Netskope Threat Coverage: LockBit

netskope.com/blog/netskope-threat-coverage-lockbit

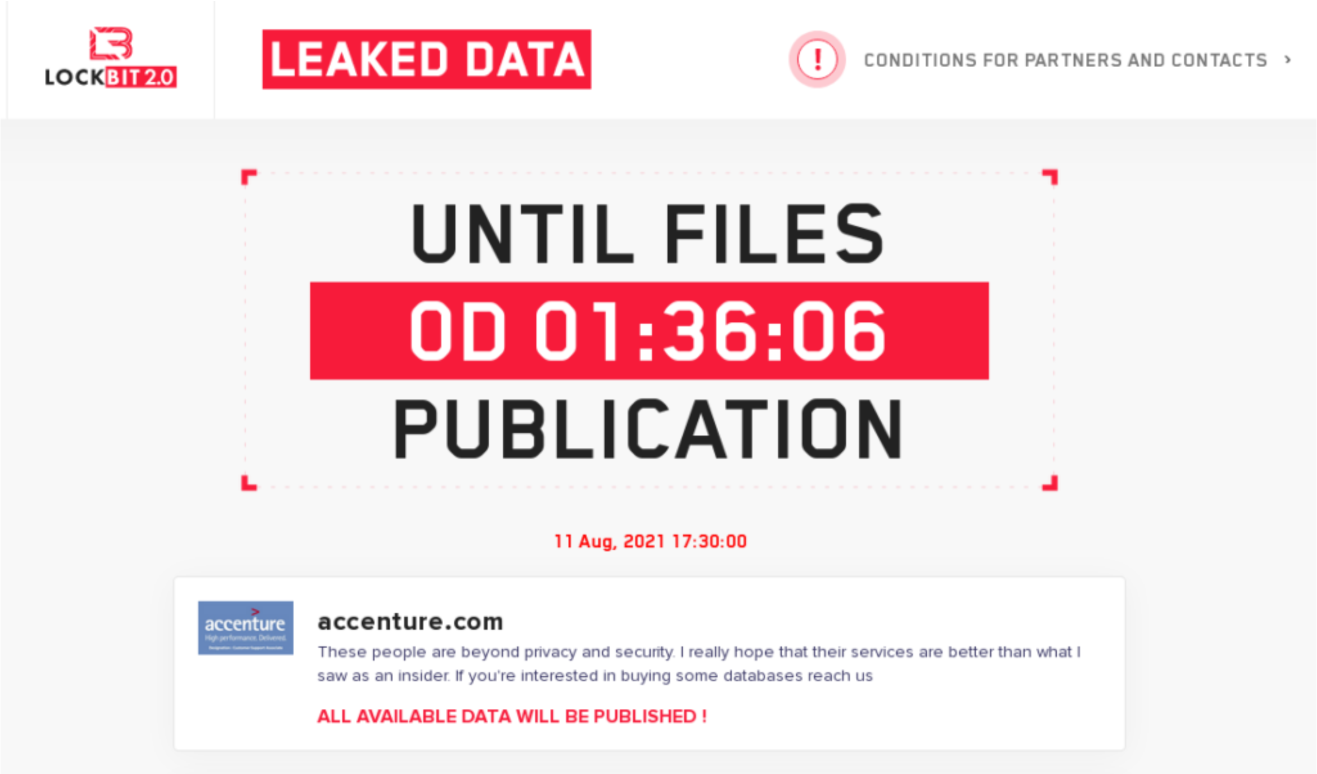
Gustavo Palazolo

August 12, 2021

Summary

LockBit Ransomware (a.k.a. ABCD) is yet another ransomware group operating in the RaaS (Ransomware-as-a-Service) model, following the same architecture as other major threat groups, like REvil. This threat emerged in September 2019 and is still being improved by its creators. In June 2021, the LockBit group announced the release of LockBit 2.0, which included a new website hosted on the deep web, as well as a new feature to encrypt Windows domains using group policy.

On August 11, 2021, the LockBit ransomware group announced in their deep web forum that they have infected the global IT consultancy company Accenture.



UNTIL FILES
0D 01:36:06
PUBLICATION

11 Aug, 2021 17:30:00

accenture.com

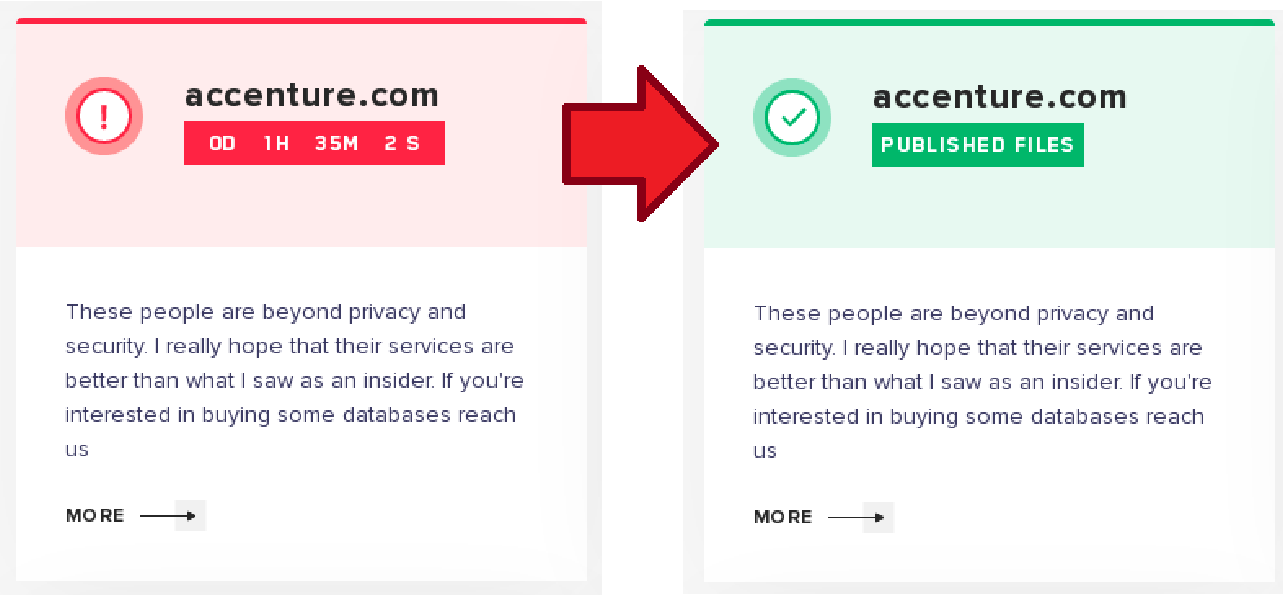
These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

ALL AVAILABLE DATA WILL BE PUBLISHED !

LockBit official website, hosted on the deep web, showing the Accenture information.

According to the company Cyble, the attackers have allegedly stolen about 6TB of data, and are demanding $50M (USD) as ransom. Also, Cyble mentioned that this attack was supposedly carried out by an insider, however, that has not been verified yet. The IT giant Accenture has confirmed the attack and also affirmed that the breach had no impact on their operations or systems.

The period established for Accenture to pay the ransom was August 11, 2021, which has now passed.


accenture.com

0D 1H 35M 2 S

These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

MORE

accenture.com

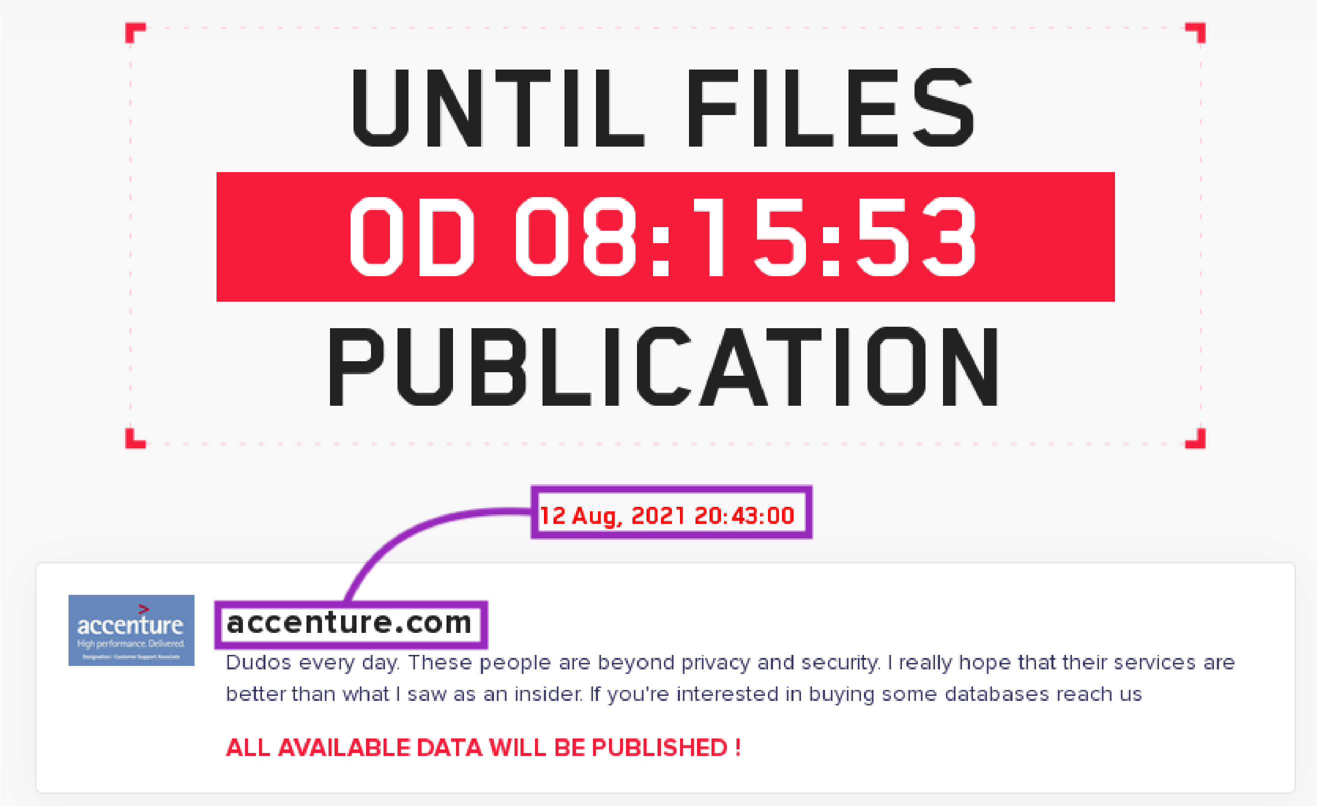
PUBLISHED FILES

These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

MORE

The original deadline for the ransom's payment has passed, according to LockBit's website.

However, as I am writing this blog post, the period to pay the ransom was changed to August 12, 2021, at the end of the day.



UNTIL FILES

0D 08:15:53

PUBLICATION

12 Aug, 2021 20:43:00

accenture.com

Dudos every day. These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

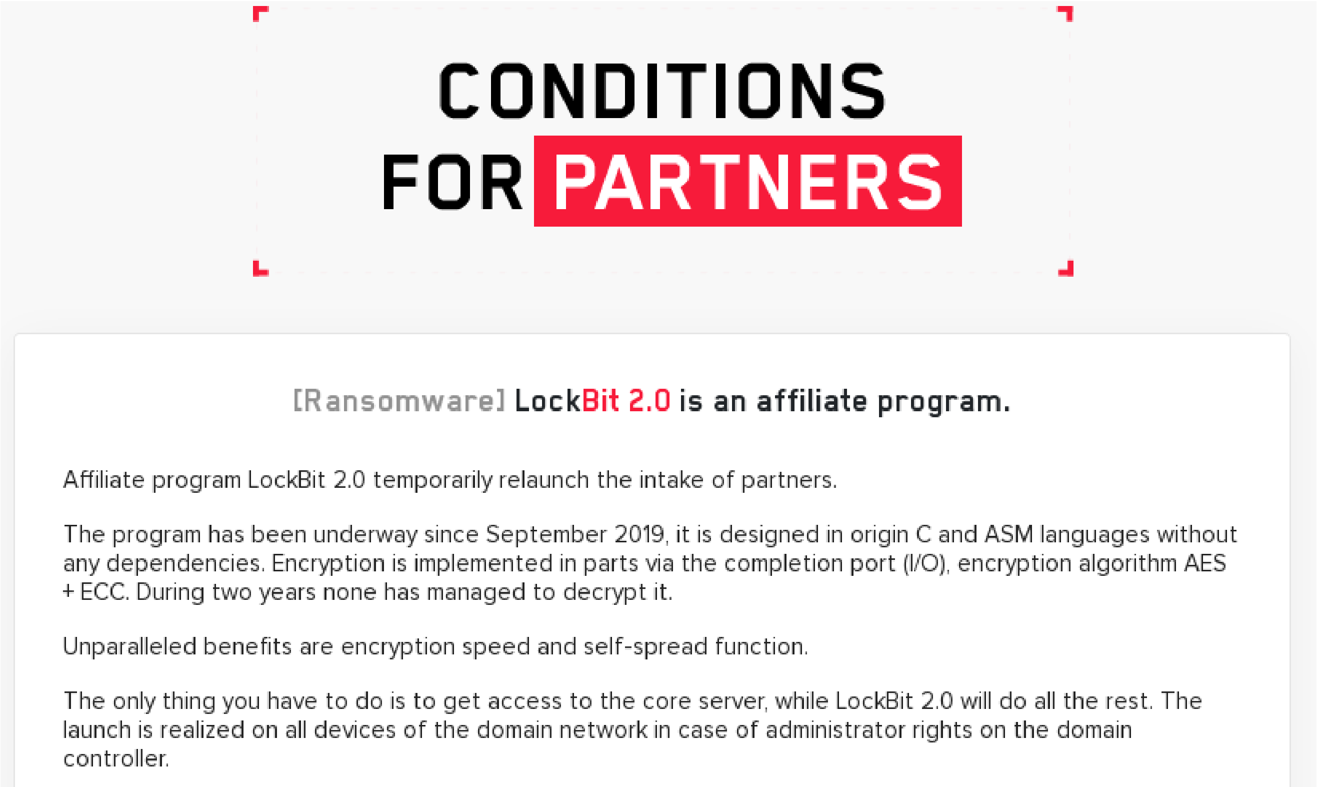
ALL AVAILABLE DATA WILL BE PUBLISHED !

New deadline established by the attackers for Accenture's ransom

At this point, it's unclear how the attack was carried out, or if LockBit really stole sensitive data from the company. In this threat coverage report, we will briefly show how LockBit works, describing some features used for anti-analysis.

Threat

LockBit ransomware is developed in both C and Assembly and uses AES + ECC to encrypt the files. The group operates in the RaaS model, and on their official website hosted on the deep web, we can find an advertisement trying to attract more affiliates into the scheme.



CONDITIONS FOR PARTNERS

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

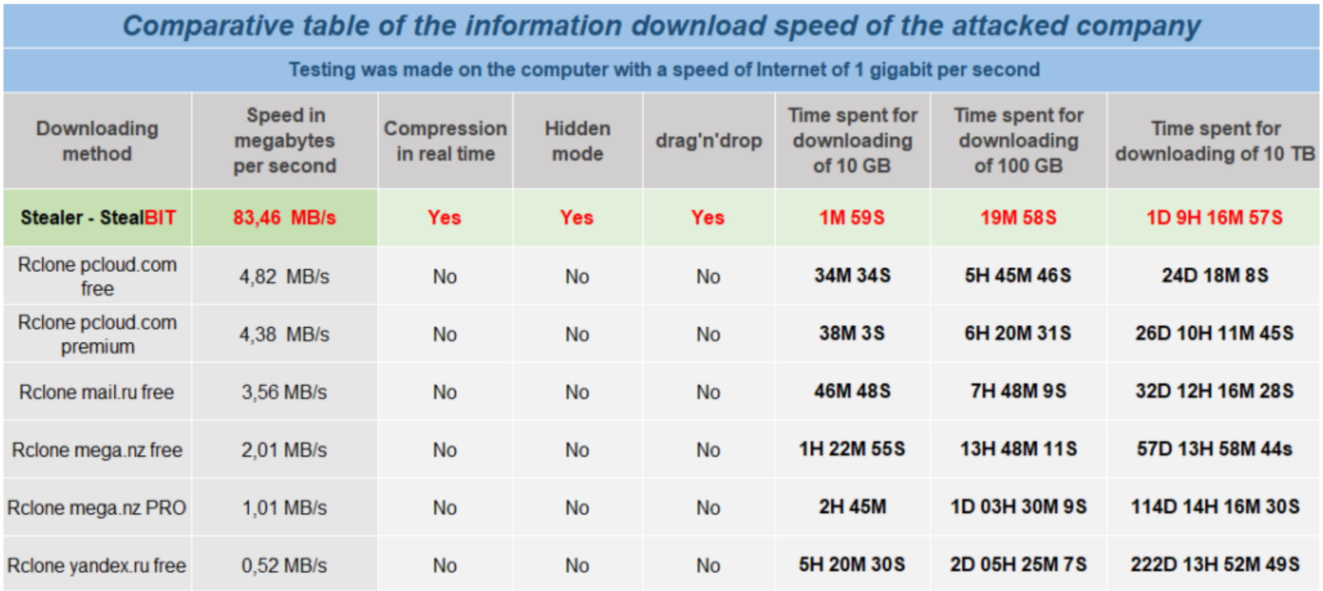
The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

LockBit "advertisement" posted on their website.

According to the page, the group is using a custom stealer named "StealBIT" to exfiltrate data from companies. They have even included a comparison between their service and other services, like MEGA and pCloud.



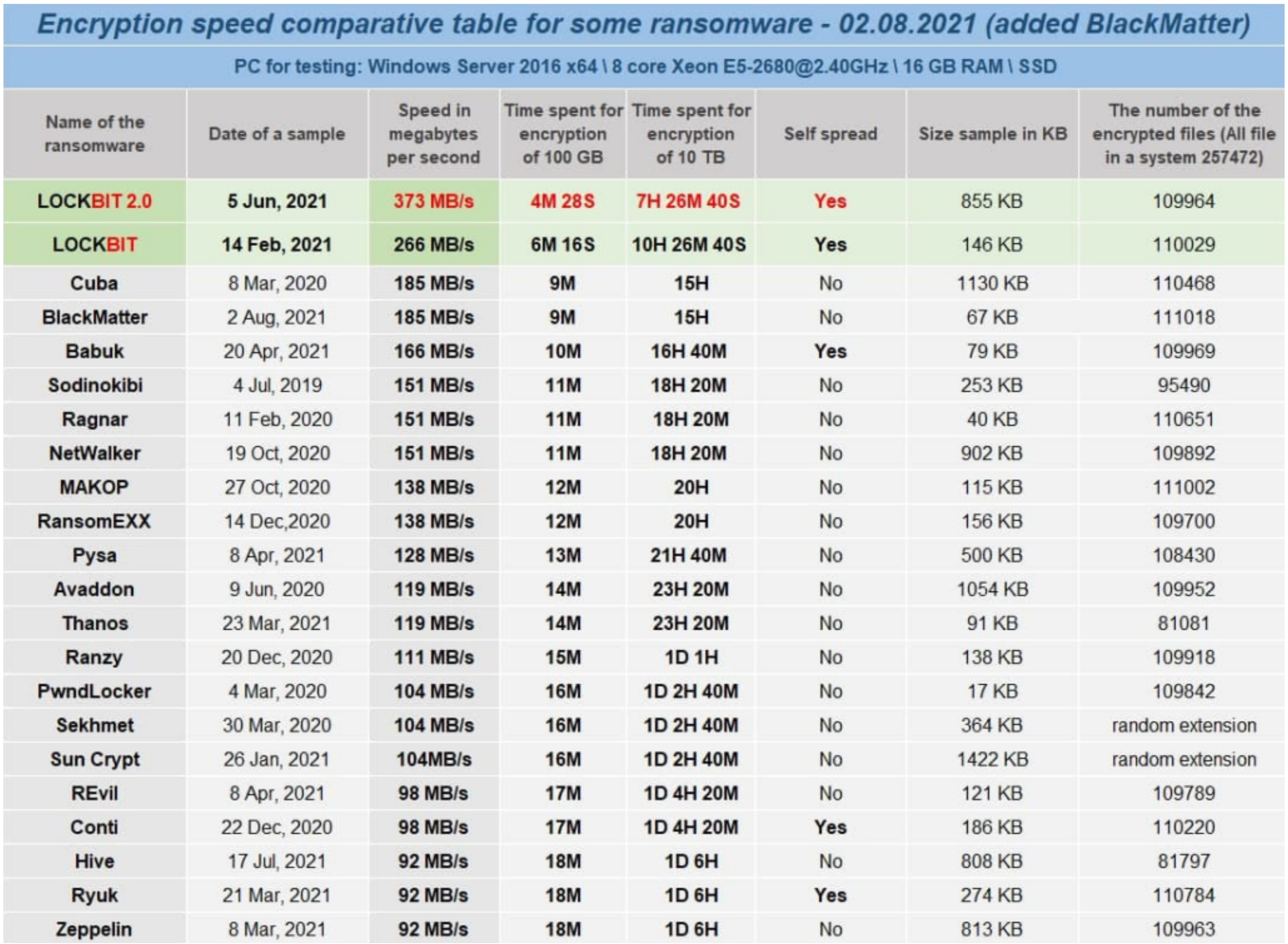
Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

LockBit "advertisement" showing how fast they are when it comes to data exfiltration.

The website also includes an encryption speed comparative between LockBit and other ransomware families, such as Ragnar, REvil, Conti, and others.



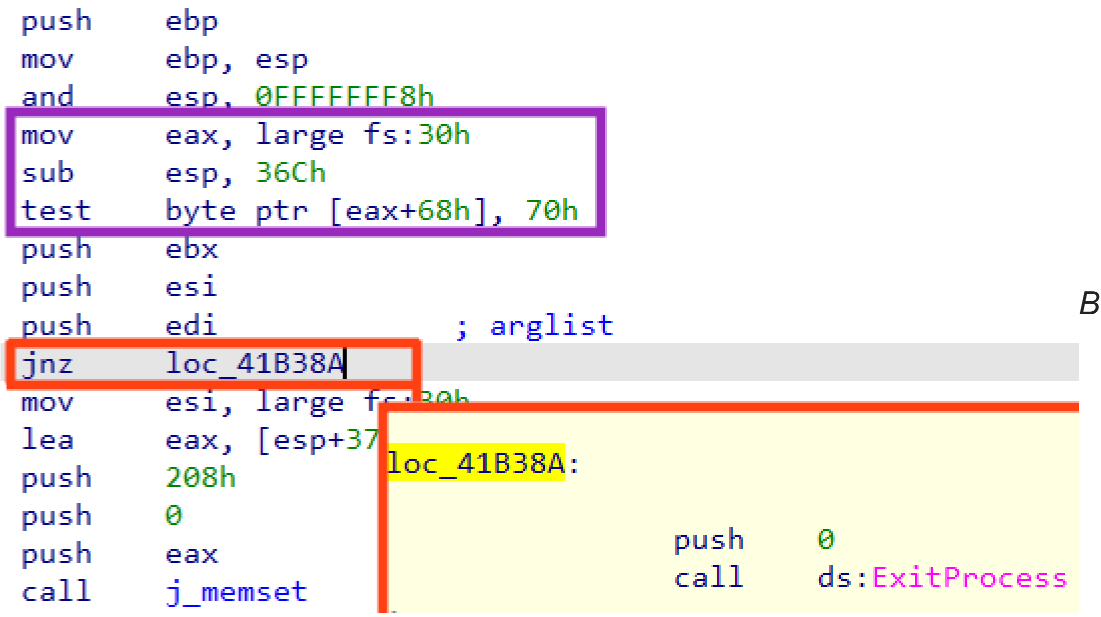
Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963

LockBit "advertisement" showing an encryption speed comparison between ransomware families.

Once the sample is executed, the code implements a very simple technique to detect if the process is being debugged, by checking the NtGlobalFlag value in the Process Environment Block (PEB) structure. This is usually done to avoid direct calls to the function `CheckRemoteDebuggerPresent` or `IsDebuggerPresent`.

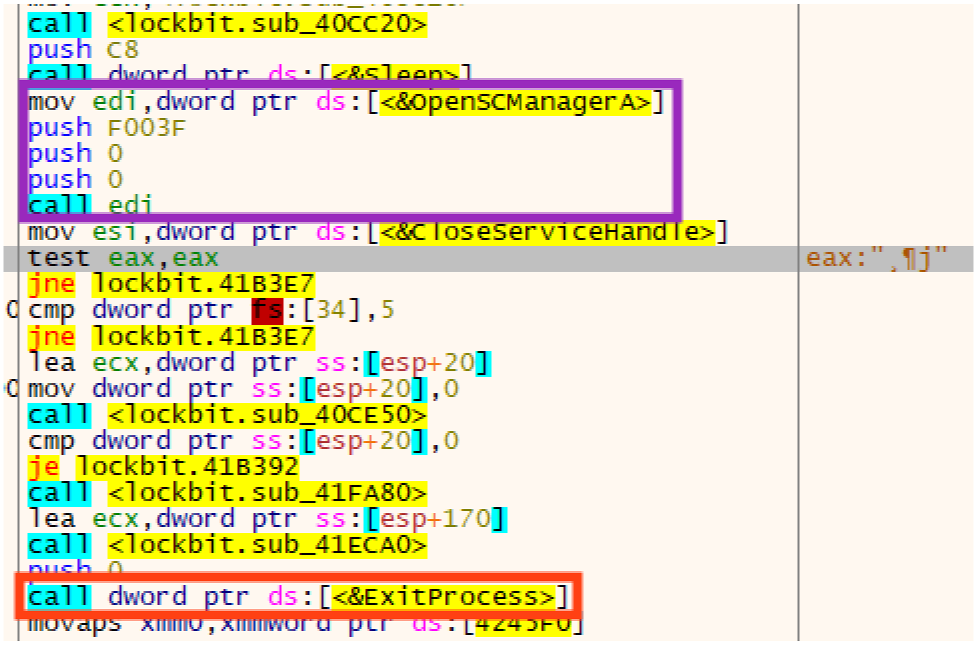


```
push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
mov     eax, large fs:30h
sub     esp, 36Ch
test    byte ptr [eax+68h], 70h
push    ebx
push    esi
push    edi             ; arglist
jnz     loc_41B38A
mov     esi, large fs:30h
lea     eax, [esp+37
push    208h
push    0
push    eax
call    j_memset
```

```
loc_41B38A:

                push    0
                call    ds:ExitProcess
```

Basic anti-debug technique.

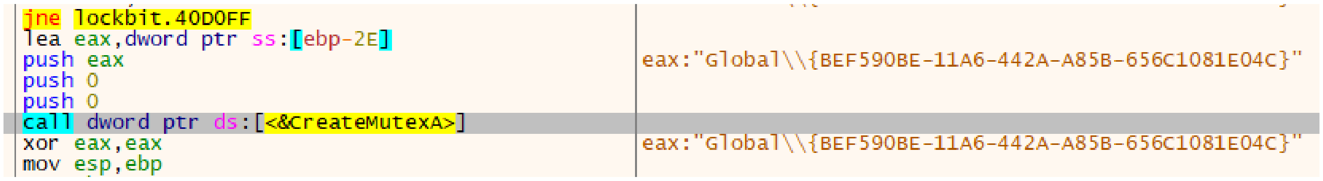
Also, LockBit verifies if the process is running with Administrator privileges by checking the return of the API `OpenSCManagerA`. If it's not a privileged process, the function will fail, consequently reaching the `ExitProcess` call.



```
call <lockbit.sub_40CC20>
push C8
call dword ptr ds:[<&Sleep>]
mov edi,dword ptr ds:[<&OpenSCManagerA>]
push F003F
push 0
push 0
call edi
mov esi,dword ptr ds:[<&CloseServiceHandle>]
test eax,eax                                          eax:",¶j"
jne lockbit.41B3E7
cmp dword ptr fs:[34],5
jne lockbit.41B3E7
lea ecx,dword ptr ss:[esp+20]
mov dword ptr ss:[esp+20],0
call <lockbit.sub_40CE50>
cmp dword ptr ss:[esp+20],0
je lockbit.41B392
call <lockbit.sub_41FA80>
lea ecx,dword ptr ss:[esp+170]
call <lockbit.sub_41ECA0>
push 0
call dword ptr ds:[<&ExitProcess>]
movaps xmm0,xmmword ptr ds:[4243F0]
```

LockBit checking if the process is privileged.

The sample also uses a Mutex to verify if there is another instance of LockBit running at the same time.

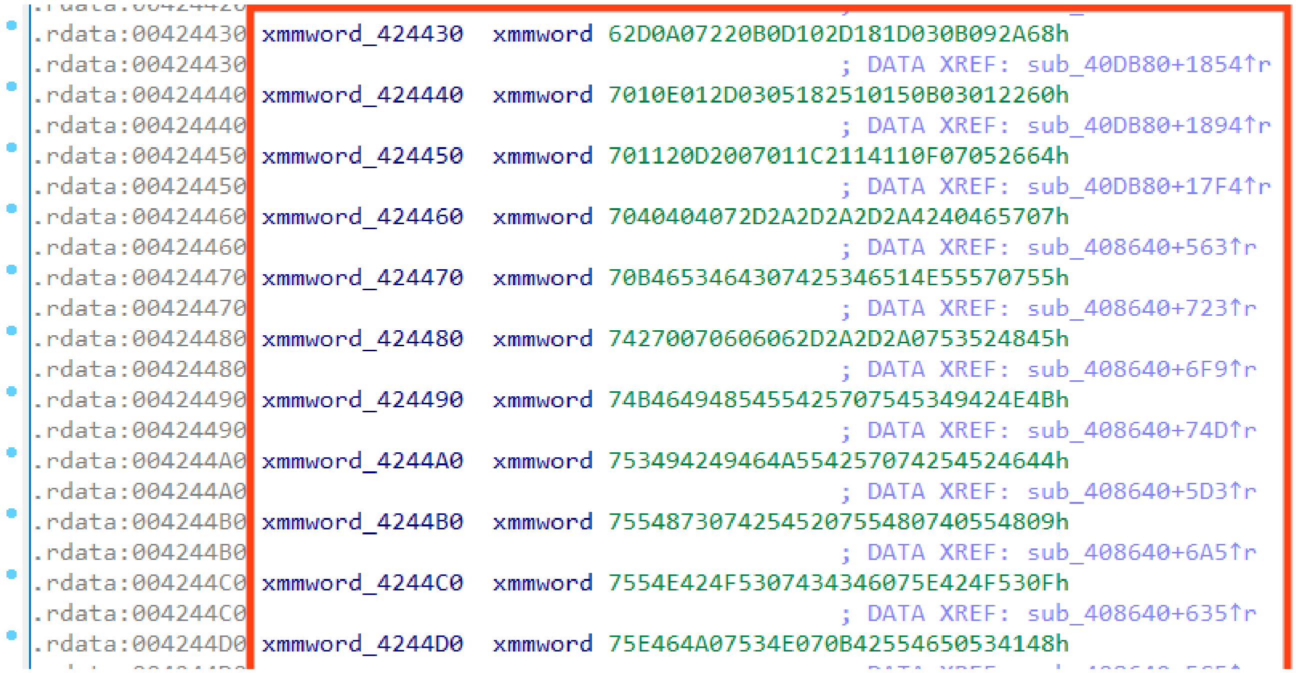


```
jne lockbit.40D0FF
lea eax,dword ptr ss:[ebp-2E]
push eax                               eax:"Global\\{BEF590BE-11A6-442A-A85B-656C1081E04C}"
push 0
push 0
call dword ptr ds:[<&CreateMutexA>]
xor eax,eax                            eax:"Global\\{BEF590BE-11A6-442A-A85B-656C1081E04C}"
mov esp,ebp
```

LockBit creating a Mutex object.

Looking at the PE .rdata section, we can see that LockBit attempts to protect some relevant information by encrypting the strings, which is just a basic protection against detection or quick analyses.

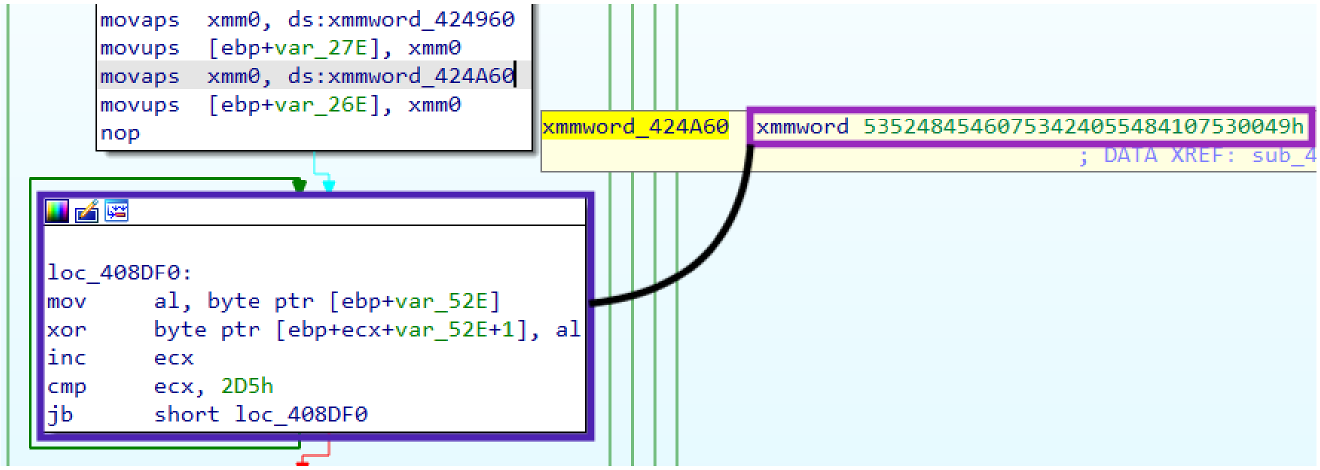
Furthermore, we can observe that LockBit is using Intel 128-bit XMM registers in the operations, probably to increase the performance of the code.



```
.rdata:00424430 xmmword_424430  xmmword 62D0A07220B0D102D181D030B092A68h
.rdata:00424430                                   ; DATA XREF: sub_40DB80+1854↑r
.rdata:00424440 xmmword_424440  xmmword 7010E012D0305182510150B03012260h
.rdata:00424440                                   ; DATA XREF: sub_40DB80+1894↑r
.rdata:00424450 xmmword_424450  xmmword 701120D2007011C2114110F07052664h
.rdata:00424450                                   ; DATA XREF: sub_40DB80+17F4↑r
.rdata:00424460 xmmword_424460  xmmword 7040404072D2A2D2A2D2A4240465707h
.rdata:00424460                                   ; DATA XREF: sub_408640+563↑r
.rdata:00424470 xmmword_424470  xmmword 70B4653464307425346514E55570755h
.rdata:00424470                                   ; DATA XREF: sub_408640+723↑r
.rdata:00424480 xmmword_424480  xmmword 74270070606062D2A2D2A0753524845h
.rdata:00424480                                   ; DATA XREF: sub_408640+6F9↑r
.rdata:00424490 xmmword_424490  xmmword 74B4649485455425707545349424E4Bh
.rdata:00424490                                   ; DATA XREF: sub_408640+74D↑r
.rdata:004244A0 xmmword_4244A0  xmmword 753494249464A554257074254524644h
.rdata:004244A0                                   ; DATA XREF: sub_408640+5D3↑r
.rdata:004244B0 xmmword_4244B0  xmmword 7554873074254520755480740554809h
.rdata:004244B0                                   ; DATA XREF: sub_408640+6A5↑r
.rdata:004244C0 xmmword_4244C0  xmmword 7554E424F5307434346075E424F530Fh
.rdata:004244C0                                   ; DATA XREF: sub_408640+635↑r
.rdata:004244D0 xmmword_4244D0  xmmword 75E464A07534E070B42554650534148h
```

LockBit encrypted strings.

The algorithm is straightforward — it decrypts the string by doing a single byte XOR operation, using the first byte of the string as a key.

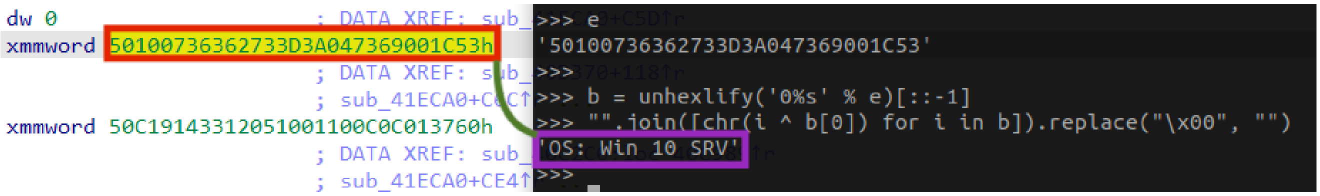


```
movaps  xmm0, ds:xmmword_424960
movups  [ebp+var_27E], xmm0
movaps  xmm0, ds:xmmword_424A60
movups  [ebp+var_26E], xmm0
nop

loc_408DF0:
mov     al, byte ptr [ebp+var_52E]
xor     byte ptr [ebp+ecx+var_52E+1], al
inc     ecx
cmp     ecx, 2D5h
jb      short loc_408DF0
```

```
xmmword_424A60  xmmword 53524845460753424055484107530049h
                ; DATA XREF: sub_4
```

LockBit string decryption algorithm.

It should be possible to decrypt LockBit strings applying the same logic.

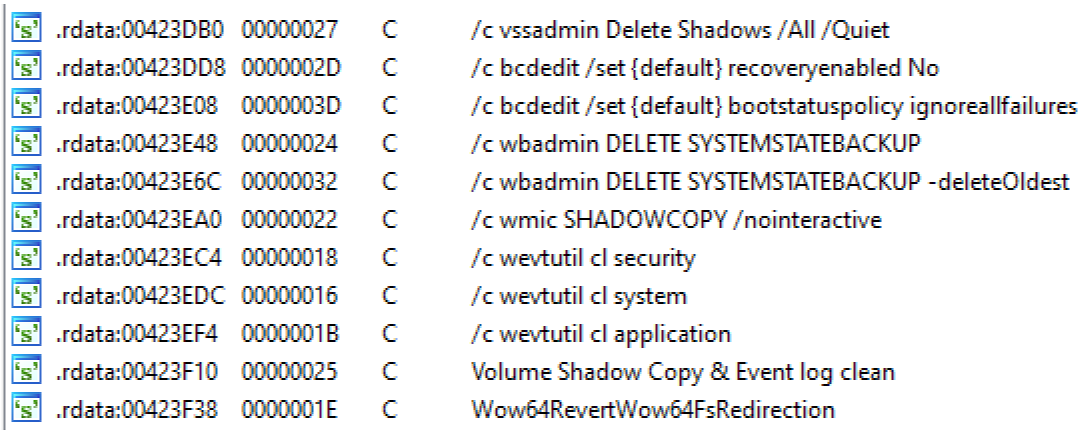


```
dw 0                                        ; DATA XREF: sub_
xmmword 50100736362733D3A047369001C53h
                                            ; DATA XREF: sub_
                                            ; sub_41ECA0+C6C↑
xmmword 50C19143312051001100C0C013760h
                                            ; DATA XREF: sub_
                                            ; sub_41ECA0+CE4↑
```

```
>>> e
'50100736362733D3A047369001C53'
>>>
>>> b = unhexlify('0%s' % e)[::-1]
>>> "".join([chr(i ^ b[0]) for i in b]).replace("\x00", "")
'OS: Win 10 SRV'
>>>
```

Decrypting LockBit's strings using Python.

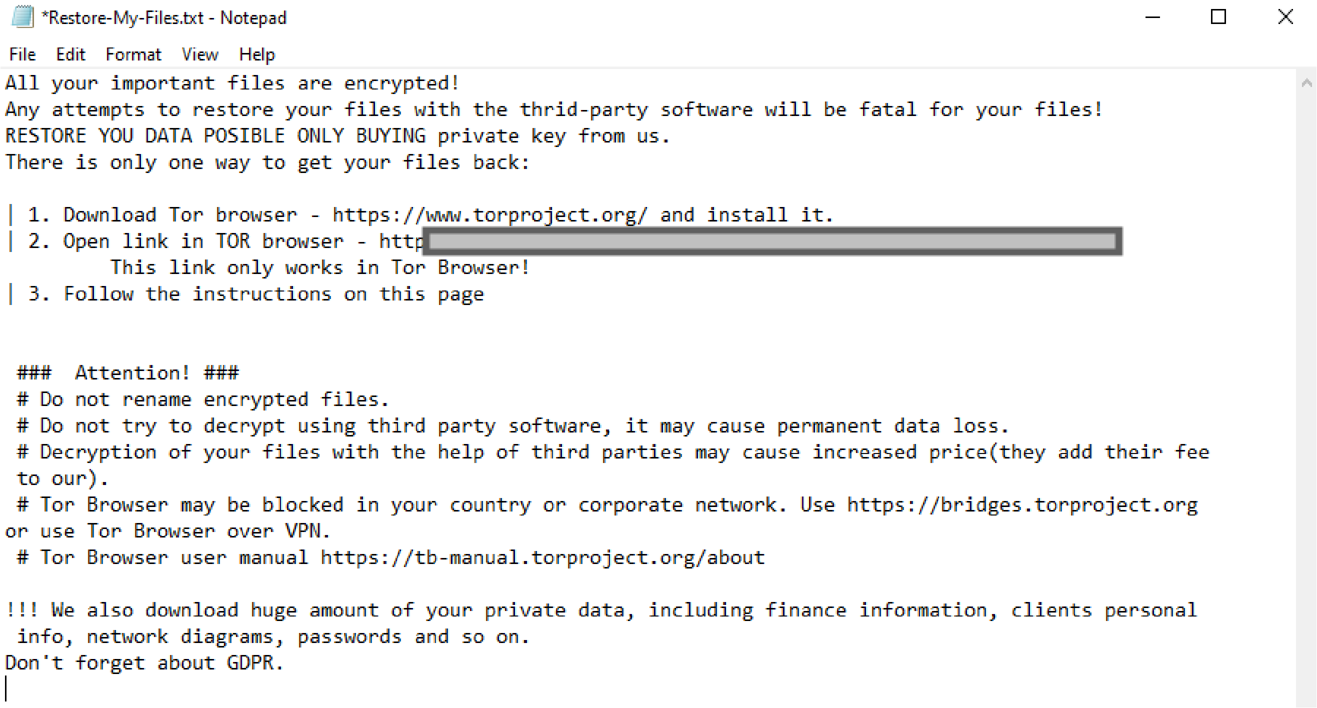
In addition, LockBit also executes a series of commands using the API `ShellExecuteA` to avoid any restoration of the files in the machine by disabling the system's recovery mode and the Windows Shadow Copies.



s	.rdata:00423DB0	00000027	C	/c vssadmin Delete Shadows /All /Quiet
s	.rdata:00423DD8	0000002D	C	/c bcdedit /set {default} recoveryenabled No
s	.rdata:00423E08	0000003D	C	/c bcdedit /set {default} bootstatuspolicy ignoreallfailures
s	.rdata:00423E48	00000024	C	/c wbadmin DELETE SYSTEMSTATEBACKUP
s	.rdata:00423E6C	00000032	C	/c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
s	.rdata:00423EA0	00000022	C	/c wmic SHADOWCOPY /nointeractive
s	.rdata:00423EC4	00000018	C	/c wevtutil cl security
s	.rdata:00423EDC	00000016	C	/c wevtutil cl system
s	.rdata:00423EF4	0000001B	C	/c wevtutil cl application
s	.rdata:00423F10	00000025	C	Volume Shadow Copy & Event log clean
s	.rdata:00423F38	0000001E	C	Wow64RevertWow64FsRedirection

Some of the commands executed by LockBit.

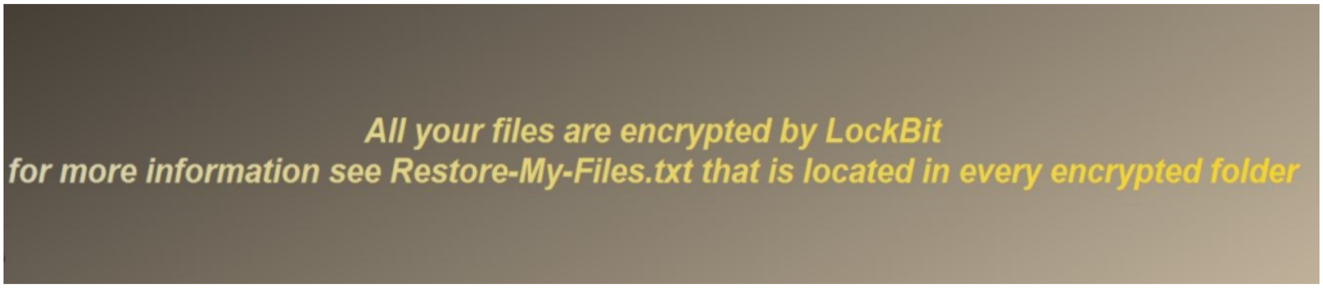
After the files are encrypted, LockBit creates the ransom note in every single directory where there are encrypted files.



```
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 - http[redacted]
         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.
```

LockBit ransom note

Lastly, the computer's wallpaper is also changed by the malware, in case encrypting the files wasn't enough to catch the victim's attention.



All your files are encrypted by LockBit
for more information see Restore-My-Files.txt that is located in every encrypted folder

LockBit wallpaper.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
  Generic.Ransom.LockBit.19F98D1F
- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
  - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
  - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox

IOCs

SHA256

6292c2294ad1e84cd0925c31ee6deb7afd300f935004a9e8a7a43bf80034abae

A full list of IOCs and a Yara rule are available in our Git repo.