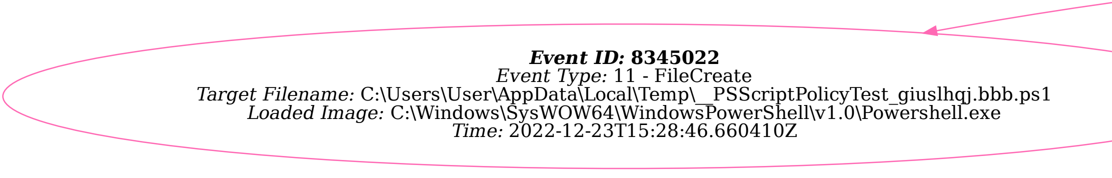
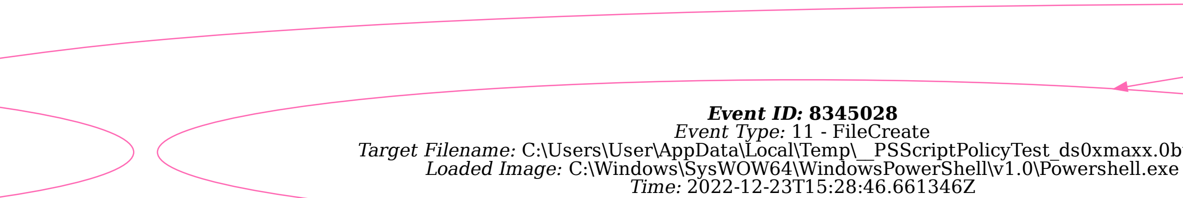
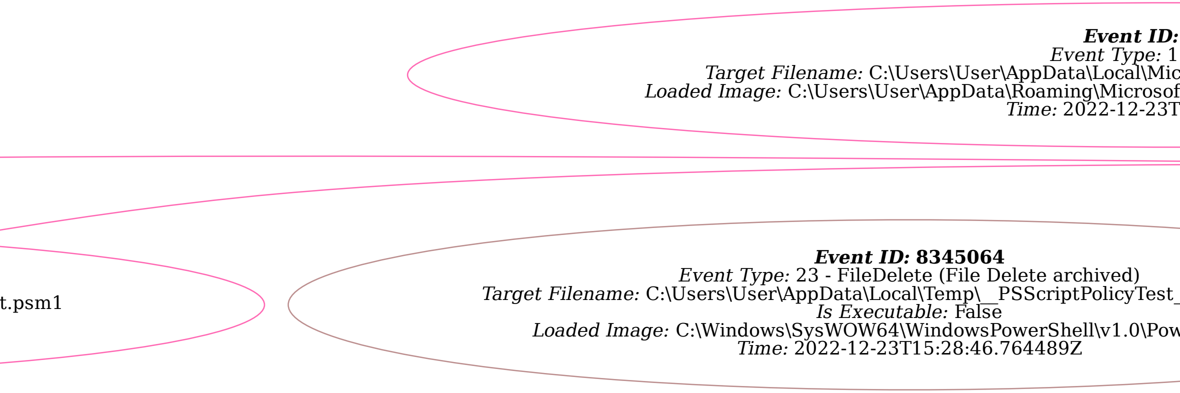


***Event ID:* 8345022**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyTest_giuslhqj.bbb.ps1
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T15:28:46.660410Z

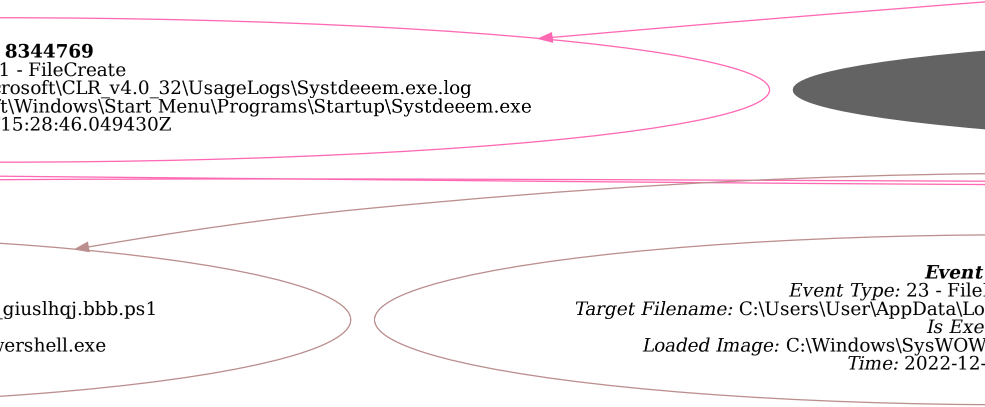

***Event ID:* 8345028**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyTest_ds0xmaxx.0b
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T15:28:46.661346Z

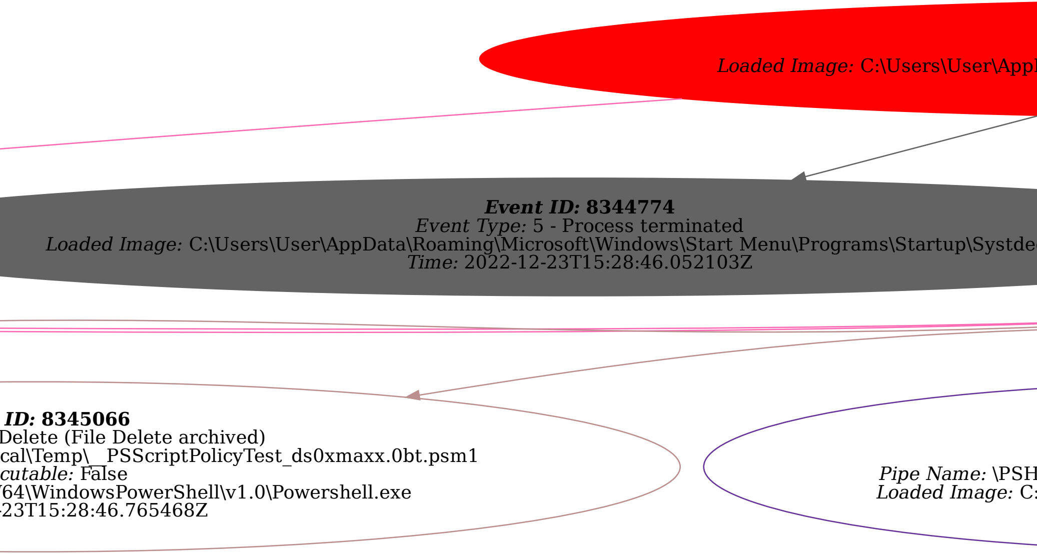


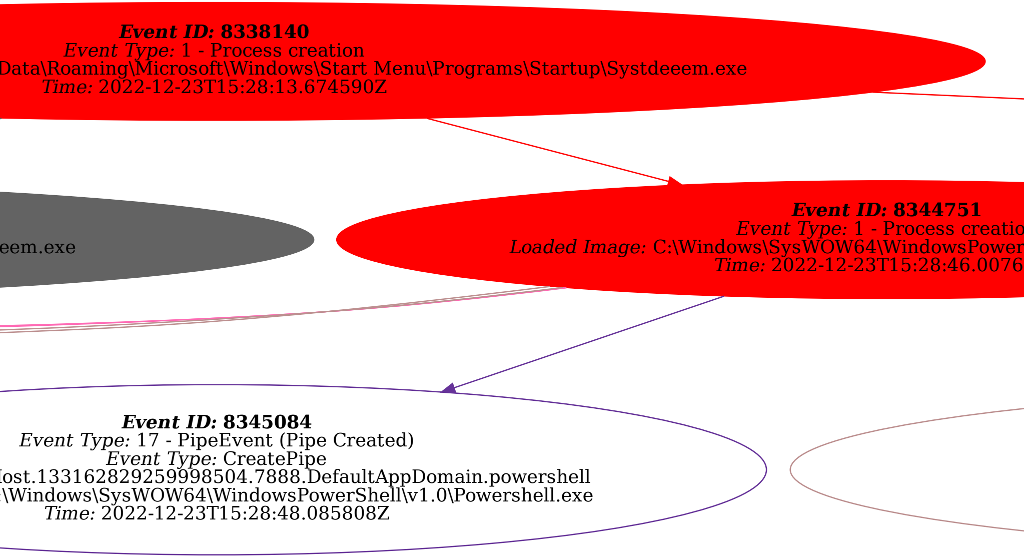
Event ID:
Event Type: 1
Target Filename: C:\Users\User\AppData\Local\Mic
Loaded Image: C:\Users\User\AppData\Roaming\Microsof
Time: 2022-12-23T

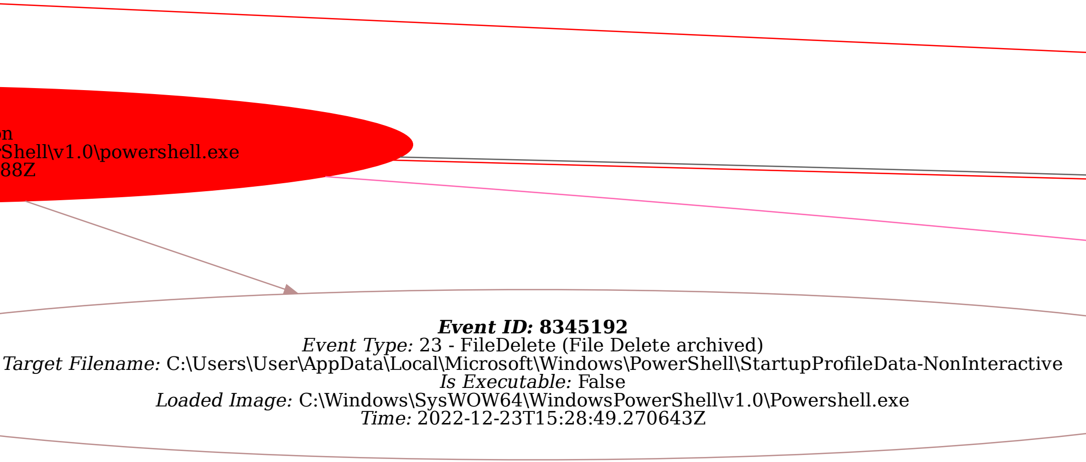
t.psm1

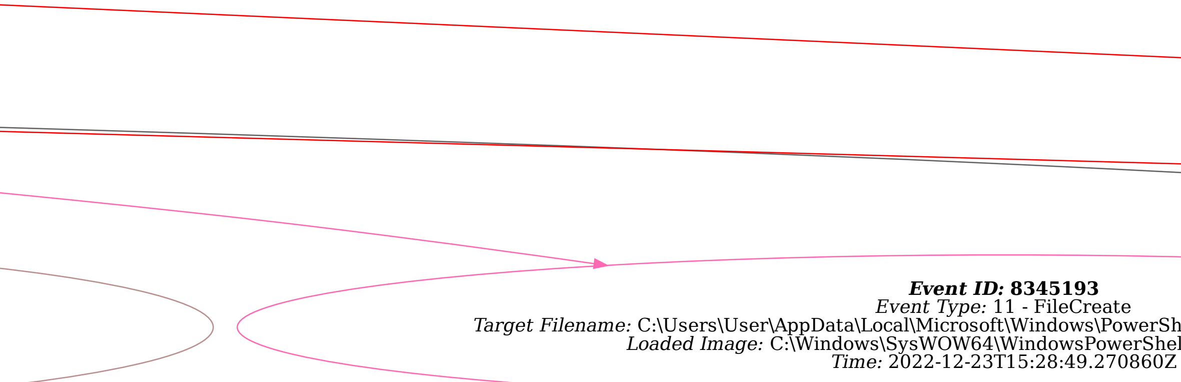
***Event ID:* 8345064**
Event Type: 23 - FileDelete (File Delete archived)
Target Filename: C:\Users\User\AppData\Local\Temp\__PSScriptPolicyTest_
Is Executable: False
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Pow
Time: 2022-12-23T15:28:46.764489Z

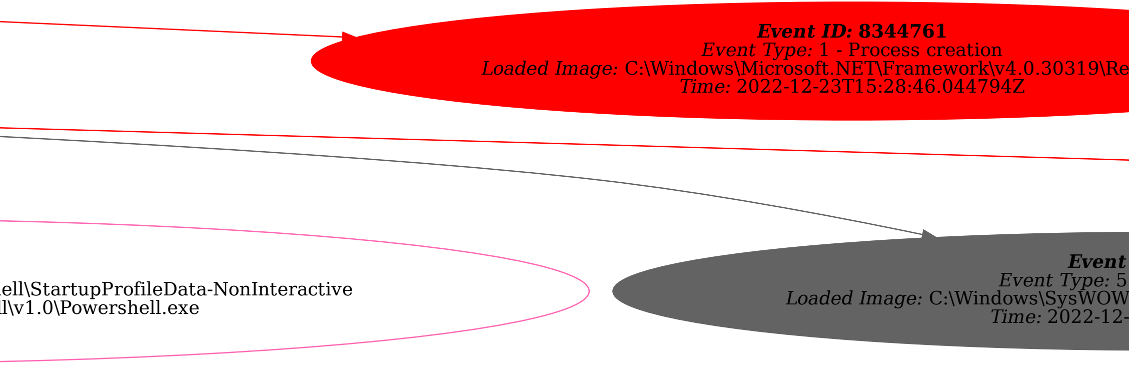

8344769
1 - FileCreate
rosoft\CLR_v4.0_32\UsageLogs\Systdeeem.exe.log
ft\Windows\Start_Menu\Programs\Startup\Systdeeem.exe
15:28:46.049430Z
_giuslhqj.bbb.ps1
vershell.exe
Event
Event Type: 23 - File
Target Filename: C:\Users\User\AppData\Lo
Is Exe
Loaded Image: C:\Windows\SysWOW
Time: 2022-12-

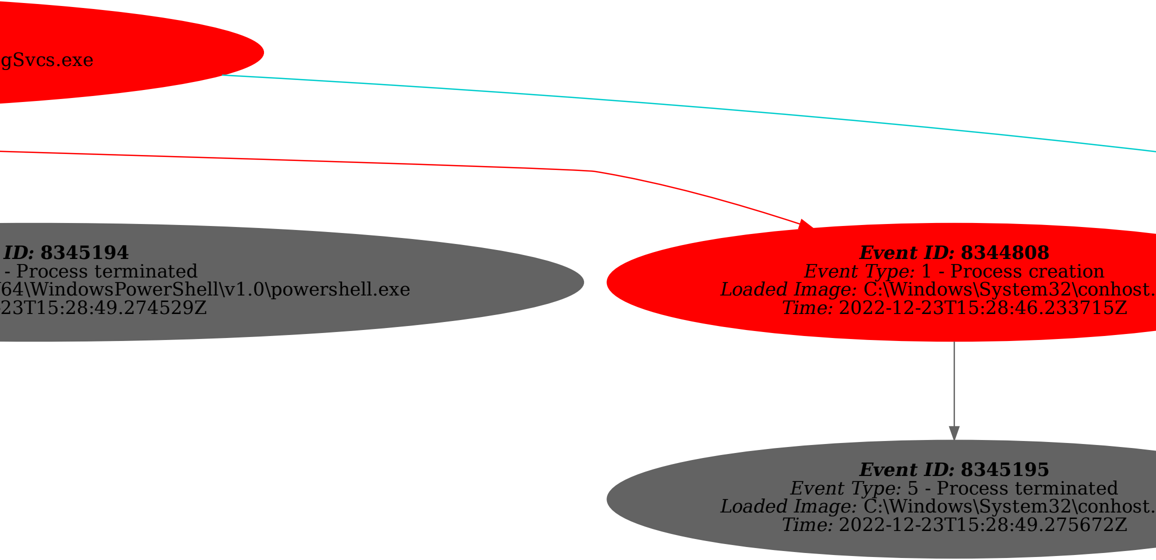

Loaded Image: C:\Users\User\AppI
Event ID: 8344774
Event Type: 5 - Process terminated
Loaded Image: C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Systdec
Time: 2022-12-23T15:28:46.052103Z
ID: 8345066
Delete (File Delete archived)
cal\Temp\__PSScriptPolicyTest_ds0xmaxx.0bt.psm1
cutable: False
/64\WindowsPowerShell\v1.0\Powershell.exe
-23T15:28:46.765468Z
Pipe Name: \PSH
Loaded Image: C:

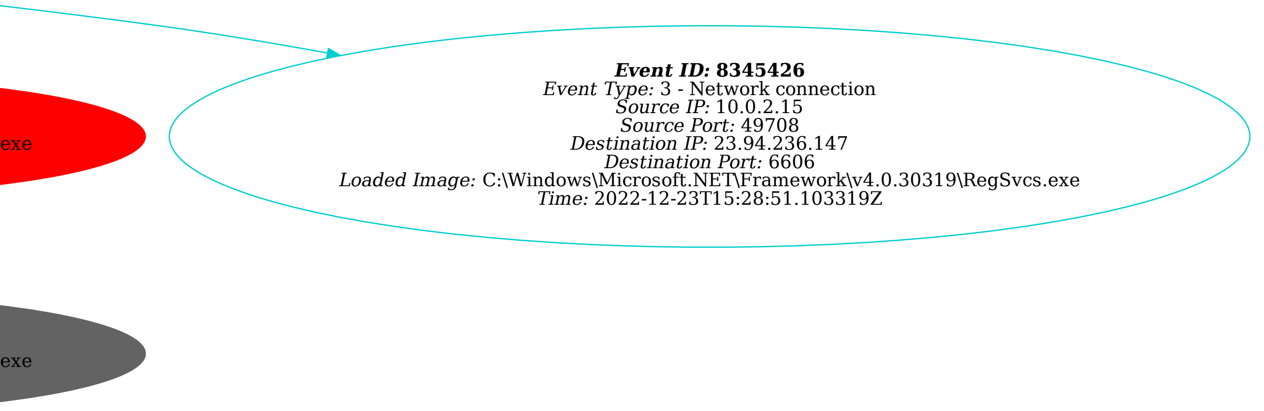

Event ID: 8338140
Event Type: 1 - Process creation
Data\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Systdeeem.exe
Time: 2022-12-23T15:28:13.674590Z
eem.exe
Event ID: 8344751
Event Type: 1 - Process creatio
Loaded Image: C:\Windows\SysWOW64\WindowsPower
Time: 2022-12-23T15:28:46.0076
Event ID: 8345084
Event Type: 17 - PipeEvent (Pipe Created)
Event Type: CreatePipe
Iost.133162829259998504.7888.DefaultAppDomain.powershell
:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T15:28:48.085808Z


on
Shell\v1.0\powershell.exe
88Z
Event ID: 8345192
Event Type: 23 - FileDelete (File Delete archived)
Target Filename: C:\Users\User\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
Is Executable: False
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Powershell.exe
Time: 2022-12-23T15:28:49.270643Z


Event ID: **8345193**
Event Type: 11 - FileCreate
Target Filename: C:\Users\User\AppData\Local\Microsoft\Windows\PowerSh
Loaded Image: C:\Windows\SysWOW64\WindowsPowerShel
Time: 2022-12-23T15:28:49.270860Z


Event ID: 8344761
Event Type: 1 - Process creation
Loaded Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Re
Time: 2022-12-23T15:28:46.044794Z
ell\StartupProfileData-NonInteractive
ll\v1.0\Powershell.exe
Event
Event Type: 5
Loaded Image: C:\Windows\SysWOW
Time: 2022-12-


gSvcs.exe
ID: 8345194
- Process terminated
/64\WindowsPowerShell\v1.0\powershell.exe
23T15:28:49.274529Z
Event ID: 8344808
Event Type: 1 - Process creation
Loaded Image: C:\Windows\System32\conhost.
Time: 2022-12-23T15:28:46.233715Z
Event ID: 8345195
Event Type: 5 - Process terminated
Loaded Image: C:\Windows\System32\conhost.
Time: 2022-12-23T15:28:49.275672Z



***Event ID:* 8345426**
Event Type: 3 - Network connection
Source IP: 10.0.2.15
Source Port: 49708
Destination IP: 23.94.236.147
Destination Port: 6606
Loaded Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Time: 2022-12-23T15:28:51.103319Z