Unknown Malware Detection Using Network Flow Pattern Classification

Researchers

Dimitri Bekerman
bekerdmi@post.bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Goals

Common computer malwares are smart, persistent and have the ability to hide themselves from the most modern anti-malware software, yet when such a malware tries to communicate with the rest of the world it most likely uses common known protocols to pass through the firewalls and network intrusion detection systems. Unfortunately, all those systems are based on static rules created manually by cyber security engineers based on previous intrusions.

Our aim is to develop a method that is based on machine learning techniques for detecting previously unknown malicious activities and in particular malware's communication with command and control servers, thus enabling the system to dynamically and independently infer the detection rule.

Description

During this research we developed cross layer attributes for network traffic aggregation to induce a reliable classifier, and classify benign and malware network traffic. Those attributes are based on DNS address resolution patterns, statistical analysis of HTTP and HTTPs transactions and network-flow anomalies of incoming and outgoing traffic. The classification model has been specifically designed to deal with NATed and encrypted traffic and also to handle high throughput networks.

Results

We evaluated our classification model on malicious captures from various sandboxes as well as from a real high bandwidth network. We managed to detect previously unknown malwares with high accuracy, with tolerable false alarm rates.