RAMSES

Internetbasierte Plattform zu forensischen Untersuchung und Verfolgung von Geldflüssen verursacht durch finanziell-motivierte Malware

Hintergrund

In den letzten Jahren ist das Internet zum Mittelpunkt vieler Geschäftstätigkeiten geworden, wobei kriminelle Aktivitäten keine Ausnahme darstellen. Das Internet erlaubt Verbrechern aus der ganzen Welt ihre kriminellen Bestrebungen wie Diebstahl und Betrug voranzutreiben, indem es ihnen ermöglicht die eigene Identität zu verschleiern. Zusätzlich ist es heutzutage möglich die verschiedensten Programme zu erwerben, um sensible Daten ohne viel Aufwand zu stehlen.

Ziel

Aus diesem Grund hat sich das Projekt RAMSES das Ziel gesetzt, eine holistische, intelligente, skalierbare und modulare Plattform für Polizeibehörden zu entwickeln, um ihnen die digitale forensische Arbeit zu erleichtern. Das System wird in der Lage sein, Informationen, die im Zusammenhang mit finanziell motivierter, zielgerichteter Malware stehen, selbstständig aus dem Internet zu filtern, diese zu analysieren und anschließend zu interpretieren.

Während des Projektes werden sowohl Entwickler und Nutzer als auch Opfer von Schadsoftware involviert, um ein besseres Verständnis zu finanziell motivierte Malware zu erhalten und zu verstehen wann und auf welchem Wege diese verteilt wird. Um diese Ziele zu erreiche, greift RAMSES auf **Big Data** Technologien zurück und beginnt mit der Sammlung von **unstrukturierten und strukturierten Daten** um anschließen darin nach Anzeichen von betrügerischem Verhalten zu suchen.

Aktivitäten

Der Fokus von RAMSES liegt dabei auf zwei Fallbeispielen: Ransomware und Banking-Trojaner. Hierfür werden die neusten Technologien herangezogen, um eine intelligente Software-Plattform zu entwickeln, die mit Hilfe von **Big Data Analysen** und **Visualisierungstools** in der Lage sein wird das Surface Web und das Deep Web abzusuchen, Manipulationen und Steganalysen in Bildern und

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

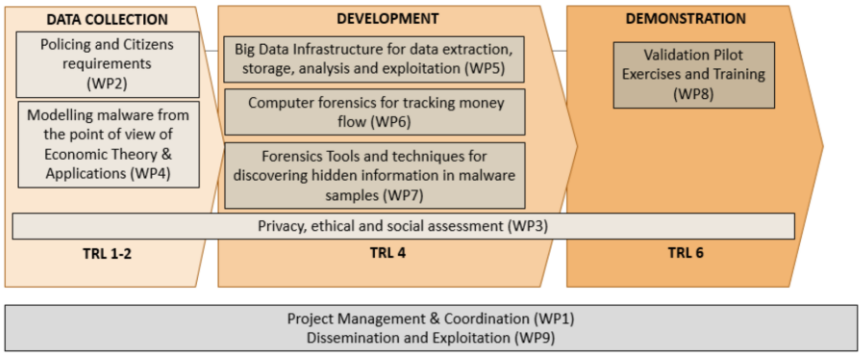
Project Duration:
01/09/2016 – 31/08/2019

Project Budget:
3.8 million euro

Project Website:
www.ramses2020.eu

Videos zu erkennen, Malware-Zahlungen zu verfolgen und Beispiele von Malware zu finden und zu analysieren.

Die Plattform wird im Laufe des Projekts in Zusammenarbeit mit Polizeibehörden in **verschiedenen europäischen Ländern** (**Portugal**, **Belgien** und **Spanien**) getestet. Zudem werden kommerzielle Potenziale während des Projektes validiert, unterstützt durch eine Machbarkeitsstudie zur Bewertung von Faktoren für die Annahme der Plattform und für angemessene Geschäftsmodelle.



Auswirkung

Die Auswirkungen von Ramses können aus zwei verschiedenen Perspektiven betrachtet werden:

Extern: Das Projekt hat das klare Ziel vor Augen, die Möglichkeiten der Internetforensik in Europa zu verbessern. Zudem wird RAMSES sowohl Open-Source als auch frei erhältliche Software nutzen. Die entwickelte Software wird für Strafvollzugsbehörden, die sich bei RAMSES registriert haben, kostenfrei sein.

Intern: Die Auswirkung von RAMSES ist besonders auf Grund des Forschungs- und Innovationsvermögens des Konsortiums relevant. Den technischen Partnern wird ermöglicht bereits existierende Technologien wirksam einzusetzen und zu verbessern. Für Strafvollzugsbehörden wird der Zugang zu Wissen gefördert, die Datenerfassung verbessert und neue Kommunikationskanäle mit Bürgern geschaffen.

Project Coordinator:
TREELOGIC

Tatiana Silva,
Tatiana.Silva@treelogic.com

Project Participants:

treelogic
Policia
University of Kent Computing
Trilateral Research
Universidad Complutense Madrid
Politecnico Milano 1863
RISSC
Hochschule für den öffentlichen Dienst in Bayern Fachbereich Polizei
Politie
Universität des Saarlandes