УДК 004.491.2
Савенко О.С. к.т.н, Лисенко С.М. к.т.н., Бобровнікова К.Ю. аспірант
Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ БОТ-МЕРЕЖ, ЩО ВИКОРИСТОВУЮТЬ ТЕХНОЛОГІЇ УХИЛЕННЯ НА ОСНОВІ DNS

Савенко О.С., Лисенко С.М., Бобровнікова К.Ю. Метод виявлення бот-мереж, що використовують технології ухилення на основі DNS. Запропоновано новий метод виявлення бот-мереж, що використовують технології ухилення на основі DNS. Метод базується на кластерному аналізі векторів ознак, отриманих шляхом дослідження корисного навантаження DNS-повідомлень. Метод використовує нечітку кластеризацію с-середніх з частковим навчанням. Застосування методу надає можливість виявляти бот-мережі, які використовують технології ухилення на основі DNS.
Ключові слова: бот-мережа, виявлення бот-мереж, технологія ухилення бот-мереж, DNS-тунелювання, «швидкозмінні» мережі, «потік доменів».

Савенко О.С., Лысенко С.Н., Бобровникова К.Ю. Метод обнаружения бот-сетей, использующих технологии уклонения на основе DNS. Предложен новый метод обнаружения бот-сетей, использующих технологии уклонения на основе DNS. Метод базируется на кластерном анализе векторов признаков, полученных путем исследования полезной нагрузки DNS-сообщений. Метод использует нечеткую кластеризацию с-средних с частичным обучением. Применение метода дает возможность обнаруживать бот-сети, которые используют технологии уклонения на основе DNS.
Ключевые слова: бот-сеть, обнаружение бот-сетей, технология уклонения бот-сетей, DNS-туннелирование, «быстросменные» сети, «поток доменов».

Savenko O.S., Lysenko S.M., Bobrovnikova K.Y. The method for botnets detection that exploit DNS-based anti-evasion technique. A new DNS-based anti-evasion method for botnets detection is proposed. It is based on a cluster analysis of the feature vectors obtained from the payload of DNS-messages. The method uses a semi-supervised fuzzy c-means clustering. Use of the developed method makes it possible to detect botnets that exploit the DNS-based evasion techniques.
Keywords: botnet, botnet detection, botnet`s evasion technique, DNS-tunneling, fast-flux service network, domain flux.

Постановка проблеми. На сьогоднішній день бот-мережі є однією з найбільш небезпечних кіберзагроз [5], а також одним з основних джерел нелегального заробітку в мережі Інтернет. Найчастіше бот-мережі використовуються для атак DDoS (розподілені атаки типу «відмова в обслуговуванні»), збору конфіденційної інформації, розсилання спаму, застосування засобів нав'язування реклами, фішингу, накрутки клік-лічильників (клікфрод), створення пошукового спаму, використання інфікованих комп'ютерів для зберігання нелегального матеріалу (піратське ПЗ тощо) та в якості проксі-серверів для анонімізації доступу в мережі Інтернет. Щороку по всьому світу бот-мережами інфікується близько 500 млн персональних комп'ютерів, кожну секунду – близько 18 ПК. За останній рік бот-мережі нанесли збитків світовій економіці в $110 млрд [5].

Однією з труднощів виявлення бот-мереж є використання ними технологій ухилення. Ряд технологій ухилення від виявлення бот-мереж базуються на використанні системи доменних імен (DNS) – DNS-тунелювання (DNS-tunneling), «швидкозмінні» мережі (fast-flux service network), технологія «потік доменів» (domain flux) та періодична зміна IP-відображення для шкідливого домена (cycling of IP mapping) [4, 7, 12, 14, 15].

Одним з способів ухилення від виявленння командно-контрольних серверів бот-мереж (C&C-серверів) є використання для зв'язку з серверами DNS-тунелювання [6, 7]. Застосування DNS-тунелювання дозволяє зловмиснику передавати довільний трафік в межах специфікації протоколу зверху DNS-протоколу, всередині полів DNS-повідомлення, використовуючи протокол DNS в якості носія для трафіку командування та контролю бот-мережею.

Високі відмовостійкість, доступність та можливість ухилятись від методу занесення до «чорних списків» DNS (DNSBL, DNS blacklist або DNS blocklist) забезпечує бот-мережам поєднання використання коротких TTL-періодів та циклічного методу round-robin DNS. Round-robin DNS є методом розподілення навантаження та забезпечення відмовостійкості за рахунок збитковості кількості серверів, коли для відповіді на запити використовується список IP-адрес серверів, що надають ідентичний сервіс, причому послідовність IP-адрес з кожною DNS-відповіддю змінюється. Прикладом таких систем є «швидкозмінні» мережі (fast-flux service network) [14].

Виокремлюють два типи таких мереж – однопоточні (single-flux) та двопоточні (double-flux). Однопоточні мережі дозволяють використовувати для повного доменного імені велику кількість пов'язаних з ним IP-адрес, які швидко змінюються, що надає змогу пов'язувати доменне ім'я з новою множиною IP-адрес у визначеному інтервалі часу. Додатково з метою підвищення рівня безпеки скомпрометовані хости використовуються для перенаправлення запитів та даних від та до C&C-серверів в якості «сліпого проксі» ("blind" proxy), коли множина циклічних IP-адрес не є кінцевим призначенням для запиту. Перенаправлення запобігає спробам відстеження вузлів такої мережі.

Двопоточні мережі забезпечують додатковий рівень захисту за рахунок збитковості: для шкідливого домена змінюються циклічно за алгоритмом round-robin множина DNS A-записів (A-record) та NS-записи (NS-records).

Більш простим методом ухилення від занесення до «чорних списків» та блокування є технології, які поєднують короткі TTL-періоди та часті зміни доменного імені C&C-сервера – «потік доменів» [4] або періодична зміна IP-відображення для доменного імені C&C-сервера [4, 15]. При технології «потік доменів» автоматична генерація доменного імені може здійснюватись алгоритмічно – комбінація буквено-цифрових символів обирається випадковим чином згідно з алгоритмом генерації доменних імен, вбудованим в тіло бота (domain generation algorithm, DGA), або за допомогою комбінацій слів з словника.

Аналіз досліджень. На сьогоднішній день існує багато підходів виявлення використання технологій ухилення бот-мереж [4, 7]. В [2] запропоновано систему виявлення шкідливих доменів на основі пасивного DNS-аналізу, що здійснює класифікацію доменних імен за 4 групами ознак, які можуть бути вилучені з DNS-трафіка: (1) часові ознаки; (2) ознаки, що базуються на DNS-відповідях; (3) ознаки, що базуються на значеннях TTL; (4) ознаки, що базуються на доменному імені.

В [12] запропоновано підхід, який дозволяє виявляти доменні імена бот-мереж, які використовують метод «швидкозмінних» мереж. Висновок щодо шкідливості доменного імені здійснюється за рядом ознак, отриманих на основі аналізу даних, вилучених з A-, NS-, SOA- та BGP-запитів щодо доменного імені: значення часу життя A-записів (TTL-періоду), IP-адрес в A- та NS-записах, а також значення таймера "retry" (визначає, як довго вторинний сервер імен повинен чекати перед тим, як зробити повторну спробу запиту первинного сервера щодо зміни серійноого номера зони, якщо попередня спроба була невдалою).

В [3] проведено аналіз можливостей використання DNS-запитів для встановлення прихованих комунікацій. Надано оцінку статистичних методів виявлення аномалій у вмісті DNS-пакетів шляхом порівняння ймовірнісних розподілів нормального та тунельованого DNS-трафіка. З метою висвітлення потенційної загрози розглянуто можливість здійснення контрзаходів з боку зловмисника.

В [8, 9] проведено аналіз великої кількості реальних DNS-запитів та обчислено порогові значення довжини запитаного імені хоста та кількості унікальних символів в ньому, що дозволяють відрізнити легітимгний DNS-трафік від тунельованого.

Описані методи мають наступні недоліки: необхідність залучення інформації, отриманої від інших сервісів (WHOIS тощо); необхідність активного DNS-зондування, тому неможливіть реалізації на основі пасивного аналізу DNS-трафіка; зосередження на виявленні вузького кола шкідливого ПЗ.

Попереднє дослідження. В [1] запропоновано метод виявлення ботів в корпоративних мережах, який ґрунтується на властивості групової активності ботів в DNS-трафіку, що проявляється в невеликому проміжку часу в одночасних або зосереджених DNS-запитах груп хостів під час спроб доступу до C&C-серверів, їх міграціях, виконанні команд або скачуванні оновлень шкідливого програмного забезпечення. Метод враховує нетипові для звичайних користувачів особливості поведінки, властиві багатьом видам бот-мереж: ігнорування TTL-періоду, здійснення DNS-запитів поза локальними DNS-серверами та підвищену кількість порожніх DNS-відповідей з кодом помилки RCODE=3 (NXDOMAIN, доменне ім'я не існує). Метод дозволяє виявляти ще невідомі боти, а також здійснювати раннє виявлення – на початковій стадії поширення інфекції в мережі.

Недоліком методу є нездатність виявляти бот-мережі, які використовують DNS-тунелювання для передачі трафіка командування та контролю, оскільки в такій бот-мережі DNS-

запити та інші дії ботів можуть не бути синхронними в часі. Також метод не здатний виявляти інфіковані групи хостів, менші за 4.

Таким чином постає задача розробки нового методу виявлення ботів, які використовують технології ухилення на основі DNS.

Метод виявлення бот-мереж, що використовують технології ухилення на основі DNS. Для виявлення бот-мереж, що використовують технології ухилення на основі DNS, запропоновано новий метод, який базується на кластерному аналізі ознак, отриманих шляхом дослідження корисного навантаження DNS-повідомлень. Метод використовує нечітку кластеризацію с-середніх з частковим навчанням. Застосування нечіткої кластеризації дозволяє отримувати високу точність та змістовність результату кластеризації [11, 13].

Об'єктами кластеризації є вектори ознак використання ботами технологій ухилення від виявлення на основі DNS, які отримано з корисного навантаження вхідних DNS-повідомлень щодо певного доменного імені.

Метод складається з наступних кроків (рис.1): (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) локалізація хостів, інфікованих ботами, що належать до бот-мереж, які використовують технології ухилення від виявлення на основі DNS, та блокування дій ботів.

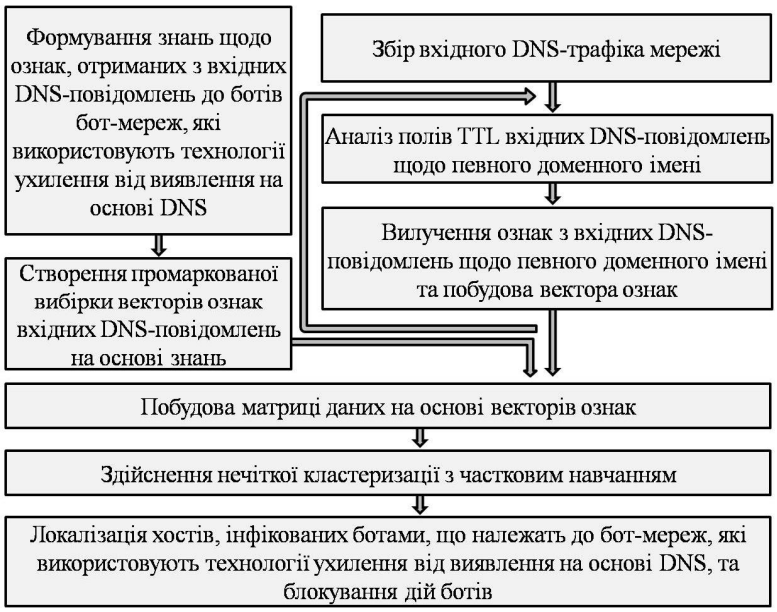

Рис. 1. Принцип функціонування методу

Формування знань щодо ознак, отриманих з вхідних DNS-повідомлень до ботів бот-мереж, які використовують технології ухилення від виявлення на основі DNS. З метою виявлення DNS-тунелювання використано ознаки, отримані шляхом аналізу корисного навантаження DNS-повідомлень: (1) довжина запитаного доменного імені [8]; (2) кількість унікальних символів в доменному імені [8]; (3) ентропія доменного імені [7]; (4) використання рідковживаних типів записів DNS (KEY, NULL тощо), або таких, які зазвичай не використовуються клієнтами (наприклад, TXT, які найбільш часто використовуються для тунелювання) [7]; (5) ентропія записів DNS, які містяться в DNS-повідомленнях (CNAME, TXT, NS, MX, KEY, NULL тощо) [6, 7]; (6) довжина DNS-повідомлення [10].

З метою виявлення використання таких методів ухилення, як «потік доменів», «швидкозмінні» мережі та періодична зміна IP-відображення для домена використано такі ознаки: (1) кількість IP-адрес, пов'язаних з доменним ім'ям; (2) середня дистанція між IP-адресами, пов'язаними з доменним ім'ям; (3) кількість A-записів, що відповідають доменному імені, у вхідному DNS-повідомленні [12]; (4) середня дистанція між IP-адресами в A-записах, що

відповідають доменному імені, у вхідному DNS-повідомленні [12]; (5) кількість унікальних IP-адрес в множинах A-записів, що відповідають доменному імені [12]; (6) середня дистанція між унікальними IP-адресами в множинах A-записів, що відповідають доменному імені [12]; (7) кількість доменних імен, які спільно використовують IP-адресу, що відповідає доменному імені [2, 4, 16]; (8) значення TTL-періоду [2, 12]; (9) ознака успішності DNS-запиту [16].

Подамо вектор ознак, отриманих з вхідних DNS-повідомлень щодо певного доменного імені *d*, наступним чином:

$$\overline{W_d} = \left(L_N, N_U, E_N, T_{\text{mod}}, T_{med}, T_{aver}, N_A, N_{IP}, S_{IP}, S_A, N_{UA}, S_{UA}, N_D, F_{UR}, E_R, L_P, F_S\right), \quad (1)$$

де L_N – довжина доменного імені;

N_U – кількість унікальних символів в доменному імені;

E_N – ентропія доменного імені;

T_{mod} – TTL-період, мода (значення у множині спостережень, яке зустрічається найбільш часто; застосуємо мінімальне значення у випадку, якщо множина є мультимодальною);

T_{med} – TTL-період, медіана (значення ознаки, яке розділяє ранжовану сукупність на дві рівні частини, де 50% нижніх одиниць ряду даних мають значення ознаки, не більше, ніж медіана, а 50% верхніх – не менше, ніж медіана);

T_{aver} – TTL-період, середнє арифметичне значення;

N_A – кількість A-записів, що відповідають доменному імені, у вхідному DNS-повідомленні (ознака використовується, якщо $N_A>1$);

N_{IP} – кількість IP-адрес, пов'язаних з доменним ім'ям (ознака використовується, якщо $N_A=1$);

S_{IP} – середня дистанція між IP-адресами, пов'язаними з доменним ім'ям (ознака використовується, якщо $N_A=1$);

S_A – середня дистанція між IP-адресами в множині A-записів для доменного імені у вхідному DNS-повідомленні (ознака використовується, якщо $N_A>1$);

N_{UA} – кількість унікальних IP-адрес в множинах A-записів, що відповідають доменному імені, у вхідних DNS-повідомленнях (ознака використовується, якщо $N_A>1$);

S_{UA} – середня дистанція між унікальними IP-адресами в множинах A-записів, що відповідають доменному імені, у вхідних DNS-повідомленнях (ознака використовується, якщо $N_A>1$);

N_D – кількість доменних імен, які спільно використовують IP-адресу;

F_{UR} – бінарна ознака використання рідковживаних типів записів DNS, або таких, які зазвичай не використовуються клієнтами;

E_R – максимальне значення ентропії записів DNS, які містяться в DNS-повідомленнях;

L_P – максимальний розмір DNS-повідомлень щодо доменного імені;

F_S – бінарна ознака успішності DNS-запиту ($F_S = 0$, якщо DNS-запит невдалий, $F_S = 1$, якщо DNS-запит успішний).

Також метод використовує функцію залежності f_{E_B} ентропії поля DNS-повідомлення від його довжини [6].

Знання формуються на основі ознак, властивих вхідним DNS-повідомленням до ботів, з метою визначення технології ухилення від виявлення на основі DNS. Знання можуть бути представлені у вигляді наступних правил:

$$if\ \left(TTL_{\text{mod}} \in [0{,}900]\ and\ \ TTL_{med} \in [0{,}900]\ and\ TTL_{aver} \in [0{,}900]\right)\ and$$

$$and\ \left(\left(N_A \in (5,\infty)\ and\ \ S_A \in (65535,\infty)\right) or \left(N_{UA} \in (8,\infty)\ and\ \ S_{UA} \in (65535,\infty)\right)\right) \Rightarrow fast\_flux$$

$$if\ TTL_{\mathrm{mod}} \in [0{,}900]\ and\ \ TTL_{med} \in [0{,}900]\ and\ TTL_{aver} \in [0{,}900]\ and$$
$$and\ F_S = 0\ and\ N_D \in [8;\infty] \Rightarrow domain\_flux$$
$$if\ TTL_{\mathrm{mod}} \in [0{,}900]\ and\ \ TTL_{med} \in [0{,}900]\ and\ TTL_{aver} \in [0{,}900]\ and$$
$$and\ N_{IP} \in (5,\infty)\ and\ S_{IP} \in (65535,\infty) \Rightarrow cycling\ \ of\ IP\ mappings$$
$$if\ \left(L_N \in [75{,}255]\ and\ \ N_U \in (27{,}37]\right) or\ E_N \geq f_{E_{B32}}\ or$$
$$or\ \ \left(E_R \geq f_{E_{B64}}\ or\ \ E_R \geq f_{E_{B256}}\right) or\ \ F_{UR} = 1\ or\ L_P > 300 \Rightarrow DNS\_tunneling \qquad (2)$$

Створення промаркованої вибірки векторів ознак вхідних DNS-повідомлень на основі знань. Промаркована вибірка формується на основі знань щодо ознак вхідних DNS-повідомлень до ботів, які застосовують технології ухилення від виявлення на основі DNS. На основі утвореної вибірки здійснюється часткове навчання кластеризатора.

Позначимо промарковану вибірку даних як $X = \{x_i\}_{i=1}^{N_x}$, а немарковану вибірку як $Y = \{y_i\}_{i=1+N_x}^{N_z}$, де N_x – кількість об'єктів в промаркованій вибірці даних, N_z – загальна кількість різних доменних імен.

Нехай $H = \{h_i\}_{i=1}^{N_h}$ – множина наперед визначених кластерів об'єктів, де N_h – кількість кластерів; належність вектора ознак кластеру h_1 свідчить про технологію ухилення «cycling of IP mapping», h_2 – «domain flux», h_3 – «fast flux», h_4 – «DNS-tunneling», h_5 – кластер, який містить нормальні запити.

Кожен вектор ознак з промаркованої вибірки даних належить одному з множини наперед визначених кластерів.

Збір вхідного DNS-трафіка мережі. Вхідний DNS-трафік збирається за допомогою мережних давачів, підключених до дзеркалюючих портів комутаторів.

Аналіз полів TTL вхідних DNS-повідомлень щодо певного доменного імені. Для багатьох видів бот-мереж характерною особливістю поведінки є ігнорування TTL-періоду. Це означає, що здійснюється очищення локального кеша DNS та виконуються повторні запити щодо доменного імені до завершення TTL-періоду. Це дозволяє підвищити мобільність бот-мережі. Тому на основі значень полів TTL опрацьовуються такі вхідні DNS-повідомлення:

1) кожне перше зафіксоване DNS-повідомлення щодо певного доменного імені в межах TTL-періоду;

2) кожне DNS-повідомлення, отримане хостом повторно в межах TTL-періоду, якщо джерелом повідомлення є нелокальний DNS-сервер, і TTL-період, зазначений в цьому повідомленні, відрізняється від залишка TTL-періоду, в межах якого було отримане це повідомлення.

Решта вхідних DNS-повідомлень відкидаються.

Якщо політика корпоративної мережі дозволяє здійснювати запити поза локальними DNS-серверами, і хости здійснюватимуть запити щодо одного й того ж доменного імені до різних DNS-серверів, то в DNS-відгуках можуть міститись різні значення TTL-періодів. Проте така особливість функціонування DNS не впливатиме на рівень виявлення, оскільки вона не береться до уваги для ботів однієї бот-мережі.

Вилучення ознак з вхідних DNS-повідомлень щодо певного доменного імені та побудова вектора ознак. Відповідні ознаки вхідних DNS-повідомлень щодо певного доменного імені вилучаються та формуються протягом визначеного періоду моніторингу на основі всіх вхідних DNS-повідомлень, які не було відкинуто на попередньому етапі.

На основі ознак вхідних DNS-повідомлень щодо певного доменного імені будується вектор ознак $\overline{W}_d$.

Побудова матриці даних на основі векторів ознак. З векторів ознак вхідних DNS-повідомлень формується матриця даних V, кожен рядок якої є вектором ознак вхідних DNS-

повідомлень $\overline{W_d}$ щодо певного доменного імені, $V = \left(v_{ij}\right)_{i=1,\,j=1}^{N_z,N_q}$, $V(i,) = \overline{W_d}$, де N_q – загальна кількість ознак вхідних DNS-повідомлень, які вказують на використання технологій ухилення від виявлення на основі DNS.

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. На даному етапі здійснюється нечітка кластеризація векторів ознак вхідних DNS-повідомлень щодо доменних імен з частковим навчанням на основі промаркованої навчальної вибірки. Задача кластеризації з частковим навчанням може бути описана функцією $f_{cluster} : \overline{V} \to H$.

Об'єктами кластеризації є вектори ознак, які отримано з корисного навантаження вхідних DNS-повідомлень щодо певного доменного імені.

Результатом кластеризації є ступені приналежності векторів ознак до п'яти кластерів, де належність вектора ознак $\overline{W_d}$ кластеру h_i, $i = \overline{1,4}$ свідчить про виконання запитів з використанням технологій ухилення. Належність вектора ознак до п'ятого кластера свідчить про виконання запитів до легітимних ресурсів.

В якості відстані між об'єктом кластеризації та центром кластера застосовано норму Махаланобіса, оскільки вона дає кращі результати, ніж Евклідова норма [11], яка використовується в базовому алгоритмі c-means.

Локалізація хостів, інфікованих ботами, що належать до бот-мереж, які використовують технології ухилення від виявлення на основі DNS, та блокування дій ботів. На основі приналежності векторів вхідних DNS-повідомлень до кластерів здійснюється визначення доменних імен, до яких зверталися боти бот-мереж. З метою блокування дій ботів, які здійснювали шкідливі запити, локалізація хостів мережі здійснюється за допомогою ведення журналювання MAC-адрес хостів, що здійснювали DNS-запити, та запитаних ними доменних імен.

Проведення експериментів. Для визначення ефективності роботи запропонованого методу було проведено ряд експериментів. З цією метою було згенеровано тестове програмне забезпечення з властивостями бот-мереж. Тестові бот-мережі мали централізовану архітектуру і використовували одну з чотирьох технологій ухилення від виявлення – періодична зміна IP-відображення для домена, «потік доменів», «швидкозмінні» мережі, DNS-тунелювання. Кожна з груп бот-мереж здійснювала DNS-запити щодо доменних імен своїх командно-контрольних серверів.

Для експериментів була використана мережа з 100 хостами, 80 з яких були інфіковані згенерованими ботами. Кожна бот-мережа здійснювала множину запитів (1000 запитів). Також було згенеровано програмне забезпечення, яке здійснювало запити до відомих легітимних доменних імен, імітуючи роботу користувачів. Дане програмне забезпечення було встановлено на кожному хості мережі. Експеримент тривав 24 години. DNS-трафік локальної мережі збирався засобами утиліти tcpdump.

В якості навчальної вибірки було промарковано 10% векторів ознак вхідних DNS-повідомлень.

На рис. 2 відображено проекцію на площину множини векторів ознак DNS-повідомлень, розподілених на кластери. Початок координат на графіку є центроїдом кластера, який містить множину вхідних DNS-повідомлень щодо легітимних ресурсів до хостів мережі.

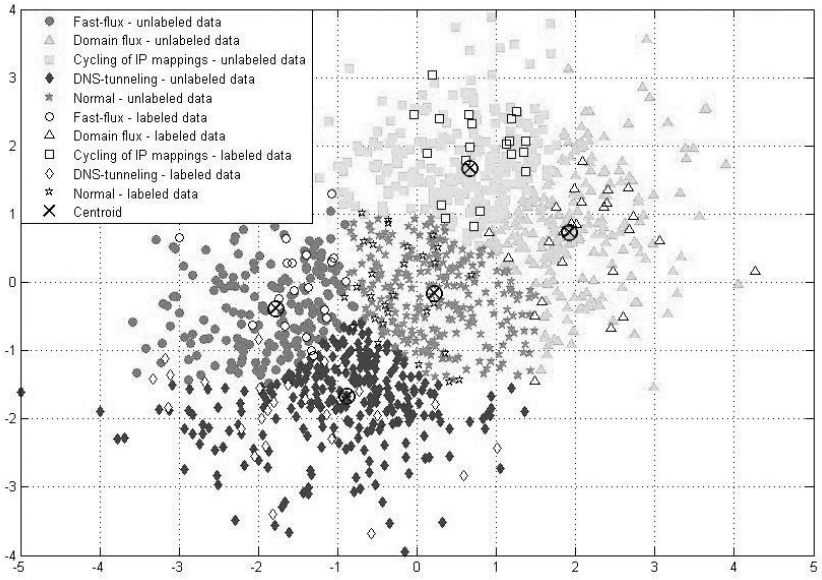

Рис. 2. Результати кластеризації

Кожен маркер (крапка) в кластері представляє множину вхідних DNS-повідомлень до інфікованих та неінфікованих хостів мережі щодо певного доменного імені. Кожен маркер свідчить про те, що визначена група хостів отримала вхідні DNS-повідомлення щодо доменного імені.

Після опрацювання файлів журналювання було локалізовано боти бот-мереж.

Результати роботи методу представлені в табл.1. Результати демонструють можливість виявлення бот-мереж, що використовують технології ухилення на основі DNS, на рівні до 96%, при цьому рівень хибних спрацювань становив 6%.

Таблиця 1. Результати експериментів: кількість запитів, здійснених ботами, виявлені запити ботів та хибні спрацювання

	Кількість запитів, здійснених ботами	Виявлені запити ботів	Хибні спрацювання, %
h_1, cycling of IP mapping	1000	980	1
h_2, domain flux	1000	940	2
h_3, fast flux	1000	940	3
h_4, DNS-tunneling	1000	980	0
Всього	4000	3840 (96%)	6

Висновки та перспективи подальшого дослідження. Запропоновано метод виявлення бот-мереж, що використовують технології ухилення від виявлення на основі DNS. Метод базується на кластерному аналізі векторів ознак, отриманих шляхом дослідження корисного навантаження вхідних DNS-повідомлень. Метод використовує нечітку кластеризацію с-середніх з частковим навчанням.

Застосування розробленого методу дає можливість здійснювати виявлення ботів бот-мереж, що використовують технології ухилення на основі DNS, з високою достовірністю.

Подальшим дослідженням є питання підвищення достовірності виявлення бот-мереж.

1. Савенко О. С. DNS-метод виявлення бот-мереж / О. С. Савенко, С. М. Лисенко, К. Ю. Бобровнікова // Інформаційні технології та комп'ютерна інженерія . – 2014. – № 3. – С. 39-45.
2. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. Bilge, L., Kirda, E., Kruegel, C., Balduzzi, M.: NDSS, 2011– pp. 1-17.
3. Quantitatively analyzing stealthy communication channels. Butler, P. Xu, K., Yao, D.: Proc. Ninth Int'l Conf. Applied Cryptography and Network Security (ACNS '11), 2011. – pp. 238-254.

4. DAMBALLA. Botnet Communication Topologies. Understanding the intricacies of botnet command-and-control. Retrieved from https://www.damballa.com/downloads/r_pubs/WP_Botnet_Communications_Primer.pdf
5. The Federal Bureau of Investigation. Demarest, J. (2014, July 15). Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C. Retrieved from http://www.fbi.gov/news/testimony/taking-down-botnets.
6. On Botnets that use DNS for Command and Control. Dietrich, C.J., Rossow, C., Freiling, F. C., Bos, H., van Steen, M., Pohlmann, N.: In: Proceedings of European Conference on Computer Network Defense, 2011 – pp. 9-16.
7. Detecting DNS Tunneling. Farnham, G., Atlasis, A.: SANS Institute InfoSec Reading Room, 2013. – pp. 1-32.
8. Guy, J. (2009, January 30). A study of DNS. Retrieved from http://armatum.com/blog/2009/a-study-of-dns/
9. Guy, J. (2009, February 13). Dns part ii: visualization. Retrieved from http://armatum.com/blog/2009/dns-part-ii/
10. Detection of DNS anomalies using flow data analysis. Karasaridis, A., Meier-Hellstern, K. S. and Hoeflin, D. A.: In GLOBECOM. IEEE, 2006. – pp. 1-6.
11. A comparison of distance-based semi-supervised fuzzy c-means clustering algorithms. Lai, D.T.C., Garibaldi, J.M.: Fuzzy Systems (FUZZ), In 2011 IEEE International Conference, 2011. – pp. 1580-1586.
12. As the Net Churns: Fast-Flux Botnet Observations. Nazario, J., Holz, T.: In: Conference on Malicious and Unwanted Software (Malware'08), 2008. – pp. 24-31.
13. Algorithms of fuzzy clustering with partial supervision. Pedrycz, W.: Pattern Recognition Letters, 1985. – Vol. 3, pp. 13–20.
14. Know your enemy: Fast-flux service networks. Salusky, W., Danford, R.: The Honeynet Project, 2007 [Online] http://www.honeynet.org/book/export/html/130.
15. Schiller, C. Botnets: The Killer Web Application/ Craig Schiller, James R. Binkley. – Syngress Publishing, 2007. – 464 p.
16. Winning with DNS failures: Strategies for faster botnet detection. Yadav, S., Reddy, A.L.N.: In: Proc. of the 7th International ICST Conference on Security and Privacy in Communication Networks, 2011.