Trojan.Rbrute или как удалить вирус в роутере?!

Как бы это дико не звучало, но есть вирусы, которые заражают не компьютеры, не планшеты или смартфоны — а ADSL-модемы и роутеры. Казалось бы — зачем? На модеме не хранятся данные банковской карты, нет логинов или паролей в соцсети и иные онлайн-сервисы. На самом деле, получив доступ к роутеру, злоумышленники могут перенаправить запросы на своих DNS-серверы, а оттуда — уже на поддельные сайты с которых Вам предложат скачать «важное» обновление браузера или антивируса. Заражению подвержены почти все устройства.

Симптомы заражения устройства:

— Индикатор «Интернет» горит, но доступа на большинство страниц нет;
— Вместо поисковиков и знакомых страниц открываются непонятные сайты;
— Компьютер не получает IP-адрес от роутера по DHCP. (IP присваивается из подсети Microsoft вида 169.254.xxx.xxx).

Как работает вирус:
Всё начинается с того, что Ваш компьютер или ноутбук инфицируется вирусом Win32.Sector, который уже скачивает и запускает Trojan.Rbrute который, в свою очередь, начинает поиск в сети роутеров и подбор пароля. В случае удачного результата — он подменяет в конфигурации роутера адреса DNS-серверов на свои. Затем все компьютеры, подключенные к нему попадают на специальную страницу, с которой скачивается Win32.Sector.

Как удалить вирус Trojan.Rbrute из роутера?

Процесс лечения прост:

1. На задней панели роутера находим кнопку Reset и зажимаем её на 10-15 секунд, до тех пор, пока устройство не моргнет всеми индикаторами и не уйдет в перезагрузку. Таким образом Вы Сбросите модема на заводские настройки.
2. Заходим в веб-интерфейс и меняем пароль на доступ со стандартного «admin» на какой-нибудь свой. Желательно посложнее.
3. Заново настраиваем подключение к сети Интернет и проверяем доступ.
4. **Очень желательно в дальнейшем!** С официального сайта производителя модема скачиваем последнюю версию прошивки для Вашей аппаратной версии(которую) и обновляем ПО. В последних версиях прошивки производитель скорее всего закрыл данную проблему.
5. После этого скачиваем последнюю версию антивирусного сканера DrWeb CureIT (http://www.freedrweb.com/cureit/?lng=ru) и проверяем им всю систему.
Последний пункт надо сделать обязательно, чтобы ни вирус-носитель Win32.Sector, ни сам Trojan.Rbrute не остались на жестком диске.