Reconstructing and investigating in-the-wild web-based malware downloads

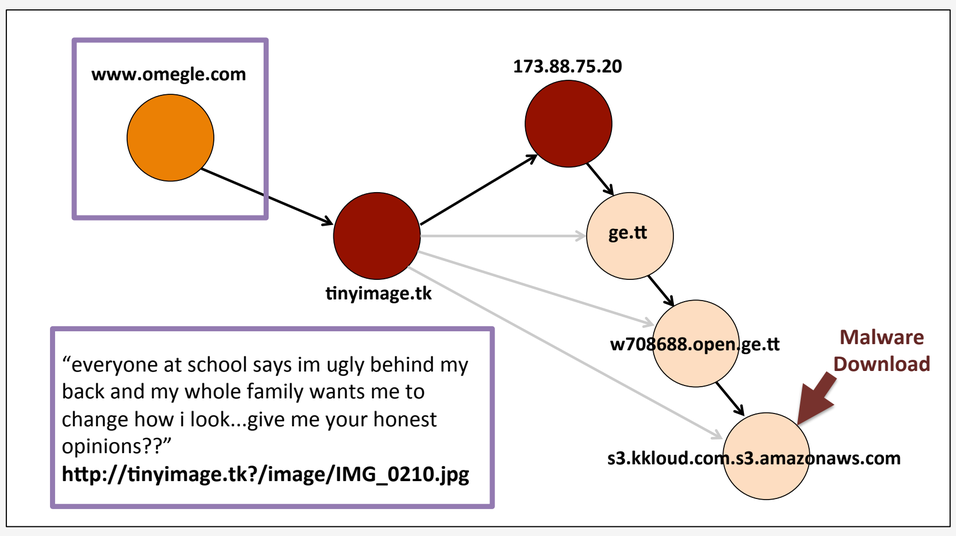
PI: Roberto Perdisci (perdisci@cs.uga.edu)

Need

- While technologies for malware detection exist, it is often very difficult to reconstruct the root cause of a malware downloads

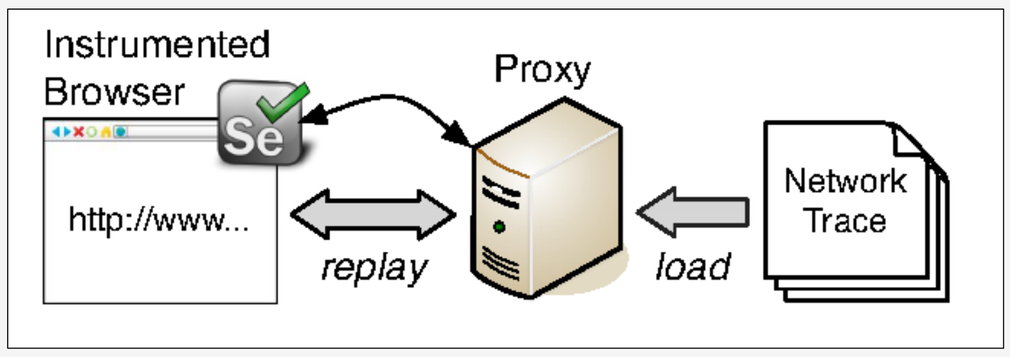
Goal

- Automatically reconstruct sequence of steps (e.g., visited pages and user actions) that bring users to malicious software downloads



Approaches

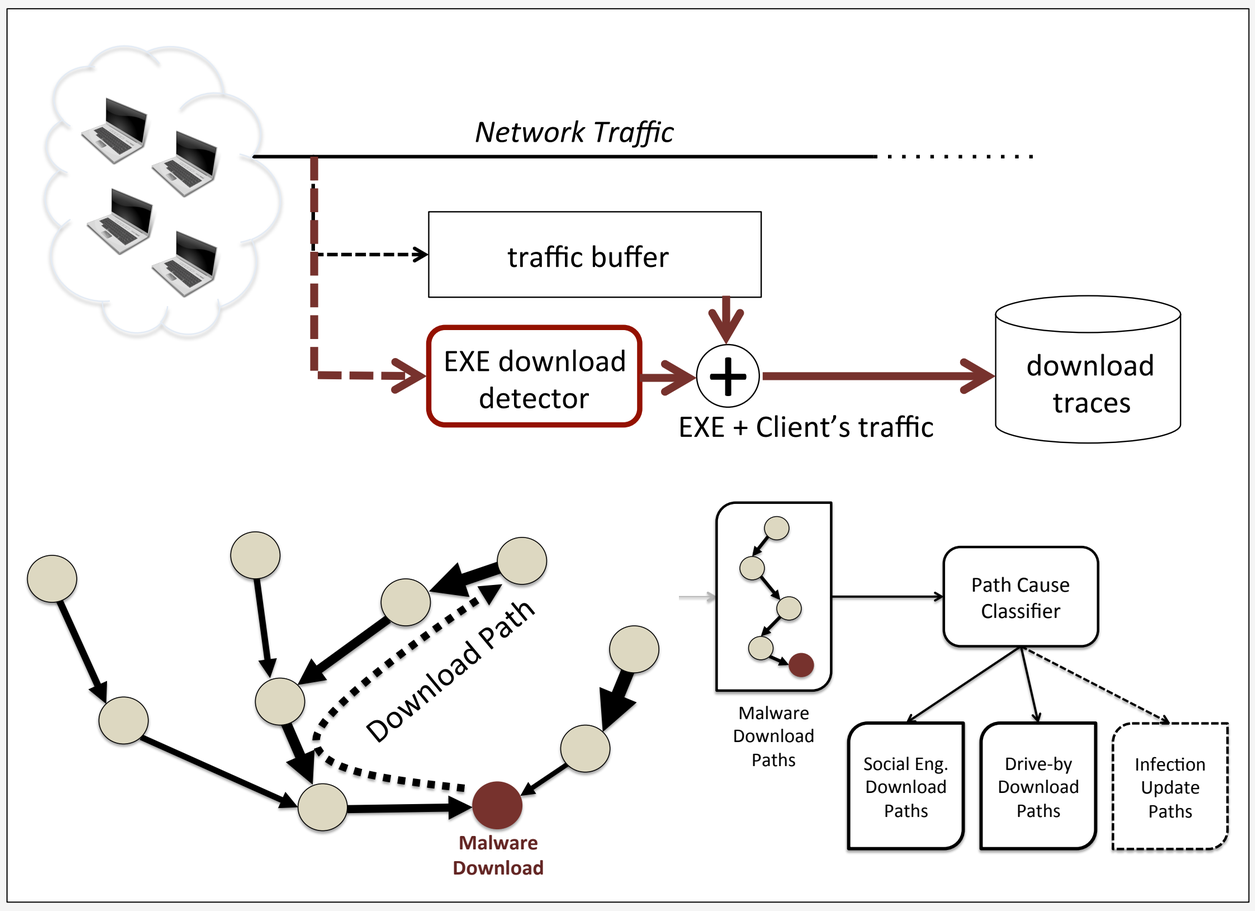
1. Efficient collection and automatic investigation of network traces related to malware downloads
2. Browser instrumentation to enable enhanced logging and automatic forensics



Collaborators

Phani Vadrevu (UGA), Bo Li (UGA), Jienan Liu (UGA), Chris Neasbitt (UGA), Babak Rahbarinia (AUM), Kang Li (UGA), Kyu Hyung Lee (UGA), Terry Nelms (GaTech), Manos Antonakakis (GaTech), Mustaque Ahamad (GaTech)

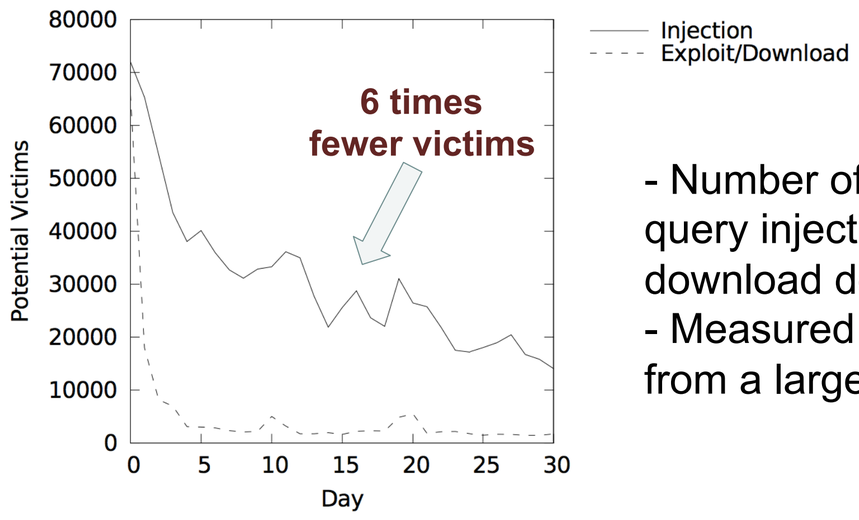
WebWitness



Results

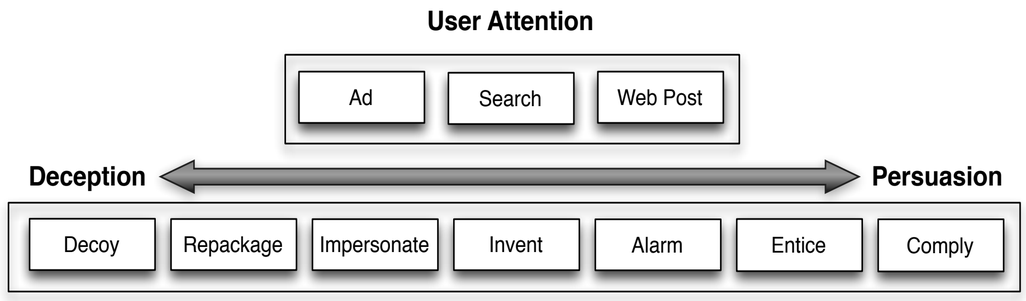
Node Labeling for Drive-By Download Paths

Experiment	Classifier	Correctly Labeled	Incorrectly Labeled
Cross-Validation	Exploit	99.19%	0%
	Landing	96.58%	0.17%
	Injection	94.87%	0.07%



- Number of hosts that query injection, exploit and download domains
- Measured on DNS traffic from a large ISP

Categorization of Social Engineering Malware Download Triggers



Publications

[1] "ClickMiner: Towards Forensic Reconstruction of User-Browser Interactions from Network Traces" ACM CCS 2014
[2] "WebCapsule: Towards a Lightweight Forensic Engine for Web Browsers" ACM CCS 2015
[3] "WebWitness: Investigating, Categorizing, and Mitigating Malware Download Paths" USENIX Security 2015
[4] "Towards Measuring and Mitigating Social Engineering Software Download Attacks" USENIX Sec. 2016
[5] "Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots" NDSS 2017

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

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

The University of Georgia
1785