

УДК 004.492.3

О.С. Савенко, С.М. Лисенко, А.Ф. Кришук
Хмельницький національний університет

ЕФЕКТИВНІСТЬ ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ БОТ-МЕРЕЖ АНТИВІРУСНОЮ МУЛЬТИАГЕНТНОЮ СИСТЕМОЮ

Савенко О.С., Лисенко С.М., Кришук А.Ф. Ефективність діагностування комп'ютерних систем на наявність бот-мереж антивірусною мультиагентною системою. В статті розглянуто дослідження ефективності діагностування комп'ютерних систем на наявність бот-мереж використовуючи антивірусну мультиагентну систему, як засіб діагностування. Проведено порівняння розробленої антивірусної системи з існуючими. Визначено рівень ефективності діагностування комп'ютерних систем на наявність бот-мереж.

Ключові слова: агент, мультиагентна система, антивірусне діагностування, ефективність
Табл. 2, Рис. 2, Літ. 11

Савенко О.С., Лысенко С.Н., Крышук А.Ф. Эффективность диагностирования компьютерных систем на наличие бот-сетей антивирусной мультиагентной системой. В статье рассмотрены исследования эффективности диагностирования компьютерных систем на наличие бот-сетей используя антивирусную мультиагентную систему, как средство диагностики. Проведено сравнение разработанной антивирусной системы с существующими. Определен уровень эффективности диагностирования компьютерных систем на наличие бот-сетей.

Ключевые слова: агент, мультиагентная система, антивирусное диагностирование, эффективность

Savenko O.S., Lysenko S.M., Kryshchuk A.F. The computer systems diagnosis efficiency for botnet presence by antivirus multi-agent systems. In article the computer systems diagnosis efficiency for botnet presence by antivirus multi-agent systems is investigated. A comparison of the developed system with existing antivirus systems is held. The level of efficiency of computer systems diagnosing for botnets presence is evaluated.

Keywords: agent, multiagent system, antivirus diagnosis, efficiency.

Вступ. Бот-мережі - один з головних і найпопулярніших інструментів сучасної кіберзлочинності. Комп'ютерні мережі, які складаються з великої кількості комп'ютерних систем, інфікованих програмами-ботами, автоматично виконують ті чи інші дії в інтересах власника або керуючого такою мережею [1-5].

Сучасні бот-мережі, виконують повний спектр зловмисних дій у корпоративних і приватних комп'ютерних систем (КС): від класичних збору адрес електронної пошти та подальшого розсилання «спаму» до розкрадання інформації для банківських рахунків та комерційного шпигунства. Бот-мережі найчастіше використовуються для DDoS-атак на Інтернет-ресурси, а також на засмічування соціальних мереж пропагандистськими, рекламними та небезпечними повідомленнями.

Аналіз останніх досліджень і публікацій. В [6] запропоновано метод визначення рівня присутності бот-мережі шляхом аналізу проявів дій ботів в ймовірно інфікованій КС. Залучення такого підходу виконується у випадку підозрілої поведінки програм на певній кількості КС корпоративної мережі. Антивірусне діагностування здійснювалося на базі побудованої антивірусної мультиагентної системи (МАС) [7, 8].

В роботі пропонувалося будувати карту-схему зв'язків корпоративної мережі, яка формувалася певними записами в кожному антивірусному агенті МАС. На базі даної інформації усі агенти здійснювали комунікативний обмін даними.

В процесі роботи на кожній комп'ютерній системі здійснювалося антивірусне діагностування присутніми в агенті сенсорами. Отримані результати антивірусного діагностування аналізувалися на предмет того, який із сенсорів спрацював та який рівень підозрілості він видав. Якщо спрацювали сенсори сигнатурного аналізатора S_1 та контрольних сум S_2 результати R_{S_1} та R_{S_2} інтерпретувалися як 100% виявлення шкідливого ПЗ.

Якщо спрацювали сенсори евристичного R_{S_3} та поведінкового R_{S_4} аналізаторів з подоланням певного порогу $n \leq \max(R_{S_3}, R_{S_4}) \leq 100$, то здійснювався аналіз рівня підозрілості і приймався рішення щодо можливого блокування дій ПЗ, і подальшого його видалення.

Ключовим моментом дослідження була ситуації, коли результати антивірусного діагностування належать проміжку $m \leq \max(R_{S_3}, R_{S_4}) < n$. В цьому випадку антивірусний агент КС здійснював опитування решти агентів на предмет прояву схожої поведінки на інших КС корпоративної мережі. Якщо в результаті опитування антивірусний агент отримав інформацію від одного або більше агентів КС щодо схожої підозрілої поведінки програмного забезпечення, то здійснювалася перебудова наявної карти мережі з помітками ймовірно інфікованих КС. З такого

набору вибиралася одна КС і змінювався її тип підключення до мережі таким чином, щоб робота бота в нових умовах була неможливою.

Рівень присутності бот-мереж визначався після опрацювання проявів бот-мережі на «перепідключеній» КС, помічених комп'ютерних системах та інших КС корпоративної мережі.

Засобами нечіткої експертної системи здійснювалося визначення рівня присутності бот-мереж, яка спростовувала або підтверджувала факт присутності бот-мережі.

Визначення рівня присутності бот-мережі шляхом аналізу проявів дій ботів в ситуації навмисної зміни типу підключення ймовірно інфікованої КС функціонувало за алгоритмом 1 [9, 10].

Для усіх КС корпоративної мережі
поки $КС_i$ функціонує
якщо $R_{s1} = \text{true}$ або $R_{s2} = \text{true}$ тоді блокувати і видаляти ПЗ;
якщо $R_{s3} = \text{true}$ або $R_{s4} = \text{true}$ і $n \leq \max(R_{s3}, R_{s4}) \leq 100$ тоді блокувати і видаляти ПЗ;
інакше якщо $R_{s3} = \text{true}$ або $R_{s4} = \text{true}$ і $m \leq \max(R_{s3}, R_{s4}) < n$ тоді опитати інші агенти; вибрати КС для перепідключення; проаналізувати рівень присутності бот-мережі в корпоративній мережі;
інакше якщо $R < m$ очікувати результати $R_{s1}, R_{s2}, R_{s3}, R_{s4}$.

Алгоритм 1. Діагностування КС на наявність бот-мереж

Розроблена МАС містить також сенсора S_7 , який дозволяє здійснювати емуляцію запуску та виконання над потенційно шкідливим ПЗ певних дій. Реакції на вказані дії дозволяють зробити висновок про присутність в ньому поліморфного коду.

Виходячи з властивостей поліморфних вірусів на сенсор S_7 виконує:

- провокативні дії по відношенню до ймовірно інфікованого файлу;
- повторні запуски підозрілого файлу для ймовірної модифікації власного коду;
- виявлення шкідливого програмного забезпечення (ШПЗ) шляхом аналізу його поведінки та можливої зміни свого тіла, що базується на принципах відомих рівнів поліморфізму.

Під провокативними діями мається на увазі виявлення властивості поліморфних вірусів створення своєї копії зі зміною власного тіла при його видаленні. Дана властивість часто призводить до того, що оригінал може бути виявлено та видалено, а нова копія бота буде невидимою для антивірусу.

Здійснення повторних запусків підозрілого ПЗ може показати ймовірну «зміну» тіла програми в результаті виконання шифрування. Виявлення такої зміни можливе завдяки побудові «відбитків» К еталонного та модифікованого файлів K' та їх подальшого порівняння. «Відбиток» K формується визначеною двійковою послідовністю $K = \alpha, \beta, \chi, \delta, \varepsilon$, де α - назва файлу; β - розмір файлу; χ - дата останньої зміни; δ - системний атрибут; ε - 128 бітний код MD5.

Сенсор S_7 також виконує роль поведінкового аналізатора, який здійснює аналіз дій з урахуванням моделей поліморфних вірусів різних рівнів. На основі знань про поліморфну природу поведінки вірусів та поведінок бот-мереж є можливим їх виявлення шляхом динамічного порівняння відомих поведінок з поведінками нових бот-мереж. Виявлення поліморфного коду здійснюється з урахуванням відкидання можливих команд-сміття, перестановок команд, команд вибору шифрувальника, самих команд шифрувальника тощо. Відомі поведінки ботів та поведінки досліджуваних об'єктів представляються послідовностями, які в подальшому порівнюються.

Для порівняння шаблонних поведінок з тією, що виконує потенційно небезпечна програма, використано алгоритм приблизного порівняння, який розв'язує задачу k-приблизного збігу. Використаний алгоритм вимагає $O(kn)$ [11].

Виходячи з концепції функціонування антивірусної МАС, в кожному агенті відбувається очікування спрацювання евристичного S_3 та поведінкового S_4 сенсорів. У випадку їх спрацювання, а також виявлення ними факту розпаковування певного файлу, виконується завантаження підозрілого програмного об'єкта в сенсор-емулятор S_7 (див. рис.1).



Рис. 1. Робота сенсора S7 в агенті мультиагентної системи, що функціонує в локальній мережі

Якщо в результаті провокативних дій виявлено створення нового файлу, або якщо у випадку повторних запусків виявлено зміну тіла файлу, або в результаті аналізу поведінки програми виявлено поведінку вірусу певного рівня поліморфізму, то сенсор S7 повідомляє процесор агента про необхідність блокування даного файлу, а також розсилання інформації про даний файл іншим агентам мультиагентної системи. Якщо перераховані дії по відношенню до файлу не виявляють ознаки присутності вірусу даний файл залишає сенсор S7.

Розроблена мультиагентна система здатна здійснювати виявлення бот-мереж на рівні 88-96%, проте в процесі антивірусного діагностування задіюються ресурси як комп'ютерних систем так і ресурси корпоративної мережі, що впливає на загальну ефективність антивірусного діагностування комп'ютерних систем.

Постановка проблеми. Таким чином, постає задача побудови методики визначення ефективності антивірусного діагностування комп'ютерних систем з урахуванням параметрів антивірусного діагностування, ресурсів операційної системи та комп'ютерних мереж, які використовує антивірусний засіб для діагностування.

Обчислення ефективності. Ефективність діагностування комп'ютерних систем (КС) на наявність шкідливого програмного забезпечення визначають агенти МАС. Сенсори, які містяться в агентах взаємодіють з одного боку з ШПЗ та з операційною системою - з іншого.

Таким чином, загальна ефективність антивірусного діагностування КС враховує результати антивірусного діагностування та програмно-апаратні ресурси, які використовуються в процесі антивірусного діагностування, і визначається:

$$P = \frac{E}{R}, \quad (1)$$

де E - ефективність роботи антивірусного засобу, яка включає достовірність роботи агента; R - ресурси, що залучаються для здійснення антивірусного діагностування.

Ресурсами, що залучаються для здійснення антивірусного діагностування, вважатимемо тривалість ДКС на наявність ШПЗ кожним з сенсорів $T_{S_1} \dots T_{S_7}$; середню тривалість обробки даних процесором агента T_A ; середній час обміну діагностичною інформацією між агентами T_N^A ; об'єми даних, що проходять від кожного з сенсорів V_{S_i} ; об'єми даних, що надходять процесору агента V_A ; об'єми даних, які обмінюються між агентами V_N^A . Ресурси, що залучаються для здійснення антивірусного діагностування $R = f(T_A, T_{S_1} \dots T_{S_7}, T_N^A, V_A, V_{S_1} \dots V_{S_7}, V_N^A)$, розраховуватимемо:

$$R = T_A \cdot V_A + T_{S_1} \cdot V_{S_1} + T_{S_2} \cdot V_{S_2} + T_{S_3} \cdot V_{S_3} + \\ + T_{S_4} \cdot V_{S_4} + T_{S_5} \cdot V_{S_5} + T_{S_6} \cdot V_{S_6} + T_{S_7} \cdot V_{S_7} + T_N^A \cdot V_N^A, \quad (2)$$

Для оцінки ефективності антивірусного діагностування введемо показник хибних спрацювань ДКС на наявність ШПЗ, який обчислимо за формулами:

$$X_M = \frac{\sum_{i=1}^s x_i}{X}, \quad (2)$$

де X - загальна кількість програм, x_i - кількість програм, віднесених антивірусним засобом до i -того типу шкідливого програмного забезпечення.

В процесі роботи антивірусного засобу явище хибних спрацювань також використовує ресурси, що відображається зниженням рівня ефективності антивірусного діагностування $R_X = f(X_M, T_{X_M}, V_{X_M})$ на величину:

$$R_X = X_M \cdot T_{X_M} \cdot V_{X_M}, \quad (3)$$

де X_M - показники хибних спрацювань; T_{X_M} - показники часу, затраченого на хибні спрацювання; V_{X_M} - об'єми даних, що проходять в процесі хибних спрацювань.

Отже, визначення ефективності діагностування КС на наявність шкідливого програмного забезпечення з урахуванням показника хибних спрацювань, складе:

$$P = \frac{E}{R + R_X}. \quad (4)$$

Достовірністю результатів роботи діагностування вважатимемо значення відношення виявленого ШПЗ до усієї кількості ШПЗ. Приймемо n_i , $i = \overline{1, s}$, $s \in N$ як кількість ШПЗ i -того типу, k_i - кількість об'єктів ШПЗ, виявлених антивірусним засобом. Тоді достовірність результатів роботи діагностування D_M складе:

$$D_M = \frac{\sum_{i=1}^s \alpha_i \cdot k_i}{\sum_{i=1}^s \alpha_i \cdot n_i}, \quad (5)$$

де α_i - відсоток i -того класу від усього ШПЗ, $0 \leq \alpha_i \leq 1$.

Під тривалістю ДКС на наявність ШПЗ T_M розглядатимемо час t_b здійснення пошуку b_j -тої сигнатури або поведінки в базі

$$T_M = \sum_{j=1}^v t_b, \quad (6)$$

де t_p - час, необхідний для занесення $l = \overline{1, \gamma}$ сигнатур та поведінок ШПЗ до бази.

Об'єми даних $V_{Mt_{ym}}$, що проходять в процесі ДКС на наявність ШПЗ агентом за одну умовну одиницю часу, визначимо як суму об'ємів даних, помножених на частоту запитів даних на одну умовну одиницю часу n_r :

$$V_{Mt_{ym}} = V_A^s \cdot n_r^s + V_{S1}^p \cdot n_r^p + V_{S2}^a \cdot n_r^a + V_{S3}^e \cdot n_r^e + \\ + V_{S4}^c \cdot n_r^c + V_{S5}^d \cdot n_r^d + V_{S6}^e \cdot n_r^e + V_{S7}^f \cdot n_r^f + V_N^g \cdot n_r^g, \quad (7)$$

де V_A^s - об'єм даних, що проходить при ДКС при обробці даних процесором агента; V_{S1}^p , V_{S2}^a , V_{S3}^e , V_{S4}^c , V_{S5}^d , V_{S6}^e , V_{S7}^f - об'єм даних, що використовується при роботі сенсорів агента; V_N^g - об'єм даних, що використовується агентами для обміну інформацією. Тоді з урахуванням часу необхідного для реалізації кожного етапу загальний об'єм даних, що проходять в процесі ДКС V_M обчислимо так:

$$V_M = V_{Mt_{ym}} \cdot n_{t_{ym}}. \quad (8)$$

а) ефективність роботи антивірусного засобу E , що визначається на основі максимізації значення достовірності діагностування КС на наявність ШПЗ $D_M \rightarrow \max$; цільове значення показника $E \rightarrow \max$;

б) ресурси, що залучаються для здійснення антивірусного діагностування, які визначаються на основі мінімізації значень середньої тривалість діагностування, середнього часу підготовки до діагностування та мінімізації об'ємів даних, що проходять в процесі ДКС, $T_A \rightarrow \min$, $T_N^A \rightarrow \min$, $T_{S1} \dots T_{S7} \rightarrow \min$, $V_N^A \rightarrow \min$, $V_{S1} \dots V_{S7} \rightarrow \min$, $V_A \rightarrow \min$, а також

мінімізації показників, що залучаються в процесі хибних спрацювань, $X_M \rightarrow \min, T_{X_M} \rightarrow \min, V_{X_M} \rightarrow \min$.

Дослідження характеристик та показників системи діагностування дають можливість здійснити визначення достовірності та ефективності антивірусного діагностування КС на наявність ШПЗ.

Основні результати дослідження. Для оцінки та порівняння загальної ефективності роботи антивірусної MAC у порівнянні з іншими відомими антивірусними засобами (АЗ) було проведено ряд експериментів.

Для дослідження ефективності антивірусних засобів було здійснено оцінку розробленої MAC, Panda antivirus, Eset Nod32, Kaspersky, Avira, Microsoft, Avast, Zillia, Dr. Web.

Експеримент проводився шляхом запуску 55 вірусних програм (ботів) [6-8].

Таблиця 1. Результати експериментів діагностування

Засіб антивірусного діагностування	достовірність роботи, %	тривалість ДКС на наявність ШПЗ, хв	середня тривалість ДКС, хв	середній час підготовки ДКС (обмін між агентами), хв	об'єми даних, що проходять в процесі ДКС, Мб	ефективності ДКС на наявність ШПЗ
MAC	95	29	1	1	2395	0.93
Panda	86	27	1	3	2389	0.87
Eset Nod32	89	22	1	3	2322	0.88
Kaspersky	91	30	1	2	2368	0,91
Avira	90	28	1	3	2322	0,88
Microsoft	76	17	1	2	2322	0,78
Avast	85	25	1	3	2380	0,81
Zillia	77	28	1	4	2340	0,76
Dr. Web	85	29	1	3	2322	0,81

Таблиця 2. Показники хибних спрацювань під час антивірусного діагностування

Засіб антивірусного діагностування	Показник ресурсів, використаних в процесі хибних спрацювань під час антивірусного діагностування, %
	MS Windows 7
MAC	5
Panda	3
Eset Nod32	4
Kaspersky	6
Avira	4
Microsoft	3
Avast	5
Zillia	5
Dr. Web	3

Загальна ефективність антивірусного діагностування представлена діаграмою на рис.2.

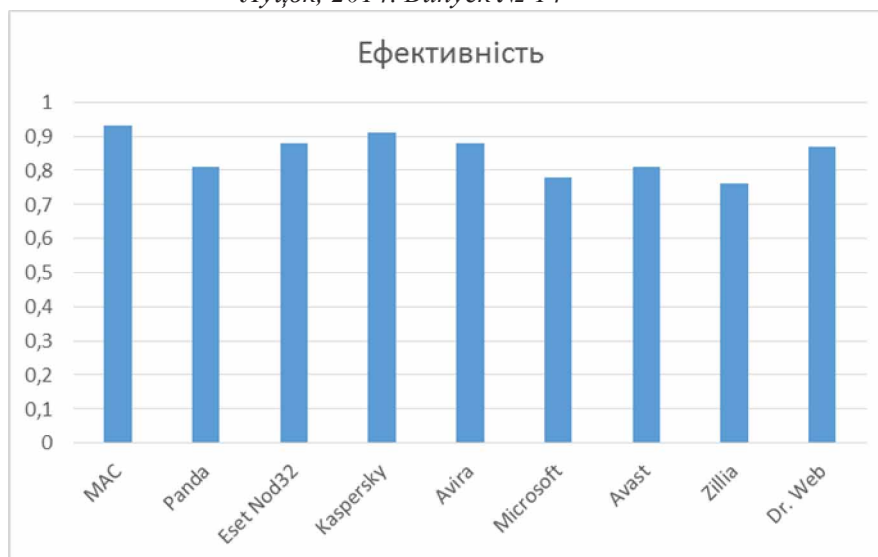


Рис. 2. Загальна ефективність антивірусного діагностування

Висновки. Для оцінки та порівняння загальної ефективності роботи запропонованої антивірусної мультиагентної системи з іншими відомими антивірусними засобами розглянуто параметри діагностування, які впливають на загальну ефективність антивірусного діагностування, а саме: достовірність роботи агента, тривалість діагностування та об'єми даних, що проходять в процесі антивірусного діагностування.

Завдяки використанню мультиагентного підходу для діагностування КС досягається високий рівень достовірності виявлення бот-мереж. Згідно запропонованої методики визначення ефективності антивірусного діагностування комп'ютерних систем з'ясовано, що розроблена мультиагентна система демонструє високу ефективність діагностування, яка склала 0,93.

1. Tim Rains Operating System Infection Rates: Application Vulnerabilities & Exploits Trend Up, Increase OS Infection Rates [Електронний ресурс] - Режим доступу : <http://blogs.technet.com/b/security/archive/2012/12/31/operating-system-infection-rates-vulnerabilities-amp-exploits-trending-up-increase-os-infection-rates.aspx>.

2. Williamson M. M. Virus throttling / M. M. Williamson, J. Twycross, J. Griffin // Virus Bulletin. – 2009.

3. VB100 Results Summary [Електронний ресурс] : Anti-Virus comparative. - <http://www.virusbtn.com/vb100/archive/summary>.

4. AV Comparatives laboratories [Електронний ресурс] – Access mode <http://www.av-comparatives.org>. – назва домашньої сторінки Інтернету.

5. Proactive/Retrospective test. [Електронний ресурс] : Anti-Virus comparative. – Режим доступу : <http://av-comparatives.org>. – назва домашньої сторінки Інтернету.

6. Савенко О.С. Процес діагностування комп'ютерних систем на наявність ботнет-мереж на основі мультиагентних технологій / О.С. Савенко, С.М. Лисенко, А.Ф. Кришук // Комп'ютерно-інтегровані технології: освіта, наука, виробництво: наук. журн. – 2013. — №11. – С.72–81.

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

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

9. Savenko O. The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode / Savenko O., Lysenko S. // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications - USA, NJ 08855-1331: IEEE Operations Center, 2011 - vol.2, pp. 845-853.

10. Savenko O. Multi-agent based approach of botnet detection in computer systems / Savenko O., Lysenko S., Kryschuk A. // Computer Networks Communications in Computer and Information Science, 2012, Volume 291, pp. 171-180.

11. Smyth, B. Computing Patterns In Strings / B. Smyth // Williams. – 2006. – С. 496.