Wacatac, DeathRansom

Wacatac Ransomware

DeathRansom Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует или делает вид, что шифрует данные пользователей с помощью XTEA, а затем требует написать на email вымогателей, чтобы узнать, как заплатить выкуп в BTC, получить программу для расшифровки и вернуть файлы. Оригинальное название: DeathRansom (указано в записке). Написан на языке C. Позже стало использоваться другое шифрование.

Обнаружения:

DrWeb -> Trojan.Encoder.30115, Trojan.Encoder.30169, Trojan.Encoder.30180, Trojan.Encoder.30188, Trojan.PWS.Siggen2.39155, Trojan.DownLoader28.53348, Trojan.Packed2.42133, Trojan.PWS.Stealer.27556, Trojan.Encoder.30493, Trojan.Encoder.32283

Antiy-AVL -> Trojan/Win32.Wacatac, Trojan/Win32.Agent

ALYac -> Trojan.Ransom.DEATHRansom

BitDefender -> Gen:Heur.Ransom.REntS.Gen.1, Gen:Variant.Ser.Midie.1067, Trojan.GenericKD.32736773, Gen:Variant.Ulise.88088, Trojan.GenericKD.42039481, Trojan.GenericKD.42040608, Trojan.GenericKDZ.59981, Gen:Variant.Ulise.87938

ESET-NOD32 -> Win32/Filecoder.DeathRansom.B, A Variant Of Win32/Kryptik.GYQM, A Variant Of Win32/Kryptik.GYPF, A Variant Of Win32/Filecoder.DeathRansom.B

Kaspersky -> Not-a-virus:HEUR:Downloader.Win32.Gen, Trojan.Win32.Chapak.*, Trojan.Win32.Agent.*, HEUR:Trojan-Downloader.Win32.Bandit.gen

Malwarebytes -> Ransom.Death, Trojan.MalPack.GS, Ransom.DeathRansom

Microsoft -> Trojan:Win32/Fuerboos.A!cl, Trojan:Win32/Tiggre!plock, Trojan:Win32/Emotet.PDS!MTB

Rising -> Backdoor.Predator!8.6DF3*, Trojan.Wacatac!8.10C01*, Trojan.Glupteba!8.AA0*, Trojan.Kryptik!1.BFC8 (CLASSIC)

Symantec -> ML.Attribute.HighConfidence, Downloader, Trojan Horse

TrendMicro -> Ransom.Win32.DEATHRANSOM.*, TROJ_FRS.0NA103KR19, TROJ_GEN.R002C0WKN19

VBA32 -> BScope.Exploit.UAC, BScope.Trojan.Wacatac, BScope.Trojan.Download, BScope.Backdoor.Predator

---

Имеется родство с DCRTR и STOP Ransomware (например: Stop-zobm, смотрите также, ссылки IA ниже в результатах анализов и обновлениях).

Изображение — логотип статьи

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

Как потом оказалось, можно было просто удалить это расширение, чтобы получить доступ к файлам. Позже стал использоваться вариант, который не добавлял расширение к зашифрованным файлам.

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 середину ноября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **read_me.txt**

Содержание записки о выкупе:

--= DEATHRANSOM =---

**********UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********

*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

All your files, documents, photos, databases and other important
files are encrypted.

You are not able to decrypt it by yourself! The only method
of recovering files is to purchase an unique private key.

Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an
email death@firemail.cc and decrypt one file for free. But this
file should be of not valuable!

Do you really want to restore your files?

Write to email

death@cumallover.me

death@firemail.cc

Your LOCK-ID: A/DWowvWRQrvUGVZL1WVxz3JX8H8BG*** [728 characters]

>>>How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/

>>> Free decryption as guarantee!

Before paying you send us up to 1 file for free decryption.

We recommeded to send pictures, text files, sheets, etc. (files no more than 1mb)

IN ORDER TO PREVENT DATA DAMAGE:

1. Do not rename encrypted files.

2. Do not try to decrypt your data using third party software, it may cause permanent data loss.

3. Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Перевод записки на русский язык:

--= DEATHRANSOM =---

**********НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ УДАЛЯЙТЕ ЭТОТ ФАЙЛ, ПОКА ВСЕ ВАШИ ДАННЫЕ НЕ БУДУТ ВОССТАНОВЛЕНЫ **********

***** НЕСОБЛЮДЕНИЕ ЭТОГО ТРЕБОВАНИЯ ПРИВЕДЕТ К ПОВРЕЖДЕНИЮ ВАШЕЙ СИСТЕМЫ В СЛУЧАЕ ОШИБОК ДЕШИФРОВКИ. *****

Все ваши файлы, документы, фотографии, базы данных и другие важные

файлы зашифрованы.
Вы не можете расшифровать это самостоятельно! Единственный метод
восстановления файлов заключается в покупке уникального закрытого ключа.
Только мы можем дать вам этот ключ, и только мы можем восстановить ваши файлы.
Чтобы убедиться, что у нас есть расшифровщик, и он работает, вы можете отправить email
на death@firemail.cc и расшифруем один файл бесплатно. Но этот файл должен быть не ценным!
Вы действительно хотите восстановить ваши файлы?
Напишите на email

death@cumallover.me

death@firemail.cc

Ваш LOCK-ID: A/DWowvWRQrvUGVZL1WVxz3JX8H8BG*** [728 символов]
>>> Как получить биткойны:
Самый простой способ купить биткойны - это сайт LocalBitcoins. Вы должны зарегистрироваться, нажать «Купить биткойны» и выбрать продавца по способу оплаты и цене.
https://localbitcoins.com/buy_bitcoins
Также вы можете найти другие места, чтобы купить биткойны и руководство для начинающих здесь:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/
>>> Бесплатная расшифровка как гарантия!
Перед оплатой вы отправьте нам 1 файл для бесплатной расшифровки.
Мы рекомендуем отправлять картинки, текстовые файлы, листы и т. д. (Файлы не более 1 Мб)
Для того, чтобы предотвратить повреждение данных:
1. Не переименовывайте зашифрованные файлы.
2. Не пытайтесь расшифровать ваши данные с помощью сторонних программ, это может привести к необратимой потере данных.
3. Расшифровка ваших файлов с помощью третьих лиц может привести к повышению цены (они добавляют свою плату к нашей) или вы можете стать жертвой мошенничества.

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**.

➤ Как показали сравнительные тесты и анализ поступающих заявлений от пострадавших, это вымогательство распространяется или сопутствует новым (на ноябрь 2019) образцам STOP Ransomware.

Например, сервис Integer Analyze **по этой ссылке** четко показывает родство файла от STOP-варианта с расширением .zobm.

➤ UAC не обходит. Требуется разрешение на запуск.

➤ Проверяет язык системы компьютера, имея в белом списке языки: русский, белорусский, казахский, украинский и татарский.

```
LPDWORD lpcbData; // [esp+18h] [ebp-10108h]
int v30; // [esp+1Ch] [ebp-10104h]
BYTE Data; // [esp+20h] [ebp-10100h]
WCHAR Buffer; // [esp+120h] [ebp-10000h]

LangID = GetUserDefaultLangID();
lpcbData = (LPDWORD)0x419;
if ( LangID == 0x419 )                  // LANG_RUSSIAN
  goto Exit_Process;
if ( LangID == 0x43F )                  // LANG_KAZAK
  goto Exit_Process;
v30 = 0x423;
if ( LangID == 0x423 )                  // LANG_BELARUSIAN
  goto Exit_Process;
lpType = (LPDWORD)0x422;
if ( LangID == 0x422 || LangID == 0x444 )   // LANG_UKRAINIAN or LANG_TATAR
  goto Exit_Process;
```

➤ Подробности шифрования

DeathRansom использует отдельную серию циклов do/while для перечисления сетевых ресурсов, логических дисков и каталогов. Он также использует QueueUserWorkItem для реализации пула потоков для своих потоков шифрования файлов.

DeathRansom создает пару из открытого и закрытого ключей RSA-2048. Используя процедуру Diffie–Hellman с эллиптической кривой (ECDH), реализованную с помощью Curve25519, она вычисляет общий секрет, используя два входных значения: 1) 32 случайных байта из вызова RtlGenRandom и 2) жестко закодированное 32-байтовое значение (открытый ключ злоумышленника). Он также создает открытый ключ Curve25519. Общий секрет - это хеш-код SHA256, который используется в качестве ключа к Salsa20 для шифрования открытого и закрытого ключей RSA.

Открытый ключ RSA используется для шифрования отдельных симметричных ключей, используемых для шифрования каждого файла. Версия зашифрованных RSA-ключей в кодировке Base64 и открытый ключ жертвы Curve25519 включены в записку о выкупе, предоставляя злоумышленникам информацию, необходимую для расшифровки файлов жертвы.

Для симметричного ключа DeathRansom вызывает RtlGenRandom для генерации 32 случайных байтов. Это 32-байтовый ключ, используемый для шифрования AES каждого файла. После шифрования файла AES-ключ шифруется открытым ключом RSA и добавляется к файлу.

DeathRansom добавляет четыре магических байта AB CD EF AB в конец зашифрованного файла и использует их как проверку, чтобы убедиться, что он не шифрует уже зашифрованный файл.

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

Шифрует все файлы, кроме тех, чьи полные пути содержат следующие строки:
programdata
$recycle.bin
program files
windows
all users
appdata
read_me.txt
autoexec.bat
desktop.ini
autorun.inf
ntuser.dat
iconcache.db
bootsect.bak
boot.ini
ntuser.dat.log
thumbs.db

Файлы, связанные с этим Ransomware:
read_me.txt
wzmjbq.exe
<random>.exe - случайное название вредоносного файла
Wacatac_2019-11-21_02-59.exe
Wacatac_2019-11-20_23-34.exe

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

Записи реестра, связанные с этим Ransomware:
HKEY_CURRENT_USER\SOFTWARE\Wacatac Access, Create
HKEY_CURRENT_USER\SOFTWARE\Wacatac\private Access, Write
HKEY_CURRENT_USER\SOFTWARE\Wacatac\public

Registry Key Name	Operations
HKEY_CURRENT_USER\SOFTWARE\Wacatac	Access, Create
HKEY_CURRENT_USER\SOFTWARE\Wacatac\private	Access, Write
HKEY_CURRENT_USER\SOFTWARE\Wacatac\public	Access, Write

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: death@firemail.cc, death@cumallover.me
BTC: -
Malware-URL:
xxxx://webparroquia.es/
xxxx://webparroquia.es/archivosadultos/Wacatac_2019-11-20_00-10.exe
xxxx://steerdemens.com/
xxxxs://iplogger.org/1zqq77
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

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

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

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

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

Обновление от 20 ноября 2019:
Топик на форуме >>
Файлы теперь реально зашифрованы.
Теперь используется комбинация алгоритма Curve25519 для схемы обмена ключами Диффи-Хеллмана с эллиптическими кривыми (ECDH), Salsa20, RSA-2048, AES-256 ECB и простого блочного алгоритма XOR для шифрования файлов.
Расширение: отсутствует. В конце зашифрованных файлов есть маркер ABEFCDAB.
Записка: read_me.txt

Email: deathransom@airmail.cc

BTC: 1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N

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

➤ Содержание записки:

??????????????????????????

??????DEATHRansom ???????

??????????????????????????

Hello dear friend,

Your files were encrypted!

You have only 12 hours to decrypt it

In case of no answer our team will delete your decryption password

Write back to our e-mail: deathransom@airmail.cc

In your message you have to write:

1. YOU LOCK-ID: bnJhtLxFGTzBdPXPCDIeH/G4PFVByYChN8ody*** [728 characters]

2. Time when you have paid 0.1 btc to this bitcoin wallet:

1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N

After payment our team will decrypt your files immediatly

Free decryption as guarantee:

1. File must be less than 1MB

2. Only .txt or .lnk files, no databases

3. Only 1 files

How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Обновление от 17 декабря 2019:

Пост в Твиттере >>

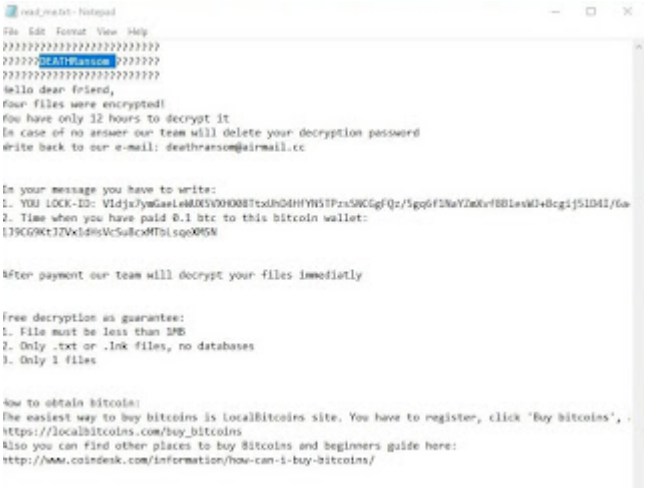
Расширение: -

Записка: read_me.txt

Email: deathransom@ainmail.cc

BTC: 1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N

Результаты анализов: **VT** + HA + VMR



Обновление от 3 января 2020:

Пост в Твиттере >>

Расширение: .wctc

Записка: read_me.txt

Email: death@cumallover.me, death@firemail.cc

Результаты анализов: **VT**

Обновление от 13 января 2020:

Пост в Твиттере >>

Расширение: **.ADHUBLLKA**

Записка: read_me.txt

Email: pr0t3eam@protonmail.com

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

➤ Обнаружения:

DrWeb -> Trojan.Encoder.30577

BitDefender -> Gen:Trojan.Heur.FU.cqW@aygBXYd

Kaspersky -> Trojan.Win32.Zudochka.dva

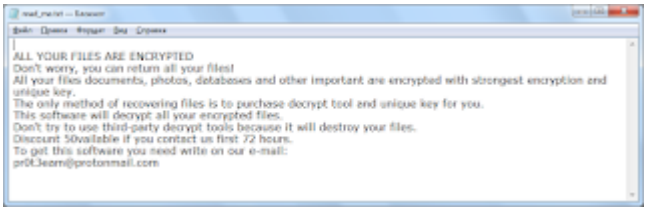
McAfee -> RDN/Ransom

Microsoft -> Trojan:Win32/Wacatac.C!ml

Symantec -> Downloader

Tencent -> Win32.Trojan.Filecoder.Akfg

VBA32 -> BScope.Exploit.UAC



➤ Содержание записки:

ALL YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!

All your files documents, photos, databases and other important are encrypted with stronges

The only method of recovering files is to purchase decrypt tool and unique key for you.

This software will decrypt all your encrypted files.

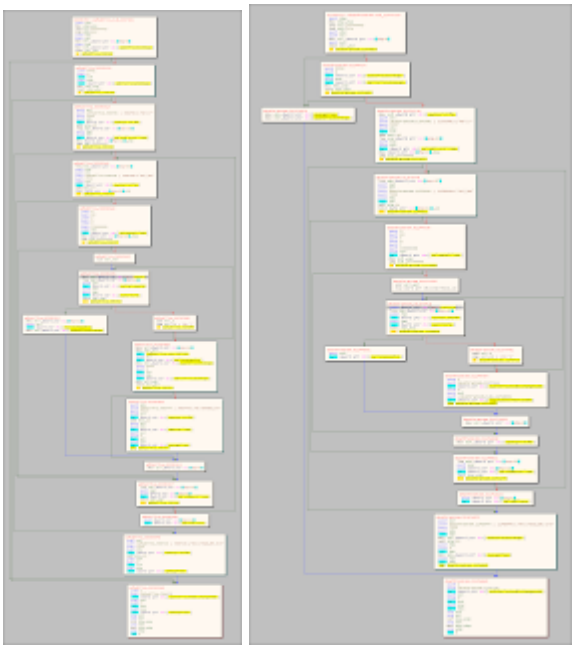
Don't try to use third-party decrypt tools because it will destroy your files.

Discount 50available if you contact us first 72 hours.

To get this software you need write on our e-mail:

pr0t3eam@protonmail.com

➤ Сравнение кода (слева код "Adhubllka", справа "DeathRansom":



Обновление от 3 августа 2020:

[Пост в Твиттере >>]

Записка: read_me.txt

Email: death@cumallover.me, death@firemail.cc

Результаты анализов: **VT** + **IA** + **TG**

➤ Содержание записки:

--= DEATHRANSOM =---

**********UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********

*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

All your files, documents, photos, databases and other important
files are encrypted.

You are not able to decrypt it by yourself! The only method
of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an
email death@firemail.cc and decrypt one file for free. But this
file should be of not valuable!

Do you really want to restore your files?

Write to email

death@cumallover.me

death@firemail.cc

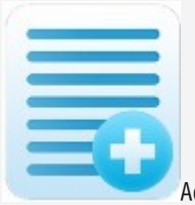
Your LOCK-ID: iB1hSZQnvagnWmsaX7Grx3a16wu/xQDfkBnqBKah6R8I6ufSG93so*** [всего 728 знаков]

>>>How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/
>>> Free decryption as guarantee!
Before paying you send us up to 1 file for free decryption.
We recommeded to send pictures, text files, sheets, etc. (files no more than 1mb)
IN ORDER TO PREVENT DATA DAMAGE:
1. Do not rename encrypted files.
2. Do not try to decrypt your data using third party software, it may cause permanent data loss.
3. Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

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

Read to links:
Tweet on Twitter + Tweet + myTweet
ID Ransomware (ID as DeathRansom)
Write-up, Topic of Support
*



Added later:
Write-up by BleepingComputer (on November 26, 2019)
Write-up by Fortinet (on January 2, 2020)
Ransomware Recap: Clop, DeathRansom, Maze Ransomware (on January 6, 2020)
Write-up by FireEye (on April 29, 2021)

Thanks:
Michael Gillespie, CyberSecurity GrujaRS, S!Ri

```
Andrew Ivanov (author)
Lawrence Abrams, FireEye
to the victims who sent the samples
```
