GhostNet

In 2008 - 2009, The Information Warfare Monitor conducted extensive field research and analysis to discover that many of the crucial machines in the OHHDL and other Tibetan organizations were infected with malware and hence sought to find out who was responsible for the attacks. Further analysis revealed a deep malware net called GhostNet that had numerous control servers and command servers. The following is a summary of the findings:

Packet data was captured multiple computers at variety of locations using WireShark. These locations included OHHLD, Tibetan Government In Exile, Offices of Tibet in New York, Drewla, etc.
Palantir Cyber was used to map various computer affecting the network and display a link between each computer and what kind of data was being sent back and forth.

The collected data was analyzed using Palantir and it was found that the malware was using http requests to upload sensitive data to CGI scripts hosted in the control server through by pass websites like macfreeresponse.com, etc. The control servers were identified through this initial contact made b the malware. Further the control server contacted other control servers and command servers. Hence a lot of the control servers and command servers were enumerated thereafter.

Later a honeypot computer was setup which was allowed to be infected by the attackers. The execution of commands on the honeypot enabled the the discovery of four specific control servers and their IP Addresses. Further the IP Addresses were found to be within a DSL range in Hainan Island. The geographic locations were pin pointed by an IP look up. It Was fond that the GhostRat Trojan was being used for remote control purposes.

The control servers directed infected computer download additional malware from command servers and hence the command servers were also mapped. The control servers helped teh user issue commands to the infected machines while the command servers were mostly used for distributing more malware.

Three of the four control servers are in China: Hainan, Guangdong and Sichuan. One of the control servers is located at a web-hosting company in the United States. Five of the six command servers are located in mainland China (Hainan, Guangdong,
Sichuan and Jiangsu) and one in Hong Kong.

The GhostRat Trojan created web pages that contained “drive by” exploit code that infected the computers of those who visit the page. Second, the attacker(s) also showed that they engaged in spear phishing in which contextually relevant emails
were sent to targets with PDF and DOC attachments which, when executed, create back doors that caused the infected computer to connect to a control server and await further instructions. A system information command let the attacker map the details of hardware and software on the system and hence exploit other invulnerabilities in the system. The attacker(s) could then execute a wide variety of commands, including file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture,as well as the ability to force the infected host to download and execute additional malware, such as a gh0st RAT update. The attacker(s) could also secretly execute programs on the target computer. This gave total control of the computer to the attacker.

Shadows In The Cloud

The Shadow investigation began as an aftremath of possible paths found in the GhostNet investigation. It began in the offices of Tibetan organizations who suspected they were targets of cyber-espionage, and broadened to include a much wider list of victims. The investigation used a number of techniques, including a DNS sinkhole we established by registering domains that had previously been used by the attackers targeting Tibetan institutions, such as a computer system at the offices of the Dalai Lama.

It was found that many of the Tibetan and Indian computers had been compromised after the GhostNet research. These included computers at Indian embassies in Belgium, Serbia, Germany, Italy, Kuwait, the United States, Zimbabwe, and the High Commissions of India in Cyprus and the United Kingdom. Field research was conducted based on the Action Research Literature that has evolved since the 1940s, as well as other field-based investigation and research techniques. The AR field-based approach feeds into the fusion methodology that guides our overall investigatory process. It employs ethical and participatory observations and structured focused interviews. Grounded research with technical interrogation were supplemented by network monitoring activities.

It was found that the computer on Tnnernet generating the malware belonged to Mr. Serta Tsultrim, a Tibetan Member of Parliament, editor of of the weekly Tibetan language newspaper Tibet Express and the director of the Khawa Karpo Tibet Culture Centre. After that specific techniques like DNS Sinhkholding, Malware Analysis, Command and Control Center Topography, Victim Identification and Data Recovery were used to help the analysis. Palantir and Wireshark were used in copious amounts to aid data collection and analysis.

One platform leveraged by the attackers in particularly interesting ways was the webmail service provided by Yahoo!. Five Yahoo! Mail accounts being used by the attackers as a component of command and control were discovered. Once a computer was compromised, the malware connected to the Yahoo! Mail accounts using Yahoo's API and created a unique folder in the Inbox of the mail account, into which an email was inserted containing the computer's name, operating system and IP address. The attacker would then send an email to the account containing a command or a command along with additional malware as an attachment. The next time that a compromised computer checked in with the email account, it then downloaded and executes the malicious attachment. It was also found that command and control servers were being run in free web hosting sites, hence it was resilient. Using this information the IP addresses were found to be linked to exisitng malware websites. These IPs were used to map the geo-location.

27 different malware forms were found on the command servers All of these had destructive capabilities including including file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture,as well as the ability to force the infected host to download and execute additional malware. This enabled complete control for the attacker on the infected systems.

Downloaded GhostRat on Ubuntu 12.04

GhostRat seems to be two exe files with additional .reg files for windows machines. I uploaded the file to virus total and a surprising piece of info was that about 70% of anti-virus scans thought it was a safe file to run, Only a handful like McCafe thought it was dangerous and detected it.

Its mostly programmed in Visual Basic 6, about 90%. The actual effects of GhostRat could not be observed since it cannot affect Linux systems

Sthitaprgayan Parida

ECE 404

HW 13 (Trojan Report)

Date Due: April 28, 2015