Московский физико-технический институт (ГУ МФТИ)

Факультет Радиотехники и Кибернетики

"Особенности платежной системы «WebMoney»"

Коробков А.Н.,314 гр.,04.04.2007г.

Эссе по курсу "Защита информации", кафедра радиотехники

http://www.re.mipt.ru/infsec

WebMoney

WebMoney — система онлайн-платежей и среда для ведения электронного бизнеса. Первоначально разработанная для использования на территории России, система действует практически по всему миру. На данный момент система насчитывает более 2млн. участников. Все транзакции в системе являются мгновенными и безотзывными.

Транзакционная система-система, реализующая транзакции над хранилищем данных. Задача транзакционной системы — обработать как можно больше транзакций в минимальное время с гарантией безошибочных результатов. Это означает, что когда отправитель посылает свои «деньги» адресату, то перевод происходит настолько быстро, насколько быстродействен канал передачи данных, установленный между парой.

Следующий пример позволит понять что такое транзакция. «Необходимо перевести с банковского счёта номер 5 на счёт номер 7 сумму в 10 денежных единиц. Этого можно достичь, к примеру, приведенной последовательностью действий:

```
Начать транзакцию
   прочесть баланс на счету номер 5
   уменьшить баланс на 10 денежных единиц
   сохранить новый баланс счёта номер 5
   прочесть баланс на счету номер 7
   увеличить баланс на 10 денежных единиц
   сохранить новый баланс счёта номер 7
Окончить транзакцию
```

Эти действия представляют из себя логическую единицу работы "перевод суммы между счетами", и таким образом, являются транзакцией.»Безотзывный, означает что перевод нельзя отменить если он произведён.)

Система поддерживает несколько типов титульных знаков(«денежных единиц»), обеспеченных различными активами и хранящихся на соответствующих электронных кошельках:

- WMR — эквивалент российских рублей (кошелек типа R),
- WMZ — эквивалент долларов США (кошелек типа Z),
- WME — эквивалент Евро (кошелек типа E),
- WMU — эквивалент украинской гривны (кошелек типа U),
- WMB — эквивалент белорусских рублей (кошелек типа B),
- WMY — эквивалент узбекских сум (кошелек типа Y),
- WMC и WMD — эквивалент WMZ для кредитных операций на C- и D-кошельках

У каждого типа титульных знаков есть свой «ГАРАНТ»-организация, хранящая и управляющая обеспечением эмиссии, устанавливающая эквивалент обмена на заявленные имущественные права, опубликовавшая на веб-сайте Системы и в ПО WebMoney Keeper оферту по купле-продаже титульных знаков гарантируемого типа, обеспечивающая юридически значимое введение в хозяйственный оборот титульных знаков гарантируемого типа в соответствии с законами страны регистрации.

Система разработана таким образом, что вы можете проводить какие-либо действия либо анонимно, либо как открытый пользователь(известно ваше имя,…).Естественно, установление истинности информации является ключевым моментом в обеспечении безопасности любых данных, проходящих через Систему.

При регистрации участнику WebMoney Transfer присваивается уникальный номер — 12-значный WM-идентификатор (WMID), необходимый для работы в Системе. WebMoney Transfer предусматривает 3 типа аутентификации:

- с помощью файлов с секретными ключами. Для запуска WM Keeper Classic (ПО для работы с Системой) необходимы: уникальный 12-значный WM-идентификатор, пароль (назначается пользователем), а также файлы с секретным ключом и кошельками, которые хранятся в памяти компьютера. Желательно сохранять резервные копии файлов ключей и кошельков на съемном носителе и хранить их в надежном месте. Это значительно облегчит восстановление доступа к кошельку в случае утраты или уничтожения файлов на компьютере

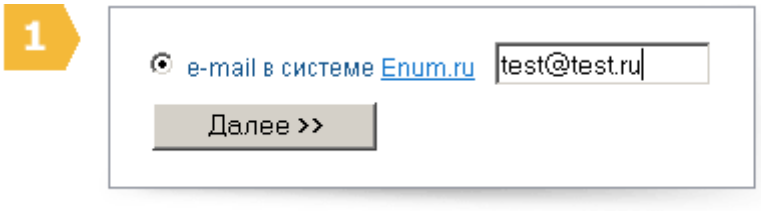
- с помощью персональных цифровых сертификатов

- с помощью системы авторизации e-Num, обеспечивающей наиболее высокий уровень безопасности информации. Принципиальное новшество заключается в том, что критичные персональные данные больше не нужно хранить на самом компьютере. Авторизация обеспечивается за счет использования одноразовых сеансовых пар: числа-логина и числа-пароля, которые меняются каждый раз при входе в систему и не повторяются. Защита обеспечивается как средствами криптографии, так и на архитектурном уровне с помощью так называемого одноразового шифроблокнота. Секретный ключ для доступа к данным хранится не в компьютере, а в мобильном телефоне пользователя, что позволяет использовать его при работе с различных компьютеров, а также исключает риск порчи или хищения ключа троянскими и другими вредоносными программами.

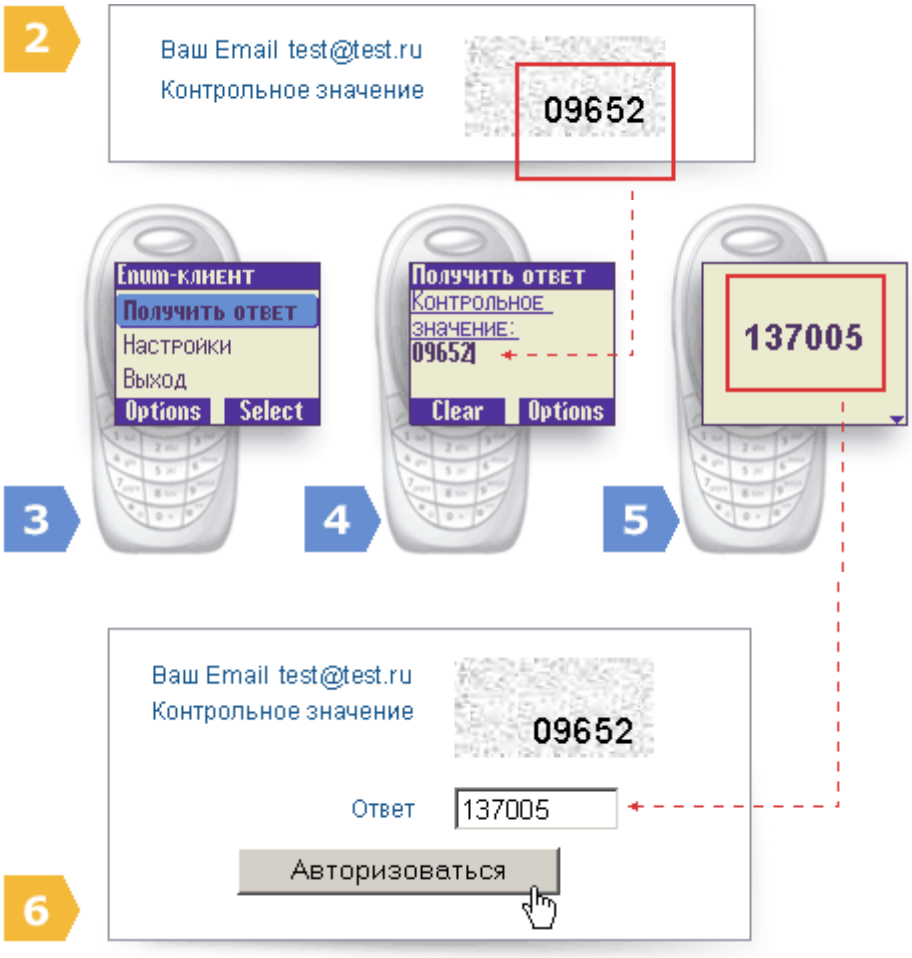
Все операции в системе – хранение WebMoney на кошельках, выписка счетов, расчеты между участниками, обмен сообщениями - совершаются в закодированном виде, с использованием алгоритма защиты информации, подобного RSA, с длиной ключа более 1040 бит. Для каждого сеанса используются уникальные сеансовые ключи, что обеспечивает гарантированную конфиденциальность совершения сделок и обмена информацией.

На системном уровне обеспечивается устойчивость по отношению к обрывам связи. При совершении трансакции средства всегда находятся либо на WM-кошельке отправителя, либо на WM-кошельке получателя. Промежуточного состояния в системе не существует. Таким образом принципиально не может возникнуть ситуации, когда WM-средства будут потеряны.

Несколько слов о E-NUM – надежная система авторизации. К достоинствам этой системы можно отнести такие качества как: высокая степень защиты, удобства и простота использования, широкий диапазон применения, экономичность.



На странице сайта, предусматривающей защищенный доступ, пользователь вводит свой e-mail



Пользователю отображается контрольное число

Пользователь запускает в телефоне или Pocket PC приложение E-num и вводит контрольное число

После ввода, на дисплее телефона отображается число-результат

Пользователь вводит число-результат в поле авторизации на сайте и получает доступ к защищенным разделам

Известные попытки атак на Систему *WebMoney*.

Попытки атак всё те же, заражение происходит стандартным путем: необходимо «попасться на удочку» -- загрузить с веб-сайта файл-носитель троянской программы (дроппер) и запустить его на выполнение. По данным "Лаборатории Касперского", пока обнаружено две версии дроппера: PHOTO.SCR (66 Кб) и Sponsors_pay_WM.EXE (70 Кб), однако имена файлов могут меняться. Эти дропперы действительно показывают фотографию незнакомки или договор на оказание услуг. Но одновременно происходит проникновение в компьютер троянской программы.”Троян”, специально рассчитанный только на WebMoney, ищет на дисках служебные файлы платежной системы и отправляет их на удаленный FTP-сайт. Одновременно он устанавливает на зараженный компьютер «клавиатурный жучок», который незаметно считывает все вводимые пользователем символы. Таким образом, злоумышленники могут получить пароли доступа к служебным файлам WebMoney и в обход криптографической защиты узнать их содержимое.

Другой пример атаки приводит снова Лаборатория Касперского" ,которая сообщает об обнаружении "троянца" "Relog" - очередной вредоносной программы, охотящейся за пользователями платежной системы WebMoney. В случае проникновения на компьютер жертвы, "Relog" предпринимает ряд действий вследствие чего злоумышленники могут получить доступ к счетам WebMoney для их неавторизованного использования.
"Relog" рассылается по электронной почте.

Зараженные письма выглядит следующим образом (оригинальная лексика сохранена):

Здравствуйте!
Вы являетесь пользователем системы WebMoney Transfer.
В связи с тем, что в нашей системе произошли небольшие технические

неполадки, компания проводит проверку своей БД пользователей. Если к вам пришло уведомительное письмо от сотрудников нашего центра, то вам необходимо пройти процесс перерегистрации.

Итак,вы обязаны пройти перерегистрацию до 05.12.02 (Если по какой-нибудь причине, вы не можете пройти процесс перерегистрации до указанного выше срока,то вам необходимо послать нам письмо на support@webmoney-relog.com, уведомляя нас об этом, и указать когда вы пройдете перерегистрацию), в противном случаи все ваши кошельки (со всеми денежными средствами на них) будут уничтожены. Денежные средства в этом случаи возврату не подлежат.

Для того, чтобы пройти перерегистрацию, необходимо скачать с сайта www.webmoney-relog.com специальную программу, которая автоматически проведет процесс перерегистрации. Вы должны скачать нашу программу, которая автоматически проводит процесс перерегистрации, распаковать ее с помощью программы Winrar (программа со всеми нужными файлами запакована в архив) и воспользоваться этой программой для перерегистрации. Скачайте программу в зависимости от вашей операционной системы.

Описание интерфейса программы перерегистрации приведено на сайте www.webmoney-relog.com

Если перерегистрация будет пройдена успешно, то можно будет вновь пользоваться программой WM Keeper Classic и нашей системой. После перерегистрации вы вновь, в полной мере, будете востановленны в системе WebMoney Transfer.

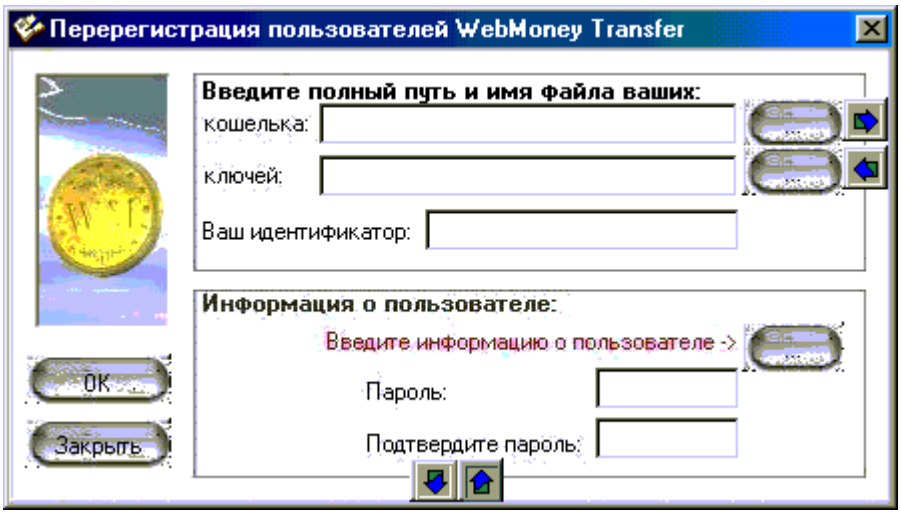
Со всеми вопросами обращаться на support@webmoney-relog.com Дополнительную информацию можно узнать на сайте www.webmoney-relog.com там же можно скачать программу для перерегистрации.

Желаем удачи!

NEVER SEND SPAM. IT IS BAD.

Рассылаемые письма содержат вложенный файл (RAR-архив с различными именами) с набором программ, необходимых для работы "троянца". В частности, в архиве находятся файлы README.TXT (инструкция по работе с пакетом) и webmoney-relogXP.exe (носитель "Relog"). При запуске последнего пользователю предлагается ввести запрашиваемые данные (в том числе и пароль). После этого "троянец" отсылает злоумышленнику данные, которые позволяют ему получить доступ к WebMoney-счету жертвы и производить с ним любые операции.

На данный момент "Лаборатория Касперского" не получила сообщений о реальных случаях заражения "Relog". Однако многие пользователи сообщают о получении ими подобных писем, что свидетельствует о произведенной массовой рассылке "троянца". В этой связи, мы рекомендуем пользователям немедленно удалять сообщения, соответствующие описанному выше шаблону.

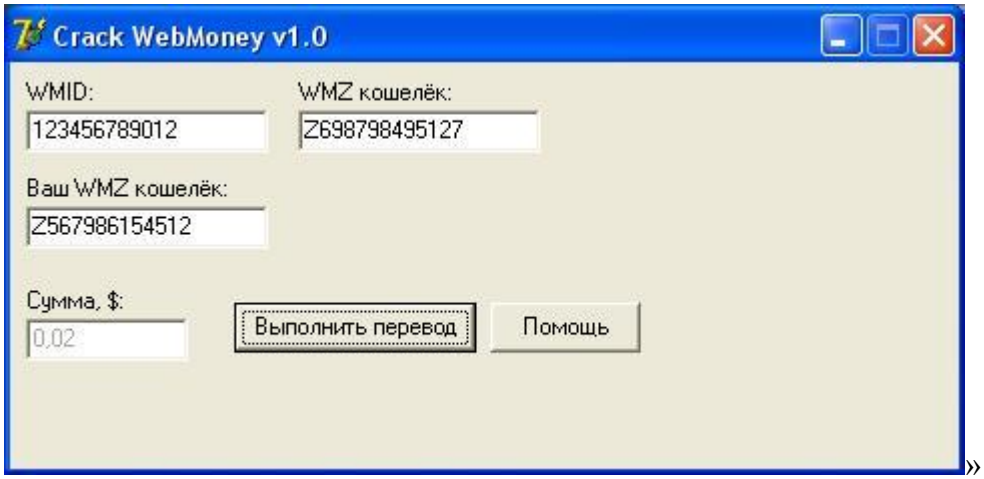


Процедуры защиты от данной вредоносной программы уже добавлены в базу данных Антивируса Касперского.

Ну и в конце для тех,кто сам хочет оказаться в роли хакеров приведу пример объявления,которое я нашёл в Intenet:

«*Продаю программу WebMoney crack v1.0, способную похитить WMZ на WebMoney. Программа не может делать деньги "из ничего", она может только похитить, т.е. перевести указанную сумму с любого Z-кошелька на ваш кошелёк. Вам понадобится WMID идентификатор и Z-кошелёк на котором вы уверены, что лежат деньги. Найти таких можно очень множество на различных сайтах. Стоимость программы 10 WMZ. Отправлять на Z128531639473. В комментариях укажите ваш рабочий e-mail. Программу вышлю в течение суток.*»

Программа не похищает ваши ключи и пароли, она не требует включеного Кипера. Можете работать с программой, а потом запустить WebMoney Keeper Classic или Light. Программа написана на Delphi.



»

Литература

1. WM-энциклопедия, http://www.webmoney.ru
2. http://ru.wikipedia.org/wiki/
3. http://www.e-num.ru/
4. Лаборатория Касперского,"Relog": новая атака на пользователей платежной системы WebMoney, http://www.kaspersky.ru/news?id=1103682