Jiacheng Yuan

yuan105

HW 13

April 24, 2018

A. At the lowest levels of data gathering, the investigators collect firewall logs and network packets for data analysis using Wireshark.

B. The investigators confirmed the existence of malware and the transfer of information between infected computers and a number of control servers from analysis data gathered by Wireshark.

C. These control servers were identified and geo-located from the captured traffic using a simple IP lookup. The investigators looked up the associated Internet Protocol address in all five Regional Internet Registries to identify the country and network to which the IP address is assigned. Then performed a reverse Domain Name System (DNS) look-up on each IP address. Once they discovered a domain name, they then looked up its registration in WHOIS and would know who registered the domain name.

The computers used as control centers contains three main components: 1) a listing of all the infected computers that have reported to the control server; 2) an interface to issue commands to the infected computers; and 3) an interface to monitor pending commands to infected computers and their results when completed.

In some cases, command centers act as control centers themselves; however, some appear to be used exclusively to host malicious files that infected computers are meant to download.

D. When the attacker(s) turns on the Trojan - gh0st RAT, he or she is able to see all the infected machines that have established connections to him or her. The gh0st RAT has a great capability of doing almost everything the owner can do on his/her own computer. The attacker(s) may 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) may also secretly execute programs on the target computer.

The attacker could perform command to instruct infected computers to download the gh0st RAT remote administration tool. The program can perform a DNS look-up and connect to the gh0st RAT owner or to a third location, a control server, when it retrieves the current IP address of the gh0st RAT owner.