Poster: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware

Esteban Alejandro Armas Vega[1], Ana Lucila Sandoval Orozco[1],
Luis Javier García Villalba[1*], Julio Hernandez Castro[2], Tatiana Silva[3], Alejandro Prada[3]

[1]Group of Analysis, Security and Systems (GASS)
Department of Software Engineering and Artificial Intelligence (DISIA)
Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases, 9, Ciudad Universitaria,28040 Madrid, Spain
Email: esarmas@ucm.es, {asandoval, javiergv}@fdi.ucm.es

[2]School of Computing, Office S129A, University of Kent
Cornwallis South Building, Canterbury CT2 7NF, UK
Email: j.c.hernandez-castro@kent.ac.uk

[3]Treelogic, Avda. Manoteras 38, Oficina D614, 28050 Madrid, Spain
Email: {tatiana.silva, alejandro.prada}@treelogic.com

***Abstract*—RAMSES project has the main goal of design and develop a intelligent platform for Law Enforcement Agencies (LEA's) to facilitate digital Forensic Investigations. The system will extract, analyse, link and interpret information extracted from Internet, in order to obtain a better understanding of how and where malware is spread and get to the main source.**

1. Introduction

The Internet has become a key piece of any business activity. Criminal activity is not an exception. Some crimes 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. Over the last years, Internet Crime ($e-Crime$) has changed its business model, becoming more professional. The more skilled criminals offer their services to other criminals with less IT skills. This is known as CaaS ($Crime-as-a-Service$) and generates around 300.000 millions of dollars per year according to the Europol [1]. Criminals often offer their skills in forums of the Deep Web and the Dark Net, where anonymisation techniques used allow users to communicate freely without being traced. In these forums, potential clients can find all type of solutions for doing illegal activities. They can buy fake ID cards, fake driver licenses or fake passports for opening banks accounts. They can also find software kits, such as the bank Trojan Zeus, which allows criminals less skilled to infect thousands of computers for stealing sensitive information.

2. Project

RAMSES Project [2] has followed a purposeful, multi-disciplinary approach in establishing the consortium (Figure 1). The consortium is made up of 11 partners from 6 European Countries: Treelogic (Project Coordinator), Trilateral Research, Research Centre on Ssecurity and Crime (RISSC), Complutense University of Madrid, University of Kent, Center for IT-Security, Privacy and Accountability (CISPA), Polytechnic of Milan, Police College of Bavaria, Police of Portugal, Police of Spain, Federal Police of Belgium. Constituted to handle scientific, technical and non-technical aspects, as well as management, dissemination, exploitation and communication capabilities to maximise impact.

Figure 1: The consortium

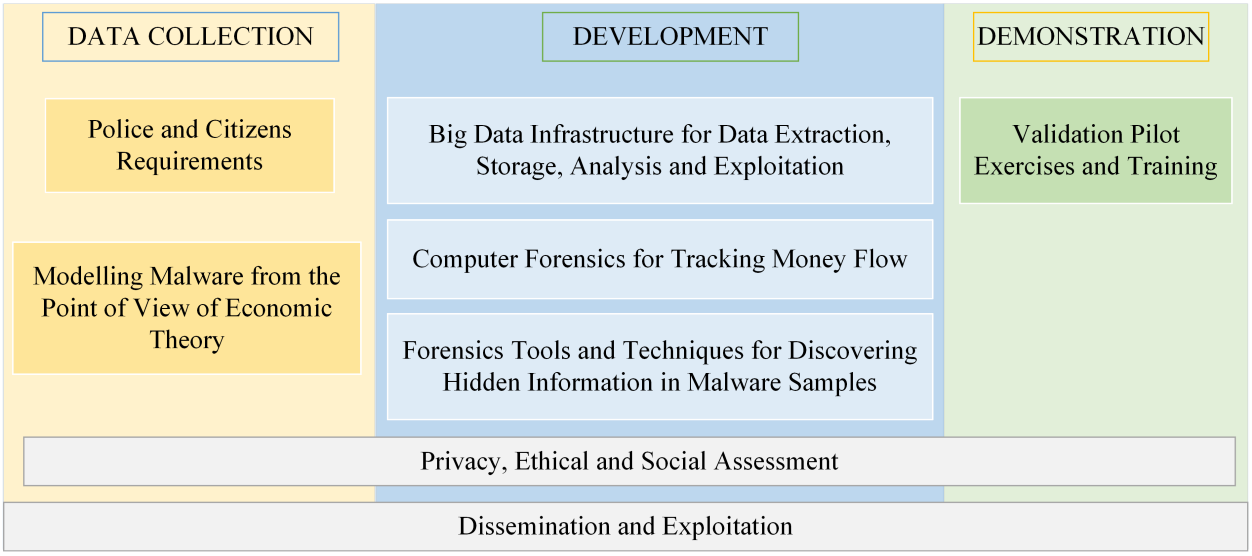

Figure 2: RAMSES Schema

3. Platform

The RAMSES project will design and develop a system to extract, analyse, link and interpret information extracted from Internet (including Deep Web and Dark net) related with financially-motivated malware in order to obtain a better understanding of how and where malware is spread and to get to the source of the threat. 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. On the other hand, many malware will be examined, in order to find evidence of who is behind the attack.

To achieve these ambitious objectives, this project will rely on disruptive Big Data technologies to firstly extract and store, and secondly look for patterns of fraudulent behaviour in enormous amounts of unstructured and structured data. Among its objectives, Ramses will focus on 2 case studies: Ransomware and Banking trojans.

In order to 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. Such strategic objective is addressed through specific objectives/goals, as described below:

- Developing effective guidelines and collaborative methodologies for LEAs investigations.
- Developing a set of tools for Internet Forensics.
- Demonstrating the impact of the RAMSES platform, through several pilot exercises in different countries, training and awareness campaigns.

Figure 2 provides the core concepts and ideas behind each goal.

4. 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 LEA's, it materializes the exploitation of existing knowledge and enhances their care cycle, improving data collection for practitioners and constituting new communication channels with citizens.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326. Website: http://ramses2020.eu

References

[1] EUROPOL. The Internet Organised Threat Assessment (iOCTA) 2014. http://tinyurl.com/javlulb.

[2] RAMSES Project – Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware. http://ramses2020.eu.