LockBit ransomware

Ransom gates

- lockbitkodidilol.onion
- lockbitks2tvnmwk.onion

Ransom note

- Restore-My-Files.txt

Ransom extension

- .lockbit

E-mail

- ondrugs@firemail.cc

Persistence

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\XO1XADpO01

Mutex

- Global{BEF590BE-11A6-442A-A85B-656C1081E04C}

Executed commands

- bcdedit /set {default} recoveryenabled No
- bcdedit /set {default} bootstatuspolicy ignoreallfailures
- vssadmin delete shadows /all /quiet
- wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
- wbadmin DELETE SYSTEMSTATEBACKUP
- wbadmin delete catalog -quiet
- wevtutil cl system
- wevtutil cl security
- wevtutil cl application
- wmic SHADOWCOPY /nointeractive
- wmic shadowcopy delete
- ping 1.1.1.1 -n 22 > Nul & "%s"
- ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"

Registry keys

- SOFTWARE\LockBit
- SOFTWARE\LockBit\full
- SOFTWARE\LockBit\Public

Folders skip-list

```
$windows.~bt
intel
```

```
msocache
$recycle.bin
$windows.~ws
tor browser
boot
system volume information
perflogs
google
application data
windows
windows.old
appdata
Windows nt
Msbuild
Microsoft
All users
Mozilla
```

Files skip-list

```
ntldr
ntuser.dat.log
bootsect.bak
autorun.inf
```

Service stop-list

```
wrapper
DefWatch
ccEvtMgr
ccSetMgr
SavRoam
Sqlservr
sqlagent
sqladhlp
Culserver
RTVscan
sqlbrowser
SQLADHLP
QBIDPService
Intuit.QuickBooks.FCS
```

```
QBCFMonitorService
sqlwriter
msmdsrv
tomcat6
zhudongfangyu
vmware-usbarbitator64
vmware-converter
dbsrv12
dbeng8
MSSQL$MICROSOFT##WID
MSSQL$VEEAMSQL2012
SQLAgent$VEEAMSQL2012
SQLBrowser
SQLWriter
FishbowlMySQL
MSSQL$MICROSOFT##WID
MySQL57
MSSQL$KAV_CS_ADMIN_KIT
MSSQLServerADHelper100
SQLAgent$KAV_CS_ADMIN_KIT
msftesql-Exchange
MSSQL$MICROSOFT##SSEE
MSSQL$SBSMONITORING
MSSQL$SHAREPOINT
MSSQLFDLauncher$SBSMONITORING
MSSQLFDLauncher$SHAREPOINT
SQLAgent$SBSMONITORING
SQLAgent$SHAREPOINT
QBFCService
QBVSS
YooBackup
YooIT
svc$
MSSQL
MSSQL$
memtas
mepocs
sophos
veeam
backup
bedbg
PDVFSService
BackupExecVSSProvider
BackupExecAgentAccelerator
BackupExecAgentBrowser
BackupExecDiveciMediaService
```

```
BackupExecJobEngine
BackupExecManagementService
BackupExecRPCService
MVArmor
MVarmor64
stc_raw_agent
VSNAPVSS
VeeamTransportSvc
VeeamDeploymentService
VeeamNFSSvc
AcronisAgent
ARSM
AcrSch2Svc
CASAD2DWebSvc
CAARCUpdateSvc
WSBExchange
MSExchange
MSExchange$
LanmanWorkstation
WebClient
```

Process kill-list

```
wxServer
wxServerView
sqlmangr
RAgui
supervise
Culture
Defwatch
winword
QBW32
QBDBMgr
qbupdate
axlbridge
httpd
fdlauncher
MsDtSrvr
java
360se
360doctor
wdswfsafe
fdhost
```

```
GDscan
ZhuDongFangYu
QBDBMgrN
mysqld
AutodeskDesktopApp
acwebbrowser
Creative Cloud
Adobe Desktop Service
CoreSync
Adobe CEF Helper
node
AdobeIPCBroker
sync-taskbar
sync-worker
InputPersonalization
AdobeCollabSync
BrCtrlCntr
BrCcUxSys
SimplyConnectionManager
Simply.SystemTrayIcon
fbguard
fbserver
ONENOTEM
wsa_service
koaly-exp-engine-service
TeamViewer_Service
TeamViewer
tv_w32
tv_x64
TitanV
Ssms
notepad
RdrCEF
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
```

```
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
wordpad
bedbh
vxmon
benetns
bengien
pvlsvr
beserver
raw_agent_svc
vsnapvss
CagService
DellSystemDetect
EnterpriseClient
VeeamDeploymentSvc
```

Extension list

```
.msstyles
.sqlitedb
.sqlite3
.diagcab
.diagcfg
.diagpkg
.sqlite
.db-shm
.db-wal
.dacpac
.theme
.icns
.lock
```

```
.tmd
.ckp
.dbc
.sql
.mwb
.rar
.dbv
.frm
.mdf
.dbt
.qry
.ndf
.sdb
.myd
.mrg
.db3
.dbs
.dbf
.sdf
.zip
.rdp
.bin
.hlp
.shs
.drv
.wpx
.bat
.rom
.msc
.spl
.ps1
.msu
.ics
.key
.exe
.dll
.lnk
.ico
.hlp
.sys
.drv
.cur
.idx
.ini
.reg
.mp3
```

```
.386
.cmd
.ani
.adv
.msi
.msp
.com
.nls
.ocx
.mpa
.cpl
.mod
.hta
.prf
.rtp
```

Ransom note:

```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for
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://lockbitks2tvnmwk.onion/?
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 l
 # Decryption of your files with the help of third parties may cause increased pri
 # Tor Browser may be blocked in your country or corporate network. Use https://br
 # Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance informati
```

SHA256

- 0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76
- 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f

- 0f178bc093b6b9d25924a85d9a7dde64592215599733e83e3bbc6df219564335
- 0f5d71496ab540c3395cfc024778a7ac5c6b5418f165cc753ea2b2befbd42d51
- 13849c0c923bfed5ab37224d59e2d12e3e72f97dc7f539136ae09484cbe8e5e0
- 15a7d528587ffc860f038bb5be5e90b79060fbba5948766d9f8aa46381ccde8a
- 1b109db549dd0bf64cadafec575b5895690760c7180a4edbf0c5296766162f18
- 1e3bf358c76f4030ffc4437d5fcd80c54bd91b361abb43a4fa6340e62d986770
- 256e2bf5f3c819e0add95147b606dc314bbcbac32a801a59584f43a4575e25dc
- 26b6a9fecfc9d4b4b2c2ff02885b257721687e6b820f72cf2e66c1cae2675739
- 2b8117925b4b5b39192aaaea130426bda39ebb5f363102641003f2c2cb33b785
- 3f29a368c48b0a851db473a70498e168d59c75b7106002ac533711ca5cfabf89
- 410c884d883ebe2172507b5eadd10bc8a2ae2564ba0d33b1e84e5f3c22bd3677
- 4acc0b5ed29adf00916dea7652bcab8012d83d924438a410bee32afbcdb995cc
- 5b9bae348788cd2a1ce0ba798f9ae9264c662097011adbd44ecfab63a8c4ae28
- 6292c2294ad1e84cd0925c31ee6deb7afd300f935004a9e8a7a43bf80034abae
- 69d9dd7fdd88f33e2343fb391ba063a65fe5ffbe649da1c5083ec4a67c525997
- 83ab7a2bcac146db472f3b930c01af5b6d3d978ead7b14a9d0ac16e1a76e9f9d
- 9bc98d15f243257c1b5bca59464abe68c680cd5482ba9f5082201dde41a016cf
- a03326ac8efa930e10091a374d40ddab9f7c2f12246d6ef7983bad93256f1f3a
- a0085da4a920e92d8f59fefa6f25551655ca911382b5e34df76a9333ac8b7214
- a08fbf01d02097094b725101309b2bf7fefc2e27724654b840b87e091aa5c9b9
- a1360645cf3113715cc023d2e4cf9f6f3a6278abcf4499f0ba7cd76c82839eb0
- c8205792fbc0a5efc6b8f0f2257514990bfaa987768c4839d413dd10721e8871
- ce8559871b410e23057393eb2d9fb76ec902da2ff1f8006ad312c81852a41f6f
- e3f236e4aeb73f8f8f0caebe46f53abbb2f71fa4b266a34ab50e01933709e877
- ec88f821d22e5553afb94b4834f91ecdedeb27d9ebfd882a7d8f33b5f12ac38d
- ffbb6c4d8d704a530bdd557890f367ad904c09c03f53fda5615a7208a0ea3e4d

Decryptors

- 09e956d140d6879cf7eacbb65dcbfbe1dea1961a31c5d0f834343ef2c886ccc1
- 9bc98d15f243257c1b5bca59464abe68c680cd5482ba9f5082201dde41a016cf

VT perks:

- vhash:"015036656d5223z12z3e05031f1z37z406001a5zb7z"
- imphash:"be232aa2621354bf5dd7b405cc99198c"

YARA rules

```
rule lockbit_clsids
{
        strings:
                $id1 = "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" ascii wide
                $id2 = "{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}" ascii wide
                $id3 = "{02B49784-1CA2-436C-BC08-72FA3956507D}" ascii wide
                $id4 = "{BEF590BE-11A6-442A-A85B-656C1081E04C}" ascii wide

        condition:
                3 of them
}
```

```
rule lockbit_mutex
{
        strings:
                $mutex = "XO1XADpO01" ascii wide

        condition:
                all of them
}
```

```
rule lockbit_uac
{
        strings:
                $uac0 = "Elevation:Administrator!new:" ascii wide
                $uac1 = "DisplayCalibrator" ascii wide
                $uac2 = "Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibrat

        condition:
                all of them
}
```

```
rule lockbit_cmd
{
        strings:
                $cmd0 = "vssadmin Delete Shadows /All /Quiet" ascii wide
                $cmd1 = "bcdedit /set {default} recoveryenabled No" ascii wide
                $cmd2 = "bcdedit /set {default} bootstatuspolicy ignoreallfailures"
                $cmd3 = "wbadmin DELETE SYSTEMSTATEBACKUP" ascii wide
                $cmd4 = "wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest" ascii wide
                $cmd5 = "wmic SHADOWCOPY /nointeractive" ascii wide
                $cmd6 = "wevtutil cl security" ascii wide
                $cmd7 = "wevtutil cl system" ascii wide
                $cmd8 = "wevtutil cl application" ascii wide

        condition:
                6 of them
}
```

```
rule lockbit_priv_masq
{
        strings:
                $masq = { ff 15 [1-4] 85 ?? 0f [1-5] 68 04 01 00 00 8d [1-5] 50 ff

                $priv = { ff 15 [1-4] 85 ?? 74 ?? 8d ?? ?? 50 8d ?? ?? 50 6a 00 ff

        condition:
                $masq or $priv
}
```