Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

ФИШИНГ

Обзор и методы защиты

Студент: *Даниленко Александр Игоревич*
Группа: *116*
Курс: *Защита информации*

г. Долгопрудный
2005г.

Содержание

1. Введение

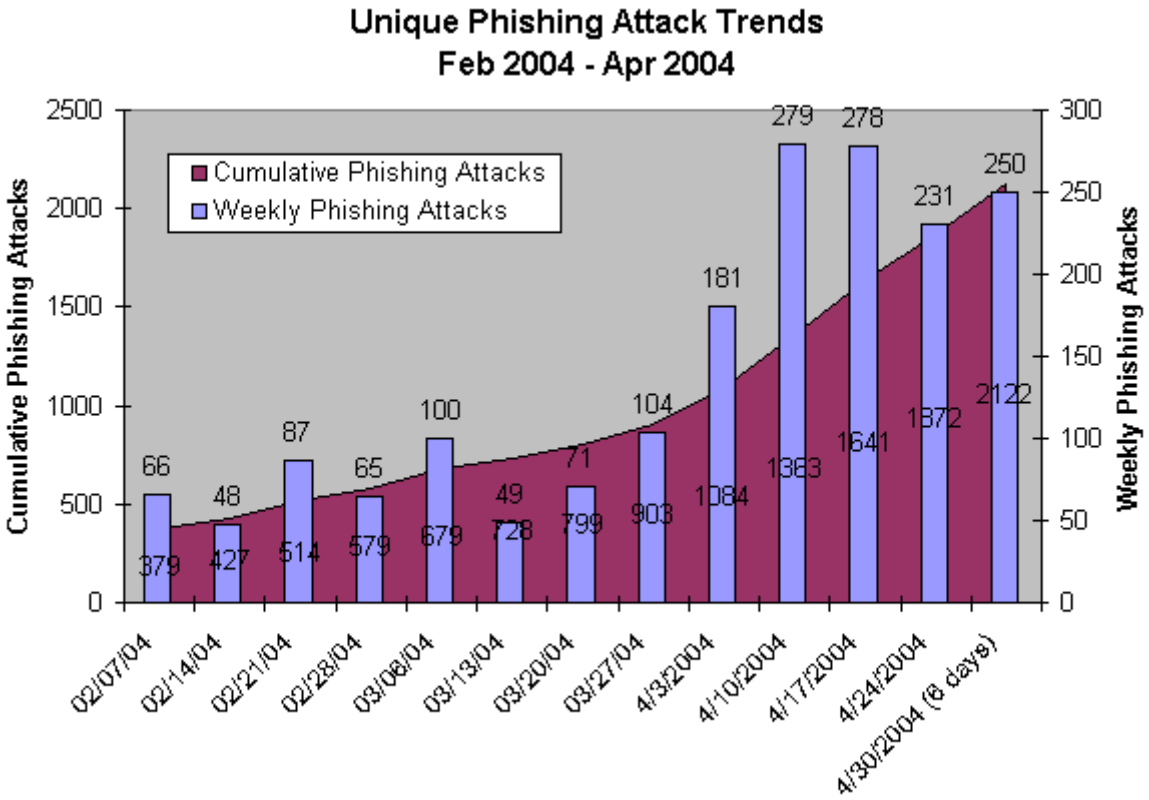
Каждый человек, активно использующий компьютер и Интернет, практически каждую неделю узнает новости о новых типах вирусов или же хакерских атак, и для нас эти явления уже стали обыденными. Вполне логично, что уже с момента появления вирусов и хакеров начались создаваться средства защиты от таких угроз, написано много статей и книг на эту тему, не говоря о том, что создание антивирусных программ стало уже индустрией. Кроме вышеназванных опасностей, которые хорошо изучены и с которыми довольно успешно справляются, на сегодняшний день существует новая угроза – фишинг.

Если описать в двух словах, то фишинг – это создание точной копии веб-страницы какой-либо коммерческой структуры (чаще всего банка) с целью завладеть секретной информацией ее клиента (личные данные, номер счета или кредитной карточки, пароль). Слово «фишинг» (от английского «fishing») означает рыбалка. Если смотреть с общей точки зрения, то фишинг очень похож на рыбалку: злоумышленник забрасывает приманку, а затем вылавливает всех, кто попался на нее.

Фишинг появился в 1996-1997 годах и стал популярным с развитием электронного бизнеса (e-business). Приведем несколько цифр показывающих тенденции развития фишинга, демонстрирующие, насколько он стал распространен:

- Число активных фишинг-сайтов обнаруженных за март: 2870
- Средняя месячная скорость роста количества фишинг-сайтов за июль 2004 – март 2005: 28%
- Число брендов, подвергшихся нападению: 78
- Число брэндов, содержащихся в списке первых 80% фишинг-нападений за март: 8
- Страна предоставляющая хостинг большинству фишинг-сайтов за март: США
- Содержат часть адреса в URL: 31%
- Только IP адрес без имени хоста: 48%
- Доля сайтов, не использующих порт 80: 3.89%
- Среднее время существования фишинг-сайта: 5.8 дней
- Наибольшее время существования сайта: 31 дней

(данные Anti-Phishing Working Group за март 2005 года: http://www.antiphishing.org)



(данные Anti-Phishing Working Group за февраль-апрель 2004 года: http://www.antiphishing.org)

2. Схема реализации фишинг-атак

Итак, суть фишинга сводиться к тому, что злоумышленник пытается обманным способом заставить человека предоставить ему конфиденциальную информацию. При этом жертва делает все самостоятельно, хотя, конечно же, и не предполагает, что на самом деле эта информация достанется злоумышленнику. Отсюда видно, что реализация фишинг атак состоит из двух частей социальной и технической:

- Социальный аспект заключается в том, чтобы заставить жертву произвести некоторые действия по вводу информации. Например, отправить пользователю письмо от имени банка с просьбой подтвердить свои персональные данные (это самый простой пример, на практике используются более хитрые методы).
- Цель технической части заключается в том, чтобы жертва ввела свои данные «туда куда надо». То есть создание копии сайта банка, использование дыр в программном обеспечении (браузерах), подмена данных DNS серверов.

3. Три вида фишинга

На сегодняшний день известны три вида фишинга: почтовый, онлайновый и комбинированный.

Первый из них, почтовый, самый старый. Он заключается в том, что жертве отправляется специальное письмо по электронной почте от авторитетного имени с требованием выслать в ответ какие-либо данные. Примером использования такой атаки может служить самый примитивный способ получения данных (логина и пароля) для подключения к Интернет. Злоумышленник шлет письмо жертве и при этом представляется сотрудником провайдера и просит выслать его логин и пароль, для убедительности можно привести множество поводов для этого: «упавший» сервер с базой данных или обновление базы, переход на новый тариф и прочее. Для того, чтобы жертва ничего не заподозрила мошенник может использовать почтовый ящик с названием сервера, похожим на название сервера провайдера.

Второй вид - онлайновый фишинг, он заключается в том, что злоумышленник копируют какие-либо сайты, на которых требуется введение персональных данных (чаще всего интернет-магазины). При этом, конечно же, надо использовать похожие доменные имена и идентичный внешний вид сайта.

Рассмотрим случай с интернет-магазином. Допустим, посетитель сайта решил купить какой-либо товар (причем число таких людей достаточно велико потому, что злоумышленники предлагают товары по очень низким ценам). Так как злоумышленники чаще всего копируют весьма известные сайты, то у их посетителей – потенциальных жертв – редко возникают подозрения. В итоге пользователи наивно полагают, что они находятся на веб-сервере реально работающего магазина с хорошей репутацией. Итак, жертва решила купить товар, для этого ей надо зарегистрироваться в системе, после этого ввести номер и прочие данные своей кредитной карты или банковского счета. Как только все это сделано, злоумышленнику остается лишь перевести деньги со счета жертвы на свой.

Почтовый, онлайновый виды фишинга существуют довольно давно. Они весьма примитивны и если даже человек и не слышал о них, то, будучи достаточно внимательным и не слишком доверчивым, может их избежать. Поэтому почтовый и онлайновый фишинг сейчас не эффективны. Однако на смену им пришел третий тип фишинга – комбинированный, и почти сразу получил широкое распространение.

Суть этого способа заключается в следующем. Так же как и в предыдущем способе, злоумышленник создает поддельную копию сайта какой-либо организации. Затем отправляет пользователям письма с просьбой зайти на сайт по приведенной ниже ссылке и произвести необходимые действия (ввести конфиденциальные данные). Именно здесь проявляется социальная часть реализации атаки, о которой мы говорили ранее. Приведем яркий пример. Однажды многие клиенты, пользующиеся пластиковыми картами крупного банка, получили важные письма от его имени. В них содержалось примерно следующее: «На Ваш счет пришел перевод на сумму $1000. По инструкции Вам необходимо подтвердить получение. Для этого необходимо открыть ссылку и заполнить необходимые данные». Очевидно, что нашлось немало людей, которые последовали требованиям письма и оставили свою секретную информацию на сайте-подделке.

4. Фарминг

Наряду с фишингом появился новый метод онлайнового мошенничества (можно считать его разновидностью фишинга), еще более изощренный и опасный – фарминг (от английского «pharming»). Фарминг-атака заключается в изменении DNS (Domain Name System) адресов для того, чтобы перенаправлять запросы, пришедшие от клиентов, с

оригинальных сайтов на их подделки. В итоге сайт, который посещают пользователи, будет не настоящим, а специально созданным злоумышленником для сбора конфиденциальной информации (особенно относящейся к онлайновым банкам).

Когда пользователь набирает в адресной строке браузера ссылку, чтобы произвести доступ к веб-странице, адрес должен быть преобразован в реальный IP-адрес в формате xxx.xxx.xxx.xxx. Для этого обычно требуется DNS-сервер, так как браузер сам не может выполнить такое преобразование. Эти серверы анализируют имена и доставляют пользователя на страницу, которую он запросил.

Фарминг-атака может быть выполнена или против DNS-сервера и тогда изменение адреса повлияет на всех пользователей при обращении к серверу, или же выполнена локально (на конкретный компьютер) тогда атака повлияет только на одного пользователя. В первом случае мошенниками обычно используются атаки на DNS-сервер известные под названием DNS-spoofing. Эти атаки не так просто выполнить, поэтому чаще используется второй способ, который гораздо эффективнее.

На каждом компьютере (с ОС Windows и Internet Explorer в качестве браузера) хранится небольшой файл hosts. Он содержит таблицу соответствия серверов и IP-адресов, которые наиболее часто посещаются пользователем. Это сделано для того, чтобы не обращаться каждый раз к DNS-серверу для преобразования часто используемых URL в IP-адрес. Итак, чтобы выполнить фарминг-атаку необходимо, во-первых, создать копию оригинального сайта, а затем подправить host-файл нужным образом. Для изменения файла можно использовать вредоносные коды (обычно трояны). В итоге, каждый раз, когда пользователь вводит ссылку в браузере с именем банка, то он попадает не на его сайт, а на его копию, созданную злоумышленником; и после того, как он вводит конфиденциальные данные, они попадают к злоумышленнику.

5. Защита

Что же делают представители организаций, чтобы обезопасить своих пользователей от мошенничества? Крупные банки, например, пытаются заранее предостеречь своих пользователей и просят их соблюдать осторожность (размещают статьи, рассылают брошюры о мошенничестве). Другие компании также применяют превентивные меры.

Как определить, что письмо пришло от злоумышленника с целью проведения фишинг-атаки и получения конфиденциальной информации? Вот несколько внешних признаков того, что письмо является обманным (по данным статьи [1]):

- Тема и тело письма бедно отформатированы и содержат много ошибок.
- Письмо начинается с неличностного приветствия, такого как Дорогой Клиент. Обычно действительные компании посылают письма, в которых обращаются к получателю по имени.
- Манера изложения письма беспокоящая или тревожная, как у писем, запрашивающих финансовую или другую персональную информацию, тревожный тон письма, сообщающего о том, что многие клиенты потеряли свои учётные записи и это может случиться и с получателем.
- Если письмо содержит ссылку, попытайтесь провести мышью над ней. Если видимая ссылка в теле письма не совпадёт со ссылкой в строке статуса, то существует большая вероятность, что письмо было подделано.

Так же предлагается профилактическая мера по предотвращению распространения таких писем – это рапортовать о них.

Что касается фарминга, то Panda Software предлагает следующие советы пользователям, чтобы помочь им не стать жертвой атак фарминга [2]:

- Использовать антивирусное ПО, совмещающее предупреждающие и реагирующие системы обнаружения. Самый простой способ манипуляции компьютером для того, чтобы он стал жертвой фарминга – использование вредоносного кода, обычно троянцев. Помните, что множество троянцев входят в систему незаметно для пользователей, так что некоторые из них могут циркулировать некоторое время, прежде чем антивирусные компании обнаружат их и создадут соответствующую вакцину. Вот почему рекомендуется использовать предупреждающую систему защиты - чтобы была возможность предотвратить угрозы и блокировать их просто по результатам анализа их поведения.
- Установить персональный брандмауэр: эта мера предосторожности помешает хакеру проникнуть в компьютер через незащищенный порт и модифицировать систему.
- Часто обновлять ПО, установленное на компьютере, или включить системы автоматического обновления, чтобы убедиться в отсутствии уязвимостей, которые могут быть использованы для проведения таких атак.

Также можно посоветовать защиту: проверка любых операций предлагаемых совершить от имени банка (или другой компании) с помощью телефонного звонка в банк, для того чтобы получить подтверждение. Хотя в этом случае встает вопрос: а зачем тогда нужен e-business?

6. Литература

1. Новая фишинг-атака Интернет-мошенников (2004г.) (http://linux.zp.ua/modules.php?op=modload&name=News&file=article&sid=104&mode=thread&order=0&thold=0)
2. В Сети появился новый вид мошенничества - фарминг (2005г.) http://www.cybersecurity.ru/crypto/3731.html
3. Феномены интернета: фишинг (2004г.) http://www.webplanet.ru/news/focus/2004/6/15/phishing.html
4. Международная антифишинговая рабочая группа APWG http://www.antiphishing.org