# FuxSocy Encryptor

id-ransomware.blogspot.com/2019/10/fuxsocy-encryptor-ransomware.html


## FuxSocy Ransomware

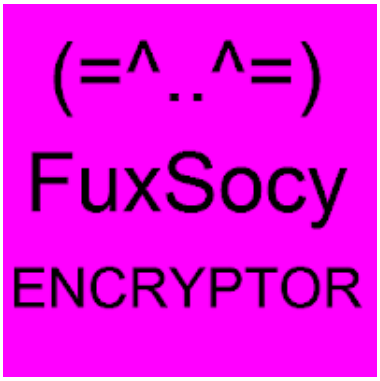
## FuxSocy Encryptor Ransomware

### (шифровальщик-вымогатель) (первоисточник)
### Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: FuxSocy ENCRYPTOR. На файле написано: нет данных.

**Обнаружения:**
**DrWeb** -> Trojan.Encoder.29846
**BitDefender** -> Generic.Ransom.Magniber.8486CAD0
**Symantec** -> ML.Attribute.HighConfidence
**TrendMicro** -> Ransom_Encoder.R002C0WJJ19
**Kaspersky** -> Trojan-Ransom.Win32.Encoder.fsc
**ESET-NOD32** -> A Variant Of Win32/Filecoder.NYE

**© Генеалогия: выясняется, явное родство с кем-то не доказано.**




Изображение — логотип статьи

Зашифрованные файлы не получают какое-то определенное расширение, но целиком переименовываются в стиле Cerber Ransomware:
**XXXXXXXXXX.XXXX**

Т.е. %10 случайных знаков%.%4 случайных знака%.

Например: KCuJB7qPLZ.9DC1 или 74rOiDMZwM.9DC1

Последние 4 знака, видимо, общие для всех файлов на одном ПК.

**Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

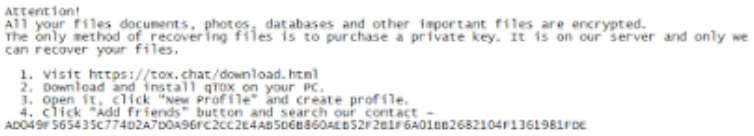
Активность этого крипто-вымогателя пришлась на начало октября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется по шаблону, который можно записать так:
**{RAND}_R_E_A_D___T_H_I_S_{RAND}.txt**
XXXXX_R_E_A_D___T_H_I_S_XXXXX.txt

Это значит, в начале названия записки стоят несколько (например, 4-8) случайных заглавных символов, потом, в конце названия после _R_E_A_D___ T_H_I_S_ снова стоят те же случайные заглавные символы.

Кроме того каждая такая txt-записка имеет разные случайные символы.

Например: **D02DGB0U_R_E_A_D___T_H_I_S_D02DGB0U.txt**


Attention!
All your files documents, photos, databases and other important files are encrypted.
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.

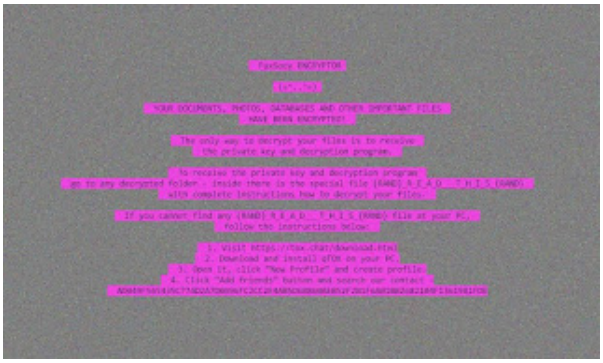
1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.
3. Open it, click "New Profile" and create profile.
4. Click "Add friends" button and search our contact -
AD049F5654B5C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

**Содержание записки о выкупе:**
Attention!
All your files documents, photos, databases and other important files are encrypted.
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.
1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.
3. Open it, click "New Profile" and create profile.
4. Click "Add friends" button and search our contact -
AD049F5654B5C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

**Перевод записки на русский язык:**
Внимание!
Все ваши файлы документов, фотографии, базы данных и другие важные файлы зашифрованы.

Единственный способ восстановления файлов - это покупка приватного ключа. Он на нашем сервере и только мы можем восстановить ваши файлы.
1. Посетите https://tox.chat/download.html
2. Загрузите и установите qTOX на свой ПК.
3. Откройте его, нажмите "Новый профиль" и создайте профиль.
4. Нажмите кнопку "Добавить друзей" и найдите наш контакт - AD049F5654B5C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

Другим информатором жертвы выступает изображение, заменяющее обои Рабочего стола. Название у этого изображения также включает в себя случайные знаки, сгенерированные также, как у текстовой записки.
Например: **RZROZP_R_E_A_D___T_H_I_S_RZROZP.jpg**



**Содержание текста:**
FuxSocy ENCRYPTOR
(=^..^=)
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder - inside there is the special file {RAND}_R_E_A_D___T_H_I_S_{RAND} with complete instructions how to decrypt your files.
If you cannot find any {RAND}_R_E_A_D___T_H_I_S_{RAND} file at your PC, follow the instructions below:
1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.
3. Open it, click "New Profile" and create profile.
4. Click "Add friends" button and search our contact AD049F5654B5C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

**Перевод текста на русский язык:**
FuxSocy ENCRYPTOR
(=^..^=)
ВАШИ ДОКУМЕНТЫ, ФОТОГРАФИИ, БАЗЫ ДАННЫХ И ДРУГИЕ ВАЖНЫЕ ФАЙЛЫ ЗАШИФРОВАНЫ!
Единственный способ расшифровать ваши файлы - это получить закрытый ключ и программу расшифровки.

Чтобы получить закрытый ключ и программу расшифровки, перейдите в любую расшифрованную папку - внутри есть специальный файл {RAND}_R_E_A_D___T_H_I_S_{RAND} с подробными инструкциями, как расшифровать ваши файлы.
Если вы не можете найти какой-либо файл {RAND}_R_E_A_D___T_H_I_S_{RAND} на своем ПК, следуйте приведенным ниже инструкциям:
1. Посетите https://tox.chat/download.html
2. Загрузите и установите qTOX на свой компьютер.
3. Откройте его, нажмите "Новый профиль" и создайте профиль.
4. Нажмите кнопку "Добавить друзей" и найдите наш контакт AD049F5654B5C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

**Технические детали**

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Используют защиту Anti-VM, чтобы затруднить запуск и исследование на виртуальных машинах.**Список файловых расширений, подвергающихся шифрованию:**
Многие популярные форматы.
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

**Файлы, связанные с этим Ransomware:**
D02DGB0U_R_E_A_D___T_H_I_S_D02DGB0U.txt - или другой в том же стиле
RZROZP_R_E_A_D___T_H_I_S_RZROZP.jpg - или другой в том же стиле
<random>.exe - случайное название вредоносного файла

**Расположения:**
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
%TEMP%\36d1130a\44f7.tmp
%TEMP%\36d1130a\ac2e.tmp

**Записи реестра, связанные с этим Ransomware:**
См. ниже результаты анализов.

**Сетевые подключения и связи:**
Email:
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

**Результаты анализов:**
Ⓗ Hybrid analysis >>
**Σ VirusTotal analysis >>**
🐞 **Intezer analysis >>**
**⋟ ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

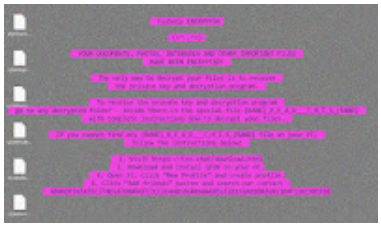
---

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

---

**=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===**

**Обновление от 22 декабря 2019:**
Пост в Твиттере >>
Расширение: **.b58d**
Пример зашифрованного файла: z5wuF6xD84.b58d
Записка: KG4YGH_R_E_A_D___T_H_I_S_KG4YGH.txt
Результаты анализов: **VT** + **AR** + **IA**

➤ Содержание txt-записки:
Attention!
All your files documents, photos, databases and other important files are encrypted.
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.

1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.
3. Open it, click “New Profile” and create profile.

4. Click “Add friends” button and search our contact – AD049F565435C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

---

**=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===**


**Thanks:**

```
Michael Gillespie, MalwareHunterTeam, Vitali Kremez
Andrew Ivanov (author)
CyberSecurity GrujaRS
to the victims who sent the samples
```