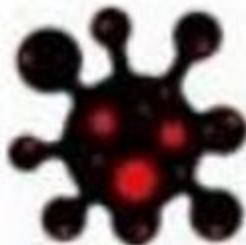


# Rektware

---

 [id-ransomware.blogspot.com/2018/09/rektware-ransomware.html](http://id-ransomware.blogspot.com/2018/09/rektware-ransomware.html)



## Rektware Ransomware

---

### PRZT Ransomware

---

(шифровальщик-HE-вымогатель)

[Translation into English](#)

---

Этот крипто-вымогатель шифрует данные пользователей, а затем даже не требует выкуп, чтобы вернуть файлы. Оригинальное название: rektware. На файле написано: нет данных. Возможно, находится в разработке. Написан на Autolt.

---

#### Обнаружение:

**DrWeb** -> Trojan.Encoder.30003, Trojan.MulDrop6.37395

**BitDefender** -> Trojan.Ransom.Rektware.A

**ESET-NOD32** -> A Variant Of Win32/Filecoder.NQF, Win32/Filecoder.G

**Malwarebytes** -> Ransom.Rektware

**Sophos AV** -> Mal/Autolt-AK

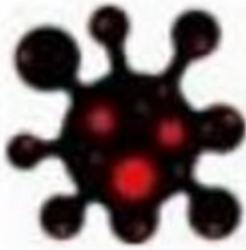
**Symantec** -> Downloader, Trojan Horse

**Tencent** -> Win32.Trojan.Raas.Auto, Win32.Trojan.Gen.Ajcb

**TrendMicro** -> Ransom\_KILLRABBIT.THAOOAAH

---

© Генеалогия: **Rektware** > новые варианты после статьи



Изображение принадлежит шифровальщику

К зашифрованным файлам добавляется случайное расширение, например:

**.CQScSFy**

**.2PWo3ja**

Вместе с переименованием файлы получают номера.



Так выглядят зашифрованные файлы

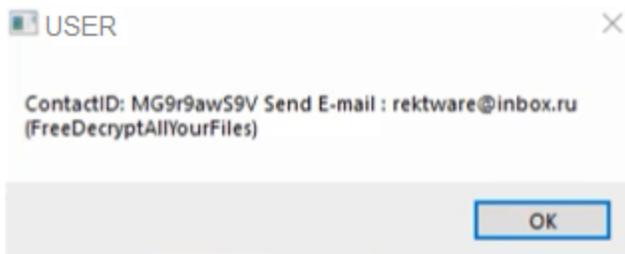


**Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришла на начало сентября 2018 г.

Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Запиской с требованием выкупа выступает файл **FIXPRZT.PRZ**



### **Содержание записки о выкупе:**

ContactID: MG9r9awS9V Send E-mail: rektware@inbox.ru  
(FreeDecryptAllYourFiles)

### **Перевод записки на русский язык:**

ContactID: MG9r9awS9V отправь на E-mail: rektware@inbox.ru  
(Бесплатное дешифрование всех твоих файлов)

### **Технические детали**

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).



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:**

FIXPRZT.PRZ

PRZT1.PRZ

PRZT2.PRZ

<random>.exe - случайное название

### **Расположения:**

\Desktop\ ->

\User\_folders\ ->

\%TEMP%\ ->

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

См. ниже результаты анализов.

## Сетевые подключения и связи:

Email: rektware@inbox.ru

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

## Результаты анализов:

 [Hybrid анализ >>](#)

 [VirusTotal анализ >>](#)

 [Intezer анализ >>](#)

 [VirusBay образец >>](#)

 [VMRay анализ >>](#)

 [ANY.RUN анализ >>](#)

 [AlienVault анализ >>](#)

 [CAPE Sandbox анализ >>](#)

 [MalShare анализ >>](#)

 [JOE Sandbox анализ >>](#)

Степень распространённости: низкая.

Подробные сведения собираются регулярно.

---

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

---

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

**Вариант от 23 сентября 2018:**

[Сообщение >>](#)

Расширение: **.xd**

Записка: не найдена

Список файловых расширений, подвергающихся шифрованию:

.avi, .bmp, .csv, .doc, .docx, .exe, .flv, .gif, .ini, .jpg, .m4a, .mkv, .mp3, .mp4, .odp, .ods, .odt, .one, .ots, .pdf, .png, .pps, .ppt, .pptx, .rtf, .swf, .vssx, .wav, .xls, .xlsx

URL: xxxx://rektware20.temp.swtest.ru

Файл: Ransomware.exe

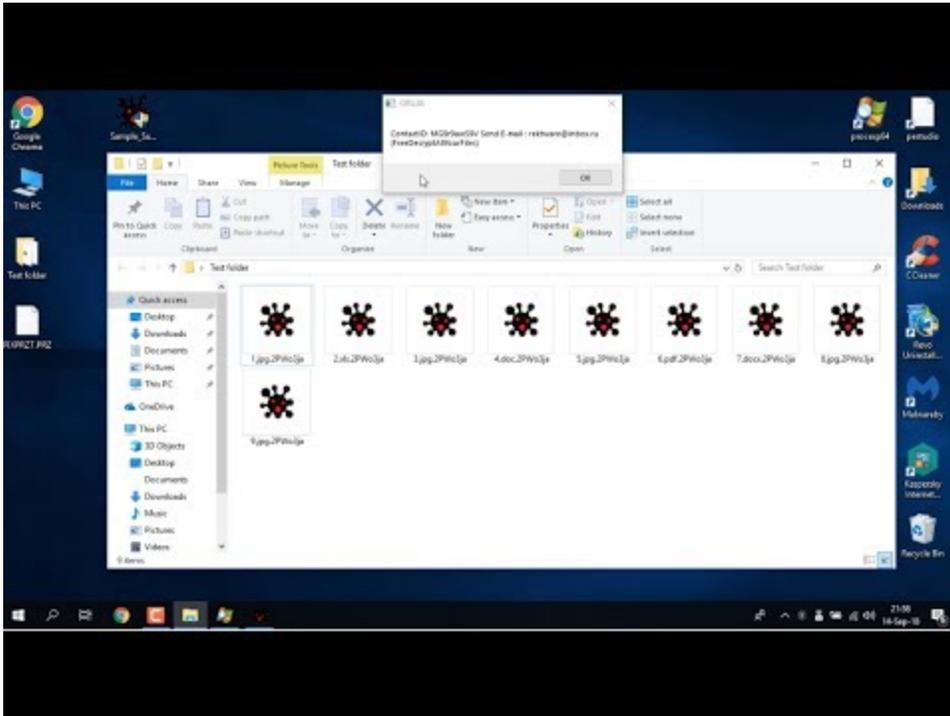
**Вариант от 13 декабря 2020:**

[Сообщение >>](#)

Расширение: **.NaNaNaNaNaNaNaNa**

Файл: Ransomware.exe

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



<https://youtu.be/d1->

WyuZ-zh0

- видеообзор от CyberSecurity GrujaRS



Thanks :

CyberSecurity GrujaRS  
Andrew Ivanov (article author)

\*  
\*

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