Speaker: Joe Johnson, Software Engineer, ICEBRG (recently acquired by Gigamon)

Analyzing Active Long Running Connections with Bro

Long running connections are often an indicator or a compromise or other malicious activity. By default, Bro will log the connection details once the connection closes. However, it does not provide visibility into these connections out of the box. This presentation will discuss using features already in Bro to provide visibility into long running connections as they are happening and why that is valuable. Additionally, the presentation will discuss the use cases and security incidents that led to needing visibility into a connection before it was closed. Finally, it will cover some of the challenges of working with this data and a few pitfalls and bugs (with fixes) in generating this data with Bro.