

TheCursedMurderer

Archived: 2026-04-05 22:41:24 UTC

TheCursedMurderer 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: The_Cursed_Murderer. На файле написано: AppGive.exe. Написан на языке программирования Python.

Обнаружения:

DrWeb -> Trojan.Encoder.30950

ALYac -> Trojan.Ransom.Python

BitDefender -> Trojan.Agent.ELBN

ESET-NOD32 -> Python/Filecoder.DA

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

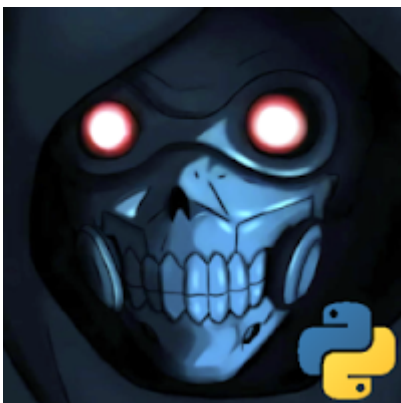
TrendMicro -> Ransom_Crypren.R002C0WB320

Symantec -> 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: **.aes**

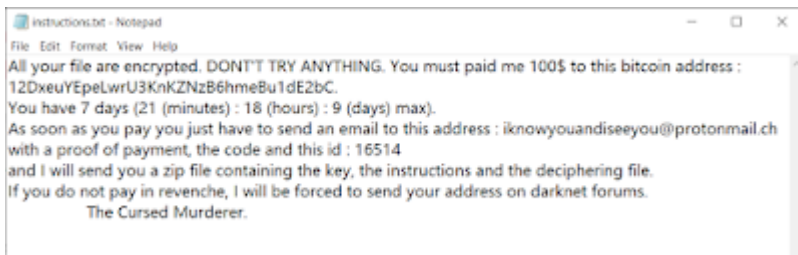


Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях.

Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на начало января 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **instructions.txt**



Содержание записки о выкупе:

All your file are encrypted. DONT'T TRY ANYTHING. You must paid me 100\$ to this bitcoin address : 12DxeuYEpeLwrU3KnKZNzB6hmeBu1dE2bC.

You have 7 days (21 (minutes): 18 (hours): 9 (days) max).

As soon as you pay you just have to send an email to this address : iknowyouandiseeyou@protonmail.ch with a proof of payment, the code and this id : 12345

and I will send you a zip file containing the key, the instructions and the deciphering file.

If you do not pay in revenche, I will be forced to send your address on darknet forums.

The Cursed Murderer.

Перевод записки на русский язык:

Все ваши файлы зашифрованы. НЕ ПЫТАЙТЕСЬ. Вы должны заплатить мне 100\$ на этот биткойн-адрес: 12DxeuYEpeLwrU3KnKZNzB6hmeBu1dE2bC.

У вас есть 7 дней (21 (минут): 18 (часов): 9 (дней) макс).

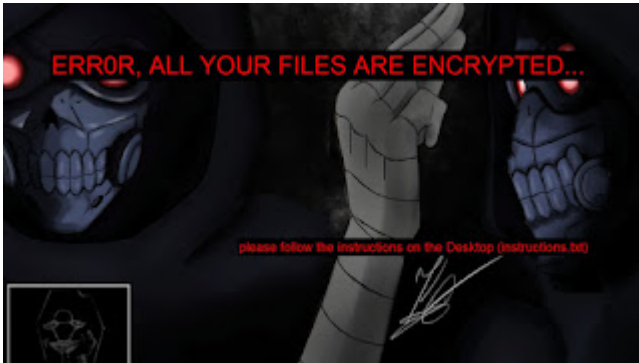
Как только заплатите, вам нужно отправить email на этот адрес: iknowyouandiseeyou@protonmail.ch с подтверждением платежа, кодом и этим id: 12345

и я вышлю вам zip-файл, содержащий ключ, инструкции и расшифрованный файл.

Если вы не заплатите, я буду вынужден выложить ваш адрес на форумах даркнета.

Проклятый убийца.

Другим информатором жертвы выступает изображение, заменяющее обои Рабочего стола.



Технические детали

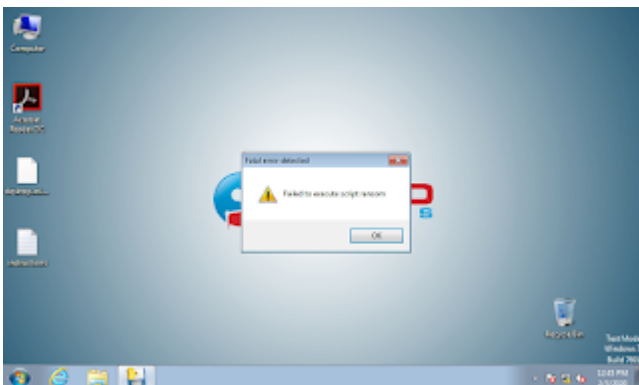
Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения 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 делайте резервное копирование важных файлов по [методу 3-2-1](#).

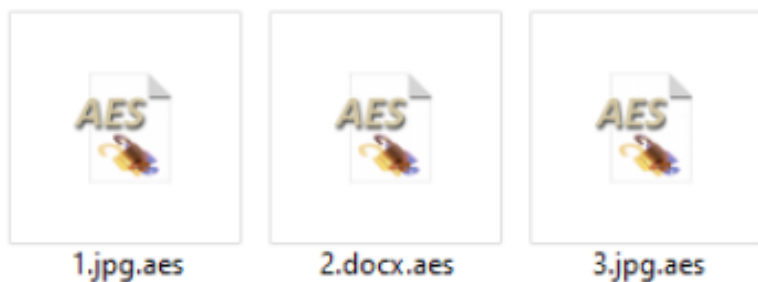
► При запуске наблюдаются ошибки.



Список файловых расширений, подвергающихся шифрованию:

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

Зашифрованные файлы получают оригинальную иконку. Такой прием мы уже видели раньше в другом Ransomware. Возможно, что TheCursedMurderer связан с предыдущим.



Файлы, связанные с этим Ransomware:

instructions.txt - название текстового файла

AppGive.exe

<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: iknowyouandiseeyou@protonmail.ch

BTC: 12DxeuYEpeLwrU3KnKZNzB6hmeBu1dE2bC

URL-сайт для загрузки изображения: xxxx://image.noelshack.com/

Изображение, использованное вымогателями не является оригинальным. Оно взято с сайта, предоставляющего обои в разном разрешении.

URL с оригинальным изображением: xxxxs://www.wallpaperflare.com/sword-art-online-sword-art-online-ii-death-gun-sword-art-online-wallpaper-zhnw



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.

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



Read to links:

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

ID Ransomware (ID as ***)

Write-up, Topic of Support

*



Thanks:

Jirehlov, GrujaRS

Andrew Ivanov (author)

to the victims who sent the samples

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

Source: <https://id-ransomware.blogspot.com/2020/01/thecursedmurderer-ransomware.html>