# https://www.fireeye.com/current-threats/apt-groups.html

## APTs targeting Telecommunications

# APT1

**Also known as:** Unit 61398, Comment Crew

**Suspected attribution:** China's People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398 部队).

**Target sectors:** Information Technology, Aerospace, Public Administration, Satellites and Telecommunications, Scientific Research and Consulting, Energy, Transportation, Construction and Manufacturing, Engineering Services, High-tech Electronics, International Organizations, Legal Services Media, Advertising and Entertainment, Navigation, Chemicals, Financial Services, Food and Agriculture, Healthcare, Metals and Mining, Education

**Overview:** APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. The group focuses on compromising organizations across a broad range of industries in English-speaking countries. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

**Associated malware:** TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS

**Attack vectors:** The most commonly observed method of initial compromise is spear phishing. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names. While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. Throughout their stay in the network (which could be years), APT1 usually installs new backdoors as they claim more systems in the environment. Then, if one backdoor is discovered and deleted, they still have other backdoors they can use. We usually detect multiple families of APT1 backdoors scattered around a victim network when APT1 has been present for more than a few weeks.

# APT3

**Also known as:** UPS Team

**Suspected attribution:** China

**Target sectors:** Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation

**Overview:** The China-based threat group FireEye tracks as APT3 is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of using browser-based exploits as zero-days (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

**Associated malware:** SHOTPUT, COOKIECUTTER, SOGU

**Attack vectors:** The phishing emails used by APT3 are usually generic in nature, almost appearing to be spam. Attacks have exploited an unpatched vulnerability in the way Adobe Flash Player parses Flash Video (FLV) files. The exploit uses common vector corruption techniques to bypass Address Space Layout Randomization (ASLR), and uses Return-Oriented Programming (ROP) to bypass Data Execution Prevention (DEP). A neat trick to their ROP technique makes it simpler to exploit and will evade some ROP detection techniques. Shellcode is stored in the packed Adobe Flash Player exploit file alongside a key used for its decryption. The payload is xor encoded and hidden inside an image.

# APT18

**Also known as:** Wekby

**Suspected attribution:** China

**Target sectors:** Aerospace and Defense, Construction and Engineering, Education, Health and Biotechnology, High Tech, Telecommunications, Transportation

**Overview:** Very little has been released publicly about this group.

**Associated malware:** Gh0st RAT

**Attack vectors:** Frequently developed or adapted zero-day exploits for operations, which were likely planned in advance. Used data from Hacking Team leak, which demonstrated how the group can shift resources (i.e. selecting targets, preparing infrastructure, crafting messages, updating tools) to take advantage of unexpected opportunities like newly exposed exploits.