Z3

id-ransomware.blogspot.com/2020/08/z3-ransomware.html

Z3 Ransomware

Z3enc Ransomware

(шифровальщик-НЕ-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует (точнее, пытается зашифровать) данные пользователей, чтобы затем потребовать выкуп за расшифровку файлов. Содержит ошибки, из-за которых не удается его вредоносные действия. Вероятно, он еще находится в разработке. Оригинальное название: z3. На файле написано: z3.exe
---
Обнаружения:
DrWeb -> Trojan.MulDrop13.50657
BitDefender -> Trojan.GenericKD.43779174
ESET-NOD32 -> A Variant Of MSIL/Filecoder.ABS
Malwarebytes -> Ransom.FileCryptor
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Ransom_FileCrypter.R002C0DI520

© Генеалогия: ??? >> Z3


Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.z3enc**

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

Записка с требованием выкупа никак не называется. См. скриншот.

Содержание записки о выкупе:
Oops! Your files have been encrypted!
To decrypt then, you must *bla bla bla*.
If you close this window, all your data will be lost.

Перевод записки на русский язык:
Ой! Ваши файлы зашифрованы!
Чтобы расшифровать, вы должны *бла бла бла*.
Если вы закроете это окно, все ваши данные пропадут.

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**.

➤ Завершает работу ПК с помощью команды:
shutdown /f /r /t 0

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:
z3.exe
z3.pdb
<ransom_note>.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла
<random>.bat
data.bin
wsgjqtyy.1kv.exe
m5u0uccp.na0.bat
bdb77b2f35c0f3e79853ea7f8bdf5b29.in.exe

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\User\Desktop\z3\z3\obj\Release\net472\z3.pdb
C:\Users\User\AppData\Local\Temp\m5u0uccp.na0.bat
C:\Users\User\AppData\Local\Temp\bdb77b2f35c0f3e79853ea7f8bdf5b29.in.exe

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 >>
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:

```
S!Ri, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples
```