Tuesday, June 2

4:20 pm – 4:40 pm

Machine-Speed Conflict: What Internet-Scale Data Reveals About Threat Actor Evolution

Nishawn Smagh

Director of Intelligence

GreyNoise Intelligence

Abstract:

GreyNoise telemetry indicates that cyber adversaries are gaining access to vulnerabilities prior to public disclosure. The research indicates that threat actors employ AI-assisted reconnaissance and machine-speed exploitation, compressing vulnerability weaponization timelines from weeks to hours. Most significantly, it reveals that attacker behavior itself offers predictive signals: An analysis of 216 malicious activity spikes from the GreyNoise Global Observation Grid revealed that 80% preceded CVE disclosures by up to six weeks.

This presentation summarizes 12 months of internet-scale threat telemetry from GreyNoise's Global Observation Grid, revealing fundamental shifts in adversary structures, motivations, and operational tactics. Through analysis of billions of malicious observations, we document the industrialization of cyber operations—where threat actors operate as distributed automation ecosystems rather than individual operators.

The key take-away is that attacker behavior offers predictive signals, providing defenders with an actionable early warning window. Defense must evolve comparably—leveraging automation, behavioral analytics, and predictive intelligence derived from internet-scale observation