RAMSES

PIATTAFORMA PER L'ANALISI FORENSE DI DISPOSITIVI CON ACCESSO A INTERNET PER IL TRACCIAMENTO DEI FLUSSI DI DENARO CAUSATI DA SOFTWARE MALEVOLO

Contesto

Internet gioca un ruolo fondamentale in ogni attività economica ed imprenditoriale. Di conseguenza, il crimine si è adattato alle nuove tecnologie. Molte delle attività criminali "tradizionali" come furti e truffe hanno trovato nell'Internet un nuovo ed efficiente mezzo per essere messe in atto e diffondersi. Ad esempio, la rete Internet permette ai criminali di nascondere le loro identità e di acquistare facilmente programmi per rubare informazioni sensibili a basso costo.

Obiettivi

L'obiettivo principale di RAMSES è progettare e sviluppare una piattaforma olistica, intelligente, scalabile e modulare di supporto alle forze dell'ordine, al fine di facilitare le investigazioni forensi. La piattaforma in questione sarà in grado di estrarre, analizzare, correlare ed interpretare le informazioni estratte da software malevoli ("malware") sviluppati per avere un ritorno economico.

Lo studio prende in considerazione acquirenti, sviluppatori e vittime di tali malware per raggiungere una migliore comprensione di come e dove il malware si diffonda e per identificare la fonte della minaccia. Per raggiungere questi obiettivi ambiziosi, questo progetto si baserà su tecnologie Big Data, in primo luogo per estrarre e memorizzare enormi quantità di dati strutturati e non, ed in secondo luogo per cercare modelli di comportamenti fraudolenti.

Attività

Ci concentreremo su 2 casi di studio: ransomware e banking trojan. Al fine di raggiungere questo obiettivo, RAMSES riunisce le più recenti tecnologie per sviluppare una piattaforma software intelligente in grado di monitorare il web (pubblico e deep web), rilevare la manipolazione ed effettuare la steganalisi di immagini e video, tracciare i pagamenti legati ai malware, estrarre ed analizzare campioni di malware ed infine **analizzare** e **visualizzare Big Data**.

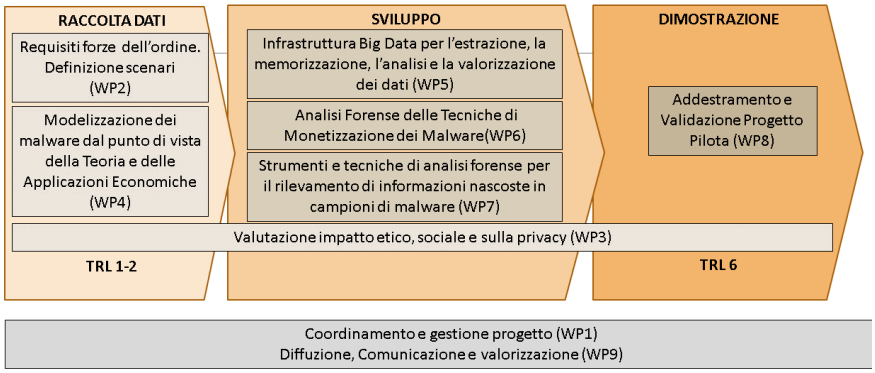
Programma di Finanziamento:
Questo progetto ha ricevuto fondi dal programma di innovazione e ricerca "Horizon 2020" dell'Unione Europea sottostante la convezione di sovvenzione N° 700326.

Durata del Progetto:
01/09/2016 – 31/08/2019

Budget del Progetto:
3.8 milioni euro

Sito Web del Progetto:
www.ramses2020.eu

I progetti pilota per la validazione avranno luogo in tre diversi Paesi dell'UE (Portogallo, Belgio e Spagna). In particolare, verrà effettuato un primo pilota da ciascuna delle forze dell'ordine e un secondo pilota di indagine collaborativo tra le stesse. Il potenziale commerciale sarà convalidato durante il progetto e sarà supportato da uno studio di fattibilità per valutare l'adozione della piattaforma e da modelli di business accurati.



Impatto:

L'impatto di RAMSES può essere analizzato da due prospettive:

Esterna: Il progetto si focalizza sul raggiungere risultati tangibili al fine di migliorare gli strumenti dell'analisi forense applicata a dispositivi con accesso a Internet in Europa. Inoltre, RAMSES intende utilizzare software open-source e libero. La piattaforma sviluppata sarà liberamente accessibile e fruibile da tutte le forze dell'ordine europee che si iscriveranno a RAMSES.

Interna: L'impatto di RAMSES è particolarmente rilevante alla luce delle capacità di ricerca e innovazione del consorzio. Ai partner tecnici, RAMSES consente loro di sfruttare e migliorare le soluzioni tecnologiche esistenti, mettendola in pratica per un problema molto specifico. Alle forze dell'ordine, RAMSES permette lo sfruttamento delle conoscenze esistenti migliorando il ciclo di indagini, la raccolta dei dati per professionisti e creando nuovi canali di comunicazione con i cittadini.

Coordinatore del Progetto:
TREELOGIC

Tatiana Silva,
Tatiana.Silva@treelogic.com

Partecipanti al Progetto:

treelogic
Policía
University of Kent Computing
Trilateral Research
Universidad Complutense Madrid
Politecnico Milano 1863
RISSC
Hochschule für den öffentlichen Dienst in Bayern Fachbereich Polizei
Politie
Universität des Saarlandes