2013 年安全漏洞的攻擊報告(Mandiant)

資料來源：MANDIANT M-Trends 2013attack the security gap (CERT 譯)
(https://www.mandiant.com/resources/m-trends/)

簡介

Mandiant 認為所謂的"資安隔閡"指的是網路攻擊的技術進步總是領先我們的防禦能力一步，而讓駭客總是有辦法能找到機會去攻擊我們的網路。雖然這隔閡很難被消除，但已有許多專家在努力解決。而且 Mandiant 發現有許多公司努力增進他們的技術來對抗資安隔閡。已經有越來越多公司不用借助 Mandiant 的幫助就可以自行發現惡意攻擊行為。

這篇報告主要著重於兩部分，第一部分是有關於我們的敵人們是運用哪些策略來攻擊我們，像是攻陷 IT 的服務提供者、駭客更進一步的偵查行為、持續性的目標式攻擊、針對網頁的攻擊等等。第二部分是駭客在 APT1 攻擊行為中所扮演的角色以及 Mandiant 提供的超過 3000 種技術指示。

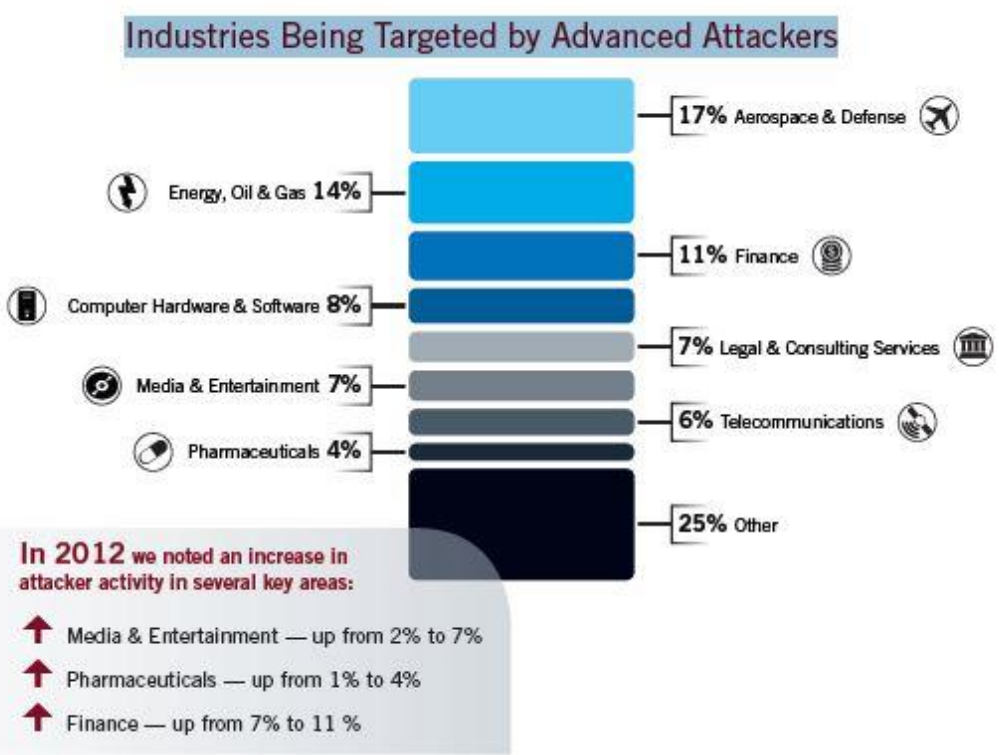

圖 1　APT 攻擊針對的目標產業類型

根據我們調查過去一年的攻擊行為，可歸納出四項趨勢：

1. 從外部而來

駭客越來越常使用委外的服務來提供駭客連線到受害者的機會。

外部的網路供應商和商業夥伴們開始以前所未有的方式連線到各組織的網路。在 2012 年，各家公司大約花 134 億美元在委外財務、會計、人力資源和採購等服務上。不過各家公司卻大約花了 252 億美元在資訊系統的委外上，這讓網路服務供應商有更多機會不受限制的連線到各個組織的網路裡。

目標式攻擊的駭客團體就利用委外服務關係這點來取得他們對特定目標的連線機會。在 2012 年的研究中，我們發現越來越多的組織因為委外管理服務的供應商被駭客所攻破且取得對各家受害企業的主要連線權。我們的許多客戶同時是被攻陷的網路服務供應商且又是接受被駭客染指的網路服務的客戶端。在許多案例中，駭客一開始會先向服務供應商下手，來取得對他們主要目標的連線手段，這些目標都是這服務供應商的客戶。在這些案例中，我們發現這些駭客會先攻破第一個受害者，也是就委外服務供應商，並取得足夠的資訊來攻擊第二個受害者。在第一個受害者中的攻擊行為會停止一段很長的時間，駭客只會在第一個受害者中建立後門程式並且在他們需要對第二個受害者再次攻擊時才會啟動。

在其他案例中，我們也看到許多服務供應商就是駭客主要的目標。例如，在我們的研究中發現，有些駭客會去對一個大型的服務供應商做攻擊，而這個供應商就是提供服務給許多小型的服務供應商的。所以駭客就可以自然而然的取得對這些小型供應商的連線。同時，其他分區的服務供應商如果有駭客感興趣的資料的話，駭客也會透過電子郵件和惡意檔案的方式來取得這些資料。

2. X 記號

駭客使用大量的網路偵查來幫助他們在攻擊受害者網路時更快更有效率

駭客會去竊取那些能幫助他們更快入侵的資料。雖然對於受害者網路的基礎偵查已經沒有多大幫助，但這幾年我們發現駭客們透過更複雜的工具和策略來當做新的偵查手段以便他們探索受害者網路。除了探索網路地圖之外，我們發現許多案例中駭客竊取的第一個檔案都是有關網路基礎設施、處理方法和 PCI 金錢支付資料。駭客也使用了不同系統管理指南來確認目標並進一步縮小範圍。我們也常看到一些案例是駭客使用原生的微軟工具（像是 dns.msc）來取得他們所需的偵查資料。

駭客從這些手上的資料來辨認網路區段和系統的錯誤配置，而從受害者網路中取得更多更好的連接。在所有這些案例中，只要擁有更深入的網路拓譜知識就可以

讓駭客更快更直接的取得受害者網路的連線。在某些案例中，駭客試圖進入生產環境網路來竊取智慧財產權。在其他案例中，駭客會試圖辨識受害者分享的網路資源，且是與其他在駭客目標清單上的組織做分享。

ITEM STOLEN	HOW THE ATTACKERS USE INFORMATION
Network Infrastructure Documentation Including Schematics and Configuration Files	Understand firewall and other IDS configurations and where vulnerabilities that can be exploited exist.
Organization Chart	Establish individuals to target in spear-phishing campaigns or to target for email and data theft.
Systems Documentation	Identify where targeted systems existing within a victim network.
VPN Configuration Files	Identify what VPN users have access to within a victim's network and target VPN credential data to steal.

圖 2 攻擊者在入侵偵察階段所偷取的資料類型

3. 一日為目標，終身為目標

進階持續性滲透攻擊持續將瞄準企業並策略性的擴張版圖，這些企業包括航空業、電腦軟體業、高科技製造業和能源工業

駭客們會依據他們的需求來挑選目標。金融取向的駭客會尋找可以竊取金錢或信用卡資料的目標來建立連線。駭客進行經濟性質的間諜活動，像是 APT，就是為了實質的利益收入，而受害者們通常都與他們的國家利益有關。在 2012 年時，Mandiant 就曾發現中華人民共和國、中共的國營組織相關操作與一連串從大量客戶端和企業發生的資料竊取的網路入侵活動有關係。Mandiant 也證實有許多組織在被駭客已 APT 的方式攻擊過一次後，又會再度遭受多次網路攻擊。根據我們大部分的研究中也發現許多組織會被一個以上的駭客團體攻擊，有時是接收前人留下來的任務而繼續攻擊。

我們在 2012 年針對客戶所做的研究，其中有 38%在修復攻擊事件所造成的傷害後又會遭到攻擊。

在經濟間諜案例中，我們看到了具有一致性和持續性的 APT 攻擊行動，針對幾乎所有我們觀察中的企業而攻擊。值得注意的是，有大量的重複攻擊行動發生在

航空業的各家企業。在所有 2012 年所觀察到的案例中，我們看到駭客們為了重新取得後門而針對先前的目標發動了超過 1000 個攻擊行動。

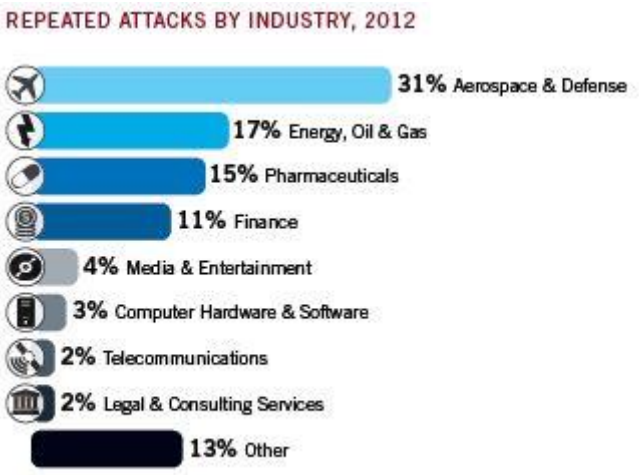

圖 3 2012 年 APT 的目標產業

4. 老派的掛馬攻擊有了新把戲

目標性駭客正在使用網路掛馬攻擊，且將利用它們來把受害者的系統打出破綻並作為往後入侵的立足點

在 Mandiant 裡，我們之前往往看到駭客們把網頁攻擊策略當做取得入侵受害者網路的連線的手段之一。但有別於舊式的網頁攻擊，Mandiant 觀察到過去一年的網頁掛馬攻擊比舊式典型的掛馬攻擊更具目標針對性。

駭客先前很常使用魚叉式釣魚攻擊和其他社交工程攻擊的策略來誘惑使用者去點擊而收到附件在電子郵件中的惡意程式。他們會寄給目標一封偽裝良好的電子郵件且附有惡意檔案，目標點開惡意檔案後他們的系統就會被攻破，而駭客就取能連到目標的連線。但使用這些廣為人知的技巧已經不夠吸引人了，防禦技術已經發展到可以抵抗這些攻擊，所以駭客們就更進一步作改進。

從攻擊的回應中 Mandiant 察覺到駭客改變了他們的策略，變成在目標組織經常瀏覽的網頁上動手腳。目標使用者在像平常一樣瀏覽被攻陷的網頁時，當他們一點擊進入網頁後惡意程式就會自動安裝到目標的系統中。一旦安裝完成，惡意程式就會收集目標的使用者名稱、密碼、瀏覽器 cookie 和這台電腦的名稱。

只要使用這種網頁攻擊，駭客就不必再為了要取得多家企業中各種不同系統的連線而寄送同樣的電子郵件。那樣反而會讓駭客要多花心思去對付反釣魚攻擊的防禦系統。

利用網頁伺服器的弱點來攻擊會讓犯罪痕跡比目標性攻擊、預謀性攻擊更隱匿。然而在 2012 年時，Mandiant 觀察到許多被攻陷的網頁伺服器都是被當做是經濟間諜（像是 APT）或犯罪威脅的第一步手段而已。

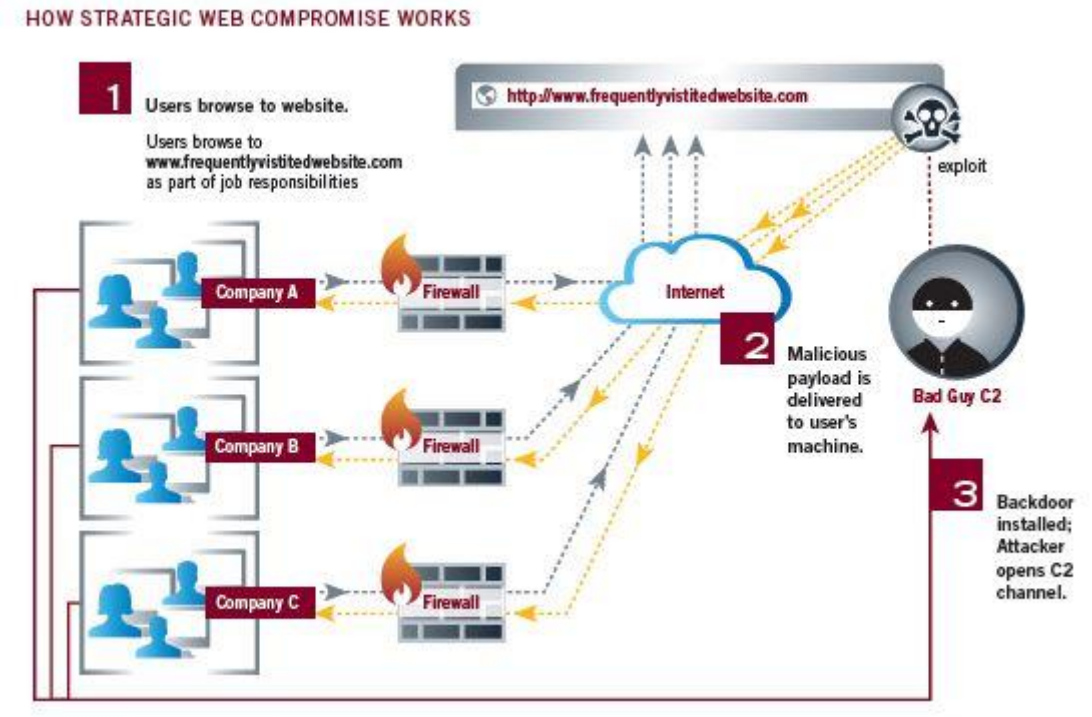

圖 4 網頁掛馬攻擊流程

APT1

中共的其中一個網路間諜單位曝光

自從 2004 年以來，Mandiant 一直在研究世界上百個組織的電腦網路漏洞，其中最嚴重、也是數量最多的就是進階持續性滲透攻擊（APT），我們在 2010 年一月首次公布有關 APT 的各個細節。如同我們的報告中所提到的，我們認為中共政府可能與這個行動有關連，但我們沒有辦法確定其參與程度。過了三年之後，現在我們已擁有證據去證實我們的假設。在我們分析了上百份報告後認為，這些活動主要是來自中國且中共政府知道這個事實。

Mandiant 一直持續追蹤世界上好幾個 APT 攻擊團體。然而這份報告把焦點放在最活躍的團體上。我們稱這個團體為”APT1”且它是超過 20 個來自於中國的 APT 攻擊團體之一。APT1 是一個獨立的組織，其中的成員至少從 2006 年就開始進行一連串的經濟間諜行動。從我們的觀察中得知，從竊取的訊息量來看 APT1 是

攻擊最頻繁的團體之一。它的影響程度和規模迫使我們不得不將它納入這份報告中。

我們所觀察到的 APT1 的活動只是冰山一角而已。雖然我們對於 APT1 的認識還不多，但我們已經分析了這個團體七年來近 150 個攻擊目標。從這些目標中我們有些不一樣的看法，我們從上海的四大網路區段來追蹤 APT1，其中兩個網路區段就坐落於浦東新區。我們發現了大量 APT1 的攻擊設備、命令與控制伺服器和作案手法（工具、策略和過程）。為了證實這幕後有人在掌控，Mandiant 找到的三個人我們都認為是屬於 APT1。這些技術人員，或可能是軍人，或許都是聽從其他人的命令行事。

我們的分析報告告訴我們 APT1 是由政府所資助的團體且它是最持久的中國網路威脅之一。我們相信 APT1 有能力發動大範圍、複雜的網路間諜活動，因為它背後有政府在撐腰。在追蹤這個攻擊行動背後的組織時，我們發現了中共解放軍編號 61398 的單位，它與 APT1 的任務性質、能力、資源都相當類似。PLA Unit 61398 的地點也和 APT1 的來源一模一樣。

一個由中國政府幫助的駭客組織可以對這麼多的企業造成規模龐大且持續時間相當長的攻擊行動，且讓人很難懷疑到 APT1 上。我們認為這麼多的證據已足夠證明 APT1 就是 Unit 61398。然而我們覺得還有另一種不太可能結論。

一個秘密、資源豐富的組織，其成員都是中國人且都與上海的電信設施有多年的密切關係，有著企業等級規模的經濟間諜行動且目標就是 Unit 61398，同時執行著與 Unit 61398 相似、大眾熟知的任務。

為什麼我們要公布 APT1

公布這些有關 Unit 61398 的相關情報對我們來說是一個難以抉擇的決定。我們長久以來一直維持的保密政策讓我們體認到不能繼續這樣下去，比起公布 APT1 的相關情報所帶來的正面意義，將來我們收集 APT1 的風險根本不算什麼。該是時候讓大家知道這個網路威脅是來自於中國，而我們想要做好我們的本分去準備資安防禦工作來有效抵抗這個威脅。讓大眾了解 APT 網路間諜的重要性的功勞是誰的已不重要。如果我們尚未對中國建立起堅固的連線，那我們的技術人員會常常因為協調問題、犯罪者的天性、周圍大型國家的安全問題和全球經濟的隱憂而無法準確掌握 APT 的攻擊行動。我們希望這份報告可以增加大家對 APT 網路漏洞的了解和一同對抗 APT 攻擊的決心。