УДК 004.492.3
О.С. Савенко, С.М. Лисенко, А.Ф. Крищук
Хмельницький національний університет

ПРОЦЕС ДІАГНОСТУВАННЯ КОМПЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ БОТНЕТ-МЕРЕЖ НА ОСНОВІ МУЛЬТИАГЕНТНИХ ТЕХНОЛОГІЙ

В роботі запропонований новий метод діагностування комп'ютерних систем на наявність ботнет-мереж з використанням мультиагентних систем. Виявлення здійснюється на основі проявів ботів в кількох комп'ютерних системах, які належать корпоративній мережі.

Ключові слова: антивірусне діагностування комп'ютерних систем, нейро-нечіткі системи, worm-віруси, ботнет-мережа, бот.

Вступ

Найбільш численні і небезпечні атаки на комп'ютерні системи (КС) за останні роки здійснює новий клас шкідливих програм – ботнет-мережі. Цей клас є інтеграцією і кооперуванням троянських програм і «worm»-вірусів. Вони є основною для виконання таких небезпечних дій, як: розподілені атаки на відмову в обслуговуванні, поширення шкідливого програмного забезпечення (ШПЗ), «фішинг», викрадення конфіденційної корпоративної інформації, організації анонімних проксі-серверів, і т.і. Особливістю ботнет-мереж є використання спеціалізованих команд і контрольованих каналів взаємодії, які забезпечують оновлення функціональних блоків ботів і виконання закладених дій та функцій [1-4].

Зважаючи на широке розповсюдження ботнет-мереж і їх руйнівний вплив, на сьогодні розроблено ряд методів виявлення ботнет-мереж в КС. Ці методи можна розділити на два напрямки: методи, що базуються на використанні КС як «приманки», та методи на основі пасивного моніторингу трафіку.

Методи, що базуються на доступі до слабо захищених мереж є потужним інструментом для розуміння і дослідження технології, архітектури та поведінки ботнет-мереж, але не є ефективними для їх виявлення [3].

При застосуванні пасивного моніторингу трафіку створюються точки пасивно контролю в реальному інтернет-трафіку для виявлення та вилучення пакетів ботнет-мережі.

Поведінкові методи класифікуються як сигнатурні і аномальні. Основним недоліком сигнатурних методів є виявлення тільки відомих ботнет-мереж. Методи на основі виявлення аномалій не вимагають попередніх сигнатур ботнет-мереж і мають низький рівень хибних спрацювань [4].

В основі методів діагностування на основі DNS є аналіз даних трафіку DNS. Основним недоліком такого підходу є висока тривалість обробки необхідних даних та величезні масштаби мережного трафіку.

Методи «Data-mining» базуються на виявленні протоколів, які використовують ботнет-мережі для комунікації з командними центрами. З огляду на еволюцію ботнет-мереж, виявлення комунікаційного трафіку ускладнюється [1-5].

Постановка задачі

Таким чином, актуальною є задача розробки нових методів діагностування КС на наявність ботнет-мереж. Перспективним є використання мультиагентних технологій, агенти яких здійснюють порівняння досліджуваної інформації про атаки та підозрілі поведінки програмного забезпечення на різних КС. Кожен агент мультиагентної антивірусної системи розміщується у всіх комп'ютерних системах корпоративної мережі для підвищення ефективності діагностування.

Основний розділ

Для підвищення достовірності антивірусного діагностування була запропонована мультиагентна антивірусна система, котра функціонує всередині корпоративної мережі [6]. Вона використовує визначену кількість агентів, які здійснюють антивірусне діагностування за допомогою набору сенсорів $A=\langle S_1, S_2, S_3, S_4, S_5, S_6\rangle$, де S_1 - сенсор сигнатурного аналізу; S_2 - сенсор контрольної суми; S_3 - сенсор евристичного аналізу; S_4 - сенсор поведінкового аналізу

[7]; S_5 - сенсор порівняльного аналізу шляхом застосування інтерфейсу програмування API і драйвера дискової підсистеми за допомогою IOS; S_6 - сенсор – «віртуальна приманка». Кожен агент містить набір ефекторів, які впливають на комп'ютерну систему з метою блокування підозрілих програм і подальшим сповіщенням інших агентів в мережі про інфікування, для того, щоб активувати виявлення підозрілих програм з подібною поведінкою. Агент містить процесор, який обробляє вхідні дані і визначає рівень присутності бота, як складової ботнет-мережі в КС. Функціонування процесу базується на використанні знань.

Метод виявлення ботнет-мереж на основі мультиагентної антивірусної системи

Процес діагностування розпочинається з побудови схематичної карти з'єднань КС деякої корпоративної мережі шляхом генерування відповідних записів в кожному антивірусному агенті мультиагентної системи. Всі агенти на основі цієї інформації спілкуються між собою.

Визначається ступінь присутності ботнет-мережі. Визначення базується на аналізі дій ботів в ситуації навмисної зміни типу підключення на ймовірно інфікованій комп'ютерній системі. Такий підхід здійснюється у разі недостатнього (низького) значення підозрілості програмного забезпеченням, але ця підозріла активність присутня в певній кількості КС корпоративної мережі.

Під час функціонування комп'ютерної системи антивірусне діагностування здійснюється за допомогою сенсорів в кожному агенті. Результати антивірусного діагностування аналізуються на предмет того, який з сенсорів спрацював, і який рівень підозрілості він продукував. Якщо спрацював сигнатурний сенсор або аналізатор контрольної суми чи API-сенсор, то результати інтерпретуються як 100% виявлення шкідливих програм. У цій ситуації виконується блокування відповідного програмного забезпечення та його подальше видалення.

В тих випадках, коли спрацювали сенсори евристичного S_3, поведінкового S_4 аналізу або сенсор «віртуальна приманка» S_6, то аналізуються рівні підозрілості R_{S_3}, R_{S_4} і R_{S_6}, і в разі подолання певного порогу n, $n \le \max(R_{S_3}, R_{S_4}, R_{S_6}) \le 100$, виконується блокування програмного забезпечення і його подальше видалення. Якщо вказаний поріг для прийняття остаточного рішення про присутність шкідливого програмного забезпечення в КС не подоланий, то він належать проміжку $m \le \max(R_{S_3}, R_{S_4}, R_{S_6}) < n$. Якщо значення належить проміжку $\max(R_{S_3}, R_{S_4}, R_{S_6}) < m$, то очікуються нові результати від сенсорів антивірусного агента. У всіх випадках інформація антивірусного агента про інфікування або підозрілу поведінку програмного забезпечення в КС повинна передаватись на інші агенти.

В основі розробленого методу лежить дослідження ситуації, коли результати виявлення антивірусними агентами ступеня присутності ШПЗ належать проміжку $m \le \max(R_{S_3}, R_{S_4}, R_{S_6}) < n$. У цьому випадку, антитивірусний агент КС запитує в інших агентів корпоративної мережі про аналогічні підозрілі поведінки деякого програмного забезпечення, яке схоже на ботнет-мережу. Якщо визначений агент отримує інформацію від одного або декількох агентів про аналогічну підозрілу поведінку певного програмного забезпечення, то ймовірно інфіковані комп'ютерні системи «помічаються» і будується нова карта мережі з врахуванням помічених КС. З множини «помічених» комп'ютерних систем обирається деяка КС для зміни типу мережного з'єднання (перепідключення) - спеціальні налаштування мережі, які перешкоджають функціонуванню мережі бота в комп'ютерній системі (змінена адреси DNS, нестандартний мережний порт, і т.д.). Вибір однієї комп'ютерної системи з «помічених» здійснюється експертною системою. Вона містить набір правил, які присутні в модулі «знання» кожного антивірусного агента. Ця КС повинні відповідати певним критеріям.

Для того, щоб обрати певну КС, необхідно проаналізувати особливості та властивості ймовірно інфікованих ботнет-мережею комп'ютерних систем. Для цього введемо поняття «відповідність» певної комп'ютерної системи. Таким чином, найбільш «відповідною» буде КС з найбільш актуальними антивірусними базами, з найвищою неперервною тривалістю роботи, операційною системою з найнижчим рівнем уразливості і кращим результатом антивірусного діагностування. Визначення «відповідності» комп'ютерної системи здійснюється з використанням системи нечіткого висновку, яка присутня в структурі агента. Кожен агент, ймовірно інфікованої КС, обчислює рівень його «відповідності», а потім взаємодіє з іншими агентами, щоб вибрати КС як найбільш «відповідну» для зміни типу підключення до мережі. Після перепідключення обраної КС, аналізуються дії бота на перепідключеній КС, на «помічених» комп'ютерних системах та інших КС корпоративної мережі; далі визначається рівень присутності ботнет-мережі.

Визначення наявності ботнет-мережі стало можливим завдяки тому, що при зміні типу підключення в деякій комп'ютерній системі, боти можуть проявити свою присутність (боти

можуть намагатися спілкуватися з іншими елементами ботнет-мережі, оновлювати списки активних ботів, переналаштувати з'єднання з урахуванням нових списків, і т. і.).

Важливим параметром для визначення комп'ютерної системи, котра буде перепідключатись, є її місце в топології корпоративної мережі. Якщо комп'ютерна система є об'єднуючим вузлом з сусідніми комп'ютерними системи в корпоративній мережі, який може бути сервером або брандмауером, то змінювати тип з'єднання цієї КС не можна.

Для визначення рівня присутності ботнет-мережі в КС потрібно проаналізувати дії ботнет-мережі після перепідключення до визначеної КС. Для цього всі прояви діляться на три категорії з відповідними рівнями, кожна з категорій повинна бути визначеною як: рівень прояву в перепідключеній КС, рівень прояву в ймовірно інфікованій КС і рівень прояву інших КС, що належать до корпоративної мережі, які ймовірно інфіковані. Для визначення можливої присутності ботнет-мережі в КС здійснюється оцінка рівня прояву для кожної з трьох категорій. Рівні прояву трьох категорій представлені у вигляді нечітких лінгвістичних змінних «рівень прояву ботнет-мережі» з трьома значеннями (« низький »,« середній », « високий ») .

Для формування функції належності для вхідної лінгвістичної змінної знаходимо для кожної дії, найбільш імовірний порт потрапляння шляхом ранжування з побудовою матриці переваги

$$S = |s_{ij}|, \text{ де } s_{ij} = \sum_{k=1}^{r} s_{ij}^{k} \cdot p_k / \sum_{k=1}^{r} s_{jk}^{k} \cdot p_k;\ s_{ji} = 1/s_{ij},\ s_{ii} = 1;\ i, j = \overline{1,m};, s_{ij} = s_i / s_j,\ 0 < s_{ij} < \infty. \quad (1)$$

Потім визначаємо для матриці S власний вектор $\Pi = (\pi_1, ..., \pi_m)$, що відповідає максимальному додатному кореню λ характеристичного полінома $|S - \lambda \cdot E| = 0$; $S \cdot \Pi = \lambda \cdot \Pi$, де E – одинична матриця. Компоненти вектора Π ($\sum \pi_i = 1$) ототожнюються з оцінкою $\mu_{X\,p}(x_i, y_j)$. В результаті одержуємо матрицю відношення $V_p = |x_i, y_j|$, у якій кожному відношенню (x_i, y_j) відповідає значення $0 \le \pi \le 1$. Наступним кроком методу є побудова оптимізованої матриці $V_p^* = |x_i, y_j|$ з відношень (x_i, y_j) із значеннями $\pi_{\max}$ $(0 \le \pi_{\max} \le 1)$ та побудова нормованої кривої функції належності $\mu_{X\,p}(R)$ вхідної змінної.

Задача визначення функції належності для вхідної змінної «рівня прояву ботнет-мережі» у перепідключеній КС розглядається як задача ранжування для кожної з функцій проникнення через системні порти з врахуванням ознак небезпеки. Задача визначення функцій належності для вхідних змінних «рівня прояву ботнет-мережі» у «помічених» КС і для решти (не інфікованих) комп'ютерних систем розглядаються як визначення рівня прояву ботнет-мережі. Необхідно враховувати небезпеку дій ботнет-мережі, кількість комп'ютерних систем і місце прояву ботнет-мережі.

Приймемо ω_j^i як ознаку прояву, при чому $\omega_j^i = 1$, якщо прояв відбувся та $\omega_j^i = 0$, якщо прояву не було; $j = \overline{1,n}$, $i = \overline{1,\gamma}$, де γ - число проявів ботів, k - число комп'ютерних систем в корпоративній мережі.

Обчислимо d_i - число ненульових проявів d_i^j в кожній комп'ютерній системі і середнє значення ω_i з ненульовим проявом ω_i^j (див. рис. 1). Якщо кількість ненульових проявів $d_i \neq 0$, то вона обчислюється як:

$$\omega_i = \sum_{j=1}^{n} \omega_j^i / d_i, \quad (2)$$

$$d = \sum_{i=1}^{\gamma} d_i \le \gamma \cdot k. \quad (3)$$

Унормовуємо ω_i, $i = \overline{1,\gamma}$, так що $\omega_1 + \omega_2 + ... + \omega_\gamma = 1$. Рівень прояву присутності ботнет-мережі в «помічених» комп'ютерних системах визначимо як:

$$P_d(d_1, d_2, ..., d_\gamma) = \frac{d!}{d_1! d_2! ... d_\gamma!} \cdot \omega_1^{d_1} \cdot \omega_2^{d_2} \cdot .... \cdot \omega_\gamma^{d_\gamma}. \quad (4)$$

Нехай k', $k' \le k$ - число «помічених» комп'ютерних систем як інфіковані. Тоді повинні бути обчислені середні арифметичні $\bar{\omega}$ для відповідного ω^j. Після цього число P_d визначається й інтерпретується як ступінь прояву ботнет-мережі в «помічених» комп'ютерних системах.

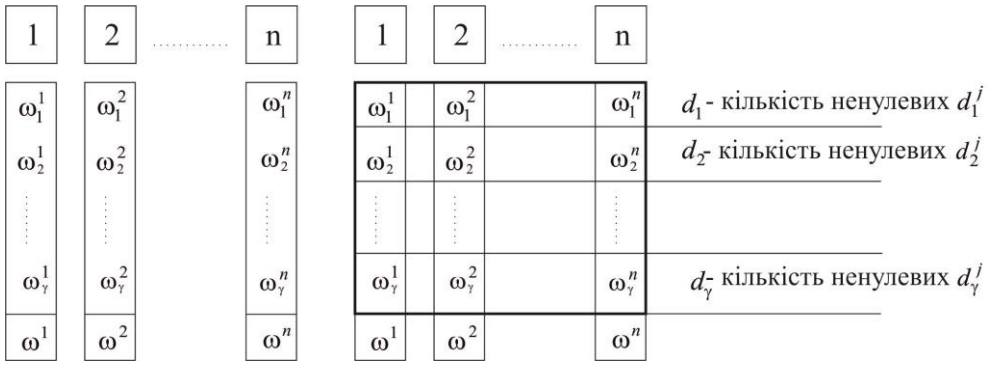
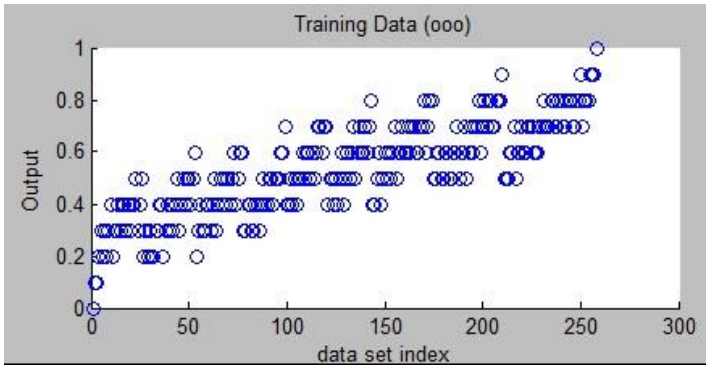


Рис. 1. Розрахунок ненульових проявів ботнет-мереж

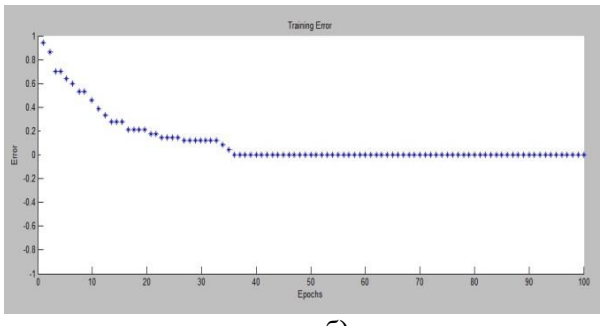
Отримання результатів рівня присутності ботнет-мережі в комп'ютерних системах здійснимо системою нечіткого висновку (FIS) на основі алгоритмів Мамдані і Сугено [6]. Система використовує рівні прояву для трьох категорій КС (перепідключених, «помічених», та інших комп'ютерних систем мережі).

Також була розроблена система, здатна зробити висновок про ступінь присутності ботнет-мереж в комп'ютерних системах з використанням адаптивної системи нейро-нечіткого висновку (ANFIS). Ці нейронні мережі на основі системи нечіткого висновку Такагі-Сугено [7], інтегрують нейронні мережі і методи нечіткої логіки [8].

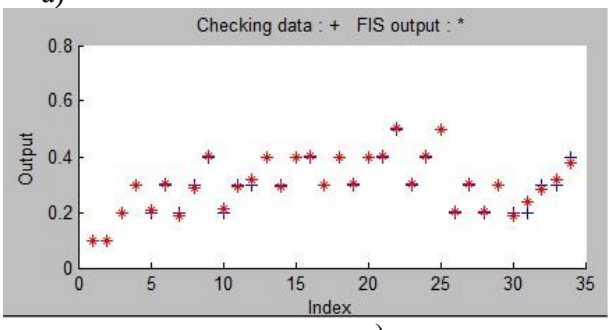
Розроблений метод використовує систему нечіткого висновку першого порядку типу Сугено з 3-входами і 1-виходом, якими є рівні прояву в перепідключеній КС, ймовірно інфікованих КС і інших комп'ютерних систем, що належать мережі (що, ймовірно, не були інфіковані). Кожен вхід має 3 гаусові функції належності і вихід має лінійну функцію належності, яка вказує ступінь присутності ботнет-мереж в комп'ютерних системах. Засобами ANFIS було згенеровано 27 правил; використано метод grid partition. Для навчання моделі був використано гібридний алгоритм. Підготовка даних представлена на рисунку 2а. Помилка навчання за 100 епох склала 0,012132. Процес навчання ANFIS показано на рисунку 2б. Перевірка даних представлена на рисунку 2в. Середня помилка перевірки склала 0,003588.



а)



б)



в)

Рис 2. Робота ANFIS системи:
а) підготовка даних; б) процес навчання; в) перевірка даних

Експерименти та дослідження

Для перевірки розробленого методу було створено програмне забезпечення та проведені відповідні експерименти.

Розглянемо приклад антивірусного діагностування КС на наявність бот як складової ботнет. З цією метою було згенеровано 60 програм з властивостями ботнет-мереж (Agobot, SDBot та GT-Bot). У ході експерименту комп'ютерні системи в мережі були інфіковані тільки одним ботом з відповідного сімейства.

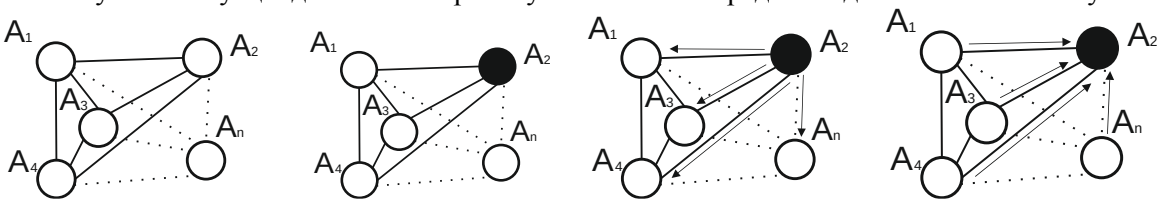
Розглянемо процес діагностування КС на наявність однієї з ботнет-мереж.

Нехай маємо мультиагентну систему B, що складається з множини агентів A, $A = \{A_1, ..., A_i\}$ (рис. 3а). В процесі її функціонування відбувається комунікація між агентами для координування дій в поточний момент часу. Кожен агент A_i надсилає діагностичну інформацію усім активним агентам корпоративної мережі.

Згідно розробленого виконується аналіз результатів діагностування, а саме належність отриманих результатів до визначених проміжків, $n \le \max(R_{Si}) \le 100$, $m \le \max(R_{Si}) < n$ або $\max(R_{Si}) < m$. В даній роботі прийнято наступні значення порогів n=80, m=40.

Нехай сенсор S_4 агента A_2 в процесі локального антивірусного діагностування видав результат поведінкового аналізатора R_{S4} з рівнем, що складає 56% (рис. 3б). Згідно методу агент виконує розсилання повідомлень T активним агентам. Повідомлення містить результати діагностування та інформацію про підозрілий програмний об'єкт. Кожен агент здійснює антивірусне діагностування на предмет наявності аналогічно підозрілого об'єкта в КС. Припустимо, що агенти A_3, A_6, A_{11}, A_{15}, A_{22}, A_{31} засобами поведінкового сенсору виявили схожу шкідливу поведінку у КС, в яких розміщені вказані агенти з результатами відповідно $R_{S4}^{A_3} = 48\%$, $R_{S4}^{A_6} = 46\%$, $R_{S4}^{A_{11}} = 58\%$, $R_{S4}^{A_{15}} = 54\%$, $R_{S4}^{A_{22}} = 60\%$, $R_{S4}^{A_{31}} = 46\%$.

Наступним кроком згідно методу пропонується виконати змінити тип підключення однієї КС до корпоративної мережі, тобто створити такі умови функціонування КС, згідно яких ймовірно присутній бот не міг здійснювати обмін інформацією з іншими ботами ботнет (рисунок 3в). З іншого боку така ситуація дозволить спровокувати ботів на предмет відновлення їх зв'язку.



а) б) в) г)

Рис. 3. Комунікація агентів

Метод передбачає визначення найбільш «відповідної» КС до вказаних в таблиці 1 критеріїв.

Таблиця 1. Лінгвістичні змінні, терми та їх значення для визначення найбільш «відповідної» КС для перепідключення

№	Назви лінгвістичних змінних	Терми лінгвістичних змінних	Значення
1	Актуальність антивірусних баз	Неактуальні	Більше 7 днів
		Дещо актуальні	Від 1 дня до тижня
		Актуальні	В межах дня
2	Тривалість роботи КС	Коротка	Більше 6 годин
		Середня	До 6 годин
		Довга	Впродовж 1 години
3	Вразливість операційної системи	Висока	Windows XP
		Вище середньої	Windows Vista
		Середня	Windows 7
		Вище низької	Windows Server 2003
		Низька	Windows Server 2008
4	Результати антивірусного діагностування	Низький	$\max(R_{S_3}, R_{S_4}, R_{S_6}) < 40$
		Середній	$40 \le \max(R_{S_3}, R_{S_4}, R_{S_6}) < 80$
		Високий	$80 \le \max(R_{S_3}, R_{S_4}, R_{S_6}) \le 100$

Інформація, що передається агентами для визначення найбільш «відповідної» КС для перепідключення подана в таблиці 2.

Таблиця 2. Інформація, що передається агентами для визначення найбільш «відповідної» КС для перепідключення

КС з агентом A_i	Актуальність антивірусних баз	Тривалість Безперервної роботи	Тип операційної системи	Результат антивірусного діагностування
A_3	1	8	Windows XP	48
A_6	2	6	Windows 7	52
A_{11}	2	44	Windows 2003	58
A_{15}	7	12	Windows XP	54
A_{22}	4	3	Windows Vista	55
A_{31}	1	55	Windows 2008	46

Визначення рівня «відповідності» засобами системи нечіткого логічного висновку (на прикладі використання алгоритму Мамдані) представлено на рисунку 4.

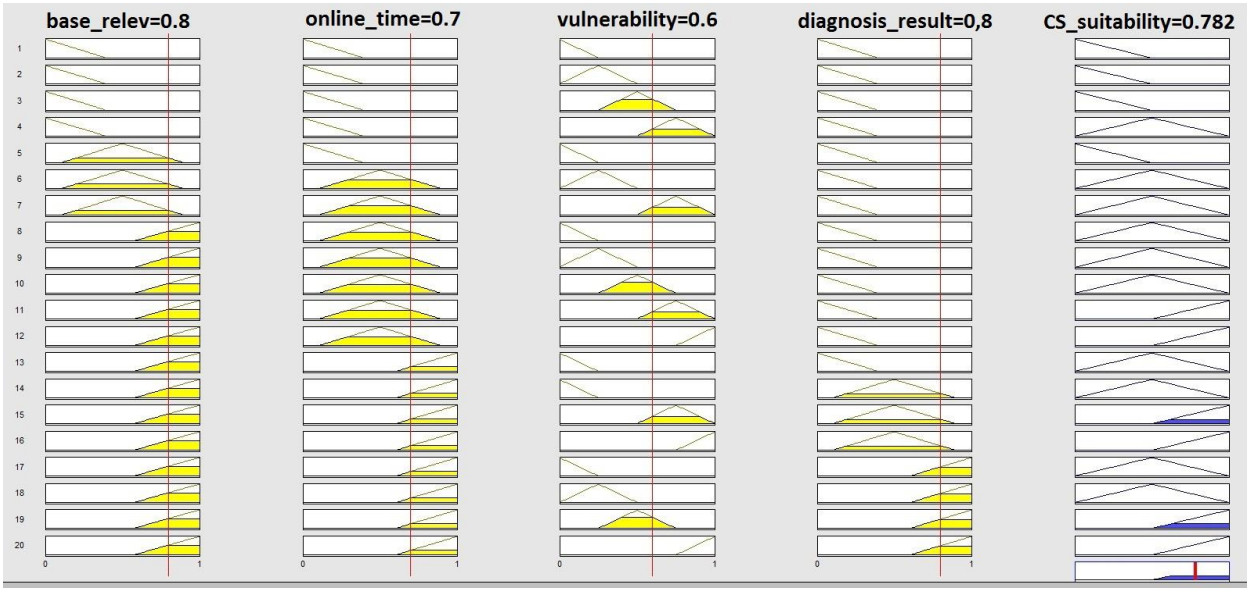


Рис. 4. Результати роботи системи нечіткого логічного висновку щодо для визначення КС, яка підлягає перепідключенню

Найвищий рівень «відповідності» продемонструвала КС з операційною системою Windows 2003. Проте оскільки дана КС є сервером, її «перепідключати» не можна. Тому такою КС обрано вузол $КС_6$.

Кожен агент після оцінки власної «відповідності» розсилає результати кожному агенту (рис. 3г). Таким чином, всередині мультиагентної системи формується масив значень, з яких обирається найбільше.

Приймемо комп'ютерну систему, що підлягає зміні типу підключення в мережі, що містить агент A_6.

З моменту зміни типу підключення усі агенти МАС повинні проінформовані про необхідність здійснення моніторингу з метою виявлення проявів ботнет.

Далі метод передбачає відслідковування подій в трьох категорія КС з метою виявлення провів ботнет-мереж: «перепідключеній» КС, «помічених» як ймовірно інфікованих КС та решти КС корпоративної мережі.

Такий моніторинг відносно ймовірно шкідливого ПЗ відбувається протягом 24 годин.

Приклад сімейств ботів та їх проявів подано в таблиці 3.

Згідно таблиці 3 відомо 22 проявив (кількість проявів може змінюватися в процесі досліджень поведінки ботнет-мереж). Тоді для ймовірно інфікованих КС побудуємо таблицю проявів (табл.4).

Також здійснимо розрахунок згідно формул (2)-(3) показники проявів.

Таблиця 3 Сімейства ботів та можливі їх прояви

Сімейства ботів / Прояви ботів	ago	DSNX	evil	G-SyS	sd	Spy
Зміна C&C сервера	1	1	-	1	1	1
Створення/керування клонами	-	1	-	1	1	-
Здійснення атак клонами	-	1	-	-	-	-
Створення шпигунського ПЗ	-	-	-	1	1	-
Знищення процесу	1	-	-	1		1
Відкриття/виконання файлів	1	1	-	1	1	1
Виконання запису логу натискання клавіш	-	1	-	-	-	1
Створення директорій	-	-	-	-	-	1
Знищення файлів/директорій	-	1	-	-	-	1
Перегляд директорій	-	1	-	-	-	1
Переміщення файлів/директорій	-	-	-	-	-	1
DCC надсилання файлів	-	1	-	-	-	1
Функціонування хибного http-сервера	-	-	-	-	-	1
Створення перенаправляючих портів	1	1	-	1	1	1
Створення хибного проксі-сервера	1	-	-	-	-	-
Завантаження файлів	1	1	-	1	1	1
DNS розширення	1	-	-	1	1	
UDP/ping «флуд»	1	-	-	1	1	
Інший DDoS «флуд»	1	-	-	1		1
Сканування / розповсюдження	1	1	-	1	1	1
Спам	1	-	-	-	-	-
Відвідування URL	1	-	-	1	1	-

Таблиця 4. Прояви ботнет в «помічених» КС

№ КС / № прояву	$КС_3$	$КС_{11}$	$КС_{15}$	$КС_{22}$	$КС_{31}$	Середнє арифметичне ω_i	Унормовані значення $\overline{\omega_i}$	Кількість ненульових проявів d_i
1	1	1	1	1	1	1	0,128205	5
2	0	0	0	0	1	0.2	0,025641	1
3	1	0	0	0	0	0.2	0,025641	1
4	0	1	1	1	1	0.8	0,102564	4
5	1	1	1	1	0	0.8	0,102564	4
6	0	0	0	0	1	0.2	0,025641	1
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	1	0.2	0,025641	1
10	1	1	1	0	0	0.6	0,076923	3
11	0	0	0	0	0	0.	0	0
12	1	1	1	1	1	1	0,128205	5
13	0	1	1	1	1	0.8	0,102564	4
14	0	0	0	0	1	0.2	0,025641	1
15	1	1	1	1	1	1	0,128205	5
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	1	0	1	1	1	0.8	0,102564	4
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0

Рівень прояву присутності ботнет-мережі в «помічених» комп'ютерних системах визначимо за формулою (4):

$$P_d = \frac{39!}{5!\cdot 1!\cdot 1!\cdot 4!\cdot 4!\cdot 1!\cdot 0!\cdot 0!\cdot 1!\cdot 3!\cdot 0!\cdot 5!\cdot 4!\cdot 1!\cdot 5!\cdot 0!\cdot 0!\cdot 0!\cdot 0!\cdot 4!\cdot 0!\cdot 0!} \cdot 0{,}128205^5 \cdot 0{,}025641^1 \cdot 0{,}025641^1 \cdot 0{,}102564^4 \cdot$$

$$\cdot 0{,}102564^4 \cdot 0{,}025641^1 \cdot 0{,}025641^1 \cdot 0{,}076923^3 \cdot 0{,}128205^5 \cdot 0{,}102564^4 \cdot 0{,}025641^1 \cdot 0{,}128205^5 \cdot 0{,}102564^4 = 0.7311$$

Рівень прояву присутності ботнет-мережі в комп'ютерних системах, що ймовірно не є інфікованими і належать до корпоративної мережі, розраховується аналогічно.

Таким чином, маючи рівні проявів для трьох категорій КС («перепідключеної» КС, «помічених» як ймовірно інфікованих та решти КС мережі), здійснюється остаточний висновок щодо присутності ботнет-мережі. Для цього використовується система нечіткого логічного висновку, на вхід якої подаються значення рівнів трьох категорій.

Лінгвістичні змінні, терми та їх значення для визначення найбільш «відповідної» КС для перепідключення представлено в таблиці 5.

Таблиця 5. Лінгвістичні змінні, терми та їх значення для визначення найбільш «відповідної» КС для перепідключення

№	Назви лінгвістичних змінних	Терми лінгвістичних змінних	Можливі прояви
1	Рівень прояву перепідключеної КС	Високий	Зміна C&C сервера, UDP/ping «флуд»
		Середній	Сканування / розповсюдження
		Низький	Створення директорій
2	Рівень прояву ймовірно інфікованих	Високий	Зміна C&C сервера, здійснення атак клонами, DNS розширення, DDoS
		Середній	Створення директорій, виконання запису логу натискання клавіш
		Низький	Створення директорій, завантаження файлів
3	Рівень прояву в інших КС мережі	Високий	Зміна C&C сервера, DDoS
		Середній	Функціонування хибного http-сервера, створення перенаправляючих портів
		Низький	Створення директорій, завантаження файлів

Приклад встановлення остаточного висновку щодо присутності ботнет-мережі представлено на рисунку 5.

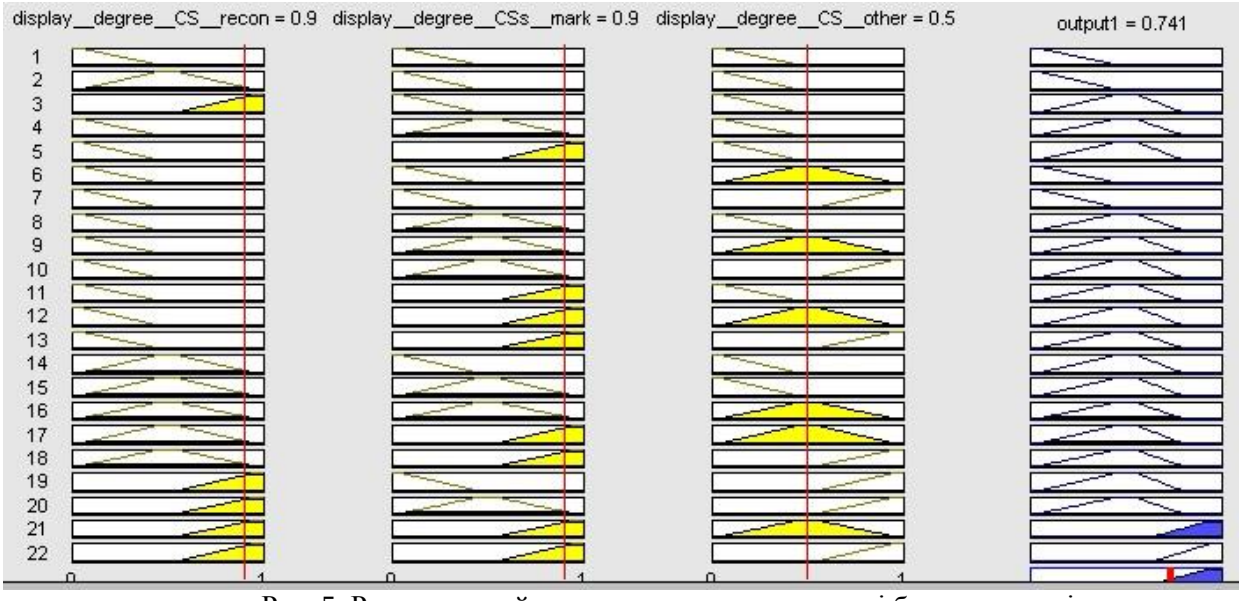


Рис. 5. Результуючий висновок щодо присутності ботнет-мережі

В загальному дослідження проводилось на протязі 8-ми місяців із залученням алгоритмів Mamdani, Sugeno, а також ANFIS-системи.

В результаті досліджень отримано наступні результати: адаптивна нейро-нечітка система демонструє кращі результати виявлення ботнет-мереж в порівнянні з нечітким підходом (використання Mamdani – 76,7%, Sugeno – 81,6%, ANFIS – 85,5%).

Результати експерименту доводять ефективність мультиагентного методу виявлення ботнет-мереж.

Висновки

Розроблено новий метод діагностування КС на наявність ботнет-мереж на основі мультиагентних систем з використанням нечіткої логіки та нейро-нечітких систем. Виявлення здійснюється з урахуванням проявів ботнет-мережі в декількох комп'ютерних системах, наявних в мережі. Розроблена адаптивна нейро-нечітка система, яка робить висновок про наявність ботнет-мереж в комп'ютерній системі. Використання зміни типу підключення дозволяє спровокувати дії ботів, як на ізольованій КС, так і на активних КС, що спрямовані на відновлення з'єднання між ботами. Обмін діагностичною інформацією дозволяє накопичувати дані про поведінку ПЗ у КС корпоративної мережі відслідковувати схожі дії ШПЗ. Для отримання висновку про рівень присутності ботнет-мережі в комп'ютерних системах використано нечіткий логічний висновок.

Застосування запропонованого методу процесі антивірусного діагностування продемонструвало високу ефективність виявлення ботнет-мереж, яка складає понад 85%.

Література

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.aspxt.
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. 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, Springer,2012, Volume 291, pp. 171-180.
7. 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.

Рецензент: Бедратюк Л.П., зав. кафедрою програмної інженерії Хмельницького національного університету, д.ф.-м..н., доцент.

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

ПРОЦЕСС ДИАГНОСТИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ НА НАЛИЧИЕ БОТНЕТ-СЕТЕЙ НА ОСНОВЕ МУЛЬТИАГЕНТНЫХ ТЕХНОЛОГИЙ

В работе предложен новый метод диагностирования компьютерных систем на наличие ботнет-сетей с использованием мультиагентных систем. Выявление осуществляется на основе проявлений ботов в нескольких компьютерных системах, принадлежащих корпоративной сети.

Ключевые слова: антивирусное диагностирование компьютерных систем, нейро-нечеткие системы, worm-вирусы, ботнет-сети, бот.

O.Savenko, S. Lysenko, A. Kryshchuk

COMPUTER SYSTEM DIAGNOSIS PROCESS FOR BOTNET DETECTION ON THE BASE OF THE MULTY-AGENT TECHNOLOGIES

The paper presents a new method for computer systems diagnosis for the botnet presence based on the multi-agent systems. Detection is based on bots' demonstrations in several computer systems that belong to a corporate area network.

Keywords: antivirus computer system diagnosis, neuro-fuzzy systems, worm-viruses, botnet, bot.