UDC 004

# NEW CONTEMPORARY CONCEPT OF BEHAVIOR ANALYSIS FOR ANTIVIRUS SOFTWARE

***I. SHEVERDIN*[1], *S. HAVRYLENKO*[2*]**

[1] *student of the Department «Computer Engineering and Programming», NTU «KhPI», Kharkov, UKRAINE*

[2] *professor of the Department «Computer Engineering and Programming», NTU «KhPI», Kharkov, UKRAINE*

*email: 7573997@gmail.com*

For today we have a lot of problem with protection our computer equipment. We did say antivirus, but in truth it is actually you will deal with an actual computer virus.

Malware these days is all about making money, and ransomware and data-stealing Trojans are much more common, but unfortunately we did face to face with contemporary antivirus software has a long time for analyze all instructions in assembly also software has flaws, and sometimes those flaws affect your security. You expect an antivirus to identify and eliminate virus, and to leave good programs alone.

What about unknowns, antivirus cannot utterly identify as good or bad? Behavior analysis based on detection can, in theory, protect you against malware.

Nevertheless, this is not always an unmixed blessing. It no uncommon for behavioral detection systems to flag many innocuous behaviors performed by legitimate programs.

Monitor Automatic Page is another approach to the problem of unknown programs.

The main concept based on creating a special maps for behavioral analysis of the processes in operating system.

Analysis of processes is a solution that guarantees detection of all types the virus attacks as well.

So the main virus purpose for execution is inject to process or be a process, even if a virus is a set of scripts will be used to script interpretation processes for launch the instructions.

Architecture is assumed that the system will be operationally dependent, it will be means a generation maps for specific operating system based on the difference between the device drivers and the various system components.

MAP is installed after Windows operating system installation, afterwards MAP performs imprinting for operating system processes so on.

To build a maps analysis uses many the system levels to analyze the behavior of the operating system state.

The basic principle of the MAP system is the map formation levels 0 and 1, the next analysis through the using of fuzzy logic to generate the statistics of harmful effects of this process on the system.

Maps of level 0 is a hardware level maps that describe the system as a whole, namely, registry, memory, disk space, stream Internet packages.

Maps of level 1 is a maps of level processes that describe the behavior of the process, namely, performing operations with disk space, registry modification, interaction with network resources, creation of new threads and communication with external processes.

Maps of level 2 is low level analysis maps process statements constituting assembly language commands. The maps contain a sequence of malicious use of commands.

After you install new software, MAP will launch the mechanism of maps comparison, which indicates that MAP on the new processes in the system, then he will switch to level 2 for the definition of instruction in the course of which would form the method of fuzzy mathematical analysis of the likelihood of viral teams in this process.

After determining the statistics, was created a new map for level 1. Also the accuracy of currently may differ from the 0 % or 100 % MAP to create a list of introspective analysis and record the processes in queue.

In repeated passes on existing processes is likely change statistics by adding new conditions in the form of maps, which can lead to an introspection bubble.

If the system does not initiate their resources, MAP performs retrospective. The user will also be statistically described, MAP through a mechanism that generates a specific map mirror saturated neural repetition.

Finally, we can sum-up and distinguish pros and cons of this concept. First of all, obviously the main advantage that lazy principle means we analyze events instead of all instructions and files in operating system.

The main disadvantage is probability of recognition error; it is all about fuzzy logic, we suppose we can fix that use decision theory.