Sign in

GossiTheDog / **ThreatHunting** Public

Notifications Fork 55 Star 567

Code Pull requests Actions Security Insights

ThreatHunting / AdvancedHuntingQueries / **DogWalk-DiagCab**

6 lines (5 loc) · 306 Bytes

Code Blame Raw

```
// blog = https://blog.0patch.com/2022/06/microsoft-diagnostic-tools-dogwalk.html
// some FPs if people download legit .diagcab files from websites

DeviceProcessEvents| where ProcessCommandLine contains @"msdt.exe"
| where ProcessCommandLine contains "/cab"
| where ProcessCommandLine contains ".diagcab"
```