Malware Network Behavioural Signature

Internship proposal

Main advisor: Axel Legay, axel.legay@inria.fr
Other advisors: Fabrizio Biondi, fabrizio.biondi@inria.fr ; Thomas Given-Wilson thomas.given-wilson@inria.fr

Required skills: Network programming, system administration, operating systems, virtual environments.

Context: The TAMIS team has a strong axis on malware analysis and classification using machine learning (ML) algorithms. This project extends this to consider network based behavior for the detection and classification of malware.

Description:
This project is to identify malware (and distinguish malware from cleanware) using the network behaviour of a binary program. The goal is to run a binary (in a sandbox) and detect all the network behaviours of the binary, and from this build a behavioural signature. This behavioural signature can then be compared with other behavioural signatures of known malware (and cleanware). The end goal is to detect malware binaries using this network activity behavioural signature.

(Note that we already have a project on distinguishing malware from cleanware using behavioural signatures, so the main goal of the Network Signature project is to produce behavioural signatures that can be used in the same way (some collaboration with the other project will likely occur to share classification knowledge, and share machine learning approaches).)

The main objectives of this project will be the creation of a testing environment where a binary sample can be run in a sandbox with a controlled network environment. This environment should allow the sample to act (and be able to respond to, or simulate various appropriate features that influence the sample's behaviour), and also collect all the sample's network activity.

Keywords: malware analysis, machine learning, networking, virtualisation

References:

Morales, J. A., Al-Bataineh, A., Xu, S., & Sandhu, R., Analyzing and exploiting network behaviors of malware. In International Conference on Security and Privacy in Communication Systems (pp. 20-34). 2010.

Roberto Perdisci, Wenke Lee, and Nick Feamster, Behavioral clustering of HTTP-based malware and signature generation using malicious network traces, NSDI'10 Proceedings of the 7th USENIX conference on Networked systems design and implementation, 2010

Saeed Nari, and Ali A. Ghorbani, Automated malware classification based on network behavior, International Conference on Computing, Networking and Communications (ICNC), 2013

Tony V Robinson, Building Virtual Machine Labs: A Hands-On Guide, CreateSpace Independent Publishing Platform, 2017.