MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms

Challenges:

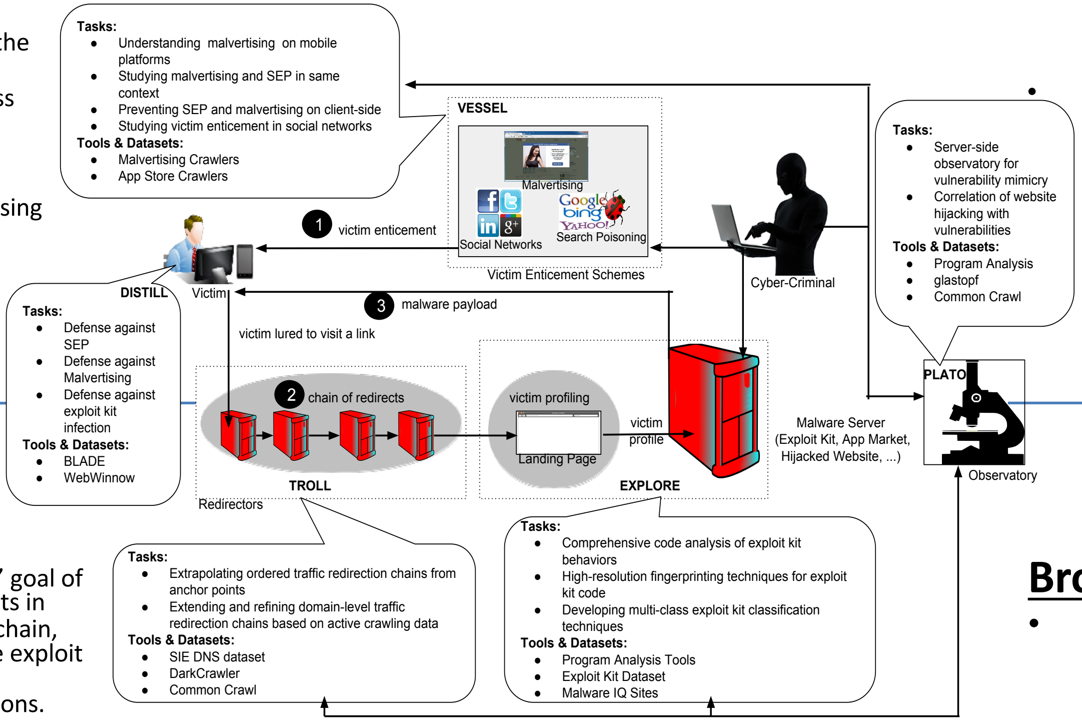
- Developing a safe and scalable infection-phase observatory
- Tracking malware redirection chains at the domain-level
- Developing multi-class APT classification techniques
- Develop deployable client-side defenses using robust signals

.

Solution:

- In line with MALDIVES' goal of pinpointing entry points in the malware delivery chain, we developed scalable exploit generation system for dynamic web applications.
- Our system uses a multi-faceted analysis to understand the behavior of server- side exploit software.

Project info (1514503, SRI International /Univ of Illinois. Chicago / Northeastern University, vinod@csl.sri.com)



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

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

Tools & Datasets:
- BLADE
- WebWinnow

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

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

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

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

PhD student Abeer Alhuzhali and PI Venkatakrishnan at the 2018 award ceremony, pic courtesy of USENIX association.

Scientific Impact:

- The project with 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
- .

Broader Impact:

- Our work was honored with a Distinguished Paper Award at the 2018 USENIX Security Symposium, and was a finalist at the 2018 NYU CSAW Applied Research Competition.
- Recent Papers at IEEE S&P 2019 Symposium (HOLMES) and TaPP 2019 on APT detection