

FCT

Archived: 2026-04-05 16:39:46 UTC

FCT

FCT 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 проекта: FCT.pdb. На исполняемом файле написано: FCT.exe. Использует библиотеку Crypto++.

Обнаружения:

DrWeb -> Trojan.Encoder.30905

BitDefender -> Gen:Variant.Johnnie.213073

ESET-NOD32 -> A Variant Of Win32/Filecoder.FCT.A

Kaspersky -> Trojan.Win32.Zudochka.dvw

Microsoft -> Trojan:Win32/Wacatac.C!ml

Tencent -> Win32.Trojan.Filecoder.Hqv

Symantec -> [ML.Attribute.HighConfidence](#), [Trojan.Gen.MBT](#)

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!

AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

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



Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.adv**



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 конец января 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: ***

Содержание записки о выкупе:

Перевод записки на русский язык:

Технические детали

Распространяется как активатор для Office ([файл Activator Office.exe](#)) или один из компонентов KMSAuto.

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, 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 сделайте резервное копирование важных файлов по [методу 3-2-1](#).

Список файловых расширений, подвергающихся шифрованию:

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:

FCT.pdb - оригинальное название проекта
FCT.exe - оригинальный исполняемый файл
<ransom_note>.txt - название текстового файла
<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\cdalv\source\repos\FCT\Release\FCT.pdb

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 ===

Ещё не было обновлений этого варианта.



Read to links:

[Tweet on Twitter](#) + Tweet + myTweet

ID Ransomware (ID as FCT)

Write-up, Topic of Support

*



Thanks:

Jirehlov, Michael Gillespie

Andrew Ivanov (author)

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).

Source: <https://id-ransomware.blogspot.com/2020/02/fct-ransomware.html>