

MRAC

Archived: 2026-04-06 00:29:52 UTC

MRAC Ransomware

(шифровальщик-вымогатель) (первоисточник)

[Translation into English](#)

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов RSA-2048, AES-256 (режим CBC), PKCS5 (CryptGenKey для каждого файла + Rand IV для каждого файла), а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: xxx.exe.

Обнаружения:

DrWeb -> Trojan.Encoder.34811

BitDefender -> Trojan.Ransom.GenericKD.47668693

ESET-NOD32 -> Win32/Filecoder.OJQ

Kaspersky -> HEUR:Trojan.Win32.Stosek.gen

Malwarebytes -> Ransom.FileCryptor

Microsoft -> Trojan:Win32/Tiggre!rfn

Rising -> Trojan.Generic@ML.84 (RDML:h+04v***

Symantec -> ML.Attribute.HighConfidence

TrendMicro -> TROJ_GEN.R002C0PLJ21

© Генеалогия: ??? >> MRAC



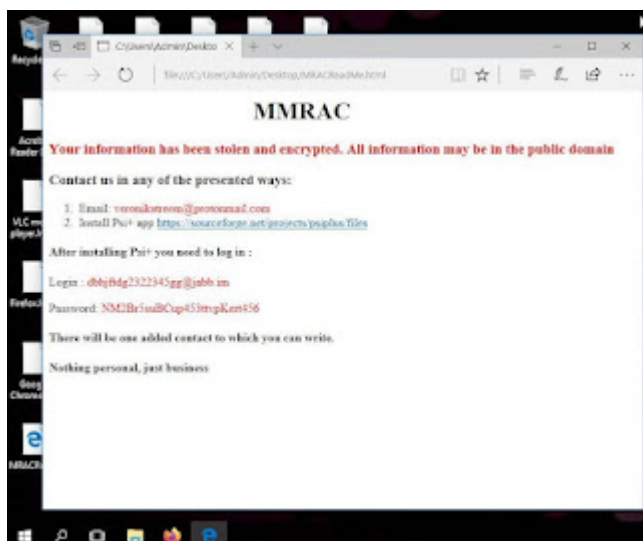
Сайт "ID Ransomware" идентифицирует это как **MRAC**.

Информация для идентификации

Активность этого крипто-вымогателя была в середине декабря 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

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

Записка с требованием выкупа называется: **MRACReadMe.html**



Содержание записки о выкупе:

MMRAC

Your information has been stolen and encrypted. All information may be in the public domain

Contact us in any of the presented ways:

Email: veronikstreem@protonmail.com

Install Psi+ app <https://sourceforge.net/projects/psiplus/files>

After installing Psi+ you need to log in :

Login : dbhjftdg2322345gg@jabb.im

Password: NM2Br5suBCup453ttvpKert456

There will be one added contact to which you can write.

Nothing personal, just business

Перевод записки на русский язык:

MMRAC

Ваша информация была украдена и зашифрована. Вся информация может быть в открытом доступе

Свяжитесь с нами любым из представленных способов:

Почта: veronikstreem@protonmail.com

Установите приложение Psi + <https://sourceforge.net/projects/psiplus/files>

После установки Psi + вам надо войти:

Логин: dbhjftdg2322345gg@jabb.im

Пароль: NM2Br5suBCup453ttvpKert456

Будет добавлен один контакт, которому вы можете писать.

Ничего личного, просто бизнес



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

Технические детали + ИОС

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](#).

- Удаляет теньевые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки.
- Завершает работу антивирусов, системные процессы и ряд служб, работа которых может помешать шифрованию файлов.

Acronis VSS Provider

Enterprise Client Service

Sophos Agent

Sophos AutoUpdate Service

Sophos Clean Service

Sophos Device Control Service

Sophos File Scanner Service

Sophos Health Service

Sophos MCS Agent

Sophos MCS Client

Sophos Message Router

Sophos SafeStore Service

Sophos Protection System Service

Sophos Web Control Service

SQLsafe

SQLsafe Filter Service

Symantec System Recovery

Veeam Backup Service Data Catalog

AcronisAgent

AcrSch2Svc

Antivirus

ARSM

BackupExecAgentAccelerator

BackupExecAgentBrowser

BackupExecDeviceMediaService

BackupExecJobEngine

BackupExecManagementService

BackupExecRPCService

BackupExecVSSProvider

bedbg

DCAgent

EPSecurityService

► После шифрования файлов самоуничтожается с помощью bat-файла.

Список типов файлов, подвергающихся шифрованию:

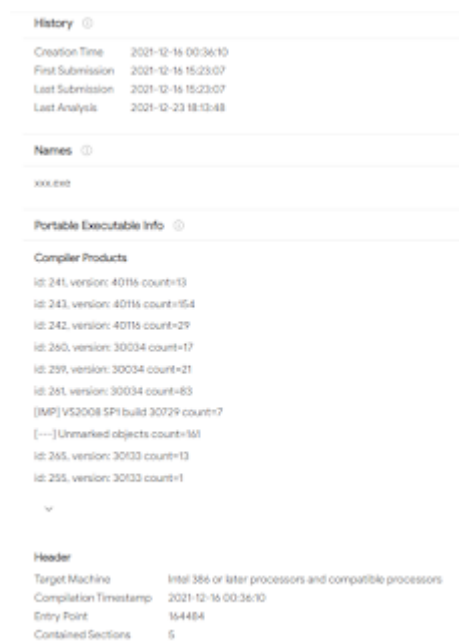
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:

MRACReadMe.html - название файла с требованием выкупа;

xxx.exe - название вредоносного файла;

MRAC.pdb - файл проекта вымогателей.



Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

C:\Users\user\Desktop\Full\App\MRAC\ENC\MRAC\Release\MRAC.pdb

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Мьютексы:

=MRAC=

| | | | | | |
|------------|---|---|---|---|---------|
| 0x00000000 | - | - | - | - | 5swI |
| 0x00100C48 | - | - | - | - | d273Q@= |
| 0x00100C80 | - | - | - | - | d5J' |
| 0x00100CE3 | - | - | - | - | >ZV3 |
| 0x00100E23 | - | - | - | - | GL |
| 0x00100E48 | - | - | - | - | edI |
| 0x00100E6B | - | - | - | - | =MRAC= |
| 0x00100E91 | - | - | - | - | X3=7# |
| 0x00100EAE | - | - | - | - | pDIT |
| 0x00100ECB | - | - | - | - | o%ko |

```

00100E50 08 00 00 00 E6 C8 79 78 49 CA BB FA 7F 8B B2 59 ...m9yxIKrsACTI>
00100E60 71 BC D5 90 3D 4D 52 41 43 3D 01 02 00 00 10 66 q3Xb^MRAC^.....f
00100E70 00 00 00 A4 00 00 49 FA 43 8D DD 15 9A 17 DD D9 ...e...IwCTM...m
00100E80 DC 17 A5 79 0F A3 AA D0 CF 95 58 3F 3D 22 3F 23 b.Gy.JcPH^X7="7#
00100E90 AE 8D D9 1F FD 13 E7 CD 6F 8F 86 26 31 DE 4F CE @*R..o.nHoU41300
00100EA0 F9 D4 2E 0A EB DD AC 04 D2 70 44 29 37 F6 98 94 mF..m^..TpD)7u"u
00100EB0 F9 2F 71 88 9D 8B D8 82 EF 68 57 CC FE 12 A7 02 m/q^S4M, nK8M0..S.
00100EC0 95 B0 2E BA DC BF 6E 25 3A 6F B3 D5 6D 5B AB AB *".ejan^:niKMOEe
00100ED0 70 61 E6 CD 99 F4 9B F1 27 88 50 3A 31 7B DE 5B pami^"b>^6P:lID[
00100EE0 0C 2C 36 8D 54 1F 48 31 46 8D 63 5E 6C 5E D9 6F .,6eP.HIF"e^l^Ho
00100EF0 87 16 8A 3A 30 44 C1 74 7F 53 49 18 42 31 54 7D !..:00mIGT.BITe.
00100F00 EF 83 3F B9 EA F6 52 5B 5F 7C EE 1A 29 6D E9 52 nF^9msh[.o.)m8R
00100F10 61 7F 7D 82 03 C7 12 FB 2A EE C2 35 63 59 08 82 a[),.S..u^o85cy.,J
00100F20 C1 E1 E6 63 08 01 8C 8D CD DD D1 8C BF 76 92 51 B0xk..B^HDCMiv^Q
00100F30 6F 0A F9 84 57 AE 11 33 8B 4F 5F B2 3D AD EC 8F o..L.MB..3no_l^=m
00100F40 BA CC 58 71 0A 80 F0 B2 90 FF BE 52 42 19 84 EC eBQq.TpI7m8B...m
00100F50 0C E8 04 6C 0C E6 93 D5 96 E6 87 5C 80 90 FB 11 .n..L..X"m^V3M.
00100F60 36 F0 AE 12 A1 90 43 3C 6B 87 6C 52 25 75 4F 6F 6pB.P7cCk-lRku0o
00100F70 C5 3F 6C C3 1B B7 E71T..

```

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: veronikstreem@protonmail.com

BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: [VT](#), [НА](#), [IA](#), [TG](#), AR, VMR, JSB

MD5: b99ce03482978a861c883bb772be3b25

SHA-1: 84ecf8f8b0de2dbb3df4b99766a84143e49eaa00

SHA-256: 768c09ad691d4af27f50934df5879166c08c0b18abf2c1a1c8561e8589a07c91

Vhash: 035056655d155560d3z22z68!z

Imphash: 000dffe70534733b98630577afdf90d9

Степень распространённости: низкая.
Информация дополняется. 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 ===



Read to links:

[Message](#) + [Message](#) + [myMessage](#)

Write-up, Topic of Support

*



Thanks:

Finch, Jiří Vinopal

Andrew Ivanov (article author)

to the victims who sent the samples

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

Source: <https://id-ransomware.blogspot.com/2021/12/mrac-ransomware.html>