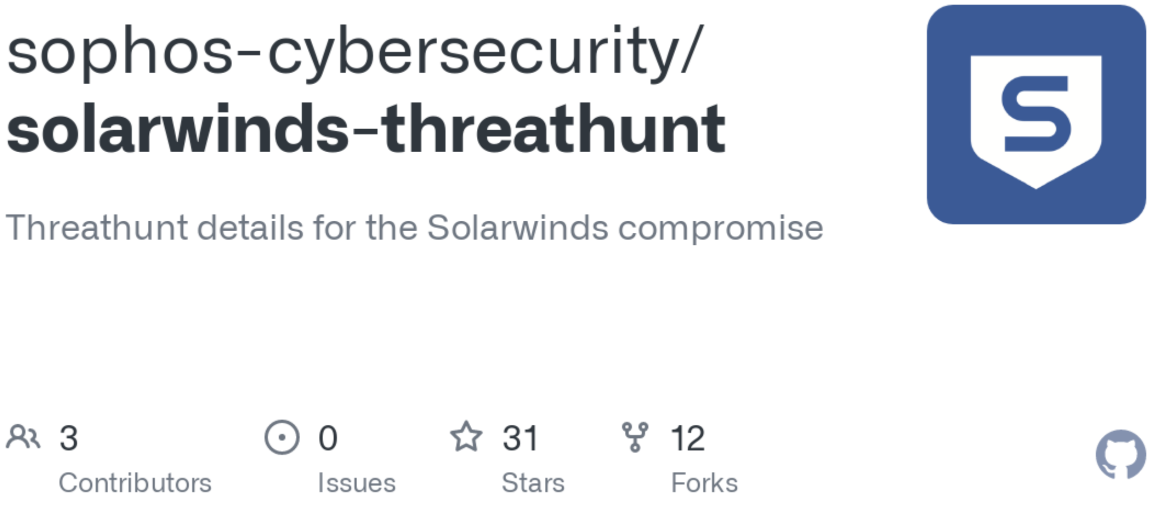
# Threathunt for the Solarwinds Compromise

github.com/sophos-cybersecurity/solarwinds-threathunt

sophos-cybersecurity



sophos-cybersecurity/
**solarwinds-threathunt**

Threathunt details for the Solarwinds compromise

3 Contributors

0 Issues

31 Stars

12 Forks

## IOCs

Published coallated IOCs for this attack

CSV of Published IOCs - https://github.com/sophos-cybersecurity/solarwinds-threathunt/blob/master/iocs.csv

RAW IOCs - https://raw.githubusercontent.com/sophos-cybersecurity/solarwinds-threathunt/master/iocs.csv

## Sophos Central Live Discover

Queries for Sophos Live Discover

1. Check if a server has Solarwinds and is vulnerable - https://github.com/sophos-cybersecurity/solarwinds-threathunt/blob/master/find-solarwinds.sql
2. Check for the specific IOCs listed by Fireeye - https://github.com/sophos-cybersecurity/solarwinds-threathunt/blob/master/ioc-hunt.md

## Splunk Searches

Useful Splunk searches for threathunting - https://github.com/sophos-cybersecurity/solarwinds-threathunt/blob/master/splunk-searches.md