

# CryptoDarkRubix

Archived: 2026-04-05 23:44:53 UTC

## CryptoDarkRubix Ransomware

### Ranet Ransomware

(шифровальщик-вымогатель, деструктор) (первоисточник)

[Translation into English](#)

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: CryptoDarkRubix или Ranet. На файле написано: ranet.exe. Среда разработки: Delphi.

#### Обнаружения:

**DrWeb** -> Trojan.Encoder.31036, Trojan.Encoder.31288

**BitDefender** -> Trojan.GenericKD.33369205, Trojan.GenericKD.42859072

**ESET-NOD32** -> MSIL/Filecoder.YF

**Malwarebytes** -> Ransom.CryptoDarkRubix

**McAfee** -> GenericRXKC-IY!76D274C82343

**Microsoft** -> Ransom:MSIL/DarkRubix.S!MTB

**Rising** -> Ransom.Crypren!8.1D6C (CLOUD), Ransom.DarkRubix!8.118D8 (CLOUD)

**Symantec** -> Trojan Horse

**Tencent** -> Msil.Trojan.Crypren.Wpte, Win32.Trojan.Agent.Ajvm

**TrendMicro** -> Ransom\_Crypren.R011C0WBQ20, Ransom.MSIL.DARKRUBIX.A

---

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: ??? >> CryptoDarkRubix (Ranet)**



Изображение — логотип статьи

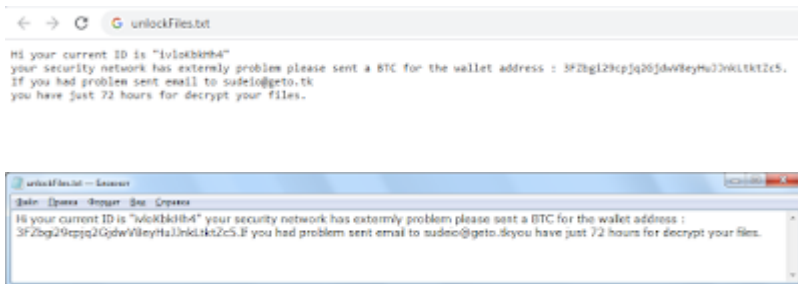
К зашифрованным файлам добавляется расширение: **.CryptoDarkRubix**



**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 февраля - начало марта 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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



#### Содержание записки о выкупе:

Hi your current ID is "ivloKbkHh4"

your security network has extermly problem please sent a BTC for the wallet address :  
3FZbgi29cpjq2GjdwV8eyHuJJnkLtkZc5.

If you had problem sent email to sudeio@geto.tk

you have just 72 hours for decrypt your files.

#### Перевод записки на русский язык:

Привет, ваш текущий ID "ivloKbkHh4"

Безопасности вашей сети имеет крайне опасные проблемы, отправьте BTC на кошелек:

3FZbgi29cpjq2GjdwV8eyHuJJnkLtkc5.

Если у вас возникли проблемы, пишите на [sudeio@geto.tk](mailto:sudeio@geto.tk)  
у вас только 72 часа для расшифровки ваших файлов.

Кроме записки используется еще изображение **darkrubixhacking.jpg**, заменяющее обои Рабочего стола, но мне не удалось получить эту картинку.

## Технические детали

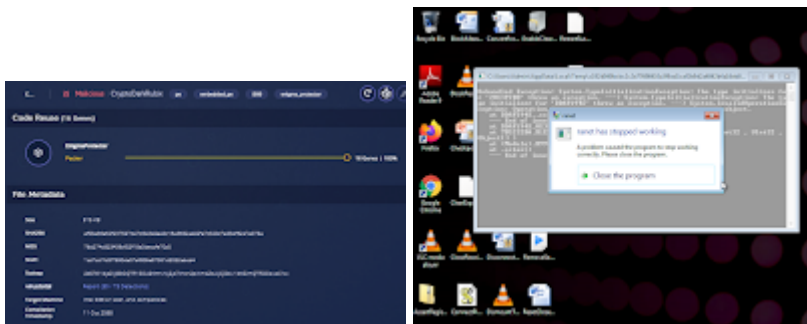
Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения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

- Файл шифровальщика защищен с помощью EnigmaProtector.
- Используется защита анти-VM, чтобы не допустить исследование на виртуальной машине.

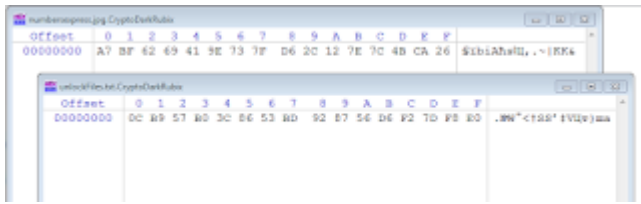


## Список файловых расширений, подвергающихся шифрованию:

.accda, .accdb, .accdc, .accde, .accdr, .accdt, .accdw, .adn, .adp, .backup, .bak, .bmpv, .csv, .cur, .doc, .docs, .docx, .dsn, .ico, .jif, .jpeg, .jpg, .laccdb, .ldf, .mad, .maf, .mam, .maq, .mar, .mat, .mda, .mdb, .mde, .mde, .mdf, .mdw, .mpp, .odc, .pdf, .pjp, .jpeg, .png, .svg, .tif, .tiff, .udl, .webp, .xla, .xlam, .xls, .xlsm, .xlsx, .xlt, .xltm, .xltx, .zip (56 расширений).

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

Содержание зашифрованных файлов минимализировано.



Таким образом, **уплата выкупа бесполезна.**

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

unlockFiles.txt - название файла с требованием выкупа

darkrubixhacking.jpg

ranet.exe - исполняемый файл вымогателя

asih.exe - исполняемый файл вымогателя (копия)

c192d040bcbc2c2e77698410a3f9ad1caf2b9d2a4842b4a16eb09f3446493a9c - случайное название вредоносного файла

#### **Расположения:**

\Desktop\ ->

\User\_folders\ ->

\%TEMP%\ ->

C:\Users\User\AppData\Local\Temp\asih.exe

C:\Users\User\AppData\Local\Temp\c192d040bcbc2c2e77698410a3f9ad1caf2b9d2a4842b4a16eb09f3446493a9c.exe

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

См. ниже результаты анализов.

#### **Мьютексы:**

См. ниже результаты анализов.

#### **Сетевые подключения и связи:**

Email: sudeio@geto.tk

BTC: [3FZbgi29cpjq2GjdwV8eyHuJnkLtkZc5](#)

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

#### **Результаты анализов:**

▼ [Triage analysis >>](#)

Ⓜ [Hybrid analysis >>](#) [HA>](#)

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

🐞 [Intezer analysis >>](#)

≥ [ANY.RUN analysis >>](#) [AR>](#)

⌘ [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 CryptoDarkRubix)

Write-up, Topic of Support

\*



Thanks:

dnwls0719, Ravi, Karsten Hahn, Michael Gillespie

Andrew Ivanov (author)

\*\*\*

to the victims who sent the samples

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

---

Source: <https://id-ransomware.blogspot.com/2020/03/cryptodarkrubix-ransomware.html>