危險迫在眉睫：
今日的漏洞將為明日的攻擊揭開序幕

TrendLabs℠ 2015 年第三季資訊安全總評

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

內容

4

資料外洩助長駭客攻擊和恐嚇勒索

8

最新攻擊再次突顯 iOS 和 Android 平台現有的問題

11

亂槍打鳥式 PoS 惡意程式攻擊造成越來越多中小企業受害

14

本季重大事件

20

威脅情勢回顧

我們已經走到一個任何東西都有可能遭到駭客攻擊的轉捩點。過去一季所出現的資安事件，恰巧突顯出行動裝置生態體系、連網裝置以及網路基礎架構等等當前的安全漏洞有多麼嚴重。如同地震儀上接收到震波很可能代表地震即將來臨，這些安全漏洞也很可能為 2016 年即將來臨的大規模衝擊事件揭開序幕。

我們看到重大資料外洩事件開始朝個人化發展，而且獲利更為驚人。駭客將不利於被害人的祕密資訊上傳到網路公共空間，不僅讓企業和個人遭受名譽上的損失，更使其喪失公信力。我們看到資料外洩的衝擊和後續效應 (也就是連帶引發的攻擊) 非常嚴重。例如，在 Hacking Team 駭客公司資料外洩事件之後即爆發一連串的系統漏洞出現。此外，恐嚇勒索也甚囂塵上，網路犯罪集團利用 Ashley Madison 偷情網站外洩的資料來恐嚇取財。相信未來的資料外洩事件很可能將依循同樣的模式發展。駭客未來勢必將洩漏更多機密資料與具毀滅性的資訊到網路公共空間，或者拿到深層網路 (Deep Web) 地下市場標售。

「亂槍打鳥」的攻擊方式，仍將是駭客創造更多受害者的有效手段。駭客已證明中小企業 (SMB) 是一群能讓歹徒賺取豐厚利潤的對象，因此針對中小企業的攻擊未來仍將層出不窮。此外還有針對知名人士 (如政治人物) 的攻擊，也將成為後續針對性攻擊 (或稱鎖定目標攻擊) 的跳板。

行動裝置平台及連網裝置當前的安全漏洞，將持續成為駭客鎖定的目標，這不僅將侵犯使用者的隱私，更可能危及使用者的人身安全。未來，裝置製造商必須和資安專家共同合作，才能確保產品和使用者的安全。

註：文中所有提到「偵測」一詞的之處，皆指趨勢科技安全防護產品在使用者裝置上發現並攔截到的威脅。除非另有說明，否則本報告當中的數字皆來自趨勢科技 Smart Protection Network™ 雲端防護基礎架構所蒐集之資料。該基礎架構結合了雲端與用戶端技術來支援企業內安裝的產品以及雲端代管式服務。

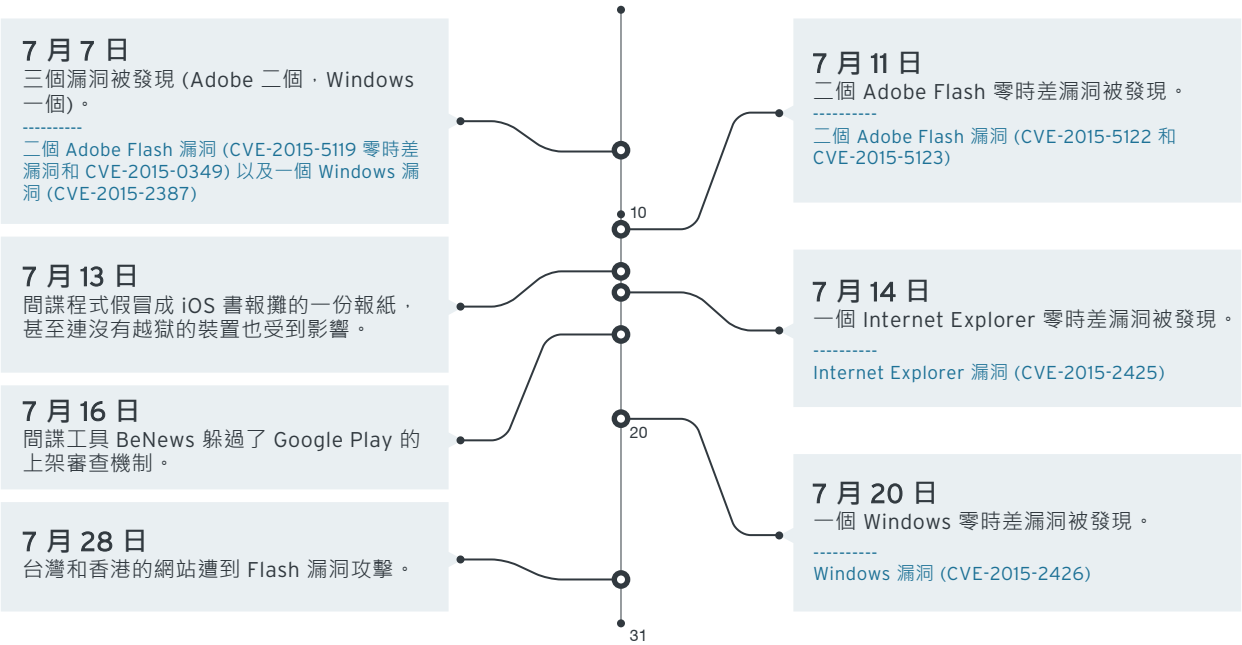
資料外洩助長駭客攻擊和恐嚇勒索

本季發生的資料外洩事件引發了一連串的後續攻擊。未來，駭客攻擊很可能依循 Ashley Madison 和 Hacking Team 資料外洩事件的相同模式，將資料外洩當成攻擊手法當中的一環，把竊取到的機密資訊外洩到網路公共空間，造成受害者名譽損失。這種手法所造成的損害，比毀損企業網站門面或分散式阻斷服務攻擊 (DDoS) 所造成的業務中斷更為嚴重。

Hacking Team 資料外洩：有如一座滿是系統漏洞的寶藏

去年七月，一家名為 Hacking Team 的義大利駭客公司宣稱其超過 400GB[1] 的機密資料遭駭客外流到網路公共空間。這些遭駭客竊取的資料當中，包含了該公司的一些機密資訊。Hacking Team 外洩事件之所以特殊，是因為這些外洩的機密能讓其他駭客掌握一些新的安全漏洞來攻擊企業基礎架構。

Hacking Team 攻擊時間表



七月份當中有多個零時差漏洞攻擊以及一個間諜工具因為 Hacking Team 資料外洩事件而出現，這些漏洞攻擊一旦成功，很可能帶來嚴重的災難。此外，台灣和香港的多個網站也遭駭客入侵並用來散布 Adobe® Flash® 漏洞攻擊。

在 Hacking Team 外洩的資料當中，目前總共被發現了五個漏洞 (其中有三個是我們所發現)，分別位於 Adobe Flash、 Internet Explorer® 及 Microsoft™ Windows®。截至今年七月為止，這些漏洞至少影響了 10 億台裝有 Adobe Flash 的裝置[2]。而 Windows 的漏洞則使得大約 78% 的桌上型電腦 (也就是含有漏洞的作業系統) 使用者陷入危險[3]。至於 Internet Explorer 11 的漏洞，則大約影響了 27% 的桌上型電腦瀏覽器使用者[4]。Flash 零時差漏洞 (CVE-2015-5119)[5] 已被整合至 Angler 和 Nuclear 漏洞攻擊套件[6]，並且用於攻擊韓國及日本的企業機構[7、8]。台灣及香港一些政府機關和媒體的網站[9] 也因為 Flash 漏洞的關係而遭到入侵，這也是 Hacking Team 外洩事件的後遺症之一。

在 Hacking Team 外流的資料當中，也包含了該公司的手機間諜程式：Remote Control System Android (RCSAndroid) 的原始程式碼。該程式可說是有史以來最專業、最精密的 Android 惡意程式[10]。RCSAndroid 的資料竊取功能包括：即時擷取螢幕畫面和語音通話、擷取 Facebook、Viber 和Skype 等應用程式的密碼與訊息內容。

不僅如此，Hacking Team 資料外洩也可能讓不知情的 iPhones® 使用者 (不論其裝置是否已越獄) 將一份假冒的報紙加到書報攤程式當中[11]。這份報紙會要求使用者提供權限來讓它存取裝置上儲存的各類型資料。不久之後，一個類似的應用程式「BeNews」也出現在 Android™ 平台[12]。BeNews 不僅能避開裝置的安全機制，還成功躲過了 Google Play™ 的審查。

Ashley Madison 資料外洩：性、謊言、勒索

Ashley Madison 偷情網站資料外洩事件因為該網站的性質特殊而引發軒然大波[13]。駭客激進團體 Impact Team 更是把握機會好好善用該網站會員的致命把柄 (偷情)。這項資料外洩事件不僅是 Avid Life Media 公司 (網站經營者) 的災難，更讓 Ashley Madison 的 3,000 多萬會員陷入泥沼當中[14]，甚至傳出有受害者因而自殺[15]。

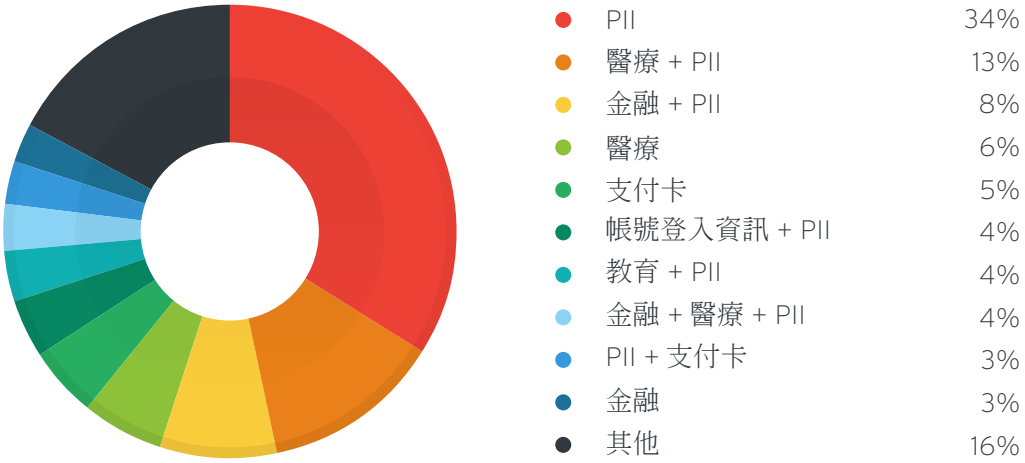
駭客很快就利用這些外流的會員資料進行一波波的勒索行動[16]，駭客透過黑函來恐嚇這些會員，並對他們勒索 1 比特幣 (相當於 291 美元) * 的贖金，不然就要將他們的秘密公開給親朋好友知道。不僅如此，我們甚至還在 Ashley Madison 的使用者帳號資料當中發現了一些趨勢科技用來誘捕駭客的電子郵件帳號和 IP 位址[17]。

任何人都有可能成為資料外洩的受害者。使用者在網路上公開的任何資訊，不曉得哪一天會遭到歹徒竊取並用於不法用途。正如 Ashley Madison 的案例告訴我們，企業資料外洩事件最後有可能演變成個人事件，而且對歹徒來說，同樣有利可圖。

** 使用 2015 年 10 月 27 日的匯率 (1 比特幣 = 291.31 美元)*

醫療機構：歹徒入侵得逞

今年九月有多家醫療機構遭到入侵，例如醫療保險公司 Excellus BlueCross BlueShield (BCBS) 據報在最近兩年之內連續遭到多次襲擊[18]。此外，UCLA Health System 的駭客攻擊事件也有大約 450 萬名病患的個人資料遭到外流[19]。這兩起案例點出醫療機構的病患資料庫正是歹徒覬覦這些機構的原因[20]。此外，趨勢科技的報告「跟著資料循線追查：各產業資料外洩情況分析」(Follow the Data: Analyzing Breaches by Industry)[21] 也指出，醫療和個人身分識別資料 (PII) 是資料外洩事件當中最常遭竊的兩大資料類型，這樣的情況未來勢必將會延續下去。



醫療資料 (醫療紀錄、保險資料等等) 與個人身分識別資訊 (PII) 是最常失竊的兩大資料類型。

Hacking Team 和其他醫療產業的資料外洩，突顯出漏洞管理扮演著相當關鍵的角色。企業機構無時無刻都應提防自己的網路及內部資料遭到任何攻擊。

「網路環境正日益惡化，而且攻擊不再只是單一事件。企業必須調整自己的資安事件應變計畫來應付第二階段的攻擊，包括二次感染或利用偷來的資訊進行恐嚇勒索。抑制駭客的入侵行動將成為事件應變的目標，企業必須盡可能降低駭客潛伏的時間，必須破壞駭客在主機上建立據點的能力，進而防止駭客發動二次感染。透過虛擬修補，再加上入侵偵測與安全資訊與事件管理 (SIEM) 及檔案一致性監控系統的整合，將是遏止 2016 年嚴重攻擊的關鍵。」

—Tom Kellermann

網路安全長

最新攻擊再次突顯 iOS 和 Android 平台現有的問題

Android 平台被發現的媒體伺服器 (Mediaserver) 系統元件漏洞，突顯出 Google、裝置製造商以及電信業者之間的資安策略需要更加整合。而 Apple 的應用程式開發工具 Xcode 和 Unity 遭到竄改，也破除了 iOS 光靠嚴格把關就能防止裝置遭到駭客攻擊的迷思。駭客隨時都在尋找資安漏洞來攻擊行動裝置使用者 (不論何種平台)，這也讓原本已經不斷倍增的行動惡意程式數量更加速成長。

Android 的最新危機：媒體伺服器元件漏洞

Android 的媒體伺服器 (Mediaserver) 是專門負責處理多媒體相關工作的系統元件，最近已成為駭客積極攻擊的目標 (未來情況應該也不會有所改變)，光是過去這一季就有五個漏洞遭到駭客攻擊。

Stagefright[22] (CVE-2015-3824) 就是一例，此漏洞可讓駭客利用一個多媒體簡訊 (MMS) 在有漏洞的裝置上安裝惡意程式，全球約 94.1% 的 Android 裝置 (截至今年七月為止) 都陷入危險當中。此外我們也發現了一個可能讓 Android 手機完全毫無反應，無法打電話或傳簡訊的漏洞[23]。根據報告指出，大約 50% 以上的 Android 裝置 (截至今年七月為止)[24] 都有這項漏洞。此外還有另一個嚴重的多媒體伺服器漏洞 (CVE-2015-3823)[25] 可能造成裝置一直不斷重新開機，並且讓駭客從遠端執行任意程式碼。在漏洞發現當時，約有 89% 的 Android 裝置可能遭到這項漏洞攻擊。最後一個是八月份出現的 CVE-2015-3842 漏洞，此問題出現在多媒體伺服器的 AudioEffect 元件當中，可讓駭客從遠端執行程式碼[26]。

為了因應最近突然暴增的 Android 漏洞，Google 終於宣布未來該平台將定期發布安全更新[27]。不過，就目前該平台更新流程零散而缺乏整合的狀態來看，我們不知道這項計畫將如何實現。若沒有裝置製造商和電信業者的配合，這些安全更新根本無法普及到所有裝置，結果裝置的漏洞依然存在。

遭到竄改的開發工具以及軟體漏洞：iOS 百密仍有一疏

Apple 一向以嚴格把關聞名，其應用程式的上架審查程序較為嚴格，應用程式也相對較為安全。不過這樣形象最近卻因為官方 App Store 及非官方應用程式商店有多款 iOS 應用程式遭駭客植入名為「XcodeGhost」的惡意程式碼而粉碎[28]。這些含有惡意程式碼的應用程式可能出現的不良行為包括：詐騙、網路釣魚，甚至竊取資料。

根據調查，此事件是因為有多家中國的 iOS 應用程式開發廠商從網路論壇下載了遭人竄改的 Xcode 開發工具來製作自己的應用程式。這些廠商並不曉得他們所使用的開發工具已被植入惡意程式，因此才會讓自己的產品遭到感染。根據趨勢科技 Smart Protection Network 全球威脅情報網的資料顯示，中國是此威脅肆虐最嚴重的地區。同樣地，2D 和 3D 遊戲開發平台 Unity 也遭到了同樣不幸的命運，被駭客植入了所謂的「UnityGhost」。

此外，iOS 的 AirDrop® 功能[29] 也成了歹徒攻擊的另一個目標。甚至就連未設定接受 AirDrop 檔案傳輸的裝置也會受到相關漏洞波及。還有另一個叫做「Quicksand」[30] 的 iOS 漏洞也被發現可能洩漏行動裝置管理 (MDM) 用戶端傳輸的資料，因此，不僅個人資料、就連企業資料也可能受到威脅。

針對上述問題，Apple 都已迅速解決。該公司已將有問題的應用程式從 App Store 下架。不過，由於該平台的用戶越來越多，未來勢必將有更多的 iOS 威脅出現。駭客將不斷發掘更多可避開 Apple 嚴格審查機制、打破其封閉世界的方法。此外，一些可同時攻擊個人和企業的跨平台威脅，如 WireLurker[31] 和 Masque[32]，勢必也會不斷出現。

「Apple 不斷成長的市占率已吸引駭客投入更多的心力來發掘 iOS 應用程式的漏洞。Apple 嚴格的 iOS 應用程式上架審查政策，反而讓駭客想出一些更聰明的招數，例如透過感染開發工具和程式庫來達到相同目的。未來，我們勢必看到更多『Ghost-XXX』之類的威脅出現。此外，駭客也可能利用竄改憑證和應用程式開發介面 (API) 的方式來散布 iOS 惡意程式。為此，Apple 必須不斷訂定更嚴格的應用程式上架審查政策才行。」

—Ju Zhu

行動威脅研究員

亂槍打鳥式 PoS 惡意程式攻擊造成越來越多中小企業受害

本季證明了中小企業是銷售櫃台系統 (PoS) 惡意程式既容易得逞又獲利頗豐的攻擊目標[33]。這很可能是因為這些企業同樣也含有大量的客戶資料庫，但卻僅有少量的安全防護措施，有時甚至沒有。未來，我們將看到越來越多這類攻擊。而新一代的支付技術，例如：EMV (Europay、MasterCard、Visa)[34] 技術、感應式 RFID 晶片信用卡[35]、行動錢包 (Apple Pay®[36] 和 Android Pay™[37])，以及最新的支付交易處理架構[38] 目前的普及速度依然緩慢，同樣也不利於交易安全的發展。

亂槍打鳥：有效的 PoS 惡意程式散布方式

本季，駭客使出渾身解數，盡可能散發大量的 PoS 惡意程式來試圖提高命中機率。他們採用一些歷久不衰的手法，例如垃圾郵件、巨集惡意程式、漏洞攻擊套件，以及殭屍網路。而他們的作法顯然奏效，因為 PoS 惡意程式偵測數量大幅成長了 66%。其中，中小企業受到的打擊最為嚴重，因為他們的防護措施遠比大型企業來得弱。

一個 PoS 記憶體擷取程式在 Angler 漏洞攻擊套件[39] 的幫助下感染了不少裝置，該套件專門利用惡意廣告和已遭入侵的網站來散布。此外，駭客更利用一個不需透過檔案安裝的木馬偵查程式來躲避偵測，成功感染了 PoS 裝置。無檔案的惡意程式會躲在一般防護軟體不會掃瞄的地方。

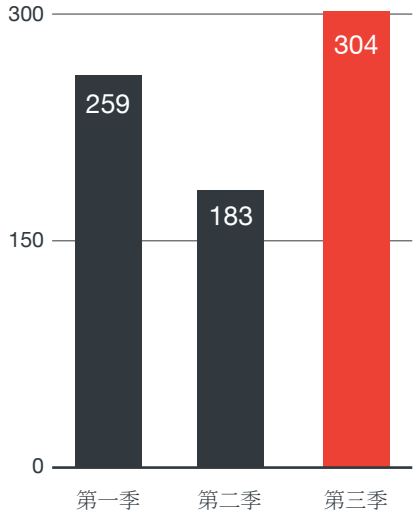
今年七月，一個新的 GamaPOS 變種[40] 利用 Andromeda 殭屍網路以及「炸魚」的方式大量散布。炸魚原本是漁夫們為了方便捕魚而使用炸藥來震暈或震死魚群再撿拾漁獲的手法。駭客們也如法泡製，盡可能轟炸他們所蒐集到每一個電子郵件地址來提高惡意程式進入 PoS 系統的機率。這些垃圾郵件會挾帶含有巨集惡意程式的附件檔案，或者指向已入侵網站的連結。根據我們的資料顯示，這類威脅的影響遍及美國 13 個州及加拿大的一個城市。

Kasidet[41] (或稱 Neutrino) 惡意程式本季也開始具備 PoS 記憶體擷取能力。Kasidet 是一款公開販售的開發工具，以分散式阻斷服務攻擊 (DDoS) 能力聞名。Kasidet 最近也利用暗藏惡意程式的垃圾郵件感染了 PoS 系統，其最近一波攻擊更占了本季 PoS 惡意程式偵測總數的 12%。

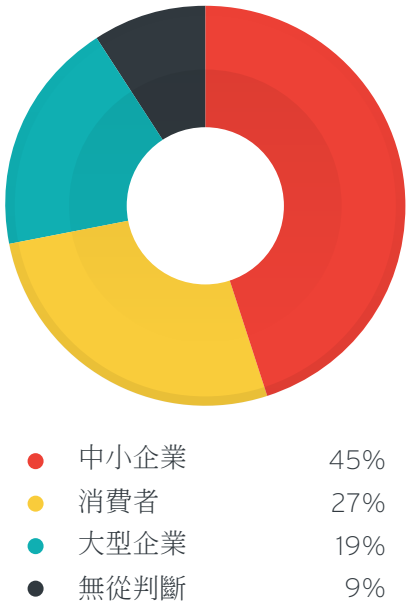
中小企業：PoS 惡意程式偏愛的攻擊目標

上一季，我們認為 PoS 記憶體擷取程式已到達飽和點，因為當時的偵測數量已大幅下滑[42]。但這一季情勢逆轉，並且以中小企業為主要受害目標。

PoS 惡意程式偵測數量 (2015 年第一季至第三季)



PoS 惡意程式偵測分布 (依市場分隔，2015 年第三季)



PoS 惡意程式偵測數量成長了將近 66%，最可能的原因是駭客採取亂槍打鳥的策略，因而找到了既容易得逞而且獲利更豐厚的目標：中小企業。

駭客本季選擇採用歷久不衰的散布技巧 (但也許是歹徒的最後一搏)，希望能在美國的商家被迫於今年十月全面採用安全性更高 EMV 信用卡之前擄獲更多受害者。

「PoS 惡意程式攻擊中小企業已不是什麼新聞，我們關於這方面的討論已有一段時間。不過最新的發展是，網路犯罪集團放棄原本的針對性攻擊方式，轉而採取傳統大規模感染的途徑，例如：垃圾郵件、殭屍網路、漏洞攻擊套件。唯一不變的是，這類惡意程式對使用信用卡的消費者仍是一大威脅。擴大攻擊範圍是一項具有風險的策略，因為惡意程式將更容易被偵測及解決，但肯定可以擄獲更多受害者。而這些新的受害者與其資料，只要能夠成功取得，就能讓網路犯罪集團對受害者本人或其聯絡人發動進一步的針對性攻擊。」

—Numaan Huq

資深威脅研究員

本季重大事件

政治人物：網路間諜行動偏愛的目標

Pawn Storm[43] 持續性網路間諜行動一向專門鎖定美國及其友邦國家與俄羅斯異議份子[44]，本季攻擊了 MH17 空難調查小組[45]。根據我們的監控資料，該行動的攻擊目標包括政府機關、媒體機構、軍事單位以及國防承包商。今年稍早 (七月)，該團體在 Java 自 2013 年以來第一個零時差漏洞 (CVE-2015-2590)[46、47] 的助長下，活動因而激增。

在一項針對北大西洋公約組織 (NATO) 某會員國軍隊及美國國防單位的攻擊中，使用了 ausameetings.com 這個網域來架設網路釣魚網站，意圖冒充 ausameetings.org 網站，也就是美國陸軍協會 (Association of the US Army，簡稱 AUSA) 的年度展覽網站。就在我們發布有關該案件的報告之後，Pawn Storm 駭客團體竟然將某個專門散布漏洞攻擊套件的網域導向趨勢科技的 IP 位址 (此舉很可能是為了報復)[48]。

除了前述提到的目標之外，Pawn Storm 駭客團體也盯上了俄國 Pussy Riot (暴動小貓) 搖滾樂團的成員，以及批評俄羅斯當局的媒體機構。俄羅斯加密軟體廠商以及前俄羅斯總理也在該團體的攻擊之列。

Pawn Storm 行動攻擊目標

2011 年	2015 年 4 月	2015 年 8 月
美國軍方	北大西洋公約組織 (NATO) 會員國	俄羅斯政治人物
美國與其友邦的大使館	美國白宮	俄羅斯搖滾樂團 Pussy Riot
美國國防承包商人員	德國國會	俄羅斯媒體從業人員
		俄羅斯軟體廠商執行長

從 2011 年開始，美國和俄羅斯的政治人物就一直是 Pawn Storm 的攻擊對象。

2015 年八月份 Pawn Storm 美國境內攻擊目標分布

- 軍方人員 35%
- 國防承包商 22%
- 政府機關 9%
- 學術機構 8%
- 媒體從業人員 7%
- 外交單位 6%
- 能源單位人員 3%
- 國內民航單位人員 2%
- 非政府組織 (NGO) 2%
- 房地產公司 2%
- 其他 4%

Pawn Storm 在美國的頭號攻擊目標分別為：軍方、國防與政府機關。

2015 年八月份 Pawn Storm 烏克蘭境內攻擊目標分布

- 軍方人員 18%
- 媒體從業人員 18%
- 政府機關 16%
- 政治人物 14%
- 學術機構 7%
- 異議份子 7%
- 能源單位人員 3%
- 非政府組織 (NGO) 2%
- 軟體廠商 2%
- 外交單位 2%
- 金融機構 2%
- 其他 9%

在烏克蘭，Pawn Storm 集團主要攻擊軍方、媒體與政府機關。

2015 年八月份 Pawn Storm 攻擊目標排行榜

今年八月 Pawn Storm 的首要攻擊目標國家為烏克蘭、美國和英國。

如同 Pawn Storm 一樣，Rocket Kitten[49] 也在本季重出江湖。這一次，該集團的攻擊目標還包括了一位協助資安研究機構 ClearSky 調查「Thamar Reservoir」攻擊行動的語言學及史前伊斯蘭 (Pre-Islamic) 文化專家。此外，參與這項調查的幕後研究人員同樣也無法倖免。

2015 年三月份和九月份 Rocket Kitten 的攻擊目標

3 月	2015 年 8 月
以色列民間機構	中東政策研究人員
以色列學術機構	中東外交單位人員
德語政府機關	中東國際事務人員
歐洲政府機關	中東國防安全人員
歐洲民間企業	中東記者

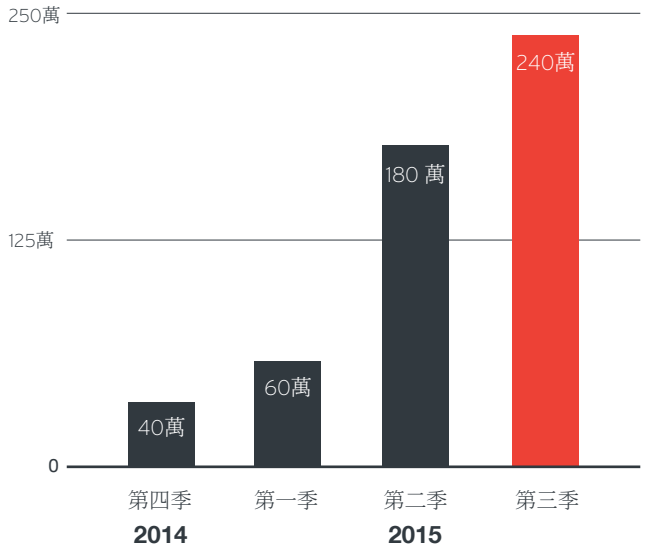
Rocket Kitten 絕大多數的攻擊對象都是外交單位和國際事務人員，此外還有來自中東的政策研究人員。

就近期的發展情況來看，未來肯定會出現更多針對政治人物的攻擊，這些攻擊將是歹徒進一步行動的跳板。

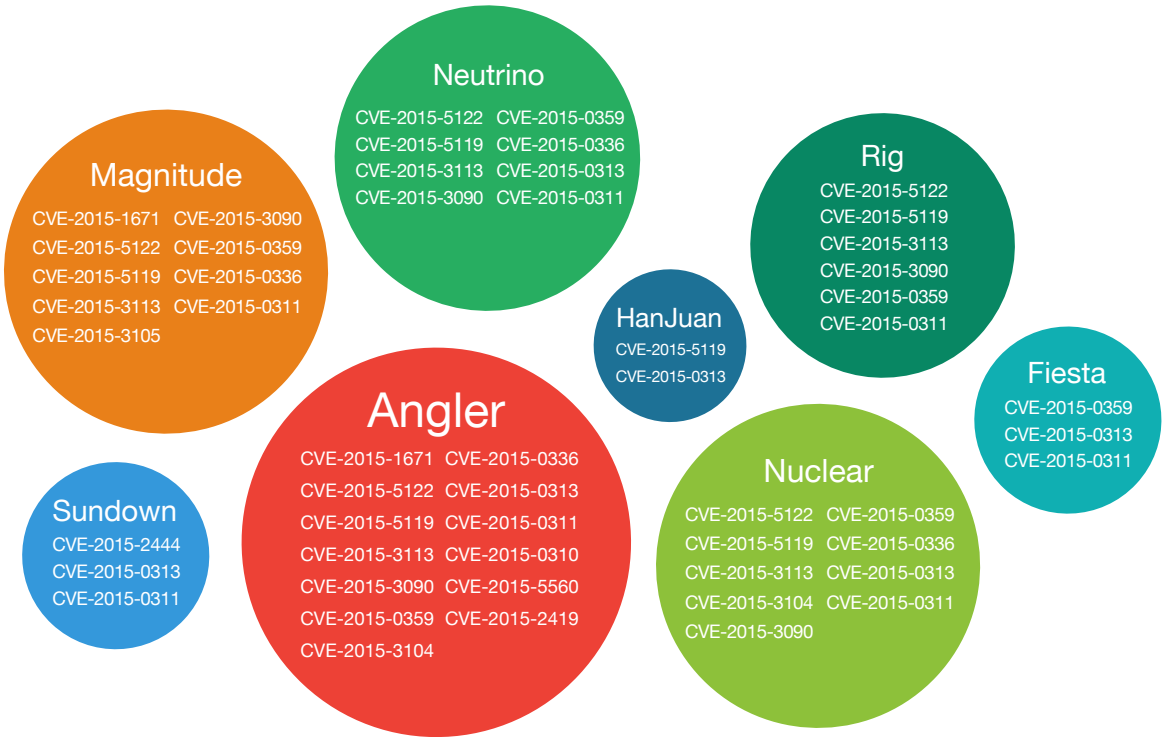
Angler：依然是使用最廣的漏洞攻擊套件

Angler 漏洞攻擊套件的作者並未因成功而自滿，反而在本季推出了新的版本。也因為如此，該套件目前仍是使用最廣的漏洞攻擊套件，甚至較上一季成長了 34%。許多駭客都利用這個套件來散布惡意程式，不只攻擊 PoS 系統，也攻擊傳統的目標 (也就是一般電腦)，目的是希望能夠盡可能擄獲更多受害者。Hacking Team 資料外洩當中被發現的 Adobe Flash 零時差漏洞也很快就被收錄到 Angler 以及其他漏洞攻擊套件，如：Neutrino 和 Magnitude。正如先前所說，Angler 的作者[50] 正積極將更多 Adobe Flash 漏洞納入他們的套件當中。

散布 Angler 漏洞攻擊套件的網址數量 (逐季分布)

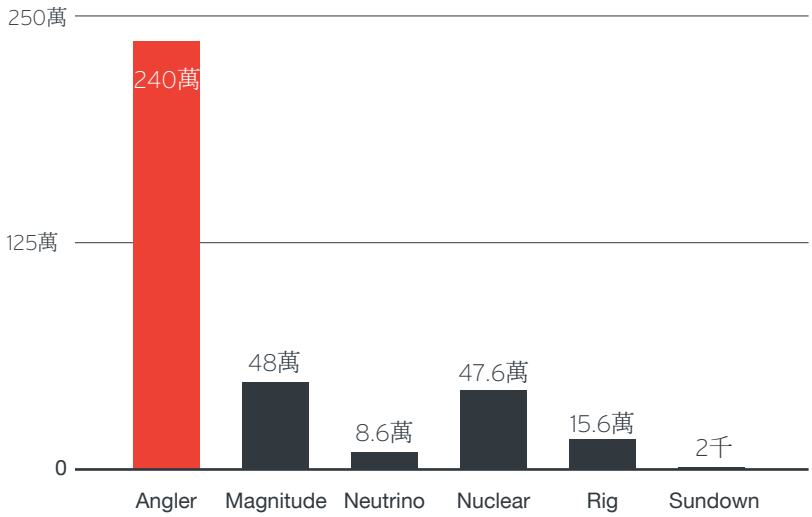


各套件收錄的漏洞 (2015 年第一季至第三季)



Angler 的更新頻率遠超過其他同期的漏洞攻擊套件，而且率先整合了 Hacking Team 資料外洩事件當中的 Adobe Flash 零時差漏洞，因而成為今日最活躍的套件。

專門散布漏洞攻擊套件的網址數量 (2015 年第三季)



今年五月至九月，連上 Angler 相關連結使用者數量明顯增加。發生在日本的網站入侵事件、Hacking Team 資料外洩事件之後的零時差漏洞攻擊，以及 PoS 惡意程式大量散布，都與 Angler 漏洞攻擊套件有關。

今年九月，約有 3,000 個日本知名網站遭駭客入侵並在網站植入惡意廣告[51]，將近 50 萬的使用者因而陷入危險當中。這些攻擊使用了吸引大量受害者的廣告橫幅，裡面暗藏惡意程式。此外也使用了目前已修正的漏洞，包括 Internet Explorer (CVE-2015- 2419)[52] 和 Adobe Flash (CVE-2015-5560)[53]，突顯使用者隨時保持軟體與系統更新的必要。

Angler 漏洞攻擊套件的持續更新，使得該套件成了本季的資安焦點。此外，Angler 還會利用 Diffie-Hellman 密碼交換協定來躲避資安防護措施[54]，讓資安研究人員更感棘手。簡而言之，Diffie-Hellman 協定可讓兩個電腦使用者產生一個共用的私密金鑰，以便在不安全的通道上安全地交換資訊。

連網裝置：安全問題重重

今日網路威脅的嚴重性更勝以往，儘管連網確實有其好處，但卻也帶來了更大的危險，受影響的不僅是連網的裝置，還有連網的使用者。

我們的研究人員在一項名為 GasPot 的實驗當中發現了專門針對加油站儲油槽監控系統的攻擊[55]。我們看到駭客竄改加油站儲油槽監控系統的資訊，很可能對公共安全帶來嚴重後果[56]。更嚴重的是，儲油槽並非唯一暴露在全球網路風險當中的連網裝置。SHODAN 是一個專門監視這類裝置的網站，在該網站所列出的不安全系統當中，除了暖氣空調和保全監控系統之外，更包含了發電廠在內。由於牽涉到水電公共設施，甚至整體經濟，因此一旦駭客攻擊得逞，將對國家帶來災難性的後果。

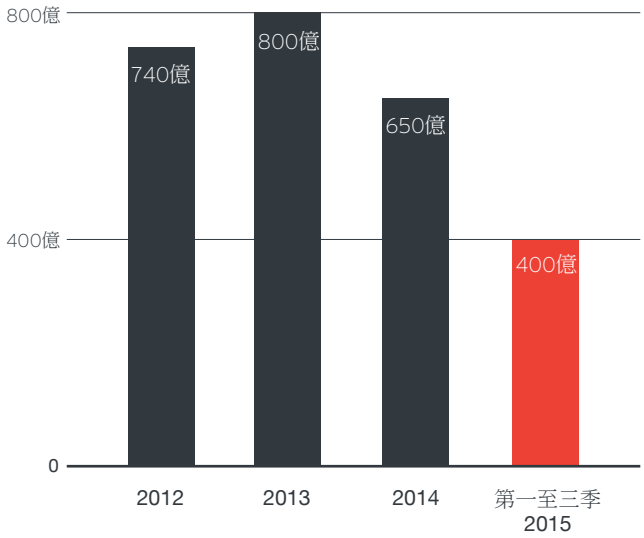
車輛遭駭客入侵，在幾年前聽來或許還是天方夜譚，但現在已慢慢成真。越來越多的車廠開始推出連網甚至自動駕駛的汽車，雖然帶來了各式各樣的好處，但也不幸地引來了威脅。本季，Chris Valasek 和 Charlie Miller 兩位研究人員的示範讓我們了解，駭客只需透過 3G 行動電話網路就能輕易操控新款 Jeep Cherokee 休旅車的一些重要系統 (引擎、剎車等等)，甚至可能造成危害駕駛人生命安全的意外[57]。

近期出現的各種連網裝置漏洞，需要裝置製造廠商與資安專家之間更密切的合作才能解決。製造商在開發最新產品時不一定會考慮到安全的問題。因此，資安研究人員可協助他們在發揮創新科技效益的同時又能確保客戶安全。

威脅情勢回顧

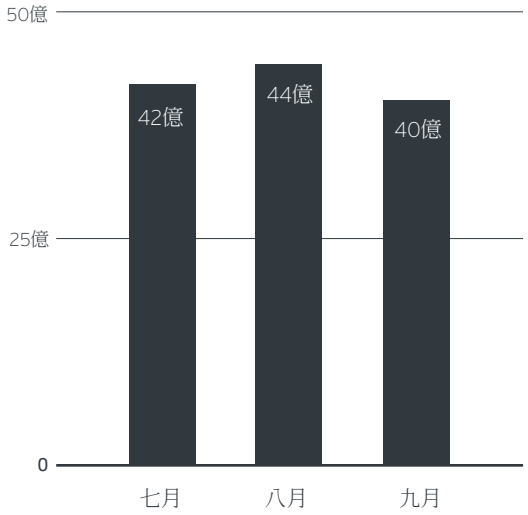
根據 Smart Protection Network 的資料，從 2012 年至今整體威脅數量一直以將近 20% 的幅度逐漸減少。其中的關鍵因素有可能是一些很普遍的威脅 (如勒索軟體) 開始運用所謂無檔案的感染方式。此外，儘管駭客普遍傾向採用亂槍打鳥的方式來散布威脅，但仍有些駭客偏好僅針對篩選過的目標 (大多為中小企業和大型企業) 進行攻擊，以確保成效。

已攔截的威脅總數 (2012 至 2015 年)



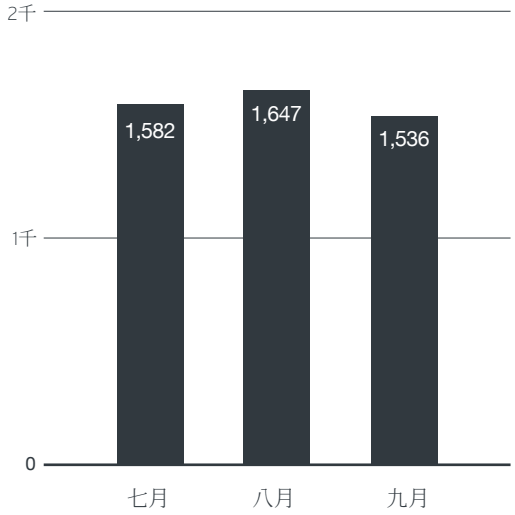
已攔截的威脅總數從 2014 年起即開始減少，這樣的趨勢一直持續至今。

已攔截的威脅總數 (2015 年第三季)



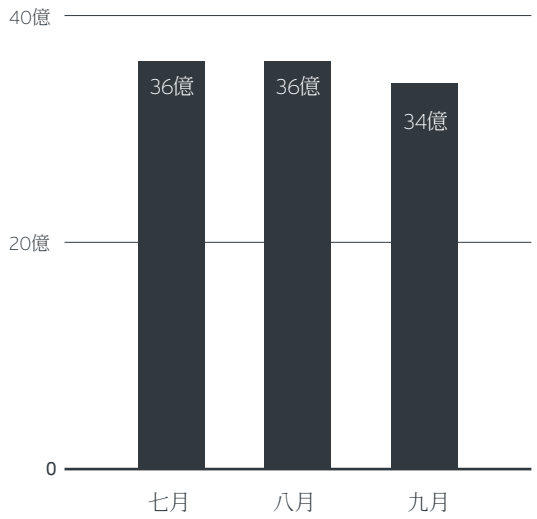
如同前一季，我們從七月至九月每個月平均攔截了 42 億次威脅。

趨勢科技整體偵測速率 (2015 年第三季)



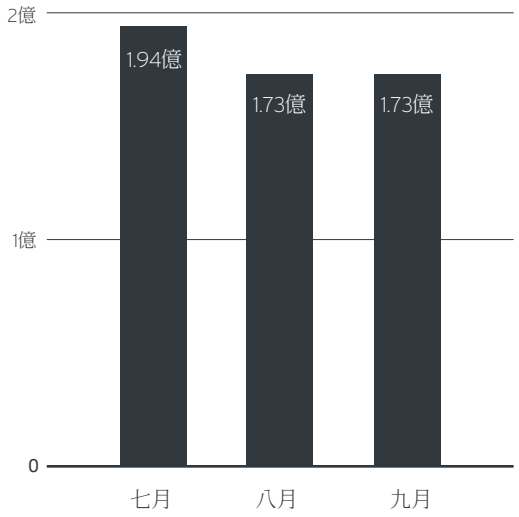
本季，我們平均每秒攔截 1,588 個威脅。

被電子郵件信譽評等查詢判定為垃圾郵件的數量 (2015 年第三季)



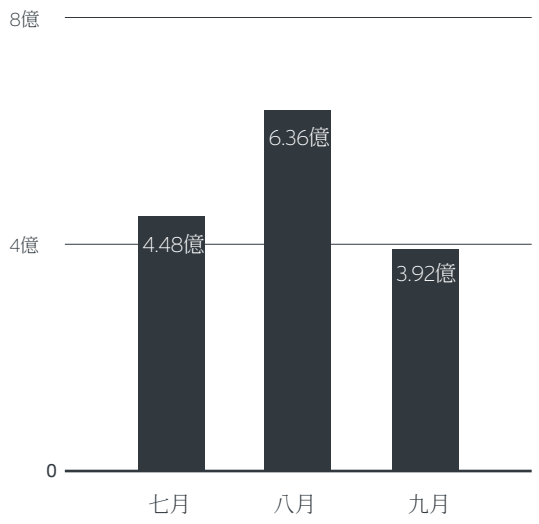
本季我們總共防止了106 億封來自已知垃圾郵件散發IP 位址的電子郵件進入使用者的收件匣當中，較上一季的105 億封稍微增加，有可能是駭客現在又開始採用垃圾郵件來散布威脅的關係。

已防止使用者存取惡意網站的次數 (2015 年第三季)



本季，我們防止使用者連上惡意網站的次數超過 5.4 億次。

已攔截的惡意檔案數量 (2015 年第三季)



本季，我們防止了超過 10 億個惡意檔案感染使用者電腦，
有可能是因為駭客使用了無檔案的植入技巧，因而導致偵測到的檔案數量減少。

已防止使用者存取的惡意網址排行榜 (2015 年第三季)

網域	防止使用者存取的原因
jsgnr.eshopcomp.com	已知會挾持瀏覽器。
a020f0.com	與 TROJ_POWELIKS 有所關聯。
sso.anbtr.com	PE_SALITY.RL 的通訊管道。
cnfg.toolbarservices.com	與瀏覽器工具列相關的已知越權廣告程式。
disorderstatus.ru	與瀏覽器工具列相關的已知越權廣告程式。
differentia.ru	會顯示惱人的彈出式頁面或訊息並將使用者帶到惡意網站。
sp-storage.spccint.com	與 Conduit 越權廣告程式有所關聯。
allmodel-pro.com	與 MultiPlug 惡意程式有所關聯。
bhinnekaonline.com	與 Ransom-AZI 木馬程式有所關聯。
92vblljpl3fqub.ru	會顯示惱人的彈出式頁面或訊息並將使用者帶到惡意網站。

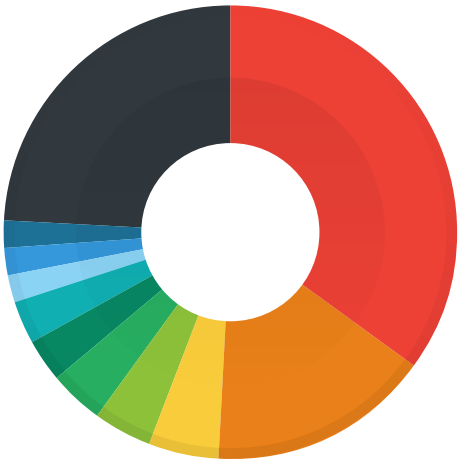
會挾持瀏覽器的網站依然是本季存取次數最多的惡意網址。

惡意網址數量最多的國家 (2015 年第三季)

美國	26%
俄羅斯	7%
中國	4%
南韓	2%
荷蘭	2%
英國	2%
德國	2%
芬蘭	2%
日本	1%
葡萄牙	1%
其他	51%

從上一季以來美國依然是惡意網址最多的國家。本季中國和俄羅斯名次互換，南韓上升了幾個名次，取代葡萄牙成為第四名。

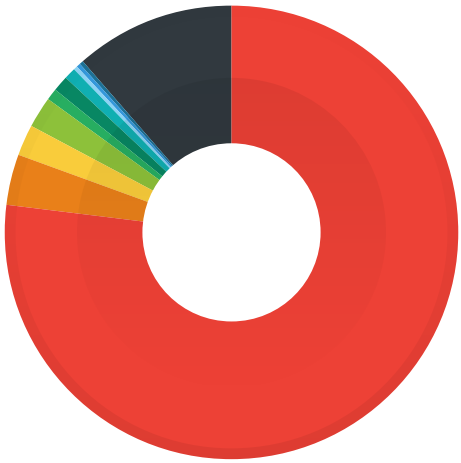
點選惡意網址的使用者數量最多的國家 (2015 年第三季)



美國	35%
日本	16%
台灣	5%
澳洲	4%
印度	4%
中國	3%
德國	3%
加拿大	2%
南韓	2%
法國	2%
其他	24%

點選惡意網址的使用者數量最多的國家在本季沒有明顯變化。

垃圾郵件最多的語言 (2015 年第三季)



英文	77.0%
中文	3.6%
德文	2.4%
俄羅斯文	2.0%
斯洛伐克文	1.1%
西班牙文	0.9%
日文	0.8%
波蘭文	0.5%
葡萄牙文	0.3%
法文	0.2%
其他	11.2%

英文依然是垃圾郵件散發者最偏愛的語言，而中文和德文所占的比例較上一季略少。

散發垃圾郵件最多的國家 (2015 年第三季)

美國	17%
越南	12%
中國	7%
俄羅斯	4%
阿根廷	4%
印度	3%
西班牙	3%
巴西	3%
義大利	3%
烏克蘭	3%
其他	41%

美國和中國為本季二大垃圾郵件來源，依然分別穩坐一、三名。
越南則取代了俄羅斯，成為本季第二名。

惡意程式家族排行榜 (2015 年第三季)

家族	數量
SALITY	8.1萬
DOWNAD	7.1萬
BARTALEX	5.8萬
GAMARUE	4.7萬
DUNIHI	4.2萬
VIRUX	3.8萬
RAMNIT	3.6萬
AUTORUN	2.6萬
DLOADR	2.6萬
SKEEYAH	2.4萬

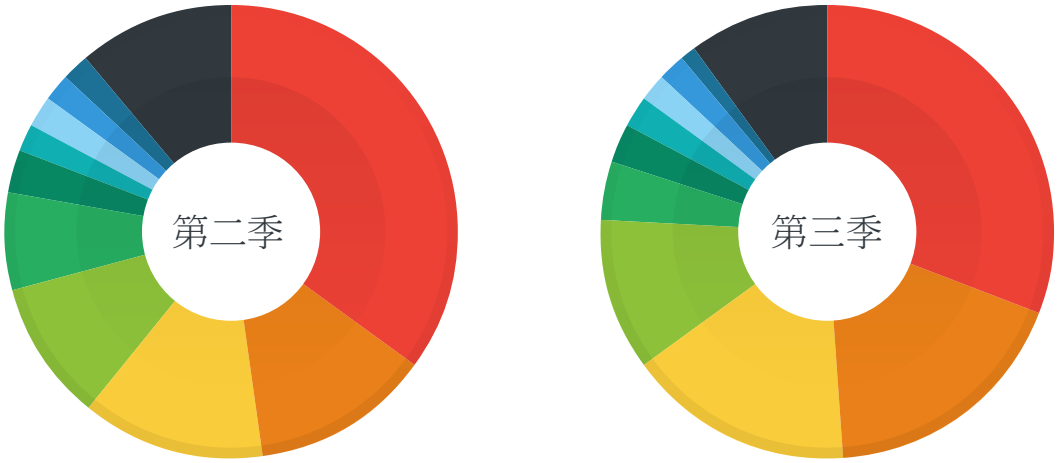
惡意程式家族排行榜 (依市場區隔，2015 年第三季)

市場區隔	家族	數量
大型企業	DOWNAD	5.6萬
	SALITY	3.3萬
	DUNIHI	2.6萬
中小企業	BARTALEX	1.8萬
	SKEEYAH	1萬
	UPATRE	8千
一般消費者	SALITY	2.8萬
	GAMARUE	2.3萬
	VIRUX	1.8萬

BARTALEX 在今年七月巨集惡意程式相關攻擊的帶動下進入本季的惡意程式家族排行榜中。BARTALEX 通常使用 Microsoft Word®文件來當成UPATRE 的下載工具。DOWNAD 從出現至今已過了七個年頭[58]，目前依然穩坐排行榜當中。可能的原因是使用者 (應該是企業用戶) 仍在使用已終止支援的舊版Windows 系統 (如 XP)，而這些系統含有該惡意程式可攻擊的漏洞。

DRIDEX[59] 是一個值得注意的網路銀行惡意程式家族。它具備多種資料竊取能力，包括：擷取表單、HTML 隱碼攻擊，以及擷取瀏覽器畫面。它專門攻擊歐洲、美國的銀行和金融機構。一般認為 DRIDEX 是 GameOver ZeuS (GoZ) 的後繼者，採用了改良的 GoZ 點對點 (P2P) 架構來防止其幕後操縱 (C&C) 伺服器被資安軟體所偵測。

網路銀行惡意程式家族十大排行榜 (2015 年第二季至第三季)



第二季		第三季	
RAMNIT	35%	RAMNIT	31%
DORKBOT	13%	DRIDEX	18%
ZBOT	13%	ZBOT	16%
EMOTET	10%	DORKBOT	11%
DYRE	7%	DYRE	4%
QAKBOT	3%	QAKBOT	3%
DRIDEX	2%	FAREIT	2%
BANKER	2%	BANKER	2%
FAREIT	2%	BANLOAD	2%
BANLOAD	2%	EMOTET	1%
其他	11%	其他	10%

RAMNIT 依然穩坐網路銀行惡意程式家族龍頭，儘管它所占的比例較上一季減少 4%。DRIDEX 所占比例則從上一季的 2% 成長至本季的 18%，最可能的原因是使用了殭屍網路的關係。

越權廣告程式家族排行榜 (2015 年第三季)

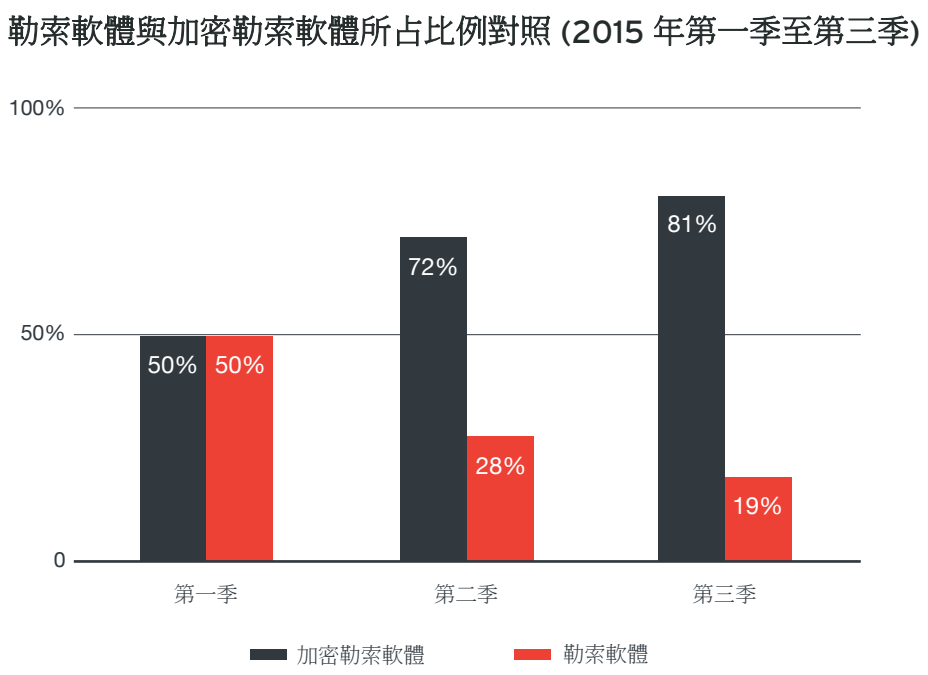
家族	數量
OPENCANDY	49.5萬
MYPCBACKUP	8.6萬
MULTIPLUG	8.4萬
ELEX	8.2萬
TOMOS	6.5萬
MONTIERA	6.2萬
REGCLEANPRO	5.8萬
DEALPLY	4.8萬
PRICEGONG	4萬
DOWNWARE	3.4萬

越權廣告程式家族排行榜 (依市場區隔，2015 年第三季)

市場區隔	家族	數量
大型企業	OPENCANDY	4.6萬
	MULTIPLUG	1.4萬
	TOMOS	9千
中小企業	OPENCANDY	1.7萬
	MULTIPLUG	3千
	ELEX	3千
一般消費者	OPENCANDY	39.8萬
	FAKEGOOG	7萬
	MYPCBACKUP	5.7萬

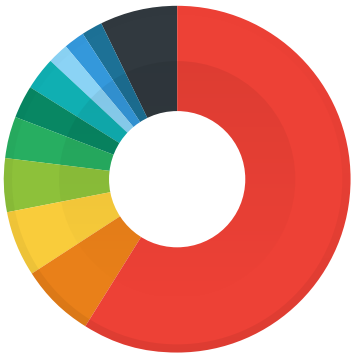
OPENCANDY 和 MYPCBACKUP 通常偽裝成免費軟體或工具列，對所有類型的使用者來說都是一項惱人的問題。

加密勒索軟體自從上一季就是一項普遍的威脅，其所占比例與一般較不具破壞性的純勒索軟體相比明顯較高，原因可能與 CryptoWall 相關的垃圾郵件數量激增有關。



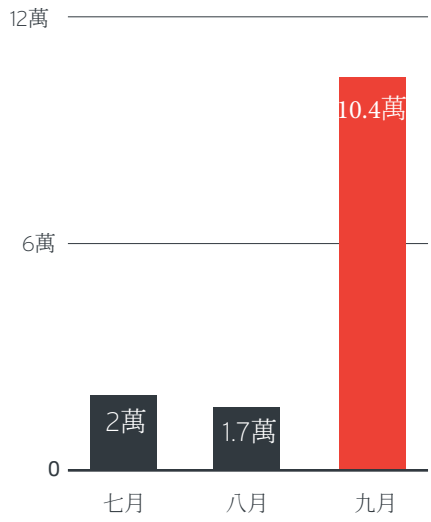
加密勒索軟體的數量持續超過勒索軟體 (逐季對照)。

勒索軟體家族排行榜 (2015 年第三季)



CRYPWALL	59%
CRILOCK	7%
REVETON	6%
RANSOM	5%
CRYPTESLA	4%
MATSNU	3%
KOVTER	3%
CRYPCTB	2%
CRYPDEF	2%
CRYPTWALL	2%
Others	7%

CryptoWall 相關的垃圾郵件數量 (2015 年第三季)



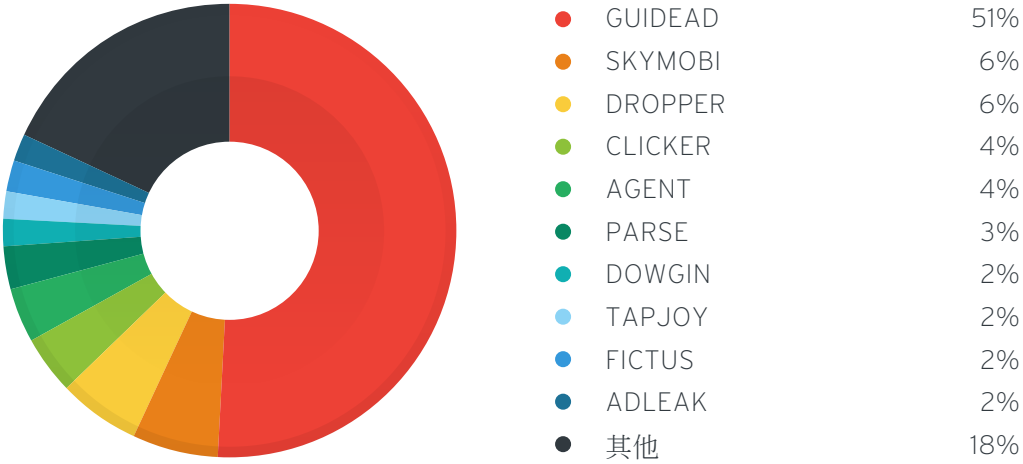
想要免於勒索軟體的威脅，使用者首先要預先攔截這類威脅，不讓它有機會在電腦上執行。根據持續監控勒索軟體的資料顯示，確實有辦法夠在 CRILOCK (或稱 TorrentLocker) 以及CRYPTOWALL 經由垃圾郵件附檔或經由郵件內含的惡意連結進入電腦之前時預先加以攔截。

Android 惡意程式家族排行榜 (2015 年第三季)

ADULTPLAYER	14%
SYPAY	9%
FAKEINST	8%
SMSSNOW	6%
OPFAKE	5%
LINKSMSHIDER	4%
SMSREG	4%
SMSTHIEF	3%
SYSSERVICE	3%
SMSSPY	3%
其他	41%

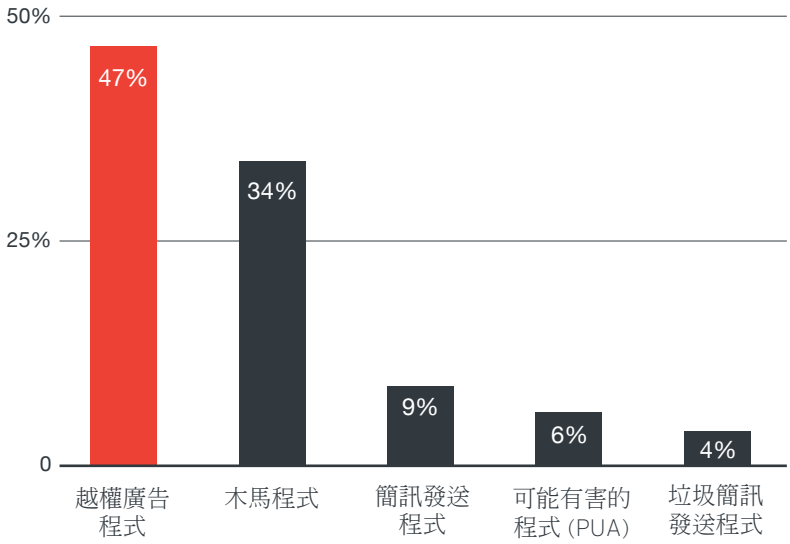
ADULTPLAYER 會暗中偷取應用程式使用者的照片，拿來進行後續的恐嚇勒索。

Android 越權廣告程式家族排行榜 (2015 年第三季)



GUIDEAD 目前被歸類為「可能有害的程式」(PUA)，是中國手機軟體平台公司 SkyMobi 的一套軟體開發套件 (SDK)，專門用來幫他人開發的應用程式做宣傳，其方式有點像一般困擾電腦使用者的惱人廣告。

Android 前幾大威脅類型分布比例 (2015 年第三季)



本季出現的 Android 威脅有將近半數都是越權廣告程式，使得該類威脅再度重回第一名的位置。而垃圾簡訊發送程式則是首度名列 Android 威脅類型排行榜。這類程式會大量發送由自動化工具產生的內容，並且有別於簡訊發送程式，後者是專門在使用者背後暗中發送簡訊的程式。

***註：**某個行動裝置威脅家族可能出現不只一種類型的行為。*

C&C 伺服器最多的國家 (2015 年第三季)

美國	28%
烏克蘭	11%
俄羅斯	8%
德國	5%
中國	4%
荷蘭	4%
英國	3%
法國	3%
南韓	3%
波蘭	2%
其他	29%

本季 C&C 伺服器最多的國家依舊是美國、烏克蘭和俄羅斯。請注意，駭客不一定位於這些國家就能控制 C&C 伺服器，因為這些伺服器皆可以從遠端遙控。

C&C 伺服器連線數量最多的國家 (2015 年第三季)

美國	38%
日本	14%
印度	7%
澳洲	5%
台灣	4%
德國	3%
法國	2%
義大利	2%
加拿大	2%
馬來西亞	2%
其他	21%

本季美國依然是 C&C 連線數量排行榜第一名。

參考資料

1. Steve Ragan。(2015 年 7 月 5 日)。*CSO*。「Hacking Team 公司遭駭，歹徒宣稱竊取了 400GB 的資料」(Hacking Team Hacked, Attackers Claim 400GB in Dumped Data)。上次存取時間 2015 年 10 月 27 日：http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html.
2. Adobe Systems Incorporated。(2015 年)。*Adobe Flash Runtimes*。「統計數字」(Statistics)。上次存取時間 2015 年 10 月 30 日：http://www. adobe.com/products/flashruntimes/statistics.html.
3. Net Applications.com。(2006-2015 年)。*Net Marketshare*。「桌上型電腦作業系統市場占有率」(Desktop Operating System Market Share)。上次存取時間 2015 年 10 月 30 日：https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=198&qpnp=1&qptimeframe=M.
4. Net Applications.com。(2006-2015 年)。*Net Marketshare*。「桌上型電腦瀏覽器版本市場占有率」(Desktop Browser Version Market Share)。上次存取時間 2015 年 10 月 30 日：https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0&qpsp=198&qpnp=1&qptimeframe=M.
5. 趨勢科技。(2015 年 8 月 16 日)。*威脅百科網站 (Threat Encyclopedia)*。「Adobe Flash Player 漏洞 (CVE-2015-5119)」(Adobe Flash Player Vulnerability [CVE-2015-5119])。上次存取時間 2015 年 10 月 27 日：http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/6994/adobe-flash-player-vulnerability-cve20155119.
6. Brooks Li。(2015 年 7 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 的 Flash 零時差漏洞已被收錄到漏洞攻擊套件當中」(Hacking Team Flash Zero-Day Integrated Into Exploit Kits)。上次存取時間 2015 年10月 27日：http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/.
7. Peter Pi。(2015 年 7 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「未修補的 Flash Player 漏洞以及其他 Hacking Team 資料外洩事件當中發現的概念驗證攻擊」(Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/.
8. Weimin Wu。(2015 年 7 月 1 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 的 Flash 零時差漏洞涉及 7 月 1 日韓國和日本所遭到的攻擊」(Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan on July 1)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-tied-to-attacks-in-korea-and-japan-on-july-1/.
9. Joseph C. Chen。(2015 年 7 月 28 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team Flash 漏洞攻擊擴大：駭客入侵香港和台灣電視台與政府相關網站並散布 PoisonIvy 遠端存取工具」(Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIvy)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-attacks-spread-compromised-tv-and-government-sites-in-hong-kong-and-taiwan-lead-to-poisonivy/.
10. Veo Zhang。(2015 年 7 月 21 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「可竊聽電話的 Hacking Team RCSAndroid 間諜工具可先破解裝置再感染裝置」(Hacking Team RCSAndroid Spying Tool Listens to Calls; Roots Devices to Get In)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/.
11. Danielle Walker。(2015 年 7 月 13 日)。*SC Magazine*。「研究機構發現 iPhone 不論越獄與否都可能感染 Hacking Team 間諜程式」(iPhones, Jailbroken and Not, Vulnerable to Hacking Team Spyware, Firm Finds)。上次存取時間 2015 年 10 月 27 日：http://www.scmagazine.com/ios-devices-dont-have-to-be-jailbroken-for-spyware-sold-by-hacking-team-to-be-installed/article/426137/.
12. Wish Wu。(2015 年 7 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 資料外洩流出的假新聞 App 程式可避開 Google Play 安全機制」(Fake News App in Hacking Team Dump Designed to Bypass Google Play)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/fake-news-app-in-hacking-team-dump-designed-to-bypass-google-play/.
13. 趨勢科技。(2015 年 8 月 20 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Ashley Madison：性、謊言、資料外洩」(Ashley Madison: A Tale of Sex, Lies, and Data Breaches)。上次存取時間 2015 年 10 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/ashley-madison-a-tale-of-sex-lies-and-data-breaches/.
14. Matthew Herper。(2015 年 9 月 1 日)。*Forbes*。「Ashley Madison 偷情網站會員人數到底是 3,000 萬還是 1,000 萬？估計人數到底如何失算。」(Were There 30 Million Cheaters on Ashley Madison, or 10? How Estimates Get Out of Hand)。上次存取時間 2015 年 10 月 27 日：http://www.forbes.com/sites/matthewherper/2015/09/01/were-there- 30-million-cheaters-on-ashley-madison-or-10-how-estimates-get-out-of-hand/.
15. Chris Baraniuk。(2015 年 8 月 24 日)。*BBC News*。「Ashley Madison 偷情網站遭駭導致會員自殺」(Ashley Madison: 'Suicides' over Website Hack)。上次存取時間 2015 年 10 月 27 日： http://www.bbc.com/news/technology-34044506.

16. Jonathan Leopando。(2015 年 8 月 31 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「婚外情約會網站 Ashley Madison 使用者遭黑函勒索」(Blackmail, Deletion Offers Hit Ashley Madison Users)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/blackmail-deletion-offers-hit-ashley-madison-users/.

17. Ryan Flores。(2015 年 9 月 8 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Ashley Madison：我們的電子郵件誘捕帳號為何會在貴公司網站註冊帳號？」(Ashley Madison, Why Do Our Honeypots Have Accounts on Your Website?)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/ashley-madison-why-do-our-honeypots-have-accounts-on-your-website/.

18. Andy Greenberg。(2015 年 9 月 10 日)。*Wired*。「駭客記事：醫療保險公司 Excellus 表示遭駭客竊取了 1,000 萬筆資料」(Hack Brief: Health Insurer Excellus Says Attackers Breached 10M Records)。上次存取時間 2015 年 10 月 27 日： http://www.wired.com/2015/09/hack-brief-health-insurance-firm-excellus-says-attackers-breached-10m-records.

19. Chad Terhune。(2015 年 7 月 17 日)。*Los Angeles Times*。「UCLA Health System 資料外洩影響 450 萬名病患」(UCLA Health System Data Breach Affects 4.5 Million Patients)。上次存取時間 2015 年 10 月 27 日： http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html.

20. TrendLabs。(2015 年 8 月 14 日)。*趨勢科技資訊安全新聞*。「鎖定醫療資料：為何醫療機構成為歹徒的覬覦目標？」(Medical Data in the Crosshairs: Why Is Healthcare an Ideal Target?)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target.

21. Numaan Huq。(2015 年 9 月 22 日)。*趨勢科技資訊安全新聞*。「跟著資料循線追查：各產業資料外洩情況分析」(Follow the Data: Analyzing Breaches by Industry)。上次存取時間 2015 年 11 月 3 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf.

22. Wish Wu。(2015 年 7 月 31 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Stagefright 漏洞除多媒體簡訊之外還有其他攻擊方式」(MMS Not the Only Attack Vector for "Stagefright")。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/mms-not-the-only-attack-vector-for-stagefright/.

23. Wish Wu。(2015 年 7 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「趨勢科技發現一個會讓 Android 裝置沒有反應的漏洞」(Trend Micro Discovers Vulnerability That Renders Android Devices Silent)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-vulnerability-that-renders-android-devices-silent/.

24. Android。*Developers*。「儀表板」(Dashboards)。上次存取時間 2015 年 10 月 27 日： http://developer.android.com/about/dashboards/index.html.

25. Wish Wu。(2015 年 8 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「重新檢視 CVE-2015-3823 漏洞：媒體伺服器 (Mediaserver) 元件漏洞造成 Heap 記憶體溢位」(Revisiting CVE-2015-3823: Mediaserver Bug Leads to Heap Overflow, Too)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/revisiting-cve-2015-3823-mediaserver-bug-leads-to-heap-overflow-too/.

26. Wish Wu。(2015 年 8 月 17 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Android 最新漏洞導致媒體伺服器 (Mediaserver) 元件再度遭到攻擊」(Mediaserver Takes Another Hit with Latest Android Vulnerability)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/mediaserver-takes-another-hit-with-latest-android-vulnerability/.

27. Marshall Honorof。(2015 年 8 月 5 日)。*Tom's Guide*。「Android 終於等到定期安全更新」(Android Finally Getting Regular Security Updates)。上次存取時間 2015 年 10 月 27 日： http://www.tomsguide.com/us/android-montly-security-updates,news-21432.html.

28. Ju Zhu。(2015 年 9 月 21 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「XcodeGhost 災難到底是怎麼來的？」(The XcodeGhost Plague–How Did It Happen?)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/the-xcodeghost-plague-how-did-it-happen/.

29. Charlie Osborne。(2015 年 9 月 17 日)。*ZDNet*。「Apple AirDrop 漏洞讓使用者可能遭到攻擊」(Apple AirDrop Flaw Leaves Users Vulnerable to Exploit)。上次存取時間 2015 年 10 月 27 日： http://www.zdnet.com/article/apple-airdrop-flaw-leaves-users-vulnerable-to-exploit/.

30. Allie Coyne。(2015 年 8 月 21 日)。*IT News*。「Apple iOS『Quicksand』漏洞使得企業資料遭竊」(Apple iOS 'Quicksand' Flaw Enables Enterprise Data Theft)。上次存取時間 2015 年 10 月 30 日： http://www.itnews.com.au/news/apple-ios-quicksand-flaw-enables-enterprise-data-theft- 408202#ixzz3q2cWNI7a.

31. Spencer Hsieh。(2014 年 11 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「與 Mac/iOS 跨平台威脅 WireLurker 保持安全距離」(Staying Safe from WireLurker: The Combined Mac/iOS Threat)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/staying-safe-from-wirelurker-the-combined-macios-threat/.

32. Brooks Hong。(2014 年 11 月 20 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Masque 攻擊行動新發現：竊取未加密的 iOS 應用程式資料」(The Other Side of Masque Attacks: Data Encryption Not Found in iOS Apps)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/the-other-side-of-masque-attacks-data-encryption-not-found-in-ios-apps/.

33. Taylor Armerding。(2015 年 1 月 12 日)。*CSO*。「為何歹徒會盯上中小企業」(Why Criminals Pick on Small Business)。上次存取時間 2015 年 10 月 27 日： http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html.

34. TrendLabs。(2015 年 8 月 1 日)。*趨勢科技資訊安全新聞*。「新一代支付交易處理技術：EMV信用」(Next-Gen Payment-Processing Tech: EMV Credit Cards)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-tech-emv-credit-cards.

35. TrendLabs。(2015 年 8 月 1 日)。*趨勢科技資訊安全新聞*。「新一代支付交易處裡技術：RFID 晶片信用卡」(Next-Gen Payment-Processing Tech: Contactless RFID Credit Cards)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-tech-rfid-credit-cards.

36. TrendLabs。(2015 年 8 月 1 日)。*趨勢科技資訊安全新聞*。「行動支付系統：Apple Pay 如何運作」(Mobile Payment Systems: How Apple Pay Works)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-payment-systems-apple-pay.

37. TrendLabs。(2015 年 8 月 1 日)。*趨勢科技資訊安全新聞*。「行動支付系統：Android Pay 如何運作」(Mobile Payment Systems: How Android Pay Works)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-payment-systems-android-pay.

38. TrendLabs。(2015 年 8 月 1 日)。*趨勢科技資訊安全新聞*。「新一代支付交易處理架構」(Next-Gen Payment-Processing Architectures)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/vinfo/us/security/news/security-technology/next-gen-payment-processing-architectures.

39. Anthony Joe Melgarejo。(2015 年 7 月 27 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「駭客使用 Angler 漏洞攻擊套件來搜尋並感染銷售櫃台 (PoS) 系統」(Angler Exploit Kit Used to Find and Infect PoS Systems)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/angler-exploit-kit-used-to-find-and-infect-pos-systems/.

40. Jay Yaneza。(2015 年 7 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「最新 GamaPoS 惡意程式利用 Andromeda 殭屍網路散布，遍及美國 13 個州」(New GamaPoS Malware Piggybacks on Andromeda Botnet; Spreads in 13 US States)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/new-gamapos-threat-spreads-in-the-us-via-andromeda-botnet/.

41. 趨勢科技。(2015 年 9 月 24 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「可擷取信用卡資料的 Kasidet 殭屍程式製作套件使得該惡意程式偵測數量飆高」(Credit Card-Scraping Kasidet Builder Leads to Spike in Detections)。上次存取時間 2015 年 10 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/.

42. TrendLabs。(2015 年 8 月)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新興浪潮：危及公共建設安全的最新駭客攻擊」(A Rising Tide: New Hacks Threaten Public Technologies)。上次存取時間 2015 年 10 月 27 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a_rising_tide.pdf.

43. Feike Hacquebord。(2015 年 4 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 攻擊活動激增，鎖定北大西洋公約組織 (NATO) 與美國白宮」(Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/.

44. Feike Hacquebord。(2015 年 8 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 在其本國境內的間諜行動曝光：烏克蘭和美國成為全球首要目標」(Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets)。上次存取時間 2015 年 10 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/.

45. Feike Hacquebord。(2015 年 22 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 攻擊 MH17 空難調查小組」(Pawn Storm Targets MH17 Investigation Team)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/.

46. 趨勢科技。(2015 年 7 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 最新消息：趨勢科技發現新的 Java 零時差漏洞攻擊」(Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/.

47. 趨勢科技。(2015 年 7 月 14 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「深入探討 Pawn Storm 如何運用 Java 零時差漏洞」(An In-Depth Look at How Pawn Storm's Java Zero-Day Was Used)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/an-in-depth-look-at-how-pawn-storms-java-zero-day-was-used/.

48. 趨勢科技。(2015 年 7 月 15 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 幕後操縱伺服器重導至趨勢科技 IP 位址」(Pawn Storm C&C Redirects to Trend Micro IP Address)。上次存取時間 2015 年 10 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-cc-redirects-to-trend-micro-ip-address/.

49. Cedric Pernet。(2015 年 9 月 1 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Rocket Kitten 最新犯罪行為：監控伊朗大學講師與資安研究人員」(Rocket Kitten Spies Target Iranian Lecturer and InfoSec Researchers in New Modus)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/the-spy-kittens-are-back-an-update-to-rocket-kitten/.

50. TrendLabs。(2015 年 8 月 18 日)。*趨勢科技資訊安全新聞*。「新興浪潮：危及公共建設安全的最新駭客攻擊」(A Rising Tide: New Hacks Threaten Public Technologies)。上次存取時間 2015 年 10 月 28 日：http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

51. Joseph C. Chen。(2015 年 9 月 30 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「3,000 個知名日本網站遭到大規模惡意廣告攻擊」(3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign)。上次存取時間 2015 年 10 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/3000-high-profile-japanese-sites-hit-by-massive-malvertising-campaign/.

52. 趨勢科技。(2015 年 7 月 30 日)。*威脅百科網站 (Threat Encyclopedia)*。「2015 年七月：Microsoft 發布 14 項資訊安全公告」(July 2015–Microsoft Releases 14 Security Advisories)。上次存取時間 2015 年 10 月 28 日：http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/3833/july-2015-microsoft-releases-14-security-advisories.

53. 趨勢科技。(2015 年 12 月 10 日)。*威脅百科網站 (Threat Encyclopedia)*。「Adobe Flash Player 整數溢位漏洞 (CVE-2015-5560)」(Adobe Flash Player Integer Overflow Vulnerability [CVE-2015-5560])。上次存取時間 2015 年 10 月 28 日：http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/8859/adobe-flash-player-integer-overflow-vulnerability-cve20155560.

54. Whitfield Diffie 與 Martin E. Hellman。(1976 年 11 月)。*IEEE*。「加密技術最新發展方向」(New Directions in Cryptography)。上次存取時間 2015 年 10 月 28 日： https://ee.stanford.edu/~hellman/publications/24.pdf.

55. 趨勢科技。(2015 年 8 月 5 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「GasPot 實驗：駭客攻擊加油站儲油槽」(The GasPot Experiment: Hackers Target Gas Tanks)。上次存取時間 2015 年 10 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/the-gaspot-experiment-hackers-target-gas-tanks/.

56. Arthur Brice。(2009 年 11 月 17 日)。*CNN*。「波多黎各大火可能是儲油槽監控系統錯誤所導致」(Puerto Rico Fire Linked to Faulty Gas-Tank-Monitoring System)。上次存取時間 2015 年 10 月 28 日：http://edition.cnn.com/2009/US/11/17/puerto.rico.fire.investigation/index.html.

57. Iain Thomson。(2015 年 7 月 21 日)。*The Register*。「Jeep 車主可能因駭客入侵而喪命：歹徒只需您車輛的 IP 位址」(Jeep Drivers Can Be Hacked to Death: All You Need Is the Car's IP Address)。上次存取時間 2015 年 10 月 28 日：http://www.theregister.co.uk/2015/07/21/jeep_patch/.

58. Arman Capili。(2008 年 11 月 30 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「DOWNAD：準備建立新的殭屍網路」(DOWNAD: Gearing Up for a Botnet)。上次存取時間 2015 年 11 月 3 日： http://blog.trendmicro.com/trendlabs-security-intelligence/downad-gearing-up-for-a-botnet/.

59. Ryan Angelo Certeza。(2014 年 12 月 6 日)。*威脅百科網站 (Threat Encyclopedia)*。「處理 DRIDEX 的善後問題」(Dealing with the Mess of DRIDEX)。上次存取時間 2015 年 10 月 28 日： http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex.

作者：
TrendLabs
趨勢科技全球技術支援與研發中心

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交流世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw

TREND MICRO™

Securing Your Journey to the Cloud

©2015 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。