

RagnarLocker

 id-ransomware.blogspot.com/2020/02/ragnarlocker-ransomware.html



RagnarLocker Ransomware

RagnarLocker 2.0 Ransomware

RagnarLocker Doxware

RagnarLocker DDoS-attack-Ransomware

RagnarLocker NextGen Ransomware

(шифровальщик-вымогатель, публикатор) (первоисточник)
[Translation into English](#)

Этот крипто-вымогатель шифрует данные крупных компаний и бизнес-пользователей с помощью AES + RSA-2048, а затем требует выкуп в ~20-60 BTC, чтобы вернуть файлы. Оригинальное название: RagnarLocker или Ragnar_Locker. На файле написано: VSERV.EXE или что-то еще.

Вымогатели, распространяющие RagnarLocker, могут публиковать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов с помощью программных средств (doxware). Кроме того, вымогатели, стоящие за этим вымогательством, используют DDoS-атаки, чтобы заставить жертву связаться с ними и договориться о выкупе.

Обнаружения:

DrWeb -> Trojan.Encoder.31062, Trojan.MulDrop11.37871, Trojan.Encoder.31231, Trojan.Encoder.31566, Trojan.Encoder.32719, Trojan.Encoder.32986

BitDefender -> Gen:Heur.Ransom.Imps.1, Generic.Ransom.Ragnar.7430B5C0

Avira (no cloud) -> TR/AD.RansomHeur.gkqib

ESET-NOD32 -> A Variant Of Win32/Filecoder.OAH, A Variant Of Win32/Filecoder.RagnarLocker.A

Malwarebytes -> Ransom.Ragnar

McAfee -> Ransom-Ragnar, Ransomware-GWY!3CA359F5085B
Rising -> Ransom.Agent!8.6B7 (CLOUD)
TrendMicro -> Ransom.Win32.RAGNAR.THBAABOA,
Ransom_Ragnar.R002C0DCA20, Ransom_Ragnar.R002C0DDS20

© Генеалогия: выясняется, явное родство с кем-то не доказано.



Изображение — логотип статьи

К зашифрованным файлам добавляется расширение по шаблону:

.ragnar_XXXXXXXX
.ragnar_<ID{8}>

Под ID здесь находится хэш NetBIOS-имени компьютера.

Примеры таких расширений:

.ragnar_44027CDE
.ragnar_46d54535



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

Активность этого крипто-вымогателя пришла на конец января - начало февраля 2020 г. Дата создания: 31 января 2020. Возможно, еще был более ранний вариант из декабря 2019 года. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется по шаблону:

RGNR_XXXXXXXX.txt
RGNR_<ID>.txt

Пример записок о выкупе:

RGNR_44027CDE.txt
RGNR_46d54535.txt

*****\What if files can't be restored ?*****

To prove that we really can decrypt your data, we will decrypt one of your locked files !
Just send it to us and you will get it back FOR FREE.

The price for the decryptor is based on the network size, number of employees, annual revenue.
Please feel free to contact us for amount of BTC that should be paid.

! IF you don't know how to get bitcoins, we will give you advise how to exchange the money.

!!

! HERE IS THE SIMPLE MANUAL HOW TO GET CONTCAT WITH US !

!!

- 1) Go to the official website of TOX messenger (<https://tox.chat/download.html>)
- 2) Download and install qTOX on your PC, choose the platform (Windows, OS X, Linux, etc.)
- 3) Open messenger, click "New Profile" and create profile.
- 4) Click "Add friends" button and search our contact
7D509C5BB14B1B8CB0A3338EEA9707AD31075868CB9515B17C4C0EC6A0CCCA750CA81606900D
- 5) For identification, send to our support data from ---RAGNAR SECRET---

IMPORTANT ! IF for some reasons you CAN'T CONTACT us in qTOX, here is our reserve mailbox (hello_company@protonmail.com) send a message with a data from ---RAGNAR SECRET---
WARNING!

- Do not try to decrypt files with any third-party software (it will be damaged permanently)
- Do not reinstall your OS, this can lead to complete data loss and files cannot be decrypted. NEVER!
- Your SECRET KEY for decryption is on our server, but it will not be stored forever. DO NOT WASTE TIME !

---RAGNAR SECRET---

MmE2RjY2N2YwNUZlYm*** [всего 88 знаков]

---RAGNAR SECRET---

Перевод записки на русский язык:

Привет КОМПАНИЯ!

Если вы читаете это сообщение, значит, ваша сеть была ВЗЛОМАНА, а все ваши файлы и данные зашифрованы.

RAGNAR_LOCKER!

***** Что происходит с вашей системой? *****

Ваша сеть была взломана, все ваши файлы и резервные копии заблокированы! Таким образом, отныне НИКТО НЕ ПОМОЖЕТ ВАМ вернуть ваши файлы, КРОМЕ НАС.
Вы можете гуглить, нет никаких ШАНСОВ для расшифровки данных без нашего СЕКРЕТНОГО КЛЮЧА.
Но не волнуйся! Ваши файлы не повреждены и не потеряны, они просто изменены. Вы можете получить их обратно, как только заплатите.

Нам нужны только ДЕНЬГИ, поэтому нас не интересует, как украсть или удалить вашу информацию, это просто БИЗНЕС \$ -)

ОДНАКО вы можете повредить свои ДАННЫЕ сами, если попытаетесь расшифровать их с помощью любой другой программы, без НАШЕГО СПЕЦИАЛЬНОГО КЛЮЧА ШИФРОВАНИЯ !!! Кроме того, вся ваша ценная и конфиденциальная информация была собрана, и если вы НЕ заплатите,

мы загрузим его для всеобщего обозрения!

***** Как вернуть ваши файлы? *****

Чтобы расшифровать все ваши файлы и данные, вы должны заплатить за ключ шифрования:

BTC кошелек для оплаты: 1E6EjTqYPHLj1uovPKKRXzMrPCсрAcVuiU

Сумма к оплате (в биткойнах): 60

***** За какое время вы должны заплатить? *****

* Вам нужно связаться с нами в течение 2 дней после того, как вы заметили шифрование, чтобы получить лучшую цену.

* Цена будет увеличена на 100% (двойная цена) через 14 дней, если нет контакта.

* Ключ будет полностью удален через 21 день, если не будет установлен контакт или не будет заключена сделка.

Некоторая содержательная информация, украденная с файловых серверов, будет загружена в открытый доступ или перепродана.

***** Что, если файлы не могут быть восстановлены? *****

Чтобы доказать, что мы правда можем расшифровать ваши данные, мы расшифруем один из ваших заблокированных файлов!

Просто отправьте его нам, и вы получите его БЕСПЛАТНО.

Цена на расшифровщик зависит от размера сети, количества сотрудников, годового дохода.

Пожалуйста, не стесняйтесь обращаться к нам за суммой BTC, которая должна быть оплачена.

! Если вы не знаете, как получить биткойны, мы дадим вам совет, как обменять деньги.

!!

! ЗДЕСЬ ПРОСТОЕ РУКОВОДСТВО КАК ПОЛУЧИТЬ КОНТАКТ С НАМИ!

!!

- 1) Зайдите на официальный сайт мессенджера TOX (<https://tox.chat/download.html>)
- 2) Загрузите и установите qTOX на свой ПК, выберите платформу (Windows, OS X, Linux и т. Д.)
- 3) Откройте мессенджер, нажмите «Новый профиль» и создайте профиль.
- 4) Нажмите кнопку «Добавить друзей» и найдите наш контакт
7D509C5BB14B1B8CB0A3338EEA9707AD31075868CB9515B17C4C0EC6A0CCCA750CA81606900D
- 5) Для идентификации отправьте в нашу службу поддержки данные от --- RAGNAR SECRET ---

ВАЖНО ! Если по каким-то причинам вы не можете связаться с нами в qTOX, вот наш резервный почтовый ящик (hello_company@protonmail.com) пришлите сообщение с данными из --- RAGNAR SECRET ---

ПРЕДУПРЕЖДЕНИЕ!

-Не пытайтесь расшифровать файлы любой сторонней программой (оно повредит данные)

-Не переустанавливайте свою ОС, это может привести к полной потере данных, и файлы не

будут расшифрованы. НИКОГДА!

-Ваш СЕКРЕТНЫЙ КЛЮЧ для расшифровки находится на нашем сервере, но он не будет храниться вечно. НЕ ТРАТЬ ВРЕМЯ !

Технические детали

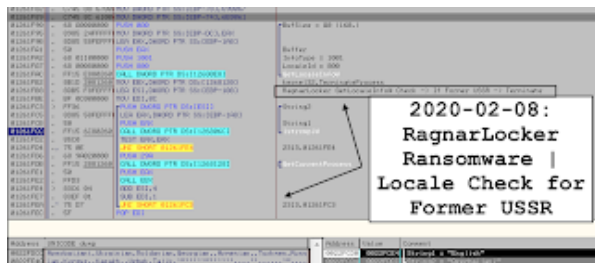
Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).



Нужно всегда использовать Актуальную антивирусную защиту!!!

Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу 3-2-1.

➤ Перед шифрованием проверяет расположение компьютера и завершает работу, если обнаруживается его принадлежность к следующим странам СНГ: Россия, Азербайджан, Армения, Беларусь, Грузия, Казахстан, Киргизстан, Молдавия, Таджикистан, Туркмения, Узбекистан, Украина.



Для этого RagnarLocker использует функцию "GetLocaleInfoW", чтобы получить язык системы пользователя (LOCALE_SYSTEM_DEFAULT) в виде строки. Затем будет проверен системный язык с помощью языков из списка исключений, а в случае совпадения вредонос прекратит работу ("TerminateProcess") с кодом ошибки 0x29A.

➤ Удаляет теньные копии файлов командами:

```
WMIC.exe shadowcopy delete (PID: 3976)
```

```
vssadmin.exe vssadmin delete shadows /all /quiet
```

➤ Перед шифрованием завершает работу следующих служб, среди которых есть программы для удаленного управления:

```
vss
```

sql
memtas
merocs
sophos
veeam
backup
pulseway
logme
logmein
connectwise
splashtop
kaseya

► Процесс шифрования:

Для каждого файла будет создан поток, который зашифрует его. После создания всех потоков RagnarLocker будет ждать бесконечное количество времени, благодаря функции "WaitForMultipleObjects". В процессе шифрования в потоках RagnarLocker проверит, имеет ли файл метку "_RAGNAR_" в конце с функцией "SetFilePointerEx", прочитав 9 байт и проверив, являются ли они этой строкой. Если файл имеет эту отметку, то он будет проигнорирован процессом шифрования.

В других случаях RagnarLocker зашифрует файл и в конце записывает зашифрованный блок ключа, используемый в блоке из 256 байтов, а одноразовый номер используется в другом блоке из 256 байтов и, наконец, добавит метку "_RAGNAR_", вместе с одним байтом как NULL для окончания строки (что составляет 9 байтов). Ключ и одноразовый номер, используемые в алгоритме Salsa20, шифруются открытым ключом RSA-2048, встроенным в шифровальщик. Это гарантирует только разработчикам RagnarLocker, имеющим закрытый ключ RSA, принадлежащий открытому ключу, используемому для дешифрования ключа и одноразового номера, приоритет в расшифровке файлов.

Перед записью этой информации RagnarLocker будет использовать функцию "LockFile", а когда процесс записи функции будет завершен, то будет использована функция "UnlockFile" для освобождения уже зашифрованного файла. Это сделано для предотвращения изменения или удаления файла в процессе шифрования.

После шифрования или, если файл уже зашифрован, RagnarLocker изменит расширение на новое, такое как ".ragnar_45EF5632".

Подробнее в статье McAfee.

Список файловых расширений, подвергающихся шифрованию:

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

kernel32.dll
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
desktop.ini
ntuser.dat
ntuser.dat.log
ntuser.ini

► В конец каждого зашифрованного файла добавляется маркер:
RAGNAR

Файлы, связанные с этим Ransomware:

VSERV.EXE
RGNR_44027CDE.txt - пример записки о выкупе
RGNR_46d54535.txt - пример записки о выкупе
malware.exe
<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: hello_company@protonmail.com
Слово "company" заменяет то, что есть в оригинальной записке.
BTC: 1E6EjTqYPHLj1uovPKKRXzMrPCcpAcVuiU
Tor-URL: hxxx://p6o7m73ujalhgvkiv.onion/**/
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:

Ⓜ **Hybrid analysis >>**
Σ **VirusTotal analysis >> VT> VT> VT> VT> VT> VT>**
🐛 **Intezer analysis >> + IA>**
⌘ **ANY.RUN analysis >>**
⌘ **VMRay analysis >>**
Ⓜ VirusBay samples >>
☐ MalShare samples >>
👁 AlienVault analysis >>
🔄 CAPE Sandbox analysis >>
🕒 JOE Sandbox analysis >>

Степень распространённости: **средний**.

Подробные сведения собираются регулярно. Присылайте образцы.

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

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



Обновление от 10 марта 2020:

Примеры расширений: **.ragnar_B1298E8D**, **.ragnar_44027CDE**

Примеры записок: **RGNR_B1298E8D.txt**, **RGNR_44027CDE.txt**

Файл: **VSD.EXE**

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



Обновление от 5 мая 2020:

Записка: **RGNR_44027CDE.txt**

Tor-URL: **hxxx://p6o7m73ujalhgkiv.onion/?p=*****

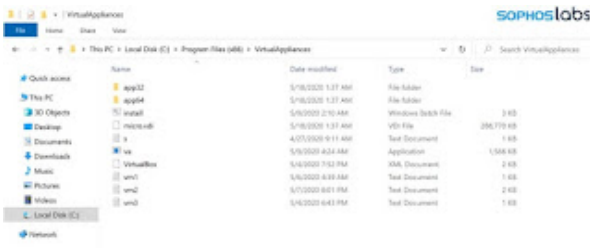
hxxx://mykgoj7uvqtgl367.onion/client/***

 PHISHING TOOL
 If you reading this message, than your network was monitored and all of your files and data has been DECRYPTED
 by SAMAN_000000 !

 [111] loaded [111]
 We NOT notify, remove, copy or move any files or you can limited them and decryption will be impossible.
 We NOT use any third party or public decryption software, it also may damage files.
 We NOT threaten or mock your system.
 There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key !
 For your convenience we will decrypt 1 of your files FOR FREE, as a proof of our capabilities.
 Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in nearest future and you will never restore your DATA.
 Contact us if you will contact us within 3 day since get penetrated - you can get a very SPECIAL PRICE.
 CONTACT US
 We have downloaded more than 1000 of data from your fileservers and if you don't contact us for payment, we will distribute it or sell to interested parties.
 Here is link to media part of your files that we have, for a proof (Don't be greedy for open the link) : http://193.50.145.201/proof/1
 We gathered the most sensitive and confidential information about your transactions, settings, contracts, clients and partners, and be assure that if you wouldn't pay,
 all files and documents could be published for everyone sites and also we would notify all your clients and partners about this leakage with direct links.
 So if you need to avoid such a fate for your reputation, better pay the amount that we asking for.

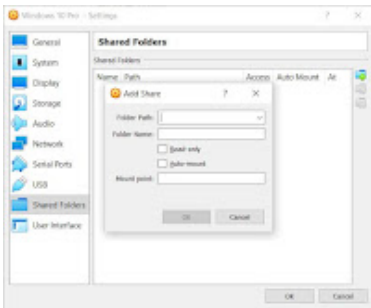
 1) Here is the (ONLY) media site to get CONTACT NOW OR via LIVE CHAT !
 http://193.50.145.201/proof/1
 2) Download and install FOR browser how this site : http://www.geturl.com
 3) For contact on live chat open our website : http://www.geturl.com/1
 4) For visit our video chats with your data, open this website : http://www.geturl.com/1
 5) If you do not contact in your area, use chat
 when you open LIVE CHAT website follow rules :
 Follow the instructions on the website.
 We the way you will find chat tab.
 Send your message there and wait for response (we are not online 24/7, so you have to wait for your turn).

 ---SAMAN_000000---
 http://www.geturl.com/1
 ---SAMAN_000000---



Эта атака начинается с создания папки инструментов, которая включает VirtualBox, виртуальный мини-диск Windows XP с именем micro.vdi и различные исполняемые файлы и сценарии для подготовки системы.

VirtualBox имеет функцию, которая позволяет операционной системе хоста обмениваться папками и дисками как сетевым ресурсом внутри виртуальной машины. Эта функция позволяет виртуальной машине подключать общий путь как сетевой диск с виртуальной машины \\VBOXSVR и получать к ней полный доступ.

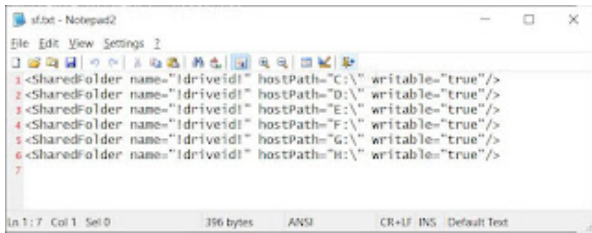


Используя пакетный файл install.bat, операторы-вымогатели сканируют локальные диски и подключенные сетевые диски на хосте и создают файл конфигурации, который автоматически разделяет их с виртуальной машиной.

```

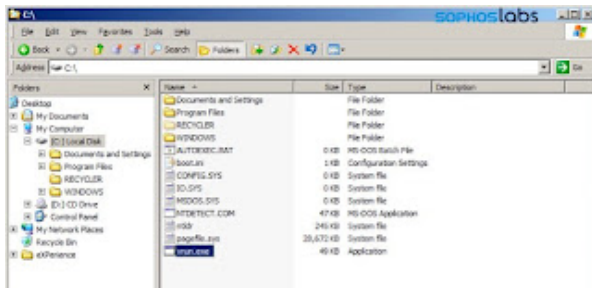
netoolvol & find "%*" > v.txt
(For /F %k In (%*) Do (
  set /a driveid=%k
  FOR %d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
    IF NOT EXIST %d%k (
      IF "%driveid%"=="%d" {
        set /a driveid=%k
      }
    )
  }
  mountvol /ifree%driveid% %k
  play -a 2 127.0.0.1
)
set d[we]d=
FOR %d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
  IF EXIST %d%k (
    set /a driveid=1
    echo "<SharedFolder name=\"%driveid%\" hostPath=\"%d%k\" writable=\"%true%\"> >>af.txt
  )
)
  
```

По завершении сценарий создает файл sf.txt, содержащий параметры конфигурации VirtualBox для автоматического совместного использования всех дисков на компьютере с виртуальной машиной.



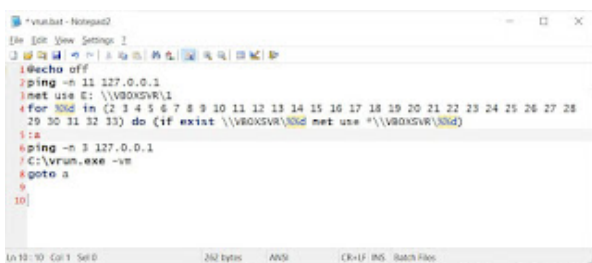
```
1 <SharedFolder name="Idriveid1" hostPath="C:\\" writable="true"/>
2 <SharedFolder name="Idriveid1" hostPath="D:\\" writable="true"/>
3 <SharedFolder name="Idriveid1" hostPath="E:\\" writable="true"/>
4 <SharedFolder name="Idriveid1" hostPath="F:\\" writable="true"/>
5 <SharedFolder name="Idriveid1" hostPath="G:\\" writable="true"/>
6 <SharedFolder name="Idriveid1" hostPath="H:\\" writable="true"/>
7
```

Затем злоумышленники запускают виртуальную машину Windows XP с созданным файлом конфигурации, используя директивы SharedFolder, созданные их пакетным файлом. При запуске все эти общие диски теперь будут доступны из виртуальной машины, а исполняемый файл RagnarLocker Ransomware будет автоматически находиться в корне диска "C".



Также включен файл vrun.bat, который находится в папке «Автозагрузка», поэтому он запускается сразу после запуска виртуальной машины.

Этот файл vrun.bat, показанный ниже, будет монтировать каждый общий диск, шифровать его и затем переходить к следующему диску, совместно используемому виртуальной машиной.



```
1 @echo off
2 ping -n 11 127.0.0.1
3 net use E: \\VBOXSVR\1
4 for %id% in (2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
5 29 30 31 32 33) do (if exist \\VBOXSVR\%id% net use *\\VBOXSVR\%id%)
6
7 ping -n 3 127.0.0.1
8 C:\vrun.exe -vm
9
10
```

Поскольку антивирусное ПО, работающее на хосте ПК жертвы, не обнаружит исполняемый файл-вымогатель или активность на виртуальной машине, оно будет успешно продолжать работу, не обнаружив, что файлы жертвы уже шифруются.

Когда шифрование будет сделано, пострадавшие найдут на своем компьютере записку с требованием выкупа, объясняющую, как была взломана их компания, и их файлы были зашифрованы.

.....SOPH0stabs
HELLO [REDACTED] !
If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
Although your security measures already been BREACHED and your files were LOCKED, we was able to make a PENETRATION
of your network AGAIN!
.....
by RAGNAR_LOCKER !
.....

Использование виртуальной машины для шифрования файлов устройства без обнаружения является инновационным подходом.

Поскольку VirtualBox и виртуальная машина Windows XP не считаются вредоносными, большинство программ обеспечения безопасности не будут обеспокоены тем, что они спокойно изменяют все данные на компьютере.

Эта атака показывает, как ПО для обеспечения безопасности с поведенческим мониторингом становится все более важным для предотвращения распространения вирусов-вымогателей. Эта атака может быть обнаружена только при обнаружении необычной массовой записи в файл.

► Если бы пострадавшие использовала функцию защиты от программ-шантажистов, реализованную в Windows 10, их ПК были бы защищены от подобной атаки, поскольку эта защита обнаружила бы записи в защищенных папках.



Официальный сайт публикации утечек:

RAGNAR LEAKS NEWS

Tor-URL: hxxx://p6o7m73ujalhgkiv.onion/

Обновление от 22-30 июля 2020:

[Пост в Твиттере >>](#)

[Пост в Твиттере >>](#)

Расширения (примеры):

.ragn@r_B8CF767A

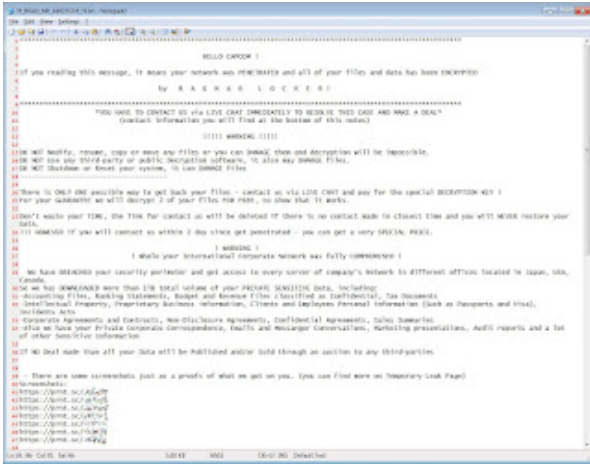
.ragn@r_44027CDE

Записки (прмиеры):

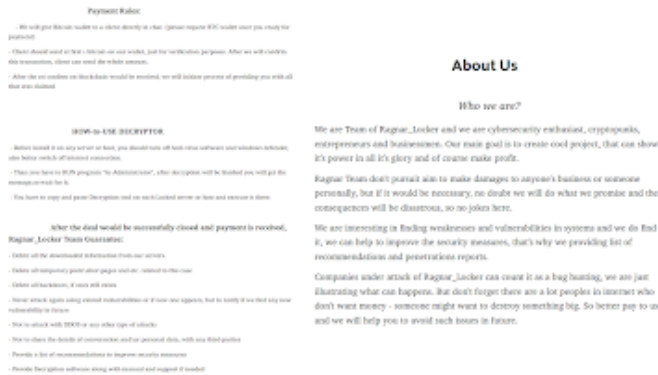
!\$R4GN4R_B8CF767A\$.txt

!\$R4GN4R_44027CDE\$.txt

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



Обновление от 6 ноября 2020: [Пост в Твиттере >>](#) **RagnarLocker о себе и своем проекте.**



"Our main goal is to create cool project, that can show it's power in all it's glory and of course make profit."

"Companies under attack of Ragnar_Locker can count it as a bug hunting"

Перевод на русский язык:

"Наша главная цель - сделать крутой проект, чтобы показать всю свою мощь и принести прибыль".

"Затронутые компании атаку Ragnar_Locker могут считать поиском ошибок"

Сообщение от 11 ноября 2020 >>

Анализы: [VT](#) + [IA](#)

=== 2021 ===

Вариант от 21 июня 2021:

[Сообщение >>](#)



Результаты анализов: [VT](#)

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



Read to links:

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

ID Ransomware (ID as RagnarLocker, RagnarLocker 2.0, RagnarLocker 2.0+)

Write-up, Topic of Support

*



Added later:

[Write-up by BleepingComputer](#) (on February 10, 2020)

[Write-up by McAfee](#) (on July 9, 2020)



Thanks:

dnwls0719, Michael Gillespie

Andrew Ivanov (author)

Vitali Kremez, Lawrence Abrams, MalwareHunterTeam
to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).