



RAMSES

## PLATAFORMA FORENSE PARA EL ANÁLISIS DE MALWARE CON FINES FINANCIEROS

### Problemática

Internet se ha convertido en una pieza clave de cualquier actividad empresarial. La actividad criminal no es una excepción. Algunos delitos anteriores a Internet, como robos y estafas, han encontrado en Internet la herramienta perfecta para desarrollar sus actividades. La red permite a los criminales ocultar su identidad real y la posibilidad de comprar herramientas específicas para robar datos confidenciales con una inversión muy baja.

### Objetivos

El objetivo general de RAMSES es diseñar y desarrollar una plataforma holística, inteligente, escalable y modular para las Agencias de Aplicación de la Ley (LEA) para facilitar las **Investigaciones Forenses digitales**. El sistema extraerá, analizará, enlazará e interpretará información extraída de Internet relacionada con el malware con fines financieros.

Se tendrán en cuenta clientes, desarrolladores y víctimas de malware con el fin de obtener una mejor comprensión de cómo y dónde se distribuye el malware y llegar a la fuente de la amenaza. Para lograr estos ambiciosos objetivos, el proyecto se basará en tecnologías **Big Data** para la extracción y almacenamiento de grandes cantidades de datos no estructurados, en primer lugar, y para la búsqueda e identificación de patrones de comportamiento fraudulento entre ellos.

### Actividades

Nos centraremos en dos estudios de caso: **ransomware** y **troyanos bancarios**. Para ello, RAMSES reúne las últimas tecnologías para desarrollar una plataforma de software inteligente, combinando scraping de surface y deep web, detección de manipulación y técnicas de estegoanálisis para imágenes y videos, seguimiento de pagos de malware, extracción y análisis de muestras de malware y **análisis Big Data** y **herramientas de visualización**.

### Programa de financiación:

Este Proyecto ha recibido financiación del Programa de Investigación e Innovación Horizonte 2020 de la Unión Europea, con el Grant Agreement No 700326.



**Duración del Proyecto:**  
01/09/2016 – 31/08/2019

**Presupuesto:**  
3.8 millones euros

**Página Web:**  
[www.ramses2020.eu](http://www.ramses2020.eu)

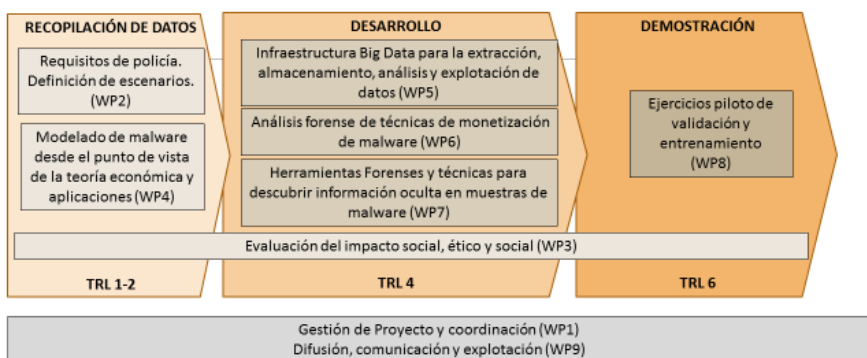


Los pilotos de validación se llevarán a cabo en **tres países europeos diferentes** (Portugal, Bélgica y España) y están divididos en dos fases, siendo el primero un piloto mono-LEA en cada país y el segundo un piloto colaborativo de investigación entre varias LEA. El potencial comercial será validado durante el proyecto apoyado por un estudio de factibilidad para evaluar los factores determinantes para la adopción de la plataforma y modelos de negocio apropiados.

**Coordinador del Proyecto:**  
TREELOGIC

Tatiana Silva,  
[Tatiana.Silva@treelogic.com](mailto:Tatiana.Silva@treelogic.com)

**Consorcio:**



treeologic



University of Kent Computing



UNIVERSIDAD COMPLUTENSE MADRID



POLITECNICO MILANO 1863



Hochschule für den öffentlichen Dienst in Bayern  
Fachbereich Polizei



UNIVERSITÄT DES SAARLANDES

## Impacto

El impacto de RAMSES puede analizarse desde dos perspectivas diferentes:

**Externa:** El proyecto se centra en alcanzar activos tangibles para mejorar las herramientas de Internet Forense en Europa. Además, RAMSES pretende utilizar software libre. La plataforma desarrollada será gratuita para aquellas agencias de seguridad europeas que se suscriban a RAMSES.

**Interna:** El impacto de RAMSES es particularmente relevante como resultado de las capacidades de investigación e innovación del consorcio. Para los socios tecnológicos, RAMSES les permite aprovechar y mejorar la tecnología existente, poniéndola en valor para un problema muy específico. Para las LEA, materializa la explotación de los conocimientos existentes y mejora su ciclo de atención, mejorando la recopilación de datos para los profesionales y constituyendo nuevos canales de comunicación con los ciudadanos.



info@ramses2020.eu



+34 902 286 386



RAMSES - H2020 Project



RAMSES H2020 Project  
@RamsesEU