GitHub - mandiant/sunburst_countermeasures

By Willi Ballenthin (Google)

Archived: 2026-04-05 12:45:23 UTC

FireEye Mandiant SunBurst Countermeasures

These rules are provided freely to the community without warranty.

In this GitHub repository you will find rules in multiple languages:

- Snort
- Yara
- IOC
- ClamAV

The rules are categorized and labeled into two release states:

- Production: rules that are expected to perform with minimal tuning.
- Supplemental: rules that are known to require further environment-specific tuning and tweaking to perform, and are often used for hunting workflows.

Please check back to this GitHub for updates to these rules.

FireEye customers can refer to the FireEye Community (community.fireeye.com) for information on how FireEye products detect these threats.

The entire risk as to quality and performance of these rules is with the users.

Please review the FireEye blog for additional details on this threat.

Please note: COSMICGALE and SUPERNOVA signatures and indicators are confirmed to detect malicious files and activity, however they have not been directly associated with the current UNC2452 Solarwinds compromise.

Source: https://github.com/fireeye/sunburst_countermeasures