MetadataBin

id-ransomware.blogspot.com/2020/10/metadata-bin-ransomware.html

MetadataBin Ransomware

Ransomware32 Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в $1000, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: ransomware.exe, ransomware32.exe. Написан на языке Rust.

Обнаружения:
DrWeb -> Trojan.Encoder.32937, Trojan.Encoder.32940
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1, Trojan.GenericKD.44206852
ALYac -> Trojan.Ransom.Filecoder
Avira (no cloud) -> TR/FileCoder.uxgkl
ESET-NOD32 -> A Variant Of Win32/Filecoder.OED

Kaspersky -> Trojan.Win32.Udochka.y, Trojan-Ransom.Win32.Encoder.klv
Malwarebytes -> ***
Rising -> Ransom.Agent!1.CDE5 (CLASSIC)
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> TROJ_GEN.R002H09JP20

© Генеалогия: ??? >> MetadataBin

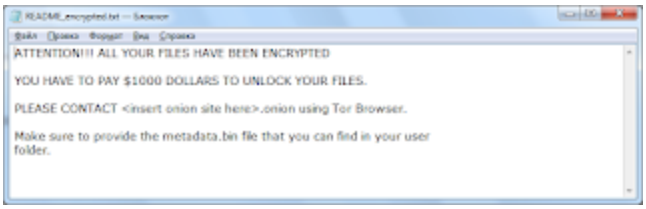
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **_encrypted**

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

Образец этого крипто-вымогателя был найден в конце октября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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



Содержание записки о выкупе:
ATTENTION!!! ALL YOUR FILES HAVE BEEN ENCRYPTED
YOU HAVE TO PAY $1000 DOLLARS TO UNLOCK YOUR FILES.
PLEASE CONTACT <insert onion site here>.onion using Tor Browser.
Make sure to provide the metadata.bin file that you can find in your user folder.

Перевод записки на русский язык:
ВНИМАНИЕ!!! ВСЕ ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ
ВЫ ДОЛЖНЫ ЗАПЛАТИТЬ $1000 ДЛЯ РАЗБЛОКИРОВКИ ФАЙЛОВ.
КОНТАКТ НА <вставьте сюда onion-сайт>.onion, используя Tor Browser.
Убедитесь, что передали файл metadata.bin, который можно найти в папке пользователя.

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**.

Список файловых расширений, подвергающихся шифрованию:

После доработки это могут быть документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
README_encrypted.txt - название файла с требованием выкупа
ransomware.exe, ransomware.bin - названия вредоносного файла
ransomware32.exe - название вредоносного файла

metadata.bin - специальный файл

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

Результаты анализов:

🔻 **Triage analysis >>**

Ⓗ Hybrid analysis >>

⋟ **ANY.RUN analysis >>**

⧖ VMRay analysis >>

Ⓥ VirusBay samples >>

 MalShare samples >>

👽 AlienVault analysis >>

🔃 CAPE Sandbox analysis >>

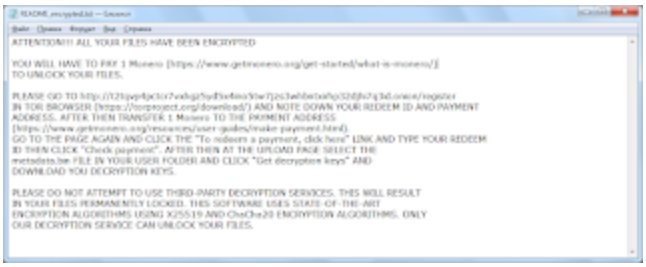
⟲ JOE Sandbox analysis >>

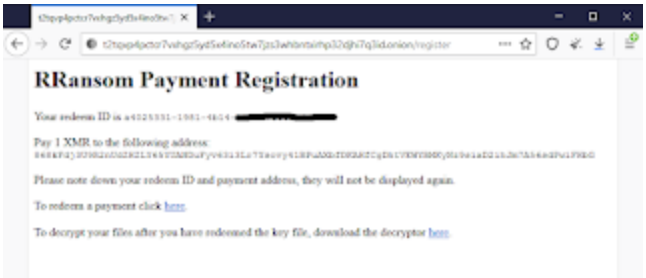
Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

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

Вариант от 12 октября 2021:
Сообщение >>
Расширение: **_encrypted**
Записка: README_encrypted.txt





Tor-URL: hxxx://t2tqvp4pctcr7vxhgz5yd5x4ino5tw7jzs3whbntxirhp32djhi7q3id.onion
Файл: hptestu.exe

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

Thanks:

```
xiaopao, 0x4143, Karsten Hahn
Andrew Ivanov (author)
***
to the victims who sent the samples
```