Title of the Project – Threat Categorization based on malware's CnC communication

Team Members – Sriram P, Jawed, Archana

Synopsis (what is the problem it is trying to address) – Threat categorization is one of the biggest challenges that the security community faces a challenge today. Malwares are hidden using multiple layers of packers, obfuscators thus hiding from revealing its true identity unless unpacked. Oflate, it is also observed that the same codebase / framework is reused by multiple RAT builders and Backdoors. Some of these packers and obfuscators are also reused across multiple malware families. This project aims at looking into the networking concept of these CnC communicating malwares and tries to parse the network packets and try to classify the threats based on the unique communication pattern used by these malware families. The rules also involves fingerprinting the TLS certificates used in the communication.

Deliverables – Python based pcap parser, Rule and fingerprinting Compiler for pcap parser, usage documentation

Diagram (Optional)

End of the Project - ----------

References:

1. https://www.youtube.com/watch?v=eEw_VZ5xdcE
2. https://www.youtube.com/watch?v=NSmkrlybZXs