

Составил:  
Версия от

Александр Сорокин  
Январь 2005

Тип Атаки:	Phishing
Относительная степень опасности (max=1)	1
Краткое описание	Вынуждение пользователя выдать конфиденциальную информации путем ввода в заблуждение
Частота атак на мои компьютеры	1-4 в день
Признаки попытки атаки	E-mails, которые выглядят как посланные от банка, провайдера и пр., однако содержащие ссылки на поддельные сайты
Механизм атаки	По большому списку адресов рассылаются e-мейлы которые выглядят как посланные банком, провайдером, страховой компании, магазином и т.п. В e-мейле содержится URL, который на первый взгляд указывает на сайт отправителя. Однако на самом деле URL указывает на поддельный сайт. Обычно такой поддельный сайт содержит форму для ввода паролей, номеров счетов, кредитных карт и т.п. якобы для "уточнения". При вводе такой информации на поддельном сайте она оказывается в руках атакующих, которые могут ее криминально использовать (например, для перевода денег со счета, покупок по кредиткам и т.п.).
Частота успешных атак	Я не попадался, но судя по сообщениям печати весьма высокая
Признаки успешной атаки (одно из или все сразу)	1. Исчезновение денег со счета в банке или с кредитки 2. Невозможность зайти на сайт банка, провайдера по имеющемуся паролю т.к. Атакующий его поменял
Способы защиты	1. Всегда вводить URL банка или провайдера руками 2. Не использовать Internet Explorer т.к. Его многие версии содержат ошибки, позволяющие атакующему изменить содержимое URL в названии страницы по сравнению с на самом деле открытой страницей

Sheet1

	3. Открывать спамовские сообщения (их надо стирать не задумываясь)
	4. Кликать в на ссылки в спаме
Примечания	1. Ссылки на поддельные сайты могут распространяться не только по e-mail, но и другими способами
	2. Существует аналогичная атака вне Интернета когда звонят по телефону и выведывают конфиденциальную информацию

# Безопаснос

AdWare/Spyware
2
Установка через Интернет на компьютере без согласия владельца программ разной степени вредононости, использование этих программ против интересов владельца
Сказать трудно, но таких сайтов много
Обычно момент атаки проследить невозможно, есть вариант атаки когда у пользователя прямо спрашивается разрешение на установку ПО на его компьютере в надежде, что он не поймет что это атака
Сайт, на который зашел пользователь содержит особым образом сформатированный URL. Такие URL обычно используют брешы в Internet Explorer для незаметной установки каких-то программ на компьютере жертвы. Такие программы могут делать на компьютере жертвы все, что угодно. Примеры: сбор информации о сайтах, посещаемых пользователем; открывание окон с рекламой; сбор информации вводимой с клавиатуры (в т.ч. паролей); превращени компьютера в релей для рассылки спама или атак на другие компьютеры.
Все мои знакомые, использующие Internet Explorer попадались хотябы раз за последние два года
1. Часто внешних признаков нет
2. Неожиданной появление окон с рекламой, часто взрослого содержания
3. Неожиданный рост траффика непонятного происхождения
1. Никогда не устанавливать на компьютере никакого ПО если на 100% не известно что это такое, особенно ПО закачанного с Интернета
2. Не использовать Intenet Explorer т.к. В нем много брешей, подбных атак на другие браузеры пока не известно

3. Не открывать ссылки из спама

1. Довольно часто заражение происходит при поиске в Интернете т.к. приходится заходить на много неизвестных сайтов

2. Попасты на опасный сайт можно делая опечатки в URL

3. Антивирусы с этим типом атаки практически не справляются

4. После заражения вычистить компьютер можно только путем перформатирования диска, да и то не всегда помогает

5. Последнее время описаны подобные атаки через музыкальные файлы для Windows Media Player

## ть в Интернете

Почтовые вирусы (черви)
3
Установка на компьютере без согласия пользователя программ, которые сами себя рассылают по электронной почте
Сейчас до 10 в день, во время эпидемий – сотни в час
Е-mailы с предложением запустить какую-то программу, посмотреть картинку и т.п., Е-mailы могут приходить как от ваших знакомых, так и от неизвестных вам людей
Программа, запущенная из e-mail, устанавливается на компьютере без ведома пользователя. Затем она рассылает себя по адресам из адресной книги.
Все мои знакомые на это попадались, однако последнее время частота эпидемий упала
1. Вам приходят e-mailы с ответами на сообщение, которых вы не посылали
2. Рост необъяснимого траффика
1. Никогда не запускать файлы, присланные по e-mail
2. Не использовать Outlook и Outlook Express т.к. Почтовые черви используют их брешы, подобных атак на другие почтовые программы пока не известно

1. Есть виды червей по действию похожих на spyware/adware, такие черви могут, например, превращать компьютер в релей для спама

<b>Макровирусы</b>
--------------------

4
---

Распространение вредоносных программ в составе файлов офисных приложений (MS Word, Excel, PowerPoint, CorelDraw)
--

Несколько в год
-----------------

Обычно атаки нераспознаваемы

Зараженный офисный документ содержит в своем теле программу, которая при открытии этого документа записывается в шаблон (.dot файлы в случае MS Word). Из зараженного шаблона программа включает себя в другие открываемые документы.
---

Заметно упала в последние годы, раньше была очень серьезной проблемой
---

Странное поведение офисного ПО, в т.ч. Медленный запуск и открывание файлов
---

1. Не открывать документы, присланные по e-mail от неизвестных отправителей
---

2. Избегать открывать офисные документы с веб страниц кроме как по большой нужде

3. Открывать докумнты, скаченные с сети или пришедшие по почте не в MS Word или Excel, а в OpenOffice или других офисных системах (подобных атак на OpenOffice пока не известно)

1. Есть неприятная комбинация этой атаки с почтовыми червями

2. Макровирусы часто вылезают из архивов старых документов.

3. Антивирусы не всегда реагируют на макровирусы, пришедшие отличным от e-maila путем

4. Иногда в Интенете встречаются офисные документы (особенно обнаруживаемые в результате поиска), которые содержат в себе вредоносный код, но не заражают компьютеры

Eavesdropping	Взломы
5	6
Перехват сообщений (e-mail, instant messages и пр.), содержащих конфиденциальную информацию	Несанкционированное проникновение на компьютер через сетевой интерфейс
Невозможно оценить	Сотни в день
Нераспознаваема	Получение неожиданных пакетов на сетевой интерфейс
Прослушивание каналов связи, анализ содержание жестских дисков компьютера. Вариант атаки – изменение содержания сообщений в интересах атакующего.	Взломщик посылает пакеты хосту в надежде установиить над ним контроль. Жертвами становятся неправильно сконфигурированные или непатченные компьютеры. Получив контроль на компьютером взломщик может устанавливать на нем свое ПО, атаковать с него другие компьютере, рассылать спам и т.д.
Я знаю пол-десятка человек, ставших жертвами этого вида атак	В основном страдают серверы. По знакомым я наблюдаю успешный взлом раз в несколько месяцев.
Главный признак – вы понимаете, что кто-то, кто не должен владеть некоей информацией, ей завладел.	1. Что-то странное творится с компьютером
	2. Рост необ”яснимого траффика
1. Использовать системы шифрования и электронной подписи при пересылке информации по открытым кналам	1. Всегда запускать firewall, открывать только самые необходимые порты
2. Не использовать октрытые каналы для пересылки конфиденциальной информации	2. Запускать на компьютере только необходимые службы

Sheet1

1. Хотя этот вид атак весьма редок, такие атаки могут иметь самые катастрофические последствия. В печати были описаны похищения людей с использованием перехваченных сообщений.	1. Эта атака представляет большую проблему для серверов, чем для домашних машин