# Шифровальщики-вымогатели The Digest "Crypto-Ransomware"

Archived: 2026-04-05 12:44:46 UTC

## ABCD Ransomware

## LockBit, LockBit 2.0 Ransomware

## Lock2Bits Ransomware

## LuckyDay Ransomware

## LockBit NextGen

## LockBit 3.0 Ransomware

## LockBit 4.0 Ransomware

## LockBit 5.0 Ransomware

**(шифровальщик-вымогатель) (первоисточник)**
**Translation into English**

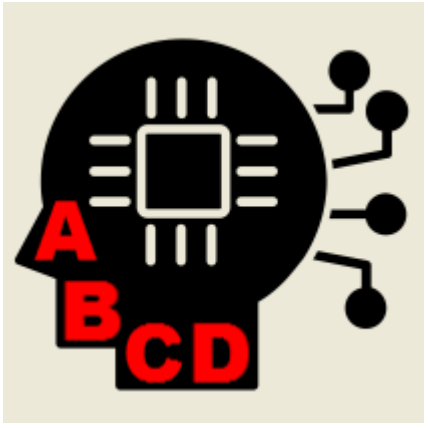
Этот крипто-вымогатель шифрует данные компаний и бизнес-пользователей с помощью AES + RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в ранних вариантах в записке не было указано. Потому для этой статьи первым было выбрано название ABCD по используемому расширению **.abcd**.Позже, в конце декабря 2019, в коде и названии появилось слово LockBit, потом стало использоваться расширение .lockbit. Дальше — больше. Похоже на то, что вымогатели не знают как себя назвать и постоянно меняют названия. По предварительным и частично подтвержденным данным среди тех, кто стоит за распространением ранних вариантов ABCD, LockBit стоят русскоязычные хакеры, в том числе граждане России, Украины, США, Канады и других стран.

Еще позже появились более новые версии: 3.0, 4.0, 5.0. См. ниже образцы.

**Обнаружения:**
**DrWeb** -> Trojan.Encoder.29662, Trojan.Encoder.30295, Trojan.Encoder.30886, Trojan.Encoder.31783
**BitDefender** -> Gen:Heur.Ransom.Imps.3, Gen:Heur.Ransom.Imps.1, Trojan.GenericKD.33815280, A Variant Of Win32/Kryptik.HDGL

**Malwarebytes** -> Ransom.LockBit
**McAfee** -> RDN/Ransom, Ransom-Lkbot!75C039742AFD
**Microsoft** -> Ransom:Win32/LockBit.A!MTB, Ransom:Win32/LokiBot!MSR
**ESET-NOD32** -> A Variant Of Win32/Filecoder.NXQ
**Avira (no cloud)** -> TR/Downloader.Gen, TR/Crypt.ZPACK.Gen
**Symantec** -> ML.Attribute.HighConfidence, Downloader

**© Генеалогия: LockerGoga > MegaCortex > Good (Goodmen), ABCD (LockBit), PhobosImposter > Lock2Bits > LockBit 2.0 > LockBit 3.0 > CriptomanGizmo и другие > LockBit NextGen**




Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.abcd** **Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность раннего вариант этого крипто-вымогателя пришлась на середину октября 2019 г. Позже вымогатели придумали этому "чуду" название и стали распространять это как LockBit. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. В январе 2020 пострадавшие были из США, Германии, Франции, Китая.

Записка с требованием выкупа называется: **Restore-My-Files.txt**


**Содержание записки о выкупе:**

All your important files are encrypted!

There is  only one way to get your files back:

1. Contact with us

2. Send us 1 any encrypted your file and your personal key

3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files

4. Pay

5. We send for you decryptor software

We accept Bitcoin

Attention!

Do not rename encrypted files.

Do not try to decrypt using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased  price(they add their fee to our)

Contact information: goeila@countermail.com

Be sure to duplicate your message on the e-mail: gupzkz@cock.li

Your personal id:

DR2JZobWr9AxQofCDEkqc8wZxBVcgqHrwHxURb/Ty6zmkjUAbPlY6QpYLTlnhROL

*****

**Перевод записки на русский язык:**

Все ваши важные файлы зашифрованы!

Есть только один способ вернуть ваши файлы:

1. Свяжитесь с нами

2. Отправьте нам 1 любой зашифрованный файл и ваш личный ключ

3. Мы расшифруем 1 файл для теста (максимальный размер файла - 1 МБ), это гарантирует, что мы можем расшифровать ваши файлы

4. Оплатить

5. Мы вышлем вам программу расшифровки

Мы принимаем биткойны
Внимание!
Не переименовывайте зашифрованные файлы.
Не пытайтесь расшифровать с помощью сторонних программ, это может привести к постоянной потере данных.
Расшифровка ваших файлов с помощью третьих лиц может привести к повышению цены (они добавляют свою плату к нашей)
Контактная информация: goeila@countermail.com
Не забудьте продублировать ваше сообщение на email: gupzkz@cock.li
Ваш личный id:
DR2JZobWr9AxQofCDEkqc8wZxBVcgqHrwHxURb / Ty6zmkjUAbPlY6QpYLTlnhROL
*****
[всего 1708 знаков]

**Технические детали**

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, 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 технологию обхода UAC.

➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки. Очищает журналы Windows.
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

➤ Использует белый список стран и языковых локализаций стран СНГ, в которых шифрование не должно

осуществляться. Список прилагается.
Азербайджанский (кириллица)
Азербайджанский (латиница)
Армянский
Белорусский
Грузинский
Казахский
Киргизский (кириллица)
Русский
Русский (Молдова)
Таджикский
Туркменский
Узбекский (кириллица)
Узбекский (латиница)
Украинский

**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:**
Restore-My-Files.txt
<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: goeila@countermail.com, gupzkz@cock.li
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

**Результаты анализов:**
Ⓗ Hybrid analysis >>
**Σ** VirusTotal analysis >>
🐞 Intezer analysis >>

⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
⩓ MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Некоторые другие более новые образцы можно найти на сайте BA:

https://bazaar.abuse.ch/browse/tag/lockbit/

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

---

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

ABCD Ransomware - с октября 2019

LockBit Ransomware - с декабря 2019

Lock2Bit Ransomware - с мая 2020

LockBit 2.0 Ransomware - с июля 2021

LockBit 3.0 Ransomware - с марта 2022

---

Отдельное использование кода LockBit Ransomware:

LockFile Ransomware - июль - август 2021

AtomSilo Ransomware - сентябрь - декабрь 2021

---

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

**Обновление от 14 ноября 2019:**
Пост на форуме >>
Пост в Твиттере >>
Расширение: .abcd

Записка: Restore-My-Files.txt

Email: supportpc@cock.li, goodsupport@cock.li


➤ Содержание записки:

All your important files are encrypted!

There is only one way to get your files back:

1. Contact with us

2. Send us 1 any encrypted your file and your personal key

3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files

4. Pay

5. We send for you decryptor software

We accept Bitcoin

Attention!

Do not rename encrypted files.

Do not try to decrypt using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

Contact information: supportpc@cock.li

Be sure to duplicate your message on the e-mail: goodsupport@cock.li

Your personal id:

ceipl0Z10GtMlyTWzHn0YOT7T2+KrRjZDspX3+6*** [всего 1708 знаков]

**Обновление от 4 декабря 2019:**

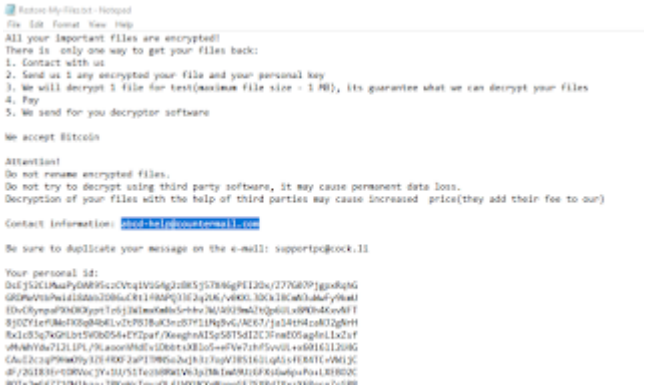
Пост в Твиттере >>

Расширение: **.abcd**

Записка: Restore-My-Files.txt

Email: abcd-help@countermail.com, supportpc@cock.li

Результаты анализов: **VT**




➤ Содержание записки:

All your important files are encrypted!

There is only one way to get your files back:

1. Contact with us

2. Send us 1 any encrypted your file and your personal key

3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files

4. Pay

5. We send for you decryptor software

We accept Bitcoin

Attention!

Do not rename encrypted files.

Do not try to decrypt using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

abcd-help@countermail.com

Contact information:

Be sure to duplicate your message on the e-mail: supportpc@cock.li

Your personal id:

DsEj52CLMwaPyDAR95szCVtqlViG4g2zBK5j57X46gPEI2Ox/Z77***

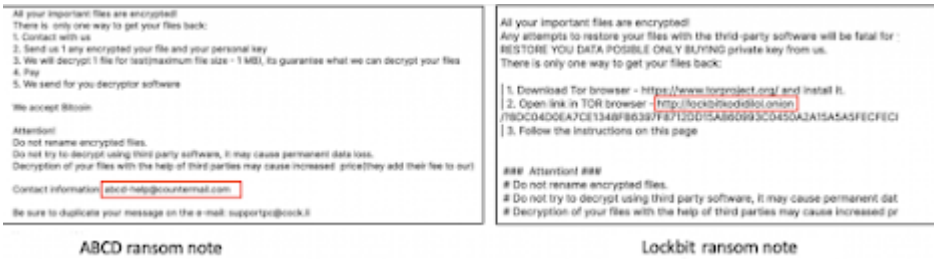
**Обновление от 30-31 декабря 2019:**

[Пост в Твиттере >>]

Новое название "**LockBit**".

Вымогатели обновили свой код, стали добавлять расширние .lockbit к зашифрованным файла и стали использовать название LockBit в записке о выкупе, отказавшись от почты с этим логином abcd.

Злоумышленник стали использовать свою собственную инфраструктуру для переговоров с жертвой.

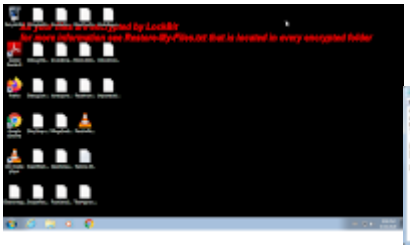



ABCD ransom note | Lockbit ransom note

Для сравнения записки старого и нового варианта.

Мы добавили новое название в заголовок статьи, т.к. в ID Ransomware для идентификации также стало использоваться это слово.

Была запущена RaaS LockBit**Обновление от 23-30 января 2020:**
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: **.lockbit**
Записка: Restore-My-Files.txt
Обход UAC: CMSTPLUA, ColorDataProxy, ICMCalibration
Раздел реестра: HKEY_CURRENT_USER\Software\LockBit
➤ Команда удаления теневых копий и путей восстановления:
C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
Файл: C:\Users\Admin\AppData\Local\Temp\Lockbit.exe
Результаты анализов: **VT** + **AR** + **AR** + **IA** + **IA** + **HA** + **VMR** + **TG**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.30886
Avast -> Win32:Fraudo [Trj]
BitDefender -> Gen:Heur.Ransom.Imps.1, Generic.Ransom.LockBit.91CBD888
ESET-NOD32 -> A Variant Of Win32/Filecoder.NXQ
Malwarebytes -> Ransom.LockBit
McAfee -> Ransom-Lkbit!889328E2CF5F
Microsoft -> Ransom:Win32/LokiBot!MSR
Rising -> Trojan.Crypto!8.364 (CLOUD)
TrendMicro -> Trojan.Win32.WACATAC.THABGBO, Ransom.Win32.LOCKBIT.A




➤ Содержание записки:
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:
| 1. Download Tor browser - hxxxs://www.torproject.org/ and install it.
| 2. Open link in TOR browser - hxxx://lockbitks2tvnmwk.onion/?D0407AC9D97C78CB9C256CA4731DB5D5

This link only works in Tor Browser!

| 3. Follow the instructions on this page

### Attention! ###

# Do not rename encrypted files.

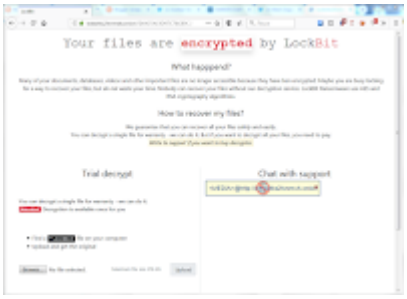
# Do not try to decrypt using third party software, it may cause permanent data loss.

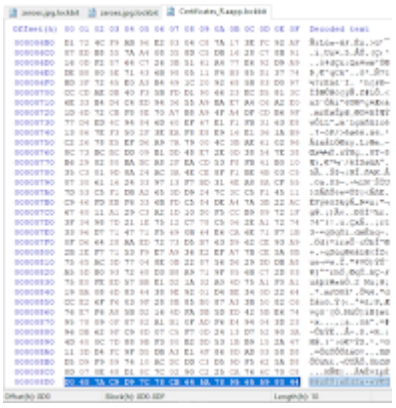
# Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

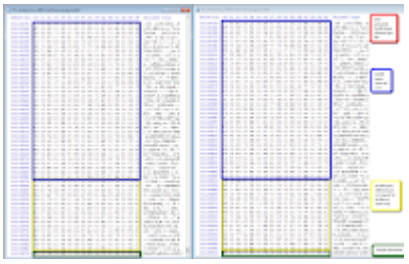
# Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org

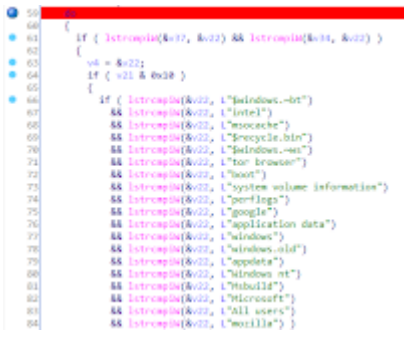
# Tor Browser user manual https://tb-manual.torproject.org/about

---








**Обновление от 2 февраля 2020:**

Расширение: .lockbit

Записка: Restore-My-Files.txt

Результаты анализа: **VT** + **AR**

Обнаружения:

DrWeb -> Trojan.Encoder.30932

BitDefender -> Generic.Ransom.LockBit.82A7AF3B

ESET-NOD32 -> A Variant Of Win32/Filecoder.Lockbit.B

Microsoft -> Ransom:Win32/LockBit.PA!MTB

TrendMicro -> Ransom.Win32.LOCKBIT.SMDS

**Обновление от 6 февраля 2020:**

Расширение: **.abcd**

Записка: Restore-My-Files.txt

Email: pcabcd@countermail.com, recoverymanager@cock.li


All your important files are encrypted!
There is  only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased  price(they add their fee to our)

Contact information: pcabcd@countermail.com

Be sure to duplicate your message on the e-mail: recoverymanager@cock.li

Your personal id:

➤ Содержание записки:

All your important files are encrypted!

There is  only one way to get your files back:

1. Contact with us

2. Send us 1 any encrypted your file and your personal key

3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files

4. Pay

5. We send for you decryptor software

We accept Bitcoin

Attention!

Do not rename encrypted files.

Do not try to decrypt using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased  price(they add their fee to our)
Contact information: pcabcd@countermail.com
Be sure to duplicate your message on the e-mail: recoverymanager@cock.li
Your personal id:
*** [всего 1708 знаков]

**Обновление от 14 февраля 2020:**

Расширение: .lockbit

Записка: Restore-My-Files.txt

Результаты анализа: **VT** + **AR** + **IA**

Обнаружения:

BitDefender -> Generic.Ransom.LockBit.91CBD888

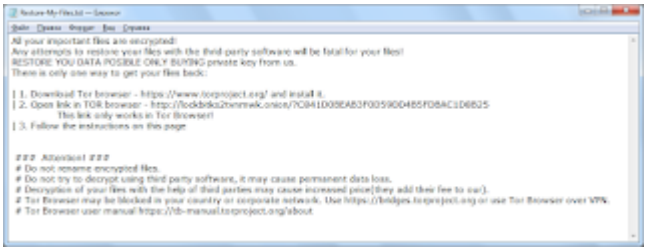
DrWeb -> Trojan.Encoder.30886

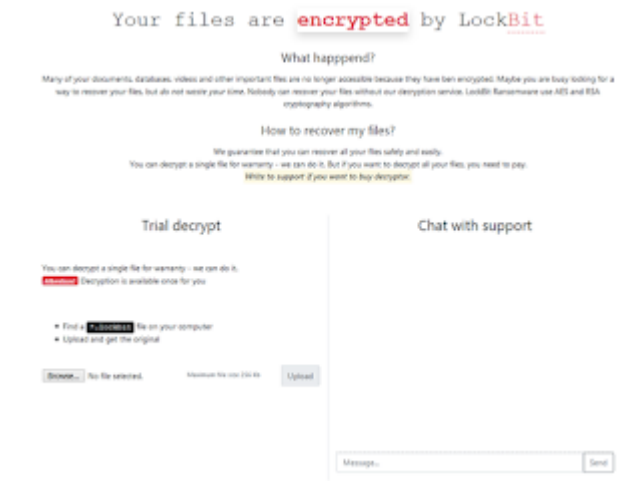
ESET-NOD32 -> A Variant Of Win32/Filecoder.Lockbit.B

Microsoft -> Ransom:Win32/LokiBot!MSR

TrendMicro -> Ransom.Win32.LOCKBIT.SMDS

**Обновление от 14 февраля 2020:**
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: **.lockbit**
Записка: Restore-My-Files.txt
Tor-URL: hxxx://lockbitks2tvnmwk.onion/*
Файл: sh1.exe
Использует сертификат от Sectigo.
Результаты анализов: **VT** + **AR**






**Обновление от 24 марта 2020:**

Расширение: .lockbit

Записка: Restore-My-Files.txt

Результаты анализов: **VT** + **VMR**

**Обновление от 4 апреля 2020:**

Расширение: .lockbit

Записка: Restore-My-Files.txt


➤ Содержание записки:

All your important files are encrypted!

Any attempts to restore your files with the thrid-party software will be fatal for your files!

RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.

There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install it.

| 2. Open link in TOR browser - hxxx://lockbitks2tvnmwk.onion/?962823C4EBE6623DCA2071AC9B8BA4BD

This link only works in Tor Browser!

| 3. Follow the instructions on this page

### Attention! ###

# Do not rename encrypted files.

# Do not try to decrypt using third party software, it may cause permanent data loss.

# Decryption of your files with the help of third parties may cause increased price(they add their fee to our).

# Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.

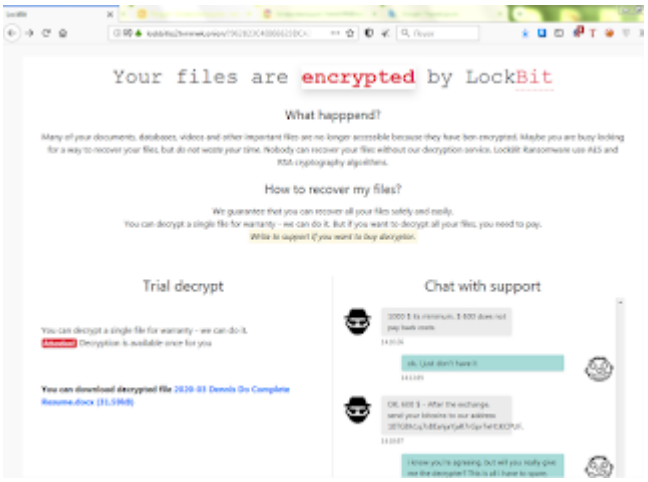
# Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.

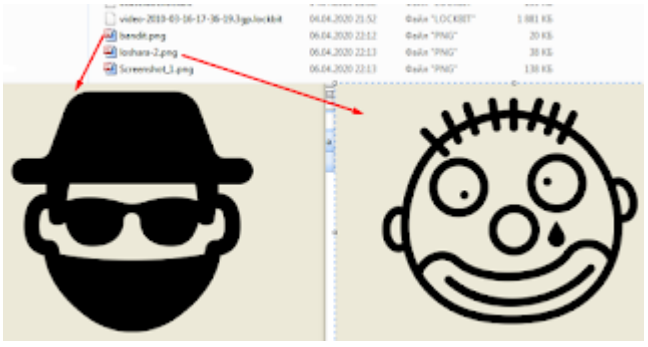
Don't forget about GDPR.

---

Содержание сайта, открываемого по ссылке:
xxxx://lockbitks2tvnmwk.onion/?962823C4EBE6623DCA2071AC9B8BA4BD




Две картинки из чата с характерными названиями.

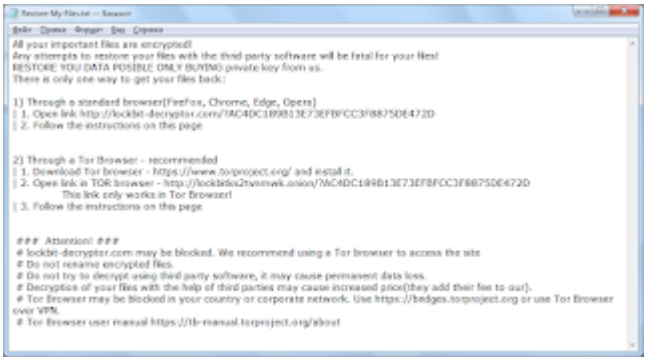


**Обновление от 10-13 мая 2020:**

Пост в Твиттере >>

Расширение: .lockbit

Записка: Restore-My-Files.txt




URL: xxxx://lockbit-decryptor.com/***

Tor-URL: xxxx://lockbitks2tvnmwk.onion/***

Также используется изображение, заменяющее обои Рабочего стола.



Результаты анализов: **VT** + **HA** + **IA** + **AR**

➤ Обнаружения:

DrWeb -> Trojan.Encoder.31783

BitDefender -> Trojan.GenericKD.33815280

ESET-NOD32 -> A Variant Of Win32/Kryptik.HDGL

Malwarebytes -> Ransom.LockBit

TrendMicro -> TROJ_GEN.R011C0WEB20

**Обновление от 12 мая 2020:**

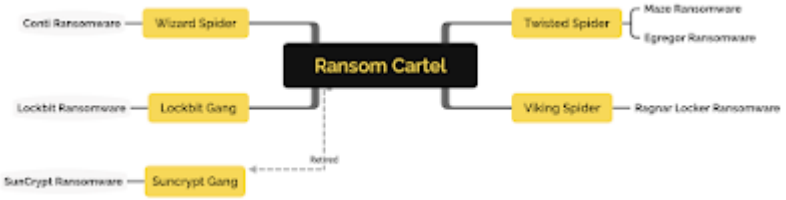
Идентифицируется как Lock2Bits

Расширение: **.lock2bits**

Записки и зашифрованные форматы файлов LockBit и Lock2Bit отличаются.

**Обновление июня 2020:**

В июне 2020 года LockBit и четыре другие банды вымогателей объявили о новом партнерстве с целью создания первого в мире картеля вымогателей - Ransom Cartel.



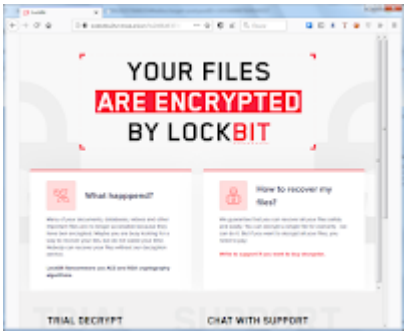

Позже стало известно, что эти группы сотрудничали и делились между собой некоторыми ресурсами, такими как данные о жертвах и инфраструктура. Например, группа LockBit делилась украденными данными жертв с Twisted Spider, который руководил операциями по вымогательству Maze & Egregor. Так Twisted Spider разместил данные одной из жертв LockBit на своем сайте утечки, чтобы еще больше оказать давление на жертву. Группы также поделились тактикой. Например, Twisted Spider — первая группа вымогателей, похитившая конфиденциальные данные и использующая их для повторного вымогательства. LockBit был одним из первых, кто применил эту тактику и использовал ее в своих собственных атаках. Вполне возможно, что LockBit первыми применили шифрование MBR в дополнение к системным данным в своих атаках. LockBit даже взял аспекты дизайна из разработки кода, первоначально использованного в программе-вымогателе Twisted Spider Egregor, например, уникальные методы антианализа, интегрированные в их полезную нагрузку. Но вполне возможно, что эти 5 групп лишь использовали картель как самопиар, чтобы повысить свою криминальную репутацию и получить известность. В настоящим картеле должны быть два основных компонента: лидерство и деньги. У данного Ransom Cartel этого не было. Они зарабатывали много денег, но между ними не было модели распределения доходов. Вместо этого каждый оставлял себе деньги, которые вымогал, и делился только доходом в рамках своей операции.

**Обновление от 22 июля 2020 или раньше:**

Пост на форуме >>

Расширение: .lockbit

Записка: Restore-My-Files.txt




➤ Содержание записки:

All your important files are encrypted!

Any attempts to restore your files with the thrid-party software will be fatal for your files!

RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.

There is only one way to get your files back:

1) Through a standard browser(FireFox, Chrome, Edge, Opera)

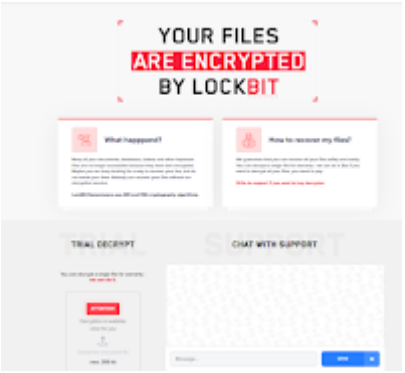
| 1. Open link hxxx://lockbit-decryptor.com/?A206EAF373BB05F8CAD0F191390CB897

| 2. Follow the instructions on this page
2) Through a Tor Browser - recommended
| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - hxxx://lockbitks2tvnmwk.onion/?A206EAF373BB05F8CAD0F191390CB897
This link only works in Tor Browser!
| 3. Follow the instructions on this page
### Attention! ###
# lockbit-decryptor.com may be blocked. We recommend using a Tor browser to access the site
# Do not rename encrypted files.
# Do not try to decrypt using third party software, it may cause permanent data loss.
# Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
# Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
# Tor Browser user manual https://tb-manual.torproject.org/about
---

**Обновление от 16 августа 2020:**

[Пост в Твиттере >>]

URL: hxxx://lockbit-decryptor.com/***
Tor-URL: hxxx://lockbitks2tvnmwk.onion/***
Результаты анализов: **VT** + **VT**



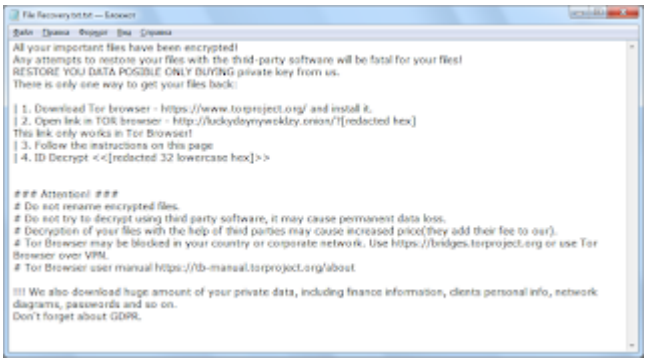

**Обновление от 5 ноября 2020:**

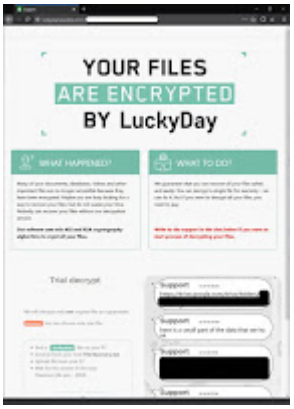
Lock2Bits переименовывается в LuckyDay.

Расширение: **.luckyday**

Записка: File Recovery.txt

Tor-URL: luckydaynywoklzy.onion



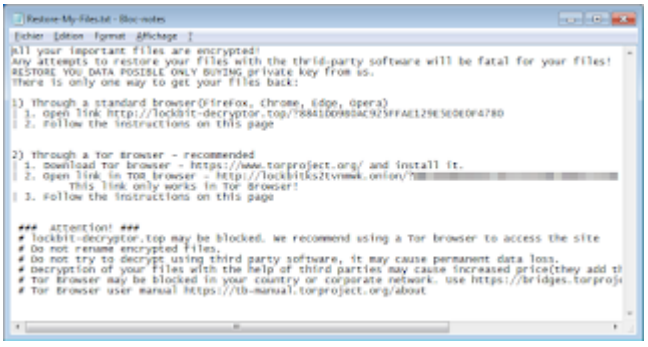




**Обновление от 17 ноября 2020:**

Расширение: .lockbit

Tor-URL: hxxx://lockbitks2tvnmwk.onion/*

Результаты анализов: **VT** + **IA**




**Вариант от 6 января 2021:**

**Вариант от 15 июля 2021** или раньше:

Версия: **LockBit 2.0** (LockBit Red)

Записка: Restore-My-Files.txt



Результаты анализов: **VT**

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34148

BitDefender -> Trojan.Generic.30034101

ESET-NOD32 -> Win32/Filecoder.Lockbit.E

Malwarebytes -> Ransom.LockBit

Microsoft -> Ransom:Win32/Lockbit.AA!MTB

Symantec -> Trojan.Gen.MBT

Tencent -> Win32.Trojan.Encoder.Hvte

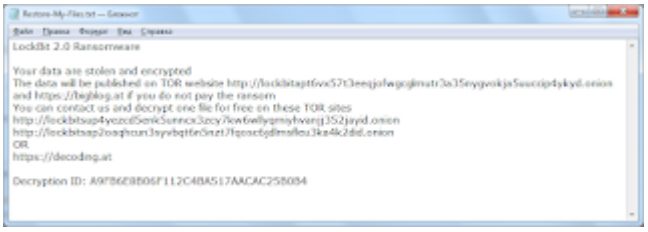
TrendMicro -> Ransom_Lockbit.R011C0DGH

**Вариант от 1 сентября 2021:**

**Вариант от 23 сентября 2021:**

LockBit 2.0 Ransomware

Записка: Restore-My-Files.txt




Результаты анализов: **VT** + **AR**

➤ Обнаружения:

DrWeb -> Trojan.Encoder.34248

ALYac -> Trojan.Ransom.LockBit

Avira (no cloud) -> TR/Crypt.XPACK.Gen

BitDefender -> Trojan.GenericKD.47129320

ESET-NOD32 -> A Variant Of Win32/Filecoder.Lockbit.E

Kaspersky -> HEUR:Trojan-Ransom.Win32.Lockbit.gen

Malwarebytes -> Ransom.LockBit

Microsoft -> Ransom:Win32/Lockbit.STA

Rising ->Ransom.LockBit!1.D854 (CLASSIC)

Symantec -> Ransom.Lockbit

TrendMicro -> Ransom.Win32.LOCKBIT.SMYEBGW

**26 октября 2021:**

Несколько цитат из этого интервью.

- Безупречная репутация - мы единственные, кто никогда никого не обманывал и не менял наш бренд. Нам доверяют.

- Нас не волнует, раскроет ли компания информацию об атаке.

- Иногда гораздо важнее украсть ценную информацию, за неразглашение которой компания готова платить больше, чем за расшифровку.

- Начать партнерскую программу легко, но держать ее открытой - это искусство.

- Мы не атакуем больницы, было несколько случаев, когда филиалы по ошибке зашифровывали стоматологические кабинеты и дома престарелых. Ключи расшифровки были выданы бесплатно.

- Встречи президентов ни на что не повлияют, все, кто серьезно работает, не живут в США или России. Лично я живу в Китае и чувствую себя в полной безопасности.

- Ни один партнер не пойдет против нашей воли, потому что мы работаем только с проверенными людьми, у которых есть кодекс чести, каждый из наших партнеров несет ответственность за свои слова и действия.

- Никто не застрахован от взлома инфраструктуры с помощью 0-days. Используя аппаратные бэкдоры АНБ, можно получить доступ к любому серверу на планете. Поэтому всегда присутствует риск быть взломанным.

- Наш путь труден и далек, мой биткойн стремится на восток. Покажите мне хотя бы одного китайца, который будет слушать, что ему говорят США, и не принимать от нас криптовалюту при обмене на наличные доллары в Гонконге.

- Нет компаний без денег, есть хитрые компании, которые не хотят тратить деньги на защиту своей сети, платить зарплату хорошим системным администраторам, а потом и на выкуп.

**=== 2022 ===**

**Обновление от 15 марта 2022:**

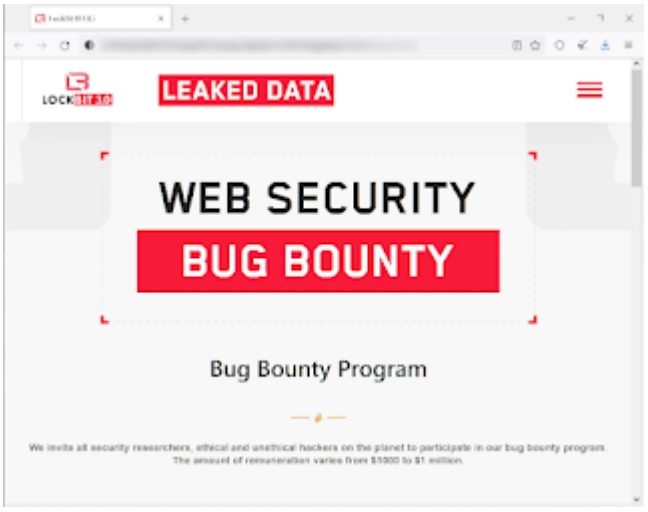
Новая версия: **LockBit 3.0** (LockBit Black)

Должны быть исправлены ошибки шифрования в базах данных MSSQL, которое могло повредить файлы MSSQL.

**Новость от 27 июня 2022:**

Дальнейшее развитие LockBit 3.0 (LockBit Black)

```
>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our
reputation. We are not a politically motivated group and we want nothing more than money. If you pay,
we will provide you with decryption software and destroy the stolen data. After you pay the ransom,
you will quickly make even more money. Treat this situation simply as a paid training for your system
administrators, because it is due to your corporate network not being properly configured that we were
able to attack you. Our pentest services should be paid just like you pay the salaries of your system
administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after
you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's
twitter https://twitter.com/hashtag/lockbit?f=live
```




Вероятно, LockBit 3.0 основан на коде BlackMatter.

➤ Ключи реестра:

HKCR\ .<Malware Extension> (Default) <Malware Extension>

HKCR\<Malware Extension>\DefaultIcon (Default) C:\ProgramData\<Malware Extension>.ico

HKCU\Control Panel\Desktop\WallPaper (Default) C:\ProgramData\<Mal ware Extension>.bmp

➤ Расположение:

ADMIN$\Temp\<LockBit3.0 Filename>.exe

%SystemRoot%\Temp\<LockBit3.0 Filename>.exe

\<Domain Name>\sysvol\<Domain Name>\scripts\<Lockbit 3.0 Filename>.exe (Domain Controller)

**Варианты июля 2022:**

Результаты анализа: **VT** + **AR** / **VT** + **TG**

**Вариант от 25 сентября 2022 или раньше:**

Сообщение: twitter.com/malwrhunterteam/status/1574260677597925376

LockBit 3.0 builder: BL00DY RANSOMWARE GANG

**=== 2023 ===**

**Подробная статья о LockBit от Jon DiMaggio - январь 2023**:

Ссылка на статью: hxxxs://analyst1.com/ransomware-diaries-volume-1/

**Новость от 7 февраля 2023:**

LockBit заявила о кибератаке на британскую службу доставки почты Royal Mail и вынудила компанию приостановить свои международные службы доставки из-за "серьезного сбоя в обслуживании".

**Отчет от 16 марта 2023:**

**=== 2024 ===**

**Новость от 19 февраля 2024:**

Правоохранительные органы 10 стран в рамках совместной операции, известной как «Операция Кронос» сорвали вымогательство с использованием LockBit 3.0 Black Ransomware. Это помогло изъять 2500 ключей и создать бесплатный дешифровщик.

**Новость от 22 февраля 2024:**

Разработчики программы-вымогателя LockBit тайно создавали новую версию своего вредоносного ПО для шифрования файлов, получившего название LockBit-NG-Dev, которое могло стать LockBit 4.0, когда в начале этой недели правоохранительные органы уничтожили инфраструктуру киберпреступника.

**Новость от 5 июня 2024:**

ФБР обнаружило 7000 ключей LockBit и призывает жертв LockBit 3.0 Ransomware связаться с ними.

**Варианты июня 2024:**

Свое название: PC Locker 3.0 by Mr.Robot

Вероятно на основе Lockbit 3.0 Black или модифицированный.

Расширение (пример): **.3R9qG8i3Z**

Записка (пример): 3R9qG8i3Z.README.txt

Telegram: @mr_robot_unlock

➤ Содержание записки:

~~~ PC Locker 3.0 by Mr.Robot~~~

>>>> Your data are stolen and encrypted

To get your files back you will have to pay a one-time fee of $45 in bitcoin or monero.

>>>> You need contact us and decrypt one file for free on these platforms with your personal DECRYPTION ID

Contact the following account on telegram

@mr_robot_unlock

or paste this link in your browser

hxxxs://t.me/mr_robot_unlock

>>>> Your personal DECRYPTION ID: ***

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom you will not receive you files NO EXCEPTIONS!

>>>> Warning! Any attempt to negotiate or you don't want to pay is INSTANT BLOCK!

>>>> Advertisement

Would you like to earn thousands of dollars $$$ ?

We sell mentorship for stealers, DDOS and ransomware.

We only work with professionals and people with money DO NOT WASTE OUR TIME.

**Новости июля 2024:**

В суде США двое человек из группы, распространявшей LockBit Ransomware признали себя виновными.

**Новость от 20 декабря 2024:**

Арестован и обвинен в содействии распространению LockBit Ransomware еще один россиянин-израильтянин, укрывавшийся в Израиле.

**Вариант от 20 декабря 2024:**

Самоназвание: LockBit 4.0 Ransomware

Сообщение:  x.com/fbgwls245/status/1870365719633985663

Сообщение: x.com/JAMESWT_MHT/status/1870368458128417254

Расширение: .<random>
~~~

Записка: Restore-My-Files.txt

Образец 32bit: C5CC3C5CEF6B382568A54F579B2965FF

Обнаружения:

DrWeb -> Trojan.Encoder.41387

ESET-NOD32 -> A Variant Of Win32/Filecoder.OSE

Malwarebytes -> Ransom.LockBit

Microsoft -> Ransom:Win32/LockBit

TrendMicro -> Ransom.Win32.LOCKBIT.YXFCXZ

---

Образец 64bit: 8FF61E4156C10B085E0C2233F24E8501

Обнаружения:

DrWeb -> Trojan.MulDrop28.53639

ESET-NOD32 -> Win64/Filecoder.Lockbit.C

Malwarebytes -> Ransom.LockBit

Microsoft -> Ransom:Win64/LockBit.M

TrendMicro -> Ransom.Win64.LOCKBIT.YXFAITTT

**=== 2025 ===**

**Вариант от 14 сентября 2025:**

LockBit 5.0 Ransomware Windows version

Расширение: **.[a-z0-9]{16}**

Записка: ReadMeForDecrypt.txt

MD5: 95daa771a28eaed76eb01e1e8f403f7c

SHA-1: cdd5717fd3bfd375c1c34237c24073e92ad6dccc

SHA-256: 7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82

Vhash: 075056657d15151"z

Обнаружения:

DrWeb -> Trojan.Encoder.43303

BitDefender -> Application.Generic.4156615

ESET-NOD32 -> Win64/Injector.ADW Trojan

Kaspersky -> HEUR:Trojan-Ransom.Win32.Lockbit.pef

Malwarebytes -> Malware.AI.3399155910

Microsoft -> Ransom:Win64/LockBit.MZZ!MTB

Tencent -> Malware.Win32.Gencirc.10c3f20b

TrendMicro -> Ransom.Win64.LOCKBIT.YXFIOZ

---

**Вариант от 20 сентября 2025:**

LockBit 5.0 Ransomware Linux version

MD5: ca93d47bcc55e2e1bd4a679afc8e2e25

SHA-1: 41e1e094c19fffde494c24ef4cab0d7577d5a025

SHA-256: 4dc06ecee904b9165fa699b026045c1b6408cc7061df3d2a7bc2b7b4f0879f4d

Vhash: 05495cf416374fc4db17277993080d5d


Обнаружения:

BitDefender -> Trojan.Linux.Ransom.38926740

DrWeb -> Linux.Encoder.617

ESET-NOD32 -> Linux/Filecoder.Lockbit.H Trojan

Kaspersky -> HEUR:Trojan-Ransom.Linux.Lockbit.five

Microsoft -> Ransom:Linux/LockBit.G!MTB

Rising -> Ransom.Lockbit/Linux!8.1993E (CLOUD)

Tencent -> Malware.Linux.Generic.1c03f032

TrendMicro -> Ransom.Linux.LOCKBIT.THIBCBD

---

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


Read to links:
Tweet on Twitter: myTweet
ID Ransomware (1st ID as ABCD, 2nd ID as LockBit, Lock2Bits)
ID Ransomware (new ID: LockBit 3.0, Lockbit 4.0)
Write-up, Topic of Support
*

Adder later:
Description of LockBit by Albert Zsigovits (on April 7, 2020)
Write-up by Albert Zsigovits from Sophos (on April 24, 2020)

Write-up by TrendMicro (on February 8, 2022)
Reverse Engineering by ChuongDong (on March 19, 2022)

Внимание!
В некоторых случаях файлы можно дешифровать!
Рекомендую обратиться по этой ссылке к Demonslay335 >>

Дешифровщик для некоторых вариантов Lockbit 3.0 Ransomware
по ссылке на сайте NoMoreRansom >>


Thanks:
Andrew Ivanov (author)
Michael Gillespie, Vitali Kremez, Albert Zsigovits, Bitshadow
to the victims who sent the samples



---