

# How I Cracked CONTI Ransomware Group's Leaked Source Code ZIP File

By Wade Hickey

Published: 2022-03-05 · Archived: 2026-04-05 20:03:52 UTC



Mar 1, 2022

1. Leaker posted full zip with password



2. Leaker posted zip without locker without password



3. Grab some known plaintext from the second, and you can crack the first with bkcrack.

Press enter or click to view image in full size

```
(kali@kali) - [~]
└─$ printf "__DECRYPT_NOTE__" > lmao

(kali@kali) - [~]
└─$ xxd lmao
00000000: 5f5f 4445 4352 5950 545f 4e4f 5445 5f5f  __DECRYPT_NOTE__
```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux]
└─$ 7z a -mm=Deflate -mx9 lmao.zip lmao

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 9 5900HX with Radeon Graphics (A50F00),ASM,AES-NI)

Open archive: lmao.zip
--
Path = lmao.zip
Type = zip
Physical Size = 159

Scanning the drive:
1 file, 16 bytes (1 KiB)

Updating archive: lmao.zip

Items to compress: 1

Files read from disk: 1
Archive size: 158 bytes (1 KiB)
Everything is Ok
```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux]
└─$ ./bkcrack -C conti Locker v2.zip -c "contiLocker/R3ADM3.txt" -P lmao.zip -p lmao
bkcrack 1.3.4 - 2022-01-01
[10:42:58] Z reduction using 8 bytes of known plaintext
100.0 % ( 8 / 8)
[10:42:58] Attack on 748436 Z values at index 7
Keys: 2a45cf92 4521624b decd8163
19.0 % (142235 / 748436)
[10:48:16] Keys
2a45cf92 4521624b decd8163
```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux]
└─$ ./bkcrack -C contiLocker v2.zip -k 2a45cf92 4521624b decd8163 -U unlocked.zip password
bkcrack 1.3.4 - 2022-01-01
[10:57:29] Writing unlocked archive unlocked.zip with password "password"
100.0 % (199 / 199)
Wrote unlocked archive.
```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux/contiLocker/locker]
└─$ ls
antihook  cacha20  disks.cpp  global_parameters.cpp  hash.h  locker.vcxproj  logs.cpp  memory.cpp  MetaString.h  ntdll.h  queue.h  search.cpp
api.cpp   common.h  filesystem.h  global_parameters.h  locker.cpp  locker.vcxproj.filters  logs.h  memory.h  network_scanner.cpp  process_killer.cpp  R3ADM3.txt  threadpool.cpp
api.h     Debug    GetApi.h    hash.cpp          locker.h    locker.vcxproj.user  main.cpp  MetaRandom2.h  network_scanner.h  process_killer.h  Release    threadpool.h

(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux/contiLocker/locker]
└─$ ls -lah
total 489K
drwxr-xr-x 6 kali kali 4.0K Sep 15 2020 .
drwxr-xr-x 7 kali kali 4.0K Jan 27 09:25 ..
drwxr-xr-x 2 kali kali 4.0K Sep 15 2020 antihook
-rw-r--r-- 1 kali kali 14K Sep 15 2020 api.cpp
-rw-r--r-- 1 kali kali 69K Sep 15 2020 api.h
drwxr-xr-x 2 kali kali 4.0K Sep 15 2020 cacha20
-rw-r--r-- 1 kali kali 311 Sep 15 2020 common.h
drwxr-xr-x 3 kali kali 4.0K Sep 15 2020 Debug
-rw-r--r-- 1 kali kali 1015 Sep 15 2020 disks.cpp
-rw-r--r-- 1 kali kali 451 Sep 15 2020 filesystem.h
-rw-r--r-- 1 kali kali 96K Sep 15 2020 GetApi.h
-rw-r--r-- 1 kali kali 853 Sep 15 2020 global_parameters.cpp
-rw-r--r-- 1 kali kali 353 Sep 15 2020 global_parameters.h
-rw-r--r-- 1 kali kali 870 Sep 15 2020 hash.cpp
-rw-r--r-- 1 kali kali 85 Sep 15 2020 hash.h
-rw-r--r-- 1 kali kali 23K Sep 15 2020 locker.cpp
-rw-r--r-- 1 kali kali 807 Sep 15 2020 locker.h
-rw-r--r-- 1 kali kali 9.0K Sep 15 2020 locker.vcxproj
-rw-r--r-- 1 kali kali 6.7K Sep 15 2020 locker.vcxproj.filters
-rw-r--r-- 1 kali kali 165 Sep 15 2020 locker.vcxproj.user
-rw-r--r-- 1 kali kali 1.3K Sep 15 2020 logs.cpp
-rw-r--r-- 1 kali kali 119 Sep 15 2020 logs.h
-rw-r--r-- 1 kali kali 9.4K Sep 15 2020 main.cpp
-rw-r--r-- 1 kali kali 611 Sep 15 2020 memory.cpp
-rw-r--r-- 1 kali kali 166 Sep 15 2020 memory.h
-rw-r--r-- 1 kali kali 982 Sep 15 2020 MetaRandom2.h
-rw-r--r-- 1 kali kali 2.7K Sep 15 2020 MetaString.h
-rw-r--r-- 1 kali kali 15K Sep 15 2020 network_scanner.cpp
-rw-r--r-- 1 kali kali 370 Sep 15 2020 network_scanner.h
-rw-r--r-- 1 kali kali 92K Sep 15 2020 ntdll.h
-rw-r--r-- 1 kali kali 2.7K Sep 15 2020 process_killer.cpp
-rw-r--r-- 1 kali kali 307 Sep 15 2020 process_killer.h
-rw-r--r-- 1 kali kali 17K Sep 15 2020 queue.h
-rw-r--r-- 1 kali kali 16 Sep 15 2020 R3ADM3.txt
drwxr-xr-x 3 kali kali 4.0K Sep 15 2020 Release
-rw-r--r-- 1 kali kali 4.6K Sep 15 2020 search.cpp
-rw-r--r-- 1 kali kali 16K Sep 15 2020 threadpool.cpp
-rw-r--r-- 1 kali kali 930 Sep 15 2020 threadpool.h
```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux/conti_locker/locker]
└─$ cat filesystem.h
#pragma once
#include "common.h"
#include "queue.h"
#include "memory.h"

namespace filesystem {

    typedef struct drive_info_ {

        std::wstring RootPath;
        TAILQ_ENTRY(drive_info_) Entries;

    } DRIVE_INFO, *PDRIVE_INFO;

    typedef TAILQ_HEAD(drive_list_, drive_info_) DRIVE_LIST, * PDRIVE_LIST;

    INT EnumerateDrives(PDRIVE_LIST DriveList);
    VOID SearchFiles(std::wstring StartDirectory, INT ThreadPoolID);
    DWORD WINAPI StartLocalSearch(PVOID pArg);

}

```

4. Now let's crack the original password

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux]
└─$ ./bkcrack -k 2a45cf92 4521624b decd8163 -r 15 ?p

bkcrack 1.3.4 - 2022-01-01
[10:55:11] Recovering password
length 0-6...
length 7...
length 8...
length 9...
length 10...
length 11...
length 12...
length 13...
length 14...
7.7 % (693 / 9025)
[16:50:26] Password
as bytes: 27 3b 23 70 5d 65 28 64 3e c4 a8 3 dc 47
as text: ';#p]e(d>I0G

```

Press enter or click to view image in full size

```
(kali@kali) - [~/bkcrack/bkcrack-1.3.4-Linux]
$ unzip -P $(echo $'\x27\x3b\x23\x70\x5d\x65\x28\x64\x3e\xc4\xa8\x03\xdc\x47') conti_locker_v2.zip
Archive: conti_locker_v2.zip
  creating: conti_locker/
  inflating: conti_locker/ContiLocker_v2.sln
  creating: conti_locker/locker/
  inflating: conti_locker/locker/search.cpp
  inflating: conti_locker/locker/ntdll.h
  inflating: conti_locker/locker/locker.h
  inflating: conti_locker/locker/GetApi.h
  inflating: conti_locker/locker/memory.cpp
  creating: conti_locker/locker/antihook/
  extracting: conti_locker/locker/antihook/antihooks.h
  extracting: conti_locker/locker/antihook/CONTI.txt
  inflating: conti_locker/locker/antihook/antihooks.cpp
  inflating: conti_locker/locker/queue.h
  inflating: conti_locker/locker/locker.vcxproj.filters
  inflating: conti_locker/locker/common.h
  inflating: conti_locker/locker/network_scanner.cpp
  inflating: conti_locker/locker/filesystem.h
  inflating: conti_locker/locker/locker.cpp
  inflating: conti_locker/locker/disks.cpp
  inflating: conti_locker/locker/process_killer.h
  inflating: conti_locker/locker/logs.cpp
  inflating: conti_locker/locker/threadpool.cpp
  inflating: conti_locker/locker/locker.vcxproj.user
  inflating: conti_locker/locker/main.cpp
  creating: conti_locker/locker/chacha20/
```

VirusTotal:

[conti\\_locker\\_v2.zip](#)

[conti\\_locker.7z](#)

[unlocked\\_conti\\_leak.zip](#)

## Get Wade Hickey's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

It's amazing what the ransomware operators know about cryptography...