



NEWSLETTER

Versione 2

Cos'è RAMSES?

RAMSES è un progetto finanziato dal programma Horizon 2020 e coordinato dal Politecnico di Milano (POLIMI).

Undici partners tecnici, scientifici e rappresentanti delle forze dell'ordine di tutta Europa stanno sviluppando una piattaforma olistica, intelligente, scalabile e modulare per facilitare le indagini forensi digitali. Il sistema estrae, analizza, collega e interpreta le informazioni estratte da Internet relative a malware finanziari.

Internet forensic platform for tracking the money flow of financially motivated malware

forze dell'ordine di tutta Europa stanno sviluppando una piattaforma olistica, intelligente, scalabile

Un set di strumenti forensi su internet!

RAMSES raccoglie le tecnologie più all'avanguardia in una piattaforma software che integra sette servizi:

- OSINT
- Darknet
- Classificatore di ransomware
- Tracciatore di bitcoin
- Analisi dei Trojan bancari
- Analisi forense multimediale
- Intelligence sui malware

Alcuni servizi comprendono più di uno strumento, molti dei quali sono online. I risultati degli strumenti offline vengono caricati sulla piattaforma RAMSES e integrati con gli altri strumenti.

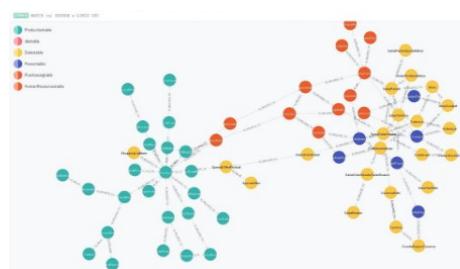
Funzionalità

Il software è grado di **ricercare** tra grandi volumi di dati già elaborati: indirizzi IP, nickname, tecnologie, nomi di RAT o qualsiasi altra parola chiave di interesse per l'inquirente.

Visualizza i risultati dell'analisi del malware, del clustering e della medicina legale.

Esplora le relazioni tra entità diverse, come indirizzi IP, nomi utente, nomi di malware, domini.

Gli **alert** possono essere stabiliti dalle forze dell'ordine per rilevare eventi importanti come la dis-anonimizzazione di un servizio nascosto che vende malware.



RAMSES searches, explores, visualizes, and alerts

Servizio OSINT

Il **servizio OSINT** (open source intelligence) integra i dati nella piattaforma RAMSES da fonti come Twitter, Pastebin, HackForums e Reddit. Le informazioni raccolte dai crawler vengono archiviate, elaborate e analizzate solo quando correlate al malware.

Servizio Darknet

Il **servizio darknet** è un motore di ricerca che consente all'utente di cercare i nomi di specifici ransomware e trojan o immettere richieste più generiche e trovare servizi nascosti sul darknet. I risultati della ricerca mostrano un elenco di servizi su Tor relativi alle parole chiave. L'utente può filtrare l'elenco utilizzando diverse categorie, ad es. "Malware rilevato" e "malware non rilevato". Inoltre, il servizio Darknet scarica informazioni sul sito Web, sulle impronte digitali sul server e le correla al fine di trovare relazioni tra i siti Web.

Servizio di classificazione dei ransomware

Il **servizio di classificazione dei ransomware** comprende due funzioni: analisi di un nuovo screenshot di ransomware e controllo dei caricamenti precedenti e dei loro risultati. Le schermate del computer infetto della vittima possono essere caricate sulla piattaforma RAMSES per identificare, classificare ed estrarre informazioni sul ransomware.



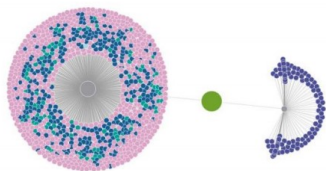


Servizio tracker bitcoin

Il **servizio tracker bitcoin** analizza la blockchain, raggruppa gli indirizzi,

classifica ed etichetta gli utenti e infine visualizza informazioni complesse estratte dalla rete bitcoin.

Ogni nodo della rete bitcoin deve memorizzare l'intera cronologia di ogni transazione (la cosiddetta blockchain). Il servizio tracker bitcoin utilizza i dati della blockchain come input e consente all'utente di cercare informazioni relative a un indirizzo bitcoin specifico.



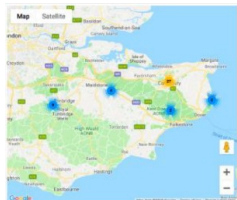
RAMSES Bitcoin tracker results output example

Servizio forense multimediale

Il **servizio forense multimediale** è un toolkit composto da due

strumenti: il primo strumento è in grado di estrarre ed elaborare metadati dettagliati, come la posizione GPS o le caratteristiche tecniche, da immagini e video. Queste informazioni possono essere utilizzate per identificare la fonte (ad es. Fotocamera digitale, telefono cellulare) di un'immagine / video quando esiste una serie di possibili fonti. Nel caso in cui non vi sia un gruppo di fonti, può essere utilizzato per raggruppare immagini / video in gruppi in cui tutti i file provengono dallo stesso dispositivo. Il secondo strumento analizza immagini e video a livello di byte, a livello di formato file e a livello di pixel per rilevare alterazioni e valutare se si tratta di falsificazione. I

risultati delle analisi vengono caricati sulla piattaforma RAMSES.



RAMSES geopositioning a set of pictures in Google Maps

Servizio di intelligence sui malware

Il **servizio di intelligence sui malware** raccoglie e

mette in correlazione le attività dei soggetti malintenzionati. Il servizio offre informazioni come indirizzi IP e famiglie di malware. Fornisce anche indicazioni su soggetti malintenzionati collegati a ransomware e/o campagne di trojan bancari. Le

informazioni raccolte non si limitano a queste campagne, ma costituiscono un campione attività dannose e forniscono prove giuridicamente rilevanti per l'attribuzione di altre attività criminali ad un partecipante malintenzionato.

Servizio di analisi del trojan bancario

Il **servizio di analisi del trojan bancario** è costituito da una versione

online e da una versione offline: la versione online è integrata nella piattaforma RAMSES e utilizza file binari di Trojan bancari come input eseguendo sia un'analisi differenziale che un'analisi forense della memoria.

La versione offline accetta come input un dump della memoria (completo o parziale), ottenuto da una macchina infetta. Esegue anche un'analisi forense della memoria. I risultati delle analisi vengono caricati sulla piattaforma RAMSES.

I prossimi passi ...

La piattaforma web RAMSES è attualmente in uso con gli strumenti (online) integrati in misura diversa. Risultati significativi possono già essere ottenuti nelle aree del tracciamento finanziario di Bitcoin associato a crimine informatico, profilazione di malware, analisi di immagini e video, scraping di social media / forum e modellazione economica di ransomware. Attualmente, sono in corso progetti pilota al fine di valutare le esigenze delle Forze dell'Ordine come utenti finali e beneficiari del prodotto. I risultati vengono utilizzati per migliorare il software RAMSES e, di conseguenza, l'esperienza dell'utente.



For more information visit us on
www.ramses2020.eu



follow us on Twitter
[#RamsesEU](https://twitter.com/RamsesEU)



or contact us via e-mail
info@ramses2020.eu



or in person at
Stefano Zanero
Politecnico di Milano
Dip. Elettronica, Informazione e Bioingegneria
Via Ponzio, 34/5
20133 Milano
ITALY

