零時差防護技術**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.Heuristic!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)。

要了解有關賽門鐵克郵件安全雲端服務的更多訊息，請點擊此處。

要了解有關賽門鐵克Stargate(*星際之門)安全引擎基於機器學習、雲知識和深度內容檢查的威脅檢測平臺的資訊，請在此聯繫賽門鐵克。

2023/02/27

PureCrypter下載程式的小破口，釀成許多政府機關的大災難

在真實網路環境發現了一起利用 PureCrypter 惡意下載程式鎖定政府機關的全新攻擊行動。感染鏈被拆解後發現有偽裝成訂單確認的惡意垃圾郵件，其中內嵌不同網址的惡意網頁鏈接。在感染鏈中被觸發的 PureCrypter 惡意程式後，啟動與呼叫程式將嘗試從被歹徒操控的非營利組織的受感染網站下載有效籌載。該攻擊行動採用各式各樣的最終有效籌載，包括 AgentTesla 鍵盤側錄與竊密程式、RedLine 竊密程式、Blackmoon 殭屍網路和 Philadelphia 勒索軟體等。

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：

- AGR.Terminate!g2
- SONAR.ProcHijack!g21

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：

- MSIL.Downloader!gen7
- MSIL.Downloader!gen8
- Packed.NSISPacker!g14
- Ransom.Philadelphia
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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: Bad Reputation Application Network Activity
- System Infected: Trojan.Backdoor Activity 634

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。

2023/02/26

土耳其橫跨歐亞大陸的航運和軍事優勢～駭客當然也不放過

土耳其是中東和歐亞地區的主要商業中心，橫跨歐亞大陸更具戰略位置，其不斷發展的經濟和友善的商業環境吸引來自世界各地的投資者和企業家。然而，許多網路罪犯也知道這一點，多年來，賽門鐵克見證無數針對土耳其行業的攻擊，以及知名的土耳其組織經常被冒名做為詐騙的幌子。

在最近的一個例子中，網路歹徒一直冒名利用土耳其最大的金融機構之一 Ziraat 銀行，以發起惡意垃圾郵件攻擊行動，並針對土耳其境內的許多行業，包括與該國有往來的外國公司。這些電子郵件（主旨：Ticari Hesap Özetiniz）包含一個惡意的 .lzh 壓縮檔的附件，並且在該壓縮檔中有一個偽裝成銀行對帳單的惡意檔案。開啟後，將會佈署 Snake 鍵盤側錄惡意程式。

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：

- Scr.Malcode!gdn30

2023/02/26

歹徒假冒菲律賓陸地運輸辦公室鎖定特定行業

賽門鐵克最近觀察到一個惡意垃圾郵件攻擊行動，其中參與者假冒菲律賓陸地運輸辦公室的名義對多個行業發動惡意垃圾郵件攻擊，包括多個國家（美國、英國、日本和荷蘭）的金融、IT 設備、汽車以及食品和飲料等行業）。惡意電子郵件（主旨：“ORDER FOR HITEK OCEANIC”）附件包含一個 .zip 壓縮檔。如果用戶觸發附件檔案內含的惡意 .bat 批次檔，他們最終會感染 Remcos，這是一種眾所周知的遠端存取木馬。

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.dropper
- SONAR.heur.dropper
- SONAR.suspbeh!gen25
- SONAR.suspbeh!gen633

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/02/24

macOS用戶請小心～熱門盜版軟體隱藏惡意挖礦程式

在真實網路環境已經發現多起全新惡意軟體散佈行動，該散佈行動使用 XMRig 惡意挖礦程式來感染 macOS 電腦。攻擊者一直利用熱門影片編輯軟體 Final Cut Pro 的盜版來傳播惡意軟體。至少自 2019 年以來，已發現同一威脅者偽裝成 Logic Pro X 或 Adobe Photoshop 等應用程式來傳播惡意挖礦程式。惡意軟體也會與時俱進在規避安全軟體偵測與長駐持久性上進步明顯。為了隱藏其 C&C 通訊，該惡意軟體也利用基於去中心化的通訊技術的隱形網路專案 (Invisible Internet Project，I2P)來增加其隱匿性。

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.Coinminer
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- WS.Malware.1

2023/02/24

沒有許仙的WhiteSnake(*白蛇)竊密惡意程式(MaaS:惡意軟體即服務)

在真實網路環境發現一種名為 WhiteSnake 的全新竊密惡意程式。該惡意軟體以 MaaS（惡意軟體即服務）的形式銷售。WhiteSnake 主要從被入侵的電腦中搜集機密資訊。搜集的資訊包括憑證、信用卡詳細資訊、cookie、螢幕截圖、來自 FTP 或電子郵件用戶端的檔案、加密貨幣錢包等。彙整後，該資料將傳輸到歹徒利用殭屍電腦所操控指定的 Telegram 雲端硬碟。

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：

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

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：

- System Infected: Trojan.Backdoor Activity 634
- WS.Malware.1

2023/02/23

利用善良人性的詐騙～以救濟為幌子的詐騙網站在土耳其和敘利亞強震後如雨後春筍般冒出

在世界各地看到多個以救濟為宗旨的網站在災後是非常普遍。這些通常是為了提供一個集中平台來協調救災工作並為受災者提供資源而建立。不幸的是，作為其犯罪活動的一部分，網路犯罪分子還在災難發生後建立以救濟為主題的網站。這些網站的目的在誘騙人們提供敏感資訊或進行欺詐性捐贈，而且它們很有說服力。

賽門鐵克觀察到許多在土耳其和敘利亞遭受兩次大地震災後出現的以救濟為主題的網站，其中一些網站為網路詐騙歹徒所操控。災後瀏覽救濟或捐助類型的網站時務必謹慎。建議只向知名的組織捐款，並在提供任何個人資訊之前驗證該網站是否為真正合法的網站。

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。