Analysing Android Malware and Testing Detection Tools

Jack Gates

BSc (Hons) Ethical Hacking

Introduction

Due to the popularity of Android smartphones, and with Android applications being a good vector for distributing malware, it has been strongly targeted by malware authors. Millions of new malicious applications are made a year.

Several articles such as (Zhou and Jiang, 2012) highlight that this malware is constantly evolving to be more sophisticated. These evolutions include improvements in their features, as well as incorporating techniques to evade analysis and detection.

The same paper also demonstrates anti-virus tools as being weak, showing that the best and worst tested tools had a detection rate of 79.6% and a 20.2% respectively. The paper suggests that many tools performed poorly because they rely on outdated methods, such as signature-based detection too strongly, as well as increasing sophistication in malware.

A lot of research since the previous paper has led to the development of new state-of-the-art detection systems that use different methods than commercial anti-virus. scanners.

Aim and Objectives

Aims:

- Gain insight into the current Android malware landscape
- Recommend improvements for detection systems

Objectives:

- Analyse recent Malware families
- Test the anti-virus scanners effectiveness
- Look for strengths and weaknesses in state-of-the-art detection systems

Method

Research: This stage performs research into different areas surrounding Android malware, necessary for understanding the following stages. Academic papers were looked at and notes were taken. The following areas touched on are:

- Malicious behaviours
- Analysis techniques and tools
- Techniques to evade analysis/detection

Analysis: This stage involved an in-depth analysis of 3 different malware families.

- Analysis tools to extract features.
- Reverse engineering tools to construct behaviour.
- A document is created for each family.

Detection: the detection stage consists of two parts:

1: Test effectiveness of anti-virus scanners

- Each malware sample is run against VirusTotal several times each.
- Un-obfuscated malware will be obfuscated then tested again.
- Each result is presented in an excel sheet.

2: Understand the strengths and weaknesses in detection systems.

- Academic proposals of different state-of-the-art detection systems will be researched.
- A document will be created evaluating each system.

Results

Analysis: The 3 following malware families belonging to the respective type were fully analysed, and a document was created for each, detailing their features and malicious behaviours.

- A Trojan-Spy named: Triout
- A Trojan-Dropper named: VikingHorde
- A Banking-Trojan named: MysteryBot

Testing Detection: Average of the top 20 and top 40 scanners could detect 97.7% and 79.1% of malware respectively.

Trends were found in detection. The discovery date had a significant impact on the detectability of each malware shown in Figure 1.

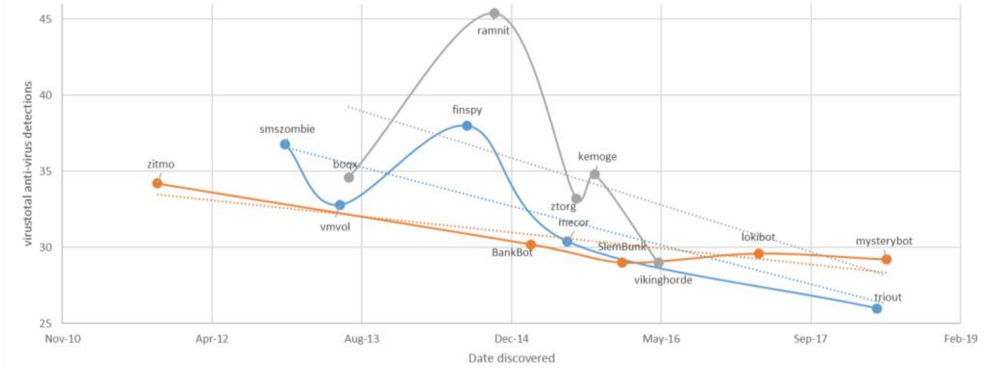

Figure 1 – detection date

Figure 2 show certain obfuscation techniques also effected the detectability of malware.

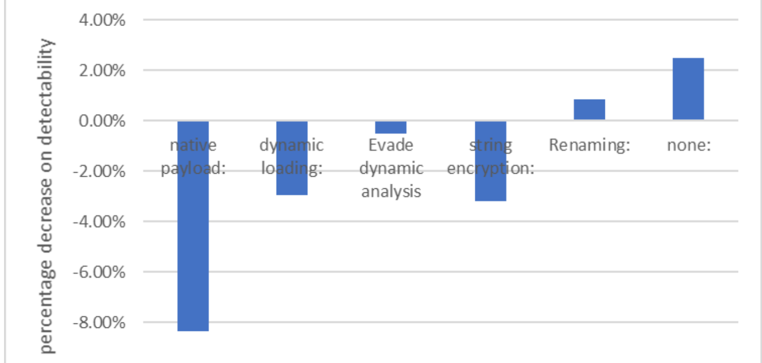

Figure 2 – obfuscation techniques

Further testing showed that obfuscating the previously un-obfuscated malware had a significant effect on its detectability.

Detection systems: 11 different detection systems were researched, showing a variety of different methods, features, and models used. They were all fully described in the detection paper.

Discussion

Malware Analysis:

- Good insight into the current capabilities of each type.
- Certain features/techniques were found to be better than others.
- Evolutions in features and evasion techniques found.

Testing Detection:

- Some anti-virus scanners were found to be weak.
- Newer detection date decreases detectability, most likely to do with many scanners using outdated methods.
- Certain evasion techniques made detection more difficult, some suggestions were made to overcome these

Detection Frameworks:

- Certain trends were found
- Areas of weakness were highlighted

Conclusion

- 3 malware families were fully analyzed.
- Some anti-virus tools have weaknesses.
- Detection systems using new methods are effective at accurately classifying malware.
- Improvements and areas of future research were highlighted.

References

Zhou, Y. and Jiang, X. (2012). Dissecting Android Malware: Characterization and Evolution. [ebook] San Francisco: North Carolina State University. Available at: http://www.ieee-security.org/TC/SP2012/papers/4681a095.pdf [Accessed 16 Sep. 2018].