Project Objective: Lay foundations for a new generation of tools and analytics to study how malware infection infrastructures are deployed, operated and then interlinked with open web sources to target victims.

http://sisl.rites.uic.edu/projects/maldives

Technical Approach and Research Challenges

- Developing a safe and scalable infection-phase observatory
- Studying malvertising and its relationship with search engine poisoning
- Understanding malvertising in mobile platforms
- Tracking malware redirection chains at the domain-level
- Developing multi-class exploit kit classification techniques
- Develop deployable client-side defenses using robust signals

PLATO HIGHLIGHTS

Platform Acquisition Observatory: Establishment of a novel server-side observatory to fully comprehend the malware infection infrastructure deployment phase.

HogMap: Using SDNs to Incentivize Collaborative Security Monitoring (SDN-NFV 2016)

TROLL HIGHLIGHTS

Traffic Redirection Observation Lablet: Explore DNS-based domain association techniques and active crawling techniques to identify malware redirection chains.

- Multi-perspective study of ransomware evolution

EXPLORO HIGHLIGHTS

Exploit-Kit Interrogation Environment: automated probes to facilitate detection and measurement of professional malware installation services.

- Defense-centric analytics of exploit kit infection traces
- Multi-family analysis and detection of exploit kits

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting

January 9-11, 2017
Arlington, Virginia