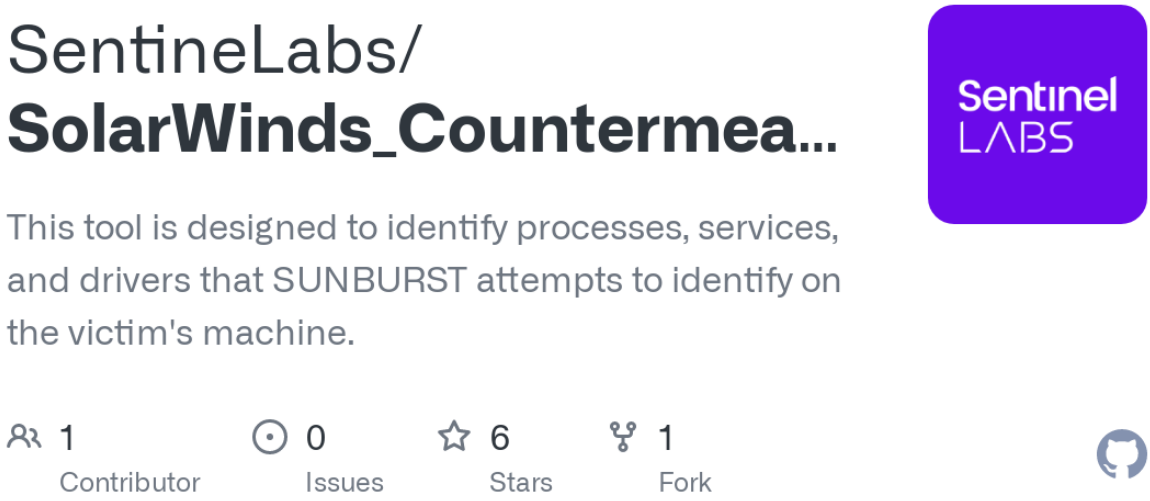
SolarWinds_Countermeasures

github.com/SentineLabs/SolarWinds_Countermeasures

SentineLabs



Description

This tool is designed to identify processes, services, and drivers that SUNBURST attempts to identify on the victim's machine.
This tool leverages the same logic SUNBURST uses to obtain a list of running processes/services/drivers, then applies the same hashing algorithm, and performs the blacklist check. The outcome/results of the blacklist check are then printed to the console.

Version 1 SHA1: 848b903a0f67f8fd71152b2b73a010fba547038c

Version 2 SHA1: d4910eaf5620528905b371c9a91fa5e3467978be

Version 3 SHA1: 37dc0e94a06257e91b041341f08dc435fe69d772

Example - when running on a system monitored by SentinelOne

```
C:\Users\infected\Desktop>S1_SUNBURST_Assessment.exe
SentinelLabs SUNBURST Assessment Tool Version 2
Description: This tool checks the current system for processes, services, and drivers
that SUNBURST attempts to identify in its blacklist, prints the match, as well as the
outcome.

[+] Checking running processes/services...
[+] Done checking running processes/services!
[+] Checking loaded drivers...
DRIVERS BLACKLIST MATCH: Loaded driver SentinelMonitor.sys matches hardcoded
blacklist hash 12343334044036541897
OUTCOME: SUNBURST will exit!

[+] Done checking loaded drivers!
```

Example - when running on a malware analyst machine

```
C:\Users\REM\Desktop>S1_SUNBURST_Assessment.exe
SentinelLabs SUNBURST Assessment Tool Version 2
Description: This tool checks the current system for processes, services, and drivers
that SUNBURST attempts to identify in its blacklist, prints the match, as well as the
outcome.

[+] Checking running processes/services...
BLACKLIST MATCH: Running process pestudio matches hardcoded blacklist hash
10235971842993272939
OUTCOME: SUNBURST will exit!

BLACKLIST MATCH: Running process dnSpy matches hardcoded blacklist hash
13825071784440082496
OUTCOME: SUNBURST will exit!

[+] Done checking running processes/services!
[+] Checking loaded drivers...
[+] Done checking loaded drivers!
```