APT1/People’s Liberation Army Unit 61398 Attacks

By David Bourque

What are APT1 and The People’s Liberation Army Unit 61398?

- APT stands for Advanced Persistent Threat
- Unit 61398 is a division of the Chinese Military that conducts computer network operations
- Report by Mandiant, a US based internet security group, claims that they are the same
- This is due to both groups having similar missions, having a large workforce, with similar staff needs, and both being based in the same location

Who They Attack

- APT1 typically attacks English speaking organizations in a variety of industries
- Most organizations they attack are in industries that China has deemed important for growth

How They Attack

- Most attacks by APT1 are conducted in the same manner
- Step 1: Initial Compromise
- Step 2: Establish Foothold
- Step 3: Escalate Privileges
- Step 4: Gather Information

Step 1: Initial Compromise

- In order to initially gain entrance into an organizations network, APT1 attacks almost always use spear phishing
- Spear Phishing is sending a personalized email with a malicious link to someone on the network

Step 2: Establish Foothold

- Once someone in the network has downloaded the malicious link, it installs a backdoor
- APT1 typically uses a WEBC2 backdoor which upon being downloaded is able to use the computer to access the internet
- It is then able to connect to a webpage that is hosted by a Command and Control (C2) server
- The backdoor, upon connecting to the website, is able to interpret certain parts of the HTML code as commands

Step 3: Escalate Privilege

- In order to gather information about the organization, APT1 needs to gain additional access to the network
- APT1 typically uses publically available tools to dump password hashes from victims systems, that they can then use to crack a password
- Tools that APT1 has used include pwdump7 and gsecdump

Step 4: Gather Information

- Now that APT1 has access to the system and legitimate credentials, through cracking a password from the hash dump, they only need to use built-in operating system commands to explore the network and gain access to files
- When they find files they want, they simply archive them and then transfer them out of the network

Resources

- http://www.voanews.com/content/us-firm-links-chinese-army-to-cyber-attacks/1606283.html
- http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- http://blog.securestate.com/apt-if-it-aint-broke/