пристроях демонструють високий рівень ефективності, тим не менше, їх спільним недоліком є високий рівень хибних спрацювань. Також суттєвим недоліком вищезазначених підходів є потреба у значних обсягах обчислювальних ресурсів, ігнорування упакованого програмного забезпечення та нездатність адаптивно реагувати на атаки нульового дня. З огляду на вищезазначене, актуальною задачею є розроблення нових методів виявлення зловмисного програмного забезпечення у мобільних ОС Android.

Список літератури

1. McAfee Mobile Threat Report Q1, 2021. [Електронний ресурс] – Режим доступу: https://www.mcafee.com/content/dam/consumer/en-us/docs/2021-Mobile-Threat-Report.pdf.

2. Amro, B. Personal Mobile Malware Guard PMMG: a mobile malware detection technique based on user's preferences / B. Amro. – International Journal of Computer Science and Network Security, 2018. – Vol. 18, No. 1. – pp. 18–24.

3. Idrees, F. Pindroid: a novel android malware detection system using ensemble learning methods / F. Idrees, M. Rajarajan, M. Conti, T. Chen, Y. Rahulamathavan. – Computers & Security, 2017. – Vol. 68. – pp. 36–46.

4. McLaughlin, N. Deep android malware detection / N. McLaughlin, J. Martinez del Rincon, B. Kang. – Proc. of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017. – pp. 301–308.

5. Alzaylaee, M. K. DL-Droid: Deep learning based android malware detection using real devices / M. K. Alzaylaee, S. Y. Yerima, S. Sezer. – Computers & Security, 89, 2020. – 101663.

6. Mariconti, E. MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Model / E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro. – ACM Trans. Priv. Sec., 2019. – Vol. 1, No. 1. – pp. 1–33.

8. Millar, S. DANdroid: A multi-view discriminative adversarial network for obfuscated Android malware detection / S. Millar, N. McLaughlin, J. Martinez del Rincon, P. Miller, Z. Zhao. – Proceedings of the tenth ACM conference on data and application security and privacy, 2020. – pp. 353-364.

Науковий керівник – к.т.н.,доцент Бобровнікова К.Ю.

Методи виявлення кіберзагроз мережного типу

УДК 004.492.2

Дмитро Сокальський[1], Яна Михасько[2]

Хмельницький національний університет, [1]sokalskij7@gmail.com, [2]yashamyy@gmail.com

Метою даної роботи є аналіз методів та класифікація виявлення кіберзагроз мережного типу.

Сьогодні однією з найпоширенішою кіберзагрозою мережного типу є атака на відмову в обслуговуванні або розподілену відмову в обслуговуванні (DOS або DDoS), яка може пошкодити або заблокувати доступ до ресурсів (рис. 1).

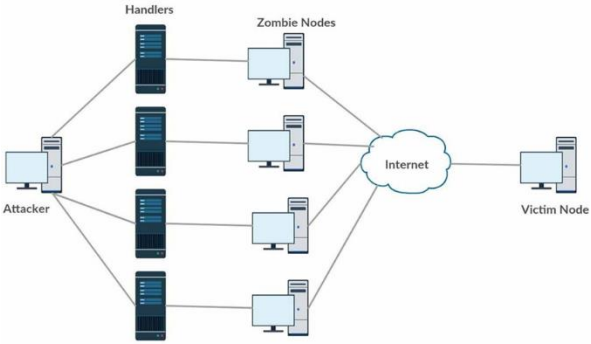

Рис. 1. Розподілена атака типу "відмова в обслуговуванні" (DDoS)

Методи виявлення та механізми захисту від DoS-атак можна умовно класифікувати за двома ознаками. Перша ознака - розташування механізму захисту в комп'ютерній мережі. Методи, які об'єднують різні схеми захисту і забезпечують їх взаємодію, зазвичай називають гібридними. Гібридні методи забезпечують кращий захист від кібератак, ніж окремі методи захисту, що працюють самостійно на різних сегментах мережі. Друга ознака - час застосування методу. Методи, які застосовуються до настання атаки, відносяться до методів запобігання, а ті методи, які використовуються під час атаки, відносяться до групи виявлення атаки і ідентифікації джерела. Після виявлення атаки застосовуються методи реакції на атаку. Найкращим варіантом є запобігання атаки. Воно може бути досягнуто на всіх етапах шляху мережевого трафіку, починаючи від джерела атаки і закінчуючи обробкою даних на стороні сервера, на який здійснюється атака. Найчастіше використовуються комбіновані засоби запобігання (IPS) і виявлення атак (IDS) - IPDS. Класифікація методів захисту від DoS-атак зображена на рисунку 2. Зазвичай у механізмах захисту на стороні сервера використовується клієнт-серверна модель для протоколів прикладного рівня. В такому випадку, сервер отримує запити, які створюються клієнтом (DNS-сервер, веб-сервер). Такий механізм мережевої взаємодії використовується в багатьох DoS-атаках.

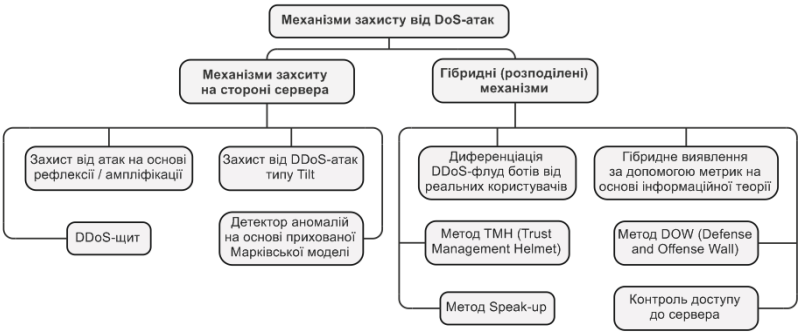

Рис. 2. Класифікація методів захисту від DoS-атак

Основними механізмами захисту проти подібних DoS-атак є:

- захист від DoS-атак на основі рефлексії/ампліфікації. Такі методи захисту спрямовані на виявлення шкідливого трафіку, який був створений при використанні таких протоколів як DNS та SIP та за допомогою різних прикладних методів, таких як, наприклад, технології машинного навчання;
- DDoS-щит - характеристики отриманих HTTP-запитів обчислюються за допомогою статистичних методів та детектор аномалій;
- захист від DDoS-атак типу Tilt призначений для моніторингу мережевого трафіку, і для різних користувачів забезпечує різні можливості.

Гібридні або розподілені механізми забезпечують захист мережі за допомогою взаємодії механізмів захисту як на стороні клієнта, так і на стороні сервера. Прикладами гібридних механізмів захисту є:

- метод Speak-Up. Принцип дії даного методу полягає у диференціації справжніх користувачів від зловмисників. Даний метод використовується для захисту від сесійних флуд-атак;
- метод DOW (Defense and Offense Wall). Даний механізм захисту використовує метод кластеризації K-Means, який призначений для виявлення та фільтрації сесійних атак, флуд-атак на основі запитів та асиметричних атак;
- диференціація DDoS-флуд-ботів від реальних користувачів. Цей механізм призначений для розрізнення звичайних користувачів та мережевих ботів;
- контроль доступу до сервера. Даний метод використовується для обмеження кількості одночасно підключених до сервера клієнтів. Контроль доступу до сервера здійснюється за допомогою приховування портів;
- метод TMH (Trust Management Helmet). В даному методі захисту використовується так зване “управління довірою”, яке призначене для розрізнення звичайних користувачів від зловмисників. Метою методу є забезпечення попереднього захисту зв’язку користувачів під час кібератаки;
- гібридне виявлення. Даний механізм захисту призначений для фільтрування підозрілих потоків та визначення параметрів поведінки користувача у мережі (швидкість HTTP-запиту, час перегляду сторінки).

Науковий керівник – науковий ступінь, д.т.н, доцент, Лисенко С.М.

Безпечна ідентифікація клієнта в протоколах передачі інформації без збереження стану

УДК 004.056.53 (043.2)

Василь Буковецький[1], Василь Різак[2]

Ужгородський Національний Університет, [1]bukovetsky@outlook.com, [2]vrizak@uzhnu.edu.ua

Стрімкий розвиток мережі Інтернет та технологій відкрив шлях до створення динамічних веб-ресурсів та клієнт-серверних додатків, які можуть надавати користувачеві персоналізовані сервіси. Такий функціонал досягається постійним обміном даними клієнтського додатку із сервером. Найпоширенішим