9. Klyuchko V. I., Shumkov E. A., Vlasenko A. V., Kernizan R. O. Arkhitektury sistem podderzhki prinyatiya resheniy [Architecture of decision support systems]. *Nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Scientific Journal of the Kuban State Agrarian University], 2013, no. 86, pp. 290–299.

10. Klyuchko V. I., Vlasenko A. V., Kushnir N. V., Kushnir A. V. *Teoriya informatsii i signalov: uchebnoe posobie* [Theory of information and signals: textbook]. Krasnodar, Kuban State Technical University], 2011, p. 132.

11. Kornienko A. A., Polyanichko M. A. Metodika obnaruzheniya i razresheniya konfliktov programmnykh sredstv zashhity ot kiberatak na zheleznodorozhnom transporte [A technique for detecting and resolving conflicts of software protection against cyber attacks in railway transport]. *Intellektualnye tekhnologii na transporte* [Intelligent Technologies in Transport], 2015, no. 1, pp. 18–21.

12. Simankov V. S., Cherkasov A. N. Metodologicheskie aspekty podderzhki prinyatiya resheniy dlya organizatsii funktsionirovaniya intellektualnoj sistemy situatsionnogo tsentra [Methodological aspects of decision support for organizing the functioning of the intellectual system of a situational center]. *Globalnyy nauchnyy potentsial* [Global Scientific Potential], 2015, no. 12 (45), pp. 114–122.

13. Khomonenko A. D., Danilov A. I., Danilov A. A. Dinamicheskie modeli otladki programm s veroyatnostnym obnaruzheniem oshibok i raspredeleniem Erlanga dlitelnosti ikh ispravleniya [Dynamic models of program debugging with probabilistic error detection and Erlang distribution of the duration of their correction]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2016, no. 16 (4), pp. 655–662.

14. Shari V. A., Burangulova O. S., Andriutsa M. V. Monitoring sostoyaniya nadezhnosti i bezopasnosti strukturno-slozhnykh sistem na osnove logiko-chislovykh modeley [Monitoring the state of reliability and safety of structurally complex systems based on logical-numerical models]. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskie nauki* [News of Southern Federal University. Engineering], 2011, no. 125 (12), pp. 35–49.

15. Antoine Delplace, Sheryl Hermoso, Kristofer Anandita. Cyber Attack Detection thanks to Machine Learning Algorithms. *University of Queensland / COMS7507: Advanced Security*, pp. 3–15.

16. Cisco IOS NetFlow Command Reference. Available at: https://www.cisco.com/c/en/us/td/docs /ios/netflow/command/reference/nf_book/nf_01.html (accessed 04.01.2020).

17. Rafal Kozik and Michal Choras. Machine Learning Techniques for Cyber Attacks Detection. *Image Processing and Communications Challenges*, 2014, vol. 5, no. 233, pp. 391–398.

18. Tang J., Deng C., Huang G.-B. & Zhao B. Compressed-Domain Ship Detection on Spaceborne Optical Image Using Deep Neural Network and Extreme Learning Machine. *IEEE Transactions on Geoscience and Remote Sensing*, 2015, no. 53 (3), pp. 1174–1185.

19. Rehák, Martin, Michal Pechoucek, Pavel Čeleda and Pavel Minarík. *CAMNEP: Agent-Based Network Intrusion Detection System*, 2008.

DOI 10.21672/2074-1707.2020.49.4.155-161
УДК 004.77

СОВРЕМЕННЫЕ МЕТОДЫ АТАК ДЕАНОНИМИЗАЦИИ НА СЕТЬ TOR

Статья поступила в редакцию 05.12.2019, в окончательном варианте – 11.03.2020.

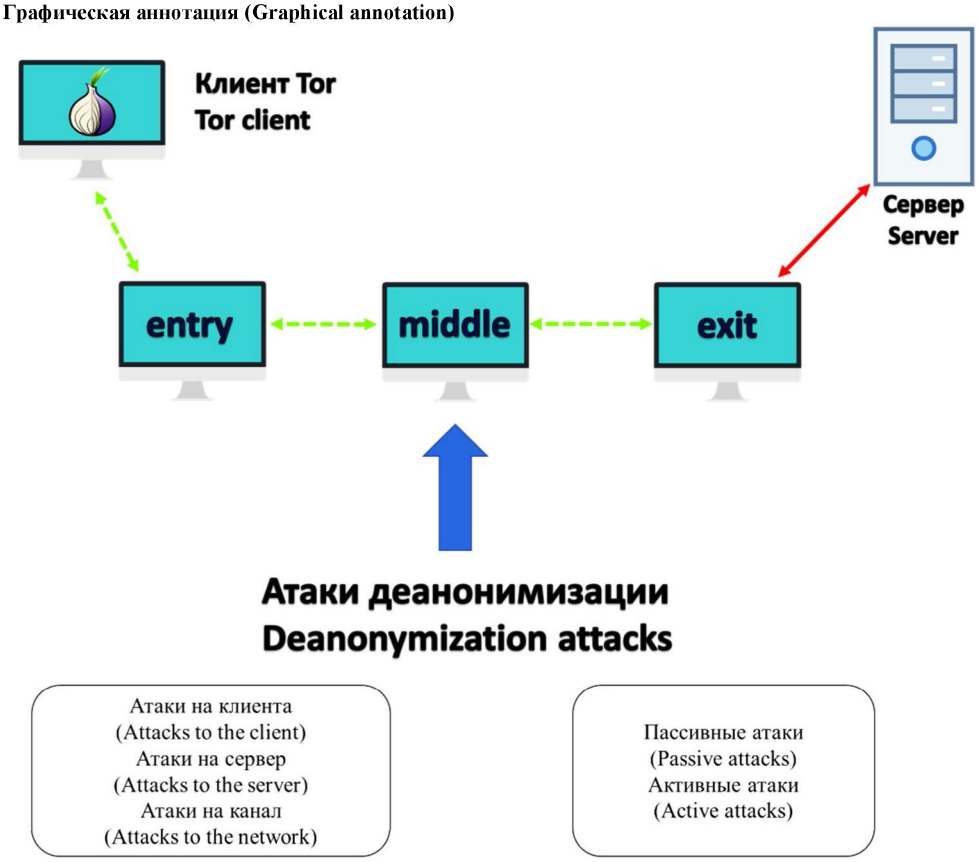
Новосельцева Алёна Вячеславовна, Краснодарский университет Министерства внутренних дел Российской Федерации, 350072, Российская Федерация, г. Краснодар, ул. Ярославская, 128,
курсант, e-mail: AlenaNov98@mail.ru

Клюев Станислав Геннадиевич, Краснодарский университет Министерства внутренних дел Российской Федерации, 350072, Российская Федерация, г. Краснодар, ул. Ярославская, 128,
кандидат технических наук, начальник кафедры информационной безопасности, e-mail: s.g.klyuev@mail.ru

В данной статье представлены современные методы атак деанонимизации на анонимную сеть Tor, а также предлагается их классификация. Изучены принципы взаимодействия узлов и построение цепочки луковой маршрутизации сети Tor. Рассмотрены более подробно атаки на клиентскую сторону сети (Raptor-атака, Torben-атака), атаки на сервер (атака с пометкой ячеек, Off-path MitM) и атаки на канал (Timing-атака, CellFlood DoS-attack). Также рассмотрены атаки в зависимости от воздействия на перехватываемый трафик (активные атаки, при которых происходит модификация трафика, и пассивные атаки, при которых трафик просто перехватывается и анализируется, но не модифицируется). Приведены примеры (прецеденты) некоторых атак и последствия. Сделан вывод о высокой значимости наличия больших вычислительных мощностей и ресурсов в осуществлении всех видов атак на Tor-сети.

Ключевые слова: анонимные сети, CellFlood DoS-атака, Tor, анализ трафика, деанонимизация, луковая маршрутизация, коррумпированные узлы, даркнет

Графическая аннотация (Graphical annotation)



MODERN METHODS OF ATTACS OF DEANIMONIZATION ON THE TOR NETWORK

The article was received by the editorial board on 05.12.2019, in the final version – 11.03.2020.

Novoseltseva Alena V., Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, 128 Yaroslavskaya St., Krasnodar, 350072, Russian Federation,
cadet, e-mail: AlenaNov98@mail.ru
Klyuev Stanislav G., Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, 128 Yaroslavskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Head of Information Security Department, e-mail: s.g.klyuev@mail.ru

This article presents modern methods of deanonymization attacks on the anonymous Tor network, and also proposes their classification. The principles of node interaction and the construction of the onion routing chain of the Tor network are studied. Attacks on the client side of the network (Raptor attack, Torben attack), attacks on the server (attack marked with cells, Off-path MitM) and attacks on the channel (Timing-attack, CellFlood DoS-attack) are considered in more detail. Also considered attack depending on exposure to intercept traffic (active attacks, in which there is traffic modification and passive attacks, in which traffic is simply intercepted and analyzed, but not modified). Examples (precedents) of some attacks and consequences are given. The conclusion is drawn about the high importance of the availability of large computing power and resources in the implementation of all types of attacks.

Key words: anonymous networks, CellFlood DoS-attack, Tor, traffic analysis, deanonymization, onion routing, corrupt nodes, darknet

Введение. В эпоху коммуникаций глобальная сеть Интернет является главным источником информационных ресурсов в повседневной жизни, средством коммуникаций в электронной форме. Будучи важнейшим элементом в жизнедеятельности пользователей-физических лиц, а также правительств и систем критической инфраструктуры, сеть Интернет должна быть защищенной на достаточно высоком уровне.

В контексте обеспечения конфиденциальности важно обеспечить скрытие как контента, которым обмениваются объекты взаимодействия, так и идентичности самих объектов. Анонимные сети как раз и предназначены для сохранения конфиденциальности такого взаимодействия. Сама

анонимность достигается за счет шифрования пользовательских данных и пересылки трафика через ретрансляторы (узлы маршрутизации) или прокси.

Однако стоит отметить, что конфиденциальность взаимодействия пользователей, которая лежит в основе всех анонимных сетей, зачастую используется в преступных целях. Преимущества анонимизации трафика играют на руку террористам, продавцам оружия и наркотиков, мошенникам, экстремистам, сбытчикам запрещенных в обороте товаров и другому преступному контингенту пользователей таких сетей.

Целью работы является исследование существующих на данный момент типов атак деанонимизации на анонимную оверлейную сеть Tor; изучение технических особенностей таких атак, а также оценка возможностей по их реализации.

Анонимная сеть Tor. Существует множество анонимных сетей, включая I2P [6], Freenet [7], MorphMix [12] или Hornet [8]. Тем не менее в настоящее время наиболее популярной луковой сетью (технология анонимного обмена информацией, при котором сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами [3]) является сеть Tor. Протокол Tor на данный момент считается одним из самых популярных сетевых протоколов для организации анонимного взаимодействия.

Tor – это анонимная сеть, которая полностью состоит из волонтерских серверов и программного обеспечения, которое позволяет получать доступ к этой сети. В ней каждый сервер является волонтёрским, и чем больше сеть из пользователей – тем выше ее анонимность. Сеть Tor крайне популярна в России, и в 2019 г. страна стала мировым рекордсменом по числу ее пользователей [5] с посещаемостью 600 тысяч человек в день.

Для построения цепочки клиент обращается к серверу каталогов HSDir и загружает список доступных узлов в сети. Далее клиент выстраивает цепочку из абсолютно случайных узлов. Сама луковая цепочка, как правило, состоит из трех ретрансляторов – входной ноды, промежуточной ноды и выходной ноды (рис. 1). Эта цепь будет активной только 10 минут, далее она перестраивается таким же случайным образом. Такое перестроение также происходит при смене целевого сервера или при личном желании клиента.

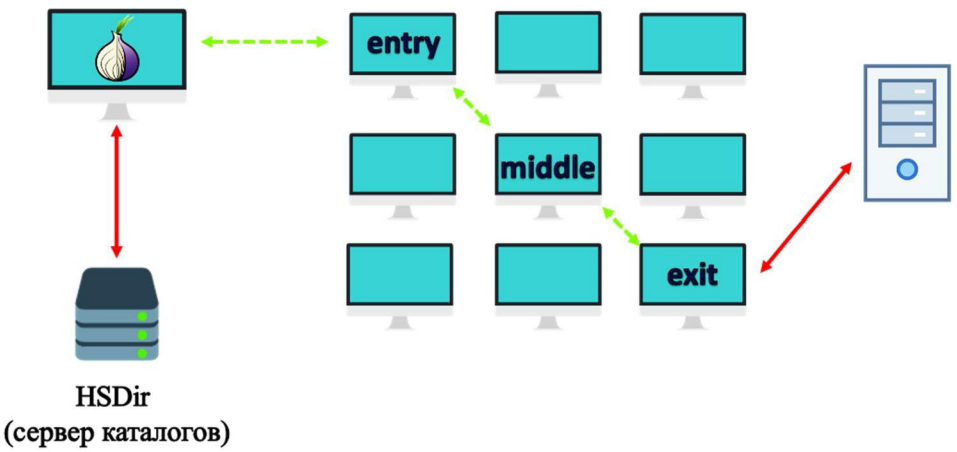


Рисунок 1 – Построение цепочки Tor

Атаки на Tor. Для организации и проведения атак анонимизации необходимо обладать определенными мощностями и ресурсами, например, коррумпированными узлами (узел, трафик которого может модифицировать и просматривать атакующий) или автономными системами.

Перед описанием особенностей атак необходимо отметить существующие на данный момент классификации атак анонимизации на Tor.

Так, в зависимости от воздействия на перехватываемый трафик выделяют активные и пассивные атаки. При активных атаках происходит модификация трафика злоумышленником. В то же время при пассивной атаке происходит лишь сниффинг сетевого трафика (т.е. его перехват), как правило, с целью его дальнейшего анализа.

В зависимости от атакуемого объекта выделяются следующие виды:

- атаки на клиента;
- атаки на сервер;
- атаки на сеть.

Атаки на клиента. Наиболее эффективными атаками на клиента являются Torben-атака [10] и RAPTOR-атака [14].

Torben attack. В данной атаке предполагается, что злоумышленник может контролировать зашифрованную связь между клиентом и входной нодой, а также может внедрять специальные маркеры на интересующую клиента веб-страницу. Эти маркеры шаблонизируют трафик, и чаще всего их источником являются рекламные баннеры. Маркер генерирует характерный шаблон трафика, и он может быть обнаружен между клиентом и входной нодой (рис. 2). Это позволяет злоумышленнику деанонимизировать посетителей отмеченных веб-страниц.

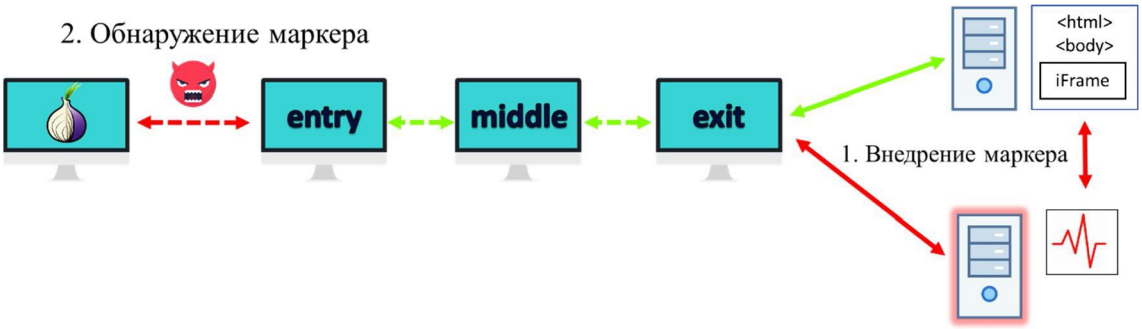


Рисунок 2 – Схема организации Torben-атаки

Маркер представляет собой 20-байтовое значение SHA-1 хэша отслеживаемого URL-адреса веб-страницы. Таким образом, существует соответствие между URL-адресами и их маркерами. Для обнаружения маркера существует многоклассовая машина опорных векторов (support vector machine – SVM) с вероятностными выводами последовательностей отдельных маркеров веб-страниц. Система использует вероятностное сравнение для выбора наиболее подходящего маркера.

По оценке исследователей, с 60 000 веб-страниц атака позволяет обнаруживать эти маркеры с точностью более 91 % без ложных срабатываний [10].

Входной узел Tor является единственным узлом, который напрямую связывается с клиентом. И чтобы побудить клиента использовать определенный «злонамеренный» узел входа, можно блокировать соединения с легальными узлами входа и предоставлять возможность соединения только с коррумпированными. На сетевом уровне это делается с помощью соответствующих политик, например, сетевыми администраторами или провайдерами.

Raptor. Routing attacks on privacy in Tor (RAPTOR) – атака на Tor, где в качестве атакующей стороны выступает автономная система. RAPTOR атака использует динамические аспекты протокола BGP (Border Gateway Protocol – протокол динамической маршрутизации).

Атака состоит из трех частей:

1) асимметричный анализ трафика. В нем анализируются поля TCP-заголовков для выявления номера TCP-последовательности и номер TCP-подтверждения доставки. Вычисляется корреляция между этими полями;

2) анализ натуральных перебоев. Путь между клиентом и входной нодой постоянно меняется, а это повышает вероятность попадания в коррумпированную автономную систему;

3) BGP-сниффинг – коррумпированная автономная система производит атаку «человек посередине» между клиентом и входным узлом. Это позволит автономной системе выполнять ассиметричный анализ трафика.

По данной атаке был проведен ряд экспериментов, и атака в 90 % случаев была успешна [14].

Атаки на сервер. В этом типе атак целью являются скрытые сервисы. Рассмотрим некоторые из них.

Cell counting attack (атака с пометкой ячеек). Атакующий в данном случае должен имеет контроль над входным и выходным узлом клиента. Входной узел дублирует любое сообщение, при этом запоминает IP-адрес и время дублирования. Контролируя выходную ноду, атакующий должен засечь дубликат и получить IP-назначения и порт обращения. Таким образом, злоумышленник может вычислить пользователя и какие сервисы он посещает (рис. 3).

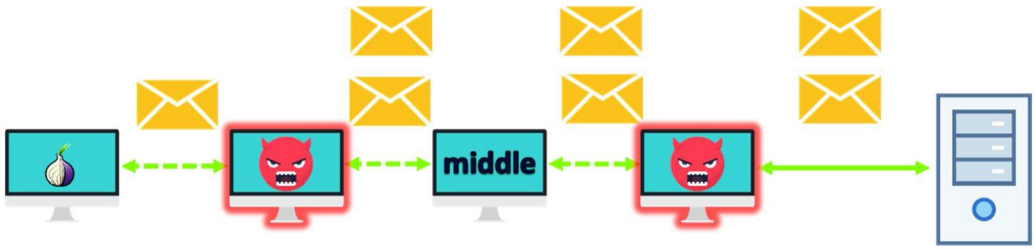


Рисунок 3 – Cell counting attack

Off-path MitM. Атака основана на слежении за метаданными скрытой службы, что позволяет атакующему узнать о ее существовании и доступности [13]. Центральным объектом атаки выступает HSDir.

HSDir – каталог скрытой службы (Hidden Service directory). Эти каталоги содержат информацию, позволяющую получать доступ к onion-доменам (псевдодомены верхнего уровня, созданные для обеспечения доступа к анонимным или псевдоанонимным адресам сети Tor [4]), не нарушая анонимности пользователя.

Злоумышленнику необходимо получить закрытый ключ скрытого сервиса. Также он должен создать клиента, который как будто бы обращается к скрытому сервису, и сервис для обманывания клиента.

Последовательность осуществления атаки показана на рисунке 4.

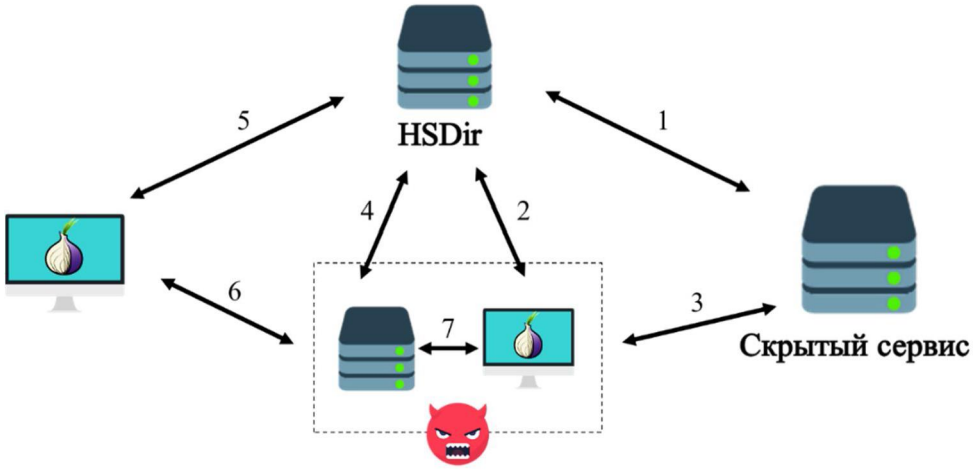


Рисунок 4 – Off-path MitM attack

Основные этапы:

1. Скрытый сервис обращается к каталогу и подгружает дескрипторы.
2. Злоумышленник извлекает информацию из необходимого каталога HSDir.
3. Имитируя работу клиента, злоумышленник устанавливает соединение со скрытым сервисом.
4. Имитируя работу скрытого сервиса, злоумышленник использует скомпрометированный закрытый ключ и загружает новые дескрипторы в HSDir.
5. Клиент, захотев подключиться к скрытому сервису, загружает дескрипторы с HSDir.
6. Клиент подключается к «скрытому сервису» (злоумышленнику).
7. Злоумышленник передает трафик клиента скрытой службе.
8. Злоумышленник находится между сервисом и выходной нодой, где трафик передается в открытом виде.

Таким образом, злоумышленник, который смог скомпрометировать закрытый ключ скрытой службы, может организовать атаку типа «человек посередине» на целевую скрытую службу.

Атаки на сеть (канал). В этом случае целью атаки является сама сеть Tor. Ориентируясь на всю сеть, важно учитывать, что в этом случае вредоносные действия могут влиять на несколько узлов.

Timing-атака. Если атакующий имеет возможность наблюдать трафик клиента и трафик на выходной ноде, то он может установить связь между ними. Данный метод построен на выстраивании корреляции временных шаблонов друг с другом и нахождении определенных зависимостей.

Идея основывается на том, что в Tor задержка по времени не может быть большой, т.е. временной шаблон пакетов данных должен сохраняться при продвижении через цепочку соединения [1].

Коррумпированный узел устанавливает соединение с другими узлами, чтобы измерить задержки соединений и замеряет эти значения. Так злоумышленник рассчитывает транспортную нагрузку на узлы в сети Tor. Когда атакующий получит шаблоны трафика всех узлов, он может воспроизвести атаку по сценарию атаки анализа траффика, высчитав корреляционные зависимости между данными о позиции ячейки, времени, IP-адресе, порте.

CellFlood DoS attack. В сети Tor существуют различные виды сообщений для обмена информацией между узлами. Именно обработка некоторых из них на узлах сети легла в основу этого вида атаки [11].

Атака использует запросы создания цепи (CREATE), которые быстро генерируются атакующим, однако они будут требовать большое количество вычислительных ресурсов от узла для ее обработки. Поэтому из-за криптографических операции обработка CREATE-сообщения занимает в 4 раза больше времени, чем его генерация.

Узел, получающий CREATE-сообщения быстрее, чем его процессор может обработать, отвечает на них, посылая DESTROY-сообщения в ответ. Следовательно, узел, находящийся под атакой, будет отклонять запросы от легитимных узлов (рис. 5).

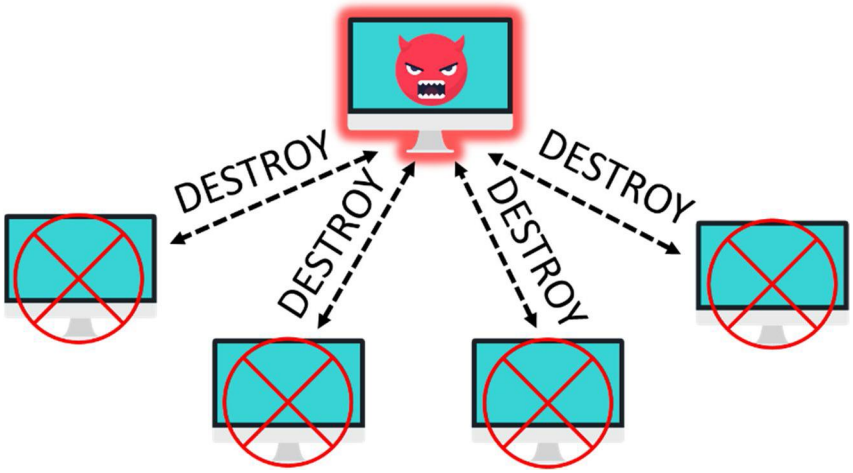


Рисунок 5 – CellFlood DoS attack

Если атакующий заинтересован в том, чтобы исключить узел или набор узлов из сети Tor, ему выгоднее использовать данный вид атаки, нежели чем обычную и более требовательную по ресурсам классическую DDoS-атаку.

В течение нескольких лет этой уязвимостью активно пользуются злоумышленники. Сначала о подобного рода типе атак сообщали легитимные сайты даркнета (анонимная сеть не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде [2]), но в последнее время уязвимость используется преимущественно для атак на подпольные торговые площадки. В марте 2019 г. администрация одного из крупнейших черных рынков даркнета Dream Market объявила о его закрытии после серии мощных DDoS-атак [9]. Через месяц после закрытия Dream Market DDoS-атакам подверглись другие крупные торговые площадки, в том числе Empire Market и Nightmare Market. Постоянные DDoS-атаки вынуждают операторов onion-сайтов переходить с Tor на I2P. Действительно DDoS в обоих случаях.

Заключение. В статье рассмотрены современные методы атак деанонимизации на анонимную сеть Tor. Изучив особенности проведения этих атак, можно сделать вывод, что для их проведения требуются большие вычислительные мощности и ресурсы, автономные системы. Поэтому проведение вышеперечисленных типов атак возможно только государственными организациями или частными компаниями, обладающими соответствующим вычислительным потенциалом.

Библиографический список

2. Авдошин С. М. Технология анонимных сетей / С. М. Авдошин, А. В. Лазаренко // Информационные технологии. – 2016. – Т. 22, № 4. – С. 284–291.

3. Даркнет – интернет-энциклопедия «Википедия». – Режим доступа: https://ru.wikipedia.org/wiki/Даркнет, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.12.2019).

4. Луковая маршрутизация – интернет-энциклопедия «Википедия». – Режим доступа: https://ru.wikipedia.org/wiki/Луковая_маршрутизация, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.12.2019).

5. Onion – интернет-энциклопедия «Википедия». – Режим доступа: https://ru.wikipedia.org/wiki/.onion, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.12.2019).

6. Россия стала мировым рекордсменом по числу пользователей Tor. – Режим доступа: https://www.cnews.ru/news/top/2019-07-17_rossiya_ustanovila_mirovoj_rekord_po_chislu_polzovatelej, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 29.12.2019).

7. I2P. – Режим доступа: https://geti2p.net, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 29.12.2019).

8. Freenet. – Режим доступа: https://freenetproject.org/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 29.12.2019).

9. Hornet. – Режим доступа: https://hornet.com/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 29.12.2019).

10. Хозяева наркорынка в даркнете бежали, прихватив чужие биткоины на $30 миллионов. – Режим доступа: https://safe.cnews.ru/news/top/2019-05-03_hozyaeva_narkorynka_v_darknete_bezhaliprihvativ, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 13.12.2019).

11. Arp D. Torben: A practical side-channel attack for deanonymizing Tor communication / D. Arp, F. Yamaguchi, K. Rieck // Proc. 10th ACM Symp. Inf. Comput. Commun. Security (ASIA CCS). – 2015. – P. 597–602.

12. Ling Z. et al., A new cell-counting-based attack against tor / Z. Ling et al. // IEEE/ACM Trans. Netw. – Aug. 2012. – Vol. 20, no. 4. – P. 1245–1261.

13. Rennhard M. Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection / M. Rennhard, B. Plattner // Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002). – Washington, DC, 2002.

14. A. Sanatinia G. Off-path man-in-the-middle attack on tor hidden services / A. Sanatinia, G. Noubir. – New England Security Day, NESD, 2017.

15. Yixin Sun. Counter RAPTOR: Safeguarding Tor Against Active Routing Attacks / Yixin Sun, Anne Edmundson, Nick Feamster, Mung Chiang, and Prateek Mittal // Security and Privacy (SP) : IEEE Symposium. – 2017. – P. 977–992.

References

1. Avdoshin S. M., Lazarenko A. V. Tekhnologiya anonimnykh setey [Technology of anonymous networks]. *Informatsionnye tekhnologii* [Information Technologies], 2016, vol. 22, no. 4, pp. 284–291.

2. *Darknet – internet-entsiklopediya «Vikipediya»* [Darknet – internet encyclopedia «Wikipedia»]. Available at: https://en.wikipedia.org/wiki/Darknet (accessed 26.12.2019).

3. *Lukovaya marshrutizatsiya – internet entsiklopediya «Vikipediya»* [Onion Routing – internet encyclopedia «Wikipedia»]. Available at: https://en.wikipedia.org/wiki/Onion_routing (accessed 26.12.2019).

4. Onion – *internet-entsiklopediya «Vikipediya»* [Onion – internet encyclopedia «Wikipedia»]. Available at: https://en.wikipedia.org/wiki/.onion (accessed 26.12.2019).

5. *Rossiya stala mirovym rekordsmenom po chislu polzovateley Tor* [Russia has become the world record holder in the number of Tor users]. Available at: https://www.cnews.ru/news/top/2019-07-17_rossiya_ustanovila_mirovoj_rekord_po_chislu_polzovatelej (accessed 29.12.2019).

6. *I2P*. Available at: https://geti2p.net (accessed 29.12.2019).

7. *Freenet*. Available at: https://freenetproject.org (accessed 29.12.2019).

8. *Hornet*. Available at: https://hornet.com/ (accessed 29.12.2019).

9. *Khozyaeva narkorynka v darknete bezhali, prikhvativ chuzhie bitkoiny na $30 millionov* [The owners of the drug market fled on the darknet, grabbing other people's bitcoins for $30 million]. Available at: https://safe.cnews.ru/news/top/2019-05-03_hozyaeva_narkorynka_v_darknete_bezhaliprihvativ (accessed 13.12.2019).

10. Arp D., Yamaguchi F., Rieck K. Torben: A practical side-channel attack for deanonymizing Tor communication. *Proc. 10th ACM Symp. Inf. Comput. Commun. Secrity (ASIA CCS)*, 2015, pp. 597–602.

11. Ling Z. et al. A new cell-counting-based attack against tor. *IEEE/ACM Trans. Netw.*, Aug. 2012, vol. 20, no. 4, pp. 1245–1261.

12. Rennhard M., Plattner B. Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002)*. Washington, DC, 2002.

13. Sanatinia A., Noubir G. *Off-path man-in-the-middle attack on tor hidden services*. New England Security Day, NESD, 2017.

14. Yixin Sun, Anne Edmundson, Nick Feamster, Mung Chiang, and Prateek Mittal. Counter RAPTOR: Safeguarding Tor Against Active Routing Attacks. *Security and Privacy (SP): IEEE Symposium*, 2017, pp. 977–992.