Abstract

Computer viruses are big threat to computer world, researchers doing work in this area have made various efforts in the direction of classification and detection methods of these viruses. Graph mining and system call arrangement are some latest research activities in this field. The computability theory and the semi computable functions are quite important in our context of analyzing malicious activity. A mathematical model like random access stored program machine with the association of attached background is used by Ferenc Leitold while explaining modeling of viruses in his paper. Computer viruses like polymorphic viruses and metamorphic viruses use more efficient techniques for their evolution so it is required to use strong models to understand their evolution and then apply detection followed by the process of removal. Code Emulation is one the strongest way to analyze computer viruses but the anti-emulation activities made by virus designers are working against it. This paper explains the static analysis of malicious codes that is used for detection of computer viruses in better manner.

Keywords: Assembly Language, Malicious Codes

I. Introduction

There are various processes that have been used in the direction of classification of computer viruses from normal files that will finally lead to their detection. Machine learning techniques are widely used in this direction. As statistics says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can be used for their detection. Malicious code designers use lot of techniques that are difficult to analyse and detect. The static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so now a days main focus is going towards the methods that are dynamic and are able to detect zero day worms but the role of static analysers can not be ignored due to their distinct properties.

The rise in the malicious threats like computer viruses are required to be handled and observed strongly to make defence against these threats. Other types of malwares are:

1. Viruses
2. Trojan horse
3. Botnets
4. Adware
5. Spyware

The mutating behaviour of metamorphic viruses is due to their adoption of code obfuscation techniques.

Figure 1 Malicious threat rise

Figure 2 Assembly file of virus
a) Dead code insertion
b) Variable Renaming
c) Break and join transformation
d) Expression reshaping
e) Statement reordering

II. Code Analysis

There are various problems that are to be identified like buffer overrun for complete detection of computer viruses. To handle these issues analysis of code is required. It includes various types of techniques.

1. Static techniques
2. Dynamic techniques
3. Hybrid techniques

Lot of work has been done in this direction. Bodik et al., explained in paper “Eliminating array bounds check on demand” about these type of techniques. Chinnek, Chvatal and other gave their views in the same direction.

Moser et al. explained the limitations of static analysis techniques, authors developed binary program obfuscation techniques that make binary more complex in terms of static analysis. They also developed rewriting tool and make experimental analysis on worms to show that it is not easy to detect code obfuscation in malicious files using static techniques, these techniques must be used with dynamic methods so that strong identification can be done.
III. Conclusion

This paper discusses about basic outline of computer viruses with their detection with static analysis. The tools and methods discussed have been developed for their analysis. In last the limitation of static analysis is discussed. This study will be helpful for researchers working in the field of computer virology.

IV. References


