進階目標式攻擊的 Mandiant 威脅報告簡介

原文出處：HELP NEY SECURITY (CERT 譯)

(http://www.net-security.org/secworld.php?id=14590)

Mandiant 發佈了它的第四次年度 M-Trend 報告，其中詳細記錄駭客們用來入侵組織和竊取資料的策略。這也突顯了組織對於事件回應的最佳實踐，且成功打擊了各家菁英駭客們。

今年的 M-Trend 也包括了 APT1 威脅團體的總覽和一個超過三千的技術指標的連結，這是 Mandiant 已經提供組織用來支撐他們的防禦。

Grady Summers, Mandiant 的副總裁同時也是這份報告的作者之一，提到"我們已經觀察到第一手消息，一個有經驗的駭客只要有足夠的時間和準確的判斷就可以入侵各種網路。每家公司如果持續問自己'我們安全嗎'，這樣是不夠的。他們該提問的是'我們怎麼知道我們今天沒有被入侵？我們會在何時知道？如果被入侵，我們該怎麼做？'"

以下是這份報告的焦點：

- **大約三分之二的組織會在他們被外部網路入侵後而學到教訓**

目標式攻擊可以一直避開防禦，但是各家組織越來越熟練於靠他們自己來發現這些攻擊。至少有 63%的受害者已經了解他們被侵害了外部組織，像是司法單位。

- **典型的進階攻擊會隱藏他們的行蹤長達 8 個月之久**

駭客們會用大約 243 天在受害者的區網上直到他們被發現，這比 2011 年還少了 173 天。縱然組織已經把從被入侵到發現之間的平均時間縮短了 40%，但有許多組織還是要等到入侵了好幾年後才發現。

- **越來越多駭客在去找外包的服務提供者來取得連到受害者們的連線**

就如同企業在金融、會計、人力資源和採購方面都持續使用外包的商業服務來替代，越來越多專業的駭客團體也利用他們的人脈來取得進入各家企業的後門。

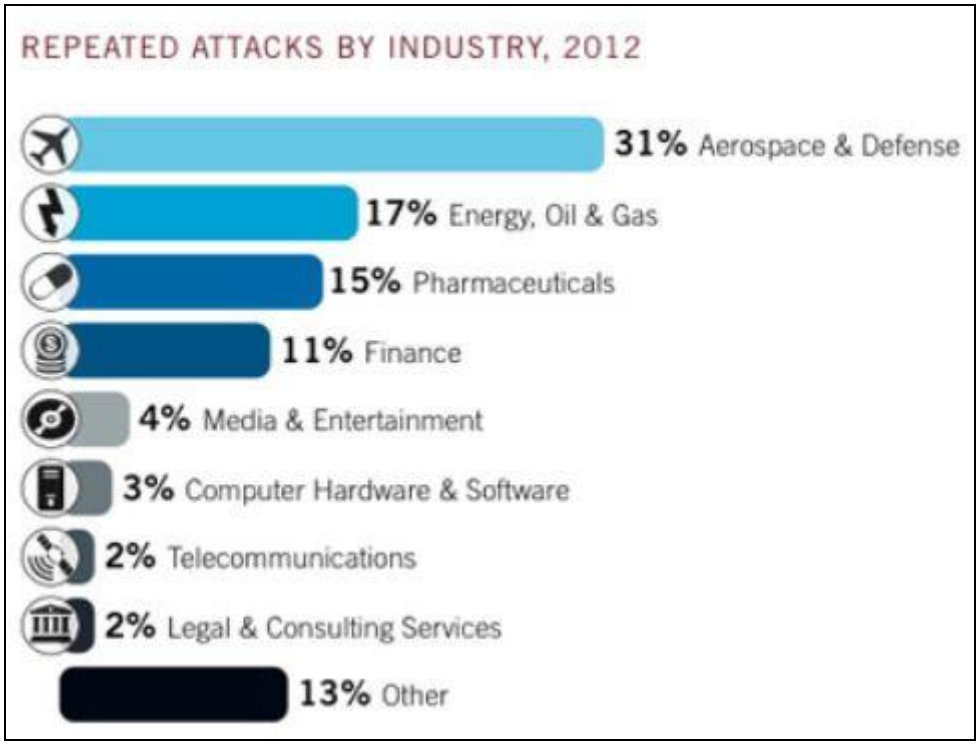
- **駭客們利用完善的網路偵查來幫助他們更快、更有效的營運受害者的網路**

駭客們經常去竊取網路基礎建設、進行中的演算法和系統管理者的資料，且會以他們事先調查的資訊來當做指引，幫助他們更快的入侵網路和了解系統的錯誤配置。

- **使用進階持續性滲透攻擊的駭客持續將目標鎖定在工業單位上，且會一直策**

略性的擴張勢力，直到他們的任務完成為止

Mandiant 察覺到在中華人民共和國的策略優先權和中共國營事業的操作之間有密切關連，且透過網路入侵來從大量的工業組織和客戶中竊取資料。排行榜中前三名的工業組織一直被針對攻擊，第一名是航太業，接下來依序為能源業、天然氣與石油和藥品業。



- **一日被當做目標，終身被當做目標**

每家組織都會被一個以上的駭客團體盯上，有時會被成功入侵。2012 年時有 38%的目標在修復完受到攻擊的漏洞後，都會被再次攻擊。在 2012 年 Mandiant 所研究的所有案例中，駭客們曾登入超過一千個他們先前攻擊過的受害者來重新取得入侵路線。

需要更完整的報告內容取點擊這裡
(https://www.mandiant.com/resources/m-trends)。