



RAMSES

INTERNET FORENSIC PLATFORM VOOR HET TRACEREN VAN DE GELDSTROOM VOOR HET TRACEREN VAN DE GELDSTROOM VAN FINANCIËEL GEMOTIVEERDE MALWARE

Achtergrond

Het internet is een sleutel onderdeel geworden van eender welke bedrijfs activiteit. De criminele activiteit is hier op geen uitzondering. Sommige misdrijven van voor de tijd van het internet, zoals diefstal en oplichting, hebben het internet als perfecte middel gevonden voor het verder ontwikkelen van hun activiteiten. Het internet laat toe om de echte identiteit van de crimineel te verbergen en de mogelijkheid om zeer goed koop tools aan te kopen om sensatieve date te stelen.

Objectieven

Het algemeen doel van RAMSES is om een volledig, slim, aanpasbaar en modulair platform te maken voor de Politie diensten om digitale forensische ondersteuning te bieden. Het systeem zal extracteren, analyseren, linken leggen en doet een interpretatie van de informatie welke uit de internet gerelateerde met financieel gemotiveerde malware werd gehaald.

Gebruikers, ontwerpers en slachtoffers van de malware zullen bevraagd worden om zo beter te kunnen begrijpen van hoe de malware is verspreid en de bron van malware terug te vinden. Om deze ambitieuze objectieven te behalen, zal dit project steunen op versturende Big Data technologie om eerst te extraheren en op te slaan, en als tweede zoeken achter patronen van fraudulent gedrag in grote hoeveelheden van gestructureerde en ongestructureerde data.

Activiteit

We zullen onze focus leggen op 2 case studies: Ransomware en bank Trojans. Om dit te doen, zal RAMSES gebruik maken van de laatste technologieën en ontwikkelingen op vlak van intelligente software, in combinatie met een doorzoeking van het publieke en deep web, door detectie van manipulaties en steganalyse te doen voor afbeeldingen en video's, het volgen van betalingen via de malware, de malwaresamples uitpakken en analyseren en **GROTE DATA analyse** en **virtualisatie tools** te gebruiken

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

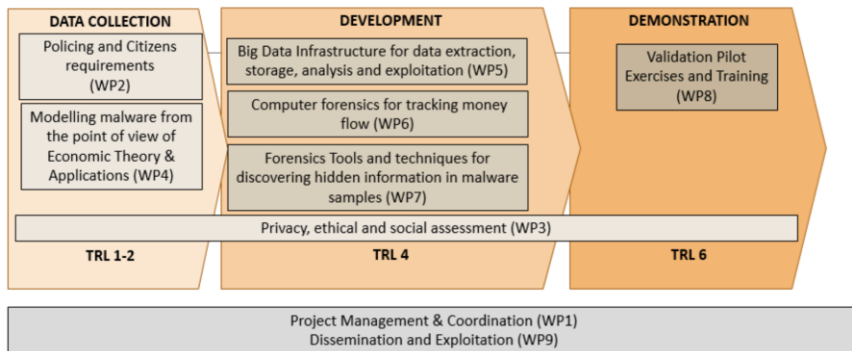


De validatie pilot projecten zal plaats vinden in **drie verschillende EU landen (Portugal, België en Spanje)** door de eerste mono-LEA pilot te zijn in elk land en de tweede gezamenlijke onderzoeks project tussen de verschillende LEA's. De commerciële mogelijkheden zullen gevalideerd worden gedurende het project en ondersteund worden door een haalbare studie om na te gaan of er een aanvaarding is voor het platform en het bijhorende bedrijfsmodel..

Project Coordinator:
TREELOGIC

Tatiana Silva,
Tatiana.Silva@treelogic.com

Project Participants:







Impact:

De impact van RAMSES kan geanalyseerd worden via twee perspectieven:

External: Het project heeft een duidelijke focus op het onderzoeken van tastbare materiële activa om een verbetering te krijgen van de tool voor forensische internet onderzoek in Europa. Bijkomstig, zal RAMSES zich toespitsen op open source en vrije software. Het ontwikkelingsplatform zal gratis zijn voor andere niet Europese politie diensten dat mee instappen in het RAMSES project.

Internal: De impact van RAMSES is voornamelijk relevant als resultaat van onderzoek en ontwikkelings mogelijkheden van dit consortium. Voor de Technologische partners, stuurt RAMSES hen aan om betaande technologiën naar een hoger niveau te brengen en deze te verbeteren, door deze te gebruiken voor een specifiek probleem. Voor de LEA's, maakt het 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 LEAs, maakt het mogelijk om een intreden te doen van de exploitatie van bestaande kennis en verbetert de zorgcyclus, verbetering van de gegevensverzameling voor de beoefenaars van juridische beroepen en nieuwe communicatiekanalen met de burger.





