

Cath3d Malwar3 . Задача на форензику.

Официальное прохождение от автора задачи (И. А. Герасимов - laf3r.github.io).

Описание

Привет, White-Hat. Мне нужна твоя помощь, я проверял свою почту и подцепил какой-то вирус. Все мои документы зашифрованы. Я остановил вирус через диспетчер задач и сделал снимок ROM моего рабочего стола. Помоги мне расшифровать мои документы.

На вход у нас подаётся файл Desktop.iso. Это снимок памяти жёсткого диска, а именно директории Desktop.



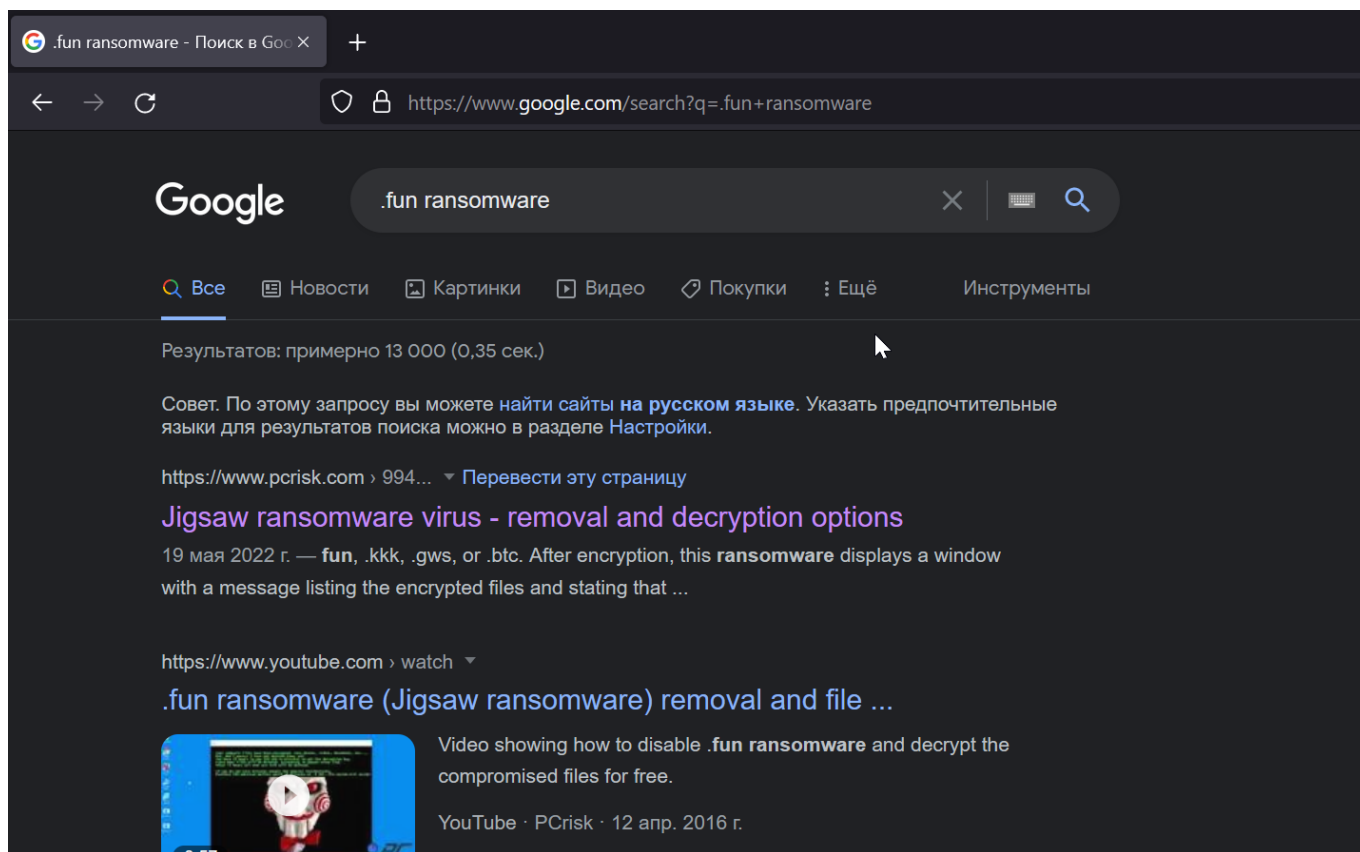
Desktop.iso

09.08.2022 21:08

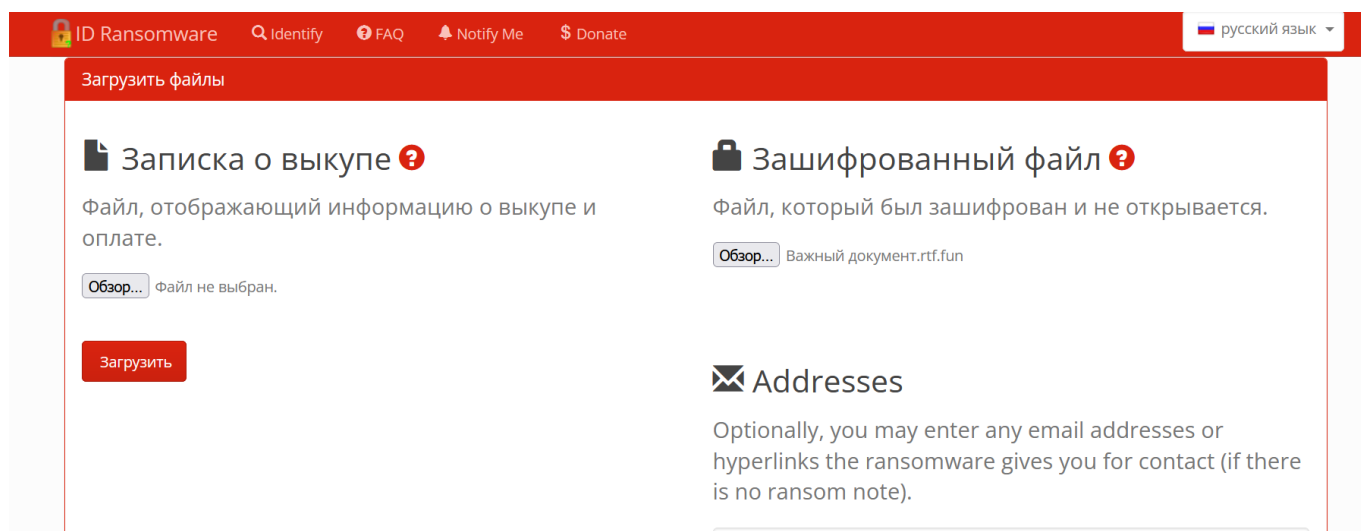
Его можно открыть через WinRar. В архиве я обнаруживаю 3 файла:

Папка с файлами			
Важный документ.rtf.fun	240	240	Файл "FUN"
заметки.txt.fun	80	80	Файл "FUN"
схема.bmp.fun	1 893 952	1 893 952	Файл "FUN"

Все они зашифрованы вирусом шифровальщиком. По расширению .fun я узнаю, что это Jigsaw Ransomware.



Теперь я иду на сайт id-ransomware.malwarehunterteam.com и загружаю туда свой зашифрованный файл. Это очень хороший ресурс. На нём можно посмотреть, известен ли шифровальщик, который зашифровал ваши данные, и доступны ли его ключи.



Я не ошибся, это действительно шифровальщик Jigsaw

1 Result

Jigsaw

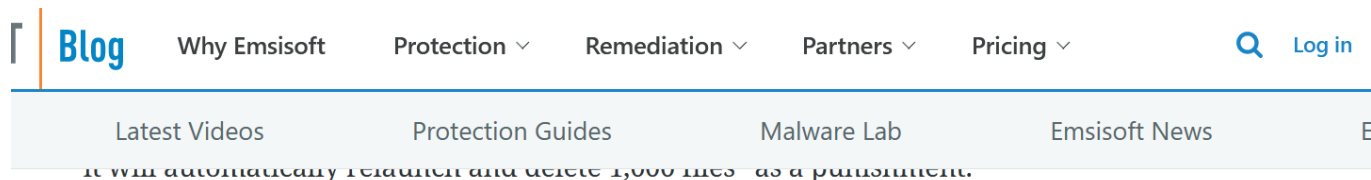
✓ Этот вымогатель дешифруем!

Опознан как

- sample_extension: .fun

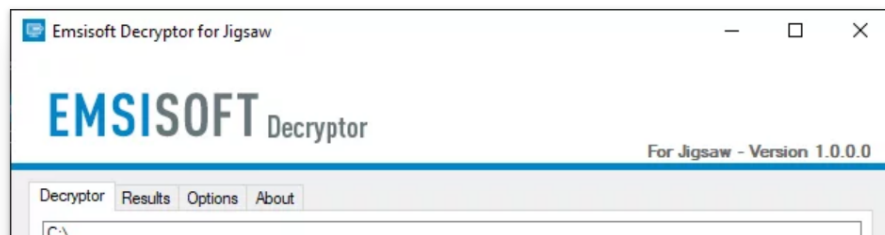
Кликните тут для подробностей о Jigsaw

Перейдя по ссылке <https://blog.emsisoft.com/en/34636/emsisoft-releases-new-decryptor-for-jigsaw-ransomware/>, я скачиваю программу, которая сможет расшифровать зашифрованные данные.




A decryptor for Jigsaw was released in 2016. Initially, the ransomware was sold on a Tor marketplace, however, it has now been open-sourced which has enabled people to create multiple variants that the original tool could not decrypt. The new tool can currently unlock 85 extensions and will be updated as new variants emerge.

[Download the Jigsaw Decryptor here](#)

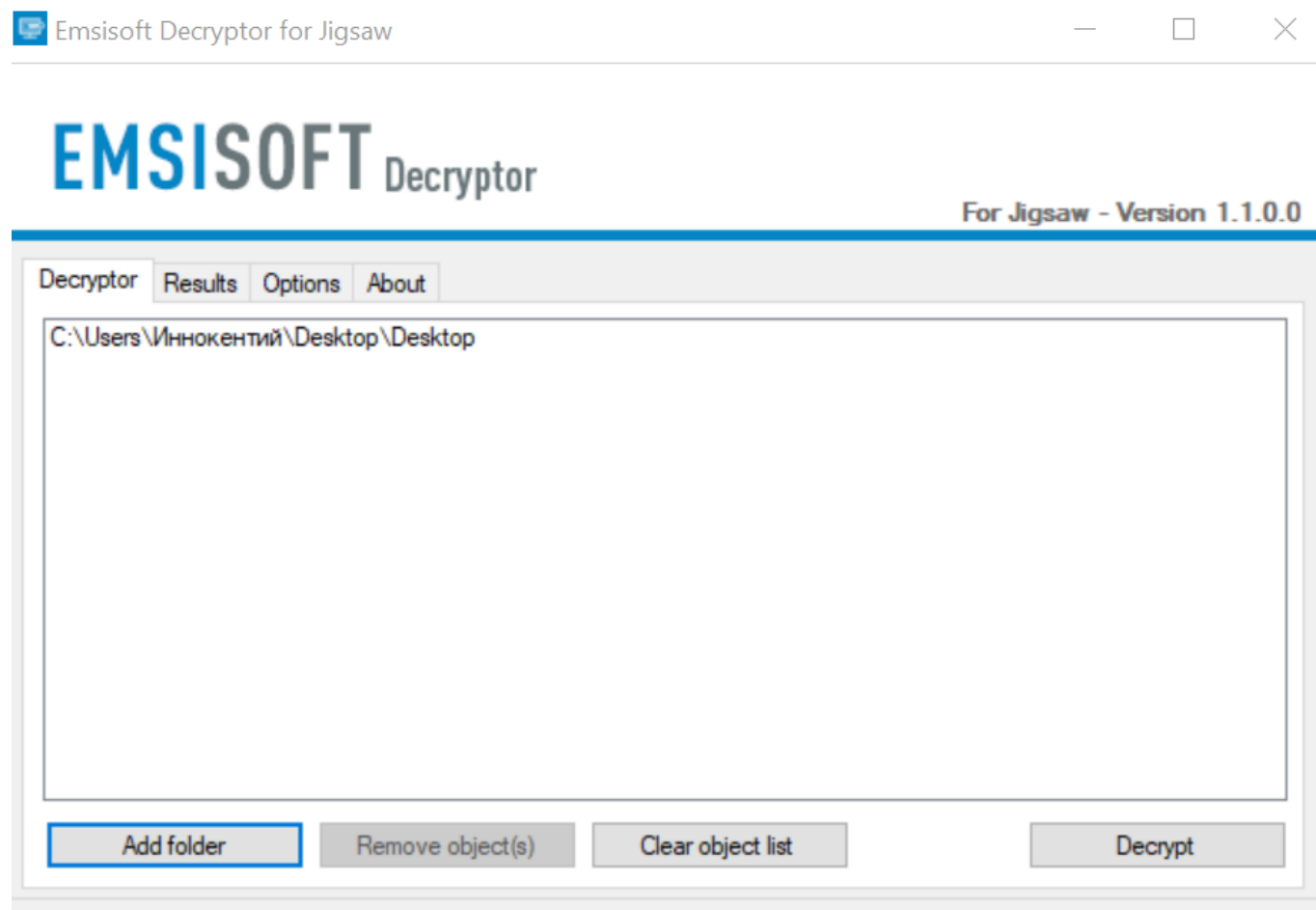


<https://www.emsisoft.com/ransomware-decryption/jigsaw/>

▼ Сегодня (5)

 decrypt_jigsaw.exe

Теперь я указываю директорию с зашифрованными данными. Ранее, я распаковывал их из iso образа, при помощи утилиты WinRAR.



Как видим, программа успешно расшифровала данные.

EMSISOFT Decryptor

For Jigsaw - Ve

Decryptor Results Options About

Starting...

File: C:\Users\Иннокентий\Desktop\Desktop\Важный документ.rtf.fun
Decrypted: C:\Users\Иннокентий\Desktop\Desktop\Важный документ.rtf

File: C:\Users\Иннокентий\Desktop\Desktop\заметки.txt.fun
Decrypted: C:\Users\Иннокентий\Desktop\Desktop\заметки.txt

File: C:\Users\Иннокентий\Desktop\Desktop\схема.bmp.fun
Decrypted: C:\Users\Иннокентий\Desktop\Desktop\схема.bmp

Finished!

Открываем "Важный документ" и видим флаг.

Имя

Дата изменения



Важный документ.rtf

09.08.2022 21:21



Важный документ.rtf.fun

Тип: Формат RTF



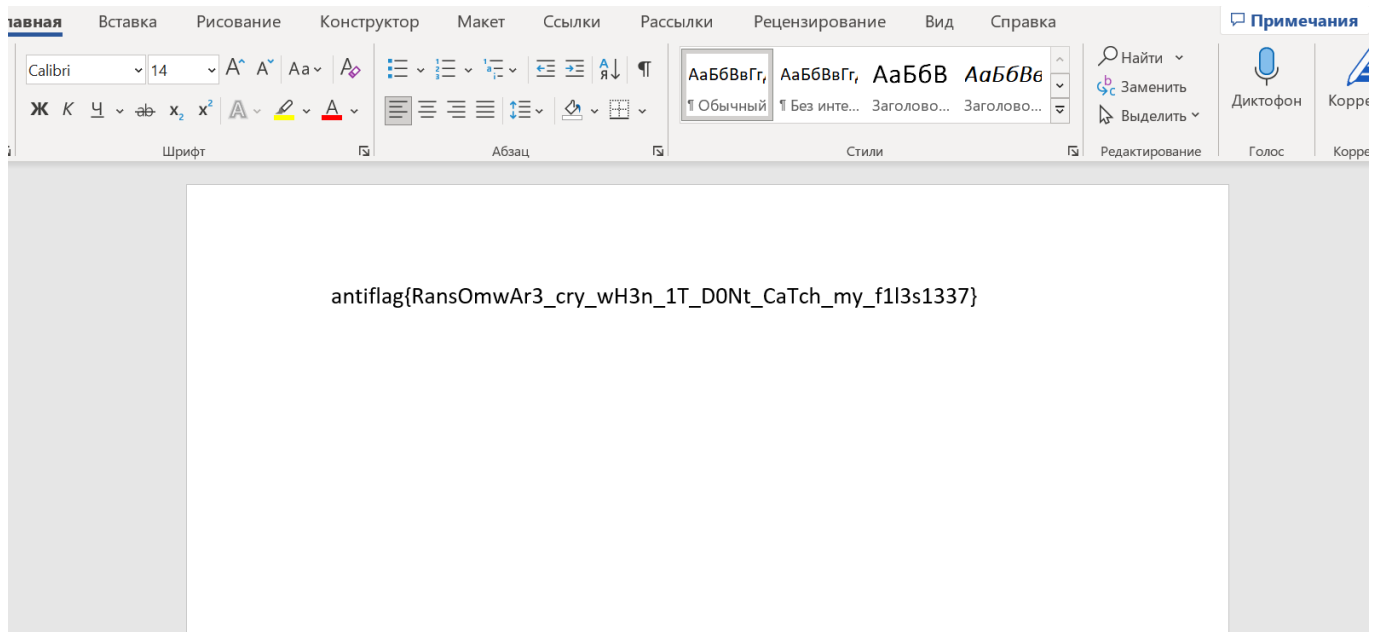
заметки.txt

Размер: 232 байт



заметки.txt.fun

Дата изменения: 09.08.2022 21



antiflag{RansOmwaR3_cry_wH3n_1T_D0Nt_CaTch_my_f1l3s1337}