保安資訊--本周(台灣時間2022/02/04)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 130 萬個受保護端點上總共阻止了 2.105 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/01/31)**

- 在**24萬7,500**台端點上，阻止了**1.120億**次嘗試掃描**Web**服務器的漏洞。
- 在**48萬3,800**台端點上，阻止了**3,900萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬700**台**Windows**伺服主機上，阻止了**2,750萬**次攻擊。
- 在**19萬600**端點上，阻止了**1,120萬**次嘗試掃描伺服器漏洞。
- 在**10萬7,000**台端點上，阻止了**540萬**次嘗試掃描在**CMS**漏洞。
- 在**17萬3,400**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**49萬8,000**台端點上，阻止了**1,350萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,000**台端點上，阻止了**400萬**次加密貨幣挖礦攻擊。
- 在**4萬6,000**台端點上，阻止了**510萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,900**台端點上，阻止了**23萬1,200**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。

2022/02/04

UpdateAgent 惡意軟體現在能夠向 MacOS 用戶提供額外的籌載

據報導，UpdateAgent 特洛伊木馬在最新的行動中主動針對 MacOS 用戶。該惡意軟體是一種資訊竊取程式，但在最近的一些攻擊中也可以看到提供新一代的有效籌載。UpdateAgent 具有多種功能，可以模擬合法軟體並繞過 Gatekeeper 防禦機制 (2012 年起 macOS 中所部署的安全機制)。自從 2020 年出現最初的變種以來，該木馬被認為其開發者還持續不斷在開發，因為它已經實現了多種功能。

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：

- Backdoor.Trojan
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- OSX.WizardUpdate

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。

2022/02/04

新的 CoinStomp 挖礦惡意軟體針對亞洲的雲端服務提供商 (CSP)

據報導，一種名為 CoinStomp 新惡意軟體針對亞洲的雲端服務提供商 (CSP)。攻擊者目的在利用 CSP 代管的雲端個體 (Instance) 進行加密。CoinStomp 採用一種與眾不同的時間戳記技術，其中植入惡意檔案的時間戳記會被改寫，以使鑑識調查更加困難。

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
- Linux.Lightaidra
- Trojan Horse
- Trojan.Gen.NPE

2022/02/03

新的 FluBot 和 TeaBot 惡意軟體行動

銀行特洛伊木馬 TeaBot 和 FluBot 已透過不同方法散布並針對全球 Android 用戶的活躍行動中被發現。FluBot 主要透過臉書聊天室 (FB Messenger) 使用帶有鏈接騙局 “影片中的人是你嗎?” 進行散佈。目標受害者點擊後被重新轉址到虛假地臉書登錄頁面。這種誘惑會誤導用戶安裝所

謂缺少的 Android 元件等，但也使攻擊者能夠直接存取憑證。TeaBot 已以類似方式部署，但新版本正透過 Google Play 商店中名為“QR Code Reader - Scanner App”應用程式散佈。該應用程式本身沒有惡意代碼，但它在執行時會在後台執行服務以檢查已註冊 Android 擁有者的國家／地區代碼。參與者分配的國家代碼定義何時跳過特定國家的代碼執行。未通過檢查的 Android 用戶會繼續從 GitHub 檢索配置檔。該檔將有另一個鏈接指向要下載的實際有效籌載。

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：

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

2022/02/03

透過搜索引擎優化(SEO)下毒散布的 Batloader

一項新的搜尋引擎最佳化（SEO）行動正在將 Batloader 惡意軟體和 Altera Agent 推送到搜索 Zoom、TeamViewer 和 Visual Studio 等生產力工具的用戶系統上。該行動使用 Batloader 惡意軟體作為攻擊鏈的第一步，然後向 Ursnif 和 Atera Agent 發送有效籌載，以推進感染和更深入地滲透到受害者的機器中。

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.Malfilter
- Trojan.Malmsi
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

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已於第一時間收錄於不安全分類列表中。

2022/02/03

巴勒斯坦仍然是 APT 組織：Arid Viper 的鎖定目標

在針對巴勒斯坦組織和激進份子的持續活動中，觀察到由 Arid Viper APT 組織開發和營運的 Micropsia 新一波 Delphi 惡意軟體。自 2021 年 10 月以來一直觀察到攻擊使用以政治為主題的網路釣魚，利用多個遠端存取木馬 (RAT) 來收集受害者的資訊。

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

基於機器學習的防禦技術：

- 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。

2022/02/03

中國駭客集團：Antlion，瞄準台灣金融機構

中國政府支持的進階持續性威脅 (APT) 駭客組織：Antlion ，在至少 18 個月時間裡一直針對台灣金融機構進行持續攻擊。攻擊者在受感染的系統上部署了一個名為 xPack 的自定義後門，這使他們能夠長期潛伏並廣泛存取受害機器。該活動的目標似乎是間諜活動，因為我們看到攻擊者竊取資料並暫存資料以從受感染的網路中洩漏。

在我們的部落格中閱讀更多資訊：中國進階持續攻擊(APT)駭客集團Antlion(*蟻獅)：以自訂義後門鎖定臺灣金融機構。

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：

- Exp.CVE-2019-1458
- Hacktool
- Trojan Horse
- Trojan.Blackhole!gen1
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- 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：

- OS Attack: Microsoft Windows SMB RCE CVE-2017-0144

基於安全強化政策(適用於使用DCS)：

Symantec 的 DCS 內建的入侵防禦功能(預設政策)就可提供針對此Antlion的零時差攻擊保護。

2022/02/02

CWP 錯誤--CVE-2021-45466 和 CVE-2021-45467

上個月，一位研究人員在 Linux 的伺服器網頁管理介面軟體 Control Web Panel（CWP）中發現了兩個嚴重錯誤。安全漏洞是程式碼注入 (CVE-2021-45467) 和檔案寫入 (CVE-2021-45466) 漏洞。結合這兩個漏洞利用將導致在易受攻擊的 Linux 伺服器上進行預先認證 (pre-authenticated) 的 RCE（遠端程式碼執行）。

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：

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: Generic Directory Traversal

2022/02/02

Dark Herring，大型高級服務活動

行動動裝置的高級服務仍然是一項利潤豐厚的業務，我們繼續觀察到攻擊者濫用它來獲取經濟利益。最近，一個攻擊者和他們在 Google Play 與第三方商店上架的數百個行動應用程式 (App) 已經被曝光。這些基本應用程式被稱為 Dark Herring，根據其描述按預期功能執行，但在安裝時會要求用戶輸入他們的電話號碼。受害者不知道的是他們將訂閱付費服務，並透過營運商直接計費 (DCB) 每月收取約 15 美元費用，這是一種線上行動支付方式，允許用戶透過手機營運商賬單收取費用來進行購買。

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

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。

2022/02/02

APT 組織 Phosphorus 利用新的後門

最近發現一個名為“PowerLess Backdoor”新後門，並由 APT 組織 Phosphorus 部署。這些攻擊是透過魚叉式網路釣魚行動進行的，一旦安裝，這個後門就能夠執行多個任務，包括下載額外的惡意軟體和洩露資料。

Powerless Backdoor包含以下能力：

- 以其他的惡意軟體感染
- 與C&C伺服器安全通訊
- 執行任意指令並終止程序
- 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：

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
- Trojan.Maljava

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。

2022/02/02

新 RaaS Sugar

最近發現一種名為 Sugar 新型勒索軟體即服務。該勒索軟體是用 Delphi 編寫，似乎從其他勒索軟體系列（例如：REvil、Clop）借用了物件／程式碼。然而，Sugar 確實不同於其他勒索軟體系列，因為它主要針對單個機器而不是網路。

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.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。

2022/02/02

StrifeWater 遠端存取木馬(RAT)-- Moses Staff 駭客集團利用的新惡意軟體

根據最近發布的一份報告，Moses Staff 威脅組織在其產品組合中新增名為 StrifeWater 的新 RAT 惡意軟體。該威脅組織似乎在有針對性勒索軟體攻擊的初始階段使用 StrifeWater。RAT 具有各種功能，例如：收集有關受感染機器的資訊、執行命令、建立持久性或下載附加模組。

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

基於機器學習的防禦技術：

- 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。

2022/02/02

MuddyWater (*渾水) 進階持續攻擊 (APT) 駭客集團針對土耳其的組織

一項新的間諜行動來自於 MuddyWater (*渾水) 進階持續攻擊 (APT) 駭客集團 (也稱為：Seedworm)，已觀察到針對土耳其的組織和政府機構。攻擊者利用惡意 PDF、Excel 檔案和可執行檔來嘗試部署大量基於 PowerShell 下載程式腳本。接下來可能會部署額外的有效籌載，例如：勒索軟體，因為該威脅組織過去已經有使用勒索軟體有效籌載的紀錄。

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
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mdropper
- Trojan.Pidief
- W97M.Downloader

基於機器學習的防禦技術：

- 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。

2022/02/01

Shuckworm APT 持續攻擊烏克蘭

Shuckworm 駭客集團（也稱為 Gamaredon、Armageddon）正在持續對烏克蘭的目標進行網路間諜攻擊。在最近幾個月的過程中，賽門鐵克發現針對該國許多組織攻擊未遂的證據。眾所周知，該組織使用網路釣魚電子郵件向目標散佈免費可用的遠端存取工具，包括遠端操縱器系統 (RMS) 和 UltraVNC，或名為 Pterodo／Pteranodon 的客製化惡意軟體。

在我們的部落格中閱讀更多資訊：Shuckworm 繼續對烏克蘭進行網路間諜攻擊

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：

- Downloader
- ISB.Downloader!gen195
- JS.Downloader
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malscript
- VBS.Downloader.Trojan

基於機器學習的防禦技術：

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

2022/02/01

Google Play 上發現了更多臉書帳號偷竊程式 (FaceStealer)

很長一段時間以來，社交媒體帳戶一直受到網路犯罪分子的覬覦。2021 年年中，我們發布一份防護公告，內容涉及一個攻擊者試圖竊取行動用戶 Facebook 憑證的惡意行動，並透過在 Google Play 上架的常用惡意應用程式來引誘他們。最近，在 Google Play 上發現更多這種臉書帳

號偷竊程式 (FaceStealer)，這一次是已知 Android 應用程序的副本。

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：

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

2022/01/30

DeadBolt 勒索軟體，攻擊 QNAP 網路儲存伺服器(NAS:Network Attached Storage)

一種名為 Deadbolt 新勒索軟體就在本月首次出現，目標針對常見的品牌：QNAP 網路儲存伺服器 (NAS:Network Attached Storage)，以加密用戶資料勒索比特幣贖金。所有被加密檔案都帶有 .deadbolt 的副檔名。勒索軟體集團並沒有此攻擊中隨附勒索說明，而是劫持登錄頁面以顯示警告，要求受害者向特定的比特幣地址支付 0.03 比特幣（按當前價格計算約為 1,100 美元）以換取解密密鑰。

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

2022/01/28

APT27 駭客集團採用 HyperBro 遠端存取木馬(RAT)，鎖定企業發動攻擊

根據最近一份報告，在真實世界網路上觀察到一系列針對德國企業的持續攻擊，已經證實是來自於 APT27 駭客集團。攻擊者正在利用一種稱為 HyperBro 遠端存取木馬 (RAT)。在最近一些攻擊中，該駭客集團一直在積極利用 ProxyLogon 漏洞以及企業密碼管理套件：Zoho Manage Engine ADSelfService Plus 中的 CVE-2021-40539 漏洞來繞過驗證檢查。

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
- 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：

- Audit: Zoho ManageEngine ADSelfService Plus CVE-2021-40539
- Attack: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server CVE-2021-26857
- Web Attack: Zoho ManageEngine ADSelfService Plus RCE CVE-2021-40539

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。

2022/01/28

Lazarus APT，利用 Windows Update 用戶端和 Github

Lazarus (北韓支持的國家級駭客集團) 集團最新的惡意軟體行動以洛克希德馬丁公司工作機會為主題進行了魚叉式網路釣魚攻擊。攻擊使用 word 檔案做為誘餌，兩者都啟用了巨集。感染例程由 LNK 和 DLL 檔案組成，最終將導致使用 Windows 更新用戶端執行惡意 DLL 以掩蓋他們的行動並逃避檢測。

該駭客集團不斷更新他們的工具集，以下列出了幾種能繞過檢測的新技術：

- 使用 KernelCallbackTable 劫持控制流程和 shellcode 執行
- 使用 Windows Update 用戶端執行惡意程式碼
- 使用 GitHub 進行 C&C 通信

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.Mdropper
- WS.Malware.1
- WS.Malware.2
- W97M.Downloader

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。

2022/01/28

Transparent Tribe (*透明部落)：進階持續威脅 (APT) 駭客組織，散布 Crimson 遠端存取木馬 (RAT)

Transparent Tribe (*透明部落)，也稱為 APT36 或 Mythic Leopard，被發現發起另一次網路攻擊行動。雖然主題以及它是如何散布給目標並未披露，但研究人員已經分析可用的感染指標(IOC)，並確定該組織使用了 ConfuserEx 打包的 "滴管" 來配送 RAT 有效籌載，並且還附帶一個誘餌圖檔。Crimson 遠端存取木馬 (RAT) 能夠收集有關受害者系統的資訊，並將其發送回他們的命令和控制伺服器 (C&C)。

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
- Trojan.Gen.NPE
- WS.Malware.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已於第一時間收錄於不安全分類列表中。