Текст · 15 октября 2024, 14:39
Никита Сологуб,

Фишинговые сайты собирают данные от имени легиона «Свобода России». Как это работает и насколько это опасно

В марте 2023 года Верховный суд признал террористической организацией легион «Свобода России» — добровольческое подразделение ВСУ, в котором сражаются российские граждане.

После этого даже переписка с представителями легиона может быть квалифицирована по тяжкой части 2 статьи 205.5 УК (участие в террористической организации — от 10 до 20 лет заключения). Люди, ищущие информацию о подразделении в интернете, стали легкой добычей для российских спецслужб. Оценить количество уголовных дел с подобным составом трудно, но новости о задержаниях появляются регулярно, а приговоры судов неизменно суровы — независимо от возраста обвиняемых и региона, в котором проходит процесс.

9 октября 2-й Западный окружной военный суд в Москве приговорил к 12 годам колонии 50-летнего оппозиционного активиста Евгения Мищенко. Он не отрицал, что «пытался выйти на связь с этой организацией», но подчеркивал, что его «участие» в деятельности легиона «Свобода России» ограничилось перепиской. Выяснять, кто именно переписывался с Мищенко от лица украинского подразделения, суд не стал.

За неделю до приговора Мищенко по 11 лет колонии получили петербуржцы Федор Коновалов и Иван Радченко, расклеивавшие листовки в поддержку «Свободы России» по поручению человека, представившегося сотрудником СБУ.

За два дня до этого 9 лет колонии получил 35-летний выпускник Московского казачьего кадетского корпуса фельдшер Иван Колосов.

В тот же день суд в Петербурге дал 10 лет колонии автослесарю Ярославу Речкалову. Он отправил пользователю с ником «Калуга» видео, в котором произносил перед камерой несколько наивный текст: «Присягаю легиону, буду служить верой и правдой, хочу воевать на стороне Украины».

В пресс-релизах силовиков о делах, связанных с легионом «Свобода России», часто упоминается «интернет-мессенджер». Автослесарь Речкалов, по версии следствия, «в интернет-мессенджере связался с участником указанной террористической организации». 39-летний хабаровчанин, имя которого не называлось, «по своей инициативе через интернет-мессенджер вступил в переписку с агентством украинских спецслужб».

Из-за таких абстрактных формулировок узнать, общался ли обвиняемый с настоящим представителем легиона или с человеком, который только выдавал себя за украинского военного, чаще всего невозможно.

Между тем проверить это легко. У легиона есть единственный действующий сайт, адрес которого

можно найти в статье «Википедии», а в разделе «Контакты» — единственный телеграм-бот для заявок «по вопросам вступления». Если адрес сайта и имя бота хотя бы на один символ отличаются от оригинальных, то перед вами фейк.

Например, в материалах дела 16-летнего школьника Арсения Турбина, который получил 5 лет колонии за расклейку листовок якобы по заданию легиона, упоминается переписка с аккаунтом *@Legionrf_bot* — на настоящем сайте подразделения такого контакта нет.

Ханипоты

Ссылки на такие фейковые боты дают сайты, мимикрирующие под настоящий сайт легиона. На это явление в августе обратил внимание живущий в Нидерландах программист Артем Тамоян.

Сайты-клоны почти полностью повторяют дизайн и контент настоящего сайта с незаметным отличием в адресе на один или несколько символов. Эти сайты можно было бы назвать фишинговыми[1], но на них

нет реквизитов для пожертвований, их единственная цель — собирать данные людей, которые ищут связи с легионом, поэтому Тамоян предпочитает термин «ханипот»[2].

Прочитав очередную новость о приговоре за участие в «Свободе России», рассказывает разработчик, он задумался, что анкеты для желающих вступить в легион — это удобный инструмент для силовиков,

который позволяет без особых усилий повысить раскрываемость по «террористической» статье.

«Это абсолютно идеальный для российских спецслужб способ заводить уголовные дела. Люди, может быть, искренне приходят, заполняют эти формы, отправляют свои данные, и у фээсбэшника на столе уже папочка с человеком и с готовым, по сути, уголовным делом», — объясняет он.

Если в телеграме поиск по запросу «Свобода России» первым выдает его официальный телеграм-канал[3],

то выдача поисковиков была замусорена ханипотами, визуально неотличимыми от настоящего сайта подразделения.

Некоторые пользователи предполагали, что сайты-клоны создает сам легион «Свобода России» — как зеркала, которые, в отличие от заблокированного официального сайта, доступны российским пользователям без *VPN*. Однако Тамоян получил от пресс-службы легиона ответ, что это не так.

«Моя личная позиция заключается в том, что люди, которые готовы брать в руки оружие и бороться с путинским режимом, заслуживают уважения. Даже если у них просто есть такое намерение, даже не доведенное до конца. Поэтому я подумал, что неплохо было бы помешать ФСБ этих людей сажать в тюрьму», — вспоминает он.

Фишинг нелегален во всем мире, в том числе и в России. Поэтому Тамоян начал рассылать провайдерам и локальным регистраторам письма

с жалобами на сайты-клоны, которые целиком копируют официальную страницу легиона.

«Я просто пишу регистратору: "Смотрите, вот этот домен, он ведет на сайт, который притворяется оригинальным сайтом, а на самом деле он фишинговый, и в этом легко убедиться. Можно зайти на "Википедию" или на официальный аккаунт в какой-либо социальной сети, где они дают ссылку на сайт". Это достаточно прозрачная и простая процедура, сомнений в том, что сайт фишинговый, возникнуть не может. Поэтому провайдеры практически сразу просто блокируют сайт за нарушение правил пользования», — объясняет разработчик.

Всего Тамоян нашел около двух десятков фейковых сайтов легиона. Практически сразу они были заблокированы провайдерами или домен-регистраторами.

След спецслужб

С уверенностью утверждать, что за сайтами-ханипотами стоят российские спецслужбы, невозможно. Но в пользу этой версии говорит сразу несколько фактов.

Во-первых, до того как Тамоян обратил внимание на проблему, выдача в *Google* и «Яндексе» кардинально отличалась: в российском поисковике ханипоты занимали первые строчки. При этом сайты-клоны не имели никакой истории упоминаний и по сути не отображались нигде, кроме выдачи «Яндекса».

Таким образом, сотрудники «Яндекса», вероятно, выводили их в топ вручную; разработчик, долго обсуждавший свою догадку с коллегами и экс-сотрудниками корпорации, говорит, что уверен в этом до сих пор.

Тамоян проверил свою гипотезу на примере другого сайта, за переписку с которым россиянам грозит уголовная ответственность: украинского проекта «Хочу жить», призывающего солдат сдаваться в плен. В отличие от сайта легиона «Свобода России», у «Хочу жить» были официальные зеркала, еще не заблокированные в России, но «Яндекс» на первом месте в выдаче все равно показывал сайт-клон. Он отличался от оригинала только ссылкой, на которую вела кнопка «Связаться с нами».

Читатели «Медиазоны» выдвинули другую версию, объясняющую разницу в выдаче между Яндексом и **Google**. Возможно, это связано не с вмешательством сотрудников, а с разницей в оформлении специальных тегов на оригинальном сайте, когда страница открывается роботами разных поисковиков. Как проверила «Медиазона», если при запросе настоящего сайта представиться роботом **Google** (задать соответствующее значение **UserAgent**), то заголовок будет содержать подробную информацию, которую поисковики используют для поднятия сайтов в выдаче.

Если представиться любым другим поисковиком, например, «Яндексом» или **DuckDuckGo**, то такой информации в заголовке не будет. Фейковые зеркала, в отличие от настоящего сайта, отдают теги для всех браузеров одинаково. Такое

> поведение сайта может влиять на его позицию в результатах поиска.

При этом после блокировки одних сайтов-ханипотов быстро появлялись другие, обратил внимание Тамоян.

«Может быть, это один человек, может быть, группа людей, но кто-то занимается этим активно, работоспособность этих сайтов реально поддерживается. Я кидаю жалобу, сайт блокируется, но покупается новый домен и так далее. Это никому не нужно, кроме российских спецслужб», — делает вывод программист.

Еще одно косвенное доказательство причастности силовиков к созданию ханипотов ему удалось получить почти случайно. Некоторые жалобы с просьбами о блокировке Тамоян адресовал администрации *CloudFlare*. В одном из ответов сервиса говорилось, что хостинг-провайдером поддельных сайтов легиона «Свобода России» была компания *Stark Industries*, которую расследователи связывали с деятельностью пророссийских хакерских групп.

«Это люди, о которых уже много известно. И известны даже конкретные имена, которые имеют прямую связь с российскими государственными службами, возможно, ГРУ или ФСБ», — говорит разработчик.

Сейчас он продолжает следить за ханипотами, но, по его словам, уже скорее в «пассивном» режиме, ведь

основная цель — убрать фейковые сайты с первых мест в выдаче поисковиков — была достигнута.

«Мне кажется, эффект получился достаточно существенный. Во-первых, самая история после твитов моих стала довольно популярной, многие об этом написали, много людей об этом узнали и, возможно, стали более осторожно подходить. Во-вторых, фээсбэшники действительно лишились первого места в выдаче, надеюсь, это усложнило им жизнь. Стоит помнить, что фээсбэшник всегда может написать сам в личку и спровоцировать дальше, поэтому вся надежда на бдительность людей. Без бдительности никак, наверное, им не помочь», — заключает Тамоян.

Редактор: Дмитрий Ткачев

Обновлено 16 октября в 21:47. Добавлена версия поведения поисковика «Яндекс», предложенная читателями «Медиазоны».

1. Фишинг — вид интернет-мошенничества. Пользователь получает ссылку, ведущую на страницу, которая внешне похожа на хорошо известный ему сайт, и вводит там свои данные.
2. «Горшочек с медом», приманка — так называют сайты, которые созданы специально, чтобы привлекать компьютерных взломщиков и собирать о них информацию.
3. Благодаря большому числу подписчиков.