Shevchuk O.I.
Student,
Supervisor: **Zelenko N.V.**
Candidate of Psychological Science, Associate Professor,
Khmelnytskyi National University

MALWARE DETECTION TECHNIQUE BASED ON ARTIFICIAL IMMUNE SYSTEMS

The analysis of the situation of malware development shows dynamic growth of its quantity. Malware represents real danger as it penetrates into computer systems (CS) in order to plunder information [1, p. 14]. Despite the regular refinement of search methods, detecting and removal malware of different functionality, regular updates of anti-virus bases, and application of high technologies, the numerous facts of plunder of the confidential information has been observed and the various destructive operations has been performed which has lead to serious negative consequences. It shows the lack of efficient existing methods for capturing malware as they are oriented on detecting existing one and are insufficiently adapted for recognizing new suspicious programs [2, p. 145].

That is why it raises the problem of protection various CS. It includes a development of new more perfect information technologies which will increase the reliability and efficiency of anti-virus software diagnosis.

Using artificial immune systems ability to recognize and classify images it has been offered a method for detecting malware. For this purpose, clonal selection algorithm has been used to distribute software and detect malware.

Artificial immune systems.

Artificial immune systems belong to the class of intelligent computing systems that use the principles of the immune system of vertebrates. Artificial Immune System (AIS) – a computer adaptive system that uses models, principles, mechanisms and functions described in theoretical immunology, which are used to solve applied problems [3, p. 81].

Clonal selection algorithm (CLONAL_G)

Methods of the AIS use the specific immunological theories that explain the function and behavior of the adaptive immune system of mammals. The basic algorithms of the AIS are: clonal selection algorithm, negative selection algorithm, immune network, dendritic algorithms.

Clonal selection algorithm can be used as a means of object recognition clonal selection algorithm (CLONAL_G) [4, p. 134].

CLONAL_G algorithm can be described as follows:

1. Random formation of a population of individual (N);

2. Each pattern R, present to N population and determine its affinity with each element of N population;

3. Select n of the best highest affinity elements of N and generate copies of these individuals proportionally to their affinity with the antigen. The higher the affinity, the higher the number of copies, and vice-versa;

4. Mutate all these copies with a rate proportional to their affinity with the input pattern: the higher the affinity, the smaller the mutation rate;

5. Add these mutated individuals to the N population and reselect m of these maturated individuals to be taken as memories of the systems;

6. Repeat steps until a certain criterion is met.

Identification and classification malware using the artificial immune systems

The artificial immune systems have an ability to recognize and classify images. Thus it is possible to build a malware detection method via AIS. For this purpose, we can use the clonal selection algorithm to detect malware.

The detection process will include the following steps: preparation of the training set of data and the direct implementation of artificial immune system to identify new malware based on similarity of behavior with the behavior of existing malware.

Malware behavioral model

Let us describe the malware behavior as a tuple: $M_v = \langle \Theta, S, V, L, Aff, \varepsilon, Z \rangle$, where Θ- the set of all the malware; S – malware life cycle stages; $V = |V_{mp}|$- a relationship matrix, where $m = \overline{1,k}$ are penetration functions into the CS via system ports $p = \overline{1,h}$ of network; $L = |L_{ab}|$- a relationship matrix, where $a = \overline{1,\sigma}$ are malware's destructive operations of operating system components $b = \overline{1,\tau}$; Aff – a function that defines the interaction between components of the CS and malware, thus the set $a \in Aff(b_i, v_j)$ is the set of possible actions, that malware causes to the CS; ε – the ration between malware and its stages $v \in \Theta$ and $s \in S$, the relationship means $v \varepsilon s$ that malware is in stage s; Z – characteristic parameters of mentioned relations, $Z = \{ z_k \}$ – the set of destructive actions with standard priority weights $P = \{ p_k \}$ $(\sum p_k = 1)$ which take into the account the level of danger to the CS.

Malware detection method based on clonal selection algorithm

Malware detection method based on clonal selection algorithm comprises the following steps [5, p. 93]:

1. The construction of set antigens by means of clonal selection algorithm based on patterns of malware behaviors (the construction of training set);

2. The tracking of system events and their logging;

3. The construction of dynamic behavior of software;

4. The dynamic comparison of behaviors among the set of antigens with investigated behavior of the software;

5. The classification of software;

6. Repetition of steps until the completion of the CS.

Experiments

In order to conduct the experiments the test software based on the suggested technique has been developed. Results are presented in the table 1.

Table 1

Results of malware detection

Software with Malware properties		Detected Malwares	Detection rate, %
Rootkit	170	103	55,68
BackDoor	811	688	84,98
Malware-PSW	318	252	77,54
Malware-Clicker	212	140	67,09
Malware Downloader	845	655	78,01
Malware-Dropper	225	139	64,15
Malware-Proxy	161	106	64,96
Malware-Spy	335	241	69,31
Malware-Notifier	159	111	57,99
Total	3236	2435	-

The results confirmed that the use of AIS for the malware detection increase the detection efficiency up to 4-13%.

We have observed the solving of important scientific problem – the increasing of reliability and efficiency of malware detection. It is based on the usage of the clonal selection algorithm. Experimental results has shown that the suggested method is capable to detect and classify malware with high efficiency. This method can be the basis for building software for viruses diagnostics.

References:

1. Michael Erbschloe, «Malwares, Worms And Spyware. A Computer Security Professional's Guide To Malicious Code. Burlington» // Elsevier Butterworth–Heinemann, 2005, 212 p.

2. Szor Peter, «The Art Of Computer Virus Research And Defense» // Addison Wesley Professional, 2005, 744 p.

3. S. Lysenko, «Adaptive Information Technology Of Computer Systems Malwares Diagnosis Methods Of Virus Diagnosis Of Computer Networks», Visnyk of Khmelnytskyi National University // Khmelnytskyi, vol. 3. 2010, pp. 194-199. (in Ukrainian).

4. O. Savenko, S. Lysenko, «The Development Of Process Of Malware Detection Using Artificial Immune Systems», Visnyk of Khmelnytskyi National University // Khmelnytskyi, vol. 5. 2008, pp. 183-188. (in Ukrainian).

5. R. Grafov, O. Savenko, S. Lysenko, «Using Fuzzy Logic To Search For Malware Software In Computing Systems», Visnyk of Chernivtsi National University // Chernivtsi, vol. 6. 2009, pp. 85-91. (in Ukrainian).