Exploring Agentic AI in Anti-Forensics

Simulation of Evasion Tactics in Digital Investigations

Ifeoluwa Ojuolape-Oria
I.H.Ojuolape-Oria@edu.salford.ac.uk
University of Salford, Manchester

Authors
- Oseodion Ofeimun
- Emmanuel Orji
- Dr Olayinka Adeboye
- Aderemi Adenihun
- Segun Akinseye

Do attackers always leave traces?

Enterprise Monitoring Limitation (Wazuh/Splunk)

- Relies on periodic scanning (Not continuous)
- Misses short-lived activity
- Creates detection blind spots

Research Gap

- Known in theory (TOCTOU)
- Not tested with autonomous AI attackers
- Lacks empirical Validation

Our Contribution

- Designed Anti-Gravity autonomous agent
- Executes full anti-forensic kill chain
- Empirically demonstrates complete evasion

Methodology Overview

- Phase 1: Rule-based baseline
  - limited
- Phase 2: Autonomous Agent
  - evaluation

Experimental Setup

- Linux + Windows systems
- SIEM (Wazuh, Splunk)
- Kernel monitoring (auditd)

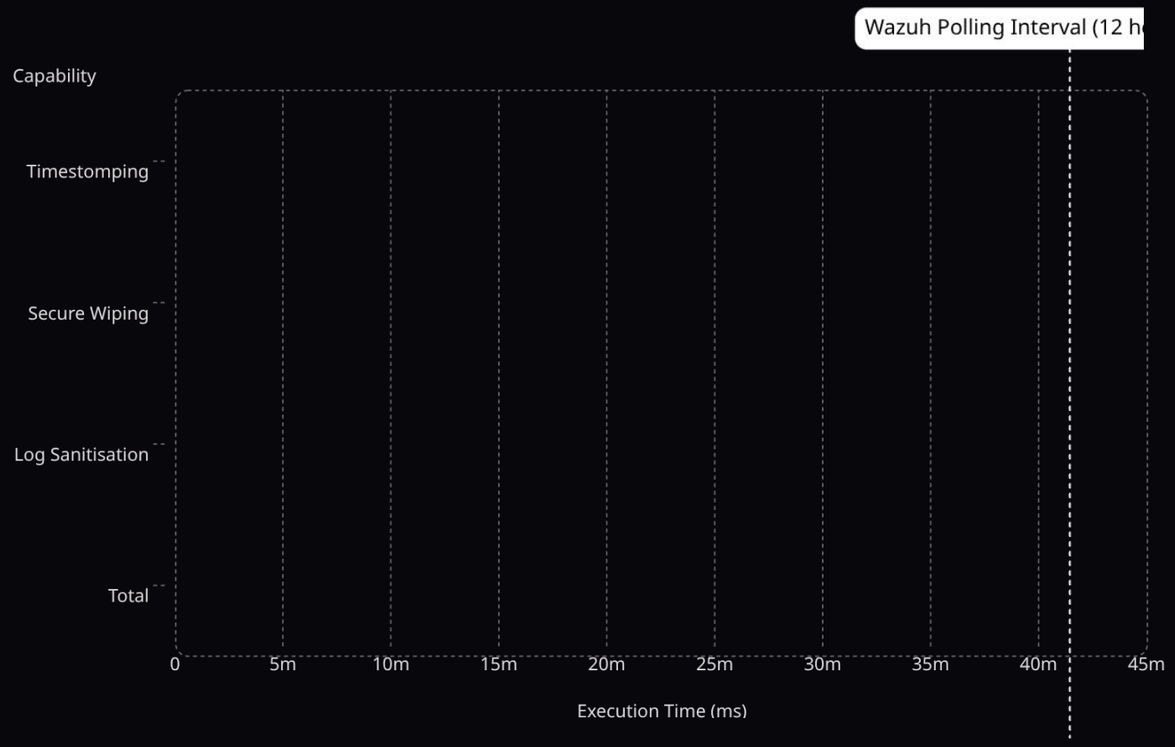
Agent Capabilities

Timestomping → Secure Wiping → Log Sanitisation

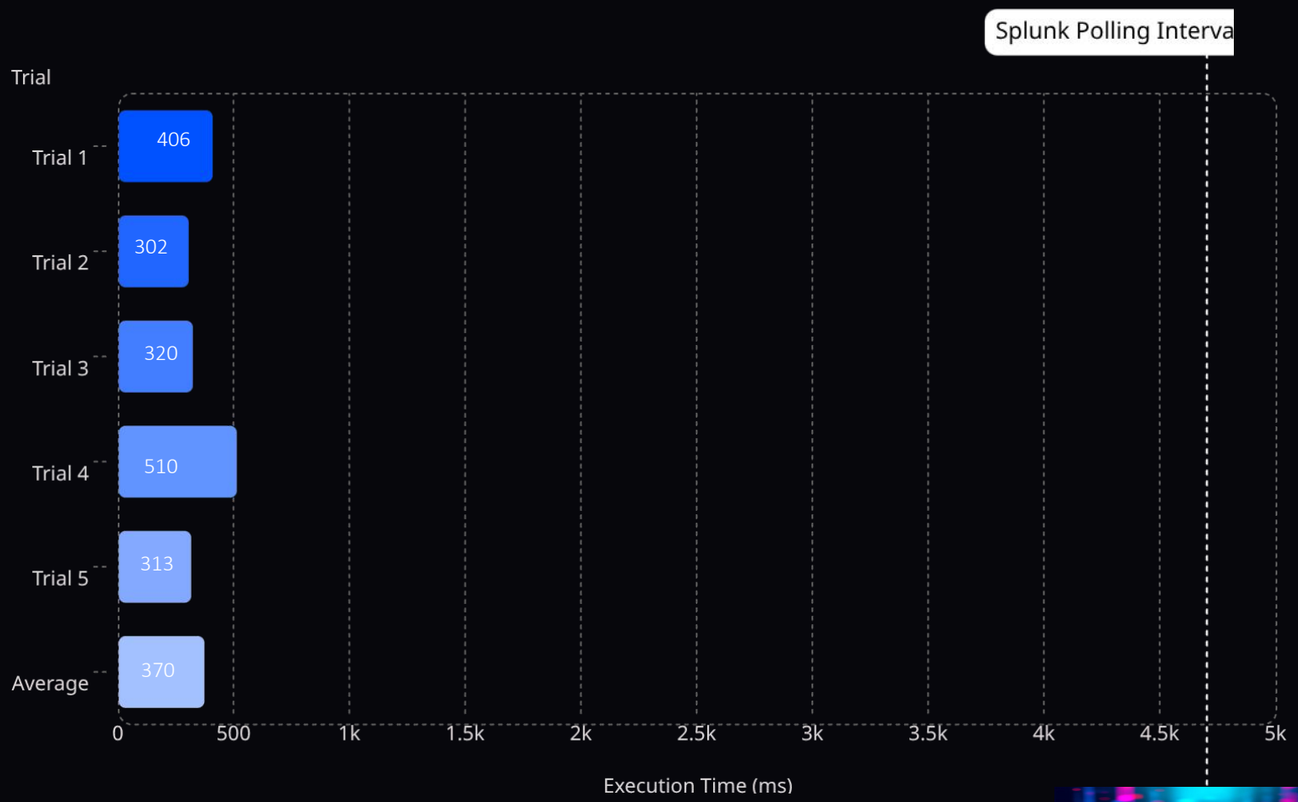
Execution Time

< 300 milliseconds (Sub-second execution)

Main Linux Experiment: Wazuh FIM



Splunk Replication Experiment: Windows



Detection Outcome

SIEM (FIM)

No detection

Kernel (auditd)

Detected

The Time Gap Problem

- Monitoring systems sample activity at fixed intervals
- Some attacks occur between scans

Why Detection Fails?

- Events occurring between scans may be missed
- Short-lived events often go unrecorded
- Results in gaps in monitoring and incomplete detection

Implications

- Enterprise systems are vulnerable
- Periodic monitoring insufficient
- Need deeper detection

Limitations

- Limited SIEM platforms
- Limited trials
- No human baseline

Conclusion

Agentic AI changes detection dynamics – not just attack speed

Thank You

Questions?