
# 保安資訊--本周(台灣時間2023/09/29)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 66 萬 9,100 台受保護端點上總共阻止了 9,060 萬次攻擊。這些攻擊中有 88.1% 在感染階段前就被有效阻止：**(2023/09/25)**

- 在**12萬8,900**台端點上，阻止了**3,860**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**20萬900**台端點上，阻止了**1,610**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬6,600**台**Windows**伺服主機上，阻止了**1,530**萬次攻擊。
- 在**7萬6,300**台端點上，阻止了**330**萬次嘗試掃描伺服器漏洞。
- 在**2萬2,300**台端點上，阻止了**150**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬1,300**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**23萬4,000**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,550**台端點上，阻止了**220**萬次加密貨幣挖礦攻擊。
- 在**12萬3,000**台端點上，阻止了**870**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**1,700**台端點上，阻止了**10萬9,900**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。

## 2023/09/29

## Gotham竊密程式(又稱Pirate 竊密程式)

最近有報導稱，被稱為 Gotham 的竊密程式已被多個駭客組織和個人用於偷渡式下載攻擊。這種威脅實際上只是將 Pirate 竊密程式重新改個名稱而已，其原始程式碼可在公共軟體開發和版本控制代管平台上取得。該竊密程式的功能相當普通，能透過 Discord webhooks 發送的自動訊息來竊取被盜資訊，並具有標準資料竊取的功能，包括竊取個人電腦上的資料、登入憑證、cookie 和來自 Chromium 瀏覽器的表格自動填充資訊。

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：**

- Infostealer

---

## 2023/09/28

## libwebp中的堆積緩衝區溢位漏洞--CVE-2023-4863

CVE-2023-4863 是最近揭露圖形檔案格式 libwebp 中，一個嚴重等級的堆積緩衝區溢位漏洞(CVSS 評分：8.8 高)。該漏洞存在於 libwebp 用於無損壓縮的霍夫曼編碼演算法中。如果開採利用該漏洞，遠端攻擊者可以使用惡意製作的 HTML 頁面執行越界記憶體寫入。此類漏洞可能會產生嚴重後果，例如：未經授權存取敏感資訊以及任意程式碼執行而導致崩潰。

在基於電子郵件的攻擊中尚未觀察到此漏洞，但我們的連結追蹤 (link Following) 和 Webpulse 技術可防止此類型的網頁式攻擊。

CVE 漏洞編號授權單位已拒絕一個名為 CVE-2023-5129 的新漏洞，因為該漏洞與 CVE-2023-4863 重複。

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-2023-4863

**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: WebP Heap Overflow CVE-2023-4863

---

## 2023/09/28

## Zanubis 手機／行動裝置惡意軟體持續鎖定秘魯的銀行和金融機構發動攻擊

Zanubis 是Android 平台上的銀行金融惡意軟體，早在 2022 年就首次出現在威脅環境中。該惡意軟體持續鎖定秘魯的銀行和金融機構發動攻擊。在今年最新的攻擊行動中，威脅者一直將惡意 Zanubis 軟體安裝包偽裝成秘魯政府組織 SUNAT 的官方 Android 應用程式 APP。該惡意軟體

受惠於受害者毫無警覺地向惡意 APP 授予存取權限來控制受害者的裝置。該惡意軟體會監視裝置上目標應用程式的任何執行情況，一旦發現就會進行資料竊取、記錄觀察到的事件或進行螢幕錄製。

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.Malapp
- Android.Reputation.2
- AppRisk:Generisk

---

## 2023/09/28

## Budworm進階持續威脅(APT)組織在針對性攻擊中使用最新版的SysUpdate後門程式

Broadcom 旗下的賽門鐵克威脅獵手團隊觀察到 Budworm 進階持續威脅 (APT) 組織最近所發起的攻擊活動，該駭客集團利用其專有的 SysUpdate 後門程式之最新版本。Budworm 駭客集團 (又稱 LuckyMouse、Emissary Panda、APT27) 採用該工具針對中東的電信公司和亞洲的政府機關。

除了其客製化的惡意軟體外，Budworm 還在這些攻擊中採用濫用系統內建或常用管理工具的就地取材攻擊以及使用網路上常見的和公開的駭客工具。看來該駭客集團的攻擊脈絡可能已在攻擊鏈的初期階段就已鍛羽而瓜，因為從遭入侵電腦上看到的唯一惡意活動只有憑證收集。

在我們的部落格文章中有更詳盡的內容，歡迎參考：Budworm：進階持續威脅 (APT) 組織，採用最新版的客製化工具攻擊政府機構與電信公司

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!g137
- SONAR.TCP!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Hacktool
- Pwdump
- Trojan Horse
- WS.Malware.2
- WS.SecurityRisk.3

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.C
- Heur.AdvML.M

## 2023/09/27

## Exela竊密惡意軟體

Exela 是新發現基於 Python 的竊密程式。Exela 可以從遭入侵的主機中傳送竊得的資料、網頁瀏覽器儲存的資料、cookie、憑證和其他機密資訊。該惡意軟體已被用於針對 Discord 用戶的攻擊行動中，可竄改 Discord 用戶端的設定，以允許資訊竊取功能。該惡意軟體借助 Discord webhook 服務來傳送竊得的資料。

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：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A!100
- Heur.AdvML.A!300
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

## 2023/09/26

## 針對中國、泰國和哈薩克的惡意垃圾郵件中利用了更多惡意的BAT批次檔

.BAT 的批次檔由於其簡單性、也是 Windows 內建的功能、容易隱藏的特性和具有腳本編寫功能…等，長期以來一直被網路上的壞蛋用於各種目的，但主要還是用作載入程式。近幾個月來，在網路威脅情境中常常發現 BatLoader 和 BatCloak 等惡意軟體家族越來越多使用這種伎倆。

在最近一個例子中，賽門鐵克所觀察到的惡意垃圾郵件攻擊行動中，其中一名參與者冒充為提供各種汽車電池的拉脫維亞的電池廠商。惡意電子郵件包含 .IMG 或 .7z 附件，其中隱藏了惡意的 .BAT 批次檔，偽裝成 PDF (在本例中為付款／銀行轉帳通知)。如果受害者成功執行，該 BAT 批次檔將會載入老牌木馬程式 Agent Tesla 。

雖然大多數惡意電子郵件針對中國和泰國的組織，但它們也針對哈薩克的組織。電子郵件和惡意附件是用各自國家的語言編寫／命名的。

觀察到的電子郵件主旨如下：

- 新銀行支付交易通知

- ประกาศการชำระเงินผ่า
- ประกาศ?การชะกาศ?การชำระ?เงินผ่า?นูนา ู?

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)。

**基於行為偵測技術(SONAR)的防護：**

- AGR.Terminate!g2
- SONAR.BatCloak!gen2
- SONAR.SuspLaunch!g84

---

## 2023/09/26

## BunnyLoader初始攻擊程式

通常，懷有惡意的網路壞蛋會盤據在威脅市場中，提供各種服務，例如：網路釣魚工具包、勒索軟體、竊密程式、後門、載入程式、漏洞利用工具等。賽門鐵克始終密切關注地下論壇上的新進者以及監控命令和控制伺服器的動靜。

最近，觀察到以紅色兔子為標誌且名稱為『BunnyLoader』的命令和控制面板。該惡意軟體與一個攻擊者有關，該攻擊者一直將其宣傳為具有竊密程式和剪貼布內容置換功能的初始攻擊程式。然而，它確實沒有比其他已知的初始攻擊程式更獨特得功能。觀察到的活動很可能與測試有關，但我們預計各種團體和個人可能會嘗試將其用於惡意活動，而這些活動的影響程度和流行程度仍不確定。

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.SuspDataRun

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan.Gen.MBT
- Trojan Horse

**基於機器學習的防禦技術：**

- Heur.AdvML.B

## 2023/09/26

## 防護亮點：「置入式行銷」的廣告詐騙／垃圾郵件網路

過去一周，兩起「置入式行銷」的垃圾／詐騙郵件攻擊行動，發送數萬封電子郵件，其內嵌的網址會重導向到詐騙網站，這些網站看起來像是推薦銷售產品的消費者研究部落格。他們提供全球免運費和大幅折扣。點擊結帳頁面會顯示「優惠結束」倒數計時，以推動銷售。

這些垃圾郵件／詐騙惡意行動於 9 月 22 日和 26 日被發現，並且由於時間和內容類型而可能存在關聯。


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已於第一時間收錄於不安全分類列表中。我們現有的垃圾郵件/詐騙郵件防護的特徵檔就能偵測並歸類內嵌的惡意網址。

**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)。

欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲深入瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。

## 2023/09/26

## ZenRAT惡意軟體偽裝成開源密碼管理軟體Bitwarden的安裝檔

ZenRAT 是最近發現的一種 Windows 平台的惡意軟體 (遠端存取木馬)。該惡意軟體偽裝成開源密碼管理軟體 Bitwarden 的安裝檔為幌子進行傳播。感染後，惡意軟體會回報至預先配置的 C&C 伺服器並請求進一步的命令。ZenRAT 具有模組化的版本升級功能、將日誌轉送至 C&C 伺服器甚至協助攻擊者竊取資訊的功能。

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：

**基於行為偵測技術(SONAR)的防護：**

- AGR.Terminate!g2
- SONAR.ProcHijack!g21
- SONAR.SuspBeh!gen625

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1

**基於機器學習的防禦技術：**

- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.A!400
- 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。

---

## 2023/09/26

## Retch勒索軟體

Retch 是一種源於開源的 Hidden Tear 勒索軟體之全新勒索軟體。該惡意軟體能針對預先定義副檔名的檔案進行加密。被加密後的檔案會被冠上 .Retch 副檔名，並附帶 .txt 文字檔的勒索贖金說明，要求受害者以比特幣支付贖金以交換解密金鑰。該勒索軟體的最新樣本已提交給全球多個國家的公共檔案掃描服務，顯示攻擊者並未針對任何特定地區或企業。

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.Cryptlocker!g38
- SONAR.RansomGen!gen3
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan.Gen.MBT
- Ransom.HiddenTear
- Ransom.HiddenTear!g1
- WS.Malware.1

**基於機器學習的防禦技術：**

- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.A!400
- 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

## 2023/09/26

## BBTok銀行金融木馬一直在持續演變

BBTok 是在 2020 年被發現一種惡名昭彰的銀行金融木馬，因其鎖定金融機構的攻擊而迅速聲名大噪，特別是針對拉丁美洲的銀行。該銀行金融木馬，主要在竊取受害者的敏感財務資訊和憑證，使網路犯罪分子能夠進行欺詐性交易並獲得對銀行帳戶的未經授權的存取。

近期被報導的攻擊行動中所出現 BBTok 的新變種是由可自訂的伺服端應用程式所產生。BBTok 幕後的攻擊者採用全新的策略、技術和程序 (Tactics, Techniques and Procedures，TTPs)，同時主要還是依靠網路釣魚電子郵件來擴大該 BBTok 新變種的傳播範圍。他們濫用系統內建或常用合法工具的就地取材攻擊來躲避資安系統的檢查與監控。

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-2022-30190!g1
- Scr.Malcode!gen
- Scr.Malcode!gen104
- Trojan.Gen.MBT

- Trojan.Malscript
- WS.Malware.1
- WS.SecurityRisk.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。

---

## 2023/09/25

## 又是Chaos的變種：NoBit勒索軟體

勒索軟體的威脅一直層出不窮且變本加厲，每天總有人遭受大大小小的勒索軟體威脅。賽門鐵克最近偵測到一種名為 NoBit 的勒索軟體，該軟體針對消費者和企業的個人電腦。他們透過將勒索軟體 (Chaos的變種) 偽裝成假冒的 Microsoft Edge 安裝程式來達到目的。根據勒索信贖金支付的內容，他們似乎並未採取雙重勒索策略，而是要求受害者支付 500 美元的贖金，同時建議受害者透過 Telegram 與他們聯繫。

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.Heur.Dropper
- SONAR.SuspBeh!gen625

**基於機器學習的防禦技術：**

- Heur.AdvML.B

---

## 2023/09/25

## 偵測到安卓平台上的網銀惡意程式Xenomorph的新版本

據報導，在 Android 平台上早就惡名昭彰的銀行金融惡意軟體：Xenomorph，持續在威脅領域發威，最新的版本目前已發現針對 30 多家美國金融機構發動攻擊，並且大有斬獲。這種威脅的行徑與許多其他行動銀行惡意軟體類似，採用經典的覆蓋技術並能夠發動自動轉帳系統 (Automatic Transfer System，ATS) 的攻擊，以竊取受害者的網銀帳號的憑證／帳密。

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。

- AppRisk:Generisk

## 2023/09/25

### 中國駭客組織：EvilBamboo打死不退

中國駭客組織 EvilBamboo 至少自 2019 年起就開始被報導為相當活躍的駭客組織，其特色是持續針對亞洲以及台灣的特定宗教團體和個人開展活動。在最近的多起攻擊行動中，一直濫用各種 Android 間諜軟體（BADBAZAAR、BADSIGNAL 和 BADSOLAR）來收集機敏資訊，就是將其惡意軟體偽裝成上架在假網站上的熱門即時通訊應用 APP 誘使人下載安裝。

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

---

## 2023/09/24

### Alloy Taurus進階持續威脅組織(APT)瞄準東南亞政府機構

在整個 2022 年，Alloy Taurus 進階持續威脅組織 (APT) 不斷試圖監視位於東南亞的政府機構。為了在目標機器中建立立足點，透過 Exchange 伺服器中的漏洞部署大量 Web shell 作為其感染媒介。此外，還安裝後門以便方便隨時存取。此類網路間諜活動可為攻擊者提供針對實體目標的大量敏感資料和智慧財產權 (IP)。

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!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Cobalt!gm1
- Backdoor.Trojan
- Hacktool
- Hacktool.Fscan
- Hacktool.PassReminder
- Trojan.Gen.MBT
- 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.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C
- Heur.AdvML.L
- Heur.AdvML.M

**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。

## 2023/09/24

## 東南亞政府機構被Alloy Taurus進階持續威脅組織(APT)鎖定

自 2021 年以來，由進階持續威脅組織 (APT)：Stately Taurus 又名 (Mustang Panda) 所發起的針對東南亞政府機構的網路間諜攻擊一直在進行，迄今為止仍觀察到類似的行動。

與其他 APT 組織相同，最初部署 Web shell 和後門程式以維持對受害者電腦的存取，然後使用各種工具和技術，允許攻擊者從受感染的網路收集和竊取敏感資訊。

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：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.TCP!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Hacktool
- Hacktool.Mimikatz
- Hacktool.Mimikatz!g4
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.1
- WS.SecurityRisk.4

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.A!300

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C
- Heur.AdvML.M

**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。