Фишинг электронной почты на примере mail.ru

Понкратов В.С.

Фишинг - это вид онлайнового мошенничества. Впервые, об этом виде преступлений общественность узнала в 1996 году. Тогда сразу несколько тысяч клиентов провайдера America Online получили электронные письма от "представителя компании" с просьбой выслать логин и пароль для входа в систему. И многие попались на эту уловку.

С тех пор извещения о фишинге появлялись периодически. Но никогда этот вид мошенничества не принимал особо широких масштабов. Фишинг (англ. phishing, от password — пароль и fishing — рыбная ловля) — вид интернет - мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, данным кредитных карт и т.п.

Если не учитывать прямую финансовую выгоду из кражи кредитных карт и перечисления с них денег, то есть еще много целей, на которые можно потратить украденные данные, например, кража логинов/паролей почтовых ящиков - минимальное, что опытный пользователь может получить - это пустить под спам, продать кому-либо и или сделать то, что ему захочется. Не может же пользователь рассылать сообщения с обычным текстом, на которое мало кто может попасться, такие сообщения для фишинга не подойдут. Хакеру нужно что-то завлекающее, то, чему наивный пользователь поверит, подойдет сервисное сообщение. Но как завлечь пользователя? - не все же сейчас ведутся на «сбой базы данных» с просьбой подтвердить пароль, поэтому нам нужно как-то завлечь неопытного пользователя.

В этой статье нам рассказывается не только что такое фишинг, но и о его структуре, как произвести фишинг-атаку.

Представьте, когда пользователь проверяет почту и обнаруживает письмо с подобным содержанием от admin@mail.ru «Здравствуйте, это администрация mail.ru. Мы производим удаление не действующих аккаунтов, если вы являетесь владельцем e-mail и в настоящие время пользуетесь это почтой, то для проверки пройдите авторизацию и т.д» и в конце всего этого сообщения ссылку на эту авторизацию (вход в систему).Выглядит заманчиво, текст конечно можно видоизменять и в общем, каждый выбирает сам, какой текст он будет писать жертве. Главное, что следует помнить: это не выпрашивать пароль на прямую. Если вы подкрепляете письмо какими-либо графическими файлами, иконками, табличками или еще чем то старайтесь чтоб по дизайну они подходили к сервису, на котором зарегистрирована почта нашей «жертвы».Пишите всегда грамотно, старайтесь избегать ошибок, если не получается написать письмо без ошибок то можно воспользоваться текстовыми редакторами Openoffice.org или MsOfficeWord или любым удобным вам способом. Вряд ли пользователь поверит письму с большим количеством ошибок.

После того как наш пользователь проходит по вашей ссылке (в это время происходит перенаправление на ложный сайт) он попадает на сайт очень похожий на mail.ru, но на самом деле это поддельный сайт (фейк). Жертва вводит там свои данный нажимает на вход и дальше пустота или идет перенаправление на настоящий mail.ru где снова пользователю придется вводить свои данные. После нажатия пользователем «Вход», его данные отправляются к нам. Хакер может сам выбрать куда эти данные будут отправляться после получения.

В июле 2006 года появилась новая разновидность фишинга, тут же получившая название вишинг. Вишинг (Vishing) назван так по аналогии с

«фишингом» -распространенным сетевым мошенничеством, когда клиенты какой-либо платежной системы получают сообщения по электронной почте от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в интернете достаточно сложно.

Вы должны помнить, что администрация сайтов никогда не будет связываться с вами, чтобы запросить какие-либо пароли, данные счетов, персональную информацию. Вам следует удалять любые полученные сообщения, запрашивающие личную информацию или содержащие ссылку, ведущую на ложный сайт, где вам предлагается эти данные ввести. Вероятнее всего, такие сообщения являются мошенничеством. Фишеры часто используют ссылки в письмах, чтобы завлечь свои жертвы на поддельные Web-сайты, имеющие похожие адреса, к примеру, vkantakte.ru вместо vkontakte.ru. Так же, если пойти по указанной ссылке, то адрес сайта в адресной строке может выглядеть как настоящий, однако, существует несколько приемов его подмены, чтобы вывести вас на поддельный сайт.

Если вы подозреваете, что полученное письмо от администрации является фальшивым, не используйте указанные в нем ссылки. Помните, что нельзя следовать ссылкам, указанным в таких письмах. Всегда вводите адреса через браузер. Обеспечьте защиту своего компьютера. Некоторые вредоносные письма содержат программы, способные собирать информацию о ваших действиях в интернете (шпионские программы) позволяющий хакерам проникать в ваш компьютер (троянские программы). Установив антивирусное ПО с последними обновлениями, вы получите помощь по обнаружению и дезинфекции такого рода вредоносных программ, а использование анти-спамных программ обезопасит ваши почтовые ящики от получения фишинговых

писем. Так же важно, особенно для пользователей широкополосного доступа к интернету, установить межсетевой экран. Это поможет, блокируя связи с нежелательными источниками, сохранить информацию на вашем ПК в безопасности. Убедитесь, что у вас установлена современная версия Web-браузера, и вы установили для нее самые последние обновления. Если у вас нет этих обновлений, обратитесь на сайт производителя. Если вы подозреваете, что получили поддельное электронное сообщение, перенаправьте его в администрацию сайт с полной копией письма которое вам пришло.

Фишинг, вишинг - эти способы «отъема денег» и кражи личной информации будут совершенствоваться. Но надеяться только на технику неразумно. Призовите на помощь здравый смысл: никогда банковское или почтовое учреждение не будет требовать от вас пересылки конфиденциальной информации. Старайтесь не ставить слишком простые пароли на авторизацию в системах, не хранить на одной почте всю важную вам информацию. В этом случае даже при успешной атаке ущерб окажется не большим.

Список литературы:

1. Устраиваем фишинг-атаки на примере mail.ru [Электронный ресурс]/ http://webcriminal.ru/forum/showthread.php?p=14838 (с изм. и доп.) - Режим доступа : (дата обращения 15.12.09)

2. Фишинг [Электронный ресурс]/ http://ru.wikipedia.org/wikiAt**)niiJHHr** (с изм. и доп.) - Режим доступа : (дата обращения 15.12.09).