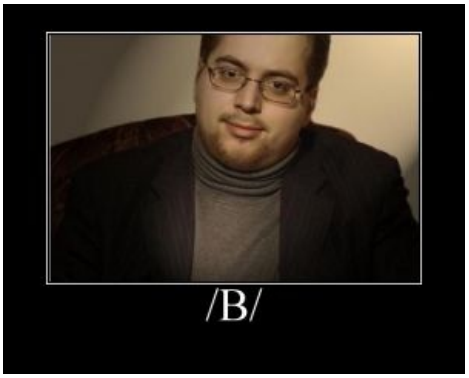
Анонимность — Urbanculture

Криптоконспирология



Анонимность — понятие, подразумевающее невозможность установления личности или авторства определенного произведения: в частности поста, статьи, комментария. Анонимность берет свое начало вовсе не с момента появления этих ваших интернетов, а с момента возникновения культуры как таковой. Большая часть произведений, которую мы называем фольклером, есть творчество анонимусов. Народные песни, частушки, былины и сказания — все это творчество анонимусов.

Причины появления и развития

Как ни парадоксально первые анонимные произведения появились не в попытках спастись от цензуры, а просто от человеческой забывчивости и отсутствия понятия авторства. Наскальная живопись, народные песни имели автора совсем короткий промежуток времени, пока кто-то помнил имя автора. Понятия авторского права еще не существовало, в виде законов оно появилось вместе с книгопечатанием. Хотя боролись за увековечивание своего имени известные авторы гораздо раньше. С момента появления религиозной и политической цензуры, преследования за высказывания против определенных сил анонимными произведения делались специально. Просто не подписать книгу или статью, папирус, оставив читателя гадать об авторстве стало нормой. Сетевая анонимность — явление зародившееся также спонтанно, как и анонимность ранних произведений культуры. До распространения элементов цензуры на компьютерную сеть особых причин искусственно оставаться анонимом не было. Но невозбранное копирование как и в народном творчестве часто приводило к утрате упоминаний об авторстве — просто всем похуй, это интернет (фидонет).

Слежка в сети и вынужденная анонимность

В современном мире понятие анонимности стало известно большинству благодаря попыткам цензурировать содержимое и узнать о пользователе интернета больше, нежели он пожелал рассказать. В связи с этим стали возникать средства обеспечивающие анонимность по желанию пользователя. Но это борьба технологий при этом ни одна из сторон не знает возможности другой и не знает сеть в совершенстве. При этом интернеты глобальны, то есть каждый кусок подчинен тем законам, которые действуют в стране расположения серверов и регистрации доменного имени. За счет разницы законов, забивания болта на выполнение тех или иных требований, наличия и совершенствования софта по обеспечению анонимности, таковая процветает. Но следует помнить: *абсолютной анонимности не существует, все тайное рано или поздно станет явным*. Все зависит от заинтересованности и комплекса применяемых мер. В задачу обеспечения анонимности должно входить четкое понимание противника, его возможностей и наличия мер противодействия ему.

Способы достижения анонимности

Таковых множество, надеяться на один способ глупо. В первую очередь нужно понять, кому не должны достаться сведения. Затем выбирать из предложенных и прочих способов.

- Использование прокси или VPN. Позволяет сменить ip-адрес, который останется в логах сервера, на котором расположен сайт. При этом владелец видит адрес сервиса, обеспечивающего анонимность. То есть может потребовать предоставить сведения о сервисе. Использование прокси и виртуальных частных сетей в других странах оправдано, если сервис не предоставляет каких-либо сведений по запросам от частных лиц и организаций. Использование такого рода сервисов для борьбы с государством или международными корпорациями часто не оправдано. Сведения могут купить, запросить через местные правоохранительные органы, либо выкрасть.
- Использование анонимных сетей. Если в задачи сервиса входит именно достижение высокого уровня анонимности, он будет являться более надежным средством, нежели прокси. В таких сервисах используется цепочка серверов, при этом они владеют только некоторой частью информации об отправителе и получателе, в большинстве случаев пропускают через себя шифрованный траффик. Тогда преследователю придется пройти по всей цепочке. Большая часть серверов в этой цепочке должна принадлежать частным лицам, поставившим ту же задачу, что и первый пользователь и не сотрудничать с представителями атакующего. Так При использовании TOP и I2P каждый пользователь является посредником при передаче траффика. При этом большинство из них по общепринятому мнению делают это добровольно, не в целях раскрытия данных других пользователей. Использование такого рода сервисов позволяет создавать цепочки прокси, отследить которые достаточно сложно.
- Использование открытого и популярного программного обеспечения. Каждая программа, с помощью которой мы получаем сведения из сети может иметь определенный уникальный отпечаток:

фингерпринт. Он состоит из версии, установленных дополнений, размера окна или разрешения экрана, куков определенных сервисов. То есть по отпечатку браузера можно сильно сузить круг пользователей, которые могли бы оставить анонимное сообщение. При использовании той же программы для незащищенного доступа к сервисам сети, можно установить круг подозреваемых. Чем более популярен браузер, тем шире этот круг, то есть труднее вычислить автора. Открытый исходный код программ позволяет проверить, не отправляет ли программное обеспечение сведений кому-либо еще, кроме непосредственного получателя, нет ли возможности получить доступ к истории посещенных сайтов.

- Использование псевдоанонимных личностей. Большая часть движков сайтов предусматривает регистрацию пользователей. Когда ее не избежать, на помощь приходит создание уникального сетевого персонажа. При этом можно выбрать рапространенный в данной тусовке ник, регистрироваться через средства обеспечения анонимности и пользоваться ими всегда. Также следует помнить о сведениях, предоставляемых добровольно с этого аккаунта. При совпадении таких сведений с данными другого пользователя атакующий может найти соответствие. Так указание небольшого города в скрытосетях может достаточно точно установить пользователя. Причина проста: в Усть-Пердюйске всего 3 пользователя I2P, 2 из них интересуются детской порнографией и не интересуются политикой. То есть автором политического вброса может стать только третий. Вычислить его можно по небольшому объему траффика, остальные качают ЦП, их траф в скрытосетях измеряется гигабайтами. Дальше вычислить пользователя может даже провайдер, не говоря уже о полиции. Псевдоанонимная личность или не имеет адреса вообще или живет в известном ему крупном городе, где пользователей скрытосетей много.
- Использование надежной криптографии. Позволит уменьшить количество пользователей, которые будут являться получателями информации. То есть любые сведения, которые должны попасть в одни руки стоит шифровать. Тут есть и серьезный минус — идентификация по ключу. При попадании ключа в сеть незащищенным способом можно однозначно установить личность его владельца. То есть использование криптографии даст возможность сохранить анонимность только при аккуратном использовании.

См. также

Примечания