Pranjit Kumar Kalita
ECE 404, HW 13

Description of the two reports

The two reports provide a context to understand the magnitude of and outreach of present-day cyber-espionage activities. The two reports are essentially provide a context to understand the serious consequences of such activities, the way these acts are carried out, the potential victims with their intended or sometimes unintended consequences, and how they are detected and investigated. To provide context, specifically these two reports pertain to a series of cyber-espionage attacks arising out of hacks and attackers in the People's Republic of China, against governmental authorities of Tibet and India, and the various coincidental information security liabilities arising out of an interconnected confidential communication-interchange system between the countries of the world today. The attackers used the disguise of social engineering, which in short, involves exploiting a user's social circles to send and execute malicious code into their machines. This is generally done through email, etc from legitimate addresses. The investigators acted upon the security viabilities of the infected computers and proceeded to employ network monitoring software that enabled them to monitor traffic and communication from control servers and command centers acting at the control of the attackers, after having verified the existence of malware. Then, using a simple DNS look-up, the identity of the command and control centers that run the GhostRAT client through its GUI web-based interface, which is the particular instance of the Trojan that is used to exploit the target computers. Also, the investigators used a honey-pot computer that would attract communication to connect with the attackers to download the GhostRAT Trojan. Once that connection was established with the owner IP address contained an executable file that is part of the initial set up, the GhostRAT owner has complete access to the infected computer. The investigators monitored this traffic to pin point the geographic locations of computers used by the attackers through their IP's. GhostRAT is executed by the GhostNET network framework, which was used for all the attacks. The GUI interface afforded the attackers with unprecedented and real-time access to the infected computer, from file registry to controlling external hardware such as webcam, etc. Finally, in light of this discovery and the magnanimous nature of cyber-espionage attacks, the reports highlight the need to proliferate on this issue, with cooperation among countries by agreeing on laws that prohibit and inhibit such activities within the borders of every responsible nation, regardless of whether or not the state actually benefits from such exploits.

Questions:

a) There have been evidence of increasing Chinese cyber-espionage attacks into Tibetan governmental computers. Therefore, at the highest level, the investigation consisted of basically trying to find out what the vulnerabilities of the Tibetan/infected computers were and then pin-pointing where these attacks were originating from, and what web-interfaces and tools the attackers used. Therefore, the investigation was divided into the following two phases with their corresponding specific information obtained:-

   1. Field based investigation – Here, the infected computers were scouted for vulnerabilities and searched for the current security framework employed. Also involved installation of network monitoring software to collect evidence of malware installed and information exchange to and from command and control centers.
   2. Computer-based scouting, target selection and data selection – In this stage, using a simple DNS lookup, the identities of the command and control centers that were infecting the computers were discovered based on the traffic and communication from the network monitoring software installed in the first phase. This phase also involved the monitoring of the infected computers to find out the list of derived-infected computers that were coincidentally impacted, as well as monitor the system operation for specific target infected computers.

b) Presence of malware (Trojans) in the infected computers was helped with installation of network monitoring software. These software collected forensic technical data from the affected computers, upon whose analyzing confirmed the evidence of malicious code/software running in those computers, along with evidence of traffic between infected computers and particular control servers.

c) The initial discovery of the control and command centers (control centers essentially in control of other control centers) was done by tracking the traffic activity of infected computers from phase one of investigation through network monitoring software. In order to get the geo-locations and/or IP locations, a simple reverse DNS lookup was done by analyzing the traffic from the previous phase. Once four control and six command centers were obtained, the next phase was to look for more, if any, IP addresses within a geographical range under control of attacker(s). To this effect, essentially a computer was set up as a honey pot to attract attackers' incoming communication to download malicious code/malware/worms into the honey pot computer. The idea was to download the identified Trojan GhostRat of choice through its network GhostNet, inorder to connect to the attacker's GhostRat client. Then once this communication was made, a series of IP address used by the attackers(s) to communicate with GhostRat infected computers discovered from stage 1 were tracked to a location in China. Thus, a combination of reverse DNS lookup along with honey pot with traffic monitoring and tracking were used to geographically pin point the location of command and control centers used by the attackers.

Control centers performed the following tasks (all these functionalities performed by the web interface of the control centers)- provide a list of all the computers infected with the GhostRat client of the GhostNet network framework, provide an interface to execute / issue commands to the computers, as well as to monitor pending commands to these infected computers and produce results when completed.

d) The specific Trojan that was used by attacked to steal large-scale information from the infected computers was GhostRAT, a remote administration tool that gives its owners full and real-time access to the infected computers. This real-time access is provided through commands that are specified by the GhostRAT owners and executed at the infected computers. So, basically what happens when a GhostRAT file is downloaded and executed in an unsuspecting computer is that it connects the particular computer to the GhostRAT owner at a third party location, through an IP address that is enclosed within an executable file that performs the GhostRAT download. Once connected to the owner, the owner has complete access to the target computer, and can then issue commands including file manager, screen capture keylogger, remote shell and system, webcam view, audio capture, as well as make the infected computer download and execute malware in the target computer.

e) The following is a bird's eye view of the capabilities of GhostRAT Trojan through its GUI interface:

1. Total control of the infected computer
2. Ability to keep track of keystrokes and mouse events
3. Control of external hardware to the infected computer such as webcam, microphone by ability to turn on and off, thus giving the capability to listen in on anything around the infected computer or in the privacy of the infected computer's physical setting
4. A list of the currently running processes on the infected computer
5. List of files and subfiles (registry) of the computer
6. The GUI provides the ability to send corrupted emails with malicious code/malware using social engineering (using address found in the infected machine)