УДК 681.3

В.Д. Погребенник, П.Т. Хромчак
Національний університет “Львівська політехніка”,
кафедра захисту інформації

РОЗРОБЛЕННЯ МОДЕЛІ СИСТЕМИ ВИЯВЛЕННЯ ЦЕНТРІВ УПРАВЛІННЯ БОТНЕТ-МЕРЕЖАМИ

Розглянуто новітні підходи та методи для реалізації механізмів виявлення центрів управління ботнет-мережами.

Modern campaigns and methods for realization of mechanisms of revealing of networks Botnet and control centres of them are considered

Вступ. Ботнет (від англ. Botnet) – мережа інфікованих хостів, якими управляє власник ботнету. Інша назва – зомбі-мережа. Проектування системи виявлення мереж ботнетів є першочерговим в галузі захисту інформації, а його актуальність зумовлена наслідками від використання як в глобальних, так і в локальних мережах. Основними способами застосування цього шкідливого виду програмного забезпечення є організація та здійснення DDoS-атак, розсилання спам-повідомлень, крадіжка конфіденційних даних, анонімний доступ в мережу Internet, фішинг. Наслідки від застосування ботнет-мереж може відчути будь-хто у будь-який час. Найбільші мережі ботнетів, такі, як Mayday чи Storm botnet, налічують десятки тисяч інфікованих хостів, а наслідки від їхнього застосування є абсолютно руйнівними.

Проблематика цієї галузі також пов'язана із раннім віком як самих ботнетів, так і відсутністю інформації про виконання досліджень в цій сфері. Нині практично не існує жодного комплексного рішення проблеми проектування системи виявлення ботнетів, за винятком проектів PlanetLab та Internet Security від AT&T. Оскільки перший – науковий проект планетарних масштабів, а другий – комерційний проект, то доступ до них значно обмежений.

Метою цієї роботи є розроблення моделі системи виявлення командних центрів управління ботнет-мережами.

Основна частина. Всі комп’ютери ботнету – інфіковані програмним забезпеченням (бот-клієнтом), яке має риси, притаманні широкому класу шкідливого ПЗ. Ботнет-мережа комп’ютерів, як правило, не об’єднана одним доменом колізій. Управляє такою мережею власник ботнету, т. зв. “ботмастер”, через віртуальні інтерфейси, наприклад, браузер, IRC-канал тощо, які називають C&C-центрами.

Класифікують ботнети залежно від типу мережевих протоколів, які вони використовують. Основні групи:

- IRC-орієнтовні. Один із найпоширеніших та ранніх видів ботнетів. Управління ботами здійснюється на основі протоколу IRC (Internet Relay Chat).
- Web-орієнтовні. Цей клас ботнетів орієнтований на управління через www, що швидко розвивається. Управління ботами здійснюється на основі протоколу HTTP (Hypertext Transfer Protocol).
- IM-орієнтовні. Для передавання команд та управління використовується канал IM-служб (Instant Messaging), наприклад, AOL, MSN, ICQ тощо. Ці ботнети не користуються високою

популярністю. Це зумовлено складністю їхнього обслуговування, а саме труднощами створення акаунтів IM-служби для кожного окремого бота.

- Інші. Вид ботнетів, які важко виявити. Цей клас реалізований на власних протоколах розробника, який ґрунтується на стеці протоколів TCP/IP. Такі ботнети важкі при написанні коду тіла програми, тому розраховані, як правило, не на клієнтські робочі станції, а на потужніші комп'ютери під управлінням Linux-, Unix-подібних ОС.
- Згідно з дослідженнями [1] близько 60 % ботнетів є IRC-орієнтованими. Та лише мала кількість використовує HTTP протокол для доступу до C&C.

Внутрішньо ботнет – це невеликий IRC-клієнт з вбудованим в його тіло сервісом. Залежно від завдань, які поставлені перед ботом, це можуть бути: поштові клієнти, проксі-сервери, троянські програми, клавіатурні шпигуни чи експлойти.

Життєвий цикл бота. На рис. 1 подано узагальнене схематичне зображення життєвого циклу бота. Загалом його можна розділити на дві основні групи. Перша – ботнети, які використовують DNS-сервер для розширення імені власного IRC чи Web-сервера. Друга група – боти, які не використовують DNS для розширення імені.

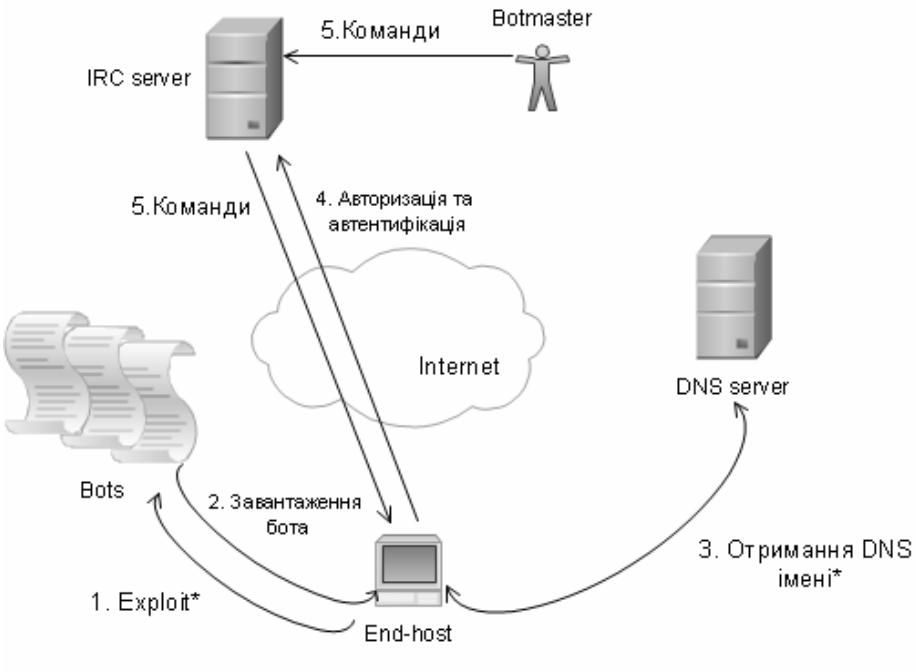

Рис. 1. Життєвий цикл бота

На першому кроці, внаслідок дії експлойту на машину-жертву, завантажується тіло бота. Цей крок є необов'язковим, тому шлях та спосіб, через який бот потрапляє на машину, може бути різним. Як тільки завантажилось тіло, наступним кроком є зараження машини. Встановившись на машині жертві, бот, згідно із запрограмованими в ньому інструкціями та властивостями, отримує ім'я власного IRC-сервера. Після цього відбувається ініціалізація з'єднання з сервером. Основним етапом ініціалізації та встановлення сесії є авторизація бота відносно сервера/каналу та ботмастера відносно популяції ботнетів. Ця процедура відбувається в три етапи. Бот автентифікується на IRC-сервері, використовуючи PASS повідомлення в заголовку пакета для успішного створення сесії. Як правило, ботмастер захищає свій C&C-канал за допомогою паролю, який вимагається від бота для підтвердження своєї автентичності. Ці дві фази автентифікації містяться в програмному тілі бота. Третя фаза, яка не стосується протоколу IRC, – це підтвердження ботмастера відносно свого ботнета (популяції). Ця остання фаза використовується з метою збереження ботнета від перехоплення іншими ботмастерами. Одразу після з'єднання з каналом, бот прослуховує т. зв. "тему дискусії" (команду від ботмастера) та виконує її.

Архітектура бота. Розрізняють дві архітектури ботнетів.

Ботнети з єдиним центром управління (централізована архітектура). Ботнети з такою архітектурою з'єднуються з одним центром управління, т.зв. C&C (Command&control Centre). C&C чекає під'єднання нових ботів, реєструє їх в своїй базі, стежить за їх станом і видає їм команди, вибрані власником ботнета із списку всіх можливих команд для бота.

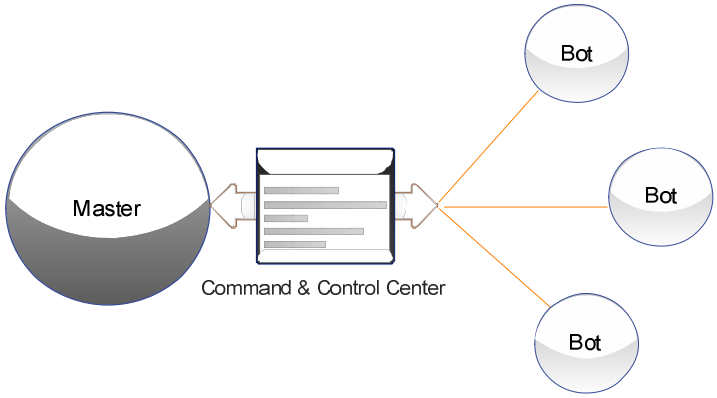

Рис. 2. Централізована архітектура управління ботнетами

Ботнети з децентралізованою архітектурою

У разі децентралізованої архітектури боти з'єднуються не з центром управління, а з декількома зараженими машинами із зомбі-мережі. Команди передаються від бота до бота: в кожного з них є список адрес декількох "сусідів", і при отриманні команди ботом від будь-кого "легального сусіда" він передає її наступним, тим самим поширює команду далі.

Переваги такої реалізації:

– важкість виявлення та нейтралізації мережі ботнетів загалом;

– труднощі, пов'язані із локалізацією ботмастера.

Недоліки:

– повільна швидкість реагування на команди від власника мережі;

– важкість передавання ідентифікаторів сусідів та їхніх адрес;

– висока ймовірність втрати мережі.

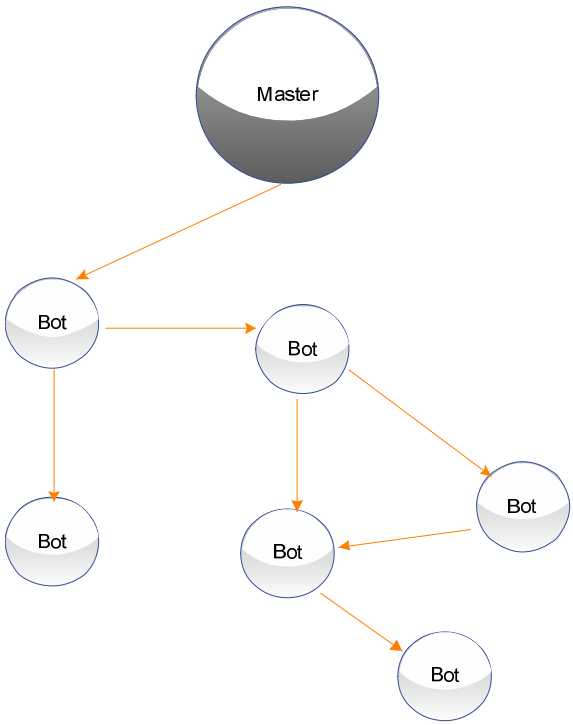

Рис. 3. Децентралізована архітектура управління ботнетами

Опис моделі системи локалізації зомбі-мережі. Під час розроблення моделі системи виявлення ботнетів (надалі СВБ) особливу увагу треба приділити характерним рисам та особливостям ботів, які можуть бути використані як основа для побудови цієї моделі. Отож при її розробленні початково заданими характеристиками є такі умови: нехай потрібно розробити модель системи виявлення центрів управління ботнет-мережами, орієнтовану на Інтернет-провайдера, з можливістю виявлення адрес та нейтралізації C&C центрів управління ботнетами. При цьому розглядаються ботнети, які використовують DNS сервер для отримання імені сервера з C&C, так і ті, які не використовують його. Також ця модель повинна забезпечувати виявлення ботнетів будь-якого з перерахованих класів: IRC-, Web-орієнтованих і тих, які використовують власні протоколи реалізації з централізованою архітектурою. Наведемо загальне схематичне подання місця системи виявлення ботнетів на прикладі невеликого ISP провайдера.

На рис. 4 зображено місце системи СВБ у логічній топології мережі ISP провайдера.

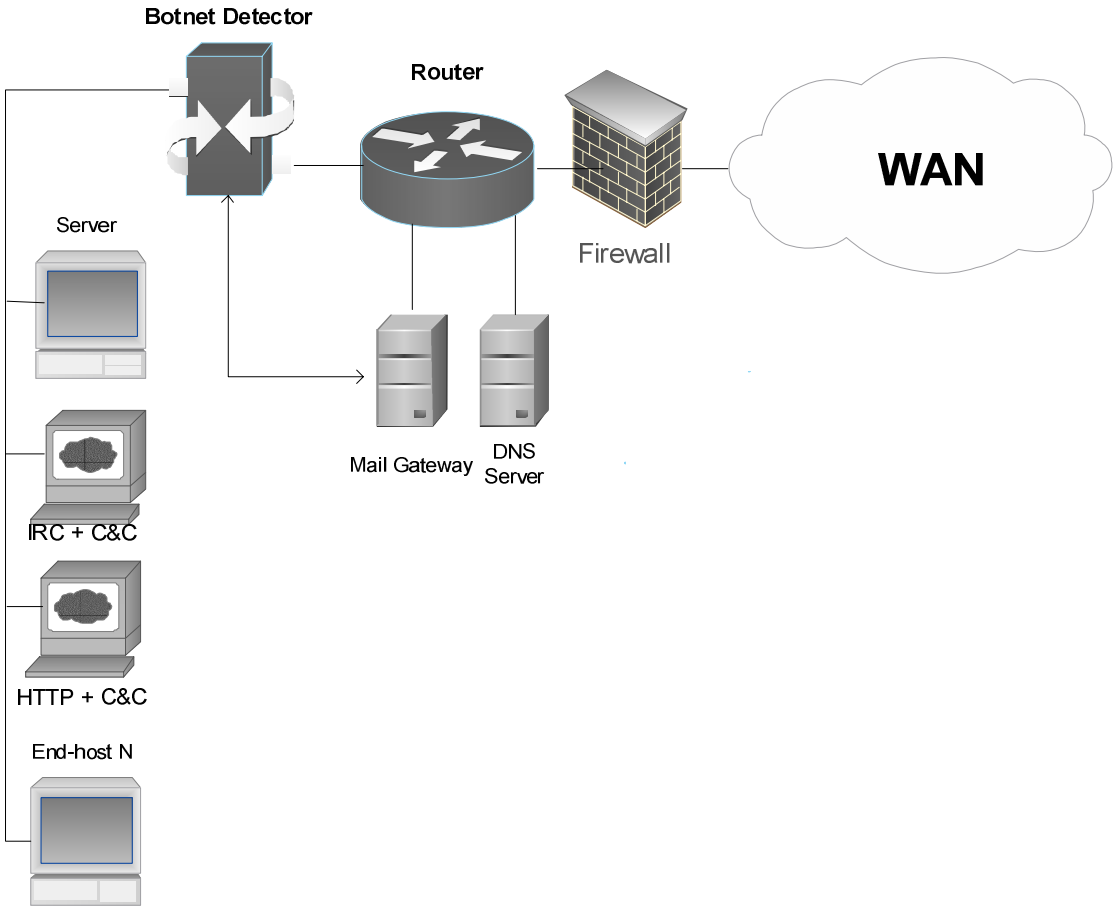

Рис. 4. Місце СВБ у логічній топології мережі ISP провайдера

Внутрішня структура СВБ. СВБ являє собою набір програмних модулів, призначених для виявлення певних класів ботнетів. Кожен модуль використовує власний механізм та методику виявлення.

На рис. 5 зображено модель СВБ системи та її модулі.

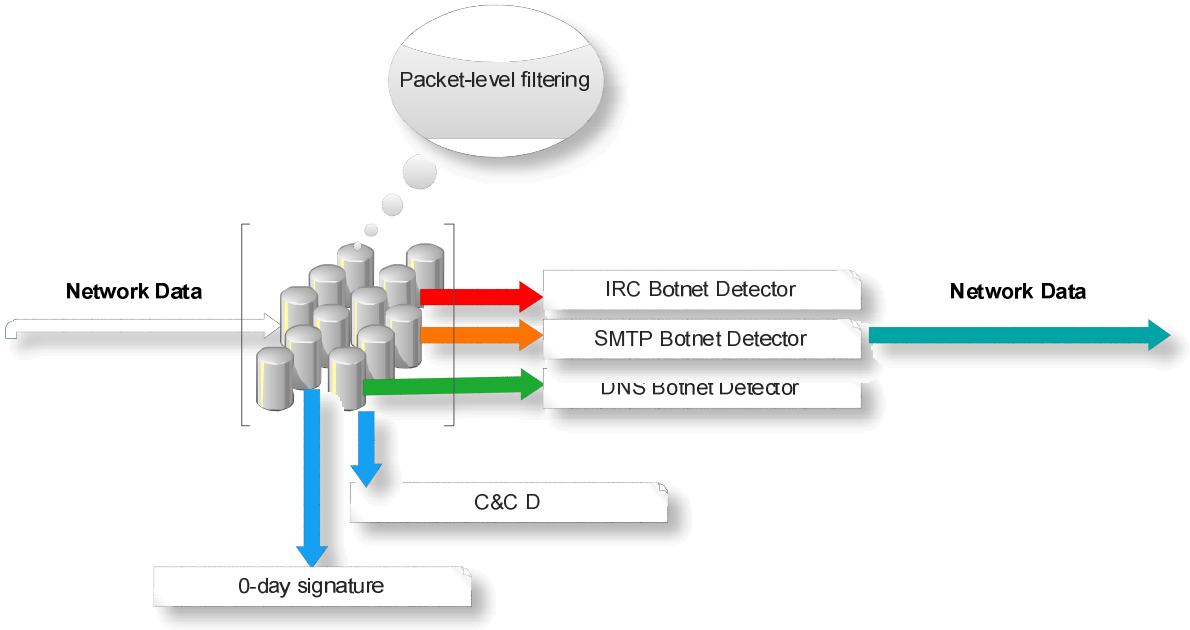

Рис. 5. Модель СВБ та її модулі

Ця модель є результатом комплексного аналізу та узагальнення технологій виявлення та роботи з окремими видами ботнентів [1–4]. Треба зауважити, що вона дворівнева і охоплює як виявлення мережі ботнетів, так і C&C центра.

Модель системи виявлення C&C. Модель системи виявлення центрів управління ботнет-мережами розглядається в контексті загальної моделі системи виявлення мереж ботнетів, зображеної на рис. 2, та є її ключовим модулем.

Іноді недостатньо виявити лише саму мережу ботнетів безпосередньо (так, наприклад, не всі комп'ютери можуть бути в онлайн-режимі). Іншим системним рішенням є спосіб виявлення C&C центрів [2].

Виявлення C&C контролерів складається з таких етапів.

Нагромадження тривог, які ідентифікують хост з підозрілою поведінкою.

Збирання даних для подальшого аналізу здійснюється за допомогою процедури сніфінгу мережевих пакетів. Розроблення програмних інтерфейсів основане на використанні бібліотечних функцій від проекту tcpdump, а саме бібліотек libpcap.

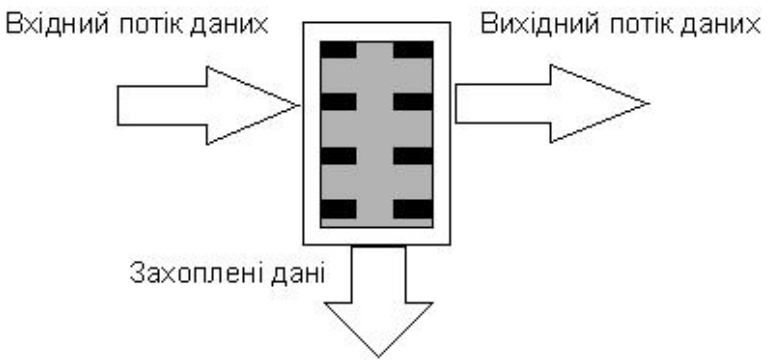

Рис. 6. Процедура сніфінгу мережевих даних

Захоплені (отримані під час процедури сніфінгу) дані виступають як вхідні дані (вибірка) для подальшого аналізу та побудови евристичних моделей “інфікованих” мережевих даних.

Аналіз мережевої активності для визначення потенційного C&C

Процедура аналізу вибірки даних, отриманих протягом часу навчання системи, дає змогу з певною імовірністю говорити про локалізацію C&C центрів.

На цьому етапі здійснюється детальний аналіз ключових параметрів, що однозначно чи відносно ідентифікують роботу C&C центру. Ключовими параметрами є такі параметри заголовку пакета, як:

– порт призначення;

– порт відправника;

– IP-адреса отримувача;

– IP-адреса відправника;

– розмір фрагмента пакета;

– розмір пакета;

– тривалість сесії;

– наявність шифрованої сесії;

– вміст даних пакета.

Основою для порівняння та пошуку схожостей у моделі інфікованого та поточного мережевого трафіку є використання таких методів:

– метод групового врахування аргументів;

– використання методів теорії ігор для визначення вагових коефіцієнтів вхідних параметрів.

Виявлення центрів управління здійснюється на основі таких моделей:

a) кількість пакетів у сесії;
b) кількість фрагментів у пакеті;
c) кількість сесій у потоці;
d) кількість сесій.

Нагромадження та аналіз потенційних C&C та ізоляція підозрілих C&C та портів контролера.

Основою для розгляду підозрілої поведінки є звіти, генеровані внутрішньою системою на основі даних активності хоста, таких, як сканування портів, відправлення листів із вірусами та спам-повідомлення, генерація DDoS трафіку. Зауважимо, що вхідними даними тут є дані як від вищенаведених модулів, так і внутрішні дані модуля, отримані на основі аналізу подібно до методу для розрахунку евристичних ознак виявлення Botnet-трафіку в IRC потоці.

Ідентифікація потенційного контролера.

Відповідно до багатьох факторів боти можуть розпочати чи завершити сесію з контролером в будь-який момент протягом доби. В такому випадку довготерміновий аналіз допомагає визначати контролери та/або створювати конфіденційніші умови виявлення контролерів.

Багато контролерів використовують порти, асоційовані із IRC (6667 6668 7000/tcp). Саме тому ці порти прослуховуються першими та перевіряються на наявність контролера. Проте багато ботів використовують технологію маскарадингу для приховування власних портів. Так, наприклад, бот W32.Spybot.ABDO використовує порт 53/tcp для з’єднання зі своїм IRC сервером. Хоча, як всім відомо, саме порт 53 використовується для багатьох DNS транзакцій. Саме тому запропоновано додатковий підхід.

Він вимагає виявлення трафіку між ботом та віддаленим хостом, котрий може бути hub-server'ом. Тут під hub-server розуміють хост, котрий має встановлено велику кількість з’єднань з великою кількістю машин на один чи декілька портів.

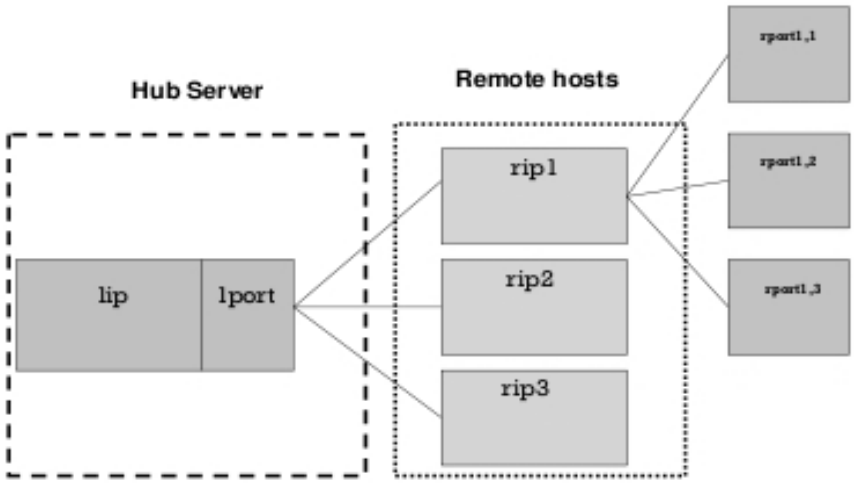

Рис. 7. Зв'язки піж парами lip/rport та rip чи rport; Lip – локальна IP; lport – локальний порт; rip – IP віддаленого хоста; rport – порт віддаленого хоста

Потрібно знайти пару lip/lport, котра асоційована з декількома rip-адресами чи декількома віддаленими портами. На основі такого аналізу можна доволі точно стверджувати про те, що віддалена машина (для ISP-сервера машина з внутрішньої мережі) може бути IRC сервером з C&C центром. Цей метод є найточнішим та найдостовірнішим з погляду виявлення C&C. Зауважимо, що виявлення центрів управління є результативнішим, ніж виявлення всієї мережі ботнетів.

Висновки. Розроблена модель ґрунтується на технологіях та механізмах виявлення ботнетів, і являє собою комплексне рішення на базі технологій фільтрації пакетів та подальшого аналізу з використанням методів аналізу групової активності DNS серверів, аналізу SMTP-трафіку на поштових шлюзах та виявлення ботнет-інфікованого трафіку серед потоку IRC. Запропоновано підхід виявлення ботнет-мереж, який ґрунтується на побудові евристичних моделей для метрик типового IRC-трафіку, їхнього подальшого порівняння, а також на інноваційному поєднанні аналізу потоку даних на основі сигнатур від систем генерації сигнатур 0-day атак.

Перевага цієї моделі полягає у тому, що вона здатна виявляти мережі ботнетів Web-, IRC-орієнтованих та тих, які використовують власні протоколи реалізації на основі стандартного стеку протоколів TCP/IP незалежно від використання DNS-сервера для розширення імені власного командного центру.

1. Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas Terzis. A Multifaceted Approach to Understanding the Botnet Phenomenon // Computer Science Department, Johns Hopkins University. 2. Anestis Karasaridis, Brian Rexroad, David Hoeflin. Wide-scale Botnet Detection and Characterization. 3. Vaibhav Nivargi, Mayukh Bhaowal, Teddy Lee. Machine Learning Based Botnet Detection. CS 229 Final Project Report. 4. Nicholas Albright, Security Researcher. Researching Botnets. 5. Крейг Закер. Компютерние сети. Модернизация и поиск неисправностей. – Санкт-Петербург, 2001. 6. W. Timothy Strayer, Robert Walsh, Carl Livadas, and David Lapsley. Detecting Botnets with Tight Command and Control. November. – 2006. 7. Carl Livadas, Robert Walsh, David Lapsley, W. Timothy Strayer. Using Machine Learning Techniques to Identify Botnet Traffic. 8. http://sectools.org/sniffers.html.