



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



1



New to X?

Sign up now to get your own personalized timeline!



Sign up with Google



Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.



Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#)
[Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies