АЛГОРИТМ РАБОТЫ И ВАРИАНТЫ БЛОКИРОВКИ СЕТИ TOR

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

Бондарь К. В.

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

Рассматривается способ блокировки одной из самых популярных систем анонимного доступа к сервисам интернета – сети Tor. Для ограничения доступа к сети и предотвращения бесконтрольной утечки конфиденциальных сведений компании предлагается специальная команда, которая позволяет получить чистый список ip адресов всех узлов системы, без большого объёма технической информации, такой как версия сети, корневые сервера, дата последнего обновления узлов, версии клиентских и серверных приложений, публичный ключ шифрования и др.

Подразделения, занимающиеся защитой информации в компаниях, вынуждены постоянно искать все новые и новые способы защиты от растущего количества программных средств и систем, позволяющих пользователям корпоративных сетей обходить средства защиты, используемые в организации. В одном случае данные программные средства и системы могут быть использованы для доступа к контенту сети интернет, к которому по распоряжению руководства доступ был ограничен, а в другом – для передачи конфиденциальной информации. Если первое относительно безобидно, хотя тоже несет некоторую угрозу проникновения вирусов и спама в сеть компании, то во втором случае бесконтрольная утечка конфиденциальных сведений может привести к серьезным убыткам.

Рассмотрим способ блокировки одной из самых популярных систем анонимного доступа к сервисам интернета – сети Tor. Изначально Tor была предназначена для анонимного доступа к веб-сайтам, для публикации материалов и отправки сообщений. Однако есть и другой взгляд на Tor – взгляд как на систему-инструмент хищения конфиденциальной информации компании, оставаясь при этом в тени. Особенно опасной эту системы делает то, что для своей работы она не требует администрирования прав на компьютере и может быть запущена с флэш-накопителя.

Принцип действия системы заключается в том, что пакеты с информацией поступают не напрямую к конечному узлу, а только после прохождения через специальные анонимные прокси-сервера: как правило, в цепочке системы Tor их три. При этом используется тройное шифрование. Анонимность достигается тем, что каждый узел в цепочке знает только адрес предыдущего и последующего узла, второй сервер не будет знать кто инициировал запрос и куда в итоге он попадет, т.к. эта информация проходит через него в зашифрованном виде.

С первого взгляда, может показаться, что если доступ в сеть интернет в организации уже реализован через прокси-сервер, то бояться нечего. Но Tor замечательно может работать через прокси-сервер компании, в этом-то и заключается проблема. Ему не нужны специфические порты, доступ через которые можно было бы ограничить, а по понятным причинам блокировать порт, через который вся организация выходит в сеть интернет, нельзя.

Для решения указанной проблемы было решено попытаться осуществить блокировку адресов тех самых промежуточных прокси-серверов, которые использует система. Для этого необходимо получить список всех узлов. Списки промежуточных узлов хранятся в открытом виде и обновляются по мере появления новых узлов. Список ip адресов активных узлов можно загрузить по адресу http://128.31.0.34:9031/tor/status/all.

Но там находится не только сами адреса, но и большой объём технической информации, такой как версия сети, корневые сервера, дата последнего обновления узлов, версии клиентских и серверных приложений, публичный ключ шифрования и др. Но важно то, что названных узлов в списке в среднем около четырех тысяч, а вручную извлекать их не совсем комфортно. В связи с этим встала задача каким-то образом автоматизировать процесс получения списка ip адресов из огромного массива данных. Для этого была специальным образом сформирована команда:

```
wget 128.31.0.34:9031/tor/status/all -q -O - | grep -E '^r' | awk '{print $7}' | sort | uniq > tor.txt
```

В итоге выполнения этой команды несложно получить чистый список ip адресов всех узлов системы Tor, который будет в дальнейшем использоваться для ограничения доступа.

В докладе предлагаются также скрипты, которые создают правило, сбрасывающее все пакеты, которые содержат у себя в теле данные для доступа к несанкционированному интернету. При применении этих скриптов никто из сети организации не сможет использовать Tor для доступа к сервисам интернета. В сети существуют Tor мосты, ip адреса которых нигде не публикуются. С этих мостов клиент может загрузить новый список узлов сети, которые сразу же начинает использовать. Для предотвращения такой возможности в докладе предлагаются скрипты для добавления строк в конфигурационный файл планировщика задач Cron.

Список использованных источников:

1. Коллективный блог для публикации новостей, связанных с информационными технологиями [Электронный ресурс]. – Режим доступа: http://www.habrahabr.ru. – Дата доступа 15.04.2013.

2. Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://www.wikipedia.org. – Дата доступа 15.04.2013.