УДК 004.492.3

А.Ф. КРИЩУК
Хмельницький національний університет

МУЛЬТИАГЕНТНИЙ МЕТОД ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ БОТНЕТ-МЕРЕЖ

В роботі запропонований новий метод діагностування комп'ютерних систем на наявність ботнет-мереж з використанням мультиагентних систем. 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.

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

A. F. KRYSHCHUK
Khmelnytskyi national university

MULTIAGENT TECHNIQUE FOR COMPUTER SYSTEM BOTNET DIAGNOSIS

Abstract. In the article the new multiagent technique for computer system botnet diagnosis is proposed. The botnet detection is performed via its activities in the corporate area network. With the usage of fuzzy logic, the analysis of the botnets' actions demonstrations in the situation of the intentionally computer system reconnection is suggested. The detection is suggested in the situations of priori uncertainty of the botnet presence in the corporate area network with taking into account the botnet demonstrations in the several computer systems available in the network.

Keywords: antivirus diagnosis, efficiency of antivirus diagnosis, Trojans, worm-viruses, botnet, polymorph code.

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 систем, 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 [5]. 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; 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.

Мультиагентний метод діагностування комп'ютерних систем на наявність ботнет-мереж. 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 ») (рис. 1).

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.

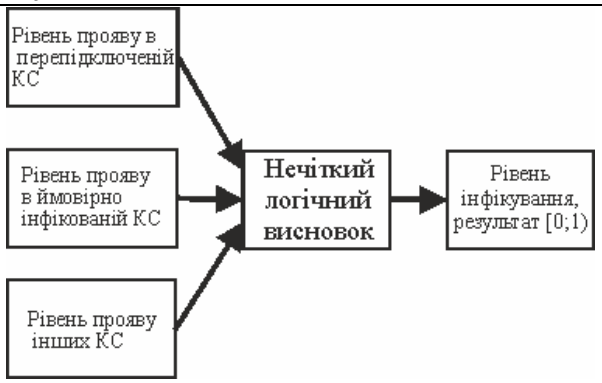

Рис. 1. Визначення рівня інфікування

Приймемо $\omega_j^i, 0 \le \omega_j^i \le 1$ – одна з ознак прояву, $j = \overline{1,n}$, $i = \overline{1,\gamma}$, де γ – число проявів ботів, k – число комп'ютерних систем в корпоративній мережі. Оцінка кожної КС може бути виконана за формулою:

$$\omega^1 = \sum_{i=1}^{q} \alpha_i^1 \omega_i^1 / \gamma \,,\ \omega^2 = \sum_{i=1}^{q} \alpha_i^2 \omega_i^1 / \gamma \,, \ldots,\ \omega^j = \sum_{i=1}^{q} \alpha_i^\gamma \omega_i^j / \gamma \,, \tag{1}$$

де α_i – коефіцієнти небезпеки деяких проявів, $\alpha_1 + \alpha_2 + \ldots + \alpha_q = 1$, $0 \le \omega^i \le 1$.

Таким чином, якщо обране деяке порогове значення для кожної КС з оцінкою ω^j, наприклад $\tau \in (0;1]$, то можна обрати і деякі групи g «підозрілих» комп'ютерних систем, якщо $\omega^j > \tau$. Далі обчислюється d_i – число ненульових проявів d_i^j в кожній комп'ютерній системі і середнє значення ω_i з ненульовим проявом ω_i^j. Якщо кількість ненульових проявів $d_i \ne 0$, то вона обчислюється як:

$$\omega_i = \sum_{j=1}^{n} \omega_j^i / d_i \,,\ \ d = \sum_{i=1}^{q} d_i \le \gamma \cdot k \,. \tag{2}$$

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

$$P_d(d_1, d_2, \ldots, d_\gamma) = \frac{d!}{d_1! d_2! \ldots d_\gamma!} \cdot \omega_1^{d_1} \cdot \omega_2^{d_2} \cdot \ldots \cdot \omega_\gamma^{d_\gamma} \,. \tag{3}$$

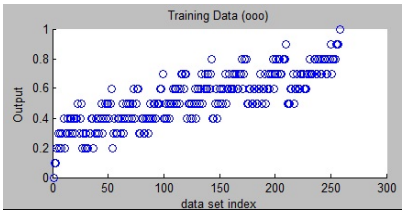

Рис. 2. Підготовка даних

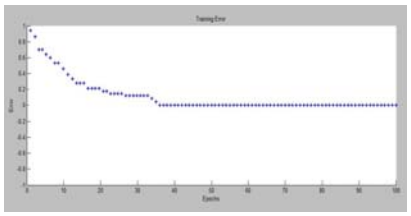

Рис. 3. Процес навчання ANFIS

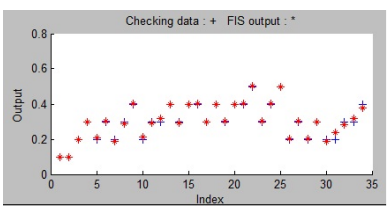

Рис. 4. Перевірка даних

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

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 2. Помилка навчання за 100 епох склала 0,012132. Процес навчання ANFIS показано на рисунку 3. Перевірка даних представлена на рисунку 4. Середня помилка перевірки склала 0,003588.

Таким чином, використання нечіткої логіки та нейро-нечітких систем дозволяє оцінити ступінь присутності ботнет-мереж в комп'ютерних системах шляхом визначення рівня їх проявів

Експерименти та дослідження

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

Для реалізації експерименту 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. Дослідження проводилось на протязі 8-и місяців і отримані наступні результати: адаптивна нейро-нечітка система демонструє кращі результати виявлення ботнет-мереж в порівнянні з нечітким підходом (без використання методу – 74,5%, з використанням Mamdani – 76,7%, з використанням Sugeno – 81,6%, з використанням ANFIS – 85,5%).

Результати експерименту доводять ефективність мультиагентного методу виявлення ботнет-мереж. Підвищення ефективності діагностування складає близько 7–10%.

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 підвищення ефективності виявлення ботнет-мереж, приріст ефективності складає близько 7–10% у порівнянні з діагностуванням відокремленої КС.

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.

5. Proactive/Retrospective test. [Електронний ресурс]. – Anti-Virus comparative. – Режим доступу : http://av-comparatives.org.

6. 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.

7. 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.

8. Гошко С.В. Энциклопедия по защите от вирусов / Гошко С.В. – М. : СОЛОН-Пресс, 2005. – 352 с.

References

1. Tim Rains "Operating System Infection Rates: Application Vulnerabilities & Exploits Trend Up, Increase OS Infection Rate" 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. TwycrossJ. Griffin, J. and Norman A. "Virus throttling", Virus Bulletin, 2009.

3. "VB100 Results Summary". Anti-Virus comparative http://www.virusbtn.com/vb100/archive/summary.

4. AV Comparatives laboratories http://www.av-comparatives.org.

5. Proactive/Retrospective test. Anti-Virus comparative. http://av-comparatives.org.

6. Savenko O., Lysenko S. "The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode," 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.

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

8. Goshko S. Encyclopedia of protection against viruses SOLON-Pres, 2005. (in Russian)

Рецензія/Peer review : 4.5.2013 р. Надрукована/Printed :19.6.2013 р.
Рецензент: Поморова О.В.