Шифровальщики-вымогатели The Digest "Crypto-Ransomware"

id-ransomware.blogspot.com/search

ABCD, LockBit

ABCD Ransomware

LockBit, LockBit 2.0 Ransomware

Lock2Bits Ransomware

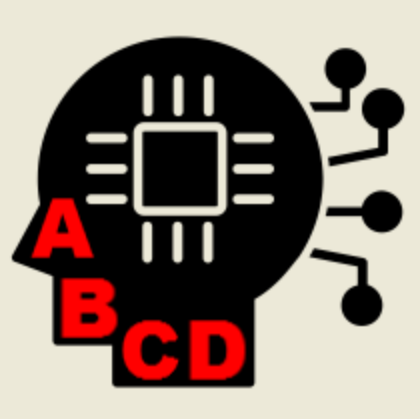
LuckyDay Ransomware

(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 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.

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



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.

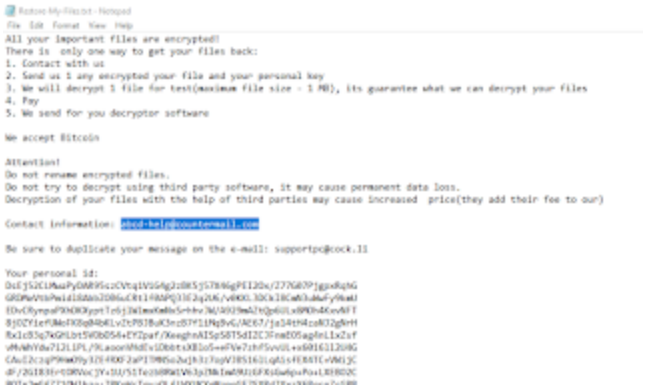
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

=== 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 >>
Откопали слово "**LockBit**".
Добавил это как второе название статьи, т.к. в ID Ransomware для идентификации также стало использоваться это слово.

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

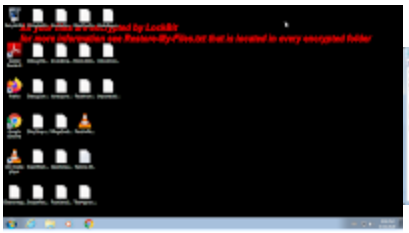
Malwarebytes -> Ransom.LockBit

McAfee -> Ransom-Lkbit!889328E2CF5F

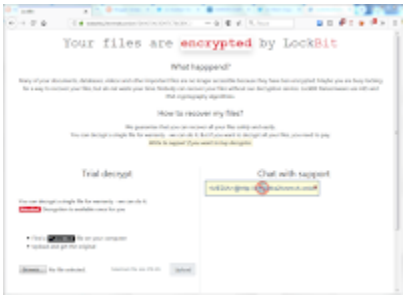
Microsoft -> Ransom:Win32/LokiBot!MSR

Rising -> Trojan.Crypto!8.364 (CLOUD)

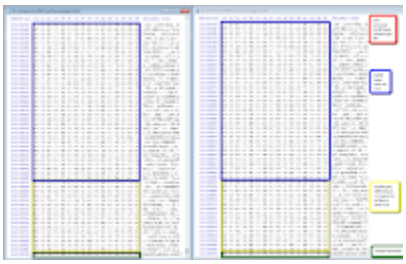
TrendMicro -> Trojan.Win32.WACATAC.THABGBO, Ransom.Win32.LOCKBIT.A




➤ 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
---





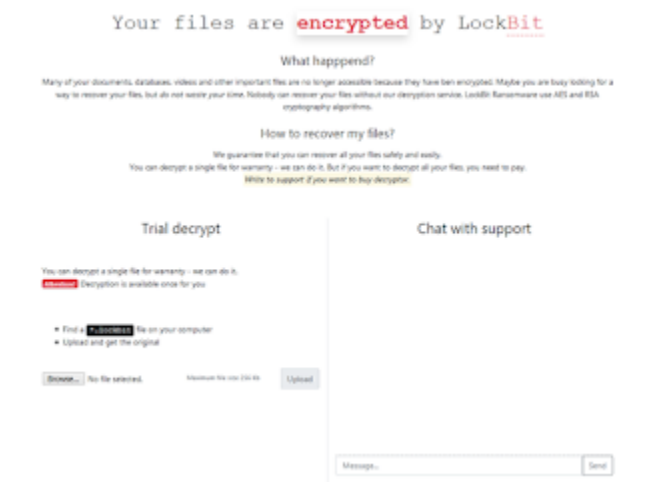


Обновление от 6 февраля 2020:
Расширение: **.abcd**
Записка: Restore-My-Files.txt
Email: pcabcd@countermail.com, recoverymanager@cock.li

➤ 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: 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:
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**

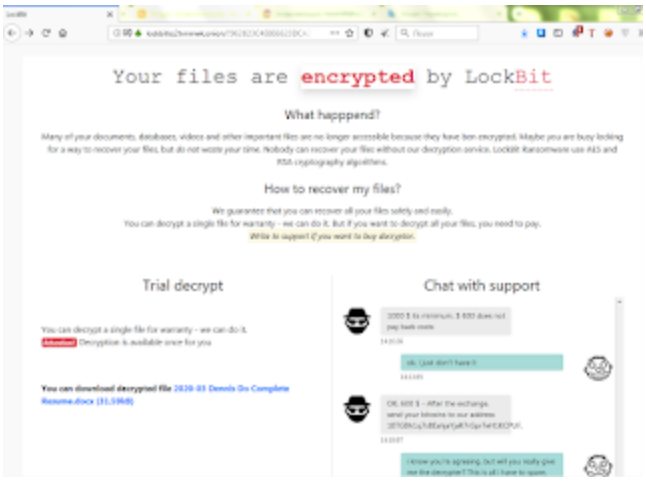


Обновление от 24 марта 2020:
Расширение: .lockbit
Записка: Restore-My-Files.txt
Результаты анализов: **VT** + **VMR**

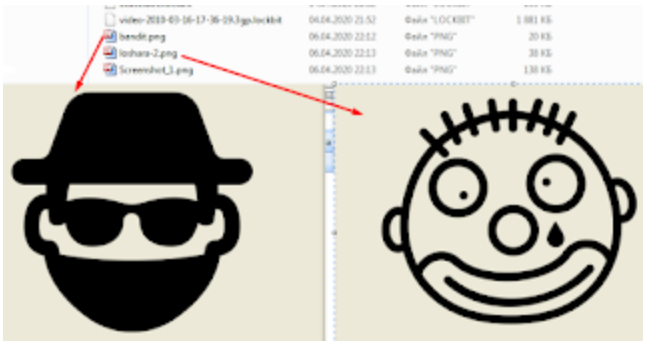
Обновление от 4 апреля 2020:
Расширение: .lockbit
Записка: Restore-My-Files.txt

➤ 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.

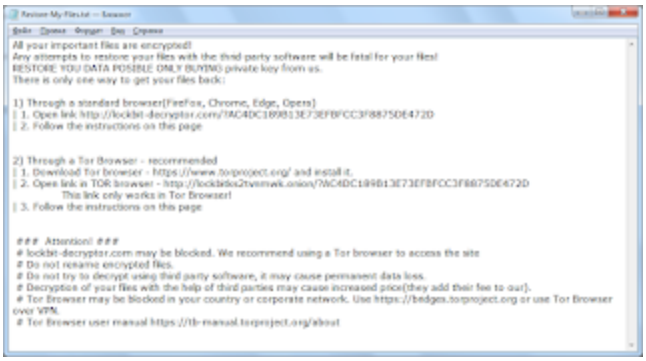
Содержание сайта, открываемого по ссылке:
xxxx://lockbitks2tvnmwk.onion/?962823C4EBE6623DCA2071AC9B8BA4BD



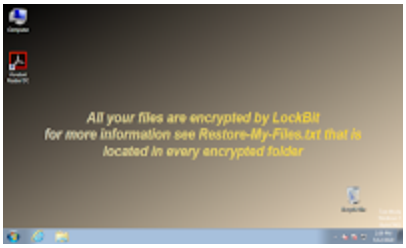
Две картинки из чата с характерными названиями.



Обновление от 10-13 мая 2020:
Пост в Твиттере >>
Расширение: .lockbit
Записка: Restore-My-Files.txt



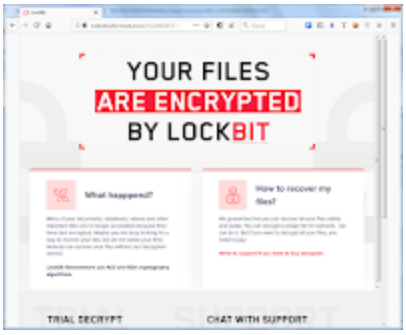
URL: xxxx://lockbit-decryptor.com/***
Tor-URL: xxxx://lockbitks2tvnmwk.onion/***
Также используется изображение, заменяющее обои Рабочего стола.



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.

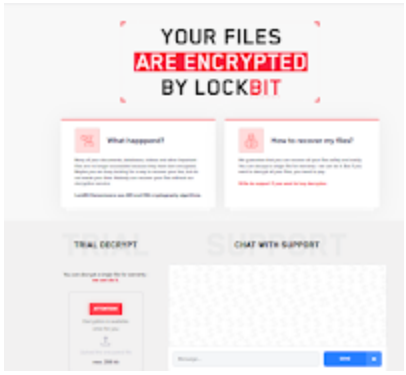
Обновление от 22 июля 2020 или раньше:
Пост на форуме >>
Расширение: .lockbit
Записка: Restore-My-Files.txt



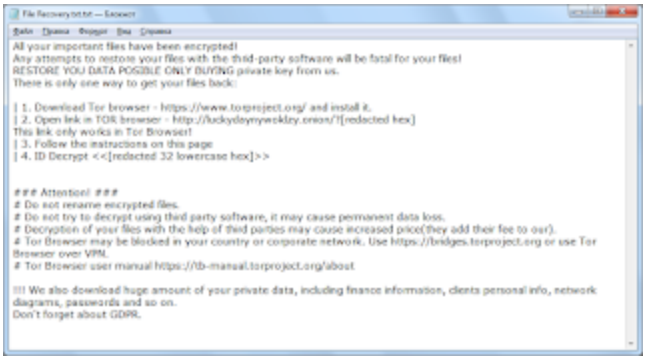
➤ Содержание записки:
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:
1) Through a standard browser(FireFox, Chrome, 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
---

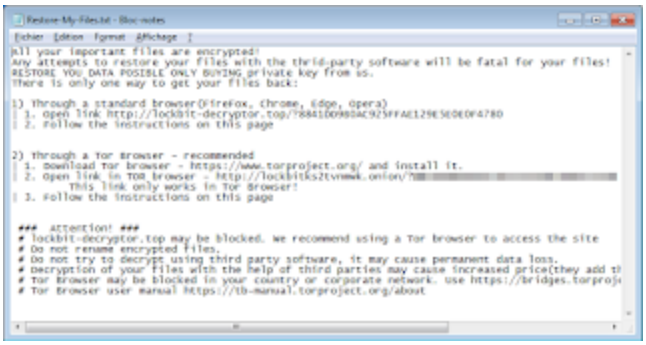
Обновление от 16 августа 2020:
Пост в Твиттере >>
URL: hxxx://lockbit-decryptor.com/***
Tor-URL: hxxx://lockbitks2tvnmwk.onion/***
Результаты анализов: **VT** + **VT**



Обновление от 5 ноября 2020:
Пост в Твиттере >>
Lock2Bits переименовывается в LuckyDay.
Расширение: **.luckyday**
Записка: File Recovery.txt
Tor-URL: luckydaynywoklzy.onion



Обновление от 17 ноября 2020:
Пост в Твиттере >>
Расширение: .lockbit
Tor-URL: hxxx://lockbitks2tvnmwk.onion/*
Результаты анализов: **VT** + **IA**



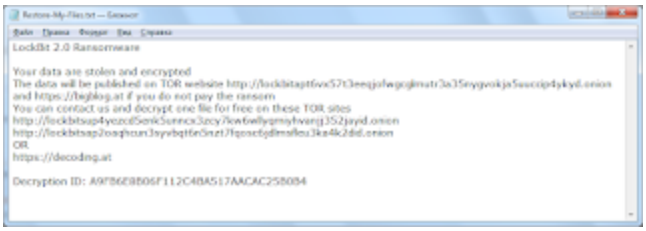
Вариант от 6 января 2021:
Сообщение >>

Вариант от 15 июля 2021:
Сообщение >>
Версия: LockBit 2.0
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:
Статья на сайте BleepingComputer >>

Вариант от 23 сентября 2021:
Сообщение >>
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:
Интервью с представителем LockBit >>
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.
Должны быть исправлены ошибки шифрования в базах данных MSSQL, которое могло повредить файлы MSSQL.
Статья об этом >>

=== 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)
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 >>

Thanks:

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

LockFile

LockFile Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует связаться через UTox, что узнать, как заплатить выкуп и вернуть файлы.
Оригинальное название: LockFile. Чёткий образец не предоставлен.

Обнаружения:
DrWeb -> Trojan.Encoder.34276
BitDefender -> Trojan.GenericKD.37457318
ESET-NOD32 -> A Variant Of Win64/Filecoder.LockFile.A
Kaspersky -> Trojan-Ransom.Win64.LockFile.a
Malwarebytes -> Ransom.LockFile
Microsoft -> Trojan:MSIL/Cryptor
Symantec -> Ransom.Lockfile

Tencent -> Win32.Trojan.Genericcryptor.Swur
TrendMicro -> Ransom.Win64.LOCKFILE.A

© Генеалогия: ✂ LockBit >> LockFile

Сайт "ID Ransomware" это идентифицирует как LockFile.

Информация для идентификации

Активность этого крипто-вымогателя была замечена в США 20 июля 2021 г., однако специалисты сообщили о нем только 20 августа 2021. Ориентирован на англоязычных пользователей, может распространяться по всему миру. Атаки LockFile были зарегистрированы в основном в США и странах Азии, а их жертвами стали как минимум 10 организаций из следующих секторов: финансовые услуги, производство, машиностроение, юриспруденция, бизнес-услуги, путешествия и туризм.

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

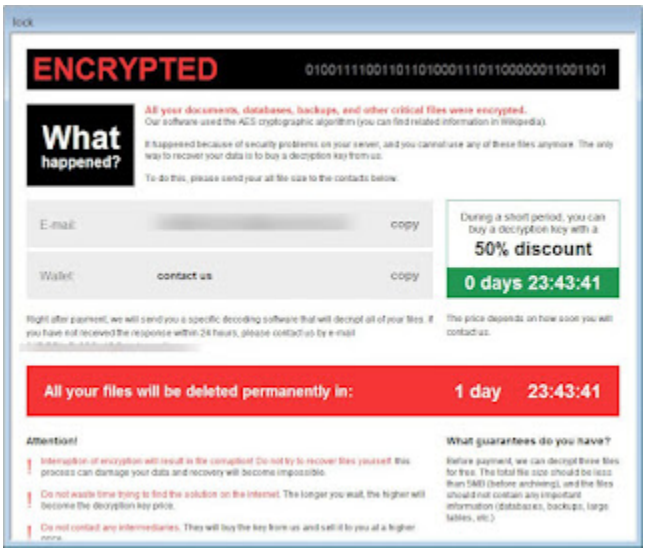
Записка с требованием выкупа в июле 2021 называлась: **LOCKFILE-README.hta**

На реальных ПК записка, видимо, имела форму:
[victim_name]-LOCKFILE-README.hta

Сообщается, что в других случаях при формирования названия записки использовался шаблон:
LOCKFILE-README-#COMPUTER#-#TIME#.hta

Пример на атакованном ПК:
LOCKFILE-README-XC64ZB-1629866461.hta

В другом варианте при формирования названия записки использовался шаблон:
LOCKFILE-FILE-#COMPUTER#-#TIME#.hta



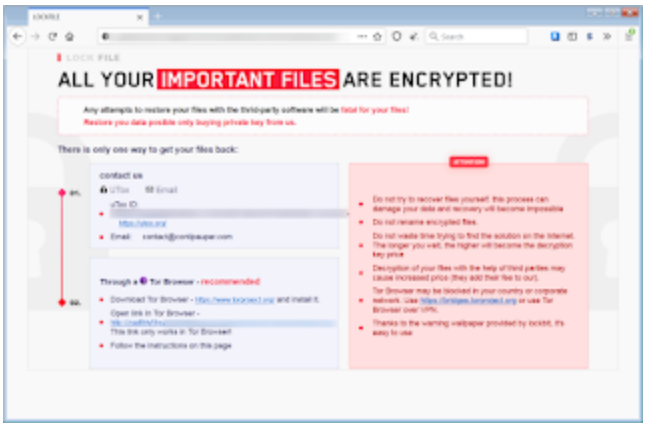
Содержание записки (часть текста):
ENCRYPTED
What happened?
All your documents, databases, backups, and other critical files were encrypted.
Our software used the AES cryptographic algorithm (you can find related information in Wikipedia).
It happened because of security problems on your server, and you cannot use any of these files anymore. The only
way to recover your data is to buy a decryption key from us.
To do this, please send your all file size to the contacts below.
E-mail: ***
Wallet: contact us
***

Эта HTA-записка очень похожа на ту, что используется в **CryLock Ransomware** с версии 2.0 (с июля 2020 года).

Но на момент написания статьи сообщается, что в августе 2021 используется название по шаблону:

[victim_name]-LOCKFILE-README.hta

В отчете исследователей есть скриншот более новой записки вымогателей, на котором Tor-адрес указан неполностью.



Примерно с мая 2020 года вымогатели из **LockBit Ransomware** использовали похожий на вид сайт. Возможно, что вымогатели из LockFile Ransomware используют их шаблон записки или как-то связаны с этой группой вымогателей.

Содержание текста о выкупе:

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:
---
01. contact us UTox Email
uTox ID: ***
hxxxs://utox.org/
Email: contact@contipauper.com
---
02. Through a Tor Browser - recommended
Download Tor Browser - hxxxs://www.torproiect.org/ and install it.
Open link in Tor Browser - hxxx://zqaflhty5hyz***
This link only works in Tor Browser!
Follow the instructions on this page

ATTENTION!
Do not try to recover files yourself, this process can damage your data and recovery will become impossible
Do not rename encrypted files.
Do not waste time trying to find the solution on the Internet.
The longer you wait, the higher will become the decryption key price

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 hxxxs://bridges.torproject.org or use Tor
Browser over VPN.
Thanks to the warning wallpaper provided by lockbit, it's easy to use

Перевод текста на русский язык:
ВСЕ ВАШИ ВАЖНЫЕ ФАЙЛЫ ЗАШИФРОВАНЫ!

Любые попытки восстановить ваши файлы с помощью сторонних программ будут фатальными для ваших файлов!
Восстановить свои данные возможно только купив у нас приватный ключ.

Есть только один способ вернуть ваши файлы:
---
01. свяжитесь с нами по UTox Email
uTox ID: ***
hxxxs://utox.org/
Email: contact@contipauper.com
---
02. Через Tor браузер - рекомендуется
Загрузите Tor браузер - hxxxs://www.torproiect.org/ и установите его.
Открыть ссылку в Tor браузере - hxxx://zqaflhty5hyz***
Эта ссылка работает только в Tor браузере!
Следуйте инструкциям на этой странице

ВНИМАНИЕ!
Не пытайтесь восстановить файлы сами, этот процесс может повредить ваши данные и восстановление станет невозможным.
Не переименовывайте зашифрованные файлы.
Не тратьте время на поиски решения в Интернете.
Чем дольше вы ждете, тем выше станет цена ключа дешифрования.
Расшифровка ваших файлов с помощью третьих лиц может привести к удорожанию (они добавляют свою цену к нашей).
Браузер Tor может быть заблокирован в вашей стране или в корпоративной сети.
Используйте hxxxs://bridges.torproject.org или используйте браузер Tor через VPN.
Благодаря предупреждающим обоям, предоставленным lockbit, им легко пользоваться

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Могут быть различия с первым вариантом.

Технические детали + IOC

Первоначальный доступ к сети осуществляется с помощью атаки ProxyShell на серверы Microsoft Exchange, эксплуатируя найденные недавно уязвимости (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). Затем злоумышленники захватывают контроллер домена организации, используя новый эксплойт PetitPotam, который под контролемLockFile принудительно выполняет аутентификацию на удаленном NTLM-реле. PetitPotam имеет несколько вариантов. На момент написания статьи официальные средства защиты и обновления Microsoft пока еще не полностью блокируют вектор атаки PetitPotam. Злоумышленники, стоящие за LockFile, полагаются на общедоступный код для использования исходного варианта PetitPotam (CVE-2021-36942).

При эксплуатации уязвимости злоумышленники используют технологию **PowerShell**, которую сами Microsoft уже много лет продвигают в своих ОС Windows как легитимную и полезную.

Злоумышленники сохраняют доступ к пострадавшей сети жертвы как минимум в течение нескольких дней от начала атаки LockFile Ransomware.

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**.

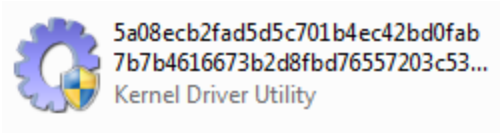
➤ Согласно исследованиям специалистов BleepingComputer этот LockFile Ransomware довольно тяжеловат для компьютеров, занимает много ресурсов и подвешивает систему.

Список типов файлов, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Пропускаемые файлы и папки, содержат следующие подстроки:
Windows, NTUSER, LOCKFILE, .lockfile

Пропускаемые типы файлов / расширения:
.exe, .jpg, .bmp, .gif, .lockfile

Файлы, связанные с этим Ransomware:
LOCKFILE-README.hta - файл с требованием выкупа;
[victim_name]-LOCKFILE-README.hta - файл с требованием выкупа;
active_desktop_render.dll - первичный вредоносный файл;
active_desktop_launcher.exe - первичный вредоносный файл;
autoupdate.exe - вредоносный файл, уникальный для каждой жертвы;
EfsPotato.exe - вредоносный файл, который использует PetitPotam;
autologin.bat - вредоносный командный файл для запуска;
autologin.exe (Hamakaze.exe) - название файла из KDU toolkit;
autologin.dll (Tanikaze.dll) - название файла из KDU toolkit;
autologin.sys - название файла из KDU toolkit;
KDU toolkit - набор инструментов Kernel Driver Utility.



Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
IP: 209.14.0.234
Tor-URL: hxxx://zqaflhty5hyz***

Email: contact@contipauper.com
UTox: скрыт

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:
IOC: **VT**, **HA**, **IA**, **TG**, AR, VMR, **JSB**

ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b62291 - active_desktop_render.dll
cafe54e85c539671c94abdeb4b8adbef3bde8655006003088760d04a86b5f915 - autoupdate.exe
36e8bb8719a619b78862907fd49445750371f40945fefd55a9862465dc2930f9 - autologin.sys
5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c5340a0f - autologin.exe
1091643890918175dc751538043ea0743618ec7a5a980187855497003652 4b75 - autologin.dll
2a23fac4cfa697cc738d633ec00f3fbe93ba22d2498f14dea08983026fdf128a - autoupdate.exe
7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac6693dea1cdad5ef193b052fd - efspotato.exe
c020d16902bd5405d57ee4973eb25797087086e4f8079fac0fd8420c716ad153 - active_desktop_render.dll
a926fe9fc32e645bdde9656470c7cd005b21590cda222f72daf854de9ffc4fe0 - autoupdate.exe
368756bbcaba9563e1eef2ed2ce59046fb8e69fb305d50a6232b62690d33f690 - autologin.sys
d030d11482380ebf95aea030f308ac0e1cd091c673c7846c61c625bdf11e5c3a - autoupdate.exe
a0066b855dc93cf88f29158c9ffbbdca886a5d6642cbcb9e71e5c759ffe147f8 - autoupdate.exe
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce autoupdate.exe

Степень распространённости: **средняя**.
Информация дополняется. 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 ===

Внимание! Файлы можно расшифровать!

Ссылка на статью >>
Ссылка на дешифровщик >>

Thanks:

Symantec Threat Hunter Team, BleepingComputer,
Andrew Ivanov (article author), Michael Gillespie,
VirITeXplorer, JAMESWT_MHT, Avast
to the victims who sent the samples