УДК 343

Бондаренко Юрий Алексеевич
кандидат юридических наук,
доцент кафедры криминалистики и правовой информатики,
Кубанский государственный университет
bondarenko_yuri@mail.ru
Кизилов Герман Максимович
студент юридического факультета им. А.А. Хмырова,
Кубанский государственный университет
bondarenko_yuri@mail.ru
Yury A. Bondarenko
Candidate of Law Sciences,
associate professor of criminalistics and legal informatics,
Kuban State University
bondarenko_yuri@mail.ru
Herman M. Kizilov
student of law department of A.A. Hmyrov,
Kuban State University
bondarenko_yuri@mail.ru

Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet»

Problems of detection and use of crimes' traces, left in the Darknet

Аннотация: *авторами предпринята попытка комплексного рассмотрения проблем поиска и обнаружения следов преступлений и оставивших их лиц в компьютерных сетях с анонимными пользователями. Методами исследования закономерностей образования, выявления и изъятия следов киберпреступлений выступили контент-анализ трафика и алгоритмизация информационных потоков при распространении информации. Обозначены технические и системные начала функционирования анонимных компьютерных сетей, показаны технологии получения сведений о действиях лиц в сети Tor. Также рассмотрена современная практика использования информационных технологий для выявления и расследования киберпреступлений, совершаемых в пределах юрисдикции Российской Федерации.*

Ключевые слова: *Darknet, Tor, деанонимизация, криптовалюта, хеш-функция, маршрутизация, трафик, киберпреступление.*

Abstract: *the authors attempt to consider the problems of search and detection of traces of crimes and persons who left them in computer networks with anonymous users. Methods of investigation of the formation, the identification and separation of traces of the crime were made by the content-traffic analysis and algorithmic*

information flows for the distribution of information. Technical and system marked the beginning of the functioning of anonymous computer networks, the information about the actions of individuals in the Tor network. Modern practice of using information technologies for detection and investigation of cybercrime committed within the jurisdiction of the Russian Federation is also considered.

Keywords: *Darknet, Tor, deanonymization, cryptocurrency, hash function, routing, traffic, cybercrime.*

Стремительное развитие технических средств накопления, хранения, поиска, преобразования и передачи информации входит во все сферы нашей деятельности и проведения досуга. Развитие же цифровых информационных сетей предопределяет практически безграничные возможности для граждан и организаций по передаче и получению информации, что уже сейчас существенным образом отражается на экономике, управлении и праве. Глобальная информационно-коммуникационная сеть Интернет объединила пользователей по всему миру, стала непременным атрибутом развития производительных сил и отношений в обществе и государстве.

Такая же тенденция относится и к изменению подходов в выборе средств и способов совершения преступлений. Набрали силу киберпреступления, для которых используют уязвимости в технических и информационных средствах коммуникации между пользователями.

По верному замечанию А.В. Руденко, «расширяя границы человеческого восприятия, инструментальные методы позволяют снизить уровень субъективизма при изучении информации»[1]. Как нам кажется, интерес к техническим средствам и технологиям получения новых сведений о преступлениях и совершивших их лицах будет только возрастать, а информационные технологии и системы станут неотъемлемой частью такого вида познавательного процесса.

Однако информационные сети могут выступать не только как техническая среда, где совершаются преступления, но и в качестве инструмента и орудия для совершения преступлений и обеспечения преступной деятельности. Поэтому на сегодняшний день актуально рассматривать феномен существования Темного интернета (англ. «Darknet», «Dark Web») и закономерности механизма следообразования там при совершении преступлений. На основе познания таких закономерностей сначала судебный эксперт, а затем следователь устанавливают обстоятельства, подлежащие доказыванию по уголовному делу. Таким образом, орган расследования получает необходимые сведения о способе воздействия на программно-аппаратную среду при совершении преступления, обнаруживает следы по его сокрытию.

---

[1] Цит. по: Руденко А.В. Психофизиологическое исследование с применением полиграфа как метод криминалистического изучения личности / А.В. Руденко; О.А. Болотова // Юридический вестник Кубанского государственного университета. 2018, № 1. С. 32.

Прежде всего следует отметить, что конфигурация интернет-пространства условно представлена тремя различными по набору функций частями:

− Surface Web;
− Deep Web;
− Darknet.

Surface Web – это сеть, которая и называется Интернетом, информация в ней общедоступна, а файлы размещены в открытом доступе, куда вход осуществляется через стандартные интернет-браузеры («Google Chrome»; «Yandex browser» и другие).

Deep Web – сеть неиндексируемых информационных ресурсов, которые не отображаются через поисковые системы стандартных интернет-браузеров.

Darknet (она же Dark Web) – скрытая сеть интернет-соединений, она доступна через систему прокси-серверов, функционирующих по принципу анонимности пользователей и анонимности посещения информационных ресурсов.

В конфигурации Dark Web, помимо разнообразных научных сообществ, профессиональных форумов и других легальных объединений, также имеются информационные ресурсы, где осуществляется продажа наркотических, психотропных веществ и их аналогов, оружия, поддельных документов, конфиденциальных и секретных сведений.

Часто средством платежей в таких незаконных сделках выступают криптовалюты, данные о транзакциях с которыми распределенны по технологии «блокчейн» (англ. «blockchain» – «цепь блоков»). Технология «блокчейн» − это непрерывная последовательная цепочка блоков (связный список), содержащих информацию об участниках транзакции. Копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга и защищены криптографическим шифрованием – «хэшированием», что обеспечивает высокий уровень анонимности транзакций его участников.

В.В. Помазанов, подвергнув анализу роль криптовалют в экономической сфере, по этому поводу отмечает, что имеются положительные и отрицательные стороны криптовалют. К первым относятся прозрачность информации о транзакциях с ними, отсутствие посредников, отсутсивие налогообложения, высокая скорость обработки транзакций и общедоступность цифровых денег. Отрицательной стороной является привлекательность криптовалют для купли-продажи незаконных товаров и услуг в силу их общей анонимности[1].

Предметом рассмотрения выступает часть сети Интернет, − Darknet («Темная сеть»). Несмотря на то, что лишь незначительная часть пользователей этой сети связана с преступлениями, исследование Darknet, а в частности программы-браузера Tor, обусловлено его повышенной скрытностью и анонимностью использования, что затрудняет поиск следов преступлений и

[1] См.: Помазанов В.В. Криптовалюта: криминалистическое прогнозирование / В.В. Помазанов; С.И. Грицаев // Российский следователь, 2018. № 11. С. 20-21.

самих преступников. Следообразование в сети Darknet возможно проследить на основе получения информации о соединениях программы-браузера Tor. Однако добывание такого рода информации невозможно без использования комплекса средств контроля информационных потоков и аппаратной среды сети.

История Dark Web начинается одновременно с историей сети ARPANET, которая явилась прообразом Интернета. Сам термин «Darknet» появился в 1970-х годах и в целях безопасности использовался для обозначения сетей, изолированных от ARPANET.

Толчком к развитию и распространению Темного интернета, каким он представлен сегодня, является изобретение «луковой маршрутизации» и интернет-браузера Tor, работающего на ее принципе и позволяющего подключаться к сети Darknet. Такой вид маршрутизации потоков информации в сети был разработан Михаэлем Ридом, Паулем Сиверсоном и Дэвидом Голдшлагом. Имеется патент на изобретение Военно-морскими силами США в № 6266704, выданный в 1998 году. Первая версия браузера Tor («The Onion Routing Progect») разработана Роджером Динглдайном и Ником Матвевсоном и запущена 20 сентября 2002 года.[1]

Принято ошибочно считать, что пользователи браузера Tor во время его использования пребывают анонимными для средств авторизации сети Интернет. Но так как анонимность в сети формируется за счет луковой маршрутизации, большинство действий, направленных на деанонимизацию пользователей сети Tor, основываются именно на ее уязвимостях.

Перейдем теперь к вопросу о закономерностях работы луковой маршрутизации. Она устроена как хронологическая последовательность следующих операций:

На первом этапе шифруются сами пользовательские данные таким образом, чтобы их можно было расшифровать только на выходном узле.

Затем маршрутизатор вначале передачи информации выбирает случайное число промежуточных маршрутизаторов и генерирует CREATE-сообщения, шифруя их симметричным ключом и указывая для каждого маршрутизатора, какой маршрутизатор будет следующим на пути. В результате сообщение имеет несколько «слоев» с информацией, где помимо основного слоя с собственно пользовательской информацией, наложены другие слои информации, использующейся для передачи данных от одного пира (участника одноранговой сети) к другому.

Промежуточный маршрутизатор своим ключом дешифрует предназначенный только ему слой, который содержит информацию о другом маршрутизаторе (пире), куда необходимо направить информацию.

Этот алгоритм повторяется несколько десятков раз, пока исходное сообщение не дойдет до своего адресата.

Таким образом, каждому маршрутизатору известно только то, от какого пира поступили данные, и какому пиру их следует доставить. Само содержание

[1] Дык Б.М. Динь Принцип работы TOR-браузера // Проблемы науки. 2017, №1. С. 53.

передаваемых сведений маршрутизатор не может расшифровать в силу отсутствия у него необходимых для этого криптографических ключей.

Практика расследования преступлений в сфере использования компьютерной информации выработала несколько способов выявления и дальнейшего исследования следов преступлений этой группы. Все возможные действия по деанонимизации можно разделить на активные и пассивные[1].

Пассивные действия заключаются в отслеживании сообщений, но без изменения содержания данных передаваемых сообщений. При реализации активных действий по установлению пользователя сети происходит изменение содержания данных и отображения процессов в сети.

К пассивным действиям по деанонимизации пользователей относятся:

− анализ трафика пользователя, основанные на установлении временной взаимосвязи между запросом на создание соединения и установкой выходного соединения (являются очень ресурсозатратными);

другие основанные на анализе трафика и нагрузки узла внутри сети:

− Low-Cost Traffic Analysis of Tor[2] − низкозатратный анализ трафика в сети Tor с помощью специализированных программных средств);

− Low-Resource Routing Acts Against Tor[3] − маршрутизация информационных потоков и их отслеживание;

− Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting[4] − скрытый анализ трафика на основе собирания информации о пропускной способности оборудования;

− Timing – анализ закономерностей работы узлов сети Tor, посредством выявления временных шаблонов в сетевом потоке с последующей их корреляцией с другими, для реализации требуется свой сервер в сети;

− Circuit fingerprinting – после установления связи пользователя со скрытой службой (посредством наблюдения проходящего трафика) используется Website fingerprinting, который основан на классификации собранных о трафике данных.

Активные действия:

---

[1] См., напр.: Авдошин С.М. Методы деанонимизации пользователей TOR / С.М. Авдошин; А.В. Лазаренко // Информационные технологии. 2016, № 5. С. 362.

[2] Murdoch S. J. Low-Cost Traffic Analysis of Tor Мердош С. Дж. Малозатратный анализ трафика в сети «Тор» Адрес доступа в сети Интернет: http:// sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf (дата обращения: 02.04.2019 г.)

[3] Bauer K. Low-Resource Routing Attacks Against Tor Бауер К. Атаки низкоресурсной маршрутизации против сети «Тор». Адрес доступа в сети Интренет: https://homes.cs.washington.edu/~yoshi/papers/Tor/wpes25-bauer.pdf (дата обращения 03.04.2019 г.)

[4] Mittal P. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting Миттал П. Анализ скрытого трафика анонимного соединения с низкой задержкой с использованием следов ее пропускной способности Адрес доступа в сети Интернет: http://www.princeton.edu/~pmittal/publications/throughput-fingerprinting-ccs11.pdf (дата обращения: 29.03.2019 г.)

− Комбинированные Timing-действия[1] (например, с использованием iframe, который содержит код, встраивающийся в https-трафик и отправляющий сигнал отслеживающему серверу);
− Tagging действия[2] − дублирование случайного сообщения на входном узле, его поиск в поступивших на выходной узел данных;
− RAPTOR[3] − серия действий по ассиметричному анализу трафика, по сбору и обработке информации о перебоях, которые приводят в силу специфики топологии и протоколов работы анонимной сети данные на нужный узел, с последующим собиранием проходящего трафика.

Каждое из описанных действий направлено на идентификацию пользователя сети. Благодаря их проведению правоохранительные органы можно выйти на след злоумышленника в Darknet и Tor.

Отличный от предыдущих способ обнаружения следов преступлений описан Фроловым А.А. и Сильновым Д.С.[4] В опубликованном ими исследовании на примере сайта с материалами порнографического содержания несовершеннолетних, расположенного в Darknet, за счет использования специального программного обеспечения проводился сбор данных, содержащих ссылки на архивы с запрещенным контентом. Такая информация, в свою очередь, размещались на сервисах файлового обмена открытой сети Интернет. Полагаем, что данный опыт следует считать успешным, однако все еще остаются сложности в блокировке подобных ресурсов в силу специфической динамики информационных процессов.

Можно заключить, что существуют и развиваются способы выявления следов преступлений даже в достаточно скрытом Темном интернете, но проблема является более широкой и требует рассмотрение иных подобного рода сетей, способов сбора сведений и доказательств из них, а также развитие и применение уже существующих методов для выявления следов злоумышленников и запрещенного на территории Российской Федерации контента.

Дальнейшее развитие инструментов по собиранию следов преступной деятельности в сети Darknet происходит в сфере развития информационных

---

[1] Abbot T. Browser-Based Attacks on Tor Эббот Т. Атаки на сеть «Tor» через браузер Режим доступа в сети Интернет: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf (дата обращения: 03.04.2019 г.)

[2] Pries R. A New Replay Attack Against Anonymous Communication Networks Прис Р. Новая атака против анонимных компьютерных сетей Адрес доступа в сети Интернет: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4533341&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D453334 (дата обращения: 30.03.2019 г.)

[3] Edmundson A. RAPTOR: Routing Attack on Privacy in Tor Эдмондсон А. РАПТОР: направляемая атака на конфиденциальность в сети «Tor» Адрес доступа в сети Интернет: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf (дата обращения: 04.04.2019 г.)

[4] Фролов А.А. Исследование механизмов распространения запрещенного содержимого в Darknet / А.А. Фролов; Д.С. Сильнов // Современные информационные технологии и ИТ-образование. 2017, № 4. С. 216.

технологий и использования специальных знаний. А это, в свою очередь, ведет к необходимости разработки в криминалистике новых средств координации действий между следователем и специалистами в сфере компьютерных технологий по обнаружению, фиксации, изъятию и исследованию цифровых следов преступлений.

Литература:

1. *Цит. по: Руденко А.В. Психофизиологическое исследование с применением полиграфа как метод криминалистического изучения личности / А.В. Руденко; О.А. Болотова // Юридический вестник Кубанского государственного университета. 2018, № 1. С. 32.*
2. *См.: Помазанов В.В. Криптовалюта: криминалистическое прогнозирование / В.В. Помазанов; С.И. Грицаев // Российский следователь, 2018. № 11. С. 20-21.*
3. *Дык Б.М. Динь Принцип работы TOR-браузера // Проблемы науки. 2017, №1. С. 53.*
4. *См., напр.: Авдошин С.М. Методы деанонимизации пользователей TOR / С.М. Авдошин; А.В. Лазаренко // Информационные технологии. 2016, № 5. С. 362.*
5. *Murdoch S. J. Low-Cost Traffic Analysis of Tor Мердош С. Дж. Малозатратный анализ трафика в сети «Тор» Адрес доступа в сети Интернет: http:// sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf (дата обращения: 02.04.2019 г.)*
6. *Bauer K. Low-Resource Routing Attacks Against Tor Бауер К. Атаки низкоресурсной маршрутизации против сети «Тор». Адрес доступа в сети Интренет: https://homes.cs.washington.edu/~yoshi/papers/Tor/wpes25-bauer.pdf (дата обращения 03.04.2019 г.)*
7. *Mittal P. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting Миттал П. Анализ скрытого трафика анонимного соединения с низкой задержкой с использованием следов ее пропускной способности Адрес доступа в сети Интернет: http://www.princeton.edu/~pmittal/publications/throughput-fingerprinting-ccs11.pdf (дата обращения: 29.03.2019 г.)*
8. *Abbot T. Browser-Based Attacks on Tor Эббот Т. Атаки на сеть «Тор» через браузер Режим доступа в сети Интернет: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf (дата обращения: 03.04.2019 г.)*
9. *Pries R. A New Replay Attack Against Anonymous Communication Networks Прис Р. Новая атака против анонимных компьютерных сетей Адрес доступа в сети Интернет: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4533341&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D453334 (дата обращения: 30.03.2019 г.)*
10. *Edmundson A. RAPTOR: Routing Attack on Privacy in Tor Эдмондсон А. РАПТОР: направляемая атака на конфиденциальность в сети «Тор» Адрес доступа в сети Интернет: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf (дата обращения: 04.04.2019 г.)*
11. *Фролов А.А. Исследование механизмов распространения запрещенного содержимого в Darknet / А.А. Фролов; Д.С. Сильнов // Современные информационные технологии и ИТ-образование. 2017, № 4. С. 216.*

Literature:

1. *Tsit. on: Rudenko A.V. A psychophysiological research using a polygraph as a method of criminalistic studying of the personality / A.V. Rudenko; O.A. Bolotova//Legal bulletin of the Kuban State University. 2018, No. 1. Page 32.*
2. *See: Pomazanov V.V. Cryptocurrency: criminalistic forecasting / V.V. Pomazanov; S.I. Gritsayev//Russian investigator, 2018. No. 11. Page 20-21.*

3. So B.M. Din Pryingqip of operation of the TOR browser//science Problems. 2017, No. 1. Page 53.

4. See, e.g.: Avdoshin S.M. Methods of de-anonymization of users of TOR / S.M. Avdoshin; A.V. Lazarenko//Information technologies. 2016, No. 5. Page 362.

5. Murdoch S. J. Low-Cost Traffic Analysis of Tor Merdosh S. Dzh. The low-cost analysis of traffic in network of "Torahs" the Address of access to the Internet: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf (date of the address: 02.04.2019)

6. Bauer K. Low-Resource Routing Attacks Against Tor Bauer K. The attacks of low-resource routing against network of "Torahs". Address of access to Intrenet networks: https://homes.cs.washington.edu / ~ yoshi/papers/Tor/wpes25-bauer.pdf (date of the address of 03.04.2019)

7. Mittal P. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting Mittal P. Analysis of the hidden traffic of anonymous connection c by a low delay of c use of traces of its throughput Address of access to the Internet: http://www.princeton.edu / ~ pmittal/publications/throughput-fingerprinting-ccs11.pdf (date of the address: 29.03.2019)

8. Abbot T. Browser-Based Attacks on Tor Abbott T. Attacks to network of "Torahs" via the Access mode browser on the Internet: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf (date of the address: 03.04.2019)

9. Pries R. A New Replay Attack Against Anonymous Communication Networks of Pris R. The new attack against anonymous computer networks the Address of access to the Internet: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4533341&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=453334 (date of the address: 30.03.2019)

10. Edmundson A. RAPTOR: Routing Attack on Privacy in Tor Edmondson A. Raptor: the directed attack on confidentiality in network of "Torahs" the Address of access to the Internet: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf (date of the address: 04.04.2019)

11. Frolov A.A. A research of mechanisms of distribution of the prohibited contents to Darknet / A.A. Frolov; D.S. Silnov//Modern information technologies and IT education. 2017, No. 4. Page 216.