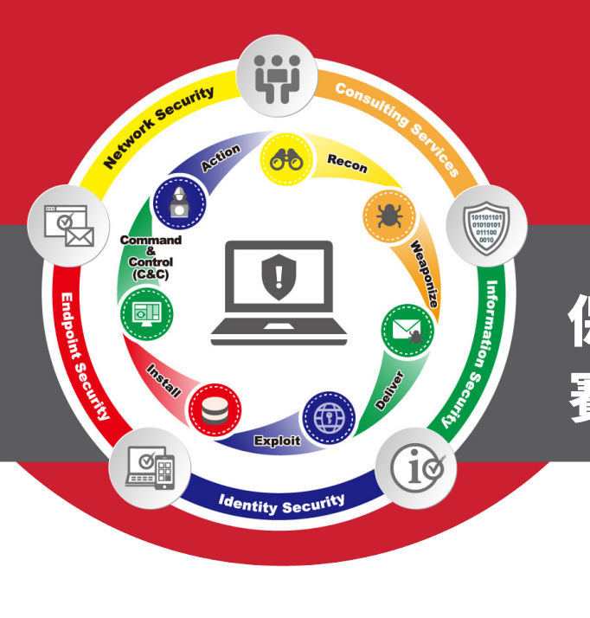

保安資訊--今日最新(台灣時間2021/09/15)
賽門鐵克原廠防護公告重點說明

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 140 萬個受保護端點上總共阻止了 2.002 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：(2021/09/13)

- **在30萬2,800台端點上，阻止了8,640萬次嘗試掃描Web服務器的漏洞。**
- **在62萬8,800台端點上，阻止了4,940萬次嘗試利用的Windows作業系統漏洞的攻擊。**
- **在9萬6,500台Windows伺服主機上，阻止了2,220萬次攻擊。**
- **在25萬2,600端點上，阻止了1,850萬次嘗試掃描伺服器漏洞。**
- **在15.01萬台端點上，阻止了790萬次嘗試掃描在CMS漏洞。**
- **在16萬5,400台端點上，阻止了470萬次嘗試利用的應用程式漏洞。**
- **在38萬6,800台端點上，阻止了720萬次試圖將用戶重定向到攻擊者控制的網站的攻擊。**
- **在6,500台端點上，阻止了420萬次加密貨幣挖礦攻擊。**
- **在64,000台端點上，阻止了470萬次向惡意軟體C&C連線的嘗試。**
- **在10,800台端點上，阻止了33萬3,000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。

2021/09/14
我們在第一時間回應：Microsoft 9 月修補發布的覆蓋範圍詳細資訊

微軟於 9 月 14 日發布了定期安排的每月更新。對於 9 月發布的版本，Microsoft 解決了 66 個漏洞。

賽門鐵克根據可用資訊提升了以下保護措施。目前正在調查其他特徵檔，可能會在隨後依需求作靈活調整或切換。

網路層防護：

- Web Attack: Microsoft MSHTML RCE CVE-2021-40444

2021/09/14
發現針對墨西哥銀行用戶的 Adroid 惡意軟體

已發現一種假冒銀行安全工具的新型行動惡意軟體。該惡意軟體針對墨西哥的用戶，據報導透過網路釣魚頁面進行分發。該虛假工具會通知用戶帳戶上發生的一些疑似的詐欺交易，並建議封鎖它們。攻擊者正在追踪用戶的登錄帳密等資料並存取受感染設備上的 簡訊內容，以便他們還可以攔截來自金融機構作為二階認證的簡訊內容。

賽門鐵克已經於第一時間提供多種有效保護。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。

手機板防毒(支援iOS/Android)：

- Android.Reputation.2
- AppRisk:Generisk

2021/09/13
被稱為「Vermilion Strike」 的 Cobalt Strike Beacon Linux 版本

最近，一組安全研究人員發現了 Cobalt Strike Beacon 的一個新變種--他們稱之為 Linux 版本的「Vermilion Strike」 ，由未知的威脅行動者所製作。合法的安全工具常常被拿來當成網路攻擊的第二階段橫行無阻的屠刀，因為它提供了被信任的增強的後攻擊(post-exploitation)能力。由於這個原因，Linux 環境現在不太安全，為了大大降低網路安全風險，持續保持警惕至關重要。

Vermilion Strike 一旦部署在受感染的 Linux 系統上就可以執行以下任務：

- 更改工作目錄
- 獲取當前工作目錄
- 追加/寫入文件
- 洩漏並上傳資料至 C&C 伺服主機
- 通過 popen 執行命令
- 獲取磁碟分割區
- 列出文件

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Heur.AdvML.B
- Heur.AdvML.C
- Meterpreter
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.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。

2021/09/13
Leafperforator(又稱Sidewinder和 Rattlesnake)APT 集團持續活躍

Leafperforator(又稱Sidewinder-*響尾蛇和 Rattlesnake-*響尾蛇)APT 集團，至少自 2012 年以來一直活躍，並繼續在南亞和東亞開展活動。眾所周知，該 APT 組織使用包含可能與目標對象相關的內容並帶有惡意附件／鏈接的客製化電子郵件進行網路釣魚。在 2020 年開始，他們被觀察到使用 Covid-19 疫情相關的主題為誘餌，利用大眾對疫情爆發流行的關注與惶恐來進行網路釣魚。已知Leafperforator 還使用DLL側載(DLL side-loading)技術來啟動其惡意軟體酬載(Payload)。

觀察到有效酬載(Payload)包含以下功能：

- 收集系統資訊
- 收集磁碟和檔案目錄資訊
- 收集感興趣的文件
- 更新惡意軟體配置
- 洩漏並上傳資料至 C&C 伺服主機

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Bloodhound.RTF.20
- Trojan.Gen.NPE
- Trojan.Horse

2021/09/13
Ghostscript 漏洞 (CVE-2021-3781)

一年前，一位研究人員發現了 GhostScript 中的一個錯誤(Bug)，並在幾週前舉行的網路安全會議上提出展示。Ghostscript 這是一組用於處理，轉換和生成 PostScript 和 PDF 格式的工具軟體。主題是關於直接影響 ImageMagick 的軟體中的零時差(RCE 漏洞利用鏈)漏洞。幾天後，另一位研究人員決定在 Artifex 於 2021 年 9 月 9 日剛剛發布的修補之前，透過 Github 發布 POC。這一行為構成了安全風險，可能使威脅行為者抓住機會並利用其攻擊中的缺陷。這個安全漏洞的 CVE ID 編號被列為：CVE-2021-3781。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Bloodhound.Exploit.842。

2021/09/13
Pysa 勒索軟體網路犯罪集團--現在也針對 Linux

據報導，Pysa 勒索軟體幕後的犯罪集團也一直針對 Linux 環境。該集團利用的一種基於 Chachi Golang 的惡意軟體的新 linux 變種已經出現。Chachi 後門在過去已經成為 Pysa 武器裝備的一部分，用於網路資訊收集、跨網路橫向移動和資料外洩等。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Trojan.Gen.NPE

網路層防護：

我們的 Webpulse(網頁脈衝)網頁自動回饋框架，已將其列為低信譽網域黑名單。

- 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。

2021/09/13
從巴西到葡萄牙--專門入侵銀行的木馬：Maxtrilha

拉丁美洲是世界上經常受到銀行惡意軟體攻擊的地區之一，這些惡意軟體通常利用惡意電子郵件和偷渡式下載來進行傳播。Maxtrilha（在 Delphi 中開發）是最近報導的一個新威脅，該威脅的幕後黑手已經在巴西開展了活動，但現在將他們的活動擴展到葡萄牙。他們通過聲稱來自政府稅務機構的電子郵件分發了此惡意軟體，其中包含轉導向到掛載惡意程式的惡意網址。該掛載的惡意程式將部署 Maxtrilha，即實際的有效負載和銀行惡意軟體，它將監視受害者存取銀行網站，然後竊取他們的登錄的憑據（帳密）。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Trojan.Gen.2

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。

2021/09/12
在 Android 平台的 888 RAT(遠端存取木馬)被發現用於網路間諜活動

Android 遠端存取工具和木馬繼續被各種網路犯罪集團和個人用來偷窺受害者。這種類型的惡意軟體非常流行，多年來，許多惡意軟體已被破解並在論壇、網站和社交媒體上免費洩露。一些攻擊者是像 BladeHawk 這樣的團體，他們一直在他們的網路間諜活動中使用一種被稱為 888 RAT 的破解 RAT（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。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。

手機板防毒(支援iOS/Android)：

- AdLibrary:Generisk
- Android.Reputation.1

2021/09/12
發現名為：S.O.V.A.的Android平台行動網銀惡意程式

行動銀行惡意軟體已經存在多年，非常流行且數量眾多。對於網路犯罪分子來說，這是一項有利可圖的業務，而且新業務經常在地下做廣告。據報導，地下市場出現了另一種手機銀行惡意軟體變種，即 S.O.V.A.，與其他普通的行動銀行惡意軟體一樣，它極度依賴覆疊(overlay)技術。

賽門鐵克已經於第一時間提供多種有效保護。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。

手機板防毒(支援iOS/Android)：

- Android.Reputation.1

2021/09/10
Lockbit 勒索軟體攻擊增加

Lockbit 是過去幾週最活躍的勒索軟體變種之一。該惡意軟體作為勒索軟體即服務(RaaS)產品的一部分出售。根據最新報導，其幕後的威脅集團一直在積極招募新的聯盟成員。這種勒索軟體變種的最新發展之一是它通過群組原則(GPO)將自身部署到 Active Directory 用戶端的新技術。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Downloader
- Heur.AdvML.B
- Heur.AdvML.C
- Ransom.Lockbit
- Ransom.Lockbit!g2
- Ransom.Lockbit!gen3
- Ransom.Lockbit!gen4
- Ransom.Lockbit!gm1
- Trojan Horse
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- SONAR.RansomLckbit!g1
- SONAR.RansomLckbit!g2
- SONAR.RansomLckbit!g3
- SONAR.SuspReg!gen28

網路層防護：

- Attack: Ransom.Lockbit Activity
- Attack: Ransom.Lockbit Activity 2
- Attack: Ransom.Lockbit Activity 3

2021/09/09
新發現來自 TNT APT 集團所發動的「挖礦」攻擊活動--「Chimaera」

一個由 TNT APT 集團發起並被稱為 Chimaera 的新活動被發現。據報導，攻擊者利用各種 shell 腳本、挖礦程式、網路聊天機器人(IRC)和開源工具，在多個平台上進行協同攻擊，包括：Windows、Linux、AWS、Docker 和 Kubernetes。與過去一樣，TNT 威脅團體一直致力於竊取系統憑據（帳密）和利用受感染的機器進行加密貨幣挖掘（挖礦）等。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Linux.Backdoor.Kaiten
- Trojan Horse
- WS.Malware.1

網路層防護：

我們的 Webpulse(網頁脈衝)網頁自動回饋框架，已將其列為低信譽網域黑名單。

- Web Attack: Webpulse Bad Reputation Domain Reques

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。

2021/09/08
Mirai 殭屍網路利用的 Realtek (台灣瑞昱) 軟體開發套件 (Software Development Kit, SDK) 漏洞

據報導，名為 Dark.IoT 的 Mirai 殭屍網路變種利用了兩個最近發現的 Realtek (台灣瑞昱)軟體開發套件漏洞，分別為 CVE-2021-35394 和 CVE-2021-35395。所披露的漏洞可能會影響來自多個不同供應商但同樣採用 Realtek(台灣瑞昱)晶片組及其SDK的無線設備。如果漏洞成功被利用，攻擊者可以獲得對受感染裝置的完全控制，利用它們進行 DDoS 攻擊或在其上運行任意代碼。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Downloader
- Linux.Mirai
- Trojan.Gen.NPE

網路層防護：

已被我們被歸類為以下的惡意攻擊／漏洞型攻擊：

- MWeb Attack: Realtek Jungle SDK RCE CVE-2021-35394
- Web Attack: Realtek Jungle SDK RCE CVE-2021-35395
- 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已於第一時間收錄於不安全分類列表中。

2021/09/08
Confluence 用戶被警告，需修補嚴重漏洞

Atlassian 於 8 月 25 日發布了針對幾個與 Confluence 服務器和資料中心實例相關漏洞的安全公告。特別是跟蹤為 CVE-2021-26084 漏洞的遠端代碼執行，它可以允許未經身份驗證的攻擊者，在未修補該漏洞的主機上遠端執行命令。該公司已發布修補程式，建議客戶升級其主機系服務器。

完成概念性驗證(Proof of Concept；POC)之後，惡意行為者掃描和利用該漏洞的跡像已經出現，以至於美國網戰司令部（US Cyber Command）發出公告警告該漏洞正在被積極利用。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Trojan.Gen.MBT

網路層防護：

已被我們被歸類為以下的惡意攻擊／漏洞型攻擊：

- Web Attack: Malicious Java Payload Upload 5
- Web Attack: Confluence RCE CVE-2021-26084

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IP位址／網域名稱已於第一時間收錄於不安全分類列表中。

2021/09/08
威脅警示：微軟發布了針對MSHTML中的遠端程式碼執行(RCE)漏洞(CVE-2021-40444) 的公告

微軟於 9 月 7 日發布了針對 MSHTML 中的遠端程式碼執行 (RCE) 漏洞 (CVE-2021-40444) 公告。據報導，該漏洞正被積極用於針對性攻擊。MSHTML 也稱為 Trident，主要用於 Internet Explorer 瀏覽器，也用於 Microsoft Office。該組件允許開發人員將 Web 瀏覽功能添加到他們自己的應用程式中。在觀察到的攻擊中，攻擊者利用該漏洞製作了惡意的 Microsoft Office 文件。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- W97M.Downloader

網路層防護：

已被我們被歸類為以下的惡意網站：

- Malicious Site: Malicious Domains Request
- Malicious Site: Malicious Domain Request 59

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。

說明：我們將持續分析這個漏洞，並提升防護機制，也會在安全公告公佈。

2021/09/07
「Pegasus」間諜軟體，被用於勒索詐騙攻擊

攻擊者持續利用「Pegasus」間諜軟體進行的惡意垃圾郵件活動，採用「散佈恐懼」的策略，試圖恐嚇其受害者，使其支付勒索贖金。上述活動聲稱 Pegasus 是一種針對手機的「完全不用按鍵」--零點擊類型的攻擊，不需要手機用戶的任何操作即可讓間諜軟體控制裝置(這部分是真的)。攻擊者勒索一個比特幣以保證刪除任何不法獲得的用戶資訊，並承諾不會公開發布資料(這部分是否屬實就非常有待商榷了)。

賽門鐵克已經於第一時間提供多種有效保護。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)。

2021/09/07
新的「PRIVATELOG」惡意軟體，利用通用紀錄檔檔案系統(CLFS)進行規避

發現了一個新的惡意軟體家族，它依賴通用紀錄檔檔案系統（Common Log File System，縮寫CLFS）來隱藏存放在註冊表交易文件中的第二階段有效籌載，以試圖逃避檢測。通用紀錄檔檔案系統 (CLFS) 是 Windows Server 2003 R2 中引入的通用日誌子系統，用於構建高性能交易日誌。被封為「PRIVATELOG」的惡意軟體還帶有自己的名為 「STASHLOG 」的安裝程式。根據已發布的報告，該惡意軟體似乎仍處於開發階段，或者可能僅用於高度針對性的活動。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Heur.AdvML.C
- Trojan Horse
- Trojan.Gen.MBT

2021/09/07
透過主題為 Windows 11 Alpha 的惡意文件，利用 VBA 巨集下載 JavaScript 後門及酬載

根據最近的一份報告，FIN7 進階持續威脅(APT)集團，持續利用主題為：Windows 11 Alpha 的惡意垃圾郵件活動，大量散布 JavaScript 後門。感染鏈始於聲稱在 Windows 11 Alpha 上建立的惡意誘餌 Word 文件，並要求收件人啟用編輯以繼續。啟用後，文件中包含的惡意 VBA 巨集，將嘗試下載 JavaScript 酬載(Payload)。據報導，該活動針對的是銷售點 (POS) 供貨商。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Heur.AdvML.B
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- W97M.Downloader

網路層防護：

我們的 Webpulse(網頁脈衝)網頁自動回饋框架，已將其列為低信譽網域黑名單。

- 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已於第一時間收錄於不安全分類列表中。

2021/09/06
出現「假冒韓國視訊APP」的手機間諜程式

在亞洲廣泛使用並明確設計用於「視訊(情色)陪伴：escort services」的行動應用 APP，實際上是一種隱蔽行動裝置上的間諜軟體，專門收集個人相關的機密資料。該 APP 可以在受感染的裝置上執行多種功能，例如：收集聯絡人、讀取和收集簡訊內容以及獲取位置詳細資訊，並且進一步的存取可以擴展到收集相簿和裝置的詳細資訊，這些非法竊取的資料，遲早會被用來勒索受害者。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.2
- W97M.Downloader

手機板防毒(支援iOS/Android)：

- 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已於第一時間收錄於不安全分類列表中。

2021/09/05
Elibomi 不會幫你報稅

報稅可能永遠是一個強大社交工程詐騙的誘餌，能跨越所有類型的媒介和平台。據報導，一種名為 Elibomi 的 Android 威脅，成為印度行動用戶社交工程詐騙活動一直反覆的目標。在最近案例中，攻擊者用聲稱印度所得稅部門的惡意簡訊引誘受害者。如果成功欺騙到受害者，會安裝虛假的報稅應用程式(Fake_App)，並在不知情的情況下填寫，最終會落入攻擊者手中的敏感資訊。更嚴重的是，這種威脅還能夠存取其他資料，例如：手機上的聯繫人和簡訊。

賽門鐵克已經於第一時間提供多種有效保護。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。

手機板防毒(支援iOS/Android)：

- AdLibrary:Generisk
- AppRisk:Generisk

2021/09/05
發現新的 JsOutProx 變種--遠端存取木馬程式(RAT, Remote Access Trojan)

JsOutProx 是另一種基於 Java 的遠端存取特洛伊木馬，它至少自 2019 年以來一直活躍在網路威脅圈。如今，該惡意軟體主要透過惡意垃圾郵件活動散布，最近還觀察到了一種新變種，這種惡意軟體幕後的參與者被稱為 Solar Spider。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Backdoor.Trojan
- Trojan.Horse

2021/09/03
近期觀察到的可疑勒索軟體活動--偽裝成遠端會議／視訊的惡意MSI安裝套件安裝程式

在一項對最近遙測技術的評估中，我們觀察到一個在美國、德國和印度出現的未知型攻擊。攻擊者使用和以前與勒索軟體活動相關惡意的行為手法、技術與過程 (Tactics, Techniques and Procedures，簡稱 TTPs，可能包含攻擊特徵、惡意軟體、弱點暴露、攻擊狙殺鏈、使用工具、事件架構、受害目標等)。

攻擊始於偽裝成 Zoom 或 TeamViewer 的遠端會議／視訊的惡意 MSI 安裝套件安裝程式。安裝程式呼叫 PowerShell 下載多層額外的下載程序腳本，進而執行 Zloader DLL。最後幾個步驟可能包括下載附加模組、權限提升和*停用系統防禦或安全軟體。(*SEP 秘訣：啟用 SEP 的竄改防護功能，可防止 SEP 被惡意程式或人為停用)

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Downloader
- Downloader.Trojan
- Hacktool
- Heur.AdvML.B
- Heur.AdvML.C
- Trojan Horse
- Trojan.Gen.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已於第一時間收錄於不安全分類列表中。

2021/09/03
好工具拿來做壞事又一樁！常用的滲透測試工具--Metasploit，也被用於加密貨幣挖掘攻擊活動

多年來常使用於滲透測試及反派團隊(Red Team)演練的 Metasploit 滲透測試平台。但也被網路犯罪分子用作其攻擊鏈的一部分。最近有報導稱，某組織使用流行的測試框架 Metasploit 及其後門模組 (Meterpreter) 部署加密貨幣挖礦。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Meterpreter
- Trojan.Gen.MBT

2021/09/02
最近觀察到的惡意垃圾郵件活動，會派送被稱為：MassLogger訊息盜取器(infostealer)，正在瞄準攻擊目標

MassLogger 是一種透過地下論壇分發之廉價且易於獲得的訊息盜取器(infostealer)。最近在 8 月觀察到的惡意垃圾郵件活動，似乎很有可能發動目標攻擊初期的釣餌派送。

惡意垃圾郵件活動，利用看似合法的商業通信，以緊急訂單或緊急事件誘騙受害者開啟包含在 zip 中的附加惡意可執行檔。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan Horse

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)。

2021/08/30
*地球巴庫(Earth Baku)進階持續威脅(APT)集團採用全新的載入器及後門程式

最近浮出水面攻擊成為頭條新聞，新的惡意軟體工具已作為*地球巴庫(Earth Baku)攻擊活動的一部分。Earth Baku 是一個進階持續威脅 (APT) 組織，也被稱為 APT41。這些攻擊主要針對太平洋地區的組織。這些工具包括 StealthMutant 和 StealthVector，它們既是 shellcode 載入器也是後門 ScrambleCross。相比之前滲透目標網路被發現時，該惡意軟體目前設計的更容易自定義，並使用更複雜的規避技術。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

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

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IP及網域名稱已於第一時間收錄於不安全分類列表中。

2021/08/27
勒索軟體Hive鎖定醫療機構、缺乏相關因應措施的企業而來

賽門鐵克安全回應中心獲悉最近美國聯邦調查局(FBI)於本月中發布了緊急警報(Flash Alert)，警告有關 Hive 勒索軟體的活動。Hive 早在今年 6 月份就被發現，並從那時起針對各種企業和醫療保健行業發動攻擊。根據警示，Hive 採用網路釣魚電子郵件及對受害者網路中有漏洞的 RDP 存取進行散播。這種勒索軟體背後的入侵者利用「雙重敲詐手段」，不僅盜竊機密資料，並威脅受害者在贖金要求得不到滿足時，將這些資料公諸於世。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Downloader
- Heur.AdvML.B
- Ransom.Hive
- Trojan Horse
- Trojan.Gen.MBT
- Behavior-based
- SONAR.RansomHive!g1
- SONAR.RansomHive!g2

網路層(IPS)防護：

- Attack: Ransom.Gen Activity 29

2021/08/26
在最新攻擊活動中觀察到「Karma」勒索軟體

最近我們知道被稱爲「Karma」的勒索軟體變種的惡意活動正在流行。惡意軟體加密受害者的檔案，並在檔案中新增 .karma 副檔名。KARMA-ENCYPTED.txt 贖金說明被放在受害者電腦上的各種目錄中。威脅者建議受害者透過贖金通知單上記載的電子郵件地址與他們聯繫。他們還威脅說，如果不滿足贖金要求，將公開洩露機密資料。

賽門鐵克已經於第一時間提供多種有效保護。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(基於病毒定義檔)防護：

- Heur.AdvML.C
- Heur.AdvML.M
- Ransom.Gen
- Trojan Horse
- WS,Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.RansomKarma!g1
- SONAR.Ransomware!g12

業界公認 **保安資訊**--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost
服務電話：0800-381500｜+886 4 23815000｜http://www.savetime.com.tw