Quick Overview of Leaked LockBit 3.0 (Black) builder program

medium.com/s2wblog/quick-overview-of-leaked-lockbit-3-0-black-builder-program-880ae511d085

S2W

September 23, 2022

S2W

Sep 22

.

6 min read

Author: HuiSeong, Yang & Hyunsik, Jeong | S2W TALON

> *: Sep 22, 2022*

Photo by on

Executive Summary

- According to a from 3xp0rt, Ali Qushji was able to infiltrate LockBit's server and acquire the builder for the ransomware
- According to , Proton, one of the programmers for the LockBit ransomware group, mentioned that the builder was leaked,
- The ransomware group indirectly admitted that the allegations above are true, saying that nothing has been hacked and that they have fired the coder.
- LockBit 3.0 Builder leaked by Ali Kushii and Proton are both shared on .

Detailed Analysis

LockBit builder flowchart

1. Build.bat

`Build.bat` creates an RSA public/private key pair by executing `Keygen.exe`, and `Builder.exe` that generates a LockBit 3.0 ransomware using the generated key pair.

```
 /F /Q %cd%\Build\*.*  -path %cd%\Build -pubkey pub.key -privkey priv.key  -type dec
-privkey %cd%\Build\priv.key -config config.json -ofile %cd%\Build\LB3Decryptor.exe
-type enc -exe -pubkey %cd%\Build\pub.key -config config.json -ofile
%cd%\Build\LB3.exe  -type enc -exe -pass -pubkey %cd%\Build\pub.key -config
config.json -ofile %cd%\Build\LB3_pass.exe  -type enc -dll -pubkey %cd%\Build\pub.key
-config config.json -ofile %cd%\Build\LB3_Rundll32.dll  -type enc -dll -pass -pubkey
%cd%\Build\pub.key -config config.json -ofile %cd%\Build\LB3_Rundll32_pass.dll  -type
enc -ref -pubkey %cd%\Build\pub.key -config config.json -ofile
%cd%\Build\LB3_ReflectiveDll_DllMain.dll
```

Command line description
The list of files created after execution is as follows.

Files created after executing Build.bat

2. config.json

`config.json` is a JSON configuration file that contains the setting values to be used when generating LockBit 3.0 Encryptor and Decryptor.

- : Configuration about the bot feature stealing information from infected devices (Not used)
- : Configuration values that determine the behaviors for the LockBit 3.0 ransomware

Configuration description

- : List of folders to exclude from encryption
- : List of files to exclude from encryption
- : List of extensions to exclude from encryption
- : List of hostnames to exclude from encryption
- : List of processes to be terminated before encryption
- : List of services to be terminated before encryption
- : List of URLs to be used as the C2 server
- : List of credentials to be used for logon
- : Ransom note content

```
~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~>>>> Your data are stolen
and encryptedThe data will be published on TOR website if you do not pay the
ransomLinks for Tor
Browser:http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onionhttp://lc
 for the normal
browserhttp://lockbitapt.uzhttp://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy
 What guarantees that we will not deceive you?We are not a politically motivated
group and we do not need anything other than your money.If you pay, we will provide
you the programs for decryption and we will delete your data.Life is too short to be
sad. Be not sad, money, it is only paper.If we do not give you decrypters, or we do
not delete your data after payment, then nobody will pay us in the future.Therefore
to us our reputation is very important. We attack the companies worldwide and there
is no dissatisfied victim after payment.You can obtain information about us on
twitter https://twitter.com/hashtag/lockbit?f=live>>>> You need contact us and
decrypt one file for free on these TOR sites with your personal DECRYPTION IDDownload
and install TOR Browser https://www.torproject.org/Write to a chat and wait for the
answer, we will always answer you.Sometimes you will need to wait for our answer
because we attack many companies.Links for Tor
Browser:http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onionhttp://lc
 for the normal browserhttp://lockbitsupp.uzIf you do not get an answer in the chat
room for a long time, the site does not work and in any other emergency, you can
contact us in jabber or tox.Tox ID LockBitSupp:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7XMPP
(Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz>>>> Your
personal DECRYPTION ID: %s>>>> Warning! Do not DELETE or MODIFY any files, it can
lead to recovery problems!>>>> Warning! If you do not pay the ransom we will attack
your company repeatedly again!>>>> AdvertisementWould you like to earn millions of
dollars $$$ ?Our company acquire access to networks of various companies, as well as
insider information that can help you steal the most valuable data of any company.You
can provide us accounting data for the access to any company, for example, login and
password to RDP, VPN, corporate email, etc.Open our letter at your email. Launch the
provided virus on any computer in your company.You can do it both using your work
computer or the computer of any other employee in order to divert suspicion of being
in collusion with us.Companies pay us the foreclosure for the decryption of files and
prevention of data leak.You can contact us using Tox messenger without registration
and SMS https://tox.chat/download.html.Using Tox messenger, we will never know your
real name, it means your privacy is guaranteed.If you want to contact us, write in
jabber or tox.Tox ID LockBitSupp:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7XMPP
(Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.bizIf this
contact is expired, and we do not respond you, look for the relevant contact data on
our website via Tor or Brave browserLinks for Tor
Browser:http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onionhttp://lc
 for the normal
browserhttp://lockbitapt.uzhttp://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy
```

3. Builder.exe

`Builder.exe` is a tool to generate LockBit 3.0 Encryptor and Decryptor. Encryptor and Decryptor are embedded in the resource section.

- 100: LockBit 3.0 Decryptor (EXE)
- 101: LockBit 3.0 Encryptor (EXE)
- 103: LockBit 3.0 Encryptor (DLL)
- 106: LockBit 3.0 Encryptor (Reflective DLL)

The parameters used during execution are as follows.

-type

- enc: Generate Encryptor
- dec: Generate Decryptor

-config

Configuration file path

-exe, -dll, -ref(reflectiveDLL)

File type to be created

-pass

- When creating an Encryptor, the password required to execute the Encryptor
- Passwords required to execute Encryptor are stored in `Password_exe.txt` and `Password_dll.txt` respectively

-pubkey, -privkey

Path of the key file to be used when creating Encryptor and Decryptor

-ofile

File path to save

4. Keygen.exe

`Keygen.exe` is a tool that generates key pairs required for encryption. The parameters used during execution are as follows.

- -path : Folder path to save generated key pair file
- -pubkey : File name to use for Encryptor as public key (256 bytes)

— The first 128 bytes contain e value (fixed at 65537), and the last 128 bytes contain N value

-privkey : File name to use for Encryptor as private key (256 bytes)

— The first 128 bytes contain d value and the last 128 bytes contain N value

Key generation is performed as follows.

- keygen.exe is written based on .
- Generates an RSA-1024 key to encrypt the file encryption key, and the value is fixed to 65537.
- When generating 512-bit prime numbers and , create a 256-byte seed with the x86 instruction.
- Then, pass the seed to the function of MIRACL to initialize the CSPRNG defined in , and use the function to get a 512-bit value, which will be used for generating a prime number.
- The keygen.exe uses a modified version of MIRACL, which uses instead of SHA-256 inside the CSPRNG from .

Afterward, a 16-byte Decryption ID is generated to identify the infected PC and stored in the DECRYPTION_ID.txt file.

File information

1. Build.bat

- MD5 : 4e46e28b2e61643f6af70a8b19e5cb1f
- SHA-1 : 804a1d0c4a280b18e778e4b97f85562fa6d5a4e6
- SHA-256 : 8e83a1727696ced618289f79674b97305d88beeeabf46bd25fc77ac53c1ae339
- FileType : BAT

2. config.json

- MD5 : a6ba7b662de10b45ebe5b6b7edaa62a9
- SHA-1 : f3ed67bdaef070cd5a213b89d53c5b8022d6f266
- SHA-256 : 3f7518d88aefd4b1e0a1d6f9748f9a9960c1271d679600e34f5065d8df8c9dc8
- FileType : json

3. Builder.exe

- MD5 : c2bc344f6dde0573ea9acdfb6698bf4c
- SHA-1 : d6ae7dc2462c8c35c4a074b0a62f07cfef873c77
- SHA-256 : a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db
- CreationTime : 2022–09–14 08:31:18
- FileType : EXE

4. Keygen.exe

- MD5 : 71c3b2f765b04d0b7ea0328f6ce0c4e2
- SHA-1 : bf8ecb6519f16a4838ceb0a49097bcc3ef30f3c4
- SHA-256 : ea6d4dedd8c85e4a6bb60408a0dc1d56def1f4ad4f069c730dc5431b1c23da37
- CreationTime : 2022–09–09 08:58:31
- FileType : EXE