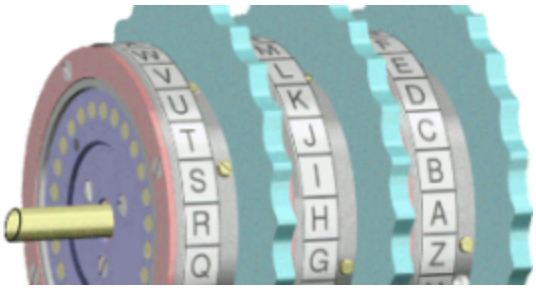
RotorCrypt

id-ransomware.blogspot.com/2016/10/rotorcrypt-ransomware.html



RotorCrypt (RotoCrypt) Ransomware

Tar Ransomware

(шифровальщик-вымогатель)

Translation into English

Как удалить? Как расшифровать? Как вернуть данные?
По ссылке выберите Управление "К" МВД России и подайте онлайн-заявление.
См. также статьи УК РФ:
ст. 272 "Неправомерный доступ к компьютерной информации"
ст. 273 "Создание, использование и распространение вредоносных компьютерных программ"

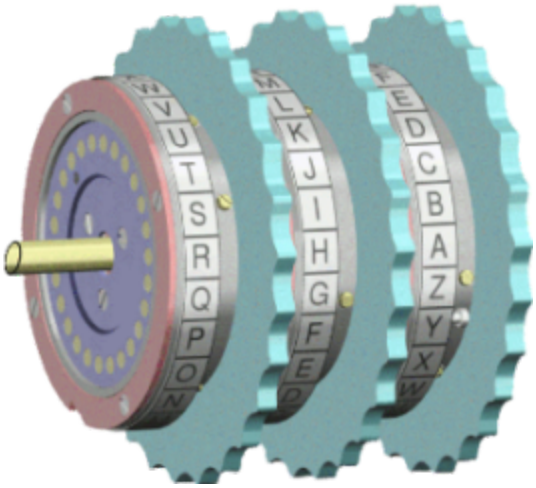
Информация о шифровальщике

Этот крипто-вымогатель шифрует данные пользователей и серверов организаций с помощью RSA, а затем требует связаться с вымоагтелями по email, чтобы вернуть файлы. За возвращение файлов в нормальное состояние вымогатели требуют выкуп в 7 биткоинов, 2000-5000 долларов или евро. Аппетит обнаглевших от безнаказанности вымогателей растёт не по дням, а по часам.

Обнаружения:
Dr.Web -> Trojan.Encoder.5342, Trojan.Encoder.29037
BitDefender -> Gen:Variant.Razy.109164, Gen:Variant.Ransom.RotorCrypt.1,

Trojan.Ransom.RotorCrypt.A, Trojan.GenericKD.12470370,
Gen:Variant.Ransom.RotorCrypt.2
Kaspersky -> Trojan-Ransom.Win32.Rotor.*, HEUR:Trojan.Win32.Generic

© Генеалогия: Gomasom > RotorCrypt



Изображение не принадлежит шифровальщику

К зашифрованным файлам добавляются составные расширения по шаблону:

<file_name>.<file_extension><ransom_extension>

На данный момент это расширения **.c400, .c300** на конце файла и email вымогателей перед ними:
!___ELIZABETH7@PROTONMAIL.COM____.c400
!_____LIKBEZ77777@GMAIL.COM____.c400
!_____GEKSOGEN911@GMAIL.COM____.c300

Таким образом файл Document.doc после шифрования станет:
Document.doc!____ELIZABETH7@PROTONMAIL.COM____.c400
Document.doc!_____LIKBEZ77777@GMAIL.COM____.c400
Document.doc!_____GEKSOGEN911@GMAIL.COM____.c300

Активность этого крипто-вымогателя пришлась на конец октября - ноябрь 2016 г., но продолжилась и в 2017-2019 годах с другими расширениями (см. внизу "Блок обновлений").

Записки с требованием выкупа называются:
readme.txt или ***readme.txt**

Содержание записки о выкупе (из версии **Tar**):
Good day
Your files were encrypted/locked

As evidence can decrypt file 1 to 3 1-30MB
The price of the transcripts of all the files on the server: 7 Bitcoin
Recommend to solve the problem quickly and not to delay
Also give advice on how to protect Your server against threats from the network
(Files sql mdf backup decryption strictly after payment)!

Перевод записки на русский язык:
Добрый день
Ваши файлы зашифрованы / заблокированы
Как доказательство можем расшифровать файл 1 до 3 1-30MB
Стоимость расшифровки всех файлов на сервере: 7 Bitcoin
Рекомендуем решить эту проблему быстро и без задержки
Кроме того, дадим советы о том, как защитить свой сервер от угроз из сети
(Файлы sql mdf backup дешифруем только после оплаты)!

Email вымогателей:
ELIZABETH7@PROTONMAIL.COM
LIKBEZ77777@GMAIL.COM
GEKSOGEN911@GMAIL.COM
и другие (см. внизу в обновлениях)

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, эксплойтов, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки командами:
vssadmin.exe delete shadows /all /Quiet
bcdedit.exe /set {current} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {current} recoveryenabled no

Список файловых расширений, подвергающихся шифрованию:

.1cd, .avi, .bak, .bmp, .cf, .cfu, .csv, .db, .dbf, .djvu, .doc, .docx, .dt, .elf, .epf, .erf, .exe, .flv, .geo, .gif, .grs, .jpeg, .jpg, .lgf, .lgp, .log, .mb, .mdb, .mdf, .mxl, .net, .odt, .pdf, .png, .pps, .ppt, .pptm, .pptx, .psd, .px, .rar, .raw, .st, .sql, .tif, .txt, .vob, .vrp, .xls, .xlsb, .xlsx, .xml, .zip (53 расширения).

Расширений может быть больше, в основном это файлы документов MS Office, изображения, архивы, базы данных, в том числе российского ПО 1С-Бухгалтерия, а также R-Keeper, Sbis и пр. Шифрованию подвержены общие сетевые ресурсы (диски, папки).

Файлы, связанные с RotorCrypt Ransomware:
iuy.exe
<random_name_8_chars>.exe
<random_name_8_chars>___.exe
DNALWmjW.exe и другие
GWWABPFL_Unpack.EXE
<random_name_8_chars>.lnk
jHlxJqfV.lnk и другие

Расположения:
%TEMP%\<random_name_8_chars>.exe
C:\Users\User_name\AppData\local\<random_name_8_chars>.exe
C:\Users\User_name\Desktop\<random_name_8_chars>.exe
C:\GWWABPFL_Unpack.EXE
%LOCALAPPDATA%\Microsoft Help\DNALWmjW.exe
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\jHlxJqfV.lnk

Записи реестра, связанные с RotorCrypt Ransomware:
См. ниже гибридные анализы.

Результаты анализов по версиям:
Гибридный анализ на Tar >>
Гибридный анализ для ELIZABETH >>
Гибридный анализ для LIKBEZ >>
Гибридный анализ на GEKSOGEN >>
VirusTotal анализ на Tar >>
VirusTotal анализ для ELIZABETH >>
VirusTotal анализ для LIKBEZ >>
VirusTotal анализ на GEKSOGEN >>

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

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

Предыстория 1:
На переходном периоде от Gomasom до Tar и RotorCrypt, и параллельно с их ранними версиями, использовались другие составные расширения "roto" и "crypt", от которых,

собственно, и произошло название шифровальщика RotorCrypt, через обнаружение Trojan-Ransom.Win32.Rotor, используемое в продуктах ЛК.
Время распространения: от июня 2015 до января 2016, с продолжением до октября 2016.

Шаблон расширений:
<file_name>.<file_extension><ransom_extension>

Список расширений (List of extensions):
.-.DIRECTORAT1C8@GMAIL.COM.roto
.-.DIRECTORAT1C@GMAIL.COM.roto
.-.directorat1c@gmail.com.roto
.-.CRYPTSb@GMAIL.COM.roto
!-==kronstar21@gmail.com=--.crypt
!==helpsend369@gmail.com==.crypt
!__crypthelp12@gmail.com_.crypt
!___prosschiff@gmail.com_.crypt
!____moskali1993@mail.ru___.crypt
!______sufnex331@gmail.com______.crypt
!______bigromintol971@gmail.com______.crypt
!_______GASWAGEN123@GMAIL.COM____.crypt
!_________pkigxdaq@bk.ru_______.crypt
!_____DESKRYPTEDN81@GMAIL.COM.crypt

Для некоторых из них, возможно и для всех, была выпущена утилита дешифровки RakhniDecryptor.
Официальная ссылка >>

Предыстория 2: Tar Ransomware
Ранняя версия Tarдобавляла к зашифрованным файлам расширение **.tar** или **___tar**
Распространение Tar пришлось на вторую половину сентября - октябрь-ноябрь 2016.
Сообщения на форуме BC.

Расширения того времени:
!____GLOK9200@GMAIL.COM____.tar
!____cocoslim98@gmail.com____.tar
Результаты анализов: HA+VT

Обновление от 22 сентября 2016:
Расширение: !_____ELIZABETH7@PROTONMAIL.COM____.tar
Результаты анализов: VT

Обновление от 10 ноября 2016:
Email: GEKSOGEN911@GMAIL.COM
Расширение по шаблону:
!_____GEKSOGEN911@GMAIL.COM____.c300

Обновление от 2 декабря 2016:
Email: DILINGER7900@GMAIL.COM
Расширение по шаблону:
!_____DILINGER7900@GMAIL.COM_____.GRANIT

Обновление от 16 декабря 2016:
Расширение: !__recoverynow@india.com__.v8
См. статью **V8Locker Ransomware**

Обновление от 26 декабря 2016:
Email: hamil8642@gmail.com
Расширение по шаблону:
!____hamil8642@gmail.com___.GRANIT

=== 2017 ===

Обновление от 20 марта 2017:
Расширение: !===contact by email=== tokico767@gmail.com.adamant
Email: tokico767@gmail.com.adamant
Пример темы >>
Описание этого варианта у Dr.Web >>
Результаты анализов: HA+VT

Обновление: апрель 2017:
Email: edgar4000@protonmail.com
Пример темы >>
Расширение по шаблону:
edgar4000@protonmail.com____.granit
Email: edgar4000@protonmail.com

Обновление от 5 июня 2017:
Расширение: ________DILIGATMAIL@tutanota.com________.pgp
Ссылка на топик >>

Обновление от 18 июня - 15 августа 2017:
Пост в Твиттере >>
Расширение по шаблону:
!______DILIGATMAIL7@tutanota.com______.OTR

Email: diligatmail7@tutanota.com
Результаты анализов: HA+VT

Обновление от 23 августа 2017:
Расширение по шаблону:
!_____PIFAGORMAIL@tutanota.com_____.SPG
Email: PIFAGORMAIL@tutanota.com
Примеры зашифрованных файлов:
Анкета.docx!_____PIFAGORMAIL@tutanota.com_____.SPG
Resume.docx!_____PIFAGORMAIL@tutanota.com_____.SPG

Обновление от 12 сентября 2017:
Расширение по шаблону: _____PIFAGORMAIL@tutanota.com_____.rar
Email: PIFAGORMAIL@tutanota.com

Обновление от 20 сентября 2017:
Пост в Твиттере >>
Расширение по шаблону: !_____INKASATOR@TUTAMAIL.COM____.ANTIDOT
Email: INKASATOR@TUTAMAIL.COM
Результаты анализов: VT

Обновление от 13-20 сентября 2017:
Пост в Твиттере >> + Пост в Твиттере >>
Расширение по шаблону: !-=solve a problem=-=grandums@gmail.com=-.PRIVAT66
Email: grandums@gmail.com
Результаты анализов: VT

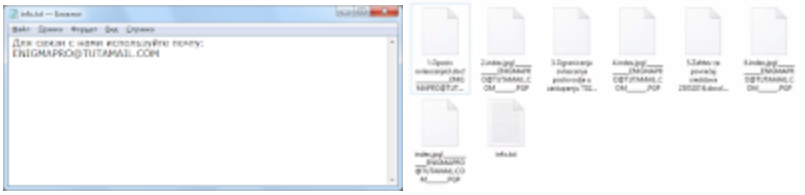
Обновление от 20 сентября 2017:
Пост в Твиттере >>
Расширение по шаблону: !==solve a problem==stritinge@gmail.com===.SENRUS17
Email: stritinge@gmail.com
Сумма выкупа: 1 BTC
Результаты анализов: VT

Обновление от 10 октября 2017:
Пост в Твиттере >>
Расширение по шаблону: !_____FIDEL4000@TUTAMAIL.COM_____.biz
Email: FIDEL4000@TUTAMAIL.COM
Результаты анализов: VT

Обновление от 17 октября 2017:
Пост в Твиттере >>
Файлы: dead rdp.exe, RarYBiHI.exe

Расширение: !_____DESKRYPT@TUTAMAIL.COM_____.rar
Email: DESKRYPT@TUTAMAIL.COM
Результаты анализов: VT

Обновление от 27 ноября 2017:
🎥 Video review
Пост в Твиттере + Tweet >>
Расширение: !_____ENIGMAPRO@TUTAMAIL.COM_____.PGP
Email: ENIGMAPRO@TUTAMAIL.COM
Записка: info.txt
Файлы: <random8>.exe
Результаты анализов: VT + HA
Скриншоты записки и файлов >>



Обновление от 25 декабря 2017:
Расширение: !_____ANCABLCITADEL@TUTAMAIL.COM_____.PGP
Email: ANCABLCITADEL@TUTAMAIL.COM
Файл: <random>.exe
Результаты анализов: VT

=== 2018 ===

Обновление от 25 января 2018:
Пост в Твиттере >>
Расширение: !==SOLUTION OF THE PROBLEM==blacknord@tutanota.com==.Black_OFFserve!
Email: blacknord@tutanota.com
Результаты анализов: VT

Обновление от 9 февраля 2018:
Пост в Твиттере >>
Расширение: !decrfile@tutanota.com.crypo
Email: decrfile@tutanota.com
Результаты анализов: VT

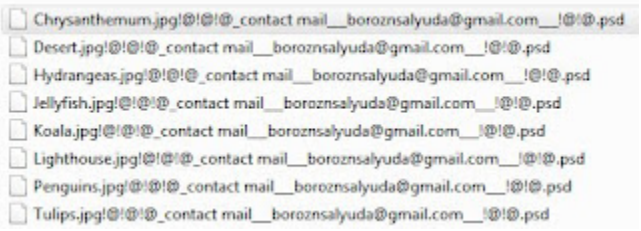
Обновление от 5 марта 2018:
Пост в Твиттере >>
Расширение с пробелами: ! ,--, Revert Access ,--, starbax@tutanota.com ,--,.BlockBax_v3.2
Email: starbax@tutanota.com
Результаты анализов: VT

Обновление от 21 мая 2018:
Пост в Твиттере >>
Расширение: !_____INKOGNITO8000@TUTAMAIL.COM_____.SPG
Email: INKOGNITO8000@TUTAMAIL.COM
Результаты анализов: VT

Обновление от 03 июня 2018:
Пост на форуме >>
Расширение: !_____INKOGNITO7000@TUTAMAIL.COM_____.SPG
Email: INKOGNITO7000@TUTAMAIL.COM

Обновление от 11 июня 2018:
Пост в Твиттере >>
Расширение: !@#$%_____PANAMA1@TUTAMAIL.com_____%$#@.mail
Email: PANAMA1@TUTAMAIL.com
Результаты анализов: VT

Обновление от 14 июня 2018:
Пост в Твиттере >>
Расширение: !@!@!@_contact mail___boroznsalyuda@gmail.com___!@!@.psd
Email: boroznsalyuda@gmail.com
Файл: WbshKnkR.exe
Результаты анализов: VT



Так выглядят зашифрованные файлы

Обновление от 14 июня 2018:

Пост в Твиттере >>

Пост в Твиттере >>

Видеообзор от CyberSecurity GrujaRS >>

Расширение: !@#$_____ISKANDER@TUTAMAIL.COM_____$#@!.RAR

Скриншот с зашифрованными файлами

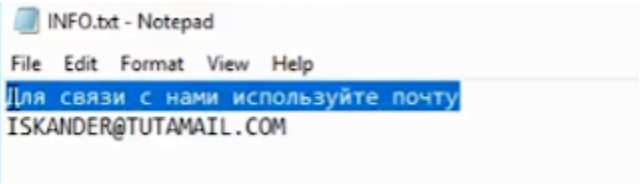
Email: ISKANDER@TUTAMAIL.COM

Записка: INFO.txt

Содержание записки:

Для связи с нами используйте почту

ISKANDER@TUTAMAIL.COM



Результаты анализов: VT

Так выглядят зашифрованные файлы

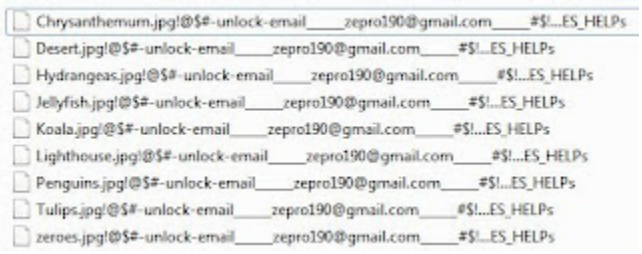
Обновление от 24 июня 2018:

Расширение: !@#$_____INKASATOR1@TUTAMAIL.COM_____$#@!.RAR

Email: INKASATOR1@TUTAMAIL.COM
Топик на форуме >>

Обновление от 25 июня 2018:
Пост в Твиттере >>
Зашифрованные файлы без расширения.
Email: patagonoa92@tutanota.com
Записка: Help.txt
➤ Содержание записки:
help mail
PATAGONIA92@TUTANOTA.COM
Результаты анализов: VT

Обновление от 9 июля 2018:
Пост в Твиттере >>
Расширение: !@$#-unlock-email_____zepro190@gmail.com_____#$!...ES_HELPs
Email: zepro190@gmail.com
Результаты анализов: VT



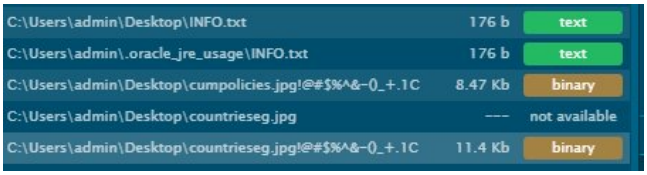
Так выглядят зашифрованные файлы

Обновление от 19 июля 2018:
Расширение: !@#$%_____PANAMA1@TUTAMAIL.com_____%$#@.mail
Email: PANAMA1@TUTAMAIL.com
Топик на форуме >>

Обновление от 21 августа 2018:
Пост в Твиттере >>
Расширение:
!@#$_(decryp in the EMail)____nautilus369alarm@gmail.com____$#@..AlfaBlock

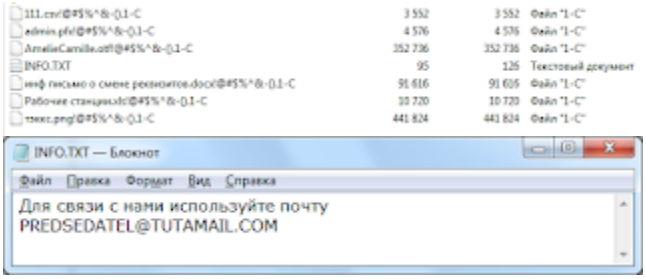

Email: nautilus369alarm@gmail.com
Результаты анализов: VT

Обновление от 10 октября 2018:
Пост в Твиттере >>
Расширение: !@#$%^&-()_+.1C
Записка: INFO.txt
Email: inkognitoman@tutamail.com, inkognitoman@firemail.cc



➤ Содержание записки:
Для связи с нами используйте почту
inkognitoman@tutamail.com
inkognitoman@firemail.cc
Результаты анализов: VT + HA + AR

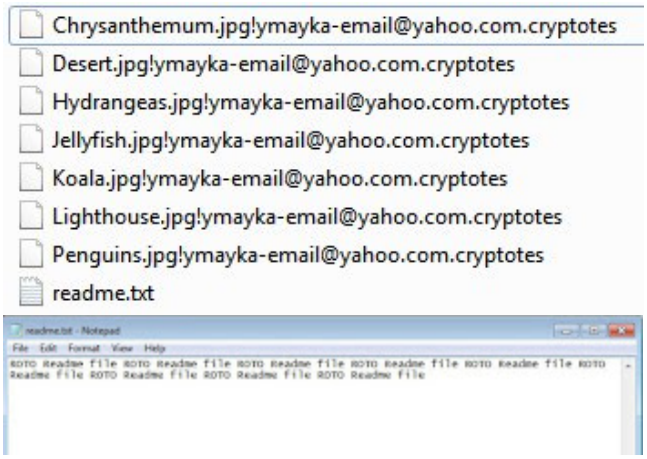
Обновление от 11 декабря 2018:
Топик на форуме >>
Расширение: !@#$%^&-().1-C



Записка: INFO.TXT
Email: PREDSEDATEL@TUTAMAIL.COM
➤ Содержание записки:
Для связи с нами используйте почту
PREDSEDATEL@TUTAMAIL.COM

=== 2019 ===

Обновление от 4 февраля 2019:
Пост в Твиттере >>
Расширение: !ymayka-email@yahoo.com.cryptotes
Записка: readme.txt



Результаты анализов: **VT**

Обновление от 1 марта 2019:
Пост в Твиттере >>
Расширение: !_!email__ prusa@goat.si __!..PAYMAN
Записка: open_payman.txt
Email: prusa@goat.si, prusa@tutanota.de
Результаты анализов: VT

➤ Содержание записки:
КАК ВОССТАНОВИТЬ ВАШИ ФАЙЛЫ ИНСТРУКЦИЯ
Внимание!!!
Мы действительно сожалеем сообщить вам, что все ваши файлы были зашифрованы нашим автоматическим программным обеспечением. Это стало возможным из-за плохой безопасности сервера.
Внимание!!!
Пожалуйста не потревожьтесь, мы смогите помочь вам восстановить ваш сервер к оригиналу государство и расшифровать все ваши файлы, быстро и безопасно!
Информация!!!
Файлы не сломаны!!!
Файлы были зашифрованы с помощью алгоритмов шифрования AES-128+RSA-2048.
Невозможно расшифровать файлы без уникального ключа дешифрования и

специального программного обеспечения. Ваш уникальный ключ расшифровки хранится на нашем сервере. Для нашей безопасности вся информация о вашем сервере и ключе для расшифровки будет автоматически удалена через 7 дней! Вы безвозвратно потеряете все свои данные!
* Обратите внимание, что все попытки восстановить файлы самостоятельно или с помощью сторонних инструментов приведет только к безвозвратной потере ваших данных!
* Обратите внимание, что восстановить файлы можно только с помощью уникального ключа расшифровки, который хранится на нашей стороне. Если вы будете пользоваться помощью третьих лиц, то добавите только посредника.
КАК ВОССТАНОВИТЬ ФАЙЛЫ???
Пожалуйста, напишите нам на e-mail (пишите на английском или используйте профессионального переводчика):айлы можно только с помощью уникального ключа расшифровки, который хранится на нашей стороне.
1 email: prusa@goat.si (Response time within 24 hours)
2 email: prusa@tutanota.de (replacement mail in the event that no reply in 24 hours by email 1)

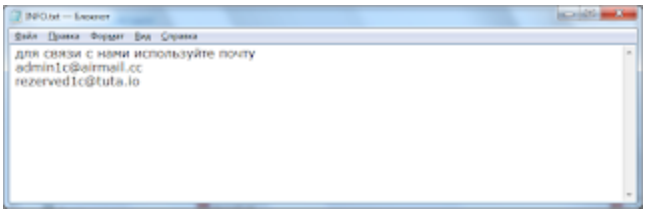
HOW TO RECOVER YOUR FILES INSTRUCTION
ATENTION!!!
We are realy sorry to inform you that ALL YOUR FILES WERE ENCRYPTED
by our automatic software. It became possible because of bad server security.
ATENTION!!!
Please don't worry, we can help you to RESTORE your server to original
state and decrypt all your files quickly and safely!
INFORMATION!!!
Files are not broken!!!
Files were encrypted with AES-128+RSA-2048 crypto algorithms.
There is no way to decrypt your files without unique decryption key and special software.
Your unique decryption key is securely stored on our server. For our safety, all information about your server and your decryption key will be automaticaly DELETED AFTER 7 DAYS!
You will irrevocably lose all your data!
* Please note that all the attempts to recover your files by yourself or using third party tools will result only in irrevocable loss of your data!
* Please note that you can recover files only with your unique decryption key, which stored on our side. If you will use the help of third parties, you will only add a middleman.
HOW TO RECOVER FILES???
Please write us to the e-mail (write on English or use professional translator):
1 email: prusa@goat.si (Response time within 24 hours)
2 email: prusa@tutanota.de (replacement mail in the event that no reply in 24 hours by email 1)
You have to send your message on each of our 3 emails due to the fact that the message

may not reach their intended recipient for a variety of reasons!
We recommed you to attach 3 encrypted files to your message. We will demonstrate that we can recover your files.
* Please note that files must not contain any valuable information and their total size must be less than 5Mb.
OUR ADVICE!!!
Please be sure that we will find common languge. We will restore all the data and give you recommedations how to configure the protection of your server.
Recovery time from 30 minutes to 10 hours, including local drives and connected devices.
We will definitely reach an agreement ;) !!!

Обновление от 13 марта 2019:
Пост в Твиттере >>
Расширение: !__help2decode@mail.com__.a800
Записка: recovery.instruction.txt
Email: help2decode@mail.com

➤ Содержание записки:
What happened to your files ?
All of your files were protected by a strong encryption with RSA-2048. More information about the encryption keys using RSA-2048 can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
What does this mean ?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.
CONTACT US BY EMAIL: help2decode@mail.com
Результаты анализов: VT + AR

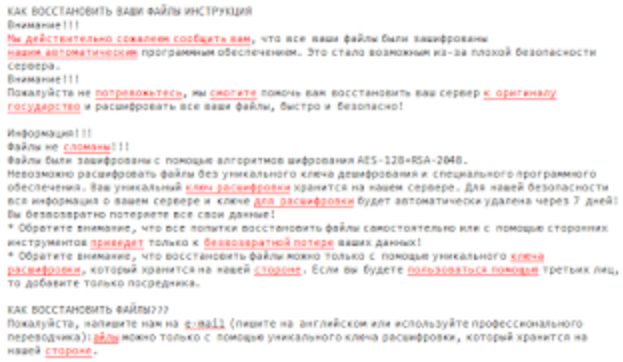
Обновление от 15 марта 2019:
Пост в Твиттере >>
Расширение: !@#$%^&-().1c
Email: admin1c@airmail.cc, rezerved1c@tuta.io
Записка: INFO.txt



➤ Содержание записки:
для связи с нами используйте почту
admin1c@airmail.cc
rezerved1c@tuta.io
Результаты анализов: **VT** + **AR** + **IA** + **HA**

Обновление от 18 марта 2019:
Пост в Твиттере >>
Расширение: **!!!! prusa@rape.lol !!!.prus**
Записка: informprus.txt
Текст записки очень корявый. Содержание, как в тексте от 1 марта 2019.

Скриншот оригинального текста записки



КАК ВОССТАНОВИТЬ ВАШИ ФАЙЛЫ ИНСТРУКЦИЯ
Внимание!!!
Мы действительно сожалеем сообщить вам, что все ваши файлы были зашифрованы
нашим автоматическим программным обеспечением. Это стало возможным из-за плохой безопасности
сервера.
Внимание!!!
Пожалуйста не потревожьтесь, мы сможите помочь вам восстановить ваш сервер к оригиналу
государство и расшифровать все ваши файлы, быстро и безопасно!

Информация!!!
Файлы не сломаны!!!
Файлы были зашифрованы с помощью алгоритмов шифрования AES-128+RSA-2048.
Невозможно расшифровать файлы без уникального ключа дешифрования и специального программного
обеспечения. Ваш уникальный ключ расшифровки хранится на нашем сервере. Для нашей безопасности
вся информация о вашем сервере и ключе для расшифровки будет автоматически удалена через 7 дней!
Вы безвозвратно потеряете все свои данные!
* Обратите внимание, что все попытки восстановить файлы самостоятельно или с помощью сторонних
инструментов приведет только к безвозвратной потере ваших данных!
* Обратите внимание, что восстановить файлы можно только с помощью уникального ключа
расшифровки, который хранится на нашей стороне. Если вы будете пользоваться помощью третьих лиц,
то добавите только посредника.

КАК ВОССТАНОВИТЬ ФАЙЛЫ???
Пожалуйста, напишите нам на e-mail (пишите на английском или используйте профессионального
переводчика)! Файлы можно только с помощью уникального ключа расшифровки, который хранится на
нашей стороне.

Показатель безграмотного текста на русском

📌 Текст на русском языке написан так безграмотно и коряво, что вызывает сомнения, что его писали знавшие русский язык. Конечно, это могли сделать и умышленно.
Email-1: prusa@rape.lol

Email-2: prusa@tutanota.de
Результаты анализов: **VT** + **AR**

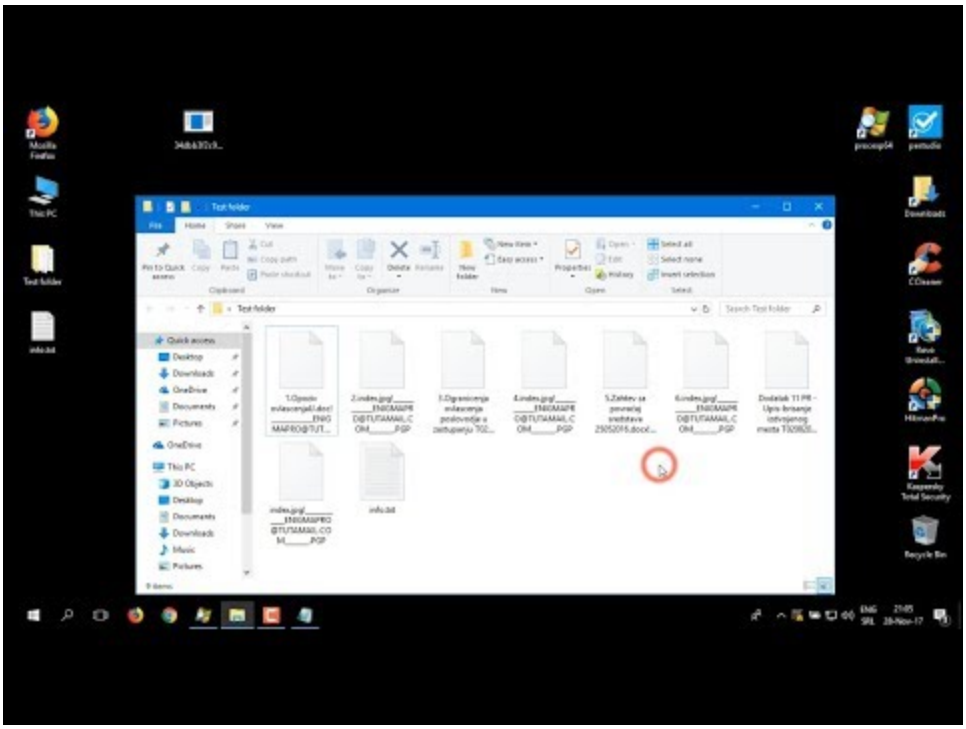
Обновление от 31 мая 2019:
Пост в Твиттере >>
Расширение: !__prontos@cumallover.me__.bak
Email: prontos@cumallover.me
Результаты анализов: VT + VMR

Обновление от 21 июня 2019:
Пост в Твиттере >>
Расширение: **!-information-..._____ingibitor366@cumallover.me_____....RT4BLOCK**
Записка: NEWS_INGiBiToR.txt
Email: ingibitor366@cumallover.me
Результаты анализов: **VT** + HA + VMR

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

Read to links:

ID Ransomware
Topic on BC
Topic on KC



https://youtu.be/mqxr1C8mf8w

Thanks:

Michael Gillespie
Andrew Ivanov (author), mike 1, thyrex, GrujaRS
*
victims in the topics of support