This must-see talk discusses a highly-regarded but rarely publicly investigated threat actor, malware similarity, and YARA. Publicly available data yields just a generic AV signature with the actor's name, leaving a void for malware analysts looking to understand the overlaps between different malware families attributed to the same actor.

Greg Lesnewich explores how analysts can use YARA as an analyzer with the console output, leveraging some simple Python scripting, to develop a malware similarity methodology. With a little – but not too much! – effort, analysts can easily build their own custom malware analysis toolkits using nothing other than freely available open source projects.

Greg's presentation highlights just how well YARA can be used to pursue an apex predator and contains plenty of examples and links to all the tools used in the talk. Greg also shares the custom tooling he built as he analyzed a notorious threat actor, which can easily be adopted or adapted by other analysts to suit their own purposes.

About the Presenter
Greg Lesnewich is senior threat researcher at Proofpoint, working on tracking malicious activity linked to the DPRK (North Korea). Greg has a background in threat intelligence, incident response, and managed detection, and previously built a threat intelligence program for a Fortune 50 financial organization.

About LABScon
This presentation was featured live at LABScon 2022, an immersive 3-day conference bringing together the world's top cybersecurity minds, hosted by SentinelOne's research arm, SentinelLabs.

Want to join us for LABScon 2023? The Call for Papers is now open!