RAMSES

PLATAFORMA FORENSE NA INTERNET PARA A LOCALIZAÇÃO DE FLUXO MONETÁRIO GERADO POR MALWARE COM MOTIVAÇÃO FINANCEIRA

Contexto

A Internet tornou-se uma peça-chave de qualquer atividade empresarial e a atividade criminosa não é exceção. Alguns crimes prévios à existência da Internet, tais como furtos e burlas, encontraram nesta a ferramenta perfeita para desenvolver as suas atividades. A Internet permite aos criminosos ocultar a sua verdadeira identidade, bem como a possibilidade de comprar ferramentas específicas para furtar dados confidenciais com um investimento muito baixo.

Objetivos

O objetivo global do projeto RAMSES é conceber e desenvolver uma plataforma modular, escalável, inteligente e holística para os serviços de aplicação da lei (LEAs) de modo a facilitar investigações forenses digitais. O sistema irá extrair, analisar, relacionar e interpretar informação extraída da Internet relacionada com *malware* com motivação financeira.

Clientes, criadores e vítimas de *malware* serão incluídos no projeto por forma a obter um melhor entendimento de como e onde o *malware* é difundido, assim como para chegar à fonte da ameaça. Para alcançar estes objetivos ambiciosos, este projeto basear-se-á em tecnologias de rutura de *Big Data* para, em primeiro lugar, extrair e armazenar e de seguida procurar padrões de comportamentos fraudulentos em enormes quantidades de dados estruturados e não estruturados.

Atividades

Centrar-nos-emos em dois casos de estudo: *ransomware* e *trojans* bancários. Para tal, o projeto RAMSES reúne os últimos avanços tecnológicos para desenvolver uma plataforma de *software* inteligente, combinando o *scraping* da *web* superficial com o da invisível, detetando manipulação e esteganálise em imagens e vídeos, localizando pagamentos de *malware*, extraindo e analisando amostras de *malware* e **analisando *Big Data*** e **ferramentas de visualização**.

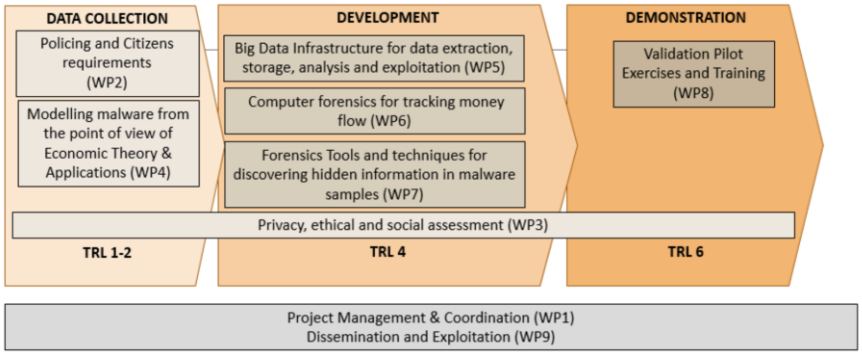
Funding Programme:
This project has received funding from the European Union's Horizon 2020 research and innovation Programme under Grant Agreement No 700326.

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

Project Budget:
3.8 million euro

Project Website:
www.ramses2020.eu

Serão realizadas validações-piloto em **três países diferentes da UE** (**Portugal**, **Bélgica** e **Espanha**), sendo a primeira apenas para um único LEA em cada local e a segunda uma investigação colaborativa entre vários LEAs. O potencial comercial será validado durante o projeto, sustentado por um estudo de viabilidade para avaliar os determinantes para a adoção da plataforma e modelos empresariais apropriados.



Impacto:

O impacto do projeto RAMSES pode ser analisado sob duas perspetivas diferentes:

Externo: O projeto centra-se claramente em aproximar os ativos tangíveis com vista a melhorar as ferramentas para a investigação forense na Internet na Europa. Adicionalmente, o projeto RAMSES visa a utilização de *software* gratuito e de fontes abertas. A plataforma desenvolvida será gratuita para os serviços europeus de aplicação da lei externos que se inscrevam no projeto RAMSES.

Interno: O impacto do projeto RAMSES é particularmente relevante como resultado das capacidades de investigação e inovação do consórcio. Aos parceiros tecnológicos, o projeto permite-lhes potenciar e melhorar a tecnologia existente, valorizando-a face a um problema muito específico. Para os serviços de aplicação da lei, materializa a exploração de conhecimento existente e melhora o ciclo de cuidados, aperfeiçoando a recolha de dados por parte dos profissionais e constituindo novos canais de comunicação com os cidadãos.

Project Coordinator:
TREELOGIC

Tatiana Silva,
Tatiana.Silva@treelogic.com

Project Participants:

treelogic

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