Наиболее популярные антивирусные программы [Электронный ресурс]. – Режим доступа: http://www.tagac.ru/270– Дата доступа: 07.03.2020.

Маскировка IP-адреса. Использование специализированных программ и сервисов

Хацкевич К.С.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

IP-адрес(*Internet ProtocolAddress, айпи адрес*) – это уникальный числовой идентификатор конкретного устройства в составе компьютерной сети, построенной на основе протокола TCP/IP. Для работы в Интернете требуется его глобальная уникальность. Для частной сети достаточно, чтобы были исключены совпадения в локальном пространстве.

настоящее время тема анонимности в интернете очень актуальна. Причин для этого много,но основная – это безопасность, так как существует очень много способов узнать личную информацию о пользователе по его IP-адресу или другим характеристикам интернет-соединения. На какой бы сайт не зашёл пользователь в интернете, он везде оставляет свои «следы», в виде информации о типе операционной системы, обозревателя исамое главное, свой IP и MAC адрес. При совокупности всех этих данных, определить его месторасположение очень просто. Также возможно проследить все его действия, совершённые, например, с домашнего компьютера. Владелец любого удалённого сервера или сайта в Интернете может точно определить, что пользователь делал на его сайте.

Существуют следующие способы маскировки (скрытия) IP-адреса:

1. *VPN-технологии* (*VirtualPrivateNetwork*) – технологии, позволяющей подменить IP-адрес без использования прокси-сервера. Внешне VPN-соединение мало чем отличается от подключения к обычной локальной сети: приложения вообще не почувствуют разницы и поэтому без какой-либо настройки будут использовать его для доступа в интернет. Когда одно из них захочет обратиться к удалённому ресурсу, на компьютере будет создан специальный GRE-пакет (GenericRoutingEncapsulation, общая инкапсуляция маршрутов), который в зашифрованном виде будет отправлен VPN-серверу. VPN-сервер, в свою очередь, этот пакет расшифрует, разберётся, в чём его суть (запрос на закачку какой-либо HTTP-страницы, просто передача данных и т.д.), и выполнит от своего лица (то есть «засветит» свой IP) соответствующее действие. Далее,

получив ответ от удалённого ресурса, VPN-сервер поместит его в GRE-пакет, зашифрует и в таком виде отправит обратно клиенту.

Прокси-сервер (от англ. proxy – «представитель, уполномоченный») – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Анонимно прокси-сервер (anonymous http proxy server) исполняет роль посредника между пользователем и конечной целью его запроса. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер подключается к указанному серверу, получает ресурс у него и передаёт клиенту.

Программы-анонимайзеры (*anonymizer*), которые выглядят как обычный поисковик, только вместо слов/фраз в них нужно вводить URL-адрес того сайта, который необходимо посмотреть. Программы-анонимайзеры также используют анонимные прокси-серверы, но поиск, проверку, подключение к анонимным прокси-серверам выполняют самостоятельно и снабжены собственным web-интерфейсом.Недостатки использования анонимайзеров: может существенно уменьшиться скорость загрузки web-страниц; на некоторых анонимайзерах не исключены проблемы с отображением русскоязычного текста; сейчас практически невозможно отыскать бесплатный прокси-сервер.

SSH-туннелинг – сетевой протокол, позволяющий производить удалённое управление компьютером и передачу файлов. Использует алгоритмы шифрования передаваемой информации. SSH-туннелинг можно рассмотреть в качестве дешёвой замены VPN. Принцип данной реализации следующий: при пересылке через SSH-туннель незашифрованный трафик любого протокола шифруется на одном конце SSH-соединения и расшифровывается на другом.

TOR (*The Onion Router*) – система, позволяющая пользователям соединяться анонимно, обеспечивая передачу пользовательских данных в зашифрованном виде. С помощью Tor пользователи могут сохранять анонимность при посещении web-сайтов, публикации материалов, отправке сообщений и работе с другими приложениями, использующими протокол TCP.

Пользователи сети Tor запускают onion-proxy на своёмкомпьютере, данное программное обеспечение подключается к серверам Tor, периодически образуя виртуальную цепочку сквозь сеть Tor, которая использует криптографию многоуровневым способом (аналогия с луком – англ. onion). Каждый пакет, попадающий в систему, проходит через три различных сервера (нода). Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй,

и, в конце, для первой. Когда первая нода получает пакет, она расшифровывает «верхний» слой шифра и узнаёт, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение onion-proxy предоставляет SOCKS-интерфейс. Программы, работающие по SOCKS-интерфейсу, могут быть настроены на работу через сеть Tor, который, мультиплексируя трафик, направляет его через виртуальную цепочку Tor, что в конечном итоге позволяет обеспечивать анонимный сёрфинг в сети.

Socks-протокол (*socks proxy server*) – самый надёжный на данный момент способ сокрытия IP-адреса. Принцип действия напоминает принцип действия прокси-серверов и выглядит так: socks-сервер принимает данные от компьютера пользователя, отправляет их на web-сервера, потом перенаправляет ответную информацию обратно к пользователю. Но есть и принципиальные отличия технологии socks-серверов и прокси-серверов: «общение» клиентского компьютера и socks-сервера происходит не по общепринятым, а по специальным протоколам (socks4, socks5 и т. д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, socks-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. Таким образом, ни один сервер никогда «не догадается», что отправляет данные не конечному пользователю, а только посреднику в лице socks-сервера. К тому же работать с технологией socks очень удобно.

К наиболее популярным специализированным программам и сервисам для обеспечения анонимности пребывания в сети Интернет относятся:

1) Complete Anonymous Web Surfing – программа, позволяющая скрыть IP-адрес пользователя при просмотре web-страниц, устанавливая подключение через один из имеющихся в наличии прокси-серверов.

2) FreeCap – программа для прозрачной переадресации подключений через SOCKS-сервер программ, которые не имеют родной поддержки SOCKS-прокси.

3) HideMyAss – сервис, обеспечивающий анонимность в Сети, скрывая пользовательский IP-адрес;

4) HideMy IP – программа для анонимного сёрфинга в интернете, позволяющая скрыть IP-адрес компьютера и защититься от атак хакеров.

5) SocksChain – программа, позволяющая работать через цепочку SOCKS или HTTP-прокси.

6) Steganos Internet Anonym – программа, которая строит длинные цепочки прокси, надёжно скрывая пользовательский IP-адрес, а также блокирует все скрипты (cookies, Active-X и Java-скрипты), способные раскрыть информацию о пользователе и его местоположении владельцам посещённых сайтов.

Surf Anonymous Free – программа, которая защищает пользователя от небезопасных сайтов, предотвращает отслеживание и мониторинг сетевого трафика.

Tor Project – приложение, представляющее программный комплекс для обеспечения анонимного статуса при сёрфинге сайтов.

TryCatchMe – сервис, который поможет зайти на заблокированный администратором сайт и сохранить практически все конфиденциальные данные при себе.

Чёрный майнинг. Как работают вирусы-майнеры. Защита компьютеров от криптовирусов

Чепикова Д.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Сегодня понятие «майнинг» уже успело засветиться на страницах узкопрофильных экономических или IT-изданий. ***Майнинг*** (от англ. mining – добыча полезных ископаемых)– деятельность по созданию новых структур для обеспечения функционирования криптовалютных платформ[1].

Везде, где существуют правила, найдутся те, кто хочет их обойти или нарушить. Мир криптовалют не является исключением, потому чтосовременные майнеры уже разработали методы,которые позволят получать цифровую валюту посредством компьютеров, принадлежащих другим людям. Так появился *чёрный майнин*г – незаконная добыча криптовалюты.

Есть два вида чёрного майнинга, подразумевающие использование чужих ПК: майнинг через браузер и вирусный майнинг.

Майнинг через браузер.

Если пользователь последует по предложенной ему ссылке на каком-либо сайте, есть возможность, что его ПК войдет в сеть по добыче криптовалют. Допустим, существует веб-сайт, который решил майнить криптовалюту на ресурсах посетителей. Сайт начинает использовать мощности пользовательских видеокарт, в то время как они, ничего не подозревая, продолжают пользоваться сайтом. Хотя выработка при таком майнинге не особо большая, злоумышленники берут количеством посетителей. Первыми за таким «экспериментом» поймали торрент-трекер Piratebay. Заметили неладное сами пользователи сайта – при посещении торрента нагрузка на процессоры увеличивалась практически до ста процентов.