УДК 004.056:004.7

Шамин Максим Алексеевич, студент, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Россия, г. Санкт-Петербург

ВЫЯВЛЕНИЕ C2-КАНАЛОВ В ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Аннотация

В статье рассматривается задача выявления каналов командного управления вредоносного программного обеспечения в сетях объектов критической информационной инфраструктуры на основе анализа сетевого трафика. Проведен анализ особенностей сетевого взаимодействия в инфраструктурах КИИ и факторов, влияющих на обнаружение вредоносной активности. Рассмотрены демаскирующие признаки каналов управления, связанные с характеристиками сетевых сессий и периодичностью соединений. Предложен подход к выявлению C2-каналов на основе анализа статистических параметров сетевых соединений, получаемых из журналов сетевого мониторинга. Показана возможность обнаружения beacon-активности без анализа полезной нагрузки трафика, что позволяет применять метод в условиях шифрования сетевых соединений и ограничений на активное воздействие на сеть.

Ключевые слова: критическая информационная инфраструктура, C2-каналы, вредоносное программное обеспечение, анализ сетевого трафика, beacon-соединения, сетевые сессии, пассивный мониторинг.

Введение

В последние годы наблюдается активная цифровизация объектов критической информационной инфраструктуры. В технологических и производственных системах все шире применяются информационные технологии, сетевые сервисы и средства удалённого управления, что приводит

к росту зависимости технологических процессов от сетевого взаимодействия [8, 9]. Объекты КИИ становятся одной из приоритетных целей для кибератак. По данным аналитических исследований компаний АО «Солар» [4] и Positive Technologies [5], российские организации регулярно подвергаются целевым атакам, направленным на государственный сектор, промышленность, энергетику и транспортную инфраструктуру. Согласно данным Positive Technologies, на Россию приходится до 14-16% всех успешных кибератак в мире [5].

Использование каналов командного управления вредоносным программным обеспечением (Command and Control, C2) является важным этапом этаки [1]. После компрометации системы злоумышленники используют такие каналы для удалённого управления заражёнными узлами, передачи команд и получения результатов выполнения вредоносных действий. При этом C2-каналы часто маскируются под легитимный сетевой трафик и могут использовать стандартные сетевые протоколы, что существенно усложняет их обнаружение традиционными средствами защиты. В условиях широкого применения шифрования трафика и возможности быстрой смены сетевых индикаторов компрометации традиционные сигнатурные методы обнаружения вредоносной активности оказываются недостаточно эффективными.

Выявление вредоносной сетевой активности в среде объектов КИИ имеет ряд ограничений. Особенностью является невозможность активного воздействия на сетевой трафик и инфраструктуру, так как любые некорректные действия могут привести к нарушению технологического процесса. В системах защиты КИИ приоритет отдается пассивным методам анализа сетевого взаимодействия [6].

Признаки C2-каналов в сетевом трафике объектов КИИ

Одним из подходов к выявлению вредоносной активности в сетях объектов критической информационной инфраструктуры является анализ демаскирующих признаков сетевого взаимодействия. Под демаскирующими

признаками понимаются характеристики сетевых соединений, которые позволяют косвенно выявить присутствие вредоносного программного обеспечения, осуществляющего взаимодействие с удалённой инфраструктурой управления. Постэксплуатационная активность вредоносного программного обеспечения сопровождается установлением каналов командного управления, которые используются злоумышленниками для передачи управляющих команд, получения результатов выполнения операций и поддержания устойчивого присутствия в атакуемой сети.

Выделяются два основных паттерна соединений, характерных для функционирования каналов управления вредоносного программного обеспечения [1]. К первому типу относятся длительные соединения, в рамках которых между узлом и сервером управления поддерживается постоянная сессия. Ко второму типу относятся периодические кратковременные соединения, формирующие так называемый beacon-трафик [2]. Оба типа соединений могут использоваться для реализации каналов управления, однако их свойства и методы выявления существенно различаются.

Длительные сетевые соединения характеризуются значительной продолжительностью и могут сопровождаться передачей больших объёмов данных. Они часто встречаются и в легитимном сетевом трафике. К ним относятся VPN-подключения, потоковая передача мультимедийных данных, соединения систем видеонаблюдения, а также длительные сеансы работы прикладных систем.

Периодические кратковременные соединения формируются в результате регулярных обращений заражённого узла к серверу управления с целью проверки наличия новых команд. Такие соединения обычно имеют небольшую длительность и сопровождаются передачей малых объёмов данных, см. рис. 1 [1]. Интервалы между последовательными соединениями имеют близкие значения, что отражает автоматизированный характер работы вредоносного программного обеспечения. Длительность отдельных сессий тоже остаётся примерно одинаковой. В условиях сетей объектов критической

информационной инфраструктуры данный тип активности особенно заметен, поскольку сетевой трафик таких систем характеризуется высокой предсказуемостью и стабильностью [3, 8] . Регулярные соединения с внешними узлами, не относящиеся к штатным технологическим взаимодействиям, могут рассматриваться как потенциальный признак функционирования канала управления.

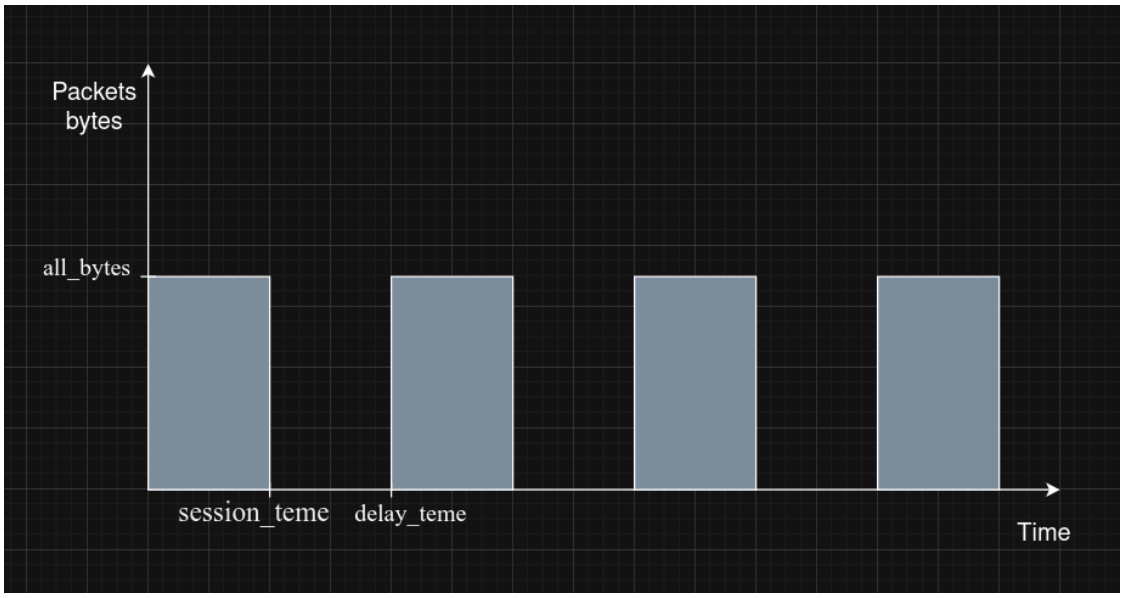

Рис. 1. Паттерн beakon-трафика

Способы выявления C2-каналов в трафике объектов КИИ

Выявление каналов командного управления вредоносного программного обеспечения в сетях объектов критической информационной инфраструктуры во многом основано на анализе сетевых соединений и их статистических характеристик. В отличие от методов, требующих анализа содержимого трафика, данный подход ориентирован на использование метаданных сетевых сессий. Источником данных для анализа могут служить журналы сетевых соединений, формируемые системами пассивного мониторинга трафика. В этих журналах фиксируется информация о параметрах сетевых сессий, включая момент установления соединения, длительность сеанса, адреса взаимодействующих узлов, используемый транспортный протокол и объем переданных данных [2] .

На основе данных о сетевых сессиях рассчитываются статистические параметры, характеризующие временную структуру соединений, их длительность и объем передаваемых данных [2] . Анализ параметров позволяет выявлять повторяющиеся паттерны сетевого взаимодействия между узлами сети, характерные для демаскирующих признаков постэксплуатационной активности.

Заключение

Проблема выявления каналов командного управления вредоносного программного обеспечения в сетях объектов критической информационной инфраструктуры напрямую связана с ограничениями на применение активных методов воздействия и широким использованием шифрования сетевого трафика. В этих условиях на первый план выходит анализ косвенных признаков сетевого взаимодействия, доступных на уровне метаданных соединений.

Рассмотренный материал показывает, что функционирование C2-каналов сопровождается формированием устойчивых паттернов сетевой активности, которые могут быть выявлены без анализа полезной нагрузки. К таким паттернам относятся как длительные соединения, так и периодические кратковременные взаимодействия. При этом именно beacon-активность обладает наибольшей выявляемостью за счёт регулярности, повторяемости временных интервалов и относительной однородности параметров сетевых сессий.

Анализ характеристик сетевых соединений, включая время установления, длительность, объём передаваемых данных и частоту обращений, позволяет формировать обобщённое представление о поведении узлов сети. В условиях КИИ, где сетевое взаимодействие отличается высокой степенью детерминированности, отклонения от типовых сценариев проявляются более явно, что повышает эффективность выявления аномальной активности.

Использование отдельных признаков не обеспечивает однозначной идентификации вредоносной активности. Сходные характеристики могут наблюдаться и у легитимных сервисов, функционирующих в штатном режиме. Это определяет необходимость комплексного анализа совокупности параметров сетевых сессий, а также учёта контекста функционирования конкретного объекта инфраструктуры. Статистический анализ сетевых соединений является обоснованным и практически применимым подходом к выявлению C2-каналов в условиях ограниченной наблюдаемости трафика. Его применение позволяет обнаруживать признаки постэксплуатационной активности даже при использовании злоумышленниками механизмов маскировки и шифрования. Эффективность данного подхода определяется возможностью выявления устойчивых аномалий в структуре сетевого взаимодействия, нехарактерных для нормального функционирования системы.

Ключевым фактором успешного обнаружения каналов управления является формирование модели нормального сетевого поведения и последующий поиск отклонений от неё на основе анализа статистических параметров соединений. Данный подход соответствует требованиям к обеспечению безопасности объектов КИИ и может рассматриваться как основа для построения систем пассивного мониторинга и выявления скрытых угроз.

Список литературы

1. Гокровенко, В. А. Выявление каналов управления проксирующего вредоносного программного обеспечения на основе анализа статистических параметров сетевого трафика / В. А. Гокровенко, М. А. Скорых // Региональная информатика и информационная безопасность : Сборник трудов XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2025. – С. 127-131. – EDN NDZOQN.

2. Скорых, М. А. Модель функционирования каналов управления вредоносного ПО в сетевом трафике ЛВС с выходом в глобальную сеть / М. А. Скорых // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2025. – № 2. – С. 79-84. – DOI 10.46418/2079-8199_2025_2_15. – EDN VOELTQ.

3. Защита АСУ ТП [Электронный ресурс]. – Режим доступа: https://cisoclub.ru/zashhita-asu-tp/

4. Аналитический отчет RT Solar [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/analytics/reports/6432/

5. Аналитический отчет RT Solar [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/analytics/reports/6432/

6. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

7. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

8. Киселев, Н. Н. Метод автоматизации процедуры аттестации объектов критической информационной инфраструктуры в удаленных регионах России / Н. Н. Киселев // Вопросы защиты информации. – 2025. – № 1(148). – С. 53-58. – DOI 10.52190/2073-2600_2025_1_53. – EDN JVLLXU.

9. Киселев, Н. Н. Законодательство и организационные меры как основа информационной безопасности критически важной информационной инфраструктуры регионального уровня управления в медицинском учреждении / Н. Н. Киселев // Вектор научной мысли. – 2025. – № 3(20). – С. 229-239. – EDN QUSTNG.