Settings

Post

RawSec
@0xrawsec

This is one way to catch executables in ADS with #Sysmon

```
{
"Name": "ExecutableADS",
"Tags": ["ADS"],
"Meta": {
  "EventIDs": [15],
  "Channels": ["Microsoft-Windows-Sysmon/Operational"],
  "Computers": [],
  "Criticality": 10,
  "Author": "0xrawsec",
  "Comments": "Heuristics trying to catch EXE in ADS. If it is an EXE it is
  very likely the IMPHASH field is not null."
  },
"Matches": [
  "$impash:  Hash ~= '(?i:(IMPHASH=00000000000000000000000000000000))'"
  ],
"Condition": "!$impash"
}
```

11:15 AM · Jun 1, 2018

1 Repost **1** Quote **7** Likes **1** Bookmark