New Search

```
1  sourcetype=_json datasource=sysmon event.code=22
2  | table timestamp host.name process.name dns.question.name dns.resolved_ip
```

Last 24 hours

✓ **21 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:27:01.000 AM) No Event Sampling

Statistics (21)

timestamp	host.name	process.name	dns.question.name	dns.resolved_ip
12/14/2025 05:02:29.369	win-3452	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 05:01:08.369	win-3453	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 05:00:30.369	win-3455	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 05:00:02.369	win-3457	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 04:54:25.369	win-3450	powershell.exe	2.tcp.ngrok.io	3.22.53.161
12/14/2025 04:54:24.369	win-3450	powershell.exe	raw.githubusercontent.com	185.199.111.133, 185.199.110.133, 185.199.109.133, 185.199.108.133
12/14/2025 04:52:08.369	win-3456	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:51:15.369	win-3460	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:51:14.369	win-3455	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:46:37.369	win-3456	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 04:46:27.369	win-3461	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 04:45:41.369	win-3451	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:44:01.369	win-3451	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 04:43:29.369	win-3454	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 04:43:13.369	win-3451	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:40:12.369	win-3454	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202

timestamp	host.name	process.name	dns.question.name	dns.resolved_ip
12/14/2025 04:37:55.369	win-3449	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 04:34:15.369	win-3456	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 04:29:36.369	win-3458	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 04:27:47.369	win-3455	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 04:25:20.369	win-3449	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10