Инженерный вестник Дона, №3 (2026)
ivdon.ru/ru/magazine/archive/n3y2026/10822

Метод выявления камуфлированных сетевых соединений, построенных на основе DNS-протокола, в корпоративной сети организации

Г.Ф. Шипулин[1,2], М.С. Широков[2]

[1]МИРЭА – Российский технологический университет, Москва
[2]Московский политехнический университет

Аннотация: Статья посвящена решению проблемы выявления камуфлированных (скрытых) сетевых соединений, построенных на основе DNS-протокола (Domain Name System, система доменных имён), в корпоративной сети организации. Исследование направлено на разработку метода выявления камуфлированных (скрытых) сетевых соединений в корпоративной сети организации. Предложенный метод основывается на вычислении энтропии поддоменных имен, пороговых значений количества получаемых ответов от DNS-сервера и доли уникальных поддоменов для каждого домена. Его применение позволяет обнаруживать все виды DNS-туннелей в циркулирующем сетевом трафике корпоративной сети, что подтверждается результатами проведенного эксперимента в рамках исследования.
Ключевые слова: туннелирование, DNS-протокол, камуфлированное сетевое соединение, энтропия, анализ сетевых соединений, информационная безопасность.

В связи с непрерывным развитием информационных технологий и средств защиты информации, совершенствуются также методы, способы и средства осуществления компьютерных атак. Одним из способов сокрытия факта компрометации злоумышленником корпоративной информационной инфраструктуры организации является использование камуфлированных (скрытых) сетевых соединений, в частности, построенных на базе DNS-протокола (Domain Name System, система доменных имён), применяемых как на этапах «доставка», «получение управления», так и «выполнение действий» согласно темпоральной модели Cyber Kill Chain [1], описывающей в семи этапах выполнение компьютерных атак.

Туннелирование представляет собой процесс организации логического сетевого канала передачи данных между двумя конечными точками в сети, формируемый поверх существующей сетевой инфраструктуры [2]. Под DNS-туннелированием понимается вид сетевой атаки, заключающийся в организации камуфлированного (скрытого) логического канала связи с

использованием протокола DNS, в рамках которого DNS-сообщения используются для передачи произвольных данных между заражённым (скомпрометированным) узлом и DNS-сервером, контролируемым злоумышленником [2].

Рассмотрим основные сценарии применения DNS-туннелирования и их соответствие этапам выполнения компьютерных атак в рамках модели Cyber Kill Chain (рис.1).

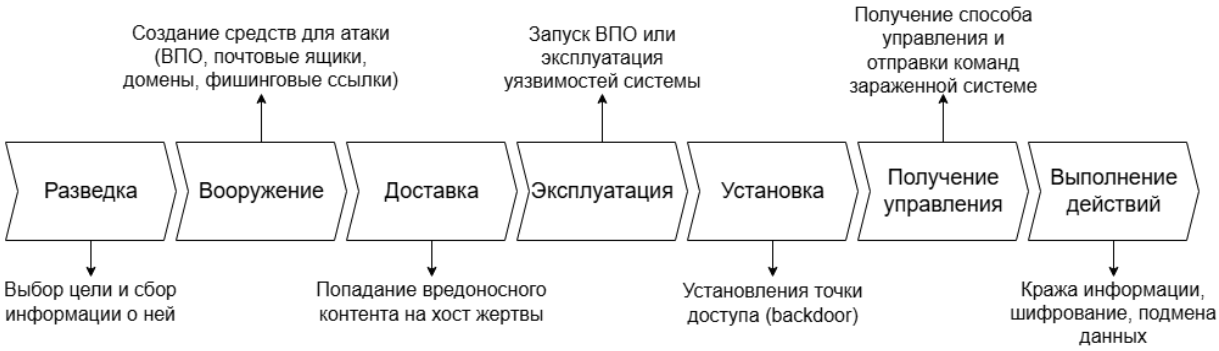

Рис. 1. – Модель Cyber Kill Chain

1. Эксфильтрация данных

Данная группа сценариев использования DNS-туннелирования применяется при отправке данных с контролируемого устройства жертвы на сервер атакующего, которые передаются в поле запрашиваемого доменного имени DNS-запроса к DNS-серверу. Успешная эксфильтрация фактически означает утечку конфиденциальной информации за пределы контролируемого периметра (например, персональных данных, платёжных реквизитов, интеллектуальной собственности) [3, 4].

Эксфильтрация относится к этапу «Выполнение действий» модели Cyber Kill Chain, поскольку выполняется уже после компрометации – когда цели злоумышленника на зараженной системе достигнуты, и данные готовы к отправке за пределы периметра корпоративной сети организации.

2. Доставка данных

Данная группа сценариев использования DNS-туннелирования предназначена для доставки данных (вредоносного программного обеспечения, управляющих инструкций) на атакованный компьютер. При этом сам DNS-туннель может выступать как канал передачи управляющих команд от сервера управления и контроля злоумышленника (Command And Control Server, C&C-сервер), так и в качестве средства транспортировки вредоносного кода либо иной полезной нагрузки [3]. При этом сами данные расположены в полях ресурсных записей DNS-ответа, например, в TXT-записях.

Таким образом, в контексте модели Cyber Kill Chain сценарии, связанные с транспортировкой вредоносного программного обеспечения посредством DNS-туннелирования, относятся к этапу «Доставка»; сценарии, связанные с организацией скрытого сетевого канала связи между C&C-сервером злоумышленника и скомпрометированным хостом в сети, относятся к этапу «Получение управления».

Стоит отметить, несмотря на разные цели применения камуфлированных (скрытых) сетевых каналов передачи данных, построенных на основе DNS протокола, технология построения и параметры таких сетевых соединения не имеют различий.

Выделяют три основных метода детектирования камуфлированных (скрытых) сетевых соединений, построенных на основе DNS протокола (DNS-туннелирования):

- на основе энтропии [5];
- на основе количества DNS-ответов [6];
- на основе качества DNS-ответов [6].

Первый метод заключается в анализе энтропии используемых доменных имен и поддоменов, участвующих в сетевом обмене. Исходя из принципов работы DNS-системы можно однозначно утверждать, что

доменное имя всегда осмысленно и не содержит случайный набор символов. Ввиду этого, можно сделать вывод, что чем выше распределение символов в домене третьего уровня и выше, тем больше вероятность, что домен используется для DNS-туннелирования, а значит и имеет больший показатель энтропии.

Для подсчета энтропии принято использовать формулу Шеннона. Пусть C – анализируемая строка, N – число символов в строке C, где M – число уникальных символов, формирующих алфавит A. Эмпирическая вероятность появления каждого символа $x \in A$ в строке C определяется как:

$$p(x) = \frac{count(x)}{N}, \quad (1)$$

где $count(x)$ – число вхождений символа x в строке C. Тогда энтропия строки C вычисляется по следующей формуле [7]:

$$H(C) = -\sum_{i=1}^{M} p(x_i) log_2 p(x_i) \quad (2)$$

Таким образом, энтропия вычисляется для произвольной строки C, являющейся поддоменным именем; чем выше значение энтропии для строки C, тем выше вероятность того, что проверяемое поддоменное имя используется для DNS-туннелирования.

Данный метод является достаточно эффективным для применения на практике, но имеет также ряд ограничений:

- большое количество ложноположительных срабатываний, поскольку DNS-запросы могут быть содержать нестандартные имена, особенно при взаимодействии с облачными сервисами или при использовании API-токенов (Application Programming Interface, программный интерфейс приложения);
- при использовании коротких поддоменных имен (записей) значение энтропии может быть в пределах заданной нормы.

Второй метод заключается в выявлении доменных имен, фигурирующих в аномально высоком количестве входящих сетевых пакетов от DNS-сервера за определенный интервал времени.

Ключевым признаком доставки данных посредством DNS-туннеля является большое количество полученных сетевых пакетов от конкретного домена. Так, при определении среднего числа ответов от DNS-сервера для каждого доменного имени в защищаемой корпоративной сети возможно выявить доменные имена с аномально высоким значением данного показателя, что позволяет отнести их к потенциальным источникам DNS-туннелирования. При этом данный метод может быть реализован посредством написания соответствующего правила детектирования и его активации в системе обнаружения вторжений, функционирующей в корпоративной сети организации.

Данный метод прежде всего предназначен и применим для детектирования DNS-туннелирования, используемого при доставке вредоносного программного обеспечения за счет большого количества передаваемых сетевых пакетов.

Третий метод заключается в выявлении доменов, которые обладают нетипичными параметрами DNS-обмена (низкий параметр TTL (Time to Live, времени жизни записи), высокая доля уникальных поддоменов, а именно количество уникальных поддоменов одного домена деленое на общее количество таких запросов).

В рамках стандартной работы DNS системы авторитетный сервер самостоятельно задает значение TTL (стандартно в диапазоне от 300 до 3600 секунд), определяющего время кэширования ответа. При реализации DNS-туннеля злоумышленники стремятся минимизировать влияние кэширования: для этого может быть использовано понижение значения TTL (например, до нескольких десятков секунд) и/или аномально большое количество уникальных поддоменных имен.

Стоит также отметить, что показатель доли уникальных имен поддоменов является статистически значимым только при достаточном

объеме наблюдений, поскольку позволяет исключить ложноположительные срабатывания, обусловленные единичными обращениями к легитимным доменным именам.

Преимуществом данного метода считается его эффективность для детектирования DNS-туннелирования, используемого в качестве канала передачи управляющих команд от сервера управления и контроля злоумышленника.

На основе анализа рассмотренных методов, их преимуществ и ограничений применения представляется целесообразным использование комбинированного подхода к детектированию камуфлированных (скрытых) сетевых соединений, построенных на основе DNS-протокола.

Предлагаемый метод включает вычисление энтропии поддоменных имен, пороговых значений количества получаемых DNS-ответов, а также доли уникальных поддоменов для каждого домена. Метод может быть применим как в режиме потокового анализа сетевого трафика с выделением всех
DNS-соединений, так и на основе уже записанного дампа сетевого трафика, и состоит в следующем:

1. Выделение в сетевом трафике всех DNS-соединений.
2. Формирование списка доменных имен и соответствующих им поддоменов из DNS-запросов.
3. Вычисление энтропии каждого поддоменного имени из сформированного в п.2 списка и сравнение с установленным пороговым значением.
4. Добавление к записям сформированного в п.2 списка значений параметров TTL в DNS-ответах и сравнение их с установленным пороговым значением.

5. Вычисление количества DNS-ответов для каждого доменного имени в выделенном сетевом трафике за установленный интервал времени, добавление к записям сформированного в п.2 списка, сравнение с установленным пороговым значением;

6. Вычисление доли уникальных поддоменов для каждого доменного имени, добавление к записям сформированного в п.2 списка, сравнение с установленным пороговым значением.

Таким образом, в результате применения данного метода будет формирован список, каждая запись которого состоит из следующих полей:

- «имя_домена»;
- «перечень_поддоменных_имен»;
- «перечень_значений_энтропии_каждого_поддоменного_имени»;
- «количество_DNS_ответов_каждого_домена»;
- «перечень_значений_TTL_каждого_поддомена»;
- «доля_уникальных_поддоменных_имен».

Все используемые рекомендованные пороговые значения были предложены в [7] или определены авторами опытным путем, представлены в таблице 1.

Таблица № 1

Рекомендованные пороговые значения

Параметр	Пороговое значение
Энтропия поддоменного имени	более 4
Количество DNS-ответов	более 100 за 15 минут
Доля уникальных поддоменов	более 0.9
Значение TTL	менее 300 секунд

Для оценки применимости предложенного метода был проведен эксперимент, в рамках которого было развернут изолированный стенд с использованием средства контейнеризации Docker. В рамках изолированной

среды был подготовлен единый дамп сетевого трафика, записанный в течение 15 минут, и включающий основные сценарии применения DNS-туннелирования (всего 5 DNS-туннелей), а также легитимные DNS-соединения в рамках стандартного DNS-обмена. Для эмуляции сценариев DNS-туннелирования использовались программные инструментальные средства «dnscat2» и «iodine» [8, 9], что позволило сгенерировать сетевой трафик с различными статистическими и поведенческими характеристиками.

Детектирование камуфлированных (скрытых) сетевых соединений, построенных на основе DNS-протокола (DNS-туннелей) выполнялось поочередно каждым из описанных в работе методов по отношению к одному сформированному дампу сетевого трафика объемом 15 Мб.

Для анализа подготовленного дампа сетевого трафика и извлечения необходимых характеристик использовалась система обнаружений вторжений с открытой лицензией Zeek, позволяющая получать детализированные журналы DNS-запросов и ответов [10].

Результаты применения разных методов детектирования каждого из сценариев DNS-туннелирования с соотношением к определенному этапу выполнения компьютерной атаки согласно темпоральной модели Cyber Kill Chain представлены в таблице 2.

Сравнительный анализ применения каждого из методов детектирования в рамках проведенного эксперимента показал, что предложенный является наиболее эффективным, поскольку с его помощью были определены все DNS-туннели в подготовленном дампе сетевого трафика.

Подводя итог, предложенный метод выявления камуфлированных сетевых соединений, построенных на основе DNS-протокола, основан на вычислении энтропии поддоменных имен, пороговых значений количества

получаемых DNS-ответов и доли уникальных поддоменов для каждого домена. Его применение позволяет повысить полноту контроля сетевого периметра организации и обнаруживаемость DNS-туннелей в циркулирующем сетевом трафике корпоративной сети, что подтверждается результатами проведенного эксперимента.

Таблица № 2

Сравнение результатов применения методов детектирования DNS-туннелей

Этап / Метод	Выполнение действий (1 DNS-туннель)	Доставка (2 DNS-туннеля)	Получение управления (2 DNS-туннеля)
на основе энтропии	1/1	0/2	1/2
на основе количества DNS-ответов	1/1	2/2	0/2
на основе качества DNS-ответов	0/1	1/2	2/2
предложенный	1/1	2/2	2/2

Литература

1. Enhancing Cybersecurity with Cyber Kill Chain. URL: lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 20.01.2026).

2. Авакьянц А.В., Урубкин М.Ю., Фатхи Д.В. Особенности реализации виртуальных туннелей на основе служебных сетевых протоколов // Инженерный вестник Дона, 2019, №1 URL: ivdon.ru/ru/magazine/archive/n1y2019/5643/.

3. Калинин А. Техники использования DNS в атаках вредоносных программ URL: anti-malware.ru/analytics/Threats_Analysis/Using-DNS-in-malware-attacks/ (дата обращения: 20.01.2026).

4. Хромова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона, 2023, №6 URL: ivdon.ru/ru/magazine/archive/n6y2023/8447/.

5. Homem I., Papapetrou P., Dosis S. Entropy-based Prediction of Network Protocols in the Forensic Analysis of DNS Tunnels // Advances in Digital Forensics. 2018. XIV. pp. 127-140.

6. Farnham G. Detecting DNS Tunneling URL: sans.org/white-papers/34152/ (дата обращения: 20.01.2026).

7. Salat L., Davis M., Khan N. DNS Tunnelling, Exfiltration and Detection over Cloud Environments // Sensors. 2023. V. 23. №5. URL: mdpi.com/1424-8220/23/5/2760.

8. Dns2Cat. URL: github.com/iagox86/dnscat2/ (дата обращения: 20.01.2026).

9. Iodine. URL: github.com/yarrick/iodine/ (дата обращения: 20.01.2026).

10. Zeek: Documentation. URL: docs.zeek.org/en/master/ (дата обращения: 20.01.2026).

References

1. Enhancing Cybersecurity with Cyber Kill Chain. URL: lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed: 20.01.2026).

2. Avak'yanc A.V., Urubkin M.Yu., Fathi D.V. Inzhenernyj vestnik Dona, 2019, №1 URL: ivdon.ru/ru/magazine/archive/n1y2019/5643/.

3. Kalinin A. Tekhniki ispol'zovaniya DNS v atakah vredonosnyh programm [Techniques of using DNS in malware attacks] URL: anti-malware.ru/analytics/Threats_Analysis/Using-DNS-in-malware-attacks/ (accessed: 20.01.2026).

4. Hromova A.R., Petrosyan L.E. Inzhenernyj vestnik Dona, 2023, №6 URL: ivdon.ru/ru/magazine/archive/n6y2023/8447/.

5. Homem I., Papapetrou P., Dosis S. Advances in Digital Forensics. 2018. XIV. pp. 127-140.

6. Farnham G. Detecting DNS Tunneling URL: sans.org/white-papers/34152/ (accessed: 20.01.2026).

7. Salat L., Davis M., Khan N. DNS Sensors. 2023. V. 23. №5. URL: mdpi.com/1424-8220/23/5/2760.

8. Dns2Cat. URL: github.com/iagox86/dnscat2/ (accessed: 20.01.2026).

9. Iodine. URL: github.com/yarrick/iodine/ (accessed: 20.01.2026).

10. Zeek: Documentation. URL: docs.zeek.org/en/master/ (accessed: 20.01.2026).

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 21.01.2026

Дата публикации: 28.02.2026