Что такое доксинг?

Вы когда-нибудь писали на форуме что-то такое, о чем вам было бы неудобно говорить публично, думая, что анонимность онлайн-мира защитит вас? Лучше быть осторожным: анонимность в онлайн скорее миф.

Doxing, сокращение от «droping dox», — это онлайн-атака, в которой хакеры выкапывают личную информацию и документы, чтобы раскрыть реальные личности людей, надеющихся остаться анонимными.

Цель часто состоит в том, чтобы опозорить или запугать жертву. Хакеры могут раскрыть личность анонимного тролля на доске объявлений, например, как способ опозорить этого человека. Они могут надеяться, что этот человек потеряет работу или потеряет доверие коллег или друзей.

Вывод? Будьте осторожны с тем, что вы говорите в Интернете. Вы можете подумать, что онлайн-мир дает вам свободу говорить или печатать что угодно. Вы можете подумать, что создание поддельных личностей дает вам возможность выразить любые мнения, которые вы хотите, независимо от того, насколько они противоречивы, без какого-либо отслеживания их связей с вами.

Но Doxing атаки реальны. Трудно полностью скрыть свою личность в Интернете. Лучшая защита от doxing — это быть осторожным с тем, что вы публикуете в Интернете, и никогда не делиться личной информацией на форумах, досках объявлений или сайтах социальных сетей.

Это не всегда были онлайн атаки

Доксинг интересен тем, что, хотя сегодня это в основном онлайн-атака, это не всегда так. В статье за 2017 год Wired.com указал, что на британский офис, ведущий работу по улучшению расовых отношений, начались доксинговые атаки. Интернет не был частью этой атаки. Вместо этого ультраправые активисты разместили номер телефона чиновника в общественных туалетах по всему Лондону. Это означало, что вечера чиновника часто прерывались гневными полуночными телефонными звонками.

Этот случай показывает, что doxing не обязательно должен быть онлайн-инструментом. Доксеры могут использовать старомодные методы для раскрытия личной информации своих целей.

Конечно, теперь doxing-атаки проводить легче благодаря социальным сетям и онлайн-форумам. Проще показать личность цели большему числу людей в Твиттере, Фейсбуке, Инстаграм и других.

И доксерам не потребовалось много времени, чтобы перейти в онлайн-мир, чтобы сделать раскрытие личной информации более легкой задачей. История Wired.com указывает на канал YouTube 2006 года, который называется Vigilantes, в качестве примера ранних атак на социальные сети, основанных на доксинге. Канал Vigilantes доксировал влогеров - видеоблогеров, которых считали расистскими или ненавистными.

Исследовательский центр киберзапугивания сказал, что сегодня доксинг, обычно включает в себя кого-то, собирающего личную информацию жертв, начиная от домашних адресов и номеров социального страхования до номеров кредитных карт или информации о банковском счете, а затем распространяя их.

Какую информацию ищут доксеры?

Какую информацию ищут хакеры в ходе подобных атак? Все, что может помочь им раскрыть личность того, кто пытается остаться анонимным.

Таким образом, используя подобные атаки хакеры могут опубликовать:

- Настоящее имя
- Номер телефона
- ИНН
- Домашний адрес
- Место работы
- Номера кредитных карт
- Номера банковских счетов
- Личные фотографии
- Профили в социальных сетях

Типы доксирования

Вы можете быть удивлены тем, как легко кому-то найти информацию о вас. Это может быть еще проще, если вы проводите много времени, размещая сообщения на досках объявлений и форумах.

Может быть, вы упомянули, что впервые путешествуете по Европе. Теперь хакер знает, что ты не живешь на этом континенте. Вы можете сделать еще один пост, в котором говорится, что вы никогда не были в Азии. Теперь этот хакер может определить, что вы не живете на этом континенте.

Возможно, вы жалуетесь на высокие налоги на недвижимость. Теперь можно точно определить ваше место жительства.

Думайте о своей онлайн-активности как о крошках. Решительные взломщики могут следовать по этому пути, пока не узнают, где вы живете, ваш возраст, пол и расу. Вооружившись этой информацией, они могут постепенно определить вашу личность.

Сниффинг пакетов

Это не единственный способ, которым люди могут взломать вашу онлайн-анонимность. Опытные хакеры могут также полагаться на технологии, чтобы получить подсказки о вашей личности. Они могут обратиться к стратегии, известной как сниффинг пакетов. В этом методе Doxer перехватывает ваши интернет-данные, ища все, от ваших паролей, номеров кредитных карт и информации о банковском счете до старых сообщений электронной почты.

Doxers осуществляют это, подключаясь к онлайн-сети, взламывая меры безопасности, а затем извлекая данные, поступающие в сеть и из нее.

Протоколирование IP

Еще один страшный трюк? Doxers также может использовать IP-логгеры. Регистраторы IP-адресов прикрепляют код, который жертвы не видят, к сообщению электронной почты. Как только жертвы открывают эти электронные письма, код отслеживает их IP-адреса и отправляет их обратно в IP-регистратор. Это легко дает doxer быструю информацию о вас.

Обратный поиск сотового телефона

Что хакеры могут узнать о вас, если у них есть номер вашего мобильного телефона? Много, благодаря таким услугам, как Whitepages. Эти услуги обратного поиска телефона позволяют вам ввести номер мобильного телефона или любой номер телефона, чтобы узнать личность человека, которому принадлежит номер.

Но это не просто ваше имя, которое люди могут узнать из такой услуги. Поиск на сайте Whitepages может также найти ваш текущий и предыдущий адреса. Хакеры также могут использовать обратный телефонный поиск для поиска ваших записей, финансовых записей и т.д.

Такие сайты, как Whitepages, взимают плату за предоставление чего-либо за пределами города и штата, связанных с номером мобильного телефона. Тем не менее, желающие заплатить могут получить много личной информации о вас с вашего мобильного телефона. Будьте осторожны с этим номером: не оставляйте его на сайтах социальных сетей, форумах или досках объявлений.

Преследование в социальных сетях

Многие докеры изучают аккаунты в социальных сетях, чтобы найти личную информацию о своих целях. Люди не только охотно делятся личной информацией на таких сайтах, как Twitter, Facebook и Instagram - например, об отпусках, новых вакансиях и переездах, - они также предоставляют множество ключевых фактов о себе при регистрации на этих сайтах, информацию, которую могут раскрыть определенные злоумышленники. Вот почему так важно сохранить вашу личную информацию в социальных сетях.

Рассмотрим Facebook. Когда вы регистрируетесь на сайте, у вас есть возможность предоставить все, начиная от даты вашего рождения до вашей средней школы и колледжа. Будьте внимательны при регистрации на сайтах социальных сетей: не заполняйте эти поля. Оставьте их пустыми.

И при публикации в социальных сетях, не будьте слишком точны в том, что вы делаете или где вы были. Подумайте о том, чтобы сделать ваши учетные записи в социальных сетях приватными, чтобы ваши сообщения могли просматривать только определенные люди.

Является ли doxing незаконным?

Вы знаете, что doxing может разрушить жизнь целей. Но является ли эта практика незаконной? Doxing не является незаконным, если раскрытая информация является частью публичной записи. Это включает в себя записи об аресте, свидетельства о браке, серьезные нарушения правил дорожного движения и записи о разводе. Если кто-то публикует эти записи, даже без вашего согласия, они не делают ничего противозаконного.

Doxing может быть незаконным, если кто-то публикует информацию, которой нет в публичной записи, такую как данные вашего банковского счета, номера кредитных карт или свидетельство о рождении. Doxers действуют незаконно, когда они получают доступ к этой информации и публикуют ее.

Впрочем, Doxing всегда неэтичен, даже если преступники торгуют только информацией, доступной для общественности.

Что делать?

Хотя нет никакого способа гарантировать, что ваши данные никогда не будут использованы против вас, есть несколько стратегий, которые вы можете использовать, чтобы уменьшить шансы. Главное - помнить о том, что вы публикуете на сайтах социальных сетей и на досках объявлений. Вот несколько советов:

- **Не переоценивайте:** не переоценивайте в социальных сетях, онлайн-форумах и на досках объявлений. Совместное использование личной информации может легко дать доксеру слишком много работы.
- **Измените настройки конфиденциальности:** сделайте свои публикации на сайтах социальных сетей приватными, чтобы их могли просматривать только избранные люди.
- **Не предоставляйте личную информацию.** При регистрации в социальных сетях не указывайте личные данные, такие как дата вашего рождения, родной город, средняя школа или информация работодателя.
- **Используйте VPN:** регистрация в виртуальной частной сети или VPN может помочь защитить вашу личную информацию от доксеров. Когда вы подключаетесь к Интернету, сначала войдя в VPN, ваш реальный IP-адрес будет скрыт. Это означает, что хакеры не смогут найти этот адрес для вашего местоположения или другой идентифицирующей информации.
- **Будьте внимательны при фишинг-письмах:** Doxers могут использовать фишинг-мошенничество, чтобы заставить вас раскрыть ваш домашний адрес, номер социального страхования или даже пароли. Будьте осторожны, когда получаете сообщение, которое предположительно приходит от банка или компании, выпускающей кредитные карты, и запрашивает вашу личную информацию. Финансовые учреждения никогда не будут запрашивать эту информацию по электронной почте.
- **Некоторая информация никогда не должна передаваться:** дайте клятву никогда не публиковать в Интернете определенные фрагменты информации, такие как номер социального страхования, домашний адрес, номер водительского удостоверения и любую информацию, касающуюся банковских счетов или номеров кредитных карт. Помните, что хакеры могут перехватывать сообщения электронной почты, поэтому вы не должны включать личные данные в свои.

Что делать, если вы все же стали жертвой? Вот несколько шагов, которые вы можете предпринять, чтобы ограничить ущерб.

- **Сообщите об этом:** сообщите об атаке на платформы, на которых была размещена ваша личная информация.
- **Привлечение правоохранительных органов:** если доксер угрожает вам лично, обратитесь в местное отделение полиции.
- **Документируйте, что произошло:** сделайте снимки экрана или загрузите страницы, на которых была размещена ваша информация. Это может помочь правоохранительным органам или другим органам, которые могут расследовать случаи доксирования.
- **Защитите свои финансовые счета.** Если доксеры опубликовали номер вашего банковского счета или номер кредитной карты, немедленно сообщите об этом в ваши финансовые учреждения. Ваш поставщик кредитных карт, скорее всего, отменит вашу карту и отправит вам новую. Вам также необходимо изменить пароли для вашего онлайн-банка и счета кредитной карты.
- **Увеличьте настройки конфиденциальности.** Настройте параметры конфиденциальности в своих профилях в социальных сетях, чтобы предотвратить отслеживание.

Оригинал