Automated Malware Analysis Techniques

Alejandro Calleja

October 24, 2016

CoSec Group, CS Department, Universidad Carlos III de Madrid

Outline

Introduction

Malicious Software

- One of the most challenging cyberthreats nowadays
- MW development has become a full-grown underground industry
- Poses a hot research topic in the systems security area

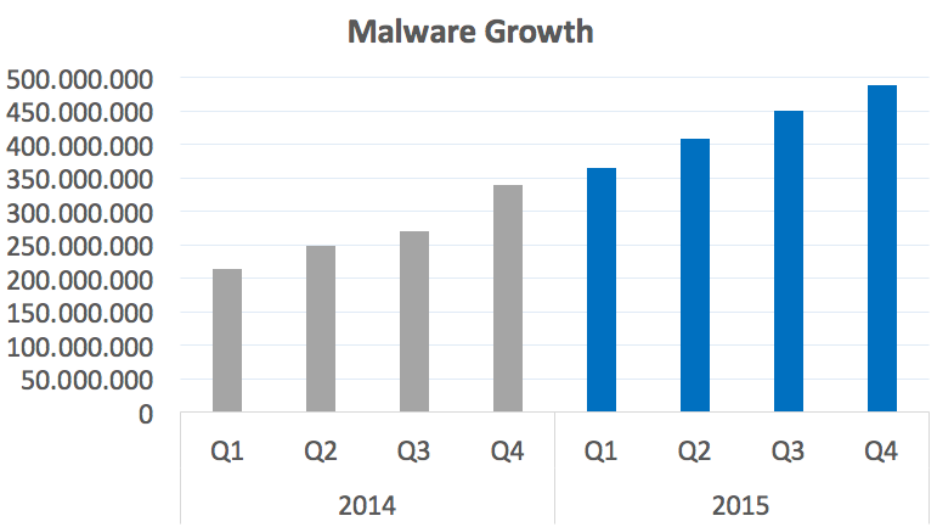
The Two Sides of Malware Fighting

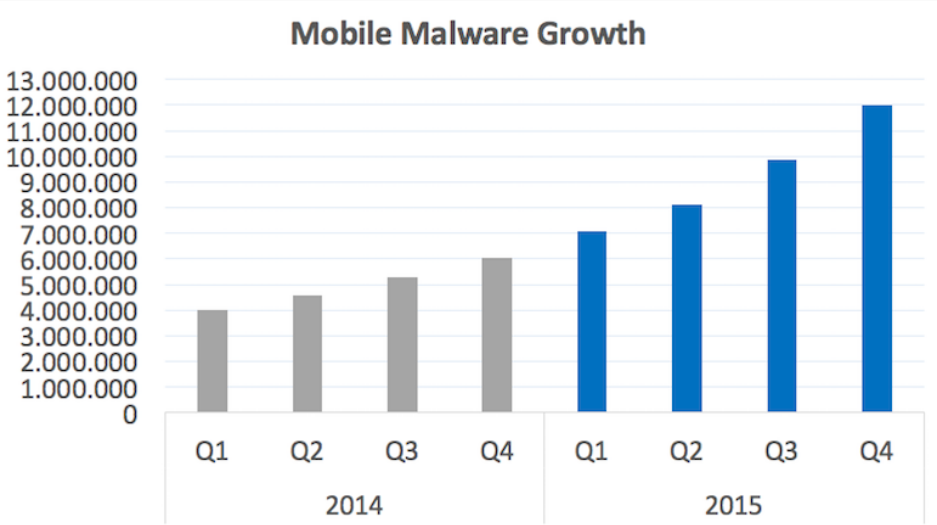
- **Malware Detection**:
  - Trial: *is this program malicious or harmless?*
  - Aided by dynamic/static analysis and pattern/signature matching
- **Malware Classification:**
  - *Is this sample new? Does this sample behave like others?*
  - Aided by static/dynamic analysis and machine learning
  - Supports the development of proper countermeasures

Motivation

Malware in Numbers

- Traditional malware growing rates are rocketing
- Same trend is also visible on mobile platforms
- *"27% of all recorded malware appeared in 2015"* - Panda Labs





Source: McAfee Labs Threat Report (May 2016)

Malware as a Sophisticated Threat

Analysis of modern malware is not an easy task

- Use to include polymorphic and metamorphic engines
- Comes equipped with non-trivial obfuscation artifacts (i.e: encrypted or packed payloads)
- Defeats dynamic analysis by detecting sandboxed execution

New paradigms, new threats

- IoT devices such IMDs or wearables are the next stop for malware writers
- Mobile platforms (Android,iOS,...) have attracted the attention of MW authors
- *What about deploying traditional countermeasures?*

Research Objectives

Research Objectives I

To understand the current situation and evolution of malicious software

- Studying its evolution in terms of size and complexity
- Understanding how to deal with modern malware targeting novel platforms
- Predicting new threats coming from the malware area

Research Objectives II

To develop novel and effective methods for characterizing and classifying malware

- Proposing new classification systems based on meaningful features (e.g: information-flows)
- Designing new methods to triage the manual analysis of massive sets of malware samples
- Rethinking the concept of "*Malware Family*" on top of experimental evidences

Published Works

Published Works

Malware Characterization and Classification

- Alejandro Calleja, Juan Tapiador, and Juan Caballero. A look into 30 years of malware development from a software metrics perspective.
  In *International Symposium on Research in Attacks, Intrusions, and Defenses 2016*, 2016
- Alejandro Martinez, Alejandro Calleja, Hector D. Menendez, Juan Tapiador, and David Camacho. ADROIT : Android malware detection using meta-information (to appear).
  In *2016 IEEE Symposium on Computational Intelligence*, 2016

Malware and other threats in IoT devices

- Alejandro Calleja, Pedro Peris-Lopez, and Juan E Tapiador. Electrical heart signals can be monitored from the moon: Security implications for ipi-based protocols.
  In *IFIP International Conference on Information Security Theory and Practice*, 2015
- Sergio Pastrana, Jorge Rodriguez-Canseco, and Alejandro Calleja. Arduworm: A functional malware targeting arduino devices.
  In *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016), Granada, Spain*, 2016

Conclusions

Conclusions

Malicious software pose an important challenge:

- High creation rates and increasing complexity
- Traditional approaches for classification and detection are outdated

Gives place to many emerging threats:

- Malware in many different architectures and platforms
- Aggressive and destructive multi-device malware types: Ransomware, Botnets, ...

Many problems are yet to be addressed:

- Understand the current scenario and predict the future evolution
- Develop effective methods for malware analysis and classification

The End

Thanks!

Q&A