ECE404
HW13
GUANSHI HE

a) For Tracking Ghostnet, the investigators was trying to gather targeted malware samples from Tibetan NGOs and to check the potential threat to computer security at the Office of His Holiness the Dalai lama in light of the targeted malware threat by running Wireshark on several key computer systems and to access the firewall logs at the Tibetan Computing Resource Centre.

b) They attempted to identify and connect to the control servers used by analyzing the data from the OHHDL obtained during the investigations. Email messages with malicious link or attachment were sent by the attackers and they were so sophisticated in the content to trick their recipients into believing that they are receiving legitimate messages. Once the link or the attachment is opened, the infected file or link will exploit a vulnerability on the user's machine and in stall the malware.

c) The investigators used reverse DNS look-ups and each IP address' record from the Regional Internet Registries to discover the identities. The control servers, basically, carry out the command from the command server, and the command servers give instructions to the control servers to implement the commands on the infected machines.

d) Once the attacker turns on the ghost RAT, the attacker is able to establish connections with all the infected machines and then have the permission to execute a large amount of commands like file manager, screen capture, key logger, remote shell, system, webcam view, audio capture and also force the infected machine to download any additional malware.
Real-time control is based on a successful connection that the Trojan had been made before. In addition to that, the attackers should set the commands on the control servers that instruct those infected machines to download remote administration Trojans in order to gain real-time control.

e) Trojans are good at occupying memory for processing and then cause the computer to crash and data corruption during the computing. Furthermore, Trojans are able to create backdoor for systems and leave chance for attackers to do anything they want remotely on the infected computers. Also, it can modify or delete files or format, destroy all content. Therefore, trojans can perform any operations that the attacker want on a targeted computer.