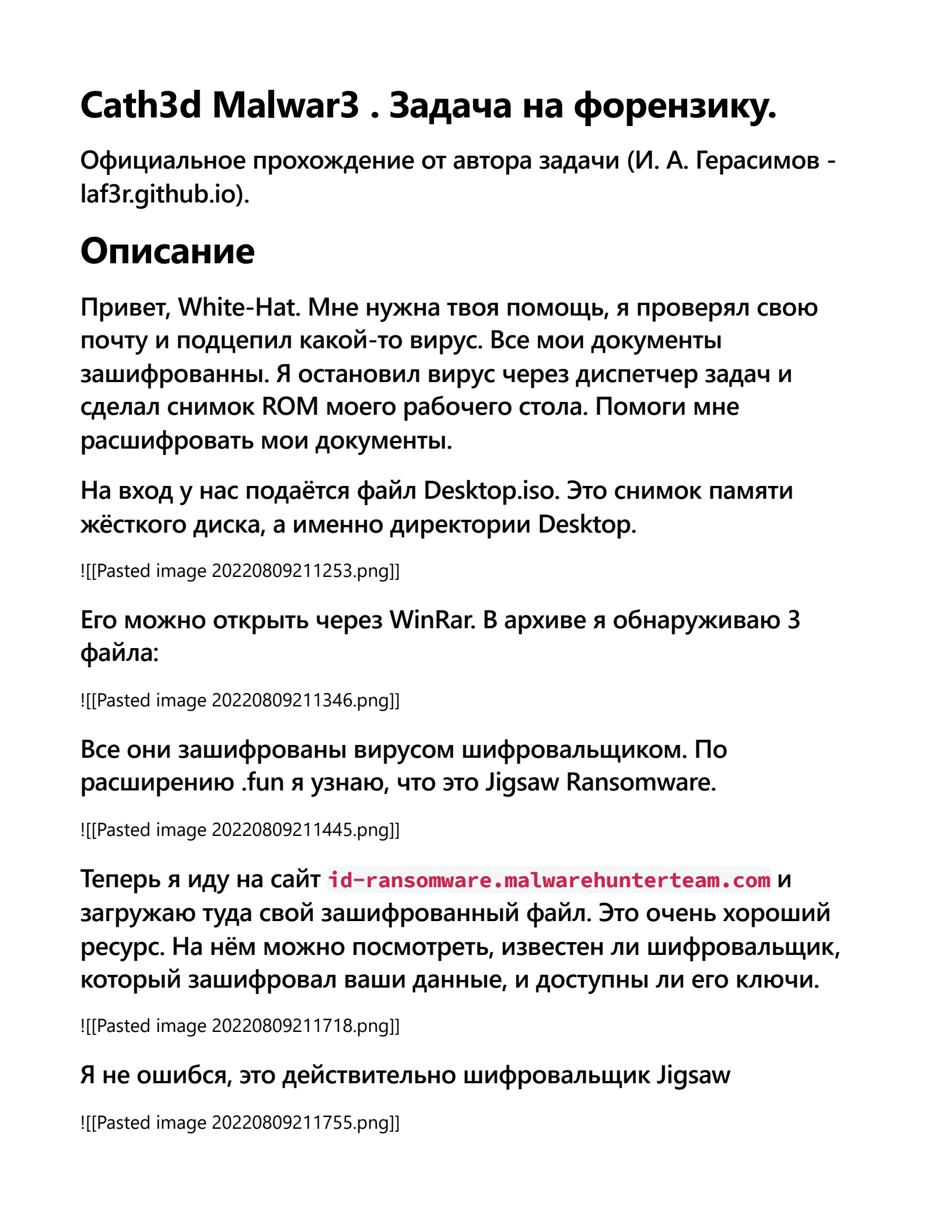
Cath3d Malwar3 . Задача на форензику.

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 зашифрованны. 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.



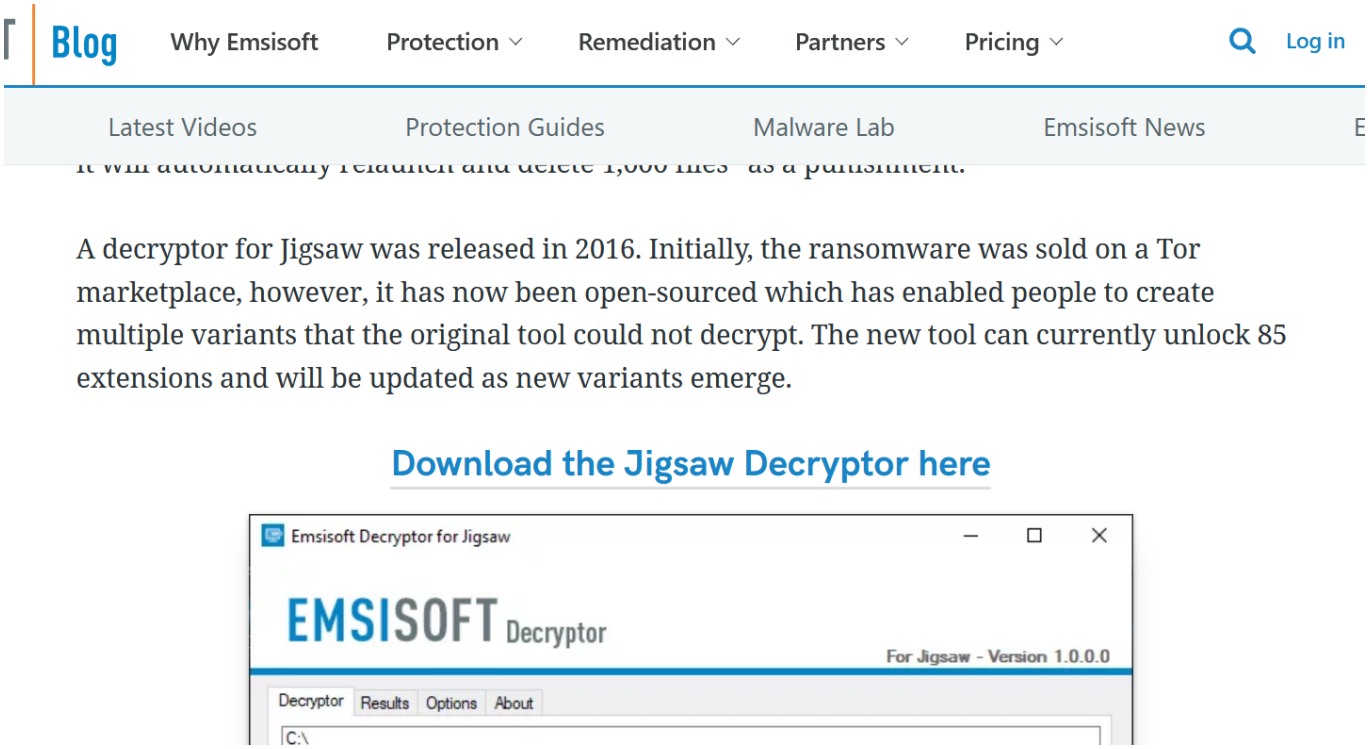
Его можно открыть через WinRar. В архиве я обнаруживаю 3 файла:

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.

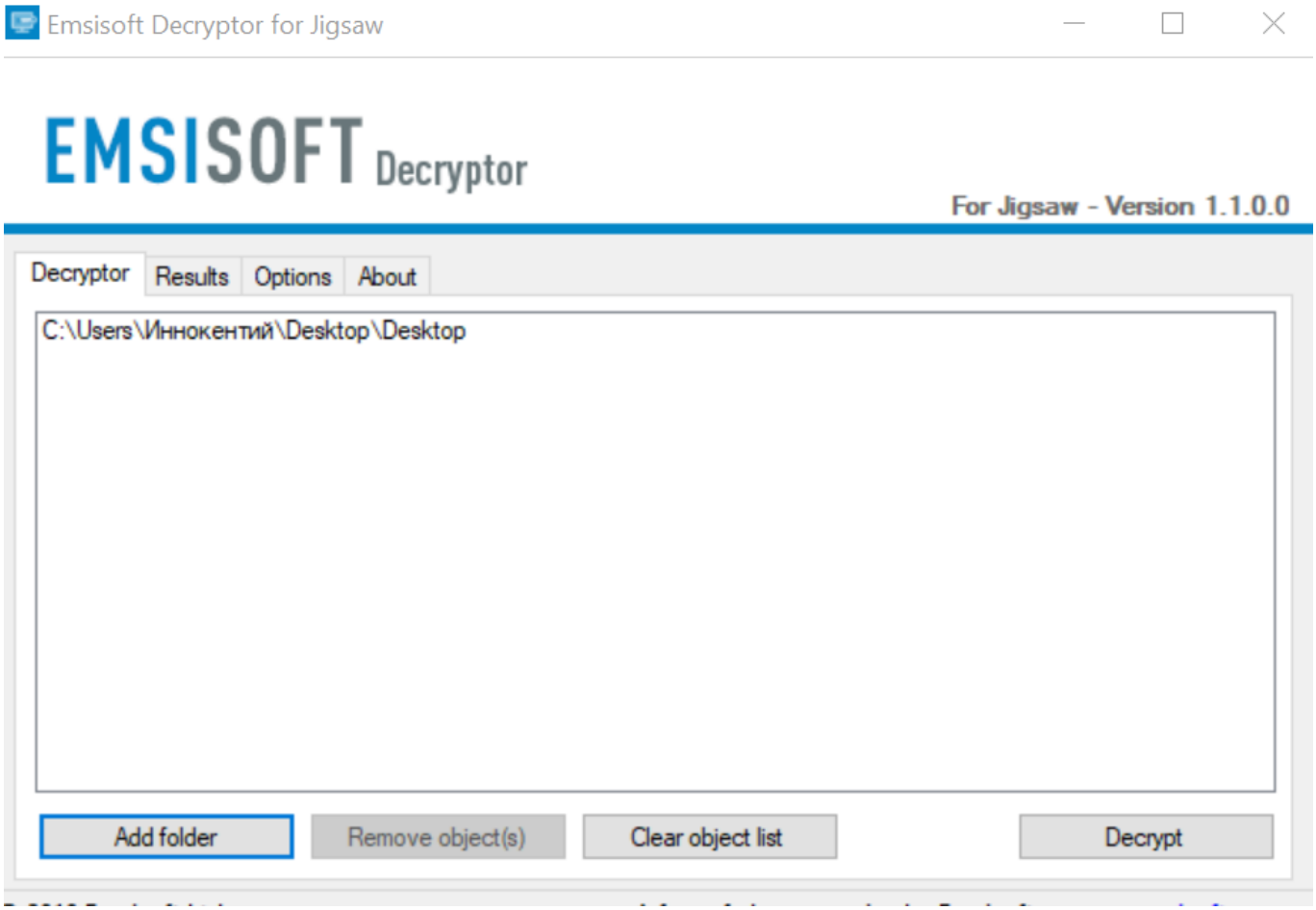
Я не ошибся, это действительно шифровальщик Jigsaw

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



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.



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{RansOmwAr3_cry_wH3n_1T_D0Nt_CaTch_my_f1l3s1337}`