Jeno

id-ransomware.blogspot.com/2020/04/jeno-ransomware.html

Jeno Ransomware

Aliases: Jest, Valeria

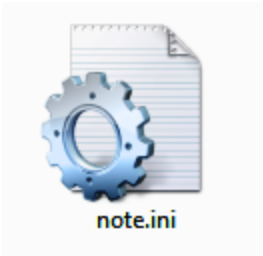
(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в 0.3 BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.31420
BitDefender -> Gen:Heur.Ransom.Imps.1
Avira (no cloud) -> TR/Dropper.Gen
ESET-NOD32 -> Win32/Filecoder.OBM
Malwarebytes -> Ransom.Valeria
Rising -> Ransom.Agent!1.C2C9 (CLOUD)
TrendMicro -> TROJ_GEN.R067C0RD220

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: FunFact ? >> Jeno (Jest, Valeria)



Изображение — логотип статьи

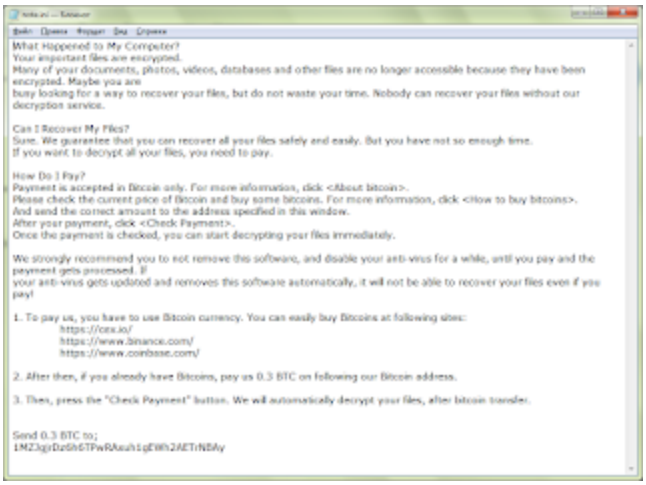
К зашифрованным файлам добавляется расширение: **.jest**

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 апреля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. На момент написания статьи и спустя 2 недели после этого нет никаких данных о распространении. Возможно, они малочисленны.

Из-за ошибки в программе или специального умысла не указано никаких контактов для связи, поэтому можно предположить, что вымогатели не собирались возвращать файлы даже после уплаты выкупа. Уплата выкупа бесполезна!

Записка с требованием выкупа называется: **note.ini**



Записка с требованием выкупа запускается с помощью команды, которая запускает Блокнот для открытия этого файла.

MachineID:	user-pc
IconFileName:	C:\Windows\System32\notepad.exe
WorkingDirectory:	C:\ProgramData\
RelativePath:	..\..\..\ProgramData\note.ini
LocalBasePath:	C:\ProgramData\note.ini
VolumeLabel:	
DriveType:	Fixed Disk

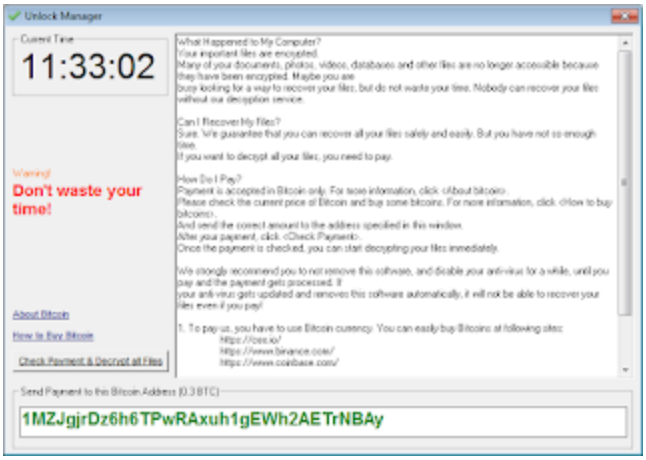
Содержание записки:
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are

busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
If you want to decrypt all your files, you need to pay.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>.
Once the payment is checked, you can start decrypting your files immediately.
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If
your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!
1. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
https://cex.io/
https://www.binance.com/
https://www.coinbase.com/
2. After then, if you already have Bitcoins, pay us 0.3 BTC on following our Bitcoin address.
3. Then, press the "Check Payment" button. We will automatically decrypt your files, after bitcoin transfer.
Send 0.3 BTC to;
1MZJgjrDz6h6TPwRAxuh1gEWh2AETrNBAy

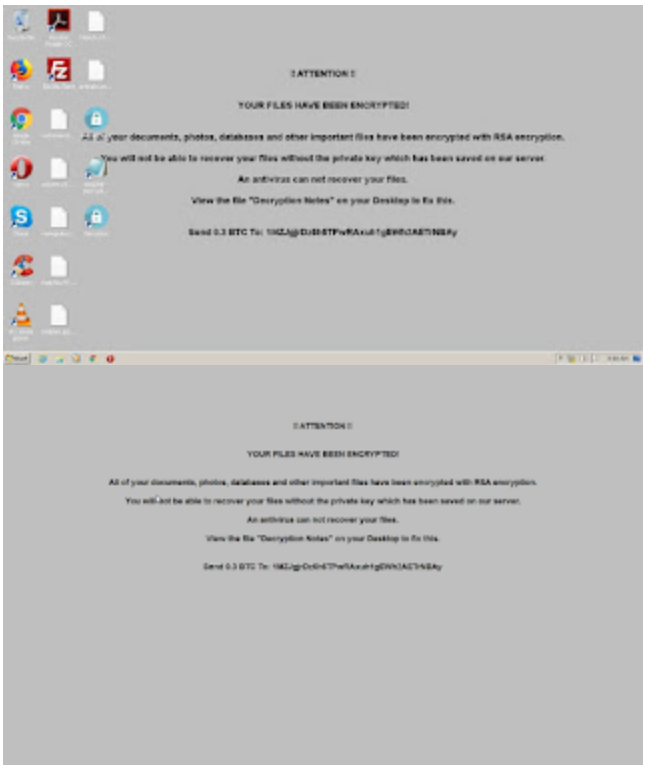
Перевод текста записки:
Что случилось с моим компьютером?
Ваши важные файлы зашифрованы.
Многие ваши документы, фото, видео, базы данных и другие файлы больше не доступны, потому что они зашифрованы. Может быть, вы ищете способ восстановить ваши файлы, но не тратьте свое время. Никто не сможет восстановить ваши файлы без нашего сервиса расшифровки.
Могу ли я восстановить мои файлы?
Конечно. Мы гарантируем, что вы можете безопасно и легко восстановить все ваши файлы. Но у вас не так много времени.
Если вы хотите расшифровать все ваши файлы, вам нужно заплатить.
Как мне оплатить?
Оплата принимается только в биткойнах. Для получения дополнительной информации нажмите <About bitcoin>.
Пожалуйста, проверьте текущую цену Биткойна и купите немного биткойнов. Для получения дополнительной информации нажмите <How to buy bitcoins>.

И отправьте правильную сумму по адресу, указанному в этом окне.
После оплаты нажмите <Check Payment>.
После того, как платеж проверен, вы можете немедленно приступить к расшифровке файлов.
Мы настоятельно рекомендуем вам не удалять эту программу и отключить антивирус на некоторое время, пока вы не оплатите и платеж не будет обработан. Если ваш антивирус обновится и автоматически удалит эту программу, он не сможет восстановить ваши файлы, даже если вы заплатите!
1. Чтобы заплатить нам, вы должны использовать валюту Биткойн. Вы можете легко купить биткойны на следующих сайтах:
https://cex.io/
https://www.binance.com/
https://www.coinbase.com/
2. После этого, если у вас уже есть биткойны, заплатите нам 0.3 BTC, на следующий наш биткойн-адрес.
3. Затем нажмите кнопку "Check Payment". Мы автоматически расшифруем ваши файлы после перевода биткойнов.
Отправьте 0.3 BTC на;
1MZJgjrDz6h6TPwRAxuh1gEWh2AETrNBAy

Другим информатором жертвы выступает экран блокировки с тем же текстом и таймером:



Еще одним информатором жертвы является изображение, заменяющее обои Рабочего стола.



Содержание текста с изображения:
!! ATTENTION !!
YOUR FILES HAVE BEEN ENCRYPTED!
All of your documents, photos, databases and other important files have been encrypted with RSA encryption.
You will not be able to recover your files without the private key which has been saved on our server.
An antivirus can not recover your files.
View the file "Decryption Notes" on your Desktop to fix this.
Send 0.3 BTC To: 1MZJgjrDz6h6TPwRAxuh1gEWh2AETrNBAy

Перевод текста на русский язык:
ВНИМАНИЕ !!
ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!
Все ваши документы, фото, базы данных и другие важные файлы зашифрованы с шифрованием RSA.
Вы не сможете восстановить ваши файлы без закрытого ключа, который был сохранен на нашем сервере.
Антивирус не может восстановить ваши файлы.
Чтобы исправить это, просмотрите файл "Decryption Notes" на Рабочем столе.
Отправь 0.3 BTC на: 1MZJgjrDz6h6TPwRAxuh1gEWh2AETrNBAy

Технические детали

На момент написания статьи и спустя 2 недели после этого нет никаких данных о

распространении. Возможно, что образец был пробной разработкой и не распространялся разработчиком с целью получения выкупа. Иначе бы был указан хотя бы один контакт для связи. Транзакции у BTC-кошелька, указанного в запсике, пустые.

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

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

Список файловых расширений, подвергающихся шифрованию:
.3fr, .ACCDB, .ACCDE, .ACCDR, .ACCDT, .ai, .arw, .asp, .aspx, .backupdb, .bak, .bas, .bay, .cdr, .cer, .cfg, .class, .conf, .config, .cpp, .cr2, .crt, .crw, , cs, .css, .db, .dbf, .den, .der, .dng, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .dxf, .dxg, .edb, .eps, .erf, .fit, .htm, .html, .indd, .java, .jpe, .jpeg, .jpg, .kdc, .log, .mail, .mdb, .mdf, .mef, .mrw, .ned, .nef, .nrp, .nrw, .ntm, .odb, .odm, .odp, .ods, .odt, .orf, .ost, .ovf, .p12, .p7b, .p7c, .pdd, .pdf, .pef, .pem, .pfx, .php, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .proj, .psd, .pst, .py, .pyc, .r3d, .rar, .raw, .rtf, , rw2, .rwl, .sldm, .sldx, .sin, .sql, .srf, .srw, .txt, .vb, .vmdk, .vmx, .wb2, .wpd, .wps, .xla, .xlam, .xlk, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .zip (132 расширения).
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
note.ini - название файла с требованием выкупа
jeno2.exe (recover.exe)
README - Decryption Note.lnk - ссылка на Рабочем столе
LNK -> C:\Windows\System32\notepad.exe
img0.jpg - изображение, заменяющее обои Рабочего стола
encryptedfiles.eco - специальный файл
<random>.exe - случайное название вредоносного файла
x64.exe
rps.exe

Расположения:
\Desktop\ ->
\User_folders\ ->

\%TEMP%\ ->
C:\ProgramData\note.ini
C:/Windows/Web/Wallpaper/Windows/img0.jpg

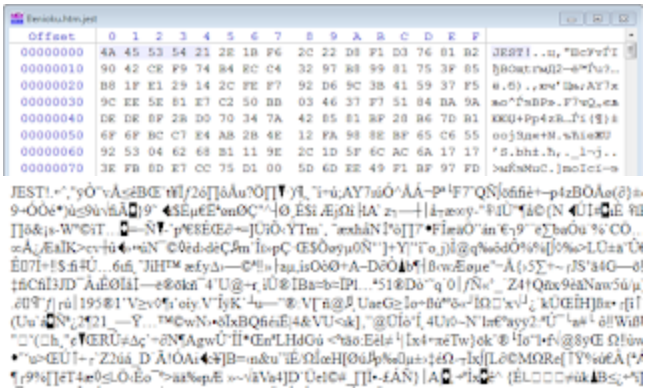
➤ Для замены обоев используется следующая команда:
C:\Windows\System32\takeown.exe /F C:\Windows\Web\Wallpaper\Windows\img0.jpg
C:\Windows\System32\icacls.exe C:\Windows\Web\Wallpaper\Windows\img0.jpg /grant Users:F

➤ Выполняет PowerShell-сценарий для удаления любых журналов.

Скриншоты свойств файла jeno2.exe:

Скриншоты кода от исследователей:

Маркер и содержимое зашифрованного файла:
JEST!



Созданные процессы:
C:\ProgramData\recover.exe
C:\Windows\System32\wbem\WMIC.exe shadowcopy delete
C:\Windows\System32\vssadmin.exe delete shadows /all /quiet

C:\Windows\System32\taskkill.exe /F /IM MSExchange*
C:\Windows\System32\taskkill.exe /F /IM Microsoft*
C:\Windows\System32\taskkill.exe /F /IM vmware*
C:\Windows\System32\taskkill.exe /F /IM Tomcat*
C:\Windows\System32\taskkill.exe /F /IM ora*
C:\Windows\System32\taskkill.exe /F /IM tns*
C:\Windows\System32\taskkill.exe /F /IM mysql*
C:\Windows\System32\taskkill.exe /F /IM sql*

Команды оболочки:
RD.exe /s C:\$Recycle.Bin /Q
wmic.exe shadowcopy delete
vssadmin.exe delete shadows /all /quiet
wbadmin.exe delete catalog -quiet
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no
taskkill.exe /F /IM MSExchange*
taskkill.exe /F /IM Microsoft*
taskkill.exe /F /IM vmware*
taskkill.exe /F /IM Tomcat*
taskkill.exe /F /IM ora*
taskkill.exe /F /IM tns*
taskkill.exe /F /IM mysql*
taskkill.exe /F /IM sql*

Завершенные процессы:
recover.exe
C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
C:\Windows\System32\wbem\WMIC.exe shadowcopy delete
C:\Windows\System32\taskkill.exe /F /IM MSExchange*
C:\Windows\System32\taskkill.exe /F /IM Microsoft*
C:\Windows\System32\taskkill.exe /F /IM vmware*
C:\Windows\System32\taskkill.exe /F /IM Tomcat*
C:\Windows\System32\taskkill.exe /F /IM ora*
C:\Windows\System32\taskkill.exe /F /IM tns*
C:\Windows\System32\taskkill.exe /F /IM mysql*
C:\Windows\System32\taskkill.exe /F /IM sql*

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: -
BTC: 1MZJgjrDz6h6TPwRAxuh1gEWh2AETrNBAy
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

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

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Ещё не было обновлений этого варианта.

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

Внимание!

```
Файлы можно расшифровать с помощью специалистов X-Force IRIS
Для информации перейдите по следующей ссылке >>
Мы никак не связаны с ними и не консультируем по этому вопросу.
```

Read to links:

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

Added later: Write-up by X-Force IRIS (on May 15, 2020)

Thanks:

Petrovic, S!Ri, Michael Gillespie
Andrew Ivanov (author)
X-Force IRIS
to the victims who sent the samples