UDC 004.92.3

O.S. SAVENKO, S.M. LYSENKO, A.F. KRYSHCHUK

Khmelnytskiy National University, Khmelnytskiy, Ukraine

MULTI-AGENT BASED APPROACH OF BOTNET DETECTION

A new approach for the botnet detection based on multi-agent system is proposed. The structure and main principles of antiviral agents' functioning within multi-agent system is developed. The principles of communication between the agent's units before and after attack on the computer system were developed. Software for realisation of antivirus multi-agent system on proposed techniques was developed. It shows growth of accuracy by 3-5% in comparison with known antivirus software. This approach is the basis for the development of new informational technology of anti-virus diagnosing based on multi-agent system in order to increase the accuracy for the botnet detection in computer systems.

Keywords: *botnet, Trojan, worm-virus, antivirus detection, multi-agent system, agent, sensor, fuzzy logic.*

Introduction

The analysis of the situation of development of the malware shows dynamic growth of their quantity. The most numerous classes of malware during last 10 years are Trojans and worm-viruses which spread and penetrate into computer system (CS) for the purpose of information plunder, DDoS attacks, anonymous access to network, spy actions, spamming that represents real danger [1] (Fig. 1).

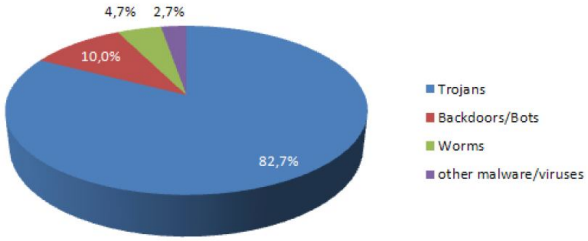

Fig. 1. Malware rate in 2011

Despite the regular refinement of methods of the search, detecting and removal Trojans and worm-viruses of different function, regular updates of anti-virus bases, the numerous facts of plunder of the confidential information are observed and the various destructive operations are performed which lead to serious negative consequences.

Common techniques used in modern antivirus software of Trojans' worm-viruses' detection are signature-based one, code emulators, encryption, statistical analysis, heuristic analysis and behavioural blocking. However, the accuracy of detection of new malware is low, and in recent years it has constantly decreased [2,3] (Fig. 2, 3).

One of the main reasons for the lack of detection accuracy is cooperating of Trojans with worm-viruses. So over the past 3-5 years there is a clear dynamics of conception of a new malware class - botnet. Place of Botnet among all malware is presented in Fig. 4.

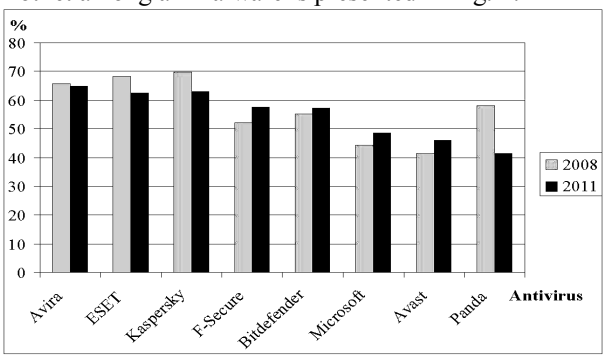

Fig. 2. Worm-viruses' detection in 2008 and 2011 years

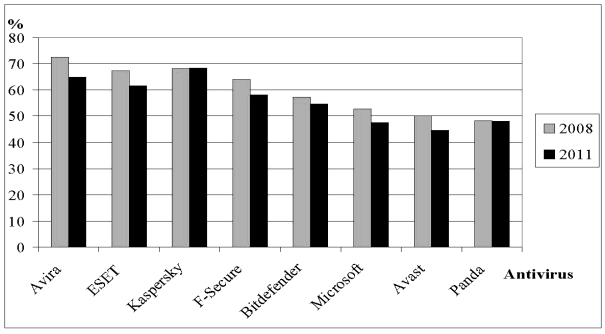

Fig. 3. Trojans' detection in 2008 and 2011 years

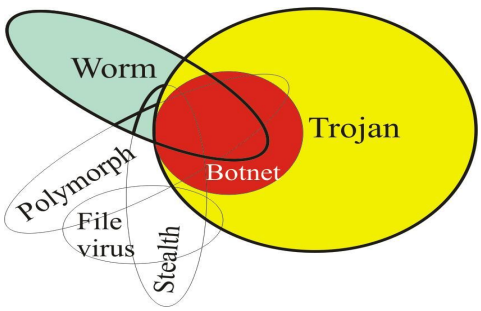

Fig. 4. Place of Botnet among all malware

That is why the actual problem of safety of various computer systems is a development of new more perfect approach of antivirus detection. One of possible way to increase the detection efficiency is a construction of virus multi-agent system in computer system for new botnet detection. For this purpose it is necessary to develop the principles of such system functioning; to describe the communication and functions' features of agents; to formalize sensors' and effectors' properties.

1. Multi-agent system of botnet detection

To increase the efficiency of botnet detection we involve multi-agent systems that will allow us to make antivirus diagnosis via agents' communication within corporate network.

Usage of multi-agent systems for botnet detection requires a generation of agents set with some structure and functionality.

Each agent should implement some behaviour and should include a set of sensors (components that directly is effected by the computer system), a set of effectors (components of that effect the computer system) and CPU - information processing unit and memory [4 – 6].

The scheme of antiviral agent multi-agent system operation is shown in Fig. 5.

Let us present agent as a tuple:

$$A = \langle P, R, K, S_1, S_2, S_3, S_4, S_5, S_6, ..S_n \rangle, \qquad (1)$$

where P – processor, which provides integration and processing data, processing optimal response to the incoming information about the computer system state, decision on the steps to be done.

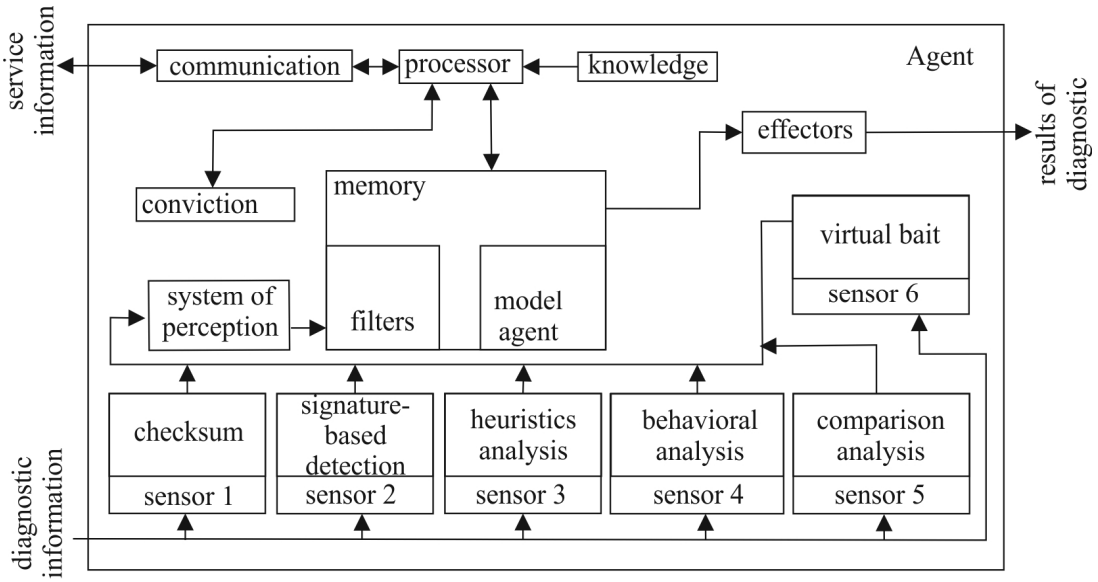

Fig. 5 The scheme of antiviral agent multi-agent system operation

R – rules, that change agent behaviour according to incoming information.

K – agent knowledge – part of rules and knowledge, that could be changed during its functioning.

S_1 – communication sensor, communicates with other agents via network protocols.

S_2 – agent of signature-based analysis; virus detection is performed by searching signatures in database; antivirus system alarms if computer is infected.

S_3 – checksum sensor.

S_4 – sensor of heuristics analysis; detection is performed in monitor mode with the use of fuzzy logic; sensor makes a conclusion about the danger degree of computer system infection with a new botnet [7].

S_5 – sensor of comparative analysis through application programming interface API and driver disk subsystem via IOS. If data on file received the first way differ from those obtained by the second way, file is infected.

S_6 – sensor - "virtual bait"; it is used for modelling of possible attacks or unauthorized access and it allows to learn the strategy of attacker and to identify a list of tools and actions intruder can do on infected computer system. If a remote administration of network is not carried out, all incoming ssh-traffic is redirected to this sensor.

The processor processes the input data and determines the level of risk of specified object in the computer system. There is a knowledge base of trusted software.

Conviction unit provides knowledge for agent in unusual situations. This will reduce the number of false positives in the new botnet diagnosis of computer system. The filters system for each sensor proposed to establish the risk factors for the evaluation of objects. Exceeding the limit values of the coefficients including the experience of all agents indicates the computer system infection with botnet.

Diagnostic information according to their functional properties each sensor is submitted.

Work results of the checksums and signature analysis sensors may not require full engagement of the agent functioning for notification of the infection with botnet, but in conjunction with results of other sensors and communication with other agents this sensors may assert this signal detection of the botnet.

Unit of perception holds summary information to the general form for further work. Then the information goes to the input of filters. Filters reject data generated by trusted programs or units (Fig.6).

Depending on the level of danger detected attacks the coefficients are defined by filters.

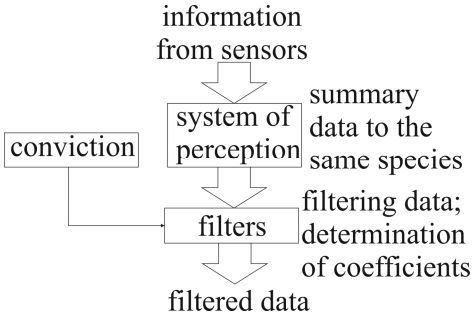

Fig. 6. The structure of filtering data unit

The data from the filters are to be processed by agent processor which determines whether the computer system is infected. Because of lack of data, the agent communicates with other agents for similar influence of programs' actions. The availability or absence of such information from other agents affects the final agent decision on a particular file or process.

When comparing the results obtained with the conviction unit data changes of coefficients and trusted programs are held.

Communications unit is responsible for encryption and decryption of interagents' information.

Agent results are transmitted to the effectors, as a means of influence on the computer system. If malware is detected agent through effectors blocks the process or processes that are responsible for performance of some malware and then notifies the user about the infection.

Agent model ensures the integrity of the agent's structure. It is realized by implementation of system checkpoints to provide the serviceability of this agent. Also after each checking all agent critical elements are stored for later restoring in case of virus attack on antivirus multi-agent system or possible failures in the computer system.

Each agent can activate the recheck the selected number of sensors to refine the results.

In situation when agent cannot communicate with other agent it is as autonomous unit and is able to detect different malware relying on knowledge of the latest updates and corrections in the trusted software base.

2. Sensor of botnet detection in monitor mode

A new technique for sensor diagnosis in monitor mode which uses fuzzy logic was developed. It is based on behavioural model of malware [7]. This sensor enables to make a conclusion about the degree of danger of CS infection by malware. For this purpose we construct the input and output linguistic variables with names: "suspicion degree of software object" - for the input linguistic variable, and "danger degree of the infection" - for output one.

The task of determination of membership function for input variable we will consider as the task of the ranking for each of mechanisms (functions) m_i of penetration ports p_j with the set of indications of danger Z and a choice of the most possible p_j with activation of some function m_i. Then we generate a matrix of advantage $M_{adv} = |q_{ij}|$. Elements of given matrix q_{ij} are positive numbers: $q_{ij} = q_i / q_j$, $0 < q_{ij} < \infty$; $q_{ji} = 1/q_{ij}$, $q_{ii} = 1$, $i, j = \overline{1,l}$, l - amount of possible results. Elements q_{ij} of matrix M_{adv} are defined by calculation of values of pair advantages to each indication separately taking into account their scales $Z = \{z_k\}$; $k = \overline{1,r}$ with usage of such formula

$$q_{ij} = \sum_{k=1}^{r} q_{ij}^{k} \cdot p_k \Big/ \sum_{k=1}^{r} q_{jk}^{k} \cdot p_k \,. \qquad (2)$$

Eigenvector $\Pi = (\pi_1, ..., \pi_m)$ is defied by using a matrix of advantage. This eigenvector answers maximum positive radical λ of characteristic polynomial $|M_{adv} - \lambda \cdot E| = 0$. $S \cdot \Pi = \lambda \cdot \Pi$, where E is an identity matrix. Elements of vector Π ($\sum \pi_i = 1$) are identified with an estimation of experts who consider the accepted indications of danger. The same procedure is performed for all m_i. As a result we receive a matrix of relationship $V_p = |m_i, p_j|$, in which each pair (relationship) m_i, p_j value $0 \le \pi \le 1$ responds. Using matrix $V_p = |m_i, p_j|$, we build matrix $V_p^* = |m_i, p_j|$ in which the relationship (m_i, p_j) is used and the elements of this relationship have value π_{max} $(0 \le \pi_{max} \le 1)$. Using matrix $V_p^* = |m_i, p_j|$, we build normalized curve for membership function $\mu_{X^p}(R)$ of an input variable.

Example of possible 20 pairs (x_i, y_j) ranked by the suspicion degree is given in fig. 7. Formation of function membership and at the stages of activation $\mu_{X^a}(R)$ and executing of the destructive actions $\mu_{X^e}(R)$ are similar.

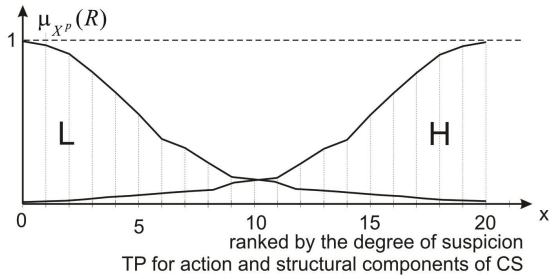

Fig. 7. Membership Function of Fuzzy Set "Suspicion Degree"

As a part of the solution of the problem the FIS using Mamdani algorithm was realized (fig. 8, 9).

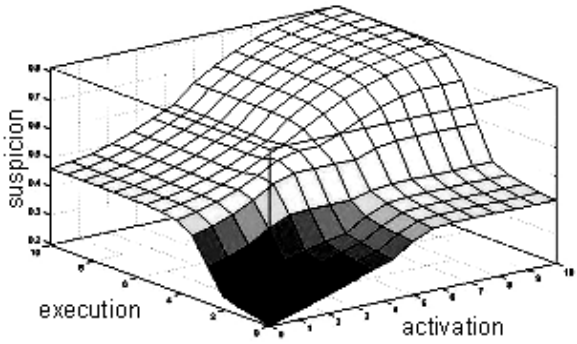

Fig. 8. Results of the fuzzy inference system implementation

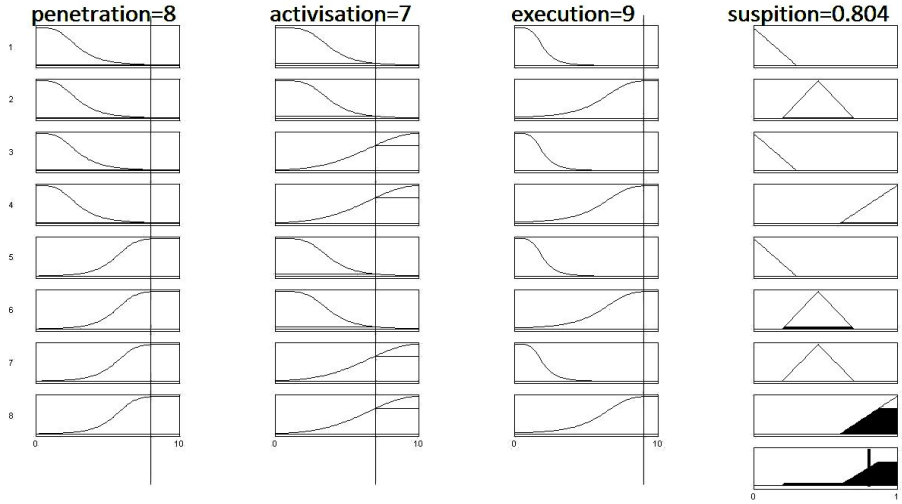

Fig. 9. Graphic representation of rules and fuzzy inference system

The results of fuzzy inference system 0.804 are interpreted as the degree of computer system infection with malware. If the resulting number exceeds some adopted threshold of danger antivirus system will block actions of the aqueous object. The sensor also transmits information about suspicious software to other agents.

3. Agents' functioning

Let a communication agent message present as a tuple:

$$< g, h, Com_x, Com_y, Mes, t >, \quad (3)$$

where g indicates whether it is a report, order or fetch of communication message; h - type of the agent message; Com_y - message receiver; Com_x - message sender, Mes - agent message content; t – sending time.

Thus the communication between the units within its sensors before attack or intrusion can be represented:

$$< R, N, Se, P, Inf_{int}, t_0 > \Rightarrow$$
$$< F, Int, P, M, Inf_{int}, t_1 > \cap$$
$$< O, C, P, Se, Inf_M, t_2 > \cup$$
$$< O, S, P, Se, Inf_M, t_2 > \cap$$
$$< O, R, P, E, Inf_{int}, Sh, t_2 > \cap$$
$$< O, I, P, Sh, Inf_{int}, t_2 >, \quad (4)$$

where R - report, O - order, F - fetch of the communication messages; N - new attack, Int - intrusion, C - continue, S - stop, Red - redirect, I - initialization as a type of the massage; P – agent processor; Se – sensors $S_1..S_5$; Sh – virtual bait; E – effectors; M - are respectively the sender and receiver of the message; Inf - the content of the message; t - time of the message sending.

The communication (interactions) between the units within its sensors after attack or intrusion can be represented:

$$AttackApproved \Rightarrow$$
$$< R, At, P, M, Inf_{int}, t_3 > \cap$$
$$< R, At, P, E, Inf_{int}, t_3 > \cap$$

$$< O, S, P, Sh, Inf_{int}, t_3 > \cap$$
$$< R, At, P, Se, Inf_{int}, t_3 > \quad (5)$$
$$\text{AttackDisapproved} \Rightarrow$$
$$< O, S, P, Sh, Inf_{int}, Se, t_3 > \cap$$
$$< O, Red, P, E, Inf_{int}, Se, t_3 > \cap$$
$$< O, Red, P, E, Inf_{int}, Se, t_3 > \cap$$
$$< O, C, P, Se, Inf_{int}, Sh, t_3 > \cap$$
$$< O, C, P, Se, Inf_{int}, Sh, t_3 >, \quad (6)$$

where At means – attack to computer system.

Let us formalize the function F which identifies the worth of agent A_l at time t and associates a real number to each of agents as the worth of that agent:

$$F: 2^{Ag} \times T \to R,$$
$$F(A_l, t) = \sum_{k=1}^{d} \frac{1}{T_a - t} N_{lk}^2 + \frac{1}{t} \frac{\Theta_{lk}}{N_{lk} + \varepsilon},$$
$$F(A_l \cup A_j, t) \geq F(A_l, t) + F(A_k, t), \quad l \neq k \quad (7)$$

where Ag - a set of agent units which are formed by combination of units with different types; Ta - the time of performing diagnosis actions; d - the number of agent components types; N_{lk} - the number of sensors of type k in agent A_l and Θ_{lk} - the sensors weight of type k within the agent no matter of their amount.

A good incentive for agents at the initial moments of reporting intrusion can be provided by sensors Se in the system in the sense that they will form better coalitions and thus collaborate. As we can see in (7) no agent in AMAS can get more advantage by changing its actions. Also the function F does not increase by changing the agents set.

4. Experimental research

Software for realisation of antivirus multi-agent system on proposed techniques was developed.

Interface results window of botnet diagnosing of computer system is shown in Fig. 10.

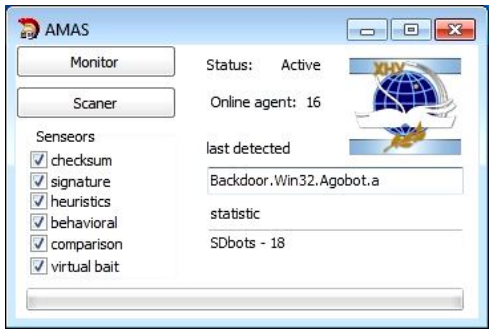

Fig. 10. Software of botnet detection

For the experimental determination of the efficiency of developed software 217 programs with the botnets' properties were generated and launched on different amount of workstations (table 1).

Table 1

Accuracy of botnet detection with developed software

Botnets (number) \ Workstations (agents)	16	24	32	40
SDbot (80)	74%	75%	78%	81%
Rbot (49)	61%	63%	64%	67%
Agobot (54)	60%	60%	62%	63%
Spybot (18)	65%	68%	71%	75%
Mytob (16)	54%	57%	60%	63%
Accuracy, %	**62.8%**	**64.6%**	**67.8%**	**69.8%**

Accuracy of botnet detection of the developed software in comparison with known is shown in Fig. 11, it shows growth of accuracy by 3-5% in comparison with known antivirus software.

Also we performed false detection experiments and it is about 3-7%. But with the growth of agents amount false detection is reducing to 2-4%.

Conclusion

A new approach for the botnet detection based on multi-agent system is proposed.

The structure and main principles of antiviral agents' functioning within multi-agent system is developed. A new technique for sensor diagnosis in monitor mode which uses fuzzy logic was developed. The principles of communication between the agent's units before and after attack on the computer system were developed. Software for realisation of antivirus multi-agent system on proposed techniques was developed. It shows growth of accuracy by 3-5% in comparison with known antivirus software.

This approach is the basis for the development of new informational technology of antivirus diagnosing based on multi-agent system in order to increase the accuracy for the botnet detection in computer systems.

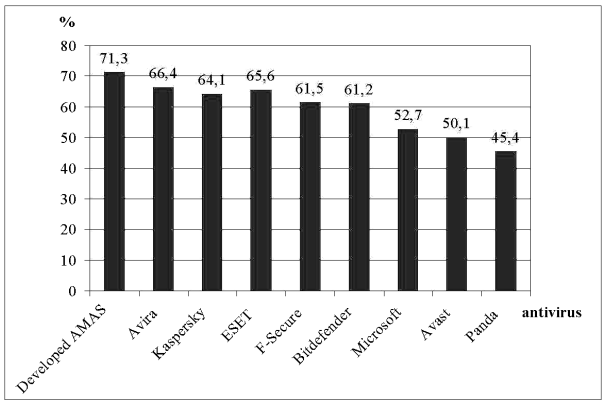

Fig. 11. Accuracy of botnet detection by developed software in comparison with known one

References

1. Goshko, S. Encyclopedia of protection against viruses [Text] / Goshko S. – Moscow : SOLON-Pres, 2005. – 352 p. (in Russian)

2. Savenko, O. Research of the antivitus technologies for malware detection [Text] / O. Savenko, S. Lysenko, A. Kryshchuk // Proceedings of the XII conference "Modern informations & electronic technologies - 2011", Vol. 1 – Ukraine, Odessaa, 2011. – P.95-96. (in Ukrainian)

3. AV Comparatives laboratories [Electronic resource] – Access mode: http://www.av-comparatives.org. – 20.03.2012.

4. Wooldridge, M. An Introduction To Multiagent Systems [Text] / Michael Wooldridge. – John Wiley & Sons LTD, 2002. – 348 p.

5. Shoham, Y. Multiagent Systems Algorithmic, Game-Theoretic, and Logical Foundations [Text] / Yoav Shoham, K. Leyton-Brown. - Cambridge University Press, 2009. – 504 p.

6. Alkhateeb, F. Multi-Agent Systems [Text] / Faisal Alkhateeb, Eslam Al Maghayreh, Iyad Doush // Modeling, Control, Programming, Simulations and Applications, 2011. – 522 p.

7. Bernikov, A.R. Malware search in the distributed simulators using the technology of fuzzy logic [Text] / A.R. Bernikov, R.P. Grafov, S.M. Lysenko, O.S. Savenko // Information technologies. – Moscow. – 2011. – № 10. – P. 42-47. (in Russian).

Поступила в редакцию 2.04.2012

Рецензент: д-р техн. наук, проф. И.А. Жуков, Национальный авиационный университет, Киев, Украина.

ВИЯВЛЕННЯ БОТНЕТ МЕРЕЖ НА ОСНОВІ МУЛЬТИ-АГЕНТНИХ СИСТЕМ

О.С. Савенко, С.М. Лисенко, А.Ф. Крищук

Запропоновано новий підхід до виявлення ботнет-мереж, який базується на використанні мультиагентних систем. Запропоновано структура та основні принципи функціонування антивірусного агента в межах мультиагентної системи. Розроблено принципи спілкування між модулями агента до та після здійснення атаки на комп'ютерну систему. Розроблено програмне забезпечення для реалізації системи антивірусних агентів на запропонованих методах. Показано зростання точності виявлення в порівнянні з відомим антивірусним програмним забезпеченням. Даний підхід – основа для розвитку нової інформаційної технології антивірусного діагностування, заснованого на мультиагентній системі, він дозволяє збільшити точність ботнет-виявлення в обчислювальних системах.

Ключові слова: ботнет-мережа, троянські програми, worm-віруси, антивірусне діагностування, мультиагентна система, агент, сенсор, нечітка логіка.

ОБНАРУЖЕНИЕ БОТНЕТ-СЕТЕЙ НА ОСНОВЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ

О.С Савенко, С.Н. Лысенко, А.Ф. Крыщук

Предлагается новый подход к обнаружению ботнет-сетей на основе мультиагентных систем. Разработана структура и основные принципы функционирования антивирусных агентов в мультиагентной системе. Были разработаны принципы взаимодействия между модулями агента до и после атаки на компьютерную систему. Разработано программное обеспечение для реализации системы антивирусных агентов на предложенных методах. Показан рост точности обнаружения по сравнению с известным антивирусным программным обеспечением. Данный подход – основа для развития новой информационной технологии антивирусного диагностирования, основанного на мультиагентной системе, он позволяет увеличить точность ботнет-обнаружения в вычислительных системах.

Ключевые слова: ботнет-сеть, троянские программы, worm-вирусы, антивирусное диагностирование, мультиагентная система, агент, сенсор, нечеткая логика.

Савенко Олег Станиславович – канд. техн. наук, доцент, декан факультета компьютерных систем и программирования Хмельницкого Национального, Хмельницкий, Украина, e-mail: kism@beta.tup.km.ua.

Лысенко Сергей Николаевич – канд. техн. наук, старший преподаватель кафедры системного программирования Хмельницкого Национального, Хмельницкий, Украина, e-mail: sirogyk@ukr.net.

Крыщук Андрей Федорович – аспирант, ассистент кафедры системного программирования Хмельницкого Национального, Хмельницкий, Украина, e-mail: rtandrey@rambler.ru.