УДК 004.056.5

А. В. Челнокова[1*]

Исследование методов обнаружения виртуальных защищенных каналов связи

[1] Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
* e-mail: chelalex1511@gmail.com

Аннотация. В статье представлено исследование методов распознавания виртуальных защищенных каналов связи, в том числе используемых для организации нелегитимного сетевого трафика. Выделены преимущества и недостатки существующих научных работ, в которых выносятся на обзор разработанные алгоритмы и методы обнаружения виртуальных защищенных каналов связи, включая виртуальные частные сети OpenVPN, семейства технологий V2Ray, средство туннелирования Stunnel и технологию луковой маршрутизации Tor. Проведена классификация на основе используемых инструментов и подходов, а также полученных результатов, представленных различными научными группами методов. Приведенное исследование предметной области может использоваться для проектирования и конфигурирования решений по безопасному и эффективному удаленному доступу к сетевым ресурсам, исключая вредоносные сетевые потоки в условиях их маскировки.

Ключевые слова: виртуальные защищенные каналы, виртуальные частные сети, машинное обучение, V2ray, OpenVPN

A. V. Chelnokova[1*]

Investigation of Detection Methods for Virtual Secure Communication Channels

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: chelalex1511@gmail.com

Abstract. The paper presents a study of methods for recognizing virtual secure communication channels, including those used to organize illegitimate network traffic. Advantages and disadvantages of the existing scientific works are highlighted, in which the developed algorithms and methods of detection of virtual secure communication channels, including virtual private networks OpenVPN, families of V2Ray technologies, tunneling tool Stunnel and onion routing technology Tor are reviewed. A classification based on the tools and approaches used, as well as the results obtained, of the methods presented by different research groups is carried out. The given study of the subject area can be used to design and configure solutions for secure and efficient remote access to network resources, excluding malicious network flows under conditions of their masking.

Keywords: virtual private communication channels, virtual private network, machine learning, V2ray, OpenVPN

Введение

В современную эпоху, когда конфиденциальность данных становится все более важной, наблюдается стремительный рост использования технологии виртуальных защищенных каналов связи (ВЗКС). Это связано с необходимостью защиты конфиденциальной информации и обеспечения безопасного доступа к дан-

ным (в том числе и удаленного). Однако зачастую ВЗКС используются злоумышленниками при вредоносных действиях с целью обеспечения анонимности и сокрытия своего реального местоположения. Так, в отчете IBM утверждается, что на 2021 год совокупные потери, возникшие вследствие различных утечек данных, составили более 4 млн. долларов США, в то время как 60% опрошенных сотрудников используют VPN для доступа к корпоративным сервисам [1]. Решение данной проблемы требует проведения различных исследований в области разработки методов обнаружения ВЗКС, включая оверлейные сети. Исследованием управления трафика в оверлейных сетях и методов идентификации злоумышленников, использующих средства анонимизации, занимается научная школа Басыни Е. А. [2–4].

Среди зарубежных ученых можно отметить такую группу, как Hua Wu, Yujie Liu, Guang Cheng, Xiaoyan Hu, чьи научные исследования сосредоточены на методах обнаружения VPN на основе глубокого обучения нейронных сетей [5, 6]. Авторы исследований демонстрируют результаты успешного обнаружения различных технологий, включая V2Ray VMess. В свою очередь отечественные ученые, такие как К. Н. Канатьев, С. Р. Шишкин, М. Д. Нурмагомедов и др., занимаются проблематикой обнаружения ВЗКС в условиях их обфускации (например, OpenVPN) [7, 8].

Развитие технологий ВЗКС оказало влияние на законодательный аспект данной области. К примеру, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) 8 ноября 2023 года выпустила Приказ № 168 [9]. Данный приказ подразумевает разработку Единого реестра для внесения веб-ресурсов с информацией об обходе блокировок.

В связи с существующей проблематикой становится актуальным решение класса задач по разработке методов обнаружения виртуальных защищенных каналов связи.

Постановка задачи

Целью настоящей работы является исследование предметной области, которое включает в себя анализ существующих научных работ, посвященных разработке новых методов обнаружения виртуальных защищенных каналов связи.

Обзор

Изучение нелегитимных виртуальных защищенных каналов связи актуально для многих ученых. С развитием данной области разработаны определенные методы обнаружения, используемые в современных системах. Так, научная группа Канатьева К. Н. рассматривала существующие методы идентификации VPN-трафика, включая трафик с использованием обфускации [10, 11]. Исследователи выделили следующие подходы: статистический анализ, метод глубокого анализа пакетов, сигнатурный анализ, методы машинного обучения. Также исследованиями признаков обнаружения VPN занимался Зюзин В. Д. [12].

Одной из ведущих групп исследователей является коллектив Hua Wu, Yujie Liu, Guang Cheng, Xiaoyan Hu. Авторы исследований решали проблему анализа

трафика на наличие вредоносных VPN в рамках магистральных сетей [5, 6]. Предлагаемое решение представлено в виде метода идентификации виртуальных частных сетей на основе выборочных данных, полученных в высокоскоростных сетях в режиме реального времени. Исследователям удалось достичь точности идентификации ВЗКС, равной 97 %, включая такие новые инструменты, как V2Ray.

Представленный метод позволяет повысить точность распознавания вредоносных ВЗКС провайдерами без дополнительных мощностей, что позволяет улучшить безопасность магистральных сетевых потоков. Из недостатков данной работы следует отметить отсутствие исследования характеристик VPN в однонаправленном трафике (видео, трансляции, распределенные системы и т.д.).

Другая значимая группа: Yu Li, Fei Wang, Shuhui Chen – занимается идентификацией VPN-трафика на основе характеристик протоколов туннелирования [13]. В качестве объекта исследования авторы рассматривают различные приложения для мобильных устройств и ПК (например, ExpressVPN, SurfShark и т.д.). Ученые в ходе исследования смогли извлечь четыре категории признаков трафика, включая два новых энтропийных признака для идентификации VPN-трафика, что позволяет разработанному методу работать даже при смешанном трафике используемых приложений. Предложенный метод идентификации VPN-трафика достигает точности 99,02 % и 95,32 % соответственно на самостоятельно собранных и публичных наборах данных VPN.

Приведенное исследование демонстрирует возможность почти всегда детектировать нелегитимный трафик, поскольку для реализации DDoS-атак злоумышленники зачастую используют мобильные устройства пользователей с VPN-приложениями для их организации в ботнеты [14]. Однако данный метод не позволяет выявлять вредоносные сетевые потоки на основе технологий, распространенных в корпоративной среде, а именно: OpenVPN, WireGuard, IPSec и др.

Также стоит выделить группу Yan Zhou, Huiling Shi, Yuhan Zhao, Wei Gao и Wei Zhang, изучающую методы обнаружения зашифрованного трафика [15]. Авторы предлагают использовать свой метод на основе модели 2D-CNN, позволяющий распознавать обычный зашифрованный трафик и инкапсулированный трафик. Согласно исследованию, результаты экспериментов подтверждают, что средняя точность составляет 98,7 % при идентификации обычного зашифрованного трафика и 97,6 % при идентификации вредоносного трафика.

Метод, представленный научной группой, позволяет обнаруживать зашифрованный трафик с инкапсуляцией без необходимости расшифрования его вложенных данных, что повышает скорость обработки сетевого трафика. Из недостатков работы следует отметить отсутствие сравнительного анализа исследованных датасетов, доступных в открытых источниках. Также авторы не указали алгоритм генерации своей выборки данных для обучения и тестирования разработанного метода.

Существуют и отечественные научные коллективы, занимающиеся проблематикой нелегитимных ВЗКС. Так, группа В. В. Лапшичёв, О. Б. Макаревич за-

нимается исследованиями в области обнаружения трафика сети Tor [16–18]. Авторы исследований разработали метод обнаружения сетевых потоков в рамках данной анонимной сети, использующий протоколы TLSv1.2 и TLSv1.3. Данный метод построен с помощью инструментов фильтрации сниффера Wireshark, что позволяет пользователю на локальной машине без затруднений блокировать вредоносный сетевой трафик. К недостаткам данных исследований можно отнести отсутствие рассмотрения трафика на основе протокола SSL, используемого во многих текущих системах.

Таким образом, в исследуемой области можно выделить несколько ключевых подходов к анализу виртуальных защищенных каналов связи, а именно:

1) подход, основанный на машинном обучении;
2) подход, основанный на глубоком обучении;
3) подход, основанный на сигнатурном анализе;
4) подход, основанный на статистическом анализе;
5) подход, основанный на глубоком анализе пакетов;
6) иные смешанные подходы.

Заключение

В рамках статьи был проведен обзор научных работ в области обнаружения нелегитимных виртуальных защищенных каналов связи, а также анализ достоинств и недостатков приведенных исследований. В результате было выявлено множество подходов к обнаружению таких каналов, включая методы машинного обучения, сигнатурного анализа трафика и т. д. Были рассмотрены как классические, так и современные методы, используемые в этой области, с учетом их применимости к современным сетевым угрозам.

Значимость работы заключается в том, что результаты проведенного исследования могут использоваться в дальнейшем для проектирования и реализации собственных решений, позволяющих распознавать вредоносный сетевой трафик, в том числе в условиях маскировки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 50 Top-Choice VPNs Cybercriminals Use Unveiled! - 2023 // AtOnce URL: https://atonce.com/blog/which-vpns-do-hackers-use (дата обращения: 22.04.2024)

2. Басыня, Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // 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. – EDN GRIZDT.

3. Басыня, Е. А. Вопросы управления трафиком в оверлейных сетях / Е. А. Басыня // Автоматика и программная инженерия. – 2014. – № 3(9). – С. 29-32. – EDN VIXJDZ.

4. Басыня, Е. А. Алгоритмы управления трафиком в оверлейной сети I2P / Е. А. Басыня, И. В. Головченко // Фундаментальные и прикладные исследования в современном мире. – 2016. – № 14-1. – С. 97-102. – EDN WZKOML.

5. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks //ICC 2022-IEEE International Conference on Communications. – IEEE, 2022. – С. 5070-5075.

6. Wu H. et al. RT-CBCH: Real-time VPN Traffic Service Identification based on Sampled Data in High-speed Networks // IEEE Transactions on Network and Service Management. – 2023.

7. Обзор методов обнаружения VPN и DNS-анализ для классификации на примере Hotspot Shield Free / К. Н. Канатьев, С. Р. Шишкин, И. И. Басыров [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 215-219. – EDN RUAXWS.

8. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху / К. Н. Канатьев, М. Д. Нурмагомедов, А. А. Гребенщиков [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 211-214. – EDN XQRIZY.

9. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций "О внесении изменений в Критерии оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет", а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", в единую автоматизированную информационную систему "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 февраля 2023 г. N 25" от 08.11.2023 № 168 // Собрание законодательства Российской Федерации. 01.12.2023 г.

10. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху / К. Н. Канатьев, М. Д. Нурмагомедов, А. А. Гребенщиков [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 211-214. – EDN XQRIZY.

11. Обзор методов обнаружения VPN и DNS-анализ для классификации на примере Hotspot Shield Free / К. Н. Канатьев, С. Р. Шишкин, И. И. Басыров [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 215-219. – EDN RUAXWS.

12. Зюзин, В. Д. Детектирование VPN трафика / В. Д. Зюзин // Современные научные исследования: актуальные вопросы, достижения и инновации : Сборник статей XXVII Международной научно-практической конференции, Пенза, 20 сентября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 9-11. – EDN OGARCY.

13. Li Y., Wang F., Chen S. VPN Traffic Identification Based on Tunneling Protocol Characteristics //2022 IEEE 5th International Conference on Computer and Communication Engineering Technology (CCET). – IEEE, 2022. – С. 150-156.

14. Хакеры начали использовать VPN в DDoS-атаках на организации в РФ // Хабр URL: https://habr.com/ru/news/667242/ (дата обращения: 22.04.2024).

15. Zhou Y. et al. Encrypted network traffic identification based on 2d-cnn model //2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). – IEEE, 2021. – С. 238-241.

16. Лапшичев, В. В. Метод обнаружения и идентификации данных сети Tor анализатором Wireshark / В. В. Лапшичев, О. Б. Макаревич // Вопросы кибербезопасности. – 2021. – № 4(44). – С. 73-80. – DOI 10.21681/2311-3456-2021-4-73-80. – EDN HXIIVD.

17. Лапшичев, В. В. Набор признаков установления https-соединения TLS v1.3 программным комплексом "Tor" / В. В. Лапшичев, О. Б. Макаревич // Известия ЮФУ. Технические науки. – 2020. – № 5(215). – С. 150-158. – DOI 10.18522/2311-3103-2020-5-150-158. – EDN GUBOER.

18. Лапшичев, В. В. Идентификация https-соединения сети "Tor" версии tls v1.3 / В. В. Лапшичев, О. Б. Макаревич // Вопросы кибербезопасности. – 2020. – № 6(40). – С. 57-62. – DOI 10.21681/2311-3456-2020-06-57-62. – EDN RPSJZT.