МЕТОД ОБНАРУЖЕНИЯ И ИДЕНТИФИКАЦИИ ДАННЫХ СЕТИ TOR АНАЛИЗАТОРОМ WIRESHARK

Лапшичёв В.В.[1], Макаревич О.Б.[2]

Цель работы: *разработка метода, позволяющего обнаруживать и идентифицировать пакеты сети Tor, в том числе, обфусцированных пакетов на локальной машине пользователя сети, снифферoм Wireshark с использованием синтаксиса фильтров, основанных на признаках пакетов сети Tor, характерных для версии шифрования TLS v1.2 и v1.3; изучение возможности использования атаки SSL Bump (расшифровка https-трафика на виртуальном сервере при помощи самоподписываемых сертификатов x.509) для преодоления обфускации пакетов сети Tor.*

Метод: *применялся программный анализ передаваемых сетевых пакетов, декомпозиция содержимого пакетов данных по признакам их размеров и принадлежности к протоколам шифрования, сравнительный метод в отношении различных версий протокола шифрования и ресурсов, синтез правил фильтрации на основе синтаксиса анализатора.*

Полученные результаты: *разработан прикладной метод, позволяющий обнаруживать и идентифицировать пакеты сети Tor, в том числе, обфусцированных пакетов на локальной машине пользователя сети, снифферoм Wireshark на основе синтаксиса фильтрации, опирающегося на признаки пакетов шифрования версии TLS v1.2 и v1.3; получены данные о невозможности использовать атаку SSL Bump для преодоления обфускации сети Tor.*

Ключевые слова: *сниффер, рукопожатие TLS, законное блокирование доступа, кибербезопасность, деанонимизация.*

DOI:10.21681/2311-3456-2021-4-73-80

1. Введение

Законное блокирование анонимной сети Tor в настоящее время является актуальной задачей информационной безопасности, в части, касающейся предотвращения противоправной деятельности пользователей данной сети путем ограничения доступа к ней. Федеральным законом от 29.07.2017 N 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» «установлен запрет на обеспечение использования в РФ информационно-телекоммуникационных сетей, информационных систем и компьютерных программ для получения доступа к запрещенным информационным ресурсам»[3]. К последним относится программный комплекс Tor, скрывающий личность и данные пользователя сети Интернет. Однако, наряду с законодательно установленной нормой, позволяющей применять санкции в отношении использования анонимайзеров (сетей, систем и программ, обеспечивающих анонимность пользователя), существует ряд вопросов, требующих решения для реализации законного блокирования.

Наряду с необходимостью идентификации пользователей программного обеспечения, позволяющего скрывать свою личность в сетях передачи данных, существует также проблема обнаружения трафика сети Tor в сетях передачи данных и возможность его идентификации.

Последнее обусловлено различными способами обеспечения анонимности пакетов, среди которых: использование с 2018 года обновленного протокола шифрования TLS версии 1.3, позволяющего шифровать не только передаваемые данные, но и сам процесс установления соединения в части, касающейся рукопожатия между клиентским и серверным программным обеспечением; использование обфускации (маскирования) пакетов между оконечным оборудованием на локальной машине и на сервере сети.

Проблематика разработки идентифицирующих признаков сети Tor в условиях обфускации обусловлена пересборкой пакетов (а значит и изменение состава и размера таких пакетов) и сокрытие их содержимого, маскируемого под обычное соединение с TLS-шифрованием.

В проведенных ранее исследованиях, направленных на выявление уникальных признаков пакетов анонимной сети Tor, были получены данные, позволяющие однозначно идентифицировать сертификат рукопожатия соединения, устанавливаемого с применением шифрования TLS версии 1.2. С началом применения в 2018 году разработчиками комплекса Tor новой версии шифрования TLS 1.3 потребовался пересмотр идентифицирующих признаков. Было установлено, что

1 Лапшичёв Виталий Витальевич, аспирант, младший научный сотрудник кафедры безопасности информационных технологий Института компьютерных технологий Южного Федерального университета, г. Таганрог, Россия. E-mail: lapshichyov@sfedu.ru

2 Макаревич Олег Борисович, доктор технических наук, профессор, профессор кафедры безопасности информационных технологий Института компьютерных технологий Южного Федерального университета, г. Таганрог, Россия. E-mail: obmakarevich@sfedu.ru

3 Сайт «Консультант Плюс». URL: http://www.consultant.ru/law/hotdocs/50476.html

в отличие от версии TLS 1.2 не шифруется только запрос пользователя сети на установление соединения client_hello [1].

Международное научное сообщество работает над вопросами, связанными с характеристиками сети Tor, обнаружением трафика данной сети, применяя для этого различные методы и средства, в том числе с использованием нейросетей [2, 3]. Большинство статей такого характера опубликованы 5-10 лет назад [4], но есть и актуальные материалы [5-7].

В российском сегменте научных изданий исследованию, а также практической реализации, методов и подходов обнаружения и идентификации данных сети Tor, посвящено малое количество статей, и большинство их опубликованы также 5 и более лет назад. Основной круг вопросов, которые затрагивают в указанных статьях, базируется на обзорах технологии сети Tor, перечислении возможных для использования атак по деанонимизации пользователей и самой сети [8-13]. Однако прикладного решения задачи по обнаружению конкретно трафика сети Tor, его идентификации, не предложено, но частично затрагивается в общей теме идентификации анонимайзеров [14-15].

Несомненно, задача по идентификации скрывающих свою личность пользователей, совершающих противоправные действия, очень важна и первостепенна. Но на наш взгляд, именно блокирование доступа к сети, обеспечивающей анонимность пользователя, максимально отвечает задачам, решение которых обеспечивает соблюдение Федерального закона N 276-ФЗ.

Предложенный метод может быть использован как для обнаружения и идентификации пакетов сети Tor в локальной и беспроводной сети, в том числе офлайн из дампов .pcap, при помощи анализатора пакетов Wireshark, так и для использования принципа в настройке программных средств, отвечающих за обеспечение информационной безопасности (например, сетевых экранов), либо при создании отдельных программных средств, отвечающих за блокировку доступа к сети Tor.

2. Идентификация рукопожатия сети Tor TLS v1.2

В настоящее время протокол версии шифрования TLS v1.2 используется в установлении соединения сети Tor в отдельных случаях довольно редко. Однако, для законченности метода необходимо упомянуть обнаружение и идентификацию данной версии, которая перестанет быть актуальной только после официального отказа разработчиков сети Tor.

Для демонстрации метода на версии TLS 1.2 используются дампы начала 2018 года, когда еще не была принята версия TLS 1.3.

Среди выявленных признаков рукопожатия TLS версии 1.2 в отношении пакета server_hello указывались следующие: описание сертификата содержит маску «TLS Certificate: CN=www.{произвольный набор цифр и латинских букв}.net (или .com)»; номер порта 443, 9001 или 8443; размер сертификата от 448 до 593 байт [16, 17].

Исследования показали, что при настройке синтаксиса фильтров Wireshark, идентифицирующим параметром является именно размер сертификата в пакете server_hello.

Поэтому для фильтра были использованы параметры: фильтрация вывода строк протокола TLS, конъюнкция параметров фильтра вида &&, строка размера сертификата (меньше либо равно 600 байт, больше либо равно 400 байт), передаваемого при рукопожатии tls.handshake.certificate_length, строка сертификата, содержащая имя сервера, выпустившего данный сертификат x509sat.uTF8String (содержит значение com) (рис. 1):

```
tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400 && x509sat.uTF8String contains com
```

Практика показала, что метод работает и без части фильтра с параметром .com. При этом результат оказался эффективнее в части, касающейся количества обнаруженных адресов (рис. 2):

```
tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400
```

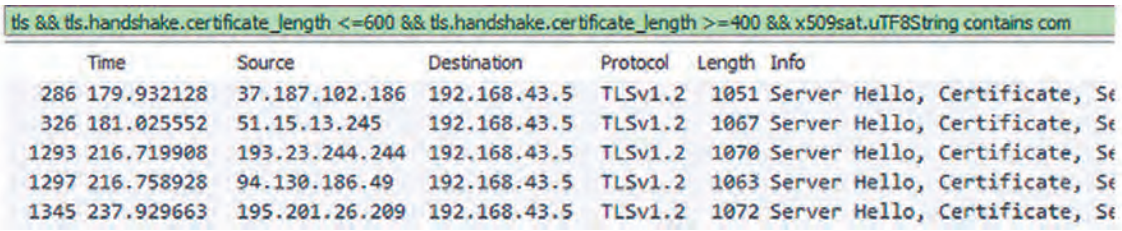

Рис.1. Результаты фильтрации рукопожатия TLS v1.2 (полный фильтр)

tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400

	Time	Source	Destination	Protocol	Length	Info
286	179.932128	37.187.102.186	192.168.43.5	TLSv1.2	1051	Server Hello, Certificate, Se
326	181.025552	51.15.13.245	192.168.43.5	TLSv1.2	1067	Server Hello, Certificate, Se
1293	216.719908	193.23.244.244	192.168.43.5	TLSv1.2	1070	Server Hello, Certificate, Se
1297	216.758928	94.130.186.49	192.168.43.5	TLSv1.2	1063	Server Hello, Certificate, Se
1345	237.929663	195.201.26.209	192.168.43.5	TLSv1.2	1072	Server Hello, Certificate, Se
1349	238.044791	128.31.0.34	192.168.43.5	TLSv1.2	1064	Server Hello, Certificate, Se

Рис.2. Результаты фильтрации рукопожатия TLS v1.2 (укороченный фильтр)

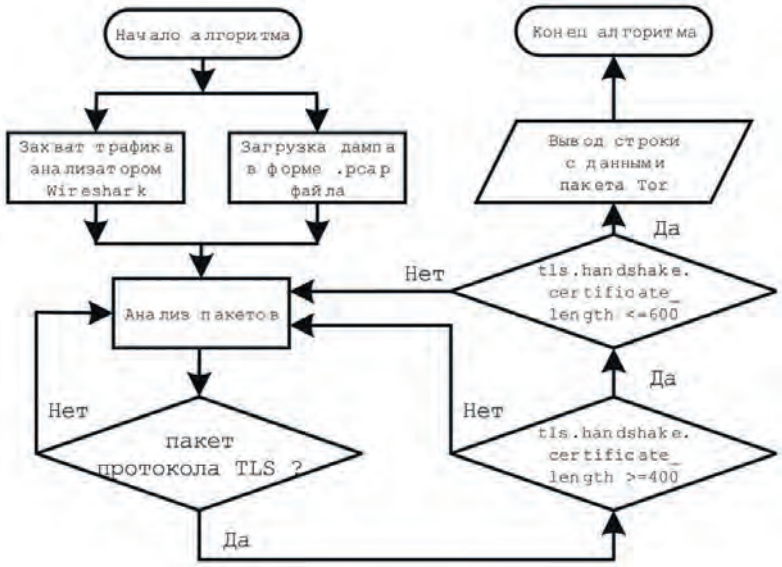

Рис.3. Алгоритм фильтрации рукопожатия TLS v1.2 (укороченный фильтр)

Алгоритм фильтрации протокола TLS v1.2 в обобщенном виде представлен ниже (рис. 3).

Таким образом, метод обнаружения и идентификации трафика сети Tor в части, касающейся протокола шифрования TLS версии v1.2, основывается на определении размера сертификата, передаваемого в пакете server_hello в процессе рукопожатия сервером в адрес пользователя, в пределах от 400 до 600 байт.

3. Идентификация рукопожатия сети Tor TLS v1.3

Широко используемый с 2018 года в обмене между серверами и пользователями сети Tor протокол шифрования TLS версии v1.3 создает трудности на пути его идентификации, так разработчики скрыли возможность анализа пакета рукопожатия server_hello, а значит и размер сертификата, который был идентифицирующим признаком для предыдущей версии протокола.

В ходе исследований был разработан набор признаков, которые включали в себя: размер пакета client_hello (369-385 байт); размер пакета server_hello (группа TLS фреймов - 1135-1148 байт, полный размер пакета – 1221-1234 байт); порядок следования фреймов пакета server_hello (server_hello-change_cipher_spec-application_data-application_data-application_data-application_data); «формула» величин фреймов пакета server_hello (155-1-23-n-281-69 байт) и их расположение в установленном порядке; величина 4-го фрейма (n, где 619 байт ≥ n ≥ 606 байт) [18].

В ходе практических исследований самым эффективным фильтром для целей метода стал размер пакета client_hello (диапазон размеров которого экспериментальным путем был установлен от 369 до 399 байт). Остальные либо неэффективны, либо сложны для использования в Wireshark.

Параметрами фильтрации пакетов были указаны: фильтрация вывода строк протокола TLS, конъюнкция параметров фильтра вида &&, строка размера пакета client_hello (меньше либо равно 399 байт, больше либо равно 369 байт), строка сертификата, содержащая имя сервера, выпустившего данный сертификат tls.handshake.extensions_server_name (содержит значение www. и .com) (рис. 4):

tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www

	Time	Source	Destination	Protocol	Length	Info
503	47.198972	192.168.0.11	51.15.151.31	TLSv1.3	388	Client Hello
504	47.199990	192.168.0.11	95.165.139.85	TLSv1.3	375	Client Hello
505	47.200327	192.168.0.11	37.147.200.2…	TLSv1.3	371	Client Hello
506	47.200455	192.168.0.11	185.220.101.…	TLSv1.3	378	Client Hello
507	47.200966	192.168.0.11	80.43.245.98	TLSv1.3	388	Client Hello
635	48.098055	192.168.0.11	37.147.200.2…	TLSv1.3	390	Client Hello

Рис.4. Результаты фильтрации рукопожатия TLS v1.3

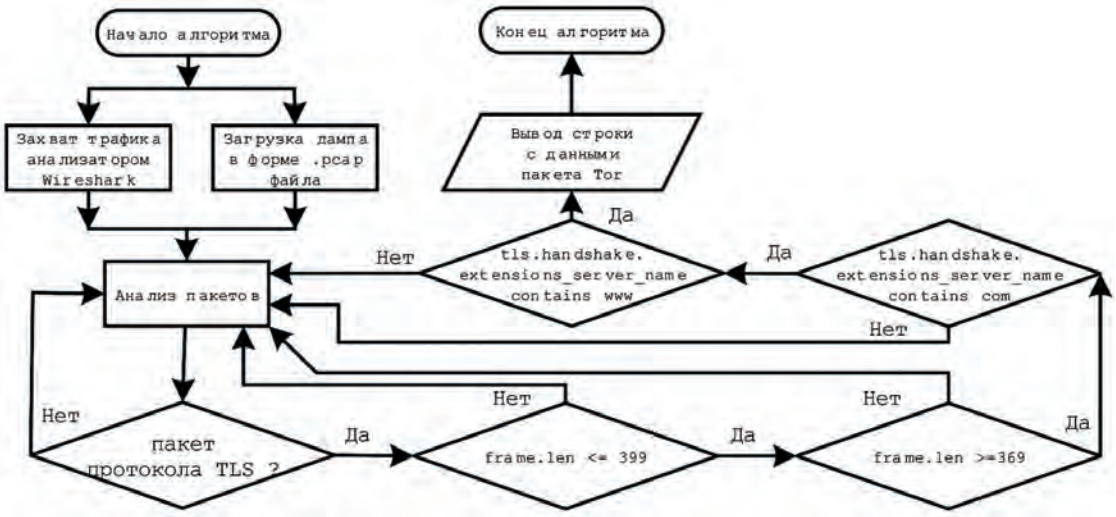

Рис.5. Алгоритм фильтрации рукопожатия TLS v1.3

```
tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www
```

Алгоритм фильтрации протокола TLS v1.3 в обобщенном виде представлен ниже (рис. 5).

Таким образом, метод обнаружения и идентификации трафика сети Tor в части, касающейся протокола шифрования TLS версии v1.3, основывается на определении размера пакета client_hello, передаваемого в процессе рукопожатия пользователем в адрес сервера, в пределах от 369 до 399 байт.

4. Идентификация в условиях обфускации

Идентификация трафика сети Tor на основе предложенного метода в условиях обфускации затруднена в связи с маскированием размера пакетов и отсутствием незашифрованных данных.

Ранее авторами высказывалось предположение об использовании атаки SSL Bump (расшифровка https-трафика на виртуальном сервере при помощи самоподписываемых сертификатов x.509) для создания условий, способствующих обнаружению и идентификации пакетов сети Tor. Однако, в ходе изучения механизмов данной атаки получены результаты, указывающие на невозможность применения данной атаки в интересах идентификации.

Использование дешифрования https-трафика в http при помощи атаки SSL Bump производится для его последующего анализа системами обнаружения вторжения (СОВ) (англ. Intrusion Detection System, IDS), предотвращения вторжения на узел (англ. Intrusion Protection System, IPS) либо для исследования системой глубокого анализа пакетов (англ. Deep Packet Inspection, DPI).

Согласно инструкциям по настройке сервиса программного виртуального сервера Squid[4] и PolarProxy[5] для https/http-преобразования применяются виртуализация и проброс портов, необходимые для осуществления расшифровки потока данных с использованием самоподписываемого сертификата X.509. Однако в отношении обфусцированного трафика это не имеет смысла, так как маскирующий слой образуется подключаемыми транспортами (англ. Pluggable Transport) поверх пакета, зашифрованного по протоколу TLS версий 1.2/1.3, и раскрыть его без указанного подключаемого интерфейса, программно включенного в состав комплекса Tor, не представляется возможным на данном этапе исследования вопроса.

4 Сайт компании АО «Лаборатория Касперского». URL: https://support.kaspersky.com/KWTS/6.1/ru-RU/181866.htm

5 Сайт компании NETRESEC. URL: https://www.netresec.com/?page=PolarProxy

Рис.6. Структурная схема трафика обфускация + шифрование TLS v1.3

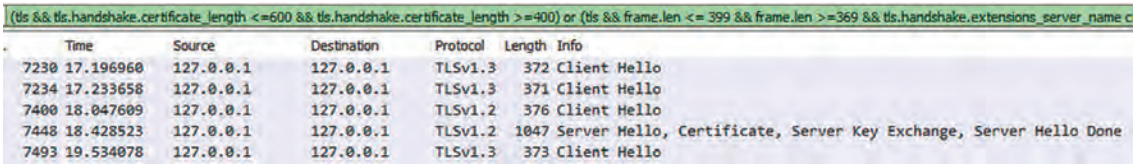

Рис.7. Обнаружение и идентификация пакетов client_hello и сертификата сети Tor

Тем не менее, в ходе использования сниффера Wireshark была отмечена особенность, связанная с применением данного анализатора пакетов на локальной машине пользователя анонимной сети Tor.

Так, при выборе loop-интерфейса захвата пакетов (локальный хост с IP-адресом 127.0.0.1) появилась возможность анализировать трафик сети Tor, идущий между подключаемым транспортом (обфускатором) и собственно браузером Firefox, включенным в состав программного комплекса Tor (рис 6).

При перехвате таких пакетов виден только входящий и исходящий на локальный хост (127.0.0.1) трафик, к тому же в зашифрованном по протоколу TLS виде. Но в таком виде данные поддаются анализу - обнаружению и идентификации пакетов client_hello и сертификатов Tor. При этом синтаксис фильтров для протокола шифрования дополнен дизъюнкцией вида or, делая фильтра универсальным для обеих версий протокола:

```
(tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400) or (tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www)
```

Для демонстрации указанного принципа через сервис предоставления мостов сети Tor были выбраны случайные IP-адреса и добавлены в окно настройки маршрутизации подключения программного комплекса: 59.167.185.220, 185.24.233.136, 37.247.48.90, 158.69.30.132, 185.220.101.239, 82.64.188.193. На скриншоте интерфейса программы эти адреса не видны, но соединение по ним перехвачено с использованием синтаксиса фильтров (рис.7).

Как видно на рисунке, был осуществлен запрос на соединение по 4 адресам, один из которых использует шифрование TLS v1.2, по 2 адресам запрос не направлен, по-видимому, в связи с их недоступностью. При этом видно, что фильтр перехватил не только размер пакета client_hello, но размер сертификата из пакета server_hello, которые являются частями одного рукопожатия. Все направленные запросы, а также установленное соединение с узлом сети Tor, обнаружены и идентифицированы.

В ходе исследований выявлена еще одна особенность, относящаяся к использованию обфускации: если пользователь включил данный режим (выбрал, например, мосты, предоставляемые сетью, а они по умолчанию идут с обфускацией), но зашел в настройки и переключается между режимами мостов (назначаемый сетью по умолчанию; получаемый через встроенный сервис; добавляемый пользователем) браузер делает запрос к входному узлу сети Tor, выделяемому по умолчанию, и такое соединение запрашивается без применения обфускации, а значит подвержено обнаружению и идентификации.

Следует также добавить, что в условиях инсталляции комплекса Tor при загрузке его с официального сайта программы и без вмешательства в конфигурацию настроек, подключение по умолчанию идет без обфускации.

Таким образом, принцип анализа пакетов на локальном хосте пользовательского устройства с применением описанного выше метода обнаружения и идентификации трафика сети Tor может быть использован для дальнейшей разработки метода блокирования соединения с сетью Tor в условиях обфускации данных.

DOI:10.21681/2311-3456-2021-4-73-80

5. Выводы

Разработан прикладной метод, позволяющий обнаруживать и идентифицировать пакеты сети Tor, снифферoм Wireshark на основе синтаксиса фильтрации, опирающегося на признаки пакетов шифрования версии TLS v1.2 и v1.3. Предложен принцип идентификации обфусцированных пакетов сети Tor на локальной машине пользователя, который можно использовать для дальнейшей разработки методов блокировки маскированного трафика. Получены данные о невозможности использовать атаку SSL Bump для преодоления обфускации сети Tor.

По итогам выполнения задач исследования в части, касающейся разработки метода обнаружения и идентификации пакетов сети Tor, выявлено, что основными пунктами алгоритма реализации метода на основе анализатора Wireshark являются:

— для протокола шифрования TLS версии v1.2 – применение значения фильтрации для определения размера сертификата, передаваемого в пакете server_hello в процессе рукопожатия сервером в адрес пользователя, в пределах от 400 до 600 байт: `tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400;`

— для протокола шифрования TLS версии v1.3 - применение значения фильтрации для определения размера пакета client_hello, передаваемого в процессе рукопожатия пользователем в адрес сервера, в пределах от 369 до 399 байт: `tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www ;`

— для обеих версий протокола – применение универсального значения фильтрации: `(tls && tls.handshake.certificate_length <=600 && tls.handshake.certificate_length >=400) or (tls && frame.len <= 399 && frame.len >=369 && tls.handshake.extensions_server_name contains com && tls.handshake.extensions_server_name contains www) .`

Достоверность результатов подтверждена экспериментами с применением программы Wireshark, в ходе которых отмечается высокая эффективность предложенного решения для решения задачи по обнаружению и идентификации данных сети Tor.

Работа выполнена при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта №23/2020.

Литература

1. Лапшичёв В.В., Макаревич О.Б. Набор признаков установления https-соединения TLS v1.3 программным комплексом «Tor» // Известия ЮФУ. Технические науки. 2020. № 5, С. 150-158. DOI: 10.18522/2311-3103-2020-5-150-158.
2. Pitpimon Choorod, George Weir. 2021. Tor Traffic Classification Based on Encrypted Payload Characteristics. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), pp. 1-6. DOI: 10.1109/NCCC49330.2021.9428874.
3. Lalitha Chinmayee Hurali, Annapurna Patil. 2020. On the fly classification of traffic in Anonymous Communication Networks using a Machine Learning approach. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, DOI: 10.1109/ANTS50601.2020.9342804.
4. Tao Wang and Ian Goldberg. Improved website fingerprinting on Tor. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (WPES '13). Association for Computing Machinery, New York, NY, USA, 2013, pp. 201–212. DOI: 10.1145/2517840.2517851.
5. Martin Steinebach, Marcel Schäfer, Alexander Karakuz, Katharina Brandl, and York Yannikos. 2019. Detection and Analysis of Tor Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, art. 66, pp. 1–10. DOI: 10.1145/3339252.3341486.
6. Florian Platzer, Marcel Schäfer, and Martin Steinebach. 2020. Critical traffic analysis on the tor network. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, art. 77, pp.1–10. DOI: 10.1145/3407023.3409180.
7. Ding Jianwei, Chen Zhouguo. 2021. Watermark Based Tor Cross-Domain Tracking System for Tor Network Traceback. In: Wang D., Meng W., Han J. (eds) Security and Privacy in New Computing Environments. SPNCE 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Cham, vol 344, pp. 54-73. DOI: 10.1007/978-3-030-66922-5_4
8. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet» // Гуманитарные, социально-экономические и общественные науки. 2019. №5. С. 97-101. DOI: 10.23672/SAE.2019.5.31422.
9. Батоев В.Б. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет // Вестник ВИ МВД России. 2016. №2. С. 37-43.
10. Волкова О.В., Высоцкий В.Л., Дроздова Е.А. Актуальные вопросы противодействия наркопреступлениям, совершенным бесконтактным способом // Пробелы в российском законодательстве. 2018. №6. С. 176-178.
11. Усманов Р.А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. №4 (46). С. 135-141.

12. Авдошин С.М., Лазаренко А.В. Методы деанонимизации пользователей Tor // Информационные технологии. 2016. Т. 22. № 5. С. 362-372.
13. Avdoshin S.M., Lazarenko A.V. Deep web users deanonimization system // Труды ИСП РАН. 2016. Т. 28, № 3. С. 21-34. DOI: 10.15514/ISPRAS-2016-28(3)-2.
14. Щербинина И.А., Кытманов Н.С., Александров Р.В. Применение технологии DNS-Rebinding для определения реального IP-адреса анонимных веб-пользователей // Вопросы кибербезопасности. 2016. №1 (14). С. 31-35.
15. Басыня Е.А., Хиценко В.Е., Рудковский А.А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22, № 2. С. 45-51. DOI: 10.21293/1818-0442-2019-22-2-45-51.
16. Lapshichyov V.V., Makarevich O.B. TLS Certificate As A Sign Of Establishing A Connection With The Network Tor. The 12th International Conference on Security of Information and Networks (SIN 2019). Proceedings of the 12th International Conference on Security of Information and Networks, 2019, pp. 92-97. DOI: 10.1145/3357613.3357628.
17. Лапшичёв В.В. Макаревич О.Б. Метод обнаружения и идентификации использования программного комплекса «Tor» // Информатизация и связь. 2020. № 3. С. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
18. Лапшичёв В.В., Макаревич О.Б. Идентификация https-соединения сети «Tor» версии TLS v1.3 // «Вопросы кибербезопасности». 2020. № 6. С. 59-62. DOI: 10.21681/2311-3456-2020-06-57-62.

METHOD FOR DETECTING AND IDENTIFICATION OF TOR NETWORK DATA BY WIRESHARK ANALYZER

Lapshichyov V.V.[6], Makarevich O.B.[7]

Purpose of the study: *development of a method that allows detecting and identifying packets of the Tor network, including obfuscated packets on the local machine of the network user, by a Wireshark sniffer using the filter syntax based on the features of the Tor network packets characteristic of the TLS v1.2 and v1.3 encryption versions; studying the possibility of using the SSL Bump attack (decrypting https traffic on a virtual server using self-signed x.509 certificates) to overcome the obfuscation of Tor network packets.*

Method: *software analysis of transmitted network packets, decomposition of the contents of data packets according to their size and belonging to encryption protocols, a comparative method in relation to different versions of the encryption protocol and resources, synthesis of filtering rules based on the syntax of the analyzer was used.*

Results: *an applied method was developed that allows detecting and identifying packets of the Tor Network, including obfuscated packets on the local machine of the network user, by a Wireshark sniffer based on the filtering syntax based on the signs of encryption packets of the TLS v1.2 and v1.3 versions; data on the impossibility of using the SSL Bump attack to overcome the obfuscation of the Tor network was obtained.*

Keywords: *sniffer, TLS handshake, legal blocking of access, cybersecurity, deanonymization.*

References

1. Lapshichyov V.V. Makarevich O.B. Nabor priznakov ustanovleniya https-soedineniya TLS v1.3 programmny`m kompleksom «Tor» // Izvestiya YuFU. Texnicheskie nauki [Izvestiya SFedU. Engineering Sciences], 2020, No 5, pp. 150-158. DOI: 10.18522/2311-3103-2020-5-150-158.
2. Pitpimon Choorod, George Weir. 2021. Tor Traffic Classification Based on Encrypted Payload Characteristics. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), pp. 1-6. DOI: 10.1109/NCCC49330.2021.9428874.
3. Lalitha Chinmayee Hurali, Annapurna Patil. 2020. On the fly classification of traffic in Anonymous Communication Networks using a Machine Learning approach. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, DOI: 10.1109/ANTS50601.2020.9342804.
4. Tao Wang and Ian Goldberg. Improved website fingerprinting on Tor. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (WPES '13). Association for Computing Machinery, New York, NY, USA, 2013, pp. 201–212. DOI: 10.1145/2517840.2517851.

6 Vitaly Lapshichyov, postgraduate student, Junior Researcher of Department of Information Technology Security of Institute of Computing Technologies and Information Security, South Federal University, Taganrog, Russia. E-mail: lapshichyov@sfedu.ru

7 Oleg Makarevich, Dr. Sc., Professor of Department of Information Technology Security of Institute of Computing Technologies and Information Security, South Federal University, Taganrog, Russia. E-mail: obmakarevich@sfedu.ru

5. Martin Steinebach, Marcel Schäfer, Alexander Karakuz, Katharina Brandl, and York Yannikos. 2019. Detection and Analysis of Tor Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, art. 66, pp. 1–10. DOI: 10.1145/3339252.3341486.
6. Florian Platzer, Marcel Schäfer, and Martin Steinebach. 2020. Critical traffic analysis on the tor network. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, art. 77, pp.1–10. DOI: 10.1145/3407023.3409180.
7. Ding Jianwei, Chen Zhouguo. 2021. Watermark Based Tor Cross-Domain Tracking System for Tor Network Traceback. In: Wang D., Meng W., Han J. (eds) Security and Privacy in New Computing Environments. SPNCE 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Cham, vol 344, pp. 54-73. DOI: 10.1007/978-3-030-66922-5_4.
8. Bondarenko Y.A., Kizilov G.M. Problemy vyyavleniya i ispol'zovaniya sledov prestupleniy, ostavlyaemyh v seti «Darknet» // Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki [Humanitarian, socio-economic and social sciences], 2019, No 5, pp. 97-101. DOI: 10.23672/SAE.2019.5.31422.
9. Batoev V.B. Problemy protivodeystviya ekstremistskoy deyatel'nosti, osushchestvlyaemoy s ispol'zovaniem seti Internet // Vestnik VI MVD Rossii [Gerald of Voronezh Institute of Russian Ministry of Interior], 2016, No 2, pp. 37-43.
10. Volkova O.V., Vysotskiy V.L., Drozdova E.A. Aktual'nye voprosy protivodeystviya narkoprestupleniyam, sovershennym beskontaktnym sposobom // Probely v rossiyskom zakonodatel'stve [Gaps in Russian Legislation], 2018, No 6, pp. 176-178.
11. Usmanov R.A. Harakteristika prestupnoy deyatel'nosti, osushchestvlyaemoy v seti Internet posredstvom servisov-anonimayzerov // Yuridicheskaya nauka i pravoohranitel'naya praktika [Legal Science and Law Enforcement Practice], 2018, No 4 (46), pp. 135-141.
12. Avdoshin S.M., Lazarenko A.V. Metody deanonimizatsii pol'zovateley Tor // Informatsionnye tekhnologii [Information Technology], 2016, b. 22, No 5, pp. 362-372.
13. Avdoshin S.M., Lazarenko A.V. Deep web users deanonimization system // Trudy ISP RAN, [Proceedings of the Institute for System Programming of the Russian Academy of Sciences], 2016, vol. 28, No 3, pp. 21-34. DOI: 10.15514/ISPRAS-2016-28(3)-2.
14. Shcherbinina I.A., Kytmanov N.S., Aleksandrov R.V. Primenenie tekhnologii DNS-Rebinding dlya opredeleniya real'nogo IP-adresa anonimnyh veb-pol'zovateley // Voprosy kiberbezopasnosti [Cybersecurity Issues], 2016, No 1 (14), pp. 31-35.
15. Basynya E.A., Hitsenko V.E., Rudkovskiy A.A. Metod identifikatsii kiberprestupnikov, ispol'zuyushchih instrumenty setevogo analiza informatsionnyh sistem s primeneniem tekhnologiy anonimizatsii // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics], 2019, vol. 22, No 2, pp. 45-51. DOI: 10.21293/1818-0442-2019-22-2-45-51.
16. Lapshichyov V.V., Makarevich O.B. TLS Certificate As A Sign Of Establishing A Connection With The Network Tor. In proceedings of the 12th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 12-15, 2019). SIN'19. ACM New York, NY, USA, 2019, pp. 92-97. DOI: 10.1145/3357613.3357628.
17. Lapshichyov V.V. Makarevich O.B. Metod obnaruzheniya i identifikatsii ispol'zovaniya programmnogo kompleksa «Tor» // Informatizatsiya i svyaz' [Informatization and communication], 2020, No 3, pp. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
18. Lapshichyov V.V. Makarevich O.B. Identifikaciya https-soedineniya seti «Tor» versii TLS v1.3 // Voprosy` kiberbezopasnosti [Issues of Cybersecurity], 2020, No 6, pp. 59-62. DOI: 10.21681/2311-3456-2020-06-57-62.