

Forum:[Hack Forums](#)

Thread: [Extracting CommandLine of Running Processes and Calculate their SHA256 Hash Checksum](#)

Hackoo - May 17, 2018, 3:40 pm

Hi ?

I want to share with you this code for Extracting CommandLine of Running Processes and Calculate their SHA256 Hash Checksum

In this script i chose those processes ProcessNames="cmd.exe" "cscript.exe" "wscript.exe" "mshta.exe" "powershell.exe" "firefox.exe" "chrome.exe"

Of course you can add another processes if you want to test ?

So, feel free to add your comments in order to improve this batch script ?

ExtractCmdLine_Hashes.bat

ExtractCmdLine_Hashes.bat ([Click to View](#))

?

Hackoo - May 21, 2018, 10:28 am

(May 17, 2018 03:40 PM)Hackoo Wrote: [CITE](#) Hi ?

I want to share with you this code for Extracting CommandLine of Running Processes and Calculate their SHA256 Hash Checksum

In this script i chose those processes ProcessNames="cmd.exe" "cscript.exe" "wscript.exe" "mshta.exe" "powershell.exe" "firefox.exe" "chrome.exe"

Of course you can add another processes if you want to test ?

So, feel free to add your comments in order to improve this batch script ?

ExtractCmdLine_Hashes.bat

ExtractCmdLine_Hashes.bat ([Click to View](#))

?

PHP Code

```
<?php
```

```
@echo off
```

```
Title Extracting CommandLine of Running Processes and  
Calculate their SHA256 Hash Checksum by Hackoo 2018
```

```
Mode 120,10 & color 0A
```

```
Set "LogFolder=LogFolder"
```

```
If Not Exist %LogFolder%\ MD %LogFolder%
```

```
Set "TmpFile=%LogFolder%\%~n0_Abs_cmdline.txt"
```

```
Set "LogFile=%LogFolder%\%~n0_cmdline.txt"
```

```
Set "Hashes=%LogFolder%\%~n0_Hashes.txt"
```

```
For %%a in (%TmpFile% %LogFile% %Hashes%) Do If Exist %%a Del %%a
```

```
Set ProcessNames="wscript.exe" "cmd.exe" "mshta.exe" "powershell.exe" "cscript.exe"
```

```
SetLocal EnableDelayedExpansion
```

```
for %%A in (%ProcessNames%) Do Call :GetCommandLine %%A
```

```
Timeout /T 2 /NoBreak>nul
```

```
Call :Extract "%TmpFile%" "%LogFile%"
```

```
cls
```

```
for /f "delims=" %%a in ('Type "%LogFile%"') do (
```

```
for /f "skip=1 delims=" %%H in ('CertUtil -hashfile "%~a" SHA256 ^| findstr /i /v "CertUtil"') do set "H=%%H"
```

```
echo %%a=!H: =!
```

```

echo %%a=!H: !=! >> "%Hashes%"
)

for /f "tokens=1,2 delims==" %%a in ('Type "%Hashes%"') do (
    If /I "%~xa"==" .vbs" MD VBS>nul 2>&1 && Type %%a > "VBS\%%~nxa.txt"
    If /I "%~xa"==" .vbe" MD VBE>nul 2>&1 && Type %%a > "VBE\%%~nxa.txt"
    If /I "%~xa"==" .hta" MD HTA>nul 2>&1 && Type %%a > "HTA\%%~nxa.txt"
    If /I "%~xa"==" .bat" MD BAT>nul 2>&1 && Type %%a > "BAT\%%~nxa.txt"
    If /I "%~xa"==" .cmd" MD CMD>nul 2>&1 && Type %%a > "CMD\%%~nxa.txt"
    Start "Chek SHA256 on VIRUSTOTAL" "https://www.virustotal.com/#/file/%%b"
)

Start "" "%Hashes%" & Exit
::*****
::
:GetCommandLine <ProcessName>
Set "ProcessCmd="
for /f "tokens=2 delims==" %%P in (
'wmic process where caption^="%~1" get commandline /format:list ^| findstr /I "%~1" ^| find /I /V "%~
nx0" 2^>nul') do (
    Set ProcessCmd=%%P
    echo !ProcessCmd!
    echo !ProcessCmd! >> "%TmpFile%"
)
Exit /b
::*****
::
:Extract <InputData> <OutPutData>
(
echo Data = WScript.StdIn.ReadAll
echo Data = Extract(Data,
"^(?^!.*(\x22w^)\b.*(w^).*(\ps1^|\hta^|\vbs^|\vbe^|\cmd^|\bat^|\exe^)"^)
echo WScript.Stdout.WriteLine Data
echo *****
echo Function Extract(Data,Pattern^)
echo   Dim oRE,oMatches,Match,Line
echo   set oRE = New RegExp
echo   oRE.IgnoreCase = True
echo   oRE.Global = True
echo   oRE.Pattern = Pattern
echo   set oMatches = oRE.Execute(Data^)
echo   If not isEmpty(oMatches^) then
echo       For Each Match in oMatches
echo           Line = Line ^& chr(34^)^& Trim(Match.Value^)^& chr(34^)^& vbcrLf
echo       Next
echo       Extract = Line
echo   End if
echo End Function
echo *****
)>"%tmp%\%~n0.vbs"
cscript /nologo "%tmp%\%~n0.vbs" < "%~1" > "%~2"
If Exist "%tmp%\%~n0.vbs" Del "%tmp%\%~n0.vbs"
exit /b
::*****
::

```

Phlox - May 21, 2018, 11:32 am

Fantastic script mate, keep up the good work.

HFDone - May 21, 2018, 1:02 pm

didnt test it but should work

```
Code for %%p in (explorer.exe wscript.exe cmd.exe mshta.exe powershell.exe cscript.exe) do (
  for /f "skip=1 delims=" %%x in ('wmic process where caption^="%%p" get commandline') do (
    for %%a in (.ps1 .PS1 .hta .HTA .vbs .VBS .vbe .VBE .cmd .CMD .bat .BAT .exe .EXE) do (
      set c=%%~xx
      if %%a==!c: !=! (
        for /f "skip=1 delims=" %%b in ('CertUtil -hashfile %%x SHA256 ^| findstr /i /v "CertUtil"') do set
b=%%b
        echo "https://www.virustotal.com/#!/file/!b: =!"
        REM Start "Chek SHA256 on VIRUSTOTAL" "https://www.virustotal.com/#!/file/!b: =!"
      )
    )
  )
)
```

pms - May 22, 2018, 12:37 pm

well written script, thank you a lot for sharing.

Erhan - May 26, 2018, 8:51 pm

Very useful script, thank you!