ЭФФЕКТИВНЫЕ МЕТОДЫ БОРЬБЫ С ФИШИНГОВЫМИ АТАКАМИ. ЧАСТЬ I.

СОВРЕМЕННЫЙ ФИШИНГ

Заимствованное слово **фишинг** (phishing) образовано от английского password – пароль и fishing – рыбная ловля, выуживание. Цель этого вида интернет-мошенничества – обманный увод пользователя на поддельный сайт с тем, чтобы в дальнейшем украсть его личную информацию (логины, пароли, адреса электронной почты и т.п.) или, например, заразить компьютер пользователя, перенаправленного на подложный сайт трояном. Заражённый компьютер может активно использоваться в ботнет-сетях для рассылки спама, организации DDOS-атак, а так же для сбора данных о пользователя и отправки их злоумышленнику. Спектр применения «выуженной» у пользователя информации достаточно широк. В последние годы активное распространение Интернет-мошенничеств привело к формированию т.н. черных рынков со своими заказчиками и исполнителями. Последние отчеты аналитиков говорят о наличии в современном мире сложной вирусной "экосистемы". Так, основная масса вирусов и троянских программ создавалась в 2008 году с целью последующей продажи. Причем, если по количеству создаваемого вредоносного ПО мировым лидером в 2008 году стал Китай, то по сложности и "инновационности" программ на первом месте оказались российские хакеры и вирусописатели.

МЕХАНИЗМЫ ФИШИНГА

Главный вектор атаки фишинга направлен на самое слабое звено любой современной системы безопасности – на человека. Далеко не всегда клиент банка точно знает, какой адрес является правильным: mybank.account.com или account.mybank.com? Злоумышленники могут использовать и тот факт, что в некоторых шрифтах строчная i и прописная L выглядят одинаково (I = l). Такие способы позволяют обмануть человека с помощью похожей на настоящую ссылки в электронном письме, при этом даже наведение курсора мыши на такую ссылку (с целью увидеть настоящий адрес) не помогает. В арсенале злоумышленников есть и другие средства от банальной подмены в локальной базе IP-адресов реального адреса на поддельный (в ОС Windows XP, например, для этого достаточно отредактировать файл hosts) до фарминга.

Ещё один вид мошенничества – подмена веб-страницы локально, «на лету». Специальный троян, заразивший компьютер пользователя, может добавлять в отображаемый браузером сайт дополнительные поля, отсутствующие на оригинальной странице. Например, номер кредитной карты. Конечно, для успешного проведения такой атаки надо знать банк или платёжную систему, которыми пользуется жертва. Именно поэтому тематические базы электронных адресов пользуются большой популярностью и являются на черном рынке ликвидным товаром.

Нежелающие нести дополнительные расходы фишеры просто направляют свои атаки на наиболее популярные сервисы – аукционы, платёжные системы, крупные банки – в надежде, что случайный получатель спамового письма имеет там учётную запись. К сожалению, надежды злоумышленников зачастую оправдываются.

ТРАДИЦИОННЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Возникшие с появлением фишинга угрозы потребовали внедрения адекватных мер защиты. В рамках данной статьи будут рассмотрены как уже широко распространённые способы противодействия фишингу, так и новые эффективные методы.

Разделение это весьма условно: к традиционным отнесем хорошо известные (в том числе и самим злоумышленникам) способы противодействия фишингу и проанализируем их эффективность в первой части данной статьи.

УНИКАЛЬНЫЙ ДИЗАЙН САЙТА

Суть этого метода такова: клиент, например, банка при заключении договора выбирает одно из предложенных изображений. В дальнейшем при входе на сайт банка ему будет показываться именно это изображение. В случае если пользователь его не видит или видит другое, он должен покинуть поддельный сайт и немедленно сообщить об этом службе безопасности. Предполагается, что злоумышленники, не присутствовавшие при подписании договора, априори не смогут угадать правильное изображение и обмануть клиента.

Однако, на практике этот способ не выдерживает критики. Во-первых, для того, чтобы показать пользователю его картинку, его сначала надо «узнать», т.е. идентифицировать, например, по логину, который он ввёл на первой странице сайта банка. Злоумышленнику не составляет труда подготовить поддельный сайт, чтобы узнать эту информацию, а для самого пользователя – эмулировать ошибку связи. Теперь достаточно обратиться на реальный сервер, ввести украденный логин и подсмотреть правильное изображение.

Другой вариант – выдать клиенту фальшивое предупреждение об истечении срока действия его изображения и предложить выбрать новое ...

ОДНОРАЗОВЫЕ ПАРОЛИ

Классические пароли являются многоразовыми: пользователь вводит один и тот же пароль каждый раз при прохождении процедуры аутентификации, не меняя его порой годами. Перехваченный злоумышленником этот пароль может неоднократно использоваться им без ведома хозяина.

В отличие от классического одноразовый пароль используются только один раз. При каждом запросе на предоставление доступа пользователь вводит новый пароль.

Для этого используются, в частности, специальные пластиковые карточки с нанесённым защитным слоем. Клиент банка каждый раз стирает очередную полоску и вводит нужный одноразовый пароль. Всего на карточку стандартного размера помещается около 100 паролей, что при интенсивном использовании услуг телебанкинга требует регулярной замены носителя.

Более удобными, но дорогими, представляются специальные устройства – генераторы одноразовых паролей. Они могут иметь разный внешний вид и принцип действия. В основном различают два типа генерации – по времени, когда текущий одноразовый пароль отображается на экране и периодически (например, раз в две минуты) меняется или по событию, когда новое значение генерируется каждый раз при нажатии пользователем на кнопку устройства.

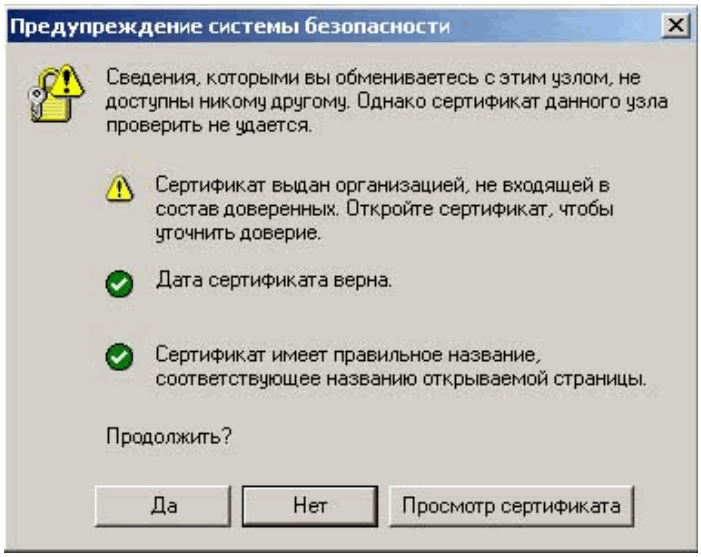
Являясь более безопасным, чем классическая парольная аутентификация, такой метод, тем не менее, оставляет злоумышленнику определённые шансы на успех. Например, аутентификация с использованием одноразовых паролей не защищена от атаки «человек посередине» – man in the middle. Суть этой атаки состоит во вклинивании в информационный обмен между пользователем и сервером, когда злоумышленник «представляется» пользователю сервером и наоборот. Вся информация от пользователя передаётся серверу, в частности и введённый им одноразовый пароль, но уже от имени злоумышленника. Сервер, получив правильный пароль, разрешает доступ к закрытой информации. Не вызывая подозрений, злоумышленник может позволить пользователю поработать, например, со своим счётом, пересылая ему

всю информацию от сервера и обратно, но при завершении пользователем своего сеанса работы не разрывать связь с сервером, а совершить нужные транзакции якобы от имени пользователя.

Чтобы не терять время в ожидании завершения сеанса пользователя злоумышленник может просто имитировать ошибку связи и не позволять работать со своим счётом. В зависимости от используемого метода генерации перехваченный одноразовый пароль будет действовать либо в течение короткого времени, либо только для первого сеанса связи, но в любом случае это даёт злоумышленнику успешно провести кражу данных или денег пользователя.

На практике аутентификация с использованием одноразовых паролей сама по себе не используется, для повышения безопасности применяется установление защищённого соединения ещё до аутентификации, например, с использованием протокола SSL.

ОДНОСТОРОННЯЯ АУТЕНТИФИКАЦИЯ



Использование протокола безопасных соединений SSL (Secure Sockets Layer) обеспечивает защищенный обмен данными между веб-сервером и пользователями. Данный протокол, разработанный в 1996 году компанией Netscape, на сегодня стал одним из самых популярных методов обеспечения защищенного обмена данными в сети Интернет. Протокол SSL, использующий ассиметричный криптографический алгоритм RSA интегрирован в большинство браузеров и веб-серверов, а для реализации защищённого соединения с использованием российской криптографии потребуется дополнительное программное обеспечение, как на сервере, так и на каждом клиентском рабочем месте.

Несмотря на тот факт, что протокол позволяет аутентифицировать не только сервер, но и пользователя, на практике чаще всего применяется только односторонняя аутентификация. Для установления SSL-соединения необходимо, чтобы сервер имел цифровой сертификат, используемый для аутентификации, Сертификат обычно выдаётся и заверяется некоей третьей доверенной стороной, в роли которой выступают удостоверяющие центры (УЦ) или центры сертификации (в западной терминологии), например, компании Thawte, Verisign и др. Роль УЦ заключается в том, чтобы подтверждать подлинность веб-сайтов различных компаний, позволяя пользователям, «поверив» одному единственному удостоверяющему центру, автоматически иметь возможность проверять подлинность тех сайтов, владельцы которых обращались к этому же УЦ.

Список доверенных удостоверяющих центров обычно хранится в реестре операционной системы или в настройках браузера. Именно эти списки и подвергаются атакам со стороны злоумышленника. Действительно, выдав фишинговому сайту сертификат от поддельного удостоверяющего центра и добавив этот УЦ в доверенные, можно не вызывая никаких подозрений у пользователя успешно осуществить атаку.

Конечно, такой способ потребует от фишера больше действий и соответственно затрат, но пользователи, к сожалению, зачастую сами помогают в краже своих данных, не желая разбираться в тонкостях и особенностях использования цифровых сертификатов. В силу привычки или некомпетентности нередко мы

нажимаем кнопку «Да», не особо вчитываясь в сообщения браузера об отсутствии доверия к организации, выдавшей сертификат.

К слову можно отметить, что очень похожий способ используют некоторые средства по контролю SSL-трафика. Дело в том, что в последнее время участились случаи, когда сайты, заражённые троянскими программами, и сами трояны используют протокол SSL с тем, чтобы миновать шлюзовые системы фильтрации трафика – ведь шифрованную информацию ни антивирусное ядро, ни система защиты от утечки данных проверить не в состоянии. Вклинивание в обмен между веб-сервером и пользовательским компьютером позволяет таким решениям заменить сертификат веб-сервера на выданный, например, корпоративным УЦ и без видимых изменений в работе пользователя сканировать трафик пользователя при использовании протокола SSL.

URL-ФИЛЬТРАЦИЯ

В корпоративной среде фильтрация сайтов используется для ограничения нецелевого использования сети Интернет сотрудниками и как защита от фишерских атак. Во многих антивирусных средствах защиты данный способ борьбы с поддельными сайтами вообще является единственным.

Выявлением фишерских сайтов и внесением их в чёрные листы занимаются многие компании от производителей антивирусных решений до банков, платёжных систем и правоохранительных органов. В частности, создаются специальные организации для борьбы с фишерами, такие как Anti Phishing Work Group (APWG).

Совместные мероприятия заинтересованных сторон в тесном сотрудничестве с регистраторами и хостинговыми компаниями позволяют оперативно закрывать поддельные сайты. Согласно отчёту самой APWG за первую половину 2008 года было выявлено 47,324 фишинговых сайтов. Совместные усилия направлены на максимально быстрое обновление чёрных списков и блокирование работы сайтов злоумышленников. Нельзя не отметить определённые успехи в этом направлении – среднее время жизни фишерского сайта составляет всего 49.5 часов. В том же отчёте, однако, приведены и средние потери пользователей и компаний в результате работы фишерского сайта, они составляют не менее $300 в час. Несложные умножения позволяют сделать вывод о высокой доходности этого вида черного бизнеса.

Вполне вероятно, что далеко не все производители средств антивирусной защиты могут похвастаться столь высокой оперативностью в обновлении баз, к тому же многие пользователи не используют никаких средств защиты на своих компьютерах или водят номера кредитных карт и другую конфиденциальную информацию со случайных рабочих мест. Ну и, наконец, не следует забывать, что приведённые данные являются усреднёнными, что означает, что реальные атаки могут наносить существенно больший урон конкретному пользователю или компании, возможно, ставя их на грань банкротства.

ОКОНЧАНИЕ В INFORMATION SECURITY, №4 , ИЮНЬ, 2009