Software tool designed to detect characteristics of the malware objects

Roman Bazylevych[1], Volodymyr Andriyenko[1], Mikael Karioti[2]

[1]Software Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: delared@i.ua

[2]Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: mikaelkarioti@gmail.com.

Abstract ***- Computer virus is the kind of phenomenon that emerged in the operation of the evolution of computers and information technology. Its essence lies in the fact that programs - viruses, endowed with a such of properties that are present in living organisms - they born, reproduce and die.*** *In order t**o ensure information security, both, individuals and entire organizations, it is necessary to raise awareness about potential threats from malicious software such as computer viruses. Simulation of operation of malicious software allows user to understand a virus and choose the possible methods of fighting it. In this research, major features of the algorithms against the security threats from malicious software are simulated.***

Key words – scenario imitation, malware, information security, virus, antivirus,imitation.

I. Introduction

The main threat to ensuring the confidentiality, integrity and approachability of information within its circulation, processing and storage in automated processing systems and storage (electronic computers), is interference with the work of their software by malware[1].

This research aimed, primarily, to create a software that would be able to mimic the action of the complex script of antivirus means in case of credible threat to the system.

Currently, the software market offers a wide range of antivirus programs. To use properly antivirus tools it is necessary to distinguish their functioning according to intended.

Since there is virtually no analogues attempt to construct a simulation model of the characteristics of malware detection, this work is very interesting and unique. Due to the development of anti-virus systems and continuous development of new methods of protection, the project is promising curriculum which, while expanding its functionality, methods of adding protection and improvement of the simulation model is able to perform interesting method to explore new technologies and methods of protection from malware detection characteristics objects.

Over the relatively short history of computer viruses antivirus industry has developed very effective measures to combat "computer now." Over time, some of them are outdated and gradually derived antivirus companies with existing arsenal, the change that came a new, and more modern and efficient technologies[2]. This generational change very typical antivirus software that is determined by the constant confrontation of virus-antivirus. The latter generates a continuous arms race: the emergence of a new virus that uses previously unknown gap in the protection of the operating system or application immediately entails adequate steps to neutralize the threat posed by anti-virus programs.

Most of the popular antivirus programs include such algorithms of immediate protecting against attempts to disrupt a stable work of operating system as disk scanning, auditor checksum software, monitor of the RAM, and heuristic scanning [3]. Mentioned above methods are selected to create a simulation model.

II. Description of the algorithm operation

Projected software tool have to simulate a work of an environment in which CPU, RAM memory, file system and the availability of access to the Internet are selected as a system resources. The model predicts an implementation of a so-called simulation script in the program. According to the simulation script the next chain of events are performed: after choosing of system resources, in the environment must be "installed" harmful objects (those that are chosen for analysis). For simplification of the typical user work, were chosen ten major types of viruses, each of which can be "run" on any stage of the operation simulation script in the shell program, namely [4]:

1. Parasitic;
2. Worm;
3. Trojan;
4. Stealth;
5. Self-encrypting;
6. Mutant;
7. Rest virus;
8. DIR-virus;
9. Retrovirus;
10. Web-worm virus.

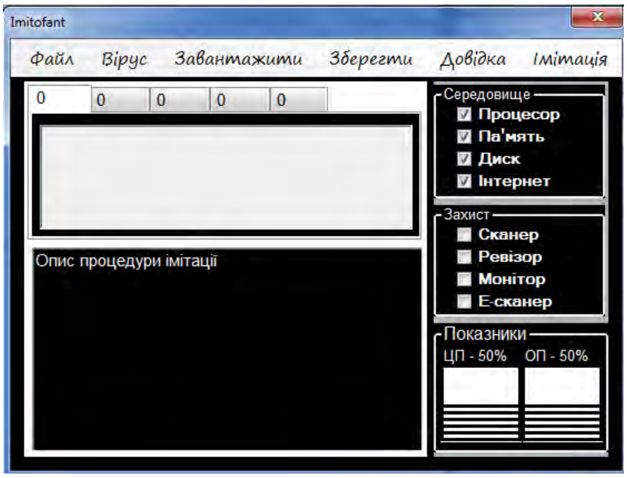
For malware, additionally, there are following advanced features, like:

1. Habitat, namely:
   - 1.1. Boot;
   - 1.2. File;
   - 1.3. File and boot;
   - 1.4. Document viruses;
   - 1.5. Network viruses

2. The method of existence, namely:
   - 2.1. Resident;
   - 2.2. non-resident viruses;

3. Degree of risk, namely:
   - 3.1. Harmless;
   - 3.2. Harmful;
   - 3.3. Hazardous;
   - 3.4. Dangerous.
4. Virus stage, namely:
   - 4.1. Latent;
   - 4.2. Incubation;
   - 4.3. The active phase;

According to defined above listed characteristics, after stage of starting up of selected protection methods, simulation model demonstrates how these methods detect malicious software objects and shows the accompanying information to this process.



Середовище

☑ Процесор
☑ Па'мять
☑ Диск
☑ Інтернет

Захист

□ Сканер
□ Ревізор
□ Монітор
□ Е-сканер

Показники

ЦП - 50% ОП - 50%

Fig. 1. Program window

In addition, except gradual text representation of each step of simulated scripts to the study of information belonging is reflected as a percentage, the amount of system memory used in this scenario imitation, and the degree of utilization of the CPU.

All data is updated according to the selected medium components, inputted malware objects available in this simulation, methods of protection. In addition, the simulation model is executed on the user information in the environment, harmful objects, and actions.

In the future, this software can be developed in a system simulation process, the study of which would allow the users much more aware of the nature and possible antiviral drugs, obstacles faced by developers of antivirus software. One of the main directions of the creation of such software, you can study and evaluation of behavioral situations, but rather, ways of development when trying to implement, the "artificial" environment, malware, along with all the potential ways of reproduction and distribution.

The most significant obstacle to the creation of this software is imperfect public knowledge in the field of anti-virus tools, algorithms rather their interaction with the environment, in an attempt to identify malware.

Very important is the process of identifying malicious software, which is by far the confidential information of companies which are engaged in developing algorithms for detecting malware and its extraction and removal of the results of it’s operations for potential PC.

Overall, this program can serve as a kind of "simulator", which would allow the user to understand the peculiarities of it’s functioning of computer system and it’s software, and what he really protecting algorithms to use for an effective anti-viral means, and what can and should be ignored.

Currently, buying antivirus software, the average user selects a "black box" because, almost always, do not fully understand it’s capabilities and, usually, most available in it, in the anti-virus tools and components, and not as necessary as reported by the manufacturing company.

Conclusion

In the future development of this software, I can highlight the main aspects of further development:

1) Research and program implementation in all existing algorithms for antivirus protection.

2) Research and implementation of software tool of all currently known types of malicious software objects.

3) Analysis and implementation of all necessary components of the environment (for this it is necessary to understand are the system resources that can, "potentiality", and collar harmful items.

4) Improved simulation scenario, to wit, removing all possible and construction, basic rules, which are anti algorithms and implementation of their basis functions in the software tool.

5) Output the user basic information about the process of passing the simulation scenario.

Due to the last point, the user will be able to bring himself do a single conclusion about the suitability of certain antiviral algorithms, depending on which type of malware it normally deal with, and what the consequences or the risks, carry, or that harmful software objects.

References

[1] V. I. Hluhih. Informacionnaya bezopasnost I zashchita dannyh: uchebnje posobie [Information security and data protection: study guide]. Irkutsk, Russia, 2011.

[2] A. A. Hladkih, Basovie principy informatsionnoy bezopasnosti vychyslitelnyh setey: uchebnoe posobie [Basic principles of information security of computer networks: a training manual]. Ullianovsk, Russia, 2009.

[3] A. P. Miklyaev. Nastolnaya kniga polzovatelya IBM PC[IBM PC User's Handbook]. Moskva, Russia, 2000.

[4] A. A. Horyachev. Practycum po informacionnym tehnologiam[Practicum on Information Technologies], Moskva, Russia, 1999.