Remove COSMICGALE and SUPERNOVA rules by itsreallynick · Pull Request #5 · mandiant/sunburst_countermeasures · GitHub

github.com/fireeye/sunburst_countermeasures/pull/5

mandiant

mandiant/sunburst_countermeasures

#5 Remove COSMICGALE and SUPERNOVA rules

2 comments 0 reviews 1 file +1 −50

itsreallynick • December 15, 2020 2 commits

Remove COSMICGALE rule

7e90a79

Please consider removing this Yara rule from the repo to reduce on-going industry confusion. Based on my analysis, shared with FEYE pre-publication on 2020-12-10, this unsigned SolarWinds "plugin" DLL may be abused maliciously - but that post-exploitation activity and filewrites occur within inetpub in-the-wild and are more indicative of web-facing exploitation with artifacts more similar to CVE-2019-8917.

As there is no tied to the software supply chain compromises, we are not currently tracking this as the same threat actor - and my understanding is that FireEye is also no longer tracking this as UNC2452. Since COSMICGALE is not referenced in the blog with this delineation, it's probably better to remove entirely to reduce industry confusion.

-YOUR BOY CARR

Remove COSMICGALE and SUPERNOVA

de96774

Removed COSMICGALE and SUPERNOVA rules as intended.