RAMSES

NIEUWSBRIEF

Versie 2

Wat is RAMSES ?

RAMSES is een door Horizon 2020 gefinancierd project gecoördineerd door POLIMI. Elf technische, wetenschappelijke en politiepartners uit heel Europa ontwikkelen een intelligent, schaalbaar en modulair platform voor wetshandhavingsinstanties (LEA's) om digitaal forensisch onderzoek te vergemakkelijken. Het systeem extraheert, analyseert, linkt en interpreteert de van het internet geëxtraheerd informatie in verband met financieel gemotiveerde malware.

Forensisch internetplatform voor het volgen van de geldstroom van financieel gemotiveerde malware

Een forensische toolset op het internet!

RAMSES brengt de nieuwste technologieën samen in een softwareplatform dat zeven tools integreert:

- OSINT-service
- Darknet-service
- Ransomware-classificatieservice
- Bitcoin-trackerservice
- Bankieren Trojan analyzer service
- Forensische multimedia-service
- Malware-inlichtingendienst

Sommige tools bevatten meer dan één tool, waarvan de meeste online zijn. Resultaten van de offline tools worden geüpload naar het RAMSES-platform en dus ook geïntegreerd.

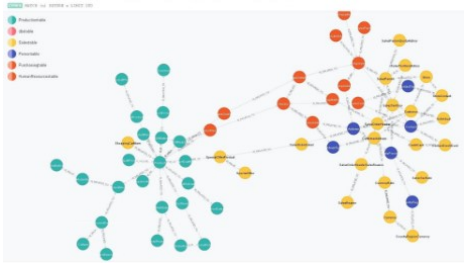
Functionaliteit

Zoeken in grote hoeveelheden data van reeds verwerkte gegevens: IP-adressen, nicknames, technologieën, namen van RAT's (remote access tools) of elk ander trefwoord dat van belang is voor de onderzoeker.

Visualiseert de resultaten van malware-analyse, clustering en forensisch onderzoek.

Onderzoekt de relaties tussen verschillende entiteiten, zoals IP-adressen, gebruikersnamen, namen van malware, domeinen.

Meldingen kunnen door LEA's worden gevonden om belangrijke gebeurtenissen op te merken, zoals de deanonimisatie van een verkoop van verborgen diensten malware.



RAMSES searches, explores, visualizes, and alerts

OSINT tool

De OSINT-service (open source intelligence) integreert gegevens in het RAMSES-platform van bronnen zoals Twitter, Pastebin, HackForums en Reddit. De informatie die door de crawlers wordt verzameld, wordt alleen opgeslagen, verwerkt en geanalyseerd wanneer deze gerelateerd is aan malware.

Darknet tool

De darknet-service is een zoekmachine die er voor zorgt dat de gebruiker namen van specifieke ransomware en trojans of meer algemene verzoeken kan invoeren om zo verborgen services op het darknet terug te vinden. De resultaten van de zoekopdracht toont een lijst van services op TOR welke gerelateerd zijn aan de opgegeven zoekterm(en). De gebruiker kan de lijst filteren op verschillende categorieën, b.v. "Malware gedetecteerd" en "malware niet gedetecteerd".

Bovendien downloadt de Darknet-service website-informatie, neemt de vingerafdruk van de server op en correleert deze om relaties tussen websites te ordenen.

Ransomware classifier service

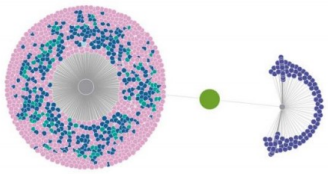
De ransomware classificatie-service omvat twee functies: analyse van een nieuwe screenshot van ransomware en de controle van eerdere uploads en hun resultaten.

Schermafbeeldingen van de geïnfecteerde computer van het slachtoffer kunnen worden geüpload naar het RAMSES-platform om relevante informatie over de ransomware te identificeren, classificeren en extraheren.

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

Bitcoin tracker tool

De bitcoin-trackerservice ontleedt de blockchain, clustert adressen, classificeert en labelt gebruikers en visualiseert uiteindelijk complexe informatie die is geëxtraheerd uit het bitcoin-netwerk.
Elk knooppunt van het bitcoin-netwerk moet de volledige geschiedenis van elke transactie opslaan (zogenaamde blockchain). De bitcoin-trackerservice gebruikt gegevens van de blockchain als invoer en stelt de gebruiker in staat om informatie te zoeken met betrekking tot een specifiek bitcoin-adres.

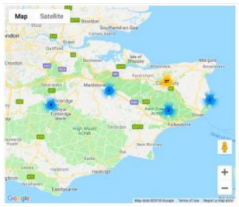


RAMSES Bitcoin tracker results output example

Multimedia forensic tool

De multimedia forensische tool is een toolkit bestaande uit twee instrumenten: het eerste instrument kan gedetailleerde metadata, zoals GPS-locatie of technische kenmerken, uit afbeeldingen en video's extraheren en verwerken. Deze informatie kan worden gebruikt om de bron (bijvoorbeeld digitale camera, mobiele telefoon) van een afbeelding / video te identificeren dit wanneer een set van mogelijke bronnen bestaat. Als er geen verzameling van bronnen is, kan deze tool worden gebruikt om afbeeldingen / video's te groeperen in sets te verzamelen waarin alle bestanden van hetzelfde apparaat afkomstig zijn.

Het tweede instrument analyseert afbeeldingen en video's op byte niveau, bestandsformaat niveau en pixel niveau om wijzigingen te detecteren en vervalsing te identificeren. Resultaten van deze analyses worden geüpload naar het RAMSES platform.



RAMSES geopositioning a set of pictures in Google Maps

Malware intelligence tool

De malware-inlichtingen tool verzamelt en correleert activiteiten van kwaadwillende actoren. De service biedt informatie zoals IP-adressen en malwarefamilies. Het biedt extra informatie over kwaadwillende actoren die zijn verbonden met ransomware en / of bank-Trojaanse campagnes.

De verzamelde informatie is niet beperkt tot deze campagnes, maar vormt een representatieve steekproef van kwaadaardige activiteiten en biedt juridisch relevant bewijs voor het toeschrijven van andere criminele activiteiten aan een kwaadwillende actor.

Banking Trojan analyser tool

De bank-trojan-analyseservice bestaat uit een online en een offline versie: de online versie is geïntegreerd in het RAMSES-platform. Het gebruikt binaire bestanden van bank-Trojaanse paarden als invoer en voert zowel een differentiële analyse als een geheugen forensische analyse uit.

De offline versie neemt een (volledige of gedeeltelijke) geheugendump als invoer, die wordt verkregen van een geïnfecteerde machine. Het voert een geheugen forensische analyse uit. Resultaten van analyses worden geüpload naar de RAMSES platform.

Volgende stappen ...

Het RAMSES-webplatform draait met de (online) tools die in verschillende mate worden geïntegreerd. Er kunnen al betekenisvolle resultaten worden geleverd op het gebied van financiële tracking van Bitcoin in verband met cybercriminaliteit, malwareprofilering, beeld- en video-analyse, scraping van sociale media / forums en economische modellering van ransomware. Momenteel worden pilootprojecten gehouden om de behoeften van LEA's als eindgebruikers van het product te beoordelen. Resultaten worden gebruikt om de software van RAMSES en de gebruikerservaring te verbeteren.

Voor meer informatie bezoek ons op
www.ramses2020.eu

Volgs ons op Twitter
#RamsesEU

Of neem contact op via e-mail
info@ramses2020.eu

Of in persoon
Stefano Zanero
Politecnico di Milano
Dip. Elettronica, Informazione e Bioingegneria
Via Ponzio, 34/5
20133 Milano

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