Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

GossiTheDog / ThreatHunting Public

Notifications Fork 55 Star 568

Code Pull requests Actions Security Insights

Files

e85884a

Go to file

- AdvancedHuntingQueries
  - CVE-2021-36934-HiveNightma...
  - CVE-2021-36934-HiveNightma...
  - DogWalk-DiagCab
  - Follina-Office.ahq
  - Hunt-PrintNightmare
  - KaseyaRansomwarePayload.ahq
  - KaseyaVSAAgent-hunt.ahq
- AzureSentinel
- EDR-BlockRules
- YARA
- LICENSE
- README.md
- Threat hunting - Potential malwa...
- porg.jpg

ThreatHunting / AdvancedHuntingQueries / DogWalk-DiagCab

GossiTheDog Update DogWalk-DiagCab e85884a · 2 years ago History

Code Blame 6 lines (5 loc) · 306 Bytes 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"
```