
# 保安資訊--本周(台灣時間2023/05/26)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 77 萬 1,200 台受保護端點上總共阻止了 9,170 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/05/22)**

- 在**15萬9,200**台端點上，阻止了**3,840**萬次嘗試掃描**Web**服務器的漏洞。
- 在**27萬2,900**台端點上，阻止了**1,930**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬1,500**台**Windows**伺服主機上，阻止了**1,380**萬次攻擊。
- 在**9萬1,300**台端點上，阻止了**250**萬次嘗試掃描伺服器漏洞。
- 在**1萬6,100**台端點上，阻止了**88萬6,200**次嘗試掃描在**CMS**漏洞。
- 在**7萬300**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**26萬9,800**台端點上，阻止了**630**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,700**台端點上，阻止了**230**萬次加密貨幣挖礦攻擊。
- 在**15萬3,200**台端點上，阻止了**1,090**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,400**台端點上，阻止了**9萬5,500**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。

## 2023/05/25

## 用於發動分散式阻斷服務攻擊(DDoS)的MDBotnet惡意軟體

MDBotnet 是一種在地下論壇上出售的全新惡意軟體。該惡意軟體的主要功能可用於發動 HTTP 和 SYN flood(洪水) 等類型的分散式阻斷服務攻擊 (DDoS)。MDBotnet 還附帶一個額外“更新程式”檔案，負責從攻擊者所操控的遠端伺服器下載最新版本的惡意軟體更新。

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
- WS.Malware.1
- WS.Malware.2

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- 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

**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。

---

## 2023/05/25

## StrelaStealer惡意竊密軟體繼續以西班牙語系使用者為目標

StrelaStealer 是一種惡意竊密程式，最初於 2022 年被發現，已知專門針對西班牙語系使用者。與去年在攻擊鏈中使用 ISO 檔案的攻擊行動相反，今年的攻擊行動轉而使用 ZIP 檔案。在被散佈的 ZIP 壓縮檔中，存在導致惡意軟體感染的惡意 .PIF 檔案。一旦在目標電腦上執行，StrelaStealer 將搜索常用的電子郵件用戶端系統（例如：Outlook 和 Thunderbird）的電子郵件帳戶憑據 (帳密)，並將收集到的訊息洩露到攻擊者所操控的 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(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：**

- Trojan Horse
- 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。

---

## 2023/05/25

## 全新駭客集團：Blacktail使用Buhti勒索軟體發動對Linux和Windows系統的攻擊

一種還算新並自稱為 Buhti 的勒索軟體攻擊行動似乎採取避開自行開發有效籌載的策略，而是利用遭洩露的 LockBit 和 Babuk 等勒索軟體家族後續變種來攻擊 Windows 和 Linux 系統。Buhti 於 2023 年 2 月首次引起公眾關注，最初據報導它會攻擊 Linux 系統。賽門鐵克的威脅獵手 (Threat Hunter) 團隊也發現在遭駭入網路上也有攻擊 Windows 系統的企圖。由於 Buhti 與任何已知的網路犯罪集團都沒有關聯，因此賽門鐵克將其幕後運營駭客集團命名為 Blacktail。

在我們的部落格文章中有更多資訊可供參考：Buhti：依賴重新改造惡名昭彰勒索軟體有效酬載所發動的全新攻擊行動。

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
- SONAR.UACBypass!gen30

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Cobalt
- Hacktool
- Meterpreter
- Ransom.Buhti
- Ransom.Lockbit!g6
- Trojan Horse
- WS.Malware.1
- WS.SecurityRisk.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: Meterpreter Reverse TCP Activity 6
- System Infected: Trojan.Backdoor Activity 123
- Web Attack: Malicious Java Payload Upload 2
- Web Attack: Malicious Java Payload Upload 19

**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。

---

## 2023/05/25

## RA Group勒索軟體

RA Group 是一個全新的勒索軟體威脅參與者，自 2023 年 4 月以來，已經發現多起其所發動的行動。該駭客集團是利用知名且已被洩露的 Babuk 勒索軟體原始程式碼再自行客製化過的版本。該惡意軟體能夠刪除受感染電腦上的陰影副本。被其加密過的檔案會被冠上 .GAGUP 的副檔名，並透過公開發布被盜資料來脅破受害者，這種伎倆就是慣用的雙重勒索策略。

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.Ransomware!g7
- SONAR.Ransomware!g16
- SONAR.Ransomware!g38
- SONAR.TCP!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Downloader
- WS.Malware.2

**基於機器學習的防禦技術：**

- Heur.AdvML.C

---

## 2023/05/25

## GoldenJackal進階持續威脅(APT)駭客集團所發起的最新間諜活動

根據最近發布一份報告，被稱為 GoldenJackal 的進階持續威脅 (APT) 駭客集團持續針對中東和南亞的政府組織和個人發動間諜行動。攻擊者利用多種攻擊媒介--包括透過偽造的 Skype 安裝程式來植入基於 .NET 惡意軟體、惡意的文件檔，像是可被開採利用 Follina 漏洞 (CVE-2022-30190) 的惡意 Word 檔，進而下載惡意 HTML 頁面。一旦攻擊者成功取得受害者電腦的存取權限，他們將嘗試竊取憑證、截取螢幕截圖、從本地系統和網頁瀏覽器竊取機密資訊，再將收集到的資訊洩露到他們所操控的 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(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：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.B
- 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
- System Infected: Bad Reputation Process Request 4

**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。

## 2023/05/24

## Rhysida勒索軟體

Rhysida 是一種剛被發現 Windows 平台上的全新勒索軟體。該勒索軟體採用多執行序加密技術，包含寫死在加密勒索軟體內的副檔名／目錄例外清單，並會將被加密的檔案冠上 .rhysida 的副檔名。Rhysida 不採常用 .TXT 文字檔格式的贖金支付說明，而是在每個被加密的目錄中以 .PDF 格式放置贖金支付說明。該惡意軟體還會更改受感染電腦上的桌面背景。

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.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g16

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A

## 2023/05/24

## 免費的永遠最貴～AhRAT安卓平台惡意軟體，透過螢幕錄影APP傳播

AhRAT 是一種安卓平台上的手機惡意軟體，是透過被植入惡意木馬程式的螢幕錄影手機APP:iRecorder 來傳播～該 APP 本身於 2021 年首次發布，最初不包含任何惡意功能。惡意程式碼似乎（源於另一種稱為 AhMyth 的行動裝置惡意軟體）是在 2022 年 8 月前後的後續更新版本中被植入。AhRAT 惡意軟體具有竊取麥克風錄音、通話記錄、簡訊、聯絡人和竊取手機中的使用者自存檔案等功能。

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：

**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
- 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。

---

## 2023/05/24

## 基於Rust的竊密程式濫用Github Codespace程式碼儲存庫進行資料外洩

網路上最近矚目的惡意程式傳播行動中，觀察到被指認為 Deltastealer 的惡意竊密程式。這是一種基於 Rust 惡意軟體以竊取瀏覽器資料、銀行資訊、加密貨幣錢包、Discord 權杖等各種用戶資訊為目標，並將收集到的資料外洩到攻擊者所控制 GitHub Codespace webhook 中。該惡意竊密程式在功能上與另一個名為 PirateStealer 的惡意軟體家族非常相似--它也以 Discord 資料和其他資訊為目標，並且還會把被盜資料提取轉存到 GitHub Codespace 的能力。

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：**

- 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!300
- Heur.AdvML.B
- 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

**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。

---

## 2023/05/24

## Black Basta勒索軟體繼續登上新聞頭條

Black Basta 勒索軟體在去年相當搶眼，且似乎決定在 2023 年繼續成為人們關注的焦點，因為它鎖定全球各個產業的許多企業。這個駭客組織是最活躍的網路犯罪集團之一，他們採用讓人聞風喪膽的雙重勒索策略，來脅迫受害者乖乖支付贖金。該勒索軟體即服務 (RaaS) 幕後營運商採用多種攻擊手法來駭入受害者電腦，包括網路釣魚電子郵件、偷渡式下載以及開採利用未修補軟體的漏洞。

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.RansomBasta!g3
- SONAR.Ransomware!g30
- SONAR.SuspLaunch!g18

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Basta
- Trojan.Gen.MBT

**基於機器學習的防禦技術：**

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

## 2023/05/23

## 一箭三雙鵰～YouTube教學影片居然一次就：傳播 Vidar竊密程式、Laplas剪貼簿竊密器(Clipper)、XMRig惡意挖礦程式等三種惡意軟體

攻擊者利用各種人性弱點～使用者渴望免費獲得某些東西而不是透過付費訂閱 YouTube 上的教學。這些用戶會在不知不覺從影片中被引誘安裝所提供連接的竊密程式，並誤信它是合法。實際上不僅給受害者帶來一種威脅，而且還帶來三重威脅。

Vidar 竊密程式就是其中之一，以收集各種機敏資料而聞名。Laplas 剪貼簿竊密器 (Clipper) 也是竊密程式的一種，其主要目的是劫持加密貨幣交易。最後，XMRig 惡意挖礦程式常被用於開採門羅幣 (XMR)。

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。

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Miner.XMRig!gen2
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse

**基於機器學習的防禦技術：**

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

---

## 2023/05/23

## TurkoRat竊密程式偽裝成合法的NodeJS套件管理工具

研究人員透過深入分析發現，看似合法的 NodeJS npm(node package manager) 套件管理工具，實際上會注入一個名為 TurkoRat 的基於開放原始碼竊密程式。只有當惡意軟體被呼叫觸發時，研究人員才能判定實際上是真正有危險的惡意軟體。TurkoRat 能夠竊取數位錢包、密碼、cookie 並修改在受害者電腦內搜查到的 discord 用戶端（及其他）。

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.1

## 2023/05/22

## 網路釣魚攻擊行動持續攻擊Eki-net(日本鐵路車票預訂和管理系統)的用戶

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。它提供一種方便快速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。

賽門鐵克已採取積極措施阻止這些行動，並在 5 月初識別出 30,000 多封與特定行動相關的電子郵件。主旨寫著：“【重要なお知らせ】「新幹線eチケットサービス」えきねっとアカウントの自動退出會處理ニツいテ”（重要提示：新幹線電子票券自動退款服務流程）。詐騙電子郵件假冒提供有關自動退款的資訊。如果毫無戒心的受害者成為此詐騙的犧牲品並點擊電子郵件中提供的網址，他們將被重導到一個用來竊取其敏感資訊的假冒 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。

---

## 2023/05/22

## 防護亮點：攻擊群組矯正

### ～防護亮點～

在世界各地，網路攻擊每天的數量都在不斷增加。且越來越複雜、越來越大膽。網路安全供應商無時無刻都不能忽略它們，否則壞人會找到方法進入。不幸的是，他們有時確實會進入。這使得資安業者需要更迫切的發揮創造力，想方設法打擊網路犯罪分子並保護我們客戶最重要的資產與商譽。

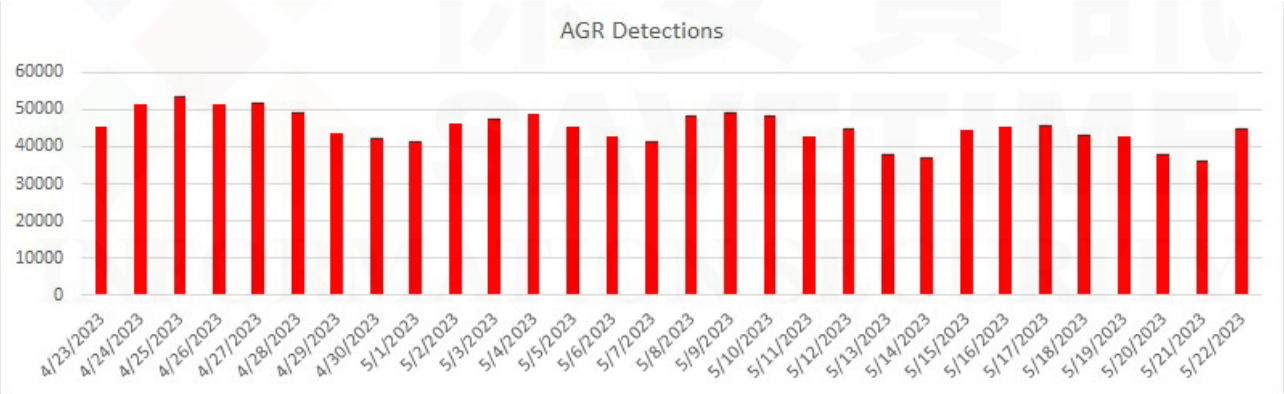
雖然靜態偵測定義檔仍然可以發揮作用並且可能永遠都會發揮作用，但行為偵測無疑是時代的潮流。靜態定義檔就像一個電燈開關--要麼開要麼關，即檔案要麼好要麼壞--行為分析技術可以確定壞的程度。與行為分析相結合可以更加確定該行為是否“足夠糟糕”而需要攔截。補充一點，有時合法但寫得不好的程式碼可能表現得很糟糕，但顯然不應該被攔截。

賽門鐵克行為安全技術致力於保護網路免受無檔案式 (Fileless) 攻擊、就地取材 (LOTL)、與基於行為的攻擊。這些動態技術監控端點上的所有相關活動，了解正常的應用程式行為模式，並經過訓練（個別實際情境）以提醒或快速阻止偏離規範的行為。連同行為分析和系統啟發

(BASH) 和行為政策強制執行 (BPE)，攻擊群組矯正 (AGR) 是這些其中的技術。AGR 是最近推出的一項功能，可識別檢測到攻擊中的所有元件，並確保刪除屬於攻擊的每個程序(Process)和執行序 (thread)。

- 傳統的惡意軟體檢測會阻止或矯正惡意軟體。單就這一點通常就足以有效地阻止攻擊。但未必每一次都有效。
- 惡意軟體通常利用包含多個可供發動就地取材攻擊 (LOTL) 的合法程序的複雜攻擊鏈。如果這些程序中的任何一個仍在執行，即使檢測到並刪除關鍵元件後，攻擊也可以重新啟動或繼續。
- AGR 會套用 BASH 群組功能，以透過追蹤程序譜系、檔案譜系和執行緒插入，將程序和檔案放入動態產生的群組中。只要偵測到惡意軟體，會判定整個群組有威脅。
- 若要判定群組有錯，AGR 會尋找群組中的每個執行中程序，並透過特殊 BPE 特徵來判定每個程序有錯。

每天，AGR 都會終止數十萬個惡意程序 (Process) 並破解多種威脅的攻擊鏈，包括後門程序、加載程序、竊密程序、勒索軟體等。僅在過去 30 天內，我們的遙測系統就記錄超過一百萬個攔截的實例。




我們最近發布一份關於 Mallox 勒索軟體的防護公告，它仍然非常活躍地鎖定全球的企業和組織。顯然針對這種威脅採取多種保護措施（第一時間就攔截任何惡意軟體顯然比為了正確命名而忽略它要好），您會注意到 AGR.Terminate!g2 就是其中之一。為了證明這種行為技術的有效性，我們的惡意軟體分析師測試一些最近的 Mallox 勒索軟體樣本，並確認幾乎所有樣本都被 AGR 捕獲（未被 AGR 阻止的內容被其他檢測阻止而大量被記錄）。好結果應該繼續下去。提升創新及改進速度的永無止境的動力必須繼續下去。

查看先前提到攻擊群組矯正(AGR)公告列表，請點擊此處。

要了解賽門鐵克行為安全性技術如何防禦就地取材(Living Off the Land)的威脅，請點擊此處。

欲深入瞭解更多有關於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。

## 2023/05/22

### CapCut 被冒名模仿成為散播竊密程式的惡意網站

研究人員最近發現幾個冒名模仿成為知名手機影片剪輯神器 CapCut 的網路釣魚網站。CapCut 是抖音 (Tiktok) 官方影片編輯器，利用該 APP 廣受歡迎來從事詐騙攻擊。冒名詐騙的 APP 在下載並執行後會注入各種惡意軟體，包括 Offx 和 Redline 竊密程式。已知 Offx 其一竊密功能是能夠從網頁瀏覽器中取得密碼和 cookie。Redline 能夠獲取儲存在網路瀏覽器和應用程式中的資料，包括憑證、信用卡和自動完成 (Autocomplete) 的資料。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- Trojan Horse
- 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

**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。

---

## 2023/05/19

### 針對人資和行銷部門的最新攻擊行動所利用的Ducktail惡意軟體

Ducktail 是近期知名的竊密程式，早在 2021 年就開始嶄露頭角。廣為人知的感染媒介是鎖定熱門的主流社交媒體帳戶（例如：LinkedIn 或 Facebook Business）為目標，以控制和／或竊取受害者的資訊、瀏覽器連線的cookie……等。利用 Ducktail 發動的最新攻擊行動主要針對人資和行銷部門的用戶。這些攻擊行動背後的攻擊者採用社交工程伎倆，通常讓受害者從上架在熱門的雲端硬碟共享平台（例如：Dropbox 或 Google Drive）下載並執行惡意有效籌載。受害者的機敏資訊會經由 Telegram API 殭屍網路傳送給攻擊者。

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.NPE
- WS.Malware.2

**基於機器學習的防禦技術：**

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

---

## 2023/05/19

## OilAlpha駭客組織鎖定阿拉伯語系的 Android 行動手機用戶為目標

根據最近一份報告，在真實網路環境上發現到鎖定對阿拉伯半島組織的新目標式攻擊活動。被稱為 OilAlpha 的駭客組織針對與沙烏地阿拉伯政府相關的阿拉伯語系之企業以及關注門的政治發展、人道主義組織和非政府組織的人士。使用 Android 的裝置的受害者被引誘下載惡意 APP，這些 APP 被植入 SpyMax 等遠端存取木馬，在某些情況下還注入 njRAT 遠端存取木馬。SpyMax 是一種行動裝置上常見的遠端管理工具 (RAT：remote administration tool)，常被攻擊者拿來濫用發動攻擊，嚴重影響受害者資料的機密性和完整性以及受害者的隱私。它功能強大，被廣泛使用，並且不需要受害者裝置上的 root 權限。

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

**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
- Trojan:Spymax

**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。