ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.7.056.5 **doi: 10.32620/reks.2019.4.01**

С. М. ЛИСЕНКО

Хмельницький національний університет, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ В УМОВАХ КІБЕРЗАГРОЗ НА ОСНОВІ САМОАДАПТИВНОСТІ

Динамічне поширення кіберзагроз зумовлює нагальну необхідність в розробленні нових методів, методик та систем їх виявлення. ***Предметом*** *дослідження є процес забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз.* ***Метою*** *є розроблення методу забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності.* ***Результати.*** *У статті представлена самоадаптивна система для забезпечення резильєнтності корпоративних мереж за наявності кібератак-мереж. Резильєнтність забезпечується адаптивним переконфігуруванням мережі. Переконфігурування мережі здійснюється із залученням сценаріїв безпеки, обраних на основі кластерного аналізу зібраних ознак Інтернет-трафіку, притаманних кібератакам. Для вибору необхідних сценаріїв безпеки запропонований метод використовує нечітку кластеризацію c-means з частковим навчанням. З метою виявлення кібератак на прикладі бот-мереж хостового типу збирається інформація про мережну активність хостів та звіти хостових антивірусів. З метою виявлення кібератак мережного типу здійснюється моніторинг мережної активності, що може свідчити про появу кібератаки. З ознак формуються вектори ознак, які підлягають кластеризації, елементи яких можуть вказувати на появу кіберзагроз у корпоративних мережах. Результатом кластеризації є віднесення кожного вектора ознак до кластеру, де кожен кластер відповідає певній кібератаці, і, в свою чергу, певному сценарію безпеки, який слід застосувати для послаблення кібератак. Приналежність вектора ознак до кластеру вказує на наявність або відсутність кібератаки та відповідно необхідність застосовувати або не застосовувати сценарій безпеки. Для здійснення часткового навчання, тобто побудови початкових центроїдів кластерів, застосовуються промарковані дані. Промарковані дані засновані на знаннях стосовно ознак, які можуть вказувати на атаки бот-мереж у мережі та подаються у вигляді множини векторів ознак. Кожен вектор промаркованих даних належить до одного із заздалегідь визначених кластерів. На основі ознак, представлених у векторах ознак, формується множина правил для опису кожної кібератаки. Множина векторів утворює навчальну вибірку, яка використовується для часткового навчання. Метою методу є вибір сценаріїв безпеки відповідно до кібератак, які здійснюються бот-мережами, для послаблення наслідків атак та забезпечення резильєнтного функціонування мережі.* ***Висновки****. Розроблено метод забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на прикладі бот-мереж на основі самоадаптивності. На основі запропонованого методу розроблено самоадаптивну систему виявлення та послаблення атак, яка демонструє здатність забезпечити стійке функціонування мережі в ситуації наявності кібератак бот-мереж на рівні 70 %.*

Ключові слова: *бот-мережа; кіберзагроза; кібератака; виявлення бот-мереж; захист мережі; самоадаптивні системи; резильєнтність; сценарій безпеки; зловмисне програмне забезпечення; DDoS-атака.*

Вступ

Вирішальною тенденцією в галузі кібербезпеки є перетворення масштабних атак у загальну проблему для компаній.

Останнім часом багатовекторні атаки домінували в розподіленій відмові в обслуговуванні (DDoS), досягаючи майже 55 відсотків типів атак. Найпопулярніші мультивекторні атаки поєднували два вектори, зокрема, UDP-Flood поєднувався з NTP Amplification, TCP SYN Flood та ICMP Flood [1].

На сьогодні основним джерелом широкомасштабних кібератак, зокрема DDoS атак, масового спаму та поширення зловмисного програмного забезпечення є бот-мережі. Бот-мережа – це мережа приватних комп'ютерів, інфікованих шкідливим програмним забезпеченням та керованих як група без відому їх власників, наприклад, для надсилання спаму [2].

За наявності кібератак важливим завданням є вжиття заходів, які дозволять послабити (mitigation) ці атаки та забезпечити стабільне функціонування мережі, тобто резильєнтність мережі.

З точки зору кібербезпеки резильєнтність - це здатність передбачати, протистояти, відновлюватись та пристосовуватися до несприятливих умов, зовнішніх впливів, атак чи порушення нормального фун-

кціонування системи [3, 4].

Поява нових кіберзагроз, збільшення кількості шкідливих програм, а також необхідність резильєнтного функціонування мереж потребують нових інноваційних підходів для забезпечення ефективної інформаційної безпеки комп'ютерних систем у корпоративних мережах [5].

Одним з підходів до забезпечення резильєнтності є надання системі властивості самоадаптивні [6]. Під час свого функціонування самоадаптивні системи здатні накопичувати інформацію з метою оцінки змін у зовнішніх та / або внутрішніх умовах та пристосовуватися до цих змін шляхом адаптації власної поведінки.

Метою адаптації може бути підвищення функціональності, ефективності системи та забезпечення її резильєнтності в умовах повної або часткової невизначеності факторів, які можуть вплинути на адаптивну систему [7].

Це означає, що самоадаптивні системи можуть бути основою нового методу виявлення бот-мереж і бути здатними реагувати на відомі та невідомі атаки, здійснювані бот-мережами. Крім того, він повинен мати можливість здійснювати переконфігурування мережної інфраструктури залежно від типу нападу, типу жертви в мережі тощо.

Аналіз публікацій. Мережні атаки, методи їх виявлення та послаблення

Сьогодні рішення проблем виявлення бот-мереж та безпеки мережі широко представлені в літературі.

Одним із способів вивчення поведінки бот-мереж є використання мереж-приманок. Наприклад, підходи [8,9] представляють детальний аналіз різних атак проти мереж-приманок на базі Linux. Підходи показують, як аналізувати атаки залежно від їх типів, таких як тривалість сесії, країни та регіональний Інтернет-реєстру (RIR) походження атаки. Крім того, мережі-приманки представлені як найефективніший інструмент виявлення та аналізу загроз з Інтернету. Автори показують останні результати для мереж-приманок на базі Dionaea (емуляція служб Windows), Kippo (емуляція служб Linux) та Glastopf (емуляція служб веб-сайтів). Недоліком підходу є те, що розмежування мереж-приманок за їх IP-адресами порівняно грубе.

В роботі [10] описаний підхід механізму захисту рухомої цілі, який захищає автентифікованих клієнтів від DDoS-атак Інтернет-сервісів. Запропонований підхід включає групу динамічних прихованих проксі-серверів для передачі трафіку між автентифікованими клієнтами та серверами. З метою захисту клієнтів вони відокремлюються від зловмисних кібервторгнень за допомогою серій переборів та постійної заміни атакованих проксі-серверів резервними проксі-серверами та перепризначенням атакованих клієнтів на нові проксі. З метою реалізації відокремлення зловмисних вторгнень автори розробили ефективний жадібний алгоритм. Крім того, з метою оцінки ресурсів, необхідних для захисту від DDoS-атак та задоволення визначених рівнів QoS (Quality of Service) під час різних атак, вивчається та оцінюється можливість карантину вторгнень з використанням запропонованого жадібного алгоритму.

У дослідженні [11] пропонується процедура вилучення інформації та виявлення бот-мереж через сліди інфікованої системи з бот-мережею з метою реконструкції атаки бот-мережі та підготовки пакету цифрових доказів, який підтверджує шкідливі дії та шкідливі наслідки цієї атаки в суді.

В [12] представлена таксономія поведінкових ознак бот-мереж, методи виявлення та захисту. Цей загальний огляд підкреслює можливості захисту мережі шляхом виявлення недоліків у існуючих підходах. Крім того, продемонстрована корисність класифікації за розмірами для оцінки методів виявлення бот-мереж за допомогою різних показників. Підхід демонструє особливості поведінки бот-мереж та вплив використання таксономії на точність виявлення бот-мереж.

Підхід, представлений у [13], описує принципи функціонування бот-мереж в різних аспектах: вибір кандидата у боти, побудова мережі, механізми / протоколи зв'язку з C&C та підходи до послаблення наслідків. Дослідження надає математичний аналіз двох підходів до усунення P2P бот-мереж: захист від атак отруєння індексу та Sybil, а також методи пасивного моніторингу, засновані на інфільтрації мережприманок чи захопленні ботів.

У статті [14] представлений підхід для виявлення як низькошвидкісних, так і високошвидкісних DDoS-атак. З цією метою автори використовують та емпірично оцінюють такі інформаційні показники, як ентропія Хартлі, Шеннона, Рені, узагальнена ентропія, розходження Кульбака-Лейблера та узагальнена міра інформаційної відстані. Дослідження включає відповідну метрику, яка полегшує побудову ефективної моделі для виявлення низькошвидкісних та високошвидкісних DDoS-атак.

У роботі [15] з метою забезпечення безпеки мережі наводиться таксономія інструментів для здійснення атак. Автори також представляють всебічний та структурований аналіз існуючих інструментів та систем, які можуть бути корисними як для зловмисників, так і для захисників мережі. У такому контексті обговорюються як переваги, так і недоліки представлених систем. Представлені рішення часто

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

використовуються в мережній інфраструктурі для забезпечення безпеки, але вони неефективні для атак нульового дня.

У [16] проаналізовано мережу підприємства, яка використовує хмарні технології та програмно-конфігуровану мережу. Автори статті вивчали вплив заходів безпеки на механізми захисту від атак DDoS у мережі підприємства. Основна ідея статті полягає в тому, щоб показати, що використання архітектури для послаблення DDoS-атак може допомогти підприємствам захищатись від таких атак. Описана архітектура інтегрує високопрограмований мережний моніторинг, що дозволяє виявляти атаку, та дієву структуру управління для забезпечення швидкої та визначеної реакцію на атаку.

В [17] представлені принципи забезпечення безпеки бездротової мережі. Викладено чітке дослідження основних аспектів безпеки в самоорганізованих мережах та інших мережах, які використовують бездротові технології для зв'язку. Розглянуто основні аспекти безпеки та часто використовувані терміни. Після вивчення критичних проблем безпеки в множині бездротових мереж запропоновано конкретні рішення для загроз безпеки. Основним недоліком запропонованого підходу є те, що він не здатний реагувати на невідомі кібератаки, які виконуються бот-мережами.

У роботі [18] представлено підхід до виявлення аномальних шаблонів мережних з'єднань за допомогою штучних нейронних мереж, імунної системи, нейронечітких класифікаторів та їх комбінацій. У статті описана архітектура системи виявлення вторгнень на основі запропонованого методу. Розроблена система виявлення вторгнень є багаторівневою: в першу чергу проводиться сигнатурний аналіз, потім використовується комбінація адаптивних детекторів. Проведені експерименти демонструють ефективність методів з точки зору хибних спрацювань, виявлень та правильність класифікації.

У [19, 20] описано метод виявлення мережних атак та шкідливого коду. Метод ґрунтується на основних принципах штучної імунної системи, де імунні детектори мають структуру штучних нейронних мереж. Основна мета запропонованого підходу – виявлення раніше невідомих кібератак. Запропонована інтелектуальна система кіберзахисту може підвищити надійність виявлення вторгнень в комп'ютерних системах і, як результат, може зменшити фінансові втрати компаній від кібератак.

Загальні недоліки перерахованих вище підходів полягають в тому, що вони не здатні адаптивно реагувати на відомі та невідомі атаки, здійснені бот-мережами, а також здійснювати переконфігурування мережної інфраструктури залежно від типу кібератаки для забезпечення резильєнтного функціонування мережі.

Виявлення атак бот-мереж у корпоративних мережах

Протягом останніх років було зроблено декілька успішних спроб вирішити проблему виявлення бот-мереж в корпоративних мережах (corporate area networks, CAN). Наші попередні підходи [21,22] пропонували виявлення бот-мереж за допомогою мультиагентної системи. Виявлення бот-мережі здійснювалося за допомогою зв'язків агентів у межах корпоративної мережі. Висновок щодо можливої присутності бот-мереж здійснювався із використанням нечіткої системи, яка враховує інформацію про наявність бот-мереж, отриману з декількох комп'ютерних систем мережі.

Подальший розвиток наших підходів до виявлення бот-мереж включав методи, засновані на використанні DNS [23]. Виявлення бот-мереж здійснювалось за допомогою пасивного моніторингу DNS у мережі та активного DNS-зондування. Це дозволило ідентифікувати бот-мережі, які використовують такі технології ухилення, як періодична зміна IP-відображення, «потік доменів», «швидкозмінні» мережі та DNS-тунелювання. Описаний метод став основою запропонованого інструменту BotGRABBER LAN, здатного збирати DNS-трафік та аналізувати ознаки, отримані з корисного навантаження DNS-повідомлень, що вказують на використання технологій ухилення від виявлення бот-мереж. Висновок про можливу присутність бот-мережі здійснювався за допомогою кластерного аналізу.

Наш підхід, представлений в роботі [24], відобразив еволюцію системи виявлення бот-мереж BotGRABBER. Він був покращений можливістю локалізації бот-мереж в CAN за допомогою не тільки аналізу DNS-трафіку, але й аналізу поведінки шкідливого програмного забезпечення на хостах мережі. Тепер система BotGRABBER здатна відстежувати та аналізувати DNS-трафік, що дозволяє зробити висновок про інфікування мережних хостів ботами. Тим не менш, навіть маючи можливість виявити загрози та локалізувати їх, описана система не в змозі забезпечити резильєнтне функціонування мережі в ситуації атаки бот-мереж. Проблема полягає в тому, що такі загрози не тільки сповільнюють мережу, але й можуть спричинити недоступність мережних служб та всієї інфраструктури, яка стає недієздатною через недостатню пропускну здатність. Враховуючи це, виникають наступні відкриті питання. Що робити у ситуації, коли бот-мережа

здійснює або вже здійснила кібератаки, і мережа нестабільна? Як реагувати на різні ситуації за наявності кібератак бот-мереж, що надходять зсередини чи ззовні мережі? І головне питання: що робити, якщо кібератака невідома антивірусним засобам?

Відповіддю може бути пропозиція побудувати систему, яка зможе адаптивно реагувати на загрози, викликані ботами бот-мережі. Таке реагування полягає у виборі необхідного сценарію безпеки мережних переконфігурувань, щоб уникнути чи послабити вплив атак бот-мереж та забезпечити резильєнтне функціонування мережі.

Самоадаптивна система для забезпечення резильєнтності корпоративних мереж за наявності кібератак бот-мереж

В роботі запропоновано самоадаптивну систему для забезпечення резильєнтності корпоративних мереж за наявності кібератак бот-мереж. Резильєнтність забезпечується адаптивним переконфігуруванням мережі. Це переконфігурування здійснюється із залученням сценарію безпеки, прийнятого на основі кластерного аналізу раніше зібраних ознак, притаманних кібератакам. З ознак формуються вектори ознак, які підлягають кластеризації. Результатом кластеризації є віднесення кожного вектора ознак до кластеру, який відповідає даній кібератаці. Метою методу є вибір необхідного сценарію безпеки мережного переконфігурування відповідно до кібератак, виконаних бот-мережами.

Запропонований підхід включає кілька етапів (рис. 1).

1. **Етап навчання** складається з наступних кроків:

1.1. Формування знань на основі ознак, які можуть вказувати на кібератаки, виконані бот-мережею.

1.2. Представлення знань про кібератаки у вигляді множини векторів ознак.

1.3. Позначення отриманих векторів ознак кібератак з метою формування кластерів, де кожен кластер відповідає певній кібератаці, і, в свою чергу, певному сценарію безпеки, який слід застосувати для послаблення кібератак.

2. **Етап моніторингу** складається з наступних кроків:

2.1. Збирання вхідного та вихідного мережного трафіку та збирання інформації про мережну активність хостів та звіти хостових антивірусів;

2.2. Побудова векторів ознак на основі інформації, отриманої з мережі та хостів.

3. **Етап виявлення** включає в себе реалізацію нечіткої c-means кластеризації з частковим навчанням отриманих векторів ознак з метою віднесення їх до одного з кластерів та вибору відповідного сценарію безпеки.

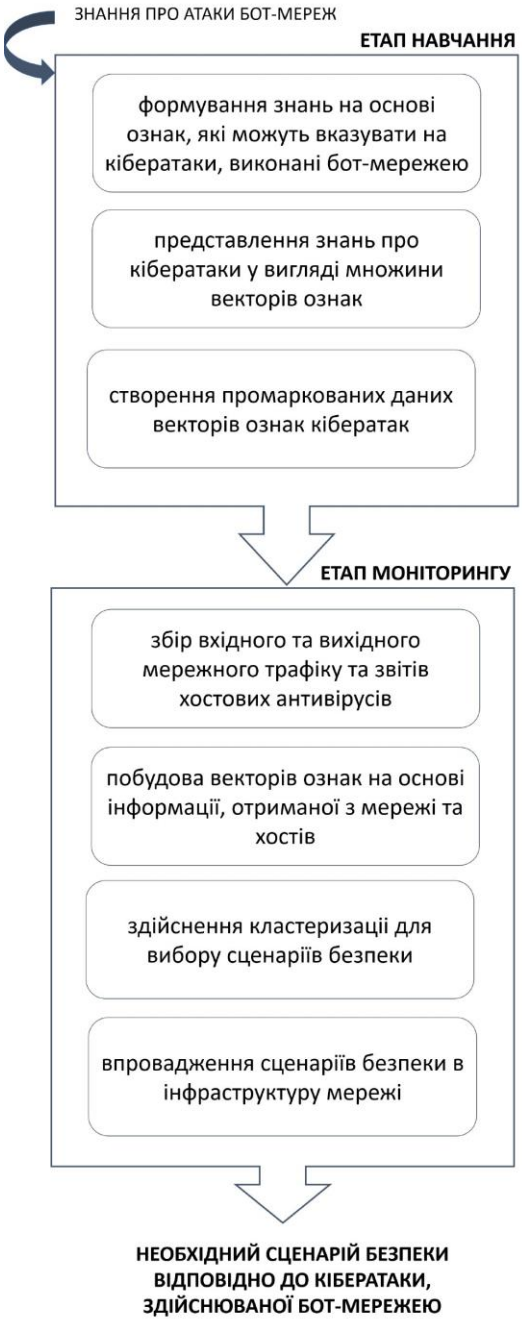


Рис. 1. Процес функціонування самоадаптивної системи для забезпечення резильєнтності корпоративної мережі за наявності кібератак бот-мереж

4. **Етап переконфігурування** включає реалізацію сценарію безпеки інфраструктури корпоративної мережі.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Обговоримо детально кожен крок запропонованого методу.

Формування знань на основі ознак, які можуть вказувати на кібератаки, виконані бот-мережею. Позначимо множину мережних компонентів, на які може бути спрямована атака бот-мережі, як B = {b_1, b_2, b_3}, де b_1 – хост мережі, b_2 – мережний пристрій, b_3 – мережний сервер, $b_i \in B$. Також позначимо множину кібератак, виконану бот-мережею, як $A = \{a_j\}_{j=1}^{N_A}$, де a_1 – атака бот-мережі, що виконується worm-вірусом; a_2 – атака бот-мережі, яка виконується шкідливим програмним забезпеченням (наприклад, троянські програми, Backdoor тощо); a_3 – атака ping flood; a_4 – атака smurf; a_5 – атака TCP SYN Flood; a_6 – атака Fragmented UDP Flood; a_7 – атака DNS Amplification; a_8 – атака TCP Reset; a_9 – атака ICMP Flood; a_{10} – атака SIP INVITE Flood; a_{11} – атака Encrypted SSL DDoS; a_{12} – атака ping sweep; a_{13} – атака SQL/PHP injection; a_{14} – атака Cross-Site Scripting; a_{15} – фішинг атака; a_{16} – атака DNS spoofing; a_{17} – атака ping of death; a_{18} – атака R-U-Dead-Yet DDos (R.U.D.Y.) [25], N_A – кількість кібератак. Ознаки, які необхідно проаналізувати для виявлення вищезазначених кібератак [23, 26, 27]:

1. l_P – середня довжина корисного навантаження у з'єднанні.
2. n_{PZ} – кількість переданих пакетів різного розміру до загальної кількості кадрів у з'єднанні.
3. b_{EH} – загальна кількість байтів у з'єднанні, виключаючи заголовок.
4. b_{TC} – загальна кількість байтів, переданих у з'єднанні.
5. d_C – тривалість з'єднання.
6. b_{OD} – кількість байтів, переданих від відправника до одержувача.
7. p_{OD} – кількість пакетів, переданих від відправника до одержувача.
8. p – протокол передачі.
9. f_{IO} – булева ознака, яка вказує, чи має вхідний трафік пов'язаний з ним вихідний трафік.
10. d_{EL} – тривалість з'єднання, що спостерігається від найбільш раннього пов'язаного вхідного або вихідного трафіку до більш пізнього трафіку.
11. b_S – загальний розмір сесії у байтах.
12. p_S – загальна кількість пакетів у сесії.
13. o_{SS}, i_{SS} – самоподібність вихідних / вхідних пакетів у сесії, визначена шляхом дослідження дисперсії в розмірі вихідних / вхідних пакетів із використанням експоненти Хьорста.
14. v_{OPS}, v_{IPS} – швидкість вихідного / вхідного трафіку, виміряна в пакетах за секунду.
15. v_{OBS}, v_{IBS} – швидкість вихідного / вхідного трафіку, виміряна в бітах на секунду.
16. v_{OBP}, v_{IBP} – швидкість вихідного / вхідного трафіку, виміряна в байтах на пакет.
17. d_{PS} – стандартне відхилення розміру пакету в межах сесії, виміряне в байтах.
18. f_{TCP} – некоректні значення TCP прапорів, спостережувані в даній сесії.
19. f_{GEO} – ознака геолокації, визначена за IP-адресою.
20. s_{RT} – час відповіді сервера, мілісекунди.
21. n_{ARP} – кількість ARP-запитів.
22. r_{NAT} – кількість записів у NAT/PAT-таблиці.
23. m_R – розмір пам'яті роутера, що використовується, мегабайти.
24. p_R – значення процесорного часу роутера,%.
25. n_{DP} – кількість відкинутих пакетів.
26. l_N – довжина доменного імені.
27. n_U – кількість унікальних символів у доменному імені.
28. e_N – ентропія доменного імені
29. t_{mod}, t_{med}, t_{aver} – TTL-періоди (мода, медіана, середнє арифметичне значення).
30. n_A – кількість A-записів, що відповідають доменному імені, у вхідному DNS-повідомленні.
31. n_{IP} – кількість IP-адрес, що пов'язані з доменним іменем s_{IP} – середня відстань між IP-адресами, пов'язаними з доменним іменем.
32. s_A – середня відстань між IP-адресами в множині A-записів для доменного імені у вхідному DNS-повідомленні.
33. n_{UA} – кількість унікальних IP-адрес в множинах A-записів, що відповідають доменному імені, в DNS-повідомленнях.
34. s_{UA} – середня відстань між унікальними IP-адресами в множинах A-записів, що відповідають доменному імені, в DNS-повідомленнях.
35. n_D – кількість доменних імен, які спільно використовують IP-адресу, що відповідає доменному імені.
36. f_{UR} – ознака використання рідковживаних типів записів DNS або DNS-записів, які зазвичай не використовуються типовим клієнтом, 0 – якщо таке використання є, 1 – інакше.
37. e_R, f_{Eb} – ентропія DNS-записів, які містяться в DNS-повідомленнях.
38. l_P – максимальний розмір DNS-повідомлень щодо доменного імені.
39. f_S – ознака успішності DNS-запиту.

Позначимо набір сценаріїв безпеки як $S = \{s_m\}_{m=1}^{N_S}$, де N_S – кількість сценаріїв безпеки, які слід застосувати залежно від типу атаки, яку здійснює бот-мережа. Таким чином, функція вибору сценарію безпеки для відновлення мережі за наявності визначеного типу атаки бот-мережі f може бути представлена як: f: $b_i \times a_j \rightarrow s_m$.

Представлення знань про кібератаки у вигляді множини векторів ознак. Усі вищезазначені ознаки є основою множини векторів ознак $X = \{x_k\}_{k=1}^{N}$, де кожна з ознак вектора x_k описує кібератаку або її відсутність, N – кількість векторів ознак. На основі ознак, представлених у векторах ознак, формується множина правил R для опису ко-

жної кібератаки. Множина векторів утворює навчальну вибірку, яка використовується для часткового навчання.

Приклад правила R_{b2}, яке описує атаку на мережні хости та здійснює вибір необхідного сценарію безпеки, може бути представлений наступним чином:

$$\text{if}\left(\left(l_N \in [75,255] \text{ and } n_U \in (27,37]\right)\text{or}\right.$$
$$\text{or}\left(e_N \geq f_{Eb32} \text{ or}\left(e_R \geq f_{Eb64} \text{ or } e_R \geq f_{Eb256}\right)\text{or}\right.$$
$$\left.\left.\text{or } f_{UR}=1\right)\right)\text{and } l_p\text{>300} \Rightarrow a_2 \Rightarrow s_2. \qquad (1)$$

ПРИМІТКА. Якщо спостерігаються різні значення щодо однієї і тієї самої атаки, то система виробляє різні сценарії безпеки. Наприклад, та сама атака може бути спрямована проти сервера або проти мережних хостів. У цьому випадку будуть використовуватися різні правила R_{bi} та застосовуватимуться різні сценарії безпеки.

Маркування отриманих векторів ознак кібератак з метою формування кластерів. Нехай c – кількість попередньо визначених кластерів векторів ознак. Кожен кластер відповідає визначеним кібератакам (і, відповідно, сценаріям безпеки, які слід застосувати), причому один з кластерів відповідає відсутності атак.

Приналежність вектора ознак x_k до і-го кластеру вказує на наявність або відсутність кібератаки та відповідно необхідність застосовувати або не застосовувати сценарій безпеки.

Для побудови центроїда (прототипу) і-го кластера, v_i, застосовуються промарковані дані. Промарковані дані засновані на знаннях стосовно ознак, які можуть вказувати на атаки бот-мереж у мережі та подаються у вигляді множини векторів ознак. Кожен вектор x_k промаркованих даних належить до одного із заздалегідь визначених кластерів.

Нечітка c-means кластеризація з частковим навчанням ґрунтується на мінімізації наступної цільової функції [28]:

$$J_k = \sum_{i=1}^{c}\sum_{k=1}^{N} u_{ik}^{p} d_{ik}^{2} +$$
$$+a\sum_{i=1}^{c}\sum_{k=1}^{N}(u_{ik}-f_{ik}b_k)^{p} d_{ik}^{2}, \qquad (2)$$

де N – загальна кількість векторів ознак, що підлягають кластеризації (промарковані та непромарковані вектори ознак); u_{ik} – значення приналежності k-го вектора ознак до і-го кластера; f_{ik} – значення приналежності k-го промаркованого вектора ознак до і-го кластера; d_{ik} – відстань між k-м вектором ознак та прототипом і-го кластера; $b = [b_k]$ – булевий індикатор, який розрізняє промарковані та немарковані вектори ознак:

$$b_k = \begin{cases} 1, \text{ якщо } x_k \text{ промаркований,} \\ 0, \text{ в іншому випадку.} \end{cases} \qquad (3)$$

Центроїд і-го кластеру, v_i, і матриця розбиття u_{ik} представлені у вигляді формул (4) [28]:

$$u_i = \frac{\sum_{k=1}^{N} u_{ik}^{2} x_k}{\sum_{k=1}^{N} u_{ik}^{2}},$$

$$u_{ik} = \frac{1}{1+a}\left\{\frac{1+a\left(1-b_k\sum_{l=1}^{c} f_{lk}\right)}{\sum_{l=1}^{c}\left(\frac{d_{ik}}{d_{lk}}\right)^{2}} + af_{ik}b_k\right\}, \qquad (4)$$

де α позначає коефіцієнт масштабування для підтримки балансу між контрольованими та неконтрольованими компонентами в межах механізму оптимізації [28].

В якості метрики відстані між k-м вектором ознак та центроїдом кластера була використана відстань Махаланобіса:

$$d_{ik} = \left\|x_k - u_i\right\|^{T} A\left\|x_k - u_i\right\|, \qquad (5)$$

при цьому A є позитивно визначеною матрицею $R_n \times R_n$.

Збір вхідного та вихідного мережного трафіку, інформації про мережну активність хостів, а також звітів хостових антивірусів. На цьому етапі методу з метою виявлення кібератак мережного типу здійснюється моніторинг мережної активності, що може свідчити про появу кібератаки. З метою виявлення кібератак хостового типу збирається інформація про мережну активність хостів та звіти хостових антивірусів. Зібрана інформація надсилається класифікатору для подальшого аналізу.

Побудова векторів ознак на основі інформації, отриманої з мережі та хостів, та здійснення нечіткої кластеризації c-means з частковим навчанням для вибору сценаріїв безпеки. Дані, зібрані на попередньому етапі, в подальшому аналізуються. Результатом аналізу є висновок щодо наявності або відсутності атаки та відповідний сценарій безпеки для переконфігурування мережі. В якості засобу вибору сценарію безпеки було застосовано нечітку кластеризацію c-means з частковим навчанням. На етапі виявлення об'єктами кластеризації є вектори ознак x_k, отримані при аналізі корисного

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

навантаження вхідного та вихідного трафіка, а також звітів антивірусних засобів про можливе інфікування хостів. Результатом кластеризації є значення приналежності u_{ik} вектора ознак x_k до кожного кластеру i. Приналежність вектора ознак x_k до і-го кластеру визначає сценарій переконфігурування мережі, який слід застосувати у випадку атаки бот-мережі.

Впровадження сценаріїв безпеки в інфраструктуру корпоративної мережі. Виходячи з вибору, зробленого на попередньому етапі, повинен бути застосований відповідний сценарій безпеки. Кожен сценарій містить перелік дій з переконфігурування мережі.

Наприклад, для послаблення наслідків R.U.D.Y. DDoS атаки на сервер, можливе обрання сценарію безпеки, який включає наступні дії:

- зменшення проміжку часу, протягом якого сервер буде чекати певних подій до відмови у запиті;

- зменшення проміжку часу, протягом якого сервер буде чекати наступних запитів в неперервному з'єднанні;

- зменшення розмірів запитів клієнтів: розмір заголовка запиту HTTP, дозволений клієнту, кількість полів заголовка HTTP-запиту, які будуть прийняті від клієнта, а також розмір рядка запиту HTTP, який буде прийнятий від клієнта;

- зменшення максимального розміру завантажуваних файлів: загального розміру тіла запиту HTTP, що надсилається клієнтом;

- розмір тіла запиту на основі XML;

- зменшення максимальної кількості запитів, які можуть бути обслуговані одночасно, при цьому будь-яка їх кількість, що перевищує ліміт, заноситься в чергу (обмеження кількості клієнтів);

- зменшення максимального розміру даних, що надсилаються до сервера: максимального розміру даних POST, а також зменшення розміру даних POST, виключаючи завантажувані файли;

- зменшення кількості даних "тіла запитів" (POST даних), які повинні зберігатись в пам'яті (RAM);

- блокування трафіку від імен хостів та IP-адрес, які є джерелами шкідливого трафіку.

ПРИМІТКА. Система також включає кілька сценаріїв безпеки, які містять рекомендації щодо перевстановлення вже інфікованих систем. У більшості випадків інфікування бот-мережею не може бути повністю усунуто автоматично, і переконфігурування мережі або хостів неефективне. Це може статися, наприклад, у ситуації пандемічних атак, таких як Petya.A [29].

Експерименти

Для визначення ефективності запропонованого методу було проведено ряд експериментів. В експериментах було використано локальну мережу з 50 хостів (кожен з операційною системою Microsoft Windows), один виділений сервер (операційна система Linux OpenSusE з nginx HTTP-сервером). Експерименти тривали 24 години. Мережний трафік захоплювався за допомогою утиліти tcpdump. Вся функціональність запропонованого методу була реалізована в системі BotGRABBER, описаній у розділі 2.2.

Під час експериментів було здійснено 150 атак різних типів на хости, сервер та маршрутизатори. Метою було визначення, чи зможе корпоративна мережа функціонувати в ситуації здійснення атак (наприклад, чи зможуть сервер, хости або мережний маршрутизатор відновити функціонування з належним часом відгуку). У даній роботі обговорюються детальні результати експериментів із залученням атак R.U.D.Y., smurf та MAC flooding [25].

R.U.D.Y. атака на мережевий сервер – це засіб низькорівневої повільної атаки, призначений для спричинення збоїв у роботі веб-сервера шляхом передачі довгих полів форми. Атака виконується за допомогою інструменту DoS, який переглядає цільовий веб-сайт та виявляє вбудовані веб-форми. Після того, як форми були виявлені, R.U.D.Y. надсилає легітимні HTTP POST-запити з аномально довгим полем заголовка «content-length», після чого починає вводити у форму інформацію по одному байту на пакет. Такий тип атак є важким для виявлення порівняно з об'ємними DDoS-атаками, які помітні через аномально високі коливання вхідного трафіку. Для того, щоб здійснити атаку R.U.D.Y., був використаний відповідний інструмент [30].

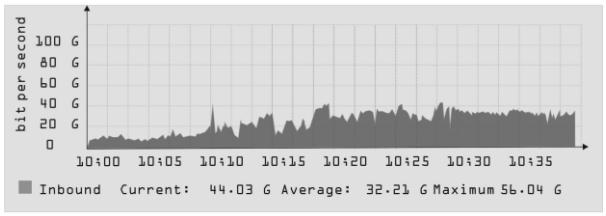
Для smurf атаки характерна велика кількість пакетів ICMP з підробленою IP-адресою жертви з використанням широкомовної IP-адреси. Це змушує пристрої в мережі у відповідь надсилати відповіді на IP-адресу джерела. Для того, щоб здійснити smurf атаку, було використано мережний генератор пакетів Hyenae [31].

Атака MAC flooding заснована на захопленні таблиці MAC-адрес (CAM-таблиці) комутатора: коли ця таблиця буде заповнена повністю, то трафік, який спрямований на адреси, які вже неможливо дізнатись, буде відтворений. Для здійснення атаки MAC flooding було використано інструмент Dsniff (macof) [32].

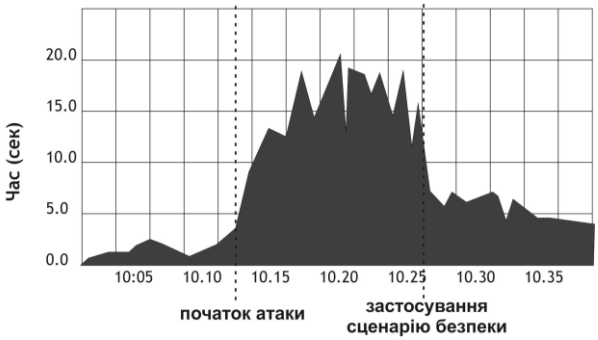
Рис. 2-4 демонструють значення рівня трафіка та часу відгуку сервера перед атакою, під час атаки та після застосування сценарію безпеки. Таким чином, можна побачити, що під час R.U.D.Y. атаки

рівень трафіка залишався майже незмінним (рис. 2, а), але час відгуку сервера збільшувався, що спричиняло недоступність сервісів (рис. 2, б).

Застосування сценарію безпеки, виробленого системою BotGRABBER, виявило незначні зміни у рівні трафіку, при цьому час відгуку сервера зменшився і сервер відновив функціонування з належним часом відгуку.



а



б

Рис. 2. Рівень трафіку (а) та час відгуку сервера (б) до, під час та після атаки R.U.D.Y.

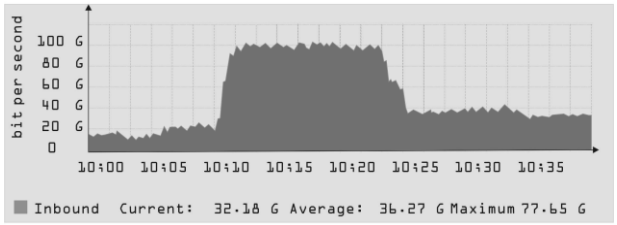
Під час smurf атаки значно підвищувався як рівень трафіку, так і час відгуку сервера. Реалізація сценарію безпеки, виробленого системою BotGRABBER, виявила значну зміну рівня трафіку (рис. 3а), в той час як час відгуку сервера зменшився до нормального рівня, і сервер також відновив функціонування з належним часом відгуку (рис. 3, б).

З іншого боку, експерименти із залученням атаки MAC flooding не лише продемонстрували зростаючий рівень трафіку та час відгуку, але й спричинили ситуацію, коли система продемонструвала неможливість автоматизованої переконфігурування мережі (рис. 4). У цій ситуації довелося виконувати заходи послаблення наслідків атаки вручну.

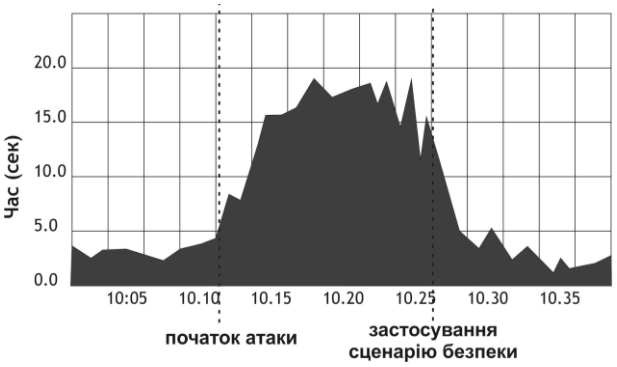
Для оцінки резильєнтності мережі було використано інтегровану метрику, представлену в [33]:

$$GR = R \times \left(\frac{RAPI_{RP}}{RAPI_{DP}} \right) \times (TAPL)^{-1} \times RA, \quad (6)$$

де R – надійність (або опір), що є мірою для оцінки здатності і кількісно визначає мінімальне значення

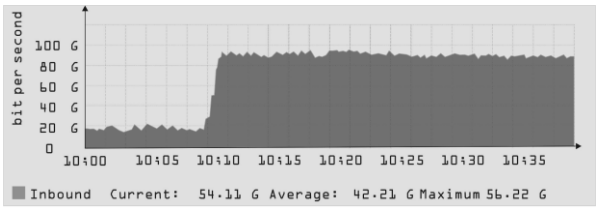


а

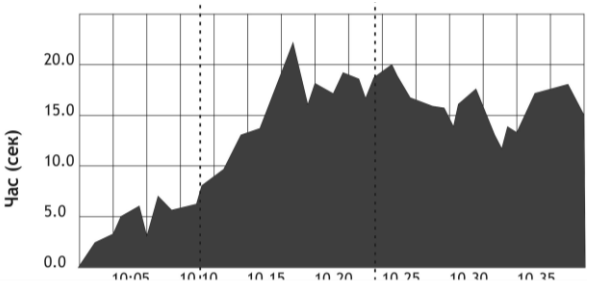


б

Рис. 3. Рівень трафіка (а) та час відгуку сервера (б) до, під час та після smurf атаки



а



б

Рис. 4. Рівень трафіка (а) та час відгуку сервера (б) до, під час та після атаки MAC flooding

MOP між t_d і t_{ns}, MOP – це показник продуктивності системи (мережі), який нормалізується між 0 і 1 (де 0 – загальна втрата функціонування і 1 – цільове значення MOP під час нормального функціонування мережі); t_d – час, коли мережа перебуває під впливом атаки бот-мережі, а t_{ns} – час, коли мережа була

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

переконфігурована на основі запропонованого сценарію безпеки; $RAPI_{DP}$ – швидкість під час фази атаки бот-мережі, яка може бути наближена до середньої кривизни функції MOP; $RAPI_{RP}$ – швидкість під час фази переконфігурування мережі; TAPL – усереднена в часі втрата продуктивності, яка враховує час появи атаки бот-мережі аж до переконфігурування мережі; RA – здатність до переконфігурування, кількісна міра, яка описує продуктивність системи, досягнуту після застосування сценарію безпеки.

Вибір відповідного значення MOP залежить від конкретного сервісу, що надається аналізованою інфраструктурою.

Вважатимемо, що переконфігурування мережі під час атаки є успішним, якщо GR> δ, де δ – попередньо визначений поріг. Враховуючи метрику резильєнтності, рівні успішної переконфігурування мережі, що призводять до послаблення атак, представлені в таблиці 1.

Таблиця 1

Підсумки результатів експериментів

Ціль атаки	Кількість атак	Кількість успішних переконфігурувань
Хости мережі	50	41
Сервер	50	38
Маршрутизатори	50	36
Всього	150	105

Таким чином, залучення адаптивної системи до BotGRABBER демонструє здатність забезпечити стійке функціонування мережі в ситуації наявності кібератак бот-мереж на рівні 70 %.

Обговорення

Незважаючи на перспективні результати експериментів, є деякі рекомендації щодо кращого функціонування BotGRABBER. Для забезпечення ефективного функціонування першим завданням є створення коректних сценаріїв безпеки. Проблема полягає в тому, що побудова сценаріїв безпеки залежить від таких складових, як мережна архітектура, мережні пристрої, операційні системи хостів, властивості та функції сервера тощо. Усі ці фактори значно впливають на зміст сценаріїв безпеки. Ось чому в подальших дослідженнях потрібно включити до BotGRABBER можливість вибору груп сценаріїв безпеки в залежності від вищезгаданих мережних компонентів із їх програмним забезпеченням.

На даний час основний недолік підходу полягає в тому, що система BotGRABBER не в змозі виявити всі кібератаки і, отже, не охоплює відповідних сценаріїв безпеки. Причиною є те, що деякі атаки є багатовекторними, а в деяких випадках неможливо побудувати всі варіанти атаки. Однак використання нечіткої кластеризації, заснованої на знаннях про атаки бот-мереж, дозволяє зробити висновок про можливі невідомі атаки, а отже, запропонувати сценарій безпеки для послаблення впливу атак бот-мереж та забезпечення надійного функціонування мережі. Інший аспект функціонування BotGRABBER полягає в тому, що існує можливість виникнення ситуації, коли сценарії безпеки можуть містити рекомендації щодо ручного налаштування замість автоматизованого переконфігурування мережі (необхідність звернутися до системного адміністратора).

Підводячи підсумки, варто зазначити, що розроблена методика демонструє прийнятні результати для забезпечення резильєнтного функціонування мережі при наявності кібератак бот-мереж. Майбутня робота повинна передбачати такі вдосконалення, як здобуття нових знань про відомі та нові кібератаки, які зможуть усунути наявні проблеми.

Висновки

У статті представлена самоадаптивна система для забезпечення резильєнтності корпоративних мереж за наявності кібератак бот-мереж. Резильєнтність забезпечується адаптивним переконфігуруванням мережі. Відповідь на питання про те, як потрібно переконфігурувати мережу, отримується за допомогою кластерного аналізу ознак кібератак, які спостерігаються в мережі та на мережних хостах. Для того, щоб обрати необхідний сценарій безпеки, запропонований метод використовує нечітку c-means кластеризацію з частковим навчанням. Об'єктами кластеризації є вектори ознак трафіку, які можуть вказувати на появу кіберзагроз у корпоративної мережі. Метою методу є вибір сценаріїв переконфігурування мережі та мережних хостів відповідно до кібератак, що виконуються бот-мережами. Використання розробленої системи дає можливість виявити високий відсоток відомих і невідомих багатовекторних кібератак, здійснених бот-мережами. Результати експериментів продемонстрували, що запропонований метод забезпечує резильєнтне функціонування мережі за наявності кібератак бот-мереж на рівні близько 70%.

Література

1. NEXUSGUARD. DDoS Threat Report 2019 Q3 [Електронний ресурс]. – Режим доступу: https://www.nexusguard.com/threat-report-q3-2017. – 9.11.2019 р.

2. Oxford Dictionaries [Електронний ресурс]. – Режим доступу: http://www.oxforddictionaries.com/definition/english/botnet?q=botnet. – 9.11.2019 р.

3. SearchDataCenter. Data center resiliency [Електронний ресурс]. – Режим доступу: http://searchdatacenter.techtarget.com/definition/resiliency. – 9.11.2019 р.

4. Giudice, M. Crowe Horwath. Resilience Going Beyond Security to a New Level of Readiness, 2016 [Електронний ресурс] / M. Giudice , C. Wilkinson. – Режим доступу: https://www.crowehorwath.com/insights/asset/cyber-resilience-readiness-level. – 9.11.2019 р.

5. Knapp, E. D. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. [Text] / E. D. Knapp, J. T. Langill. – Syngress, 2014. – 460 p.

6. Software engineering for self-adaptive systems: A research roadmap [Text] / B. H. Cheng, R. De Lemos, H. Giese, P. Inverardi, J. Magee, J. Andersson, G. D. M. Serugendo // Software engineering for self-adaptive systems. – Springer Berlin Heidelberg, 2009. – P. 1-26.

7. Self-adaptive systems: A survey of current approaches, research challenges and applications [Text] / F. D. Macas-Escriv, R. Haber, R. Del Toro, V. Hernandez // Expert Systems with Applications. – 2013. – Vol. 40, No. 18. – P. 7267-7279.

8. Zuzcak, M. Behavioral analysis of bot activity in infected systems using honeypots [Text] / M. Zuzcak, T. Sochor // Communications in Computer and Information Science. – Springer, Cham, 2017. – Vol. 718. – P. 118-133.

9. Sochor, T. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection [Text] / T. Sochor, M. Zuzcak // 22nd Int. Conf. Computer Networks: Communications in Computer and Information Science. – Springer International, Cham, 2015. – P. 69-81.

10. A moving target DDoS defense mechanism [Text] / H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, A. Stavrou // Computer Communications. – 2014. – Vol. 46. – P. 10-21.

11. Javadianasl, Y. A Practical Procedure for Collecting More Volatile Information in Live Investigation of Botnet Attack [Text] / Y. Javadianasl, A. A. Manaf, M. Zamani // Multimedia Forensics and Security . – Springer, 2017. – P. 381-414.

12. A taxonomy of botnet behavior, detection, and defense [Text] / S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, S. A. Khayam // IEEE communications surveys & tutorials. – 2014. – Vol. 16, No. 2. – P. 898-924.

13. Analysis of Peer-to-Peer botnet attacks and defenses [Text] / P. Wang, L. Wu, B. Aslam, C. C. Zou // Propagation phenomena in real world networks. – Springer International Publishing, 2015. – P. 183-214.

14. Bhuyan, M. H. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection [Text] / M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita // Pattern Recognition Letters. – 2015. – Vol. 51. – P. 1-7.

15. Network attacks: Taxonomy, tools and systems [Text] / N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, J. K. Kalita // Journal of Network and Computer Applications. – 2014. – Vol. 40. – P. 307-324.

16. DDoS attack protection in the era of cloud computing and software-defined networking [Text] / B. Wang, Y. Zheng, W. Lou, Y. T. Hou // Computer Networks. – 2015. – Vol. 81. – P. 308-319.

17. Pathan, A. S. K. Security of self-organizing networks: MANET, WSN, WMN, VANET [Text] / A. S. K. Pathan. – CRC press, 2016. – 638 p.

18. Branitskiy, A. Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers [Text] / A. Branitskiy, I. Kotenko // 2015 IEEE 18th International Conference on Computational Science and Engineering (CSE), 2015. – P. 152-159.

19. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques [Text] / M. Komar, A. Sachenko, S. Bezobrazov, V. Golovko // Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2016. Communications in Computer and Information Science. – Springer, Cham, 2017. – Vol. 783. – P. 36-55.

20. The methods of artificial intelligence for malicious applications detection in Android OS [Text] / S. Bezobrazov, A. Sachenko, M. Komar, V. Rubanau // International Journal of Computing. – 2016. – Vol. 15, No. 3. – P. 184-190.

21. Lysenko, S. Botnet detection technique for corporate area network [Text] / S. Lysenko, O. Savenko, A. Kryshchuk, Y. Kljots // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013. – P. 363-368.

22. Savenko, O. Multi-agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic [Text] / O. Savenko, S. Lysenko, A. Kryshchuk // International Conference on Computer Networks. – Springer, 2013. – P. 146-156.

23. Antievasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing [Text] / O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, K. Bobrovnikova // International Conference on Computer Networks. – Springer International Publishing, 2016. – P. 83-95.

24. Information Technology for Botnets Detection Based on Their Behaviour in the Corporate Area Network [Text] / S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk, B. Savenko // International Conference on Computer Networks. – Springer, Cham, 2017. – P. 166-181.

25. IMPERVA INCAPSULA [Електронний ресурс] – Режим доступу: https://www.incapsula.com/ddos/attack-glossary. – 9.11.2019 р.

26. RUDY Attack: Detection at the Network Level and Its Important Features [Text] / M. M. Najafabadi, T. M. Khoshgoftaar, A. Napolitano, C. Wheelus // FLAIRS Conference, 2016. – P. 288-293.

27. Alejandre, F. V. Botnet Detection using Clustering Algorithms [Text] / F. V. Alejandre, N. C.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Corts, E. A. Anaya // Research in Computing Science. – 2016. – Vol. 118. – P. 65-75.

28. Pedrycz, W. Fuzzy clustering with partial supervision [Text] / W. Pedrycz, J. Waletzky // IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). – 1997. – Vol. 27, No. 5. – P. 787-795.

29. VIRUS BULLETIN. Grooten, M. VB2017 videos on attacks against Ukraine, 2017 [Електронний ресурс] – Режим доступу: https://www. virusbulletin.com/blog/2017/12/vb2017-videos-attacks-against-ukraine/. – 9.11.2019 р.

30. SOURCE FORGE. R-U-Dead-Yet? (RUDY) Original source code files [Електронний ресурс] – Режим доступу: https:// sourceforge.net/projects/r-u-dead-yet/. – 9.11.2019 р.

31. SOURCE FORGE. Hyenae [Електронний ресурс]. – Режим доступу: https://sourceforge.net /projects/hyenae/. – 9.11.2019 р.

32. dsniff [Електронний ресурс]. – Режим доступу: https://www.monkey.org/~dugsong/dsniff. – 9.11.2019 р.

33. Linkov, I. Resilience and risk: Methods and application in environment, cyber and social domains [Text] / I. Linkov, J. M. Palma-Oliveira. – Springer, 2017. – 580 p.

References

1. *NEXUSGUARD*. DDoS Threat Report 2019 Q3. Available at: https://www.nexusguard.com /threat-report-q3-2017 (accessed 9.11.2019).

2. *Oxford Dictionaries*. Available at: http://www. oxforddictionaries.com/definition/english/botnet?q=bot net (accessed 9.11.2019).

3. *SearchDataCenter*. Data center resiliency. Available at: http://searchdatacenter.techtarget. com/definition/resiliency (accessed 9.11.2019).

4. Giudice, M., Wilkinson, C. *Crowe Horwath. Resilience Going Beyond Security to a New Level of Readiness*, 2016. Available at: https://www. crowehorwath.com/insights/asset/cyber-resilience-readiness-level (accessed 9.11.2019).

5. Knapp, E. D., Langill, J. T. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014. 460 p.

6. Cheng, B. H., De Lemos, R., Giese, H., Inverardi, P., Magee, J., Andersson, J., Serugendo, G. D. M. Software engineering for self-adaptive systems: A research roadmap. In: *Software engineering for self-adaptive systems*, Springer Berlin Heidelberg, 2009, pp. 1-26.

7. Macas-Escriv, F. D., Haber, R., Del Toro, R., Hernandez, V. Self-adaptive systems: A survey of current approaches, research challenges and applications. *Expert Systems with Applications*, 2013, vol. 40, no. 18, pp. 7267-7279.

8. Zuzcak, M., Sochor, T. Behavioral analysis of bot activity in infected systems using honeypots. In: *Communications in Computer and Information Science*: Springer, Cham, 2017, vol. 718, pp. 118-133.

9. Sochor, T., Zuzcak, M. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. In: *22nd Int. Conf. Computer Networks: Communications in Computer and Information Science*: Springer International, Cham, 2015, pp. 69-81.

10. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A. A moving target DDoS defense mechanism. *Computer Communications*, vol. 46, 2014, pp. 10-21.

11. Javadianasl, Y., Manaf, A. A., Zamani, M. A Practical Procedure for Collecting More Volatile Information in Live Investigation of Botnet Attack. In: *Multimedia Forensics and Security*, Springer, 2017, pp. 381-414.

12. Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., Khayam, S. A. A taxonomy of botnet behavior, detection, and defense. *IEEE communications surveys & tutorials*, 2014, vol. 16, no. 2, pp. 898-924.

13. Wang, P., Wu, L., Aslam, B., Zou, C. C. Analysis of Peer-to-Peer botnet attacks and defenses. In: *Propagation phenomena in real world networks*, Springer International Publishing, 2015, pp. 183-214.

14. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, vol. 51, 2015, pp. 1-7.

15. Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., Kalita, J. K. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, vol. 40, 2014, pp. 307-324.

16. Wang, B., Zheng, Y., Lou, W., Hou, Y. T. DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, vol. 81, 2015, pp. 308-319.

17. Pathan, A. S. K. (Ed.). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016. 638 p.

18. Branitskiy, A., Kotenko, I. Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers. In: *2015 IEEE 18th International Conference on Computational Science and Engineering (CSE)*, 2015, pp. 152-159.

19. Komar, M., Sachenko, A., Bezobrazov, S., Golovko, V. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques. In: *Ginige A. et al. (eds) Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2016. Communications in Computer and Information Science*: Springer, Cham, vol. 783, 2017, pp. 36-55.

20. Bezobrazov, S., Sachenko, A., Komar, M., Rubanau, V. The methods of artificial intelligence for malicious applications detection in Android OS. *International Journal of Computing*, 2016, vol. 15, no. 3, pp. 184-190.

21. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: *Proceedings of the 2013 IEEE 7th*

International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013, pp. 363-368.

22. Savenko, O., Lysenko, S., Kryshchuk, A. Multi-agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. In: *International Conference on Computer Networks*: Springer, 2013, pp. 146-156.

23. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A., Bobrovnikova, K. Antievasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing. In: *International Conference on Computer Networks*: Springer International Publishing, 2016, pp. 83-95.

24. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., Savenko, B. Information Technology for Botnets Detection Based on Their Behaviour in the Corporate Area Network. In: *International Conference on Computer Networks*: Springer, Cham, 2017, pp. 166-181.

25. *IMPERVA INCAPSULA.* Available at: https://www.incapsula.com/ddos/attack-glossary (accessed 9.11.2019).

26. Najafabadi, M. M., Khoshgoftaar, T. M., Napolitano, A., Wheelus, C. RUDY Attack: Detection at the Network Level and Its Important Features. In: *FLAIRS Conference*, 2016, pp. 288-293.

27. Alejandre, F. V., Corts, N. C., Anaya, E. A. Botnet Detection using Clustering Algorithms. *Research in Computing Science*, vol. 118, 2016, pp. 65-75.

28. Pedrycz, W., Waletzky, J. Fuzzy clustering with partial supervision. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 1997, vol. 27, no. 5, pp. 787-795.

29. *VIRUS BULLETIN.* Grooten, M. VB2017 videos on attacks against Ukraine, 2017. Available at: https://www.virusbulletin.com/blog/2017/12/vb2017-videos-attacks-against-ukraine/ (accessed 9.11.2019).

30. *SOURCE FORGE.* R-U-Dead-Yet? (RUDY) Original source code files. Available at: https:// sourceforge.net/projects/r-u-dead-yet/ (accessed 9.11.2019).

31. *SOURCE FORGE.* Hyenae. Available at: https://sourceforge.net/projects/hyenae/ (accessed 9.11.2019).

32. *dsniff.* Available at: https://www.monkey.org/ ~dugsong/dsniff (accessed 9.11.2019).

33. Linkov, I., Palma-Oliveira, J. M. (Eds.) *Resilience and risk: Methods and application in environment, cyber and social domains.* Springer, 2017. 580 p.

Надійшла до редакції 10.11.2019, розглянута на редколегії 10.12.2019

МЕТОД ОБЕСПЕЧЕНИЯ РЕЗИЛЬЕНТНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ В УСЛОВИЯХ КИБЕРУГРОЗ НА ОСНОВЕ САМОАДАПТИВНОСТИ

С. Н. Лысенко

Динамическое распространение киберугроз предопределяет необходимость в разработке новых методов, методик и систем их обнаружения. **Предметом** исследования является процесс обеспечения резильентности компьютерных систем в условиях киберугроз. **Целью** является разработка метода обеспечения резильентности компьютерных систем в условиях киберугроз на основе самоадаптивности. **Результаты**. представлена самоадаптивная система для обеспечения резильентности корпоративных сетей при наличии кибератак бот-сетей. Резильентность обеспечивается адаптивным изменением конфигурации сети. Изменение конфигурации сети осуществляется с привлечением сценариев безопасности, выбранных на основе кластерного анализа собранных признаков Интернет-трафика, присущих кибератакам. Для выбора необходимых сценариев безопасности предложенный метод использует нечеткую кластеризацию c-means с частичным обучением. С целью выявления кибератак хостового типа собирается информация о сетевой активности хостов и отчеты хостовых антивирусов. С целью выявления кибератак сетевого типа осуществляется мониторинг сетевой активности, которая может свидетельствовать о появлении кибератаки. Из признаков формируются векторы признаков, подлежащих кластеризации, элементы которых могут указывать на появление киберугроз в корпоративных сетях. Результатом кластеризации является отнесение каждого вектора признаков к кластеру, где каждый кластер соответствует определенной кибератаке, и, в свою очередь, определенному сценарию безопасности, который следует применить для ослабления кибератак. Таким образом, принадлежность вектора признаков к кластеру указывает на наличие или отсутствие кибератаки и соответственно необходимость применять или не применять сценарий безопасности. Для осуществления частичного обучения, то есть построения начальных центроидов кластеров, применяются промаркированные данные. Промаркированные данные основаны на знаниях относительно признаков, которые могут указывать на атаки бот-сетей в сети и представляются в виде множества векторов признаков. Каждый вектор промаркированных данных принадлежит к одному из заранее определенных кластеров. На основе признаков, представленных в векторах признаков, формируется множество правил для описания каждой кибератаки. Множество векторов образует обучающую выборку, которая используется для частичного обучения. Целью метода является выбор сценариев безопасности в соответствии с кибератаками, которые осуществляются бот-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

сетями, для ослабления последствий атак и обеспечения резильентного функционирования сети. **Выводы**. Разработан метод обеспечения резильентности компьютерных систем в условиях киберугроз на основе самоадаптивности. На основе предложенного метода разработана самоадаптивная система обнаружения и ослабления атак, которая демонстрирует способность обеспечить устойчивое функционирование сети в ситуации наличия кибератак бот-сетей на уровне 70 %.

Ключевые слова: бот-сеть; киберугрозы; кибератака; обнаружение бот-сетей; защита сети; самоадаптивные системы; резильентность; сценарий безопасности; вредоносное программное обеспечение; DDoS-атака.

SELF-ADAPTIVE METHOD FOR THE COMPUTER SYSTEMS RESILIENCE IN THE PRESENCE OF CYBERTHREADS

S. Lysenko

The dynamic expansion of cyber threats poses an urgent need for the development of new methods, methods, and systems for their detection. The **subject** of the study is the process of ensuring the resilience of computer systems in the presence of cyber threats. The **goal** is to develop a self-adaptive method for computer systems resilience in the presence of cyberattacks. **Results**. The article presents a self-adaptive system to ensure the resilience of corporate networks in the presence of botnets' cyberattacks. Resilience is provided by adaptive network reconfiguration. It is carried out using security scenarios selected based on a cluster analysis of the collected network features inherent cyberattacks. To select the necessary security scenarios, the proposed method uses fuzzy semi-supervised c-means clustering. To detect host-type cyberattacks, information about the hosts' network activity and reports of host antiviruses are collected. To detect the network type attacks, the monitoring of network activity is carried out, which may indicate the appearance of a cyberattack. According to gathered in the network information concerning possible attacks performed by botnet the measures for the resilient functioning of the network are assumed. To choose the needed scenario for network reconfiguration, the clustering is performed. The result of the clustering is the scenario with the list of the requirement for the reconfiguration of the network parameters, which will assure the network's resilience in the situation of the botnet's attacks. As the mean of the security scenario choice, the semi-supervised fuzzy c-means clustering was used. The clustering is performed based on labeled training data. The objects of the clustering are the feature vectors, obtained from a payload of the inbound and outbound traffic and reports of the antiviral tool about possible hosts' infection. The result of clustering is a degree of membership of the feature vectors to one of the clusters. The membership of feature vector to cluster gives an answer to question what scenario of the network reconfiguration is to be applied in the situation of the botnet's attack. The system contains the clusters that indicate the normal behavior of the network. The purpose of the method is to select security scenarios following cyberattacks carried out by botnets to mitigate the consequences of attacks and ensure a network functioning resilience. **Conclusions**. The self-adaptive method for computer systems resilience in the presence of cyberattacks has been developed. Based on the proposed method, a self-adaptive attack detection, and mitigation system has been developed. It demonstrates the ability to ensure the resilient functioning of the network in the presence of botnet cyberattacks at 70 %.

Keywords: botnet; cyber threat; cyberattack; botnet detection; network defense; self-adaptive systems; resilience; security scenario; malware; DDoS attack.

Лисенко Сергій Миколайович – канд. техн. наук, доцент кафедри комп'ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна.

Sergii Lysenko – PhD, Associate Professor of Computer Engineering & System Programming Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: sirogyk@ukr.net, ORCID Author ID: 0000-0001-7243-8747,
Scopus Author ID: 54420643500, ResearcherID: I-1728-2018
https://scholar.google.com.ua/citations?hl=uk&user=TuAfytwAAAAJ&view_op=list_works