Homework Number: 13

Name: Adam Bahrainwala

ECN Login: abahrain

Due Date: 24/04/14

The researchers used wireshark to track and trap packets of information being exchanged with the control and command server. They would use the packets captured to flag for suspicious activity. Once they found the packets they were looking for they were able to locate the Trojan on the system. The Trojan was a ghostRAT system that was communicating with a control and command server. Through further investigation, it appeared that the Trojan and its companion C&C server where based in China. The Chinese attackers used targeted email attachments to lure the victims into installing the Trojan. The Trojan was designed to collect sensitive documents and send them back to the server. The Trojan would install and then preform a reverse DNS lookup to find its master. The research team used Virus Total to detect the Trojan on the infected systems. The software would scan the machine and found the Trojan by its determined signature. They then isolated the Trojan on the system and used it to track back to the host server. They would follow packets from sent from the Trojan back to the server to find the IP address and physical location of the server. The bulk of the servers where based in China, however, some were found in other parts of the globe. This can be attributed to the use of a dynamic DNS system. The control server that was found had many components to it and was able to force computer to download files from servers also under the attacker’s control. The attackers could also make the computers send back private or confidential data. The attackers used gh0stRAT to control the computers. This Trojan is able to control almost every aspect of the computer. From turning on the webcam to searching and sending files back to a command server. The Trojan would constantly check in with the command server and see if there was a command to be executed. When the attacker was away from their end, the server IP would change to throw off suspicion.

After looking and manipulating the gh0stRAT Trojan, I see that it is very powerful and can cause a great deal of damage. The system isn’t very smart in the sense that it can’t sustain without a master to command it. For example a worm can scan, find a file, and then return that file to the attacker without constant upkeep.