RAMSES

NEWSLETTER

Version 1 I February 2018

What is RAMSES?

RAMSES is a H2020 funded project coordinated by Treelogic. It brings together 11 partners from all over Europe and combines experts from the technical, the research and the Law Enforcement sector. Under the topic „Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware", the RAMSES consortium is designing and developing a holistic, intelligent, scalable and modular platform for Law Enforcement Agencies (LEAs) to facilitate digital Forensic Investigations. Thereby, the system will extract, analyze, 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 behavior in enormous amounts of unstructured and structured data.

Internet Forensic platform for tracking the money flow of financially-motivated malware

Why RAMSES?

During the 1980s and 1990s, malicious programs were mostly created as a form of vandalism or prank. But in the course of the last years, a majority of malware programs have been written with a financial or profit motive in mind. In order to counteract this phenomenon and to support Law Enforcement Agencies in their fight against financially-motivated malware, the RAMSES consortium is not only developing a platform to facilitate digital Forensic Investigations but also conducts research in the field of financially motivated malware. To get an impression of our work, please find below some extracts of the findings and results so far.

Altcoins-Alternative to Bitcoins

In 2013, CryptoLocker made - probably for the first time - use of the Bitcoin digital currency platform to collect ransom money. The advantages of using cryptocurrency were made apparent in the aftermath, with a final sum of $3,000,000 being credited to the operators. Though the ransomware itself was thwarted in early June 2014, the use of digital currency as a means of collecting ransoms on a large scale had been proven effective. Since then, most ransomware families have made use of Bitcoin to receive ransom. The decentralised and deregulated nature of the blockchain makes it ideal for such nefarious activity, though it is not resilient against analytical tracking techniques. As the Bitcoin blockchain is public in all respects, it is possible to trace transactions, even those that have been performed using mixing services. This has led to an interest in altcoins, cryptocurrencies other than Bitcoin that boast improved anonymity and privacy features. Altcoins vary in nature, from stores of value (like Bitcoin) to service-driven mini-economies. This leads to a dizzying array of different crypto-currencies, some in definitions to outline how they resist current

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

graphic techniques and provides a technical, financial and criminological analysis of each discussed altcoin. (UNIKENT) **Read more**

Digital Surveillance by LEAs

Malware are growing at exponential rates and continue to be the first of the top cyber-threats. Financial/ banking malware is a category of the cybercrime overall phenomenon, which has been built to scan a computer machine or an entire computer network, to gain information associated with financial transactions. This malware manages to bypass secure information technologies developed specifically to protect the monetary assets of financial institutions and their customers and targets mainly electronic fund transfers (EFT) and Automated Clearing House (ACH) transactions. While Trojans being one of the most common and dangerous types of malware, ransomware are becoming more targeted and sophisticated. special units dealing with cybercrime, efficacy and efficiency is still hindered by the lack of adequate procedures, as well as human and technological resources. Forensic expertise and digital forensic are becoming crucial for LEAs during all their activities in order to investigate and prosecute cybercrime. The complexity of the area requires the implementation of cyber intelligence as new intelligence discipline, including unique training, education, skill sets and tradecraft required to successfully conduct meaningful collection and analysis in the cyber domain. In addition, the international character of these crimes demonstrates the importance of strong networking and close cooperation on a European and international scale, as well as the need of agile and rapid information exchange procedures.

The Research Centre on Crime and Security (RISSC) together with project partners develops a comprehensive and multifaceted analysis of financially motivated malware, presenting how they work as well as the sources they derive from; the approaches and practices used for digital monitoring by Law Enforcement Agencies as well as the role of advanced techniques in the fight against this malicious software. (RiSSC) **Read more**

Economic modeling of malware

Ransomware is a growing, diversifying and highly profitable criminal enterprise which exploits trust and/ or limited technical knowledge to take control of a target computer, encrypting data and holding it to may be employed by criminals to increase the profitability of ransomware. With growing numbers of privacy focused cryptocurrencies, it may also be possible for Bitcoin friction to be eased, allowing a much more rapid growth of ransomware in both the short and long term. Convergence to optimal strategies and higher ransom values, either by design, or simple trial and error, is therefore inevitable. The University of Kent focuses on these economic phenomena and analyses the use of strategies that involve threats, negotiation, price discrimination, and more, to help define the current state of ransomware. (UNIKENT) **Read more**

Analysis system for malware

The RAMSES Project aims to design and implement a holistic, intelligent, scalable and modular software platform for Law Enforcement Agencies to facilitate digital forensic investigations. The system should extract, analyse, link and interpret information extracted from the Internet (surface and deep web) and related to financially-motivated malware.

The system comprises two different tools which allow different and automated types of forensic analysis. The first, BitIodine, is a modular framework which parses the blockchain, clusters addresses that are likely to belong to the same user or group of users, classifies such users, labels them, and finally visualizes complex The University of Kent outlines in cooperation with consortium partners the current state of the art in ransom strategy and compares current criminal strategies with optimal profit models. This work provides the foundation for the development of a predictive economic model of ransomware as a profit-driven criminal enterprise. (POLIMI) **Read more**

For more information visit us on:
www.ramses2020.eu

or contact us via email:
info@ramses2020.eu