零日漏洞(0-day exploit)和零日攻擊(0-day attack)

3 月 7 日網路上出現了一則新聞, “Goolge 工程師要求趕快更新, Chrome 爆零日大漏洞”[1], 我們知道電腦和手機連上了網路, 就得冒著各式各樣的風險, 但這個零日漏洞指的又是什麼呢?

“零日漏洞”或“零時差漏洞”指的是在軟、硬體開發方還沒有發現, 或已發現但還沒有修補的系統上或程式上的安全漏洞。而“零日攻擊”或“零時差攻擊”則是指這些具有風險的弱點一旦被發現，在修正程式發佈之前, 攻擊者即已利用這個漏洞開發出惡意軟體所進行的攻擊。

那零日攻擊和我們有什麼關係呢? 舉例來說:義大利有一家名為 HackingTeam 的公司, 這間公司的主要業務是賣給各國政府簡單、易用、好安裝的遠端監控軟體, 用來安裝在被監控者的手機和電腦中, 而其客戶包含了美國、德國、韓國、俄羅斯等大國。而這些被動了手腳的手機和電腦, 則包含了我們所熟悉的 Android、Windows、Mac OS、Linux 等作業系統的設備、甚至連冷門的 Windows Phone 也有。而安裝軟體的過程可能僅僅是使用者瀏覽了某個網頁、開啟了某個 e-mail 的附件，或是在 Google Play 市集中下載了一個免費的 App。透過這些安裝的軟體政府部門就可以監控受害者的 GPS、相機、麥克風、簡訊、通話等資訊[2]。但要在別人電腦或手機中無聲無息地安裝遠端控制軟體並不是一件簡單的事, HackingTeam 需要許多的零日漏洞來達到這個目的, 因此就花了大錢向駭客購買了漏洞[3]。而後 HackingTeam 公司被駭客入侵, 洩漏

出了高達 400GB 的資料，其中不乏大量的駭客程式和零日漏洞的資訊。

圖片來源: 近期駭客攻擊案例分享，行政院國家資通安全會報 技術服務中心[3],

根據蘭德公司(RAND)的研究，有 25%的零日漏洞存活時間長達 9.5 年。該報告並將零日漏洞分為三類，第一類是未被公開的現存漏洞，第二類是已被揭露的漏洞，其中部份已經被修補，第三類則是殭屍漏洞，這些漏洞只存在於程式的舊版本之中，新版本則已經修復[4]。

參考資料:

1. “Google Chrome 爆出零日漏洞，呼籲即時更新,” engadget 中文版 https://chinese.engadget.com/2019/03/08/chrome-update-zero-day/
2. “當駭客被駭！你的一舉一動難逃監視,” 今周刊 http://www.businesstoday.com.tw/article/category/80394/post/201507160024/%E7%95%B6%E9%A7%AD%E5%AE%A2%E8%A2%AB%E9%A7%AD%EF%BC%81%E4%BD%A0%E7%9A%84%E4%B8%80%E8%88%89%E4%B8%80%E5%8B%95%E9%9B%A3%E9%80%83%E7%9B%A3%E8%A6%96?utm_source=%E4%BB%8A%E5%91%A8%E5%88%8A&utm_medium=autoPage
3. “近期駭客攻擊案例分享,” 行政院國家資通安全會報 技術服務中心, http://download.nccst.nat.gov.tw/attachfilepromo/%E8%AD%B0%E9%A1%8C%E4%BA%8C_%E8%BF%91%E6%9C%9F%E9%A7%AD%E5%AE%A2%E6%94%BB%E6%93%8A%E6%A1%88%E4%BE%8B%E5%88%86%E4%BA%AB_0119.pdf
4. “研究:1/4 零時差漏洞平均壽命長達 9.5 年,” iThome, https://www.ithome.com.tw/news/112723