УДК: 004.8

ПОИСК И ВЫЯВЛЕНИЕ ЗАРАЖЕННЫХ БОТНЕТОМ УСТРОЙСТВ В КОМПЬЮТЕРНОЙ СЕТИ

Тащилин А.А. – магистр.
Научный руководитель – старший преподаватель Акутин А.С.
Саратовский государственный технический университет
имени Гагарина Ю.А.
Российская Федерация, г. Саратов

Современный ландшафт киберугроз характеризуется усилением угроз, обусловленных развитием информационно-коммуникационных технологий. Одним из наиболее значимых рисков является существование ботнетов — сетей компьютеров, захваченных злоумышленниками и используемых для осуществления широкого спектра незаконных операций. К таким действиям относятся распространение противоправного контента, осуществление DDOS-атак различной интенсивности, внедрение шпионского программного обеспечения, кража персональных данных пользователей, массовая рассылка нежелательной рекламы и искусственное увеличение числа просмотров веб-ресурсов [1].

Таким образом, одной из актуальных задач на сегодняшний день становится задача идентификации зараженных ботнетом устройств в компьютерной сети.

Рассмотрим существующие разработки для выявление сетевой активности ботнета. В исследование [1] предложен метод, который позволяет обнаружить ботнетов на основе анализа функционирования ботов, участвующих в конкретной атаке. Особенность метода заключается в возможности идентифицировать ботов не принимавших участия в атаке за счёт работы распределенной сети интеллектуальных агентов. Предлагаемый метод идентификации ботов базируется на средстве защиты от распределенных DDOS-атак с возможностью обнаружения атаки в сети цели атаки, а предотвращения генерации атаки в сети источника. Данная разработка не учитывает, что ботнет может использоваться не только для проведения DDOS-атаки. Очень часто запросы от зараженных устройств идут с не большой периодичностью в разное время. В исследование [2] описывается разработка интеллектуальной системы обнаружения сетевых атак и вторжений. Для реализации системы используется гибридная нейросетевая модель для обнаружения сетевых атак на основе федеративного трансферного обучения, демонстрирующая высокую эффективность классификации. Однако существенным недостатком является отсутствие анализа уязвимостей самой системы федеративного обучения к потенциальным атакам на процесс агрегации моделей или подмене клиентов, что ставит под вопрос безопасность применения в реальных условиях. В исследование [3] предложено выявление аномалий сетевого трафика на основе нечёткого прогнозирования динамических рядов объемов IP-пакетов с использованием

нескольких моделей временных рядов. Однако ключевым недостатком метода является зависимость точности прогноза от ручного подбора параметров универсума и функций принадлежности, что снижает адаптивность системы к изменяющимся сетевым условиям и требует постоянного вмешательства эксперта. Разработанный метод в исследовании [4] обнаруживает аномалии сетевого трафика путем анализа параметра Хёрста на основе R/S-анализа и сравнения с эталонными статистическими порогами. Однако предложенное решение является недостаточно полным, поскольку оно неспособно надежно детектировать сложные аномалии, не нарушающие глобальную самоподобную структуру трафика, такие как низкоскоростные и целевые атаки. В работе [5] предложена методика создания многоагентной системы для распознавания угроз информационной безопасности, основанная на событийном моделировании и агентных сценариях, редактируемых специалистами. Однако, ключевым недостатком системы является отсутствие в её архитектуре механизма разрешения конфликтов между агентами при получении противоречивых данных, что существенно снижает достоверность итоговой оценки угрозы в реальных условиях. В работе [6] предложен базовый механизм выявление сетевых аномалий на основе базы сигнатур. Однако разработанная система обладает существенным недостатком, заключающимся в неспособности надежно обнаруживать полиморфные и многоэтапные атаки.

Показанные проблемы использования существующих методов позволяют предложить комбинированный подход, объединяющий преимущества разных методик выявления сетевой активности ботнетов и компенсирующий их недостатки. Целью предлагаемой системы является создание эффективного решения для комплексной идентификации заражённых ботнетом устройств путём интеграции методов машинного обучения, анализа поведенческой динамики сетевого трафика и событийного моделирования. Система должна обеспечивать гибкость адаптации к различным типам угроз, минимизацию ложных срабатываний, и повышение устойчивости к новым видам ботнетов. Для достижения поставленной цели выделены следующие ключевые задачи:

1. Обнаружение аномального поведения: Выявление отклонений от нормального сетевого профиля устройства, таких как изменение частоты отправки пакетов, подключение к необычным доменным именам или необычные временные закономерности передачи данных;

2. Выявление характерных признаков работы бота: Анализ уникальных паттернов коммуникации заражённого устройства с командными серверами ботнета, использование нестандартных протоколов связи и шифрования сообщений;

3. Идентификация заражённых устройств на основе выявленных признаков: Создание специализированных алгоритмов сопоставления найденных аномалий с признаками известного ботнета для точного выявления потенциально заражённых узлов;

4. Координация агентов системы: Организация взаимодействия компонентов системы таким образом, чтобы обеспечить эффективную обработку

сигналов тревоги и совместное принятие решений относительно потенциальных угроз;

5. Контроль и мониторинг работы агентов: Постоянный контроль работоспособности каждого компонента системы, своевременное устранение сбоев и восстановление работоспособности в критических ситуациях;

6. Накопление информации: Сбор, хранение и систематизация всей полученной информации о поведении заражённых устройств и активности ботнетов для последующего анализа и улучшения эффективности системы;

7. Визуализация атак и ботнетов: Предоставление операторам наглядных инструментов отображения структуры ботнета, характера распространения инфекции и результатов противодействия атакам.

Системы будет реализована на основе многоагентного подхода. В качестве многоагентной модели системы будет использоваться понятие алгебраической системы, предложенной в исследовании [1]. MAS представляет собой:

$$MAS = (A, E, R, ORG), \quad (1)$$

где A – множество агентов; E – среда, в которой находится данная MAS; R – множество взаимодействий между агентами; ORG – множество базовых организационных структур, соответствующих конкретным функциям агентов. Отдельный агент описывается, как:

$$A_i = (E_i, R_i, ORG_i, C), \quad (2)$$

где E_i – элементы коммуникационной среды, включая источники информации, R_i - подмножество связей данного агента с другими ($R_i \subseteq R$), ORG_i– подмножество, описывающее организационную структуру агента; C – внутренняя структура агента. Также этот подход может быть приложен к системам с распределенным децентрализованным реестром [7,8].

Проведённый анализ существующих подходов и технологий показал необходимость разработки усовершенствованной системы идентификации ботнетов. Была сформулирована цель создания комплекса мер, обеспечивающего своевременное обнаружение и нейтрализацию заражённых устройств. Поставлены задачи, охватывающие обнаружение аномалий, идентификацию характерных признаков работы ботов и координацию усилий по противодействию угрозам.

Для решения поставленных задач выбрана многоагентная архитектура, обладающая необходимой гибкостью и способностью адаптироваться к разнообразным сценариям эксплуатации ботнетов. Тем не менее, остаются нерешённые вопросы, касающиеся повышения производительности, устойчивости к внешним факторам, оптимизации алгоритмов обработки данных и совершенствования процессов принятия решений агентами. Дальнейшие исследования будут направлены на углублённую разработку этих аспектов, обеспечивая надёжную защиту инфраструктур от угроз ботнетов.

Список литературы:

1. Косенко, М.Ю. Метод идентификации ботнетов на основе многоагентного подхода / М. Ю. Косенко, А. В. Мельников // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2015. – № 2. – С. 89-96. – EDN TTUFUV;

2. Распределённая система обнаружения сетевых атак на основе федеративного трансферного обучения / В. И. Васильев, А. М. Вульфин, В. М. Картак [и др.] // Вопросы кибербезопасности. – 2024. – № 6(64). – С. 117-129. – DOI 10.21681/2311-3456-2024-6-117-129;

3. Гасанов, В.И. Выявление аномалий в сетевых трафиках на основе нечёткого моделирования динамических рядов изменений объёмов IP-пакетов / В. И. Гасанов // Автоматизация и измерения в машино- приборостроении. – 2018. – № 2(2). – С. 59-70. – EDN YLQONN;

4. Карачанская, Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е. В. Карачанская, Н. И. Соседова // Безопасность информационных технологий. – 2019. – Т. 26, № 1. – С. 98-110. – EDN YZELNB.

5. Токарев, В.Л. Конструирование многоагентной системы для распознавания угроз информационной безопасности / В. Л. Токарев // Инновационное развитие науки и техники: Сборник статей VI Международной научно-практической конференции, Саратов, 10 декабря 2020 года. – Саратов: Научная общественная организация "Цифровая наука", 2020. – С. 10-20. – EDN ELXJFL.

6. Лукацкий А.В. Обнаружение атак своими силами. [Электронный ресурс] // информационная безопасность без паники и всерьез: [сайт]. [2001]. URL: https://bugtraq.ru/library/security/luka/autodetect.html (дата обращения 15.11.2025);

7. Акутин, А.С. Реализация алгоритма доказательства с нулевым разглашением в технологии цифровой личности в управлении информационно-технологическими процессами предприятия / А. С. Акутин, А. В. Бровко // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2024. – № 2. – С. 113-122. – DOI 10.17308/sait/1995-5499/2024/2/113-122. – EDN CHYCZZ;

8. Акутин, А.С. Приложение задачи поиска минимального покрытия в графе для повышения надежности системы цифровой личности / А. С. Акутин, В. В. Печенкин // Моделирование, оптимизация и информационные технологии. – 2025. – Т. 13, № 2(49). – DOI 10.26102/2310-6018/2025.49.2.015. – EDN VGIUEG