TREND MICRO 趨勢科技

2013 年

台灣進階持續性威脅 APT 白皮書

目錄

前言 3

社交工程電子郵件攻擊 4

- 找到攻擊進入點 4
- 社交工程技術 5
- 電子郵件附加檔案 8
- 小結 9

APT 惡意程式 10

- 駭客工具 13
- 產業分析 14
- 中繼站 17
- 小結 18

資安事件調查 19

- 如何發覺被駭 20
- 何時發覺被駭 20
- 小結 22

結論 23

前言

進階持續性威脅（APT）是指一種威脅類型，可以長時間潛伏在網路或系統內來達到它們的目的（通常是竊取資料）而不被偵測到。我們在今年連續看到了幾起嚴重的 APT 事件，從南韓爆發大規模的網路攻擊，到國內政府公文系統被駭事件。再次讓人認識到此種威脅的嚴重程度。趨勢科技的資安事件處理團隊長期以來協助國內政府機關與民間企業調查處理 APT 事件，這份白皮書就根據台灣的事件處理數據加上趨勢科技的全球威脅情報進行統計分析，呈現出台灣目前 APT 攻擊的現況。

從這份白皮書裡，我們可以看到有超過了 80% 的受駭組織不知道自己遭受到 APT 攻擊。而且受駭目標並不僅限於政府單位，還包括了高科技產業、金融業和中小企業等。受駭組織也往往要等到駭客入侵很長一段時間才會發覺，例如高科技產業，平均要經過 346 天才會發現自己遭受到 APT 攻擊。最長的甚至要到 1019 天才會察覺。更有 77% 的受駭組織在發現時已經被駭客取得完全的掌控。不過經過調查，只有僅僅 50% 的受害電腦內會被找出惡意程式。這也告訴了我們並無法依靠一般的資安解決方案來解決 APT 問題。今天 IT 團隊所面臨的挑戰是如何保護他們的網路來對抗 APT 攻擊 – 由人所發起的電腦入侵攻擊，會積極的找尋並攻陷目標。

為了幫助企業制訂對抗 APT 攻擊的策略，趨勢科技的資安事件處理團隊透過這份白皮書來分享台灣 APT 攻擊的現況。讓 IT 團隊可以對 APT 攻擊有更深一層的認識，了解駭客所會用到的戰術和運作。有助於建立本地威脅智慧和回應方式。

這份白皮書分析了趨勢科技在全台灣近 500 家 ESO(中大型企業防毒委外服務，Expert Service Offering) 客戶在 2012 年所回饋的社交工程電子郵件攻擊、APT 惡意程式資料，加上對受駭單位進行資安事件調查的結果來綜觀剖析 APT 的現實狀況。

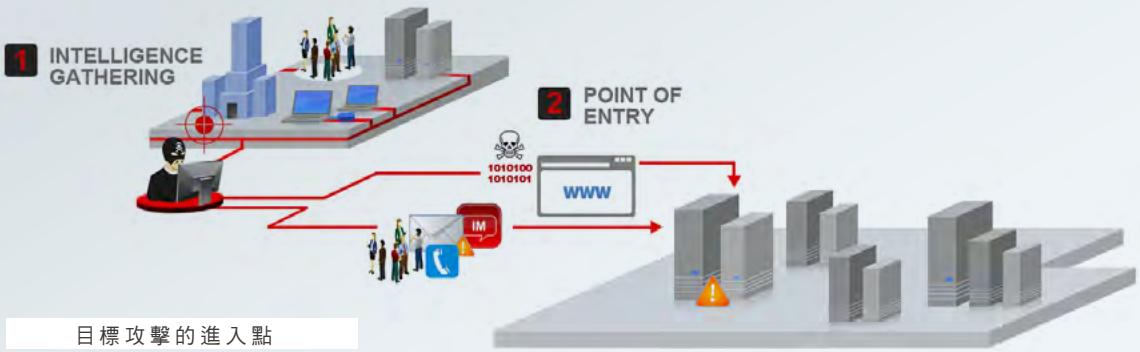
社交工程電子郵件攻擊

找到攻擊進入點

要增加 APT 攻擊成功的機率，攻擊者首先會對選擇的目標進行偵察。偵察可被定義為「分析目標以獲得關於目標防禦措施、軟體部署狀態的資料，目標身分的詳細資訊，關鍵人士的權責區分以及相關的各種資訊，好應用在社交工程上」。

在攻擊前的偵察一般和人比較相關。在這階段，攻擊者分析他們的對象以獲得進入目標網路的機會。通常會透過社交工程電子郵件。雖然人的相關資訊，像目標名字、職稱和電子郵件地址可能會從幕後黑手所提供，不過網路還是很方便的資訊來源。社群網站、企業、學術刊物和單位網站都讓駭客有機會去獲取對他們目標進行社交工程攻擊的各種相關資訊。我們在台灣竟曾經發現過，有駭客根據單位網頁上的研討會聯絡資料來假造社交工程電子郵件的手法。

攻擊前的偵察讓攻擊者可以確認目標組織中的攻擊對象。這些人通常是位居目標組織內特定的職務，可能自身擁有重要文件或可以存取攻擊者所想要的資料。一旦確認，攻擊者會取得他們的電子郵件地址以作為攻擊之用。

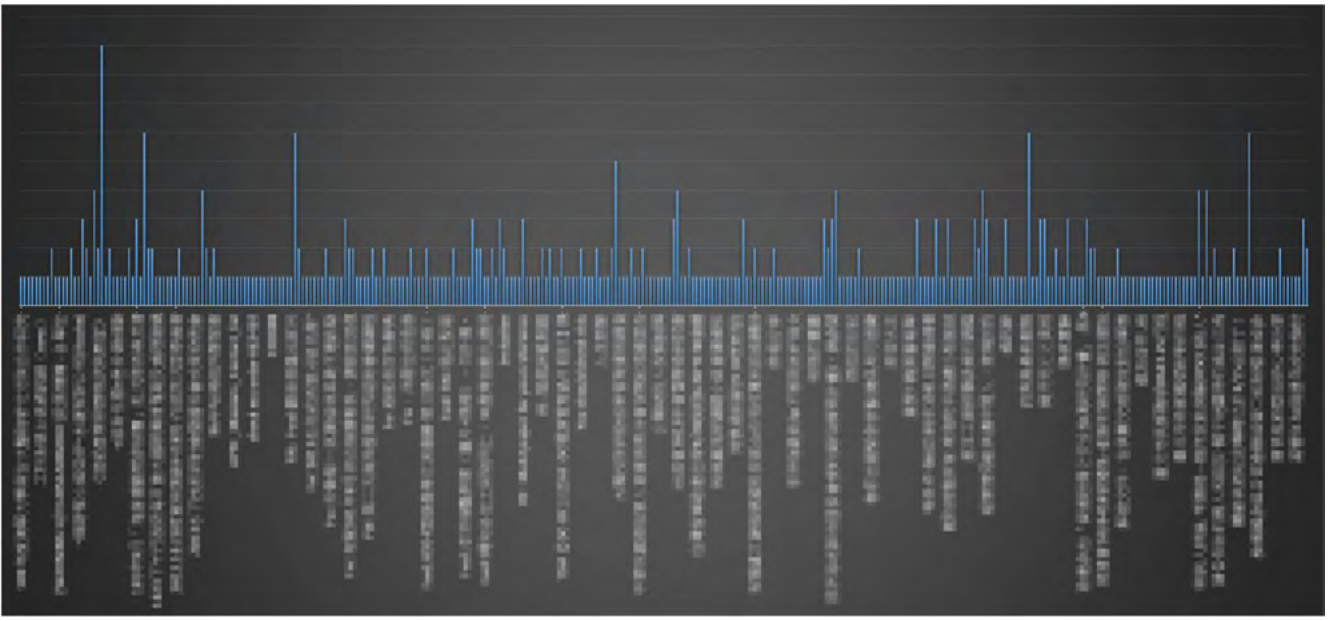


目標攻擊的進入點

社交工程電子郵件攻擊

社交工程技術

為了讓收件者可以相信誘騙用的電子郵件，攻擊者精心客製化社交工程電子郵件主旨、內容、或附件名稱，與目標使用者工作或生活習習相關的議題，只要用到一個或多個以上伎倆，就能夠說服收件者去下載和打開附加檔案。而根據我們在台灣所進行事件調查分析的結果，可以看出這些電子郵件的主旨和附檔名都相當的具有針對性，而且重複性極低。所以下面，我們就透過趨勢科技台灣 ESO 客戶所回饋的資料來進行分析，以了解社交工程攻擊在台灣的面貌。

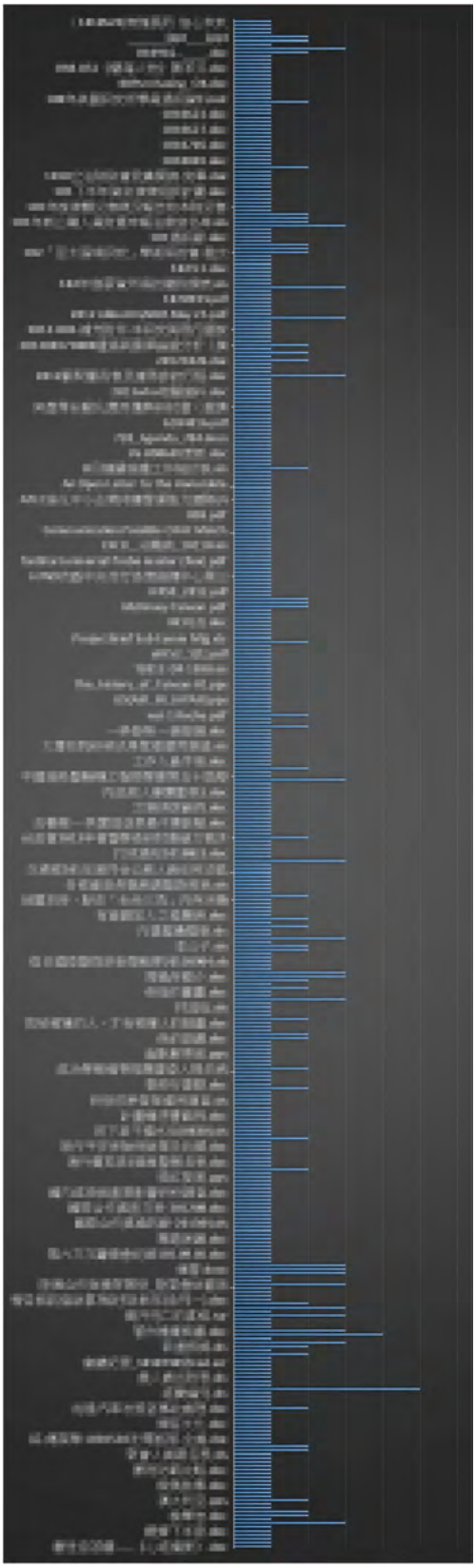


電子郵件主旨統計：APT 社交工程電子郵件重複性極低（為保護客戶隱私，主旨已做適當的遮蓋處理。）

首先，我們可以從上圖看出，APT 攻擊所使用的社交工程電子郵件重複性極低，同一個主旨不會用在超過五起不同的攻擊上。

社交工程
電子郵件攻擊

電子郵件附件統計：APT 社交工程電子郵件針對性極高

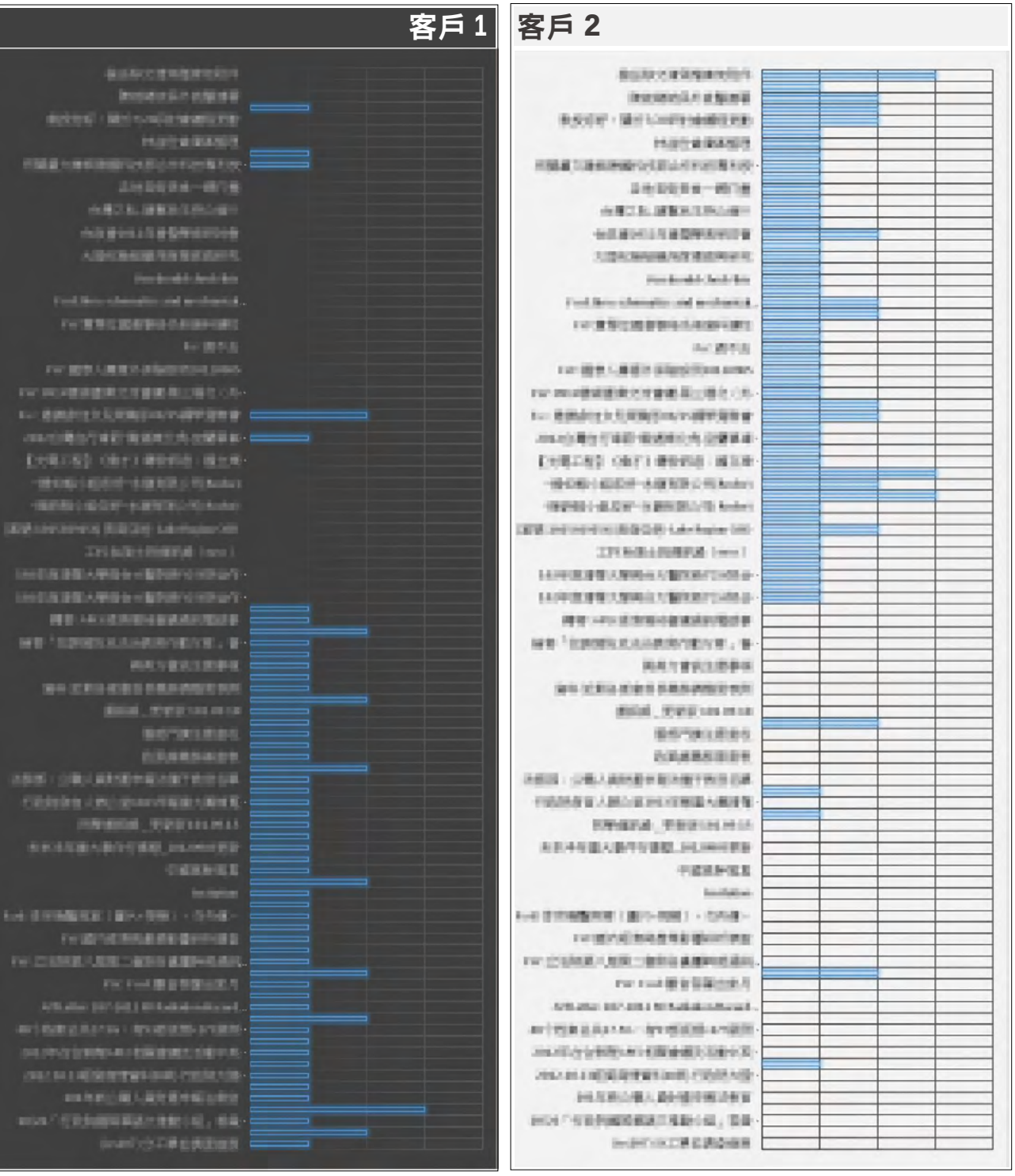


（為保護客戶隱私，主旨已做適當的遮蓋處理。）

接著我們可以進一步的從左圖分析發現，就算所使用的是相同的漏洞攻擊碼，附件檔案名稱重覆性也很低，代表駭客每次一次攻擊都是精心策劃，設計可吸引目標使用者開啟的附件名稱。

我們的研究團隊對於這些回饋的資料進行進一步的分析，看看是否相同體系的單位會收到一樣的電子郵件。結果可以在下頁圖裡看到，客戶 1 與客戶 2 是同屬相同體系的政府機關。但是他們兩者之間所收到的社交工程郵件主旨的相關係數是：-0.55616，代表了客戶 1 與客戶 2 收的信幾乎完全不同。可見駭客會針對不同受害者來設計不同的社交工程郵件。

社交工程電子郵件攻擊



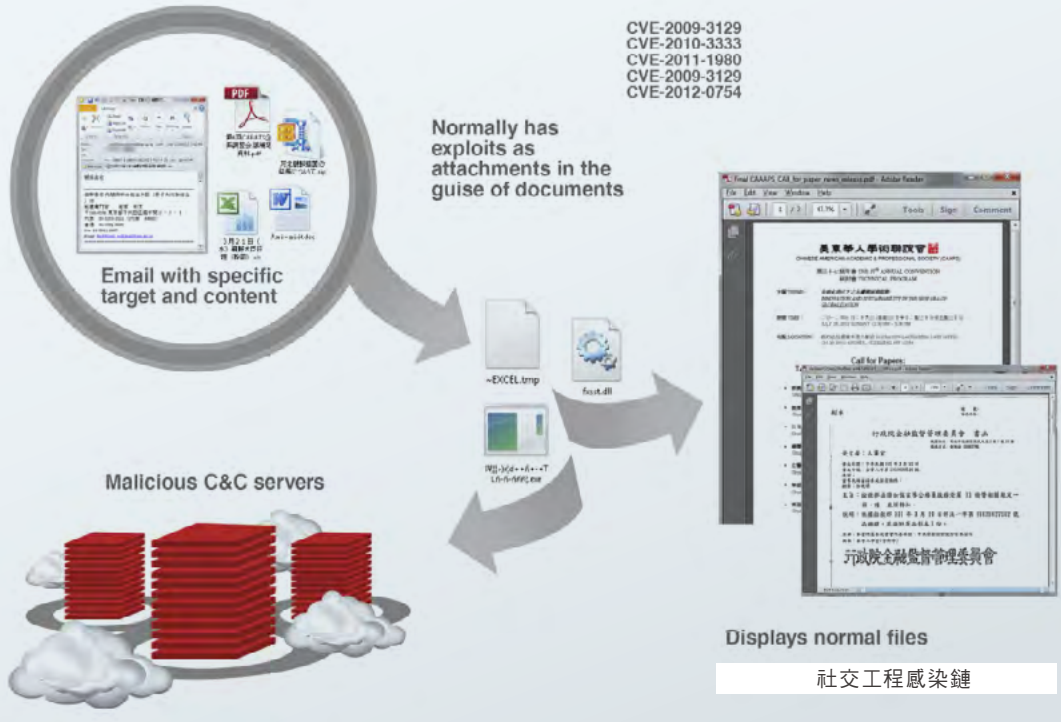
APT 社交工程電子郵件高度客製化。左邊欄位為主旨，右邊欄位為收到的數量。(為保護客戶隱私，主旨已做適當的遮蓋處理。)

社交工程
電子郵件攻擊

電子郵件附加檔案

一般的單位內電子郵件經常會加上附加檔案，這已經成為正常電子郵件通訊的一部分。常見的如微軟 Word 檔案。因為 Windows 的普及。連帶的微軟 Office 套件也非常的普及。還有可以跨平台的 PDF 檔案。有需多公司機關會使用 PDF 檔案，因為它支援多個平台，可以很容易地散布、歸檔和儲存。

而毫無疑問的，攻擊者也了解到利用電子郵件來散播攻擊工具是非常有效的作法。駭客還會利用許多其他常用軟體漏洞，像是 AdobeFlash Player、微軟 PowerPoint 和 Excel ，提升攻擊成功率。下圖是一般常見的社交工程電子郵件感染鏈。駭客製造出具有針對性檔案名稱的漏洞攻擊惡意文件，再透過社交工程電子郵件寄送給目標。要特別說明的是，APT 攻擊並不一定只會使用零時差攻擊，主要還是會用有效且可靠的漏洞攻擊碼。



社交工程感染鏈

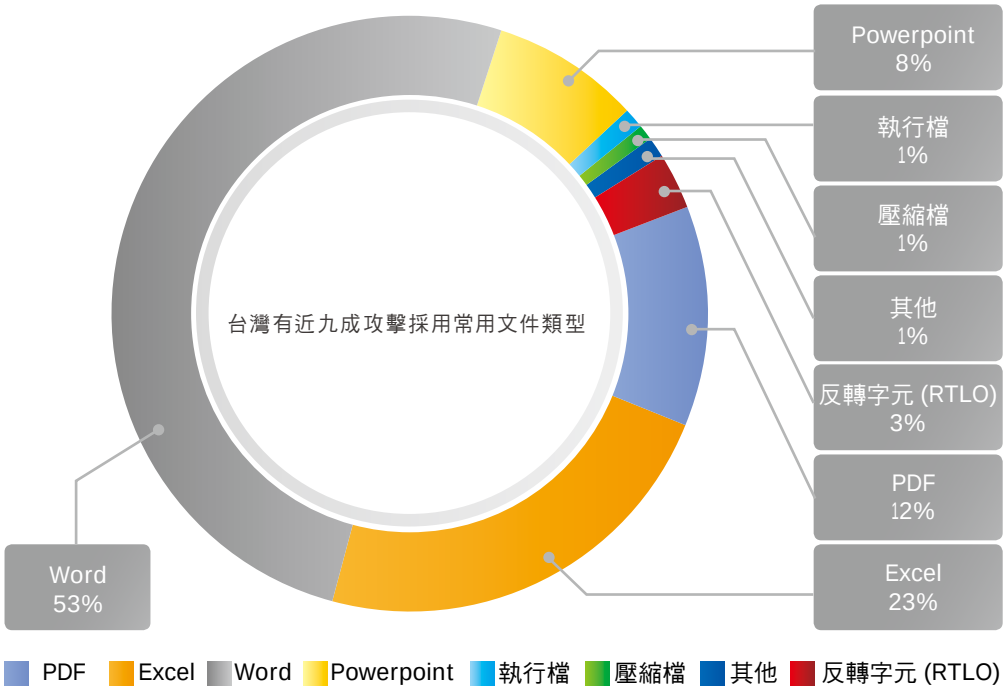
從全球 APT 攻擊資料來看，最常被使用的惡意附件檔類型是 Word 文件。而這一點也跟台灣的狀況相符。從下圖可以看出，有近九成的攻擊採用文件類型檔案。其中 Word 文件佔了一半以上（51%）。其次是 Excel（23%）和 PDF（12%）。執行檔（1%）並不常用於社交工程電子郵件。

社交工程
電子郵件攻擊

現今駭客僅少在 APT 社交工程電子郵件中夾帶可執行檔 (EXE 檔) 為附件是因為，通常帶有這類附檔的電子郵件通常會被防護設備，如郵件閘道器偵測並加以封鎖。

因此駭客會針對 EXE 檔案會先經過壓縮，如 RAR 和 ZIP，然後再傳送給攻擊目標。駭客也可能將壓縮檔甚至設有密碼保護，解壓縮密碼顯示在出現在電子郵件本文內，由使用者開啟時輸入，如此可以防止惡意附件被防護設備所偵測。

另外駭客也經常多種使用手法，針對惡意附件的檔案的顯示進行裝冒或混淆，例如假圖示偽裝成、利用檔名反轉字元 (RTLO)、或使用加入許多空格的檔案名稱來隱藏正確的檔名



小結

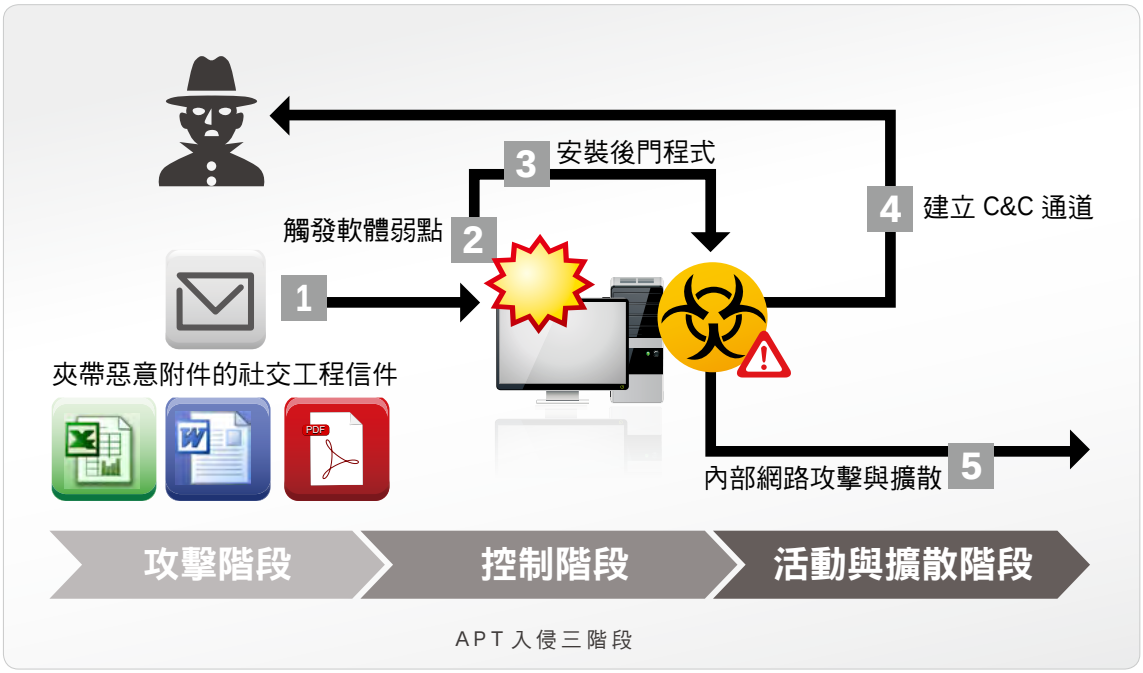
從本節對社交工程電子郵件的分析中可以看出，APT 的攻擊郵件會大量利用常用文件類型附件作為攻擊途徑。而經由針對 APT 社交工程電子郵件的數量、主旨、附件進行統計分析後可以得出三個結論。

- **小批量** 社交工程電子郵件每次的寄送量都不大，只寄送給目標受害者，不會像垃圾郵件一樣出現成千上萬的數量。
- **針對性** 社交工程電子郵件的主旨和附件檔案名稱都會針對目標受害者來特別製作，以求符合現實。
- **不重覆性** 社交工程電子郵件不會重複寄送給不同的單位。

所以從上述結論來看，現在常用於對抗垃圾郵件的機制，像是依據電子郵件主旨、附件名稱來進行阻擋的作法，用在對抗 APT 攻擊時並不具有實務意義。

APT 惡意程式

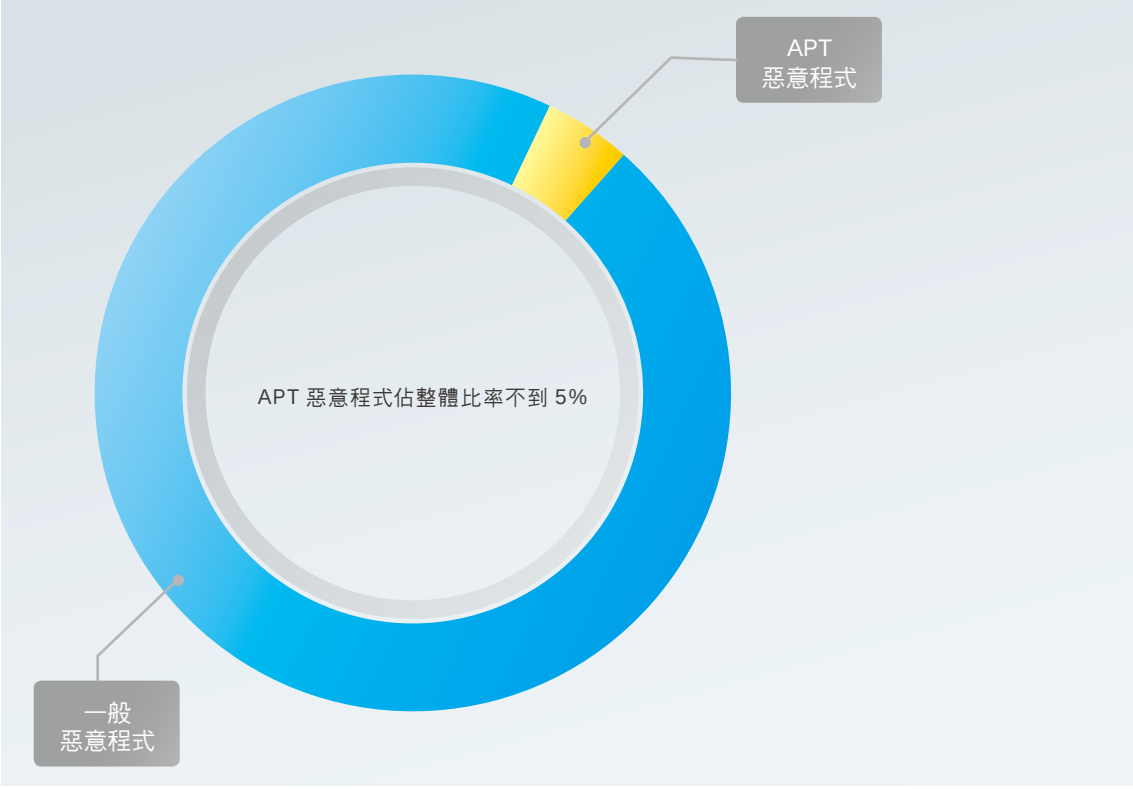
接下來我們從 APT 所用的惡意程式來看 APT 的特性。APT 主要可以分為三個階段 – 攻擊階段、控制階段、活動與擴散階段。攻擊階段就是想辦法進入目標網路，通常是透過社交工程電子郵件。一旦社交工程電子郵件順利進入目標網路，並且讓受駭者執行成功。那麼就會進入了下一個階段 – 控制階段。駭客會想辦法控制受駭系統，藉由安裝後門程式（例如遠端存取木馬或是一些駭客工具）來遠端存取受駭網路。在這階段，攻擊者可以利用遠端存取木馬來分析目標網路。包括了解是用什麼作業系統和受害者電腦上所執行的安全軟體，以進入第三階段 – 活動與擴散階段。此時駭客已經掌握了重要帳號和受駭網路，可以存取本地網路、代理伺服器和其他網路內的機器。基本上已經可以為所欲為，不一定需要後門程式了。而之前所獲得的資訊也會被用來維持持續性，進行橫向擴散，持續的從目標網路獲取資料。



APT 入侵三階段

APT 惡意程式

所以不要將 APT 所使用的惡意程式和一般的惡意程式混為一談，認為可以使用傳統的安全措施來對付它們。大部分用於 APT 攻擊的惡意程式都是量身打造及經過測試，確保可以順利避過目標的防毒方案，好讓自己不會出現在安全軟體的雷達上。加上許多惡意程式都會在潛入後的數小時內變形，讓它們更容易避開病毒碼掃瞄，好繼續進行橫向擴散。而且也因為 APT 惡意程式的針對性，所以 APT 惡意程式的數量跟一般惡意程式相較起來要少得多。接下來我們也一樣從趨勢科技的台灣 ESO 用戶所回饋的資料來分析 APT 惡意程式的特性。我們可以從下圖裡看出，APT 惡意程式佔整體的比例不到 5%。

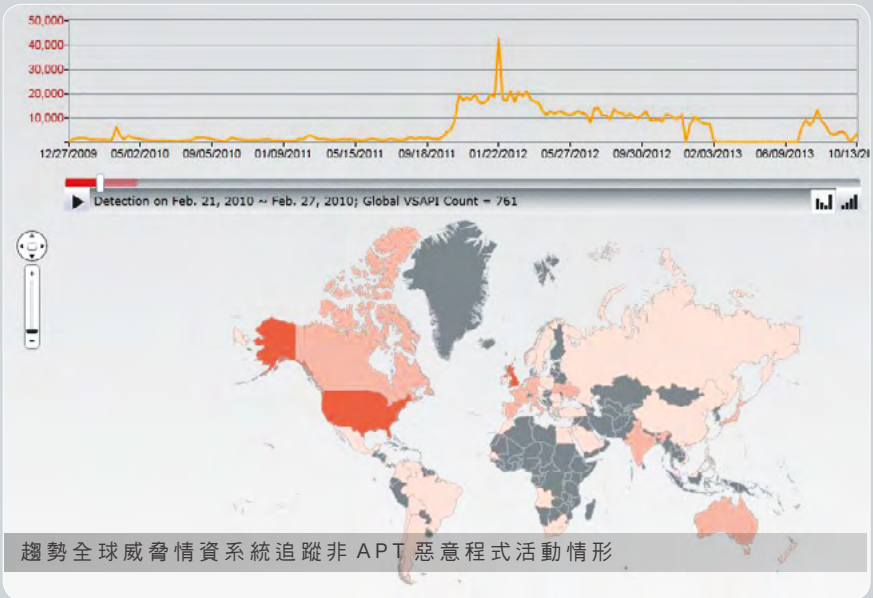


同時它的行為模式也和一般惡意程式大不相同。不像一般惡意程式的目的是盡可能的散播以找到最多的受害者，讓利益最大化。從趨勢科技的全球威脅情資系統可以看得出來，一般惡意程式會從開始就一直維持在高峰期，尋求最大的感染數量。但是 APT 惡意程式則是會盡量保持低調，務求一擊必中，以免因為被發現而加入了黑名單或是病毒特徵碼中。所以我們可以從另一張圖看到，APT 惡意程式會一直處在潛伏狀態，直到遇到機會才會出現，接著繼續潛伏。這樣才可以盡可能的不被人注意。

而且從趨勢科技的全球威脅情資系統還可以看到另一個事實，就是 APT 惡意程式具備有地域性，所以特定的 APT 惡意程式都只會出現在特定國家。並不會像一般惡意程式一樣會想辦法進行全球化的擴散。所以綜合以上幾點，我們都可以了解到 APT 惡意程式是非常客製化，而且具有針對性。並不是傳統的防毒措施所可以防禦的，因為它的設計就是要特製來穿透傳統的防禦措施。

APT 惡意程式

趨勢全球威脅情資系統追蹤 APT 惡意程式活動情形

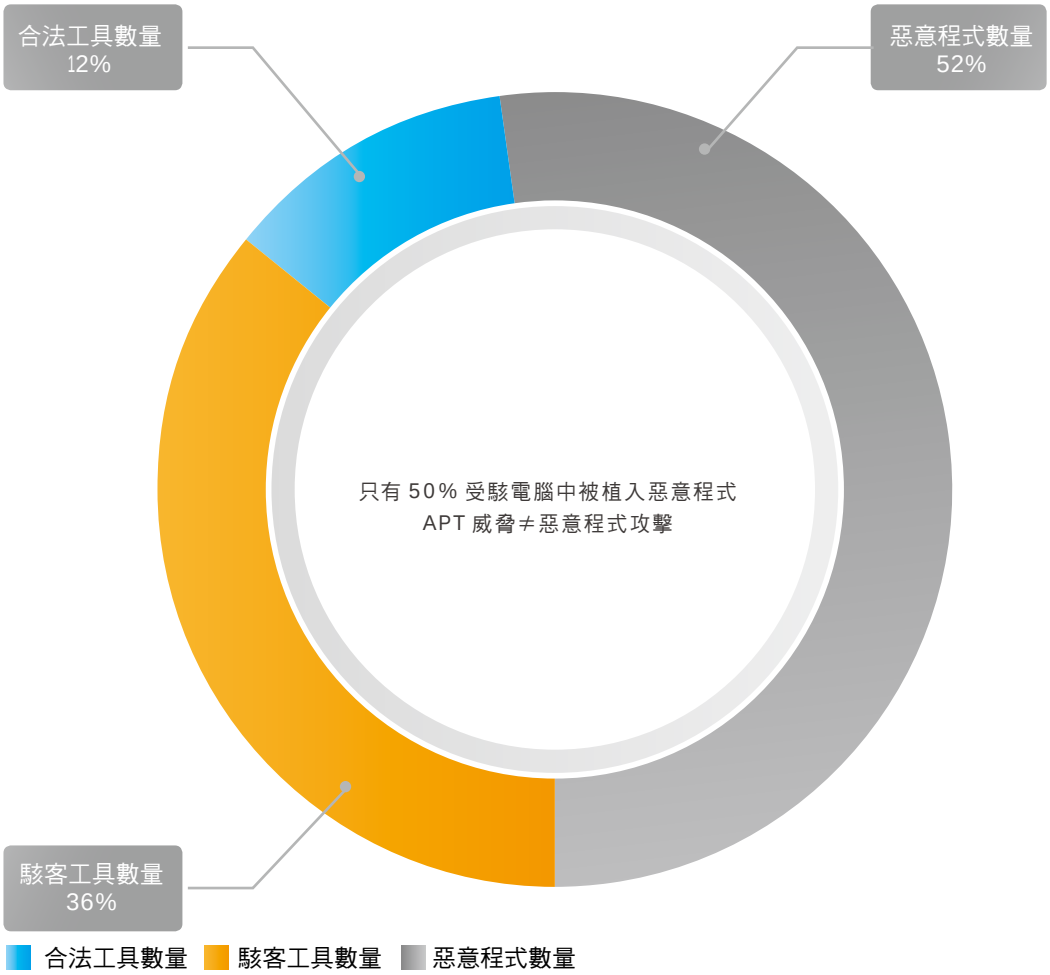


趨勢全球威脅情資系統追蹤非 APT 惡意程式活動情形

另外，APT 事件不僅僅不會用一般的惡意程式，為了保持低調性，有時甚至不會使用一般定義上的惡意程式，尤其是到了擴散階段，駭客已經不需要靠後門程式來取得遠端控制能力，可以進一步的降低被發覺的機會。從趨勢科技在台灣進行 APT 事件處理所得到的資料分析可以看出，只有一半的受駭電腦上可以找到惡意程式，

有許多是使用（合法）駭客工具，讓它更加不容易被安全軟體所偵測。所以在受電腦上單靠一般的自動化偵測或清除工具並無法完全找到並解決問題，這也再次說明傳統基於特徵碼的端點安全防護並不足夠。攻擊者可以製作並測試出多面向的目標攻擊以用來閃避這些產品的偵測，傳統防禦是整體安全防護的一個重要部分，但必須包含在更整體的防護策略中，包括啟發式偵測、動態信譽評比服務和主動式網路監控，互相搭配來進行防護。

APT 惡意程式



駭客工具

駭客工具是程式行為本身無惡意行為，例如接受駭客操控、向外傳輸資料等，但被駭客做為惡意行為用途。這類駭客工具不會隨時執行或啟動，這意味著在 APT 事件的處理調查裡更難發覺。此外，它也讓攻擊者省下自己開發工具的麻煩。常見到的駭客或合法工具有：

密碼回復工具	用來將應用程式或作業系統存放在本地硬碟或註冊表內的密碼或密碼雜湊值取出的工具。通常被用來複製或偽造使用者帳號以取得管理者權限。雜湊值注入（Pass-the-hash）是種常見的方式讓攻擊者透過偷來的密碼雜湊值取得管理者權限。
使用者帳號複製工具	當攻擊者取得密碼後，用來複製使用者帳號的工具。一旦取得足夠權限，攻擊者就可以繞過系統的安全措施，執行惡意企圖。

APT 惡意程式

檔案操作工具	用來操作檔案（複製、刪除、修改時間標記、搜尋特定檔案）的工具。它被用來修改存取過檔案的時間標記或刪除特定組件以掩飾入侵的痕跡。它也可以讓攻擊者透過副檔名搜尋所需要的關鍵文件。
排程工具	用來關閉或建立排程的軟體。這可以讓攻擊者透過關閉軟體更新排程以降低受感染系統的安全性。同樣地，也可以做為惡意用途。例如，攻擊者可以建立排程以在特定時間自動竊取檔案。
FTP 工具	用來執行 FTP 傳輸的工具，像是將檔案上傳到特定 FTP 站台。因為在網路上的 FTP 傳輸看起來比較不那麼可疑，有些 APT 事件的幕後黑手會偏好將竊取來的資料上傳到遠端 FTP 站台，而不是上傳到中繼站。要特別指出的是，有好幾個合法的 FTP 應用程式也被網路犯罪份子所用。
資料壓縮工具	這些工具本身並非惡意，也不被視為入侵用的工具。在大多數情況下，這些都是合法的檔案壓縮工具，像是 WinRAR，只是被攻擊者用來將多個偷來的檔案加以壓縮合併。這可以在資料竊取階段，幫攻擊者將偷來的文件合成一個單一檔案上傳。在少數情況下，我們也看到這些應用程式被組合設定來壓縮預先定義好的一組檔案。

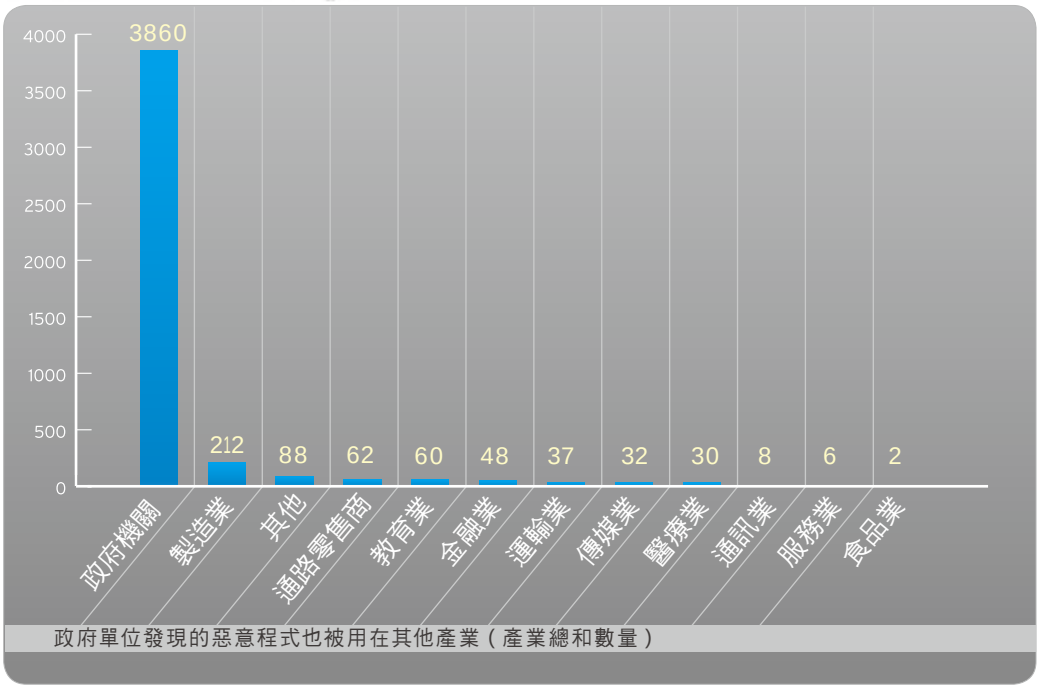
因為這些是灰色軟體，甚至是合法工具，所以一般的防毒軟體並不會加以偵測。這時候就必須要靠 IT 團隊可以充分掌握自己的內部網路系統，去察覺原本不存在的排程或工具軟體的出現，才有辦法去察覺駭客的潛伏。

產業分析

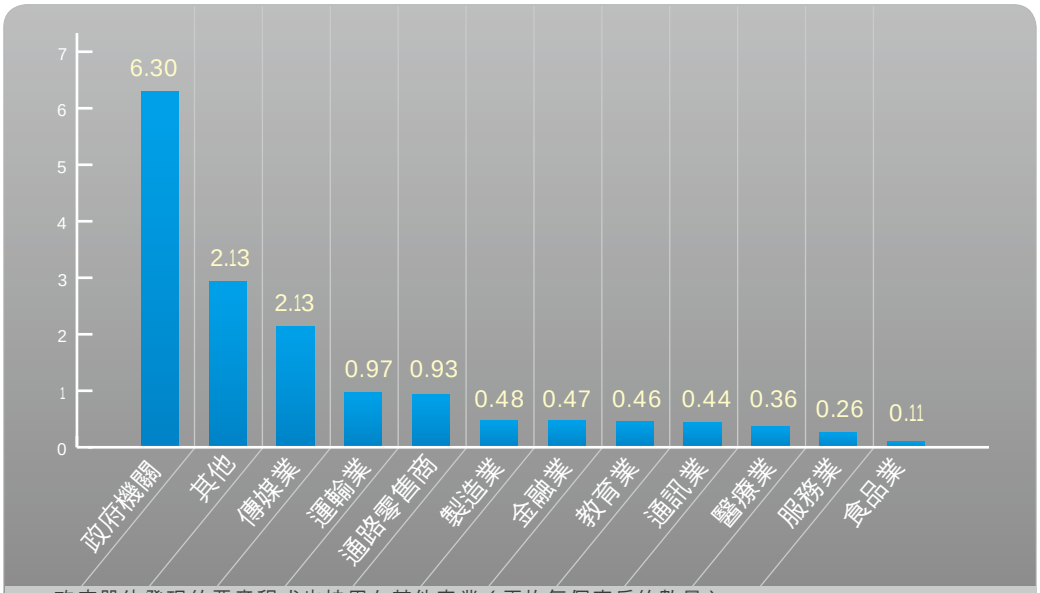
接下來，我們對那些可被偵測到的 APT 惡意程式數據來進行分析。一般可能會認為，在台灣會遭受 APT 攻擊的目標是政府機關。但是這也讓政府機關有較高的安全意識，會願意配合資安事件的調查，並且反饋惡意程式來進行分析。所以雖然這張圖表裡呈現的 APT 惡意程式主要來自政府機構，但這原因也是因為反饋來源大部分來自政府。所以我們這節所想要分析的是，到底 APT 事件是不是只會發生政府機構，這些攻擊和其他產業之間有沒有什麼關連。

從下圖的數量分布圖來看，最高的是政府機關，接著就是高科技製造業，而接下來的其他各種產業的受害單位其實都與政府機關有關係。我們可以從惡意程式樣本分析看到，這些從政府機關所採樣來的惡意程式，也會出現在其他產業上。代表其他產業也都會被連帶的當成目標攻擊。

APT 惡意程式



政府單位發現的惡意程式也被用在其他產業（產業總和數量）



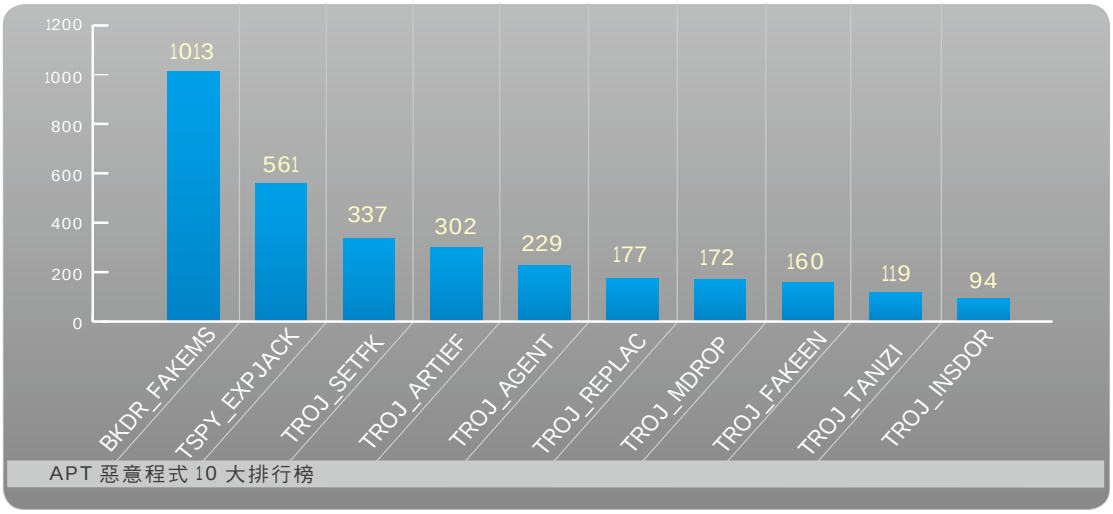
政府單位發現的惡意程式也被用在其他產業（平均每個客戶的數量）

而接下來，我們在從 APT 惡意程式的排行榜來進行分析。這十大 APT 惡意程式中主要可以分為兩大類，一類是載入器（Downloader），像是 TROJ_MDROP。這類惡意程式通常是隨著社交工程電子郵件進到受駭網路內。一旦入侵成功，就開始對中繼站進行連線，去下載真正的後門程式來進行後續的攻擊。

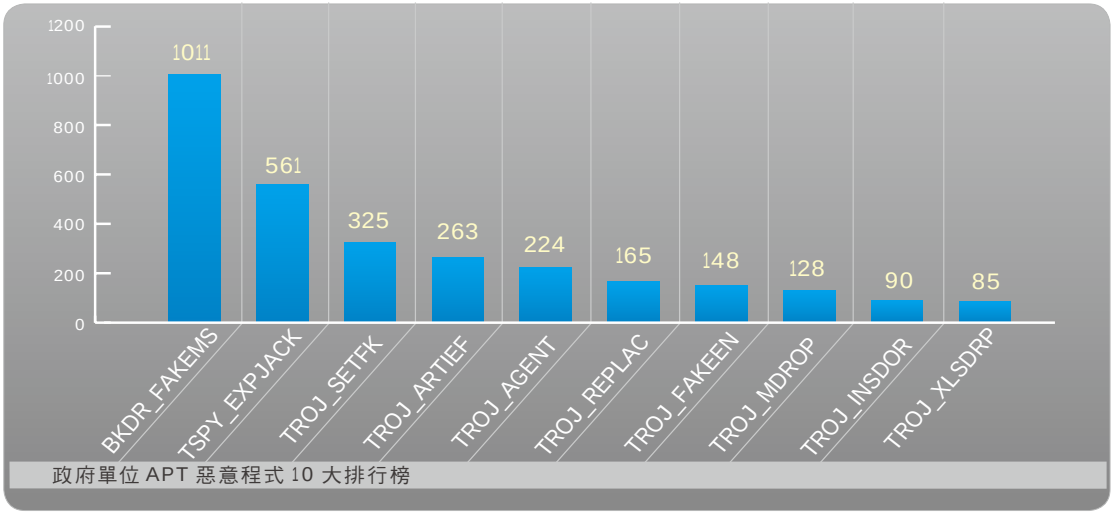
第二類就是後門程式（像是 BKDR_FAKEMS），真正的 APT 惡意程式主體。這類程式通常不會出現第一波的攻擊內，而是經由載入器下載而來。所以這類程式通常也很難被偵測到。如果目標單位沒有在第一波攻擊時即時擋住，而讓這些後門程式被下載放入內部網路，這時就很難被偵測到，多半只能等到事件調查時才會被發現。

APT 惡意程式

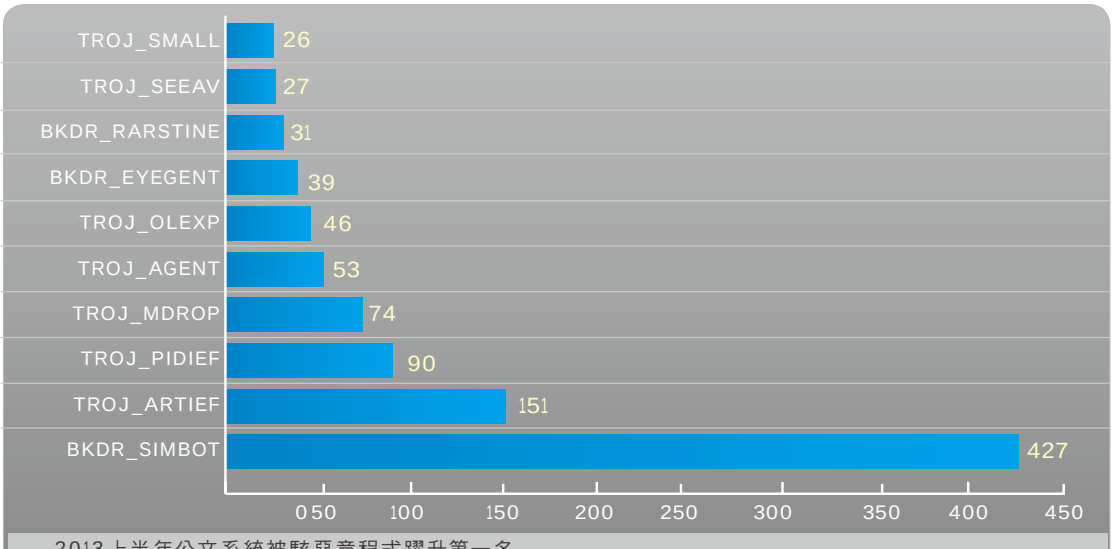
而我們也可以看到，雖然底下這兩個十大 APT 惡意程式的排行大致相同。但是從第七名之後就有所不同。這也代表了這些惡意程式的攻擊目標主要在政府以外的產業。所以也再次的證明了政府以外的公司機關也是被攻擊的目標。而從這個事實我們也可以了解，民間企業的確會是 APT 攻擊的目標。駭客組織也很有可能會針對民間企業來客製化惡意程式以進行攻擊，只是因為回饋的數量不夠，所以沒辦法確知是否有單獨針對民間企業的 APT 惡意程式。



APT 惡意程式 10 大排行榜



政府單位 APT 惡意程式 10 大排行榜



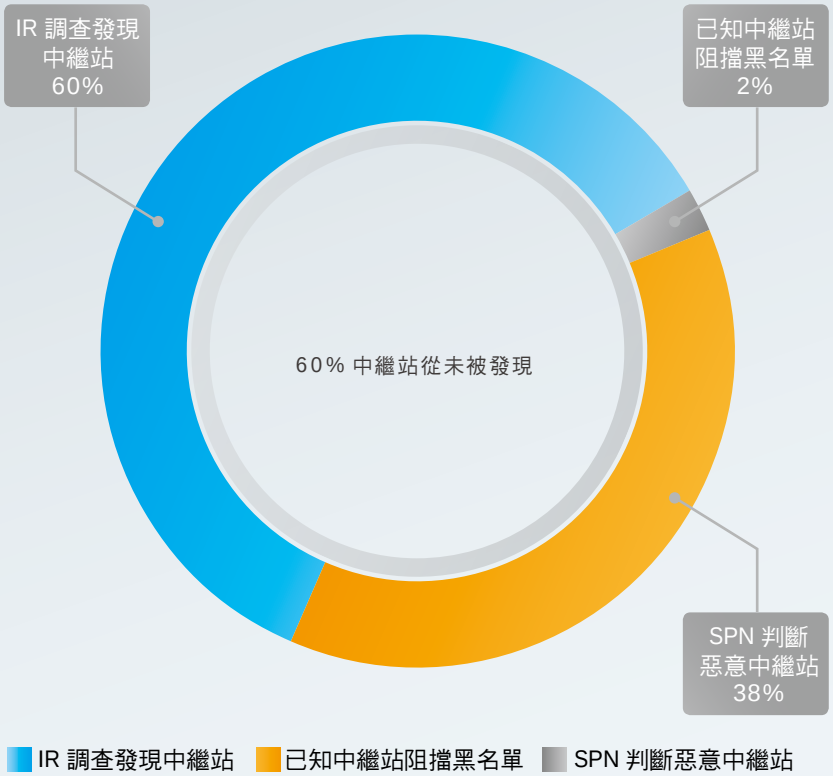
2013 上半年公文系統被駭惡意程式躍升第一名

APT 惡意程式

中繼站（C&C）

前面提到，APT 惡意程式會透過中繼站來下載後門程式以進行進一步的攻擊。所以傳統的防禦思維會希望透過偵測中繼站連線來發覺 APT 攻擊。但是就和社交工程電子郵件和 APT 惡意程式一樣，APT 所使用的中繼站也一樣具有非重複性的特性。所以我們在下圖裡可以看到，APT 所使用的中繼站出現在已知的中繼站黑名單內僅僅佔了 2%。透過趨勢科技的全球威脅情資系統可以偵測到 38% 的 APT 中繼站。不過還是有高達 60% 的中繼站是在事件處理調查時才發現的。這再次說明了 APT 高度針對性和潛伏的特性。

所以應該如何去對抗這樣針對性和愈發客製化的工具？這時候就需要有客製化的防禦，首先要在網路環境內可以客製化黑名單以偵測和封鎖這些 APT 中繼站。而建立客製化黑名單的方式就必須要靠主動式監控技術，加上自動回饋機制以取得即時的分析結果。才可以對 APT 攻擊產生即時的反應，並加以偵測或封鎖。



APT 惡意程式

小結

因為駭客組織在進行攻擊時會針對特定目標進行客製化，因此傳統防禦很難偵測到 APT 惡意程式，而且 APT 惡意程式的總量也佔全體惡意程式的極小部分。因為的它的存在只針對特定的目標。這一點我們也可以從趨勢科技的全球威脅情資系統裡面看出來。APT 惡意程式的分佈相當的具有地域性，不會大規模的出現在全球各地。

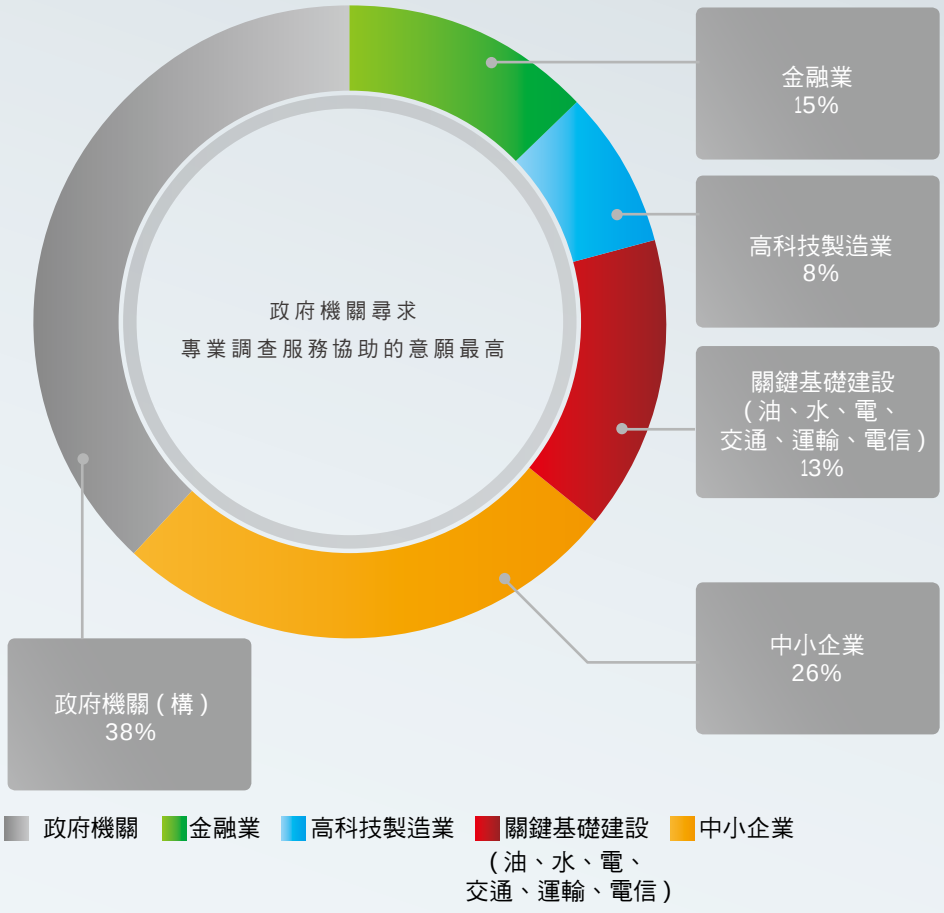
目前的 APT 惡意程式主要來源是泛政府機關，包括一般的政府機關以及跟其有業務往來的企業單位。但這種某程度上也代表了其它產業缺乏 APT 防禦機制與警覺性。因為我們可以看到，相同的 APT 惡意程式會出現在製造業、金融業等，代表 APT 攻擊是全面性的，並不是針對政府機關。而且我們也可以看到有些 APT 惡意程式的主要攻擊對象是民間企業，而非政府機關。所以如果一般企業有對 APT 攻擊的正確認識，可以建立主動監控系統，加上自動回饋機制以取得即時的分析結果，就可以更加掌握網路內 APT 攻擊的狀況。這邊的自動回饋機制並不單指可疑的程式，還包含了可疑的社交工程電子郵件和網路活動。

資安事件調查

我們在前面分析了APT事件的攻擊手法和行為模式，攻擊者會如何進行入侵，控制和活動擴散。接下來，我們就要從受駭者的角度來進行分析。

前面提到過，因為政府機關是駭客的主要攻擊對象。所以政府機關對於駭客入侵有比較高的認識與了解，也比較願意去面對入侵的事實並且尋求幫助。所以在趨勢科技台灣資安調查小組的經驗裡，政府機關尋求專業調查服務協助的意願最高。這也是為什麼我們可以在下圖看到，接受資安事件調查的對象中，政府機關以及泛政府機關的關鍵基礎設施佔了近一半。接下來是金融業和高科技製造業。

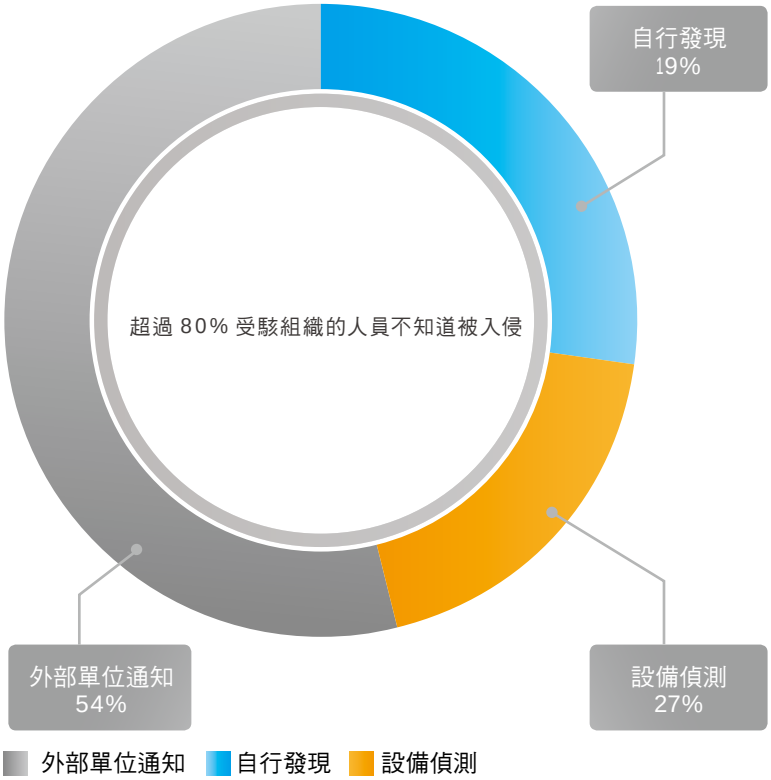
令人驚訝的是中小企業也在榜上有名。一般人可能會認為只有大型企業才是會被攻擊的目標，不過中小企業還是會有駭客覬覦的資料以及可以獲利的地方。在我們的事件調查過程中發現，中小企業主要是會遭受民間型駭客組織的攻擊。



資安事件調查

如何發覺被駭

絕大多數的受駭組織其實不容易發現自己的環境遭受到攻擊。大部分的組織是經由外部單位通知（54%）才發現，例如政府機關有行政院國家資通安全會報的技術服務中心負責監看政府網路，當發現異常網路流量時會通知該單位。接下來是經由設備的偵測（27%），例如安裝趨勢科技的 Deep Discovery 之後發現可疑的入侵跡象。而能夠自行發現遭受入侵的只佔了 19%。

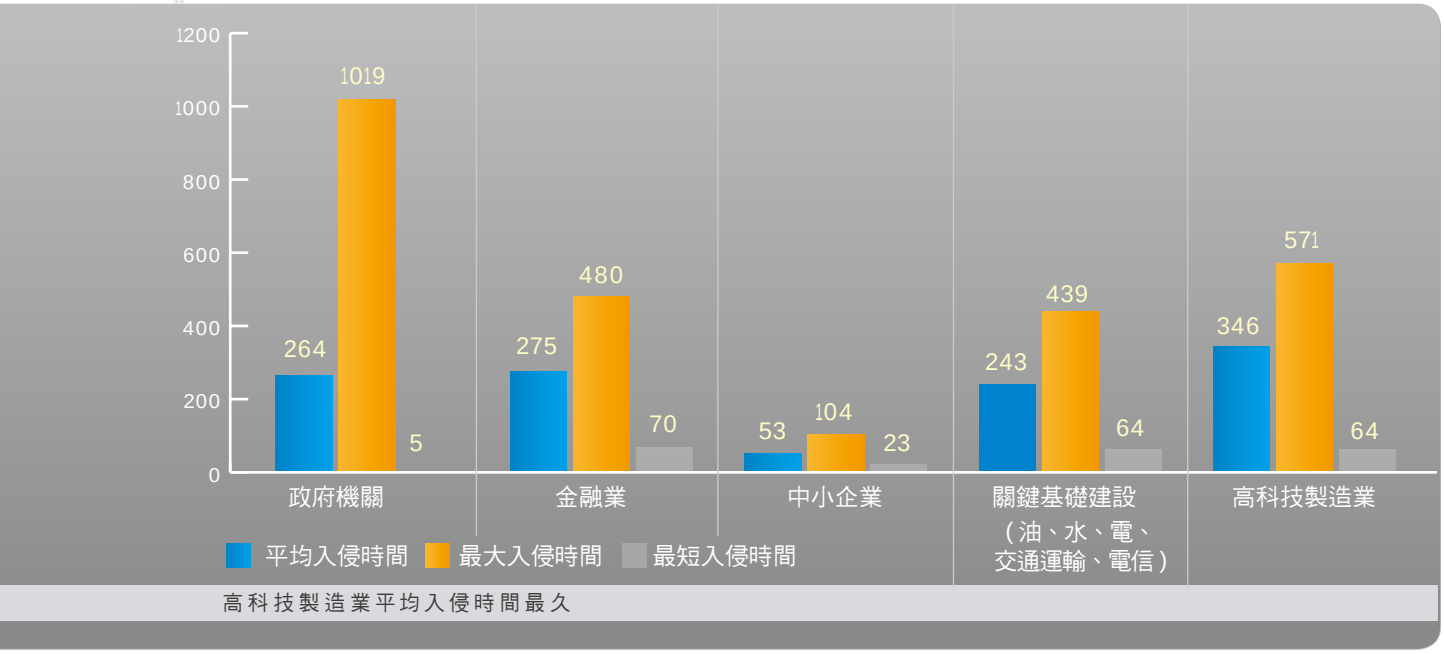


何時發覺被駭

因為 APT 的隱匿性，所以當這些受駭單位發覺並且進行事件調查時，駭客往往都已經入侵了一段時間。從下圖中我們可以看到，高科技製造業的平均入侵時間最久（346 天），接下來是金融業的 275 天，第三名則是政府機關的 264 天。

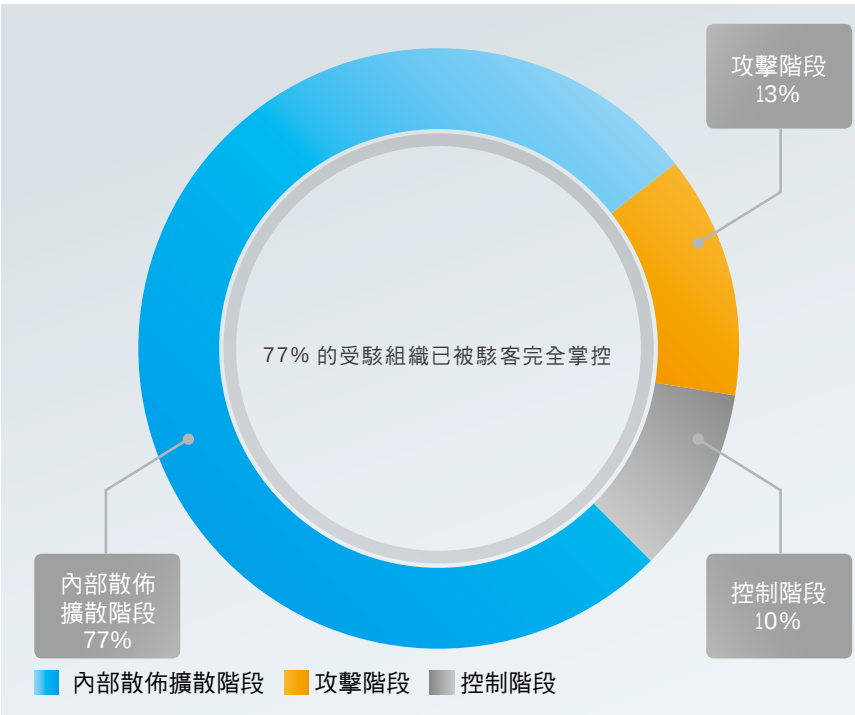
從這個數據我們可以再度發現到，民間企業遭受到攻擊的機會絕對不會比政府機關還要來得少。而且因為一般企業對於 APT 的認知程度較低，一方面認為自己不會是被攻擊的目標，另一方面也偏向傳統的安全防禦觀念，所以沒有專責的單位負責監控，而防禦的能力也較為不足。所以也造成了一旦受駭，往往嚴重程度就超過想像，所以自然的發覺入侵的時間也會變得比較長。

資安事件調查

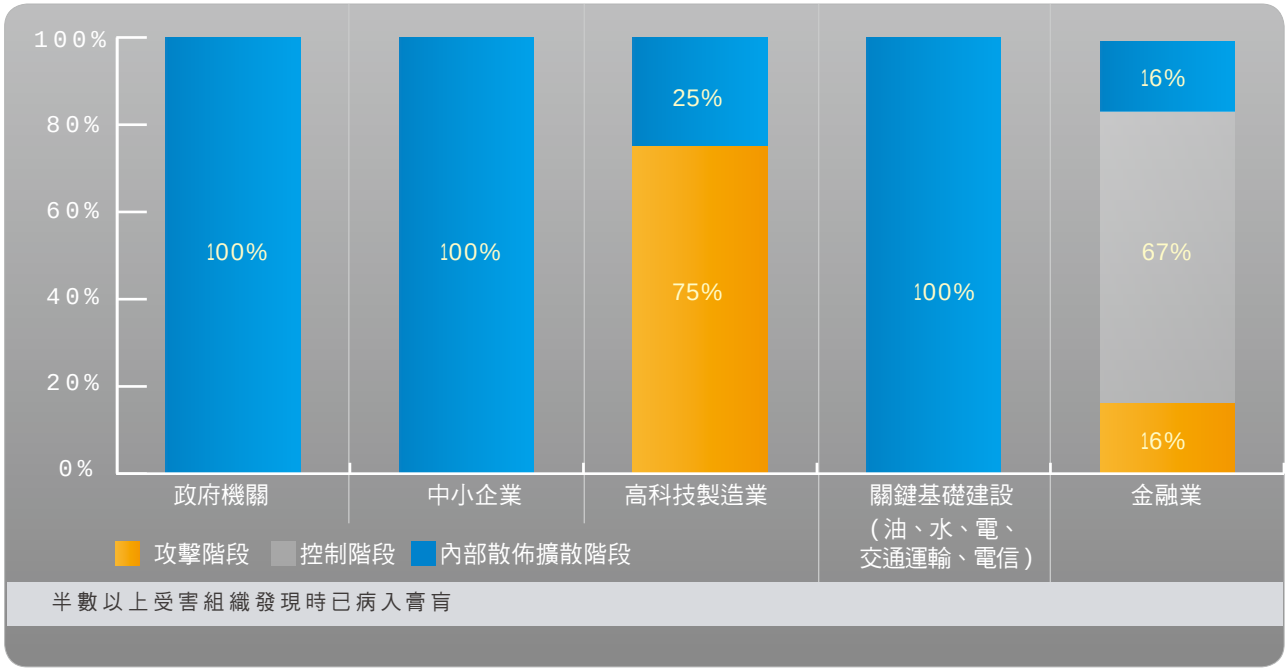


高科技製造業平均入侵時間最久

也因為往往要入侵一段時間後才會被發覺，所以等到我們的團隊進行事件調查時，被駭組織通常已經病入膏肓了。根據趨勢科技資安事件處理的資料，能夠在攻擊階段就加以發現的組織只有 13%。代表這些公司機構可以在駭客進行社交工程攻擊時就察覺，進而展開應變措施。有 10% 的組織是在控制階段時發覺，也就是駭客還在使用後門程式，開始要進行橫向擴散去掌握重要帳號或伺服器時偵測到。但是絕大部分的公司機構發覺時都已經在內部擴散階段了。代表此時駭客已經完全掌握了對內部系統網路的控制，可以說已經可以為所欲為的階段。



資安事件調查



進一步來看每個產業別 APT 受害深度 。政府機關、中小企業、關鍵基礎建設從我們調查的案件中 ，每一個都是已經處於最後的散布擴散階段 。而高科技約有 25% 是到了散布擴散階段，剩下 75% 是一但發現攻擊，例如有收到 APT 攻擊信件，立即請專業人員服務 ，所以得以受陷不深。金融業有 16% 處於散布擴散階段，67% 已經被駭客控制單點主機，16% 則是處於攻擊階段 。政府之所以會完全淪陷，某種程度也正因為駭客攻擊最猛烈、最積極，同時操控也最頻繁。處於這種高密度的攻擊下，想要倖免也很難。

小 結

從趨勢科技對台灣受駭單位所進行的資安事件調查中可以了解到，高科技產業、關鍵基礎設施和金融業的攻擊來源與政府單位所遇到的相似，而且受駭深度不亞於政府機關。只是因為政府機關對於 APT 的認知較為深切，同時也有專責單位負責監控並進行通知，所以也比較願意配合進行調查。而民間企業往往不願意面對遭受 APT 攻擊，或僅想當做一般病毒攻擊處理，也往往會錯失偵測良機，使得發現時間往往拖得很長。

而中小企業則是遭受到民間組織型駭客的攻擊最為嚴重，造成財務上的鉅額損失。所以各個產業都可能是被攻擊的對象，只是攻擊的來源或是被覬覦的目標不同。

而再討論到為何無法使用傳統的安全防禦技術來對抗 APT 攻擊。相同的，傳統的網路偵測技術是安全防護的重要一環。但像是網路入侵防禦系統以及次世代防火牆等傳統網路偵測技術並無法處理客製化的攻擊活動。因為所用來連線的中繼站或進行攻擊的網路協定都不在黑名單之內。尤其是當駭客已經進入網路內部，取得足夠權限來進行橫向擴散時，這些傳統的網路偵測技術更是無用武之地，因為此時都是用正常權限來對重要系統及檔案進行存取。

而且如果想要當做一般病毒事件處理，依靠自動化的惡意程式清除工具只能看到攻擊的冰山一角，結果讓駭客可以繼續留在網路內部活動。所以過度依賴這類工具只會成為惡性循環。還是要強化對 APT 的認識，可以主動監控，自動回饋分析並加以事件調查才能有效解決。

結論

在 2011 年，全球的 IT 資安預算達到 550 億美元，並在 2012 年增長至 600 億，但是我們還是可以在這兩年間看到不少國際化的大型企業出現嚴重的資料外洩事件。從已經被披露出來的 APT 事件分析中我們可以看到，這些受駭公司通常都已經安裝了傳統的安全防護，像是基於特徵碼的端點安全產品，入侵偵測防禦系統和防火牆等。讓人不禁要去思考，這些攻擊到底是如何繞過現有的安全防禦。

而這份白皮書就從攻擊面向來分析台灣的 APT 威脅現況，並且提供了答案。從社交工程電子郵件的主旨、檔案，APT 惡意程式以及駭客所用的中繼站等資料分析，在在都顯示出 APT 的針對性、客製化、地域性與潛伏性。這也是為什麼傳統的安全解決方案並無法有效的去偵測或反應 APT 攻擊。當面對這些針對性及量身打造的攻擊時，傳統防禦如防火牆、入侵偵測防禦系統和防毒都已經不足以偵測及封鎖此類攻擊。還是需要能夠對內部網路進行主動監控，察覺任何可疑的活動。配合自動回饋及分析機制去處理可疑的程式、郵件以及網路活動。加上對分析結果進行事件調查才能夠完整的解決 APT 事件。

從 APT 的事件處理調查結果裡也可以看出，在台灣，APT 並不是只有政府才會面臨到的問題。對於民間企業來說，APT 也是現在進行式的威脅。所以無論是政府、電信、金融、製造、醫療保健或服務業，不同機構都必須要保護其貴重的知識產權及數據資產。了解威脅及攻擊者的演變是偵測、對付及阻止此類攻擊的第一步。我們希望可以藉由這份綜觀的 APT 情資分析來加深對威脅全貌的了解，以作為資安防護策略訂定的參考依據。