ECE404 hw13
Yinuo Li
PUID 0025773439

Tracking GhostNet: Investigating a Cyber Espionage Network

Summary:
After 10 months of investigation, researchers from Munk Centre for International Studies at the University of Toronto discovered the GhostNet. The investigation was carried out after the researchers approached the Dalai Lama's representative in Geneva suspecting that their computer network had been infiltrated. It was found that more than 1000 computers in more than 100 countries can be considered as high-value targets and there were increase in allegations that China-based hackers are responsible for high-level penetrations of computer systems in various countries. This paper focused on the investigations of Chinese cyber espionage against Tibet and the identification of command and control servers.

Shadows IN THE CLOUD: Investigating Cyber Espionage 2.0

Summary:
This paper explains a complicated ecosystem of cyber espionage which consists of computer network systems in India, Geneva, the U.S. and some other countries. By manipulating multiple cloud computing systems and social network platforms, the hackers hidden in malware ecosystem managed prolonged control with the operating systems located in China. This report talks about the recovery of exfiltrated data from Indian government, including one encrypted diplomatic document, two "SECRET" documents, six "RESTRICTED" documents, and five "CONFIDENTIAL" documents.

a. **At the lowest levels of data gathering, what information did the investigators collect and what tools did they use for that purpose?**

   Network monitoring software was installed on various computers so as to collect forensic technical data from affected computer systems, and initial analysis confirmed the existence of malware and the transfer of information between infected computers and a number of control servers.

b. **How did they identify the malware (the Trojans) present in the infected computers?**

   During an analysis of attacks which occurred during the 2008 Beijing Olympics they discovered the location of a control server that was later identified as part of the network which infected a computer in the private office of the Dalai Lama. They were able to gain access to the command interface of this control server and identify the infected computers which reported back to this server. Researchers monitoring the use of socially engineered malware attacks against the Tibetan community have identified over eight different Trojan families in use. Control over some targeted machines is maintained using the Chinese ghost RAT.

c. **How did the investigators discover the identities (meaning the IP addresses and the geographic locations) of the computers used as the command and control centers? Also, what role was played by the computers used as control centers and what role by the computers used as command centers?**

The data collected in Dharamsala and at Tibetan missions abroad led to the discovery of four control servers and six command servers. These control servers were identified and geo-located from the captured traffic using a simple IP lookup. The system was actively monitored for two weeks, which allowed us to derive an extensive list of infected systems, and to also monitor the systems operators as the operators specifically instructed target computers.

d. **What was the capability of the specific Trojan that played a large role in stealing information from the infected computers? How did this Trojan allow the humans to control in real-time the infected machines?**

The GhostNet system directs infected computers to download a Trojan known as ghost RAT that allows attackers to gain complete, real-time control. These instances of ghost RAT are consistently controlled from commercial Internet access accounts located on the island of Hainan, China. Trojan horse programs and other associated malware are often cited as vectors for conducting sophisticated computer-based espionage. These Trojans generally allow for near-unrestricted access to the infected systems. After infecting the target, the Trojan packed in the Word document performed a DNS look-up to find its control server and then connected to that server.

e. **Try downloading the Trojan into a linux machine and see what you can infer about its capabilities. Report on what you find out.**

Trojan is a harmful piece of software that looks legitimate. Users are typically tricked in to loading and executing it on their systems. After it is activated, it can achieve any number of attackes on the host, form irritating the user to damaging the host. Trojans are able to create back doors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.