Leverage PAVO in your security searches for the Sunburst cyberattack

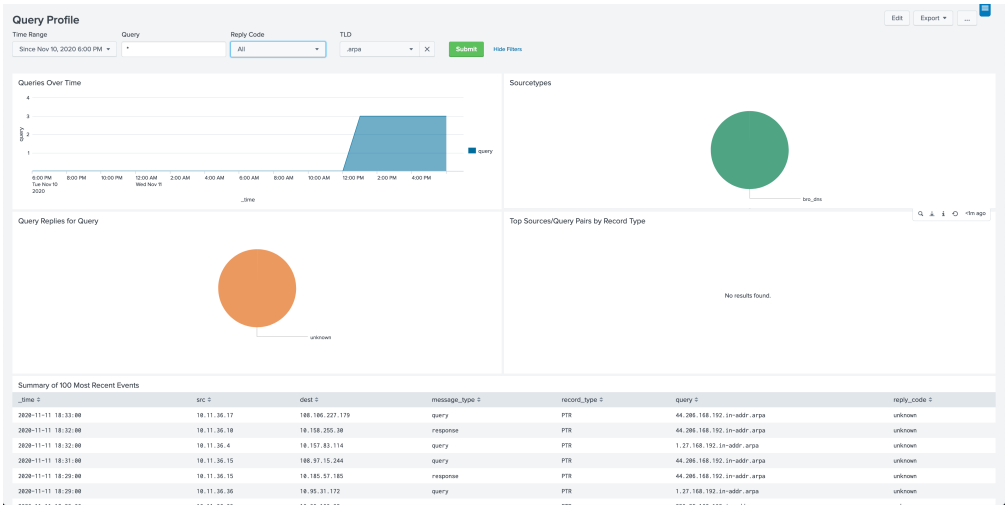
Everyone was taken aback by the scope of the SolarWinds cyberattack, Sunburst. As more details of the attack were released by various organizations around the world, our clients found an advantage in already having a Splunk Dashboard created that could search for key indicators of compromise. Here is what they used.

Sunburst, in short, is malware that spreads via a compromised vender supply chain (software update of a popular tool), that then uses a command-and-control network to download malicious payloads or instructions.

One of the best ways to search for indicators of compromise is to search for the DNS calls or Network Traffic to the malicious command and control network. Enter, the PAVO Network Traffic App for Splunk and PAVO DNS App for Splunk.

Our clients used the *IP Profile* and *Network Traffic Search* Dashboards in the Network Traffic App to look for IP addresses associated with the Sunburst attack. The bad actors associated with these types of attacks often change IP addresses, thus making it hard to maintain a watchlist. Most clients quickly pivoted to search for related domain names. In this case the domain *avsvmcloud[.]com* has been identified by industry security experts.

Additionally, our clients used the *Query Profile* Dashboard in our DNS App to quickly search for the aforementioned domain. If any communications are found, the *Query Profile* Dashboard provides valuable information such as time, source, destination and type of query to jump start the investigation.



You may have already vetted your network against Sunburst, but PAVO can provide other valuable advantages for you. This is a real-world example for keeping and using PAVO in your Splunk deployment. Access PAVO here for any further needs.