RAMSES

SÍNTESE

O projeto RAMSES, teve como objetivo o desenvolvimento de uma plataforma que facilita as investigações digitais de caráter forense ao extrair, analisar e interpretar informação recolhida da Internet relacionada com *malware* de motivação financeira, permitindo por exemplo, detetar a manipulação de mensagens ocultas em imagens e vídeos ou o controlo de pagamentos de *malware*. Este projeto combina a pesquisa na web pública e profunda com ferramentas de análise e visualização de grande quantidade de dados.

Polícia Judiciária

Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica
(UNC3T)

Unidade de Telecomunicações e de Informática
(UTI)

Área de Projetos, Inovação e Conhecimento
(APIC)

2019

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

SUMÁRIO do PROJETO

O RAMSES (GA 700326) é um projeto de desenvolvimento e inovação (RIA), cofinanciado pelo Programa-Quadro Horizonte 2020 da União Europeia e proveniente de uma candidatura H2020-FCT- 2015 "Fight against Crime and Terrorism" no tópico 4 "Internet Forensics to combat organized crime: Security, Fight against criminality, Forensic technologies, others".

Foi registado com o Grant Agreement Nº. 700326 tendo o valor máximo de financiamento atribuído esta PJ sido de 207 843,75€. A execução final foi de 208 057,51€ o que corresponde a uma execução de 101%.

O objetivo do RAMSES foi desenvolver uma plataforma que combina ferramentas de pesquisa na web pública/profunda e de visualização de grande quantidade de dados, designadamente:

- OSINT service
- Darknet service
- Ransomware classifier service
- Bitcoin tracker service
- Banking Trojan analyse service
- Multimedia forensic service
- Malware intelligence service

Estas ferramentas permitem realizar a extração, análise e interpretação de informação relacionada com *malware* de motivação financeira - como por exemplo fazer a deteção a manipulação de mensagens ocultas em imagens e vídeos e o controlo de pagamentos de *malware* - facilitando assim as investigações digitais de caráter forense pelas polícias de investigação criminal.

Com duração de 42 meses (início a 01-09-2016 e final a 30-11-2019), o RAMSES envolveu a sinergia de um consórcio constituído por 12 entidades europeias, entre as quais esta Polícia Judiciária, cuja participação realizou-se na qualidade de *end-user.*

A PJ contribuiu na identificação dos requisitos, na definição dos cenários de utilização, na validação da sua adequação, na organização e validação de um Piloto em Lisboa, na

participação em piloto colaborativo com Polícia Espanhola e Belga bem como na organização de uma Conferência e demonstração do produto final que decorreu em Lisboa nos dias 20 de novembro de 2019.

1. PARTICIPANTES

O RAMSES foi gerido por um consórcio de 12 parceiros cuidadosamente selecionados, com competências complementares particularmente adaptadas à natureza multidisciplinar do projeto: 2 parceiros industriais, 4 PME, 3 parceiros académicos / de investigação e 3 LEAs / utilizadores-piloto, provenientes de seis países europeus diferentes - Bélgica, Portugal, Espanha, Itália, Reino Unido e Alemanha, conforme tabela 1 em baixo.

Nome	Acrónimo	Nacionalidade
POLITÉCNICO DI MILANO	POLIMI	Itália
POLÍCIA JUDICIÁRIA	PJ	Portugal
UNIVERSITY OF KENT	UNIKENT	Reino Unido
RISSC - CENTRO RICERCHE E STUDI SUSICUREZZA E CRIMINALITA ASSOCIAZIONE	RISSC	Itália
UNIVERSIDAD COMPLUTENSE DE MADRID	UCM	Espanha
HOCHSCHULE FUR DEN OFFENTLICHEN DIENST IN BAYERN	BayFHVR	Alemanha
TRILATERAL RESEARCH LTD	TRI	Reino Unido
SERVICE PUBLIC FEDERAL INTERIEUR	BFP	Bélgica
UNIVERSITAT DES SAARLANDES	USAAR	Alemanha
MINISTERIO DEL INTERIOR	MI	Espanha
TREE TECHNOLOGY SA	TREETK	Espanha

Tabela 1 - Participantes no RAMSES

2. ATIVIDADE

Para o desenvolvimento da participação da PJ no projeto, estavam previstos 39.75PM, que foram integralmente cumpridos e ultrapassados, conforme a tabela 2 e gráfico 1 abaixo.

WP	PM previstos	PM executados
WP1	2.5	2.9
WP2	5.5	2.4
WP3	2.5	1.9
WP4	2.0	0.5
WP5	1.0	0.1
WP6	1.5	1.3
WP7	1.0	1.0
WP8	17.5	23
WP9	6.0	6.6
TOTAL	**39.75**	**40.05**

Tabela 2 - PM previstos e executados

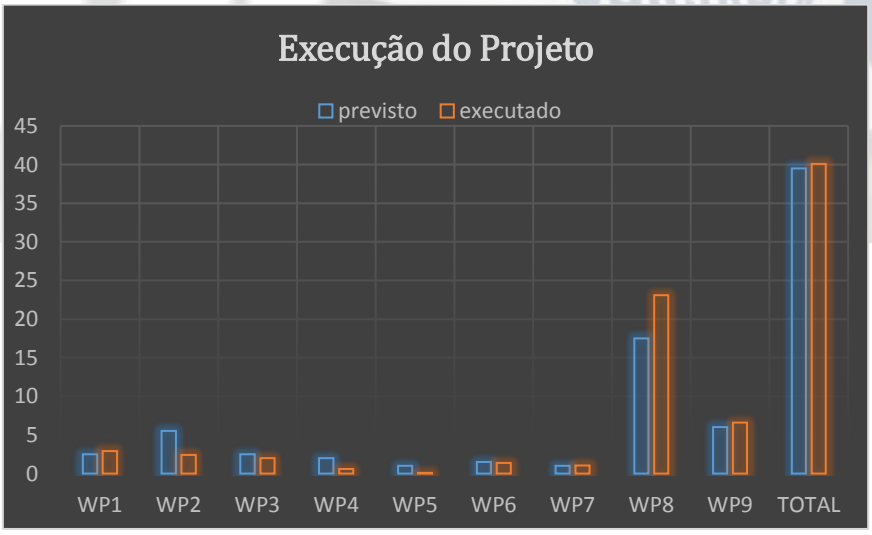

Gráfico 1 – Previsão e Execução

O trabalho desenvolvido pela Polícia Judiciária no RAMSES contou com a participação da Unidade operacional UNC3T e da UTI, acompanhadas pela área de Projetos Inovação e Conhecimento (UTI/APIC) – que garantindo a gestão do projeto ao longo de 42 meses (com um total de 4982 horas de trabalho e 40.5 PM de esforço) conduziu o RAMSES a uma boa execução.

3. PILOTOS

Os Pilotos tiveram o objetivo de avaliar a plataforma e as ferramentas do RAMSES pelos usuários finais (LEAs), tendo tido lugar em dois momentos no segundo período do projeto. De forma a serem familiarizados com a plataforma e antes de prosseguir para teste real, foi realizado um treino inicial dos LEAs que decorreu em duas sessões presenciais.
A primeira sessão teve lugar em setembro de 2018, em Madrid e a segunda em janeiro 2019 em Lisboa. Para além disso, foram disponibilizados aos mesmos, através de uma plataforma *e-learning Moodle*, materiais úteis e exercícios de casos para treino *online* a todos os LEAs envolvidos no RAMSES.

O piloto 1 (setembro de 2018 a fevereiro de 2019) foi projetado para envolver exclusivamente os parceiros da RAMSES - Portugal, Bélgica e Espanha e o Piloto 2 (setembro e outubro de 2019) e a avaliação dos resultados alcançados durante este Piloto foi feita através de um questionário *online* respondido pelos LEAs envolvidos nos testes. Foi com base nos resultados destes questionários que os parceiros técnicos puderam aperfeiçoar a capacidade do RAMSES em responder melhor aos requisitos dos usuários finais.
O piloto 2 destinou-se a validar a plataforma RAMSES, testando suas atuais capacidades para apoiar os LEAs - Parceiros do Consórcio - na troca de informações relevantes, enquanto realizavam dois exercícios cooperativos de investigação forense entre eles.

4. CONFERÊNCIA e DEMONSTRAÇÃO FINAL

A Conferência Final do RAMSES teve lugar no dia 20 de novembro de 2019 em Lisboa na sede desta Polícia Judiciária e contou com a participação de cerca de 100 pessoas desde os membros do Consórcio, a funcionários de várias áreas e departamentos desta Polícia Judiciária a convidados do Ministério Público bem como a outras polícias europeias.

O evento iniciou-se com a apresentação do RAMSES, as suas metas e objetivos. Com familiarização ao conceito, abordagem do projeto e resultados do mesmo no

desenvolvimento de uma plataforma holística, inteligente, escalável e modular que facilita a investigação digital forense aos LEAs, conforme figura 1.

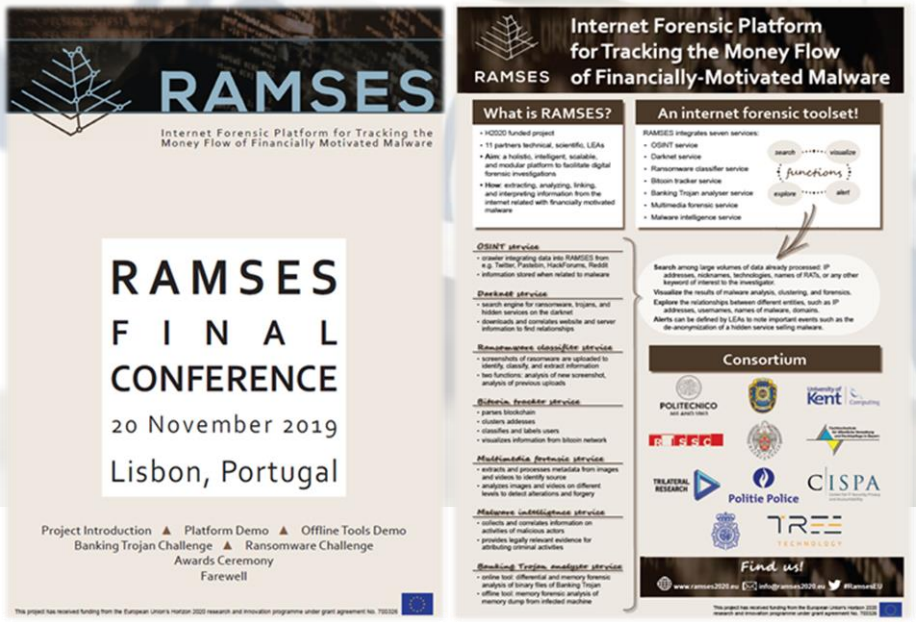

Figura 1 – Posters da Conferência Final

No final da Conferência, foi proporcionado um Workshop "*The Banking Trojan and Ransomware Challenges*" aos participantes, que estando divididos em 10 grupos, puderam ser eles próprios a explorar as ferramentas operacionais da plataforma RAMSES. Este desafio garantiu uma demonstração dinâmica do RAMSES, bom humor

e satisfação dos participantes ao atingir o objetivo principal: explorar a plataforma e conhecer as ferramentas.

Figura 2 – RAMSES Challenge

A conferência terminou com um debate proveitoso em que todos os convidados puderam participar e uma cerimónia de entrega de prémios.

Figura 2 – Foto de Grupo do RAMSES na Conferência

5. CONSIDERAÇÕES FINAIS

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.

O objetivo global do projeto RAMSES foi 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, que usando tecnologias de rutura de *Big Data* para extrair e armazenar e de seguida procurar padrões de comportamentos fraudulentos em enormes quantidades de dados estruturados e não estruturados.
O impacto do projeto RAMSES pode ser analisado sob duas perspetivas diferentes.

Numa perspetiva externa, o projeto centrou-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 visou a utilização de software gratuito e de fontes abertas. A plataforma desenvolvida será gratuita para os serviços europeus de aplicação da lei inscritos no projeto RAMSES.

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

DSID - Lisboa 2020

POLICIA JUDICIÁRIA