DOI 10.37882/2223-2966.2023.10.12

ВОЗМОЖНОСТЬ ОБНАРУЖЕНИЯ СКРЫТЫХ САЙТОВ И СЛУЖБ СЕТИ DARKNET С ПОМОЩЬЮ НОВОГО ПРОТОКОЛА TOR

THE ABILITY TO DETECT HIDDEN SITES AND SERVICES OF THE DARKNET NETWORK USING THE NEW TOR PROTOCOL

A. Dzhurov
E. Revyakina
L. Cherkesova
D. Korochentsev

Summary. In this paper, a study was carried out on the possibility of detecting hidden sites and services of the DarkNet network using the new TOR protocol. DarkNet is a pseudo-anonymous place for posting online content, which is often used to spread destructive information. Many studies have attempted to estimate the size of the DarkNet, however, studies show that previous size estimates are inaccurate due to the hidden lifecycle of the service. In light of the new Tor protocol for DarkNet, which will prevent the launch of a relay to explore DarkNet sites. The paper presents an analysis of the scanning and effectiveness of the site detection mechanism for law enforcement agencies. Effective strategies for scanning and monitoring hidden services in DarkNet are considered. The analysis of the differences between hidden services, which often rise and fall, and more stable services, and also analyzed the types of services offered by Toronions.

Keywords: information security, destructive content anonymity, onion services, hash function, DarkNet.

Джуров Александр Андреевич
Аспирант,
Донской государственный технический университет
Ревякина Елена Александровна
К.т.н., доцент,
Донской государственный технический университет
revyelena@yandex.ru
Черкесова Лариса Владимировна
Д.ф.–м.н., профессор,
Донской государственный технический университет
chia2002@inbox.ru
Короченцев Денис Александрович
К.т.н., доцент,
Донской государственный технический университет
mytelefon@mail.ru

Аннотация. В данной работе выполнено исследование, возможности обнаружения скрытых сайтов и служб сети DarkNet с помощью нового протокола TOR. DarkNet — это псевдо-анонимное место для размещения онлайн-контента, который часто используется для распространения деструктивной информации. Во многих исследованиях предпринимались попытки оценить размер DarkNet, однако исследования показывают, что предыдущие оценки размера неточны из-за скрытого жизненного цикла службы. В свете нового протокола Tor для DarkNet, который предотвратит запуск реле для изучения сайтов DarkNet. В работе представлен анализ сканирования и эффективности механизма обнаружения сайтов для правоохранительных органов. Рассмотрены эффективные стратегии сканирования и мониторинга скрытых служб в DarkNet. Проведен анализ на различия между скрытыми сервисами, которые часто растут и падают, и более стабильными сервисами, а также проанализированы виды услуг, предлагаемых Toronions.

Ключевые слова: информационная безопасность, деструктивный контент анонимность, сервисы onion, хэш-функция, DarkNet.

Введение

Tor — это инструмент для обеспечения анонимности и конфиденциальности при использовании Интернета, разработанный «Tor Project». Это делается путем инкапсуляции пользовательского трафика на уровнях шифрования и маршрутизации его через три промежуточных узла (onionмаршрутизаторы (onionrouters или ORs)) так, что злоумышленник не может раскрыть: источник, место назначения и контент в одном и том же сетевом местоположении. В академической литературе этот тип сети часто называют смешанной сетью и означает, что в точке входа в сеть личность пользователя известна, но его трафик зашифрован, а в точке выхода его трафик доступен для чтения, но его личность неизвестна.

Tor DarkNet — это функция, предоставляемая Tor, при которой два узла (например, клиент и сервер) могут общаться друг с другом, не зная личности друг друга [1]. Анонимный сервер или скрытая служба может предлагать любую обычную интернет-службу на основе TCP. Пользователь, желающий связаться со скрытой службой, сначала будет искать информацию через узел (HSDir) в распределенной хэш-таблице (DHT), чтобы найти точки введения (IPs), которые будут ретранслировать сообщение в скрытую службу [2]. Затем пользователь попросит вводные узлы передать сообщение с подробным описанием случайно выбранной точки встречи (RP), и обе стороны построят к ней трехцелевую цепь. Поскольку и точка входа, и точка рандеву имеют три промежуточных перехода между ними и пользователем, а также между ними и сервером, ни один из них не знает личности каждой из сторон. Скрытая служба и пользо-

ватель теперь соединены через 6 переходов, которые, в свою очередь, через точку рандеву, а также идентичность друг друга (рисунок 1).

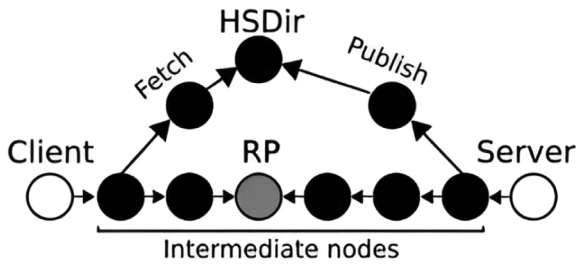

Рис. 1. Сетевой путь скрытых служб

Считается, что скрытые службы Tor обеспечивают абсолютную анонимность. Существует множество опубликованных атак деанонимизации, которые используют простую корреляцию трафика и не требуют значительных ресурсов. Кроме того, правоохранительные и другие органы добились успеха в поиске и обнаружении преступников, действующих в DarkNet, используя уязвимости в программном обеспечении Tor.

В то время как проект Tor и другие заинтересованные стороны часто описывают скрытые службы как пример конфиденциальности и анонимности для политических диссидентов, академическая литература рисует совершенно иную картину, где большинство скрытых служб способствуют преступной деятельности. Учитывая криминально ориентированный контент в DarkNet Tor, многие правоохранительные органы и фирмы, занимающиеся кибербезопасностью, имеют законные интересы в сканировании и сборе информации о скрытых службах.

В данной работе определим эффективные стратегии изучения DarkNet в отношении сканирования и мониторинга скрытых служб. Одна из ключевых проблем — это размер DarkNet, который определяем, как общее количество одновременно доступных скрытых служб. Покажем, что существующие оценки размера DarkNet сильно завышены, и что стратегия сканирования может существенно повлиять на результаты, полученные в любом исследовании, а также можно оценить влияние методологии на оценку доступных служб (например, по портам) и влияние нового протокола скрытых служб на исследования DarkNet.

1. Предлагаемая методология

1.1. Принцип работы Tor

Как описано выше, Tor использует DHT для публикации информации, используемой для связи со скрытыми службами. Tor DHT по конструкции похож на Chord DHT в том, что узлы-участники DHT отображаются на круг вместе с данными для хранения с помощью хеш-функции. В случае Tor это хеш-функция $\boldsymbol{H} : \boldsymbol{X} \rightarrow \{0,1\}^{160}$ — это псевдослучайная односторонняя функция SHA-1, отображающая входной набор X в набор битовых строк длиной 160. Использование хеш-функции, демонстрирующей сильные псевдослучайные характеристики, важно для обеспечения равномерного распределения по кругу (рисунок 2). Каждое ИЛИ отображается на круге с помощью H(PKOR), где PKOR — это кодировка ASN.1 открытого ключа ИЛИ.

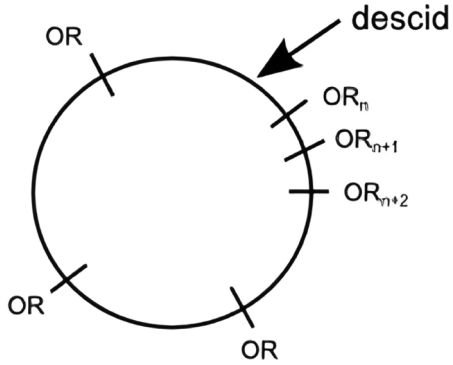

Рис. 2. Отображение скрытых служб Tor TorDHT

Каждая из скрытых служб Tor отображается в круге (рисунок 2) с использованием уникального идентификатора дескриптора (ID), как определено в уравнении (1),

$$\boldsymbol{descid} = \boldsymbol{H}\Big(\boldsymbol{P}\big[0:10\big] \,||\, \boldsymbol{H}\big[\boldsymbol{t_p} \big\| \boldsymbol{d} \big\| \boldsymbol{r}\big]\Big) \qquad (1)$$

где $P = H(PK_{onion})$ и P[a:b] обозначает байты от a до b–1 из P, d — необязательный файл cookie дескриптора(общий секрет), используемый для обеспечения аутентификации на стороне клиента для скрытых служб, которые доступны не всем пользователям.

Наконец, $\boldsymbol{r} \in \{0,1\}^8$ определяется как значение реплики и может быть 0 или 1. Значение реплики обеспечивает степень избыточности, путем хеширования сначала со значением 0, а затем снова со значением 1, это дает два различных (с высокой вероятностью) места в DHT для публикации дескриптора.

Период времени t_p определяется в уравнении (2), учитывая время t по времени UNIX (секунды с 00:00 1 января 1970 г.). Результатом этого является то, что t_p изменяется один раз в день в любом из 256 интервалов, определенных первым байтом P. Это гарантирует, что все скрытые службы не будут пытаться изменить свои серверы публикации одновременно.

$$\boldsymbol{t_p} = \frac{\boldsymbol{t} + \boldsymbol{P}\big[0:1\big] * \frac{86400}{256}}{86400} \qquad (2)$$

Каждая скрытая служба, после сопоставления всех ИЛИ и себя с кругом DHT, публикует свой дескриптор

в трех ИЛИ справа от своего идентификатора дескриптора в DHT. Поскольку скрытая служба отображается на круг в двух местах, всего шесть ИЛИ получают копию дескриптора. Скрытая служба публикует текстовый документ, создавая цепь к каждому из обозначенных ИЛИ и устанавливает HTTP-соединение с портом своего каталога.

Благодаря природе Tor с открытым исходным кодом, можно модифицировать ретранслятор Tor для регистрации запросов скрытых служб (например, посетителей) и публикаций для создания списка скрытых служб. Эффект от использования уравнения (2) заключается в том, что, запустив несколько статических узлов, со временем можно будет наблюдать весь DHT.

В работе [4] представлено исследование, в котором информация из Tor DHT использовалась для сканирования скрытых служб и классификации контента. Автор собрал образец скрытых служб, представленных за один день, и смог охватить 60000 скрытых служб. Затем использовал наивный классификатор Байеса для классификации контента по простым категориям.

Исследования в этом направлении изложены в работе [5], где авторами выполнен анализ данных из сети Tor DHT за период в шесть месяцев. По их оценкам, в то время было около 45000 скрытых служб, но был значительный отток. Они классифицировали контент вручную, чтобы избежать ошибок классификации, и обнаружили, что большая часть контента носит криминальный характер. Примечательно, что они обнаружили, что большинство посещений, скрытых служб приходилось на те, на которых размещен деструктивный контент.

1.2. Измерение размера DarkNet и DarkWeb

Гипотеза истинного размера DarkNet заключается в том, что многие скрытые службы недолговечны, и поэтому ежедневная совокупная статистика количества скрытых служб, например, опубликованная Tor, является завышенной.

Чтобы получить точную оценку количества скрытых служб, нужно иметь возможность видеть все onion каждый день. Это невозможно, потому что нельзя наблюдать за всем DHT Tor, не контролируя все узлы. Однако можно наблюдать часть DHT, а затем экстраполировать глобальные цифры. Выборка DHT стала проще благодаря двум конструктивным решениям Tor. Во-первых, скрытые службы публикуются в шести местах DHT, что означает, что один ретранслятор наблюдает в шесть раз больше публикаций, чем если бы скрытая служба была опубликована только в одном месте. Во-вторых, поскольку скрытая служба публикуется в разных частях DHT каждый день, и это место рандомизируется с использованием псевдослучайной функции, у каждого есть идеальный механизм рандомизированной выборки. Следовательно, можно надежно делать обобщения о большей совокупности на основе небольшой выборки.

Для исследования onion — псевдодомен верхнего уровня, созданный для обеспечения доступа к анонимным или псевдоанонимным адресам сети Tor, был выполнен запуск шесть реле в течение шести месяцев. Реле настроены для получения флага HSDir, чтобы они участвовали в распределенной хэш-таблице для публикации и запросов на скрытые службы [6]. Набор тестов

Сканирование портов долгоживущих (n = 14972) и краткосрочных услуг (n = 352)

Порт	При публикации	Снимок	Выше < 24 часов
22 (ssh)	12.1%	10.59%	–
23 (Telnet)	0.6%	0.09%	–
25/110 (Mail)	1.1%	4.13%	–
53 (DNS)	–	0.05%	–
80 (http)	54.6%	74.16%	51.4%
443 (https)	2.0%	3.61%	–
IRC (all)	1.2%	1.36%	–
3306 (MySQL)	–	0.08%	–
XMPP (all)	–	1.36%	–
8060 (OnionCat)	–	0.89%	–
8080	0.9%	0.41%	–
8333 (Bitcoin)	0.3%	1.0%	–
9878 (Riccochet)	1.1%	0.67%	–
11009 (TorChat)	–	0.37%	–
15441 (Zeronet)	26.1%	0.77%	48.6%

Рис. 3. Набор тестов для сканирования

выглядит следующим образом: после публикации сразу же выполнена проверка доступностиonion и затем сканируем его порт (n =352) (рисунок 3). Выполнялись повторы каждые два часа, с регистрацией времени от публикации до ApTest (инструменты тестирования автоматизации).

В последнее время проект Tor активно пытается остановить изучение DarkNet, и, таким образом, использовать технику, похожую на «honeyonions». В этом случае они каждый день публикуют onion-приманку для выбранных наборов реле и смотрят, какие из них посещаются, чтобы идентифицировать те, которые собирают данные.

Анализ проведенных ранее исследований показал, что через некоторое время после публикации происходит быстрое падение в первые несколько дней тех onions, которые достижимы, после чего с течением времени она начинает медленно снижаться. Кроме того, через 24 часа после публикации доступно менее половины наблюдаемых onions [7]. Более того, примерно 30 % недоступны, то есть вообще не получилось подключиться к ним. Причины этого неясны, но, если сервер имеет неправильные часы, он будет публиковать в неправильных частях DHT, что делает его недоступным. Альтернативные объяснения заключаются в том, что onions просто запускается для короткого теста, а затем останавливается.

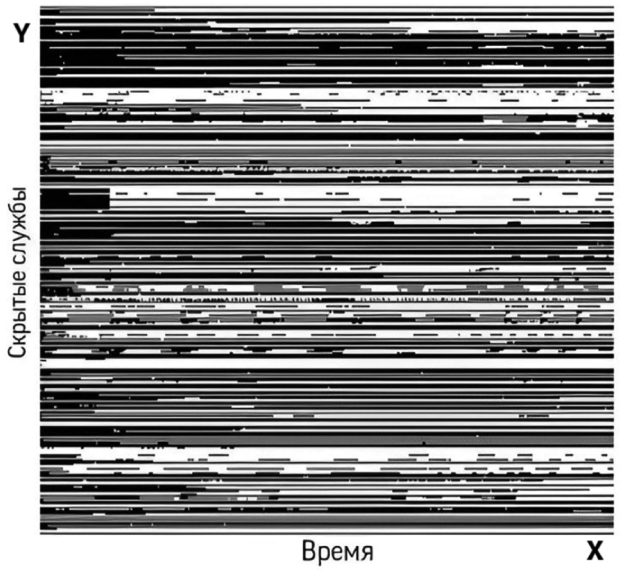

Рис. 4. Карта достижимости скрытого сервиса (время = 25 дней)

На рисунке 4 показан образец скрытых сервисов и их доступность в определенные моменты времени. Каждая линия на оси Y представляет одну скрытую службу, а каждый пиксель на оси X представляет двухчасовое окно. Белый означает, что HS был доступен в этом окне, а черный означает обратное. Сразу видно, что большое количество HSes не было достижимо в каждый момент времени, но также есть небольшое количество. Следовательно, сканирование не может быть разовым событием, потому что в противном случае эти службы будут упущены — его следует повторять как можно чаще.

Для тех, кто перемещается по DarkNet с использованием HSDirs в качестве сидов, кажется вполне разумным обнаружить, что большинствоonions недоступны — это не показатель сбоя в методологии. Можно сказать, что данные метрик Tor завышают размер DarkNet в два или более раз [8]. Это связано с тем, что подсчета публикаций недостаточно, чтобы установить, что onion работает весь день или что она вообще доступна. Вместо этого можно сделать вывод, что DarkNet Tor составляет примерно половину размера, который считался ранее.

2. Результаты исследований и их анализ

2.1. Предлагаемые службыToronions

Далее рассмотрим виды услуг, предлагаемых Toronions. Учитывая большой оборот скрытых услуг, необходимо было более четко понять причины текучести. Хотя долгоживущие услуги изучались много раз, нам не известны какие-либо документы, в которых рассматривались бы те onion, которые работают только в течение короткого периода времени.

Чтобы установить услуги, предлагаемые скрытой службой, выполняется проверка, какие порты открыты. На первом этапе получается дескриптор, затем создается канал к скрытой службе и отправляем ячейку RELAY_ BEGIN с различными портами назначения и наблюдаем за ответом. Если цепь замкнута или возвращается отказ, то порт закрыт, в противном случае он открыт. В более поздних версиях Tor, цепь замыкается при попытке неверного порта, что значительно замедляет сканирование портов (согласно предыдущему академическому исследованию [8,9]. Конечно, по-прежнему можно идентифицировать открытые и закрытые порты, но, по нашему опыту, сканирование 10000 из возможных 65535 портов для одного onionзаняло около 24 часов. Поэтому принят подход к сканированию наиболее вероятных открытых портов, которые были определены путем сочетания построения списка на основе предшествующих знаний, сбора портов из существующих общедоступных / частных сканеров портов DarkNet (путем запуска скрытых служб и записи текущих сканирований.) и сканирование нескольких скрытых сервисов в полном объеме. Окончательный список выглядит следующим образом: 22 (ssh), 23 (telnet), 25 (smtp), 53 (dns), 80 (http), 81, 110 (pop3), 113 (identity), 135 (smb), 161. , 443 (https), 445 (smb), 1337, 1433 (mssql), 3306 (mysql), 4444, 5222 (xmpp), 5223 (xmpp), 5901(vnc), 6667(irc), 6668 (irc), 6669 (irc), 6697 (irc), 8060 (onioncat), 8080, 8081, 8333 (bitcoin), 9051 (tor), 9200 (elasticsearch), 9500, 9878 (ricochet.im), 10000, 11009

(torchat), 15441 (zeronet), 17993, 22222, 27017 (mongodb) и 31337.

К сканированию портов применяются следующие подходы:

1. сканирование порта скрытой службы, как только получаем публикацию в HSDir;
2. подсчет из последней точки, которые выросли менее чем через 24 часа после публикации:
3. сканирование изученных скрытых служб, которые работают в определенный день, — представляя собой снимок DarkNet в определенный момент времени.

Интересно, что веб-сервисы составляют большинство скрытых сервисов в обоих случаях, но Zeronet представлен значительно больше при мгновенном сканировании, и эти onions работают менее 24 часов, что указывает на то, что эти узлы, как правило, имеют короткий срок службы. Из результатов следует также обратить внимание на небольшое количество замеченных служб ricochet.im (обмен мгновенными сообщениями), потому что это часто неофициально упоминается в сообществе Tor как причина всплеска количества скрытых служб. SSH также предлагается на удивительно большом количестве сервисов, что, вероятно, связано с одной из двух причин: 1) операторы используют Tor для анонимного доступа к своим серверам, чтобы снизить риск идентификации; или 2) многие пользователи используют Tor для преодоления межсетевых экранов для доступа к инфраструктуре.

Некоторые провайдеры хостинга Tor запускают две onionsна каждую предлагаемую услугу, одну для общедоступного компонента и одну для удаленного доступа SSH, что снижает возможность связывания, хотя есть некоторые предыдущие работы по использованию sshkeycans для связывания сервисов вместе.

Вместе с тем, анализируются различия между скрытыми сервисами, которые часто растут и падают, и более стабильными сервисами. Для этого вычисляется количество переходов между состояниями (из включенного в выключенное и наоборот) и выполняется нормализация их с течением времени. Для тех сервисов, которые постоянно находятся в сети, переходов не будет. То есть, которые остаются в сети в течение короткого периода времени, а затем исчезают навсегда, будут иметь один переход, в то время как те, которые идут вверх и вниз, будут иметь гораздо больше. Чтобы нормализовать это с течением времени, для каждой службы делится ее измеренное время жизни на количество записанных переходов между состояниями, чтобы производить переходы в день (обозначается tpd). Затем назначается этот номер портам, предлагаемым службой, и представляем данные в таблице 1. Включены только те скрытые службы, у которых наблюдались существенные изменения состояния.

Таблица 1.

Количество портов, предлагаемых против смены состояний в день

Port	Min. tpd	Max tpd	Avg. tpd
22	2.6	17	6
80	2.1	17.2	5.5
15441	2.1	52.5	12.6

Из данных видно, что web, ssh и Zeronet учитывают большинство сервисов, которые демонстрируют частое поведение вверх и вниз. Примечательно, однако, что на Zeronet приходилось значительно больше этих услуг, чем на два других типа, до 12 переходов в день (например, исчезновение на 6 периодов).

В заключение можно сказать, что большой вклад в высокий оборот скрытых сервисов вносят серверы Zeronet, еще один DarkNet, который может использовать Tor для обеспечения некоторой анонимности. Узлы Zeronet, кажется, работают в течение относительно короткого периода времени.

2.2. Анализ существования скрытых служб Tor

Когда скрытые службы Tor публикуются в DHT, они подписывают документы ключом, который представлен их доменным именем (xxxx.onion). Именно по этой причине можно собирать скрытые служебные адреса на узлах DHT. В версии 3 службы Tor использовались слепые подписи для подписания документов, публикуемых в HSDirs. Результатом этого является прекращение возможности запуска HSDirs для сбора скрытых служебных адресов для изучения DarkNetTor, и основным механизмом исследования будет сканирование с известных исходных сайтов. Однако стоит отметить, что, если кто-то знает адрес скрытой службы через другой механизм, тем не менее, можно будет получить скрытый ключ и, таким образом, измерить популярность в HSDir (путем поиска грубой силы).

Использование поискового робота для изучения адресов HS будет означать, что те скрытые сервисы, которые не перечислены и не связаны с ними, не будут обнаружены [9,10]. Это представляет проблему для правоохранительных органов и вносит потенциальную предвзятость при любых попытках изучения DarkNetTor. Для исследования последствий невозможности узнать все адреса, выбираем общие начальные точки и просматриваем DarkNet, записываем, какие скрытые службы используются, а затем сравнивают их с теми, которые были изучены через HSDirs.

Далее выбираются две общие отправные точки для создания начальных списков поисковых роботов: 1) reddit — популярный дискуссионный сайт;

и 2) HiddenWiki — популярная отправная точка для тех, кто просматривает DarkNetTor. На Redditнаправлены на два под-Reddit, которые, как известно, широко используются пользователями Tor, /r/ TOR и /r/onions, где был изучен 601 уникальный onion. Для скрытой Wikibыли просканированы самые популярные Wiki в наборе данных (hwikis25cffertqe.onion) и скрытые вики без цензуры (mijps *****. Onion), изучив 1852 уникальных onions, чтобы оценить эффективность этих двух общих источников в качестве начальных списков, используемых для запуска симулятора сканирования. Симулятор берет ранее просканированные данные и повторно посещает каждую onion, доступную по следующим гиперссылкам (и упоминаниям onion) из списков сидов выше. Симулятор рекурсивно переходит по всем ссылкам, пока не будет достигнуто максимального количества onions, как это сделал бы краулер (поисковый робот, используемы поисковой системой для обнаружения новых страниц в интернете).

Результаты показаны в таблице 2. Чуть меньше половины DarkWeb достижимо при использовании общих списков исходных данных и поискового робота. Ключевой вопрос: другая половина, имеющая какое-либо значение. Из оставшихся 3786 сайтов, на которые поисковик не попал, было 1898 уникальных сайтов.

Таблица 2.

Изученные сиды onion из Reddit

Seed Source	Total onions	Onions up	Reachable	Reachable (%)
Reddit	601	272	3047	44.6 %
Hidden Wiki	1852	482	3038	44.5 %
Combined	2240	580	3047	44.6 %

Наиболее популярными из них были адреса управления и контроля ботнета (компьютерная сеть, состоящая из большого количества компьютеров, на которых скрытно установлено вредоносное ПО, позволяющее злоумышленникам удаленно выполнять любые действия с использованием вычислительных ресурсов зараженных машин), клоны ОС Debian и несколько сайтов с деструктивной информацией [11]. Чтобы оценить их важность, суммируется общее количество запросов, поступающих на сайты, доступные через сканер, и сравниваются с количеством запросов, которые не доступны. На доступные сайты приходилось 2008437 запросов в день, а на недоступные — только 35782 запроса. Таким образом, можно сказать, что, хотя поисковый робот обнаруживает, что менее половины этих сайтов можно изучить с помощью HSDirs, он находит большую часть сайтов, которые посещают пользователи (или 98 % активности).

Таким образом, переход на протокол версии 3 защитит тех, кто действительно хочет, чтобы его не нашли, но, за исключением нескольких классов сайтов, большинство из них хотят привлечь пользователей к своим скрытым службам и будут рекламировать их как можно шире. Однако скрытые сервисы ботнета можно найти с помощью традиционных каналов анализа вредоносных программ, и можно надеяться, что традиционные методы разведки правоохранительных органов возобладают против деструктивных сайтов [12].

Чтобы оценить популярность, необходимо посчитать упоминания на Reddit путем просчета количества уникальных страниц Reddit, на которых была указана onion, и сравнили с количеством запросов, замеченных в HSDirs. Ровно 272 onions, упомянутые на Reddit, были замечены в найденных ранее каталогах, и, следовательно, получилось оценить их популярность. После рассчитывается коэффициент детерминации между количеством упоминаний и количеством запросов в HSDir, который составляет $R^2 = 0.288$. Таким образом, можно сказать, что существует слабая корреляция, но использования одного показателя Reddit недостаточно для измерения популярности. Например, сайтом с наибольшим количеством упоминаний в Reddit была DarkNet-onionFacebook; однако при оценке HSDir наиболее часто посещались рынок наркотиков и места жестокого обращения с детьми.

Вывод

В результате проведенных исследований было выяснено, что проект Tor подсчитывает совокупное количество скрытых онлайн-сервисов за один день, и более половины из них исчезают в течение дня. Кроме этого, было обнаружено, что HTTP был наиболее часто предлагаемой услугой в более долгоживущих onions, но для более короткоживущих onionsZeronet был заметным компонентом — развивающимся DarkNet. Кроме того, сервис riccochet.im играет очень небольшую роль в количестве доступных скрытых сервисов, несмотря на распространенные подобные заявления в сообществе Tor. Использование традиционных источников для списков скрытых сервисов для засева поискового робота DarkNet — эффективное средство понимания активности в DarkNet, при этом на доступные сайты (из общедоступного начального списка) приходится 98% посещений. В то время как введение нового протокола скрытых услуг скроет деятельность тех, кто нигде не публикует свою onion, многие действия требуют публикации для привлечения пользователей.

ЛИТЕРАТУРА

1. Барабанов, В.О. Способы организации информации в теневых и глубоких сетях // В.О. Барабанов, Г.И. Афанасьев // Теория и практика современной науки. 2017. №2 (20).
2. Молдовян, Д.Н. Протоколы слепой цифровой подписи на основе скрытой задачи дискретного логарифмирования //Д.Н. Молдовян, Молдовян А.А., Гурьянов Д.Ю. // Информационно-управляющие системы. 2020. №3
3. Свищёв, А.В. Darknet: полезный инструмент или источник угрозы //А.В. Свищёв, А.С. Лаухина // Colloquium-journal. 2020. №10 (62).
4. Сухов, С.Н. Возможности современных информационных систем по анализу darknet // Научный компонент. 2021. №4 (12).
5. Biryukov, A. Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization // A. Biryukov, I. Pustogarov, R. Weinmann //Conference: IEEE Symposium on Security and Privacy 2013. — 2013, Pp 80–94 / DOI:10.1109/SP.2013.15
6. Owen, G. Empirical analysis of Tor Hidden Services //G. Owen, N. Savage // Computer Science. — 2016 /DOI:10.1049/iet-ifs.2015.0121
7. Goulet, D. Hidden-service statistics reported by relays //G. David, J. Aaron, K. George, L. Karsten // Tor Tech Report 2015-04-001. — 2015.
8. George, K. "Major Key Alert!" Anomalous Keys in Tor Relays //K. George, C. Roberts, L. Roberts, P. Winter // Financial Cryptography. — 2017 / DOI:10.1007/978-3-662-58387-6_1
9. Bonneau, J. Anonymity for Bitcoin with accountable mixes // J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. Kroll, W. Edward // Princeton University, University of Maryland, Concordia University — USA, Canada. — 25 с.
10. Прусаков, Д.А. Способы компьютерных преступлений // Д.А. Прусаков // Вестник науки и образования. 2021. №14-1 (117).
11. Ляшенко К.А., Поркшеян В.М., Черкесова Л.В., Ревякина Е.А., Енгибарян И.А., Бурякова О.С., Решетникова О.А. Модификация классического квантового протокола bb84, повышающая его характеристики // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 2. С. 100–115.
12. Methodology for neural networks training at analyzing the context of event at emotions recognizing Kovtun Y., Cherckesova L., Revyakina E., Safaryan O., Roshchina E., Porksheyan V. Всборнике: Robotics, Machinery and Engineering Technology for Precision Agriculture. Proceedings of XIV International Scientific Conference «INTERAGROMASH 2021». Сер. «Smart Innovation, Systems and Technologies», Singapore, 2022. С. 65–71.