

Gibberish, Velar

Archived: 2026-04-05 18:49:45 UTC

Gibberish Ransomware

Variants: Anenerbex, Velar, UPPER

(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: в записке не указано. На файле написано: нет данных.

Обнаружения:

DrWeb -> Trojan.Encoder.30868, Trojan.Encoder.31489

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

ESET-NOD -> 32A Variant Of Win32/Filecoder.NSF, A Variant Of Win32/Kryptik.HCPQ

Microsoft -> Ransom:Win32/Filecoder!MSR

Qihoo-360 -> Generic/Trojan.Ransom.ec8

Rising -> Trojan.Filecoder!8.68 (CLOUD)

Tencent -> Win32.Trojan.Filecoder.Hvix

TrendMicro -> Ransom_Filecoder.R002C0DBJ20

VBA32 -> BScope.TrojanRansom.Kuntala

Symantec -> ML.Attribute.HighConfidence

© Генеалогия: ??? >> **Gibberish, Anenerbex, Velar, UPPER**



Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.uk6ge** или **.<random>**

Этимология названия:

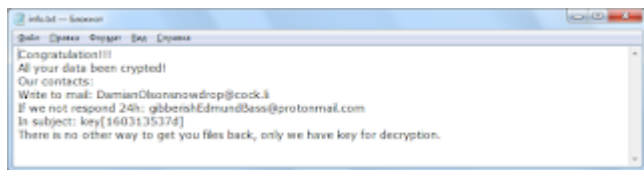
Нет никаких данных о том, как вымогатели могли назвать свое "творение". С неизвестного "взятки гладки". Но они использовали слово "gibberish" (в переводе с англ. "тарабарщина") в одном из логинов почты, как бы подчеркивая это слово. Поэтому **Gibberish** стало названием и заголовком статьи.



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

Образец этого крипто-вымогателя был обнаружен в середине февраля 2020 г. Штамп даты: 4 июля 2019 г. (Где ж его носило столько времени?) Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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



Содержание записки о выкупе:

Congratulation!!!

All your data been crypted!

Our contacts:

Write to mail: DamianOlsonsnowdrop@cock.li

If we not respond 24h: gibberishEdmundBass@protonmail.com

In subject: key[160313537d]

There is no other way to get you files back, only we have key for decryption.

Перевод записки на русский язык:

Поздравляем!!!

Все ваши данные зашифрованы!

Наши контакты:

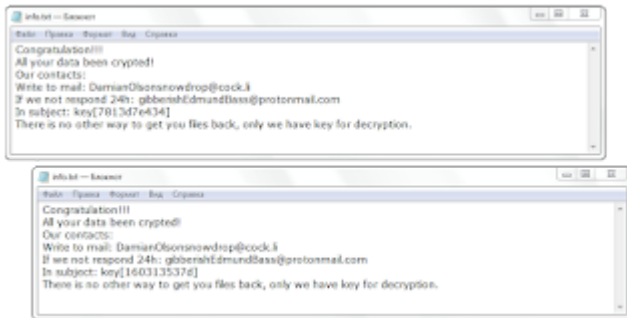
Писать на почту: DamianOlsonsnowdrop@cock.li

Если мы не ответим за 24 часа: gibberishEdmundBass@protonmail.com

В теме: key[160313537d]

Иного пути вернуть файлы нет, только у нас есть ключ для расшифровки.

Я сравнил несколько вариантов записок и обнаружил, что каждый раз генерируется новый ключ.



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](#).

► Удаляет теньные копии файлов с помощью команды:

```
vssadmin delete shadows /all /quiet
```

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:

info.txt - текстовый файл записки о выкупе

A1.exe

A2.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-1: DamianOlsonsnowdrop@cock.li

Email-2: gibberishEdmundBass@protonmail.com

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 >>](#) [AR>](#)

⌘ VMRay analysis >>

Ⓜ VirusBay samples >>

⌘ MalShare samples >>

👁 AlienVault analysis >>

🔄 CAPE Sandbox analysis >>

🕒 JOE Sandbox analysis >>

Степень распространённости: **средняя**.

Подробные сведения собираются регулярно. Присылайте образцы.

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

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

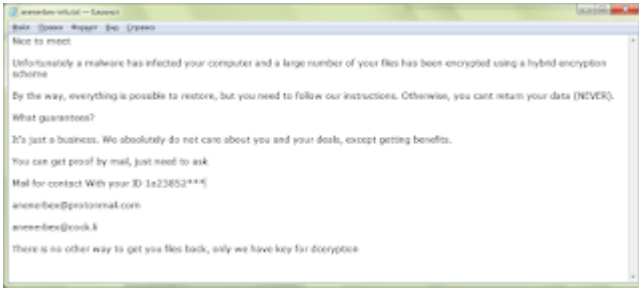
Обновление от 10 марта 2020:

[Топик на форуме >>](#)

Расширение: **.anenerbex**

Записка: anenerbex-info.txt

Email: anenerbex@protonmail.com, anenerbex@cock.li



► Содержание записки:

Nice to meet

Unfortunately a malware has infected your computer and a large number of your files has been encrypted using a hybrid encryption scheme

By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

What guarantees?

It's just a business. We absolutely do not care about you and your deals, except getting benefits.

You can get proof by mail, just need to ask

Mail for contact With your ID 1a2b3c5***

anenerbex@protonmail.com

anenerbex@cock.li

There is no other way to get you files back, only we have key for dcrption

Обновление от 18-19 марта 2020:

[Пост в Твиттере >>](#)

Расширение: **.Velar**

Записка: readme.txt

Email-1: lanthanumRosaKiddgentile@cock.li

Email-2: affrontUmerSummers@tutanota.com

Файл: 1,2.exe

Результаты анализов: **VT** + **HA** + **IA** + **AR**

Обнаружения:

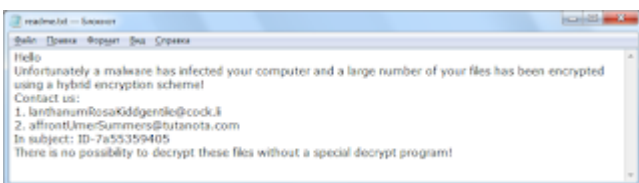
DrWeb -> Trojan.Encoder.30868

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1

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

Symantec -> ML.Attribute.HighConfidence

TrendMicro -> TROJ_FRS.0NA103CI20



► Содержание записки:

Hello

Unfortunately a malware has infected your computer and a large number of your files has been encrypted using a hybrid encryption scheme!

Contact us:

1. lanthanumRosaKiddgentile@cock.li
2. affrontUmerSummers@tutanota.com

In subject: ID-7a55359***

There is no possibility to decrypt these files without a special decrypt program!

Обновление от 22 марта 2020:

[Пост в Твиттере >>](#)

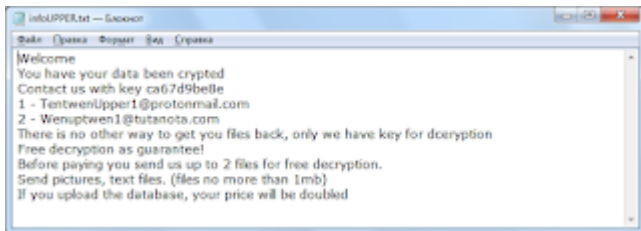
Расширение: **.UPPER**

Записка: infoUPPER.txt

Email-1: TentwenUpper1@protonmail.com

Email-2: Wenuptwen1@tutanota.com

Результаты анализов: [VT](#) + [HA](#) + [IA](#) + [AR](#)



► Содержание записки:

Welcome

You have your data been crypted

Contact us with key ca67d9b***

1 - TentwenUpper1@protonmail.com

2 - Wenuptwen1@tutanota.com

There is no other way to get you files back, only we have key for dcrption

Free decryption as guarantee!

Before paying you send us up to 2 files for free decryption.

Send pictures, text files. (files no more than 1mb)

If you upload the database, your price will be doubled

Обновление от 9 апреля 2020:

[Пост в Твиттере >>](#)

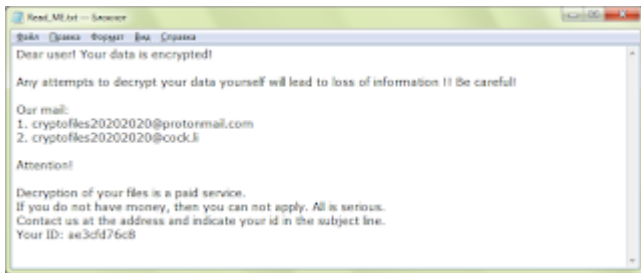
[Топик на форуме >>](#)

Расширение: **.~~~~**

Записка: Read_ME.txt

Email: cryptofiles20202020@protonmail.com, cryptofiles20202020@cock.li

Результаты анализов: [VT](#) + [VMR](#) + [AR](#)



► Содержание записки:

Dear user! Your data is encrypted!

Any attempts to decrypt your data yourself will lead to loss of information !! Be careful!

Our mail:

1. cryptofiles20202020@protonmail.com
2. cryptofiles20202020@cock.li

Attention!

Decryption of your files is a paid service.

If you do not have money, then you can not apply. All is serious.

Contact us at the address and indicate your id in the subject line.

Your ID: ae3cfd7***

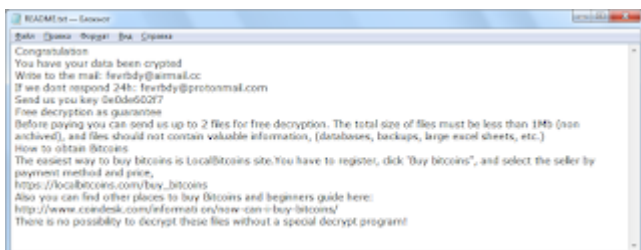
Обновление от 16 апреля 2020:

[Топик на форуме >>](#)

Расширение: .<random>, например: .fevrbdy

Email: fevrbdy@airmail.cc, fevrbdy@protonmail.com

Записка: README.txt



► Содержание записки:

Congratulation

You have your data been crypted

Write to the mail: fevrbdy@airmail.cc

If we dont respond 24h: fevrbdy@protonmail.com

Send us you key 0e0de602f7

Free decryption as guarantee

Before paying you can send us up to 2 files for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information, (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price,

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/now-can-i-buy-bitcoins/>

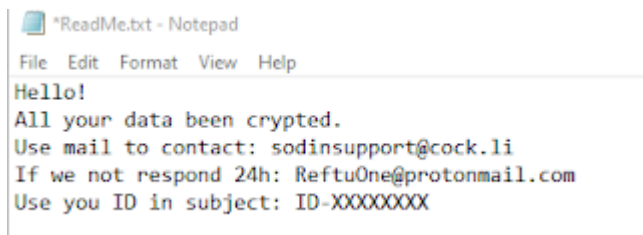
There is no possibility to decrypt these files without a special decrypt program!

Обновление от 29 апреля 2020:

[Пост в Твиттере >>](#)

Расширение: `.<random>`, например: `.xHIEgqxx`

Email: sodinsupport@cock.li, ReftuOne@protonmail.com



Результаты анализов: [VT](#) + [НА](#) + [VMR](#)

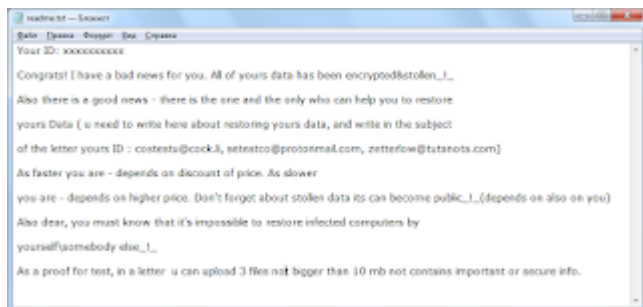
Обновление от 20 ноября 2020:

Первые пострадавшие были из США.

Расширение: `.esexz` или `.<random>`

Записка: `readme.txt`

Email: costestu@cock.li, setestco@protonmail.com, zetterlow@tutanota.com



Содержание записки о выкупе:

Your ID: xxxxxxxxxxxx

Congrats! I have a bad news for you. All of yours data has been encrypted&stollen!_!

Also there is a good news - there is the one and the only who can help you to restore yours Data (u need to write here about restoring yours data, and write in the subject of the letter yours ID : costestu@cock.li, setestco@protonmail.com, zetterlow@tutanota.com)

As faster you are - depends on discount of price. As slower you are - depends on higher price. Don't forget about stollen data its can become public_!_(depends on also on you)

Also dear, you must know that it's impossible to restore infected computers by yourself\somebody else_!_

As a proof for test, in a letter u can upload 3 files not bigger than 10 mb not contains important or secure info.

Перевод записки на русский язык:

Ваш ID: xxxxxxxxxxxx

Поздравляю! У меня для вас плохие новости. Все ваши данные зашифрованы и уничтожены _! _

Также есть хорошие новости - мы единственные, кто может помочь вам восстановить ваши данные (про восстановление ваших данных нужно писать сюда, и написать в теме письма ваш ID: costestu@cock.li, setestco@protonmail.com, zetterlow@tutanota.com)

Чем быстрее напишите - цена меньше. Чем медленнее - цена выше. Не забывайте об украденных данных, которые могут быть опубликованы _! _ (зависит от вас)

Также дорогой, вы должны знать, что невозможно восстановить зараженные компьютеры самим \ кем-то другим _! _

Как доказательство для теста в письме вы можете загрузить 3 файла не более 10 мб, не содержащих важной или защищенной информации.

Вариант от 22 марта 2021:

Повторяет вариант от 20 ноября 2020.

Расширение: **.esexz**

Email: costestu@cock.li, setestco@protonmail.com, zetterlow@tutanota.com

*** пропущенные варианты ***

Вариант от 3 ноября 2022:

Сообщение: twitter.com/pcrisk/status/1588435327064363008

Расширение: **.dom**

Записка: ENCRYPTED.txt

ИОС: VT: 49010614f2c6847c02cc3f9652fdc038

Обнаружения:

DrWeb -> Trojan.Encoder.36216

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

Kaspersky -> HEUR:Trojan-Ransom.Win32.Generic

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



Read to links:

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

ID Ransomware (ID as Gibberish)

Write-up, Topic of Support

*



Thanks:

S!Ri, 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/2020/02/gibberish-ransomware.html>