Detect SUNBURST Backdoor Attack With Corelight & Zeek | Corelight

By John Gamble

Published: 2020-12-15 · Archived: 2026-04-05 18:48:05 UTC

Home/Blog/Finding SUNBURST backdoor...

Zeek

UPDATE 12-16-20: Corelight Resources

- WEBCAST RECORDING – Finding SolarWinds backdoors with Zeek, Suricata & Corelight – **watch here**
- WEBCAST SLIDE DECK – **download link**
- IOCs SPREADSHEET – **Corelight/Zeek Queries Table – to hunt for Sunburst IOCs**

FireEye's threat research team has **discovered** a troubling new supply chain attack targeting SolarWind's **Orion** IT monitoring and management platform. The attack trojanizes Orion software updates to deliver malware called SUNBURST, which opens a stealthy backdoor for command-and-control and other malicious activity that blends in with Orion Improvement Program (OIP) protocol traffic.

Scott Runnels, a Mandiant researcher involved in the discovery, **revealed** that Zeek played a key role in FireEye's investigation and discovery of this new threat:

Given the widespread use of the Orion software we want to provide the community and our customers with some preliminary guidance on how to use Zeek and related tools to manually find and automatically detect this novel threat in their environment.

We will host a webinar this **Wednesday, Dec. 16 t**o deep dive on these methods and tools, which include:

- **Zeek log queries**: Network IOCs for this attack span a range of protocols parsed by Zeek including DNS, HTTP, and X509 certificates. Targeted queries in your SIEM against Zeek logs can reveal potential evidence of compromise related to this attack, for example:

Source	Log	Fields	Splunk Log Query	Raw Zeek Logs Query
FireEye	http	host	path="http" | spath host | where host="*.avsvmcloud.com"	zgrep "awsvmcloud.com" *http*
FireEye	http	uri, host	path="http" uri="swip/upd/*" | spath host | where host!="*.solarwinds.com"	zgrep "swip/upd/" *http* | grep -v solarwinds.com
FireEye	dns	subject	path="dns" query="*awsvmcloud.com"	zgrep "awsvmcloud.com" *dns*

- **Sigma rules/queries**: Community-developed Sigma rules to detect SUNBURST are available in SOC Prime's Threat Detection Marketplace, which you can access **here**. Corelight customers with supported SIEM platforms (Splunk, Elastic, Humio, QRadar, ArcSight, Chronicle, et al.) can copy/paste the queries and/or detections directly into their SIEM environment.

- **Suricata Rules in ET Open Ruleset**: Proofpoint Emerging Threats has added detections as Suricata rules in their latest ET Open Ruleset release, which you can download **here**. Corelight customers with AP 200, AP 1001, and/or AP 3000 Sensors and a Suricata subscription can download and run these rules on their sensors.

Again, we will host a webinar on Wednesday, Dec. 16 at 7a PST / 10a EST / 3p GMT to deep dive on these methods and tools.

If you would like to attend, please register here: https://www3.corelight.com/finding-sunburst-solarwinds-zeek-suricata

---

Source: https://corelight.blog/2020/12/15/finding-sunburst-backdoor-with-zeek-logs-and-corelight/