

# ThunderX, Ranzy Locker

Archived: 2026-04-10 03:18:38 UTC

## ThunderX Ransomware

## Ranzy Locker Ransomware

(шифровальщик-вымогатель) (первоисточник)

[Translation into English](#)

Этот крипто-вымогатель шифрует данные пользователей с помощью Salsa20, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: ThunderX. На файле написано: нет данных.

---

### Обнаружения:

**DrWeb** -> Trojan.Encoder.32480, Trojan.Encoder.32485, Trojan.Encoder.32806, Trojan.Encoder.33314

**BitDefender** -> Trojan.GenericKD.34388567, Gen:Heur.Ransom.Imps.1

**ESET-NOD32** -> A Variant Of Win32/Filecoder.ODD, A Variant Of Win32/Filecoder.RanzyLocker.A

**Malwarebytes** -> Ransom.FileCryptor, Ransom.Ranzy

**Microsoft** -> Trojan:Win32/Ymacro.AA64, Ransom:Win32/FileCrypter.MB!MTB

**Rising** -> Trojan.Generic@ML.85 (RDML:\*\*\*, Ransom.FileCrypter!8.11F42 (TFE\*)

**Symantec** -> ML.Attribute.HighConfidence, Downloader, Ransom.RanzyLocker

**TrendMicro** -> Trojan.Win32.WACATAC.ТННАНВО, Ransom.Win32.THUNDERX.SMTH

---

© Генеалогия: [Ako](#) ⇒ ThunderX > Ranzy Locker

Знак "⇒" здесь означает переход на другую разработку. См. "[Генеалогия](#)".



Изображение — логотип статьи

К зашифрованным файлам добавляется случайное расширение: **.<random>**

Примеры таких расширений:

- .BuchX**
- .SNwyR**
- .cyekE**

В обновленном варианте стало использоваться расширение: **.tx\_locked** (т.е. "ThunderX locked").

Позже, вариант Ranzy Locker получил расширения **.RNZ** и **.ranzy**



**Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях.

Там могут быть различия с первоначальным вариантом.

Ранняя активность этого крипто-вымогателя прихлась на конец августа - начало сентября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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

```

Attention! Your network has been locked
All files on each host has been encrypted
For this server all encrypted files have extension: .Ubnqf

----

You cant open or work with encrypted files while it encrypted
All backups has been deleted or formatted, do not worry, we can help you restore your files
We use strongest encryption algorithms, the only way to return your files back - contact us and receive decryption program.
Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee

----

Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li
And attach in first letter this file or just send all info below (copy all info!):

Steps:
1. Copy this file to the root of the infected drive
2. Run the file
3. Wait for the ransomware to encrypt your files
4. Contact us for the decryption program
5. Receive the decryption program
6. Run the decryption program
7. Your files will be restored
8. Delete this file
9. Delete the ransomware
10. Delete the ransomware
11. Delete the ransomware
12. Delete the ransomware
13. Delete the ransomware
14. Delete the ransomware
15. Delete the ransomware
16. Delete the ransomware
17. Delete the ransomware
18. Delete the ransomware
19. Delete the ransomware
20. Delete the ransomware
21. Delete the ransomware
22. Delete the ransomware
23. Delete the ransomware
24. Delete the ransomware
25. Delete the ransomware
26. Delete the ransomware
27. Delete the ransomware
28. Delete the ransomware
29. Delete the ransomware
30. Delete the ransomware
31. Delete the ransomware
32. Delete the ransomware
33. Delete the ransomware
34. Delete the ransomware
35. Delete the ransomware
36. Delete the ransomware
37. Delete the ransomware
38. Delete the ransomware
39. Delete the ransomware
40. Delete the ransomware
41. Delete the ransomware
42. Delete the ransomware
43. Delete the ransomware
44. Delete the ransomware
45. Delete the ransomware
46. Delete the ransomware
47. Delete the ransomware
48. Delete the ransomware
49. Delete the ransomware
50. Delete the ransomware
51. Delete the ransomware
52. Delete the ransomware
53. Delete the ransomware
54. Delete the ransomware
55. Delete the ransomware
56. Delete the ransomware
57. Delete the ransomware
58. Delete the ransomware
59. Delete the ransomware
60. Delete the ransomware
61. Delete the ransomware
62. Delete the ransomware
63. Delete the ransomware
64. Delete the ransomware
65. Delete the ransomware
66. Delete the ransomware
67. Delete the ransomware
68. Delete the ransomware
69. Delete the ransomware
70. Delete the ransomware
71. Delete the ransomware
72. Delete the ransomware
73. Delete the ransomware
74. Delete the ransomware
75. Delete the ransomware
76. Delete the ransomware
77. Delete the ransomware
78. Delete the ransomware
79. Delete the ransomware
80. Delete the ransomware
81. Delete the ransomware
82. Delete the ransomware
83. Delete the ransomware
84. Delete the ransomware
85. Delete the ransomware
86. Delete the ransomware
87. Delete the ransomware
88. Delete the ransomware
89. Delete the ransomware
90. Delete the ransomware
91. Delete the ransomware
92. Delete the ransomware
93. Delete the ransomware
94. Delete the ransomware
95. Delete the ransomware
96. Delete the ransomware
97. Delete the ransomware
98. Delete the ransomware
99. Delete the ransomware
100. Delete the ransomware

```

**Содержание записки о выкупе (1-й вариант):**

Attention! Your network has been locked  
 All files on each host has been encrypted  
 For this server all encrypted files have extension: .SNWyR  
 ----  
 You cant open or work with encrypted files while it encrypted  
 All backups has been deleted or formatted, do not worry, we can help you restore your files  
 We use strongest encryption algorithms, the only way to return your files back - contact us and receive decryption program.  
 Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee  
 ----  
 Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li  
 And attach in first letter this file or just send all info below (copy all info!):

key: eyJleHQiOiIuU053eVliLCJrZXkiOiJKMElr\*\*\* [totally 1012 chars]

personal id: AX90F\*\*\*

**Перевод записки на русский язык (1-й вариант):**

Внимание! Ваша сеть заблокирована

Все файлы на каждом хосте зашифрованы

Для этого сервера все зашифрованные файлы имеют расширение: .SNwyR

----

Вы не сможете открыть зашифрованные файлы или работать с ними, пока они зашифрованы

Все резервные копии удалены или отформатированы, не волнуйтесь, мы можем помочь вам вернуть ваши файлы

Мы используем самые надежные алгоритмы шифрования, единственный способ вернуть ваши файлы - написать нам и получить программу дешифрования.

Не беспокойтесь о гарантиях - вы можете БЕСПЛАТНО расшифровать любые 3 файла в качестве гарантии

----

Пишите нам: deloneThunder@protonmail.com или ThunderBirdXeX@cock.li

И прикрепите в первом письме этот файл или просто отправьте всю инфу ниже (скопируйте всю инфу!):

ключ: eyJleHQiOiIuU053eVliLCJrZXkiOiJKMElr \*\*\* [всего 1012 символов]

персональный id: AX90F \*\*\*

---

```
Attention! Your network has been locked by ThunderX
Your computers and server are encrypted
For this server all encrypted files have extension: .tx_locked
Follow our instructions below and you will recover all your data

----

You cant open or work with files while it encrypted - we use strongest encryption algorithm ***
All backups are deleted or formatted, do not worry, we can help you restore your files

The only way to return your files back - contact us and receive decryption program.

Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee

----

Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li
And attach in first letter this file or just send all info below (copy all info):

Key:
eyJleHQiOiIuU053eVliLCJrZXkiOiJKMElr***
personal id: AX90F***
```

Сравните ранний вариант с более новым вариантом записки.

**Содержание записки о выкупе (2-й вариант):**

Attention! Your network has been locked by ThunderX

Your computers and server are encrypted

For this server all encrypted files have extension: .tx\_locked

Follow our instructions below and you will recover all your data

----

You cant open or work with files while it encrypted - we use strongest encryption algorithm \*\*\*

All backups are deleted or formatted, do not worry, we can help you restore your files

The only way to return your files back - contact us and receive decryption program.

Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee

----

Contact us: deloneThunder@protonmail.com or ThunderBirdXeX@cock.li

And attach in first letter this file or just send all info below (copy all info!):

key: \*\*\*

personal id: \*\*\*\*\*

### **Перевод записки на русский язык (2-й вариант):**

Внимание! Ваша сеть заблокирована ThunderX

Ваши компьютеры и сервер зашифрованы

Для этого сервера все зашифрованные файлы имеют расширение: .tx\_locked.

Следуйте нашим инструкциям ниже, и вы восстановите все свои данные

----

Вы не можете открывать файлы или работать с ними, пока они зашифрованы - мы используем самый надежный алгоритм шифрования \*\*\*

Все резервные копии удалены или отформатированы, не волнуйтесь, мы поможем вам восстановить ваши файлы

Единственный способ вернуть ваши файлы - связаться с нами и получить программу для дешифрования.

Не беспокойтесь о гарантиях - вы можете БЕСПЛАТНО расшифровать любые 3 файла в качестве гарантии

----

Пишите нам: deloneThunder@protonmail.com или ThunderBirdXeX@cock.li

И прикрепите в первом письме этот файл или просто отправьте всю инфу ниже (скопируйте всю инфу!):

ключ: \*\*\*

персональный id: \*\*\*\*\*

### **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](#).

➤ Удаляет теньные копии файлов с помощью команды:

```
wmic.exe SHADOWCOPY /nointeractive
```

```
vssadmin.exe Delete Shadows /All /Quiet
```

### **Список файловых расширений, подвергающихся шифрованию:**

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

### **Список пропускаемых расширений:**

.dll, .exe, .ini, .lnk, .key, .rdp

### **Пропускаемые директории:**

AppData, boot, PerfLogs, PerfBoot, Intel, Microsoft, Windows, Tor Browser.

### **Файлы, связанные с этим Ransomware:**

readme.txt - название файла с требованием выкупа

<random>.exe - случайное название вредоносного файла

LockerStub.pdb - название файла проекта

### **Расположения:**

\Desktop\ ->

\User\_folders\ ->

\%TEMP%\ ->

C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb

### **Записи реестра, связанные с этим Ransomware:**

См. ниже результаты анализов.

### **Мьютексы:**

См. ниже результаты анализов.

### **Сетевые подключения и связи:**

Email: deloneThunder@protonmail.com, ThunderBirdXeX@cock.li

ВТС: -

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

### **Результаты анализов:**

▼ [Triage analysis >>](#)

Ⓜ [Hybrid analysis >>](#)

Σ [VirusTotal analysis >>](#) [VT>](#)

🐞 [Intezer analysis >>](#) [IA>](#)

⌘ 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 ===

**Обновление от 7 сентября 2020:**

[Сообщение >>](#)

Расширение: **.tx\_locked**

Записка: readme.txt

Результаты анализов: [VT](#) + [IA](#)

```
Attention! Your network has been locked by ThunderX
Your computers and servers are encrypted
For this reason all important files have been encrypted. As I said
follow our instructions below and you will recover all your data
...
You can open or save your files while in encrypted - we use strongest encryption algorithm ***
All locked file deleted or corrupted, do not worry, we can help you restore your files.
The only way to restore your files back - contact us and receive decryption program.
Do not worry about guarantees - you can always try it files for free as guarantee
...
Contact us: mbhelp@protonmail.com or akodesh@tutanota.com
and attach to them below this file or just send all info below (copy all info):
...
[Base64 encoded text]
```

**Обновление от 14 сентября 2020:**

[Сообщение >>](#)

Расширение: **.tx\_locked**

Записка: readme.txt

Email: mbhelp@protonmail.com

akodesh@tutanota.com

Результаты анализов: [VT](#) + [VMR](#) + [IA](#)

**Обновление от 29 сентября 2020:**

Самоназвание в записке: Ranzy Locker

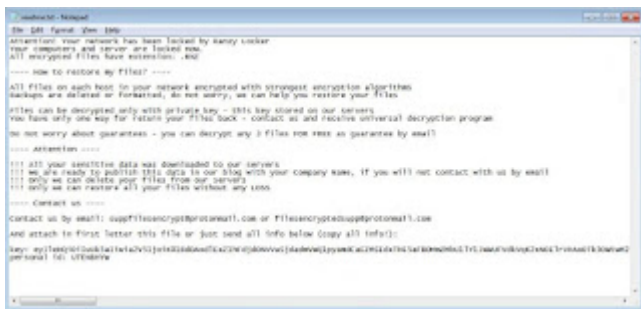
Название файла проекта: C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb

Расширение: **.RNZ**

Записка: readme.txt

Email: [suppfilenencrypt@protonmail.com](mailto:suppfilenencrypt@protonmail.com), [filesencryptedsupp@protonmail.com](mailto:filesencryptedsupp@protonmail.com)

Результаты анализов: [VT](#) + [IA](#) + [HA](#)



### Обновление от 5 октября 2020:

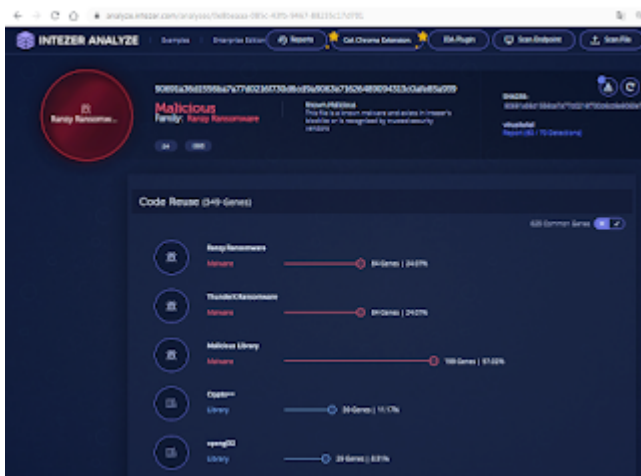
Вымогатели подготовили замену.

Новый образец вредоного ПО: [VT](#) + [IA](#)

Дата создания: 5 октября 2020.

Дата загрузки на анализ: 21 октября 2020.

На скриншоте от Intezer видно, что в этом образце есть гены обеих версий.



**History**

Creation Time	2020-10-06 07:25:56
First Submission	2020-10-21 11:41:00
Last Submission	2020-10-21 11:41:00
Last Analysis	2020-11-21 05:57:25

**Names**

fb1cb20566a073e1f9e26840e23c4d.virus

**Portable Executable info**

**Compiler Products**

- kl 205, version: 26715 count=10
- kl 205, version: 26715 count=149
- kl 205, version: 26715 count=16
- kl 205, version: 28427 count=17
- kl 205, version: 28427 count=21
- kl 205, version: 28427 count=42
- kl 257, version: 26715 count=21
- [...] Unmarked objects count=141
- kl 205, version: 28612 count=10
- kl 255, version: 28612 count=1
- kl 191, version: 0 count=1
- kl 256, version: 28612 count=1

**Header**

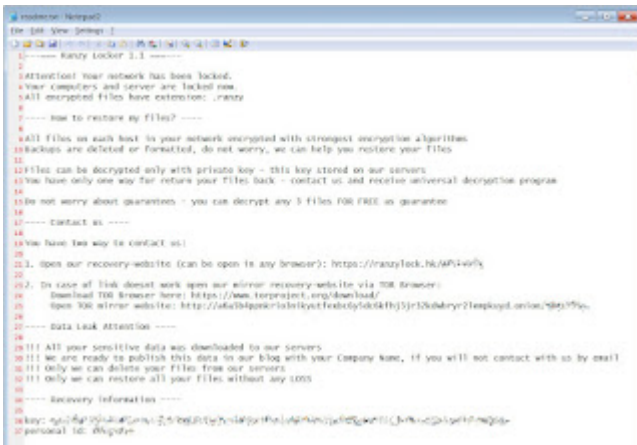
Target Machine	Intel x86 or later processors and compatible processors
Compilation Timestamp	2020-10-06 07:25:56
Entry Point	35e00
Contained Sections	4

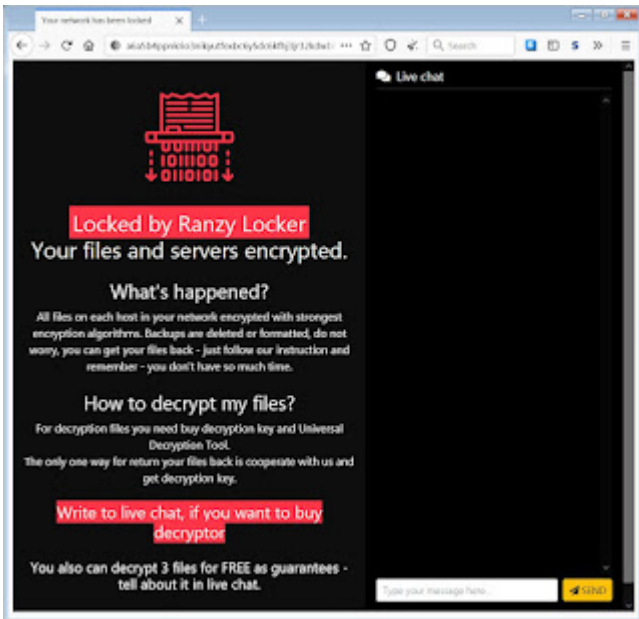
## Обновление от 16 октября 2020:

Расширение: **.ranzy**

Записка: **readme.txt**

Сайт: **hxxxs://ranzylock.hk/\*\*\***





Теперь официально сообщается:

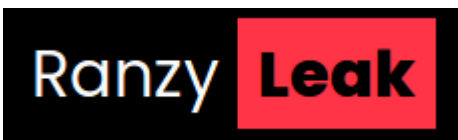
- 1) этот шифровальщик получил новое название Ranzy Locker;
- 2) Группа, управляющая Ranzy Locker, запустила сайт "Ranzy Leak" для публикации украденных данных.

### Обновление от 16 октября 2020:

Версия: Ranzy Locker 1.1

Расширение: .ranzy

Теперь используются 2 сайта в сети Tor: один вместо email для общения с жертвами, другой называется "Ranzy Leak", для публикации украденных данных. Кстати этот домен ранее использовался вымогателями Ako Ransomware.



```
----- Ranzy Locker 1.1 -----
Attention! your network has been locked.
your computer's and server are locked now.
All encrypted files have extension: .ranzy

---- How to restore my files? ----

All files on each host in your network encrypted with strongest encryption algorithms
Backups are deleted or formatted, do not worry, we can help you restore your files

Files can be decrypted only with private key - this key stored on our servers
You have only one way for return your files back - contact us and receive universal decryption program
do not worry about guarantees - you can decrypt any 3 files for FREE as guarantee

---- contact us ----

You have two way to contact us:
1. open our recovery-website (can be open in any browser): https://[redacted]
2. in case of link doesn't work open our mirror recovery-website via TOR browser:
   download TOR browser here: https://www.torproject.org/download/
   Open TOR mirror website: [redacted]

---- Data Leak Attention ----
!!! All your sensitive data was downloaded to our servers
!!! we are ready to publish this data in our blog with your company name, if you will not contact with us by email
!!! only we can delete your files from our servers
!!! only we can restore all your files without any loss

---- Recovery information ----
key: [redacted]
personal id: [redacted]
```

### Обновление от 28 октября 2020:







Read to links:

[Tweet on Twitter](#) + [Tweet](#) + [myTweet](#)

ID Ransomware (ID as ThunderX)

Write-up, Topic of Support

\*



Thanks:

S!Ri, Michael Gillespie

Andrew Ivanov (author)

Tesorion

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).

---

Source: <https://id-ransomware.blogspot.com/2020/08/thunderx-ransomware.html>