MalwareLab
At the Cyber Security Research Center

Detection and Attribution of APT Malware aimed at SCADA Systems

Head of Malware Lab: Dr. Nir Nissim

MalwareLab
At the Cyber Security Research Center

Idea 1 – Detection of APT Malware aimed at SCADA Systems

Motivation:

- Critical Infrastructures (e.g. water, electricity, etc.), are managed and operated by SCADA Systems
- Thus, SCADA Systems are an attractive target for cyber attacks
- Advanced Persistent Threats (APTs) are very sophisticated and evasive cyber attacks
- Cyber attackers and APT groups create APT attacks and target them towards SCADA Systems

Our Proposal:

- To gather and form large, representative and diverse collection of APT and benign samples
- To create a comprehensive dynamic analysis environment that allow the APT malware perform their entire behavior
- To execute the samples in the designated environment through a dynamic analysis and extract informative features
- To explore and develop a data science based new unknown APT detection model that leverages both analyses types

MalwareLab
At the Cyber Security Research Center

Idea 2 – Attribution of APT Malware aimed at SCADA Systems

Motivation:

- APT malware are created by variety of APT groups, each has special characteristics
- Some APT groups tend to cooperate with others, sharing code and techniques , while others works independently
- Knowing the origin of the APT malware allows to better protect SCADA systems in multiple aspects:
- 1) Learn the attack and evasion techniques in order to better detect such attacks in the future
- 2) Learn how to respond in case of such attack

Our Proposal:

- To study and explore variety of security reports and thus label our large APT malware samples to their APT groups
- To learn and extract informative features to well distinguish between the different APT groups.
- To explore and develop a data science based attribution model for new unknown APT malware