[19] Охрімчук В. В. Метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення : дис. канд. техн. наук: 21.05.01 / Охрімчук В. В. Житомир, 2021. 170 с.
[20] Кібератаки Російської Федерації. хронологія. URL: http: // surl. li / ewssc (дата звернення: 20.01.2023).
[21] Положенцев А., Гнатюк С. Black Energy як загроза об'єктам критичної інфраструктури України // "Information, communication, society" (ICS-2016). LVIV 2016. С. 32-33.
[22] Підрозділи кібернетичної безпеки Збройних Сил України перейшли на бойовий режим роботи. URL: http: // surl.li / ewsrw (дата звернення: 18.01. 2023).
[23] Під час захоплення українських кораблів були DDoS-атаки на сайт Міноборони. URL: http:/ /surl.li/ewsrt (дата звернення: 18.01.2023).
[24] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки оперативного центру реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України URL: http: // surl. li / ewsrl (дата звернення: 27.01.2023).
[25] Толуб Н. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. URL: http: // surl. li / ewssy (дата звернення: 28.01.2023).

FEATURES OF ANTI-UKRAINIAN INFORMATION (CYBER) INFLUENCE ON UKRAINE

Since the day of independence of Ukraine, its information space and cyberspace, after the development and implementation of information technologies in all spheres of society, are constantly under powerful foreign informational and cybernetic influences. The hybrid war launched by Russia in 2014 forced Ukraine to reconsider its approaches to ensuring information and cyber security. And with the beginning of a large-scale invasion, this issue became especially urgent. To carry out anti-Ukrainian information (cyber) influence, the Russian leadership used significant human, material and financial resources, thanks to which it was possible to effectively "brainwash" not only the majority of its citizens, but also a part of our compatriots. Therefore, unfortunately, this led to the support of a part of the Ukrainian citizens of the Kremlin's aggressive policy against Ukraine. The article analyzed the main information operations of Russia against Ukraine, as well as the implementation of cyber-attacks on its critical information infrastructure. As a result of the analysis, the features of anti-Ukrainian information (cyber) influence on Ukraine were established. Knowledge of the features of the enemy's destructive actions in the information and cyberspace will make it possible to create effective methods and means of countering them in the future.
Keywords: information war, information conflict, information and psychological influences, information struggle, cyber space, cyber-attack, cyber incident.

Левченко Олександр Віталійович, заслужений. діяч науки і техніки. України, доктор військових наук, професор, начальник Житомирського військового інституту імені С. П. Корольова.
Oleksandr Levchenko, honored science and technology figure of Ukraine, doctor of military sciences, professor, head of Korolov Zhytomyr military institute.
E-mail: zvir@post.mil.gov.ua.
Orcid ID: 0000-0001-6254-591X.

Охрімчук Володимир Васильович, кандидат технічних наук, професор кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова.
Volodymyr Okhrimchuk, candidate of technical sciences, professor at the Chair of Information Protection and Cybersecurity of Korolov Zhytomyr military institute.
E-mail: okhrimchuk84@ukr.net.
Orcid ID: 0000-0001-7518-9993.

DOI: 10.18372/2410-7840.24.17378
УДК 004.7:004.056.5

МОДИФІКОВАНИЙ МЕТОД ВИЯВЛЕННЯ DDoS-АТАК ПРИКЛАДНОГО РІВНЯ НА РЕСУРСИ ВЕБСЕРВЕРІВ

Аркадій Кравчук, Володимир Погорелов

Кількість підключених до мережі Інтернет пристроїв збільшується щороку, разом з тим частішають випадки проведення DDoS-атак, які спричиняють простій атакованої системи. Основною проблемою захисту є вчасне виявлення атаки в режимі реального часу та встановлення її джерела. Атаки прикладного рівня схожі

на кліентський трафік, бо вони мають низьку швидкість надсилання запитів та використовують вразливості ПЗ для того, щоб виснажувати обчислювальні ресурси. Причому HTTP є найпоширенішим протоколом серед атак прикладного рівня, а наявні методи не характеризуються одночасно високою точністю і швидкодією. Запропоновано покращений метод аналізу даних Інтернет-трафіку для ідентифікації DDoS-атак прикладного рівня на рівні протоколу HTTP, який матиме менший час реагування на вторгнення, ніж в наявних методів, та ідентичний рівень точності виявлення зловмисного трафіку. В основі модифікованого методу застосовано підхід на основі обчислення інформаційної ентропії з новими атрибутами, які характеризують прикладний рівень. Було знайдено параметри HTTP запитів, аналіз яких свідчить про проведення низькошвидкісних DDoS-атак, та виведено формули для обчислення їх ентропії. Запропонований метод дозволяє підвищити швидкодію ідентифікації джерел DDoS-атак на вебсервери, в тому числі для тих, які використовують протокол HTTPS завдяки розробленню проміжного ПЗ для вебфреймворків. Описано структурно-логічну організацію системи виявлення атак. Розглянуте рішення на основі мікросервісної архітектури може покращити захист вебсерверів від DDoS-атак, оскільки час ідентифікації зменшився, а точність збільшилась.

Ключові слова: *DDoS-атаки, HTTP, HTTPS, LR-DDoS, проміжне ПЗ, вебфреймворк, мікросервіси, інформаційна ентропія.*

ВСТУП

Одним із актуальних трендів на сьогодні є процес цифрової трансформації суспільства, бізнес-процесів та загалом різних видів діяльності і взаємодій. Тобто все більше стає сервісів та послуг, які реалізуються або автоматизуються за допомогою прикладного програмного забезпечення, яке, в свою чергу, зазвичай виконується на серверах в дата-центрах. Причому для отримання таких послуг користувачу достатньо мати пристрій із виходом до мережі Інтернет. Саме завдяки всесвітній мережі, відповідним протоколам передачі даних та сучасній мережевій інфраструктурі існує можливість швидко обмінюватись інформацією на як завгодно великих відстанях. Доказом популярності віддаленого використання комп'ютерних ресурсів є стрімкий розвиток хмарних технологій, які надають Інтернет-користувачам онлайн-сервіси для зберігання, обробки та аналізу даних, пропонують можливості для спільної роботи над проектами тощо. Причому треба зазначити, що для цього зазвичай розробляються вебзастосунки, адже вони не потребують додаткового ПЗ, окрім браузера, а комунікація між кінцевим користувачем і вебсервером відбувається через протокол HTTP. Проблеми ж для даної сфери можуть нести кіберзагрози, серед яких DDoS-атаки займають помітне місце. Розподілені атаки на відмову в обслуговуванні роблять недоступними атаковані ресурси комп'ютерних систем шляхом надмірного перенавантаження запитами, внаслідок чого як власники, так і користувачі можуть понести матеріальні збитки. Відсутність захисту від DDoS-атак спричиняє тривалий простій атакованої системи, що призводить до зменшення продуктивності Інтернет-ресурсу, втратити репутації та довіри від клієнтів, а це цілком може мати погані наслідки для бізнесу.

Згідно з дослідженнями, які оглядають загрози та заходи безпеки для Інтернету речей [1], кількість пристроїв, підключених до мережі Інтернет, суттєво збільшується щороку, разом з тим частішають випадки проведення кібератак. Оскільки левову частку усіх загроз становлять розподілені атаки на відмову в обслуговуванні, то питання захисту ресурсів комп'ютерних систем від DDoS-атак є актуальним. Загалом захист від таких атак можна розкласти на задачі виявлення шкідливого трафіку та його подальше блокування. Основною проблемою є саме вчасне виявлення ознак проведення атаки в режимі реального часу та встановлення її джерела, тобто звідки вона здійснюється. Адже одночасно зі зловмисними запитами, що виснажують ресурси, можуть бути запити від звичайних користувачів, яких не варто обмежувати в доступі до сервісів.

За моделлю OSI DDoS-атаки бувають мережевого, транспортного, прикладного та інших рівнів. Серед них, зокрема, окремо наголошують на атаках транспортного та прикладного рівнів [2], і якщо перші спрямовані на фізичне переповнення пропускної здатності каналів зв'язку, що може бути вирішено потужнішим мережевим обладнанням та простими методами ідентифікації і блокування, то з останніми дійсно є проблема. Оскільки

атаки прикладного рівня важче відрізнити від клієнтського трафіку через їх подібність, окрім того поява нових різновидів таких атак теж ускладнює цю задачу. Для атак мережевого рівня наявні ефективні методи на основі статистичного аналізу, тому що основним критерієм у цьому випадку є швидкість отримання пакетів від джерела атак. Згідно з проведеними оглядами та дослідженнями [3], для виявлення DDoS-атак прикладного рівня існуючі методи не характеризуються одночасно високою точністю і швидкодією, бо класичні методи на основі сигнатур чи статистичного аналізу, які були розроблені для мережевого рівня, мають великий рівень помилок в даному випадку, а методи з використанням машинного навчання потребують набагато більше часу для аналізу даних. Найбільш ж поширеним протоколом серед атак прикладного рівня є HTTP [2], тому вебсервери чи не найбільше потребують захисту від них.

Отже, проблема ідентифікації DDoS-атак на ресурси вебсерверів є актуальною та вимагає нових ефективних рішень. Тому у даній статті пропонується модифікований метод виявлення DDoS-атак прикладного рівня, який виявлятиме джерела атак достатньо швидко, не втрачаючи при цьому точності ідентифікації.

ПОСТАНОВКА ЗАДАЧІ

Метою цього дослідження є розробка покращеного методу аналізу даних Інтернет-трафіку для ідентифікації DDoS-атак прикладного рівня на рівні протоколу HTTP, який матиме менший час реагування на вторгнення, ніж в наявних методів, та ідентичний рівень точності виявлення зловмисного трафіку.

АНАЛІЗ НАЯВНИХ ДОСЛІДЖЕНЬ

У дослідженні [4] пропонується метод на основі теорії інформації, його головна ідея полягає у пришвидшенні обчислення інформаційної ентропії параметрів мережевих пакетів для виявлення DDoS-атак. Такий підхід реалізує доволі простий спосіб ідентифікації аномалій шляхом порівняння показників ентропії поточного трафіку з еталонними значеннями звичайного. Більші значення ентропії будуть тоді, коли певна інформаційна характеристика є більш випадковою, тобто у випадку клієнтського трафіку. А пакети, які були згенеровані DDoS-атаками, матимуть схожість у певних атрибутах, що зменшуватиме значення їх ентропії. Оскільки інформаційна ентропія за Клодом Шенноном включає в себе обчислення логарифма ймовірності появи символу чи стану з допустимої множини, дослідники вирішили спростити дану формулу, щоб збільшити швидкодію цього процесу. Для цього вони вирішили сфокусуватися тільки на кількості надісланих пакетів за певний проміжок часу, ігноруючи інші атрибути, що дозволило вивести нову формулу, яка мала нижчу обчислювальну складність. Запропонований цими дослідниками метод мав гарні результати точності класифікації тільки для атак мережевого рівня, тому що саме вони характеризуються високою швидкістю надсилання пакетів. DDoS-атаки прикладного рівня є низькошвидкісними, а отже і рівень помилок очікувано буде високим. Тому доцільно обрати інші атрибути трафіку для даного способу в контексті його використання для ідентифікації атак на рівні протоколу HTTP.

Дослідники у статті [5] розробили метод ідентифікації DDoS-атак для прикладного рівня, використовуючи той же підхід із обчисленням інформаційної ентропії. Щоправда, було обрано зовсім інші характеристики, які відображають поведінку користувачів на вебсайтах, і тому запропонований метод показав пристойні результати щодо точності виявлення атак на вебсервери. Це було досягнуто завдяки використанню таких атрибутів, як-от: IP-адреса відправника запиту та URL запитуваного ресурсу. Також дослідники вивели формули для розрахунків ентропії вищеперерахованих характеристик, з чого потім формується відповідний вектор, завдяки аналізу якого можна ідентифікувати атаку. Поставлений експеримент показав, що запропонований метод ефективно відрізняє DDoS-атаки від масованого сплеску відвідуваності (flash crowd), коли, наприклад, під час акції певного товару кількість переглядів його сторінки раптово зростає. Однак обчислювальна складність цього методу є більшою ніж у попередньо розглянутому методі, а тому бажано підвищити швидкодію або ще більше збільшити точність виявлення атак.

У роботі [6] йдеться про розпізнавання DDoS-атак в програмно-конфігурованих мережах за допомогою вдосконаленого методу опорних векторів (ASVM). Даний метод відноситься до категорії машинного навчання і є покращеною реалізацією класичного методу опорних векторів (SVM).

Вдосконалення за словами дослідників полягає в тому, що запропонований ASVM є методом багатокласової класифікації, що надає на виході три класи, на відміну від одного як у звичайного SVM. Адже загалом просто метод опорних векторів застосовується для бінарної класифікації, його сенс полягає в застосуванні операцій із лінійної алгебри для перетворення вхідних даних, а саме: до вектору характеристик досліджуваного об'єкту додається новий атрибут, який позначає категорію. Для класифікації кожен вектор випробовується двома можливими варіантами значення класу та обчислюється розділова гіперплощина разом з величиною відстані між поточним елементом та протилежним йому за значенням категорії. У випадку знаходження найбільшої відстані між двома різними об'єктами за класом, об'єкту, що аналізується, присвоюється відповідна категорія. Але так як SVM відноситься до методів з керованим навчанням, то перед застосуванням необхідно підготувати промаркований набір тестових даних та провести тренування моделі, що можна віднести до недоліків даного підходу. Ідея втілення багатокласового ASVM полягає в тому, що значення характеристик клієнтського та будь-якого зловмисного трафіку зазвичай не є лінійно розділеними, а тому бінарна класифікація може мати високий рівень помилок в даному випадку. Задля цього дослідники модифікували метод SVM таким чином, щоб він класифікував трафік як SYN-флуд, UDP-флуд або нормальний. Тобто замість ідентифікації всіх можливих видів атак як зловмисного в одній узагальненій категорії, модель тренується на конкретних різновидах DDoS-атак – це дозволяє підвищити точність їх виявлення, адже значення атрибутів в межах одного типу атаки будуть дійсно подібними. Заявляється, що точність запропонованого методу становить 97%, проте, проблема виявлення атак саме на рівні протоколу HTTP не розкривається.

У дослідженні [7] для виявлення DDoS-атак пропонується використати глибинну нейронну мережу (DNN) з гіперпараметром, який можна налаштувати, та розріджений автокодувальник (AE). Наведений метод у цій статті використовує штучні нейронні мережі та пропонує архітектуру, яка поєднує розріджений AE для виокремлення важливих атрибутів із вхідних даних з DNN, яка виконує класифікацію трафіку щодо ідентифікації DDoS-атак. Тобто AE виокремлює ознаки і зменшує розмірність для досягнення нелінійних узагальнень, він має один вхідний шар, кілька прихованих шарів для кодування і один вихідний шар для декодування. DNN схожа на штучну нейронну мережу, за винятком того, що вона має численні глибокі приховані шари. Кожен шар у DNN складається з одного або кількох штучних нейронів або вузлів таким чином, що ці нейрони повністю з'єднані від шару до шару. Новизна полягає в тому, що для визначення оптимальних значень гіперпараметрів для AE застосовано пошук по сітці, який автоматично визначає найкращі значення для параметра розрідженості, кількості шарів і нейронів у кожному шарі, щоби зменшити похибку класифікації. Також було запропоновано нормування та ортогоналізацію ваг нейронної мережі DNN під час навчання. За словами дослідників точність становить 98%, однак часова складність внаслідок комплексності програмної системи є вищою за всі попередні розглянуті методи.

Теоретичне підґрунтя методу

Загалом існує багато способів виявлення DDoS-атак, тим часом дослідники класифікують та узагальнюють їх за наступними підходами [3]: на основі сигнатур, аномалій та гібридні. Аналізуватимемо підходи саме на основі аномалій, бо сигнатурний підхід не є адаптивним через те, що він порівнює поточні характеристики Інтернет-трафіку з наперед встановленим шаблоном, тобто зразком атрибутів пакетів, які використовувались зловмисниками у атаці. Тому методи на основі сигнатур не можуть виявляти нові типи атак, а підтримувати набір сигнатур шкідливих пакетів в актуальному стані є нетривіальним завданням. Алгоритми, які знаходять аномалії в параметрах мережевих пакетів, якраз націлені на ідентифікацію нетипової поведінки, тому краще виявляють різні види DDoS-атак та є більш поширеними на практиці [3].

В свою чергу розподілені атаки на відмову в обслуговуванні можуть поділятися за швидкістю надсилання пакетів на дві категорії: високошвидкісні (HR-DDoS) та низькошвидкісні (LR-DDoS). Високошвидкісні атаки мають на меті виснажити канали передачі даних, тому відносяться до атак мережевого рівня. Так як в даному досліджені

розглядається проблема ідентифікації атак прикладного рівня, тому необхідно розробити метод, який справлятиметься саме з низькошвидкісними атаками. Бо LR-DDoS використовує вразливості прикладного програмного забезпечення і виснажує обчислювальні ресурси (як-от: процесора, оперативної пам'яті тощо) шляхом надсилання спеціальних запитів. Такі атаки мають низьку швидкість, щоб бути схожими на користувацькі запити, і використовують протоколи 7 рівня моделі OSI і запитують ресурсоємні операції, як, наприклад, зчитування з бази даних або запис в неї великого об'єму інформації.

Серед підходів на основі аномалій, виділяють наступні більш вузькі класи методів: на основі статистичного аналізу, теорії інформації та машинного навчання. Високою швидкодією ідентифікації DDoS-атак відзначається метод, який обчислює інформаційну ентропію мережевих пакетів [8]. Інформаційна ентропія є мірою невизначеності випадкової величини, вона обчислюється за досить простою формулою: $H(x) = -p(x)\log_2 p(x)$, де $p(x)$ – ймовірність появи символу x з певного алфавіту. Але в класичній реалізації цей метод використовує в якості вхідних параметрів дані про IP-адресу, порт та інші атрибути мережевого рівня моделі OSI. У зв'язку з цим для виявлення LR-DDoS атак даним методом необхідно адаптувати процес збору параметрів, додавши характеристики запитів з прикладного рівня, та вивести формули обчислення значень їх ентропії.

Вебсервери, атаки на ресурси яких розглядаються в даному дослідженні, використовують саме HTTP протокол для комунікації з клієнтами на прикладному рівні. В загальному це відбувається наступним чином: користувач надсилає HTTP запит, а сервер після його обробки надсилає HTTP відповідь цьому користувачу. Оскільки DDoS-атаки здійснюються саме на сервери від зловмисників, які виступають в ролі клієнтів, то необхідно досліджувати атрибути HTTP запитів.

Цей протокол використовує простий текстовий формат та визначає спеціальну структуру для запиту і відповіді, тобто їх параметри розташовані у визначеному порядку відповідно до стандарту. HTTP запит складається з наступних складових елементів: стартовий рядок запиту, набір заголовків та тіло запиту. У стартовому рядку розміщується важлива інформація, а саме: метод запиту та URI запиту. Комбінація методу та URI запиту є, по суті, унікальним ідентифікатором ресурсу, до якого звертається користувач на вебсервері. Бо один і той самий URI може виконувати різну бізнес-логіку при різних методах: для GET, наприклад, відбувається пошук всіх товарів, в той час як для POST запиту може виконуватись додання нової одиниці товару в каталог. Загалом, метод і URI варто вибрати як атрибут для дослідження, оскільки така пара відображає загалом цільову мету запиту. Тому що для звичайних користувачів властиво відкривати різні сторінки, причому серед них будуть більш популярні, як, наприклад, сторінка контактів, товарів тощо. А от DDoS-атаки або перенавантажитимуть певний ресурс за фіксованим URI, або перебиратимуть всі можливі ресурси, що теж є нетиповою поведінкою для користувачів. Також інформація про клієнта міститься в заголовках запиту, а саме поле User-Agent, яке вказує назву браузера та його версію, звідки відправився запит. Цю характеристику також слід використати для виявлення атак на відмову в обслуговуванні, бо в масованих запитах від зловмисників зазвичай версія та назва утиліти, з якої вони надсилаються, однакова. Окрім цього, важливим полем в заголовках HTTP запиту є Content-Length, що позначає розмір тіла запиту. У випадку DDoS-атаки на ресурс, який, наприклад, додає новий елемент в базу даних, зловмисники можуть відправляти великий файл, розмір якого здебільшого не буде змінюватись від запиту до запиту. І тому даний атрибут теж можна використати для ідентифікації атак, адже у звичайних користувачів розмір тіла POST запитів на різні ресурси буде варіюватись.

Завдання щодо збору атрибутів з прикладного рівня, який використовується вебсервером, не є простим, як це може здатися на перший погляд. Якщо мова йде про HTTP протокол, то, звісно, всі дані можуть бути отримані з мережевих пакетів, які можна захоплювати на сервері, наприклад, утилітою tcpdump. Тобто з .pcap файлів, що зберігають всю інформацію про пакети, які були надіслані через певний мережевий інтерфейс, можна витягнути інформацію зі всіх рівнів моделі OSI, в тому числі і прикладного, прочитавши таким чином HTTP запит або відповідь. Але зараз дуже

особлива увага приділяється захисту інформації для того, щоби унеможливити перехоплення персональних або інших чутливих даних (наприклад, паролі) в Інтернеті. Тому сьогодні абсолютна більшість вебсайтів використовує протокол HTTPS, який шифрує всі дані в запитах, замість застарілого HTTP. Протокол HTTPS використовує криптографічні протоколи TLS або SSL, що унеможливлює прочитання сторонніми особами даних на рівнях, що йдуть вище них, тобто на рівні протоколу HTTP. Отже, неможливо прочитати атрибути прикладного рівня з протоколу HTTPS шляхом просто захоплення пакетів на відповідних мережевих інтерфейсах, а протокол HTTP є не актуальним на даний момент. Для розв'язання цієї проблеми в рамках даного дослідження пропонується наступне архітектурне рішення: розробити та застосувати проміжне програмне забезпечення (middleware) для вебфрейморків, яке збиратиме необхідні атрибути запитів та надсилатиме їх програмі виявлення DDoS-атак засобами взаємодій між процесами, наприклад через іменований канал або сокет. Майже всі популярні вебфреймворки дозволяють вбудовувати додаткове ПЗ [9], яке виконуватиметься до або після всіх налаштованих обробників, що власне і дає змогу вирішити дану проблему.

Повертаючись до інших підходів для виявлення DDoS-атак, то слід також відзначити методи машинного навчання, а саме: метод опорних векторів, штучні нейронні мережі – вони мають високу точність ідентифікації LR-DDoS атак, але водночас мають і велику обчислювальну складність [4]. Так як задачею дослідження є підвищення швидкодії, то для даних методів можна використати розподілене обчислення на декількох вузлах для пришвидшення цього процесу.

Опис запропонованого методу

Запропонований в даному дослідженні метод розроблявся для протоколу HTTP та HTTPS, бо вони є одними із найпопулярніших прикладних протоколів в мережі Інтернет, оскільки зазвичай саме веб-сайт є кінцевим інтерфейсом для отримання інформації чи надання послуг.

Спершу розглянемо складові частини та елементи поставленого завдання. Проблему обраної предметної області можна поділити на дві великі частини: виявлення DDoS-атак та боротьба з їх наслідками. Для того, щоби виявити факт проведення атаки на відмову в обслуговуванні необхідно виконати наступні кроки: зібрати дані, обробити зібрані дані, провести класифікацію оброблених даних обраним методом, визначити джерела атак відповідно до вставлених класів на попередньому кроці. Боротьба з наслідками DDoS-атак включає в себе блокування нових виявлених джерел атак, але ця частина не буде досліджуватись, бо в даній статті розкривається проблема саме виявлення атак.

Оскільки виявлення DDoS-атак складається з декількох послідовних кроків, то є сенс використати мікросервісний архітектурний стиль для програмної реалізації даної системи. Це дозволить масштабувати її на декілька серверів, що може підвищити швидкодію розроблюваного ПЗ. Взаємозв'язок між запропонованими мікросервісами показано на діаграмі компонентів (рис. 1).

Отже, в даному дослідженні для виявлення атак на відмову в обслуговувані розглядається ПЗ, що складається з шести компонентів, причому два з них призначені тільки для збереження інформації про джерела атак та відображення цієї інформації на запит користувача (база даних Redis та клієнтський консольний інтерфейс відповідно). Далі в статті буде детально розглянуто запропоновані мікросервіси.

Опис класифікатора DDoS-атак

Головним компонентом в розроблюваній системі, безперечно, є класифікатор DDoS-атак, адже саме він визначає яким чином треба обробляти вхідні дані та ідентифікує зловмисний трафік. Тому спершу розглянемо цей компонент. В даному дослідженні було запропоновано модифікувати метод на основі інформаційної ентропії для виявлення DDoS-атак. В звичайній реалізації цього методу обчислюється ентропія кількості мережевих пакетів H_c від кожного відправника s_i за такою формулою:

$$H_c(s_i) = -p_c(s_i)\log_2 p_c(s_i);\ p_c(s_i) = \frac{c_i}{\sum_j c_j}, \quad (1)$$

де $p_c(s_i)$ – ймовірність появи пакетів від відправника s_i; c_i – кількість пакетів від *i*-го відправника за встановлений проміжок часу.

Як зазначалось раніше, модифікація вищеописаного методу полягає в обчисленні інформаційної ентропії для нових параметрів з прикладного рівня. Аналізуючи дослідження про DDoS-атаки HTTP протоколу [10], було визначено атрибути HTTP запитів, аналіз яких може вказати на факт проведення LR-DDoS атаки, а саме: URI запиту та його HTTP метод, клієнт (User-Agent) запиту, розмір запиту, час обробки запиту вебсервером.

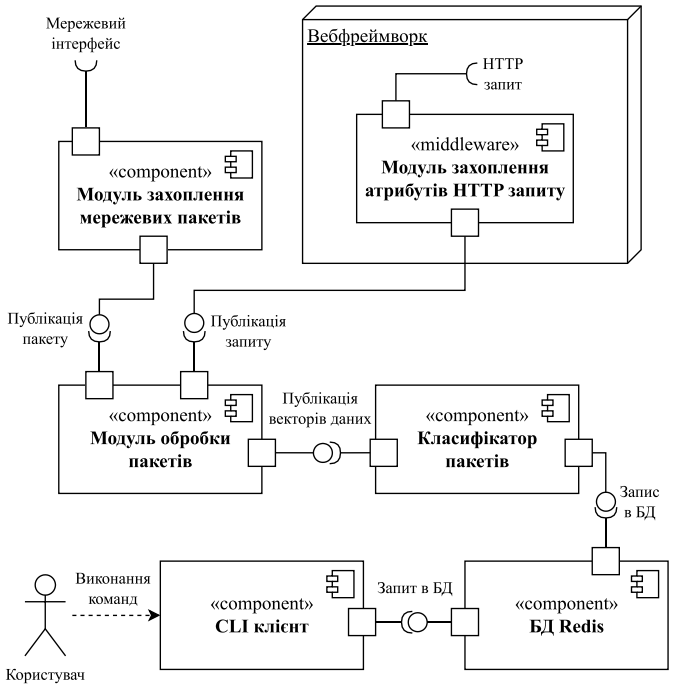

Рис. 1. UML діаграма компонентів системи

Для обчислення ентропії вищезазначених характеристик, необхідно адаптувати формулу (1) та вивести спосіб розрахунку ймовірностей появи цих атрибутів. Нехай, кожен HTTP запит можна представити певною множиною її значень $\{s,u,a,l,t\}$, де: s – IP адреса та порт джерела; u – URI та метод запиту; a – клієнт, з якого робився запит (User-Agent); l – розмір тіла запиту; t – час обробки запиту. З масиву множин всіх запитів для кожного унікального джерела s_i можна визначити унікальні URI і методи запитів u_j^i, а також кількість повторів відповідної унікальної пари – позначимо як $c(u_j^i)$. Тоді для відправника s_i ентропія такого параметру як URI та метод запиту H_u становитиме:

$$H_u(s_i) = -\sum_j p_u(u_j^i)\log_2 p_u(u_j^i);$$
$$p_u(u_j^i) = \frac{c(u_j^i)}{\sum_i \sum_j c(u_j^i)}, \quad (2)$$

де $p_u(u_j^i)$ – ймовірність появи унікальної пари URI і методу запиту u_j^i від джерела s_i серед всіх зафіксованих пар від всіх відправників за встановлений проміжок часу.

Відповідно для інших запропонованих атрибутів, а саме: клієнт запиту, розмір тіла запиту – ентропія обчислюється аналогічно як в формулі (2). Тільки ймовірність для характеристики часу обробки запиту вебсервером буде розраховуватись іншим чином. Час обробки запиту можна вважати неперервною випадковою величиною. Для запитів з однаковим URI та методом час надання відповіді сервером теж буде приблизно однаковим, тому можна сказати, що розподіл цієї величини є нормальним. З цього випливає, що ймовірність $p_t(t_j^i)$ для характеристики часу обробки t_j^i певного запиту від *i*-го відправника для *j*-ої пари URI та методу запиту буде дорівнювати ймовірності попадання значення нормально розподіленої випадкової величини в заданий інтервал:

$$p_t(t_j^i) = \Phi\left(\frac{t_j^i + \delta - a_j}{\sigma_j}\right) - \Phi\left(\frac{t_j^i - \delta - a_j}{\sigma_j}\right), \quad (2)$$

де $\Phi(x)$ – значення функції Лапласа для змінної x; a_j – середнє значення часу обробки запиту для *j*-ої пари URI та методу запиту; σ_j – середнє квадратичне відхилення значення часу обробки запиту для відповідної *j*-ої пари URI та методу запиту; δ – додатне значення для допустимого часового інтервалу, яке близьке до 0, причому $\delta \ll t_j^i$.

Формулу (3) слід використати як значення ймовірності для обчислення ентропії характеристики часу обробки запиту H_t. Таким чином зна-

чення H_t можна обчислити за допомогою наступної формули:

$$H_t(s_i) = -\sum_j p_t(t_j^i)\log_2 p_t(t_j^i). \quad (3)$$

Отже, було виведено формули (2) – (4) для обчислення інформаційної ентропії чотирьох нових запропонованих атрибутів для виявлення DDoS-атак на ресурси вебсерверів.

Для присвоєння відповідного класу нормального чи зловмисного трафіку HTTP запитам слід обчислити згадані вище значення ентропії 4-ох атрибутів і також значення ентропії кількості пакетів за формулою (1) від кожного відправника за часовий проміжок Δt. Тобто загалом матимемо п'ять характеристик, ентропію яких треба обчислити. Тому кожне джерело пакетів (їх відправник) за час спостереження Δt характеризується вектором з п'яти чисел. У випадку, коли хоча б два значення з п'яти перевищує встановлений поріг, то даний відправник позначається як джерело DDoS-атак. Порогове значення для кожного атрибуту можна обчислити шляхом знаходження середніх значень ентропій цих параметрів на тестовому наборі даних, в якому зловмисні пакети промарковані відповідним чином. Надалі для покращення точності даного методу можна розглянути спосіб коригування порогових значень відповідно до зміни статистичних показників, наприклад, зміни дисперсії величин атрибутів.

Характеристика взаємодії запропонованих мікросервісів між собою та особливості збору та обробки вхідних даних для вищеописаного класифікатора будуть розглянуті далі.

Особливості програмної реалізації методу

Нагадаємо, що загальна архітектура запропонованого методу складається з наступних етапів: збір, обробка, класифікація даних та ідентифікація джерел атак. Етап збору даних має свої особливості, адже треба отримати інформацію з декількох рівнів моделі OSI. Вхідні пакети транспортного рівня можна отримати, якщо є доступ до маршрутизатора або мережевого інтерфейсу за допомогою програми tcpdump. А для отримання необхідної інформації з прикладного рівня треба розробити middleware для вебсерверу – аргументація цього вже наводилась раніше. В даному досліджені для перевірки гіпотези було запропоновано програмний модуль для вебфреймворку Express.js, який вимірює час обробки кожного запиту та зберігає поля заголовків з необхідними атрибутами. Щоби зіставити потім ці дані з даними відповідних мережевих пакетів, middleware для кожного запиту визначає IP-адресу та порт відправника і отримувача. Зібрана інформація з різних джерел відправляється до модуля обробки даних за допомогою протоколу MQTT.

Обробка даних полягає у формуванні єдиного об'єкту параметрів з транспортного та мережевого рівнів: для цього серед зібраної інформації об'єднуються атрибути з однаковим часом захоплення, адресами відправника та отримувача. Для класифікації формується масив об'єктів з оброблених параметрів за певний часовий проміжок розміром Δt (наприклад, 5 хв.). Даний масив надається вищеописаному класифікатору, який в результаті обчислень зберігає інформацію про нові джерела атак в БД Redis. За допомогою консольного інтерфейсу можна переглянути виявлені DDoS-атаки, інформація про які отримується з бази даних.

Результати експериментальних досліджень

Запропонований метод було реалізовано на мові програмування Python. Для порівняння взято метод SVM з дослідження [11] і також реалізовано на цій ж мові. Було використано публічний набір даних CICIDS 2017 [12] як вхідні дані. В цьому датасеті були захоплені LR-DDoS атаки прикладного рівня, причому на рівні протоколу HTTP. Завдяки наявності .csv файлу з класами та .pcap файлу із захопленими пакетами можна було провести експеримент, в якому досліджувалась робота запропонованого методу та SVM. В поставленому експерименті вимірювались точність та час роботи методів. Результати досліджень були внесені до табл. 1.

Таблиця 1

Показники якості класифікації DDoS-атак натренованими моделями

Показники	Запропонований метод	SVM
Точність, %	96.59	95.76
Час роботи, мс	45.92	71.64

Для порівняння вищезгаданих методів у якості вхідних даних надавався масив, розмір якого

становив 500 векторів, в яких містились атрибути пакетів зі згаданого вище набору даних. Тобто час роботи в табл. 1 означає час, який витратив класифікатор для визначення класу відповідним мережевим пакетам. Вимірювання проводились на комп'ютері з оперативною пам'яттю 32 ГБ та процесором Intel Core i5-4430 (3.00 ГГц) декілька разів, причому в табл. 1 відображено якраз середнє арифметичне значення усіх запусків. Точність обчислювалась за звичайною формулою для бінарної класифікації. Для оброблення кожних п'ятсот векторів, в яких містяться атрибути HTTP запитів, в середньому витрачалось 45.92 мілісекунд запропонованим методом, а методом SVM – 71.64 мілісекунд на одному й тому самому комп'ютері. Отже, запропонований в даному дослідженні метод має дійсно більшу швидкодію.

ВИСНОВКИ

Отже, дана стаття була присвячена розробці модифікованого методу виявлення DDoS-атак прикладного рівня. Запропонований метод дозволяє підвищити швидкодію ідентифікації джерел DDoS-атак на вебсервери. Ідея дослідження полягала в тому, щоб використати метод на основі інформаційної ентропії, який має малу обчислювальну складність, та адаптувати його для прикладного рівня шляхом виведення способу обчислення ентропії для атрибутів HTTP запиту, серед яких є час його обробки. Також було запропоновано захоплювати параметри запитів прикладного рівня за допомогою проміжного ПЗ для вебфреймворків (middleware), що вирішує проблему прочитання атрибутів із захищеного протоколу HTTPS. Було описано структурно-логічну організацію системи виявлення DDoS-атак, починаючи зі збору даних та закінчуючи встановленням джерел атак. Експериментально перевірено роботу запропонованого методу та порівняно з методом опорних векторів, у результаті чого було встановлено вищу швидкодію та точність класифікації у першого з них. Тому розглянуте рішення на основі мікросервісної архітектури може бути застосовано для покращення захисту вебсерверів від LR-DDoS атак, оскільки час ідентифікації зменшився, а її точність збільшилась. Це дасть змогу зменшити збитки відповідним компаніям від таких типів кіберзагроз.

Подальшого дослідження потребують наступні питання: алгоритм коригування порогового значення для ідентифікації атак; використання розподіленого обчислення для нових додаткових параметрів (наприклад, статистичних) на кластерах Hadoop екосистеми або Kubernetes.

ЛІТЕРАТУРА

[1] S. Bhatt, Rachit, P.R. Ragiri. Security trends in Internet of Things: a survey [Text] // SN Applied Science, 2021, Vol. 3, № 1. P. 1-14.

[2] Kumar, G. Denial of service attacks – an updated perspective [Text] // Systems science & control engineering, 2016, Vol. 4, № 1. P. 285-294.

[3] P. Kaur, M. Kumar, A. Bhandari. A review of detection approaches for distributed denial of service attacks [Text] // Systems Science & Control Engineering, 2017, Vol. 5, № 1. P. 301-320.

[4] G. No, I. Ra An efficient and reliable DDoS attack detection using a fast entropy computation method [Text] // 2009 9th International Symposium on Communications and Information Technology, 2009. P. 1223-1228.

[5] Y. Zhao, W. Zhang, Y. Feng. A classification detection algorithm based on joint entropy vector against application-layer DDoS attack [Text] // Security and Communication Networks, 2018. P. 1-8.

[6] Myint Oo, S. Kamolphiwong, T. Kamolphiwong M. Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN) [Text] // Journal of Computer Networks and Communications, 2019, P. 1-12.

[7] A. Bhardwaj, V. Mangat, R. Vig. Hyperband tuned deep neural network with well posed stacked sparse AutoEncoder for detection of DDoS attacks in cloud [Text] // IEEE Access, 2020, Vol. 8. P. 181916-181929.

[8] Bhuyan, M.H. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric [Text] // Security and Communication Networks, 2016, Vol. 9, № 16. – P. 3251-3270.

[9] X. Li, M. Eckert, J.-F. Rubio. Context aware middleware architectures: survey and challenges [Text] // Sensors, 2015, Vol. 15, № 8. P. 20570-20607.

[10] Mohammed, A. A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks [Text] // The Scientific World Journal, 2015, Vol. 2015, Article ID 238230.

[11] Perez-Diaz, J.A. A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks

using machine learning [Text] // IEEE Access, 2020, Vol. 8. P. 155859-155872.
[12] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization [Text] // Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018, Vol. 1. P. 108-116.

A MODIFIED METHOD FOR DETECTING APPLIED-LEVEL DDOS ATTACKS ON WEB SERVER RESOURCES

The number of devices connected to the Internet is increasing every year, while DDoS attacks are becoming more frequent, causing downtime of the attacked system. The main challenge is to detect an attack in real time and identify its source. Application layer attacks are similar to client traffic in that they have a low request rate and use software vulnerabilities to drain computing resources. Moreover, HTTP is the most common protocol among application layer attacks, and existing methods are not characterized by both high accuracy and speed. An improved method for analyzing Internet traffic data to identify application-level DDoS attacks at the HTTP protocol level is proposed, which will have a shorter response time to intrusions than existing methods and an identical level of accuracy in detecting malicious traffic. The modified method is based on the calculation of information entropy with new attributes that characterize the application layer. We have found the parameters of HTTP requests, the analysis of which indicates low-rate DDoS attacks, and derived formulas for calculating their entropy. The proposed method makes it possible to increase the speed of identifying the sources of DDoS attacks on web servers, including those that use the HTTPS protocol, by the development of middleware for web frameworks. The structural and logical organization of the attack detection system is described. The proposed method based on the microservice architecture can improve the protection of web servers from DDoS attacks, since the identification time has decreased, and the accuracy has increased.

Keywords: DDoS attacks, HTTP, HTTPS, LR-DDoS, middleware, web-framework, microservices, information entropy.

Кравчук Аркадій Андрійович, магістрант, студент кафедри програмного забезпечення комп'ютерних систем факультету прикладної математики КПІ ім. Ігоря Сікорського.
Arkadii Kravchuk, master student, student of the department of computer system software, faculty of applied mathematics, Igor Sikorsky Kyiv Polytechnic Institute.
E-mail: arkakrava@gmail.com.
Orcid ID: 0000-0002-6128-206X.

Погорелов Володимир Володимирович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Pogorelov, PhD in engineering, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: volodymyr.pogorelov@gmail.com.
Orcid ID: 0000-0002-6100-1504.

DOI: 10.18372/2410-7840.24.17379
УДК 004.056

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ЗДІЙСНЕННЯ КІБЕРВПЛИВУ

Олексій Самчишин, Ганна Носова

У сучасному інформаційному суспільстві широке поширення одержав такий тип віртуальних спільнот як соціальні мережі. Завдання таких соціальних інтернет-сервісів полягає у тому, щоб забезпечити користувачів всіма можливими шляхами взаємодії одне з одним. Соціальні мережі, окрім виконання функцій підтримки спілкування, обміну думками вирішення своїх професійних потреб, політичних амбіцій, задоволення своїх інтересів у мистецтві, дозвіллі й одержання інформації членами віртуальних спільнот, все частіше стають об'єктами й засобами інформаційного та кібервпливу. Основними етапами проведення кібероперацій у соціальних інтернет-сервісах, що використовуються найчастіше, вважається: моніторинг відкритих джерел, акаунтів, груп, застосування методів соціальної інженерії і безпосередньо реалізація кібервпливів. В