MRAC

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

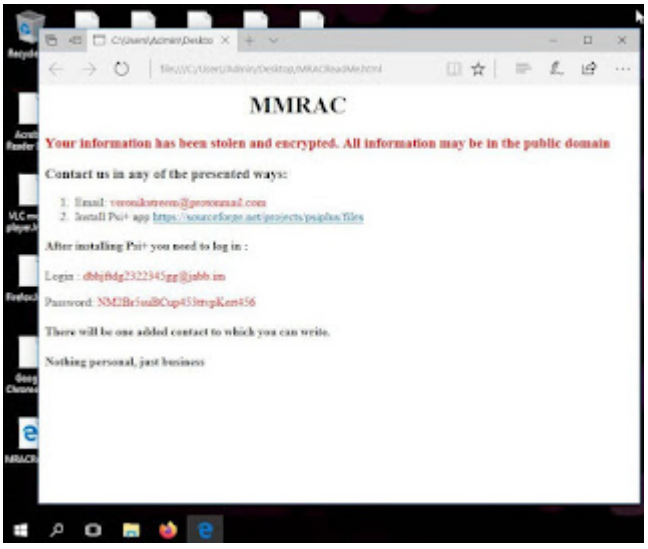
IDR IDENTIFIED

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 + IOC

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**.

➤ Удаляет теневые 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

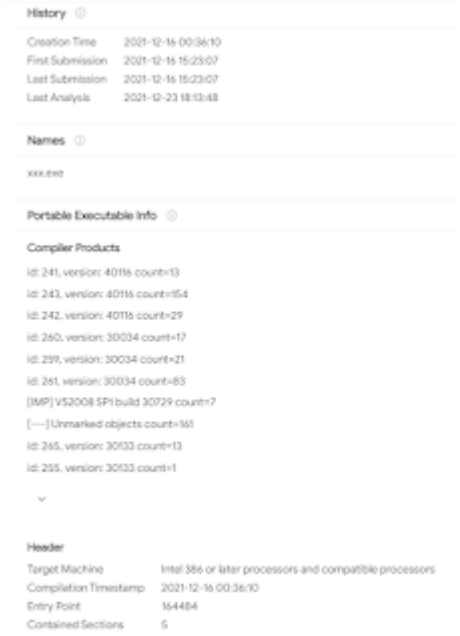
EPSecurityService

➤ После шифрования файлов самоудаляется 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.



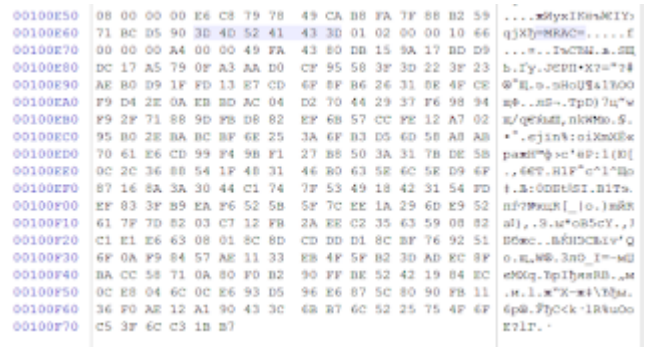
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

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

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

Мьютексы:

=MRAC=



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**, **HA**, **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
