DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

PROJECTE DE DOCTORAT INDUSTRIAL
EXPEDIENT 2015 DI 077

DADES DE L'EMPRESA I DE L'ENTORN ACADÈMIC

Títol del projecte
Machine Learning for Malware Behaviour Analysis

Empresa
ENEO Tecnología S.L.

Responsable de l'empresa
Jose Ignacio Murcia García

Universitat o Centre de Recerca
Universitat Pompeu Fabra

Director/a de tesi
Vanesa Daza Fernández

Treballador/a de l'empresa i doctorand/a
Alberto Redondo Hernández

BREU DESCRIPCIÓ DEL PROJECTE DE RECERCA

Malicious software is one of the major threats on the Internet today. A variety of malicious software, ranging from classic computer viruses to Internet worms and bot networks, targets computer systems linked to the Internet. Proliferation of this threat is driven by a criminal industry which systematically attacks networked hosts for illegal purposes, such as distribution of spam messages or gathering of confidential data. Unfortunately, the increasing amount, diversity and level of sophistication of malicious software make classic security techniques, such as anti-virus scanners ineffective. In contrast to static techniques, dynamic analysis of binaries during run-time enables monitoring the behavior of malicious software, which is often indicative for malicious activity. Hence, there has been substantial research on the development of tools for collection and monitoring of malicious software. While monitoring binaries during run-time provides means for studying the behavior of malicious software, it is by itself not sufficient to alleviate the threat of malicious software proliferation. What is needed is the ability to automatically analyze the behavior of malicious software binaries. Something similar happens with Intrusion Prevention Systems (IPS). They can analyze traffic in a huge network in order to prevent malicious activities, which may be aimed at stealing or disrupting information, or corrupting network protocols. The level of sophistication of current cyberattacks, their increasing frequency, as well as their dynamic nature make again classic security systems, such as Snort, not very effective. Hence, also in this scenario, research aims at designing tools for collection and monitoring of traffic networks that analyze and predict the behavior of malicious behaviors from log entries.

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

Agència de Gestió d'Ajuts Universitaris i de Recerca
AGAUR

DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

This project will investigate the automatic analysis of data gathered in cybersecurity scenarios using state-of-the-art machine learning techniques. In particular, the project will investigate scalable clustering, regression and classification techniques for detecting security-related anomalies as well as feature selection techniques to allow scalable computation with a large number of features. The project will focus on the application of machine learning to incremental and real-time analysis of collected data in order to process the behavior of a large number of binaries on a daily basis. This incremental analysis will significantly reduce the run-time and memory overhead of batch analysis methods, while providing accurate discovery of novel security-related disfunctionalities.

Generalitat de Catalunya
Departament d'Empresa i Coneixement
Secretaria d'Universitats i Recerca

AGAUR Agència de Gestió d'Ajuts Universitaris i de Recerca