SUNBURST SolarWinds Malware - Tools, Tactics and Methods to get you started with Reverse Engineering

By @DhrubapadaSinha

Published: 2020-12-18 · Archived: 2026-04-02 10:52:21 UTC

Here we take a look inside so of the most complex, elegant, well-crafted malware I've seen, known as SUNBURST and responsible for the global SolarWinds compromise. This code is a malicious DLL, loaded by the parent platform and blends in exceptionally well to the whole code-ecosystem. We start by using DNSpy to decompile the .NET code, giving us access to the source code and I show you my methodologies for finding stuff of interest and how to go down the rabbit hole with your analysis. We cover FNV-1 hashing (something I'd never heard of!) and also variances of the Base64 encoding routine which the bad guys are using the mask their malicious code. This is one of the most fascinating backdoors I've had hands on, and there is much more to come with the analysis and I'd love to hear how you get on pulling a part this code too. Special thanks to the folks at FireEye, their research on this malware is exceptional. LINKS ===== https://www.fireeye.com/blog/threat-r... https://github.com/fireeye/sunburst_c... https://www.volexity.com/blog/2020/12... https://us-cert.cisa.gov/ncas/alerts/... https://cyber.dhs.gov/ed/21-01/ https://en.wikipedia.org/wiki/Fowler%... TOOLS ====== dnSpy - https://github.com/dnSpy/dnSpy PeStudio - https://www.winitor.com FNV-1 Hashing tool - https://github.com/cybercdh/hacks/tre... SAMPLE ======= https://app.any.run/tasks/4fc6b555-4f... FOLLOW ====== You can join in the conversation by following me at _/ cybercdh_ THANKS ======= If you LIKED this video, please hit the THUMBS UP. If you LOVED it, please SUBSCRIBE! Many thanks for watching, it means a lot. Peace out. @cybercdh

---