Detecting Supernova web shell malware

Your company uses SolarWinds Orion business software, which is vulnerable to the Supernova malware attack. This attack exposes SolarWinds Orion via an in-memory web shell. Supernova leverages what was a zero-day vulnerability to install a trojanized .NET DLL. This DLL is not digitally signed like the Sunburst DLL was, which is one of the reasons multiple researchers believe that this is a different threat actor using a vulnerability to load their malicious code to vulnerable systems. The malware that is loaded is a web shell. This MITRE ATT&CK technique, T1505, is used by adversaries to backdoor web servers and establish persistent access to systems. You know you need to patch your SolarWinds software, but you also need to look for signs that your systems have been compromised.

Required data

- Vulnerabilities
- Endpoint
- Web

How to use Splunk software for this use case

Depending on what information you have available, you might find it useful to identify some or all of the following:

- Systems vulnerable to Supernova malware
- File hashes associated with the Supernova trojanized DLL
- DLL loaded in a specific process
- .NET assemblies being compiled
- Web shell present in web traffic events

Next steps

After running each of the searches, you will need to gather evidence, remove the malware, and remediate the vulnerability.

The content in this use case comes from previously published blogs, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:

- Blog: SUPERNOVA Redux, with a generous portion of masquerading
- Blog: Using Splunk to Detect Sunburst Backdoor

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Blog: Onboarding Threat Indicators into Splunk Enterprise Security: SolarWinds Continued