RAMSES

INTERNET FORENSIC PLATFORM FOR TRACKING THE MONEY FLOW OF FINANCIALLY-MOTIVATED MALWARE

Background

The Internet has become a key piece of any business activity. Criminal activity is not an exception. Some crimes previous to the Internet, such as thefts and scams, have found in the Internet the perfect tool for developing their activities. The Internet allows criminals hiding their real identity and the possibility to purchase specific tools for stealing sensitive data with a very low investment.

Objectives

The overall objective of RAMSES is to design and develop a holistic, intelligent, scalable and modular platform for Law Enforcement Agencies (LEAs) to facilitate digital Forensic Investigations. The system will extract, analyse, link and interpret information extracted from Internet related with financially-motivated malware.

Customers, developers and malware victims will be included in order to obtain a better understanding of how and where malware is spread and to get to the source of the threat. To achieve these ambitious objectives, this project will rely on disruptive Big Data technologies to firstly extract and storage, and secondly look for patterns of fraudulent behaviour in enormous amounts of unstructured and structured data.

Activities

We will focus on 2 case studies: ransomware and banking Trojans. In order to do this, RAMSES brings together the latest technologies to develop an intelligent software platform, combining scraping of public and deep web, detecting manipulation and steganalysis for images and videos, tracking malware payments, extraction and analysis of malware samples and **Big Data analysis** and **visualizations tools**.

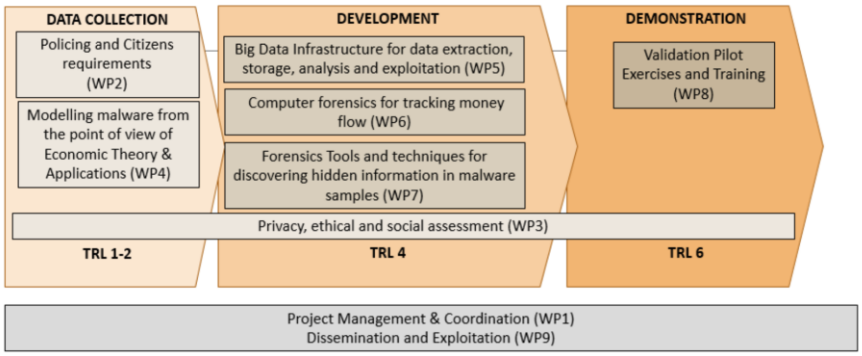
Funding Programme:
This project has received funding from the European Union's Horizon 2020 research and innovation Programme under Grant Agreement No 700326.

Project Duration:
01/09/2016 – 31/08/2019

Project Budget:
3.8 million euro

Project Website:
www.ramses2020.eu

Validation pilots will take place in **three different EU countries** (**Portugal**, **Belgium** and **Spain**) being the first a mono-LEA pilot in each site and the second a collaborative investigation pilot between several LEAs. Commercial potential will be validated during the project supported by a feasibility study to assess determinants for the adoption of the platform and appropriate business models.



Impact:

The impact of RAMSES can be analysed from two different perspectives:

External: The project has a clear focus on reaching tangible assets towards improving the tools for Internet Forensics in Europe. Additionally, RAMSES aims to use open-source and free software. The developed platform will be free to external European Law Enforcement Agencies that sign up for RAMSES.

Internal: The RAMSES impact is particularly relevant as a result of the research and innovation capacities of the consortium. For technological partners, RAMSES enables them to leverage and improve existing technology, putting it in value for a very specific problem. For LEAs, it materializes the exploitation of existing knowledge and enhances their care cycle, improving data collection for practitioners and constituting new communication channels with citizens.

Project Coordinator:
TREELOGIC

Tatiana Silva,
Tatiana.Silva@treelogic.com

Project Participants:

treelogic

Politia

University of Kent | Computing

Trilateral Research

Universidad Complutense Madrid

Politecnico Milano 1863

RSSC Research Centre on Security and Crime

Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei

Politie

Universität des Saarlandes