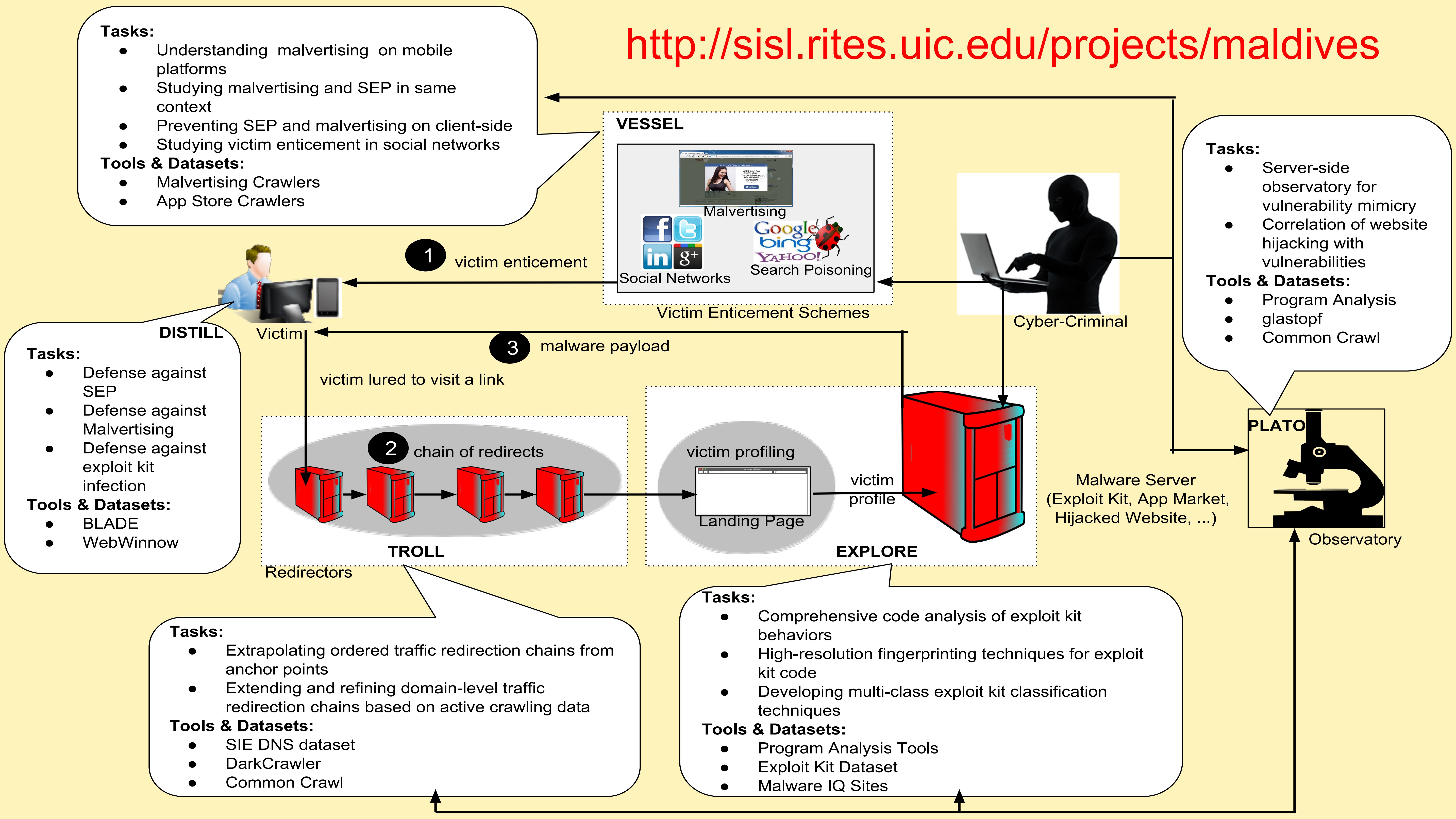
# MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms

PIs: Vinod Yegneswaran (SRI), Phil Porras (SRI), Long Lu (Stony Brook), Venkat Venkatakrishnan (University of Illinois @ Chicago)

**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

**VESSEL**

**Tasks:**
- Understanding malvertising on mobile platforms
- Studying malvertising and SEP in same context
- Preventing SEP and malvertising on client-side
- Studying victim enticement in social networks

**Tools & Datasets:**
- Malvertising Crawlers
- App Store Crawlers

**PLATO**

**Tasks:**
- Server-side observatory for vulnerability mimicry
- Correlation of website hijacking with vulnerabilities

**Tools & Datasets:**
- Program Analysis
- glastopf
- Common Crawl

**DISTILL**

**Tasks:**
- Defense against SEP
- Defense against Malvertising
- Defense against exploit kit infection

**Tools & Datasets:**
- BLADE
- WebWinnow

**TROLL**

**Tasks:**
- Extrapolating ordered traffic redirection chains from anchor points
- Extending and refining domain-level traffic redirection chains based on active crawling data

**Tools & Datasets:**
- SIE DNS dataset
- DarkCrawler
- Common Crawl

**EXPLORE**

**Tasks:**
- Comprehensive code analysis of exploit kit behaviors
- High-resolution fingerprinting techniques for exploit kit code
- Developing multi-class exploit kit classification techniques

**Tools & Datasets:**
- Program Analysis Tools
- Exploit Kit Dataset
- Malware IQ Sites

## 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 Acquistion 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)

## VESSEL HIGHLIGHTS

**Victim Enticement Schemes Evaluation Lablet**: Developing comprehensive tools to measure victim enticement schemes like malvertising, SEO poisoning etc.

- Mobile malvertising scanning and analytics framework

## 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

## EXPLORE 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