RAMSES

NEWSLETTER

Versão 2

O que é o RAMSES?

O RAMSES é um projeto financiado pelo Horizonte 2020, coordenado pelo POLIMI. Onze parceiros técnicos, científicos e policiais de toda a Europa estão a desenvolver uma plataforma holística, inteligente, expansível e modular para as autoridades responsáveis pela aplicação da lei, visando facilitar as investigações forenses digitais. O sistema extrai, analisa e interpreta informações extraídas da Internet, relacionadas com *software* malicioso financeiramente motivado.

Plataforma forense da Internet para rastrear o fluxo monetário de software malicioso financeiramente motivado

Um conjunto de ferramentas forenses na Internet!

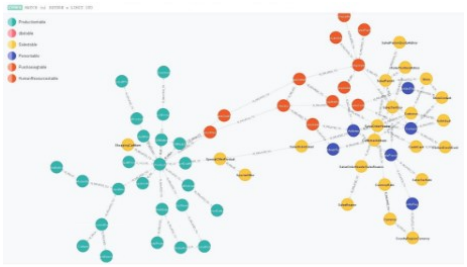
O RAMSES reúne as tecnologias mais recentes numa plataforma- de *software* que integra sete serviços:

- Serviço OSINT
- Serviço Internet obscura
- Classificador de *software* de sequestro
- Serviço de rastreio de *bitcoin*
- Serviço de análise de troianos bancários
- Serviço forense multimédia
- Serviço de informações em matéria de *software* malicioso

Alguns serviços incluem mais do que uma ferramenta. A maioria destas encontra-se em linha. Os resultados das ferramentas fora de linha são carregados na plataforma do RAMSES e são igualmente integrados.

Functionalidades

Pesquisar grandes volumes de dados já objeto de-tratamento: endereços IP, nomes alternativos, tecnologias, nomes dos RAT ou qualquer outra palavra-chave de interesse para o investigador.
Visualizar os resultados da análise do software maligno, dos agrupamentos e da atividade forense.
Explorar as relações entre diferentes entidades, tais como endereços IP, nomes de utilizador, nomes de programas maliciosos, domínios.
Alertas podem ser definidos pelas autoridades de aplicação da lei de modo a detetar eventos importantes, tais como a revelação de um serviço oculto anónimo que vende *software* malicioso.



RAMSES pesquisa, explora, visualiza e alerta

Serviço **OSINT**

O serviço OSINT (*open-source intelligence* ou informações de fontes abertas) integra dados na plataforma do RAMSES de fontes como o Twitter, Pastebin, HackForums e Reddit. As informações recolhidas pelos robôs de pesquisa só são armazenadas, processadas e analisadas quando relacionadas com *software* malicioso.

Serviço Internet obscura

O serviço Internet obscura (darknet service) é um motor de pesquisa que permite ao utilizador procurar os nomes de um *software* de sequestro e troianos específicos ou fazer pedidos mais genéricos e encontrar serviços ocultos na Internet obscura. Os resultados da pesquisa mostram uma lista de serviços no Tor relacionados com a(-s) palavra(s)-chave. O utilizador pode filtrar a lista através de diferentes categorias, por exemplo, «*software* malicioso detetado» e «*software* malicioso não detetado».
Além disso, o serviço Internet obscura descarrega informações sobre o sítio Web, recolhe as impressões digitais do servidor e correlaciona as mesmas a fim de detetar relações entre sítios Web.

Classificador de *software* de sequestro

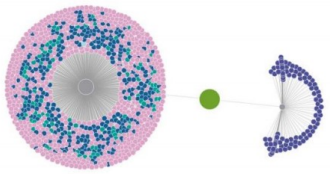
O classificador de *software* de sequestro inclui duas funções: análise de uma nova captura de ecrã de *software* de sequestro (*ransomware*) e verificação de carregamentos anteriores e dos seus resultados. As capturas de ecrã do computador infetado da vítima podem ser carregadas na plataforma do RAMSES para identificar, classificar e extrair informações pertinentes sobre o *software* de sequestro.

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

RAMSES

Serviço de rastreio de *bitcoin*

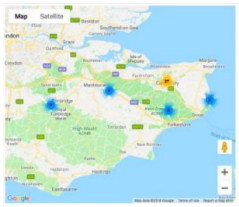
O serviço de rastreio de *bitcoin* analisa a cadeia de blocos, agrupa endereços, classifica os utilizadores e atribui-lhes uma etiqueta e, por último, visualiza informações complexas extraídas da rede de *bitcoin*.
Cada nó da rede *bitcoin* deve conservar toda a história de cada transação (a chamada «cadeia de blocos»). O serviço de rastreio de *bitcoin* utiliza dados da cadeia de blocos como entrada e permite ao utilizador pesquisar informações relativas a um endereço de *bitcoin* específico.



Exemplo de saída de resultados do serviço de rastreio de bitcoin do RAMSES

Serviço forense multimédia

O serviço forense multimédia é um conjunto de ferramentas que consiste em dois instrumentos: o primeiro instrumento é capaz de extrair e processar metadados pormenorizados de imagens e vídeos, tais como a localização GPS ou características técnicas. Estas informações podem ser utilizadas para identificar a fonte (por exemplo, câmara digital, telemóvel) de uma imagem/vídeo quando existe um conjunto de fontes possíveis. No caso de não existir uma variedade de fontes, pode ser utilizado para agrupar imagens/vídeos em conjuntos em que todos os ficheiros sejam provenientes do mesmo dispositivo.
O segundo instrumento analisa imagens e vídeos a nível dos *bytes*, do formato do ficheiro e dos píxeis, para detetar alterações e concluir falsificações. Os resultados das análises são carregados na plataforma do RAMSES.



Geoposicionamento do RAMSES a um conjunto de imagens no Google Maps

Serviço de informações em matéria de *software* malicioso

O serviço de informações em matéria de software malicioso recolhe e correlaciona atividades de intervenientes mal-intencionados. O serviço oferece informações como os endereços IP e uma família de software malicioso. Fornece informações adicionais sobre intervenientes mal-intencionados ligados a campanhas de software de sequestro e/ou de troianos bancários. A informação recolhida não se limita a estas campanhas, campanhas, mas constitui uma amostra representativa das atividades maliciosas e fornece provas juridicamente relevantes para a atribuição de outras atividades criminosas a um interveniente malicioso.

Serviço de análise de troianos bancários

O serviço de análise de troianos bancários consiste numa versão em linha e noutra fora de linha: a versão em linha encontra-se integrada na plataforma do RAMSES. Utiliza ficheiros binários de troianos bancários como entrada e efetua tanto uma análise diferencial como uma análise forense em memória.
A versão fora de linha utiliza um depósito de memória (completo ou parcial) como entrada, que é obtido a partir de uma máquina infetada. Efetua uma análise forense em memória. Os resultados das análises são carregados na plataforma do RAMSES.

Próximos passos…

A plataforma Web do RAMSES está a funcionar com a integração das ferramentas (em linha) em graus variáveis. Já podem ser obtidos resultados significativos nos domínios da localização financeira de *bitcoin* associada à cibercriminalidade, da caracterização do *software* malicioso, da análise de imagens e de material vídeo, do *scraping* dos meios de comunicação social / fóruns e da modelização económica de *software* de sequestro. Estão atualmente a ser realizados projetos-piloto para avaliar as necessidades das autoridades de aplicação da lei enquanto utilizadoras finais do produto. Os resultados são utilizados para melhorar o *software* do RAMSES e a experiência do utilizador.

Para mais informações, visite-nos em
www.ramses2020.eu

Siga-nos no Twitter
#RamsesEU

Ou contacte-nos por correio eletrónico
info@ramses2020.eu

Ou pessoalmente para
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.