ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

Выполнил студент бакалавриата,
техник по защите информации:
Емельянов Григорий Андреевич

Москва, 2024

Использование информационно-телекоммуникационных сетей в преступных целях

Статья посвящена не преступлениям, связанным с нарушениями целостности, доступности и конфиденциальности информации, а именно распространению преступных действий через информационно-телекоммуникационные сети. Будут рассмотрены лишь некоторые из способов использования сети Интернет и других информационно-телекоммуникационных сетей в целях, рассматриваемых законодательством РФ как преступления, влекущие за собой разные виды ответственности.

Распространение запрещённых веществ в информационно-телекоммуникационных сетях

Распространение запрещенных веществ в глобальных сетях представляет серьезную угрозу для общества. Наркотики, психотропные вещества и другие запрещенные препараты могут быть легко приобретены через интернет, что создает возможность для преступников и наркодилеров уклониться от наказания и расширить свои операции на международном уровне.

В данном разделе описывается скорее получение первоначального доступа к наркотрафику и торговым площадкам, а не весь процесс их работы и функционирования. Получить первоначальный доступ к торговым площадкам в сети, обычному человеку, если он заранее не знает об их существовании, достаточно проблематично. Поэтому для получения первоначального доступа, зачастую используются уличные наклейки, стикеры, визитки, граффити, надписи на стенах, столбах, транспортных остановках, асфальте, подземных и наземных переходах и т. п (примеры можно увидеть на рисунке 1). Преступники указывают номер телефона, по которому можно связаться, QR-код пользователя преступника или чат-бота в мессенджере Телеграм. Стоит быть осторожным, так как некоторые подобные контакты, с

предложением лёгкого заработка, или даже работы вахтой, в итоге могут привести человека в заточение на рабскую деятельность.

Рисунок 1 – Незаконные надписи/наклейки, ведущие к связи с преступником

В случае перехода в чат-бот выбирается категория вашей деятельности: покупка, продажа, работа. Все дальнейшие действия также могут проходить в чат-боте, однако нередки случаи, когда данный чат-бот создан и работает исключительно с целью обмана пользователей и незаконного заработка. Отличительная особенность чат-бота, которая будет выделять его прозрачность – переход на известную сетевую площадку оборота наркотрафика для совершения сделки через сеть Интернет.

Также, первоначальный доступ к торговым площадкам может осуществляться через администратора (куратора). Здесь подразумевается именно работа в данной сфере. В личном сообщении мессенджера Телеграм преступник задаёт пару уточняющих вопросов, а затем просит заполнить стандартную форму по пунктам: возраст, город проживания, опыт работы в данной сфере, наличие водительских прав, мотивация, карьерный рост, знание методов и средств анонимности в сетях (Proxy, VPN, Tor), пожелания к работе. Стоит отметить, что преступники не просят создать секретный чат в мессенджере и общаются достаточно откровенно.

Затем происходит регистрация на известной сетевой площадке оборота наркотрафика. В данных сервисах заботятся о безопасности, для начала необходимо пройти капчу, потом зарегистрироваться с паролем по высоким требованиям стандартов безопасности, без идентификации человека по его номеру телефона или электронной почте, затем ещё раз пройти капчу. В системе может использоваться двухфакторная аутентификация, публичный PGP ключ и другие средства защиты.

Такие площадки используют много «зеркальных» сайтов, во избежание остановки деятельности после блокировки основного сайта, а также могут использоваться для балансировки нагрузки. Копия основного веб-сайта, хранится на другом домене, сервере или имеет отличный от главного URL-адрес, при этом, все они будут ссылаться на один и тот же основной сервер, для получения данных о пользователях и др. Резкая блокировка всех сайтов и борьба государства с этими сервисами приводит к появлению других аналогичных площадок, в том числе с использованием мессенджера Телеграм.

После регистрации преступник просит перейти в раздел «Работа» и выбрать его сообщество (группу). Все финансовые операции происходят через криптовалюту, обычно Bitcoin (BTC). Идентификатор Bitcoin кошелька является уникальным идентификатором для отправки и получения денежных средств и состоит из 40–50 символов. Также его можно приобрести с помощью обычных банковских карт известных платёжных систем на данном торговом сайте, в разделе «Обмен». Для первой работы необходимо выплатить залог, обычно от 3 тысяч до 5 тысяч рублей, в зависимости от количества и качества товара, во избежание обмана новичком. Новичок получает данные о получении товара и о том, куда его надо спрятать. Клиент, купив товар на торговой площадке, автоматически получает его координаты на карте местности.

Подобные организованные преступные сервисы (часто именуемые «даркнет») предоставляют доступ не только к покупке запрещённых веществ, но и к другим преступным видам деятельности: поддельные документы, сетевые атаки, слежка за человеком, заказные убийства и многое другое. Они

реализуются не только через сеть Интернет, но и через популярную анонимную сеть Tor.

Сейчас, в век информационных технологий, не обязательно встречаться с преступниками напрямую, всё общение анонимизируется и шифруется, финансовые операции практически невозможно отследить, а найти товар на улице не составит большого труда. Таким образом, достаточно несложно получить доступ к наркотрафику, покупать товар или работать в этой сфере, что повышает уровень преступности в стране.

Ложные вакансии о предоставлении работы

Ложные вакансии используют на популярных сервисах онлайн-рекрутинга в злоумышленных целях, обманывая жертв для получения финансовой выгоды. Зачастую в таких вакансиях заявляют о высокой заработной плате при минимальной нагрузке, свободный график, работу на дому, отсутствие бюрократии и т. п.

Обычно такие вакансии предлагают следующие виды работ: сортировка или рукоделие на дому, создание бизнеса по выращиванию чудо-ягод и фруктов на дому, расшифровка аудиозаписей, работа «курьером», набор текста, перепродажа товара на маркетплейсах, тестирование игр, мошеннические вакансии, составление комментариев/отзывов, работа тайным покупателем.

Методы обмана примерно идентичны: для получения первого заработка необходимо ввести все данные вашей банковской карты на фишинговом сервисе. В противном случае злоумышленники могут угрожать своим жертвам разными способами, приводить в аргументы статьи УК РФ или Федеральные законы, психологически давить на людей, проводить сетевые атаки в отношении жертвы, компрометировать действия от имени жертвы, шантажировать.

Также нередки случаи, когда официальный работодатель просит выполнить несколько тестовых заданий (например, большую монотонную

работу) для определения компетентности претендента на должность. После выполнения задания работодатель либо не отвечает, либо заявляет о низком уровне навыков, тем самым, облегчая внутреннюю работу компании, которую за них выполняют якобы кандидаты на должность.

Некоторые методы социальной инженерии в социальных сетях и сервисах объявлений

Социальные сети. В социальных сетях злоумышленники создают идеальную страницу магазина: создают поддельные отзывы, делают записи о продаже и выгодности приобретения товара, указывают место расположения их склада или магазина. Отличить поддельный магазин можно по следующим признакам:

- Все записи страницы сообщества сделаны в один-два дня.
- Отзывы, лайки и комментарии созданы поддельными страницами пользователей сети (их также можно определить по первому пункту, а также по идеальности заполнения всех разделов открытой страницы).
- Отсутствуют контакты администратора сообщества.
- Отсутствуют контакты самого сообщества (или не отвечают на сообщения).
- Создаётся ощущение идеализированной страницы.
- Цены на товары как минимум наполовину ниже средней рыночной стоимости.
- Данный магазин нельзя найти в сети Интернет.
- Данный магазин отсутствует в помещении, указанном на странице.

Сервисы объявлений. После публикации товара на некоторых популярных сервисах объявлений в течение часа приходят сообщения от покупателей. Они заявляют, что уже перевели деньги на сервис для покупки товара, а продавцу необходимо их только получить. Злоумышленники, изучив схему взаимоотношения клиентов (а именно подобным образом и происходит покупка товара), предлагают перейти по ссылке (на фишинговый сайт, с

похожим доменом) и ввести там все данные банковской карты, чтобы якобы получить деньги за товар. Дальше злоумышленники пытаются психологически давить на жертву, что деньги перевели, а жертва пытается его обмануть, или заявляют, что нашли более выгодный вариант товара.

Можно сделать вывод, что переписку ведут не боты, а люди, так как вступают в прямой осмысленный диалог, используют присущие людям ошибки в грамматике. Сервисы объявлений предпринимают попытки для разоблачения и блокировки злоумышленных действий и аккаунтов, но не имеют общей политики и профилактики предупреждений данного вида мошенничества.

Распространение файлов обмена в обход легитимных сервисов

Файлообменники часто используют для распространения нелицензионного или лицензионного программного обеспечения в обход официального легитимного сервиса правообладателя. Также они применяются для распространения киноконтента в обход платных видеохостингов, правообладателей на контент. Для реализации таких целей были придуманы специальные сервисы и сетевые протоколы, Proxy серверы, виртуальные частные сети (VPN), а также «многозеркальные» сайты в сети Интернет, нарушающие законодательство в области авторского права. Организация систем и сетей, на которых работают данные сервисы, приведены ниже.

BitTorrent — пиринговый (P2P — сеть, основанные на равноправии участников) сетевой протокол для кооперативного обмена файлами через Интернет. Часто в пиринговой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются все узлы. Файлы передаются частями, каждый torrent-клиент, получая (скачивая) эти части, в то же время отдаёт (закачивает) их другим клиентам, что снижает нагрузку и зависимость

от каждого клиента-источника и обеспечивает избыточность данных (пример отображён на рисунке 2). Каждый клиент имеет возможность временно блокировать отдачу другому клиенту. Предпочтение отдаётся пирам, которые сами передали этому клиенту много сегментов. Таким образом, пиры с хорошими скоростями отдачи поощряют друг друга по принципу «ты — мне, я — тебе».

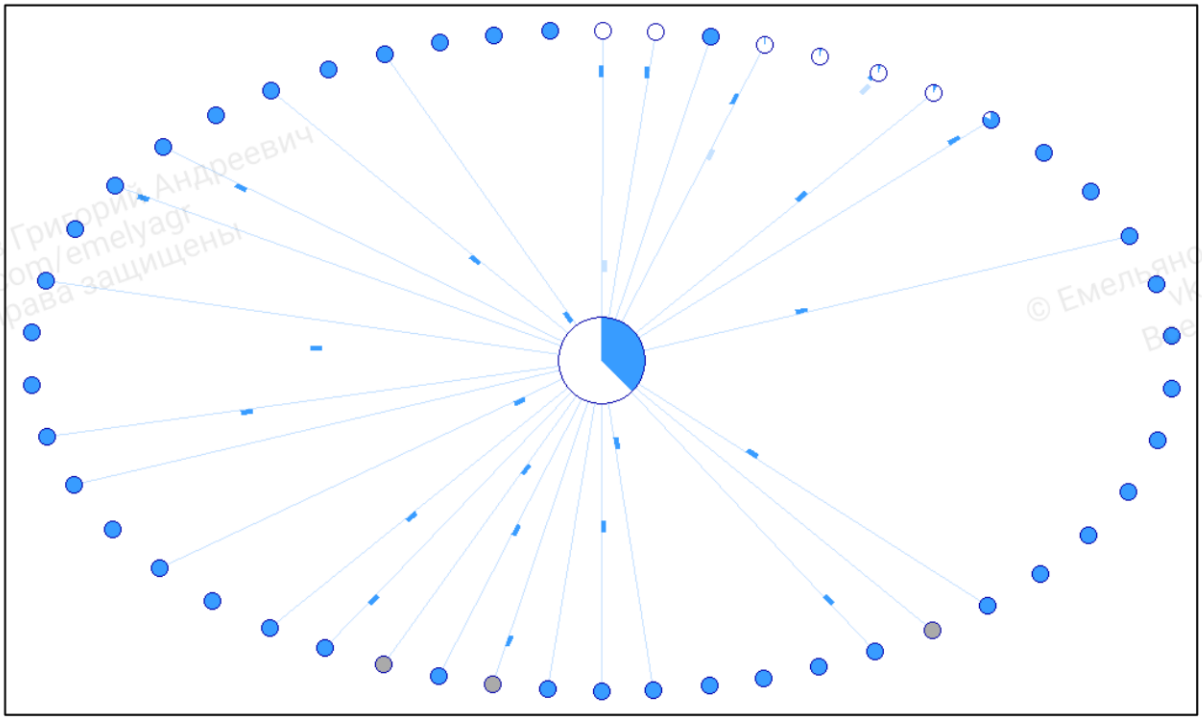

Рисунок 2 – Пример получения/раздачи файлов

µTorrent — кроссплатформенный BitTorrent-клиент (веб-интерфейс), отличающийся небольшим размером и высокой скоростью работы при достаточно большой функциональности. В январе 2011 года количество пользователей в месяц достигло отметки в 100 миллионов. Пример веб-интерфейса µTorrent представлен на рисунке 3.

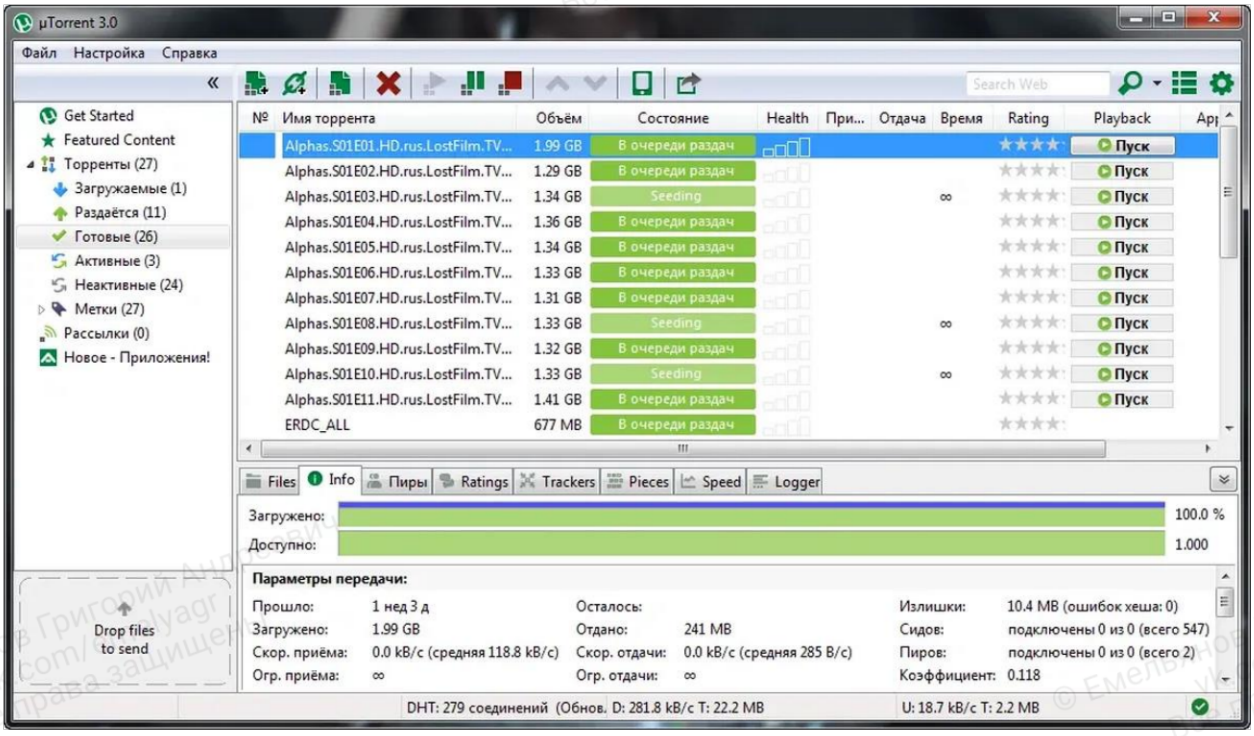

Рисунок 3 – Веб интерфейс µTorrent 3.0

Tor — свободное и открытое программное обеспечение для реализации второго (V2) и третьего (V3) поколения так называемой луковой маршрутизации. Сеть является самостоятельной и не входит в сеть Интернет. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде через несколько случайных узлов (прокси-серверов). С помощью Tor пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов — узлов. Технология Tor также обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом. Tor оперирует сетевыми уровнями onion-маршрутизаторов, позволяя обеспечивать анонимные исходящие соединения и анонимные скрытые службы.

I2P — анонимная компьютерная сеть. Сеть I2P является оверлейной (т. е. работает поверх другой сети — Интернет), устойчивой (отключение узла не повлияет на функционирование сети), анонимной (невозможно или сложно определить IP-адрес узла) и децентрализованной (не имеющей центрального сервера). При передаче данных между узлами сети применяется шифрование. Внутри сети I2P можно разместить любой сервис (или службу) (форум, блог, файлообменник, электронную почту, систему для мгновенного обмена сообщениями (чат), систему для совместного использования файлов, VoIP и т. д.) с сохранением анонимности сервера. В сети I2P работают http-серверы; адреса сайтов находятся в псевдодоменном пространстве «.i2p». Поверх сети I2P можно строить одноранговые сети (P2P), например, BitTorrent, eDonkey, Kad, Gnutella и т. д. Использует чесночную маршрутизацию, которая является дополнением к луковой маршрутизации.

Таким образом, злоумышленное использование файлообменников является серьезной проблемой, которая может привести к краже личной информации, распространению вредоносных программ и нарушению авторских прав.