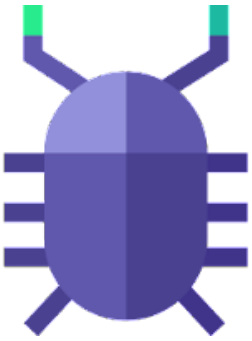
AvosLocker

id-ransomware.blogspot.com/2021/07/avoslocker-ransomware.html

AvosLocker Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English



Этот крипто-вымогатель шифрует данные бизнес-пользователей и компаний с помощью AES-256, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: AvosLocker. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.34160, Trojan.Encoder.34232, Trojan.Encoder.34361
ALYac -> Trojan.Ransom.Avaddon, Trojan.Ransom.AvosLocker
Avira (no cloud) -> TR/Cryptor.gxzkf, TR/Cryptor.aviyo
BitDefender -> DeepScan:Generic.Ransom.BTCWare.AB3FFEB6, Trojan.GenericKD.46739893
ESET-NOD32 -> A Variant Of Win32/Filecoder.OHU
Kaspersky -> HEUR:Trojan-Ransom.Win32.Cryptor.gen
Malwarebytes -> Ransom.Avaddon, Ransom.AvosLocker
Microsoft -> Ransom:Win32/Avaddon.P!MSR, Ransom:Win32/Avaddon
Rising -> Trojan.Generic@ML.82 (RDML:4Ey*
Symantec -> Ransom.AvosLocker, Ransom.AvosLocker!gm1
TrendMicro -> Ransom_Avaddon.R002C0DGJ21, Ransom_Cryptor.R002C0PH721

© Генеалогия: ✂ Avaddon >> AvosLocker

IDR IDENTIFIED ✓

Сайт "ID Ransomware" это идентифицирует как **AvosLocker**.
Информация для идентификации

Активность этого крипто-вымогателя была в начале июля 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

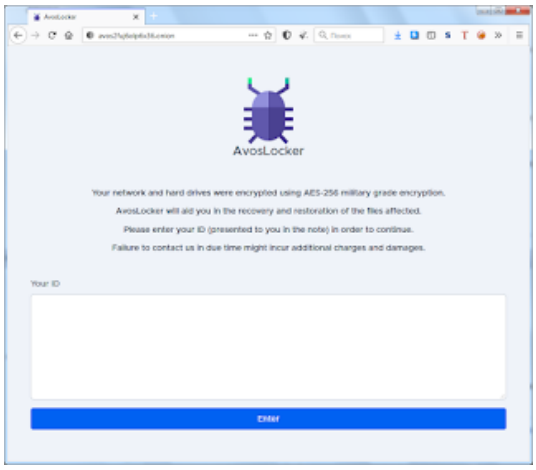
К зашифрованным файлам добавляется расширение: **.avos**

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

Содержание записки о выкупе:
Attention!
Your files have been encrypted using AES-256.
We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key & application.
You may do so by visiting us at hxxx://avos2fuj6olp6x36.onion.
This is an onion address that you may access using Tor Browser which you may download at hxxxs://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.
Hurry up, as the price may increase in the following days.
Message from agent: If you fail to respond in 4 days, the cost of decryption will double up and we will leak some of your data. In 10 days, we will leak all the data we have.
Your ID: 35b1fc*** [totally 64 characters]

Перевод записки на русский язык:
Внимание!
Ваши файлы были зашифрованы с использованием AES-256.
Мы рекомендуем не выключать компьютер, если процесс шифрования не завершен, т.к. ваши файлы могут быть повреждены.
Чтобы расшифровать ваши файлы, вы должны заплатить за ключ дешифрования и приложение.
Вы можете сделать это, посетив нас по адресу hxxx://avos2fuj6olp6x36.onion.
Это onion-адрес, к которому вы можете получить доступ через браузер Tor, который можно скачать на hxxxs: //www.torproject.org/download/
Информация, такая как цена, время до её повышения и т.д., будет вам доступна, когда вы введете свой ID, показанный ниже в этом примечании, на нашем сайте.
Спешите, в ближайшие дни цена может вырасти.
Сообщение от агента: Если вы не ответите за 4 дней, цена расшифровки удвоится, и мы выложим некоторые ваши данные. После 10 дней мы выложим все данные, которые у нас есть.
Ваш ID: 35b1fc *** [всего 64 символа]

Ошибки в записке говорят о том, что английский неродной язык для автора текста. Или кто-то умышленно имитирует незнание английского языка.



Содержание текст на сайте:
AvosLocker
Your network and hard drives were encrypted using AES-256 military grade encryption.
AvosLocker will aid you in the recovery and restoration of the files affected.
Please enter your ID (presented to you in the note) in order to continue.
Failure to contact us in due time might incur additional charges and damages.
Your ID ***

Перевод текста на сайте:

AvosLocker
Ваша сеть и жесткие диски зашифрованы шифрованием военного уровня AES-256.
AvosLocker поможет вам вернуть пострдавшие файлы.
Введите ваш ID (показанный вам в записке), чтобы продолжить.
Отсутсвие контакта с нами может повлечь за собой дополнительные расходы и ущерб.
Ваш ID ***

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

Технические детали + IOC

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**.

Список типов файлов, 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:
GET_YOUR_FILES_BACK.txt - название файла с требованием выкупа;
<random>.exe - случайное название вредоносного файла

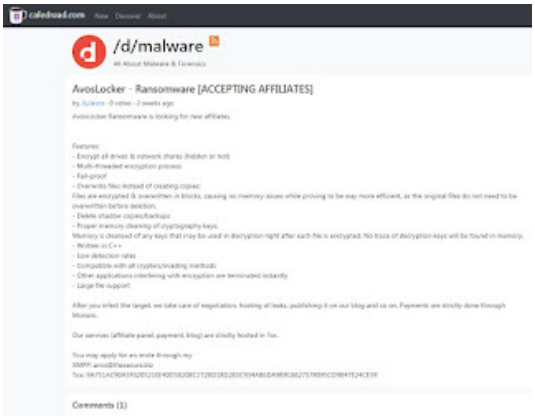
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

C:\Users\User\AppData\Local\Temp\43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856.exe

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Сообщение на сайте Cafedreed: hxxxs://cafedread.com/post/avoslocker-ransomware-accepting-affiliates-ef5f80c705df9a407db3



Tor-URL: hxxx://avos2fuj6olp6x36.onion
XMPP: avos@thesecure.biz
Email: avos@mail2tor.com
XMR (Monero): ***

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:
IOC: **VT**, **HA**, **IA**, **TG**, AR, VMR, JSB
MD5: d285f1366d0d4fdae0b558db690497ea
SHA-1: f6f94e2f49cd64a9590963ef3852e135e2b8deba

SHA-256: 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856
Vhash: 045056655d15556093z52z57nz1fz
Imphash: a24c2b5bf84a5465eb75f1e6aa8c1eec

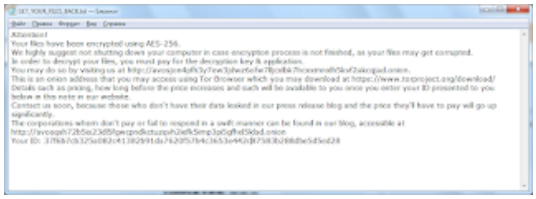
Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

Некоторые другие образцы можно найти на сайте BA:
https://bazaar.abuse.ch/browse/tag/AvosLocker/

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

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

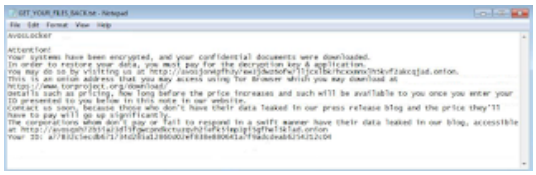
Вариант от 4 августа 2021:
Сообщение >>
Расширение: .avos
Записка: GET_YOUR_FILES_BACK.txt



Tor-URL: hxxx://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad.onion

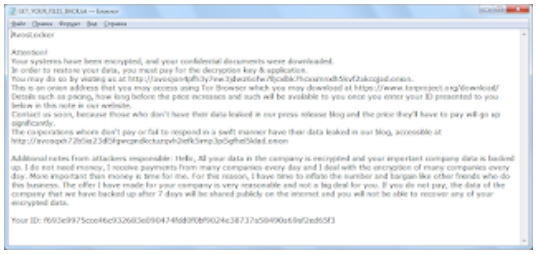
hxxx://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion
Файл: potter.exe
Результаты анализов: IOC: **VT**, **AR**,
MD5: fe977e2028bbb774952df319042e3cab

Вариант от 26 сентября 2021:
Сообщение >>
Расширение: **.avos2**
Записка: GET_YOUR_FILES_BACK.txt



Результаты анализов: IOC: VT, TG
MD5: b76d1d3d2d40366569da67620cf78a87
➤ Обнаружения:
DrWeb -> Trojan.Encoder.34361
BitDefender -> Gen:Variant.Doina.23104
ESET-NOD32 -> A Variant Of Win32/Filecoder.OHU
Malwarebytes -> Ransom.AvosLocker
Microsoft -> Ransom:Win32/AvosLocker.PAC!MTB
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Possible_SMAVOSLOCKERTHA

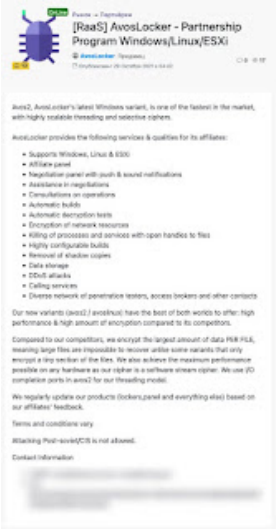
Вариант от 31 октября 2021:
Сообщение >>
Расширение: .avos2
Записка: GET_YOUR_FILES_BACK.txt
Результаты анализов: : VT, TG
MD5: 937232f73c1db87b7dd29e098d4395f6



➤ Содержание записки:
AvosLocker
Attention!
Your systems have been encrypted, and your confidential documents were downloaded.
In order to restore your data, you must pay for the decryption key & application.
You may do so by visiting us at hxxx://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad.onion.
This is an onion address that you may access using Tor Browser which you may download at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.
Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.

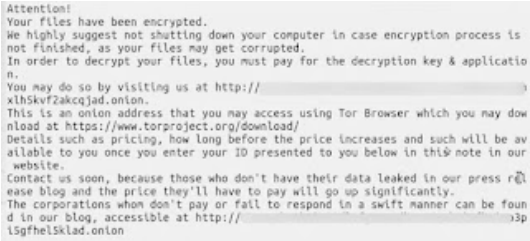
The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog, accessible at hxxx://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion
Additional notes from attackers responsible: Hello, All your data in the company is encrypted and your important company data is backed up. I do not need money, I receive payments from many companies every day and I deal with the encryption of many companies every day. More important than money is time for me. For this reason, I have time to inflate the number and bargain like other friends who do this business. The offer I have made for your company is very reasonable and not a big deal for you. If you do not pay, the data of the company that we have backed up after 7 days will be shared publicly on the internet and you will not be able to recover any of your encrypted data.
Your ID: f693e9975cce46c932683e090474fdd0f0bf9024e38737a58490a69af*******

Вариант от 29 октября 2021:
Сообщение >>
Статья на сайте BC >>
Версии: Avos2 и AvosLinux

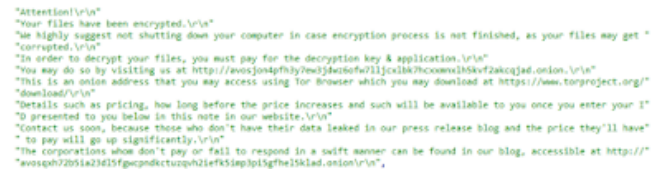

[RaaS] AvosLocker - Partnership Program Windows/Linux/ESXi

Новость декабря 2021:
Операторы AvosLocker используют PDQ Deploy, легитимный инструмент развертывания для автоматизации управления исправлениями, чтобы разместить несколько пакетных сценариев Windows на целевой машине, что помогает им подготовить почву для атаки.
Эти сценарии изменяют или удаляют ключи реестра, принадлежащие определенным инструментам безопасности конечных точек, включая Windows Defender и продукты от Kaspersky, Carbon Black, Trend Micro, Symantec, Bitdefender и Cylance.
Подробнее в статье на сайте BleepingComputer >>
=== 2022 ===

Вариант от 10 января 2022:
Сообщение >>
Статья на сайте BleepngComputer >>
Подробный анализ >>
Названия: AvosLocker, AvosLinux
Расширение: **.avoslinux**
Записка: README_FOR_RESTORE



```
Attention!
Your files have been encrypted.
We highly suggest not shutting down your computer in case encryption process is
not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key & applicatio
n.
You may do so by visiting us at http://
xlh5kvf2akcqjad.onion.
This is an onion address that you may access using Tor Browser which you may dow
nload at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be av
ailable to you once you enter your ID presented to you below in this note in our
 website.
Contact us soon, because those who don't have their data leaked in our press r
ease blog and the price they'll have to pay will go up significantly.
The corporations whom don't pay or fail to respond in a swift manner can be foun
d in our blog, accessible at http://
iSgfhel5klad.onion
```



```
"Attention!\r\n"
"Your files have been encrypted.\r\n"
"We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get "
"corrupted.\r\n"
"In order to decrypt your files, you must pay for the decryption key & application.\r\n"
"You may do so by visiting us at http://avosjon4pfh3y7ew3jdwz6ofw7ilJcxlbk7hcxxmnxlh5kvf2akcqjad.onion.\r\n"
"This is an onion address that you may access using Tor Browser which you may download at https://www.torproject.org/"
"download/\r\n"
"Details such as pricing, how long before the price increases and such will be available to you once you enter your I"
"D presented to you below in this note in our website.\r\n"
"Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have"
" to pay will go up significantly.\r\n"
"The corporations whom don't pay or fail to respond in a swift manner can be found in our blog, accessible at http://"
"avosqxh72b5ia23d15fgwcpndkctuzqvh2ief k5imp3pi5gfhel5klad.onion\r\n",
```

Алгоритм шифрования: Salsa20
Класс файла: ELF64
Результаты анализов: IOC: **VT** + **AR**
➤ Обнаружения:
DrWeb -> Linux.Encoder.126
Avast -> ELF:Filecoder-DC [Trj]
Avira (no cloud) -> LINUX/FileCoder.olrti
BitDefender -> Trojan.Linux.Generic.237462
ESET-NOD32 -> A Variant Of Linux/Filecoder.AvosLocker.A
Kaspersky -> HEUR:Trojan-Ransom.Linux.Agent.p
Microsoft -> Ransom:Linux/AvosLocker.A!MTB
Rising -> Ransom.FileCryptor!8.1A7 (CLOUD)
Symantec -> Trojan.Gen.NPE
TrendMicro -> Trojan.Linux.ZYX.USELVAB22

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

Read to links:

myMessage + Message + Message
Write-up, **Topic of Support**
*

Thanks:

Michael Gillespie, dnwls0719
Andrew Ivanov (article author)
***
to the victims who sent the samples