Всем салют! Сегодняшняя наша лекция посвящена социальной сети Вконтакте и взлому учетных записей пользователей ее же.

Лекция 1. «Взлом VK»

Мы составили для Вас список методов, которые помогут вам завладеть чужой учеткой. Давайте пробежимся по каждому из них, а затем разберем самые оптимальные способы и выберем, какой же подойдет именно вам в конкретной ситуации.

Обзор

Фишинг

Наверное, самый распространённый метод взлома страниц в социальных сетях.
Суть заключается в создании идентичной по структуре и дизайну страницы, на которой сайт запрашивает логин и пароль. Когда они введены, данные отправляются прямиком в наши руки.

Кейлоггер (клавиатурный шпион)

Этот метод, наверное, самый простой из всех. И к тому же, самый действенный, каким бы опытным не был пользователь, обнаружить кейлоггер, не проводя целенаправленно его поиск – невозможно. Устанавливаем кейлоггер на компьютер жертвы, наше ПО начинает записывать абсолютно всё, что вводится на клавиатуре, и отправляет эти данные нам. Причём нам даже не обязательно иметь доступ к компьютеру, чтобы установить подобную программу. Достаточно лишь заставить жертву запустить файл, который мы ей отправим, завернув в заманчивую и красивую обертку.

Конечно, опытный пользователь не станет запускать неизвестные программы, полученные непонятно от кого, но не стоит забывать, что у всех нас есть родственники, друзья, которые с удовольствием запустят файл с

названием «photo.exe» или что-то в этом роде. А так же о том, что мы можем вшить наше ПО в вполне себе безобидную программу.

Стиллер

Многие люди используют такую функцию в браузере, как «запомнить пароль». Это позволяет им не вводить пароль каждый раз при входе в свой аккаунт. Это довольно опасно для жертвы и опять же, прекрасно для нас. Устанавливаем на компьютер программу, которая будет брать данные из из всех браузеров и отправлять их нам.

Взлом мобильного телефона

Ввиду того, что многие люди используют свои телефоны для того, чтобы заходить в свои социальные сети, взломать их становится проще. Если мы каким-либо образом можем получить доступ к телефону жерты, то сможем получить доступ и к ее страничке ВКонтакте, банку и куче других, потенциально интересных нам вещей. Существует много различных инструментов и приложений для отслеживания чьего-то смартфона. К примеру, Spy Phone Gold и Mobile Spy.

Дубликат СИМ-карты

Самый действенный способ, но требует затрат (Если вы, конечно, не работник одного из сотовых операторов). Стоит нам создать дубликат СИМ-карты и можно считать, что все акки жертвы уже у нас. Стоит такая услуга от 1 до 3к рублей и выполняется сотрудниками-крысами в стане оператора.

Самый опасный способ с точки зрения преследования по закону. Но самый простой в реализации. Если кто-то из вас все же решится, то предоставим по запросу контакты исполнителя. Его лучше использовать для интернет-банкинга, например. Когда на кону большие суммы денег. Лучше все делать не в своем городе. Телефон, ноут (если задействован) – в утиль сразу же после окончания.

Метод подделки DNS

Метод будет работать только в ситуации, когда жертва и мы находимся в одной и той же сети. Этот способ позволяет нам создать фейковую страницу авторизации, и, как результат, получить данные, введённые пользователем и, следовательно, доступ к его странице.

К оружию!

Фишинг

Давайте рассмотрим, как создать фишинговый сайт ВК (по аналогии, подойдет так же и для других соц.сетей и т.д.)

Мы подготовили для вас уже настроенные скрипты страницы входа. (будет приложено к лекции).

Все, что вам остается – это залить готовый скрипт на хостинг и гнать на него жертву.

Могу от себя посоветовать несколько хостингов:
https://www.000webhost.com/ - совершенно бесплатный хостинг.
https://www.host-food.ru// - стабильный и очень дешевый (Иногда администрация может банить, если будут жалобы)

К сожалению вк не пропускает подозрительные ссылки, даже если они предварительно сокращёны.
Поэтому делаем редирект и прогоняе ссылку на наш сайт через blogger.com:
1. Регистрируемся
2.Создаём новый блог
3.в управлении блогом нажимаем изменить HTML
4. Стираем всё и вставляем это:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE html>
```

```
<html b:css='false' b:defaultwidgetversion='2' b:layoutsVersion='3'
b:responsive='true' b:templateUrl='indie.xml' b:templateVersion='1.1.1'
expr:dir='data:blog.languageDirection' xmlns='http://www.w3.org/1999/xhtml'
xmlns:b='http://www.google.com/2005/gml/b'
xmlns:data='http://www.google.com/2005/gml/data'
xmlns:expr='http://www.google.com/2005/gml/expr'>
<meta content='0; url= ' http-equiv='Refresh'/>
<head>
<b:skin version='1.1.0'><![CDATA[
]]></b:skin>
</head>
<body>
<b:section class='footer' id='footer' name='Footer' showaddelement='false'
tag='footer'/>
</body>
</html>
```

***где URL вставляем ссылку на наш фишинг сайт**

5. сохраняем
6. Копируем ссылку на наш блог и уже после всего проделанного сокращаем через vk.cc

Готово!

Кейлоггер

Тут трудностей не возникнет, если только кто-то из вас не пропускал лекции ☺

Используем уже изученный нами sAINT.

Стиллер

Будем использовать платный стиллер Azorult
Вам – бесплатно ☺
Будет прикреплен к лекции.

Его возможности вас порадуют, однозначно:

Функционал:
Стиллер сохраненных паролей, cookies, автозаполнений из браузеров:
- **Google Chrome**
- **Mozilla Firefox**
- **Internet Explorer**
- **Microsoft Edge**
- **YandexBrowser**
- **Opera**
- **InternetMailRu**
- **ComodoDragon**
- **Amigo**
- **Bromium**
- **Chromium**
- **360Browser**
- **Nichrome**
- **RockMelt**
- **Vivaldi**
- **GoBrowser**
- **Sputnik**
- **Kometa**
- **Uran**
- **QIPSurf**
- **Epic**
- **Brave**
- **CocCoc**
- **CentBrowser**
- **7Star**
- **ElementsBrowser**
- **TorBro**
- **Suhba**
- **SaferBrowser**
- **Mustang**
- **Superbird**
- **Chedot**
- **Torch**
- **Waterfox**
- **Cyberfox**
- **Comodo IceDragon**
- **PaleMoon**

(Cookies в формате Netscape, в админке имеется конвертер в JSON)

Стиллер сохраненных паролей из:
Почтовые клиенты
- **Outlook**
- **Thunderbird**

FTP клиенты
- **Filezilla**
- **WinSCP**

IM-клиенты
- **Pidgin**
- **PSI**
- **PSI Plus**

Стиллер криптокошельков:
Anoncoin, Armory, BBQcoin, Bitcoin Core, Bytecoin, Craftcoin, DashCoin, Devcoin, Digitalcoin, Electrum, Fastcoin, Feathercoin, Florincoin, Franko, Freicoin, GoldCoin, I0coin, Infinitecoin, Ixcoin, Junkcoin, Litecoin, Luckycoin, Megacoin, Mincoin, Monero, MultiBit, Namecoin, NovaCoin, Phoenixcoin, PPCoin, Primecoin, ProtoShares, Quarkcoin, Tagcoin, Terracoin, Worldcoin, Yacoin, Zetacoin

Стиллер переписки из Skype
Стиллер куки-файлов Telegram, по которомы можно попасть на аккаунт
Стиллер файлов клиента Steam (ssfn+vdf)
Возможность сделать снимок экрана в процессе работы стиллера (screenshot)

Мощный граббер файлов:
- Возможность указывать стартовые каталоги для поиска
- Фильтр по маске имени файла
- Фильтр по размеру файла
- Обработка подпапок
- Обработка ярлыков
- Исключения

Сбор системной информации:
- Список установленных программ и их версий
- Древовидный список запущенных процессов
- Информация о процессоре, видеокарте, ОЗУ, разрешении экрана, раскладках клавиатуры, таймзоне, имя пользователя, компьютера, версия ОС

Встроенный лоадер:
- После отправки отчета может скачать и запустить указанный файл

Нужный функционал включается/выключается в админке

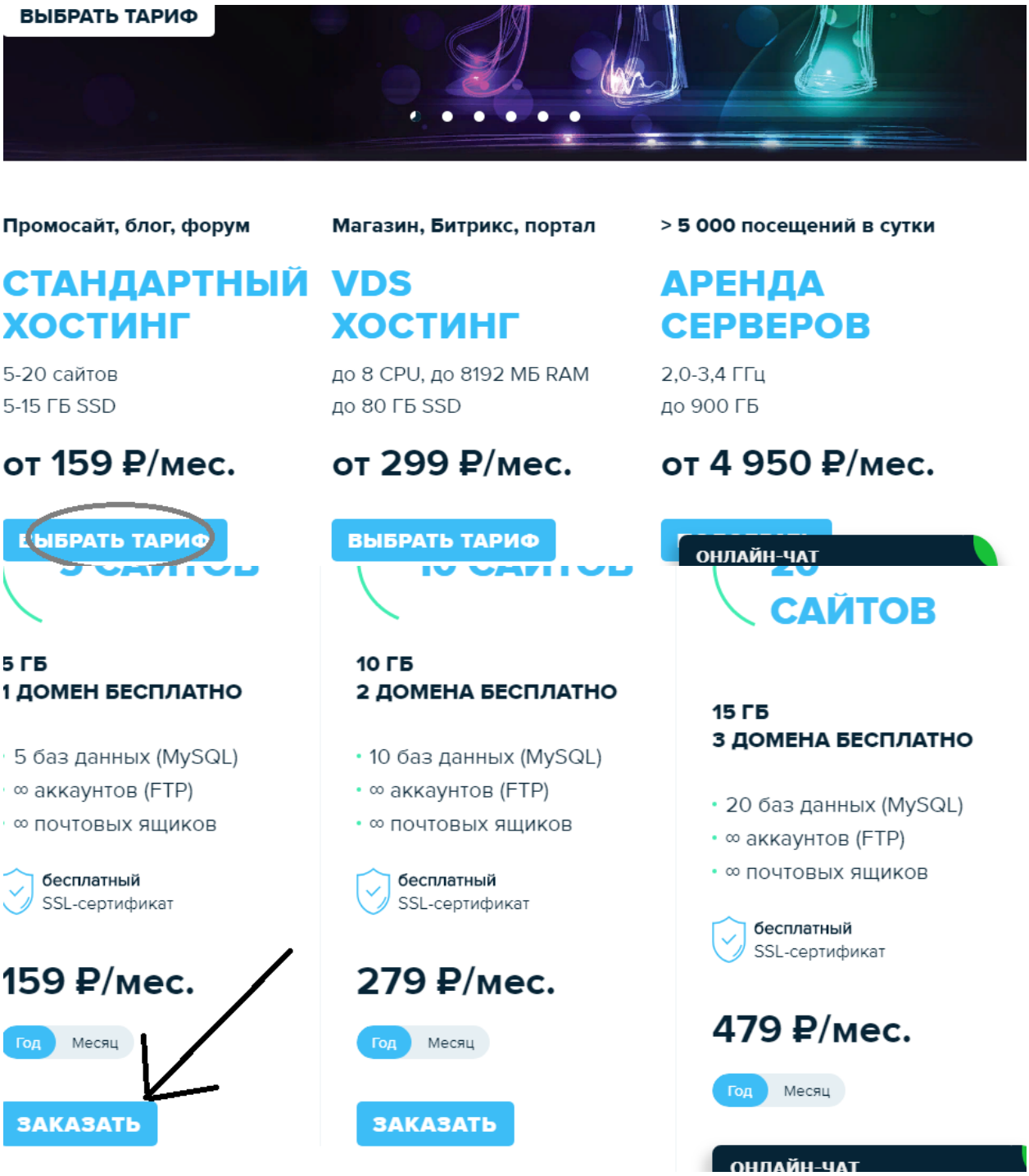
Админка
- Устанавливается на ваш хостинг
- Имеет различные фильтры в списке отчетов и паролей.
- Возможность скачать отчет с машины, который представляет из себя zip-архив с данным

Дополнительные функции
- Стиллер умеет перезапускаться от имени юзера, если запущен от имени системы
- Самоудаление после отправки отчета (включается в админке)
- Поддержка .bit доменов
- Возможна сборка в dll

Установка:

Проходим регистрацию на хостинге Sweb

Сразу говорю, хостинг бесплатный, точнее с тест периодом, просто читайте и смотрите внимательно !



Дальше все стандартно, пишем почту, вводим каптчу, регистрируем аккаунт..
После регистрации на почту придет письмо, где будут данные для входа в панель управления и FTP

SpaceWeb <no-reply@sweb.ru> чт, 10 янв., 17:10 (5 дн. назад)
кому: я

Здравствуйте!

Добро пожаловать в SpaceWeb! Ваш аккаунт успешно создан и полностью готов к работе.

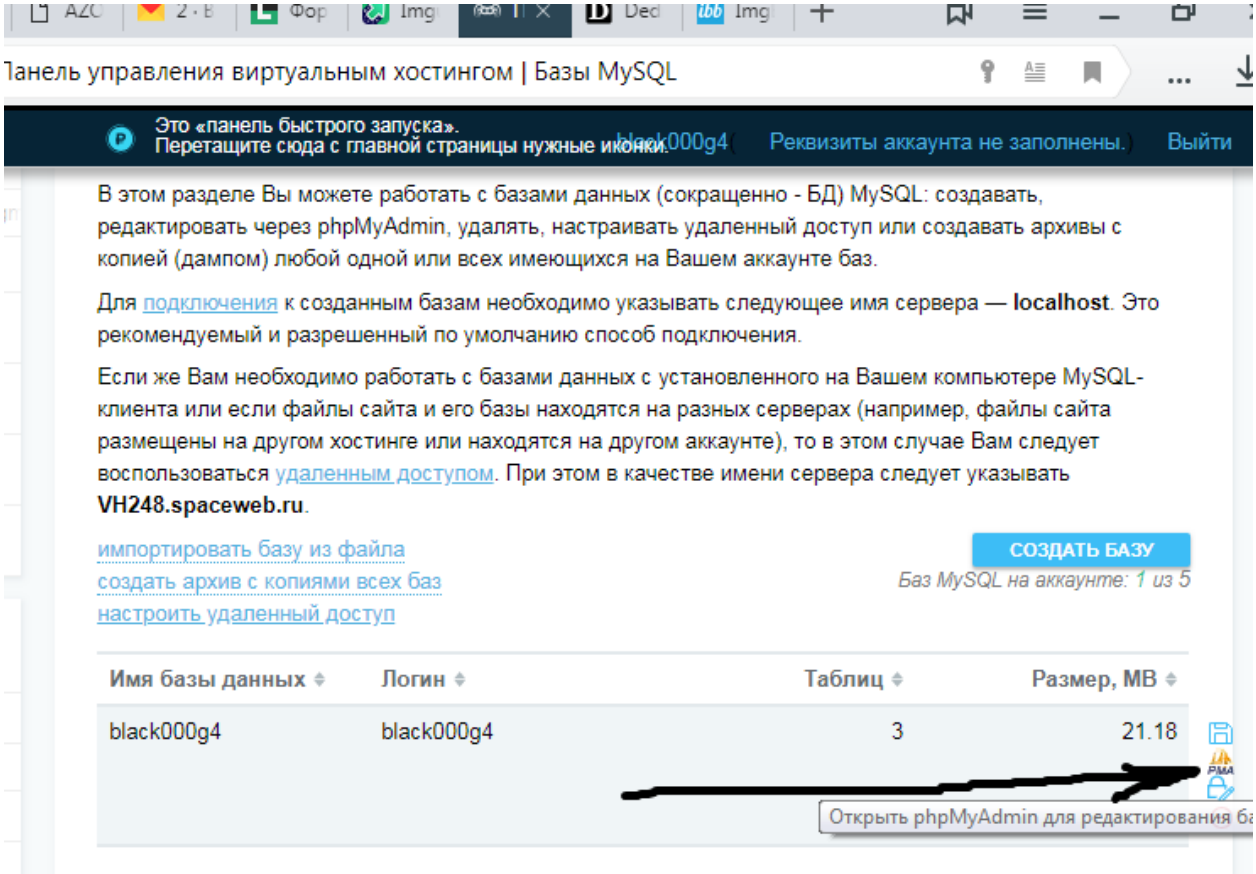
Вам предоставлен тестовый период: в течение 14 дней вы можете совершенно бесплатно пользоваться хостингом и лично убедиться в его надежности!

ИНФОРМАЦИЯ О ЗАКАЗЕ
Виртуальный хостинг на 1 мес. по тарифному плану Взлёт: 199 руб.
Доменное имя: нет
Итого (сумма к оплате): 199 руб.

ДАННЫЕ ДЛЯ ВХОДА В ПАНЕЛЬ УПРАВЛЕНИЯ, FTP- И SSH-ДОСТУПА:
Логин
Пароль:
IP-адрес сервера:

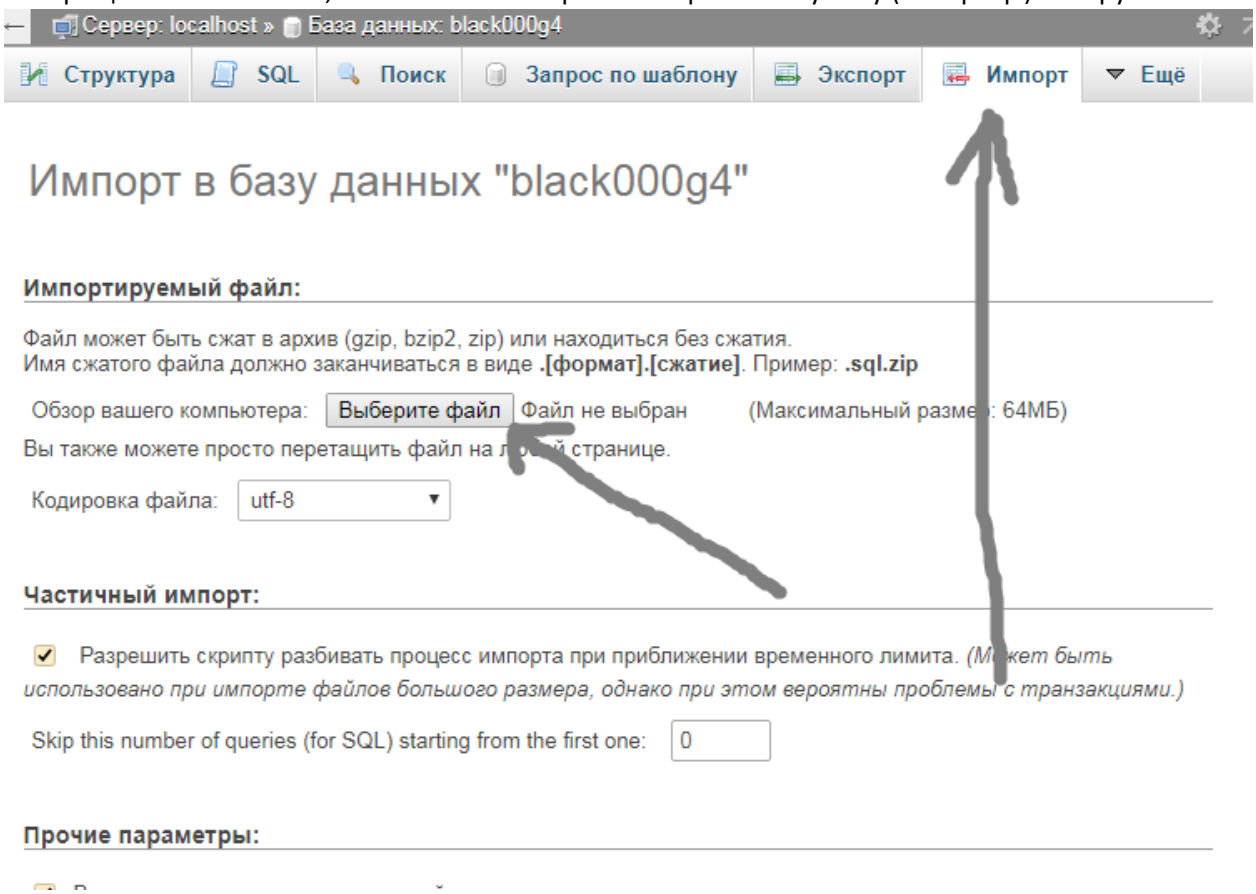
Качаем Filezilla, вводим Ip адрес сервера, логин, пароль и подключаемся к серверу.. Сворачиваем Filelzilla **(не закрываем и идем дальше)**

Переходим на хостинге в панеле управления в раздел Базы MYSQL. Создаем базу, придумываем пароль (логин дан по умолчанию), далее нажимаем сюда



вводим придуманный вами пароль от базы..
Далее просто открываем папку со стиллером, переходим в папку panel - panel - info и копируем файл dump.sql на рабочий стол.

Возвращаемся на хостинг, Нажимаем "импорт" - выбираем нашу базу (dump.sql) и загружаем

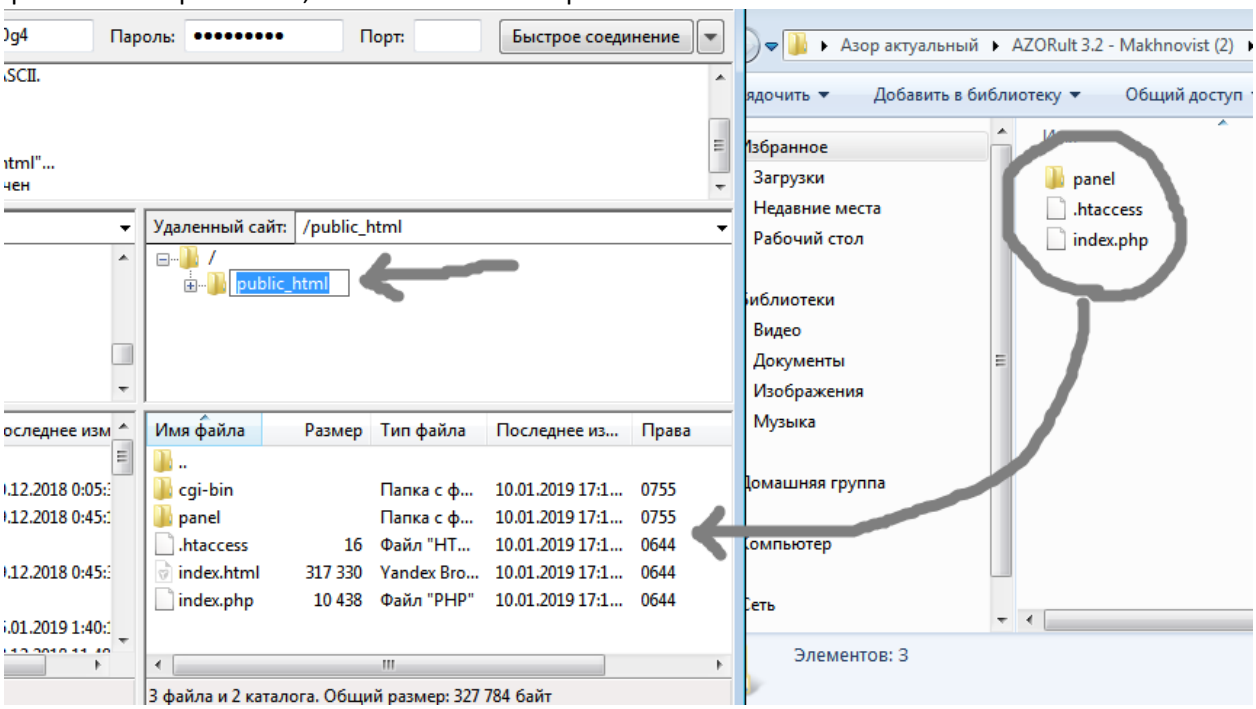


Далее качаем Notepad ++ , переходим в папку со стиллером, находим файл index.php , открываем его через Notepad ++ , и прописываем имя базы 9 совпадает с базой) и пароль от базы , как на скрине

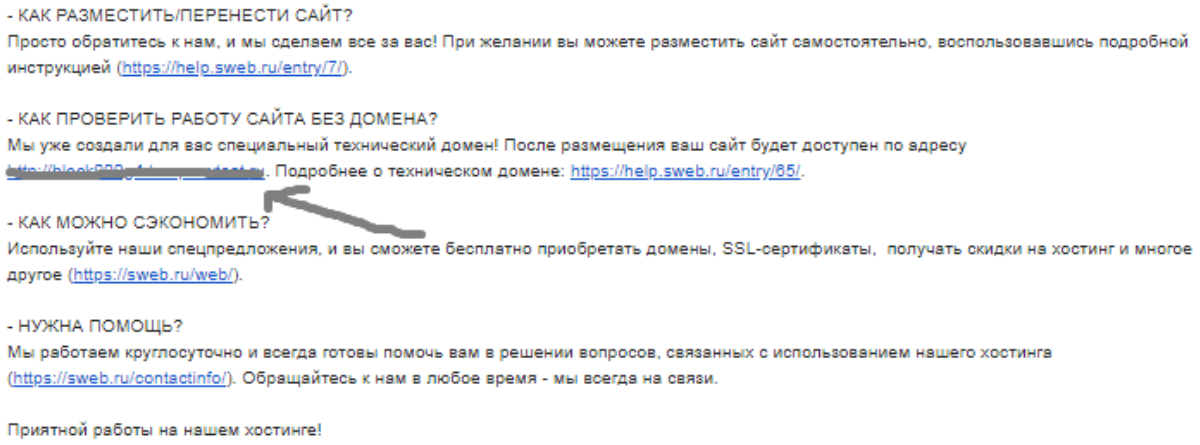
```
//                  !!! ВНИМАНИЕ !!!
//      Кодировка этого файла UTF-8 без BOM
//      И после изменения данных она должна остаться такой-же
//      Для редактирования этого файла не используйте стандартный блокнот windows! Он сбивает кодировку
//      Используйте редактор файлов в ПУ сервера(cPanel/ISP)
//      Или используйте Notepad++ ( https://notepad-plus-plus.org/ )
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////

    define('PANELPATH',     ".//panel/");       //Путь к админке, изменить только panel, слэши не трогать!
    define('DB_HOST',       'localhost');       //Сервер базы данных, без необходимости не менять!
    define('DB_USER',       '[redacted]');          //Имя пользователя БД. Заменить root на имя пользователя
    define('DB_PASS',       '[redacted]');              //Пароль пользователя БД. Вписать между кавычек пароль
    define('DB_NAME',       '[redacted]');      //Имя базы данных. Заменить azorult2 на имя базы
    define('ADMIN_PWD',     '444');             //Пароль в админку. Заменить 123 на новый пароль



////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////
```

Дальше открываем нашу настроенную Filezill-у , нажимаем на папку publik_html и перетаскиваем

файлы стиллера на хост, в точности как на скрине:



Осталось совсем немного, на пути к успеху. Переходим на нашу почту, открываем письмо от хостинга, находим тестовый домен, который они предоставили:


- КАК РАЗМЕСТИТЬ/ПЕРЕНЕСТИ САЙТ?
Просто обратитесь к нам, и мы сделаем все за вас! При желании вы можете разместить сайт самостоятельно, воспользовавшись подробной инструкцией (https://help.sweb.ru/entry/7/).

- КАК ПРОВЕРИТЬ РАБОТУ САЙТА БЕЗ ДОМЕНА?
Мы уже создали для вас специальный технический домен! После размещения ваш сайт будет доступен по адресу [redacted]. Подробнее о техническом домене: https://help.sweb.ru/entry/65/.

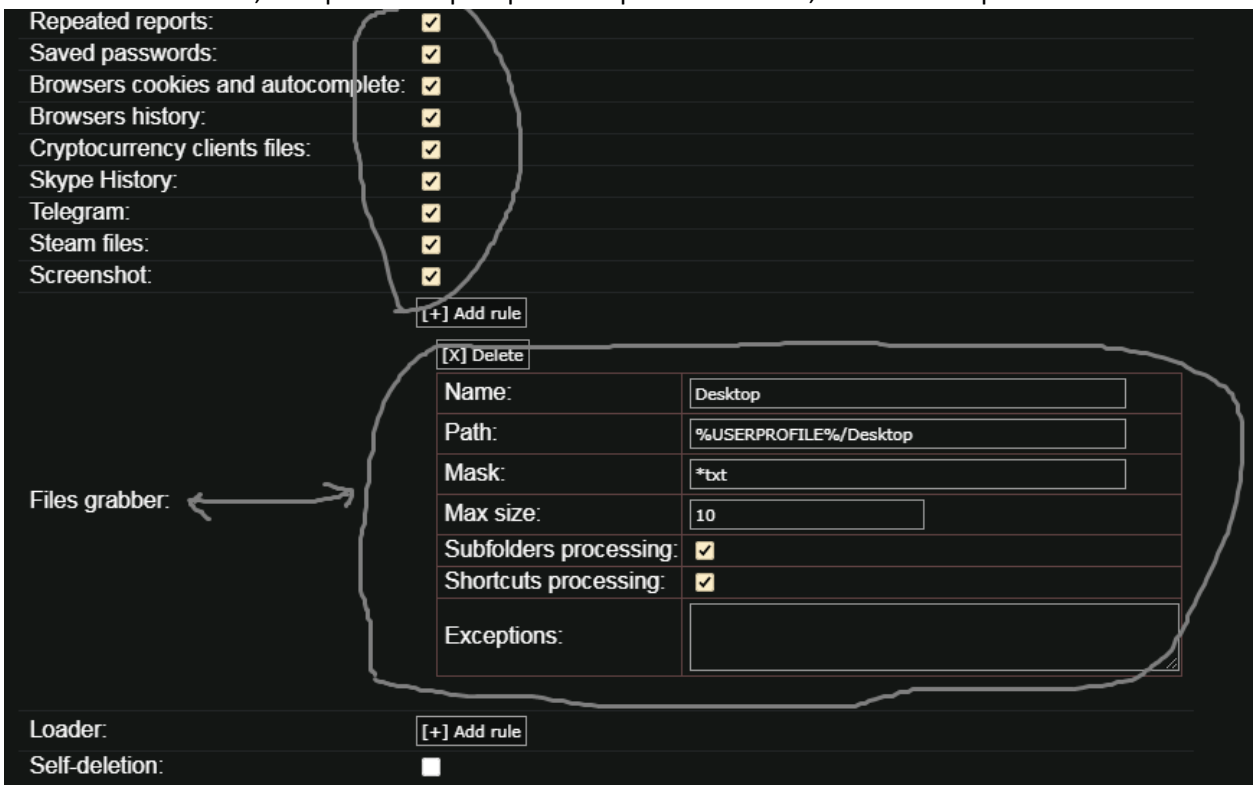
- КАК МОЖНО СЭКОНОМИТЬ?
Используйте наши спецпредложения, и вы сможете бесплатно приобретать домены, SSL-сертификаты, получать скидки на хостинг и многое другое (https://sweb.ru/web/).

- НУЖНА ПОМОЩЬ?
Мы работаем круглосуточно и всегда готовы помочь вам в решении вопросов, связанных с использованием нашего хостинга (https://sweb.ru/contactinfo/). Обращайтесь к нам в любое время - мы всегда на связи.

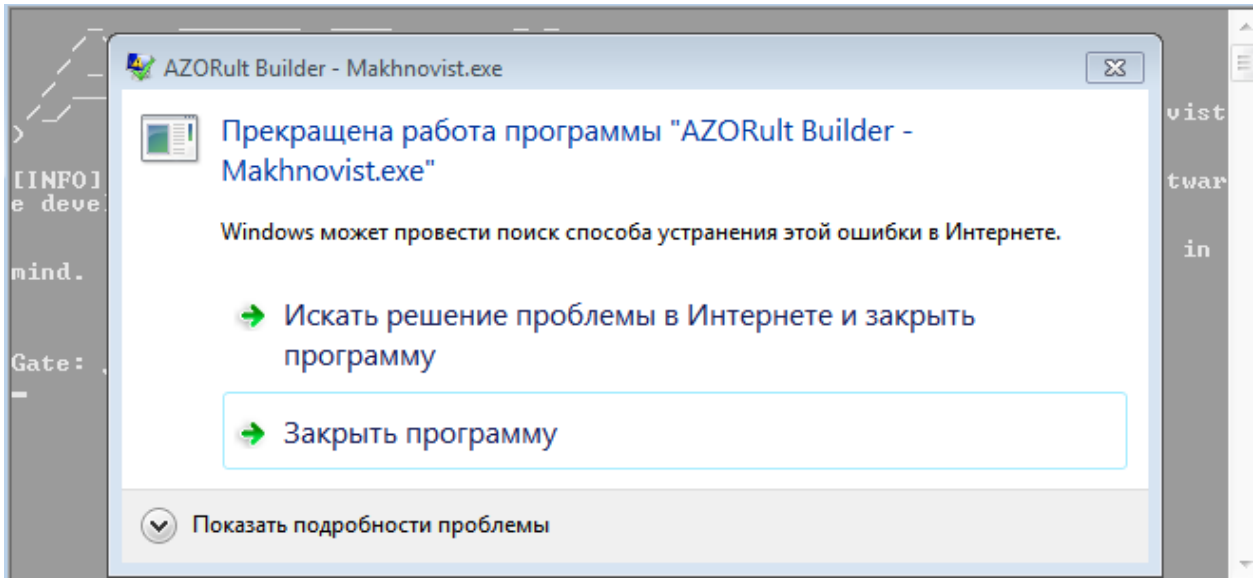
Приятной работы на нашем хостинге!

Далее пишем ссылку: Ваш Домен/panel/admin.php , вставляем ее в браузер и попадаем на админ панель вашего стиллака.. Вводим пароль (редактируется в index.php, забыл упомянуть, на скрине видно) и заходим в админку.

Ставим все галочки , Настраиваем граб файлов с рабочего стола, все как на скрине



Открываем билдер и прописываем ссылку: http://Вашдомен/index.php . Далее ваш билд добавится в папку с билдером. Если выскочит такая ошибка:



ничего страшного , просто закройте.

Далее заходим в папку с билдером, и находим там непонятный файл с названием bin. Открываем свойства файла и дописываем расширение, что бы получилось bin.exe. Это и есть Ваш вирус, открыв который жертва нарвется на вашу ярость и мощь !