

BlackKingdom

Archived: 2026-04-05 20:43:03 UTC

BlackKingdom Ransomware

BlackKingdom 2.0 Ransomware

BlackKingdom NextGen

Aliases: Black_Kingdom, DemonCrypt, DemonWare, CoderWare

(шифровальщик-вымогатель) (первоисточник)

[Translation into English](#)

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-256, а затем требует выкуп в \$10.000 в BTC, чтобы вернуть файлы. Оригинальное название: Black_Kingdom Ransomware. На файле написано: нет данных. Написан на языке Python 3.8.

Обнаружения:

DrWeb -> Python.Encoder.8, Python.Encoder.15, Trojan.Encoder.33173, Python.Encoder.25

BitDefender -> Generic.Ransom.BlackKingdom.CDC***

ESET-NOD32 -> Python/Filecoder.DL

F-Secure -> Trojan.TR/Ransom.pigrx

Malwarebytes -> Trojan.Banker.Python

Symantec -> Trojan.Gen.MBT


Tencent -> Malware.Win32.Gencirc.10b8b856

TrendMicro -> TROJ_FRS.VSNTBS20, Ransom.Win32.DEMONCRYPT.A

© Генеалогия: другие Python-ransomware >> BlackKingdom > [GammAWare](#), DemonWare
> [CoderCrypt](#)

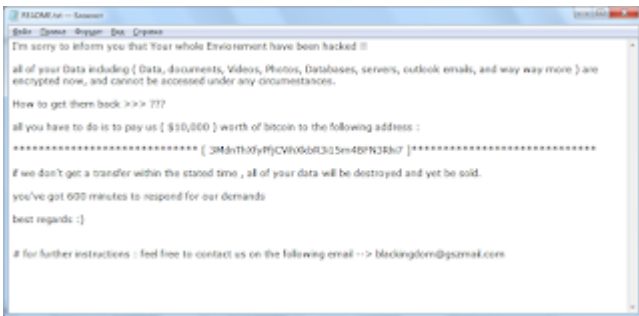


Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.DEMON**  **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 2020 г. Штамп даты: 5 января 2020. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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



Содержание записки о выкупе:

I'm sorry to inform you that Your whole Enviornment have been hacked !!
all of your Data including (Data, documents, Videos, Photos, Databases, servers, outlook emails, and way way more) are encrypted now, and cannot be accessed under any circumstancases.
How to get them back >>> ???
all you have to do is to pay us (\$10,000) worth of bitcoin to the following address :
***** [3MdnThXfyPjCVihXkbR3i15m4BFN3Rhi7]*****
if we don't get a transfer within the stated time , all of your data will be destroyed and yet be sold.
you've got 600 minutes to respond for our demands

best regards :)

for further instructions : feel free to contact us on the following email --> blackingdom@gszmail.com

Перевод записки на русский язык:

Извините, что сообщаю, что все ваше окружение взломано!

все ваши данные, включая (данные, документы, видео, фото, базы данных, серверы, почта Outlook и многие другие), зашифрованы и недоступны при любых обстоятельствах.

Как вернуть их >>> ???

все, что вам нужно сделать, это заплатить нам (10 000 долларов) в биткойнах на следующий адрес:

***** [3MdnThXfyPfcVihXkbR3i15m4BFN3Rhi7] *****

Если мы не получим перевод в указанный срок, все ваши данные будут уничтожены и еще проданы.

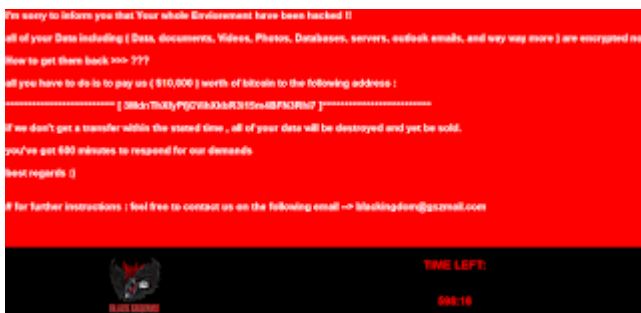
у вас есть 600 минут, чтобы ответить на наши требования

с уважением :)

для дальнейших инструкций: не стесняйтесь обращаться к нам на следующий адрес email ->

blackingdom@gszmail.com

Другим информатором выступает экран блокировки. Текст аналогичен тому, что есть в записке. На обдумывание ситуации дается всего 600 минут (10 часов).



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](#).

► Используется уязвимость в Microsoft Exchange для первоначального доступа к целевым компьютерам ([ССЫЛКА](#)). **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:

README.txt - название текстового файла

payload.txt.exe

<random>.exe - случайное название вредоносного файла

Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Сетевые подключения и связи:

Email: blackingdom@gszmail.com

BTC: 3MdnThXfyPfcVihXkbR3i15m4BFN3Rhi7

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

Результаты анализов:

📄 [Hybrid analysis >>](#)

Σ [VirusTotal analysis >>](#)

🐞 [Intezer analysis >>](#)

⌘ [ANY.RUN analysis >>](#) [AR>](#) [AR>](#)

⌘ [VMRay analysis >>](#)

Ⓜ [VirusBay samples >>](#)

⌘ [MalShare samples >>](#)

👁 [AlienVault analysis >>](#)

🔄 [CAPE Sandbox analysis >>](#)

🕒 [JOE Sandbox analysis >>](#)

Степень распространённости: низкая.

Подробные сведения собираются регулярно. Присылайте образцы.

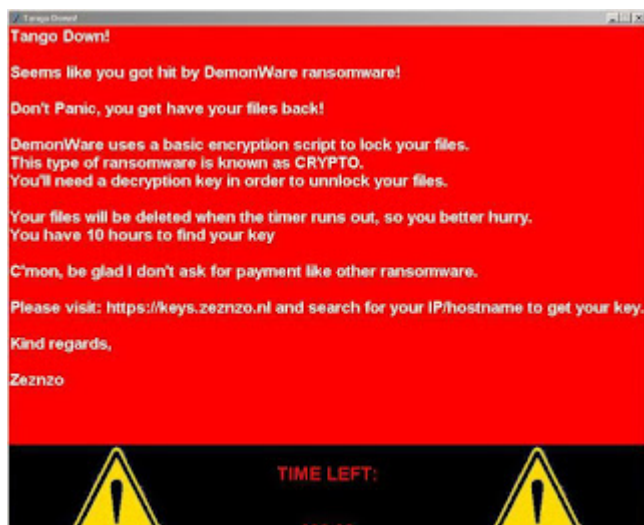
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

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

Обновление от 4 июня 2020:

Самоназвание: **DemonWare Ransomware**

Расширение: .DEMON



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

► Обнаружения:

DrWeb -> Python.Encoder.15

ALYac -> Trojan.Ransom.Filecoder

Avira (no cloud) -> TR/Ransom.fckkx

BitDefender -> Trojan.GenericKD.33965521

ESET-NOD32 -> Python/Filecoder.DM

Symantec -> ML.Attribute.HighConfidence

Tencent -> Win32.Trojan.Generic.Huqg

Whatsap: +63 997 401 3126 - страна Филиппины

```
hey damn!
Seems like you got hit by CodeWare ransomware!
warning! take a screenshot of this page. If you lose the information here, you'll never get to us, and it would be impossible to get your docs
don't panic, you get have your files back!

CodeWare uses a basic encryption script to lock your files. This type of ransomware is known as CRV90.
you'll need a decryption key in order to unlock your files.
your files will be deleted when the timer runs out, so you better hurry. you have 10 hours to find your key
when you pay you'll send you to the bitcoin address below.
you will need to send a single as proof to our e-mail address.
and if the recipient to correct, your code to get your files to your e-mail address. It will be sent back to you via e-mail.
But you have to be quick for that, because you have 10 hours. If you do not pay within 10 hours, your files will be permanently deleted.
and it would be out of reach again. If you don't know how to get bitcoins,
https://buy.bitcoin.com
can quickly get your credit or debit card online from the website.
Please type the bitcoin address shown on the screen in the wallet field on the website. If you try to shut it down by force,
you'll lose your docs. Because if you lose your bitcoin address,
you won't be able to pay, and you'll never get your files back.

email: cubafocoder@protonmail.com
bitcoin address: 13dVfHfRpyw6jsaw87yfvatqzts
telegram: @Koderwan
whatsapp: +63 997 401 3126
```

Замаскирован под установщик игры Cyberpunk 2077.

Файлы: CyberPunk2077.sfx.exe -> CyberPunk2077.exe

Результаты анализов: [VT](#) + [AR](#) / [VT](#)

► Обнаружения:

DrWeb -> Trojan.Encoder.33173

BitDefender -> Generic.Ransom.BlackKingdom.ACC0B5B4

ESET-NOD32 -> Python/Filecoder.CL

Kaspersky -> Trojan-Ransom.Win32.Alien.ao

Malwarebytes -> Ransom.FileCryptor

Rising -> Trojan.Generic@ML.94 (RDML:nCVGX9EypX0WbcZQRQa+Ig)

Symantec -> ML.Attribute.HighConfidence

Tencent -> Malware.Win32.Gencirc.11b17c94

TrendMicro -> Ransom_Alien.R03FC0P

Имеется версия для мобильных устройств под управление ОС Android.

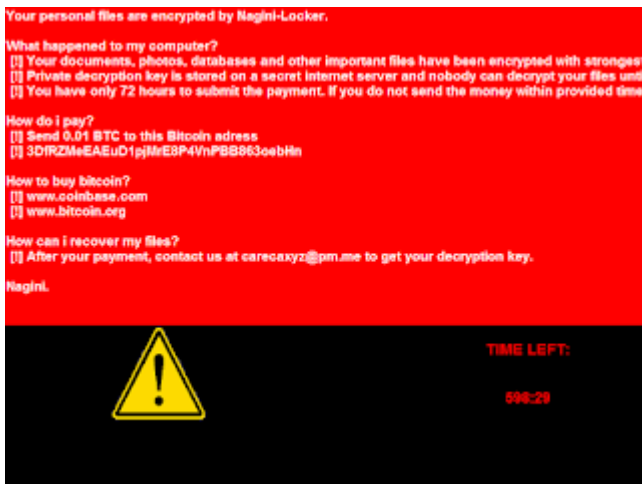
Сообщение от 21 декабря 2020:

Самоназвание: Nagini-Locker

Расширение: .DEMON

Email: carecaxyz@pm.me

BTC: 3DfRZMeEAEuD1pjMrE8P4VnPBB863oebHn



Вариант от 19 марта 2021:

Самоназвание: Blackkingdom Ransomware.

Использует уязвимости Microsoft Exchange Server ProxyLogon для шифрования серверов.

Расширение случайное для каждого файла: **.<random>**

Примеры: **.cnjl**, **.tMIBl**, **.WNoBGi9**

<input type="checkbox"/>	Commande_4501042655.pdf.cnjl	19.03.2021 2:41	Файл "CNIL"	126 KB
<input type="checkbox"/>	Commande_4501042704.pdf.WNoBGi9	19.03.2021 2:41	Файл "WNoBGi9"	131 KB
<input checked="" type="checkbox"/>	decrypt_file.Txt	19.03.2021 5:19	Текстовый докум...	3 KB
<input type="checkbox"/>	IMG_0001.JPG.cZwJ	19.03.2021 3:27	Файл "CZwJ"	411 KB
<input type="checkbox"/>	lettre eplenier 2018.docx.tMIBl	19.03.2021 2:50	Файл "tMIBl"	13 KB
<input type="checkbox"/>	Notepad++-lnk.iridFe	18.03.2021 22:43	Файл "iRiDFE"	2 KB
<input type="checkbox"/>	ViceVesa PRO.lnk.c3W30t	18.03.2021 21:27	Файл "c3W30t"	1 KB
<input type="checkbox"/>	winzip licence.PNG.tRFJA	19.03.2021 3:27	Файл "tRFJA"	39 KB

Записка: decrypt_file.Txt

Email: support_blackkingdom2@protonmail.com

Сумма выкупа: \$10.000 в BTC.

BTC: 1Lf8ZzcEhhRiXpk6YNQFpCJcUisiXb34FT

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

► Обнаружения:

DrWeb -> Python.Encoder.25

ALYac -> Trojan.Ransom.BlackKingdom

BitDefender -> Trojan.GenericKD.45955218

Emsisoft -> Trojan.Ransom.BlackKingdom.B (B)

ESET-NOD32 -> Python/Filecoder.GO

Microsoft -> Ransom:Win64/Filecoder!MSR

Qihoo-360 -> Win64/Ransom.BlackKingdom.H8oAFg8A

Rising -> Ransom.BlackKingdom!1.D420 (CLASSIC)

TrendMicro -> Ransom.Win64.BLACKKINGDOM.B

```

decrypt.txt
-----
[ We Are Back ]
-----

We hacked your (( Network )) , and now all files, documents, images,
databases and other important data are safely encrypted using the strongest algorithms ever.
You cannot access any of your files or services .
But do not worry. You can restore everything and get back business very soon ( depends on your actions )

before I tell you you can restore your data, you have to know certain things :
We have shut down most of your data ( especially important data ) , and if you don't contact us within 7 days, your data will be released to the public.
To see what happens to those who didn't contact us, just google : ( Blackkingdom ransomware )

-----
[ What guarantees ]
-----

We understand your stress and anxiety, so you have a free opportunity to test our service by instantly decrypting one or two files. For free
just send the files you want to decrypt to (support_blackkingdom@protonmail.com)

-----
[ How to contact us and recover all of your files ]
-----

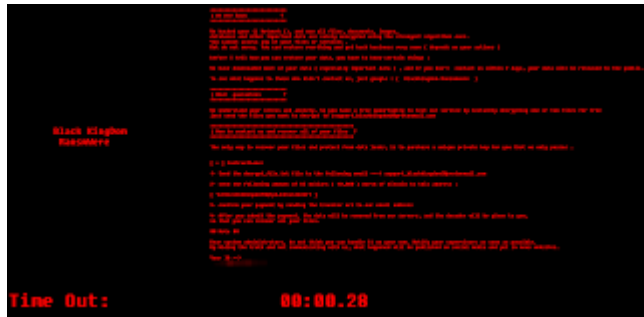
The only way to recover your files and protect from data leaks, is to purchase a unique private key for you that we only possess .

[ * ] Instructions:
1- Send the decrypt.txt file to the following email ==> support_blackkingdom@protonmail.com
2- send the following amount of us dollars ( 10,000 ) worth of bitcoins to this address :
[ 1P8Z1c8M8d9pW9qyC10z1d0000? ]
3- confirm your payment by sending the transfer url to our email address
4- After you submit the payment, the data will be removed from our servers, and the decoder will be given to you,
so that you can recover all your files.

## Note ##
Dear system administrators, do not think you can handle IT on your own. Notify your superiors as soon as possible.
By hiding the truth and not communicating with us, what happened will be published on social media and get in news websites.

Your sig:
0186f760a040a7616

```



► Содержание записки:

| We Are Back ?

We hacked your ((Network)), and now all files, documents, images, databases and other important data are safely encrypted using the strongest algorithms ever.

You cannot access any of your files or services.

But do not worry. You can restore everything and get back business very soon (depends on your actions)

before I tell how you can restore your data, you have to know certain things :

We have downloaded most of your data (especially important data) , and if you don't contact us within 2 days, your data will be released to the public.

To see what happens to those who didn't contact us, just google : (Blackkingdom Ransomware)

| What guarantees ?

We understand your stress and anxiety. So you have a free opportunity to test our service by instantly decrypting one or two files for free

just send the files you want to decrypt to (support_blackkingdom2@protonmail.com

| How to contact us and recover all of your files ?

The only way to recover your files and protect from data leaks, is to purchase a unique private key for you that we only posses .

[+] Instructions:

1- Send the decrypt_file.txt file to the following email ==> support_blackkingdom2@protonmail.com

2- send the following amount of US dollars (10,000) worth of bitcoin to this address :

[1Lf8ZzcEhhRiXpk6YNQFpCJcUisiXb34FT]

3- confirm your payment by sending the transfer url to our email address

4- After you submit the payment, the data will be removed from our servers, and the decoder will be given to you, so that you can recover all your files.

Note

Dear system administrators, do not think you can handle it on your own. Notify your supervisors as soon as possible.

By hiding the truth and not communicating with us, what happened will be published on social media and yet in news websites.

Your ID ==>

sk8mO7mFsozUf6xPrfn

Вариант от 24 августа 2021:

Расширение: .svux

Email: CSGVyzko@mail2tor.com

Файл: FREE VBUCKS GENERATOR 2021 FREE NO FAKE 1 LINK MEGA 100% REAL.exe

Результаты анализов: [VT](#)

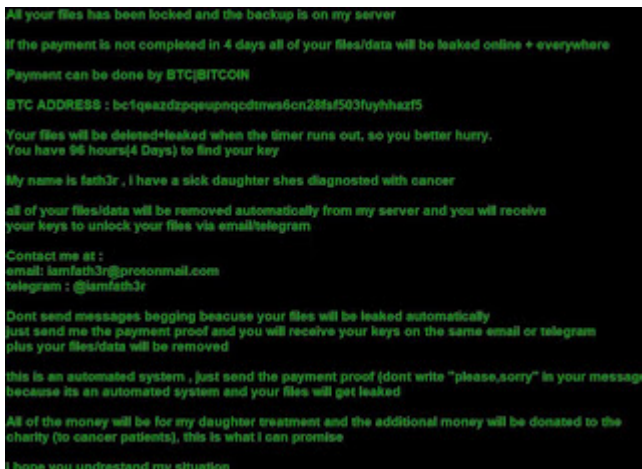
Вариант от 7 марта 2022:

Самоназвание: Fath3r Ransomware

Email: iamfath3r@protonmail.com

Telegram: @iamfath3r

BTC: bc1qeazdzpqpupnqcdtnws6cn28fsf503fuyhhazf5



Файл: payload.exe

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

MD5: f3ff8e85a6b9ac336273c4e51156f36a

SHA-1: 7f745a260c30aefddc12f34276e73d00c9ea745f

SHA-256: 73abef1e8cd548939010ad5c4937fe5bdabfb0b9a12d711debfa9a53925647fe

Vhash: 027076655d15551565504013z3005fmz11fz

Imphash: c5640c7a22008f949f9bc94a27623f95

► Обнаружения:

BitDefender: Generic.Ransom.BlackKingdom.09C2D51C

DrWeb: Trojan.PWS.Siggen3.12711

ESET-NOD32: Python/Filecoder.DM

Malwarebytes: Trojan.Agent

Microsoft: Trojan:Win32/Wacatac.B!ml

Rising: Ransom.Agent!1.D430 (CLASSIC)

Tencent: Win32.Trojan.Filecoder.Efbb

TrendMicro: TROJ_GEN.R002C0WC722

=== 2025 ===

Новость мая 2025:

США предъявили обвинения администратору вируса-вымогателя Black Kingdom в атаках на Microsoft Exchange. Обвиняется гражданин Йемена Рами Халед Ахмед. [Статья об этом >>](#)

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



Read to links:

[Message](#) + [Message](#) + [myMessage](#)

ID Ransomware (ID as BlackKingdom)

Write-up, Topic of Support



Thanks:

GrujaRS, 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/2020/02/blackkingdom-ransomware.html>