Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Threat Intelligence and Attack Detection

Author(s): Olga E. Segou (NCSRD), Isidoros Monogioudis (HMOD)

CC RG-1 and CT RG-1 - Threat and attack intelligence, attack simulation infrastructures
CC RG 2 - Automatic malware research, advanced automatic malware defence and shielding
CC RG-5 - Research on information propagation in non-centralized media (available research is available on state-controlled media)
CT RG-13 - Develop realistic threat model for wearable devices
CC RG-18 - Innovative process-aware behavioural-based intrusion detection system capable of identifying any deviation from normal activities for the processes being monitored
CT RG-32 – How to engage operators/exchangers in information exchange
CC RG-32, CC RG-54, CT RG-54 - Early detection of supply chain attacks
CC RG-38, CT RG-38 and CT RG-50 - Gathering knowledge about attack statistics per critical component
CC RG-39, CT RG-39 and CT RG-10 - Infrastructures for attack simulations
CC RG-84 - Technologies to monitor and control the production process and detect deviations from acceptable behaviour
CC RG-89 - Advanced anti-phishing solutions
CC RG-96 - Research on advanced malware detection and prevention techniques on mobile devices
CC RG-99 - Intelligent IDS, hardening mechanisms and awareness
CC RG-105 - Advanced techniques for DDOS detection

ABSTRACT

The increasing use of ICT in more areas of human activity has created new possible threats and attack modalities compromising a variety of different targets. New technologies such as IoT, Wearables etc. are not hardened against cyber-attacks. Critical Industrial Systems are targets of new malware. DDOS and phishing attacks have become more common than ever, while new threats and new types of malware (such as ransomware, mining malware etc.) prove difficult to combat. It is, therefore, an imperative need to further improve threat intelligence and gain a better understanding of how threats develop and what makes them persist. Therefore, actions are expected to lead to improved threat intelligence and threat modelling, solutions to simulate attacks, design of component- and system-level penetration testing, intrusion and attack detection and overall improved protection of a variety of targets, be it desktop/mobile devices, wearables, individuals, IoT etc.

Threat and Attack intelligence improvement, by developing attack simulation infrastructures and advanced risk analysis and modelling.

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **2 STREPs + 1 IPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, CERTs/CSIRTs**

The evolution of cyber-attacks and the continuous development of more sophisticated tactics, techniques and procedures usually overcomes most traditional security measures. Therefore, in order to better understand where are the weakest points that are being exploited and to test current or future protection solutions, we need to develop attack simulation structures. This will help to create the more specific conditions where an attack can take place and design or adjust security measures focused on specific needs and requirements.

Realistic attack simulation will contribute to the advanced threat modelling that will result in a more efficient dynamic risk analysis of current and near future attacks. It will also feed with valuable information the intelligence lifecycle that will produce more reliable and accurate threat intelligence.

The great value of an attack simulation infrastructure will improve the knowledge of attack context improving significantly the quality of threat intelligence and detection operations. It is also expected to lead to the design of solutions for component- and system-level penetration testing.

RESEARCH ACTION #2

Intelligent intrusion and malware detection, system hardening and situation awareness across a complex environment.

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **2 STREPs + 2 IPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **52 months**
ACTORS: **government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, CERTs/CSIRTs**

Attack detection currently relies mainly on known attack patterns and techniques. There is also a behavioural analysis and reputation model but with not sufficient results especially in avoiding false positives.

Although it is commonly accepted that protective measures have limited efficiency and more effort should be put in reactive – response measures, proactive defence still remains the first layer of security and needs continuous update and improvement.

The main objective of preventive security operations remains the block of intrusion attempts. This combined with advanced hardening and situation awareness can deliver better results in preventing cyber-attacks before being executed at the targeted environment.

Current intrusion and malware detection technologies need to be further improved by integrating advanced intelligence mechanisms, big data analytical procedures, prediction techniques in order to address threats and on-going attacks in a timely and efficient way.

The biggest challenge in the future will be to handle and manage a complex cyber environment with many different devices and technologies that keep growing (e.g. IoT, wearable devices, social media offering data as a commodity etc.)

RESEARCH ACTION #3

Protection of organisations from critical data leaks caused by intentional or unintentional insider threats

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **1-2 STREPs + 2 IPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **56 months**
ACTORS: **government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, social media companies**

Leaks of sensitive or even classified material is a major and growing concern among a variety of different organisations. An employee might commonly disclose important information unintentionally due to misuse of social media, lost or stolen personal devices containing sensitive material, falling victim to cyber-attacks such as phishing, click-jacking or other social engineering attacks etc. In other cases, a person might willingly disclose information for malicious purposes, sometimes even after termination due to poor administration of personal accounts.

In order to minimise the risk of critical data leaks, organisations require cost-effective and socially acceptable solutions for:

- Employee pre-screening processes that are compliant with EU legislation on privacy and non-discrimination,
- Proper device management,
- Social Media management,
- Employee training and tools to protect against phishing, click-jacking and social engineering attacks,
- Accountability processes that can uncover erratic behaviours indicating a possible insider threat,
- Proper employee termination processes that minimise the risk of leaked data.

Social acceptance of such solutions is also a major factor that could hinder their adoption. Proposed solutions should take into account the EU legislation on privacy and non-discrimination and be respectful to the employees' dignity and human rights. Furthermore, solutions should be as less intrusive and disrupting to everyday workflow as possible.

RESEARCH ACTION #4

Understanding the economic impact of digital currencies and their role in enabling new forms of cyber and organised crime

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **2 STREP + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **law enforcement, research/academia, ICT industry, government**

Digital currencies have recently arisen as Internet-based services that enable on-the-spot, cross-border, irreversible exchange of money or ownership, illustrating similar properties as physical/national currencies. In the past few years, hundreds of digital currencies have been created, following either more stable/centralised or volatile/decentralised architectures.

The rapid and irreversible use of such currencies along with improved anonymity and have created a new market sector and have enabled new business models to flourish. Law enforcement, however, has also recognised that they enable criminal activity ranging from money laundering and tax evasion to illegal immigration and trafficking. Furthermore, new forms of cybercrime have appeared such as:

- New forms of malware: Digital currency processes are often computationally intensive. Digital currency users might voluntarily offer use of their own systems' processing power in exchange for compensation, a process known as mining. This has lead cybercriminals to mining malware that installs on desktop or mobile devices and utilises their processing power to generate illicit revenue.
- Currency Mixing: Mixing is the process of obfuscating the source of a transaction by mixing different currencies and funds, usually for a transaction fee.
- "Crime-as-a-Service": Europol warns that digital currencies enable cybercriminals to come together in an ad-hoc, per-project basis thus forming a new "Crime-as-a-Service" business model.

Law enforcement thus faces novel challenges related to digital currencies. In order to combat new forms of cyber and organised crime fostered by decentralised digital currencies, there needs to be:

- an in-depth understanding and econometric analysis of business models arising from digital currencies,
- an analysis of possible gaps in EU legislation that enable unregulated use of digital currencies,
- an analysis of the profiles and behavioural patterns of legitimate and illicit digital currency users,
- Further analysis of the technical aspects should lead to the creation of tools to improve tracing of illicit transactions,
- Mitigation of new malware threats such as mining malware.