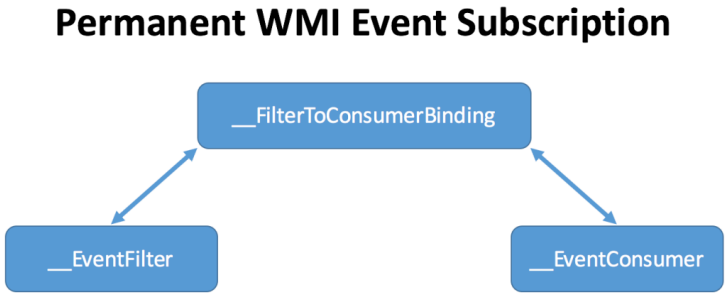
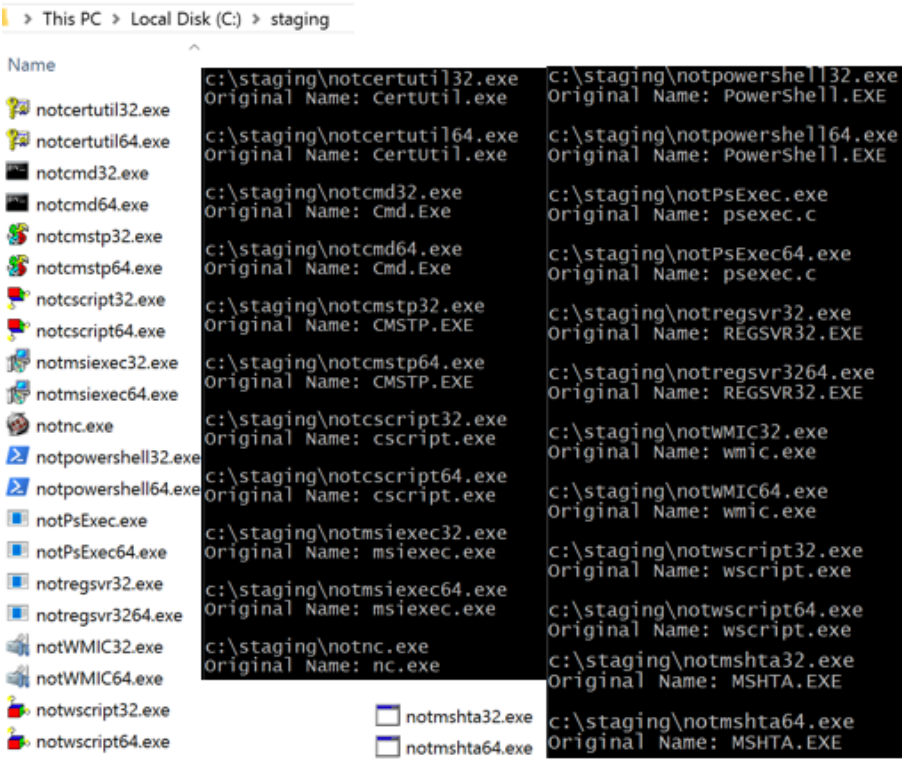

ARIZONA
EXPIRES
09-20-01
DRIVER LICENSE
LIC NO B0038182 CL D ENDORSEMENTS
EXPIRES 092001
NICK PAPPAGIORGIO
658 VIA DEL RAPOSA
YUMA AZ 85737
SEX WEIGHT HEIGHT EYES HAIR ORGAN DONOR
M 180 60 BR BN NO
ISSUE DATE RESTRICTION MED CODE BIRTHDATE
011596 011565
SIGNATURE OF APPLICANT
STA NO. B084415

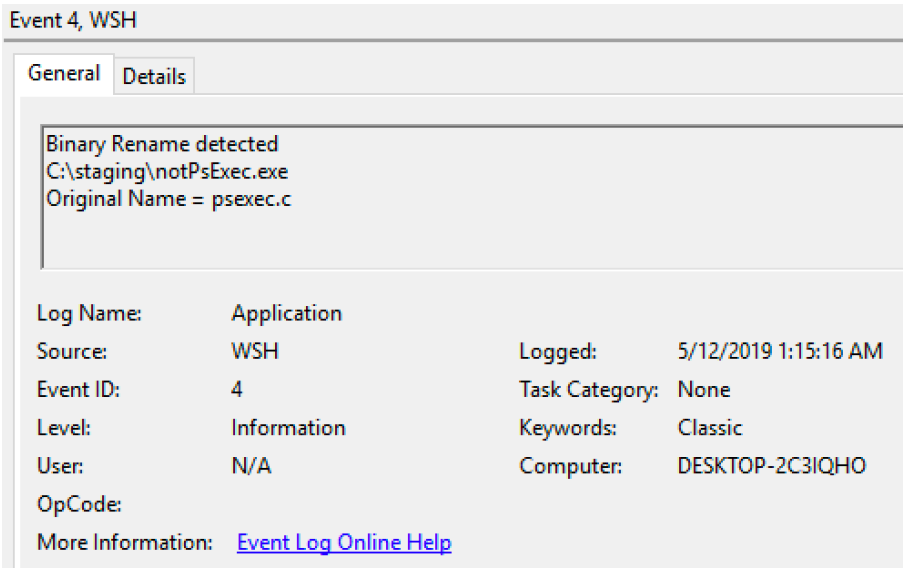
```
Function dfgfgeropu(DesDir As String)
    FileCopy DesDir & "\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs", DesDir & "\ProgramData\YANG.txt"

    Dim arcPath As String
    arcPath = DesDir & "\\Windows\\SysWOW64"
    If dirExists(arcPath) = True Then
        FileCopy DesDir & "\Windows\SysWOW64\wscript.exe", DesDir & "\ProgramData\YING.exe"
    Else
        FileCopy DesDir & "\Windows\System32\wscript.exe", DesDir & "\ProgramData\YING.exe"
    End If
End Function
```



```
$Name = 'BinaryRename_Example'
$Query = 'SELECT ProcessId FROM Win32_ProcessStartTrace'
$EventNamespace = 'root/cimv2'
$Class = 'ActiveScriptEventConsumer'
```


This PC > Local Disk (C:) > staging
Name
notcertutil32.exe
notcertutil64.exe
notcmd32.exe
notcmd64.exe
notcmstp32.exe
notcmstp64.exe
notcscript32.exe
notcscript64.exe
notmsiexec32.exe
notmsiexec64.exe
notnc.exe
notpowershell32.exe
notpowershell64.exe
notPsExec.exe
notPsExec64.exe
notregsvr32.exe
notregsvr3264.exe
notWMIC32.exe
notWMIC64.exe
notwscript32.exe
notwscript64.exe
notmshta32.exe
notmshta64.exe
c:\staging\notcertutil32.exe
Original Name: CertUtil.exe
c:\staging\notcertutil64.exe
Original Name: CertUtil.exe
c:\staging\notcmd32.exe
Original Name: Cmd.Exe
c:\staging\notcmd64.exe
Original Name: Cmd.Exe
c:\staging\notcmstp32.exe
Original Name: CMSTP.EXE
c:\staging\notcmstp64.exe
Original Name: CMSTP.EXE
c:\staging\notcscript32.exe
Original Name: cscript.exe
c:\staging\notcscript64.exe
Original Name: cscript.exe
c:\staging\notmsiexec32.exe
Original Name: msiexec.exe
c:\staging\notmsiexec64.exe
Original Name: msiexec.exe
c:\staging\notnc.exe
Original Name: nc.exe
c:\staging\notpowershell32.exe
Original Name: PowerShell.EXE
c:\staging\notpowershell64.exe
Original Name: PowerShell.EXE
c:\staging\notPsExec.exe
Original Name: psexec.c
c:\staging\notPsExec64.exe
Original Name: psexec.c
c:\staging\notregsvr32.exe
Original Name: REGSVR32.EXE
c:\staging\notregsvr3264.exe
Original Name: REGSVR32.EXE
c:\staging\notWMIC32.exe
Original Name: wmic.exe
c:\staging\notWMIC64.exe
Original Name: wmic.exe
c:\staging\notwscript32.exe
Original Name: wscript.exe
c:\staging\notwscript64.exe
Original Name: wscript.exe
c:\staging\notmshta32.exe
Original Name: MSHTA.EXE
c:\staging\notmshta64.exe
Original Name: MSHTA.EXE


Event 4, WSH
General
Details
Binary Rename detected
C:\staging\notPsExec.exe
Original Name = psexec.c
Log Name: Application
Source: WSH
Logged: 5/12/2019 1:15:16 AM
Event ID: 4
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: DESKTOP-2C3IQHO
OpCode:
More Information: Event Log Online Help

wmilog.txt

```
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcertutil32.exe|CertUtil.exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcertutil64.exe|CertUtil.exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcmd32.exe|Cmd.Exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcmd64.exe|Cmd.Exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcmstp32.exe|CMSTP.EXE
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcmstp64.exe|CMSTP.EXE
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcscript32.exe|cscript.exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notcscript64.exe|cscript.exe
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notmshta32.exe|MSHTA.EXE
2019-05-12T11:38Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notmshta64.exe|MSHTA.EXE
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notmsiexec32.exe|msiexec.exe
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notmsiexec64.exe|msiexec.exe
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notnc.exe|nc.exe
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notpowershell32.exe|PowerShell.EXE
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notpowershell64.exe|PowerShell.EXE
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notPsExec.exe|psexec.c
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notPsExec64.exe|psexec.c
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notregsvr32.exe|REGSVR32.EXE
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notregsvr3264.exe|REGSVR32.EXE
2019-05-12T11:39Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notWMIC32.exe|wmic.exe
2019-05-12T11:40Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notWMIC64.exe|wmic.exe
2019-05-12T11:40Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notwscript32.exe|wscript.exe
2019-05-12T11:40Z|DESKTOP-2C3IQHO|Binary Rename detected|C:\staging\notwscript64.exe|wscript.exe
```

```
cdm /c echo <string>
```

-
-
-
-
-
-