OutCrypt

Archived: 2026-04-06 00:26:49 UTC

OutCrypt Ransomware

(шифровальщик-не-вымогатель, деструктор) (первоисточник)

[Translation into English]

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем даже не требует выкуп, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: dirtytest.exe. Не оставляет никаких контактов для связи, фактически файлы повреждаются без возможности расшифровки.

Обнаружения:
DrWeb -> Trojan.Encoder.32250
BitDefender -> Trojan.GenericKD.43472275
ESET-NOD32 -> A Variant Of Generik.FWAEXBH
Kaspersky -> Trojan-Ransom.Win32.Encoder.jmq
Qihoo-360 -> Win32/Trojan.Ransom.c50
Rising -> Ransom.Encoder!8.FFD4 (CLOUD)
Symantec -> Trojan.Gen.6
Tencent -> Win32.Trojan.Encoder.Wvkj
TrendMicro -> Ransom_Encoder.R06BC0WGE20

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: ??? >> OutCrypt

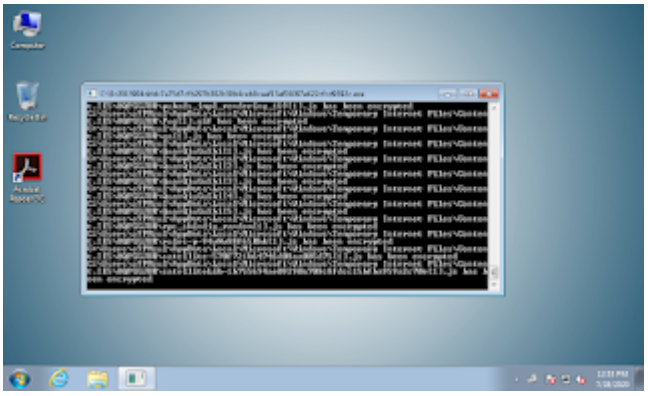
Изображение — логотип статьи

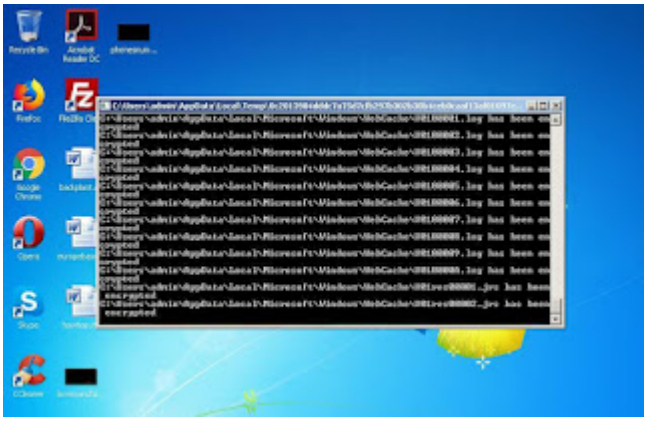
К зашифрованным файлам добавляется расширение: **_out**

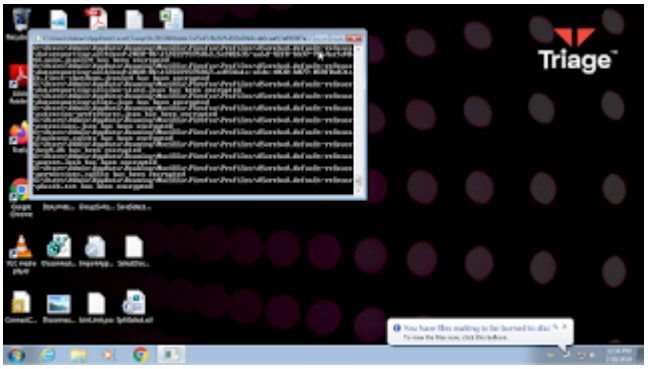
Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Образец этого шифровальщика был обнаружен в начале июля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа не оставляется.







Мы проверили это на разных машинах. Для каждого файла только сообщается, что он зашифрован. Нет никакого сообщения от тех, кто шифрует файлы.

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**.

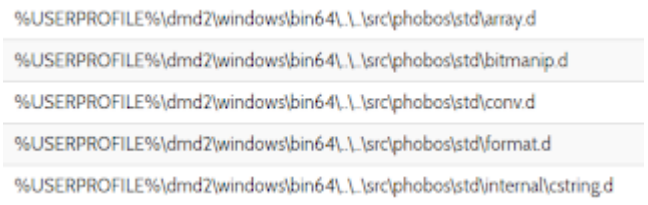
Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

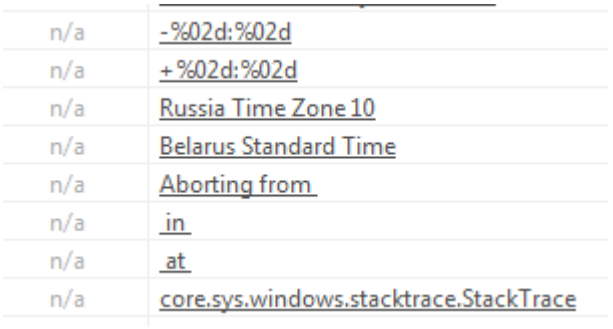
Файлы, связанные с этим Ransomware:
dirtytest.exe - исполняемый файл
desktop.ini_out - автозагружаемый файл
<random>.exe - случайное название вредоносного файла

Примечательно, что файл **desktop.ini_out** добавляется в Автозагрузку Windows.

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini_out
...\AppData\Local\dub\packages\crypto-0.2.13\crypto\src\crypto\aes.d
...\AppData\Local\dub\packages\crypto-0.2.13\crypto\src\crypto\padding.d

Скриншоты, которые могут быть интересны:





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 ===

Read to links:
Tweet on Twitter + Tweet + myTweet
ID Ransomware (ID as OutCrypt)
Write-up, Topic of Support
*

Thanks:
xiaopao, GrujaRS, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples
