Вредные советы: как заразить свой «мобильник»

Заразить свой мобильный телефон вы должны непременно сами, поскольку, благодаря заложенным в архитектуру мобильного телефона принципам, почти никакие уязвимости не помогут хакерам проникнуть на ваш телефон без вашего ведома и разрешения. И сегодня мы расскажем, как это сделать.

Способ первый: необходимо зайти на предложенный вам определённый ресурс, чтобы с него загрузить желанный зловред. Для этого необходимо в сроке поискового сайта набрать, например, «игры для Android скачать» и нажать на одну из верхних строк в результатах поиска. Часто такие сайты действительно содержат игры, но игры эти не простые, а с сюрпризом, причём весьма неприятным. Люди склонны доверять сайтам из верхних строчек результатов поиска - если на сайт заходят тысячи людей, думают они, значит, там точно найдётся нужная игра или программа. О безопасности в таких случаях люди думают редко и недолго.

Поздравляем, вы стали жертвой «чёрной раскрутки» сайтов! Злоумышленники используют «неэтичные» методы поисковой оптимизации, заставляющие поисковую систему показывать вредоносный ресурс в верхних строчках результатов поиска. Для того, чтобы поднять сайт в топ результатов поиска нередко используются, например, «ботнеты» - целые сети «зомбированных компьютеров», которые вводят в Google или Yandex поисковые запросы и заходят на нужный вредоносный сайт, повышая его рейтинг. Кроме того, ссылки на нужную злоумышленникам страницу публикуются на всевозможных форумах, досках объявлений и в комментариях на новостных сайтах. Там их находят краулеры поисковых систем (программы, собирающие и анализирующие контент веб-сайтов для поисковой системы), и рейтинги вредоносного сайта растут ещё больше.

Способ второй: пройдите по ссылке из смски хорошо знакомого вам человека. Такие смски обычно не внушают подозрений, особенно если их текст выглядит правдоподобно, а вы любите обсуждать фотографии знакомых или рады немного отвлечься от работы очередным образчиком сетевого юмора, которым, не подозревая об этом, хочет поделиться ваш знакомый. Но на открывшемся сайте вы, вполне вероятно, получите ещё и зловредный «бонус». Знакомьтесь: это результат работы смс-червя, который, попав на ваш телефон, начинает рассылать смс-сообщения всем, кто находится у вас в списке контактов.

Способ третий: зайдите на легитимный сайт и перейдите по предложенной на нём ссылке, не разбираясь в источнике и природе её появления – с большой вероятностью вы получите на свой телефон зловред. Желая угадать ваши желания, хакеры взламывают популярные сетевые ресурсы со множеством посетителей: новостные сайты, интернет-магазины, тематические порталы. Если программное обеспечение сайта содержит уязвимости, в его страницы внедряется код, перенаправляющий посетителей на другой сайт, содержащий уже зловреды.

Способ четвёртый: скачайте новую очень интересную игру (или приложение) из магазина приложений. Такой игрой может оказаться вполне легитимная программа с внедрённым в неё вредоносным кодом, специально созданное приложение, только «делающее вид», что выполняет какие-либо полезные функции, или совсем уж «откровенный» зловред, единственной маскировкой которого являются только лишь имя да иконка. Подобные программы обычно загружаются в неофициальные магазины приложений, которые либо совсем не фильтруют загружаемые в них приложения, либо делают это не слишком тщательно, обычно ограничиваясь автоматической проверкой с помощью антивируса. Однако, известны случаи попадания таких программ и в официальные магазины Google Play и App Store. Компании, конечно, стараются оперативно «чистить» свои магазины, но и злоумышленники не сидят сложа руки.

Способов заразить свой мобильный телефон, конечно, намного больше, ибо смекалка злоумышленников всегда на шаг впереди изобретательности производителей средств защиты. Выше мы перечислили наиболее часто используемые и удобные для вас способы, с помощью которых вы всегда сможете быстро добиться долгожданного результата.

Подготовлено по материалам СМИ