Summary for "Unknown Malware Detection Using Network Traffic classification"

Krishna Sindhuja Kalusani

USC ID: T25568677

Abstract: From the most modern anti-malware software and from most experienced IT engineers modern malware software utilizes sophisticated ways to hide itself. Few malware is left under radar for years, by stealing, disrupting and damaging systems. Inorder to receive new tasks, software updates or to leak collected data the initiator of the attack is being communicated using internet. In some cases proxy is used as communication algorithm with C&C center.

When Malware programs are in an urge to detect them they are capable of hiding themselves in systems or disabling their activity. In order to detect malicious activities on targeted systems trusted monitoring is required. Few studies are conducted on malware families. In different layers or protocols various malwares are reflected, rendering partial perspectives inadequate. With high accuracy the existing solutions for the tasks assigned are solved but it is difficult to adapt the constant evolution of existing malware types. In reality, when attackers understand that their technique is discovered they develop a new technique that can bypass existing anti-malware mechanisms. Study includes detection of malicious communication including interaction with C&C servers in-order to enable alerts about the intrusion. Using supervised learning methods the solution is based. A solution is offered which can detect previously unknown malware based on previously learned ones. This solution is dynamically adaptive which has always been one step ahead of attackers.

Contributions:

- These traits benefit to discover malicious activities. Few methods and techniques which are used for network classification are adapted to achieve the goal.

- The analysis of DNS, HTTP, and SSL protocols is obtained by proposed method. The added strength is to take into account the fact that targeted machines which can be behind NAT.
- It is effective for encrypted traffic and malware using legitimate networks.
- Traffic behavioral patterns are analyzed.

Weakness: For the evaluation of the approach, traffic is used which included malware generated in different sandboxes. The test continued multiple types of malware that were not included in the data used in the training. While the results are compared to some of today's most popular rule-based NIDS, the proposed method analyses only traffic behavior not its content. In future the research is intended to extend towards transfer learning techniques in-order to evaluate and detect malware networks. Also the method can be made suitable for higher bandwidths.