

# InfoDot

 [id-ransomware.blogspot.com/2019/10/infodot-ransomware.html](https://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 пришла 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**

```
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
```

### **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-инъектов, 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@sharebyu[dot]com с инструкциями по расшифровке, которые не позволяют расшифровать файлы или содержат ошибку в наборе команд.

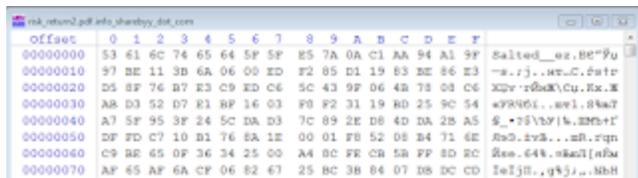
► Использует taskkill.exe для завершения процессов:

```
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.



```
offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 53 61 6c 74 65 64 5f 5f 85 7a 0a c1 aa 94 a1 9f Salted__ez.BE"fu
00000010 97 BE 11 3B 6A 06 00 ED F2 85 D1 19 83 BE 86 E3 -e.rj..m..C.fete
00000020 D5 8F 76 B7 E3 C9 ED C6 5C 43 9F 06 4B 78 08 C6 XQv-rdsk\Cu..K..K
00000030 AB D3 52 D7 E1 8F 16 03 F8 F2 31 19 8D 25 9C 54 w9906i..w1.8wa7
00000040 A7 5F 95 3F 24 5C DA D3 7C 89 2E D8 4D DA 2B A5 $_*75\5F\%.zmb+r
00000050 DF 7D C7 10 B1 76 8A 1E 00 01 F8 52 08 B4 71 6E $eD.zvB...m1.rqn
00000060 C9 BE 65 0F 36 34 25 00 A4 8C FE CB 5B FF 8D 8C $ee..64k..kna1[rfu
00000070 AF 65 AF 6A CF 06 82 67 25 BC 3B 84 07 D8 DC CD TeTjD..q%j...shH
```

property	value
md5	46c4480c841060f6a61b732f99310
sha1	D1EE0F7EE02056604D030CF8A021AC2A3F72
sha256	1B016071200F4A4871C4E2605A2FF4864317985C0E7614F868A313E14
first-bytes-hex	53 61 6c 74 65 64 5f 5f 85 7a 0a c1 aa 94 a1 9f BE 11 3B 6A 06 00 ED F2 85 D1 19 83 BE 86 E3 D5
first-bytes-text	S a l t e d _ _ e z . B E " f u
size	109302 (bytes)
entropy	7.908

### 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

```
00000000 53 61 6C 74 65 64 5F 5F BA 78 08 EA 22 C7 B7 CA Salted_ex.e"3-X
00000010 C9 1F CD E2 7C 0C F0 A3 A1 68 99 68 64 84 48 70 &.Ha|8pJ9k*ndr9p
00000020 A1 37 1E EE C3 18 12 BA CC F1 C8 79 BE FD 39 BC 97.c".eM8Tys9j
00000030 98 AB D7 15 4F 5B C9 C2 DD E3 ED 82 77 09 98 F3 eT.O[8Dzov,v.y
00000040 RD 09 45 D8 BE 48 80 E2 93 C2 78 E6 B8 D0 7C CF w.EBsh"a"8xw8P[2
00000050 26 D2 85 05 65 3D AD 65 80 00 88 DA A3 0E 4A 7E eT.Xe--wh.8bJ.J-
00000060 6B 1D D4 02 03 F1 EC 7F 03 3F 0C 6C 1E 9C A7 0D k.e..c8f.7bl.a8.
00000070 D7 8D 59 41 24 8C 33 5D 58 E8 D0 12 18 E6 98 35 42Yaa8JXnP..mh5
00000080 54 F9 7F E3 18 AE E4 E1 99 EF AA 07 1C 30 C9 12 Twie.6a9*mc..08.
00000090 2B 6A DF 58 90 AB 3F E2 E1 93 63 87 0F 27 DF 47 +j0X5E7m8"c-.*8C
000000A0 47 15 30 84 50 BA 5D A7 6D 4C 0C 82 37 4D CF C9 G.0rFe|8ml8,7M8
```

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



Thanks :

Michael Gillespie, Andrew Ivanov (author)

\*\*\*

\*\*\*

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles.