УДК 004.9

ВОЗМОЖНОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПО АНАЛИЗУ DARKNET

CAPABILITIES OF MODERN INFORMATION SYSTEMS FOR DARKNET ANALYSIS

Сухов Сергей Николаевич,
доцент кафедры криминалистики Нижегородского филиала Санкт–Петербургской академии Следственного комитета Российской Федерации, кандидат юридических наук,доцент

suhov.sn@skspba.ru

Ключевые слова:
дарквеб, даркнет, onion-сканеры, мониторинг ресурсов.

Автор рассматривает актуальные вопросы мониторинга и анализа скрытого сегмента сети Интернет, анализирует функциональные особенности сети Tor, описывает возможности открытых инструментов для поиска в Dark web, приводит примеры поисковых инструментов (ресурсов), осуществляющих поиск по скрытому сегменту сети Интернет. Отдельно рассматривается возможность ресурса Dark Web Monitor, представляющего собой специализированную информационно-аналитическую платформу, которая аккумулирует информацию, полученную с различных ресурсов Dark web.

Keywords:
darkweb, darknet, onion scanners, Dark Web Monitor, resource monitoring.

The author considers topical issues of monitoring and analysis of the hidden segment of the Internet, analyzes the functional features of the Tor network, describes the possibilities of open tools for searching in darkweb, gives examples of search tools (resources) that search for a hidden segment of the Internet. Separately, the possibility of the Dark Web Monitor resource is considered, which is a specialized information and analytical platform that accumulates information obtained from various darkweb resources.

Дарквеб – это содержание всемирной паутины, которое существует в даркнетах, оверлейных сетях, использующих Интернет, но требующих специального программного обеспечения, конфигурации или авторизации для доступа.

Даркнет, в свою очередь, является общим термином для всех сетей, инфраструктура которых накладывается на инфраструктуру Интернета. Чаще всего под даркнетом имеется в виду сеть Tor, но есть еще много доступных даркнетов, таких как I2P, Freenet, Zeronet, GNUnet и несколько других. Все они вместе составляют дарквеб. Место дарквеба и даркнета в структуре Интернета наглядно отображено на рис. 1.

Рис. 1. Дарквеб и даркнет в структуре Интернета

Рассмотрим более подробно наиболее популярный даркнет «Луковый» маршрутизатор (Tor) – сеть с открытым исходным кодом, которая опирается на протокол (набор правил), известный как «луковая маршрутизация», используемый для анонимной связи по компьютерной сети. Tor – это крупнейшая сеть, используемая в «темном» интернет-сегменте. Можно перемещаться в этой пиринговой сети, используя специальный веб-браузер, называемый «Tor Browser»[1].

Использование Tor Browser:

- анонимизация клиента в открытой сети;
- анонимизация сервера и клиента в сети Tor;
- устойчивость к «подслушиванию»;
- устойчивость к анализу трафика;
- инструмент обхода цензуры.

1 Официальный сайт Torproject. URL: https://www.torproject.org/ru/.

Необходимо отметить, что использование Tor Browser для просмотра ресурсов открытой сети и скрытых сервисов будет организовано по разным схемам, структурно отразим особенности построение схемы подключения на рис. 2.

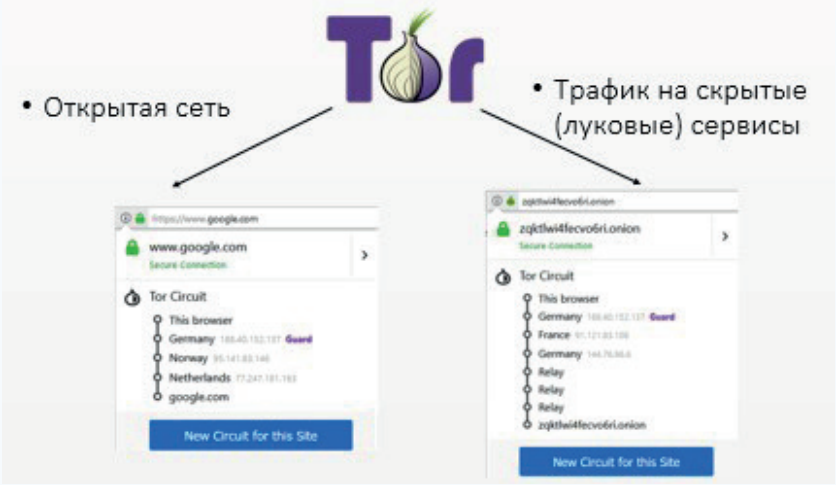

Рис. 2. Схемы подключения Tor Browser

Как мы видим из рис. 2, при использовании Tor Browser для просмотра открытых ресурсов сети Интернет, например сайта https://www.google.com/, цепочка подключения включает использование трех узлов, а при переходе на «луковый» сервис в цепочку включены уже шесть узлов сети Tor.

Количество доступных узлов для подключения и использования сети Tor можно увидеть на официальном ресурсе разработчика: https://metrics.torproject.org (рис. 3).

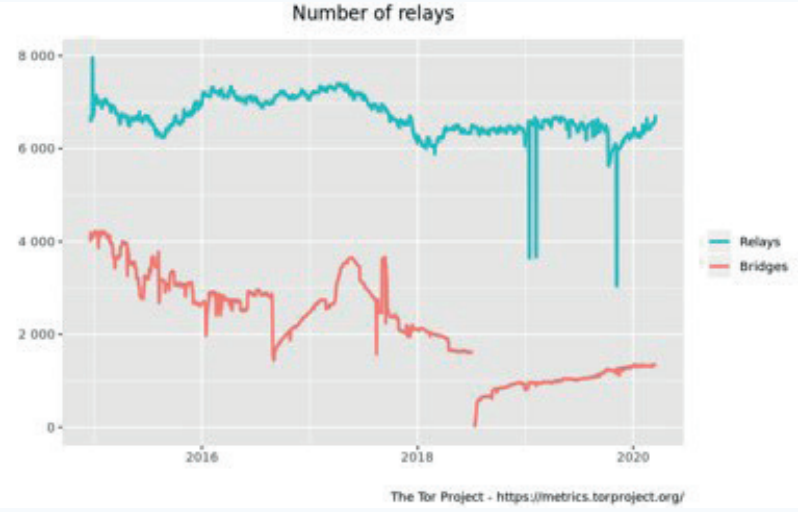

Рис. 3. Количество узлов сети Tor

Среди наиболее распространенных ресурсов сети Tor (услуги, контент, товары в даркнебе) можно выделить следующие основные группы:

– незаконные товары;
– незаконные услуги;
– незаконный контент;
– darknet-магазины;
– форумы и социальные медиа.

Мониторинг ресурсов даркнеба имеет отличительные особенности. Среди инструментов мониторинга даркнеба можно выделить две большие груммы:

– инструменты для мониторинга открытого Интернета;
– инструменты мониторинга скрытых ресурсов.

Среди наиболее известных инструментов для мониторинга ресурсов даркнеба в открытом Интернете можно привести для примера такие ресурсы, как:

– Darknetlive (https://darknetlive.com/) – источник новостных статей и ссылок;
– Darksearches (https://darksearch.io/) – сервис для поиска скрытых сервисов в сети Tor;
– Ahmia (https://ahmia.fi) – сервис для поиска скрытых сервисов в сети Tor и I2P. Также существует как «луковый» сервис;
– Reddit (https://www.reddit.com/r/onions) – Onions;
– (https://www.reddit.com/r/darknet/) – Darknet;
– (https://www.reddit.com/r/deepweb/) – Deep web;
– Duckduckgo (https://duckduckgo.com) – поисковая система с конфиденциальностью, стандартная поисковая система при установке Tor-браузера. Также существует как «луковый» сервис.

Инструменты для мониторинга даркнеба в скрытом интернете (onion-сканеры):

– Ahmia: http://msydqstlz2kzerdg.onion/;
– Torch: http://xmh57jrzrnw6insl.onion/;
– Not Evil: http://hss3uro2hsxfogfq.onion/;
– VisiTOR: http://visitorfi5kl7q7i.onion/search/;
– OnionLand Search: http://3bbaaaccczcbdddz.onion/;
– Candle: http://gjobqjj7wyczbqie.onion/;
– Oculus: http://jdpskjmgy6kk4urv.onion/;
– Fresh Onions;
– http://vps7nsnlz3n4ckiie5evi5oz2znes7p57gmrvundbmgat22luzd4z2id.onion

и многие другие.

Выше были перечислены источники преимущественно для англоязычной аудитории. Если говорить о русскоязычном сегменте, то можно отметить такие источники, как:

– http://doe6ypf2fcyznaq5.onion – Ru-Wiki, каталог ссылок и материалы;
– http://godnotabatovgyqz.onion – каталог ссылок с отзывами;
– http://oneirunda366dmfm.onion – «Яндекс» даркнета.

Поиск по ресурсам дарквеба без использования специальных аналитических платформ крайне затруднителен. Dark Web Monitor[2] – информационно-аналитическая платформа, которая уже 7 лет является одним из основных инструментов правоохранительных органов по мониторингу дарквеба. Используется странами Евросоюза, Европолом для анализа дарквеба.

Dark Web Monitor собирает информацию об онлайн-действиях в дарквебе в таких сферах, как наркотики, оружие, киберпреступность, контрафактная продукция и т.д.

Доступ к информации, собранной в Дарквебе, осуществляется через браузер (рис. 4).

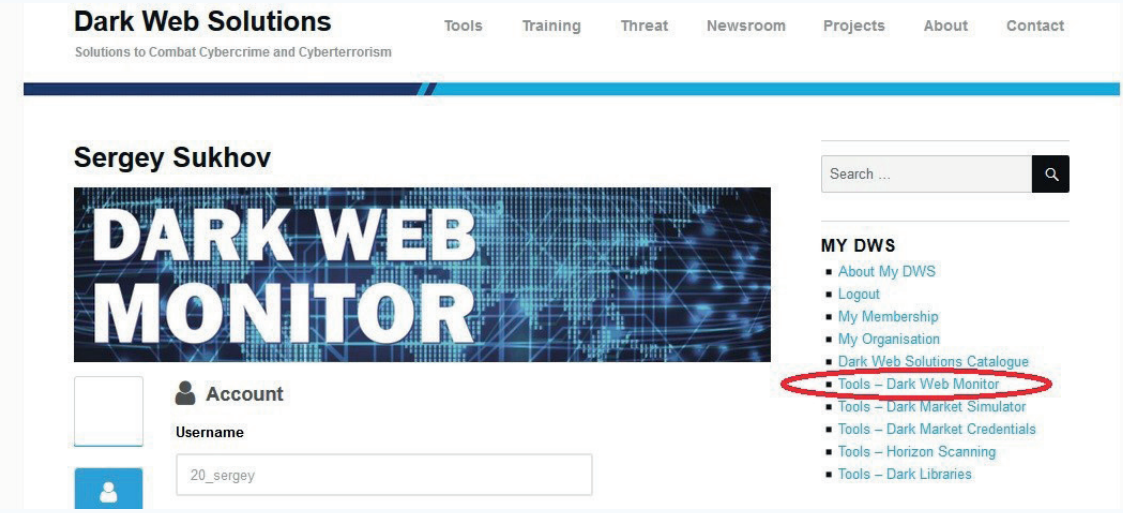

Рис. 4. Dark Web Monitor как один из инструментов мониторинга и анализа дарквеба

Помимо формирования архива активности дарквеба, среди решений для борьбы с киберпреступностью и кибертерроризмом разработчиками Dark Web Monitor предлагаются и другие интересные инструменты (рис. 4), например симулятор торговой площадки или «обменника» дарквеба. Данные инструменты возможно использовать как для самообразования, так и для включения в учебные курсы по формированию профессиональных компетенций в сфере мониторинга и анализа дарквеба.

2 Официальный сайт Dark Web Solutions (Solutions to Combat Cybercrime and Cyberterrorism). URL: https://dws.pm.

Рис. 5. Стартовая страница Dark Web Monitor

На стартовой странице (рис. 5) размещаются обобщенные статистические показатели по основным направлениям мониторинга даркнета.

Среди основных разделов мониторинга:

– домены;
– торговые площадки;
– форумы;
– используемые адреса криптокошельков, e-mail, PGP ключей, «никнеймов» пользователей (рис. 6).

Данная информация копируется и заносится в структурированный информационный массив, с возможностью поиска по интересующим объектам, с сохранением «скиншотов» страниц, переписки пользователей, например на форумах (рис 6).

Возможно добавление вновь появляющихся ресурсов даркнета, работа по API.

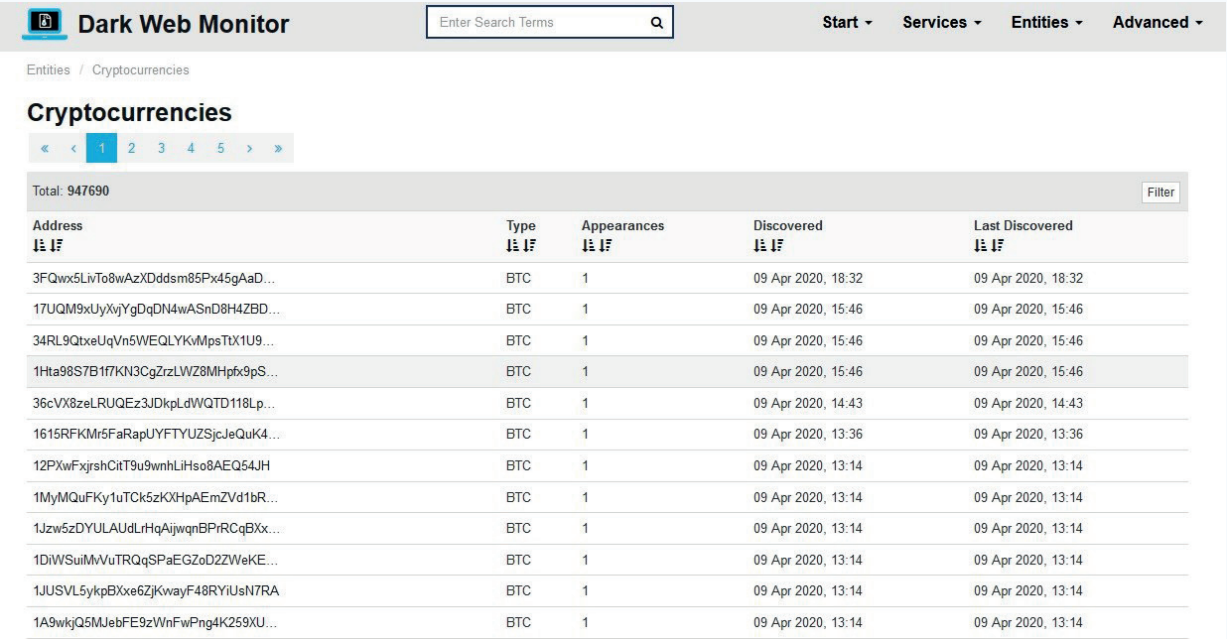

Рис. 6. Мониторинг криптовалют

Использование Dark Web Monitor на сегодняшний день является практически единственной возможностью по получению архивной и текущей информации об активности в скрытом сегменте интернета.