



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.

```
C:\Users\petrovich\Documents\RUSAnalyzer.exe
##
## Анализ возможных действий программ-вымогателей ##
##
##           ESET Russia 2016           ##
##      Email: support@esetnod32.ru      ##
##      Phone: 8(800) 200 01 57         ##
#####
===
Запуск в 24-11-2016 18:22:38 от имени пользователя "petrovich".
Агрессивный режим: False,
Тихий режим: False,
Не сканировать локальные диски: False,
Версия программы: 0.9.0.1
===
Папка "ria-data-241116-182238" создана для сохранения результатов анализа
===

*** Отказ от дальнейших обязательств ***
Вся ответственность и риск при выборе программного обеспечения для достижения нужных результатов, а также при установке, использовании и получении результатов, которые Вы будете достигать с помощью этого программного обеспечения, лежит на Вас.
Вы согласны? <у/п>
```

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  ria-data-160916-135057, 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

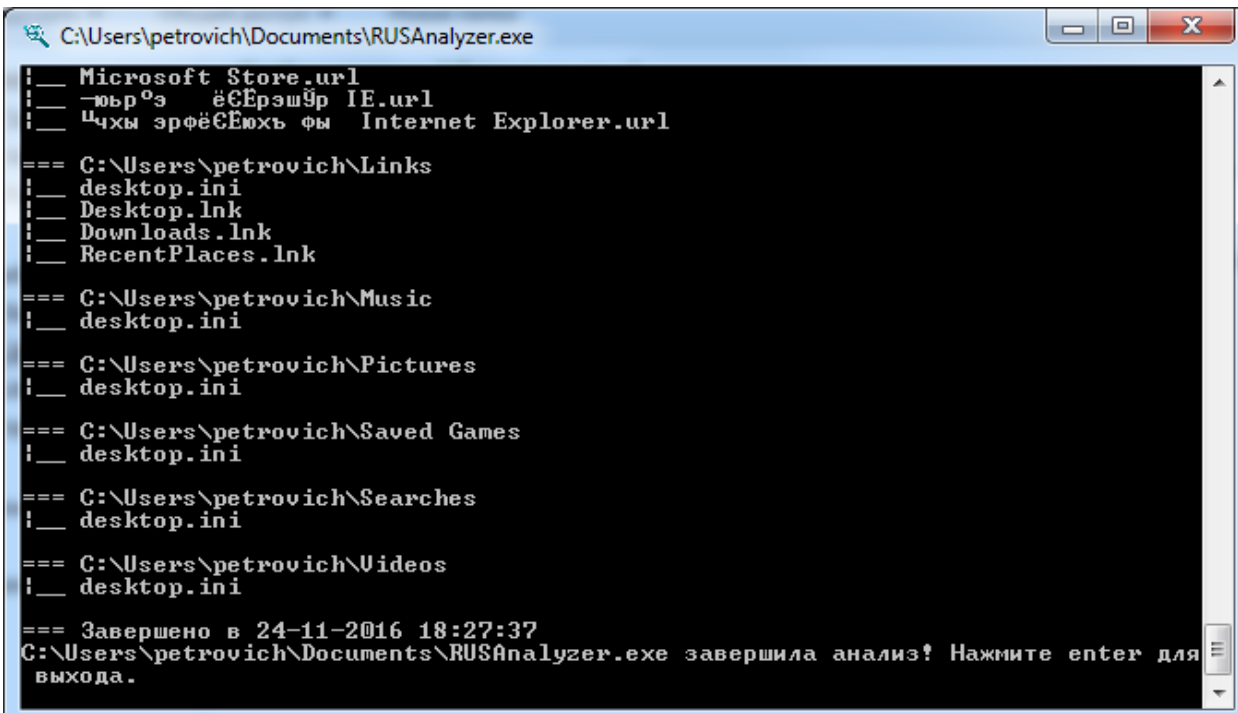
Не проверять локальные диски:

При необходимости, можно игнорировать проверку локальных дисков и сразу перейти к проверке 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:



```
C:\Users\petrovich\Documents\RUSAnalyzer.exe
|_ Microsoft Store.url
|_ -юьр 0э ёёЕрэш9р IE.url
|_ Чхы эрфёСЕюхъ фы Internet Explorer.url

=== C:\Users\petrovich\Links
|_ desktop.ini
|_ Desktop.lnk
|_ Downloads.lnk
|_ RecentPlaces.lnk

=== C:\Users\petrovich\Music
|_ desktop.ini

=== C:\Users\petrovich\Pictures
|_ desktop.ini

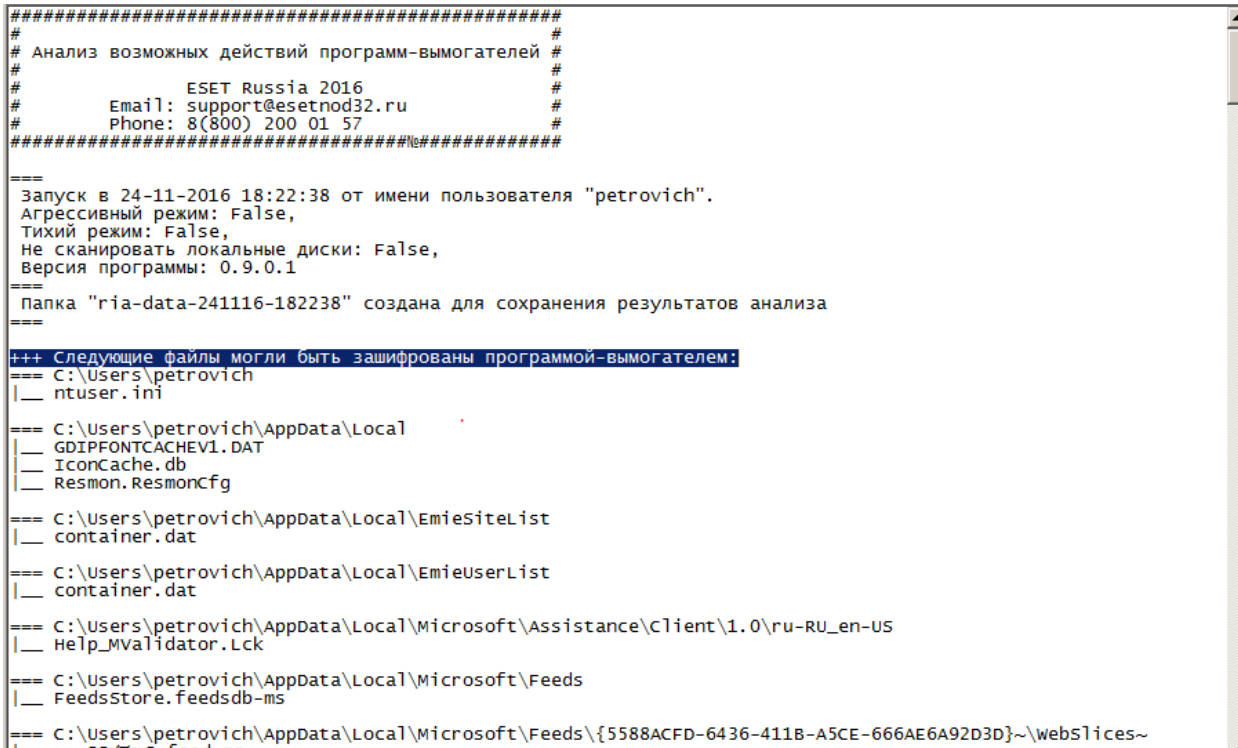
=== C:\Users\petrovich\Saved Games
|_ desktop.ini

=== C:\Users\petrovich\Searches
|_ desktop.ini

=== C:\Users\petrovich\Videos
|_ desktop.ini

=== Завершено в 24-11-2016 18:27:37
C:\Users\petrovich\Documents\RUSAnalyzer.exe завершила анализ! Нажмите enter для
выхода.
```

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



```
#####
#
# Анализ возможных действий программ-вымогателей #
#
# ESET Russia 2016 #
# Email: support@esetnod32.ru #
# Phone: 8(800) 200 01 57 #
#####

===
Запуск в 24-11-2016 18:22:38 от имени пользователя "petrovich".
Агрессивный режим: False,
Тихий режим: False,
Не сканировать локальные диски: False,
Версия программы: 0.9.0.1

===
Папка "ria-data-241116-182238" создана для сохранения результатов анализа
===

+++ Следующие файлы могли быть зашифрованы программой-вымогателем:
=== C:\Users\petrovich
|_ ntuser.ini

=== C:\Users\petrovich\AppData\Local
|_ GDIPFONTCACHEV1.DAT
|_ IconCache.db
|_ Resmon.ResmonCfg

=== C:\Users\petrovich\AppData\Local\EmieSiteList
|_ container.dat

=== C:\Users\petrovich\AppData\Local\EmieUserList
|_ container.dat

=== C:\Users\petrovich\AppData\Local\Microsoft\Assistance\Client\1.0\ru-RU_en-US
|_ Help_MValidator.Lck

=== C:\Users\petrovich\AppData\Local\Microsoft\Feeds
|_ FeedsStore.feedsdb-ms

=== C:\Users\petrovich\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\webSlices~
|_ feed-ms
```