МЕТОД ОБНАРУЖЕНИЯ ФАКТОВ ОБХОДА БЛОКИРОВОК РЕСУРСОВ СЕТИ ИНТЕРНЕТ

Ишкуватов С. М.[1], Бегаев А. Н.[2], Комаров И. И.[3], Левко И. В.[4]

DOI: 10.21681/2311-3456-2024-3-76-84

Цель исследования: *разработка и экспериментальное исследование метода обнаружения фактов обхода блокировки трафика, осуществляющего доступ к запрещённым Интернет-ресурсам.*

Методы исследования: *системный анализ, теория метрических пространств, математическая статистика, теория систем искусственного интеллекта, теория обработки экспериментальных данных.*

Полученные результаты: *систематизированы информативные признаки, используемые актуальными методами и средствами блокировки запрещённых ресурсов сети Интернет, а также способы обхода таких блокировок; определена новая совокупность информативных признаков, обеспечивающая решение задачи исследования; предложен обобщённый метод обнаруженя фактов обхода блокировки запрещённых ресурсов сети Интернет и получено экспериментальное подтверждение его продуктивности.*

Научная новизна *полученных результатов определяется систематизацией нормативно-правовых и организационно-технических требований к средствам обнаружения и блокирования доступа к запрещённым ресурсам сети Интернет, что обеспечивает формирование прогнозов их развития; использованием авторской совокупности методов мониторинга трафика на основании анализа цифровых отпечатков коммуникационных протоколов и закономерностей следования и объёма передаваемых данных, обеспечивающих возможность выявления и анализа информативных признаков обычно скрытых для пассивного наблюдателя; разработкой обобщённого метода обнаружения факта обхода блокировки трафика на основании анализа устойчивых закономерностей, присущих коммуникационным сессиям.*

Вклад авторов: *Бегаев А. Н. – определение технико-экономических ограничений и требований к реализации метода обнаружения факта обхода блокировки трафика; Комаров И. И. – постановка задачи и определение плана исследования; Ишкуватов С. М. – анализ информативных признаков, разработка метода обнаружения факта обхода блокировки трафика, проведение эксперимента; Левко И. В. – анализ нормативно-правовых аспектов регулирования доступа к Интернет-ресурсам, анализ и интерпретация результатов эксперимента.*

Ключевые слова: *Интернет-цензура, фильтрация трафика, туннелирование трафика, маскирование сессии, пассивный наблюдатель, цифровой отпечаток, глубокий анализ пакетов.*

A METHOD FOR DETECTING FACTS OF CIRCUMVENTION OF INTERNET RESOURCE LOCKS

Ishkuvatov S. M.[5], Begaev A. N.[6], Komarov I. I.[7], Levko I. V.[8]

The purpose of the study: *development and experimental study of a method for identifying facts of circumvention of traffic blocking, providing access to prohibited Internet resources.*

Research methods: *system analysis, theory of metric spaces, mathematical statistics, theory of artificial intelligence systems, theory of experimental data processing.*

1 Ишкуватов Сергей Маратович, аспирант факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: sysroot0@gmail.com, ORCID ID: 0000-0002-4006-3693

2 Бегаев Алексей Николаевич, кандидат технических наук, генеральный директор АО «Эшелон-СЗ», Санкт-Петербург, Россия. E-mail: begaev@mail.ru, ORCID ID: 0000-0003-1186-7614

3 Комаров Игорь Иванович, кандидат физико-математических наук, доцент, доцент факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: i_krov@mail.ru, ORCID ID: 0000-0002-6542-4950

4 Левко Игорь Владимирович, кандидат технических наук, доцент, Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, Россия. E-mail: levko_iv@mail.ru

5 Sergei M. Ishkuvatov, Ph.D. student, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: sysroot0@gmail.com

6 Alexey N. Begaev, Ph.D., CEO of JSC North-West Echelon, St. Petersburg, Russia. E-mail: begaev@mail.ru

7 Igor I. Komarov, Ph.D., (in Maht.), Associate Professor, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: i_krov@mail.ru

8 Igor V. Levko, Ph.D., Associate Professor, Mozhaisky Military Aerospace Academy, St. Petersburg, Russia. E-mail: levko_iv@mail.ru

The results obtained: *the informative signs used by current methods and means of blocking prohibited Internet resources, as well as ways to circumvent such locks, are systematized; a new set of informative signs providing a solution to the research problem is determined; a generalized method for detecting facts of circumventing the blocking of prohibited Internet resources is proposed and experimental confirmation of its productivity is obtained.*

The scientific novelty *of the results obtained is determined by the systematization of regulatory and organizational and technical requirements for means of detecting and blocking access to prohibited Internet resources, which ensures the formation of forecasts for their development; using the author's set of traffic monitoring methods based on the analysis of digital fingerprints of communication protocols and patterns of sequence and volume of transmitted data, providing the possibility of identifying and analyzing informative signs usually hidden to a passive observer; the development of a generalized method for detecting the fact of bypassing traffic blocking based on the analysis of stable patterns inherent in communication sessions.*

Contribution of the authors: *Begaev A. N. – definition of technical and economic limitations and requirements for the implementation of the method of detecting the fact of bypassing traffic blocking; Komarov I. I. – setting the task and defining the research plan; Ishkuvatov S. M. – analysis of informative signs, development of a method for detecting the fact of bypassing traffic blocking, conducting an experiment; Levko I. V. – analysis of regulatory aspects of regulating access to Internet resources, analysis and interpretation of experimental results.*

Keywords: *Internet censorship, traffic filtering, traffic tunneling, session masking, passive observer, digital fingerprint, deep packet analysis.*

Введение

Обеспечение информационной безопасности государства в условиях информационного противоборства сопряжено с разрешением объективного противоречия между соблюдением прав и свобод субъектов и необходимостью регулирования информационного потока в условиях глобальной доступности данных. С точки зрения технологических задач кибербезопасности выделяются ряд взаимосвязанных направлений, связанных с: выявлением и анализом сематического воздействия на пользователя [1, 2]; разработкой методов и средств анализа киберустойчивости сложных технических систем [3, 4]; совершенствованием методов реализации организационных решений в технических системах [5–7].

В контексте общего тренда развития правового обеспечения информационной безопасности России [8, 9], и в частности – согласно поправкам в Законы «О связи[9]» и «Об информации, информационных технологиях и защите информации[10]», вступившим в силу с 1 ноября 2019 года, операторы связи обязаны устанавливать специализированное оборудование для обеспечения безопасности и контроля передаваемой информации, в том числе – оборудование анализа и фильтрации трафика для ограничения доступа к запрещённым ресурсам сети Интернет, определённое в Законе как Технические Средства Противодействия Угрозам (ТСПУ). Закон предусматривает административную ответственность за нарушение требований по пропуску трафика через ТСПУ, а также уголовную ответственность за нарушение порядка их установки, эксплуатации и модернизации.

Одной из сложнейших задач практической реализации мер государственной политики в области кибербезопасности является обнаружение и управление трафиком, взаимодействующим с запрещёнными ресурсами. Эта задача осложняется использованием методов сокрытия самого факта обращения, высокой ресурсоёмкостью методов глубокого анализа трафика (DPI – Deep Packet Inspection), а также недостаточным уровнем развития научно-методического аппарата обнаружения такого трафика в общем потоке легитимных обращений, что приводит к низкой селективности используемых технических решений.

Таким образом актуализируется задача совершенствования научно-методического аппарата обнаружения и блокировки нежелательного трафика, особенно в условиях сознательного обхода запретов и ограниченности доступных вычислительных ресурсов.

Методы и средства блокировки нежелательного трафика

ТСПУ имеют целью фильтрацию трафика и блокировку доступа к запрещённым ресурсам сети Интернет. В Российской Федерации используются достаточно широкий спектр отечественных решений

9 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (в действующей редакции).

10 Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ (в действующей редакции).

DPI[11], которые адаптированы для работы с единым реестром ресурсов Роскомнадзора[12]:

- ✓ СПАК «Equila» от ООО «Напа Лабс»,
- ✓ СПО «CyberFilter» от ИП Кучебо Н.Н.,
- ✓ СПО «Барьер» от АО «Энвижн Груп»,
- ✓ СПО «АДМ Filter» от ООО «АДМ Системы»,
- ✓ СПО «ZapretService» от ИП Пономаренко И.Р.,
- ✓ СПО «Ideco Selecta ISP» от ООО «Айдеко»,
- ✓ СПО «Carbon Reductor DPI» от ООО «Карбон Софт»,
- ✓ СПО «SkyDNS Zapret ISP» от ООО «СкайДНС»,
- ✓ СПАК «Тиксен-Блокировка» от ООО «Эд-АйТи»,
- ✓ СКАТ DPI от ООО «ВАС Экспертс»,
- ✓ СПАК EcoFilter от ООО «РДП.РУ»,
- ✓ СПО «UBIC» от ООО «Безопасный интернет»,
- ✓ САПК «Периметр-Ф» от ООО «МФИ Софт».

В зависимости от способа установки оборудования [10] возможны следующие типы блокировки.

- Пассивная блокировка – не предполагает работы в разрыв соединения и запрет обмена данными между узлами. При обнаружении признака запрещённого ресурса, в канал инжектируются пакеты завершения соединения. При такой организации оборудование DPI получает для анализа «отзеркалированный» трафик, а непосредственного запрета обмена не происходит.
- Активная блокировка, предполагающая работу в разрыв соединения и полноценную MITM-инжекцию в сессиях, имеющих признаки обращения к запрещённым ресурсам. Активная блокировка – ресурсозатратный подход: при превышении допустимой нагрузки могут возникнуть проблемы при передаче разрешённых сессий, поэтому обязательно применение механизма Bypass[13], который в случае перегрузки пустит трафик по альтернативному маршруту.

На практике в среде специалистов разрабатываются программные решения, позволяющие определить применяемые типы блокировок, например blockcheck[14].

Технически блокировка отдельной Web-страницы возможна лишь в случае использования протокола HTTP, доля которого непрерывно сокращается. Для протоколов, использующих шифрование HTTPS или QUIC, возможна только полная блокировка сессии. Согласно публичной документации приведённых выше ТСПУ можно сделать выводы о номенклатуре и эффективности применения информативных признаков, используемых для принятия решения о блокировке трафика, а именно:

- блокировка по IP-адресу – характеризуется простотой реализации, высокой производительностью, но крайне низкой селективностью: в случае использования сети доставки контента (CDN – Content Delivery Network) одновременно с запрещённым ресурсом будет заблокировано множество легитимных, поскольку одному IP-адресу соответствует множество сторонних ресурсов;
- блокировки по значениям полей HTTP HOST, HTTP URL являются достаточно универсальными, поскольку могут блокироваться только определённые Web-страницы. Однако протокол HTTP уже практически полностью вытеснен протоколом HTTPS, который не позволяет пассивному наблюдателю определить запрашиваемую страницу;
- блокировка по TLS SNI (Server Name Indication) не всегда применима, так как поле является опциональным, оно сообщает серверу к какому ресурсу обращается клиент во время TLS-рукопожатия;
- сертификат сервера, к которому обращается клиент: проверяется в том случае если не использовалось расширение TLS SNI.

Очевидно, что существующая практика блокировки запрещённых Интернет-ресурсов не в полной мере соответствует организационным решениям и правовым требованиям, что актуализирует задачу разработки методов автоматического обнаружения нежелательного трафика, обладающих повышенной селективностью и приемлемой ресурсоёмкостью, базирующихся на использовании новых информативных признаков.

Методы и средства обхода блокировки трафика

Блокировки Интернет-ресурсов, особенно случайные блокировки легитимных ресурсов, находящихся на одних серверах с запрещёнными, побуждают пользователей применять различные инструменты для обхода таких запретов. Известны следующие типы программных средств, применяемых для обхода ограничений и скрывающих от пассивного наблюдателя информативные признаки, по которым принимается решение о блокировке.

- Программы-фрагментаторы сессий, работа которых основана на том, что протокол TCP допускает нарушение хронологии передачи пакетов, их фрагментацию или потерю. Принимающая сторона, может восстановить исходную хронологию и перезапросить потерянные фрагменты. Известны следующие виды искусственной фрагментации:

11 Российские производители DPI и их платформы URL: https://vasexperts.ru/blog/dpi/rossijskie-proizvoditeli-dpi-i-ih-platformy/ (дата обращения: 10.02.2024).

12 Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено -URL: https://eais.rkn.gov.ru/ (дата обращения: 10.02.2024)

13 Устройства Bypass предполагают коммутацию входного пакета на выход, минуя вышедшие из строя определённые функциональные блоки URL: https://moxa.pro/blogs/articles/obzor-bypass-ustroystva-obu-102 (дата обращения: 10.02.2024)

14 https://github.com/ValdikSS/blockcheck

- TCP-фрагментация для первого пакета данных;
- TCP-фрагментация пакетов, содержащих Keep-Alive;
- синтаксическое смешивание с целью обхода встроенных шаблонов ТСПУ, но с сохранением корректности с точки зрения спецификации протокола HTTP (произвольное изменение регистра букв; изменение пробельных символов; добавление пробелов к заголовку; перенос строк в Unix-стиле);
- введение в заблуждение DPI (отправка ложных пакетов с низким TTL, некорректными контрольными суммами, некорректным порядком следования TCP Sequence/Acknowledgment);
- фрагментация поля TLS Client Hello таким образом что часть имени сервера будет находиться в одном пакете, а продолжение в другом.

Задача детектирования таких сессий осложняется тем, что некоторые протоколы, такие как Jabber, могут начать процедуру TLS-рукопожатия после обмена нешифрованной служебной информацией, что означает, что дефрагментация и анализ пакета не может ограничиваться только первыми несколькими пакетами сессии. Искусственная фрагментация пакетов сессии позволяет разбить передаваемый признак на разные пакеты[15], тем самым сделать невозможным его определение без полной фрагментации и сборки сессии. Поскольку все приведённые выше признаки, кроме IP-адреса, не всегда передаются в первом пакете сессии, оборудование ТСПУ должно либо резервировать вычислительные ресурсы и память для дефрагментации каждой проходящей через него сессии, либо выявлять признаки блокировки только в целых пакетах.

- Программы, использующие eSNI или Encrypted Client Hello и позволяющие скрыть доменное имя запрашиваемого ресурса: предполагается одновременное использование протоколов DNS over TLS, DNS over HTTPS, DNS over QUICK или других протоколов, шифрующих запросы DNS.
- Программы, использующие трудно детектируемые протоколы (например, Telegram и некоторые протоколы BitTorrent).
- Использование туннелирования трафика различными VPN-решениями: предполагается наличие сервера за оборудованием ТСПУ, соединение с которым осуществляется с помощью туннеля (например, OpenVPN, IPsec, Wireguard). В таком случае все приведённые информативные признаки передаются в шифрованном виде, исключающем их выявление оборудованием ТСПУ.
- Туннелирование трафика инструментами[16], не являющимися распространёнными VPN-решениями (например, туннелирование TLS over SSH, TLS over TLS с использованием программ Shadowsocks, OCserv).
- Туннелирование с использованием стеганографии – организуется туннель между абонентом и сервером, находящемся за ТСПУ. Однако скрывается сам факт использования туннеля: трафик маскируется под другой тип (например, инструмент XRay, который маскирует трафик под TLS-сессии популярных приложений, воспроизводя их цифровые отпечатки (ЦО)).

Таким образом современное состояние противоборства технологий блокировки трафика и их обхода характеризуется следующими тезисами.

- ✓ С увеличением доступных вычислительных ресурсов методы, связанные с фрагментацией пакетов, теряют актуальность: оборудование ТСПУ дефрагментирует сессии или их начальные пакеты до завершения процедуры рукопожатия сторон.
- ✓ Все сессии, использующие расширение eSNI, могут быть заблокированы при обнаружении поддержки такого расширения клиентом в процессе TLS-рукопожатия.
- ✓ Протоколы, шифрующие DNS-запросы, могут быть заблокированы по конечным точкам; их блокировка по IP-адресу не должна повлиять на доступность других ресурсов.
- ✓ Очевидно, что блокировки только нешифрованных ответов DNS, содержащих адреса запрещённых ресурсов, недостаточно ввиду массового распространения альтернативных протоколов, использующих шифрование.
- ✓ Блокировка всех протоколов, которые не удалось идентифицировать ТСПУ, приведёт к блокировкам множества частных нераспространённых протоколов и неработоспособности множества простых сетевых устройств и не распространённых сервисов.
- ✓ Блокировка всех VPN-соединений, также невозможна, такт как этот протокол легитимно используется множеством организаций для обеспечения связи своих филиалов, удалённого доступа сотрудников во внутреннюю сеть или личные рабочие места через сеть Интернет.
- ✓ Допустимой является блокировка сессий с конечными точками известных VPN-сервисов анонимайзеров, но такой подход будет иметь ограниченную эффективность виду большого числа подобных сервисов и относительной простоты их миграции.

15 Автономный способ обхода DPI и эффективный способ обхода блокировок сайтов по IP-адресу. URL: https://habr.com/ru/post/335436 (дата обращения: 10.02.2024)

16 Современные технологии обхода блокировок: V2Ray, XRay, XTLS, Hysteria, Cloak и все-все-все. URL: https://habr.com/ru/articles/727868/ (дата обращения: 10.02.2024).

✓ Сохраняется основное противоречие организации блокировки в условиях плохой селективности: при строгой блокировке всегда будут затронуты сторонние ресурсы и сервисы, а мягкая не обеспечивает достижения поставленных целей.

Постанова задачи, гипотеза исследования и эксперимент

Задача исследования состоит в разработке метода обнаружения обходов блокировок трафика, базирующегося на новых информативных признаках и позволяющего отличить штатное использование протоколов от их применения в качестве инструментария обхода блокировок.

Гипотеза исследования: «*Средства, используемые для обхода блокировок трафика, обладают устойчивыми информативными признаками, сохраняющимися при применении стандартных методов их использования*».

Проверка гипотезы исследования проведена экспериментальным путём с применением авторского теоретического аппарата [11–13], расширяющего возможности принятия решения в задачах кибербезопасности за счёт анализа ЦО коммуникационных протоколов и выявленных закономерностей между порядком следования и объёмом передаваемых данных в процессе взаимодействия.

Экспериментальный стенд включает компьютер с ОС Windows и облачный Linux-сервер, между которыми организовывались туннели с помощью широко распространённых программ OCserv и XRay.

Для получения записей на сервере использованы средства screen, tcpdump и сервер телефонии Asterisk. На клиентской части – nekoray[17] и VoIP-клиент. Записаны сессии инструмента TLS over TLS OCserv и сессии туннелей XRay для трафика Web-браузера и тестового VoIP-звонка.

Для оценки качества детектирования сохранены обычные TLS-сессии, не являющиеся сессиями инструментов туннелирования. С помощью авторского инструментария все сессии дефрагментировались и исследовались с целью выявления устойчивых закономерностей.

Информативные признаки сессий туннелей, организованных OCserv

Демаскирующие признаки туннелирования трафика инструментами, не являющимися распространёнными VPN-протоколами, определяются тем, что средство, которое реализует туннель TLS over TLS или SSH over TLS создаёт сессии, выделяющиеся *продолжительностью*, а также частичным сохранением *объёмных закономерностей* исходного (маскируемого) трафика. Пассивному наблюдателю доступны признаки внешнего TLS или SSH-рукопожатия, а такие рукопожатия, в свою очередь, также имеют свои ЦО JA3(JA4), HASSH.

Экспериментально подтверждено, что все сессии инструмента OCserv, несмотря на возможность маскировки под обычные HTTPS-сессии за счёт задания произвольных конечных точек TLS Server Name, ЦО TLS соответствует реализации OpenConnect, которая не используется иначе, как для организации туннелей, что является явным признаком попытки маскирования туннелированной сессии.

Наблюдаемый ЦО отличается от ЦО популярных браузеров и также может однозначно характеризовать сессию туннеля. В табл. 1 приведены известные значения ЦО, полученные из базы данных Cisco Mercury[18], полужирным шрифтом выделена строка с ЦО, соответствующая сессиям туннелей.

Естественно, что признаком для блокировки трафика, генерируемого данным средством, будет обнаружение такого ЦО TLS, кроме того, должен быть заблокирован трафик и его новых реализаций, содержащий ЦО близких соседей, найденных по методу [11].

Дополнительными демаскирующими признаками таких сессий являются:

– распределения длин пакетов, сильно отличающихся от остальных сессий, не являющимися туннелями;
– аномальная частота появления сессий с подобным адресатом.

Информативные признаки стеганографически туннелированного трафика

Типичным примером программы для стеганографического сокрытия туннелированного трафика является XRay. Будучи установлен на сервер, он переадресует все HTTPS-запросы не от своей клиентской части на запрашиваемый ресурс. Клиентская часть в точности воспроизводит процесс TLS-рукопожатия с произвольно выбранным ЦО; проблемы поддержки всех возможных опций и алгоритмов шифрования нет, поскольку серверная часть в любом случае проигнорирует их и ответит сообщением TLS-рукопожатия сервера с постоянным ЦО JA3S, после чего начнётся обмен шифрованными пакетами.

Пакеты TLS-рукопожатия отправляются сторонами исключительно с целью ввести в заблуждение пассивного наблюдателя и убедить его в том, что сессия является обычной сессией TLS. Выявление возможно по заранее известным последовательностям обмена информацией.

Несмотря на то, что ЦО TLS-сессии туннеля может быть задан произвольно, все они не являются сессиями TLS, а только выглядят так для пассивного

17 Ресурс разработки nekoray URL: https://github.com/MatsuriDayo/nekoray (дата обращения: 10.02.2024).

18 База данных ЦО Cisco Mercury URL: https://github.com/cisco/mercury/blob/main/resources/fingerprint-db-tls-os.json.gz (дата обращения: 10.02.2024)..

Таблица 1.

Известные ЦО различных версий OpenConnect

JA3 полное представление	JA4
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49187-49200-52392-49172-49199-49171-49191-157-49309-53-61-156-49308-47-60-159-52394-49311-57-107-158-49310-51-103,5-10-11-13-35-51-43-65281-0-45-28-21,23-24-25-29-256-257-258-259-260,0	t13d351200_bfa337485184_b4c318310b83
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49187-49200-52392-49172-49199-49171-49191-157-49309-53-61-156-49308-47-60-159-52394-49311-57-107-158-49310-51-103,5-10-11-13-35-51-43-65281-0-45-28-21,23-24-25-29-30-256-257-258-259-260,0	**t13d351200_bfa337485184_5671b5df5029**
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49187-49200-52392-49172-49199-49171-49191-157-49309-53-61-156-49308-47-60-159-52394-49311-57-107-158-49310-51-103,5-10-11-13-35-51-43-65281-45-28-21,23-24-25-29-256-257-258-259-260,0	t13i351100_bfa337485184_b4c318310b83
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49187-49200-52392-49172-49199-49171-49191-157-49309-53-61-156-49308-47-60-159-52394-49311-57-107-158-49310-51-103,5-10-11-13-35-51-43-65281-45-28-21,23-24-25-29-30-256-257-258-259-260,0	t13i351100_bfa337485184_5671b5df5029
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49200-52392-49172-49199-49171-157-49309-53-156-49308-47-159-52394-49311-57-158-49310--51,5-10-11-13-35-51-43-65281-45-28-21,23-24-25-29-256-257-258-259-260,0	t13i291100_723694b0fccc_b4c318310b83
771,4866-4867-4865-4868-49196-52393-49325-49162-49195-49324-49161-49200-52392-49172-49199-49171-157-49309-53-156-49308-47-159-52394-49311-57-158-49310--51,5-10-11-13-35-51-43-65281-45-28-21,23-24-25-29-256-257-258-259-260,0	t13i291100_723694b0fccc_b4c318310b83
771,49195-49196-49286-49287-49161-49187-49162-49188-49266-49267-49324-49325-49160-49199-49200-49290-49291-49171-49191-49172-49192-49270-49271-49170-156-157-49274-49275-47-60-53-61-65-186-132-192-49308-49309-10-158-159-49276-49277-51-103-57-107-69-190-136-196-49310-49311-22,5-65281-35-10-11-13,23-24-25-21-19,0	t12i540600_a499d9840d02_10551b21ac36
771,49196-49287-52393-49325-49162-49188-49267-49195-49286-49324-49161-49187-49266-49160-49200-49291-52392-49172-49192-49271-49199-49290-49171-49191-49270-49170-157-49275-49309-53-61-132-192-156-49274-49308-47-60-65-186-10-159-49277-52394-49311-57-107-136-196-158-49276-49310-51-103-69-190-22,5-65281-35-10-11-13,23-24-25,0	t12i570600_45f33a1adcc2_10551b21ac36

наблюдателя. Протокол TLS разделяет данные, отправляемые сторонами, на субпакеты; для каждого субпакета указываются его тип и длина, которые доступны пассивному наблюдателю. Соответственно, он может отслеживать процесс установления соединения и хронологию обмена данными сторонами, анализируя типы субпакетов и их объёмы.

Субпакеты типа CLIENT_HELLO имеют ЦО, который может быть произвольно выбран из обширного списка. Каждый клиентский пакет TLS-рукопожатия всегда содержит поле идентификатор сессии (Session ID) с целью убедить пассивного наблюдателя, что сессия является возобновлением некой предыдущей сессии, чтобы сократить процедуру рукопожатия и легитимировать отсутствие в ответе сервера его сертификата.

Субпакеты туннеля SERVER_HELLO всегда имеют ЦО JA3S «15af977ce25de452b96affa2addb1036», который не меняются из сессии в сессию.

Субпакеты типа APPLICATION_DATA, содержат шифрованную информацию, которая не может быть дешифрована пассивным наблюдателем без наличия

сессионных ключей. Однако длина этих полей известна из заголовка, она определяется размером зашифрованного сообщения и алгоритмом шифрования, выбранным сервером.

Возможность выделять типы и размеры пакетов позволяет пассивному наблюдателю синтезировать сценарии взаимодействия и отслеживать объёмы передаваемых данных. Все сессии исследованных туннелей начинались одинаково по сценарию (Листинг 1).

Листинг 1.

Начало сессий туннелей, организованных XRay

```
CLIENT              SERVER
C:CLIENT_HELLO,
                    S:SERVER_HELLO,
                    S:CHANGE_CIPHER_SPEC,
                    S:APPLICATION_DATA(52),
                    S:APPLICATION_DATA(5562),
                    S:APPLICATION_DATA(281),
                    S:APPLICATION_DATA(69),
C:CHANGE_CIPHER_SPEC,
C:APPLICATION_DATA(69),
…
```

где: C – пакет от клиента, S – пакет от сервера, в скобках – постоянные размеры пакетов.

При туннелировании VoIP-сессии равномерно передаваемые RTP-пакеты кодека G.711, имеющие полную длину 200 байт, порождают в сессии туннеля пакеты APPLICATION_DATA длиной 205 байт, с периодичностью ≈ 0,02 сек. Например, симплексная сессия туннеля XRay (рис. 1), замаскированная под сессию TLS в момент VoIP звонка, использующего RTP-кодек G.711 PCMU [14].

Подобная закономерность позволяет выявлять VoIP-сессии в туннеле с помощью искусственных нейронных сетей [15–17] или без них, как это предложено в работе [18].

Метод обнаружения фактов обхода блокировок ресурсов сети Интернет

Обобщённый метод обнаружения фактов обхода блокировок ресурсов сети Интернет способом скрытого туннелирования трафика, использованный в работе, предполагает последовательный анализ доступных для пассивного наблюдателя устойчивых информативных признаков, причём сложность последующих этапов возрастает.

В первую очередь выполняется вычислительно простая:

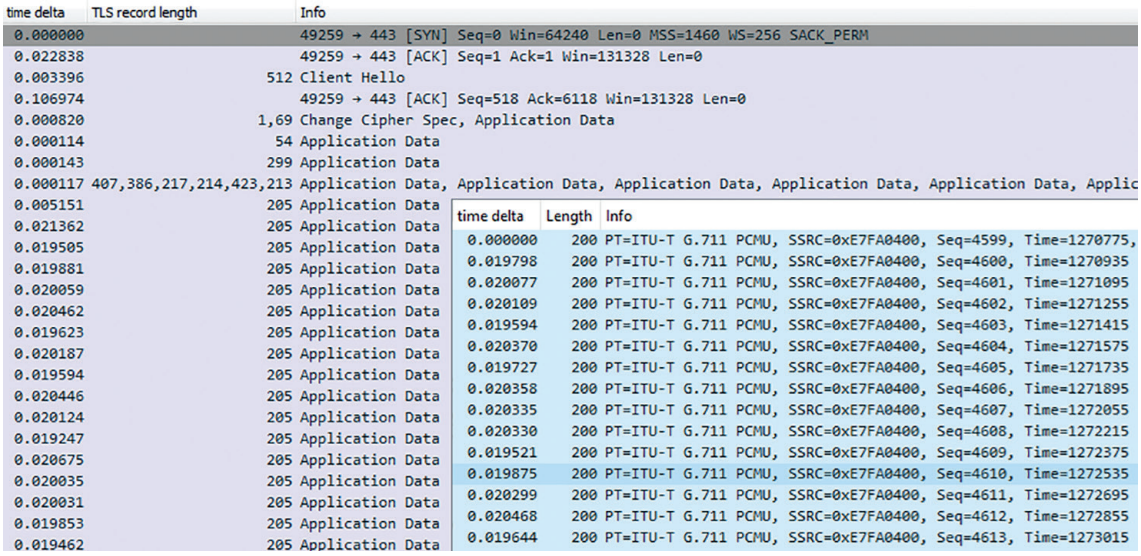
- проверка ЦО TLS на строгое соответствие ЦО реализации OpenConnect,
- в случае получения неизвестного ЦО выполняется его проверка на удалённость от ЦО OpenConnect по методу [11].

Для выявления сессий, использующих стеганографию:

- беспрепятственно пропускаются все первичные сессии, использующие полную процедуру рукопожатия, которая не применяется инструментами обхода блокировок ресурсов;
- проверяются ЦО ответа сервера JA3S;
- при отсутствии признаков нарушений на предыдущих этапах – проверяется соответствие сценария обмена данными после рукопожатия.

Среди оставшихся сессий следует выбрать количественно доминирующие сессии с конечными точками за границей ТСПУ.

Только для оставшихся и соответствующих всем критериям сессий проводить анализ распределения длин и периодов следования пакетов.



time delta	TLS record length	Info
0.000000		49259 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.022838		49259 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.003396	512	Client Hello
0.106974		49259 → 443 [ACK] Seq=518 Ack=6118 Win=131328 Len=0
0.000820	1,69	Change Cipher Spec, Application Data
0.000114	54	Application Data
0.000143	299	Application Data
0.000117	407,386,217,214,423,213	Application Data, Application Data, Application Data, Application Data, Application Data, Applic
0.005151	205	Application Data
0.021362	205	Application Data
0.019505	205	Application Data
0.019881	205	Application Data
0.020059	205	Application Data
0.020462	205	Application Data
0.019623	205	Application Data
0.020187	205	Application Data
0.019594	205	Application Data
0.020446	205	Application Data
0.020124	205	Application Data
0.019247	205	Application Data
0.020675	205	Application Data
0.020035	205	Application Data
0.020031	205	Application Data
0.019853	205	Application Data
0.019462	205	Application Data

time delta	Length	Info
0.000000	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4599, Time=1270775,
0.019798	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4600, Time=1270935
0.020077	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4601, Time=1271095
0.020109	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4602, Time=1271255
0.019594	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4603, Time=1271415
0.020370	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4604, Time=1271575
0.019727	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4605, Time=1271735
0.020358	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4606, Time=1271895
0.020335	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4607, Time=1272055
0.020330	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4608, Time=1272215
0.019521	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4609, Time=1272375
0.019875	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4610, Time=1272535
0.020299	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4611, Time=1272695
0.020468	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4612, Time=1272855
0.019644	200	PT=ITU-T G.711 PCMU, SSRC=0xE7FA0400, Seq=4613, Time=1273015

Рис. 1. Сессия туннеля XRay, замаскированная под сессию TLS (слева), нешифрованные пакеты RTP-сессии (справа)

По результатам экспериментальной проверки предлагаемого обобщённого метода получены следующие характеристики качества обнаружения скрытого туннелирования трафика:

- Все сессии, организованные средством OCserv, однозначно идентифицированы по ЦО TLS. Можно утверждать, что данный ЦО всегда будет соответствовать только сессиям туннелей и никогда – сессиями Web-браузера.
- Все 1975 исследованных сессий имели несовпадающие для разных сессий значения Session ID, строгое совпадение объемнохронологического сценария обмена субпакетами в начале каждой сессии.
- Для сессии XRay содержащей VoIP G.711 результат работы искусственной нейронной сети, спроектированной для исследования трафика OpenVPN:

FTP: 6.44%	(0.06437485)
RTP G.711: 76.7%	(0.7669719)
RTP G.723.1: 0.14%	(0.0014005811)
RTP G.729: 1.53%	(0.015301358)
HTTP: 0.02%	(0.00019485639)
RDP: 14.01%	(0.14014894)
SMB: 1.16%	(0.011607527)

Выводы

Поиск способов выявления сессий, являющихся скрытыми туннелями, а также новых способов их сокрытия идут параллельно. Обнаружение информативных признаков, однозначно идентифицирующих такие туннели, приводит к попыткам их сокрытия в новых версиях ПО. Вместе с тем, искусственное маскирование туннелированных сессий, в том числе для сокрытия от пассивного наблюдателя вновь обнаруживаемых информативных признаков (устойчивых закономерностей), приводят к снижению эффективности коммуникации.

В результате исследования выдвинута и экспериментально подтверждена гипотеза о сохранении доступности пассивному наблюдателю устойчивых информативных признаков стандартного функционирования средств, используемые для обхода блокировок трафика.

В частности, показаны примеры успешного детектирования туннелей при передаче по ним не типичных видов трафика (например VoIP). В данном случае использованы сохраняющиеся закономерности распределения длин пакетов с поправкой на объём служебной информации.

В качестве примера детектирования стеганографически организованного туннеля проведён анализ сессий, организованных с помощью инструмента XRay. В результате обнаружена устойчивая хронологическая последовательность сообщений, что позволяет безошибочно определять такие сессии.

С точки зрения оптимизации вычислительных затрат на анализ трафика предложена последовательность шагов обобщённого метода обнаружения фактов обхода блокировок ресурсов сети Интернет: последовательно усложняющиеся процедуры проверки обеспечивают потапный контроль правил и снижение числа сессий, требующих обработки с использованием систем искусственного интеллекта. Ей должны подвергаться только сессии, имеющие все косвенные признаки: присутствие Session ID, совпадение известный ЦО ответа сервера JA3S, совпадение последовательности обмена при установлении соединения.

Литература

1. *Чеповский А. А. Об особенностях построения и анализа графов взаимодействующих объектов в сети telegram-каналов // Вопросы кибербезопасности. – 2022. – №. 1 (53), с. 75–81. DOI:10.21681/2311-3456-2022-2-75-81*
2. *Капицын С. Ю., Рюмшин К. Ю., Варенница В. В. Логико-лингвистический механизм формирования «бумажных» пуль при информационном противоборстве // Вопросы кибербезопасности. – 2022. №. 1 (53), с. 93–99. DOI:10.21681/2311-3456-2022-1-93-99*
3. *Новикова Е. С. и др. Обнаружение вторжений на основе федеративного обучения: архитектура системы и эксперименты // Вопросы кибербезопасности. – 2023. – № 6 (58), с. 50–66. DOI:10.21681/2311-3456-2023-6-50-66*
4. *Коноваленко С. А. Методика оценивания информационной устойчивости гетерогенной системы обнаружения компьютерных атак // Вопросы кибербезопасности. – 2023. – №. 6 (58), с. 67–80. DOI:10.21681/2311-3456-2023-6-67-80*
5. *Шадрина А. Д. Способы защиты информации в веб-приложении // Программно-техническое обеспечение автоматизированных систем. – 2021. – с. 116–119.*
6. *Гурина Л. А., Айзенберг Н. И. Поиск эффективного решения по обеспечению защиты от киберугроз сообщества микросетей со взаимосвязанными информационными системами // Вопросы кибербезопасности. – 2023. – №. 3 (55). – с. 37–49. DOI:10.21681/2311-3456-2023-3-37-49*
7. *Павленко Е. Ю. и др. Распознавание киберугроз на адаптивную сетевую топологию крупномасштабных систем на основе рекуррентной нейронной сети // Вопросы кибербезопасности. – 2022. – №. 6 (52), с. 93–99. z DOI:10.21681/2311-3456-2022-6-93-99*
8. *Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. – 2021. – №. 4 (44). – С. 61–72. DOI:10.21681/2311-3456-2021-4-61-72*
9. *Карцхия А. А. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности. – 2020. – №. 6 (40). – С. 72–82. DOI:10.21681/2311-3456-2020-6-72-82*
10. *VAS Experts. СКАТ – Система контроля и анализа трафика. VAS Experts. URL: https://vasexperts.ru/wp-content/uploads/2022/07/filtracziya-po-spiskam-rkn-i-minyusta.pdf (дата обращения: 10.02.2024)*

11. *Ишкуватов С. М., Швед В. Г., Филькова И. А. Метод оценки близости цифровых отпечатков реализаций протоколов // Защита информации. Инсайд. – №. 2. – с. 29–33.*
12. *Ишкуватов С. М., Комаров И. И. Анализ аутентичности трафика на основании данных цифровых отпечатков реализаций сетевых протоколов // Научно-технический вестник информационных технологий, механики и оптики. – 2020. – Т. 20. – №. 5. – С. 747–754.*
13. *Ишкуватов С. М., Бегаев А. Н., Комаров И. И. Метод автоматической классификации цифровых отпечатков TLS-протокола // Вопросы кибербезопасности. – 2024. – №. 1 (59), с. 67–74. DOI:10.21681/2311-3456-2024-1-67-74*
14. *Henning Schulzrinne, Stephen Casner, Ron Frederick, Van Jacobson. RTP: A transport protocol for real-time applications. RFC 3550. 2003 г.*
15. *Ali Rasteh, Florian Delpech, Carlos Aguilar-Melchor et al. Encrypted internet traffic classification using a supervised spiking neural network. Neurocomputing. 2022 г., Т. 503., 8.*
16. *Gupta Neha, Jindal Vinita, Bedi Punam. Encrypted traffic classification using extreme gradient boosting algorithm. International Conference on Innovative Computing and Communications. 2022 г., Т. Volume 3 / Springer., 9.*
17. *Islam Faiz Ul, Liu Guangjie, Liu Weiwei. Identifying VoIP traffic in VPN tunnel via flow spatio-temporal features. Mathematical Biosciences and Engineering. 2020 г., Т. 15, 5.*
18. *Ишкуватов, С. М. Способ и алгоритм определения типа трафика в шифрованном канале связи // Труды учебных заведений связи. 2022 г., Т. 8, 4.*