A One Year Study of Enterprise/Government IoT and Botnet

Craig Labovitz, Ph.D.
Chief Technology Officer, Network Intelligence, Analytics, and DDoS Security
Nokia Deepfield

Nokia will present results from a one-year study of IoT device behaviors across government and enterprise networks around the world. Using honeypots, active device crawling / discovery and real-time, passive security telemetry from collaborating CSP, Nokia tracked both legitimate and malicious activity across 50+ million devices in 2022. Nokia will focus our talk on a 500K subset of IoT / CPE devices actively engaged in DDoS, scanning and other malicious activity. Nokia will show examples of specific U.S. government and DoD endpoints co-opted into ongoing attacks against enterprise and extra-national governmental infrastructure throughout the Internet. Lastly, we will consider network architecture requirements for mitigating these attacks.