УДК 004.056.52

СПОСОБЫ ОБНАРУЖЕНИЯ ИСПОЛЬЗОВАНИЯ ПОЛЬЗОВАТЕЛЕМ VPN СОЕДИНЕНИЯ

Старун И.Г. (Университет ИТМО), **Гурьев Н.А.** (Университет ИТМО)
Научный руководитель – Югансон А.Н.
(Университет ИТМО)

Аннотация. В докладе рассмотрены способы обнаружения использования пользователем VPN соединения, применение которых не требует знания персональных данных пользователя и прочей личной информации. Даны рекомендации по их применению.

Введение.

В настоящее время использование VPN соединения становится все более популярным среди пользователей сети Интернет. Одной из основных целей применения этой технологии является достижение анонимности, чем, в числе прочих, пользуются злоумышленники при совершении киберпреступлений. В связи с этим актуальным становится вопрос обнаружения пользователей, использующих средства анонимизации. Данная процедура может быть применена, например, при первичном сигнатурном анализе пользователей интернет-ресурса с целью определения потенциальных злоумышленников. При мониторинге активности необходим повышенный контроль за такими посетителями ресурса. На данный момент обнаружение пользователей, использующих VPN, применяется администраторами информационной безопасности Интернет-ресурсов хаотично и неполноценно, так как отсутствует достаточная научная база для совершения проверки.

Основная часть.

Для обнаружения пользователей, использующих VPN соединение, возможно применение следующих способов, не требующих знания персональных данных пользователей и прочей личной информации (сообщений, истории посещений ресурсов и т. д.):

- проверка адреса провайдера на наличие в базе адресов VPN;
- проверка страны принадлежности адреса провайдера и IP-адреса на нетипичность для пользователей конкретного ресурса;
- сравнение временных зон браузера и IP-адреса пользователя;
- сравнение языков браузера и IP-адреса;
- обнаружение туннеля путем двустороннего пинга;
- проверка цифрового отпечатка fingerprint на наличие нестандартных значений MTU и MSS;
- проверка на утечку DNS серверов, используемых пользователем, для их сравнения с DNS-серверами VPN сервисов;
- анализ открытых портов на совпадение с портами протоколов VPN.

Для достижения наибольшей эффективности проверки на использование VPN рекомендуется одновременно применять несколько способов обнаружения.

Выводы.

В качестве проверки эффективности предложенных способов проверки было проведено их испытание на пользователях, использующих 9 различных VPN сервисов: Tunnel Bear, Hotspot Shield, VPN Gate, Nord VPN, Express VPN, PrivateVPN, Ultra VPN, Cyber Ghost, Surfshark. Во всех случаях как минимум один способ обнаружения дал положительный результат. Таким образом, одновременное применение рассмотренных способов обнаружения использования VPN соединения позволяет выявить большую часть пользователей VPN сервисов.

Предложенная методика рекомендуется к внедрению для использования в автоматическом режиме при первичном анализе посетителей Интернет-ресурсов. Это

позволит выявить пользователей, требующих повышенного уровня мониторинга их активности. Применение рассмотренных способов в ручном режиме является менее предпочтительным и может быть использовано в отдельных случаях: например, при тестировании, оценке и сравнении VPN сервисов.