Egregor

id-ransomware.blogspot.com/2020/09/egregor-ransomware.html

Egregor Ransomware

Egregor Doxware

(шифровальщик-вымогатель, RaaS, публикатор) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью AES+RSA, а затем требует связаться в течение 3 дней для уплаты выкупа в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Хакеры-вымогатели: Twisted Spider Extortion Group. Среди вымогателей есть граждане Украины, по другим данным это международная хакерская группа.

Вымогатели, распространяющие **Egregor**, угрожают опубликовать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов. На момент публикации статьи еще не было известно о публикациях украденных данных, вымогатели только угрожали, что данные будут опубликованы в СМИ. Позже появилась информация, что операторы Maze перешли на Egregor.

Обнаружения:
DrWeb -> Trojan.Siggen10.31058
BitDefender -> Gen:Variant.Zusy.313821
ESET-NOD32 -> A Variant Of Win32/Kryptik.HEDE
Malwarebytes -> ***
Rising -> Trojan.Generic@ML.88 (RDML:5pA***
Symantec -> Trojan.Gen.2

Tencent -> Win32.Trojan.Johnnie.Pdmk
TrendMicro -> TROJ_GEN.R002H09IO20, TROJ_FRS.0NA103IQ20

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: Maze > Sekhmet > Egregor

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.<random>**

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 сентября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **RECOVER-FILES.txt**

Содержание записки о выкупе:

```
[redacted base64]
---EGREGOR---
```

| What happened? |

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

| What does it mean? |

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

| How it can be avoided? |

In order to avoid this,
To avoid this issue you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing AGREEMENT.

| What if I do not contact you in 3 days? |

If you do not contact us in the next 3 DAYS we will begin DATA publication.

| I can handle it by myself |

It is your RIGHT, but in this case all your data will be published for public USAGE.

| I do not fear your threats! |

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.

| You have convinced me! |

Then you need to CONTACT US, there is few ways to DO that.
I. Recommended (the most secure method)
  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR browser
  c) Open our website with LIVE CHAT in the TOR browser:
http://egregor[redacted].onion/[redacted]
  d) Follow the instructions on this page.
II. If the first method is not suitable for you
  a) Open our website with LIVE CHAT: https://[redacted].top/[redacted]

b) Follow the instructions on this page.
Our LIVE SUPPORT is ready to ASSIST YOU on this website.

| What will I get in case of agreement |

You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing your network perimeter.
And the FULL CONFIDENTIALITY ABOUT INCIDENT.

Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
[redacted base64]
---EGREGOR---

Перевод записки на русский язык:
╭

| Что произошло? |

Ваша сеть АТАКОВАНА, ваши компьютеры и серверы БЛОКИРОВАНЫ,
Ваши личные данные ЗАГРУЖЕНЫ.

| Что это значит? |

Это значит, что скоро СМИ, ваши партнеры и клиенты УЗНАЮТ о вашей ПРОБЛЕМЕ.

| Как этого избежать? |

Чтобы этого избежать,
Чтобы избежать этой проблемы, вы должны СВЯЗАТЬСЯ С НАМИ не позднее 3 ДНЕЙ и заключить СОГЛАШЕНИЕ о восстановлении данных и устранении нарушений.

| Что делать, если я не свяжусь с вами в течение 3 дней? |

Если вы не свяжетесь с нами в следующие 3 ДНЕЙ, мы начнем публикацию ДАННЫХ.

| Я справлюсь сам |

Это ваше ПРАВО, но в этом случае все ваши данные будут опубликованы для публичного использования.

| Я не боюсь ваших угроз! |

Это не угроза, а алгоритм наших действий.
Если у вас есть сотни миллионов НЕНУЖНЫХ долларов, вам нечего бояться.
Это ТОЧНАЯ СУММА денег, которую вы потратите на восстановление и выплаты из-за ПУБЛИКАЦИИ.

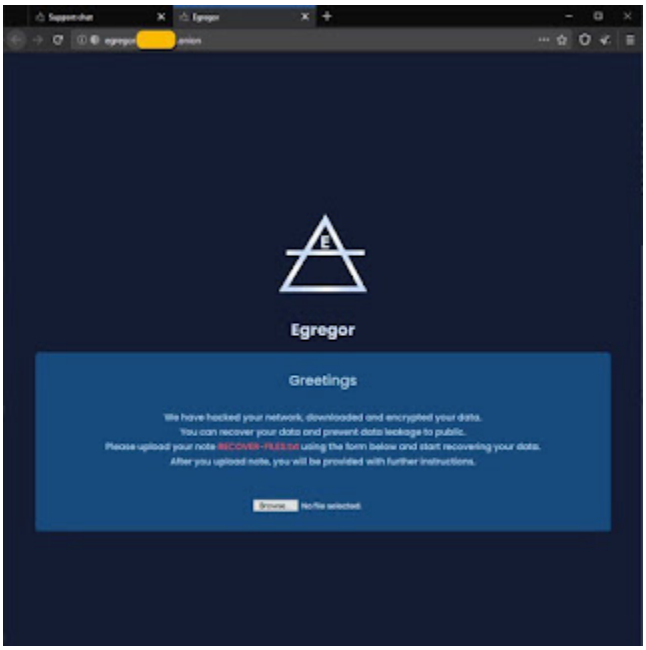
| Вы меня убедили! |

Тогда вам нужно СВЯЗАТЬСЯ С НАМИ, есть несколько способов сделать это.
I. Рекомендуемый (самый безопасный метод)
  а) Загрузите специальный браузер TOR: https://www.torproject.org/
  б) Установите браузер TOR
  с) Откройте наш веб-сайт с помощью LIVE CHAT в браузере TOR: http://egregor[скрыто].onion/[скрыто]
  г) Следуйте инструкциям на этой странице.
II. Если первый способ вам не подходит
  а) Откройте наш веб-сайт в ЖИВОМ ЧАТЕ: https://[скрыто].top/[скрыто]
  б) Следуйте инструкциям на этой странице.
Наша Живая ПОДДЕРЖКА готова помочь ВАМ на этом сайте.

| Что я получу в случае соглашения |

ВЫ ПОЛУЧИТЕ ПОЛНУЮ РАСШИФРОВКУ ваших машин в сети, ПОЛНЫЙ СПИСОК ФАЙЛОВ загруженных данных,
подтверждение УДАЛЕНИЯ загруженных данных с наших серверов, РЕКОМЕНДАЦИИ по охране периметра вашей сети.
И ПОЛНАЯ КОНФИДЕНЦИАЛЬНОСТЬ ОБ ИНЦИДЕНТЕ.
---------- ----------
Не редактируйте этот специальный технический блок, он нужен нам для авторизации.
---EGREGOR---
[скрыто base64]
---EGREGOR---

Сайт вымогателей находит в сети Tor.



Содержание текста на сайте:
Egregor
Greetings
We have hacked your network, downloaded and encrypted your data.
You can recover your data and prevent data leakage to public.
Please upload your note RECOVER-FILES.txt using the form below and start recovering your data.
After you upload note, you will be provided with further instructions.

Перевод на русский язык:
Egregor
Приветствую
Мы взломали вашу сеть, скачали и зашифровали ваши данные.
Вы можете вернуть свои данные и остановить утечку данных в открытый доступ.
Загрузите записку RECOVER-FILES.txt, используя форму ниже, и начните возврат своих данных.
После загрузки записки вам будут предоставлены дальнейшие инструкции.

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**.

➤ Egregor Ransomware использует три разные функции Windows API, чтобы проверить компьютер на принадлежность к России или и некоторым странам СНГ и прекратит работу, если обнаружит следующие локали:

0423 Белорусский (Беларусь)
0428 Таджикский (кириллица, Таджикистан)
042B Армянский (Армения)
042C Азербайджанский (латиница, Азербайджан)
0437 Грузинский (Грузия)
043F Казахский (Казахстан)
0440 Киргизский (Киргизия)
0442 Туркменский - Туркмения
0443 Узбекский (латиница, Узбекистан)
0444 Татарский (Россия)
0818 Румынский (Молдова)
0819 Русский (Молдова)
082C Азербайджанский (кириллица, Азербайджан)
0843 Узбекский (кириллица, Узбекистан)

➤ Для каждого шифруемого файла используется новое случайное расширение. Используется файловый маркер из двух DWORD в EOF XOR'd вместе до определенного значения для идентификации зашифрованных файлов. >>

➤ Подробности шифрования:
Шифровальщик использует функции API GetLogicalDriveStrings и GetDiskFreeSpace для определения имён и типов логических дисков, подключенных к устройству, в дополнение к количеству доступного на них свободного места.
Открытый RSA-ключ встроен в конфигурацию. Для каждого шифруемого файла генерируется пара закрытого и открытого ключей. Открытый ключ используется для шифрования симметричных ключей, которые позже будут использоваться для шифрования каждого файла. Для каждого шифруемого файла создается уникальный симметричный ключ.

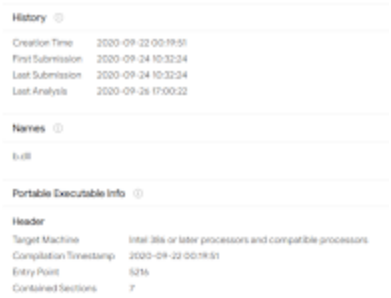
Схема генерации ключей:

- С помощью CryptGenKey создается 2048-битная пара RSA-ключей (т.н. сеансовый ключ).
- Затем ключ экспортируется с помощью API CryptExportKey.
- Экспортированный ключ шифруется с помощью ChaCha с использованием случайно сгенерированного ключа и IV.
- Ключи ChaCha зашифрованы с помощью функции CryptEncrypt и открытого RSA-ключ, встроенного в конфигурацию.
- Зашифрованный ключ ChaCha и зашифрованный сеансовый ключ сохраняются на диск по жестко заданному пути %ProgramData%\dtb.dat

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:
RECOVER-FILES.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла
b.dll - представленный для анализа файл
testbuild.pdb - название файла проекта



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

M:\sc\p\testbuild.pdb

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: http://egregor***.onion

Email: -
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
➤ **Triage analysis >>**

Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >> AR>**
⧖ 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 ===

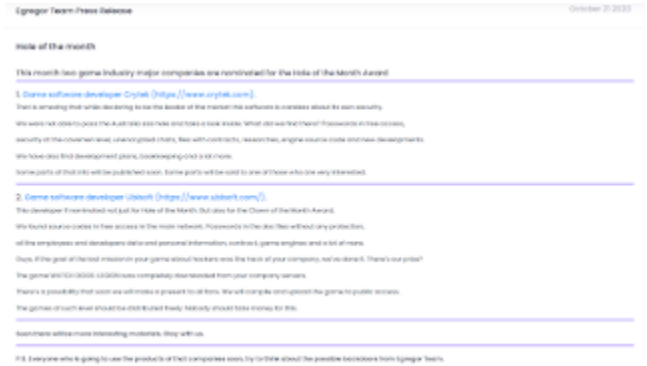
Maze Ransomware - май 2019 - ноябрь 2020
Sekhmet Ransomware - март 2020 - октябрь 2020
Egregor Ransomware - сентябрь 2020 - февраль 2021

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

Обновление от 12 октября 2020:
Статья на сайте BC >>

Расширение: **.CRYTEK**
Пострадавшие компании Ubisoft и Crytek

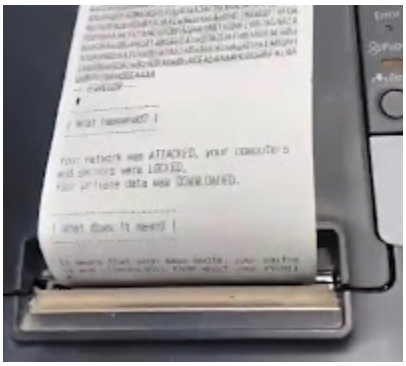
Обновление от 12 октября 2020:
Сообщение >>



Обновление от 29 октября 2020:
Статья о закрытии вымогательского проекта "Maze Ransomware" и переход операторов вымогателей на "Egregor Ransomware".
Вымогатели также подтверждили, что Maze, Sekhmet, Egregor являются их вымогательскими програмами.

Более того, пострадавшие от Egregor после уплаты выкупа получают. Sekhmet Decryptor.

Обновление от 18 ноября 2020:
Статья об этом >>
Деятели стоящие за Egregor Ransomware решили заявить о себе оригинальным способом. Чтобы привлечь внимание жертвы после атаки они стали с помощью сценария добавлять в печать на принтер своё сообщение. Это не отдельно взятый случай. Egregor многократно печатает записки о выкупе на всех доступных сетевых и местных принтерах.



| What happened? |

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

| What does it mean? |

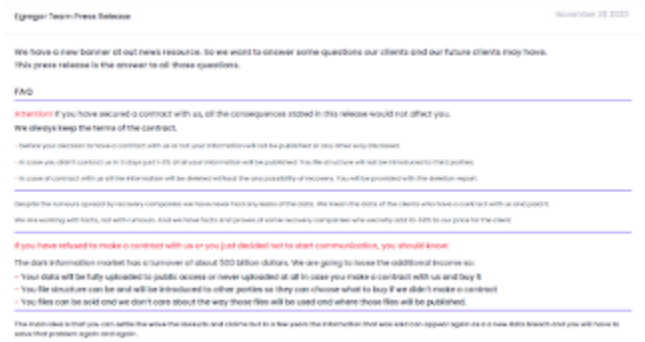
It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

***

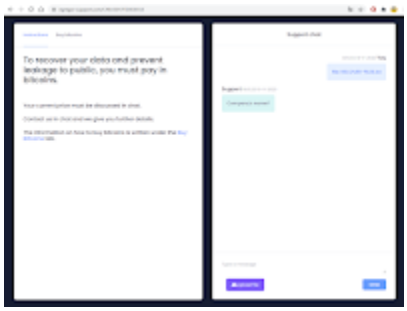
Это сообщение полностью есть в начале статьи, нет смысла повторть его здесь. Важно отметить, что вымогатели делают это для того, чтобы повысить осведомленность общественности об атаке и усилить давление на организацию-жертву, вынуждая её заплатить выкуп. Многие организации, государственные и финансовые учреждение предпочитают скрывать инциденты с вымогательством.

Обновление от 30 ноября 2020:
Выплата выкупа теперь называется **контрактом**. 👾

If you are a client who refused to conclude a contract and did not find information about yourself on our website or did not find some of your files, this does not mean that we forgot about you, it only means that your information was sold and only therefore it did not appear in free access!



Обновление от 1 декабря 2020:
Сообщение >>
Расширение: **.SEBsC**
Записка: RECOVER-FILES.txt
Tor-URL: xxxx://egregor4u5ipdzhv.onion/C4BA3647FD0D6918
URL: xxxxs://egregor-support.com/C4BA3647FD0D6918
Файл проекта: G:\Intel\Logs\qqqqq.pdb
Файл: qq.dll
Результаты анализов: **VT** + **AR**

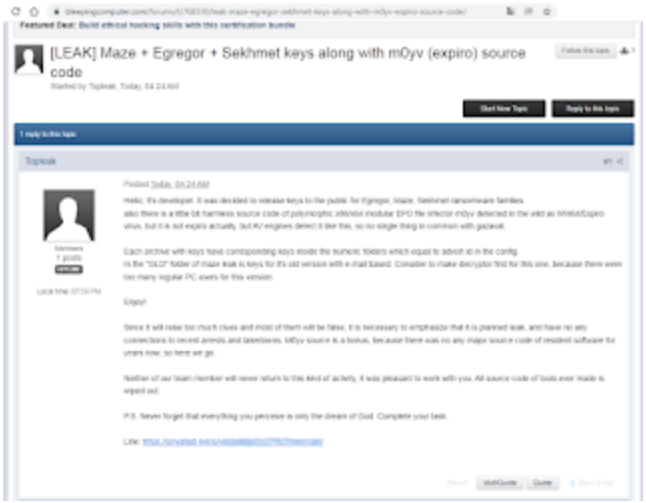


Обновление от 10 февраля 2021:
В ходе совместной операции полиции Франции и Украины удалось арестовать некоторых участников вымогательства Egregor Ransomware.

Статья на сайте FranceInter >>
Статья на сайте BleepingComputer >>

=== 2022 ===

Новость от 9 февраля 2022
Представитель группы вымогателей выложил в общий доступ на форуме BleepingComputer ключи дешифрования для пострадавших от Maze, Sekhmet, Egregor Ransomware.
Ссылка на скриншоте скрыта, чтобы не дать возможность использовать вредоносные файлы инфектора m0yv, которые были в архиве.



Внимание!
Теперь есть дешифровщик >>
Скачайте Emsisoft Decryptor for Maze/Sekhmet/Egregor >>

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

Read to links:

Message + Message + **myTweet**
ID Ransomware (ID as Egregor)
Write-up, Topic of Support
Added later: Write-up (on December 7, 2020)

Thanks:

Michael Gillespie, MalwareHunterTeam
Andrew Ivanov (author)
Tom Roter (Minerva Labs)
to the victims who sent the samples