MedusaLocker

MedusaLocker Ransomware

MedusaLocker NextGen

MedusaLocker 'cut-to-use', 'cut-to-confuse'

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-256 + RSA-2048, а затем требует написать на email вымогателей, чтобы заплатить выкуп, получить программу дешифровки и вернуть файлы. Оригинальное название: в записке не указано. На файле проекта написано: MedusaLocker.pdb. В реестре создается раздел "Medusa".

Обнаружения:

DrWeb -> Trojan.DownLoader30.26418, Trojan.DownLoader30.27698, Trojan.Encoder.30026

BitDefender -> Trojan.GenericKD.32594787, Trojan.GenericKD.41882000

Malwarebytes -> Ransom.Medusa

ESET-NOD32 -> A Variant Of Win32/Filecoder.MedusaLocker.C

GData -> Win32.Trojan-Ransom.Filecoder.BO

Microsoft -> Trojan:Win32/Bluteal!rfn

Symantec -> Trojan.Gen.2, Trojan.Gen.MBT

TrendMicro -> Ransom.Win32.MEDUSALOCKER.A

Kaspersky -> Trojan.Win32.DelShad.azp, Trojan-Ransom.Win32.Medusa.g

---

© Генеалогия: MedusaLocker >> MedusaLocker v.2, v.3, v.4...

Изображение — только логотип статьи

К зашифрованным файлам добавляется расширение **.encrypted**

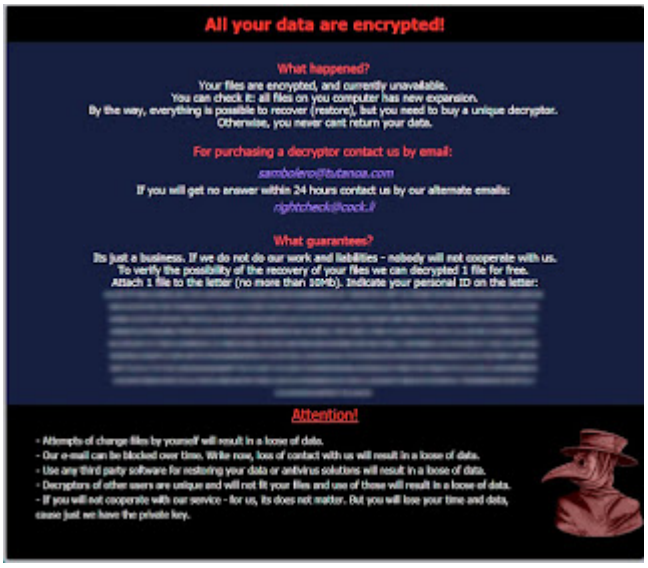
По другим данным известны варианты со следующими расширениями:
.bomber
.boroff
.breakingbad
.locker16
.newlock
.nlocker
.skynet

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

Первые образцы были обнаружены в конце сентября, но активность этого крипто-вымогателя пришлась на начало октября 2019 г. Штамп времени создания файла: 5 октября 2019. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется:
HOW_TO_RECOVER_DATA.html

Первый вариант записки



Второй вариант записки (другие email-адреса)

Содержание записки о выкупе:

All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.

Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

Folieloi@protonmail.com

If you will get no answer within 24 hours contact us by our alternate emails:

Ctorsenoria@tutanota.com

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.

To verify the possibility of the recovery of your files we can decrypted 1 file for free.

Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
[id]
Attention!
- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

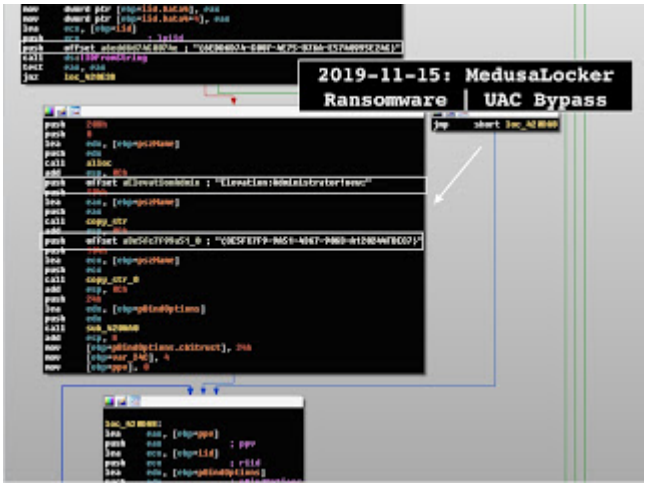
Перевод записки на русский язык:
Все ваши данные зашифрованы!
Что случилось?
Ваши файлы зашифрованы и теперь недоступны.
Вы можете проверить это: все файлы на вашем компьютере имеют новое расширение.
Кстати, все можно вернуть (восстановить), но нужно купить уникальный расшифровщик.
Иначе вы никогда не сможете вернуть свои данные.
Для покупки дешифратора свяжитесь с нами по email:
sambolero@tutanoa.com
Если вы не получите ответ за 24 часа, свяжитесь с нами по email:
rightcheck@cock.li
Какие гарантии?
Это просто бизнес. Если мы не будем выполнять свою работу и обязательства - никто не будет с нами сотрудничать.
Для проверки возможности восстановления ваших файлов мы можем бесплатно расшифровать 1 файл.
Прикрепите 1 файл к письму (не более 10 Мб). Укажите свой личный ID в письме:
[id]
Внимание!
- Попытки самостоятельно изменить файлы приведут к потере данных.
- Наш email может быть заблокирован с течением времени. Напишите сейчас, потеря связи с нами приведет к потере данных.
- Использование любой сторонней программы для восстановления ваших данных или антивирусных решений приведет к потере данных.
- Расшифровщики других пользователей уникальны и не будут соответствовать вашим файлам, и их использование приведет к потере данных.
- Если вы не будете сотрудничать с нашим сервисом - для нас это не имеет значения. Но вы потеряете свое время и данные, потому что только у нас есть закрытый 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-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**.

➤ Использует технологию обхода консоли учетных записей (Bypass UAC) с помощью интерфейса CMSTPLUA COM. Схема из твита Vitali Kremez.



➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки командами:
vssadmin.exe Delete Shadows /All /Quiet
wmic.exe SHADOWCOPY /nointeractive
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest

➤ Стремится завершить следующие процессы, чтобы убедиться, что все файлы данных закрыты и ничто не мешает шифрованию файлов:
wrapper, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, sqlservr, sqlagent, sqladhlp, Culserver, RTVscan, sqlbrowser, SQLADHLP, QBIDPService, Intuit.QuickBooks.FCS, QBCFMonitorService, sqlwriter, msmdsrv, tomcat6, zhudongfangyu, SQLADHLP, vmware-usbarbitator64, vmware-converter, dbsrv12, dbeng8, wxServer.exe, wxServerView, sqlservr.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe,

RTVscan.exe, Defwatch.exe, sqlbrowser.exe, winword.exe, QBW32.exe, QBDBMgr.exe, qbupdate.exe, QBCFMonitorService.exe, axlbridge.exe, QBIDPService.exe, httpd.exe, fdlauncher.exe, MsDtSrvr.exe, tomcat6.exe, java.exe, 360se.exe, 360doctor.exe, wdswfsafe.exe, fdlauncher.exe, fdhost.exe, GDscan.exe, ZhuDongFangYu.exe

Вдобавок к этому использует функционал Windows Restart Manager (менеджер перезагрузки), чтобы получить доступ к наибольшему количеству файлов и зашифровать их.

➤ MedusaLocker создаёт новый ключ в реестре для хранения своего имени файла, но не пути к нему. Это значение сохраняется в: HKEY_CURRENT_USER\SOFTWARE\MDSLK\Self. Неизвестно насколько это важно для работы вредоносной программы, но MDSLK — это похоже на сокращение от MeDuSa LocKer. Подобные ключи использовались и другими шифровальщиками для определения того, была ли машина инфицирована ранее другой версией шифровальщика.

Подробности о шифровании:
При шифровании файлов будет использовано шифрование AES для шифрования каждого файла, а затем ключ AES будет зашифрован открытым ключом RSA-2048, включенным в исполняемый файл Ransomware.

Список файловых расширений, подвергающихся шифрованию:
Многие популярные форматы.
Это могут быть документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

При шифровании пропускаются файлы с расширениями:
.exe, .dll, .sys, .ini, .lnk, .rdp, .encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, .skynet

При шифровании пропускаются следующие папки с файлами:
USERPROFILE
PROGRAMFILES(x86)
ProgramData
\AppData
WINDIR
\Application Data
\Program Files
\Users\All Users
\Windows
\intel
\nvidia

После шифрования MedusaLocker "спит" 60 секунд, затем снова начинает сканирование дисков ПК на наличие незашифрованных и новых файлов.

Вырезки из кода с описанными параметрами

Файлы, связанные с этим Ransomware:

HOW_TO_RECOVER_DATA.html

Readme.html

svchostt.exe

svchostt

l.bat

<random>.exe - случайное название вредоносного файла

MedusaLocker.pdb

Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

%UserProfile%\AppData\Roaming\svchostt.exe

C:\Windows\System32\Tasks\svchostt

Оригинальное название проекта:

C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject\MedusaLocker\Release\MedusaLocker.pdb

Записи реестра, связанные с этим Ransomware:

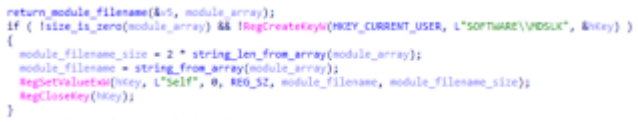
HKCU\SOFTWARE\Medusa

HKCU\SOFTWARE\Medusa\Name s

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ "EnableLinkedConnections" = 1

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA 0

HKEY_CURRENT_USER\SOFTWARE\MDSLK\Self



См. ниже результаты анализов.

Сетевые подключения и связи:

Email-1: Folieloi@protonmail.com, Ctorsenoria@tutanota.com

Email-2: sambolero@tutanoa.com, rightcheck@cock.li

BTC: -

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

Результаты анализов:

Ⓗ **Hybrid analysis >>**

Σ **VirusTotal analysis >> VT>>**

🐞 **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 ===

Вариант от 16 октября 2019:

Пост в Твиттере >>

Расширение: **.skynet**

Записка: Readme.html

Вариант от 19 октября 2019:

[Пост в Твиттере >>]

Список части функционала.

Вариант от 22 октября 2019:

[Топик на форуме >>]

Расширение: .encrypted

Записка: HOW_TO_RECOVER_DATA.html

Email: crypt2020@outlook.com, cryptt2020@protonmail.com

➤ Содержание записки:

Your files are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.
For purchasing a decryptor contact us by email:
crypt2020@outlook.com
If you will get no answer within 24 hours contact us by our alternate emails:
cryptt2020@protonmail.com
What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
180DEF11957324D2AA7F08C25D3BA34663DCD79CAA***. [1024 знака и точка]
Attention!
? Attempts of change files by yourself will result in a loose of data.
? Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
? Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
? Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
? If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Предположительное обновление от 28 октября 2019:

Пост в Твиттере >>

Расширение: **.decrypme**

Записка: HOW_TO_OPEN_FILES.html

Email: decoder83540@protonmail.com, decoder83540@cock.li

➤ Содержание записки:

All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.
For purchasing a decryptor contact us by email:
mrromber@cock.li
If you will get no answer within 24 hours contact us by our alternate emails:
mrromber@tutanota.com
What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
494BE5A953057552DF16891CD4EB271C1356F888C8C98FA80785*** [всего 1024 знака]
Attention!
- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Вариант от 5-10 ноября 2019:

Пост на форуме >>

Расширение: **.ReadTheInstructions**

Email: fartcool@protonmail.ch, bestcool@keemail.me

Записка: INSTRUCTIONS.html

➤ Содержание записки:

All your data are encrypted!
What happened?
Your files are encrypted, and currently unavailable.
You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.
For purchasing a decryptor contact us by email:
fartcool@protonmail.ch
If you will get no answer within 24 hours contact us by our alternate emails:
bestcool@keemail.me
What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:
D86B576A7CE932E7ADC143B9480C931EBC9AF8625CEF5*** [всего 1024 знака]
Attention!
- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Вариант от 11-12 ноября 2019:

Пост в Твиттере >>

Расширение: .ReadTheInstructions
Email: rdp_unlock@outlook.com, rdpunlock@cock.li
Записка: INSTRUCTIONS.html
Результаты анализов: **VT**

Вариант от 14 ноября 2019:

Пост на форуме >>

Расширение: .ReadTheInstructions
Email: sypress@tutanota.com, sypresss@protonmail.com
Записка: INSTRUCTIONS.html

➤ Содержание записки:

All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.

Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

sypress@tutanota.com

If you will get no answer within 24 hours contact us by our alternate emails:

sypresss@protonmail.com

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.

To verify the possibility of the recovery of your files we can decrypted 1 file for free.

Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:

A7EA72ACBFB3EE64E58408796B07B7DF746BD57984B *** [всего 1024 знака]

Attention!

- Attempts of change files by yourself will result in a loose of data.

- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.

- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.

- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.

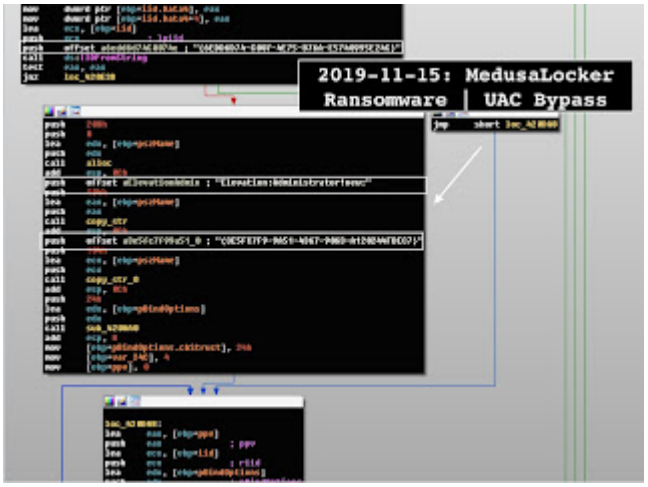
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Вариант от 15 ноября 2019:

Пост в Твиттере >>

UAC bypass using CMSTPLUA COM

Использует обход UAC с помощью интерфейса CMSTPLUA COM



Вариант от 20 ноября 2019:

Топик на форуме >>

Расширение: .ReadTheInstructions

Email: crypt2020@outlook.com, cryptt2020@protonmail.com

Записка: INSTRUCTIONS.html

Результаты анализов: VT

Вариант от 25 декабря 2019:

Топик на форуме >>

Расширение: **.READINSTRUCTIONS**

Записка: RECOVER_INSTRUCTIONS.html

Email: 777decoder777@protonmail.com, 777decoder777@tfwno.gf

➤ Содержание записки:

All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.

Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

777decoder777@protonmail.com

If you will get no answer within 24 hours contact us by our alternate emails:

777decoder777@tfwno.gf

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.

To verify the possibility of the recovery of your files we can decrypted 1 file for free.

Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:

041786A32071FD1D5BF472AE737A831C3F0EEABE36F5D5998DB4E8F377*** [всего 1024 знака]

Attention!

- Attempts of change files by yourself will result in a loose of data.

- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.

- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.

- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.

- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Вариант от 25 декабря 2019:

Расширение: **.ReadInstructions**

Записка: Recovery_Instructions.html

Email: AndrewMiller-1974@protonmail.com

BrianSalgado@protonmail.com

➤ Содержание записки:

YOUR PERSONAL ID:
457CF0616667D9882D479D1F01E094187F20A5B6D0AA88A505 [всего 1024 знаков]
/!\ YOUR COMPANY NETWORK HAS BEEN PENETRATED /!\
ALL YOUR IMPORTANT FILES HAVE BEEN ENCRYPTED!
YOUR FILES ARE SAFE! JUST MODIFIED ONLY. (RSA+AES)
ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMENANTLY DESTROY YOUR FILE.
DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.
NO SOFTWARE AVAILABLE ON INTERNET CAN HELP YOU. WE ONLY HAVE
SOLUTION TO YOUR PROBLEM.
WE GATHERED HIGHLY CONFIDENTIAL/PERSORNAL DATA. THESE DATA
ARE CURRENTLY STORED ON A PRIVATE SERVER. THIS SERVER WILL BE
IMMEDIATELY DESTROYED AFTER YOUR PAYMENT. WE ONLY SEEK MONEY
AND DO NOT WANT TO DAMAGE YOUR REPUTATION. IF YOU DECIDE TO
NOT PAY, WE WILL RELEASE THIS DATA TO PUBLIC OR RE-SELLER.
YOU WILL CAN SEND US 2-3 NON-IMPORTANT FILES AND WE WILL
DECRYPT IT FOR FREE TO PROVE WE ARE ABLE TO GIVE YOUR FILES
BACK.
CONTACT US FOR PRICE (BITCOIN) AND GET DECRYPTION SOFTWARE.
AndrewMiller-1974@protonmail.com
BrianSalgado@protonmail.com
MAKE CONTACT AS SOON AS POSSIBLE. YOUR DECRYPTION KEY IS ONLY STORED
TEMPORARLY. IF YOU DON'T CONTACT US WITHIN 72 HOURS, PRICE WILL BE HIGHER.
WE GATHERED HIGHLY CONFIDENTIAL/PERSORNAL DATA. THESE DATA ARE CURRENTLY
STORED ON A PRIVATE SERVER. THIS SERVER WILL BE IMMEDIATELY DESTROYED AFTER
YOUR PAYMENT. WE ONLY SEEK MONEY AND DO NOT WANT TO DAMAGE YOUR REPUTATION.
IF YOU DECIDE TO NOT PAY, WE WILL RELEASE THIS DATA TO PUBLIC OR RE-SELLER.

=== 2020 ===

Вариант от 15 января 2020:

Пост в Твиттере >>

Видимо тот же самый вариант от 25 декабря 2019.

Вариант от 18 февраля 2020:

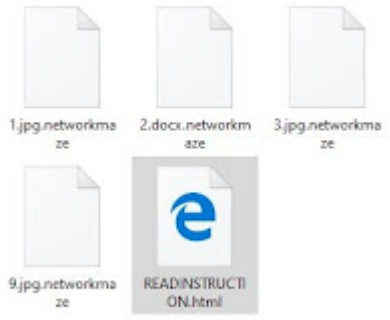
Пост в Твиттере >>

Расширение: **.networkmaze**

Записка: READINSTRUCTION.html

Email: berstife@gmail.com, best@desharonline.top

Результаты анализов: **VT** + **VMR**



Вариант от 22 февраля 2020:

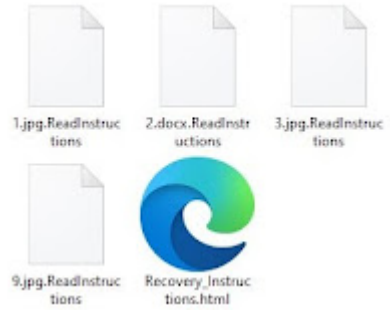
Пост в Твиттере >>

Расширение: .ReadInstructions

Записка: Recovery_Instructions.html

Email: malieholtan@protonmail.com, emergency911service@outlook.com

Результаты анализов: **VT** + **IA** + **VMR**



Вариант от 7 апреля 2020:

Расширение: **.deadfiles**

Вариант от 8 апреля 2020:

Расширение: **.abstergo**

Записка: HOW_TO_RECOVER_DATA.html

Email: mrromber@tutanota.com, mrromber@cock.lii

➤ Содержание записки:

YOUR PERSONAL ID:
B1B801EF63CAAEC7233CE2C770EFAA59139F2E829BF8665DC6B44EC3 [всего 1024 знаков]
/!\ YOUR COMPANY NETWORK HAS BEEN PENETRATED /!\
ALL YOUR IMPORTANT FILES HAVE BEEN ENCRYPTED!
YOUR FILES ARE SAFE! JUST MODIFIED ONLY. (RSA+AES)
ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMENANTLY DESTROY YOUR FILE.
DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.
NO SOFTWARE AVAILABLE ON INTERNET CAN HELP YOU. WE ONLY HAVE
SOLUTION TO YOUR PROBLEM.
WE GATHERED HIGHLY CONFIDENTIAL/PERSORNAL DATA. THESE DATA
ARE CURRENTLY STORED ON A PRIVATE SERVER. THIS SERVER WILL BE
IMMEDIATELY DESTROYED AFTER YOUR PAYMENT. WE ONLY SEEK MONEY
AND DO NOT WANT TO DAMAGE YOUR REPUTATION. IF YOU DECIDE TO
NOT PAY, WE WILL RELEASE THIS DATA TO PUBLIC OR RE-SELLER.
YOU WILL CAN SEND US 2-3 NON-IMPORTANT FILES AND WE WILL
DECRYPT IT FOR FREE TO PROVE WE ARE ABLE TO GIVE YOUR FILES
BACK.
CONTACT US FOR PRICE (BITCOIN) AND GET DECRYPTION SOFTWARE.
mrromber@tutanota.com
mrromber@cock.lii
MAKE CONTACT AS SOON AS POSSIBLE. YOUR DECRYPTION KEY IS ONLY STORED
TEMPORARLY. IF YOU DON'T CONTACT US WITHIN 72 HOURS, PRICE WILL BE HIGHER.

Вариант от 4 мая 2020:

Топик на форуме >>

Расширение: **.himynameisransom**

Записка: HOW_TO_RECOVER_DATA.html

Email: decoderforyou@protonmail.com

decoderforyou@cock.li

Вариант от 18 мая 2020:

Пост на форуме >>

Расширение: .ReadInstructions

Записка: Recovery_Instructions.html

Email: supp0rtdecrypti0n@protonmail.com

➤ Содержание записки:

YOUR PERSONAL ID:

D59994A63BC1F4AEF34D04BA61832D50DF5E42049366B8667 [всего 1024 знаков]

/!\ YOUR COMPANY NETWORK HAS BEEN PENETRATED /!\
All your important files have been encrypted!
Your files are safe! Only modified. (RSA+AES)
ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMANENTLY CORRUPT IT.
DO NOT MODIFY ENCRYPTED FILES.
DO NOT RENAME ENCRYPTED FILES.
No software available on internet can help you. We are the only ones able to
solve your problem.
We gathered highly confidential/personal data. These data are currently stored on
a private server. This server will be immediately destroyed after your payment.
If you decide to not pay, we will release your data to public or re-seller.
So you can expect your data to be publicly available in the near future..
We only seek money and our goal is not to damage your reputation or prevent
your business from running.
You will can send us 2-3 non-important files and we will decrypt it for free
to prove we are able to give your files back.
Contact us for price and get decryption software.
{{URL}}
* Note that this server is available via Tor browser only
Follow the instructions to open the link:
1. Type the addres "https://www.torproject.org" in your Internet browser. It opens the Tor site.
2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it.
3. Now you have Tor browser. In the Tor Browser open "{{URL}}".
4. Start a chat and follow the further instructions.
If you can not use the above link, use the email:
supp0rtdecrypti0n@protonmail.com
Make contact as soon as possible. Your private key (decryption key)
is only stored temporarily.
IF YOU DON'T CONTACT US WITHIN 72 HOURS, PRICE WILL BE HIGHER.

Вариант от 30 мая 2020:

Пост в Твиттере >>

Расширение: **.VinDizelPux**

Записка: Recovery_Instructions.html

Email: dec_helper@outlook.com, dec_helper@excic.com

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

Вариант от 12 июня 2020 или раньше:

Пост в Твиттере >>

Расширение: **.EG**

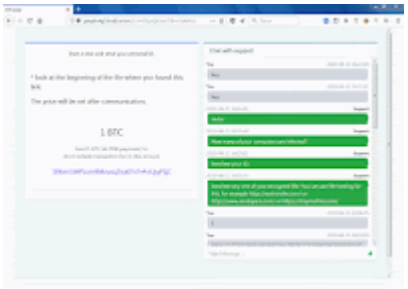
Записка: Recovery_Instructions.html

Email: dec_helper@dremno.com, dec_helper@excic.com

Сумма: 1 BTC

BTC: 1BkmiGWPLum8MzusqZsq6Tn7v4oUjqPLjC

Tor-URL: hxxx://gvlay6u4g53rxdi5.onion/***



Вариант от 29 июня 2020:

Пост в Твиттере >>

Расширение: **.support**

Записка: Recovery_Instructions.html

Email: dec_restore@protonmail.com, decrestore@cock.li

Результаты анализов: **VT** + **AR**

Вариант от 29 июля 2020:

Пост в Твиттере >>

Расширение: **.deadfiles**

Записка: HOW_TO_RECOVER_DATA.html

Email: rescuerr@protonmail.com, rescuer@cock.li

Вариант от 8 сентября 2020:

Пост в Твиттере >>

Расширение: **.networkmaze**

Записка: HOW_TO_RECOVER_DATA.html

Вариант от 12 сентября 2020 или раньше:

Топик на форуме >>

Расширение: **.spartanvladimir60@mail.ru**

Email: spartanvladimir60@mail.ru

Сумма выкупа: $10000

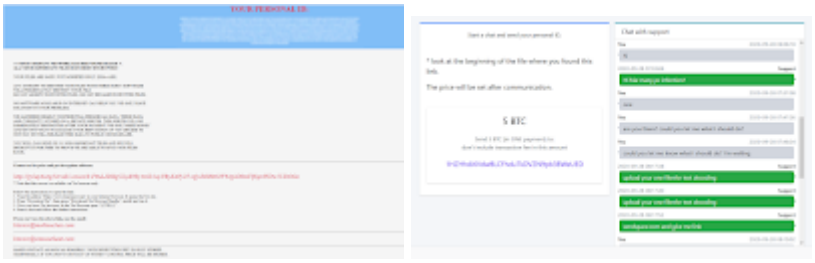
Вариант от 28 сентября 2020:

Расширенеие: **.lr**

Email: bitcoin@mobtouches.com

bitcoin@sitesoutheat.com

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



Вариант от 14 декабря 2020 или раньше:

Расширение: **.inprocess**

Расширение: **.ReadInstructions**

Записка: Recovery_Instructions.txt

Вариант от 27 января 2021:

Расширение: **.divsouth**

Email: support@welchallym.com, support@bigweatherg.com

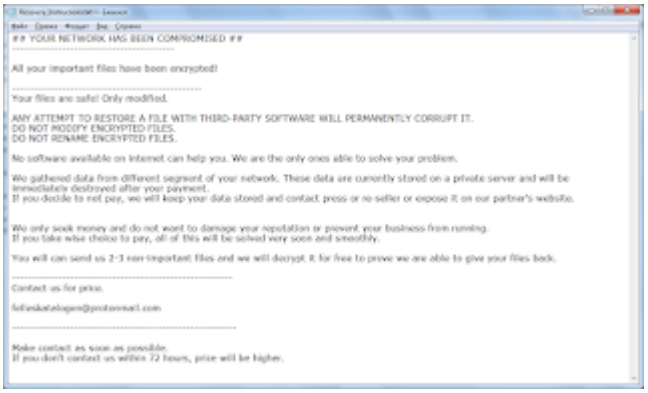
Вариант от 31 января 2021:

Расширение: .ReadInstructions

Записка: Recovery_Instructions.txt

Email: felleskatalogen@protonmail.com

Результаты анализов: **VT** + **HA** + **TG**



➤ Содержание записки:

YOUR NETWORK HAS BEEN COMPROMISED

All your important files have been encrypted!

Your files are safe! Only modified.

ANY ATTEMPT TO RESTORE A FILE WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT.

DO NOT MODIFY ENCRYPTED FILES.

DO NOT RENAME ENCRYPTED FILES.

No software available on internet can help you. We are the only ones able to solve your problem.

We gathered data from different segment of your network. These data are currently stored on a private server and will be immediately destroyed after your payment.

If you decide to not pay, we will keep your data stored and contact press or re-seller or expose it on our partner's website.

We only seek money and do not want to damage your reputation or prevent your business from running.

If you take wise choice to pay, all of this will be solved very soon and smoothly.

You will can send us 2-3 non-important files and we will decrypt it for free to prove we are able to give your files back.

Contact us for price.

felleskatalogen@protonmail.com

Make contact as soon as possible.

If you don't contact us within 72 hours, price will be higher.

Вариант от 12-13 февраля 2021:

Расширение: **.lockfilesCO**

Расширение: **.lockfilesKR**

Email: helper@atacdi.com, helper@buildingwin.com

Recovery_Instructions.html

Результаты анализов: **VT** + **VT**

Вариант от 6 марта 2021 (предположительное родство):

Расширение: **.1btc**

Шифрование: AES-256 + RSA-2048 + ChaCha

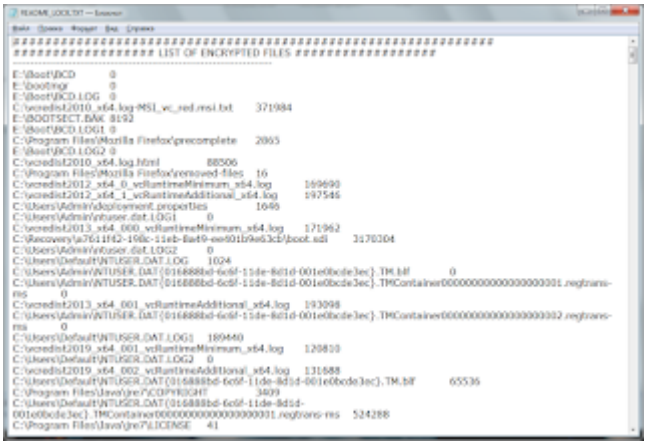
Записка: !!!HOW_TO_DECRYPT!!!.mht

Список файлов: README_LOCK.TXT

Email: cmd@jitjat.org, dirhelp@keemail.me

Результаты анализов: **VT** + **TG**


All your valuable data has been encrypted!

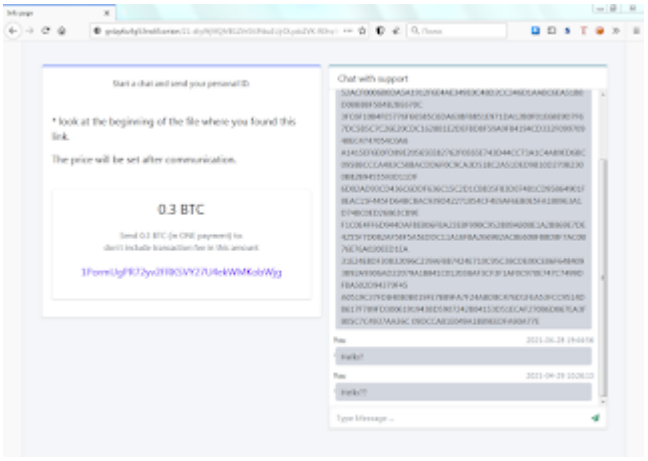


Вариант от 28 апреля 2021:

Записка: Recovery_Instructions.html

helper2@aveuva.com, helper2@biehes.com

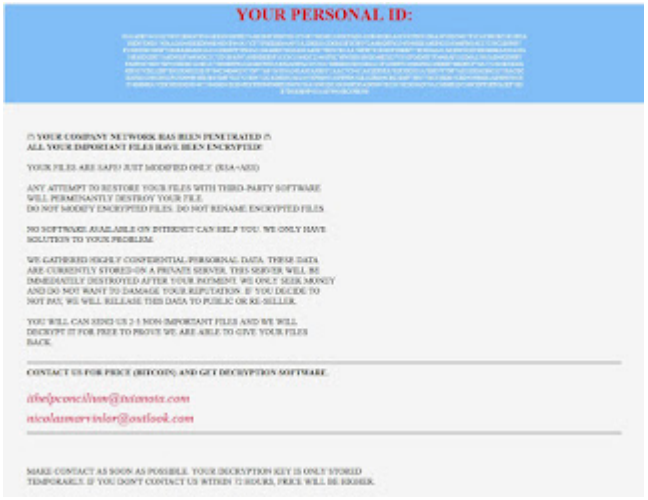
Tor-URL: hxxx://gvlay6u4g53rxdi5.onion/*



Вариант от 30 мая 2021:

Расширение: .Readinstruction

Email: ithelpconcilium@tutanota.com, nicolasmarvinlor@outlook.com



Вариант от 7 декабря 2021:

Расшиение: **.lockfile**

Записка: HOW_TO_RECOVER_DATA.html

Email: rapid@aaathats3as.com, rpd@keemail.me

=== 2022 ===

Вариант от 14 апреля 2022:

Расширение: **.stopfiles**

Записка: Recovery_Instructions.html

Результаты анализов: **VT** + **IA**

Обнаружения:

DrWeb -> Trojan.Encoder.35226

BitDefender -> Generic.Ransom.MedusaLocker.*

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

Rising -> Ransom.MedusaLocker!1.C21A (CLOUD)

TrendMicro -> Ransom.Win32.MEDUSALOCKER.SMTH

Вариант от 8 июня 2022:

Расширение: **.EMPg296LCK**

Записка: !_HOW_RECOVERY_FILES_!.HTML

Результаты анализа: **VT** + **IA**

=== 2022-2023 ===

Варианты в FarAttack Ransomware

С конца (ноябрь, декабрь 2022 или раньше), варианты с MedusaLocker payload (т.н. MedusaLocker3) стали использоваться в атаках Far Attack Ransomware.

=== 2024 ===

Вариант от 5 марта 2024:

Расширение: **.duralock05**

Записка: HOW_TO_BACK_FILES.html

Email: assistant01@backup.capital, assistant01@decodezone.net

IOC: **VT**: MD5: 8648ba384a53b8509b642381a743f255

Обнаружения:

DrWeb - Trojan.Encoder.38448

ESET-NOD32 - A Variant Of Win32/Filecoder.MedusaLocker.

Malwarebytes - Ransom.Medusa

Microsoft - Ransom:Win32/MedusaLocker.A!MTB

TrendMicro - Ransom.Win32.MEDUSALOCKER.SMTH

Вариант от 5 марта 2024:

Расширение: **.genesis15**

Записка: HOW_TO_BACK_FILES.html

assistant01@backup.capital, assistant01@decodezone.net

IOC: **VT**: MD5: 94ccc29e051d0099f99c5d3f2bee4ec7

Обнаружения:

DrWeb - Trojan.Encoder.38448

ESET-NOD32 - A Variant Of Win32/Filecoder.MedusaLocker.

Malwarebytes - Ransom.Medusa

Microsoft - Ransom:Win32/MedusaLocker.A!MTB

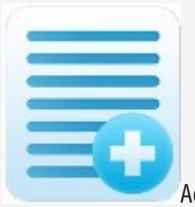
TrendMicro - Ransom.Win32.MEDUSALOCKER.SMTH

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

Read to links:

Tweet on Twitter + Tweet + Tweet + myTweet

ID Ransomware (ID as MedusaLocker)
Write-up, Topic of Support
🎥 Video review >>


Added later:
TAU Threat Analysis: Medusa Locker Ransomware (June 03, 2020)
*
*

- видеообзор от CyberSecurity GrujaRS

Thanks:
CyberSecurity GrujaRS, dnwls0719, Michael Gillespie
Andrew Ivanov (author)
Lawrence Abrams, MalwareHunterTeam, Vitali Kremez
to the victims who sent the samples

Source: http://id-ransomware.blogspot.com/2019/10/medusalocker-ransomware.html