保安資訊--本周(台灣時間2025/06/20)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 35 萬 9,500 台受保護端點上總共阻止了 5,530 萬次攻擊。這些攻擊中有 83.7% 在感染階段前就被有效阻止：**(2025/06/16)**

- 在**7萬8,300**台端點上，阻止了**2,630**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬7,300**台端點上，阻止了**580**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,900**台**Windows**伺服主機上，阻止了**610**萬次攻擊。
- 在**4萬8,500**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,200**台端點上，阻止了**81萬800**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,900**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**6萬9,400**台端點上，阻止了**150**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**110**台端點上，阻止了**70萬2,400**次加密貨幣挖礦攻擊。
- 在**13萬2,400**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**474**台端點上，阻止了**7萬600**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。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 17 萬 700 個受保護端點上阻止了總計 780 萬次攻擊。**(2025/06/16)**

- 使用網頁信譽情資，在 **164.5K** 個端點上阻止 **740** 萬次攻擊。
- 攔截 **18K** 個端點上 **271.3K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **4.7K** 個端點上攔截 **124.7K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **181** 個端點上攔截 **2.4K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2025/06/19

銀行／金融惡意軟體：Godfather的全新變種採用虛擬化技術

在真實網路情境裡發現安卓 (Android) 手機／行動裝置平台上的銀行／金融惡意軟體：Godfather 的全新變種。該惡意軟體利用裝置上的虛擬化技術劫持多個合法應用程式。該 Godfather 的全新變種不會像大多數銀行變種那樣顯示一個簡單的偽裝登錄畫面，而是執行一個虛擬化框架，允許它在自己的沙箱中運行已針對行動銀行 APP 的虛擬化副本。這讓攻擊者更能控制虛擬化 APP 的行為，並能更有效率地收集目標敏感資訊。與之前的變種類似，Godfather 仍依賴濫用 Android 的存取服務來執行其惡意行動。

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：

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
- AppRisk:Generisk

2025/06/19

CVE-2023-0386--存在Linux核心所有權管理不當漏洞在在真實網路情境裡遭開採濫用

CVE-2023-0386 是存在 Linux Kernel 高嚴重性 (CVSS 風險評分：7.8) 的所有權管理不當漏洞。雖然此漏洞早在 2023 年就已被揭露，並且已被修補。隨著該漏洞在真實網路情境中已遭大肆開採濫用的報導明顯增加，這一周此漏洞已被加入 CISA 已知已攻擊漏洞 (KEV) 目錄。該漏洞一旦遭開採濫用，攻擊者可能會在易受攻擊的系統上提升權限。

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：

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 的強化功能提供多種方式降低攻擊面和暴露程度，例如：鎖定網路暴露程度，讓有漏洞的裝置無法透過公共網際網路被攻擊。
- 針對此漏洞，賽門鐵克 DCS 為 Linux 伺服器工作負載提供多層次防護。
- DCS 強化的 Linux 伺服器可防止在可寫位置寫入任意檔案，並拒絕執行任何任意程式碼。
- DCS 強化的政策也可以防止所有入埠和離埠連線到伺服器。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/06/19

與駭客組織FIN7有關聯的GrayAlpha駭客組織，使用PowerShell類型的惡意程式載入器和TDS來散播NetSupport遠端存取木馬(RAT)

據報導，與駭客組織 FIN7 有關聯的網路犯罪團體 GrayAlpha 正在發動複雜的惡意軟體攻擊行動，採用多種感染媒介，透過自訂 PowerShell 類型的惡意程式載入器、PowerNet 和 MaskBat 散佈 NetSupport 遠端存取木馬 (RAT)。該組織假冒可信賴的軟體更新頁面和公用程式下載入口，誘騙受害者執行惡意軟體。他們的策略包括偽造瀏覽器更新、偽造公用程式網站和名為 TAG-124 的惡意流量分配系統 (TDS：Traffic Distribution System)。為了避免被偵測到，GrayAlpha 依賴防彈代管主機和模仿合法服務的網域。

網路知識：防彈代管 (bulletproof hosting)，泛指網站服務業者所提供的主機位於司法比較不嚴謹的地區，執法與查核有相當的困難度，這種服務特別受到非法服務的喜愛。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen150

- Scr.xSense!gen3
- Scr.xSense!gen5
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malscript
- Web.Reputation.1
- WS.Malware.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。

2025/06/18

進階持續性威脅(APT)駭客組織：「Librarian Ghouls」發動的全新網路間諜行動

進階持續性威脅 (APT) 駭客組織：「Librarian Ghouls」(又稱為 Rare Werewolf 和 Rezet) 發起一項新的網路間諜行動，主要針對俄羅斯、白俄羅斯和哈薩克的機構，集中在工業組織和工程學校以及火箭、航空、太空、國防和石化產業等領域。

初始的感染媒介包括高度針對性的魚叉式釣魚電子郵件，偽裝成來自可信任組織的合法通訊，並帶有偽裝成官方文件 (例如：付款通知) 的密碼保護檔案。當接收者使用電子郵件本身一般提供的密碼開啟這些檔案，然後擷取並執行隨附的有效酬載，感染鏈就開始了。

一旦受害者開啟壓縮檔，就會開啟自解檔安裝程式，進而使用系統公用程式來隱藏和執行惡意程序。在感染鏈的末端，威脅者會竊取敏感資料，並在受害者系統上部署加密貨幣挖礦程式。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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

2025/06/18

傳播DeerStealer惡意竊密軟體的網路攻擊行動，同時借力HijackLoader惡意程式載入器

最近發現有攻擊行動利用 HijackLoader 惡意程式載入器散佈 DeerStealer 惡意竊密軟體的有效酬載。攻擊者利用 ClickFix 社交工程伎倆，引誘毫無戒心的受害者下載惡意 .msi 安裝程式，進而執行 HijackLoader。威脅者利用 DeerStealer 有效酬載從遭入侵的主機收集和滲透各種敏感資訊，包括瀏覽器儲存的資料、加密貨幣錢包、cookie、剪貼簿資料、憑證、銀行資訊或自動填寫資料等。惡意軟體還為攻擊者提供隱藏 VNC 的功能，允許未經授權的遠端控制連線。

網路知識：ClickFix 為「複雜的社交工程手法」，偽裝成系統錯誤訊息或文件註冊提示，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- 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：

- Audit: Bad Reputation Application Activity
- 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。

2025/06/18

程式碼共享平臺Paste.ee遭濫用，駭客利用Unicode欺騙攻擊，散布XWorm遠端存取木馬(RAT)

我們觀察到一個複雜的惡意軟體攻擊行動，該攻擊行動是由一個易於引誘人受騙的檔案名稱之 JavaScript 檔案所引爆，其目的是為了下載惡意的有效酬載。攻擊鏈開始於散佈偽裝成傳送通知的惡意 JavaScript 檔案釣魚電子郵件。腳本以不尋常的 Unicode 字元偽裝，與合法服務 paste.ee 聯繫，以取得並執行惡意軟體感染下一階段的程式碼。此有效酬載被識別為 XWorm 遠端存取木馬 (RAT)，能夠記錄按鍵、資料外洩，並在受感染的系統上建立持久性／常駐能力的後門。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen40
- MSIL.XWorm!gen2
- Scr.Malcode!gdn*
- Scr.xSense!gen*
- Web.Reputation.1
- Web.Reputation.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

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

2025/06/18

XDSpy攻擊行動採用經混淆空白LNK捷徑檔的伎倆

全新的 XDSpy 惡意軟體攻擊行動是由 SadFuture 威脅份子所為，目標是東歐和俄羅斯的政府單位。威脅者利用篡改過的 Microsoft Windows 捷徑 (LNK) 檔案引爆攻擊鏈，以嵌入過多空白掩蓋的混淆惡意指令。一旦被執行，LNK 檔案會傳送 ETDownloader，隨後會取得 XDigo 後門 (一個採用 Go語 言撰寫的惡意軟體)。XDigo 會建立加密的 C&C 通訊，收集敏感資料 (包括螢幕截圖和剪貼簿內容)，加密資料並將其滲透到 C&C 伺服器。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.NSISPacker!g14
- Scr.Mallnk!gen6
- 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!400
- Heur.AdvML.A!500

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: Bad Reputation Application Activity

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。

2025/06/17
防護亮點：木馬程式Masslogger再度成為駭客圈青睞的焦點

木馬程式Masslogger 重出江湖

木馬程式 Masslogger 至少從 2020 年就開始活躍，這幾個月來全球各地的各種威脅組織和獨立行動者利用這隻惡意程式所發動攻擊明顯增加，目標是各行各業以及公共組織。

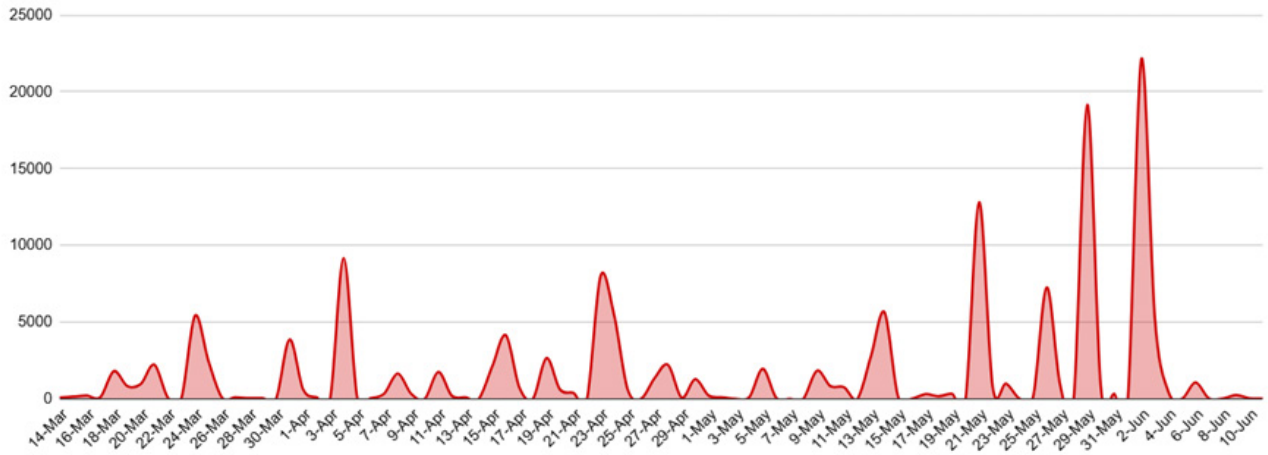
雖然不同的攻擊行動和攻擊者所偏愛的戰略多所不同，但 MassLogger 涉入的攻擊始終遵循一種有跡可循的模式：社交工程的網路釣魚電子郵件、隱蔽的執行技術，以及從受感染的系統中擷取敏感憑證。

在透過電子郵件發動初始攻擊後，大多數的攻擊行動會採用直截了當的方法--以詐術附加壓縮檔內含木馬程式 Masslogger 的二進位檔案。然而，更老練的攻擊者通常會擴充此方法，利用 JavaScript、VBScript、Batch 或 PowerShell 等腳本式的惡意程式載入器，以及 NSIS 和 SCR 等可執行格式的替代方案，來繞過安全軟體的偵測並提高有效酬載的執行成功率。

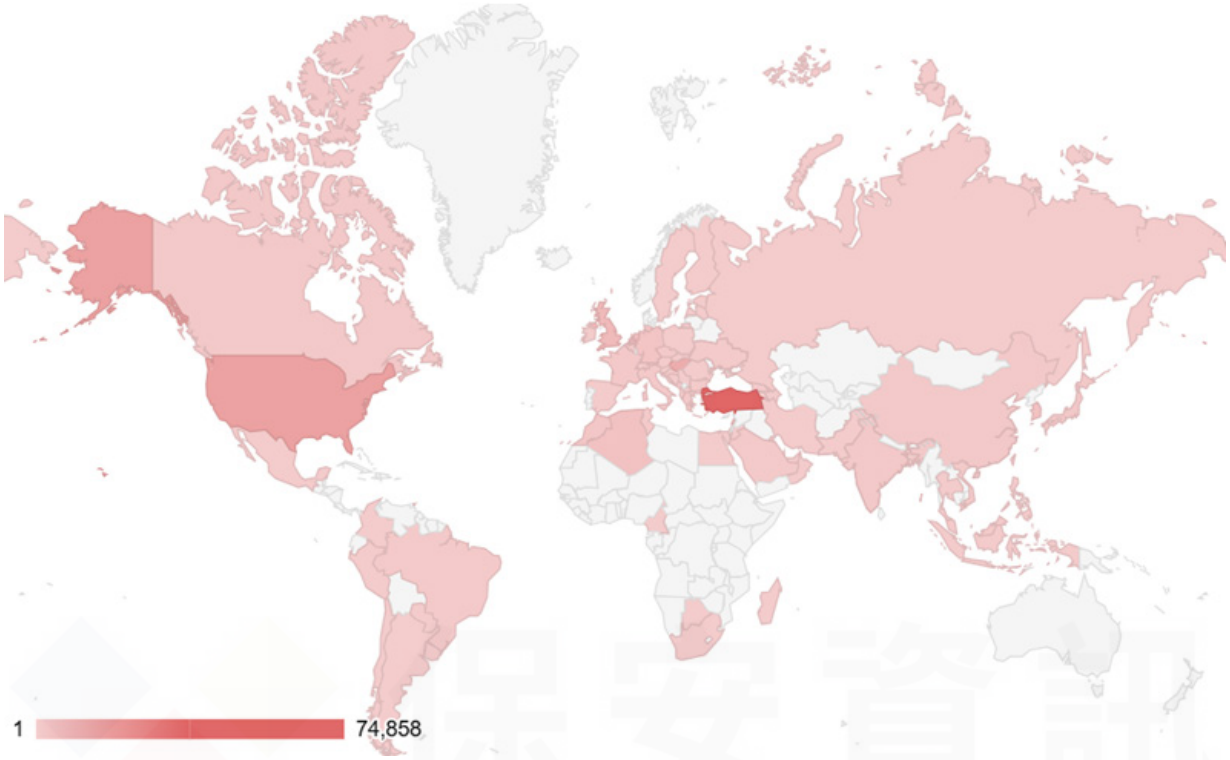
在過去半年，MassLogger 活動一直持續，並在多個地區觀察到幾次急劇的飆升。我們的資料顯示，儘管每日的偵測通常持平，但週期性的峰值 (特別是在五月底和六月初)，顯示出較大的波動。

土耳其是最受影響的國家，防毒引擎偵測到的次數超過 74,000 次，其次是美國以及數個歐洲和拉丁美洲國家。此分佈情況顯示廣泛的機會主義目標策略，很可能是利用當地化的誘餌和利用遭入侵的基礎設施進行傳送。

MassLogger 偵測趨勢



MassLogger 偵測熱圖



鎖定憑證為目標

MassLogger 是一款普通的憑證竊取惡意軟體，其設計目的是在嘗試滲透敏感用戶資料時隱藏其行蹤。它的目標是廣泛的憑證來源，包括網頁瀏覽器、電子郵件用戶端 (例如：Outlook 和 Thunderbird)、FTP 應用程式 (例如：FileZilla)、VPN 軟體等。

此威脅支援多種通訊方法做為外洩手段。常見的技術包括透過 SMTP(電子郵件) 傳送竊取的資料、透過 FTP 上傳或使用 HTTP POST 請求傳送至攻擊者控制的伺服器。在某些自訂變種中，攻擊者透過利用 Telegram Bot API 將 MassLogger 配置為使用 Telegram bots 來滲透日誌。這可讓惡意軟體直接將竊取的資料傳送到操作者的聊天帳戶，使用加密且看似合法的 HTTPS 流量，試圖繞過防火牆並逃避網路監控。

MassLogger 操控者最近使用的 Telegram 殭屍權杖範例：

- bot7341689230:AAHymAZAjTKDwQdX3qK2HITohVFwhbvLPIc
- bot7398536732:AAFG_GQm2-o0UoJEIV0aVrSPCtyqz5VEliU
- bot7646451386:AAGgex98cq9UD2k8MPa66b
- bot8004081294:AAEeQb3kkdq-mgW3gSkEAnMJX0fU078688E
- bot8185619395:AAFoycueqDVSZD7Vj-U3AfAuKB5byVNAYJU。

對應 MITRE ATT&CK 框架的攻擊戰略

以下是最近觀察到的木馬程式 Masslogger有效酬載對應到 MITRE ATT & CK 框架的戰術和技巧：

- 執行 (TA0002)：透過排程任務／工作 (T1053)、指令與腳本編譯器 (T1059)，特別是 PowerShell (T1059.001、T1086) 與 base64 編碼的有效酬載執行惡意行為。同時利用 Native API (T1106) 和 Shared Modules (T1129) 來動態載入和執行程式碼。

- 持續性／常駐能力 (TA0003)：透過排程任務／工作 (T1053) 和註冊表 Run 機碼／啟動資料夾 (T1060、T1547.001) 建立持續性，將惡意指令碼置入啟動目錄。此外，它還會修改註冊表 (T1112)、建立或操控 Windows 服務 (T1543.003)，並包含使用 Bootkits (T1542.003) 的預先作業系統啟動 (T1542) 支援。
- 權限提升 (TA0004)：透過程序注入 (T1055) 和存取權限操控 (T1134) 獲得提升的執行權限。也會使用「建立或修改系統程序」(T1543) 及「開機或登入自動啟動執行」(T1547) 維持系統層級服務的持續性。
- 防禦規避 (TA0005)：使用 Rootkit (T1014) 元件、混淆檔案或資訊 (T1027)、軟體封裝 (T1027.002、T1045) 及程序注入 (T1055) 來避免偵測。它會在執行時解除混淆內容 (T1140)、隱藏惡意視窗 (T1143、T1564.003)，並採用指標刪除 (T1070)、修改註冊表 (T1112) 和停用或修改工具 (T1562.001)。它還運用反射式程式碼載入 (T1620)，並使用隱藏檔案和目錄 (T1564.001) 隱藏生成物。
- 憑證存取 (TA0006)：嘗試透過作業系統憑證轉存 (T1003)、檔案中的憑證 (T1081) 及註冊表中的憑證 (T1214) 收集憑證。它會搜尋不安全的憑證 (T1552)，且會竊取 Web Session Cookies (T1539)。
- 搜尋 (TA0007)：查詢註冊表 (T1012)、搜尋系統網路組態 (T1016)、執行進程搜尋 (T1057)、系統資訊搜尋 (T1082) 以及檔案與目錄搜尋 (T1083)。它還會檢查已安裝的軟體 (T1518)，並透過偵錯程式偵測使用沙箱規避技術。
- 收集 (TA0009)：使用本機系統資料 (T1005)、電子郵件收集 (T1114) 和自動收集 (T1119) 收集敏感檔案和資料。收集的資料會透過 (T1560.002) GZip 進行壓縮。
- 指揮與控制 (TA0011)：透過應用層通訊協定 (Application Layer Protocol，T1071) 建立 C2 通訊，使用動態解析 (Dynamic Resolution，T1568) 建立彈性的基礎架構，並使用加密通道 (Encrypted Channel，T1573) 加密通訊。
- 影響 (TA0040)：可透過資料破壞 (T1485) 進行破壞行動，並可能從事資源劫持 (T1496)，影響系統效能或可用性。

Symantec 的防護

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g483

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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：

- CL.Suspexec!gen*
- Downloader
- Hacktool
- ISB.Downloader!gen*
- ISB.Heuristic!gen*
- ISB.Houdini!gen7
- JS.Redirector
- MSIL.Packed.*
- Packed.NSISPacker!g*
- Phish.ScptML.L
- Scr.Malarchive!gen*
- Scr.Malcode!gdn*
- Scr.Malcode!gen*
- Scr.Mallnk!gen*
- Scr.xSense!gen*
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Malautoit!g*
- Trojan.Malcab
- Trojan.xSense.C
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A

- 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：

- Wudit: Untrusted Telegram API Connection

欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，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攻擊的威脅，請點擊此處。
欲了解 Carbon Black Endpoint，請點擊此處。
欲了解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。
欲深入了解更多有關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。
欲深入了解更多有關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。
欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。
欲了解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

2025/06/17

假冒金融機構的電郵通知，引誘台灣使用者下載惡意軟體

有威脅份子透過偽裝成金融單位的官方通訊，針對台灣使用者進行攻擊。該組織發送的惡意電子郵件正文或附件中含有連結，目的是傳送 Gh0stCring、HoldingHands 或 winos 惡意軟體家族的有效酬載。其他詳細資訊請參閱 Fortinet 的報告。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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!gen

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Pidief
- WS.Malware.1
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2025/06/17

CVE-2025-48828--新發現存在商業化的網路論壇軟體套件：vBulletin的遠端程式碼執行(RCE)漏洞

CVE-2025-48828 是一個最近被揭露的影響 vBulletin(一個商業論壇軟體平台) 的嚴重 (CVSS 風險評分：9.0) 範本引擎漏洞。此漏洞遭遭攻擊者開採濫用，可讓攻擊者使用精心製作的條件將惡意 PHP 程式碼注入 vBulletin 的範本。CVE-2025-48828 漏洞與另一個 vBulletin 漏洞 (CVE-2025-48827) 一起使用的話，會在受影響的實例上導致完全遠端執行程式碼。

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: vBulletin CVE-2025-48828

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就內建的系統鎖定政策可保護底層作業系統伺服器免受此漏洞攻擊，包括防止執行任意指令，以及限制讀取重要作業系統檔案的存取權限。此政策也會阻擋上傳任何惡意的 PHP webshell。
- DCS 預設防禦政策透過封鎖所有入埠和離埠連線，防止攻擊者存取有漏洞的系統。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/06/17

義大利PEC郵箱的用戶，正面臨MintsLoader惡意軟體的攻擊

一起全新的 MintsLoader 惡意軟體攻擊行動正在鎖定義大利，展示攻擊者貼近義大利政府行政機關辦公日曆表的策略。該攻擊活動在週三而非慣常的週一發動，以配合義大利國定假日後工作週的開始。這種延遲每週第一個工作天的策略，目的是在使用者完成當周重要工作後的短暫休息後讀取電子郵件時，較沒警覺心，針對他們進行攻擊，以達到最大的效果。該攻擊行動利用遭入侵的 PEC(Posta Elettronica Certificata) 信箱來散佈惡意軟體，典型的是惡意竊密程式，使用的是 PowerShell 類型 MintsLoader。攻擊鏈包括附件有經混淆 JavaScript 檔案連結的電子郵件、動態網域生成 (DGA)，以及透過 PowerShell 指令碼傳送的有效酬載。

網路知識：PEC 郵箱是一款專門為企業量身定制的電子郵件服務，其全稱為“Posta Elettronica Certificata”，意為“認證電子郵件”，是義大利政府推出的一項郵件認證服務。PEC郵箱提供安全可靠的電子郵件收發，同時通過獨特的驗證機制，確保郵件內容的合法性和真實性。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!aat171
- Scr.Malscript!gen31
- Scr.xSense!gen3
- Web.Reputation.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。

2025/06/16

Pickai後門程式

有人觀察到一款名為 Pickai(AI Pickpocket) 全新後門惡意軟體透過流行 ComfyUI 框架中的漏洞進行傳播。Pickai 以 C++ 寫成，透過 JSON 和 TMUX 設定等看似無害的設定檔進行傳播。一旦被執行，它就會啟用遠端指令執行、建立rebound shell，並使用反偵錯與程序偽裝技術來達到隱身與持續性的目的。其主要目標是從受遭入侵的系統中竊取敏感的 AI 相關資料。P.S.ComfyUI 可以讓使用者利用拖曳的方式來建立圖片生成之工作流程。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.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。

2025/06/16

駭客利用合法的遠端存取工具「Netbird」，進行針對財務長們的網路釣魚行動

據觀察，一起全新的偽造招聘人員魚叉式網路釣魚攻擊行動鎖定非洲、加拿大、歐洲、中東和南亞各地的銀行、能源公司、保險公司和投資公司的高階金融主管。攻擊者假冒 Rothschild & Co. 的招募人員，使用多階段攻擊來安裝一個名為 Netbird 的合法遠端存取工具。感染鏈從一封釣魚郵件開始，目的是引誘收件人打開包含鏈結的 PDF 附件。此連結會引導至一個自訂的圖靈 (CAPTCHA) 驗證機制，當解開此連結時，會重定向至一個隱藏的網頁，最終下載一個 ZIP，解壓縮為一個 VBS 腳本。一旦安裝並執行，Netbird 就會為攻擊者提供對受害者系統的持久隱藏存取權 (長期被監控)。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- ISB.Downloader!gen*
- Scr.Malcode!gen
- Scr.xSense!gen*
- Web.Reputation.1
- 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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。