FastWind

id-ransomware.blogspot.com/2020/07/fastwind-ransomware.html

FastWind Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, но довольно странным образом, блоками по 16 байт, а затем требует написать на email вымогателей, чтобы узнать как заплатить выкуп в # BTC, получить дешифровщик и вернуть свои файлы. Оригинальное название: FastWind. На файле написано: нет данных.

Обнаружения:
DrWeb ->
BitDefender ->
ALYac ->
Avira (no cloud) ->
ESET-NOD32 ->
Malwarebytes ->
Rising ->
Symantec ->
TrendMicro ->

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: ??? >> FastWind

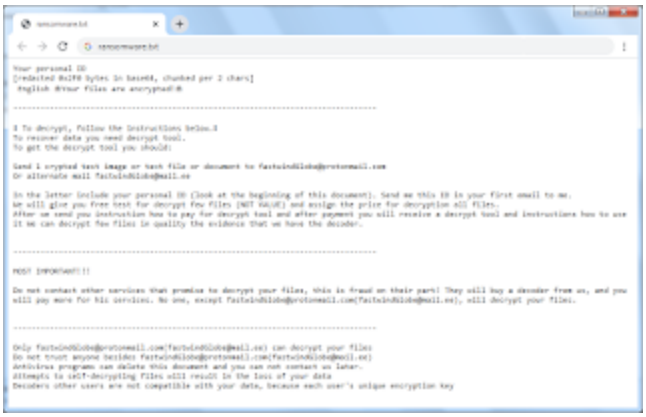
Изображение — логотип статьи

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

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

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



Содержание записки о выкупе:
Your personal ID
[redacted 0x2F0 bytes in base64, chunked per 2 chars]
English ☣Your files are encrypted!☣

⬇ To decrypt, follow the instructions below.⬇
To recover data you need decrypt tool.
To get the decrypt tool you should:
Send 1 crypted test image or text file or document to fastwindGlobe@protonmail.com
Or alternate mail fastwindGlobe@mail.ee
In the letter include your personal ID (look at the beginning of this document). Send me this ID in your first email to me.

We will give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files.
After we send you instruction how to pay for decrypt tool and after payment you will receive a decrypt tool and instructions how to use it We can decrypt few files in quality the evidence that we have the decoder.

MOST IMPORTANT!!!
Do not contact other services that promise to decrypt your files, this is fraud on their part! They will buy a decoder from us, and you will pay more for his services. No one, except fastwindGlobe@protonmail.com(fastwindGlobe@mail.ee), will decrypt your files.

Only fastwindGlobe@protonmail.com(fastwindGlobe@mail.ee) can decrypt your files
Do not trust anyone besides fastwindGlobe@protonmail.com(fastwindGlobe@mail.ee)
Antivirus programs can delete this document and you can not contact us later.
Attempts to self-decrypting files will result in the loss of your data
Decoders other users are not compatible with your data, because each user's unique encryption key

Перевод записки на русский язык:
Ваш личный ID
[здесь 0x2F0 байт в base64, разделены по 2 знака]
English ☣Ваши файлы зашифрованы!☣

⬇ Для расшифровке следуйте инструкциям ниже.⬇
Для восстановления данных вам нужен инструмент расшифровки.
Чтобы получить инструмент расшифровки вам нужно:
Отправить 1 зашифрованное тестовое изображение, текстовый файл или документ на fastwindGlobe@protonmail.com
Или альтернативную почту fastwindGlobe@mail.ee
В письме укажите свой личный ID (смотрите в начале документа). Отправьте мне этот ID в своем первом письме.
Мы сделаем вам бесплатную тест-расшифровку нескольких файлов (НЕЦЕННЫХ) и назначим цену для расшифровки всех файлов.
После того, как мы отправим вам инструкцию о том, как оплатить инструмент расшифровки, а после оплаты вы получите инструмент для расшифровки и инструкции по его использованию. Мы можем расшифровать несколько файлов в качестве доказательства того, что у нас есть декодер.

САМОЕ ВАЖНОЕ!!!
Не связывайтесь с другими службами, которые обещают расшифровать ваши файлы, это мошенничество с их стороны! Они купят у нас декодер, а вы заплатите больше за их услуги. Никто, кроме fastwindGlobe@protonmail.com (fastwindGlobe@mail.ee), не расшифрует ваши файлы.

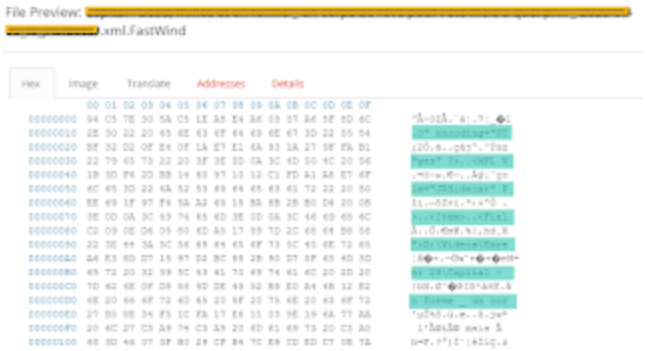
---------- ----------
Только fastwindGlobe@protonmail.com (fastwindGlobe@mail.ee) могут расшифровать ваши файлы
Не доверяйте никому, кроме fastwindGlobe@protonmail.com (fastwindGlobe@mail.ee)
Антивирусные программы могут удалить этот документ, и вы не можете связаться с нами позже.
Попытки самостоятельно расшифровать файлы приведут к потере ваших данных
Декодеры других пользователей не совместимы с вашими данными, потому что у каждого пользователя уникальный ключ шифрования

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**.

➤ Выполняет шифрования блока из 16-байт с такими же пропусками.



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:
ransomware.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

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

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: fastwindGlobe@protonmail.com, fastwindGlobe@mail.ee
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >>
🐞 Intezer analysis >>
⋟ ANY.RUN 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:

Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples