УДК 004.056:004.738.5

студентка О.В. Червоная
ГВУЗ «Национальный горный университет»

ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КОРОТКИХ ССЫЛОК

В работе рассмотрены сферы применения коротких ссылок, указаны их преимущества и недостатки. Описаны возможные уязвимости и атаки, а также методы защиты от них. Проанализирован общий уровень безопасности использования коротких ссылок.

На сегодняшний день короткие ссылки стали нормой для социальных сетей, таких как Facebook, Vk, Twitter. Несколько лет назад толчок этому тренду дал сервис Tinyurl.com, а с повсеместным распространением Twitter и его ограничением в 140 символов, использование сокращенных URL сильно шагнуло вперед.

Сама концепция сокращенных ссылок удобна и практична. Помимо изначально понятного преимущества, связанного с уменьшением количества вставляемых в запись символов, большинство сервисов Shorten URLS также позволяют просматривать статистику кликов и степень распространения пользовательской ссылки.

Однако, в любом положительном инструменте всегда изначально заложена возможность его использования не во благо. Учитывая тот факт, что сокращение ссылок уже вышло за рамки социальных сетей и переместилось на сайты и блоги, все чаще пользователи жалуются, что под видом сокращенной ссылки скрываются опасные и нежелательные для посещения сайты [1].

Одной из самых главных проблем сокращенной ссылки является то, что пользователь не может увидеть куда в действительности она ведет. Таким образом, подобный функционал может использоваться злоумышленниками: сайты, пытающиеся установить троянские программы и черви на ваш компьютер при их первом же открытии ресурса, попытки импортировать в систему специальные фильтры для Gmail, фишинг и т.д. Особо распространенными стали взломы кошельков Webmoney [4].

В качестве защиты можно использовать принципы пассивной безопасности и переходить исключительно по тем ссылкам, которые предоставлены пользователями, которым вы доверяете, а также не переходить на сайты с настораживающими названиями и не открывать ссылки от незнакомых людей. Однако, нужно учитывать, что в том же Twitter не все пользователи, делая «ретвит», обязательно проверяют, куда ведет ссылка и переходят по ней. Срабатывает обратная сторона того самого эффекта доверия: если я знаю этого пользователя, от него не должно быть ничего плохого, следовательно, можно просто «ретвитнуть» сообщение на основании темы, не читая.

Но даже в том случае, если пользователь уже перешел по этой ссылке, но его антивирус не заблокировал угрозу, его компьютер будет инфицирован, а сам пользователь об этом не узнает и распространит вирус дальше.

Как же бороться с данной проблемой не делая ручную проверку каждой ссылки на каждом сайте? Для этого можно использовать плагин для Firefox под названием «Long URL Please». Он позволяет в автоматическом режиме, при загрузке страницы, преобразовывать короткие ссылки, созданные с помощью большинства популярных сервисов, в оригинальные URL. Плагин работает с большинством популярных сервисов сокращения ссылок, например: bit.ly, goo.gl, tinyurl.com, cli.gs, digg.com, fb.me, is.gd, j.mp, kl.am, su.pr и прочими. Далее пользователь уже работает с оригинальными ссылками и видит на какой сайт она переходит [1].

Некоторые файлообменники также пользуются технологией коротких ссылок. Они формируют для них специальные короткие ссылки типа cl.ly/abcd. В феврале 2012 года, пользователем ресурса http://habrahabr.ru ShamanS был проведен эксперимент, где был написан скрипт, который генерирует короткие ссылки (4-х буквенные) случайным образом с учетом регистра [3]. Далее скрипт обращается по генерированному адресу и проверяет есть ли там что-нибудь. Если находит, тогда записывает ссылку, название файла и размер в базу данных. Если не находит, то ищет дальше,

пока не переберет все варианты ссылок. Таким образом, в результате работы скрипта было проверено 224 ссылки, из них работающими были 92. Была возможность скачать и ознакомиться со всеми файлами, но если бы у них была настройка приватности, то такая возможность была бы недоступна.

Если же нет возможности отказаться от коротких ссылок, то можно воспользоваться предложением от компании McAfee. Производитель антивирусного программного обеспечения McAfee сообщил о своем собственном сервисе сокращения ссылок, который препятствует пользователям посещать веб-сайты с вредоносными программами. Этот новый безопасный сервис сокращения ссылок укорачивает ссылку сразу же, без сканирования ее адреса назначения. Вместо этого, при переходе по сокращенной ссылке, сканируется веб-сайт на наличие любого злонамеренного содержания. Саймон Хант, вице-президент и главный инженер компании, написал что «повышая уровень глобальных интеллектуальных средств по предотвращению угроз McAfee, новая программа создает сокращенные ссылки и проверяет их по базам данных на наличие известных угроз, спама, хостингов вредоносных приложений, контроля загрузки и т.д. до того, как сайт откроется» [2].

Перечень литературы:

1. http://www.proofsite.com.ua/article-3457.html
2. http://www.bezpeka.com/ru/news/2010/09/24/McAfee-cutting-links.html
3. http://habrahabr.ru/blogs/infosecurity/138870/
4. http://devilart.net/000000-list-94/352-chernyi-spisok-saitov-po-vzlomu-webmoney-koshelkov.html