Differentiating Remote Access Initiated Network Traffic From Locally Induced Network

Pei-Ting Lee
Computer and Information Technology

Problem

As malware continue to grow at a rapid speed, they are becoming more prominent in the computer forensics field. From a forensic investigation perspective, it is important to identify malware, especially those with remote control capabilities, on a suspect machine. When evidences of cybercrimes are discovered on suspect machines, the presence of malware may indicate some other perpetrator other than the owner. This paper aims to find patterns that can differentiate network activities initiated by attackers through installed malware from those executed by the actual owner of the machine.

Significance

In network forensics, evidences located in captured network packets may be used to find the identity of the attacker. If the machine from which these packets originated from was compromised by some remote access malware, there may be ambiguity to who initiated those network packets, the owner of the machine or the remote attacker? It is important to differentiate the network traffic initiated by the two to be able to better identify the real perpetrator.

Methodology and Results (In Progress):

Capture Network Packets
- Two virtual machines, one with remote access to the other
- Browse web through remote access + local machine
- Wireshark - Capture network traffic from victim

Extract Flows
- Packets constructed into flows
- Tshark

Sort Packets
- Remote access control packets between attacker and victim [1]
- Network packets initiated by attacker through remote access
- Network packets initiated by victim machine owner

Find Pattern
- Find pattern between control packets and remote access initiated network packets
- Differentiate network packets initiated by attacker and victim

References:

[1] Li, S., Yun, X., Zhang, Y., Xiao, J., & Wang, Y. (2012). A General Framework of Trojan Communication Detection Based on Network Traces. Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on, 49-58.