Многоликий фишинг (Часть 1)

Фишинг – давно (если это слово применимо к связанным с интернетом вещам) известная совокупность методов несанкционированного получения киберзлоумышленниками конфиденциальной информации пользователей. Давно известная, но, тем не менее, совсем не потерявшая свою актуальность угроза – ежегодно миллионы пользователей по всему миру становятся жертвами изобретательности фишеров, придумывающих всё новые разновидности фишинга.

Только ежемесячно в мире рассылается более 6 миллиардов фишинговых писем (данные 2015 года). Больше всего (17%) фишинговых атак, по данным компании «Лаборатория Касперского», совершается на пользователей именно России. И примерно 80% пользователей не в состоянии распознать фишинговые письма (исследование компании Intel Security, проведённое в 2015 г.).

Почему фишинг выгоден злоумышленникам? Приличный «улов» (фишинг переводится с английского как «рыбалка») при вполне позволительных затратах. Арифметика фишинга примерно такова:

- Отправлено писем – 2 000 000 шт;
- Получено пользователями писем – 100 000 шт. (или 5%, большая часть всё же задерживается спам-фильтрами сетевого оборудования и почтовых серверов);
- Нажали на фишинговую ссылку – 5 000 чел (или 5%);
- Ввели данные на фишинговом сайте – 100 чел (или 2%);
- Средняя прибыль с каждой жертвы – 1200 долларов (согласно общемировой статистике);
- Итого общая прибыль лишь от одной фишинговой рассылки – 120 000 долларов.

Вполне неплохо, если учесть, что исходная рассылка выполняется автоматически и занимает меньше часа. Воистину, плохой день на рыбалке лучше, чем хороший день на работе!

Мы неоднократно писали, что фантазия злоумышленников практически неисчерпаема. Разнообразие методов фишинга – ещё одно тому подтверждение. Изобретательность преступников, позволяющая им с помощью самых хитроумных методов создавать практически неотличимые от реальных фишинговые письма или сайты, побуждая пользователя самостоятельно отдавать конфиденциальную информацию (или доступ к ней), у некоторых специалистов-безопасников вызывает даже нечто схожее с восхищением «красотой» реализации фишинга.

Наиболее часто используемым методом фишинга, конечно же, является email-фишинг или фишинг с помощью сообщений электронной почты. Обычно, ничего не подозревающий пользователь получает в свой почтовый ящик сообщение, в котором некто, обычно от лица какой-либо организации, просит пользователя выполнить некие действия – проверить правильность документа (а для этого открыть вложение в присланном сообщении), или подтвердить данные своей учётной записи, например, в онлайн-банке (а для этого открыть содержащуюся в письме ссылку, ведущую на умело мимикрирующийся под настоящий сайт с формой ввода данных, откуда они попадают прямо к злоумышленникам), или, наоборот, опровергнуть кем-то когда-то поданную на пользователя жалобу (иск, оформленный кредит, выставленный счёт и т.д.). Часто подобный призыв к действиям сопровождается словами «срочно» или «незамедлительно», или же получателю ставится определённый срок («если Вы не опровергните жалобу до 29 февраля, Вам отключат газ»), до которого он непременно должен выполнить требуемые жуликами действия. Таким образом злоумышленники вводят пользователя в состояние смятения и паники, не дают трезво обдумать ситуацию (роковая ошибка!), вынуждают подчиниться их указаниям и, тем самым, совершить ошибку. Фишинговые сообщения, как правило, рассылаются от банков, органов государственной власти (судебные приставы, налоговая служба, суды и т.д.) либо интернет-сервисов (почтовых сервисов (gmail.com, yandex.ru, mail.ru и других), облачных хранилищ (DropBox, Google Диск и т.д.) или сайтов онлайн-объявлений (avito.ru, hh.ru и других)).

В следующей части мы рассмотрим некоторые другие разновидности многоликого фишинга.

Многоликий фишинг (Часть 2)

В современной практике фишинга есть и более хитроумные способы обмана потенциальных жертв. Сегодня о некоторых из них.

Целая «гроздь» методов фишинга основана на подмене легального содержимого нелегальным – называется всё это «спуфингом». Фишеры наловчились умело подменять практически всё, что можно прислать в email-сообщении: отправителя и его email-адрес, тему письма, вложение в письмо, содержимое и ссылки на сайты. Например, email-адрес отправителя может выглядеть как вполне легальный, скажем, support@paypal.com. Нюанс здесь, однако, в том, что первая буква «а» в наименовании домена адреса (paypal.com) – кириллическая («русская»). Таким образом, подобный домен зарегистрирован злоумышленниками и не имеет никакого отношения к платёжному сервису PayPal. «На глаз» такая подмена неразличима.

Аналогичным образом поступают с доменами в ссылках фишинговых писем: такая ссылка может выглядеть почти как настоящая за счёт «мимикрии» – например, может вести на поддельный сайт mai1.ru вместо настоящего mail.ru. Иногда также используются похожие до смешения буквосочетания «rn» вместо «m» и «cl» вместо «d». Такую подмену заметить можно, но лишь присмотревшись.

Другой пример – динамическая подмена ссылки в email-сообщении: если навести «мышку» на ссылку в письме, будет отображён один адрес перехода, а при нажатии на ссылку специальный скрипт меняет ссылку, и в действительности пользователь переходит на поддельный сайт.

Именно поэтому лучший совет для борьбы с подменой ссылок и доменов – не полениться набрать ссылку самостоятельно в адресной строке браузера. Если у вас есть причины вообще открывать ссылку.

Иногда вы можете получить сообщение, в котором будет файл-вложение с именем, например, «rcs.mp3». Судя по расширению, резонно предположить, что вам прислали музыкальный файл в формате «mp3» (в которых крайне редко бывает какое-либо вредоносное ПО). На деле же, при открытии файла запускается троянская программа-вирус. Фокус в том, что если в имени файла поставить определённый невидимый так называемый управляющий символ, то имя файла меняется на обратное – то есть «3pm.scr» превращается в «rcs.mp3».

Ещё одним распространённым видом фишинга является направленный (целевой) фишинг – в этом случае фишинговая атака направлена не на неограниченно широкий круг неизвестных злоумышленнику жертв, а на вполне определённого, нужного для злоумышленника, человека. Целью является получение конфиденциальной информации конкретного пользователя-жертвы. Для этого злоумышленник предварительно осуществляет сбор информации о жертве. Если жертвой является высокопоставленное лицо, то подготовка целевой атаки может осуществляться очень тщательно, с применением всех законных и незаконных способов, при этом используются соцсети, сотовые операторы, базы госорганов и т.д. В итоге злоумышленник, хорошо зная фактическую информацию о «жертве», её круг общения, составляет сообщение, которое неминуемо должно вызвать доверие у «жертвы» и привести к совершению ею нужных преступнику действий по раскрытию своей конфиденциальной информации.

Такие атаки весьма трудоёмки и затратны, поскольку подготовка отнимает большую часть времени. Однако, усилия должны окупиться, поэтому целью подобных атак являются, как правило, не «простые люди». Как следствие, целевые атаки характеризуются намного более высокой эффективностью нежели обычный фишинг.

Ранее мы упоминали, что никакое ПО не может обеспечить 100% защиту от вредоносных сообщений, поэтому главным и наиболее действенным способом защиты от фишинга, в том числе, от целевого, является внимательность при использовании электронной почты и своевременный вопрос «зачем?» - «зачем я получил это письмо?». И если вы не можете ответить на этот вопрос, не ожидали такого письма и не знаете его отправителя – в 99% случаев такое письмо окажется спамом или фишингом (или и тем и другим).

Многоликий фишинг (Часть 3)

Вопреки распространённому мнению, фишинг это не только поддельные email-сообщения и сайты. Каналы коммуникаций злоумышленника с потенциальной жертвой, в принципе, могут быть любыми – электронная почта, приложения для мгновенного обмена сообщениями («аська», Skype и т.п.), телефон или даже обычная (неэлектронная) почта. В этой, заключительной, части цикла про фишинг мы как раз и рассмотрим примеры использования для фишинга иных каналов, кроме электронной почты.

Возьмём, к примеру, Skype. Это приложение активно используется миллионами пользователей по всему миру, многими для деловых контактов, а потому не могло не привлечь внимание злоумышленников. В профилях пользователей Skype можно найти массу персональных данных (имя, дату рождения, адреса электронной почты, телефоны и т.д.). Лакомая цель - собранные персональные данные можно использовать для целевого фишинга.

Однажды вы получаете в Skype запрос на добавление в «контакты» от неизвестного пользователя, в котором, кроме того, содержится сообщение о том, что вы получили новое персональное сообщение и его можно посмотреть на некоем, указанном тут же в сообщении, но незнакомом вам, сайте. Если нажать на ссылку, будет предложено скачать файл-«видеоплеер», который на самом деле является вредоносным ПО, запрашивающим у пользователя права администратора компьютера и, в случае предоставления таковых, ворует персональные данные, скачивает и устанавливает на компьютер загрузчик рекламных сообщений и включает компьютер в так называемую «ботнет» - сеть компьютеров-«зомби», используемых во вредоносной деятельности в интернете без ведома владельцев таких компьютеров.

Разумеется, есть и другие примеры фишинга с помощью Skype, однако, всем им можно успешно противостоять, если помнить базовые правила:

1. Не открывать незнакомые файлы (вложения) и ссылки;
2. Регулярно обновлять базу антивируса.

Телефонный фишинг обычно используется для целевых фишинг-атак наряду с email-фишингом и иными методами. Телефонный фишинг можно отнести к довольно дорогим методам мошенничества - чтобы умело «развести» жертву, злоумышленник должен быть хорошим психологом и актёром, а это требует подготовки и опыта. Да и сама подготовка атаки, сбор данных о жертве и её окружении и разработка сценария атаки, довольно дорога и занимает время. Но и противостоять такой целевой атаке неподготовленной жертве намного сложнее – хорошо поставленная атака, проводимая опытным психологом, почти не оставляет шансов на защиту.

Примеры фишинга «по переписке» (то есть с использованием обычной почты) можно пересчитать по пальцам руки – понятно, что такой путь злоумышленников к логинам-паролям и прочим целям чрезвычайно долог, а потому сам метод неэффективен.

Подводя итог нашему краткому экскурсу в «мир» фишинга, ещё раз хотим подчеркнуть, что главное оружие против фишинга – здравый смысл и внимательность. Когда кто-то, особенно незнакомый, просит вас что-либо сделать – на это всегда полезно смотреть через «призму» его мотивации, то есть задать вопрос «зачем (или почему) он просит меня это сделать?». Но даже если причины понятны и кажутся резонными, необходимо проявлять должную внимательность и обращать внимание на такие признаки фишинговых сообщений, как поддельный адрес отправителя, отсутствие персонализированного обращения к вам, а также наличие речевых, грамматических и орфографических ошибок.

Соблюдение данных, в общем-то, простых правил, наряду с актуальным антивирусным ПО, убережёт вас от абсолютного большинства проблем, являющихся следствием фишинга.