RAMSES

BOLETÍN DE NOTICIAS

¿Qué es el Proyecto RAMSES?

RAMSES es un proyecto del programa H2020 financiado por la Comisión Europea y coordinado por el Politecnico di Milano (POLIMI). Su consorcio esta formado por once socios técnicos, científicos y policiales de toda Europa. El objetivo principal RAMSES es desarrollar una plataforma holística, inteligente, escalable y modular para las Agencias Policiales (APs) y facilitar las investigaciones forenses digitales. RAMSES extrae, analiza, relaciona e interpreta la información extraída de Internet vinculado al malware motivado económicamente.

> Plataforma forense de Internet para rastreo del flujo de dinero generado por malware económicamente

Herramientas forenses para Internet!

RAMSES reúne las mejores y mas recientes tecnologías en una plataforma de software que integra siete servicios:

- Servicio OSINT
- Servicios de Darknet
- Servicio clasificador de Ransomware
- Servicio de rastreo de Bitcoin
- Servicio de análisis de Troyanos Bancarios
- Servicio forense Multimedia
- Servicio de inteligencia de malware

Algunos servicios comprenden más de una herramienta, la mayoría de las cuales están en línea. Sin embargo, los resultados de las herramientas offline se suben a la plataforma RAMSES y, por lo tanto, también se integran.

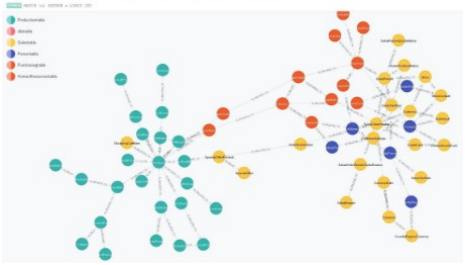
Funcionalidades

Buscar entre grandes volúmenes de datos ya procesados: Direcciones IP, apodos, tecnologías, nombres de RATs, o cualquier otra palabra clave de interés para el investigador.

Visualizar los resultados de análisis de malware, clustering y análisis forense.

Explorar las relaciones entre diferentes entidades, tales como direcciones IP, nombres de usuario, nombres de malware, dominios.

Alertas las APs pueden definir las alertas y señalar eventos importantes como la desanonimización de un servicio oculto que vende malware.



RAMSES searches, explores, visualizes, and alerts.

Servicio OSINT

El servicio OSINT (**o**pen **s**ource **int**elligence) integra en la plataforma RAMSES datos de fuentes como Twitter, Pastebin, HackForums y Reddit. La información recopilada por los rastreadores se almacena, procesa y analiza solo sí está relacionada con malware.

Servicio de Darknet

El servicio de Darknet es un motor de búsqueda que permite al usuario buscar los nombres de ransomware y troyanos bancarios específicos o introducir solicitudes más genéricas y encontrar servicios ocultos en la darknet. Los resultados de la búsqueda muestran una lista de servicios en Tor relacionados con la(s) palabra(s) clave. El usuario puede filtrar la lista utilizando diferentes categorías, por ejemplo, "malware detectado" y "malware no detectado".

Además, el servicio Darknet descarga información del sitio web, toma las huellas dactilares del servidor y lo correlaciona para encontrar relaciones entre sitios web.

Servicio clasificador de Ransomware

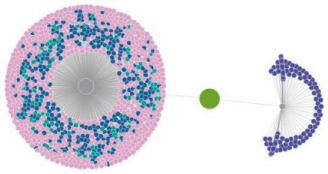
El servicio clasificador de ransomware incluye dos funciones: el análisis de una nueva captura de pantalla de ransomware y la comprobación de las cargas anteriores y sus resultados.

Las capturas de pantalla del equipo infectado de la víctima se pueden subir a la plataforma RAMSES para identificar, clasificar y extraer información relevante sobre el software de rescate.

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

Servicio de rastreo de Bitcoin

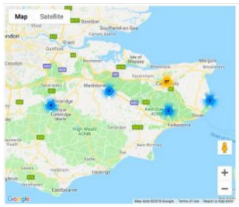
El servicio de rastreo de bitcoin analiza el blockchain, agrupa las direcciones, clasifica y etiqueta a los usuarios, y finalmente visualiza la información compleja extraída de la red de bitcoin.
Cada nodo de la red bitcoin debe almacenar el historial completo de cada transacción (el llamado blockchain). El servicio de seguimiento de bitcoin utiliza datos de la cadena de bloques como entrada y permite al usuario buscar información relacionada con una dirección de bitcoin específica.



Ejemplo de resultado de este servicio en RAMSES

Servicio forense Multimedia

El servicio forense multimedia es un conjunto de herramientas que consta de dos instrumentos: El primer instrumento es capaz de extraer y procesar metadatos detallados, como la ubicación GPS o las características técnicas, de imágenes y vídeos. Esta información puede utilizarse para identificar la fuente de origen (por ejemplo, cámara digital, teléfono móvil) de una imagen/vídeo cuando existe un conjunto de posibles fuentes. En caso de que no haya un grupo de fuentes, se puede utilizar para agrupar imágenes/ videos en conjuntos en los que todos los archivos se originan desde el mismo dispositivo.
El segundo instrumento analiza imágenes y vídeos a nivel de byte, formato de archivo y nivel de píxeles para detectar alteraciones e identificar falsificaciones. Los resultados de los análisis se suben a la plataforma RAMSES.



RAMSES localización de un grupo de imágenes en Google Maps

Servicio de inteligencia de

El servicio de inteligencia de malware recoge y correlaciona la información de las actividades de los actores maliciosos. El servicio ofrece información como direcciones IP y familia de malware. Proporciona información adicional sobre actores maliciosos conectados a campañas de ransomware y/ o troyanos bancarios. La información recopilada no se limita a estas campañas, sino que constituye una muestra representativa de actividades maliciosas y proporciona pruebas legalmente relevantes para atribuir otras actividades delictivas a un actor malicioso.

Servicio de análisis de troyanos bancarios

El servicio de análisis de troyanos bancarios consta de una versión online y otra offline: La versión online está integrada en la plataforma RAMSES. Utiliza archivos binarios de troyanos bancarios como entrada y ejecuta tanto un análisis diferencial como un análisis forense de memoria.
La versión offline toma como entrada un volcado de memoria (completo o parcial), que se obtiene de un equipo infectado. Ejecuta un análisis forense de memoria. Los resultados de los análisis se cargan en la plataforma RAMSES.

Próximos pasos ...

La plataforma web RAMSES funciona con las herramientas (en línea) que se están integrando en mayor o menor medida. Ya se pueden obtener resultados significativos en las áreas de seguimiento financiero de Bitcoin asociadas con la ciberdelincuencia, la creación de perfiles de malware, el análisis de imágenes y vídeos, los medios sociales / foro de raspado, y el modelado económico del software de rescate. Actualmente, se están llevando a cabo proyectos piloto para evaluar las necesidades de las APs como usuarios finales del producto. Los resultados se utilizan para mejorar el software de RAMSES y la experiencia del usuario.

Para mas información visítanos en
www.ramses2020.eu

Síguenos en Twitter
#RamsesEU

Contáctanos vía correo electrónico
info@ramses2020.eu

Dirección de correo postal
Stefano Zanero
Politecnico di Milano
Dip. Elettronica, Informazione e Bioingegneria
Via Ponzio, 34/5
20133 Milano
ITALY

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