**Summary**

“BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation” is an academic study and experiment where Georgia Institute of Technology and SRI International team up together to present a new type of network monitoring strategy which integrates infection recognition and coordination dialogs. Over the last decade, malware has become the source of most botnet initiated denial of service attacks. The typical stages of malware infection are as follows: inbound scanning, exploit usage, egg downloading, outbound bot coordination dialog, and outbound attack propagation. However, botnets are different from most other malware in that they seek to establish a line of communication to a command and control channel from which they can be directed and updated. Intrusion detection systems typically only monitor incoming packets. BotHunter utilizes a multi-threat attack recognition strategy – SNORT – which involves three main components: malware/botnet rule based detection, SLADE (payload analysis) and SCADE (incoming and outgoing traffic analysis). These three components are analyzed by the Java BotHunter correlator algorithm which produces a bot infection profile consistent of relevant information such as confidence score, victim IP, attacker IP, etc. SLADE analyzes the payload for metrics to include payload size deviation. The correlator algorithm determines that a potential botnet infection has crossed the threshold.

The strengths of this paper are the thorough experiments. The authors tested various setups using different botnet malware and provided results which were impressive for an experimental