Статья Создаем RAT для ANDROID с помощью простого конструктора AhMyth

Благодаря стараниям Илона Маска сегодня можно управлять «Теслой» , не умея водить машину. А благодаря разработчику, который скрывается под ником AhMyth (и так же назвал свою программу), любой желающий может создать троян для Android, совершенно не умея программировать. Как? Сейчас покажу.

Термином RAT (Remote Access Tool) принято называть утилиты удаленного администрирования. Они могут использоваться в благих целях по своему прямому назначению, как, например, знаменитый TeamViewer, а могут устанавливаться злодеями в глубокой тайне от пользователя. В подобных случаях RAT нередко расшифровывают как Remote Access Trojan, и прямой перевод английского слова rat — «крыса» — тут приходится как нельзя кстати.

AhMyth RAT (Remote Access Trojan) — это приложение с открытым исходным кодом, в настоящее время находится на стадии бета-версии. Программа ориентирована на пользователей Windows, но на GitHub можно найти исходники и для Unix-подобных платформ.

AhMyth RAT состоит из двух компонентов.

1. Серверное приложение, с помощью которого можно управлять зараженным устройством и генерировать файлы APK с вредоносным кодом. Создано оно на Electron framework — фреймворке, разработанном в GitHub для создания простых графических приложений.

2. Клиент ский APK, содержащий вредоносный код, который позволяет получить удаленный доступ к зараженному устройству. То есть наш APK будет выпол нять функции бэкдора.

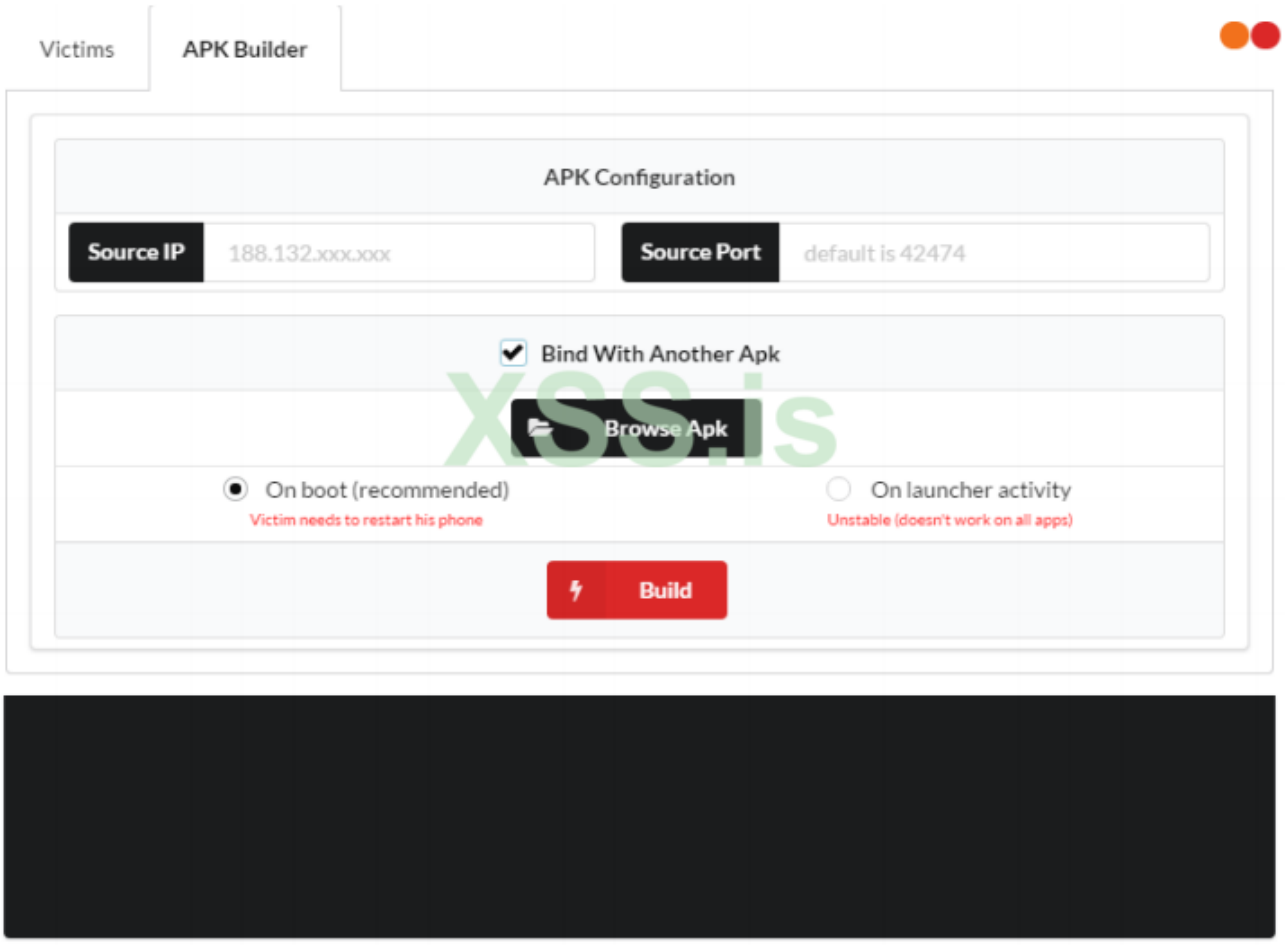
УСТАНОВКА AHMYTH RAT

Серверная часть устанавливается очень просто, тем более автор выложил в свободный доступ бинарники программы. Но при желании можно скомпилировать ее из исходников. Лично я проводил свои тесты на машине под управлением Windows 10.

Для работы утилиты нам необходима виртуальная машина Java. Устанавливаем ее с официального сайта . Затем нужно скачать бинарники самой AhMyth. Их ты можешь найти в официальном репазитории, вкладка Assets. При скачивании лучше отключить антивирус, чтобы его не хватил удар от про исходящего.

СОЗДАЕМ ЗАРАЖЕННЫЙ APK

Что бы создать файл APK для Android, открой вкладку APK Builder. Внешний вид конструктора вредоносных мобильных приложений показан на следующей иллюстрации.



Вкладка с конструктором APK

Пользоваться этим инструментом очень просто. В окне Source IP мы прописываем IP-адрес атакующей машины (этот адрес потом легко вычисляется при исследовании вредоноса). В поле Source Port ты можешь указать порт, который будет зарезервирован машиной для прослушивания подключений. По умолчанию используется порт 42 474.

Без использования дополнительной опции Bind With Another Apk ты сгенерируешь мобильное приложение только с вредоносным кодом. И это практически бесполезно, поскольку заставить юзера установить такую программу можно разве что под пытками.

Но есть проверенный способ создания малвари, который используют все продвинутые вирмейкеры: найти в интернете какой-нибудь APK и склеить его с вредоносом. Для этого поставь флажок Bind With Another Apk, выбери нужный APK и укажи метод интеграции вредоноса в телефон. Есть два метода: при запуске зараженного APK или при перезагрузке телефона после установки RAT. Авторы программы рекомендуют второй вариант.

Осталось нажать кнопку Build — по умолчанию зараженный файл сохраняется в папку **C:\Users\<Your_Username>\AhMyth\Output**.

РАСПРОСТРАНЕНИЕ И ЗАРАЖЕНИЕ

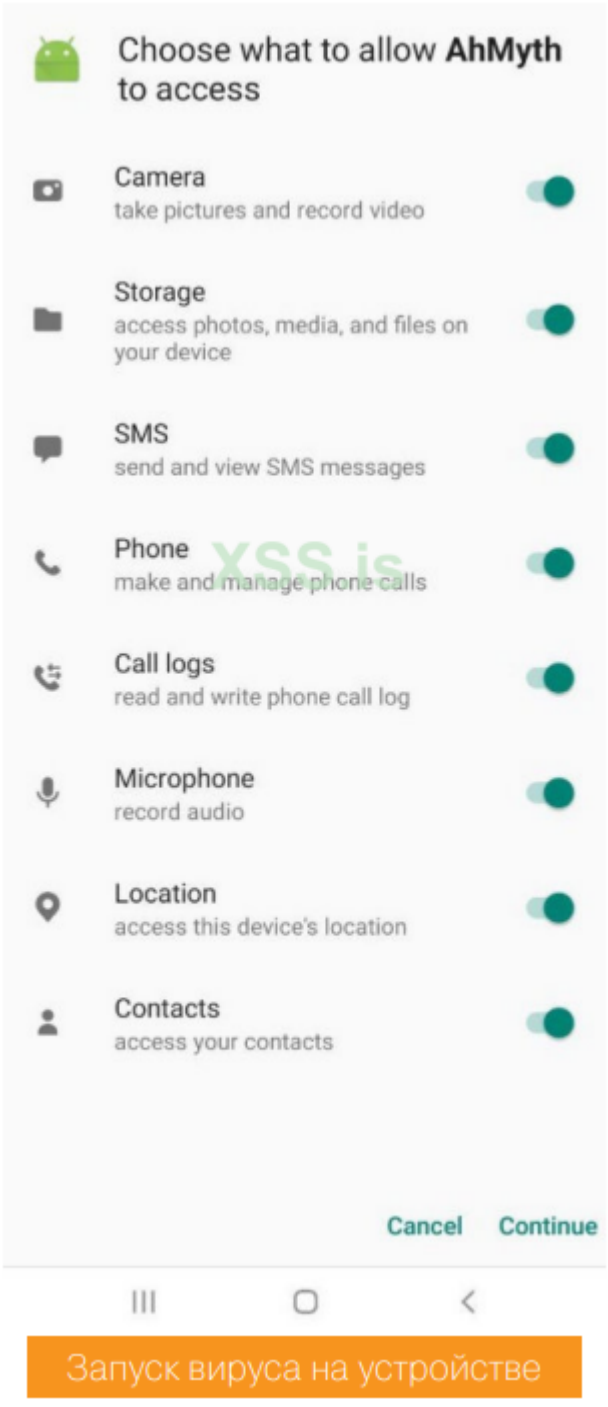
Как распространяются собранные таким методом вредоносы — это отдельная тема для дискуссий. Отмечу только, что в Google Play регулярно обнаруживают зараженные RAT программы и столь же регулярно их оттуда выпиливают, что не мешает малвари появляться в этом каталоге снова. Кроме того, методы социальной инженерии никто не отменял. Но помни, что для активации трояна после установки приложения обязательно нужно запустить или перезагрузить зараженное устройство (в зависимости от настроек билдера).

Для успеха также требуется, чтобы в настройках целевого устройства был отключен параметр «Установка только из доверенных источников».

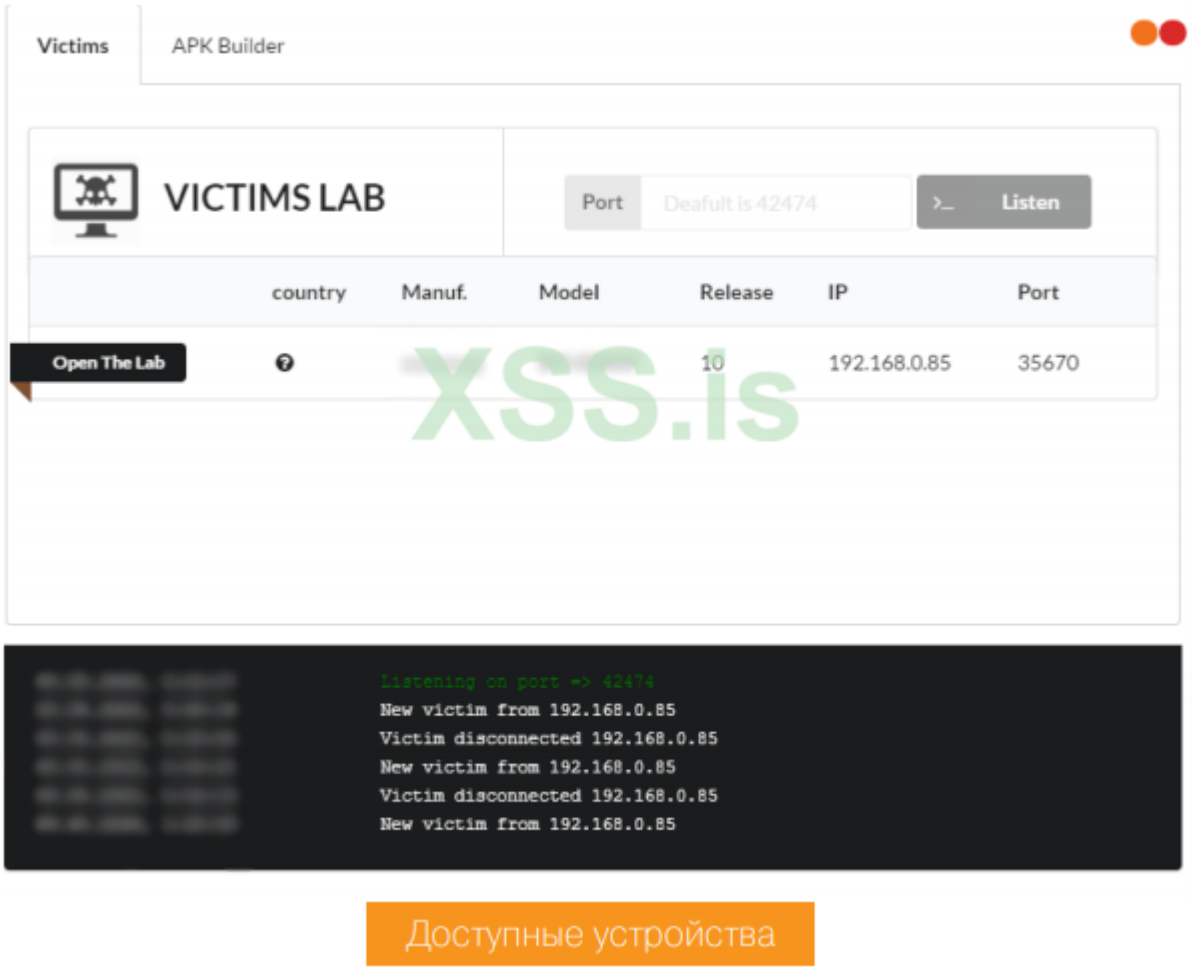
СОЕДИНЯЕМСЯ С ЗАРАЖЕННЫМ УСТРОЙСТВОМ

Теперь нам нужно перейти во вкладку Victims и вбить в поле тот же порт, что мы указывали раньше, чтобы сервер ждал подключений от зараженных устройств. Опять же если ты ничего не менял при сборке APK, то ничего не надо указывать и здесь.

Нажимаем на Listen, и, если наш APK успешно заразил мобильное устройство, мы увидим новое подключение.



Запуск вируса на устройстве



Программа также логирует все действия в консоли, расположенной в нижней части окна. Значения колонок журнала в целом очевидны. Country — страна, в которой работает зараженное устройство. Manuf — компания — изготовитель девайса. Model — код или название модели устройства. Release — версия операционной системы зараженного девайса (в моем случае это Android 10). IP — IP-адрес устройства, а Port — порт, через который инфицированный девайс подключился к атакующей машине. Теперь пора переходить к активным действиям — для этого смело жми на кнопку Open The Lab.

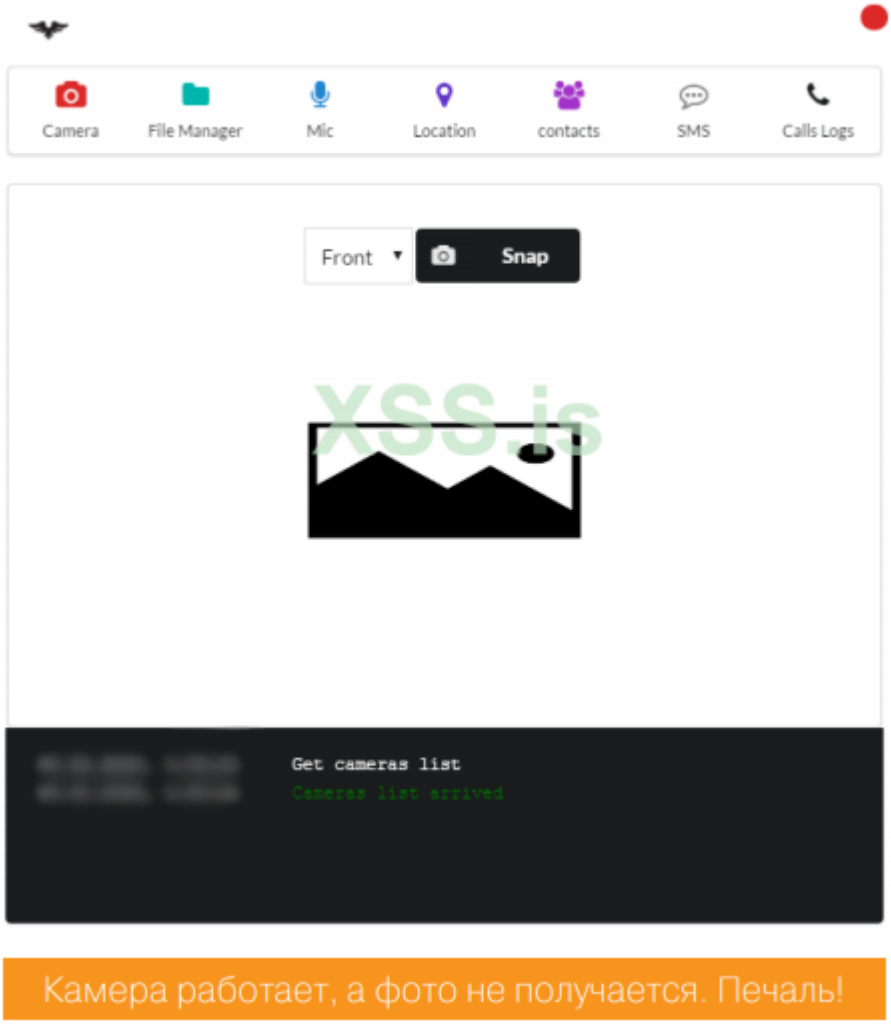
ВОЗМОЖНОСТИ АНМУТН

Нашему вниманию будет предложено меню из семи пунктов, которое открывает доступ к разным функциям программы.

> При подключении к устройству возможны небольшие перебои в работе сервера, однако потом подключение восстанавливается. Немного терпения!

Камера

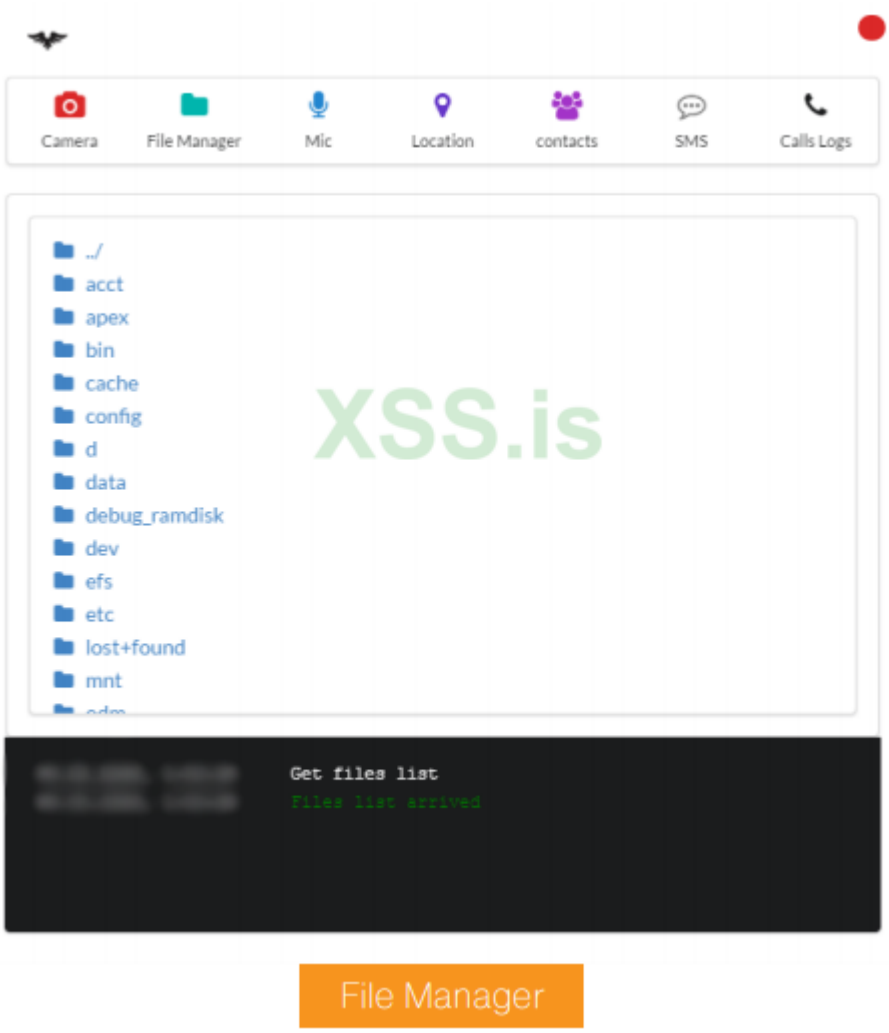
Для начала заглянем в раздел Camera. Выбери камеру: фронталку (Front) или основную (Back) — и можешь сделать снимок нажатием на кнопку Snap. Правда, у меня почему-то не получилось толком сфотографировать, хотя все мои камеры на устройстве были успешно инициализированы.



Камера работает, а фото не получается. Печаль!

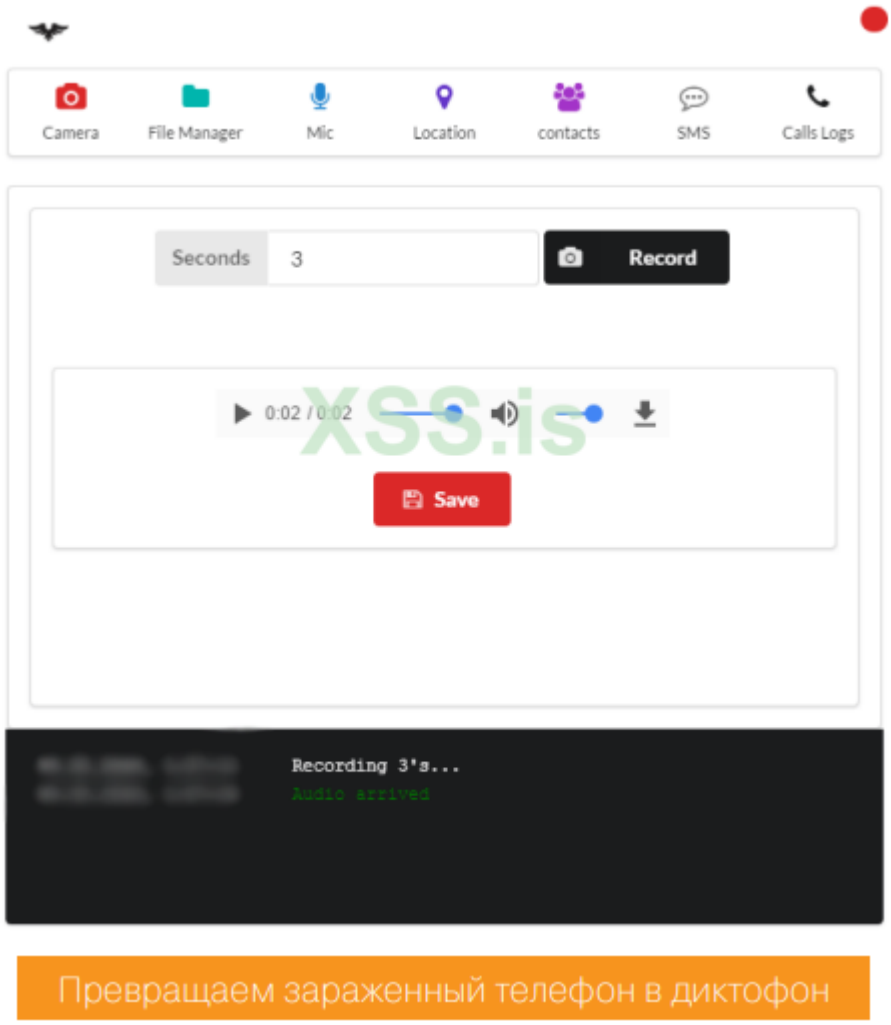
Файловый менеджер

Файловый менеджер здесь не такой продвинутый, как в других подобных утилитах, однако все равно это очень полезная вещь. С его помощью можно как минимум скачивать нужные нам файлы с зараженного устройства. Как видишь, начальная директория — это корневой каталог, к которому есть доступ только с правами администратора.



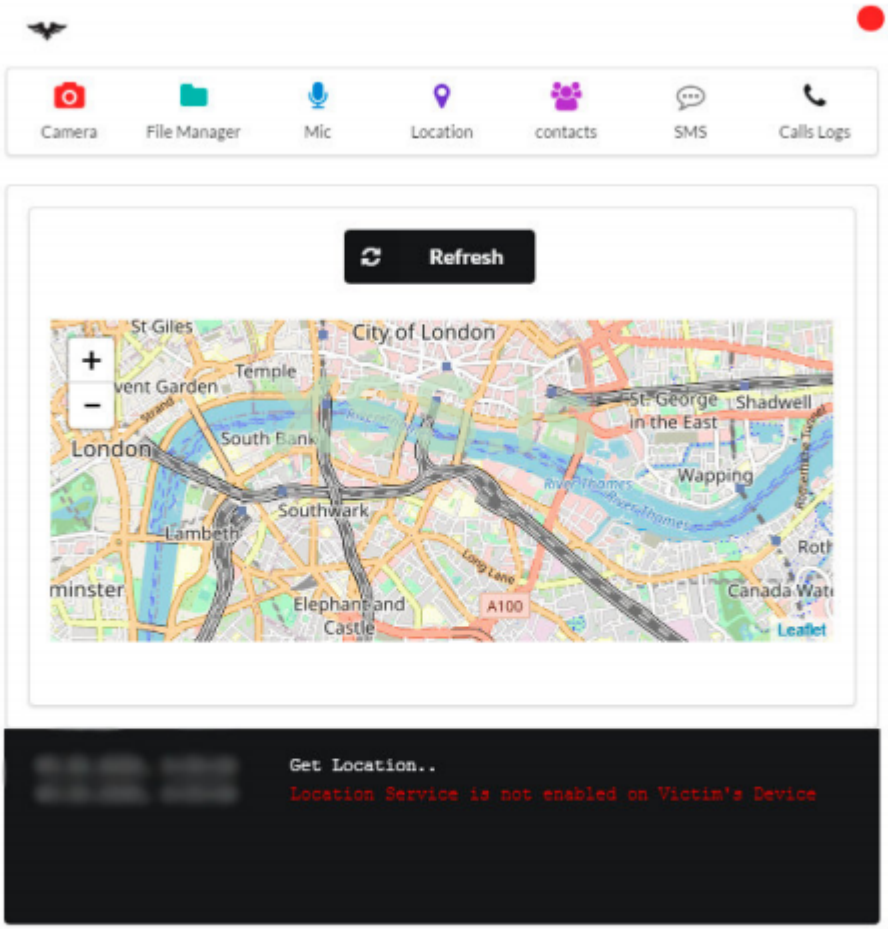
Микрофон

Эта функция позволяет использовать микрофон устройства в фоновом режиме и записать все, что «слышит» телефон в течение указанного времени (в окне Seconds нужно числом задать продолжительность записи в секундах). Далее жмем Record и ждем. Полученный файл можно прослушать прямо в окне программы или сохранить себе на машину.



Геопозиция

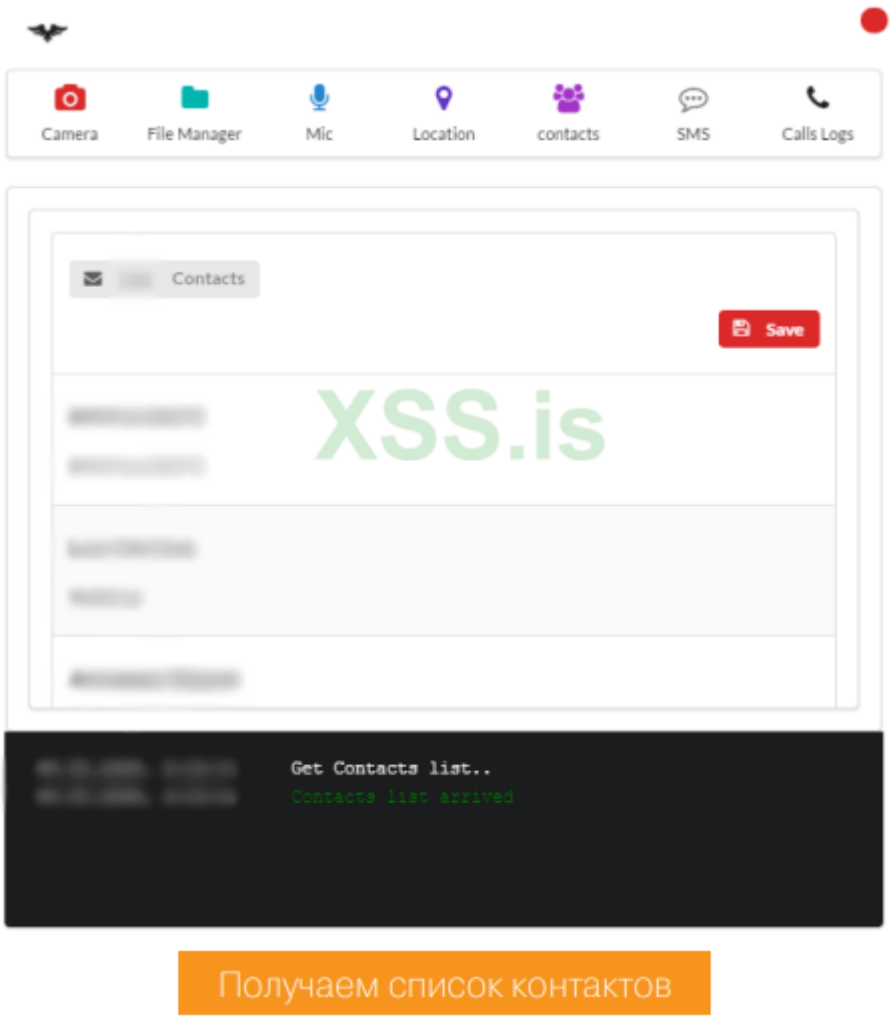
На мой взгляд, это самая интересная возможность AhMyth. Если на инфицированном устройстве включена передача геоданных, ты сможешь узнать геопозицию человека с точностью до десяти метров. Известно, что неопытные пользователи очень редко вспоминают об этом параметре и оставляют его включенным. Плюс некоторые приложения (те же карты), использующие передачу геоданных, когда-нибудь да заставят человека включить эту функцию.



Тут можно узнать геопозицию зараженного телефона

Контакты

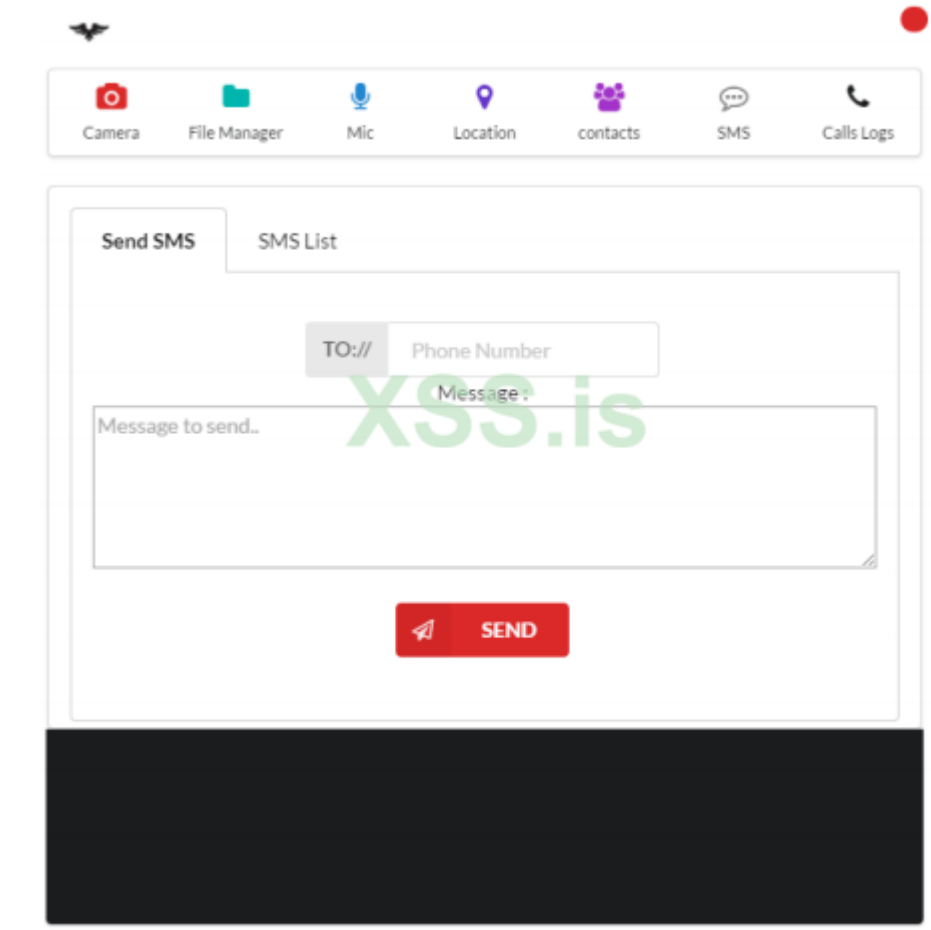
С помощью этой функции можно вытащить весь список контактов, которые записаны в телефоне. Есть возможность скачать весь список контактов себе на машину.



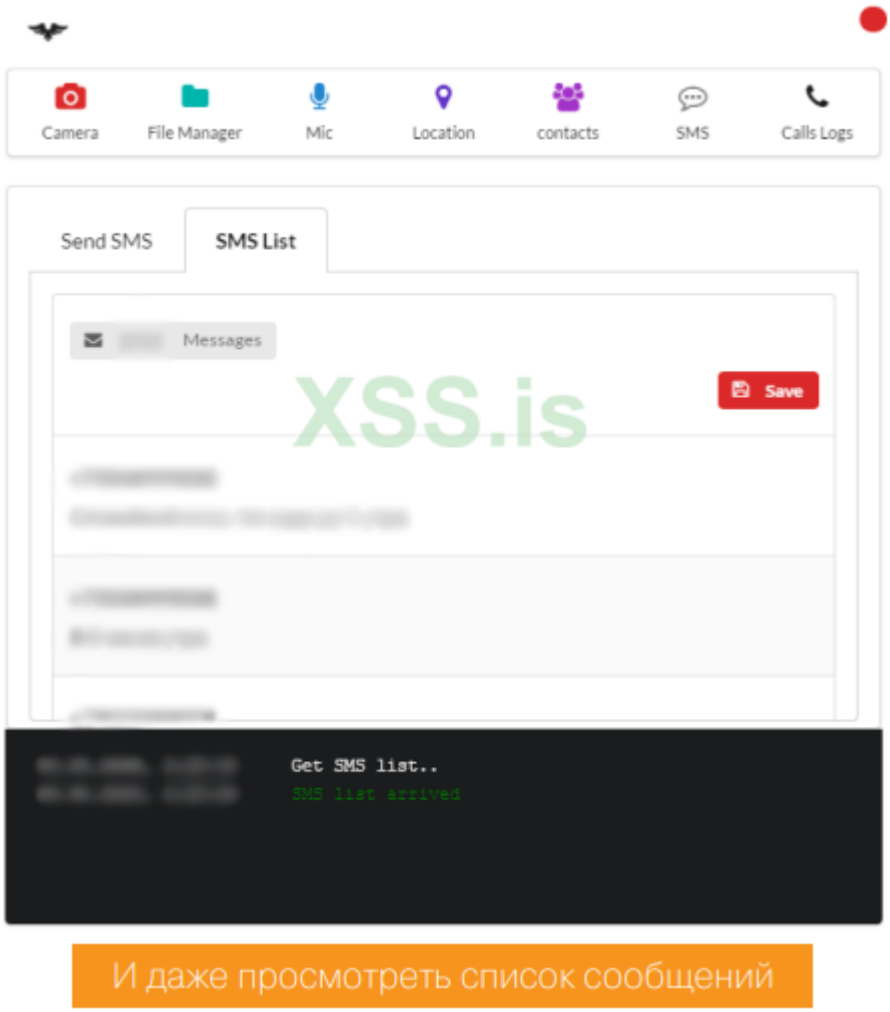
Получаем список контактов

SMS

Еще один очень любопытный раздел. С его помощью мы можем отправить кому-то SMS или просмотреть и скачать все сообщения, которые пришли на это устройство. Что бы отправить SMS, зайди во вкладку Send SMS, укажи номер телефона получателя (поле TO://), а в поле Message вбей желаемый текст сообщения. После этого останется только нажать на кнопку SEND. Эту функцию можно использовать для сброса паролей учетных записей владельца зараженного устройства, например для взлома «Вконтакте» или Instagram.



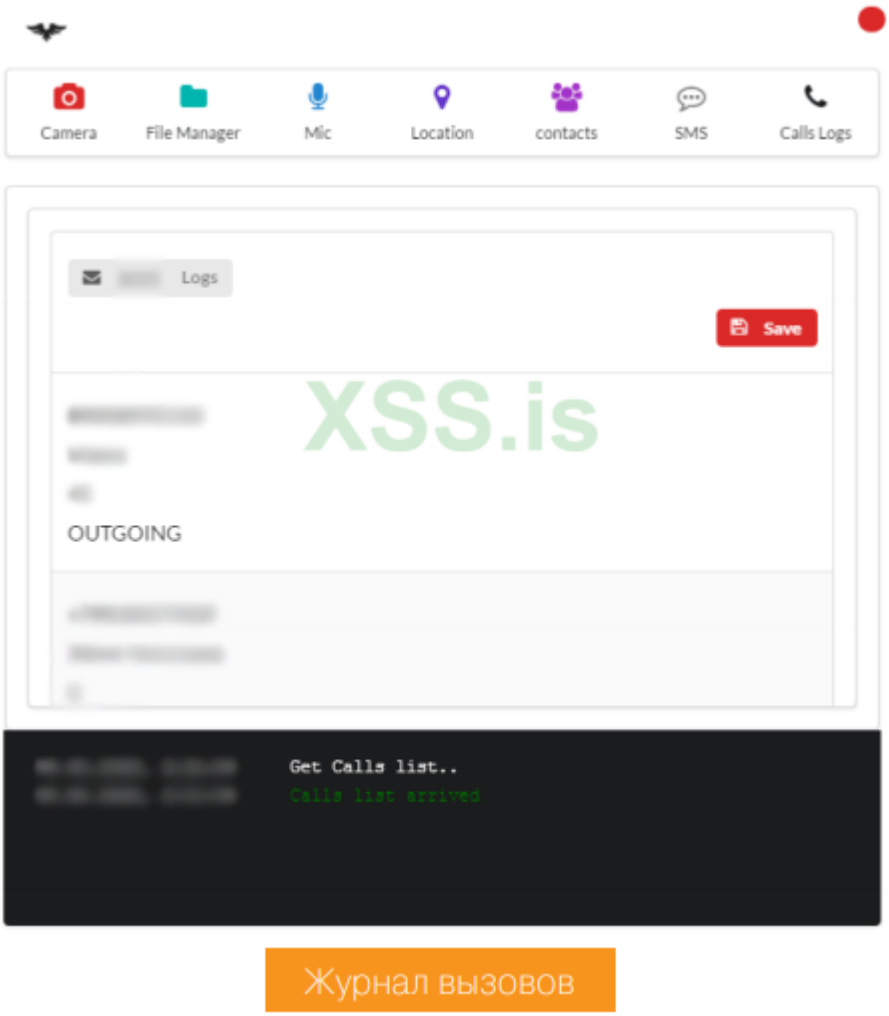
Мы можем отправить сообщение любому получателю



И даже просмотреть список сообщений

Журнал вызовов

Этот раздел открывает перед нами возможность просмотреть список телефонных вызовов. Тут представлено четыре блока информации о каждом вызове: номер, с которым связывалось зараженное устройство; название контакта, к которому привязан этот номер на зараженном устройстве; время длительности вызова (в секундах); тип вызова (входящий или исходящий).



Очень полезный инструмент — разумеется, в умелых руках.

КАК ЗАЩИТИТЬСЯ ОТ RAT?

Как бы банально это ни звучало, никогда не давай свой телефон в чужие руки и не устанавливай сомнительные приложения. На самом деле это практически единственный способ обеспечить собственную безопасность. И конечно же, всегда обращай внимание на предупреждения системы о возможном вреде, который может причинить устройству скачанное приложение.

НАПУТСТВИЕ

Надеюсь, что ты будешь использовать утилиту AhMyth RAT только в исследовательских целях на своих личных устройствах. Не забывай: "Чем больше сила, тем больше и ответственность".][

AhMyth/**AhMyth-Android-RAT**

Android Remote Administration Tool

7 Contributors | 196 Issues | 3k Stars | 1k Forks