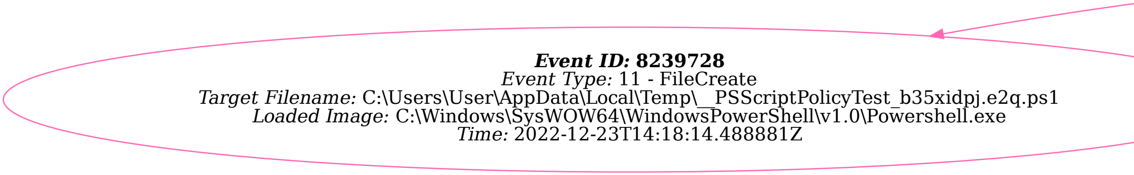
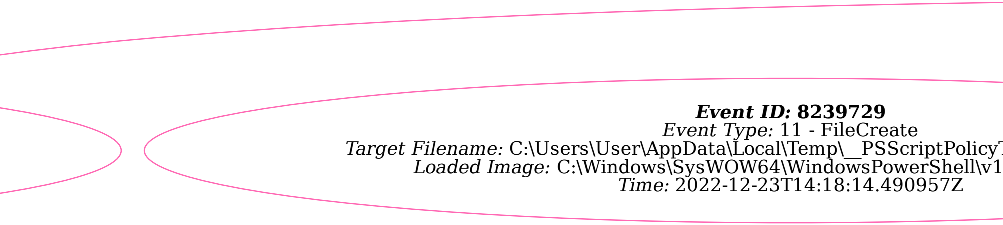
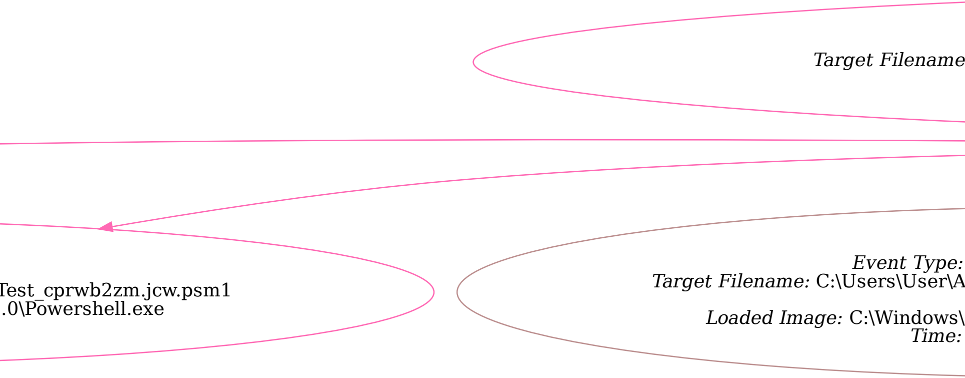
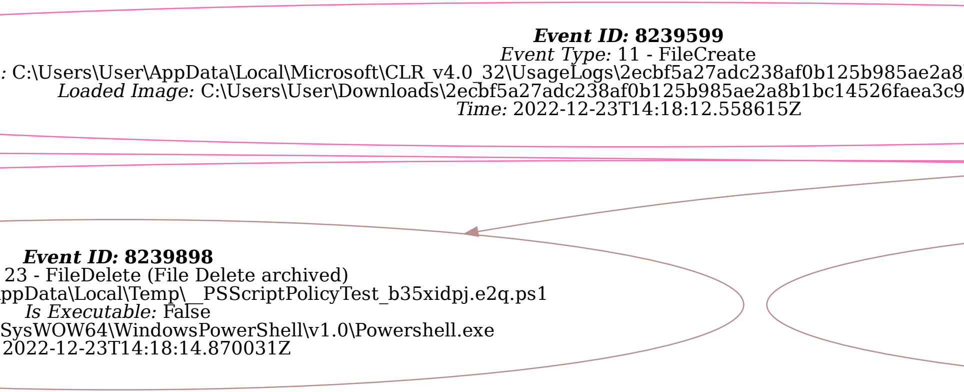


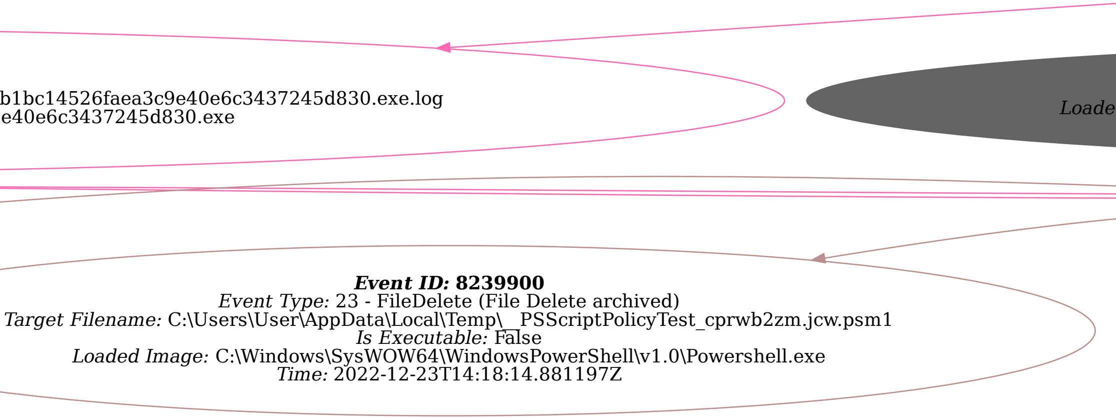
***Event ID:* 8239728**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyTest_b35xidpj.e2q.ps1
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T14:18:14.488881Z



***Event ID:* 8239729**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyT
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1
Time: 2022-12-23T14:18:14.490957Z


Target Filename
Test_cprwb2zm.jcw.psm1
.0\Powershell.exe
Event Type:
Target Filename: C:\Users\User\A
Loaded Image: C:\Windows\
Time:

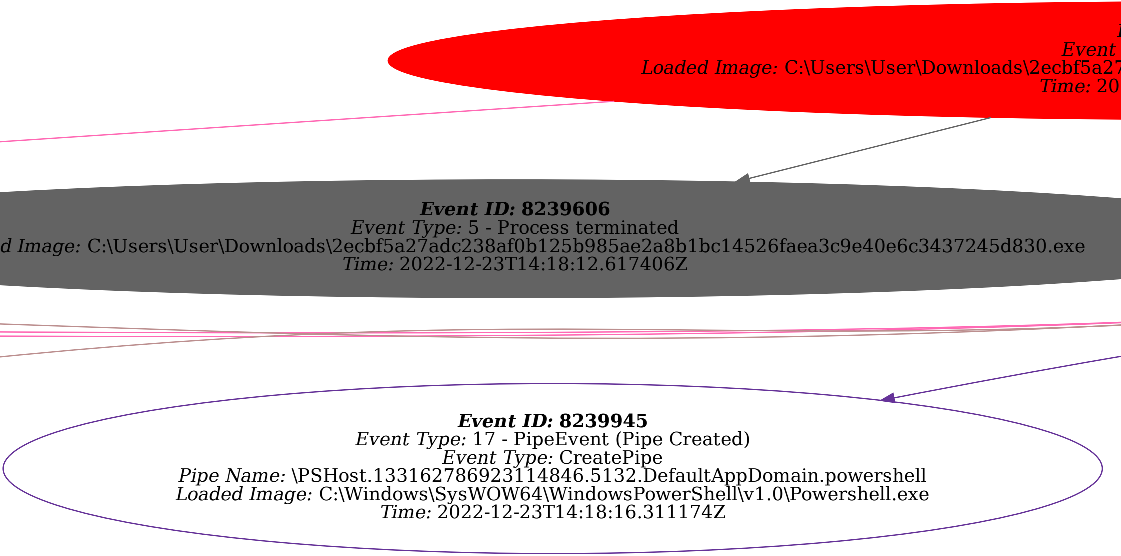

Event ID: 8239599
Event Type: 11 - FileCreate
: C:\Users\User\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2ecbf5a27adc238af0b125b985ae2a8
Loaded Image: C:\Users\User\Downloads\2ecbf5a27adc238af0b125b985ae2a8b1bc14526faea3c9
Time: 2022-12-23T14:18:12.558615Z
Event ID: 8239898
23 - FileDelete (File Delete archived)
ppData\Local\Temp\__PSScriptPolicyTest_b35xidpj.e2q.ps1
Is Executable: False
SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
2022-12-23T14:18:14.870031Z



b1bc14526faea3c9e40e6c3437245d830.exe.log
e40e6c3437245d830.exe

Loade

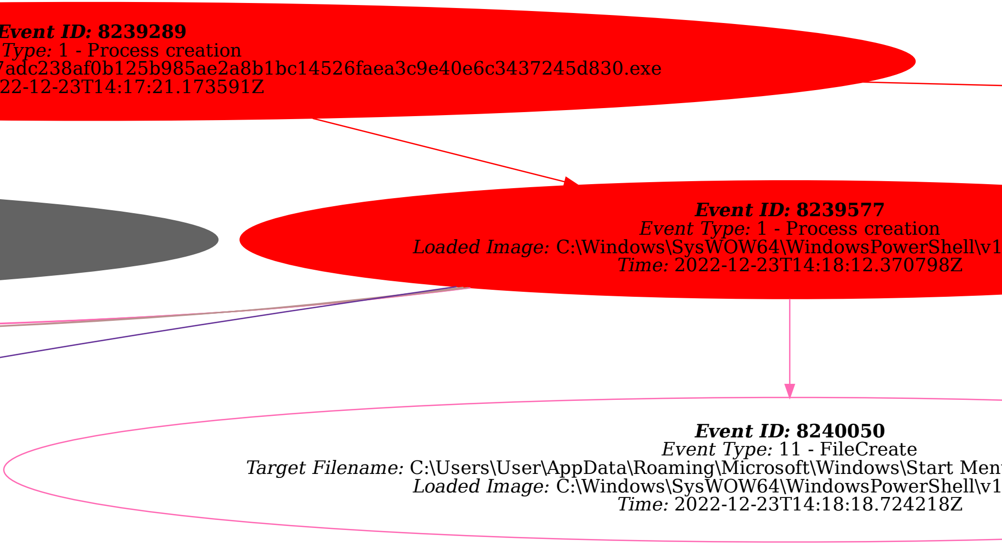
***Event ID:* 8239900**
Event Type: 23 - FileDelete (File Delete archived)
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyTest_cprwb2zm.jcw.psm1
Is Executable: False
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T14:18:14.881197Z

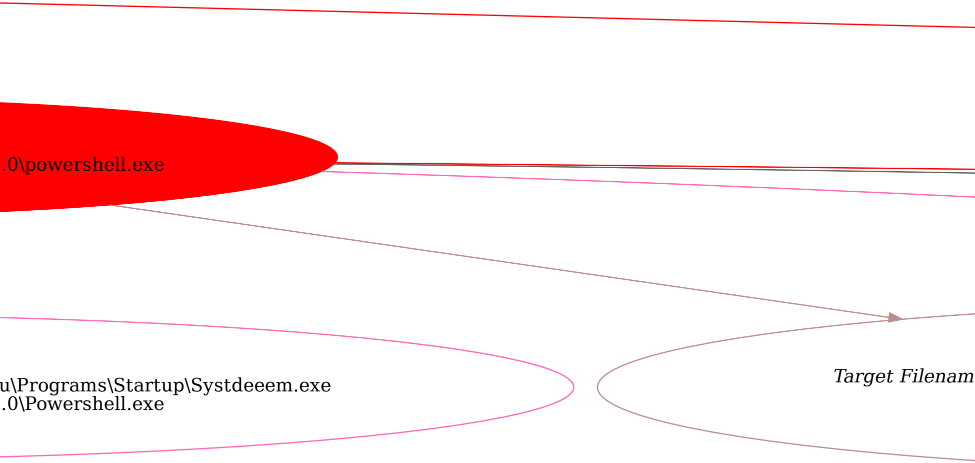


Event
Loaded Image: C:\Users\User\Downloads\2ecbf5a27
Time: 20

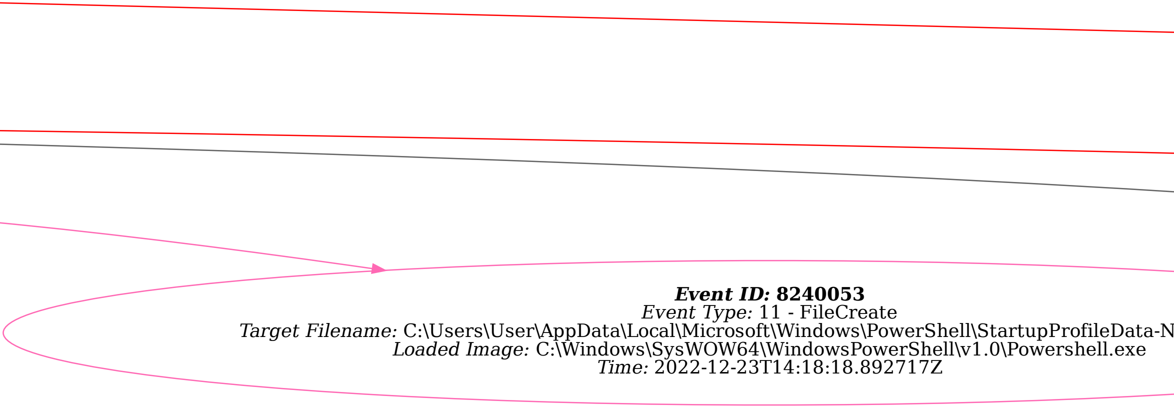
***Event ID:* 8239606**
Event Type: 5 - Process terminated
d Image: C:\Users\User\Downloads\2ecbf5a27adc238af0b125b985ae2a8b1bc14526faea3c9e40e6c3437245d830.exe
Time: 2022-12-23T14:18:12.617406Z

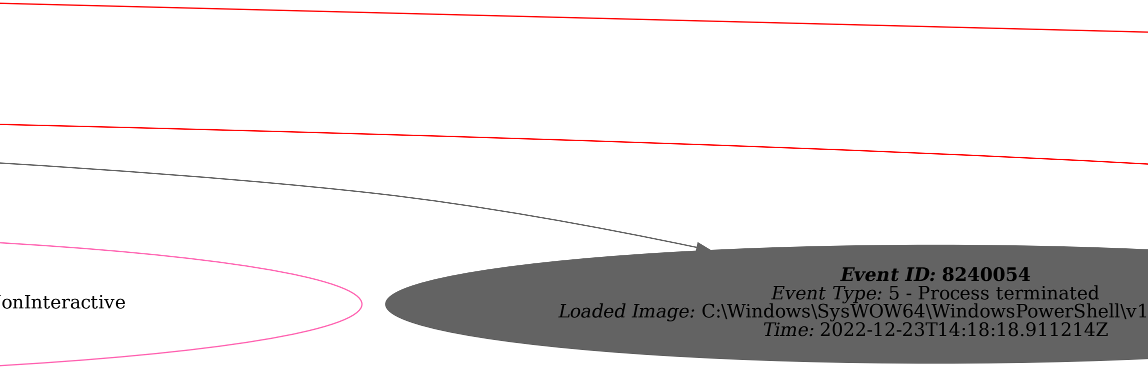
***Event ID:* 8239945**
Event Type: 17 - PipeEvent (Pipe Created)
Event Type: CreatePipe
Pipe Name: \PSHost.133162786923114846.5132.DefaultAppDomain.powershell
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T14:18:16.311174Z

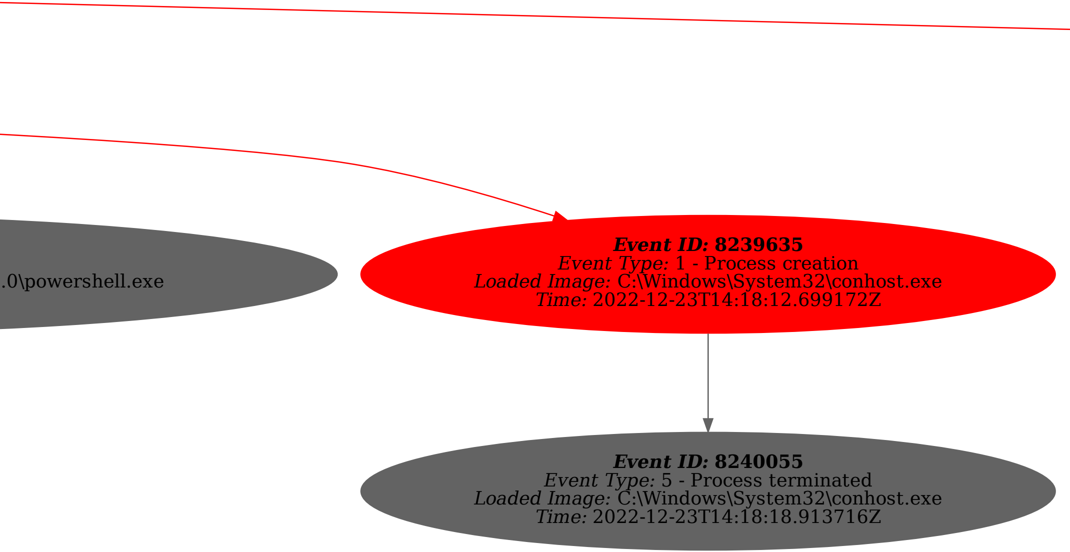

Event ID: 8239289
Type: 1 - Process creation
7adc238af0b125b985ae2a8b1bc14526faea3c9e40e6c3437245d830.exe
22-12-23T14:17:21.173591Z
Event ID: 8239577
Event Type: 1 - Process creation
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1
Time: 2022-12-23T14:18:12.370798Z
Event ID: 8240050
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Men
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1
Time: 2022-12-23T14:18:18.724218Z

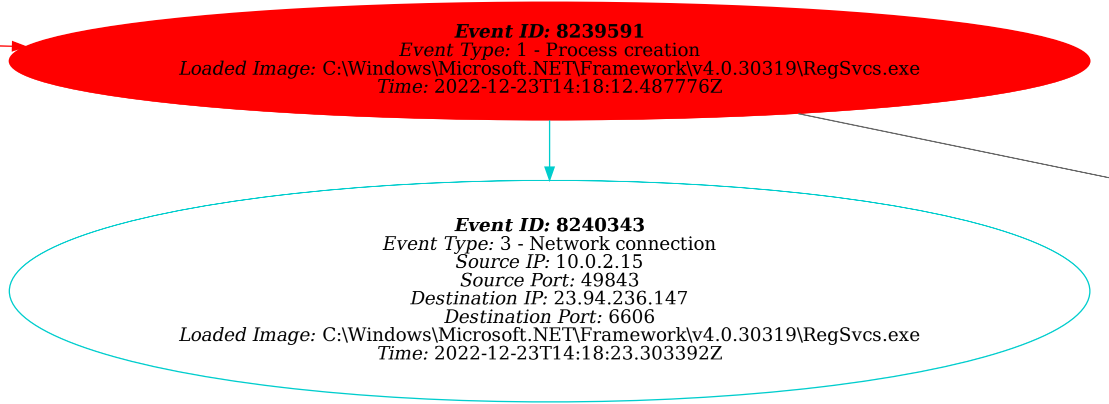

.0\powershell.exe
u\Programs\Startup\Systdeeem.exe
.0\Powershell.exe
Target Filenam

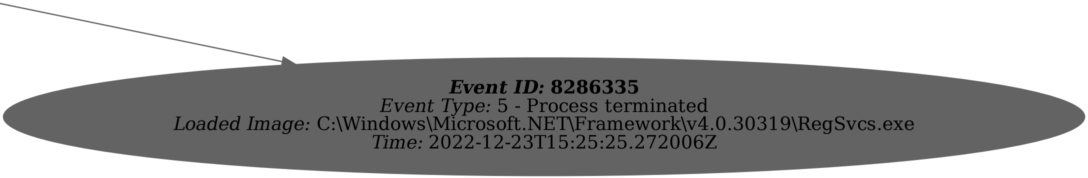
***Event ID:* 8240052**
Event Type: 23 - FileDelete (File Delete archived)
e: C:\Users\User\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
Is Executable: False
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T14:18:18.889113Z


***Event ID:* 8240053**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-N
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T14:18:18.892717Z


onInteractive
Event ID: 8240054
Event Type: 5 - Process terminated
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1
Time: 2022-12-23T14:18:18.911214Z


.0\powershell.exe
Event ID: 8239635
Event Type: 1 - Process creation
Loaded Image: C:\Windows\System32\conhost.exe
Time: 2022-12-23T14:18:12.699172Z
Event ID: 8240055
Event Type: 5 - Process terminated
Loaded Image: C:\Windows\System32\conhost.exe
Time: 2022-12-23T14:18:18.913716Z


Event ID: 8239591
Event Type: 1 - Process creation
Loaded Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Time: 2022-12-23T14:18:12.487776Z
Event ID: 8240343
Event Type: 3 - Network connection
Source IP: 10.0.2.15
Source Port: 49843
Destination IP: 23.94.236.147
Destination Port: 6606
Loaded Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Time: 2022-12-23T14:18:23.303392Z



***Event ID:* 8286335**
Event Type: 5 - Process terminated
Loaded Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Time: 2022-12-23T15:25:25.272006Z