Joint Conference on Neural Networks, – 2006, – P. 3955-3962.

5. Сайт розробників бібліотеки OpenCV [Електронний ресурс]: Бібліотека для маркування зв'язних областей cvBlobsLib – Режим доступу: http://opencv.willowgarage.com/wiki/cvBlobsLib.

6. J. C. Hsien, U.S. Liou, S.Y.Chen. Road Sign Detection and Recognition Using Hidden Markov Model / Asian Journal of Health and Information Sciences. – 2006 - Vol. 1, No. 1. - P. 85-100.

7. «Выглядит похоже». Как работает перцептивный хэш [Електронний ресурс] : Режим доступу: http://habrahabr.ru/post/120562/

References

1. C. Bahlmann, Y. Zhu, V. Ramesh, M. Pellkofer. "A system for traffic sign detection, tracking, and recognition using color, shape, and motion information." Intelligent Vehicles Symposium. – 2005. – Proceedings. IEEE, June 2005. pp. 255–260,

2. H. Ohara, I. Nishikawa, S. Miki, N. Yabuki. "Detection and recognition of road signs using simple layered neural networks" Neural Information Processing, 2002. – ICONIP '02. Proceedings of the 9th International Conference on. – 2 vol.2, Nov. 2002. pp. 626–630.

3. Paclk P., Novovicov J. "Road sign classification without color information." In Proceedings of the 6th Conference of Advanced School of Imaging and Computing. – 2000.

4. Y. Y. Nguwi, A. Z. Kouzani. Automatic road sign recognition using neural networks [Text] / International Joint Conference on Neural Networks, – 2006, – P. 3955-3962.

5. Website Developer Library OpenCV [Електронний ресурс] : Library for labeling of connected regions cvBlobsLib Web Resource: http://opencv.willowgarage.com/wiki/cvBlobsLib

6. Road Sign Detection and Recognition Using Hidden Markov Model / J. C. Hsien, U.S. Liou, S.Y.Chen // Asian Journal of Health and Information Sciences. – 2006 - Vol. 1, No. 1. - P. 85-100.

7. "Looks like." How does the perceptual hash. Web Resource: http://habrahabr.ru/post/120562/

Рецензія/Peer review : 20.10.2013 р. Надрукована/Printed :24.11.2013 р.
Рецензент: Николайчук Я. М., д.т.н., проф. завідувач кафедри Спеціалізованих комп'ютерних систем Тернопільського національного економічного університету

УДК 004.492.3

А.Ф. КРИЩУК
Хмельницький національний університет

МОДЕЛЬ ПРОЦЕСУ ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ БОТНЕТ-МЕРЕЖ

В роботі запропоновано нову модель процесу діагностування комп'ютерних систем на наявність ботнет-мереж з використанням мультиагентних систем. Кожен агент мультиагентної системи включає в себе набір сенсорів, які виконують антивірусне діагностування.

Процес діагностування складається з чотирьох підпроцесів: моніторинг подій в кожній комп'ютерній системі корпоративної мережі; сканування комп'ютерної системи на наявність шкідливого програмного забезпечення, реалізація зв'язків між агентами мультиагентних систем; обробка інформації, отриманої від сенсорів, щоб зробити висновок про наявність ботнет-мережі в корпоративній мережі.

Ключові слова: бот, ботнет-мережа, антивірусне діагностування, модель процесу антивірусного діагностування, модель антивірусного агента, модель мультиагентної системи, нечітка логіка, експертна система.

A. F. KRYSHCHUK
Khmelnytskyi national university

MODEL OF THE COMPUTER SYSTEM DIAGNOSIS PROCESS FOR BOTNET PRESENCE

Abstract. The new model of the computer system diagnosing process for botnet presence in the corporate area network is proposed. It is based on the use of multi-agent system. The new botnet detection technique based on multi-agent system with the use of fuzzy logic is proposed. The detection is performed 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. Fuzzy expert system for making conclusion about botnet presence degree in computer systems is developed.

Keywords: bot, botnet, antiviral diagnosis, model of antiviral diagnosis process, antiviral agent model, multi-agent system model, fuzzy logic, expert system.

Вступ

З ростом складності ботнет-мереж і високого рівня навичок та організованості зловмисників у кіберпростору знижується рівень безпеки та конфіденційності інформації в глобальній мережі Інтернет. З часом все складніше діагностувати комп'ютерні системи на наявність ботнет-мереж. Дуже великі розміри ботнет-мереж дозволяють відійти від загальноприйнятої клієнт-серверної структури, що дозволяє керувати окремими ботами, щоб виконувати різні типи атак за допомогою всієї ботнет-мережі.

Із створенням нових та вдосконаленням існуючих ботнет-мереж зловмисники створюють нові проблеми для інтернет-спільноти. Захист від вторгнення і визначення місця розташування зловмисника є досить складним завданням в силу різних фактів: 1) механізм, який використовується в побудові та підтримці ботнет-мереж і подальшому виконанні можливих атак є незалежним один від одного; 2) всі «боти» у ботнет-мережі є джерелами атак; 3) ботнет-мережі залишаються в стані спокою, поки не будуть задіяні для здійснення конкретної атаки.

Особливістю ботнет-мереж є використання спеціалізованих команд і контрольованих каналів взаємодії, які забезпечують оновлення функціональних частин ботів. Деякі ботнет-мережі пов'язані з незаконною грошовою діяльністю [1-2].

Існує багато моделей і методик для виявлення ботнет-мереж. Ці методи можна розділити на методи на основі мережних приманок і на основі пасивного моніторингу трафіку.

«Honeynet» є потужним інструментом для розуміння технології і характеристик ботнет-мереж, та відстеження поведінки ботнет-мереж. Це не дуже ефективно для виявлення ботнет-мережі.

Пасивний моніторинг трафіку. Базується на створенні точок пасивного контролю в реальному інтернет-трафіку і для виявлення та вилучення пакетів пов'язаних з діяльністю ботнет-мереж [3].

Поведінкове діагностування: методи, які базуються на поведінці ШПЗ можуть бути додатково класифіковані як сигнатурні і аномальні.

Сигнатурне діагностування: основний недолік діагностування з використанням сигнатурного аналізу в тому, що вони обмежуються тільки виявлення відомих ботнет-мереж.

Діагностування з пошуком аномалій: цей алгоритм не вимагає попередніх даних про ботнет-мережі і має підвищений рівень помилкових і хибних спрацювань.

Діагностування на основі «DNS»: гібрид поведінкового методу та методу аналізу даних, що здійснюється над «DNS» трафіком. Основним недоліком такого підходу є висока тривалість обробки мережевого трафіку, та великий об'єм даних при здійсненні діагностування [4].

Постановка задачі

Тому актуальним завданням є розробка нової моделі процесу діагностування комп'ютерних систем (КС) на наявність ботнет-мереж в корпоративній мережі, що дозволяє створювати більш досконалі методи для виявлення нових 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

Метою дослідження є процес діагностування комп'ютерних систем на наявність ботів як частини ботнет-мереж. Саме тому важливим завданням є розробка моделі процесу діагностування, яка повинна включати можливість відображення особливостей моделі ботнет-мереж [5].

Запропоновано процес антивірусного діагностування присутності ботнет-мереж в комп'ютерній системі, яка належить до корпоративну мережу (CAN) виконується. Процес діагностування базується на використанні мультиагентної системи (МАС). Кожен агент МАС включає в себе набір сенсорів, які виконують антивірусне діагностування.

Розіб'ємо процес діагностування на чотири підпроцеси: моніторинг подій в кожній комп'ютерній системі корпоративної мережі; сканування комп'ютерної системи на наявність ШПЗ, реалізація зв'язків між агентами мультиагентних систем; обробка інформації, отриманої від сенсорів, щоб зробити висновок про наявність ботнет-мережі в корпоративній мережі.

Моніторинг комп'ютерних систем здійснюється із запуском комп'ютерної системи. Процедура сканування комп'ютерної системи здійснюється на вимогу користувача або в заданий час.

Представимо модель процесу діагностування у вигляді кортежу

$$D =< \beta, \psi, \sigma, \theta >, \tag{1}$$

де β – процес моніторингу, ψ – процес сканування комп'ютерних систем, σ – процес комунікації, θ – обробка інформації від сенсорів з подальшим здійсненням висновку про можливу наявність бота в комп'ютерній системі.

На основі моделі процесу діагностування представлена формалізована схема процесу діагностування комп'ютерних систем на наявність бота, яка зображена на рис.1.

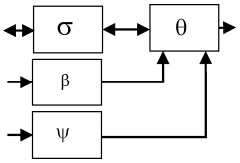

Рис. 1. Формалізована схема діагностування комп'ютерних систем на наявність ботнет-мереж

Мультиагентна система містить множину агентів, які використовуються для антивірусного діагностування. Також мультиагентна система виконує функції зв'язку для координації дій агента в поточний момент, і для його кооперування (обмін інформацією).

Для того, щоб досягти своїх цілей агенти об'єднані в в групи і працюють разом, збираючи і ділячись своїми знаннями і можливостями один одного.

Зобразимо модель мультиагентної системи у вигляді кортежу:

$$B =< H, A, L, O >, \tag{2}$$

де H – множина станів корпоративної мережі; $A = \{A_1, ..., A_i\}$ – множина агентів як частини антивірусної мультиагентної системи; $L = \{L_1, ..., L_i\}$ – множина станів агента; $O : H \times L_1, ..., L_i \to H$ – функція, що описує

реакції агентів на можливі дії мережі.

Розглянемо агент, як систему, яка функціонує в комп'ютерній системі і є частиною антивірусної МАС. Агент може взаємодіяти з іншими агентами, щоб здійснення раціональних автономних дій для досягнення деяких цілей.

Беручи до уваги функції агента представимо модель агента як кортеж:

$$A =< P, I, L, C, \rho, \mu >, \tag{3}$$

де P – процесор, який робить висновок про можливе інфікування комп'ютерної системи ботом на основі отриманих даних і знань агента; I – множина станів агента; L – множина дій агента, $L = \{L_1, ..., L_i\}$, де $L_i = \{l_1, ..., l_i\}$ – множина дій ефекторів, які впливають на об'єкти діагностування; $C =< Z, T, R, V >$ – блок зв'язку, який виконує обмін інформацією між агентами, де Z – системна інформація, T – множина результатів агента A_i (інформації, яка приходить від інших агентів), R – результати процесора (інформація, яка надсилається іншим агентам), V – функція, що визначає який сигнал агент A_i може відправити кожному агенту в поточний час, $V_{A_i} : Z \times R \cap Z \times T \to V$.

Представимо процесор як кортеж:

$$P =< U, W, R >, \tag{4}$$

де $U =< R_{S_i}, T, R >$ – пам'ять агента, яка складається з R_{S_i} – множина результатів, отриманих за допомогою датчиків; T – множина результатів агента, R – множина результатів, отриманих з процесора, які вказують на можливе інфікування комп'ютерної системи ботом;

$W = \{X, Y\}$ – множина правил для визначення присутності ботнет-мережі в корпоративній мережі, а також знання про можливі прояви ботів у комп'ютерних системах, що відноситься до корпоративної мережі.

Множина станів агента може бути представлена у вигляді кортежу

$$I =< S_i, E, R_{S_i} >, \tag{5}$$

де S_i - множина сенсорів агента [6, 7]; E – множина об'єктів діагностування.

$\rho : I \times R_{S_i} \cap I \times T \to I$ - функція оновлення стану агента, яка враховує інформацію сенсорів та інформації комп'ютерної мережі;

$\mu : I \to L$ - рішення функція вирішення, яка пов'язує поточний внутрішній стан агента з деякою дією.

Комунікація агентів. Зв'язок використовується агентами для координації своїх дій в поточний момент часу. Агенти повинні ділитися інформацією, яка може вплинути на результати агентів. Агентам необхідно обмінюватись інформацією так швидко, як це можливо, щоб реагувати на зміни в корпоративній мережі.

Один агент може надсилати кожному агенту тільки один сигнал в даний момент часу. Функція $Send_{ag_i}$ змінюється при взаємодії з корпоративною мережею, і відправлені або отримані сигнали впливають на рішення дій інших агентів. Вибір дії і зміни стану виконується в два етапи: визначення і посилає сигнали, і вибір дій.

Встановимо антивірусний агент на кожній комп'ютерній системі. Наприклад, агент отримує дані (результати) від сенсорів R_{S3}, R_{S4} і R_{S6}. Наприклад, ступінь підозрілості має значення, яке долає заданий рівень небезпеки m. Використовуючи вузол зв'язку С агент надсилає повідомлення до інших активних агентів МАС. Агенти зберігають повідомлення і повертають оброблену інформацію. Після отримання повідомлень від інших агентів процесор Р агента визначає подальші заходи по відношенню до підозрілого об'єкта.

Модель процесу 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 [5].

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»).

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 $\omega_j^i, 0 \le \omega_j^i \le 1$ – 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 $\omega_1+\omega_2+...+\omega_\gamma=1$. Рівень прояву присутності ботнет-мережі в «помічених» комп'ютерних системах визначимо як:

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

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).

Експерименти та дослідження

Для перевірки запропонованої моделі процесу антивірусного діагностування розроблено нове програмне забезпечення та була проведена низка експериментів.

Дослідження проводили протягом 8 місяців, і були отримані наступні результати: за допомогою запропонованої методики виявлення ботнет-мереж продемонстровані кращі результати в порівнянні з простими локальним діагностуванням.

Для реалізації експерименту були отримані 60 програм з властивостями ботнет-мереж (Agobot, SDBot і GT-Bot). У ході експерименту комп'ютерні системі у мережі були інфіковані тільки одним «ботнетом» і діагностування проводилось на протязі 24 годин. Результати експерименту в порівнянні з місцевим виявлення наведені у таблиці 1 та на рис. 2.

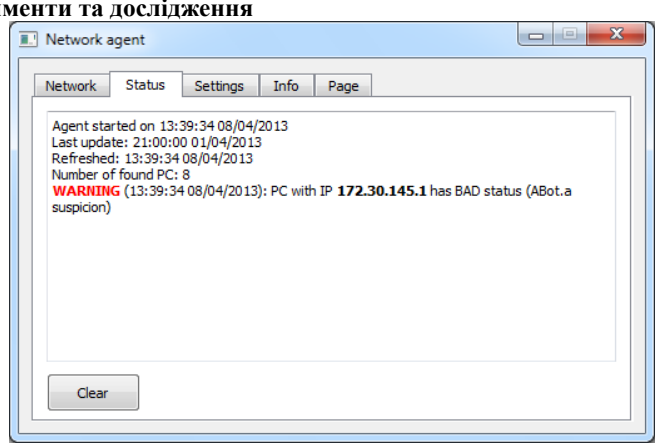

Рис. 2. Результати в програмному забезпеченні

Таблиця 1

Результати експерименту

	Локальне діагностування	**MAC діагностування**
Agobot	12	14
SDBot	18	20
GT-Bot	16	17
Всього	**46 (76,6%)**	**51 (85%)**

Висновки

Запропонована нова модель процесу діагностування комп'ютерних систем на наявність ботнет-мереж в корпоративній мережі. Вона базується на використанні мультиагентної системи.

На основі нової моделі запропоновано новий метод виявлення ботнет-мереж на основі мультиагентних систем з використанням нечіткої логіки. Виявлення здійснюється в ситуаціях апріорної невизначеності присутності ботнет-мереж в корпоративній мережі з урахуванням проявів ботнет-мереж у декількох комп'ютерних системах, доступних в мережі.

Використовуючи нечітку логіку, проводиться аналіз дій ботнет-мереж в ситуації навмисного перепідключення комп'ютерної системи. Розроблена нечітка експертна система для ухвалення висновку про рівень присутності ботнет-мереж в комп'ютерних системах. Нечітка експертна система враховує рівень прояву в перепідключених комп'ютерних системах, ймовірно інфікованих комп'ютерних системах і рівень прояву в інших комп'ютерних системах доступних в корпоративній мережі, які, ймовірно, не були інфіковані.

Використання нової моделі процесу діагностування доводить ефективність виявлення ботнет-мереж з його зростанням, який складає близько 7-10%. У той же час збільшення помилкових спрацьовувань не спостерігалося.

Література

1. Cooke, E. The zombie roundup: Understanding, detecting, and disrupting botnets / E. Cooke, F. Jahanian, and D. McPherson // Proceedings of the USENIX SRUTI Workshop. 2005. – P. 39–44.

2. C. Mazzariello. IRC traffic analysis for botnet detection / C. Mazzariello // Fourth International Conference Information Assurance and Security ISIAS'08. – 2008. – P. 318–323.

3. Akiyama M. A proposal of metrics for botnet de-tection based on its cooperative behavior / M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S. Yamaguchi // Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium. 2007. – P. 82–82.

4. Choi H. Botnet detection by monitoring group activities in DNS traffic / H. Choi, H. Lee, H. Lee, and H. Kim // In proceedings of the 7th IEEE International Conference on Computer and Information Technology. IEEE Computer Society. 2007. – P. 715–720.

5. Savenko O. Review of botnet detection tech-niques. / Savenko O., Lysenko S, Kryshchuk A // Proceedings of the international conference "10 IEEE East-west design and test simposium, 2012. - P.479-482.

6. Savenko O. Botnet detection based on multi-agent approach / Savenko O., Lysenko S, Kryshchuk A // Radioelectronic and computer systems. – 2012. – №5. – P.97-112 (in Ukrinian).

7. Savenko, O., Lysenko, S., Kryschuk, A. Multi-Agent Based Approach of Botnet Detection in Computer Systems / Savenko, O., Lysenko, S., Kryschuk, A. // 19th Conference on Computer Networks, CN 2012, Szczyrk, Poland. CCIS. Springer, Heidelberg 2012. V. 291. P. 171-180.

References

1. Cooke, E. The zombie roundup: Understanding, detecting, and disrupting botnets / E. Cooke, F. Jahanian, and D. McPherson // Proceedings of the USENIX SRUTI Workshop. 2005. – P. 39–44.

2. C. Mazzariello. IRC traffic analysis for botnet detection / C. Mazzariello // Fourth International Conference Information Assurance and Security ISIAS'08. – 2008. – P. 318–323.

3. Akiyama M. A proposal of metrics for botnet de-tection based on its cooperative behavior / M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S. Yamaguchi // Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium. 2007. – P. 82–82.

4. Choi H. Botnet detection by monitoring group activities in DNS traffic / H. Choi, H. Lee, H. Lee, and H. Kim // In proceedings of the 7th IEEE International Conference on Computer and Information Technology. IEEE Computer Society. 2007. – P. 715–720.

5. Savenko O. Review of botnet detection tech-niques. / Lysenko S, Kryshchuk A // Proceedings of the international conference "10 IEEE East-west design and test simposium, 2012. - P.479-482.

6. Savenko O. Botnet detection based on multi-agent approach / Lysenko S, Kryshchuk A // Radioelectronic and computer systems. – 2012. – №5. – P.97-112 (in Ukrinian).

7. Savenko, O., Lysenko, S., Kryschuk, A. Multi-Agent Based Approach of Botnet Detection in Computer Systems / Savenko, O., Lysenko, S., Kryschuk, A. // 19th Conference on Computer Networks, CN 2012, Szczyrk, Poland. CCIS. Springer, Heidelberg 2012. V. 291. P. 171-180.

Рецензія/Peer review : 27.9.2013 р. Надрукована/Printed :24.11.2013 р.
Рецензент: Шалапко Ю.І., д.т.н., проф.

УДК 004.75

Е.В. РЫНДИЧ
Черниговский национальный технологический университет

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ В РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЯХ

В статье представлен анализ современных глобальных сетей с целью их использования в распределенных вычислениях. В качестве способа организации взаимодействия вычислительных узлов предложено использовать ресурсы социальных сетей. Широкое распространение социальных сетей и большое количество пользователей позволяет построить распределенную архитектуру с большим количеством установленных доверительных связей.

Ключевые слова: связь, глобальные сети, распределенные вычисления.

Y.V. RYNDYCH
Chernihiv National University of Technology

USING SOCIAL NETWORKING IN DISTRIBUTED COMPUTING

Abstract – The aim of the research – to explore probability of using social networks in distributed computing. Relevance of research caused fact that modern science and technology more and more attention paid to high-performance computing. Such calculations often performed using clusters or supercomputers. These systems can significantly reduce the time to perform calculations by the decomposition of the problem and the parallel execution of several sub-tasks.

The wide spread of social networks and a large number of users allows to build distributed architecture with lots of established trust relationships. Proposed to build a logical network topology using users contacts in a social network. Such approach to computer network has a number of advantages, among which is to provide high data security and user resources, as well as the high stability of the logical topology . Security is provided by private resources, due to the peculiarities of the runtime computing tasks - browsers. The stability provided by the topology of the users who use social networking sites with a certain regularity.

Keywords: communication, wide area networks, distributed computing.

Введение

Актуальность тематики исследования обусловлена тем, что в современной науке и технике все большее внимание уделяется высокопроизводительным вычислениям. Такие вычисления чаще всего выполняют с использованием кластеров или суперкомпьютеров. Эти системы позволяют значительно уменьшить время выполнения расчетов за счет декомпозиции задачи и параллельного выполнения нескольких подзадач. Использование компьютерных сетей связано со стремительным развитием как технических возможностей сети Интернет, развитием веб-технологий, а также вычислительных мощностей персональных компьютеров.

Согласно закону Мура, количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 24 месяца. А использование новых технологий производства вычислительных элементов позволяет предположить, что при этом их производительность возрастает значительно быстрее. Практика