УДК 004.491.2

К.Ю. БОБРОВНІКОВА
Хмельницький національний університет

МЕТОДИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ БОТ-МЕРЕЖ НА ОСНОВІ АНАЛІЗУ DNS-ТРАФІКА

Розроблено програмне забезпечення інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка, яке дозволяє виконувати наступні задачі: виявлення бот-мереж на основі їх групової активності в DNS-трафіку; виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, на базі пасивного моніторингу DNS-трафіка та активного DNS-зондування; локалізація інфікованих хостів мережі. Застосування розробленого програмного забезпечення надає можливість виявляти інфіковані ботами хости мережі з високою ефективністю.

Ключові слова: бот-мережа, DNS-трафік, групова активність в DNS-трафіку, технології ухилення бот-мереж.

K.Y. BOBROVNIKOVA
Khmelnytsky National University

THE METHODS AND THE SOFTWARE OF INFORMATION TECHNOLOGY FOR BOTNETS DETECTION BASED ON DNS-TRAFFIC ANALYSIS

The software of information technology for botnets detection that based on an analysis of the DNS traffic was developed. It allows to perform the following tasks: botnets detection based on their group activity in DNS traffic; detection of botnets that use DNS-based evasion techniques based on passive DNS monitoring and active DNS probing; localization of infected hosts in the network. Usage of the developed software makes it possible to detect infected hosts by bots of the botnets with high efficiency.

Keywords: botnet, DNS-traffic, group activity in DNS-traffic, botnet`s evasion techniques.

Вступ

На сьогоднішній день бот-мережі є глобальною загрозою інтернет-безпеці. Бот-мережа – це система контролю над зараженими комп'ютерними системами (ботами), яка характеризується динамічною географічно розподіленою структурою та можливістю анонімного керування інфікованими хостами незалежно від їх географічного розташування. Бот-мережі використовуються для здійснення DDoS-атак (розподілених атак типу «відмова в обслуговуванні»), поширення шкідливого програмного забезпечення, викрадення конфіденційних даних, здійснення корпоративного шпіонажу, організації анонімних проксі-серверів, організації фішингу, застосування засобів нав'язування реклами, здійснення клік-шахрайств (Click Fraudulence), поширення спаму, надання сервісу віддалених машин, використання інфікованих комп'ютерів для зберігання нелегального матеріалу тощо.

Переважна більшість бот-мереж для керування інфікованими хостами використовує DNS [1]. Висока інформативність та доступність DNS-трафіка надають широкий спектр можливостей для виявлення бот-мереж на основі дослідження DNS-трафіка. Незначні обсяги DNS-трафіка в порівнянні із загальним трафіком мережі призводять до зменшення потреби в обсягах обчислювальних ресурсів, необхідних для аналізу.

Постановка задачі

В [2] було розроблено інформаційну технологію (ІТ) виявлення бот-мереж на основі аналізу DNS-трафіка, яка усуває недоліки відомих ІТ. З метою ефективної організації процесу виявлення бот-мереж в корпоративних мережах повстає задача розробки програмного забезпечення (ПЗ) інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка.

Методи ІТ виявлення бот-мереж на основі аналізу DNS-трафіка

Для організації та підвищення ефективності процесу виявлення бот-мереж в мережах було розроблено програмне забезпечення, що реалізує ІТ виявлення бот-мереж на основі аналізу DNS-трафіка [2]. Інформаційна технологія побудована на базі двох методів виявлення бот-мереж: методу виявлення бот-мереж на основі їх групової активності в DNS-трафіку [3] та методу виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS [4].

Групова активність ботів в DNS-трафіку є характерною властивістю бот-мереж, що проявляється в зосереджених в невеликому проміжку часу групових DNS-запитах хостів (тобто синхронних DNS-запитах) під час спроб доступу до командно-контрольних серверів (C&C-серверів) бот-мереж, їх міграціях, виконанні команд або скачуванні оновлень шкідливого програмного забезпечення.

Метод враховує особливості поведінки інфікованих груп хостів, характерні для багатьох видів бот-

мереж: групове ігнорування TTL-періоду DNS, тобто очищення групами хостів локальних кешів DNS та здійснення повторних DNS-запитів щодо доменного імені до завершення TTL-періоду; здійснення DNS-запитів, використовуючи нелокальні DNS-сервери. Метод також відслідковує підвищену кількість порожніх DNS-відповідей з кодом помилки NXDOMAIN (доменне ім'я не існує).

Метод виявлення бот-мереж на основі їх групової активності в DNS-трафіку складається з наступних кроків [3]: (1) збір вхідного DNS-трафіка; (2) співставлення з «білим» та «чорним» списками доменних імен; (3) виявлення груп хостів, які ігнорують TTL-період; (4) побудова вектора щільності розподілу DNS-запитів в часі для перевірки синхронності запитів; (5) побудова матриці спостереження для збору та аналізу вхідного DNS-трафіка; (6) виявлення групової активності шляхом аналізу групових запитів щодо одного й того самого доменного імені; (7) побудова нижньотрикутної матриці мір Браун-Бланке для порівняння груп; (8) формування векторів ознак для пар групових запитів щодо різних доменних імен; (9) аналіз векторів ознак з метою виявлення інфікованих хостів.

Метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, спрямований на виявлення таких технологій ухилення, як періодична зміна IP-відображення для шкідливого домена (cycling of IP mapping), технологія «потік доменів» («domain flux»), технологія «швидкозмінних» мереж (fast-flux service network) та DNS-тунелювання (DNS-tunneling) [4–8]. Метод заснований на кластерному аналізі векторів ознак, вилучених з корисного навантаження DNS-повідомлень, отриманих на основі пасивного моніторингу вхідного DNS-трафіка мережі, та залучає активне DNS-зондування в разі необхідності усунення невизначеності частини результатів кластеризації.

Метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, складається з наступних кроків [4]: (1) збір вхідного DNS-трафіка мережі; (2) аналіз полів TTL вхідних DNS-повідомлень щодо певного доменного імені; (3) вилучення ознак з вхідних DNS-повідомлень щодо певного доменного імені та побудова вектора ознак; (4) побудова матриці даних на основі векторів ознак; (5) здійснення нечіткої кластеризації з частковим навчанням з метою виявлення запитів, які можуть свідчити про функціонування ботів, що належать до бот-мереж, які використовують технології ухилення від виявлення на основі DNS; (6) здійснення активного DNS-зондування з метою усунення невизначеності частини результатів кластеризації; (7) локалізація хостів, інфікованих ботами, та блокування дій ботів.

В основі часткового навчання кластеризатора лежать знання про ознаки, які вказують на використання технологій ухилення від виявлення бот-мереж на основі DNS.

На рис. 1 надано схему застосування розробленої ІТ виявлення бот-мереж на основі аналізу DNS-трафіка. На схемі $КС_1$-$КС_4$ позначено комп'ютерні системи мережі, інфіковані ботами бот-мережі, що здійснюють групову активність в DNS-трафіку, $КС_5$ – комп'ютерна система, інфікована ботом бот-мережі, шо застосовує технології ухилення від виявлення на основі DNS, $КС_6$-$КС_n$ – неінфіковані комп'ютерні системи. Програмне забезпечення, що реалізує ІТ виявлення бот-мереж, дозволяє виконувати наступні задачі (рис. 1): виявлення бот-мереж на основі їх групової активності в DNS-трафіку; виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, на базі пасивного моніторингу DNS-трафіка та активного DNS-зондування; локалізація інфікованих ботами комп'ютерних систем мережі.

Локалізація інфікованих комп'ютерних систем здійснюється за допомогою ведення файлів журналювання, в які заносяться MAC-адреси хостів, що ініціювали DNS-запити, і запитані ними доменні імена.

Програмне забезпечення ІТ виявлення бот-мереж на основі аналізу DNS-трафіка

При розробці програмного забезпечення було використано мову програмування C++. В якості середовища розробки було обрано Microsoft Visual Studio. В програмній реалізації було використано модуль з пакету Fuzzy Logic Toolbox, що входить до складу пакету прикладних програм для розв'язання задач технічних обчислень Matlab.

Принцип функціонування системи може бути описаний наступним чином. Вхідний DNS-трафік мережі збирається за допомогою множини мережних давачів, підключених до дзеркалюючих портів комутаторів. В якості мережних давачів застосовуються вузли з встановленою на них утилітою tcpdump або Wireshark. Файли із зібраним вхідним DNS-трафіком надходять в систему, розшифровуються та аналізуються.

Головне вікно програми містить 4 вкладки: Settings (налаштування), Lists Management (керування списками), Analysis (Аналіз), Help (довідка). Інтерфейс розробленого ПЗ відображено на рис. 3-5. Вкладка Settings надає можливість адміністратору мережі здійснити налаштування системи. Блок Mode дозволяє встановити рівні основних параметрів [3, 4], які використовуються системою. Кожен параметр має три рівні: Low (мінімальний), Medium (оптимальний), High (посилений). Блок DNS-servers надає можливість вказати IP-адреси локальних DNS-серверів мережі. Також передбачена можливість ввімкнення або вимкнення функції здійснення активного DNS-зондування з метою уточнення результатів діагностування.

Вкладка Analysis надає можливість завантажити файл з вхідними даними з метою проведення його аналізу. Блок Result відображає результати роботи ПЗ, а саме: MAC-адреси інфікованих та підозрілих хостів мережі, а також додаткову інформацію, яка містить підстави, на яких прийнято відповідне рішення щодо інфікованості або підозрілості хоста (виявлення групової активності та/або виявлення застосування технологій ухилення бот-мереж на основі DNS). Також забезпечена можливість формування, перегляду та

друку звіту з результатами діагностування мережі.

Вкладка Lists Management надає можливість редагування бази даних, що містить «білий» список відомих легітимних доменних імен, «чорний» список відомих доменних імен бот-мереж, «сірий» список доменних імен бот-мереж, виявлених із застосуванням розробленого ПЗ.

Вкладка Help дозволяє отримати довідкову інформацію стосовно розробленого ПЗ.

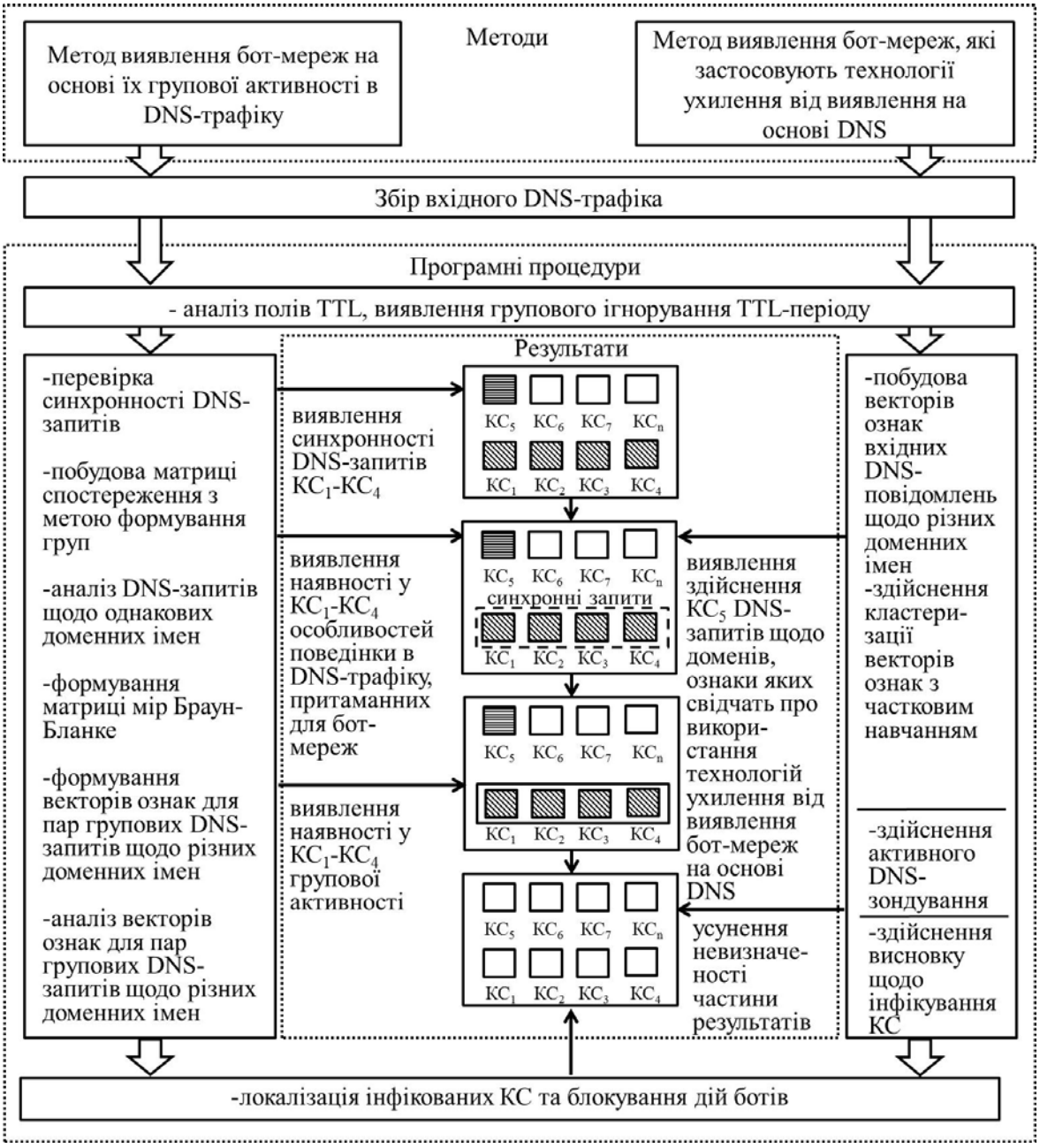

Рис. 1. Схема застосування ІТ виявлення бот-мереж на основі аналізу DNS-трафіка

Експерименти

З метою демонстрації результатів роботи розробленого ПЗ було створено множину спеціального програмного забезпечення, яке мало властивості ботів бот-мереж з централізованою архітектурою. Множина ботів за функціональними властивостями була пропорційно розподілена на групи, кожна з яких відповідала одній з чотирьох технологій ухилення бот-мереж – «потік доменів», «швидкозмінні» мережі, DNS-тунелювання, періодична зміна IP-відображення.

На період проведення експериментів з метою імітації C&C-серверів бот-мереж було зареєстровано множину доменних імен, які розглядались як шкідливі. C&C-сервери мали можливість імітувати застосування технологій ухилення на основі DNS (здійснювали такі дії, як періодична зміна IP-відображення, зміна доменних імен, циклічна зміна A-записів та NS-записів DNS для доменного імені за алгоритмом round robin, передача трафіка командування та контролю за допомогою застосування DNS-тунелювання тощо). В залежності від функціональності створені боти здійснювали відповідні типи DNS-

запитів щодо шкідливих доменних імен, які не були попередньо відомі та не використовувались для навчання. Певна частина групових DNS-запитів ботів була синхронною. Створеними ботами було інфіковано мережу з 100 хостів. Кожна бот-мережа відтворювала різні сценарії здійснення DNS-запитів в різний час. З метою імітації активності користувачів хости мережі також здійснювали DNS-запити щодо легітимних ресурсів.

Експеримент тривав 24 години, протягом яких шляхом застосування розробленого ПЗ було виявлено, проаналізовано та класифіковано 3075 DNS-відповідей. Візуалізація результатів збору вхідного DNS-трафіка мережі та результати роботи розробленого програмного забезпечення відображені на рис. 2–5.

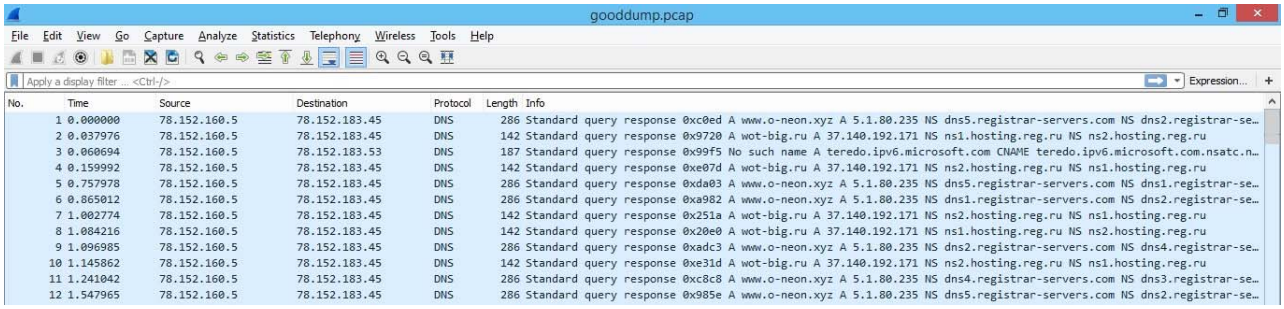

Рис. 2. Візуалізація результатів збору вхідного DNS-трафіка мережі

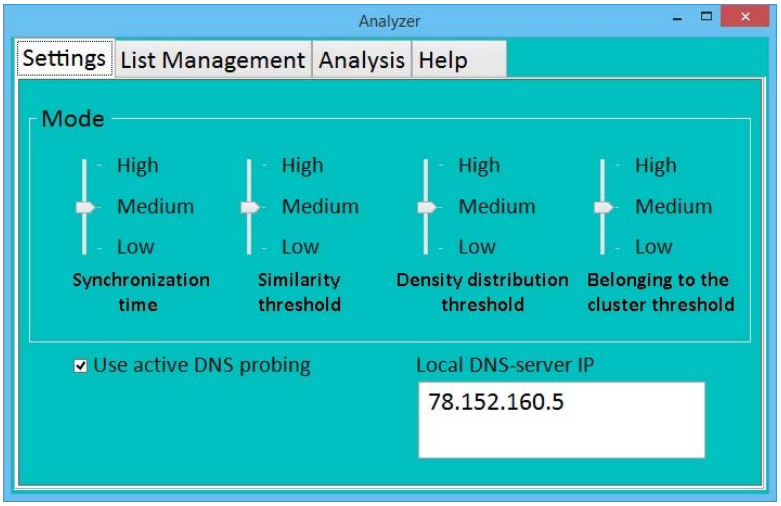

Рис. 3. Налаштування параметрів системи

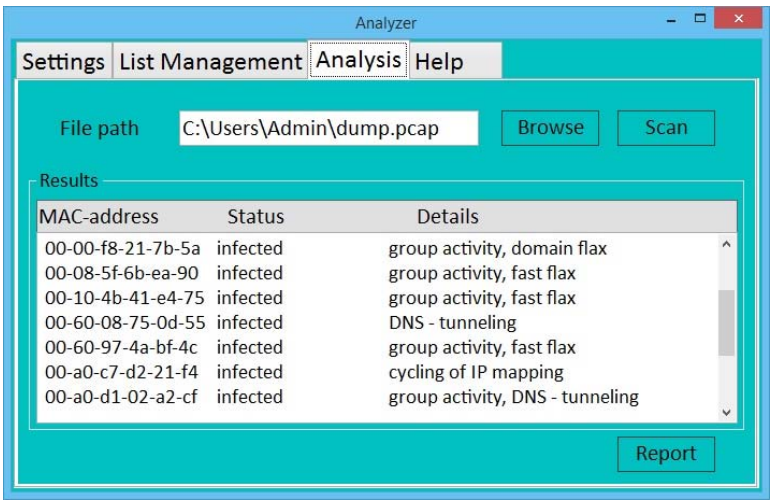

Рис. 4. Результати аналізу вхідного DNS-трафіка мережі

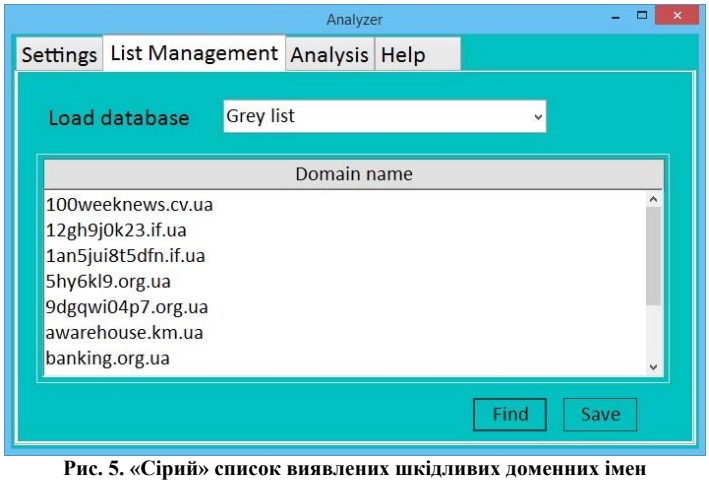

Рис. 5. «Сірий» список виявлених шкідливих доменних імен

В табл. 1 представлено кількість виявлених DNS-відповідей щодо шкідливих доменів. Таким чином, результати застосування запропонованого ПЗ демонструють здатність виявлення бот-мереж на рівні до 96%, в той час як рівень хибних спрацювань становить близько 4 %.

Таблиця 1

Результати експериментів: кількість DNS-запитів, здійснених ботами, виявлені DNS-відповіді ботів та хибні спрацювання

Назва технології ухилення	Кількість DNS-запитів, здійснених ботами / з них групові	Виявлені DNS-відповіді / з них на групові DNS-запити	Хибні спрацювання, %
Періодична зміна IP-відображення	481 / 321	476 / 321	1
«Потік доменів»	1796 / 1520	1753 / 1509	1
«Швидкозмінні» мережі	615 / 429	558 / 421	2
DNS-тунелювання	183 / 47	180 / 44	0
Всього	3075 / 2317	2967 / 2295 (96% / 99%)	4

Висновки

Розроблено програмне забезпечення інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка. Наведено результати застосування програмного забезпечення, які демонструють здатність виявлення бот-мереж на рівні до 96% з рівнем хибних спрацювань близько 4 %. Розроблене програмне забезпечення надає можливість виявляти як відомі, так і ще невідомі боти.

Література

1. DAMBALLA. Botnet Detection for Communications Service Providers [Електронний ресурс]. – Режим доступу : https://www.damballa.com/downloads/r_pubs/ WP_Botnet_Detection_for_CSPs.pdf.

2. Бобровнікова К.Ю. Модель інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка / К.Ю. Бобровнікова // Вісник Хмельницького національного університету. – 2015. – № 6 (231). – С. 164–172.

3. Pomorova O. A Technique for the Botnet Detection Based on DNS-Traffic Analysis / Oksana Pomorova, Oleg Savenko, Sergii Lysenko, Andrii Kryshchuk and Kira Bobrovnikova // Computer Networks 22th International Conference, CN 2015, Brunow, Poland, June 16–19, 2015. Proceedings, pp. 127–138.

4. Lysenko S. DNS-based Anti-evasion Technique for Botnets Detection / Sergii Lysenko, Oksana Pomorova, Oleg Savenko, Andrii Kryshchuk and Kira Bobrovnikova // Proceedings of the 2015 IEEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAAACS'2015, Warsaw, Poland, September 24–26, 2015, Vol. 1, pp. 453–458.

5. DAMBALLA. Botnet Communication Topologies. Understanding the intricacies of botnet command-and-control [Електронний ресурс]. – Режим доступу : https://www.damballa.com/downloads /r_pubs/WP_Botnet_Communications_Primer.pdf

6. Farnham, G., Atlasis, A. Detecting DNS Tunneling // SANS Institute InfoSec Reading Room, 2013. – pp. 1–32.

7. Salusky, W., Danford, R. Know your enemy: Fast-flux service networks. The Honeynet Project, 2007 [Електронний ресурс]. – Режим доступу : http://www.honeynet.org/book/export/html/130.

8. Schiller C. Botnets: The Killer Web Application / Craig Schiller, James R. Binkley // Syngress Publishing, 2007. – 464 p.

Рецензія/Peer review : 3.2.2016 р. Надрукована/Printed :19.4.2016 р.
Рецензент : д.т.н., проф. Мартинюк В.В.