Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Anti-malware Research

Author(s): Evangelos Markatos (FORTH), Lorenzo Cavallaro (RUHL)

CT RG–55/34 and CC RG-2/8/35 Research in malware analysis field, advanced malware defence and shielding
CT RG–9 and CC RG-11 Design of advance malware detection, analysis and prevention tools and techniques for lifelogging
CT RG–94 and CC-RG-100 Advanced malware analysis tools and techniques and mitigation of infection techniques
CT RG–101 and CC-RG-105 Research on advanced malware detection and prevention techniques on mobile devices

ABSTRACT

Malicious Software (malware) has always been a vehicle of choice for cybercriminals and cyberterrorists to deliver their attacks. What was once started as an activity for fun has now consolidated into a well-established business model mostly driven by profit and political motifs. Malware is nowadays responsible for most of the malicious activities on the Internet (e.g., sensitive and financial information theft, DDoS, spam, click fraud), playing a fundamental role in more complex attacks. Despite the non-negligible research effort invested by the academic and industry community, statistics and trends provide a clear evidence that malicious software still represents one of the most pressing Internet threats undermining the security, privacy and safety of Internet users - an increasingly worrying concern that nowadays is not only confined to traditional computing devices, but that also spreads to mobile, critical infrastructure and Internet of Things at a very fast pace. Dealing with malware will be the challenge for the next decade.

RESEARCH ACTION #1

Research in malware analysis field, advanced malware defence and shielding

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **5-10 Research and Innovation Actions, 1 CSA**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **5 years**
ACTORS: **security industry, SMEs, Universities, Research Centres**

The analysis, classification and detection of malicious software has been the focus of a number of research efforts, in recent years. The problem space is large and requires a holistic approach geared towards building on sound techniques (e.g., machine learning, program analysis, software verification) that can be shown to work in real operational settings. To further exacerbate the problem, novel techniques must address the problem posed by evasive malware, engineered to hinder automatic analysis attempts represent; there is the need to develop techniques to automatically reason about behaviours or syntactic artefacts aimed at bypassing protections.

A holistic approach would require to research along the following dimensions:

- **Detection**. Find if the system is infected with malware. Develop novel mechanisms (beyond signature matching) that will evaluate the overall behaviour of the system and detect when malware is suspected to be present. Detection can be both passive and active in an effort to force the malware to reveal itself.

- **Prevention**. Prevent malware from entering the system in the first place. Take a whole-system-image approach to exploit information coming from several different sources over a long period of time.

- **Tolerance**. Operate in the presence of malware. Design systems that can function correctly (to a large extent) even when they are infected with malware that cannot be eradicated.

RESEARCH ACTION #2

Advanced malware detection and prevention techniques on mobile devices

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **5-10 Research and Innovation Actions, 1 CSA**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **5 years**
ACTORS: **security industry, SMEs, NGOs, Universities, Research Centres**

Over the past few years we have seen a rapid increase in the use and deployment of mobile devices. People are using their smartphones and tablets much more than they use their traditional computers; young people have also started to re-discover wristwatches in the face of devices that can do much more than tell the time: measure steps, measure heart rate, and comment on health status. In this exciting new world, smart mobile devices will be an attractive target for cybercrime and cyberterrorism. Remote possession and control of these devices, through malware, will provide a wealth of opportunities for an attacker: know the whereabouts of the target, know his/her vulnerable spots, provide them with faulty information, steal their data, steal their money, extort them, place bogus information in the device, interfere with all physical world structures it controls (smart cars, smart homes, etc.).

In this new environment we need a whole new approach to deal with malware:

- **Measuring and Monitoring**. Although traditional computers have extensive measuring, monitoring and logging facilities, smart devices have little, if any at all. We need research in order to develop mechanisms that will let us measure and monitor the behaviour of smart and embedded devices. Without being able to fully monitor a device, malware will always be able to slip between the cracks and hide.
- **Control**. Provide users with the ability to control their devices and their data. Provide more transparency in all actions and shed light into who is accessing what. Provide users with the ability to grant access to data and resources as well as the ability to revoke this access on-demand. Change the access model from a server-centric to a user-centric one.
- **Change the model**. Conduct research in alternative models of detection. Detect malicious behaviour even if no malicious executable (i.e. malware) can be detected. Develop novel ways to handle and tolerate malicious behaviour which may come from any type of interaction.