VoidCrypt

id-ransomware.blogspot.com/2020/04/void-voidcrypt-ransomware.html

VoidCrypt Ransomware

Aliases: Void, Chaos

Variants & NextGen: Spade, Nyan, Pepe, Encrypted, Ninja, Lalaland, Peace, Hidden, Exploit, Bitch, Honor, Help, Mifr, Sophos, Hmm*, Heirloom, Snoopdogg, Backup, Extortionist, Hydra, Dpr, Musk, Revenant, Poker, Iwan, Crm, Temlown, ADA

(шифровальщик-вымогатель, RaaS) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES (режим GCM или похожий) + RSA-2048, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальные названия: Void, Chaos, но в записке не указано. На файле написано: void или что-то еще. Использует библиотеку Crypto++. Часто модифицируется.

Уплата выкупа не гарантирует расшифровку.

Обнаружения:
DrWeb -> Trojan.Siggen9.36699, Trojan.Encoder.31534, Trojan.Encoder.32640, Trojan.Encoder.33514, Trojan.Encoder.34782

ALYac -> Trojan.Ransom.Filecoder, Trojan.Ransom.Ouroboros, Trojan.Ransom.VoidCrypt
Avast/AVG ->Win32:RansomX-gen [Ransom]
Avira (no cloud) ->TR/FileCoder.zdeun
BitDefender -> Gen:Heur.Ransom.Imps.1, DeepScan:Generic.Ransom.AmnesiaE.*
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.E
Malwarebytes -> Ransom.Ouroboros, Ransom.VoidCrypt

McAfee -> Ransomware-GYP!BA454585B9F4
Microsoft -> Trojan:Win32/Ashify.J!rfn, Ransom:Win32/Ouroboros.GG!MTB
Rising -> Ransom.Gen!8.DE83 (CLOUD), Ransom.Agent!1.C4E7 (CLOUD)
Symantec -> ML.Attribute.HighConfidence, Downloader
Tencent -> Win32.Trojan.Gen.Pfsv, Win32.Trojan.Gen.Htwa
TrendMicro -> TROJ_GEN.R002H09DB20, Ransom.Win32.OUROBOROS.AE, Ransom.Win32.OUROBOROS.B

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: Ouroboros ✂ > Void, VoidCrypt > new variants > Void NextGen > Spyro

Изображение — логотип статьи

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

Фактически используется составное расширение по шаблону:
.[<email_ramsom>][ID-<ID{15}>].Void

Примеры зашифрованных файлов:
file001.tif.[USDATAdecrypt@gmail.com][ID-PDTN4Z29J67Q***].Void
file001.doc.[xtredboy@protonmail.com][ID-EJHPFWKYCNQ5***].Void
file001.jpg.[stevenxx134@gmail.com][ID-9WFL61BO03TSIC7].Void

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 пришлась на начало апреля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Пострадавшие из России, Польши и других стран.

Записка с требованием выкупа называется: **Decryption-Info.HTA**

Содержание записки о выкупе:
Your Files has Been Encrypted
Your Files Has Been Encrypted with AES + RSA Algorithm
If You Need Your Files You Have To Pay Decryption Price
You can Send Some Little Files Less Than 1MB for Test (The Test Files Should not Contain valuable Data Like Databases Large Excel Sheets or Backups
After 48 Hour Decryption Price Will be Doubled so You Better Contact us Before Times Up
Using Recovery Tools or 3rd Party Application May cause Damage To Your Files And increase price
The Steps You Should Do To Get Your Files Back:
1- Contact Email on Files And Send ID on The Files Then Do agreement on a Price
2- Send Some Files for Decryption Test (Dont Pay to Anyone Else who is Not Able to Decrypt Your Test Files!)
After Geting Test Files Pay The price in Bitcoin And Get Decryption Tool + RSA key
Your Case ID :EJHPFWKYCNQ5***
Our Email : xtredboy@protonmail.com
In Case Of No Answer : Encryptedxtredboy@protonmail.com

Перевод записки на русский язык:
Ваши файлы были зашифрованы
Ваши файлы были зашифрованы с алгоритмом AES + RSA
Если вам нужны ваши файлы, вы должны оплатить стоимость расшифровки
Вы можете отправить несколько маленьких файлов менее 1 МБ для теста (тест-файлы не должны содержать ценные данные, такие как базы данных, большие листы Excel

или резервные копии)
После 48 часов цена расшифровки удвоится, так что вам лучше связаться с нами, прежде чем время выйдет
Использование инструментов восстановления или сторонних приложений может привести к повреждению ваших файлов и повышению цены
Шаги, которые вы должны сделать, чтобы вернуть ваши файлы:
1- Контакт по email на файлы и отправить ID на файлы, а затем сделать соглашение о цене
2. Отправьте несколько файлов для тест-расшифровки (не платите никому, кто не может расшифровать ваши тест-файлы!)
После получения тест-файлов заплатите цену в биткойнах и получите инструмент дешифрования + ключ RSA
ID вашего дела: EJHPFWKYCNQ5***
Наш email: xtredboy@protonmail.com
В случае отсутствия ответа: Encryptedxtredboy@protonmail.com

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 легитимные утилиты Everything и Process Hacker 2.

➤ Согласно отчетам Intezer Analyze есть определенное родство с другими проектами программ-вымогателей, например, с Ouroboros.

Слева скриншот "генов" шифровальщика, а справа — "гены" оригинального дешифровщика. Это может говорить о том, что разработчик VoidCrypt использовал часть разработки из предыдущих проектов.

➤ Оригинальный дешифровщик без закрытого RSA ключа бесполезен.
➤ Используется RSA-2048, потому взломать ключ не получится. VoidCrypt отправляет на свой сервер публичный RSA ключ, вместе с ID и IP-адресом жертвы. Публичный ключ и приватный ключ статичны.

По данным исследователя Майкла Джиллеспи, если пострадавшие фиксировали сетевой трафик во время заражения, то ключ может быть перехвачен. Если трафик не фиксировался, то закрытый ключ RSA не получить.

➤ Скриншоты кода:

➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки, запускает команды по сети, завершает работу серверных служб, управляющих база данных, отключает файервол и прочее:

stevenxx134@gmail.com.exe
cmd.exe %WINDIR%\system32\cmd.exe /c net stop SQLWriter
net.exe net stop SQLWriter (PID: 3708)
net1.exe %WINDIR%\system32\net1 stop SQLWriter
cmd.exe %WINDIR%\system32\cmd.exe /c net stop SQLBrowser
net.exe net stop SQLBrowser
net1.exe %WINDIR%\system32\net1 stop SQLBrowser
cmd.exe %WINDIR%\system32\cmd.exe /c net stop MSSQLSERVER
net.exe net stop MSSQLSERVER
net1.exe %WINDIR%\system32\net1 stop MSSQLSERVER
cmd.exe %WINDIR%\system32\cmd.exe /c net stop MSSQL$CONTOSO1
net.exe net stop MSSQL$CONTOSO1
net1.exe %WINDIR%\system32\net1 stop MSSQL$CONTOSO1
cmd.exe %WINDIR%\system32\cmd.exe /c net stop MSDTC
net.exe net stop MSDTC
net1.exe %WINDIR%\system32\net1 stop MSDTC
cmd.exe %WINDIR%\system32\cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
cmd.exe %WINDIR%\system32\cmd.exe /c bcdedit /set {default} recoveryenabled no
cmd.exe %WINDIR%\system32\cmd.exe /c wbadmin delete catalog -quiet
cmd.exe %WINDIR%\system32\cmd.exe /c net stop SQLSERVERAGENT
net.exe net stop SQLSERVERAGENT
net1.exe %WINDIR%\system32\net1 stop SQLSERVERAGENT
cmd.exe %WINDIR%\system32\cmd.exe /c net stop MSSQLSERVER
net.exe net stop MSSQLSERVER
net1.exe %WINDIR%\system32\net1 stop MSSQLSERVER
cmd.exe %WINDIR%\system32\cmd.exe /c net stop vds
net.exe net stop vds
net1.exe %WINDIR%\system32\net1 stop vds
cmd.exe %WINDIR%\system32\cmd.exe /c netsh advfirewall set currentprofile state off
netsh.exe netsh advfirewall set currentprofile state off
cmd.exe %WINDIR%\system32\cmd.exe /c netsh firewall set opmode mode=disable
netsh.exe netsh firewall set opmode mode=disable

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

Файлы, связанные с этим Ransomware:
Decryption-Info.HTA - название файла с требованием выкупа, но в более новых вариантах это файл !INFO.HTA;
IDo.txt, но в более новых вариантах может быть файл IDk.txt;
pubkey.txt, но в более новых вариантах могут быть файлы pkey.txt, prvkey.txt.key, prvkey*.txt.key, prvkey3.txt.key
<random>.exe - случайное название вредоносного файла;
stevenxx134@gmail.com.exe - файл из примера, представленного в анализе.

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\ProgramData\IDo.txt
C:\ProgramData\pubkey.txt
D:\yo\chaos\Release\chaos.pdb

Использует сервисы определения IP-адресов:
xxxx://www.sfml-dev.org/ip-provider.php

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email-1: xtredboy@protonmail.com, Encryptedxtredboy@protonmail.com
Email-2: USDATAdecrypt@gmail.com
Email-3: stevenxx134@gmail.com
Email-4: steven77xx@mail.ru, Steven77xx@protonmail.com
URL изображения замка (VT-проверка): xxxxs://i.ibb.co/2PXVhhm/1.png

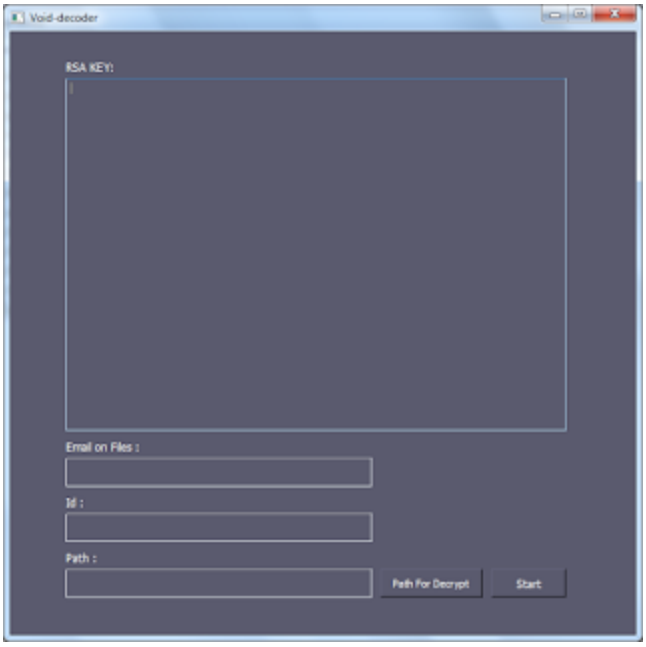
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**

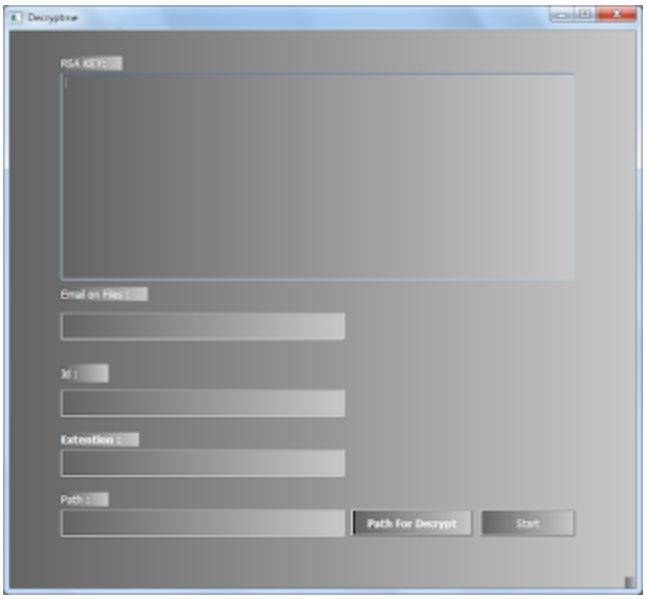
🐞 **Intezer analysis >>**
⩾ **ANY.RUN analysis >>**
🔻 **Triage analysiss >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

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

=== ОРИГИНАЛЬНЫЕ ДЕШИФРОВЩИКИ === DECRYPTORS/DECODERS ===



Вариант 2020 года (ранний)



Вариант 2021 года

Наличие оригинального дешифровщика не обеспечивает расшифровку файлов, т.к. требуется RSA-ключ, который есть только у вымогателей.

Если файлы очень нужны, рекомендуем попытаться договориться с вымогателями о снижении суммы выкупа.
Если никто не отвечает с email-адресов, указанного в записке с требованием выкупа, отправьте им еще одно письмо.
Если что-то пойдет не так, то вы можете отправить друг другу сообщение через комментарии на этой странице.

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

Zeropadypt Ransomware - с апреля 2019.
Ouroboros Ransomware (разные версии) - июнь-октябрь 2019.
Ouroboros Ransomware v6 - октябрь-декабрь 2019.
Ouroboros Ransomware v7 - с января 2020.
VoidCrypt (Void, Chaos) Ransomware - с апреля по август 2020.
Более новые варианты см. ниже в разделе обновлений.

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

Вариант от 10-11 апреля 2020:
Расширение: .Void
Пример составного расширения: .[DECRPToffice@gmail.com][ID-YOP64ULC0ZNK2BH].Void
Email: DECRPToffice@gmail.com, DECRPT@tutanota.com
Специальные файлы: IDo.txt, pubkey.txt
Файл EXE: DECRPToffice@gmail.com.exe
Результаты анализов: **VT** + **HA** + **IA** + **AR**

Вариант от 14 апреля 2020:
Пост на форуме >>
Расширение: .void
Записка: Decryption-Info.HTA
Email: SupportVoid@elude.in, SoporteVoid@tutanota.com

Вариант от 20 апреля 2020:
Расширение: .Void
Email: encryptc4@elude.in
BTC: 194Bhb2JsFo56uXtHJXcKL6Nnb2g9mreYf

Вариант 22-26 апреля 2020:
Расширения: .void
Email: DECRPToffice@gmail.com
DECRPT@tutanota.com
Hichkasam@protonmail.com
helpdiamond@protonmail.com
➤ Содержание записки:
Your Files has Been Encrypted
Your Files Has Been Encrypted with AES + RSA Algorithm
If You Need Your Files You Have To Pay Decryption Price
You can Send Some Little Files Less Than 1MB for Test (The Test Files Should not Contain valuable Data Like Databases Large Excel Sheets or Backups
After 48 Hour Decryption Price Will be Doubled so You Better Contact us Before Times Up
Using Recovery Tools or 3rd Party Application May cause Damage To Your Files And increase price
The Steps You Should Do To Get Your Files Back:
1- Contact Email on Files And Send ID on The Files Then Do agreement on a Price
2- Send Some Files for Decryption Test (Dont Pay to Anyone Else who is Not Able to Decrypt Your Test Files!)
After Geting Test Files Pay The price in Bitcoin And Get Decryption Tool + RSA key
Your Case ID :0HJ2IBSWF4*****

Our Email : DECRPToffice@gmail.com
In Case Of No Answer : DECRPT@tutanota.com

Вариант от 27 апреля 2020:
Записка: Decryption-Info.HTA
Email: unl0ckerpkx@tutanota.com

Вариант от 2 мая 2020:
Сообщение >>
Записка: Decryption-Info.HTA
Email: BrillianceBK@protonmail.com
LizardBkup@protonmail.com

Вариант от 5 мая 2020:
Пост на форуме >>
Расширение: .Void
Пример составного расширения: .[Elmershawn@aol.com][ID-YPRVMKTQ3ABOHUC].Void
Elmershawn@aol.com
Записка: Decryption-Info.HTA
Email: Elmershawn@aol.com

Вариант от 5 мая 2020:
Расширение: .Void
Пример составного расширения: .[encryptc4@elude.in][ID-3QXAC6HWP15CKJO].Void
Записка: Decryption-Info.HTA
Email: encryptc4@elude.in, encryptc4@protonmail.com

Вариант от 1-11 июня 2020:
Расширение: .Void
Пример составного расширения: .[decoderma@tutanota.com][ID-VKSQ8N24CPZTU1O].Void3аписка: Decryption-Info.HTA
Email: decoderma@tutanota.com, decoderma@protonmail.com
Специальные файлы: IDo.txt, pubkey.txt
Файл EXE: decoderma@tutanota.com.exe
Результаты анализов: **VT** + **HA** + **IA** + **AR** + **TG**

➤ Содержание записки:
Your Files has Been Encrypted
Your Files Has Been Encrypted with AES + RSA Algorithm
If You Need Your Files You Have To Pay Decryption Price
You can Send Some Little Files Less Than 1MB for Test (The Test Files Should not Contain valuable Data Like Databases Large Excel Sheets or Backups
After 48 Hour Decryption Price Will be Doubled so You Better Contact us Before Times Up
Using Recovery Tools or 3rd Party Application May cause Damage To Your Files And increase price
The Steps You Should Do To Get Your Files Back:

1- Contact Email on Files And Send ID on The Files Then Do agreement on a Price
2- Send Some Files for Decryption Test (Dont Pay to Anyone Else who is Not Able to Decrypt Your Test Files!)
After Geting Test Files Pay The price in Bitcoin And Get Decryption Tool + RSA key
Your Case ID :N0GXF7YZ31L4***
Our Email : decoderma@tutanota.com
In Case Of No Answer : decoderma@protonmail.com

Вариант 17 июня 2020:
Расширения: .Void
Email: missdecryptor@protonmail.com
VoidFiles@tutanota.com
VoidFiles@protonmail.com

Вариант 22-25 июня 2020:
Расширения: .Void
Email: Pentagon11@protonmail.com
guaranteedsupport@protonmail.com

Вариант от 7 июля 2020:
Сообщение >>
Расширение: .Void
Пример составного расширения: .[coronavirus19@tutanota.com][ID-RKF4U16NY3L5QV3].Void
Записка: Decryption-Info.HTA
Email: coronavirus19@tutanota.com, ghostmax@cock.li
Результаты анализов: **VT** + **HA** + **IA**

Вариант 7-17 июля 2020:
Расширения: .Void
Email: guaranteedsupport@protonmail.com

decrypterfile@mailfence.com
hosdecoder@aol.com

Вариант от 10 июля 2020:
Сообщение >>
Расширение: .Void
Пример составного расширения: .[decrypterfile@mailfence.com][ID-KF4U1Y3L5R6NQV3].Void
Записка: Decryption-Info.HTA
Email: decrypterfile@mailfence.com, decrypterfile@protonmail.com
Файл: decrypterfile@mailfence.com.exe
Результаты анализов: **VT** + **HA** + **IA**

Вариант 22-28 июля 2020:
Расширения: .Void
Email: hosdecoder@aol.com
sleepme134@gmail.com
colderman@mailfence.com

Вариант от 2 августа 2020:
Пост на форуме >>
Расширение: .Void
Пример составного расширения: .[encrypt4u@tutanota.com][ID-14CAHRSI*******].Void
Email: encrypt4u@tutanota.com

Вариант от 9 августа 2020:
Сообщение >>
Пост на форуме >>
Сообщение >>
Расширение: **.Spade**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Spade
Составное расширение (пример): .[encryptfile@protonmail.com][JU0W5VC7I43M9TX].Spade
Записка: Read-For-Decrypt.HTA
Email: encryptfile@protonmail.com, encryptfile@cock.li
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.32312
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.D96CE88E
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.E
Malwarebytes -> Ransom.Ouroboros
Rising -> Ransom.Agent!1.C4E7 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Filecoder.Wogk

TrendMicro -> CallTROJ_GEN.R002H0CHA20

➤ Содержание записки:
Your Files Has Been Encrypted
All Your Files , Documents , photos , Databases and other important files are encrypted
And have Extention .Spade
If You Need Your Files You Have To Pay
You can Send 1 Little File Less Than 2MB for Test (The Test Files Should not be Databases Large Excel Sheets or Backups
After 24 Hour Decryption Price Will be Doubled so You Better Contact us as soon as possible
Using Recovery Tools or 3rd Party Applications is useless you can try tough
1- Contact Email on Files And Send ID on The Files Then Do agreement on a Price
2- Send Some Files for Decryption Test (Dont Pay to Anyone Else who is Not Able to Decrypt Your Test Files!)
After Geting Test Files Pay The price in Bitcoin And Get Decryption Tool + RSA key
Your ID :JU0W5VC7I43M9TX
our Email :encryptfile@protonmail.com
In Case Of No Answer :encryptfile@cock.li

Вариант от 28 августа 2020:
Топик на форуме >>
Сообщение >>
Расширение: .Spade
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Spade
Составное расширение (пример): .[rsaencrypt@tutanota.com][UTEO6F1MLDG30QH].Spade
Записка: Read-For-Decrypt.HTA
Email: rsaencrypt@tutanota.com, rsaencrypt@protonmail.ch

Вариант от 18 сентября 2020:
Топик на форуме >>
Расширение: .Spade
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Spade
Составное расширение (пример): .[Wannadecryption@gmail.com]
[PSBW2FGV4CJ3YU1].Spade
Email: Wannadecryption@gmail.com
Файл: dwm.exe
Результаты анализов: **VT** + **IA**

Вариант от 18 сентября 2020:
Топик на форуме >>
Расширение: .Spade
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Spade
Составное расширение (пример): .[SpadeEncrypt@tutanota.com]
[2XPU94ACJRDM6IZ].Spade
Email: SpadeEncrypt@tutanota.com, SpadeEncrypt@protonmail.com

Вариант от 24 сентября:
Email: ftworksergey@gmail.com
deccoder431@protonmail.com
helpsdec@tutanota.com

Пострадавшие сообщили, что после уплаты выкупа, с этих адресов ведётся дополнительное вымогательство денег. Выдержка их переписки с вымогателями:
Пострадавший пользователь:
Мы оплатили, вы обещали скинуть код после оплаты первой части.

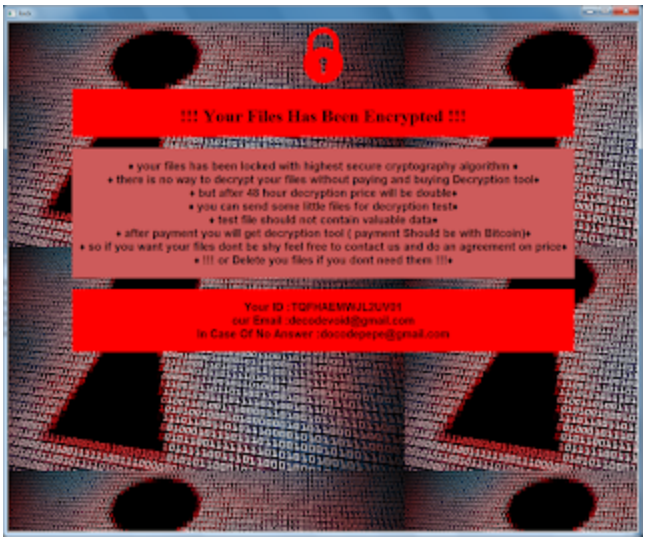
Ответ вымогателей:
Да, подтверждаем. Нет проблем, и наш админ вам доверяет.
Вы можете получить помощь от Google по выбору способа оплаты.

Снова ответ вымогателей:

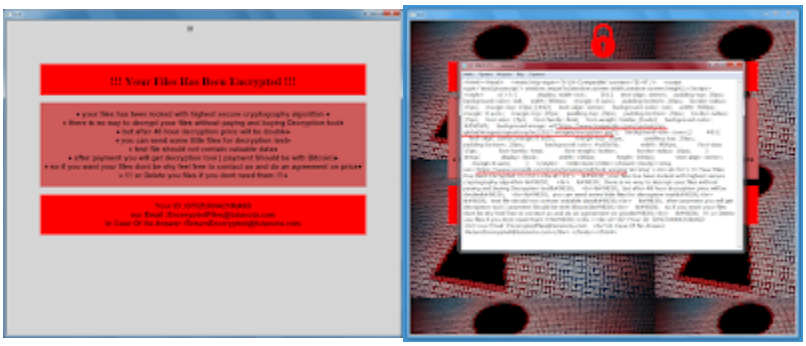
Мы не просили дополнительных денег. Один раз наш администратор вам доверял, а вы заплатили небольшую сумму. Чтобы вернуть доверие нашего администратора, вам придется заплатить остальную сумму, потому что мы вам больше не доверяем.

Вариант от 30 сентября 2020:
Сообщение >>
Топик на форуме >>
Расширение: **.nyan**
Составное расширение (пример): .[decinfo7@gmail.com][5IBQ6JU4K7NPDS0].nyan
Email: decinfo7@gmail.com

Вариант от 7 октября 2020:
Сообщение >>
Топик на форуме >>
Расширение: **.pepe**
Составное расширение (пример): .[decodevoid@gmail.com][TQFHAEMWJL2UV01].pepe
Записка: !INFO.HTA
Email: decodevoid@gmail.com, docodepepe@gmail.com
➤ Содержание записки:
!!! Your Files Has Been Encrypted !!!♦ your files has been locked with highest secure cryptography algorithm ♦
♦ there is no way to decrypt your files without paying and buying Decryption tool♦
♦ but after 48 hour decryption price will be double♦
♦ you can send some little files for decryption test♦
♦ test file should not contain valuable data♦
♦ after payment you will get decryption tool (payment Should be with Bitcoin)♦
♦ so if you want your files dont be shy feel free to contact us and do an agreement on price♦
♦ !!! or Delete you files if you dont need them !!!♦Your ID :TQFHAEMWJL2U***
our Email :decodevoid@gmail.com
In Case Of No Answer :docodepepe@gmail.com



Вариант от 8 октября 2020:
Сообщение >>
Топик на форуме >>
Идентификация на сайте ID-Ransomware >>
Расширение: **.Encrypted**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Encrypted
Составное расширение (пример): .[EnceryptedFiles@tutanota.com][GY0ZUXN421RIA6D].Encrypted
Записка: !INFO.HTA
Email: EnceryptedFiles@tutanota.com, ReturnEncerypted@tutanota.com



➤ В записке теперь используются два онлайн-изображения:

https://www.kaspersky.com/content/en-global/images/repository/isc/2017-images/encryption.jpg
https://www.iconsdb.com/icons/preview/red/lock-xxl.png
➤ Содержание записки:
!!! Your Files Has Been Encrypted !!!♦ your files has been locked with highest secure cryptography algorithm ♦
♦ there is no way to decrypt your files without paying and buying Decryption tool♦
♦ but after 48 hour decryption price will be double♦
♦ you can send some little files for decryption test♦
♦ test file should not contain valuable data♦
♦ after payment you will get decryption tool (payment Should be with Bitcoin)♦
♦ so if you want your files dont be shy feel free to contact us and do an agreement on price♦
♦ !!! or Delete you files if you dont need them !!!♦Your ID :GY0ZUXN421RIA6D
our Email :EnceryptedFiles@tutanota.com
In Case Of No Answer :ReturnEncerypted@tutanota.com

Вариант от 13 октября 2020:
Топик на форуме >>
Расширение: **.ninja**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].ninja
Составное расширение (пример): .[dr8002dr@mailfence.com][EIPDQY84TM6X1V2].ninja
Записка: !INFO.HTA
Email: dr8002dr@mailfence.com

Вариант от 14 октября 2020:
Сообщение >>
Расширение: **.lalaland**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].lalaland
Составное расширение (пример): .[recover10@tutanota.com][LIEP5WCT1JBDSVZ].lalaland
Записка: !INFO.HTA
Результаты анализов: **VT** + **IA**

Вариант от 17 октября 2020:
Сообщение >>
Расширение: **.Peace**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Peace
Составное расширение (пример): .[peace491@tuta.io][U1OR08LYSBGXF3D].Peace
Записка: !INFO.HTA
Email: peace491@tuta.io
Результаты анализов: **VT + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.32640
ALYac -> Trojan.Ransom.VoidCrypt
Avira (no cloud) -> TR/AD.OuroborosRansom.fkiqo
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.*
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.E
Malwarebytes -> Ransom.VoidCrypt

Вариант от 23 октября 2020:
Сообщение >>
Расширение: **.Hidden**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].Hidden
Составное расширение (пример): .[Wannadecryption@gmail.com]
[J61FB5P23IKT***].Hidden
Email: Wannadecryption@gmail.com
Записка: !INFO.HTA
➤ Содержание записки:
!!! Your Files Has Been Encrypted !!!
♦ your files has been locked with highest secure cryptography algorithm ♦
♦ there is no way to decrypt your files without paying and buying Decryption tool♦
♦ but after 48 hour decryption price will be double♦
♦ you can send some little files for decryption test♦
♦ test file should not contain valuable data♦
♦ after payment you will get decryption tool (payment Should be with Bitcoin)♦
♦ so if you want your files dont be shy feel free to contact us and do an agreement on price♦
♦ !!! or Delete you files if you dont need them !!!♦
Your ID :J61FB5P23IKT***
our Email :Wannadecryption@gmail.com
In Case Of No Answer :Wannadecryption@gmail.com

Вариант от 28 октября 2020:
Сообщение >>
Расширение: **.bitch**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].bitch
Составное расширение (пример): .[sleepme134@gmail.com][Z7G1J92VROQT***].bitch
Email: sleepme134@gmail.com

Вариант от 29 октября 2020:
Сообщение >>
Расширение: **.exploit**
Составное расширение (шаблон): .[email_ramsom][<ID{15}>].exploit
Составное расширение (пример): .[alix1011@mailfence.com]
[IGR4QWBC1HO2JNY].exploit
Записка: !INFO.HTA
Email: alix1011@mailfence.com
Результаты анализов: **VT + IA**
Вариант от 16 ноября 2020:
Сообщение >>
Расширение: **.honor**
Составное расширение (пример): .[honorsafe@keemail.me][XXXXXXXXXXXXXXX]*.honor
Email: honorsafe@keemail.me, honorsafe@protonmail.ch
Под * - разные номера.
Записки: !INFO.HTA, !INFO2.HTA

Вариант от 1 декабря 2020:
Сообщение >>
Расширение: **.help**
Составное расширение (пример): .[galivertones@aol.com][XXXXXXXXXXXXXXX].help
Записка: !INFO.HTA
Результаты анализов: **VT + IA**

Вариант от 3 декабря 2020:
Сообщение >>
Расширение: .Void
Email: 666lilium666@gmail.com, gregoryluton021021@gmail.com
По сообщению пострадавшего, обманывают, не предоставляют дешифровку, хотят больше денег.

Вариант от 7 декабря 2020:
Топик на форуме >>
Расширение: .Spade
Составное расширение (пример): .[lossdata@tutanota.com][1KUGSZMEY0JRP5T].Spade
Email: lossdata@tutanota.com

Вариант от 11 декабря 2020:
Топик на форуме >>
Расширение: **.mifr**
Составное расширение (пример): .[Hiden_pro@aol.com][VAI08SP61LHCXZ9].mifr
Записка: !INFO.HTA
Email: Hiden_pro@aol.com, Hiden_pro@tutanota.com

Вариант от 13 декабря 2020:
Сообщение >>
Расширение: **.Sophos**
Составное расширение (пример): .[encryptadm@criptext.com]
[VAICXP61L8S5XY5].Sophos
Записка: !INFO.HTA

Email: encryptadm@criptext.com, decryptadm@criptext.com
Файл проекта: C:\Users\Legion\source\repos\curl\Release\curl.pdb
Файл: LOL.exe
Результаты анализов: **VT** + **IA**

=== 2021 ===

Вариант от 4 января 2021:
Пост на форуме >>
Сообщение >>
Расширение: **.hmmmmmmmm**
Составное расширение (пример): .[Windows358@tuta.io]
[3MUPT6SILJF2QNK].hmmmmmmmm
Записка: !INFO.HTA
Email: Windows358@tuta.io, windows358@mailfence.com

Вариант от 6 января 2021:
Пост на форуме >>

Расширение: **.heirloom**
Записка: !INFO.HTA
Составное расширение (пример): .[rebkeilo@gmail.com][NZX1IC9GYJMSH6K].heirloom
Email: rebkeilo@gmail.com, decode.emf@tutanota.com

Вариант от 10 января 2021:
Топик на форуме >>
Расширение: **.hmmmmm**
Составное расширение (пример): .[Adm0251@tuta.io][P9TJVIU3MWAC2Y5].hmmmmm
Email: Adm0251@tuta.io, Aser51a0@protonmail.io
Записка: !INFO.HTA

Вариант января или февраля:
Расширение: **.k2**
Составное расширение (пример): .[Helpforfiles@xmpp.es][3R1EO5WNJM7A6DQ].k2
Записка: !INFO.HTA
Email: helpforfiles@xmpp.es, helpforfiles@cock.li, helpforfiles@criptext.com

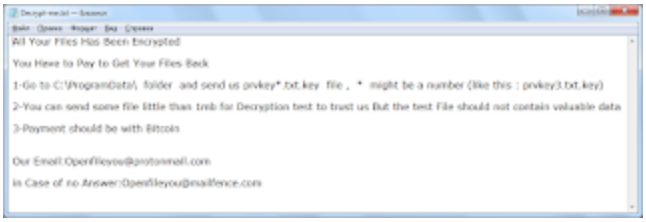
Вариант от 22 января 2021:
Расширение: .Spade
.[whiopera@tutanota.com][UZ82E3JFASPT476].Spade

Записка: !INFO.HTA
Email: whiopera@tutanota.com, whiopera@aol.com

➤ Содержание записки:
Your Files has Been Encrypted
Your Files Has Been Encrypted with AES + RSA Algorithm
If You Need Your Files You Have To Pay Decryption Price
You can Send Some Little Files Less Than 1MB for Test (The Test Files Should not Contain valuable Data Like Databases Large Excel Sheets or Backups
After 48 Hour Decryption Price Will be Doubled so You Better Contact us Before Times Up
Using Recovery Tools or 3rd Party Application May cause Damage To Your Files And increase price
The Steps You Should Do To Get Your Files Back:
1- Contact Email on Files And Send ID on The Files Then Do agreement on a Price
2- Send Some Files for Decryption Test (Dont Pay to Anyone Else who is Not Able to Decrypt Your Test Files!)
After Geting Test Files Pay The price in Bitcoin And Get Decryption Tool + RSA key
Your Case ID :XXXXXXXXXXXXXXX
Our Email : whiopera@tutanota.com
In Case Of No Answer : whiopera@aol.com

Вариант от 16 февраля 2021:
Видимо вариант аналогичный предыдущему. Это подтверждает, что он продолжает распространяться.
Расширение: .Spade
Составное расширение (пример): .[whiopera@tutanota.com][9E3NH7AGLM5T1BV].Spade
Email: whiopera@tutanota.com, whiopera@aol.com
Записка: !INFO.HTA

Вариант от 25 февраля 2021:
Сообщение >>
Сообщение >>
Расширение: **.Snoopdogg**
Составное расширение (пример): .[Openfileyou@protonmail.com][MJ-MJ3902574681].Snoopdogg
Записка: Decrypt-me.txt
Email:Openfileyou@protonmail.com, Openfileyou@mailfence.com

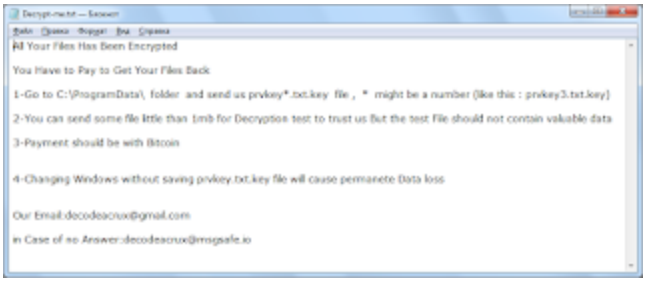


Специальные файлы: idk.txt, pkey.txt, prvkey2.txt, prvkey2.txt.key, prvkey*.txt.key, prvkey3.txt.key
Файл: Openfileyou@protonmail.com.exe (добавляется в Автозагрузку)
Результаты анализов: **VT** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33514
ALYac -> Trojan.Ransom.VoidCrypt
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.4685843F
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Ikarus -> Trojan-Ransom.Ouroboros
Malwarebytes -> Generic.Malware/Suspicious
Microsoft -> Trojan:Win32/Ymacco.AA16
Rising -> Trojan.Filecoder!8.68 (CLOUD)
Tencent -> Win32.Trojan.Filecoder.Swvd
TrendMicro -> TROJ_GEN.R002H09BP21

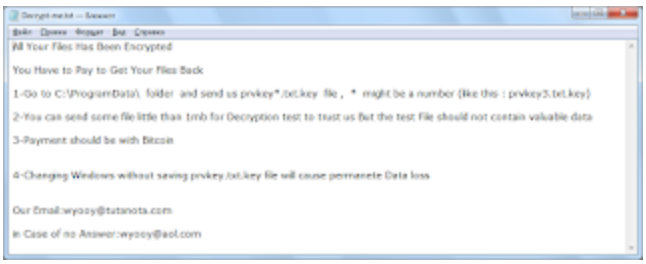
Вариант от 16 марта 2021:
Расширение: **.Backup**
Составное расширение (пример): .[unlockdata@criptext.com][MJ-XK8920513570].Backup
Записка: Decrypt-me.txt
Email: unlockdata@criptext.com, unlockdata@rape.lol

Вариант от 25 марта 2021:
Топик на форуме >>
Расширение: **.Extortionist**
Составное расширение (пример): .[openthefile@tutanota.com][MJ-WV0183796245].Extortionist
Email: openthefile@tutanota.com, openthefile@tutanota.com

Вариант от 1 апреля 2021:
Топик на форуме >>
Расширение: **.Acrux**
Составное расширение (пример): .[decodeacrux@gmail.com][MJ-ZV7502894316].Acrux
Записка: Decrypt-me.txt
Email: decodeacrux@gmail.com, decodeacrux@msgsafe.io



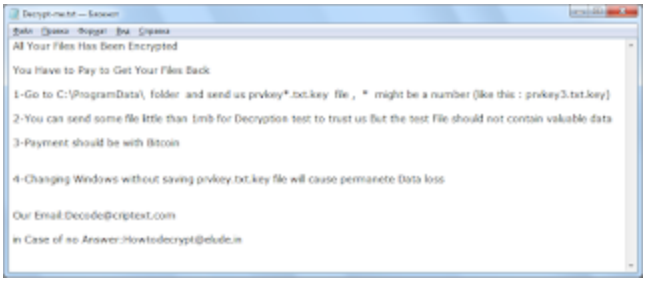
Вариант от 12 апреля 2021:
Сообщение >>
Расширение: **.hydra**
Составное расширение (пример): .[wyooy@tutanota.com][MJ-XXXXXXXXXXXX].hydra
Записка: Decrypt-me.txt



Расположения:
C:\Users\Legion\source\repos\last project\Release\curl.pdb

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\wyooy@aol.com.exe
Файл: wyooy@aol.com.exe
Результаты анализов: **VT** + **TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33834
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Kaspersky -> HEUR:Trojan.Win32.Stosek.gen
Malwarebytes -> Ransom.FileCryptor
Microsoft -> Ransom:Win32/HydraCrypt.PAA!MTB
Qihoo-360 -> Win32/Ransom.Amnesia.HwoCiSgA
Rising -> Trojan.Filecoder!8.68 (CLOUD)
Tencent -> Win32.Trojan.Stosek.Wncv
TrendMicro -> TrojanSpy.Win32.AMNESIAE.USMANDC21

Вариант от 28 апреля 2021:
Топик на форуме >>
Расширение: **.Dpr**
Составное расширение (пример): .[Decode@criptext.com][MJ-HJ1650237498].Dpr
Записка: Decrypt-me.txt
Email: Decode@criptext.com, Howtodecrypt@elude.in

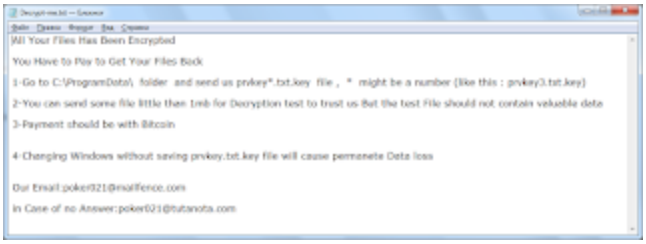


Вариант от 1 мая 2021:
Пост на форуме >>
Расширение: **.Musk**
Составное расширение (пример): .[xmasnpor@tuta.io][MJ-KI8624530179].Musk
Записка: Decrypt-me.txt

Вариант от 6 мая 2021:
Расширение: **.Revenant**
Составное расширение (пример): .[<email>][MJ-XXXXXXXXXXXX].Revenant
Записка: Decrypt-me.txt
Email: xsmaxs@tutanota.com, xsmaxs@aol.com
Файл: xsmaxs@tutanota.com.exe
Результаты анализов: **VT** + **HA** + **IA**

➤ Обнаружения:
DrWeb -> Trojan.Encoder.33910, Trojan.Encoder.34144
ALYac -> Trojan.Ransom.VoidCrypt
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.5182A77C
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Malwarebytes -> Ransom.VoidCrypt
Tencent -> Win32.Trojan.Stosek.Piam
TrendMicro -> Ransom.Win32.VOIDCRYPT.SM

Вариант от 28 мая 2021:
Сообщение >>
Расширение: **.poker**
Составное расширение (пример): .[poker021@mailfence.com][MJ-AY9754083261].poker
Записка: Decrypt-me.txt
Email: poker021@mailfence.com, poker021@tutanota.com



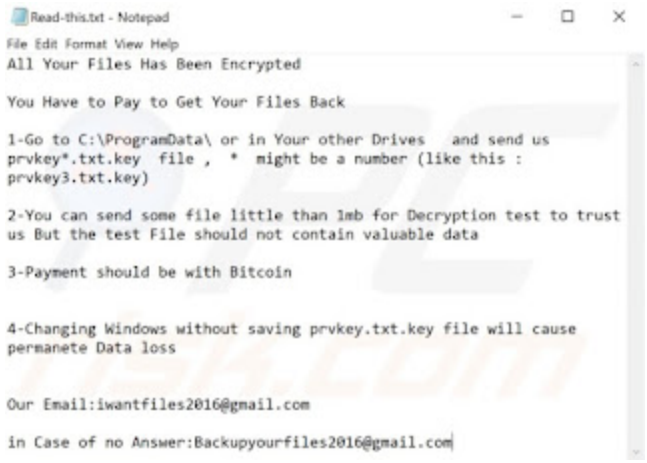
Дополнительно: CPU/GPU miner XMRig
Файл проекта: C:\Users\legion\source\repos\last project\release\curl.pdb
Результаты анализов: **VT + HA + IA + TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33514
ALYac -> Trojan.Ransom.VoidCrypt
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.99954073
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Kaspersky -> HEUR:Trojan.Win32.Stosek.gen
Microsoft -> Ransom:Win32/HydraCrypt.PAA!MTB
Rising -> Trojan.Filecoder!8.68 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Stosek.Hpc
TrendMicro -> Ransom_HydraCrypt.R002C0DDH21

Есть пропущенные варианты...

Вариант от 3 августа 2021:
Сообщение >>
Расширение (пример): .[email][ID]**.grandeur**

Вариант от 24 августа 2021:
Расширение: **.K2**
Составное расширение (пример): .[Helpforfiles@criptext.com][MJ-KC0647293158].K2
Email: Helpforfiles@criptext.com

Вариант от 1 сентября 2021:
Сообщение >>
Расширение: **.lwan**
Составное расширение (пример): .[iwantfiles2016@gmail.com][MJ-RQ2376815072].lwan
Email: iwantfiles2016@gmail.com, Backupyourfiles2016@gmail.com
Записка: Read-this.txt

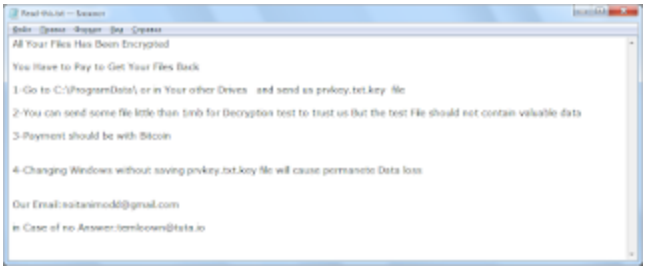


Вариант от 13 сентября 2021:
Сообщение на форуме >>
Расширение: **.lambda**
Составное расширение (пример): .[whirmx@gmail.com][MJ-LB0625153567].lambda
Записка: Read-this.txt
Email: whirmx@gmail.com, whirmx@tutanota.com

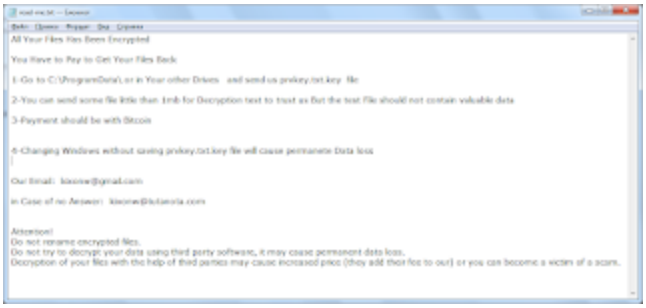
Вариант от 21 сентября 2021:
Сообщение на форуме >>
Расширение: **.crm**
Составное расширение (пример): .[poytemol@gmail.com][MJ-LB0726138549].crm
Записка: Read-this.txt
Email: poytemol@gmail.com

Вариант от 26 сентября 2021:
Расширение: **.temlown**
Составное расширение (пример): .[noitanimodd@gmail.com][MJ-WA9473106825].temlown

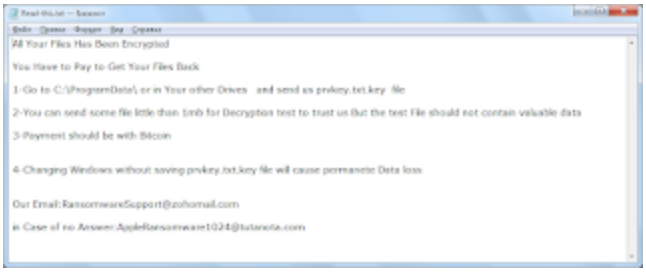
Записка: Read-this.txt
Email: noitanimodd@gmail.com, temloown@tuta.io



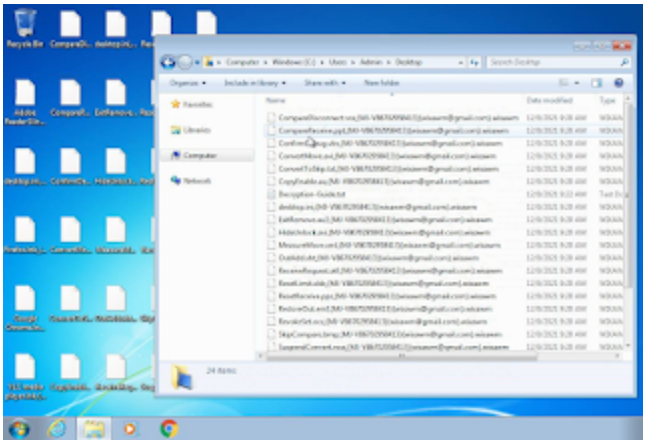
Вариант от 8 октября 2021:
Сообщение на форуме >>
Расширение: **.ADA**
Составное расширение (пример): .[kixonw@gmail.com][MJ-XXXXXXXXXXXX].ADA
Записка: read-me.txt
Email: kixonw@gmail.com, kixonw@tutanota.com
Файл ключа: prvkey.txt.key

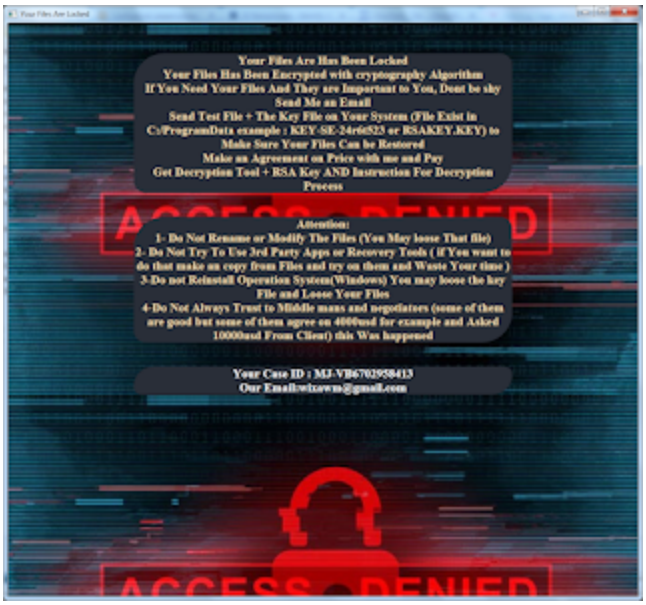


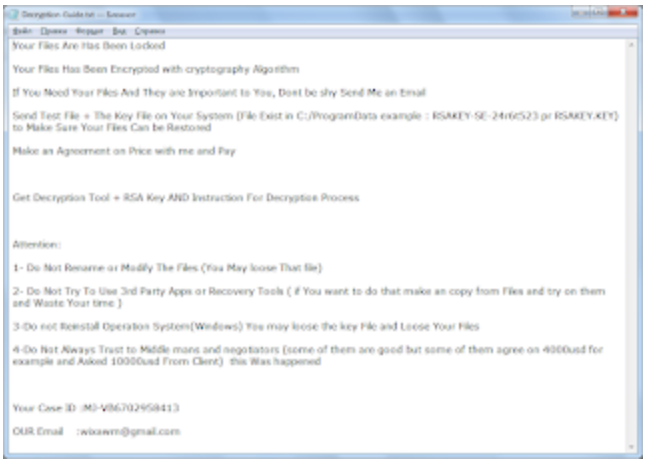
Вариант от 24 ноября 2021:
Сообщение на форуме >>
Составное расширение (пример): .[RansomwareSupport@zohomail.com][MJ-XXXXXXXXXXXX].crypyt
Записка: Read-this.txt
Email: RansomwareSupport@zohomail.com, AppleRansomware1024@tutanota.com



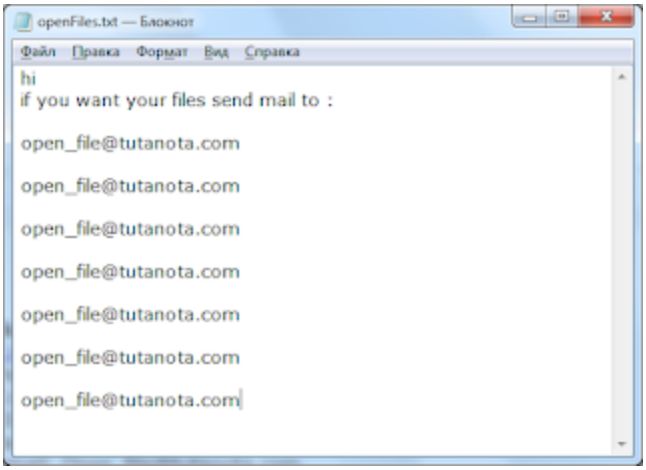
Вариант от 7 декабря 2021:
Сообщение >>
Расширение: **.wixawm**
Составное расширение (пример): ,(MJ-TE8273190645)(wixawm@gmail.com).wixawm
Записки: Decryption-Guide.txt, Decryption-Guide.HTA
Email: wixawm@gmail.com
Результаты анализов: **VT** + **TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.34724
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Microsoft -> Ransom:Win32/Taleb.PAA!MTB
Tencent -> Malware.Win32.Gencirc.11dacb8a
TrendMicro -> Ransom.Win32.Wixawm.THLAOBA



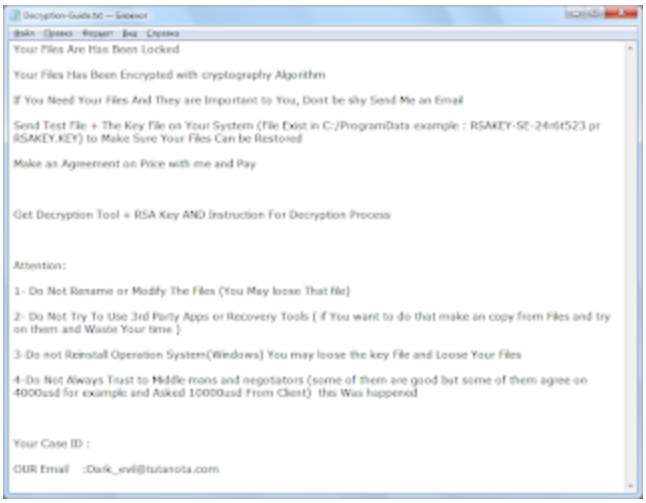




Вариант от 12 декабря 2021 или раньше:
Сообщение >>
Расширение: **.lilium**
Составное расширение (пример): .[Open_file@tutanota.com][I0QNXLFZ5CHA350].lilium
Записка: openFiles.txt
Email: Open_file@tutanota.com

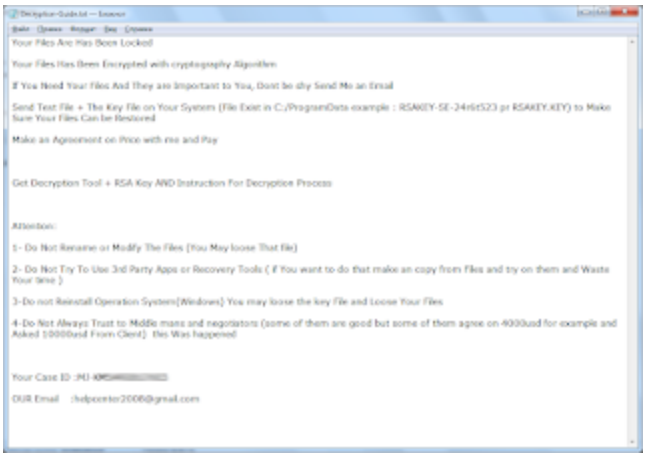


Вариант от 26 декабря 2021:
Сообщение >>
Расширение: **.killer**
Составное расширение (пример): .(MJ-UW3765438901)(Dark_evil@tutanota.com).killer
Записки: Decryption-Guide.txt, Decryption-Guide.HTA
Email: Dark_evil@tutanota.com



=== 2022 ===

Вариант от 20 января 2022 или раньше:
Сообщение >>
Расширение: .wixawm
Составное расширение (пример): ,(MJ-KM5452617602) (helpcenter2008@gmail.com).wixawm
Записки: Decryption-Guide.txt, Decryption-Guide.HTA
Email: helpcenter2008@gmail.com
Другие файлы: IDk.txt, pkey.txt, RSAKEY.key



Вариант от 7 февраля 2022:

Сообщение >>

Расширение: **.Godox**

Составное расширение (пример): .(MJ-PH7316520894)(Folperdock@gmail.com).Godox

Записки: Decryption-Guide.txt, Decryption-Guide.HTA

Email: Folperdock@gmail.com

Файл: Taleb.Ransom.exe

➤ Обнаружения:

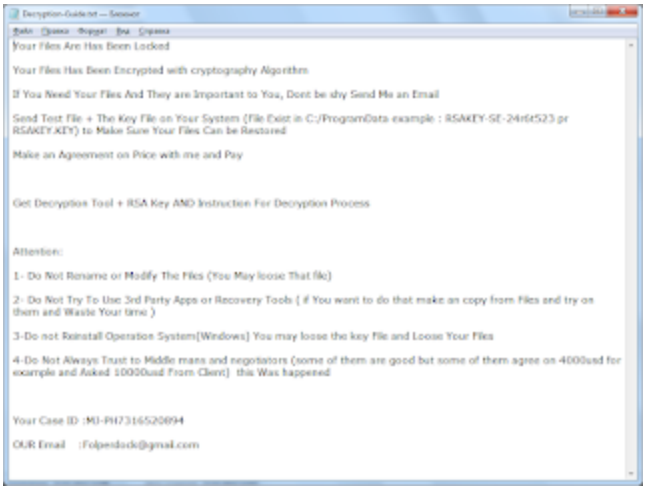
DrWeb -> Trojan.Encoder.34668

BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.0C6334A1

ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G

Microsoft -> Ransom:Win32/Taleb.PAA!MTB

TrendMicro -> Ransom_Taleb.R002C0DBN22

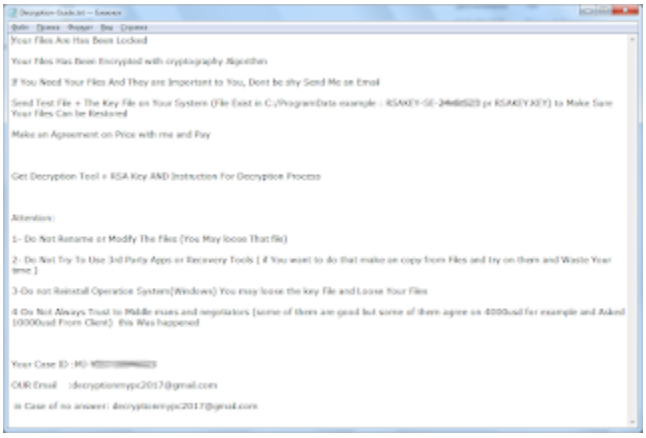


Вариант от 1 марта 2022:

Расширение: .help

Составное расширение (пример): .[marcosmelborn@aol.com][MJ-IL7853194653].help

Записки: Decryption-Guide.txt, Decryption-Guide.HTA
Email: marcosmelborn@aol.com
Файл: marcosmelborn@aol.com.exe
Вариант от 17 марта 2022:
Расширение: **.Joker**
Составное расширение (пример): .(MJ-YI5718946543)
(decryptionmypc2017@gmail.com).Joker
Записки: Decryption-Guide.txt, Decryption-Guide.HTA
Email: decryptionmypc2017@gmail.com



Вариант от 8 апреля 2022:
Сообщение >>
Расширение: **.Gilfillan**
Записки: Decryption-Guide.HTA, Decryption-Guide.txt
Файл: windows update.exe
Результаты анализов: **VT + IA**
Вариант от 8 апреля 2022:
Сообщение >>
Расширение: **.Cj**
Записки: Decryption-Guide.HTA, Decryption-Guide.txt
Email: decryptcj@gmail.com
Файл: decryptcj@gmail.com.exe (urfusjw4y.dll)
Результаты анализов: **VT**
Обнаружения:
DrWeb -> Trojan.Encoder.35172
BitDefender -> DeepScan:Generic.Ransom.AmnesiaE.40F5C717
ESET-NOD32 -> A Variant Of Win32/Filecoder.Ouroboros.G
Microsoft -> Trojan:Script/Phonzy.A!ml
TrendMicro -> TROJ_GEN.R002C0WD822

Вариант от 17 мая 2022:

Сообщение >>
Расширение: **.BTC**
Составное расширение (пример): .(MJ-GW8351096274)
(RansomwareSupport@ZohoMail.com).BTC
Записка: unlock-info.txt
Email: ransomwaresupport@zohomail.com
Результаты анализов: **VT** + **IA**

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

Thanks:

```
Andrew Ivanov (author), Michael Gillespie
dnwls0719, Kangxiaopao, Sandor, Emmanuel_ADC-Soft
Intezer Analyze
to the victims who sent the samples
```