



Dr.WEB®

www.drweb.com

Защита систем электронных платежей на стороне клиента

Проблема и ее решения

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Ситуация 1. В сети уже используется антивирус. Достаточно ли его?

Ситуация 2. В сети установлена в дополнение к антивирусу система распределения доступа и система защита от атак – как правило на уровне рабочих станций. Достаточно ли просто установить защиту?

Как убедить руководство, что купленная по рекомендации защита просто смешит вирусы?

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Можно рассчитать ТСО и положить результат расчета на стол директора - а можно просто рассказать об реальностях ЖИЗНИ

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Спросите где он получает информацию? Какие сайты посещает для этого в интернете. Куда ходят в интернете ваши бухгалтеры – и с каких машин они ходят в интернет – не с тех ли самых, с которых они делают переводы средств в банке?

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

- Политика
- Экономика
- Происшествия
- Общество
- Пресс-конференции
- Новости туризма
- ▣ РБК - Регионы
- ▣ Новостям лекты

- Курсы ЦБ РФ
- FOREX
- Прогнозы валют
- Национал валюты

- Акции
- Паевые фонды
- Облигации, госбумаги
- Биржи online
- Фондовые индексы
- Мировые финансы
- База эмиссий

- Поиск кредита



thinkstock.com

 "Стеклопозитный полет" антирекорды по числу и бизнесе
 С течением времени сокращаются.

ВИДЕО

- Autonews.ru: Lada K...
- Л.Спириди: "Зенит"
- Выборы президента

Бизнес-газета РБК д:

- «Единая Россия» г
- Рассчитывая на удл
- сладости

расширенный поиск | тематический каталог | алфавитный указатель

ФОРМЫ ОТЧЕТНОСТИ
Формы налоговой и бухгалтерской отчетности, которые применяются в 2011 году

Название формы отчетности	Крайний срок сдачи	Бланки и комментарии к ним
Декларации по акцизам на табачные изделия	26 марта 2012	► Как заполнить
Декларация по акцизам на подакцизные товары, кроме табачных изделий	26 марта 2012	► Как заполнить
Декларация по налогу на прибыль	28 марта 2012	► Как заполнить
Налоговый расчет о выплаченных иностранным организациям доходах	28 марта 2012	► Как заполнить
Бухгалтерская отчетность	30 марта 2012	► Как заполнить
Форма отчетности 4-ФСС	15 апреля 2012	► Как заполнить
Декларация по НДС	20 апреля 2012	► Как заполнить

 ди в Москве отпущены, сообщает ГУМВД
 ина назвал отратительным "панк-молебен" в
 подготавливают "рейтинг надежд" нового кабинета
 емы россиян связаны с загруженностью на

f+ t+ B+ Комментарии

Интернет велик, но большинство посещают одни и те же сайты – причем ежедневно.

Сайты новостные, сайты финансовые...

Нужно же быть в курсе!

Защити созданное


 © ООО «Доктор Веб»,
 2012

www.drweb.com

И как правило для людей одной специальности это одни и те же сайты

Но это означает, что вы сами назначаете место встречи с хакерами.

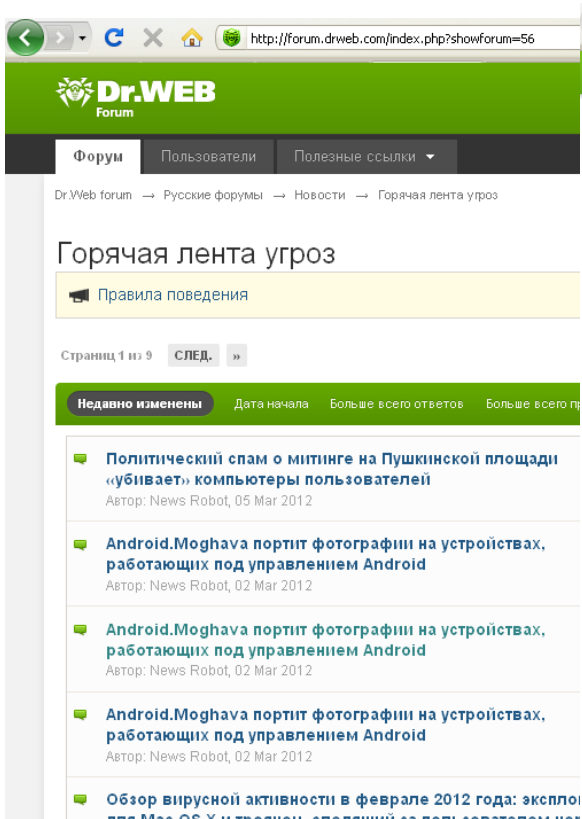
Априори зная ваши предпочтения они легко могут организовать на вас атаку – и делают это

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com



Dr.Web Forum

Пользователи | Полезные ссылки

Dr.Web forum → Русские форумы → Новости → Горячая лента угроз

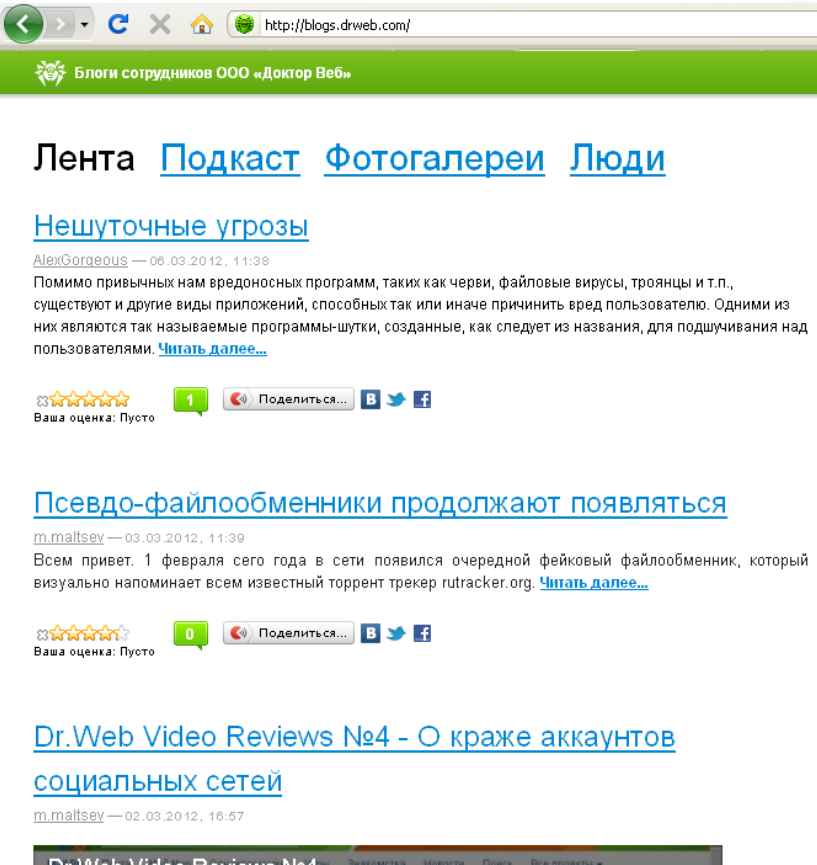
Горячая лента угроз

Правила поведения

Страниц 1 из 9 СЛЕД. »

Недавно изменены | Дата начала | Больше всего ответов | Больше всего просмотров

- Политический спам о митинге на Пушкинской площади «убивает» компьютеры пользователей**
Автор: News Robot, 05 Mar 2012
- Android.Moghava портит фотографии на устройствах, работающих под управлением Android**
Автор: News Robot, 02 Mar 2012
- Android.Moghava портит фотографии на устройствах, работающих под управлением Android**
Автор: News Robot, 02 Mar 2012
- Android.Moghava портит фотографии на устройствах, работающих под управлением Android**
Автор: News Robot, 02 Mar 2012
- Обзор вирусной активности в феврале 2012 года: эксплойты для Mac OS X и троянец, сделавший из пользователей чат**



Блоги сотрудников ООО «Доктор Веб»

Лента [Подкаст](#) [Фотогалереи](#) [Люди](#)

Нешуточные угрозы

AlexGorgeous — 06.03.2012, 11:38

Помимо привычных нам вредоносных программ, таких как черви, файловые вирусы, троянцы и т.п., существуют и другие виды приложений, способных так или иначе причинить вред пользователю. Одними из них являются так называемые программы-шутки, созданные, как следует из названия, для подшучивания над пользователями. [Читать далее...](#)

★★★★★ 1 | Поделиться... | В | f

Ваша оценка: Пусто

Псевдо-файлообменники продолжают появляться

m.maltsev — 03.03.2012, 11:39

Всем привет. 1 февраля этого года в сети появился очередной фейковый файлообменник, который визуально напоминает всем известный торрент трекер rutracker.org. [Читать далее...](#)

★★★★★ 0 | Поделиться... | В | f

Ваша оценка: Пусто

Dr.Web Video Reviews №4 - О краже аккаунтов социальных сетей

m.maltsev — 02.03.2012, 16:57

Dr.Web Video Reviews №4

Защити созданное



© ООО «Доктор Веб»,
2012
www.drweb.com

Читая новости о горячих угрозах – воспринимаете ли вы их не как информацию, а как руководство к действиям?

Согласно исследованиям интернет четко разделен по зонам интересов. Посетители одних сайтов не ходят на другие.

Скорее всего люди, принимающие решения о покупке, не читают новости IT-безопасности и не знают о текущем уровне опасности

Скажите им как страшно жить!

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Во всех компаниях так или иначе используются деньги. И все компании взаимодействуют с банками через систему дистанционного банковского обслуживания

И криминал подозревает об этом!

Защити созданное



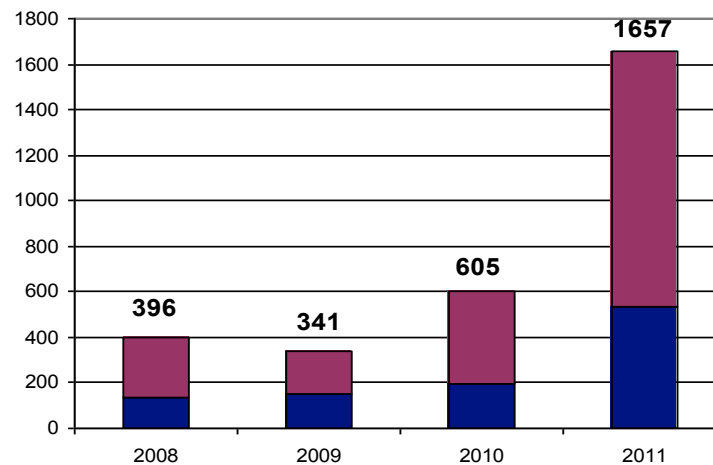
© ООО «Доктор Веб»,
2012

www.drweb.com

Дистанционное банковское обслуживание – предоставление платежных и информационных услуг удаленным клиентам кредитной организации посредством телекоммуникационных средств и сетей передачи данных.

Предоставление платежных услуг посредством ДБО регулируется Федеральным законом «О национальной платежной системе» в статье 9 Порядок использования электронных средств платежа.

тыс. ед.



■ Счета ДБО ■ в т.ч. через Интернет и мобильные телефоны

Количество счетов клиентов КО в РБ, доступ к которым предоставлен дистанционным способом

Основные вехи эволюции несанкционированных платежей в ДБО

- 2008- 2010 годы – кража ключей ЭЦП и паролей к ним. В ответ на указанную атаку в период 2009-2010 годов в КО были внедрены средства неотчуждаемого хранения ключей с СКЗИ на борту
- В конце 2010 года появились первые атаки, обходящие внедренное средство защиты - совершение платежей непосредственно с ПК клиента с помощью удаленного управления ПК
- В 2011 году атаки удаленного управления, также в 2011 году появились сообщения о возможности атаки подмены платежного поручения. В итоге в 4 квартале 2011 году – уже 50% платежей, приведших к потерям, совершалось непосредственно с ПК клиента (удаленное управление или, возможно, подмена платежного поручения)
- 31.01.2012 прошло сообщение в рамках межбанковского обмена о том, что для банк-клиента от BSS была реализована атака подмены платежного поручения.



Цель атаки:

- Несанкционированный перевод денежных средств, в том числе со счета юридического лица на счет физического лица в другом банке или на банковские карты коммерческих банков для обналичивания или на счета организаций, открытые в других коммерческих банках с компьютера злоумышленника
- Создание ботнета
- Заказная атака

Вывод средств производится на:

1. банковские карты для обналичивания,
2. счета мобильных телефонов, в основном «Билайн» (услуга «МОБИ.Деньги»)
3. электронные кошельки виртуальных платежных систем, в основном Яндекс.Деньги, Qiwi.

От момента совершения мошеннической операции до вывода средств проходит 1-3 минуты!

Защити созданное



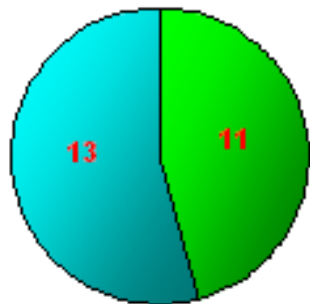
© ООО «Доктор Веб»,
2012

www.drweb.com

Виды атаки:

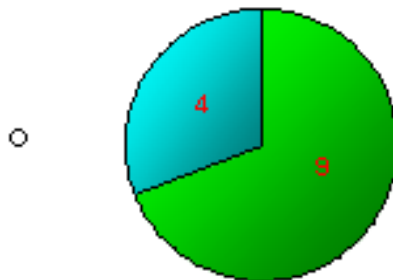
- Атака на каналы передачи данных
- Вирусная атака на сервер
- Атака на компьютер через Интернет с целью кражи секретного ключа ЭЦП, паролей
- Атака на компьютер через Интернет с целью захвата удаленного управления ресурсами компьютера
- Атака с целью подмены документа при передаче его на подпись
- Атака с целью подмены части или всего использующегося ПО
- Внедрение программных закладок или троянских программ

Последствия инцидентов



- - в основном эти попытки были предотвращены СИБ банка без ущерба для средств клиентов
- - имело место факты хищения денежных средств клиентов

Средняя сумма хищений денежных средств



- - до 1 млн руб.
- - от 1 до 10 млн. руб.

Дистанционное банковское обслуживание реализуется по разному – как правило через системы:

- Банк-клиент (с использованием специально разработанного ПО, работающего на стороне клиента)
- Мобильный клиент с работой через специальное ПО, плагин к браузеру или СМС
- Обслуживание через банкомат или терминал (АТМ клиент)

При этом работа возможна и с рабочего места, и с мобильного устройства и из дома. Банк априори не знает откуда должно прийти указание на перевод средств

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Для защиты передачи данных и удаленной работы традиционно используются:

- ✓ Средства, обеспечивающие защиту каналов связи (VPN и SSL VPN)
- ✓ Двухфакторная аутентификация с помощью токенов, смарткарт, OTP, систем подтверждения через SMS
- ✓ Системы криптографической защиты дисков, данных и подтверждения сообщений (SecretDisk, PGP...)
- ✓ Системы контроля целостности и контроля запуска приложений
- ✓ Системы антивирусной защиты
- ✓ Системы распределения и контроля доступа, в том числе контроля операций (идентификация, аутентификация и оповещение)

Защити созданное



Для защиты непосредственно систем ДБО используются:

- Виртуальные клавиатуры
- Аутентификация в системе ДБО
- Запрет входящих каналов на время работы ДБО
- Подтверждение платежей с помощью криптокалькуляторов (потенциально с использованием ключевых параметров платежа) или SMS
- Организация доверенной среды (загрузка доверенной операционной системы) - изоляция рабочего места ДБО от внешнего мира (LiveCD) или использование защищенного терминального режима доступа
- Защита платежных данных при передаче – шифрование данных
- Защищенное хранение ключей ЭЦП. Незвлекаемое хранение на USB-токенах и смарт-картах
- Ввод платежной информации на внешних устройствах (гарантия совпадения показываемой и формируемой платежки)

Что из этих средств уже скомпрометировано?

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Но!

- Виртуальные клавиатуры обходятся снятием экрана
- Аутентификация в системе ДБО – зависит от пользователей – социальная инженерия использовалась и используется
- Организация доверенной среды - изоляция рабочего места ДБО от внешнего мира на LiveCD обходится с помощью буткитов
- Виртуальные среды (в том числе на Java) взламываются путем подмены базовых компонент
- Использование внешних систем подразумевает использование программных компонент, что позволяет компрометировать и эти устройства, считавшиеся панацеей
- Подтверждение по SMS не подходит для большинства компаний

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

76.76.116.124/esClient/_Logon/Logon.aspx?ReturnUrl=/esclient/Default.aspx

просто, быстро, безопасно.

НОВОСТИ


24 декабря 2010
О НОВОЙ ВЕРСИИ
СБЕРБАНК ОНЛ@ЙН
Уважаемые клиенты!

Информируем Вас, что с 24 декабря 2010 г. введена в эксплуатацию новая версия Сбербанк ОнЛ@йн. В этой версии расширен список возможных операций. Подробнее можно прочесть в руководстве пользователя. Открыть руководство пользователя можно со страницы входа в Сбербанк ОнЛ@йн.

Вход на личную страницу

/ подключение /

Для того, чтобы войти в Сбербанк ОнЛ@йн, подключите услугу мобильный банк:



Карта, по которой был осуществлен вход в систему, не подключена к мобильному банку. Доставка SMS невозможна

Введите номер телефона:

Обратите внимание - номер мобильного телефона вводится без кода страны

ДАЛЕЕ **ОТМЕНА**

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com



Сбербанк России :: Сбербанк ОнЛ@йн :: Доступн...

Для этого веб-узла нужна следующая надстройка: "Adobe Flash Player" от "Adobe Systems Incorporated". Если вы доверяете этому веб-узлу и этой надстройке и разрешаете ее выполнение, щелкните здесь...

СБЕРБАНК
Всегда рядом

Поиск

О БАНКЕ
ПРЕСС-ЦЕНТР
АНАЛИТИКА
АКЦИОНЕРАМ И ИНВЕСТИТОРАМ
ОТДЕЛЕНИЯ И БАНКОМАТЫ

Москва

+7 495 500 5550
8 800 555 5550
Звонки по России бесплатно

ЧАСТНЫМ ЛИЦАМ

МАЛОМУ БИЗНЕСУ

Требуется принятие Оферты!

Использование сервиса предполагает Ваше полное согласие со всеми условиями Оферты, которая является публичным Договором с физическим лицом.

Ваш номер телефона:
Формат: 79*****

На ваш телефон придет смс, с кодом для авторизации.
Договор считается заключенным и приобретает силу с момента совершения Вами действий (в т.ч. генерации пароля клиента в системе и инсталляции приложения на мобильное устройство), предусмотренных в Оферте и означающих безоговорочное присоединение и выполнение Вами всех условий Оферты без каких-либо изъятий или ограничений в соответствии со ст. 428 ГК РФ.

Продолжить

СБЕРБАНК ОнЛ@ИИ

- Консультирование предпринимателей
- Реестр залогов Сбербанка
- Сбербанк Лизинг

Сбербанк ОнЛ@йн

Управление вашим счетом через интернет. [Войти в систему «Сбербанк ОнЛ@йн».](#)

КАК ПОЛЬЗОВАТЬСЯ Сбербанк ОнЛ@йн

http://sberbank.ru/moscow/ru/s_m_business/

Характер жалоб клиентов кредитных организаций на несанкционированное списание средств со счета

	Физические лица	Юридические лица
Количество жалоб в 2011 г.	7	4
Похищено со счетов клиентов кредитных организаций	428 тыс. руб	10,3 млн. руб
Характер хищений	<ul style="list-style-type: none">• кража пароля при использовании системы «Интернет-банкинг»;• кража контрольного номера перевода при переводе денежных средств по системе Western Union;• при совершении операции получения наличных средств в банкомате	компрометация ключей ЭЦП

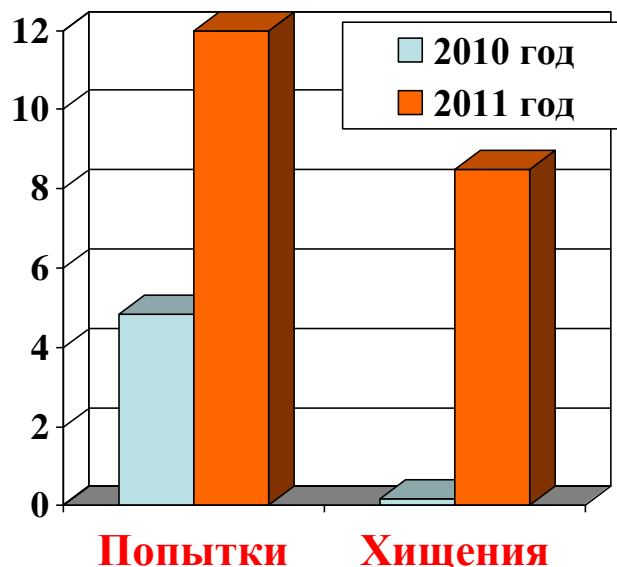
Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

млн. руб.



2010г.:

- 2 из 6 попыток успешные (33%);
- посягательств на 4,8 млн.руб.,
- похищено 175 тыс.руб. (4%)
- средняя сумма хищения 90 тыс. руб.

2011г.:

- 9 из 23 попыток успешные (~40%);
- посягательств на 12 млн.руб.
- похищено 8,5 млн.руб. (70%)
- средняя сумма хищения 450 тыс. руб.

На данный момент сформировалась развитая система киберпреступности, целью которых является хищение денежных средств. Система использует для продвижения вирусов следующие ресурсы сети Интернет:

- Фишинг
- Создание ложных сайтов
- Взлом сайтов и размещение на них вредоносных систем
- Взлом компьютеров и перехват управления

В преступных группировках существует четкая специализация – одни разрабатывают вирусы и взламывают компьютеры и сервера, другие создают фиктивные фирмы для перевода средств, третьи обналичивают украденные средства. Типичная структура состоит из организаторов, исследователей систем, разработчиков, взломщиков сайтов и распространителей вредоносного ПО («Заливщики»), а также дропперов



К сожалению, меры защиты преодолшаются.
Поскольку...

- Современные информационные технологии принципиально не защищены от заражения новыми вирусами в условиях свободного использования ресурсов Интернет
- Низкий уровень понимания рисков и угроз информационной безопасности приводит к игнорированию ими элементарных требований информационной безопасности
- Применение любых средств защиты упирается в человека, как самое слабое звено в системе защиты
- В условиях масштабных заражений всегда найдутся люди, которые что-либо нарушают и в первую очередь становятся жертвами мошенников
- Недостатки законодательства, интернациональность и распределенность членов криминальных сообществ осложняют взаимодействие и координацию работы правоохранительных органов.

Защити созданное



Кто скрывается за кражей данных?

- 74% - внешние источники
- 20% - инсайдеры
- 32% - «так называемые» бизнес-партнеры
- 39% - комбинация участников

Как происходят кражи?

- 67% способствовали значительные ошибки
- 64% способствовала хакерская активность
- 38% использовали malware
- 22% имели в составе злоупотребление привилегиями
- 9% произошли путем физических атак

91% всех компрометаций связаны с работой ОПГ

“2010 Data Breach Investigations Report”, Verizon Business

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Спросите, помнит ваш собеседник WinLock?

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Троянцы семейства Trojan.Carberp нацелены на хищение денежных средств компаний и частных лиц. Распространяется Trojan.Carberp с использованием набора эксплоитов Black Hole Exploit Kit — коллекции уязвимостей, эксплуатирующих ошибки и недокументированные возможности современного ПО, в частности, браузеров и операционных систем. В большинстве случаев жертве Black Hole не нужно предпринимать вообще никаких действий для того, чтобы «получить троянца»: заражение происходит автоматически при просмотре инфицированных веб-сайтов

Разработкой и “продвижением” **Trojan.Carberp** занимается организованная группа: разработчики находятся в одной стране, сервера, с которых непосредственно распространяется троян – в другой, организаторы – в третьей

Неизвестные вновь разместили вредоносный код на сайте писателя Экслера

МОСКВА, 27 янв - РИА Новости. Неизвестные хакеры атаковали сайт писателя Алексея Экслера - в пятницу через один из рекламных скриптов, размещенных на сайте, посетителям ресурса автоматически загружался опасный вирус Carberp, о чем стало известно корреспонденту РИА Новости в ходе попытки посетить сайт.

Предыдущая аналогичная атака была зафиксирована на exler.ru 16 января.

Троянская программа Carberp используется хакерами в том числе для похищения денежных средств из систем дистанционного банковского обслуживания. Владелец атакованного сайта признал наличие проблемы, но сообщил о том, что она была устранена в пятницу примерно в 13.30 мск.

"Проблема уже исправлена. Связана она с рекламным скриптом, в который пробирался вирус. Мы пытались решить эту проблему, но этот рекламный скрипт Trojanская программа использует атаку человек-в-браузере для хищения финансовых данных пользователей. Него использования. Н

Представители компании Trusteer обнаружили новую версию троянской программы Carberp, жертвой которой становятся клиенты французского провайдера широкополосной сети Free. Атака рассчитана на хищения банковской информации, а также данных дебетовых карт жертв с помощью атаки человек в браузере (Man in the Browser, MitB).



<http://updates.drweb.com/> - только для обновлений за 2012-03-02:

Trojan.Carberp.14(2) Trojan.Carberp.15(7) Trojan.Carberp.194
Trojan.Carberp.195 Trojan.Carberp.196 Trojan.Carberp.197 Trojan.Carberp.198
Trojan.Carberp.199 Trojan.Carberp.200 Trojan.Carberp.201 Trojan.Carberp.202
Trojan.Carberp.203 Trojan.Carberp.204 Trojan.Carberp.205 Trojan.Carberp.206
Trojan.Carberp.207 Trojan.Carberp.208(14) Trojan.Carberp.209
Trojan.Carberp.210 Trojan.Carberp.211 Trojan.Carberp.213 Trojan.Carberp.214
Trojan.Carberp.215 Trojan.Carberp.216 Trojan.Carberp.217 Trojan.Carberp.218
Trojan.Carberp.219 Trojan.Carberp.220 Trojan.Carberp.221 Trojan.Carberp.222
Trojan.Carberp.224 Trojan.Carberp.225 Trojan.Carberp.226 Trojan.Carberp.227
Trojan.Carberp.228 Trojan.Carberp.229 Trojan.Carberp.230 Trojan.Carberp.231
Trojan.Carberp.232 Trojan.Carberp.233 Trojan.Carberp.234 Trojan.Carberp.235
Trojan.Carberp.236 Trojan.Carberp.237 Trojan.Carberp.238 Trojan.Carberp.239
Trojan.Carberp.240 Trojan.Carberp.241 Trojan.Carberp.242 Trojan.Carberp.243
Trojan.Carberp.244 Trojan.Carberp.245 Trojan.Carberp.246 Trojan.Carberp.247
Trojan.Carberp.248 Trojan.Carberp.249 Trojan.Carberp.250 Trojan.Carberp.251
Trojan.Carberp.252 Trojan.Carberp.253 Trojan.Carberp.254 Trojan.Carberp.255
Trojan.Carberp.256 Trojan.Carberp.257 Trojan.Carberp.258 Trojan.Carberp.259
Trojan.Carberp.260 Trojan.Carberp.261 Trojan.Carberp.262 Trojan.Carberp.263
Trojan.Carberp.264 Trojan.Carberp.265 Trojan.Carberp.266 Trojan.Carberp.267
Trojan.Carberp.29(14) Trojan.Carberp.33(10) Trojan.Carberp.45(4)
Trojan.Carberp.5(3) Trojan.Carberp.60(6) Trojan.Carberp.61 Trojan.Carberp.80



На данный момент ситуация я **Trojan.Carberp** напоминает ситуацию с прошлогодним WinLock'ом – новые модификации, протестированные заранее на последних версиях антивирусов выходили ежедневно – и естественно антивирусам требовалось время, чтобы начать удалять новый для них вид угрозы. При этом **Trojan.Carberp** гораздо опаснее – если WinLock просто не давал работать и требовал отправки SMS, то **Trojan.Carberp** направлен на длительную работу в системе.

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Современные вредоносные программы:

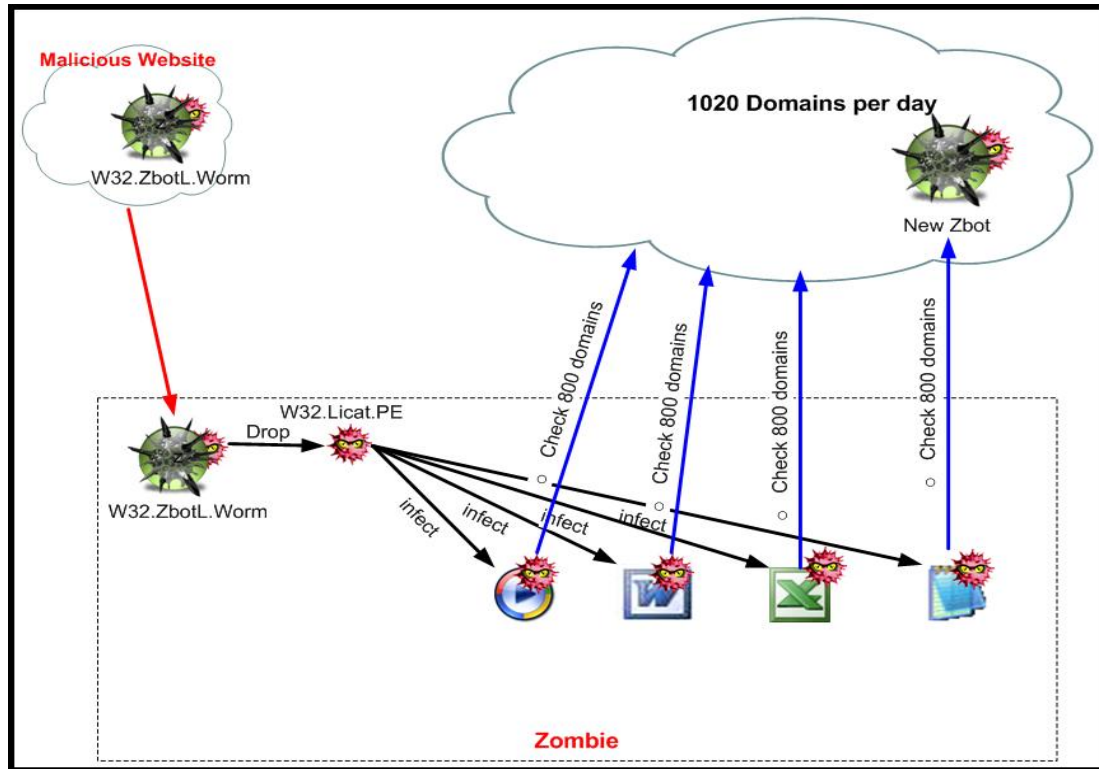
- Создаются профессионалами и на момент создания не обнаруживаются антивирусами - и более того предпринимают попытки удаления антивируса
- Используют самые последние разработки в области создания вредоносного ПО. Тот же **Trojan.Carberp** для перехвата связанной с работой ДБО информации использует различные методы: это логирование нажатий пользователем клавиш, вклинивание в HTTP-трафик в поисках учетных данных и передаваемых значений экранных форм, встраивание в процессы программ системы банк-клиент, создание скриншотов в моменты ввода важной информации, перехваты отдельных функций, которые могут участвовать в передаче данных, поиск и похищение сертификатов и ключей. Все варианты троянцев зашифрованы вирусными упаковщиками. Среди команд, которые способен выполнять **Trojan.Carberp**, имеются директивы запуска произвольных файлов на инфицированном компьютере, команда установки сеанса «удаленного рабочего стола» по протоколу RDP, и даже удаления на зараженном ПК операционной системы. Таким образом **имеется возможность выполнения банковских проводок с использованием удаленного доступа** – в уже имеющейся или параллельной сессии



Современные вредоносные программы:

- Отлично маскируются в системе. **Trojan.Carberp** запускаясь на инфицированной машине, предпринимает целый ряд действий для того, чтобы уйти от средств контроля и наблюдения. После успешного запуска троянец внедряется в другие работающие приложения, а свой основной процесс завершает, таким образом, вся его дальнейшая работа происходит частями внутри сторонних процессов, что является его характерным свойством. **Миф о том, что появление любого вируса можно заметить визуально отжил себя окончательно**
- конкурируют между собой - в **Trojan.Carberp** имеется возможность уничтожения «конкурирующих» банковских троянцев
- действуют в составе ботнетов, управляемых из одного (или нескольких) командных центров. Таким образом зараженная машина или сеть служит еще и источником заражения
- благодаря возможности удаленного управления и возможности использования плагинов имеется возможность организации атаки на конкретную компанию по заказу извне. **На данный момент имеются версии плагинов под большинство известных банковских систем!**





И не забываем о старых угрозах!

Защити созданное



Ситуация 1. В сети уже используется антивирус. Достаточно ли его?

Ситуация 2. В сети установлена в дополнение к антивирусу система распределения доступа и система защита от атак – как правило на уровне рабочих станций. Достаточно ли просто установить защиту?

Что может противопоставить этому системный администратор имея в наличии антивирус? Если он использует только антивирус (или если более точно файловый монитор, отслеживающий файловую активность), то ничего.

Перед выпуском вредоносные программы тестируются на антивирусах и сразу после выпуска не обнаруживаются ими. Через некоторое время новая зараза будет найдена, но за это время деньги уже уйдут.

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Но современный антивирус не равен файловому антивирусу.

С помощью входящей в его состав системы ограничения доступа можно разрешить доступ сотрудникам только к избранным сайтам

Антивирус имеет функцию проверки ссылок – это тоже нужно использовать.

Антивирус может не позволять сотрудникам изменять настройки самостоятельно по причине, что “все тормозит” руководствуясь правилами внесенными через систему централизованного управления

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Антивирус уже установлен? Но достаточно ли одного его?

Все антивирусы рано или поздно начнут ловить новую модификацию, но одни начнут это делать раньше, другие позже (в том числе и в зависимости от того, где находятся их вирусные аналитики). В связи с этим является правильной практика, рекомендованная СТО БР РФ (и реализуемая в банках) по использованию нескольких антивирусов – до того, как файл дойдет до пользователя, он должен быть проверен двумя антивирусами – например на шлюзе и почтовом сервере или почтовом сервере и машине пользователя.

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Рабочие станции защищены, а мобильные устройства нет?

Уже существует первый банковский троянец для платформы Android - Android.SpyEye.1.

При обращении к различным банковским сайтам, адреса которых присутствуют в конфигурационном файле троянца, в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого, которое может включать различный текст или веб-формы. Таким образом, ничего не подозревающая жертва загружает в браузере настольного компьютера или ноутбука веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», а также предложение загрузить на мобильный телефон специальное приложение, содержащее троянскую программу.

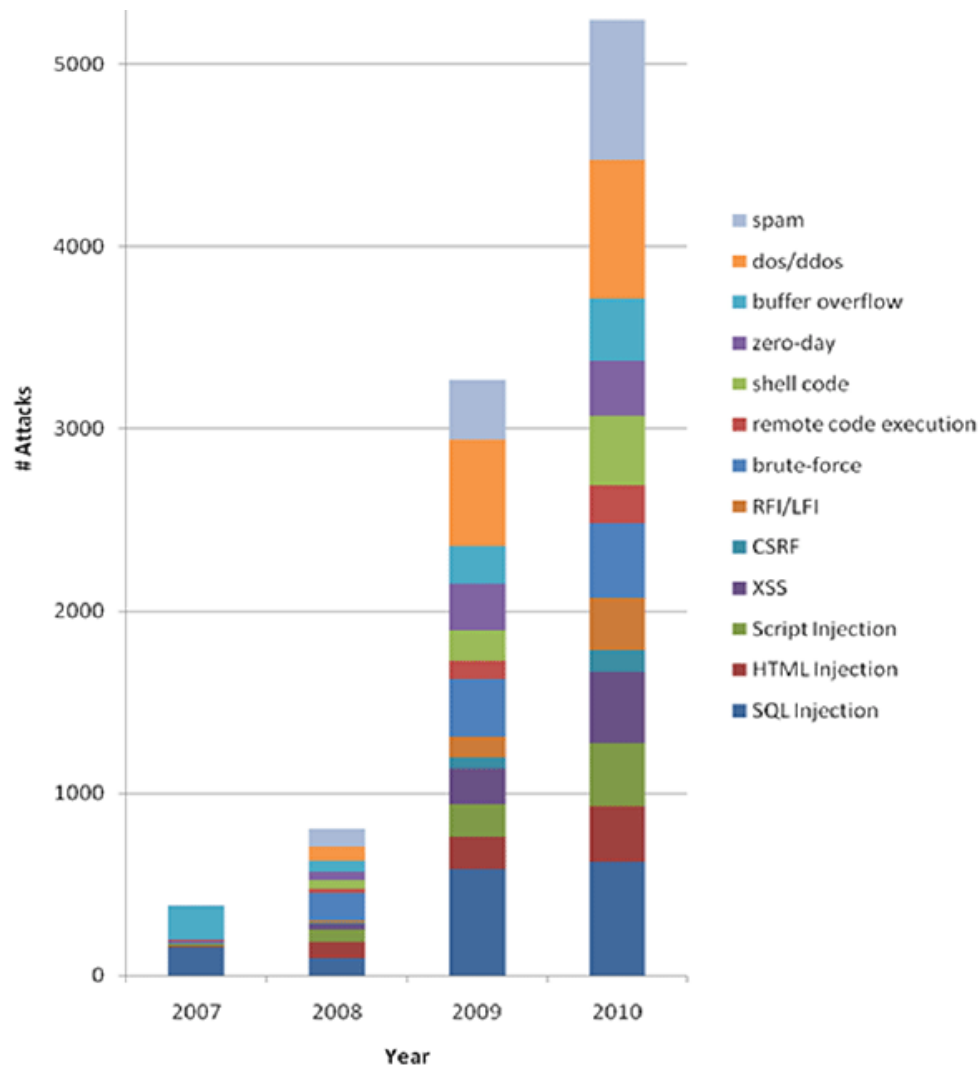
Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com

Попытки проникновения в ДБО будут только увеличиваться



- Количество “интересующихся” всё возрастает
- Успешные взломы широко освещаются
- Мобильность распространяется всё шире



По видам ДБО различают:

- системы Клиент-Банк для физических лиц
- системы Клиент-Банк для юридических лиц
- системы обслуживания по картам VISA и Mastercard

Как правило в компании используются несколько систем – например система Клиент-Банк, обслуживающая счета компании и зарплатные карточки сотрудников

Нужно ли защищать только средства компании или средства сотрудников тоже требуют защиты? Не это ли цена за лояльность?

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com



Remember!

Дюма. Двадцать лет спустя

- Заражен может быть любой компьютер или сервер – вне зависимости от установленной операционной системы. Заражение незащищенного узла сети – лишь вопрос времени. Вирусы создаются не только для рабочих станций и серверов, но и для принтеров и сетевых устройств.
- Как показывает практика, в утечке данных бывают виноваты не только хакеры, но и сотрудники компании, имеющие бесконтрольный доступ к любым данным и не представляющие их ценности.

Защити созданное



Вопросы?

**Благодарим за внимание!
Желаем Вам процветания и еще больших успехов!**

www.drweb.com

Защити созданное



© ООО «Доктор Веб»,
2012

www.drweb.com