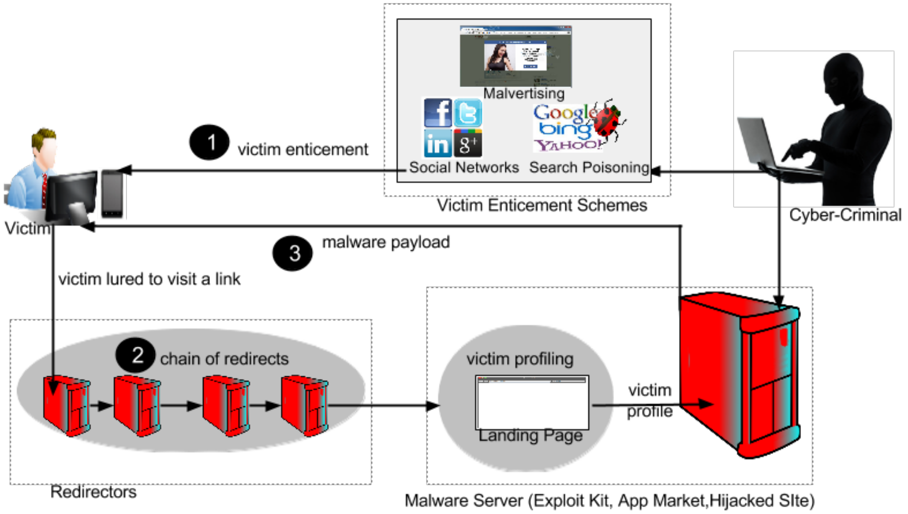
MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms



Challenges:

- Development of exploit kit interrogation environment
- Studying mobile malvertising and victim enticement techniques
- Designing scalable data collection and analysis platform for cyber-threat analytics
- Development of robust efense mechanisms

Milestones:

- **SRI:** Development of DNS-based traffic analysis tools as well as active strategies for uncovering hidden traffic redirection chains
- **SBU:** Conducted a large-scale measurement study of malvertising infrastructure and develop new detection tools.
- **UIC:** Development of exploit kit interrogation environment

Scientific Impact:

- Development of novel technologies and analytics that collectively inform research community on how malware infection infrastructures are deployed, operated and interlinked with open web sources
- Collection of ransomware DNS and system traces, across entire lifecycles.

Broader Impact:

- Improved threat intelligence for service providers by uncovering hidden structures of interlinked malware campaigns.
- The tools built as part of this project will be shared with the broader community.

Project PIs **SRI:** Vinod Yegneswaran, Phillip Porras **Stony Brook:** Long Lu **UIC:** Venkat Venkatakrishnan