RAMSES

NEWSLETTER

Ausgabe 2 | Mai 2019

Was ist RAMSES?

RAMSES ist ein von H2020 finanziertes Projekt und wird von POLIMI koordiniert. Elf Partner aus ganz Europa aus Technik, Wissenschaft und der Polizei entwickeln eine ganzheitliche, intelligente, skalierbare und modulare Plattform für Strafverfolgungsbehörden, um digitale forensische Ermittlungen zu erleichtern. Das System extrahiert, analysiert, verknüpft und interpretiert Informationen aus dem Internet, die mit finanziell motivierter Malware in Verbindung stehen.

Forensische Internetplattform zur Verfolgung des Geldflusses von finanziell motivierter Malware

Forensische online Tools!

RAMSES vereint die neuesten Technologien in einer Softwareplattform, die sieben Dienste integriert:

- OSINT-Service
- Darknet-Service
- Ransomware Classifier Service
- Bitcoin Tracker Service
- Banking Trojan Analyser Service
- Multimedia Forensic Service
- Malware Intelligence Service

Einige Dienste umfassen mehr als ein Tool, die meisten davon sind online. Auch die Ergebnisse der Offline-Tools werden auf die RAMSES-Plattform hochgeladen und damit ebenfalls integriert.

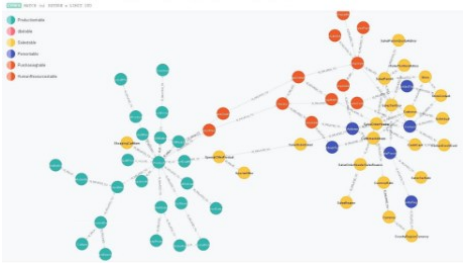
Funktionalitäten

Suche in großen, bereits verarbeiteten Datenmengen: IP-Adressen, Spitznamen, Technologien, Namen von RATs sowie jedes andere Schlüsselwort von Interesse.

Visualisierung der Ergebnisse von Malware-Analyse, -Clusterbildung und -Forensik.

Untersuchung der Beziehungen zwischen verschiedenen Einheiten, wie z.B. IP-Adressen, Benutzernamen, Namen von Malware und Domänen.

Warnmeldungen können für wichtige Ereignisse definiert werden, wie z.B. die De-Anonymisierung eines versteckten Dienstes, der Malware verkauft.



RAMSES sucht, visualisiert, untersucht und warnt

OSINT-Service

Der *OSINT* (Open Source Intelligence)-*Service* integriert Daten aus Quellen wie Twitter, Pastebin, HackForums und Reddit in die RAMSES-Plattform. Die von Crawlern gesammelten Informationen werden nur, wenn sie im Zusammenhang mit Malware stehen, gespeichert, verarbeitet und analysiert.

Darknet-Service

Der *Darknet-Service* ist eine Suchmaschine, die es dem Nutzer ermöglicht, die Namen bestimmter Ransomware und Trojaner nachzuschlagen oder allgemeinere Anfragen zu stellen und versteckte Dienste im Darknet zu finden. Die Ergebnisse der Suche zeigen eine Liste der Dienste auf Tor, die sich auf das/die Schlüsselwort(e) beziehen. Der Nutzer kann die Liste nach verschiedenen Kategorien filtern, z.B. "Malware erkannt" und "Malware nicht erkannt".

Darüber hinaus lädt der Darknet-Service Webseiteninformationen herunter, erstellt Fingerabdrücke auf dem Server und korreliert diese, um Beziehungen zwischen Webseiten zu finden.

Ransomware Classifier Service

Der Ransomware Classifier Service umfasst zwei Funktionen: die Analyse eines neuen Screenshots einer Ransomware und die Überprüfung früherer Uploads sowie deren Ergebnisse.

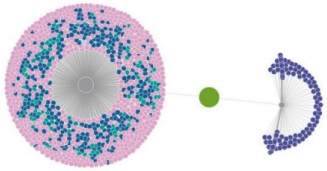
Screenshots des infizierten Computers können auf die RAMSES-Plattform hochgeladen werden, um relevante Informationen über die Ransomware zu identifizieren, zu klassifizieren und zu extrahieren.

Dieses Projekt wurde im Rahmen der Finanzhilfevereinbarung Nr. 700326 aus dem Forschungs- und Innovationsprogramm der Europäischen Union Horizont 2020 finanziert.

Bitcoin Tracker Service

Der *Bitcoin Tracker Service* analysiert die Blockchain, bündelt Adressen, klassifiziert und kennzeichnet Nutzer und visualisiert schließlich komplexe Informationen aus dem Bitcoin-Netzwerk.

Jeder Knoten des Bitcoin-Netzwerks muss die gesamte Historie jeder Transaktion speichern (sogenannte Blockchain). Der Bitcoin Tracker Service verwendet Daten aus der Blockchain und ermöglicht es dem Nutzer, nach Informationen im Zusammenhang mit einer bestimmten Bitcoin-Adresse zu suchen.



Ergebnisbeispiel des RAMSES Bitcoin Tracker

Multimedia Forensic Service

Der *Multimedia Forensic Service* ist ein Toolkit, das aus zwei Instrumenten besteht: Das erste Instrument ist in der Lage, detaillierte Metadaten wie GPS-Daten oder technische Merkmale aus Bildern und Videos zu extrahieren und zu verarbeiten. Diese Informationen können verwendet werden, um die Quelle (z.B. Digitalkamera, Mobiltelefon) eines Bildes/Videos zu identifizieren, wenn eine Reihe von möglichen Quellen vorhanden ist. Falls es keine Auswahl an Quellen gibt, kann er verwendet werden, um Bilder/Videos zu gruppieren, in denen alle Dateien vom gleichen Gerät stammen.

Das zweite Instrument analysiert Bilder und Videos auf Byte-, Dateiformat- und Pixelebene, um Veränderungen zu erkennen und auf Fälschungen zu schließen. Die Analyseergebnisse werden auf die RAMSES-Plattform hochgeladen.

RAMSES Geopositionierung einer Bilderserie in Google Maps

Malware Intelligence service

Der Malware Intelligence Service sammelt und korreliert die Aktivitäten bösartiger Akteure. Der Dienst bietet Informationen wie IP-Adressen und Malware-Familie. Er bietet zusätzlich Informationen über böswillige Akteure im Zusammenhang mit Ransomware- und/oder Trojaner-Angriffe auf Banken. Die gesammelten Informationen sind nicht auf diese Angriffe beschränkt, sondern stellen eine repräsentative Stichprobe schädlicher Aktivitäten dar und liefern rechtlich relevante Beweise für die Zuordnung anderer krimineller Aktivitäten zu einem bestimmten Akteur.

Banking Trojan Analyser Service

Der *Banking Trojan Analyser Service* besteht aus einer Online- und einer Offline-Version: Die Online-Version ist in die RAMSES-Plattform integriert. Sie verwendet Binärdateien von Bank-Trojanern und führt sowohl eine Differentialanalyse als auch eine forensische Speicheranalyse durch.

Die Offline-Version nutzt den (vollständigen oder teilweisen) Speicherauszug, der von einem infizierten Computer bezogen wird. Sie führt eine forensische Speicheranalyse durch. Die Analyseergebnisse werden auf die RAMSES-Platform hochgeladen.

Nächste Schritte…

Die (Online-)Tools sind aktuell unterschiedlich stark in die RAMSES-Plattform integriert. Aussagekräftige Ergebnisse lassen sich bereits in den Bereichen Financial Tracking von Bitcoin im Zusammenhang mit Cyberkriminalität, Malware Profiling, Bild- und Videoanalyse, Social Media / Forum Scraping und ökonomische Modellierung von Ransomware liefern. Derzeit werden Pilotprojekte durchgeführt, um die Bedürfnisse der LEAs als Endnutzer zu ermitteln. Die Ergebnisse werden verwendet, um die Software von RAMSES und die Benutzerfreundlichkeit zu verbessern.

www.ramses2020.eu

#RamsesEU

info@ramses2020.eu

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

Dieses Projekt wurde im Rahmen der Finanzhilfevereinbarung Nr. 700326 aus dem Forschungs- und Innovationsprogramm der Europäischen Union Horizont 2020 finanziert.