Maoloa

id-ransomware.blogspot.com/2019/02/maoloa-ransomware.html

Maoloa Ransomware

Unnamed RDP-Reset Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью SHACAL-2 (но в коде есть что-то от SHA-512 и SHA-224), а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.11539, Trojan.Encoder.28101, Trojan.Encoder.30969
ESET-NOD32 -> Win32/Filecoder.Maoloa.A, Win32/Filecoder.Maoloa.E
Ikarus -> Trojan-Ransom.Maoloa
BitDefender -> Trojan.Ransom.Maoloa.A
Avira -> TR/Maoloa.*
Другие обнаружения, определенные как GlobeImposter, ошибочные и их можно не учитывать!

© Генеалогия: ✂️ GlobeImposter > предыдущие варианты > Maoloa, Alco, другие Unnamed Ransomware

Почему это не GlobeImposter?
Майкл Джиллеспи подтвердил, что это не GlobeImposter. Идентификатор жертвы и маркеры файлов вообще другие. Анализ текста показывает совпадение знаков и текста в некоторых вариантах GlobeImposter 2.0 прошлого года и одной версии декабря 2017 года. Таким образом, это фальшивый GlobeImposter и обнаружения на VT ошибочные.

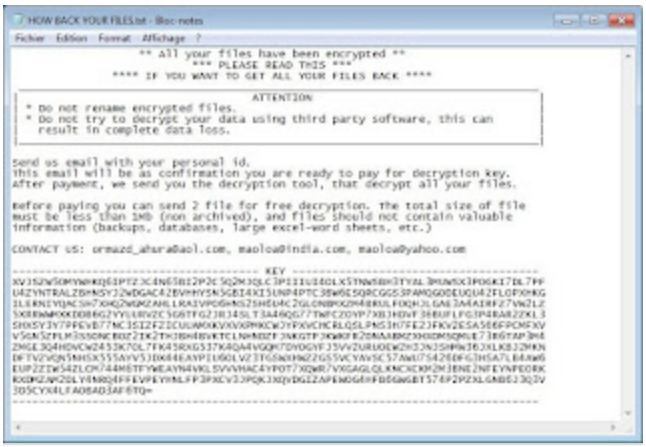
Изображение — только логотип статьи

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

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 найден в начале февраля 2019 г. Штамп времени: 3 февраля 2019. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Нет никаких данных о массовом распространении. Вероятно, что это тестовый или единичный экземпляр.

Записка с требованием выкупа называется: **HOW BACK YOUR FILES.txt**



```
** All your files have been encrypted **
*** PLEASE READ THIS ***
**** IF YOU WANT TO GET ALL YOUR FILES BACK ****

ATTENTION
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, this can
  result in complete data loss.

Send us email with your personal id.
This email will be as confirmation you are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.
Before paying you can send 2 file for free decryption. The total size of file
must be less than 1Mb (non archived), and files should not contain valuable
information (backups, databases, large excel-word sheets, etc.)
CONTACT US: ormazd_ahura@aol.com, maoloa@india.com, maoloa@yahoo.com
---------- KEY ----------
{{ID}}
-------------------------
```

Содержание записки о выкупе:

** All your files have been encrypted **
*** PLEASE READ THIS ***
**** IF YOU WANT TO GET ALL YOUR FILES BACK ****
_____ATTENTION
| * Do not rename encrypted files.
| * Do not try to decrypt your data using third party software, this can
| result in complete data loss.
|_____
Send us email with your personal id.
This email will be as confirmation you are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.
Before paying you can send 2 file for free decryption. The total size of file
must be less than 1Mb (non archived), and files should not contain valuable
information (backups, databases, large excel-word sheets, etc.)
CONTACT US: ormazd_ahura@aol.com, maoloa@india.com, maoloa@yahoo.com
---------- KEY ----------
{{ID}}

Перевод записки на русский язык:

** Все ваши файлы были зашифрованы **
*** ПОЖАЛУЙСТА ПРОЧТИТЕ ЭТО ***
**** ЕСЛИ ВЫ ХОТИТЕ ВЕРНУТЬ ВСЕ ФАЙЛЫ ****

ВНИМАНИЕ
* Не переименовывайте зашифрованные файлы.
* Не пытайтесь расшифровать ваши данные с помощью сторонних программ, это может привести к полной потере данных.

Отправьте нам письмо с вашим личным id.
Это письмо будет подтверждением того, что вы готовы заплатить за ключ расшифровки.
После оплаты мы отправим вам инструмент дешифрования, который расшифрует все ваши файлы.
Перед оплатой вы можете отправить 2 файла для бесплатной расшифровки. Общий размер файла должен быть менее 1 МБ (не в архиве), и файлы не должны содержать ценной информации (резервные копии, базы данных, большие таблицы Excel и т. д.)
СВЯЗЬ С НАМИ: ormazd_ahura@aol.com, maoloa@india.com, maoloa@yahoo.com
---------- KEY ----------
{{ID}}

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, 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**.

➤ Удаляет теневые копии файлов с помощью команды:
vssadmin.exe Delete Shadows / All / Quiet

➤ Очищает журналы Windows.
➤ Сбрасывает настройки RDP на дефолтные (меняет атрибуты файла Default.rdp).
➤ Отключает работу баз данных, сервисных служб, отключает оповещения об их остановке при загрузке системы:
MongoDB, SQLWriter, MSSQLServerOLAPService, MSSQLSERVER, MSSQL$SQLEXPRESS, ReportServer, OracleServiceORCL, OracleDBConsoleorcl, OracleMTSRecoveryService, OracleVssWriterORCL, MySQL

Список файловых расширений, подвергающихся шифрованию:
.1ch, .acl, .acrodata, .adr, .aod, .bak, .bdic, .bin, .blog, .conf, .contact, .crl, .css, .customUI, .dat, .db, .db-journal, .dic, .doc, .docm, .docx, .dot, .dotm, .emf, .eot, .etl, .feed-ms, .fey, .fingerprint, .gif, .htm, .icc, .idx, .ini, .jpg, .jrs, .js, .json, .jsonlz4, .ldb, .lib, .library-ms, .little, .lnk, .log, .lst, .lz4, .lz4, .mozlz4, .mp3, .obi, .oeaccount, .old, .one, .onecache, .onetoc2, .pb, .pma, .png, .pset, .pst, .rdy, .rtf, .sbstore, .searchconnector-ms, .search-ms, .sig, .sqlite, .sqlite3, .srs, .store, .ttf, .txt, .url, .vkf, .vpol, .vrt, .wfe, .win, .wmdb, .wmv, .woff, .wpl, .wtv, .xml
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы без расширений и многие другие типы файлов.

Файлы, связанные с этим Ransomware:
HOW BACK YOUR FILES.txt
<random>.exe - случайное название

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

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

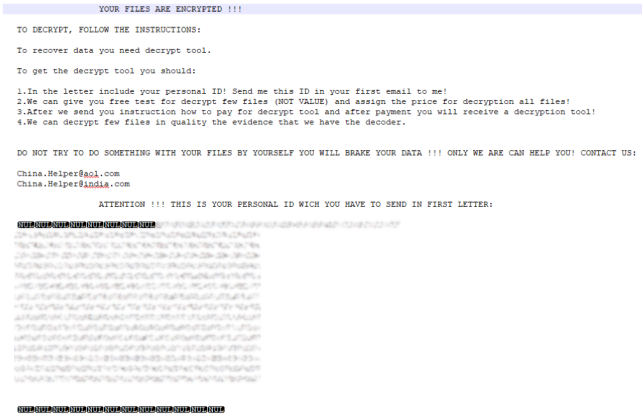
Сетевые подключения и связи:
Email: ormazd_ahura@aol.com, maoloa@india.com, maoloa@yahoo.com
BTC: ***
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
⧁ **ANY.RUN analysis >>**
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно.

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

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===
Обновление от 6 ноября 2018 и даже раньше (в сентябре 2018)**:**
Пост в Твиттере >>
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.Ox4444**
Этимология названия расширения: **ox** - по-английски: вол, бык.
Результаты анализов: **VT** + **VMRay**



YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:

China.Helper@aol.com
China.Helper@india.com

ATTENTION !!! THIS IS YOUR PERSONAL ID WICH YOU HAVE TO SEND IN FIRST LETTER:

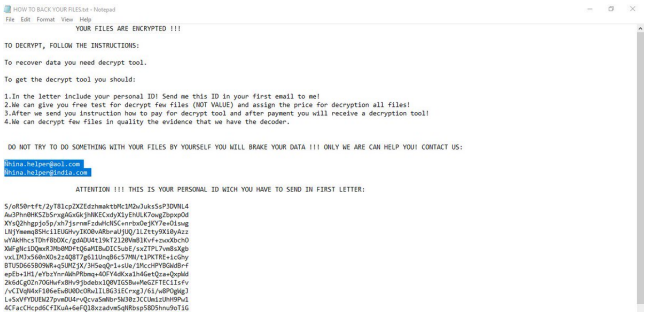
Обновление от 28 февраля 2019:
Расширение: **.brydreed**
Email: informerdecrypted@aol.com, brydreed@india.com
Записка: HOW TO BACK YOUR FILES.TXT
➤ Содержание записки:
** All your files have been encrypted **
*** PLEASE READ THIS ***
**** IF YOU WANT TO GET ALL YOUR FILES BACK ****

ATTENTION
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, this can result in complete data loss.

Send us email with your personal encryption KEY.
This email will be as confirmation your are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.
Before paying you can send 2 file for free decryption. The total size of file must be less than 1Mb (non archived), and files should not contain valuable information (backups, databases, large excel-word sheets, etc.)
CONTACT US: informerdecrypted@aol.com, brydreed@india.com
---------- KEY ----------
N5ET35KOBD6T7*****ORP7KA2A=

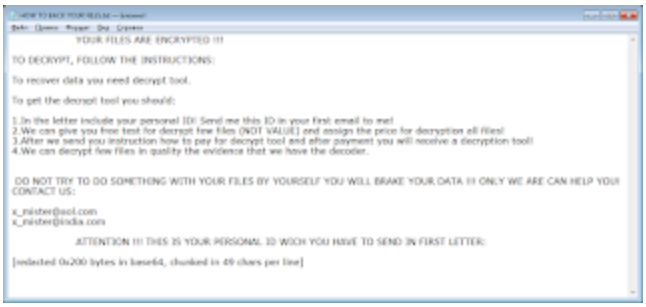
Обновление от 1 марта 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Пост в Твиттере >>
Расширение: **.Alco4444**
Этимология названия расширения: **алько** - южноамериканская дикая собака.
Записка: HOW TO BACK YOUR FILES.txt

Email: Ñhina.helper@aol.com, Ñhina.helper@india.com
Вероятно, правильные адреса: China.Helper@aol.com, China.Helper@india.com
Результаты анализов: **VT**

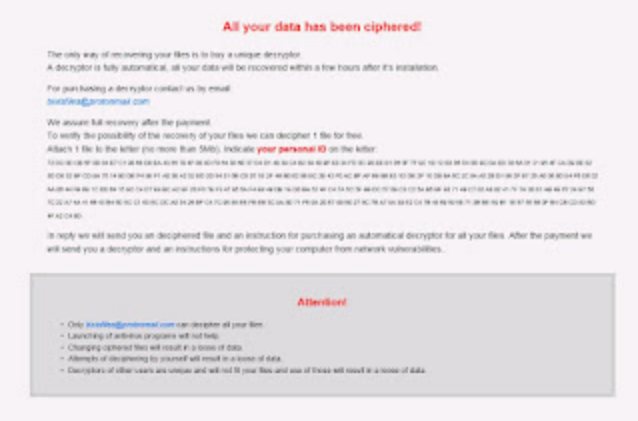


➤ Содержание записки:
YOUR FILES ARE ENCRYPTED !!!
TO DECRYPT, FOLLOW THE INSTRUCTIONS:
To recover data you need decrypt tool.
To get the decrypt tool you should:
1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.
DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:
Ñhina.helper@aol.com
Ñhina.helper@india.com
ATTENTION !!! THIS IS YOUR PERSONAL ID WICH YOU HAVE TO SEND IN FIRST LETTER:
S/oR50rtft/2yT81cpZXZEdzhmaktbMclM2w]uksSsP3DV***

Обновление от 20 марта 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.Mr-X666**
Результаты анализов: **VT**

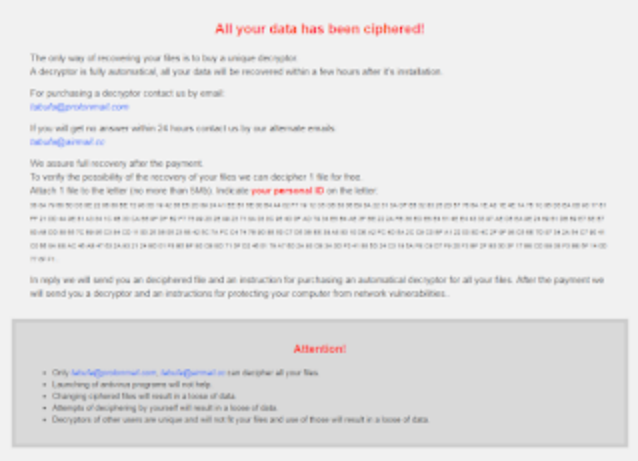


Обновление от 10 апреля 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.Tiger4444**
Этимология названия расширения: tiger - по-английски: тигр.
Записка: how_to_back_files.html или HOW TO BACK YOUR FILES.txt



Обновление от 11 апреля 2019:
Топик на форуме >>
Расширение: **.tabufa**
Email: tabufa@protonmail.com, tabufa@airmail.cc

Файл EXE: meaykdxuvtfy.exe или типа того.
Записка: how_to_back_files.html или другой файл.



➤ Содержание записки:
All your data has been ciphered!
The only way of recovering your files is to buy a unique decryptor.
A decryptor is fully automatical, all your data will be recovered within a few hours after it's installation.
For purchasing a decryptor contact us by email:
tabufa@protonmail.com
If you will get no answer within 24 hours contact us by our alternate emails:
tabufa@airmail.cc

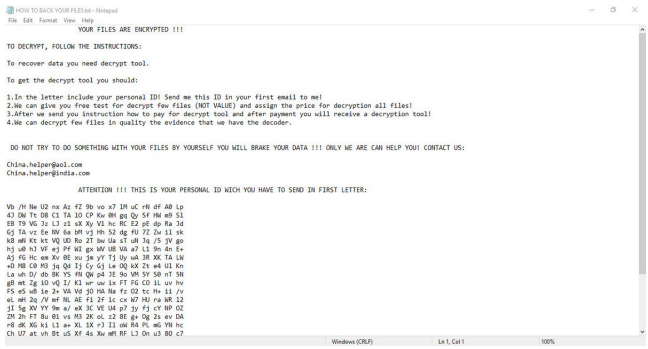
We assure full recovery after the payment.
To verify the possibility of the recovery of your files we can decipher 1 file for free.
Attach 1 file to the letter (no more than 5Mb). Indicate your personal ID on the letter:
38 8A 79 68 5D D3 8E *** .
In reply we will send you an deciphered file and an instruction for purchasing an automatical decryptor for all your files. After the payment we will send you a decryptor and an instructions for protecting your computer from network vulnerabilities..
Attention!
Only tabufa@protonmail.com, tabufa@airmail.cc can decipher all your files.
Launching of antivirus programs will not help.
Changing ciphered files will result in a loose of data.
Attempts of deciphering by yourself 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.

Обновление от 17 апреля 2019:
Расширение: **.systems32x**
Записка: HOW TO BACK YOUR FILES.TXT
Email: systems32x@gmail.com
systems32x@yahoo.com
systems32x@tutanota.com
help32xme@usa.com
additional.mail@mail.com

```
                ** All your files have been encrypted **
                    *** PLEASE READ THIS ***
            **** IF YOU WANT TO GET ALL YOUR FILES BACK ****

+-------------------------------------------------------------------------+
|                                 ATTENTION                               |
| * Do not rename encrypted files.                                        |
| * Do not try to decrypt your data using third party software, this can  |
|   result in complete data loss.                                         |
+-------------------------------------------------------------------------+

Send us email with your personal encryption KEY.
This email will be as confirmation your are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.

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

CONTACT US:
systems32x@gmail.com
systems32x@yahoo.com

ADDITIONAL CONTACTS:
systems32x@tutanota.com
help32xme@usa.com
additional.mail@mail.com

---------------------------------- KEY ----------------------------------
IT3SIZK2FJN73DXVSPMSI3KW474IRWXENQQNDLGSO6NDNU7N3DGEVC75VM5A5DKA6TGBI7AKU6YH6VEG
RWKKA4OT7D7LYEUDKHUGB3ZAPOKBNHMRZRWDVM4K5T4P4IABDMJQOM3IIEEK4M5YKTEYUJN2HNXCELX6U
EQ3RQV3IP565NINOE4CKSKYXBXEOR5W4RY3LROR2WKNSRFYLE732QVEIJDJFMJMPMBES6IM3WEGCRZ2O
WH6YXFTFG2V2AV7J6OBGSHBGUAG5AVM6RUW5OUVHR4GRH43OTOL72GTD7POQ2H6DOAGZ4UHAUYYVKY4B
36OPSM5XE7MDYDD2I34J3ZTPUT2BPW5EXVR5IJ3IUKC3FVG5WAKCDXTPAPFO4SVG52LB8J7Q1YQFIFGBY
87ZAHVASVR2VCV63EXUNUPY26LTULPSFA4HP7FA7AZFWOH76Q2JTHZA7FA2EUKAE3WEPTHVLS4NTUHJH
8RIA6W6IU2R54LDZTJ5RCRQ243Q55AIJJL3M2GVKIETDJBHSFUMVBY4EI42ID6A35FLVSHBFIPOLM7I
GKVQTFB2EUF53DS6TOIEILIAGRK7NYUPBC3RSDCUDDH6FHCSADLHIGSFOR2WNARVXCQCSQO6AUHCNHKS
PCUBXOYOUQUKPMMUMLFCRDWOLLDEB4I7OLWAL345OALVW7AFEWNFARV2WCWUARX5YSVPBAB3TR5CPQBD
Y4SZKRS3A2LTOF2G3M67JNOCXCKQRGCXJGFVSVWBUYAGR2H4ISMF7V3KODTQWFLHPIFLTGBOBCQYPMSG
J2O4A43A4WEJPVMUP2PA=
-------------------------------------------------------------------------
```

Обновление от 27 апреля 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**

Расширение: **.Pig4444**
Этимология названия расширения: **pig** - по-английски: свинья, поросенок.
Записка: HOW TO BACK YOUR FILES.txt
Результаты анализов: VT + VMR



Обновление от 3-5 мая 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.Tiger4444**
Этимология названия расширения: **tiger** - по-английски: тигр.
Записка: HOW TO BACK YOUR FILES.txt
Результаты анализов: **VT + VMR**

Обновление от 18 мая 2019:
Пост в Твиттере >>
Расширение: **.[epta.mcold@gmail.com]**
Записка: !INSTRUCTI0NS!.TXT
Email: epta.mcold@gmail.com, epta.mcold@yahoo.com, epta.mcold@aol.com

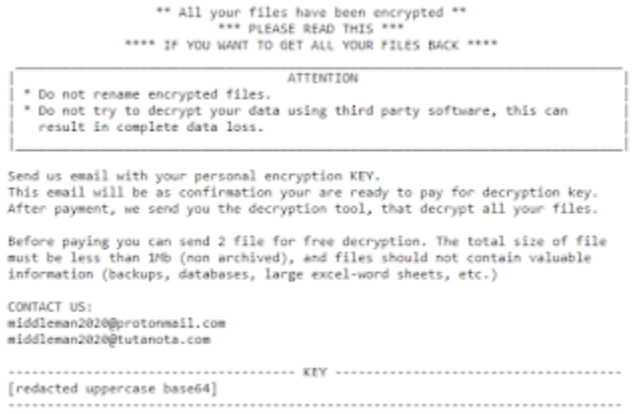
➤ Содержание записки:
** All your files have been encrypted **
*** PLEASE READ THIS ***

**** IF YOU WANT TO GET ALL YOUR FILES BACK ****

| ATTENTION
| * Do not rename encrypted files.
| * Do not try to decrypt your data using third party software, this can
| result in complete data loss.

Send us email with your personal encryption KEY.
This email will be as confirmation your are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.
Before paying you can send 2 file for free decryption. The total size of file
must be less than 1Mb (non archived), and files should not contain valuable
information (backups, databases, large excel-word sheets, etc.)
CONTACT US:
epta.mcold@gmail.com
epta.mcold@yahoo.com
ADDITIONAL CONTACTS:
epta.mcold@aol.com
---------- KEY ----------
EFLNUW6RCNGXJOBXRNJ4JETCGDCJ6ZN76WWLKAG5YHLT27A***

Email: middleman2020@protonmail.com, middleman2020@tutanota.com



Обновление от 18 июня 2019:
Пост в Твиттере >>
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.pig4444**
Этимология названия расширения: **pig** - по-английски: свинья, поросенок.
Записка: HOW TO BACK YOUR FILES.TXT

YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:

China.Helper@aol.com

ATTENTION !!! THIS IS YOUR PERSONAL ID WICH YOU HAVE TO SEND IN FIRST LETTER:

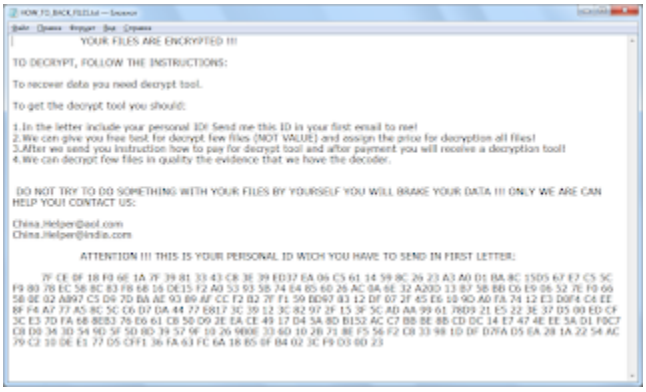
Обновление от 21 июня 2019:

Этот вариант подробно описан в статье **Alco Ransomware >>>**

Расширение: **.Horse4444**

Этимология названия расширения: **horse** - по-английски: лошадь, конь.

Записка: HOW_TO_BACK_FILES.txt



YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:

China.Helper@aol.com
China.Helper@india.com

ATTENTION !!! THIS IS YOUR PERSONAL ID WICH YOU HAVE TO SEND IN FIRST LETTER:

Обновление от 1 июля 2019:

Пост в Твиттере >>

Это не относится напрямую к Maoloa Ransomware!

Email: Decryptcn@protonmail.ch

URL: xxxx://47.92.55.239/s/

Записки: HOW_TO_BACK_YOUR_FILES.txt на китайском и английском языках

HOW_TO_BACK_YOUR_FILES.txt - на английском языке

Текст записки взят из Maoloa или Alco, которые сам имитируют записку GlobeImposter, но имеют свои особенности.

Идентификация в IDR: сначала "Fake GlobeImposter", потом "ChineseRarypt" по моему названию в статье **ChineseRarypt Ransomware**.
Помещает файлы в Rar-архив вместо шифрования. Пароль может находиться в той же директории, в Rar-файле. Статья от Tencent по этому фальшивому GlobeImposter >>

Обновление от 10 июля 2019:
Топик на форуме >>
Расширение: **.shelbyboom**
Email: shelbyboom@protonmail.com, shelbyboom@cock.li
Записка: how_to_back_files.html


All your data has been ciphered!

The only way of recovering your files is to buy a unique decryptor.
A decryptor is fully automatical, all your data will be recovered within a few hours after it's installation.

For purchasing a decryptor contact us by email:
shelbyboom@protonmail.com

If you will get no answer within 24 hours contact us by our alternate emails:
shelbyboom@cock.li

We assure full recovery after the payment.
To verify the possibility of the recovery of your files we can decipher 1 file for free.
Attach 1 file to the letter (no more than 5MB). Indicate your personal ID on the letter.

In reply we will send you an deciphered file and an instruction for purchasing an automatical decryptor for all your files. After the payment we will send you a decryptor and an instructions for protecting your computer from network vulnerabilities.

Attention!

- Only shelbyboom@protonmail.com, shelbyboom@cock.li can decipher all your files.
- Launching of antivirus programs will not help.
- Changing ciphered files will result in a loose of data.
- Attempts of deciphering by yourself 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.

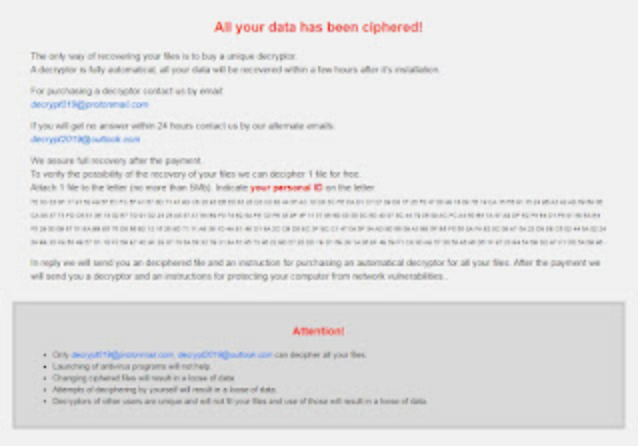
Обновление от 17 июля 2019:
Топик на форуме >>
Расширение: **.diller13**
Записка: how_to_back_files.html
Email: diller13@protonmail.com, diller13@cock.li

➤ Содержание записки:
All your data has been ciphered!
The only way of recovering your files is to buy a unique decryptor.
A decryptor is fully automatical, all your data will be recovered within a few hours after it's installation.
For purchasing a decryptor contact us by email:
diller13@protonmail.com
If you will get no answer within 24 hours contact us by our alternate emails:
diller13@cock.li
We assure full recovery after the payment.
To verify the possibility of the recovery of your files we can decipher 1 file for free.
Attach 1 file to the letter (no more than 25Mb). Indicate your personal ID on the letter:
20 44 81 30 49 01 D0 83 *** (768 заков с пробелами).
In reply we will send you an deciphered file and an instruction for purchasing an automatical decryptor for all your files. After the payment we will send you a decryptor and an instructions for protecting your computer from network vulnerabilities..
Attention!
Only diller13@protonmail.com, diller13@cock.li can decipher all your files.
Launching of antivirus programs will not help.
Changing ciphered files will result in a loose of data.
Attempts of deciphering by yourself 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.

Обновление от 22 июля 2019:
Этот вариант подробно описан в статье **Alco Ransomware >>>**
Расширение: **.Rabbit4444**
Записка: не найдена.

Обновление от 25 августа 2019:
Новая идентификация: статья Maola Ransomware >>
Расширение: **.decrypt019**

Записка: how_to_back_files.html
Email: decrypt019@protonmail.com, decrypt2019@outlook.com


All your data has been ciphered!

The only way of recovering your files is to buy a unique decryptor.
A decryptor is fully automatical, all your data will be recovered within a few hours after it's installation.

For purchasing a decryptor contact us by email:
decrypt019@protonmail.com

If you will get no answer within 24 hours contact us by our alternate emails:
decrypt2019@outlook.com

We assure full recovery after the payment.
To verify the possibility of the recovery of your files we can decipher 1 file for free.
Attach 1 file to the letter (no more than 5Mb). Indicate your personal ID on the letter.

In reply we will send you an deciphered file and an instruction for purchasing an automatical decryptor for all your files. After the payment we will send you a decryptor and an instructions for protecting your computer from network vulnerabilities.

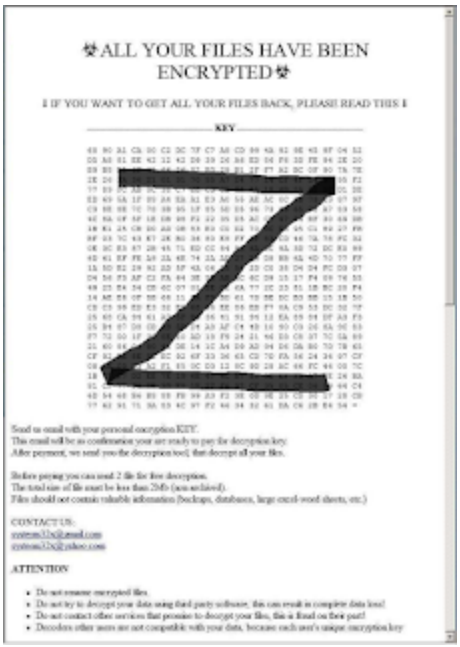
Attention!

- Only decrypt019@protonmail.com, decrypt2019@outlook.com can decipher all your files.
- Launching of antivirus programs will not help.
- Changing ciphered files will result in a loose of data.
- Attempts of deciphering by yourself 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.

--- пропущенные варианты ---

=== 2020 ===

Обновление от 22 января 2020:
Расширение: **.system32x**
Email: systems32@gmail.com, systems32x@yahoo.com
Специальный файл ids.txt содержит ID, написанный 9 раз.
Записка в EXE-формате: !!INSTRUCTIONS!!.exe
EXE-файлы: msopsm.exe, system32x.exe
Результаты анализов: **VT** + **VT** + **VT**


☣ALL YOUR FILES HAVE BEEN ENCRYPTED☣

! IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS !

KEY

Send us email with your personal encryption KEY.
This email will be as confirmation your are ready to pay for decryption key.
After payment, we send you the decryption tool, that decrypt all your files.

Before paying you can send 2 file for free decryption.
The total size of file must be less than 2MB (non-archived).
Files should not contain valuable information (backups, databases, large excel-word sheets, etc.)

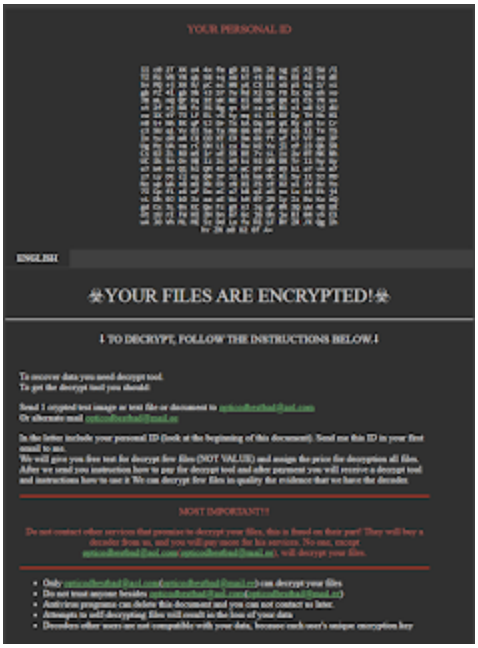
CONTACT US:
systems32x@gmail.com
systems32x@yahoo.com

ATTENTION

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, this can result in complete data loss!
- Do not contact other services that promise to decrypt your files, this is fraud on first part!
- Decoders other users are not compatible with your data, because each user's unique encryption key

=== 2021 ===

Вариант от 20 января 2021:
Топик на форуме >>
Расширение: .Encrypted
Email: opticodbestbad@aol.com, opticodbestbad@mail.ee
Записка: info.html
Результаты анализов: **VT** + **TG**



Вариант от 10 апреля 2021:
Сообщение >>
Расширение: **.charlie.j0hnson**
Записка: HOW TO RETURN YOU FILES.exe
Результаты анализов: **VT** + **IA** + **TG**

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

Read to links:

+ myTweet
ID Ransomware (ID as Maoloa)
Write-up, Topic of Support
*

Thanks:

S!Ri, Michael Gillespie
Andrew Ivanov (author), Thyrex
Petrovic
*