InfoDot

id-ransomware.blogspot.com/2019/10/infodot-ransomware.html

InfoDot Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью алгоритмов AES-256 (режим CBC) и RSA-2048, а затем требует выкуп в 4 BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: bigdata.exe

Обнаружения:
DrWeb -> Trojan.Encoder.29861
BitDefender -> Trojan.GenericKD.31831899
ESET-NOD32 -> A Variant Of Generik.BNRBGWT
Kaspersky -> Trojan-Ransom.Win32.Crypren.afgd

© Генеалогия: MorrisBatchCrypt > InfoDot

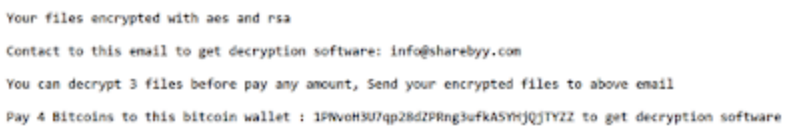
Изображение — логотип статьи

К зашифрованным файлам добавляются расширения:
.info@sharebyy[dot]com
.info@mymail9[dot]com

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 вторую половину октября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **help_to_decrypt.html**



Содержание записки о выкупе:
Your files encrypted with aes and rsa
Contact to this email to get decryption software: info@sharebyy.com
You can decrypt 3 files before pay any amount, Send your encrypted files to above email
Pay 4 Bitcoins to this bitcoin wallet : 1PNvoH3U7qp28dZPRng3ufkA5YHjQjTYZZ to get decryption software

Перевод записки на русский язык:
Ваши файлы зашифрованы с AES и RSA
Пишите на этот email, чтобы получить программ расшифровки: info@sharebyy.com
Вы можете расшифровать 3 файла, прежде оплаты любой суммы. Отправьте ваши зашифрованные файлы на email выше.
Заплатите 4 биткойна на этот биткойн-кошелек: 1PNvoH3U7qp28dZPRng3ufkA5YHjQjTYZZ, чтобы получить программе расшифровки

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**.

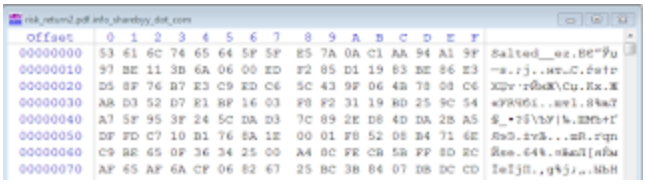
➤ Использует библиотеку OpenSSL для шифрования и дешифрования файлов.

➤ После уплаты выкупа пострадавший получает файлы в формате Original_filename**.bin**.info@sharebyy[dot]com с инструкциями по расшифровке, которые не позволяют расшифровать файлы или содержат ошибку в наборе команд.

➤ Использует taskkill.exe для завершения процессов:
C:\Windows\system32\cmd.exe /c taskkill /IM sql* /f

Подробности о шифровании:
Он использует OpenSSL для шифрования файлов с помощью AES-256 (CBC PKCS#7 padding) и генерирует защищенные ключи для каждого файла (CryptGenRandom), зашифрованные RSA-2048.

В первом варианте, который мы увидели использовался маркер **SALTED__**, во втором его уже не было.



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

Файлы, связанные с этим Ransomware:
help_to_decrypt.html
bigdata.exe
<random>.exe - случайное название вредоносного файла

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

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

Название проекта из ресурсов:
C:\Users\alara\documents\visual studio 2013\Projects\enc\Release**enc.pdb**

Сетевые подключения и связи:
Email-1: info@sharebyy.com
Email-2: info@mymail9.com
BTC: 1PNvoH3U7qp28dZPRng3ufkA5YHjQjTYZZ
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>** **VT>>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲

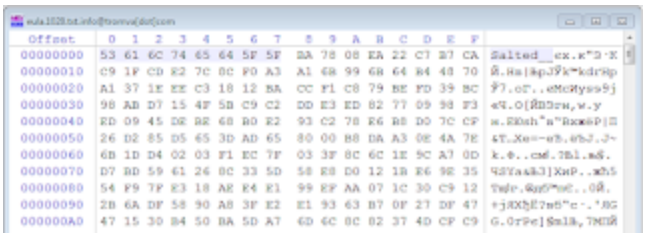
Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Вариант от 14 октября 2021:
Сообщение >>

Расширение: .info@tromva[dot]com
В зашифрованных файлах используется маркер **Salted__**
Записка: help to decrypt.html
Email: info@tromva.com



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

Thanks:

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