

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.

![[Pasted image 20220809211253.png]]

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

![[Pasted image 20220809211346.png]]

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

![[Pasted image 20220809211445.png]]

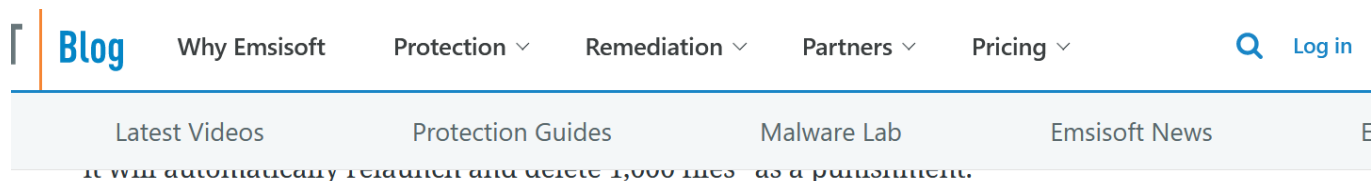
Теперь я иду на сайт id-ransomware.malwarehunterteam.com и загружаю туда свой зашифрованный файл. Это очень хороший ресурс. На нём можно посмотреть, известен ли шифровальщик, который зашифровал ваши данные, и доступны ли его ключи.

![[Pasted image 20220809211718.png]]

Я не ошибся, это действительно шифровальщик Jigsaw

![[Pasted image 20220809211755.png]]

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](#)



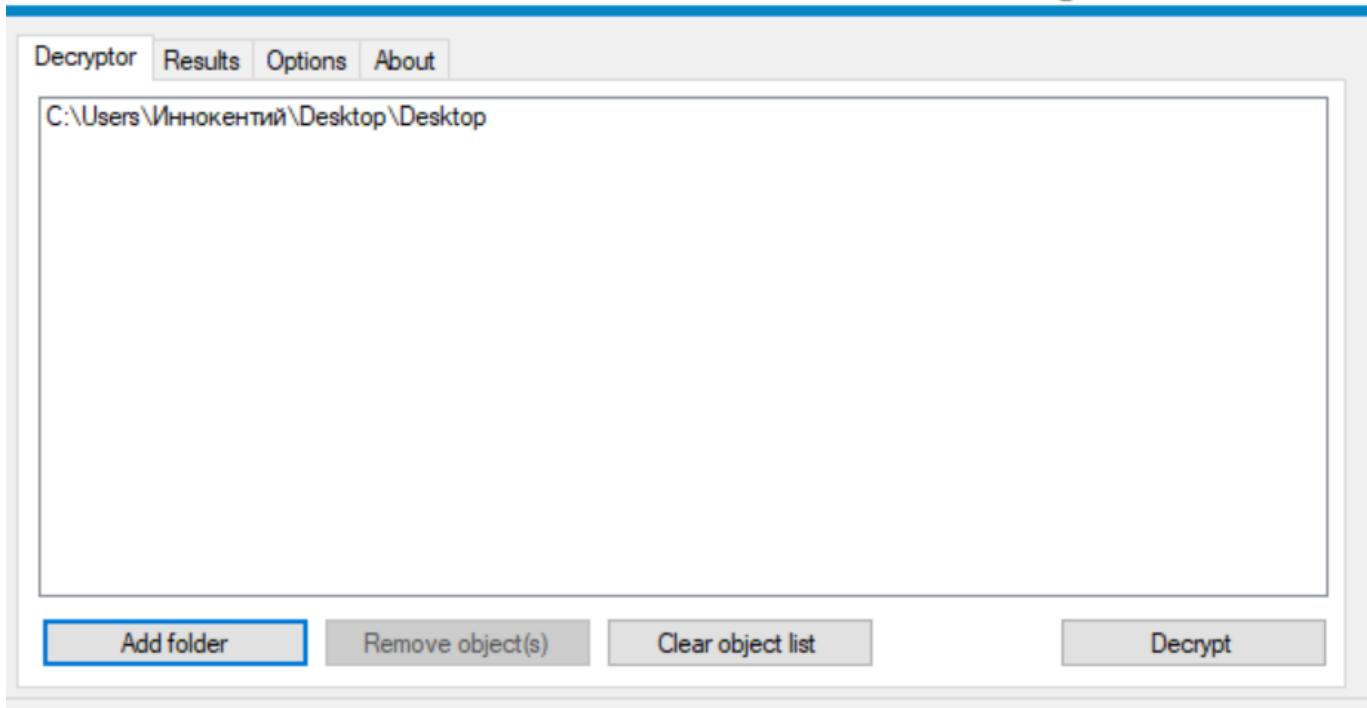
<https://www.emsisoft.com/ransomware-decryption/jigsaw/>



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

EMSIOSFT Decryptor

For Jigsaw - Version 1.1.0.0



Как видим, программа успешно расшифровала данные.

![[Pasted image 20220809212233.png]]

Открываем "Важный документ" и видим флаг.

![[Pasted image 20220809212311.png]] ![[Pasted image 20220809212329.png]]

antiflag{Rans0mwAr3_cry_wH3n_1T_D0Nt_CaTch_my_f1l3s1337}