# МЕХАНИЗМ ВЫЯВЛЕНИЯ ИСПОЛЬЗОВАНИЯ АНОНИМНОГО ДОСТУПА В ИНТЕРНЕТ ЧЕРЕЗ СЕТЬ TOP ИЗ КОРПОРАТИВНОЙ СЕТИ КОМПАНИИ И БЛОКИРОВКИ ТАКОГО ДОСТУПА

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Бондарь К. В.*

*Сечко Г. В. – канд. техн. наук, доцент*

Рассматриваются вопросы выявления использования анонимного доступа в интернет из корпоративной сети компании и блокировки такого доступа.

Анонимные сети — это компьютерные сети, созданные для достижения анонимности в Интернете и работающие поверх глобальной сети [1-3]. Специфика таких сетей заключается в том, что разработчики вынуждены идти на компромисс между степенью защиты и лёгкостью использования системы, её «прозрачностью» для конечного пользователя. Важен также аспект сохранения анонимности и конфиденциальности при условии воздействия методов социальной инженерии или какого-либо давления на оператора сервера. Многоуровневое шифрование и распределённый характер анонимных сетей, устраняя единую точку отказа и единый вектор атак, позволяют сделать перехват трафика или даже взлом части узлов сети не фатальным событием. За анонимность пользователь расплачивается увеличением времени отклика, снижением скорости, а также большими объёмами сетевого трафика.

Из-за своей универсальности использовать анонимный доступ (в обход корпоративной защиты) на рабочем месте очень просто. Этим и пользуются некоторые недобросовестные сотрудники различных компаний, не ставя в известность об этом руководство. Таким образом, анонимный доступ в интернет несет, с одной стороны, благо для анонимных сотрудников-пользователей, тратящих своё оплаченное работодателем рабочее время на несанкционированный работодателем доступ в интернет (при санкционированном доступе нет нужды посещать интернет анонимно), а с другой стороны наносит явный ущерб работодателю, у которого они работают. В первую очередь этот ущерб определяется угрозой не только бесконтрольно получать доступ к закрытым ресурсам компании-работодателя, но и в обход систем защиты информации в компании передавать конфиденциальную информацию конкурентам своего работодателя, поскольку известно, что наиболее дешёвым способом получения конфиденциальной и даже секретной информации конкурента является вербовка его недобросовестных сотрудников. В связи с этим анонимные сети рассматриваются как угроза для бизнеса.

Наиболее известная и развитая среди существующих анонимных сетей — сеть Tor [1]. Первая практическая реализация сети этого типа в рамках проекта Free Haven появилась в 2002 году. Как результат развития первой реализации стало второе поколение этой сети — проект Tor. Суть его в том, что клиентская сторона формирует цепочку из трёх произвольно выбранных узлов сети Tor. Среди них есть входной (entry node) по отношению к клиенту узел и выходной (exit node). Сеть Tor при этом функционирует как шлюз между клиентом и внешней сетью. Каждый Tor-сервер «знает» о предшествующем ему и последующем, но не более того, а замыкающие узлы не знают, кто находится на другой стороне канала и кто инициировал соединение. Отсутствие логической связи между отправителем и сообщением гарантирует надёжную анонимность [2-3].

В докладе для выявления использования анонимного доступа в интернет из корпоративной сети компании предлагается механизм, позволяющий не только выявлять использование анонимного доступа, но и блокировать такой доступ. Механизм базируется на том, что Tor имеет тысячи точек входа. Выявив каждую из этих точек и блокируя доступ к ним на центральном маршрутизаторе, можно полностью ограничить использование клиентом корпоративной сети. Помимо этого на основании сопоставления ip адресов будет обнаружен и конечный пользователь, решивший воспользоваться анонимным доступом в сеть. Для начала мы получаем список Tor хостов и записываем их в файл при помощи команды tcpdump -n -i fxp0 src 195.12.66.1 -w FILE_NAME. Следующим шагом будет выделение из полученного списка строк адресов и добавление их в черный список для блокировки этих адресов на маршрутизаторе компании [2-3].

Предлагаемый механизм выявления использования анонимного доступа в интернет через сеть Tor из корпоративной сети компании и блокировки такого доступа содержит ряд команд и скриптов, подробно анализируемых и обсуждаемых в докладе

Список использованных источников:

1. Анонимные сети [Электронный ресурс]. – Электронные данные – Режим доступа: http://ru.wikipedia.org/wiki/ – Дата доступа: 05.01.2014.
2. Бондарь К.В. Алгоритм работы и варианты блокировки сети TOR // 49-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 4 мая 2013 года). – Минск: БГУИР, 2013. – 91 с. с ил. – С. 62
3. Бондарь К.В. Блокировка анонимного доступа в интернет для корпоративной сети // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 212-213.