Cybersecurity & Malware Analysis

Research Statement: Cybersecurity, Digital Forensics & Malware Analysis

My cybersecurity research centers on understanding adversarial behavior, malware evolution, and data■driven threat■intelligence pipelines. I focus on fileless malware, reverse engineering, memory forensics, and anomaly detection methods that leverage mathematical modeling and machine learning.

Key areas of focus:

• Behavioral and memory■resident analysis of fileless malware.

• Static and dynamic reverse engineering using disassembly, sandboxing, and instrumentation.

• Threat intelligence correlation and MITRE ATT&CK;■based adversary profiling.

• SIEM■driven anomaly detection and event correlation using statistical and ML models.

• Network packet forensics using Wireshark, Suricata, and Zeek.

My long■term research goal is to develop computational methods that strengthen detection and response workflows, enabling defenders to anticipate and disrupt modern cyber threats.