RAMSES

NEWSLETTER

Version 2 | May 2019

What is RAMSES ?

RAMSES is a H2020 funded project coordinated by POLIMI. Eleven technical, scientific, and police partners from all over Europe are developing a holistic, intelligent, scalable, and modular platform for Law Enforcement Agencies (LEAs) to facilitate digital forensic investigations. The system extracts, analyzes, links, and interprets information extracted from the internet related with financially motivated malware.

> Internet forensic platform for tracking the money flow of financially motivated malware

An internet forensic tools set !

RAMSES brings together the latest technologies in a software platform which integrates seven services:

- OSINT service
- Darknet service
- Ransomware classifier service
- Bitcoin tracker service
- Banking Trojan analyser service
- Multimedia forensic service
- Malware intelligence service

Some services comprise more than one tool, most of which are online. Results of the offline tools are uploaded to the RAMSES platform and thereby also integrated.

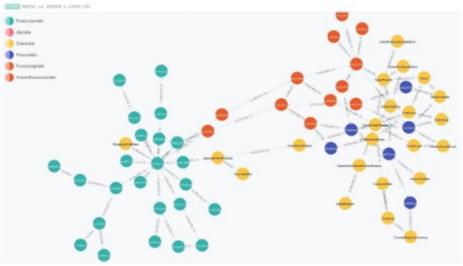
Functionalities

Search among large volumes of data already processed: IP addresses, nicknames, technologies, names of RATs, or any other keyword of interest to the investigator.

Visualize the results of malware analysis, clustering, and forensics.

Explore the relationships between different entities, such as IP addresses, usernames, names of malware, domains.

Alerts can be defined by LEAs to note important events such as the de-anonymization of a hidden service selling malware.



RAMSES searches, explores, visualizes, and alerts

OSINT service

The *OSINT* (**o**pen **s**ource **int**elligence) *service* integrates data into the RAMSES platform from sources such as Twitter, Pastebin, HackForums, and Reddit. The information gathered by crawlers is only stored, processed, and analyzed when related to malware.

Darknet service

The *darknet service* is a search engine enabling the user to look up the names of specific ransomware and trojans or enter more generic requests and find hidden services on the darknet. Results of the search show a list of services on Tor related to the key word(s). The user can filter the list using different categories, e.g. “malware detected” and “malware not detected”.

Furthermore, the Darknet service downloads website information, fingerprints the server, and correlates it in order to find relationships between websites.

Ransomware classifier service

The *ransomware classifier service* includes two functions: analysis of a new ransomware screenshot and checking of previous uploads and their results.

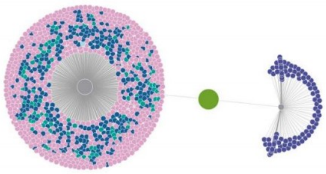
Screenshots of the victim’s infected computer can be uploaded to the RAMSES platform to identify, classify, and extract relevant information about the ransomware.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700326.

RAMSES

Bitcoin tracker service

The *bitcoin tracker service* parses the blockchain, clusters addresses, classifies and labels users, and finally visualizes complex information extracted from the bitcoin network.
Each node of the bitcoin network must store the entire history of every transaction (so-called blockchain). The bitcoin tracker service uses data from the blockchain as input and allows the user to search for information related to a specific bitcoin address.



RAMSES Bitcoin tracker results output example

Multimedia forensic service

The *multimedia forensic service* is a toolkit consisting of two instruments: The first instrument is able to extract and process detailed metadata, such as GPS location or technical features, from images and videos. This information can be used to identify the source (e.g. digital camera, cell phone) of an image/video when a set of possible sources exists. In case there is no pool of sources, it can be used to group images/videos into sets in which all files originate from the same device.
The second instrument analyzes images and videos on byte level, file format level, and pixel level to detect alterations and conclude forgery. Results of analyses are uploaded to the RAMSES platform.

RAMSES geopositioning a set of pictures in Google Maps

Malware intelligence service

The *malware intelligence service* collects and correlates activities of malicious actors. The service offers information such as IP addresses and malware family. It provides additional intelligence on malicious actors connected to ransomware and/or banking Trojan campaigns. The information gathered is not limited to these campaigns but constitutes a representative sample of malicious activities and provides legally relevant evidence for attributing other criminal activities to a malicious actor.

Banking Trojan analyser service

The *banking trojan analyser service* consists of an online and an offline version: The online version is integrated into the RAMSES platform. It uses binary files of banking Trojans as input and runs both a differential analysis and a memory forensics analysis.
The offline version takes a (complete or partial) memory dump as input, which is obtained from an infected machine. It runs a memory forensics analysis. Results of analyses are uploaded to the RAMSES
platform.

Next steps ...

The RAMSES web platform is running with the (online) tools being integrated to a varying degree. Meaningful results can already be delivered in the areas of financial tracking of Bitcoin associated with cybercrime, malware profiling, image and video analysis, social media / forum scraping, and economic modeling of ransomware. Currently, pilot projects are being held in order to assess LEAs' needs as end-users of the product. Results are used to improve the RAMSES' software and the user experience.

For more information visit us on
www.ramses2020.eu

follow us on Twitter
#RamsesEU

or contact us via e-mail
info@ramses2020.eu

or in person at
Stefano Zanero
Politecnico di Milano
Dip. Elettronica, Informazione e Bioingegneria
Via Ponzio, 34/5
20133 Milano

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326.