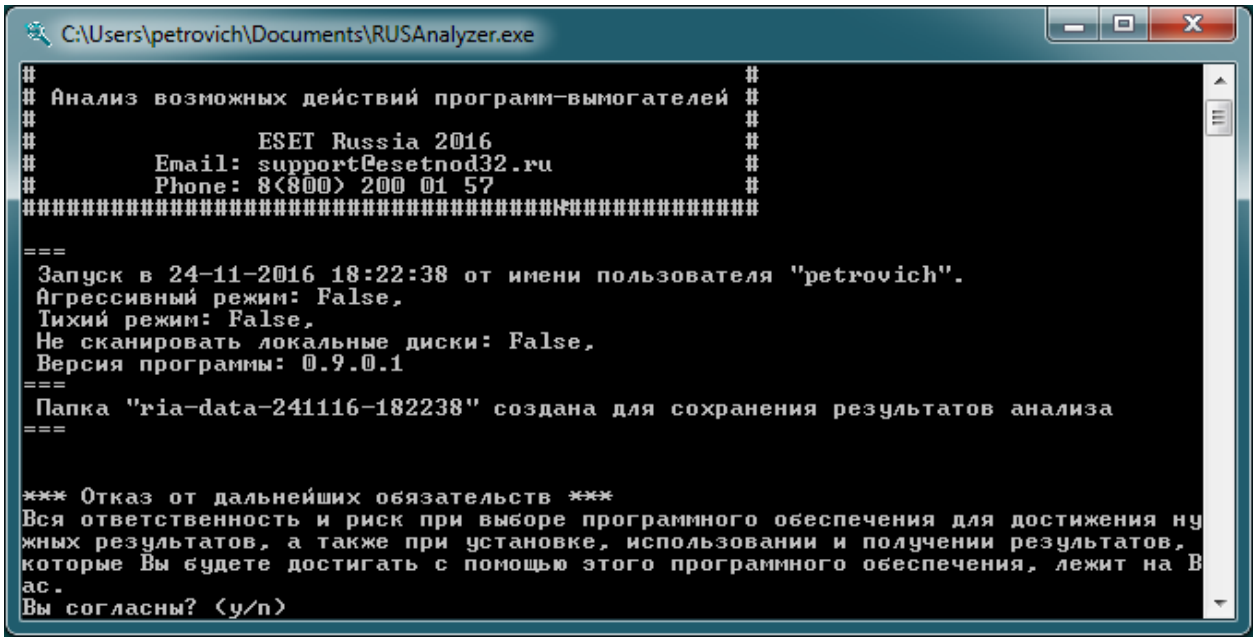
Утилита для анализа возможных действий программ-вымогателей (Ransomware Impact Analyzer)

Данное ПО помогает увидеть, какие файлы и папки могут быть зашифрованы, если на ПК запустить программу-вымогатель.

Программа **Ransomware Impact Analyzer**, по умолчанию, проверяет только локальные диски. Если есть необходимость проверить сетевые ресурсы (сетевые диски / общие расшаренные папки), необходимо запустить утилиту в агрессивном режиме.



Варианты запуска утилиты:

-h --help	Вывести справку и выйти
-a	Агрессивный режим (может занять много времени)
-s	Только запись в журнал без вывода на экран <Тихий режим>
-o < имя файла >	Файл журнала
-d < имя папки >	Папка сохранения результатов анализа
-y	Принять условия (пакетный режим)
-l	Не сканировать локальные диски

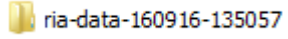
Агрессивный режим:

Утилита проверяет не только локальные файлы и папки, но и проверяет сеть на наличие общих сетевых ресурсов. Если таковые обнаружатся, Ransomware Impact Analyzer проверяет, есть ли опасность шифрования данных на этих ресурсах.

Тихий режим:

Утилита не выводит информацию о работе на экран.

Сохранение отчета:

По умолчанию, утилита ведет лог в той же папке, откуда была запущена. При этом создается папка вида 

, где цифрами обозначены день, месяц, год – текущее время

Если есть необходимость, то Вы можете указать желаемое имя файла журнала и/или папку, в которую будет записан файл журнала

Например, так:

```
E:\ESET_RIA>RUSAnalyzer.exe -o "eset_ria_01" -d "E:\ESET_RIA\logs"
```

Пакетный режим:

По умолчанию, Ransomware Impact Analyzer требует от пользователя принять условия использования ПО. Если Вы запускаете утилиту пакетно, есть возможность автоматически принять эти условия, введя параметр **–y**

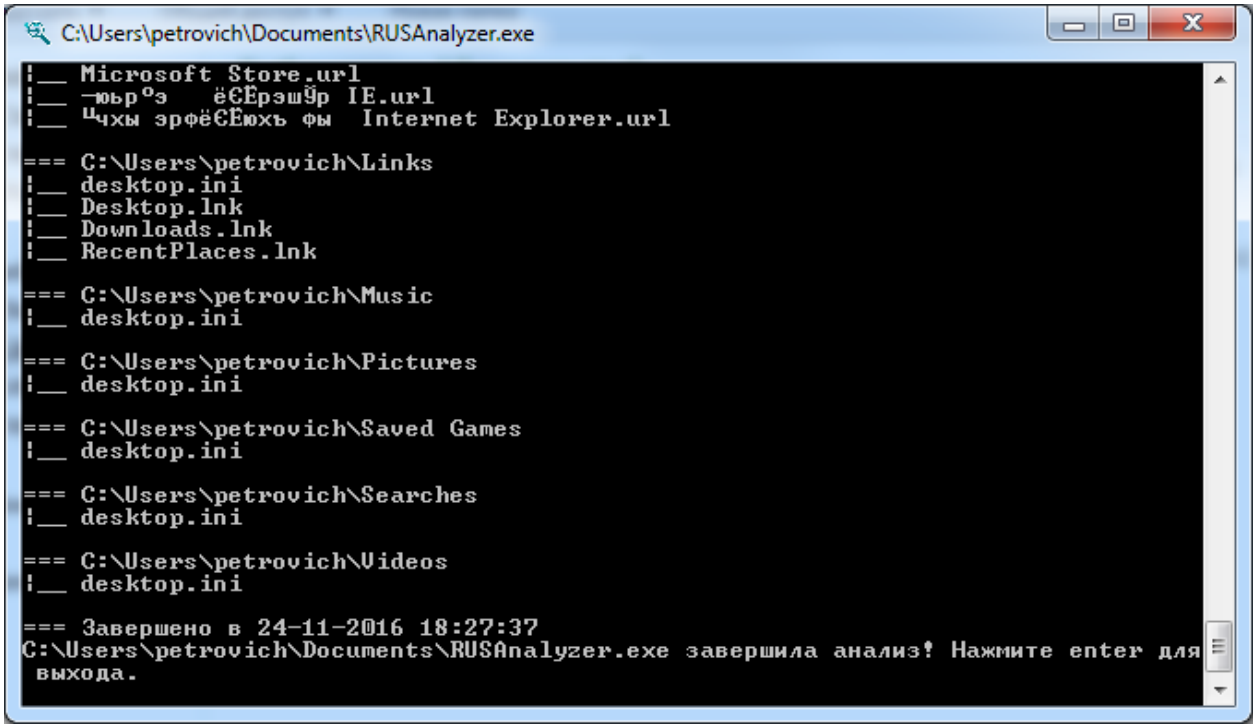
Не проверять локальные диски:

При необходимости, можно игнорировать проверку локальных дисков и сразу перейти к проверки общих сетевых ресурсов.

Для этого необходимо запустить Ransomware Impact Analyzer с параметром **–l**

Журнал работы:

По окончании работы анализатора, будет выведено сообщение, что анализ завершен:



Вы можете просмотреть подробный отчет обо всех файлах, которые могут быть подвержены несанкционированному шифрованию: