https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw

Archived: 2026-04-05 23:14:14 UTC

```
MD5: 0e0b7b238a06a2a37a4de06a5ab5e615

Backup & Shadow Copy Removal:
cmd.exe /c vssadmin.exe delete shadows /all /quiet & bcdedit /set {default} bootstatuspolicy ignorea

Oddity:
fuckav

Mutex:
hate

Link:
https://pbs.twimg.com/media/Dn4vwaRW0AY-tUu.jpg:large

URL:
zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion

Extension Blacklist:
nemty
log
LOG
CAB
cab
CMD
cmd
COM
com
cpl
CPL
exe
EXE
ini
INI
dll
DLL
lnk
LNK
url
URL
```

```
ttf
TTF
DECRYPT.txt

File/Folder Blacklist:
$RECYCLE.BIN
rsa
NTDETECT.COM
ntldr
MSDOS.SYS
IO.SYS
boot.ini
AUTOEXEC.BAT
ntuser.dat
desktop.ini
CONFIG.SYS
RECYCLER
BOOTSECT.BAK
bootmgr
programdata
appdata
windows
Microsoft
Common Files


isRu check:
Russia
Belarus
Kazakhstan
Tajikistan
Ukraine


 ------ NEMTY PROJECT ======

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has
By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, y

[+] What guarantees? [+]

It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us.
It's not in our interests.
If you will not cooperate with our service - for us, its does not matter. But you will lose your tim
```

```
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website: zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay

When you open our website, follow the instructions and you will get your files back.


{"General": {"IP":"[IP]","Country":"[Country]","ComputerName":"[ComputerName]","Username":"[Username
```

Source: https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw