

KEKW

 id-ransomware.blogspot.com/2020/03/kekw-ransomware.html



KEKW Ransomware

KEKW-Locker Ransomware

(шифровальщик-вымогатель, деструктор, стиратель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES, а затем в шутку требует выкуп в 1 миллион BTC. Оригинальное название: в записке не указано. На файле написано: KEKW.exe

Обнаружения:

DrWeb -> Trojan.Encoder.31348

BitDefender -> Trojan.GenericKD.42888790

Avira (no cloud) -> TR/Ransom.xrlse

ESET-NOD32 -> A Variant Of MSIL/Filecoder.YR

Malwarebytes -> Ransom.Kekw

Rising -> Ransom.Genasom!8.293 (CLOUD)

Symantec -> Trojan.Gen.2

Tencent -> Msil.Trojan.Encoder.Wnlz

TrendMicro -> Ransom.MSIL.KEKW.A

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: ??? >> KEKW



Изображение — логотип статьи

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



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 пришлось на вторую половину марта 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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



Содержание записки о выкупе:

RANSOM MESSAGE

GIVE ME 1 MILLION BITCOIN at RANSOM.onion

AES Encryption Key: G3Xgfd9aizCCOCZurvAINaEs09RbA23iFjs3kysSDIZQ=

AES Encryption IV: cswzut8/X3qc6xglSDSu9Q==

Другой вариант:

RANSOM MESSAGE

GIVE ME 1 MILLION BITCOIN at RANSOM.onion

AES Encryption Key: pG1fWp5RUk9Rp6NITUCuUYSI3zhLhy/E9BgcOoMC9ak=

AES Encryption IV: rBvS7Ew31YbPQ2byHd76fA==

Перевод записки на русский язык:

RANSOM СООБЩЕНИЕ

Дайте мне 1 миллион биткойнов на RANSOM.onion

AES-ключ шифрования: G3Xgfd9aizCCOCZurvAINaEs09RbA23iFjs3kysSDIZQ=

AES IV шифрование: cswzut8 / X3qc6xglSDSu9Q==

Технические детали

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](#).

➤ На момент написания статьи было неизвестно, помогут ли данные, указанные в записке, восстановить файлы. Во всяком случае пострадавшие не смогут сами восстановить данные. Сумма выкупа нереальная, значит, это больше вредительство, чем вымогательство.

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:

Decrypt.txt - название файла с требованием выкупа
KEKW.exe

<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

C:\Users\Jacob\source\repos\KEKW\obj\Debug\KEKW.pdb



Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Мьютексы:

См. ниже результаты анализов.

Сетевые подключения и связи:

URL: ransom.onion

Email: -

BTC: -

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

Результаты анализов:

Ⓜ [Hybrid analysis >>](#)

Σ [VirusTotal analysis >>](#)

🐞 [Intezer analysis >>](#)

≧

⌘ [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 ===

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

Ещё не было обновлений этого варианта.

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



Thanks :

GrujaRS

Andrew Ivanov (author)

to the victims who sent the samples

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