Отже, за допомогою наведених формул можна еквівалентно замінювати задані ймовірнісні характеристики. Тому розрахунок накопиченої ймовірності зводиться до визначення потенціалу виявлення або інтенсивності пошуку.

Висновки

Оцінено зміни ймовірності виявлення порушення стану об'єкта залежно від кількості спостережень, відстані та різних швидкостей порушника.

1. Політило Р. В. Підвищення надійності ультразвукових систем охоронної сигналізації / Погребенник В. Д., Політило Р. В. // Збірник тез доповідей VII Міжнародної науково-технічної конференції «Приладобудування 2008: стан і перспективи». – К.: НТУ «Київський політехнічний інститут», 2008. – С. 105–106. 2. Політило Р. В. Вибір параметрів первинних вимірювальних перетворювачів ультразвукових засобів охоронної сигналізації / Погребенник В. Д., Політило Р. В. // Збірник матеріалів IУ Міжвузівської науково-технічної конференції науково-педагогічних працівників «Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні». – Львів: ІППТ, 2009. – С. 48–49. 109. 3. Абчук В.А. Поиск объектов / Абчук В.А., Суздаль В.Г. – М.: Сов. радио, 1977. – 336 с. 110. 4. Бакут П.А. Обнаружение движущихся объектов / Бакут П.А., Жулина Ю.В., Иванчук Н.А. – М.: Сов. радио, 1980. – 288 с.

УДК 004.4

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

ПАСИВНІ МЕТОДИ ВИЯВЛЕННЯ БОТНЕТ-МЕРЕЖ

Підсумовано та описано групи пасивних методів виявлення ботнет-мереж. Наведено основні недоліки та переваги роботи кожного з них.

Ключові слова: ботнет-мережі, пасивні методи.

Groups of passive techniques of botnet detection mechanisms are described and summarized in this article. Base advantages and disadvantages of each of them are also shortly noted.

Key words: botnet detection mechanisms, passive techniques.

Вступ

Група пасивних методів виявлення ботнет-мереж ґрунтується на методах, які отримують дані виключно за допомогою спостереження за роботою мережі. Такий підхід уникає прямої взаємодії з середовищем передавання даних, що дає змогу залишатись анонімним та непоміченим як для програм, так і для аналітика. Проте пасивні методи мають ряд обмежень, які стосуються даних, отриманих для аналізу.

У цій роботі наведено різноманітні підходи для здійснення вимірювань показників активності ботнету та його виявлення. Методи, що застосовують для аналізу мережевих даних, застосовують техніки, які фокусуються на певній абстракції даних та протоколах, що використовуються в галузі ботнетів. Ці методи не обмежуються архітектурою мережі та можуть застосовуватись до будь-якої з них.

Мета роботи – підвести підсумки щодо використання та групування пасивних методів виявлення ботнет- мереж, а також висвітлити основні недоліки та переваги роботи кожного з них в умовах роботи в інформаційній мережі контрольованої зони.

Аналіз пакетів

Один з найпоширеніших методів підвищення рівня захищеності корпоративної мережі передачі даних – аналіз даних та контроль пакетів. Основна ідея методу полягає в аналізі та порівнянні різноманітних полів пакета, що стосуються конкретного протоколу та/або його корисного навантаження ii заздалегідь визначеними шаблонами аномального або підозрілого трафіку.

Так, наприклад, це може бути пакет, котрий містить частину коду, призначеного для поширення шкідливого програмного забезпечення (ПЗ); з'єднання з IP-адресою, яка достовірно є хостом з шкідливим вмістом; файловий сервер, котрий раптово починає здійснювати активність, пов'язану з протоколом IRC (Internet Relay Chat). Часто ці шаблони називають сигнатурами, або сигнатурами виявлення.

Важливими засобами, які працюють та використовують таку методику, є системи виявлення втручань IDS (Intrusion Detection System). Ціль IDS – охорона периметра середовища передачі даних (часто – локальної мережі) від різноманітних загроз безпеки, в якій вона розміщена, та, за необхідності, впровадження превентивних заходів і формування інформаційних попереджень, якщо виявлено загрозу інформаційній безпеці.

Ці системи поділяють на два основні типи:

- Мережево-орієнтовані (NIDS, від англ. Network-based intrusion detection system).
- Хост-орієнтовані (HIDS, від англ. Host-based intrusion detection system).

Коли IDS не лише повідомляє про небезпеку а й приймає рішення та застосовує правила політик, спрямовані на її нейтралізацію, така система називається IPS (Intrusion Prevention System) – система попередження втручань.

Типово такими правилами є відкидання пакетів або закриття з'єднань, що стосуються аномальної активності. Іншим популярним варіантом є перенаправлення даних та з'єднань до систем подальшого аналізу. Інформацію, отриману в процесі аналізу, використовують для наповнення “чорних списків” (перелік ненадійних хостів) та одержання нових сигнатур.

Проте системи виявлення втручань мають такі недоліки:

- Повна інспекція вмісту пакетів є ресурсоємною процедурою та слабо масштабується в мережах з високим навантаженням. Використання технік вибірки чи фільтрування підвищує ризик пропускання шкідливих пакетів.
- Виявити можна лише ті потоки, які містять відомі шаблони. Саме тому існують різноманітні техніки уникнення виявлення. Наприклад, такою технікою є розподіл шкідливого контенту між декількома пакетами, цим маскують дані. Лише частина сигнатури міститиметься у конкретному пакеті. Поки що ця техніка працює виключно в так званих системах з “packet-wise” аналізом, але не у системах, котрі “збирають” структуру даних декількох пакетів. Проте існують й інші техніки, що використовують кодування та шифрування з метою уникнення виявлення.
- IDS-системи мають високий рівень помилкових результатів виявлень атак та загроз. З одного боку, сенсори IDS повинні бути налаштованими дуже точно, щоб не пропустити шкідливого контенту, а з іншого – це може спричинити проблеми, пов'язані з класифікацією корисних пакетів як шкідливих.

У контексті досліджень ботнетів та аналізу пакетів системи виявлення втручань використано в декількох проектах для автоматизованого розпізнавання ботнет-мереж.

Ранні підходи до виявлення зомбі-мереж використовували техніку інспекції даних для виявлення аномальної активності [1]. Так, наприклад, один з алгоритмів виявлення IRC-орієнтованих мереж ботнетів оснований на особливостях сканувань, які використовують ботнет-хости. Він складається з двох компонентів: IRC та TCP-компоненти. Перший – вимірює рівень активності TCP-протоколу відносно окремо взятої IP-адреси. Він визначається відношенням кількості пакетів з прапорцями SYN, RST, FIN до всіх пакетів сесії кожні тридцять секунд. Якщо значення цієї компоненти близьке до 1, то це свідчить про високу ймовірність сканування ботнету інфікованими хостами. Другий компонент складається з двох модулів обліку IRC, які збирають інформацію та статистику про IRC канали, з одного боку, та активність конкретних IP-адрес відправників – з іншого. Дані з обох компонент порівнюють та корелюють для виявлення таких IRC-каналів,

в яких можуть міститись інфіковані клієнти ботнет-мережі, про що свідчить високе значення рівня активності.

Проте такий підхід є нестійким в умовах, в яких використовується шифрування повідомлень IRC або нестандартне кодування, оскільки воно не допускає можливості кореляції компоненти IRC щодо TCP.

Результати аналізу пакетів з використанням вищеописаного методу для тестової мережі наведено нижче в табл. 1.

Роз'яснення до табл. 1:

- Подія JOIN – приєднання користувача до каналу.
- Подія PRIVMSG – отримання приватного повідомлення.

Таблиця 1

Результати аналізу пакетів методом виявлення аномальної активності

Ім'я каналу IRC	К-ть повідомлень	К-ть подій типу JOIN	К-ть повідомлень типу PRIVMSG	Рівень активності в каналі	К-ть інфікованих хостів	Канал шкідливий
F7	118	19	99	6	4	Так
s3reporter	2259	25	2234	3	1	Так
thespicebox	23	8	15	2	1	Так

Метод, що поєднує декілька технік моніторингу, застосовано в програмному продукті BotHunter [2]. Це ПЗ стежить за вхідним та вихідним потоком пакетів та виконує кореляцію даних на основі діалогів для виявлення інфікованих потоків. Ядро кореляційного механізму складається з IDS-системи SNORT, яка додатково містить декілька спеціально налаштованих правил аналізу та програм, спрямованих на виявлення шкідливо-орієнтованого ПЗ. Ці компоненти містять засоби розпізнавання різних стадій процесу зараження хостів. Так само в цій системі будь-які подальші дії розглядаються як спроба контакту з сервером управління (C&C) за умови, що хост бере участь в активності, пов'язаній із завантаженням шкідливих модулів.

Аналіз параметрів потоку

Метод аналізу параметрів потоку можна розглядати як техніку для дослідження мережевого трафіку на абстрактному рівні. Замість того, щоб аналізувати окремі пакети, як описано в попередньому розділі, потік передачі даних розглядають у вигляді єдиної агрегованої форми. У цьому контексті записи про потік складаються з декількох характеристик, що описують та характеризують конкретний мережевий трафік. Типовими атрибутами є: адреса відправника та отримувача, відповідні порти сторін та протоколи, які використовуються, тривалість сесії, кількість переданих пакетів даних тощо. Оскільки цей метод не бере до уваги вміст пакета, він дає можливість аналізувати дуже велику кількість потоків. Складність аналізу полягає в отриманні потоків із загальної кількості пакетів. Для цього одержують та аналізують заголовки пакетів, що містять інформацію про сесію. Типово, для кожної сесії, за якою йде спостереження, активність вимірюють за допомогою "лічильника старіння". Якщо спостерігається активність, лічильник старіння встановлюється в деяке значення часу та починає зменшуватись з моменту активності. Якщо час сплинув, то поточна сесія вважається завершеною. Таке стеження, як правило, викликає значне навантаження на систему, що фіксує дані про потік. Щоб зменшити навантаження, використовують механізм вибіркового відбору мережевого трафіку, наприклад, реєструють лише один з n пакетів.

Мережевий протокол NetFlow, що є власністю компанії Cisco Systems, розглядається де-факто як стандарт для аналізу потоків. Маршрутизатори, які його використовують, можуть бути

налаштовані для агрегації та збору даних про потоки, що проходять через нього, та подавати дані у вигляді записів про потоки з подальшим спрямуванням до зовнішніх пристроїв, які здійснюють їх аналіз. Мета аналізу записів про потік – ідентифікація зразків трафіку, які можна використати для відокремлення шкідливих мережевих даних від нешкідливих та створення схеми виявлення потенційних шкідливих зв'язків.

Т. Страєр проаналізував різні алгоритми для виявлення IRC чат трафіку та потоків, що належать IRC C&C ботнетам [3]. Він підготував вибірку з експериментальних даних трафіку та розділив процес виявлення на дві стадії. Перший етап складається з виділення IRC-орієнтованих потоків із загальної кількості. Другий етап виконує розділення шкідливого та нешкідливого IRC-трафіку. Страєр зауважив, що вибір вхідних параметрів, які використовують у формуванні потоків, дуже істотно впливає на кінцевий результат розпізнавання. Страєр виділив розмір пакета як найважливіший атрибут, а також параметри зміни цієї величини в часі. Результати виявлення шкідливих потоків даних у тестовому наборі для класифікаторів J48 наївним методом Байєса (NB) та байєсівським методом (BN) наведено у табл. 2.

Таблиця 2

Результати класифікації шкідливих потоків у тестовому наборі

Атрибут	Оптимальний набір атрибутів потоку		
	J48	NB	BN
Тривалість потоку (duration)	+	+	+
Максимальне початкове вікно навантаження (MaxWindow)	+	+	+
Ініціатор потоку (role)	+	+	+
Середнє значення байт/пакет для потоку (bpp)	+	+	+
Середнє значення біт/пакет для потоку (bps)	+	+	+
Середнє значення пакетів/секунду для потоку (pps)	+	+	+
Відсоток пакетів, задіяних у потоці (PctPktsPushed)	+	+	+
Відсоток пакетів, що потрапили у відповідну категорію розміру пакета (PctBppHistBin0-7)	+	+	+
Дисперсія часу прибуття пакета для потоку (varIAT)		+	+
Дисперсія величини байт/пакет для потоку (varBpp)		+	+
Ймовірність неправильного відкидання (FNR) (%) Ймовірність неправильного прийняття рішення (FPR) (%)	2.46	2.21	2.49
	14.17	14.73	15.04

Застосовуючи вищенаведену методику, Т. Страєру вдалось з'ясувати, що наївний метод Байєса найкраще дає змогу класифікувати IRC-орієнтовані потоки з урахуванням зважених значень показників FNR і FPR та швидкодії.

Існують програмні платформи для виявлення P2P-ботнетів, основані на припущенні, що боти, які належать до одного і того самого ботнету, поводяться схоже, окрім відправлення та отримання повідомлень управління [4]. Така система розділена на декілька модулів. Перший модуль займається агрегацією мережевого трафіку від пристроїв маршрутизації та комутації. Другий модуль відфільтровує добре відомі легальні ресурси на основі IP-адрес, щоб зменшити навантаження на систему аналізу вибірки даних. На наступному модулі трафік збирається в потоки з використанням програми мережевого аудиту ARGUS. Над цими записами потоків виконують процес клас-

теризації за спільними ознаками і формують групи подібності. Паралельно з цим виконується аналіз вмісту пакетів. Дані, отримані на цьому етапі, корелюють між собою, що підвищує точність розпізнавання ботнет-належних даних.

Метод TAMD (Traffic Aggregation for Malware Detection) здійснює пошук збігів шаблонів та мережевих потоків [5]. Під час цього процесу застосовують різні правила вибірки потоків: вибирають ті потоки, які містять інформацію про з'єднання із спільним зовнішнім ресурсом, рівень завантаження якого вищий за середній в мережі; потоки, що належать до хоста зі спільною операційною системою (оскільки більшість ботнетів залежать від певних ОС) тощо, як міра подібності. Метод TAMD був застосований до потоків мережі з більш ніж 33 тисячами активних та індивідуальних IP-адрес, які були змішані із ботнет-потоками даних від ботнету з одним клієнтом та даними від ботнету з більш ніж 300 зомбі-хостами [1, 5]. TAMD виявив всі одиничні ботнети та 87.5 % потоків, що належали великому ботнет-трафіку.

М. Джеласіті та В. Біліцкі [6] запропонували метод виявлення ботнетів на основі аналізу автономних систем (AS). Враховуючи той факт, що багато методів виявлення P2P ботнет-мереж потребують ручного втручання в сенсі реверсного аналізу та реконструкції протоколу, вони проаналізували автоматичний алгоритм для виявлення децентралізованих мереж з використанням графів розсіювання трафіку (Traffic Dispersion Graphs). Навіть за допомогою досить простої мережевої моделі вони виявили, що застосування локальних підходів виявлення P2P ботнет-мереж є малоефективним та не дуже перспективним, оскільки видимість в цих мережах може бути дуже обмеженою всередині однієї AS, особливо коли боти прагнуть зберегти низьку кількість підключень до інших ботів.

DNS-орієнтовані методи

Коли хост скомпрометований ботнетом, він встановлює з'єднання або до центра управління C&C, або з іншими ботами залежно від його архітектури. Це вимагає інтеграції протоколу передачі даних у шкідливе ПЗ. Існує два способи визначення точки контакту бота та центра управління:

- Інтеграція фіксованої IP адреси в тіло бота.
- Інтеграція доменного імені.

Використання другого способу відкриває значно більше можливостей та забезпечує гнучкість управління. Передовсім одне доменне ім'я може бути асоційоване з декількома IP- адресами, що дає змогу створити надлишкову завадостійку архітектуру управління. Ці адреси не повинні бути статичними, а можуть змінюватись динамічно чи на вимогу. Контактну інформацію, яка потрібна для реєстрації доменного імені, як правило, підроблено або вона недостовірна і тому її не можна використати для розслідування. Та все ж, коли такий домен виявлений, його можна використати для подальшого аналізу та дій, пов'язаних зі збором всієї можливої інформації, що стосується його роботи. Зокрема, пасивну DNS-реплікацію можна використати для збирання різноманітної інформації з сервера та її подальшого архівування для аналізу. Це дозволяє ідентифікувати комп'ютери, які виконували різноманітні запити, що стосуються шкідливого домена, або автоматично виявляти тайпсквотинг. Тайпсквотинг сприяє досягненню високого рівня відвідування веб-ресурсу за рахунок використання доменних імен, близьких за написанням до адрес популярних сайтів, з розрахунку на помилку частини користувачів.

З технічного погляду такі домени досить легко можуть блокувати реєстратори на глобальному рівні або оператори DNS-серверів. Як альтернативу протидії ботнетам такі доменні імена можна використати для моніторингу вхідних запитів від ботів. Такий метод більш відомий як “sinkholing”. Проте, якщо бот використовує IP-адресу для контакту з центром управління безпосередньо, то ботнет не можна нейтралізувати процедурою відкликання доменного імені чи взяттям під контроль відповідних DNS-серверів. Всі ці особливості роботи дають змогу застосовувати різноманітні пасивні техніки вимірювань роботи DNS. Якщо домен значиться як “інфікований”, то найімовірніше, що всі вхідні запити надходять від інфікованих хостів, саме це дає змогу відстежити нові зараження. Витонченіші методи можуть бути розроблені на основі запитів, які стосуються шкідливих доменів, типово з можливістю відображення зв'язків у вигляді просторових діаграм.

Ботнети схильні демонструвати координовану поведінку, яка називається груповою активністю. Так, щоразу, коли C&C-сервер має проблеми з каналом зв'язку чи мігрує на нове доменне ім'я, це призводить до зростання активності з боку всіх ботів учасників ботнету. Всі асоційовані боти майже одночасно починають відправляти DNS-запити, що стосуються їх центра управління. Навіть більше, координована шкідлива активність, така як DDoS чи розсилання спаму, також позначиться на зростанні рівня групової активності, що дає змогу отримати інформацію про конкретний бот, який належить до цієї групи [7]. Також використання сервісів динамічного DNS (DDNS) вказує на наявність C&C серверів, що також використовується у цьому методі аналізу активності.

Р. Вілламарін-Саломон та Дж. Брустоліні [8] також запропонували метод виявлення C&C серверів. У своїй роботі вони порівняли різні алгоритми та оцінили їх ефективність. Вони дійшли висновку, що аномальна кількість періодичних NXDOMAIN-відповідей є важливим індикатором присутності ботнету. NXDOMAIN-відповідь генерується DNS-сервером, якщо доменне ім'я, що запитується, не може бути перетворене на IP-адресу. В контексті ботнетів це явище виникає через часту зміну доменного імені центра управління та/або проблеми з доступністю сервера. Вони також встановили, що метод, оснований на NXDOMAIN відповідях, менш схильний до хибних виявлень, ніж інші алгоритми.

Інший хост-орієнтований метод, схожий на вищенаведений, запропонував Дж. Моралес [9]. Він дослідив, як процеси реагують на відповіді, отримані від DNS-сервера одразу після запиту. Проаналізувавши деякі зразки ботів, було встановлено, що, окрім прямих спроб з'єднання через процедуру перетворення доменного імені, вони виконують також зворотні DNS-запити. Метою такої поведінки є отримання додаткових доменних імен, пов'язаних з ботнетом, для створення його надлишковості та, як наслідок, підвищення завадостійкості.

Результати аналізу поведінки програмного забезпечення трьох категорій (боти, інше шкідливе ПЗ, нешкідливе ПЗ) залежно від результатів перетворення доменного імені наведено в табл. 3.

Таблиця 3

Поведінка ПЗ залежно від результатів перетворення доменного імені

	DNS активність (к-ть подій)			
	Тип 1	Тип 2	Тип 3	Тип 4
Боти				
Ozdok	0	0	0	1
Bobax	2	1	0	1
Wopla	0	0	0	1
Waledac	0	25	9	7
Virut	0	0	0	1
Інше шкідливе ПЗ				
Netsky	12	10	2	0
Bredolab	0	1	0	0
Lovgate	1	0	1	0
Brontok	0	0	0	1
Ursnif	0	0	1	0
Нешкідливе ПЗ				
BitTorrent	1	0	0	0
avp	0	0	0	0
cuteftp32	1	0	0	0
LimeWire	0	0	0	0
Skype	0	0	0	0

Роз'яснення до табл. 3:

- Тип 1 – Успішне пряме перетворення імені. Підключення не відбулось.
- Тип 2 – Успішне зворотне перетворення імені. Підключення не відбулось.
- Тип 3 – Неуспішне зворотне перетворення імені. Підключення відбулось.
- Тип 4 – Неуспішне зворотне перетворення імені. Підключення не відбулось.

Як видно з вищенаведених результатів, ботам та іншому шкідливому ПЗ притаманна поведінка, що описана четвертим та третім типами відповідно. На підставі цих спостережень Моралес створив евристику, яка допомагає підвищити рівень виявлення такого роду шкідливого ПЗ для хост-орієнтованого антивірусного та іншого ПЗ.

Р. Мацуба вивчав зміни в зразках DNS-трафіку від хостів, інфікованих ботом, що призначений для розсилання спаму [10]. Він встановив, що отримання пошти через POP- протокол (Post Office Protocol) генерує значно менше DNS-трафіку, ніж відправлення пошти через SMTP (Simple Mail Transfer Protocol). Як правило, пошта адресується декільком адресатам, що належать різним доменам, імена яких, своєю чергою, повинні бути коректно перетворені за допомогою DNS в IP-адреси. Там, де відбулось зараження таким ПЗ, зростає SMTP-трафік, і це дає змогу досить ефективно виявляти боти виключно за допомогою моніторингу DNS-трафіку.

Аналіз спам-записів

Однією з найголовніших рис ботнетів є поширення спаму. Практично непрямий підхід для виміру ботнетів та їх активності – аналіз інформації про спам. Слово “непрямий” тут означає, що замість того, аби досліджувати, наприклад, команди управління, аналізуються безпосередньо спам-повідомлення. Очевидно, цим методом можна помітити лише ті боти, які беруть участь у відправленні спаму. Для підвищення ефективності створюють відображення та карти зв'язків між ботнетами та спамом. Це можливо завдяки тому факту, що він розсилається у межах так званих кампаній. Оскільки спам-повідомлення генеруються та розсилаються ботом, вони мають певну схожість, що становить основу конкретного процесу генерації зразків. Під час характеризування також беруть до уваги й інші властивості, такі як: характеристики SMTP-сесії, заголовки тіла листа тощо. Всі ці особливості дозволяють порівнювати спам-повідомлення та агрегувати їх у кампанії та асоціювати отримані кластери з відповідними ботнетами. Для того, щоб такий механізм працював ефективно, зразки спам-листів одержують з ізольованих ботів, які працюють у контрольованому середовищі. На основі заголовків спам-листів можна встановити місце знаходження ботів, а отже, і загальну картину розподілення ботнету.

Недоліком цього методу є те, що можна ідентифікувати лише ті хости, які беруть безпосередню участь у розсиланні спаму. Також, з різних причин, боти можуть не брати участь в спам-активності. Так, наприклад, в імплементації коду бота може бути відсутній модуль, що відповідає за спам, або ця функціональність відімкнена ботмастером у випадку, якщо він вважає, що клієнт перебуває в мережі, яка аналізується. Впровадження спам-приманок може стати суттєвим додатком для такого методу. Спам-приманка – це електронна поштова адреса, що призначена для отримання неочікуваної пошти і не використовується як користувацька та поширюється на форумах, інформаційних каналах тощо. Це дає змогу виявляти основні вектори розсилання спаму й одержувати невідомі зразки шкідливого ПЗ та спам-листів

Аналіз файлів журналювання

Сучасні програми та комп'ютерні системи не лише виконують специфічні завдання, а й повністю документують їх активність у так звані лог-файли. У контексті спам-записів аналіз файлів журналювання є непрямим методом вимірювання та виявлення, котрий має справу із записами, що містять інформацію про дії ботів. Лог-файли, які аналізують, можуть розташовуватись в різних місцях та формуватись різноманітними програмно-апаратними комплексами. Це уможливлює паралельний аналіз вхідних даних від декількох джерел.

Як правило, журнали дозволяють виявляти аномальну активність у мережі. До такої аномалії зараховують, наприклад, нетипову утилізацію ресурсів та сервісів, чи помітні, несуттєві послідов-

ності запитів та відповідей. У цьому контексті утилізація охоплює як кількісні, так і якісні показники.

Наприклад, значне зростання кількості запитів до мережевого сервісу може викрити ботнет-активність. Навіть те, як певний протокол чи сервіс використовується з погляду синтаксичних та семантичних особливостей, може допомогти виявити боти, особливо при стандартних схемах їх взаємодії.

Помічено, що боти використовують URL-адреси для внутрішніх цілей і тому провокують надлишкове зростання активності [1]. Наприклад, бот-мережі Conficker використовують прості запити HTTP, спрямовані до відомих веб-сайтів для синхронізації часу та перевірки стану з'єднання з Інтернетом. Проте, на перший погляд, записи журналу, створеного внаслідок такої поведінки, виглядатимуть як звичайні запити HTTP, згенеровані ПЗ користувацьких комп'ютерів. Такий приклад ілюструє труднощі диференціації поведінки, створеної шкідливим ПЗ, та звичайною активністю.

Концентруючись на аномаліях у файлах журналювання, А. Лінарі показав, що ботнет-мережі можуть бути виявлені й виміряні без будь-яких обов'язкових припущень щодо базової архітектури ботнету [11]. Він продемонстрував свій підхід у дослідженні, в якому аномалії в запитах розподіленого сервісу WHOIS були використані для виявлення і реєстрації діяльності зомбі-мережі.

Висновки

У роботі описано та підсумовано використання пасивних методів виявлення ботнет-мереж, що ґрунтуються на різноманітних технологічних рішеннях та не потребують втручання в роботу інформаційної мережі. Наведено приклади конкретних технік, описано загальні особливості їх роботи, а також основні переваги та недоліки цих методів.

1. An algorithm for anomaly-based botnet detection. Binkley, J. R., Singh, S. In: Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'06), 2006. 2. BotHunter: detecting malware infection through IDS-driven dialog correlation. Gu, G., Porras, P., Yegneswaran, V., Fong, M., Lee, W. In: Proceedings of the 16 th USENIX Security Symposium on USENIX Security Symposium (SS'07), 2007. 3. Using machine learning techniques to identify botnet traffic. Livadas C., Walsh, R., Lapsley, D., Strayer, T. In: Proceedings of the 31st IEEE Conference on Local Computer Networks, 2006. 4. A Proposed Framework for P2P Botnet Detection. Zeidanloo, H. R., Manaf, A., Ahmad, R., Zamani, M., Chaeikar, S. In: IACSIT International Journal of Engineering and Technology, Vol.2, No.2, 2010. 5. Traffic aggregation for malware detection. Yen, T.-F., Reiter, M. K. . In: Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA '08), 2008. 6. Towards automated detection of peer-to-peer botnets: on the limits of local approaches. Jelasity, M., Bilicki, V. In: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more (LEET'09), 2009. 7. Botnet Detection by Monitoring Group Activities in DNS Traffic. Choi, H., Lee H., Lee H., Kim H. In: Proceedings of the 7th IEEE International Conference on Computer and Information Technology (CIT '07), 2007. 8. Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic. Villamarin-Salomon, R., Brustoloni, J.C. In: Proceedings of the 5th IEEE Consumer Communications and Networking Conference (CCNC'08), 2008. 9. Analyzing DNS activities of bot processes. Morales, J.A., Al-Bataineh, A., Shouhuai, Xu, Sandhu, R. In: Proceedings of the 4th International Conference on Malicious and Unwanted Software (MALWARE), 2009. 10. Traffic Analysis on Mass Mailing Worm and DNS/SMTP. Musashi, Y., Sugitani, K., Matsuba, R. In: Proceedings of the 19th IPSJ SIGNotes Computer Security, 2002. 11. A methodology for anomaly and botnet detection and characterisation from application logs. Linari, A., Buckley, O., Duce, D., Mitchell, F., Morris, S. 2010.