New Search

```
1  sourcetype=_json datasource=sysmon event.code=13
2  | table timestamp host.name process.name registry.key registry.value
```

Last 24 hours

✓ **21 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:26:13.000 AM) No Event Sampling

Statistics (21)

timestamp	host.name	process.name	registry.key	registry.value
12/14/2025 05:03:09.369	win-3452		System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName	FriendlyName
12/14/2025 05:01:22.369	win-3456		System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName	FriendlyName
12/14/2025 05:01:10.369	win-3458	spoolsv.exe	System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName	FriendlyName
12/14/2025 05:00:06.369	win-3451	spoolsv.exe	System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName	FriendlyName
12/14/2025 04:53:49.369	win-3457	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion	driverVersion
12/14/2025 04:49:36.369	win-3460	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 4)\DsDriver\driverVersion	driverVersion
12/14/2025 04:46:54.369	win-3452		System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion	DriverVersion
12/14/2025 04:44:18.369	win-3449	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion	driverVersion
12/14/2025 04:43:27.369	win-3455	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion	driverVersion
12/14/2025 04:42:23.369	win-3450	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion	driverVersion
12/14/2025 04:41:15.369	win-3454	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5)\DsDriver\driverVersion	driverVersion

timestamp	host.name	process.name	registry.key	registry.value
12/14/2025 04:40:30.369	win-3449	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion	driverVersion
12/14/2025 04:34:02.369	win-3450		System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion	DriverVersion
12/14/2025 04:33:42.369	win-3456		System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName	FriendlyName
12/14/2025 04:32:12.369	win-3449	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion	driverVersion
12/14/2025 04:28:15.369	win-3457	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion	driverVersion
12/14/2025 04:25:36.369	win-3461	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion	driverVersion
12/14/2025 04:25:30.369	win-3455	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 4)\DsDriver\driverVersion	driverVersion
12/14/2025 04:25:22.369	win-3456	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion	driverVersion
12/14/2025 04:24:52.369	win-3456		System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion	DriverVersion
12/14/2025 04:24:12.369	win-3449	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion	driverVersion