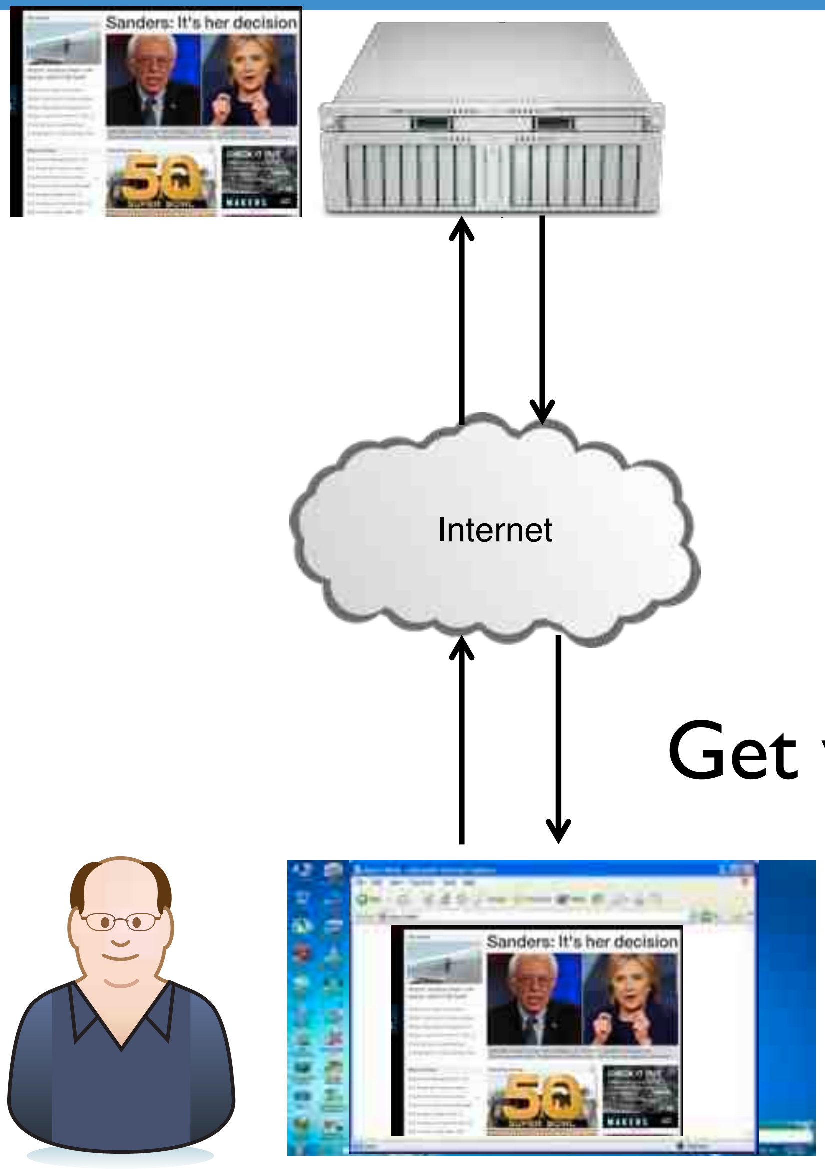
Cache, Trigger, Impersonate: Enabling Context-Sensitive Honeyclient Analysis On-the-Wire

By **Teryl Taylor**, Kevin Z. Snow, Nathan Otterness and Fabian Monrose

University of North Carolina at Chapel Hill

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Motivation



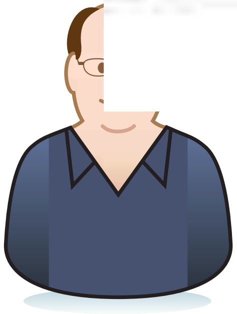
Get www.somenews.com

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

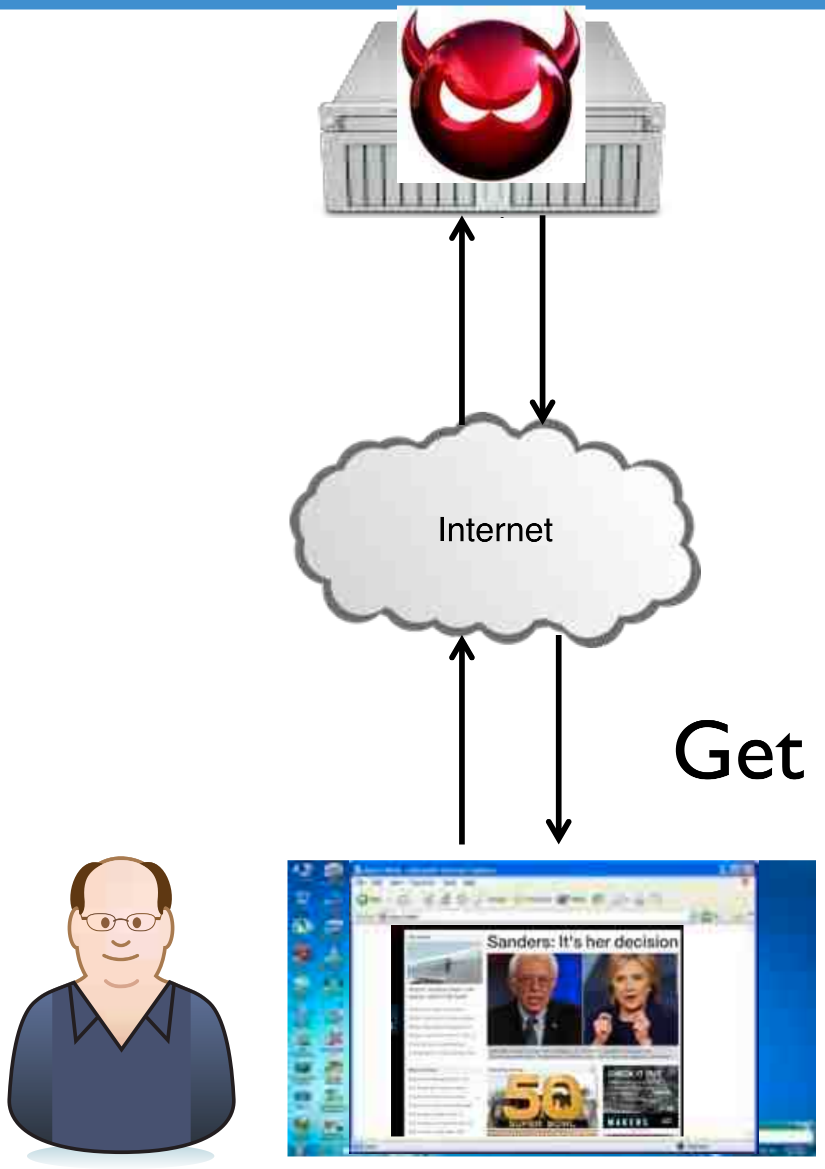
Motivation

Sanders: It's her decision

```
<html>

<h1>Sanders: It's her
decision</h1>

<iframe
src="http://www.exploitkit.com"/>


</html>
```

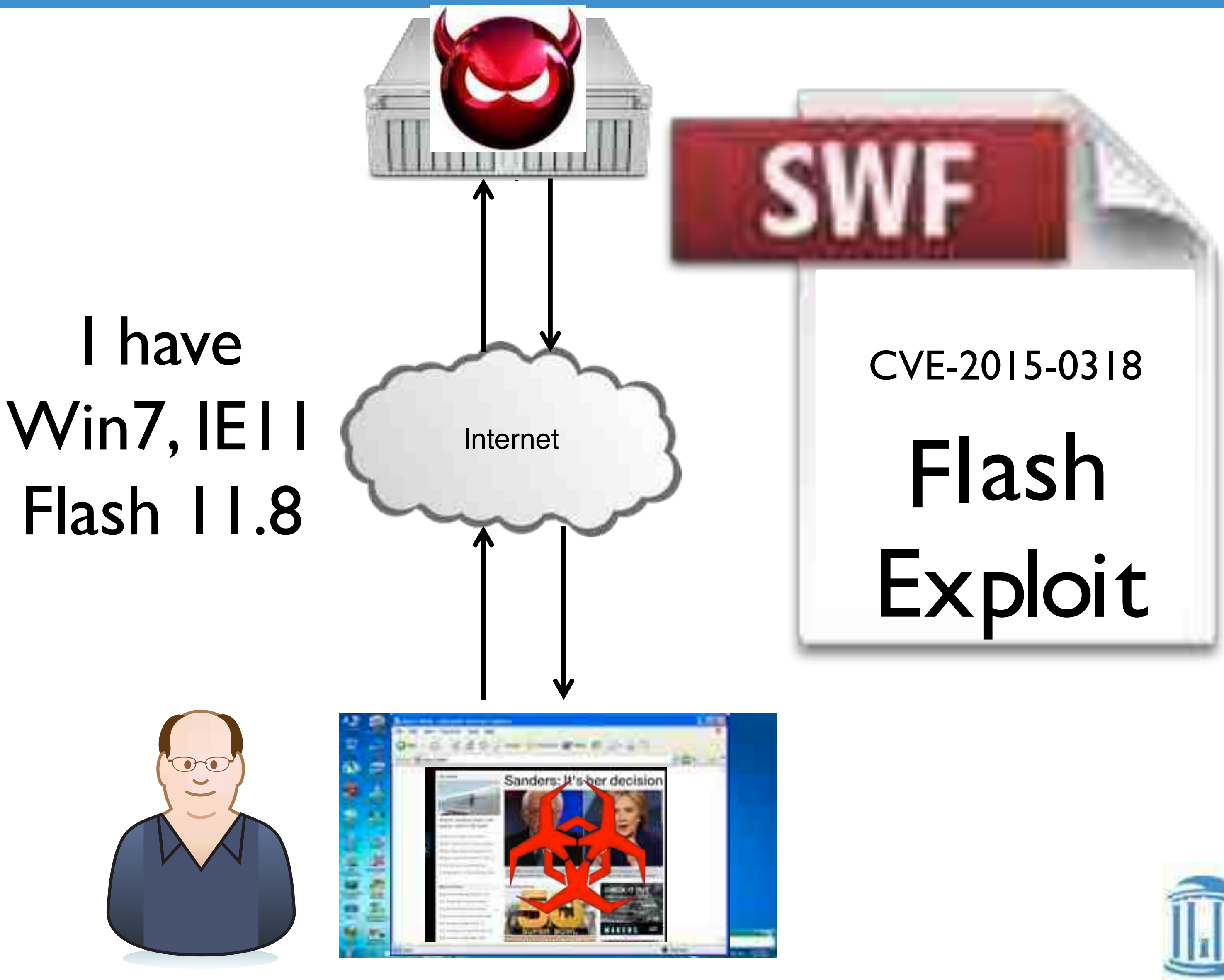


Motivation



Get www.exploitkit.com

Motivation



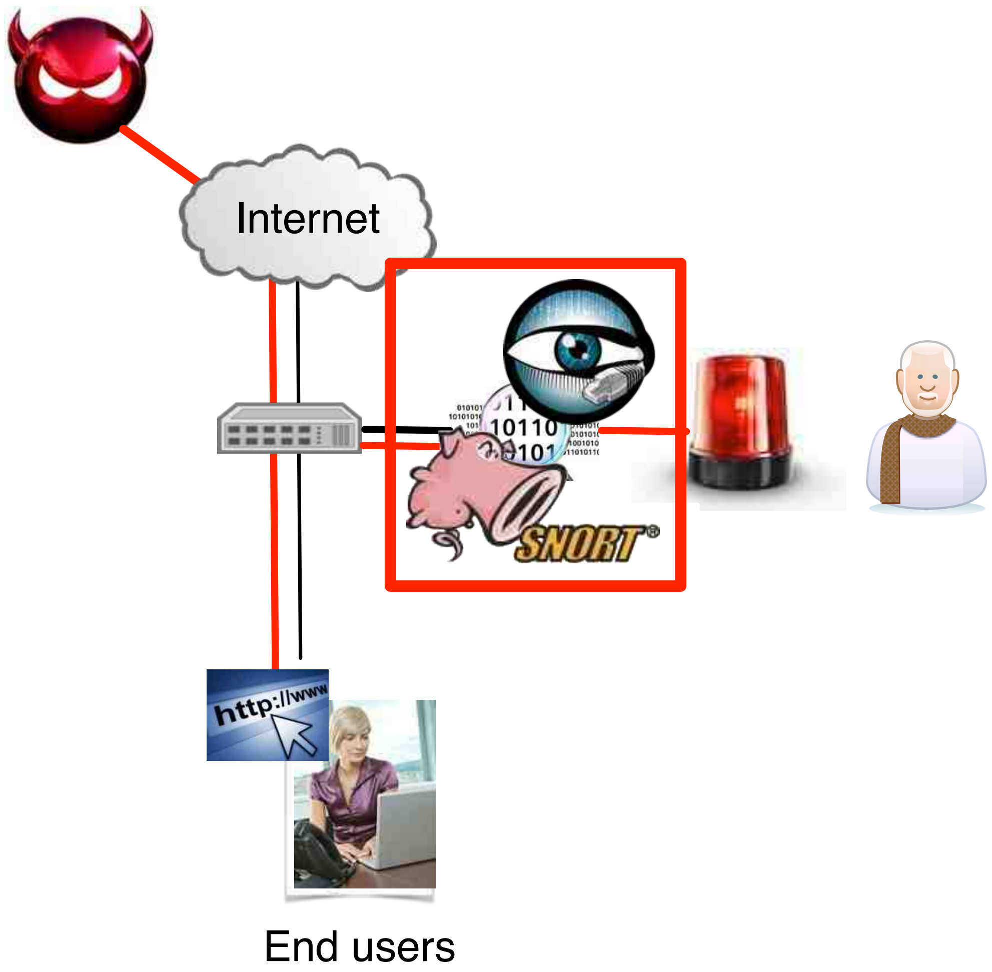
I have
Win7, IE11
Flash 11.8

CVE-2015-0318

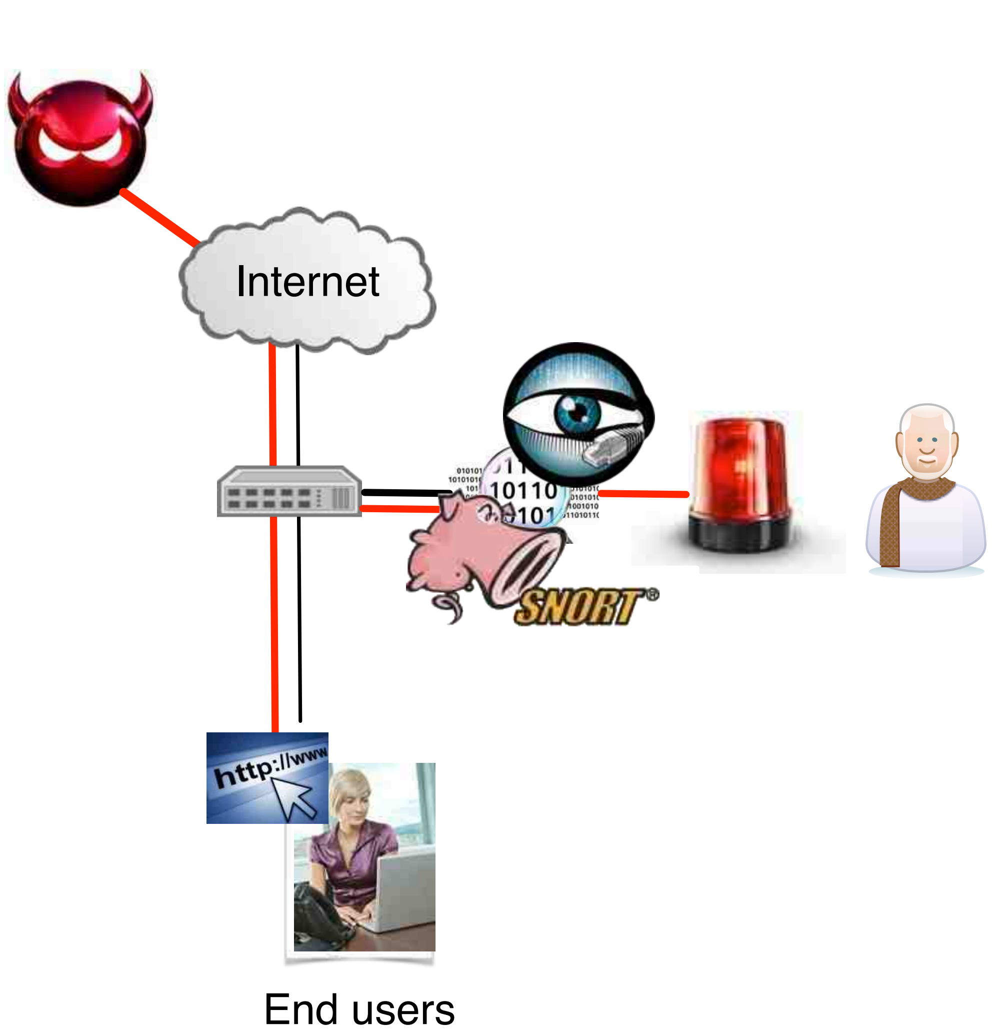
Flash
Exploit

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Current Approaches

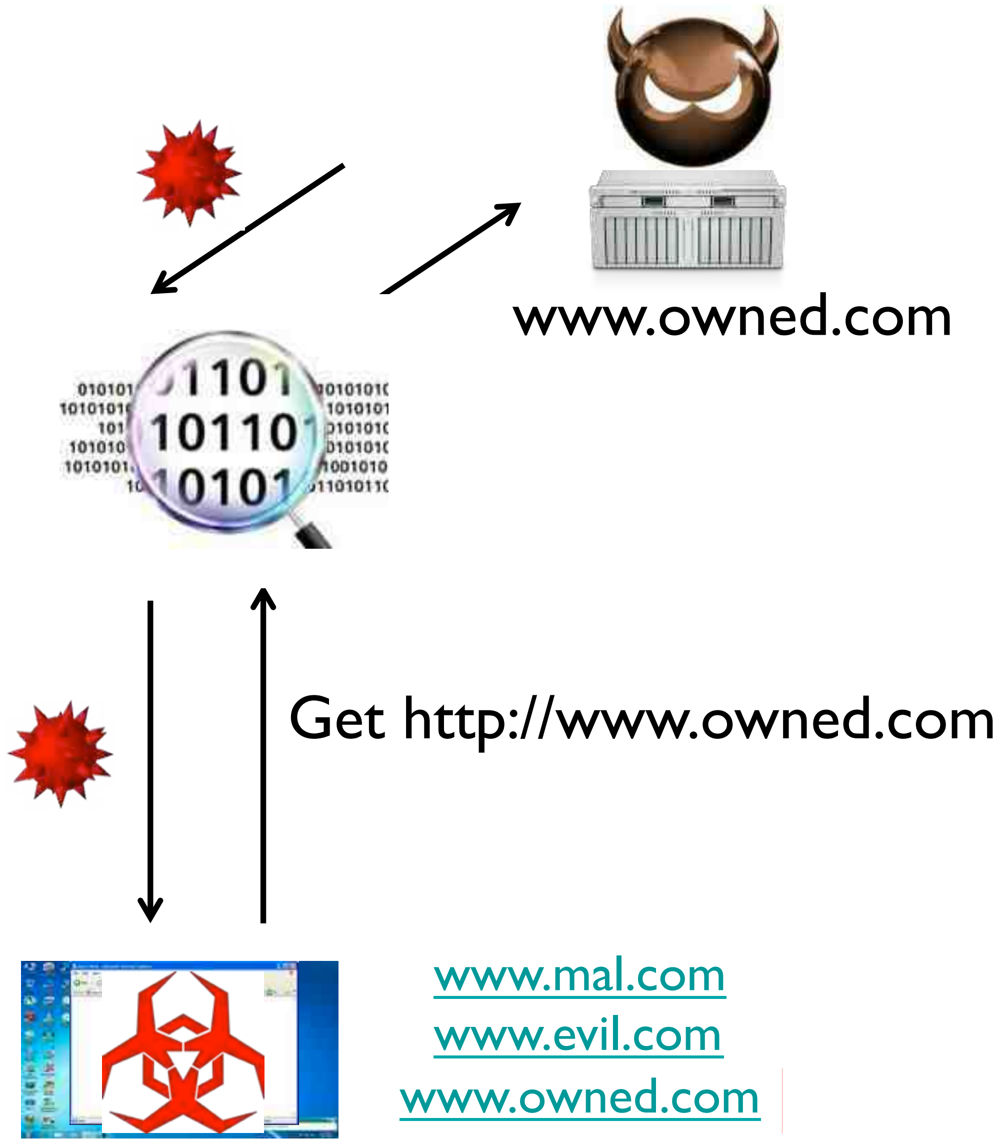


Current Approaches



Internet

End users



www.owned.com

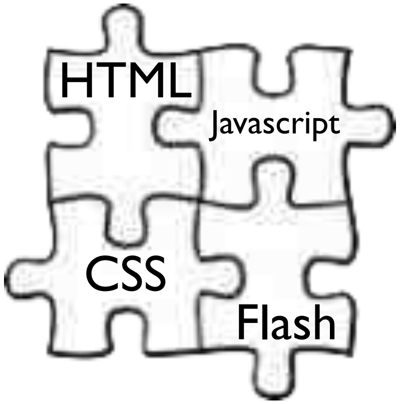
Get http://www.owned.com

www.mal.com
www.evil.com
www.owned.com

Operational Challenges and Constraints

- Limit interaction with the client or server.
- Must handle the fire hose of data.

- Attackers spread exploits across multiple web resources.



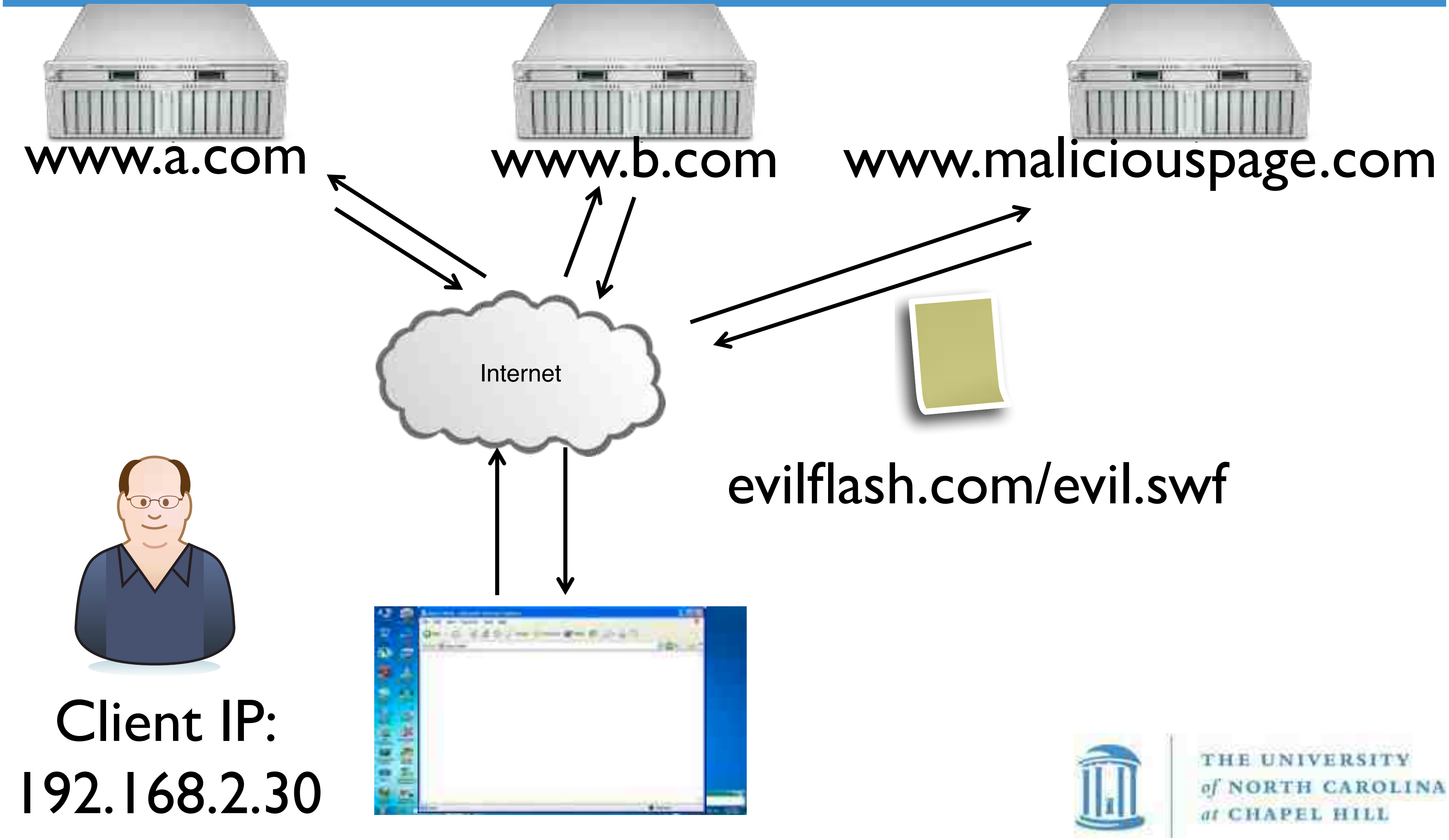
- Limited to memory storage.

Framework

- CACHE:
  - A small time window of traffic.
- TRIGGER:
  - On a potentially exploitable file type.
  - Flash comprises 75% for popular kits.

- IMPERSONATE:
  - The client and server using the semantic cache and a honeyclient.

Example



www.a.com

www.b.com

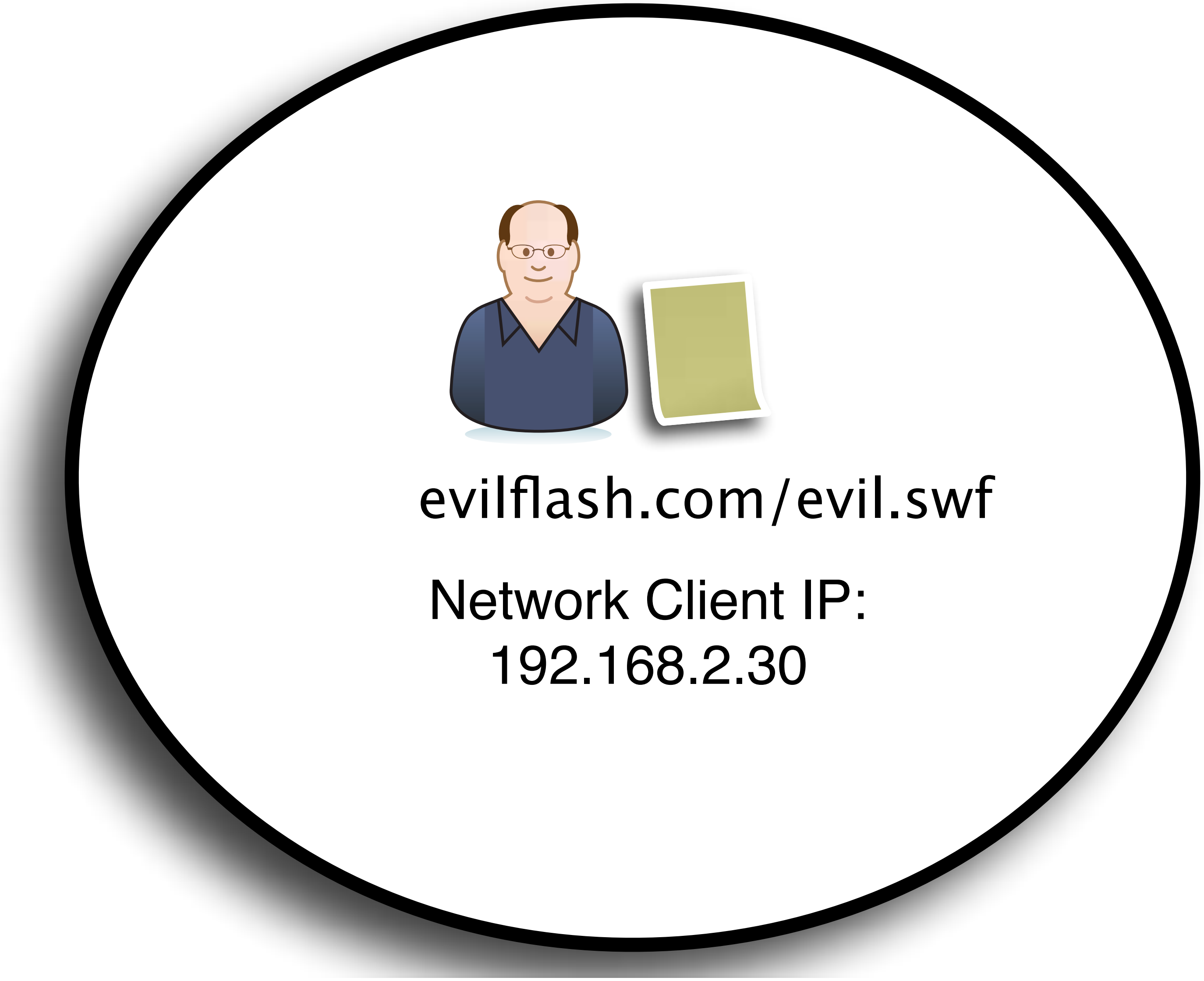
www.maliciouspage.com

evilflash.com/evil.swf

Client IP:
192.168.2.30

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

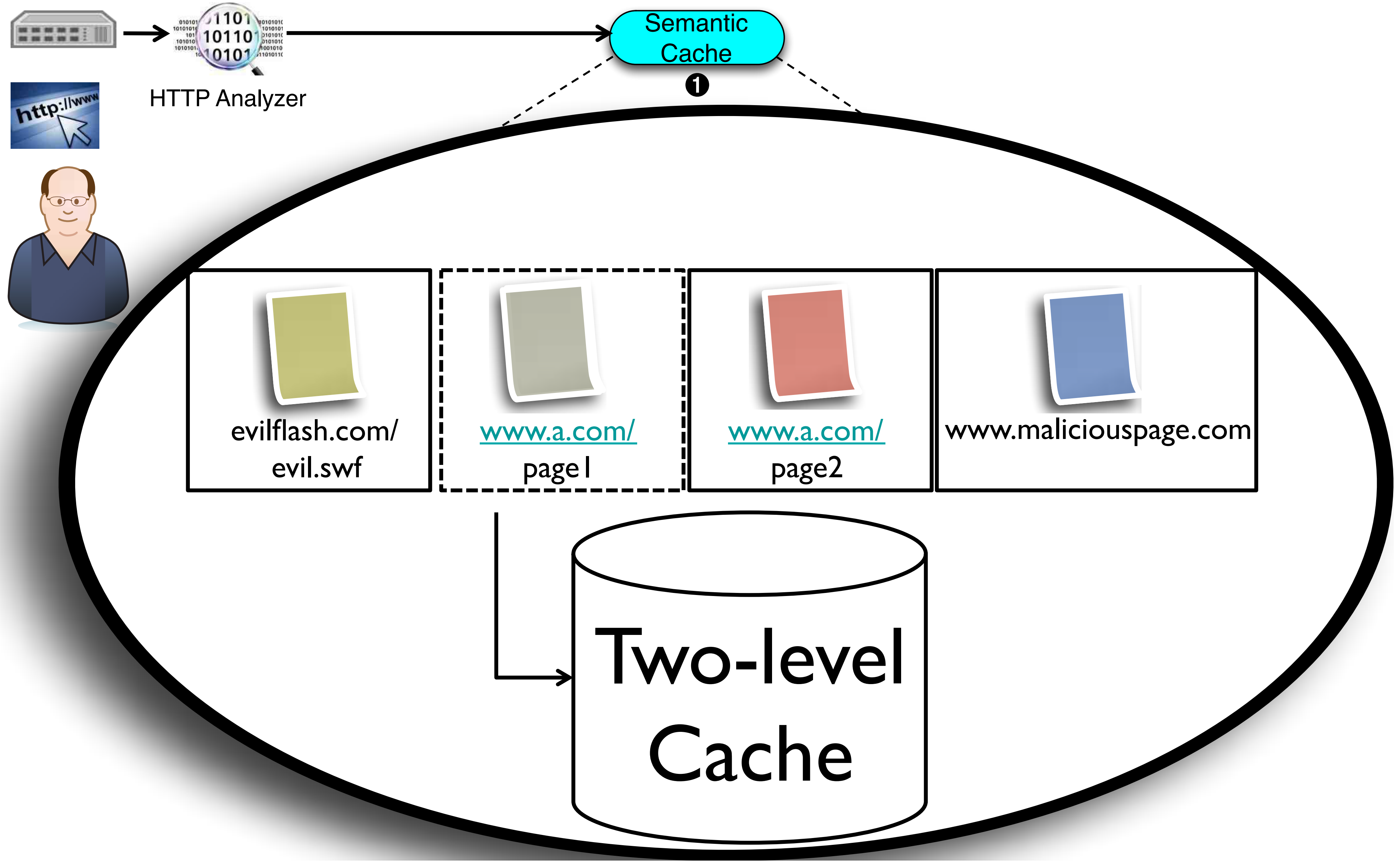
Example Cont'd



evilflash.com/evil.swf

Network Client IP:
192.168.2.30

CACHE



HTTP Analyzer

Semantic Cache

❶

evilflash.com/ evil.swf

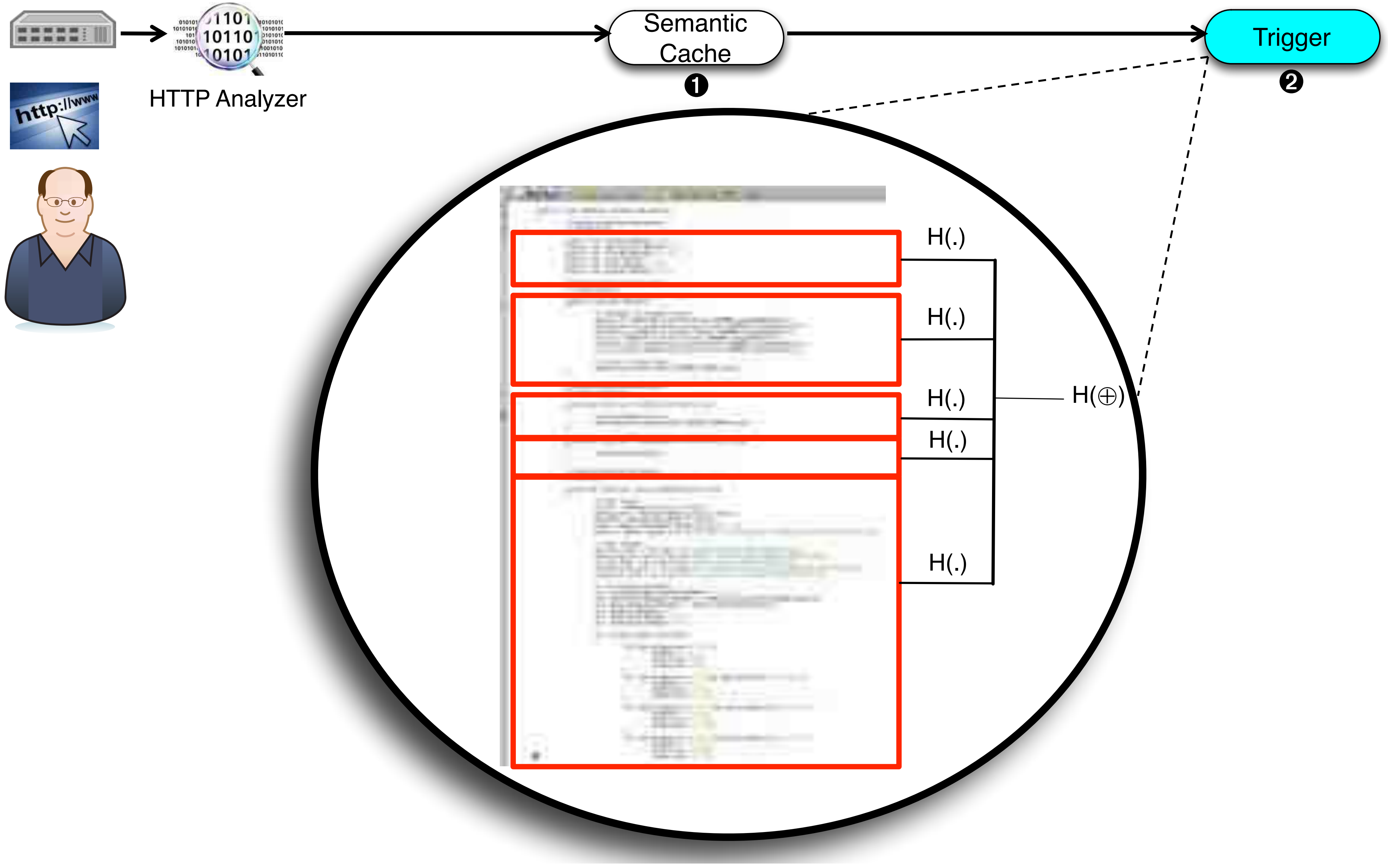
www.a.com/ page1

www.a.com/ page2

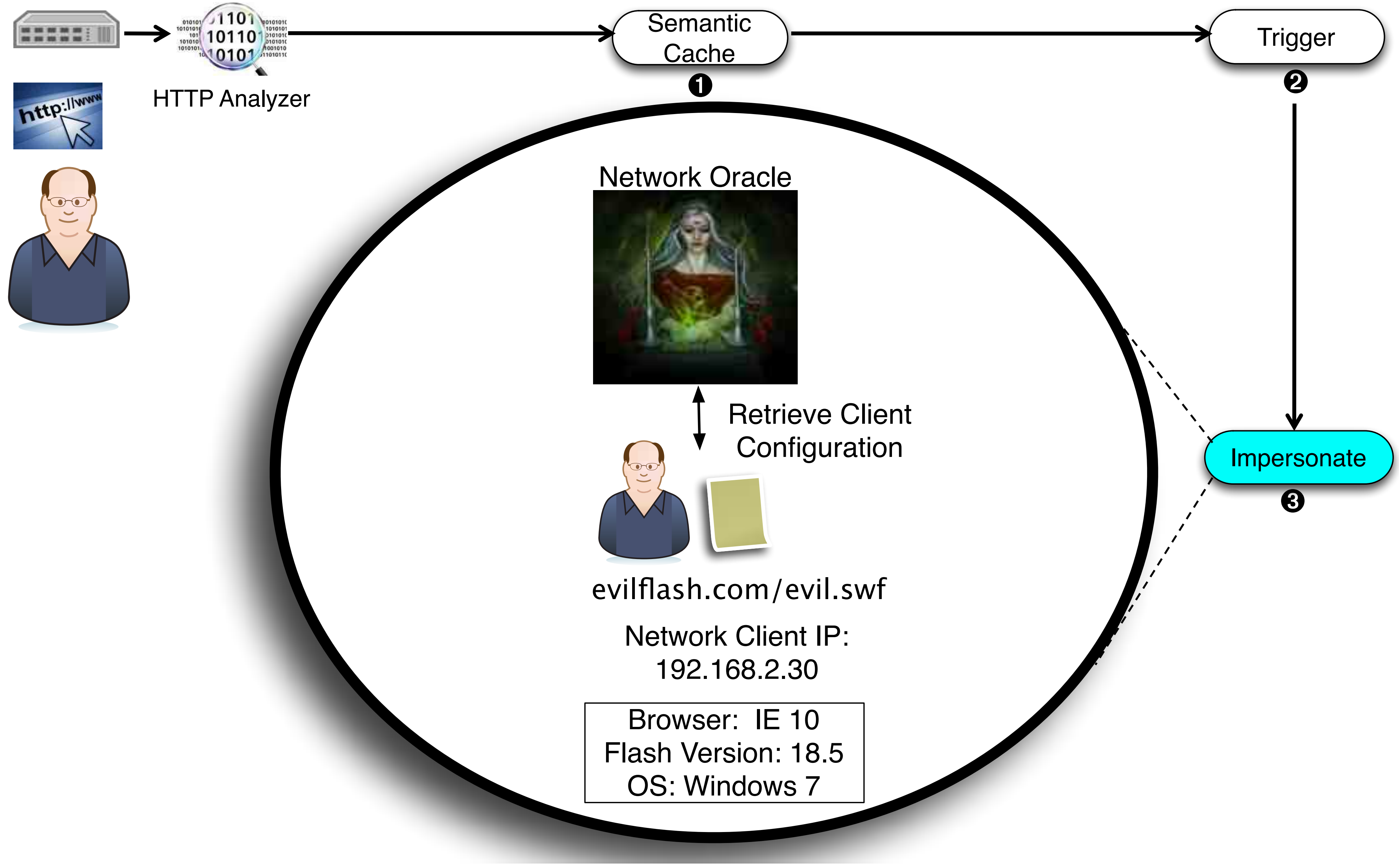
www.maliciouspage.com

Two-level Cache

TRIGGER



IMPERSONATE



HTTP Analyzer

Semantic Cache

❶

Trigger

❷

Impersonate

❸

Network Oracle

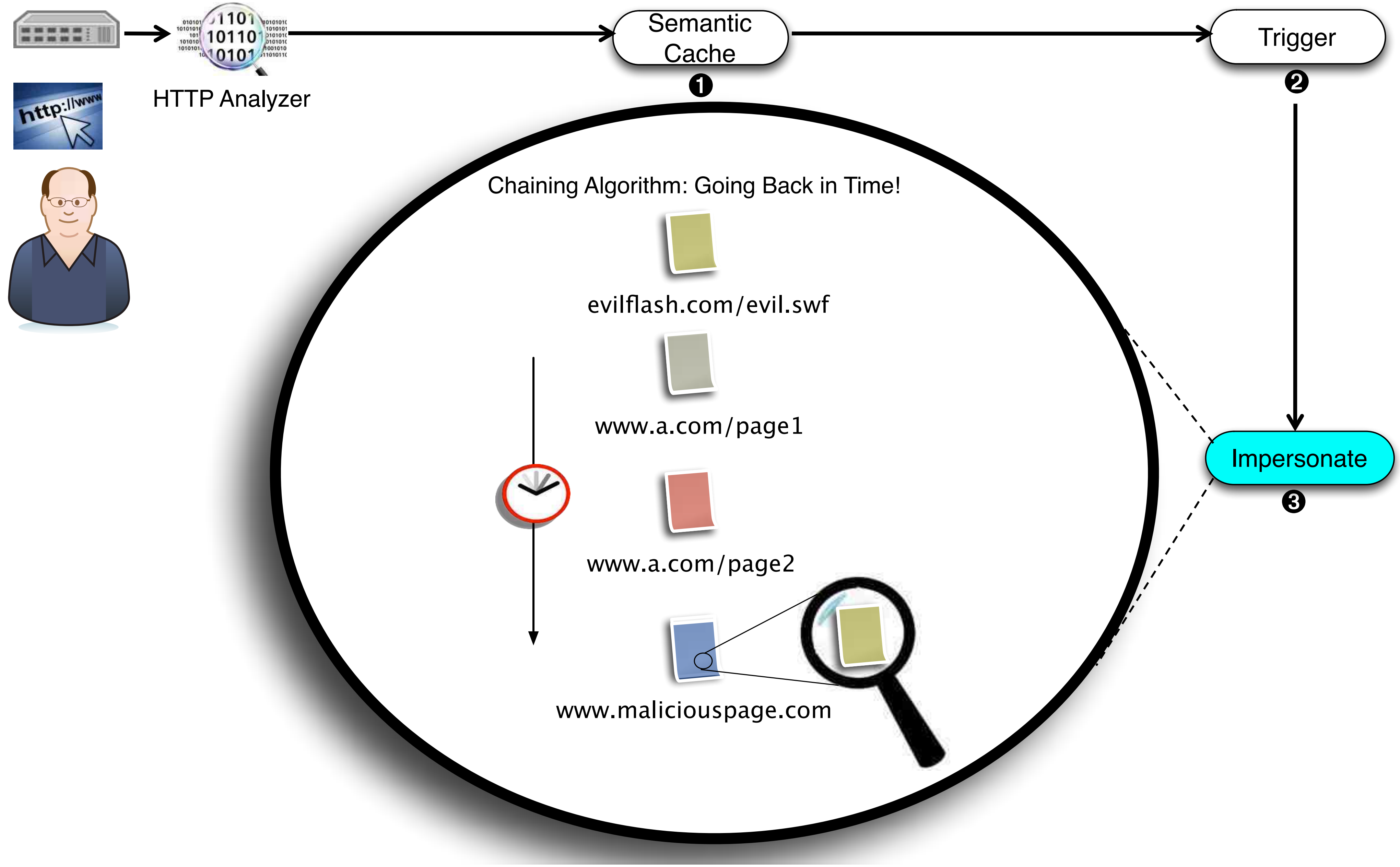
Retrieve Client Configuration

evilflash.com/evil.swf

Network Client IP:
192.168.2.30

Browser: IE 10
Flash Version: 18.5
OS: Windows 7

IMPERSONATE



HTTP Analyzer

Semantic Cache

❶

Trigger

❷

Impersonate

❸

Chaining Algorithm: Going Back in Time!

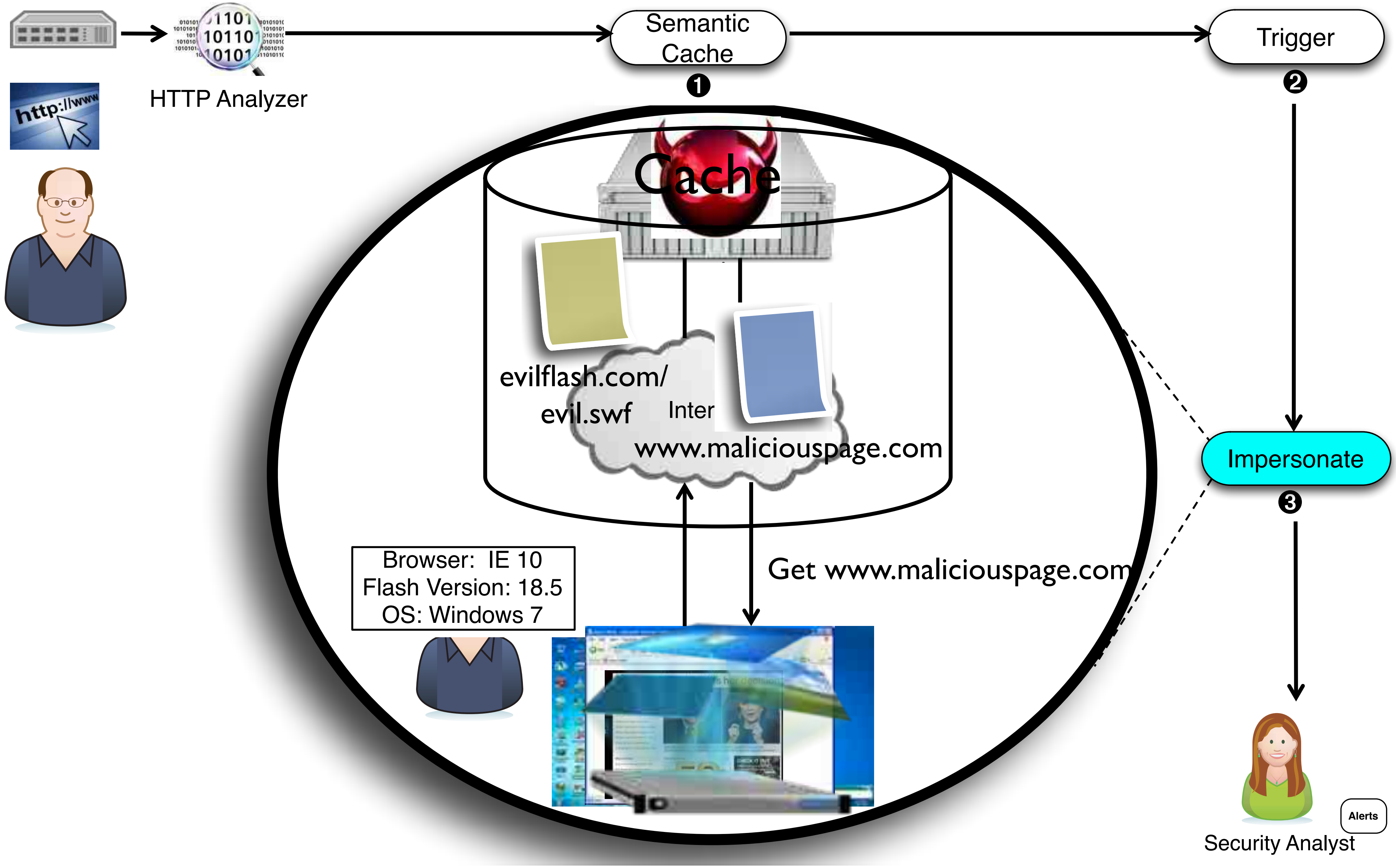
evilflash.com/evil.swf

www.a.com/page1

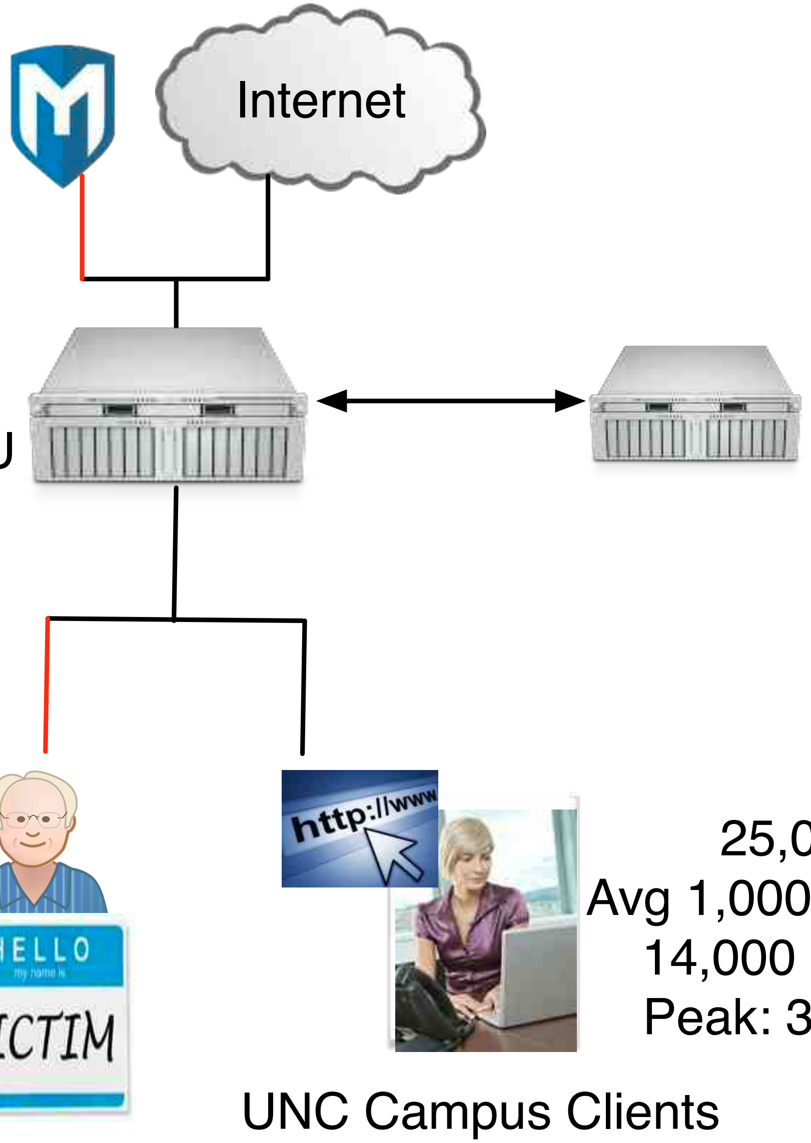
www.a.com/page2

www.maliciouspage.com

IMPERSONATE



Evaluation - Campus



Metasploit Server
Serves: 11 Flash exploits
Affects: 3 Flash Versions

Internet

Dell R410
128 GBs RAM
8 Core Xeon 2100 CPU
EndaceDAG Card

ShellOS: 5 VMs
Chrome, IE, Firefox
Headless Browser: HTMLUnit

Windows 7
Firefox/IE
3 Flash Versions

25,000 Students
Avg 1,000 Concurrent Users
14,000 HTTP flows/min
Peak: 35,000 flows/min

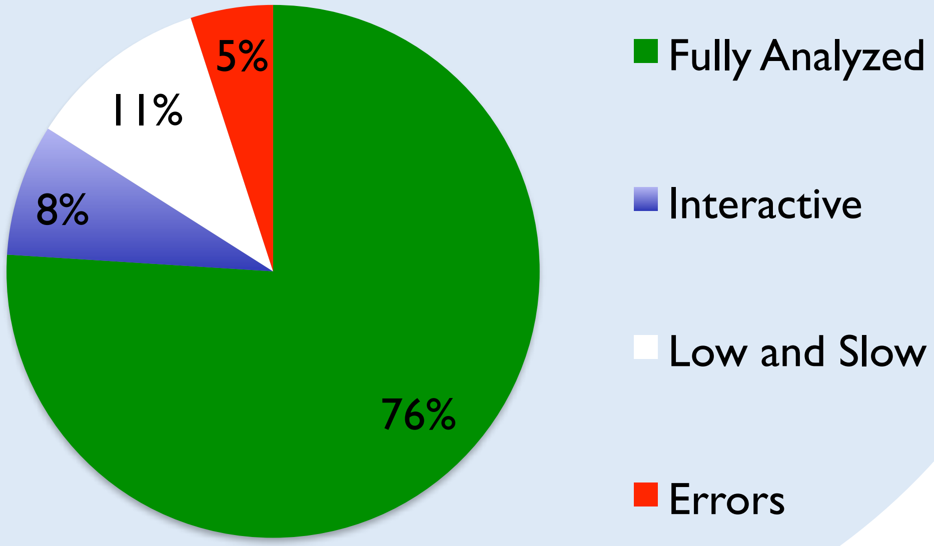
UNC Campus Clients

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Evaluation – Results

Total: 576,000

Filtered: 99% of Flash Files.



- Found on avg 2 malicious sites per day

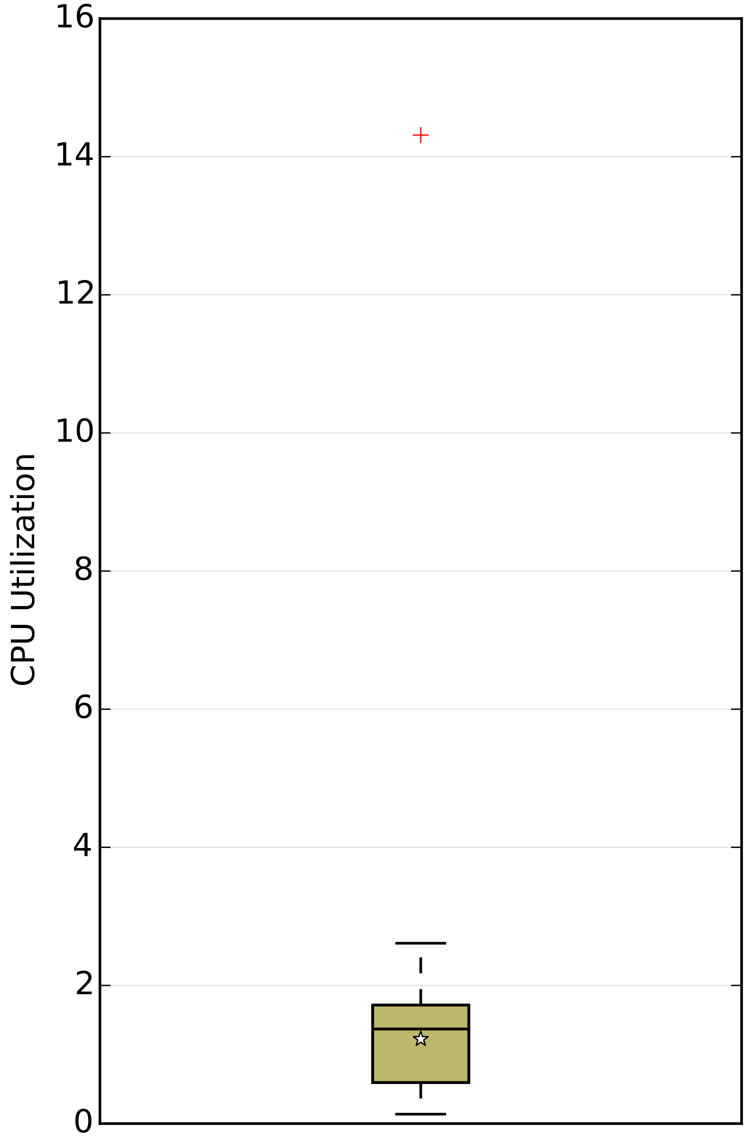
Conclusion: Honeyclient to the Wire

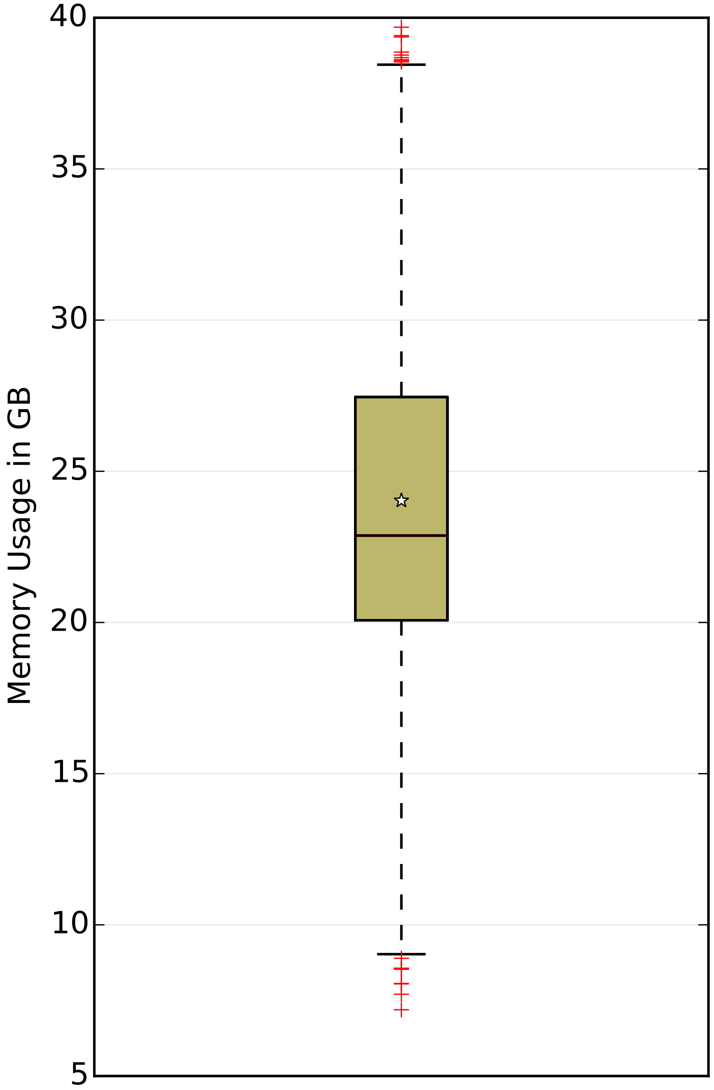
- Current network-based approaches are too slow to react.
- We propose a framework that:
  - Caches minutes worth of web objects.
  - Triggers an analysis on exploitable file types.
  - Impersonates both the client and the server.
- Demonstrated utility on a large campus network.

Questions?

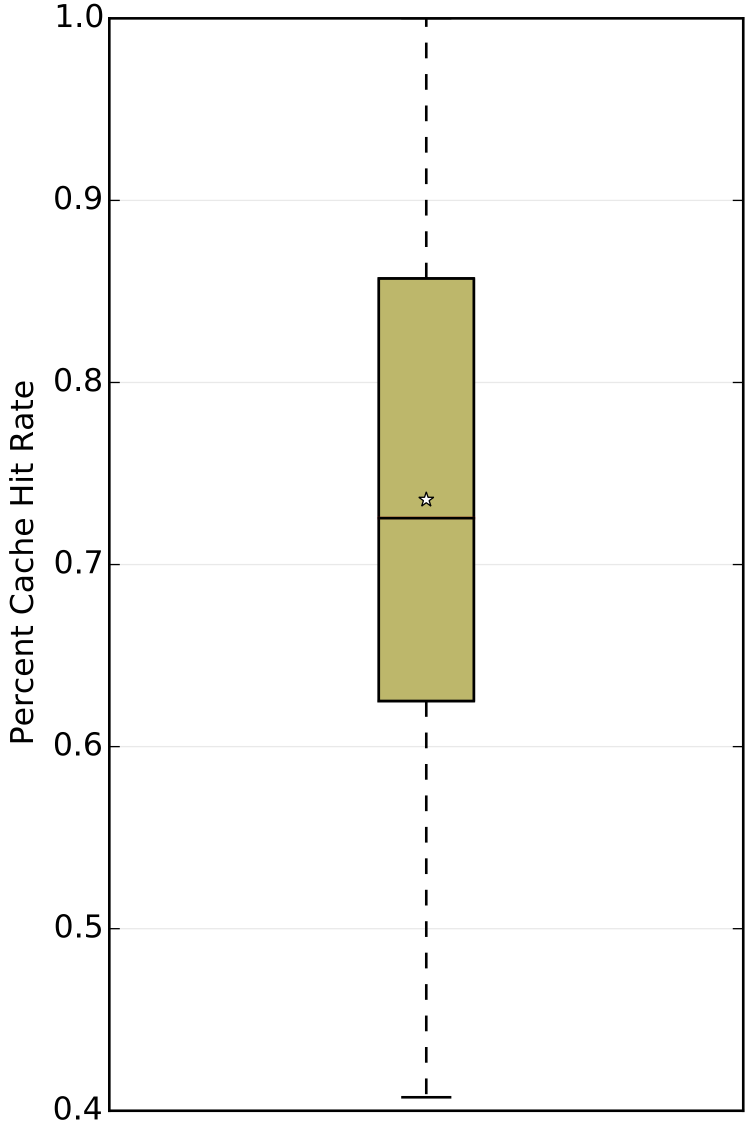
THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

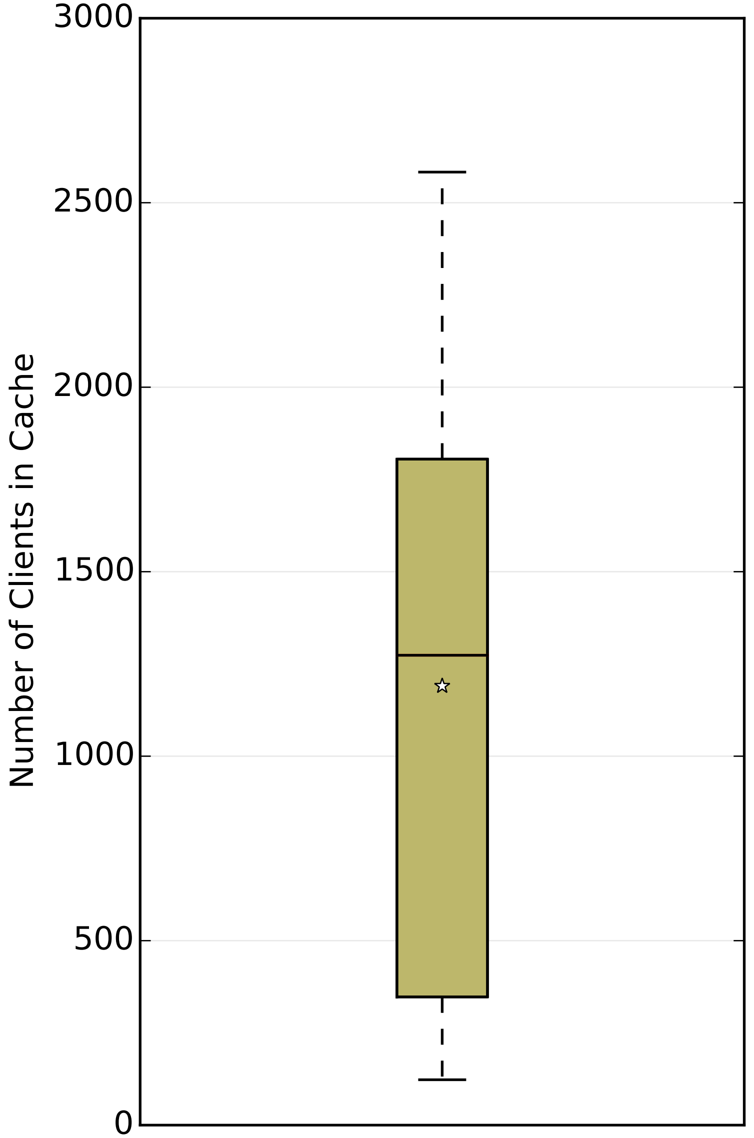
Evaluation – Performance



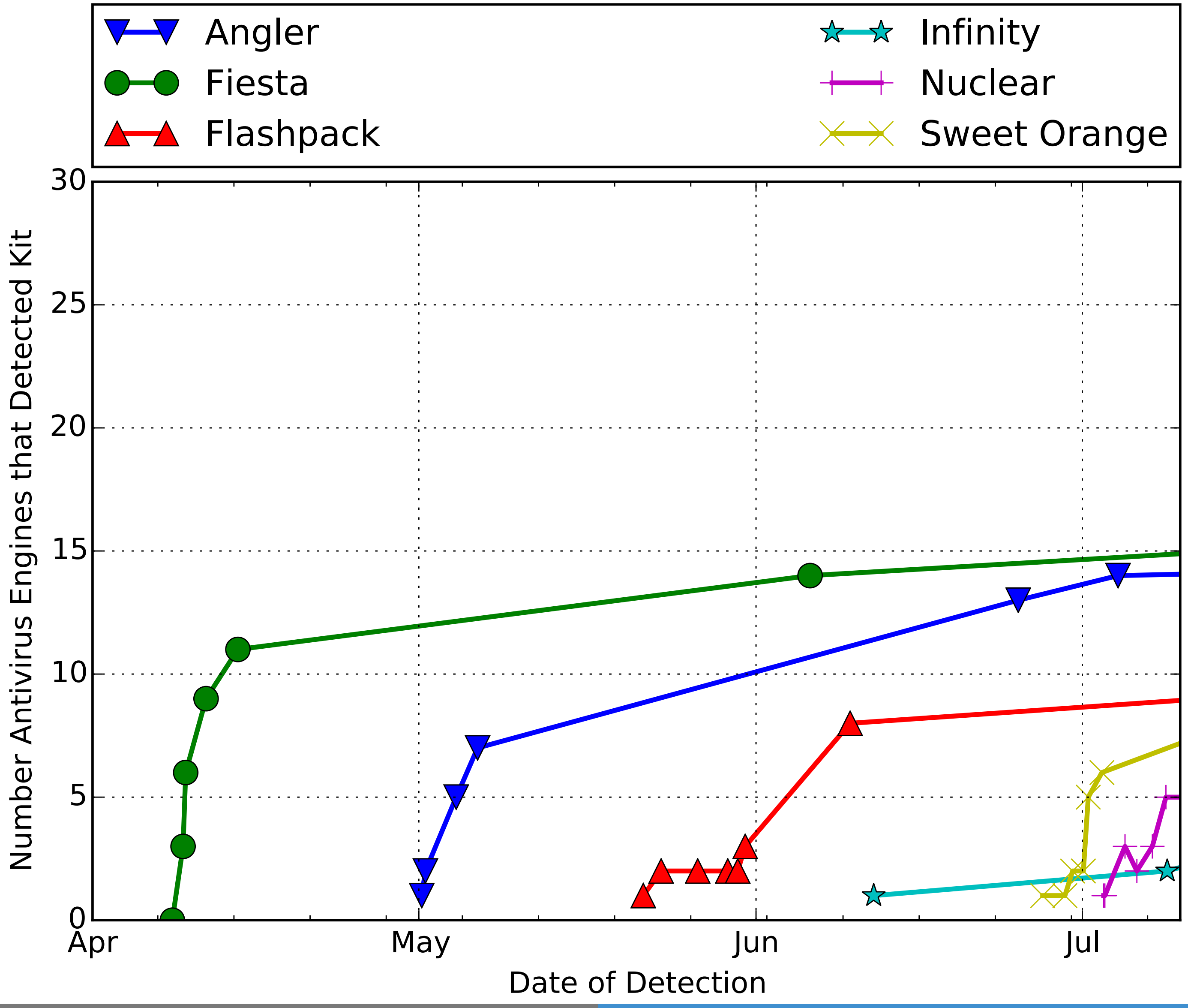


Evaluation – Cache

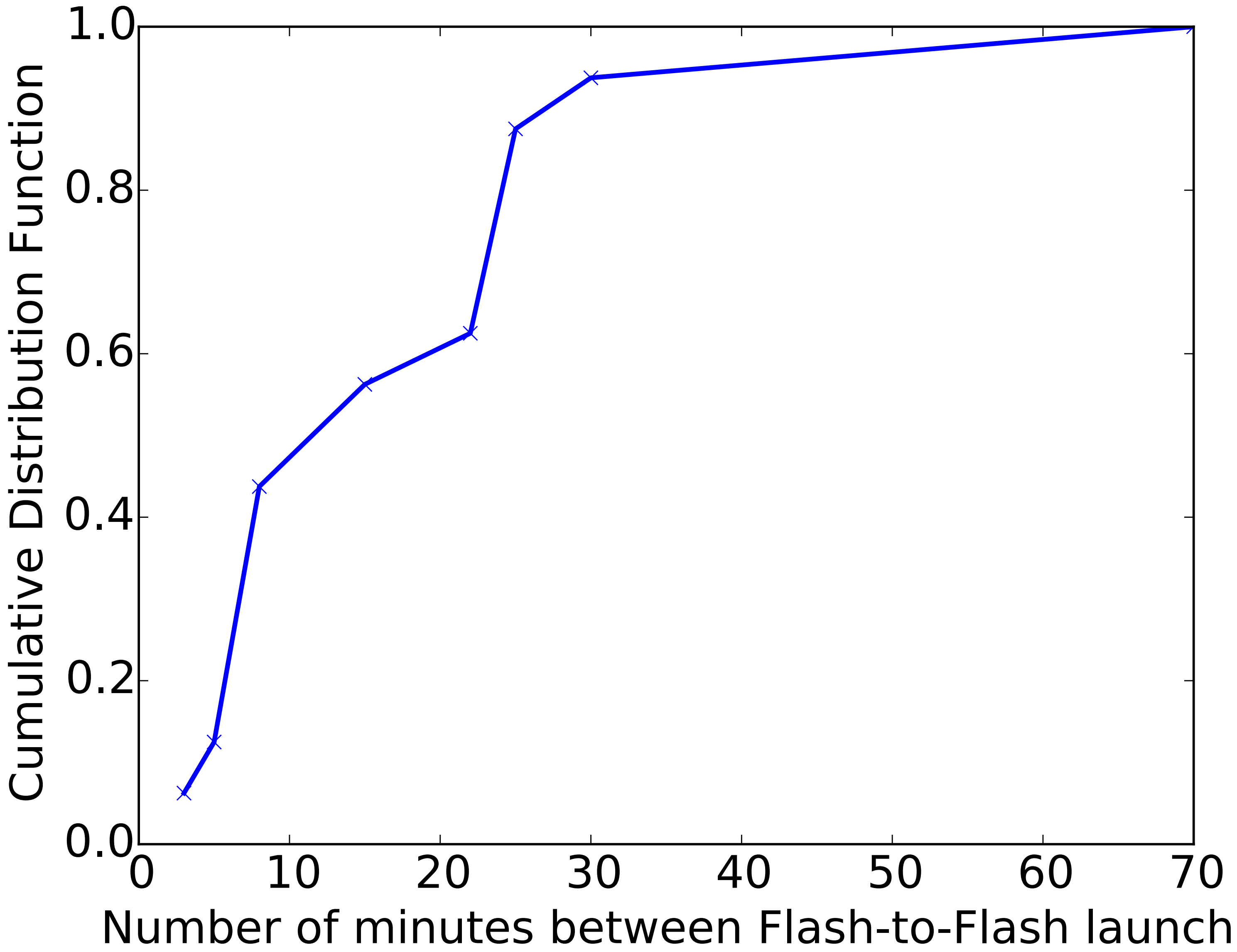




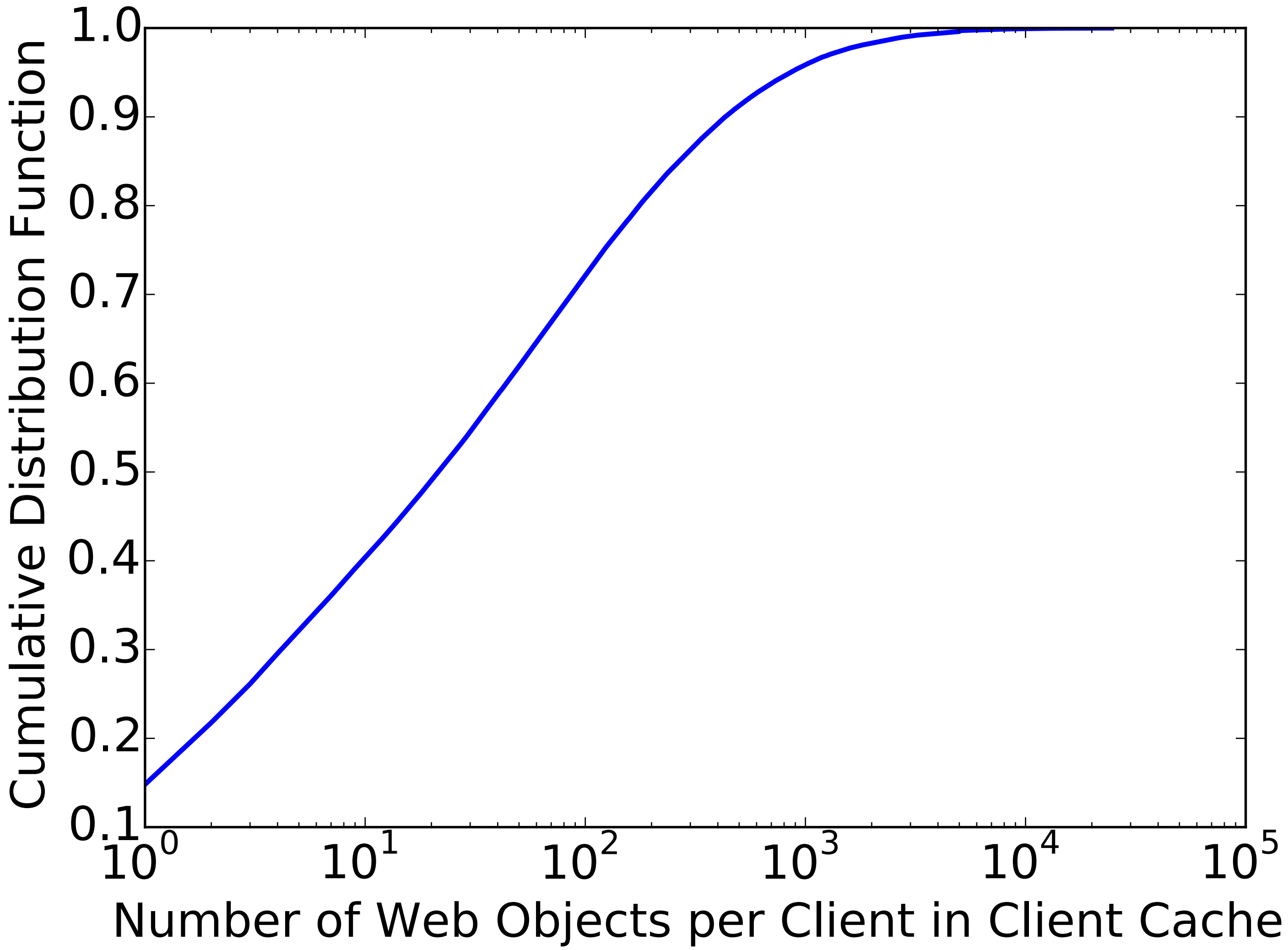
Evaluation – VirusTotal over Time



Evaluation – Minutes between Flash-in-Flash



Evaluation – Length of Client Cache



❹ Honeyclients

- Honeyclient H1 (ShellOS):
  - Process contains code injection/code reuse payload.
  - Process memory exceeds tunable threshold – heap spray.
  - Process terminates or crashes.

(Snow et. al, ShellOS: Enabling Fast Detection and Forensic Analysis of Code Injection Attacks, USENIX Security, 2011.)

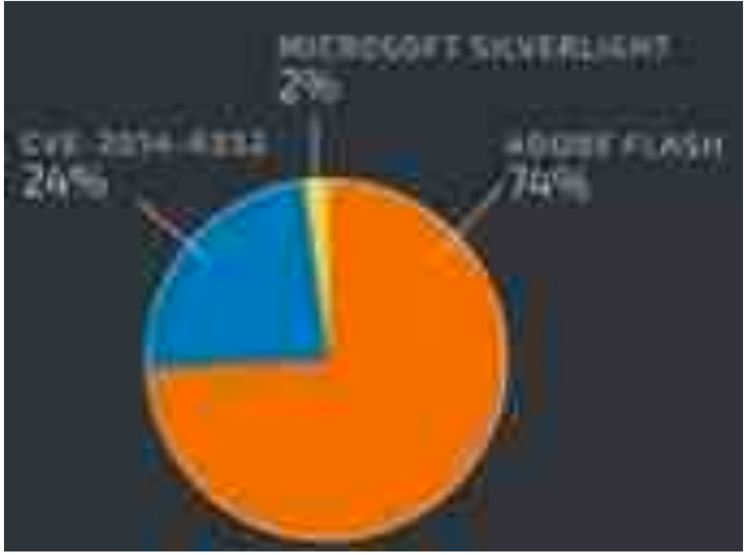
❹ Honeyclients

- Honeyclient H2 (Cuckoo Sandbox):
  - Process uses known anti-detection technique.
  - Process spawns another process.
  - Process downloads exe or dll file.
  - Process accesses registry or system files.

(https://cuckoosandbox.org/)

Exploit Kits – Corporate Ownage as a Service

The Angler Exploit Kit Exposed: Making $60 Million Annually by Delivering Ransomware



Targeted Victims / day: 90,000

Exploits Served Per Day: 9,000

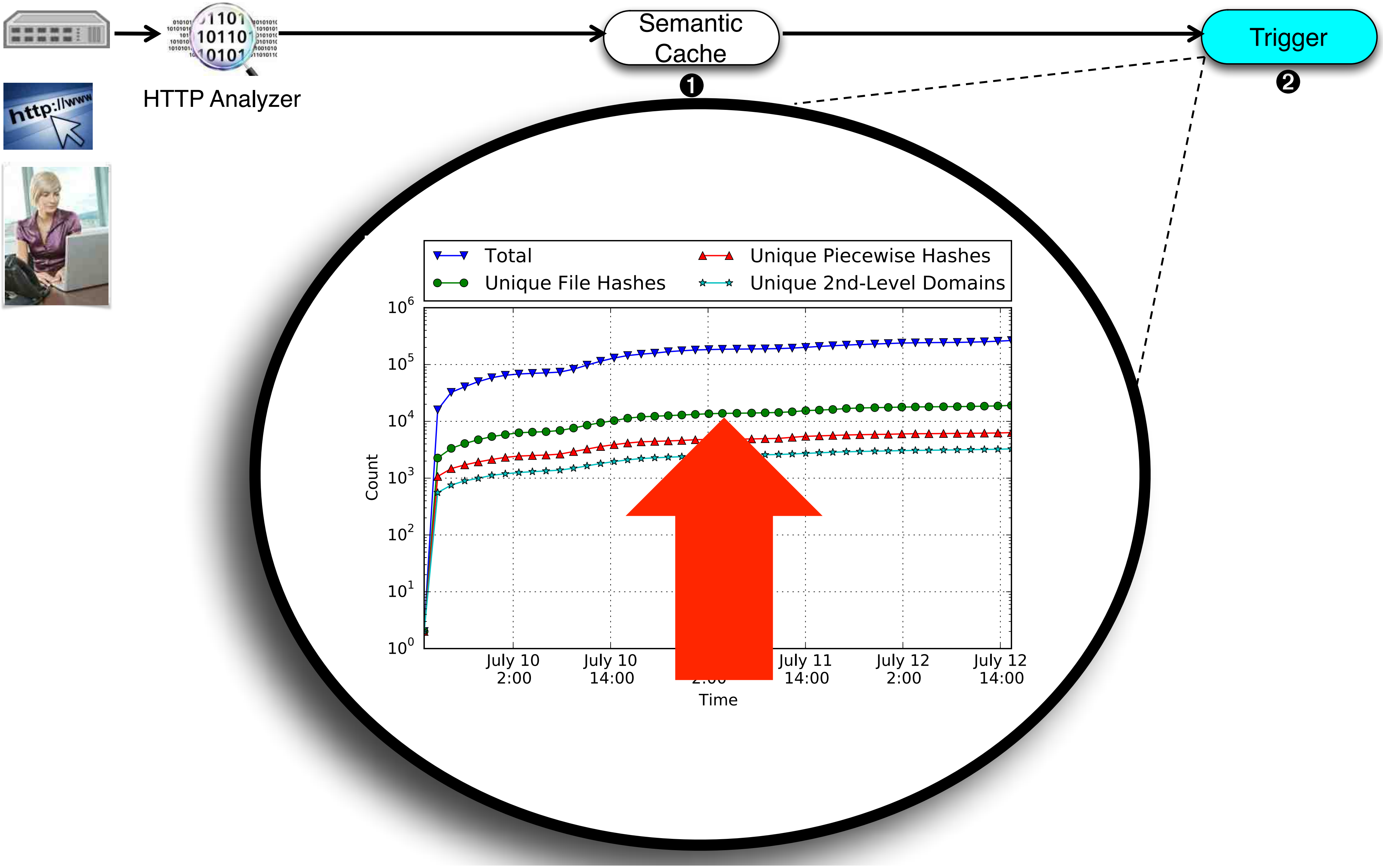
Successful Infections: 40%

Ransomware Delivered: 62%

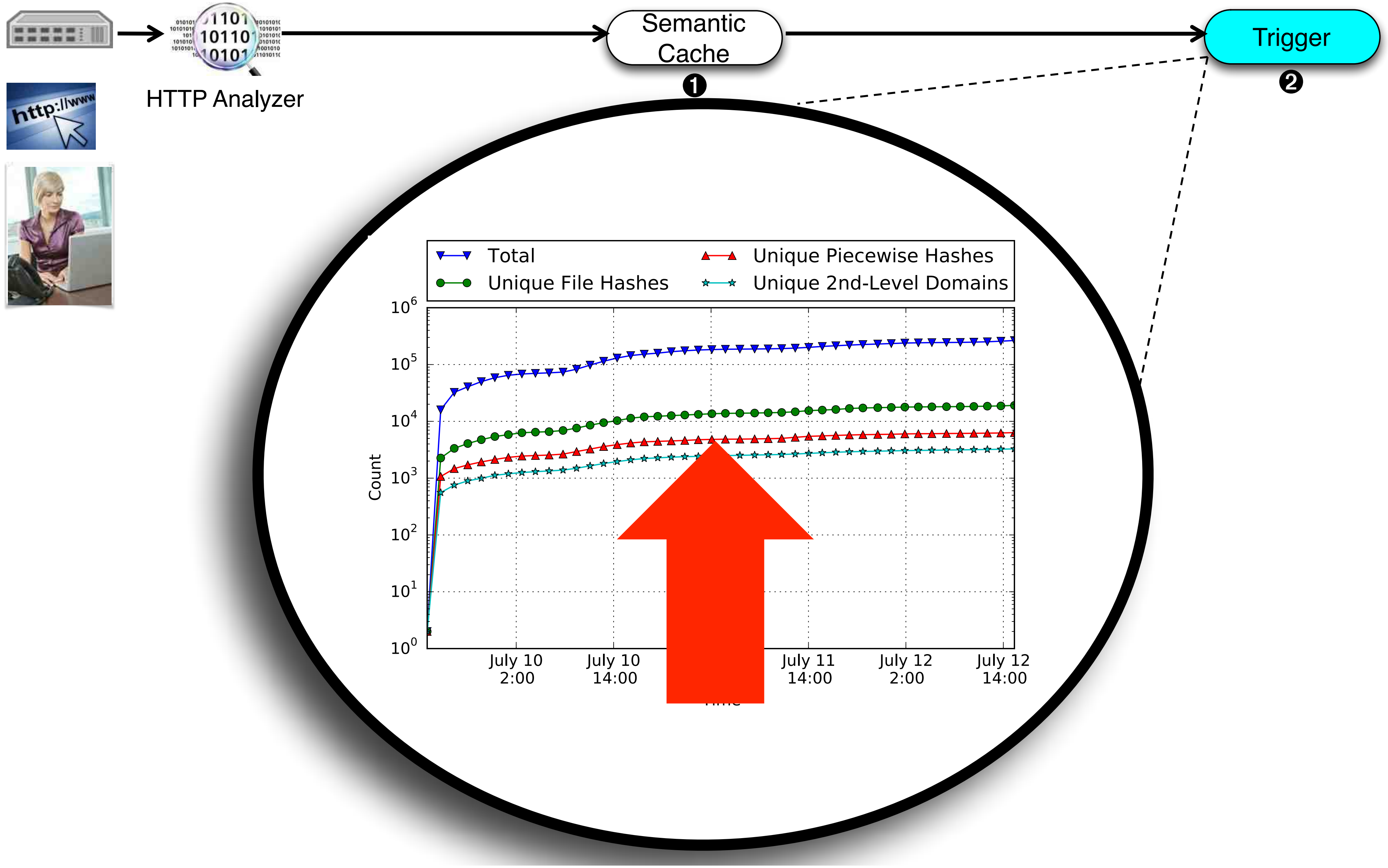
- Cisco Talos Group: http://www.talosintel.com/angler-exposed/
- October 2015

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Impact of File Hashing



Impact of Piecewise Hashing



HTTP Analyzer

Semantic Cache

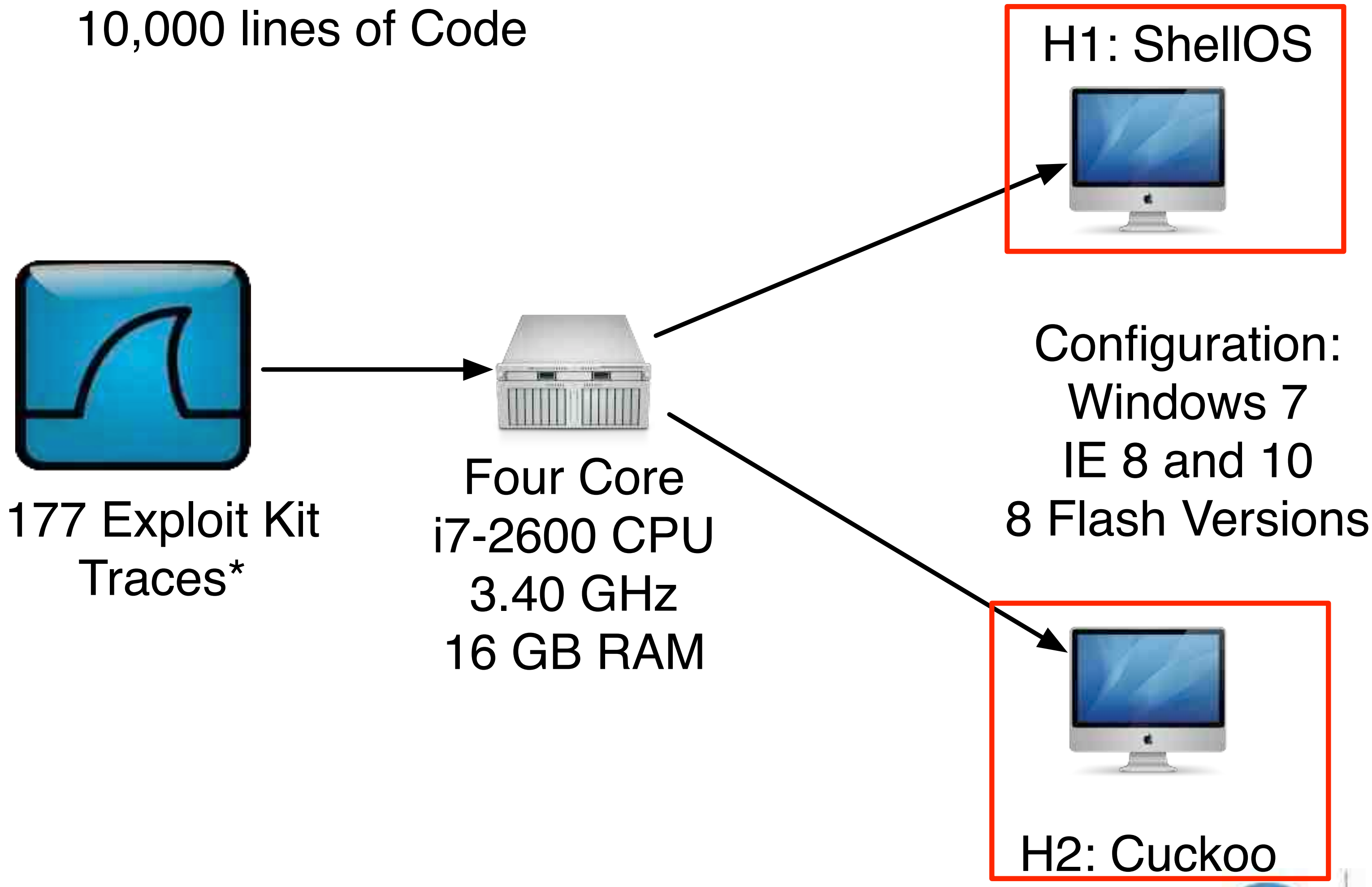
❶

Trigger

❷

Evaluation – Detection Performance

Prototype:
10,000 lines of Code



177 Exploit Kit
Traces*

Four Core
i7-2600 CPU
3.40 GHz
16 GB RAM

H1: ShellOS

Configuration:
Windows 7
IE 8 and 10
8 Flash Versions

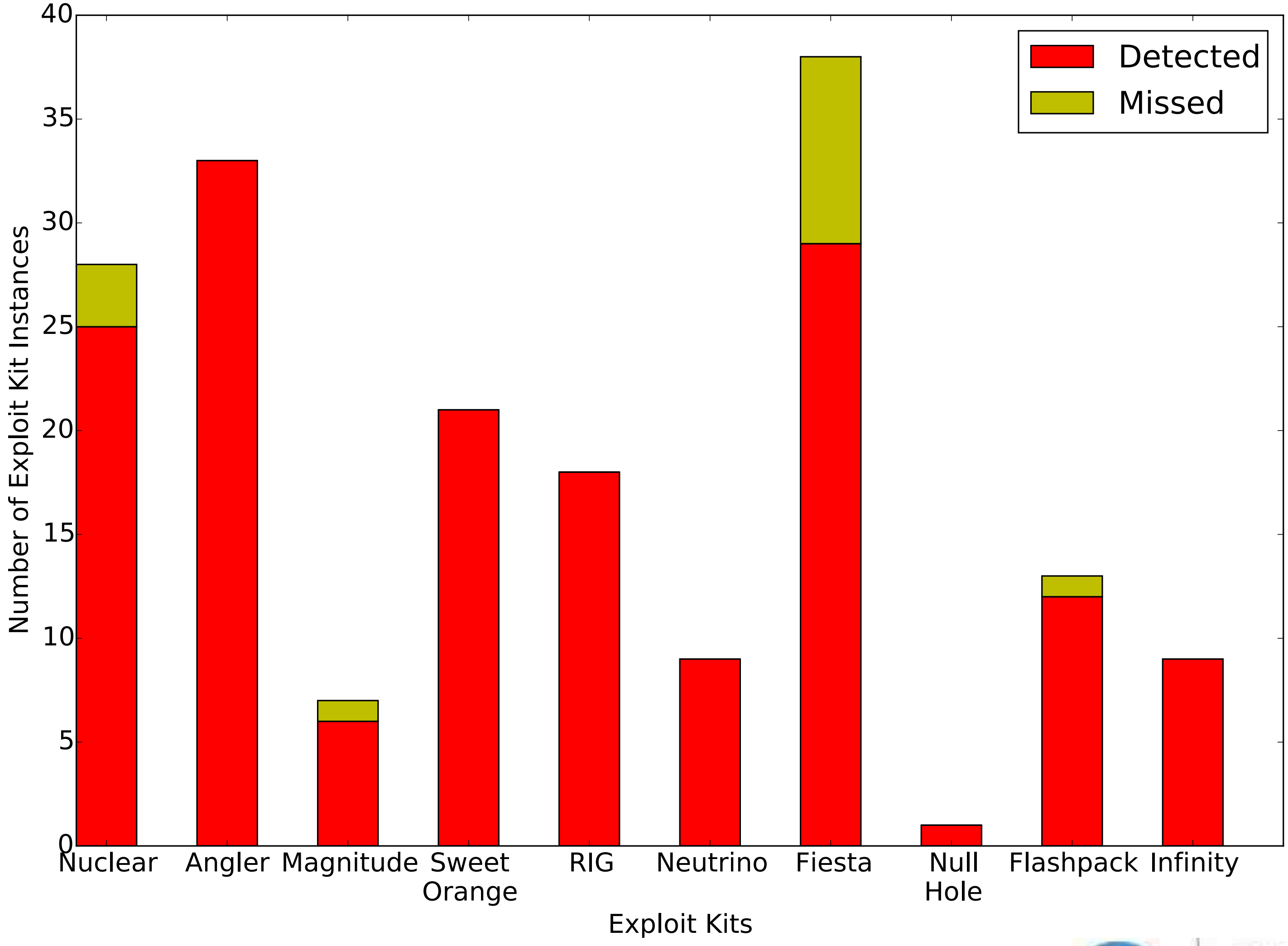
H2: Cuckoo

Monitors Code Injection/ Reuse.

Monitors OS Changes.

*www.malware-traffic-analysis.net

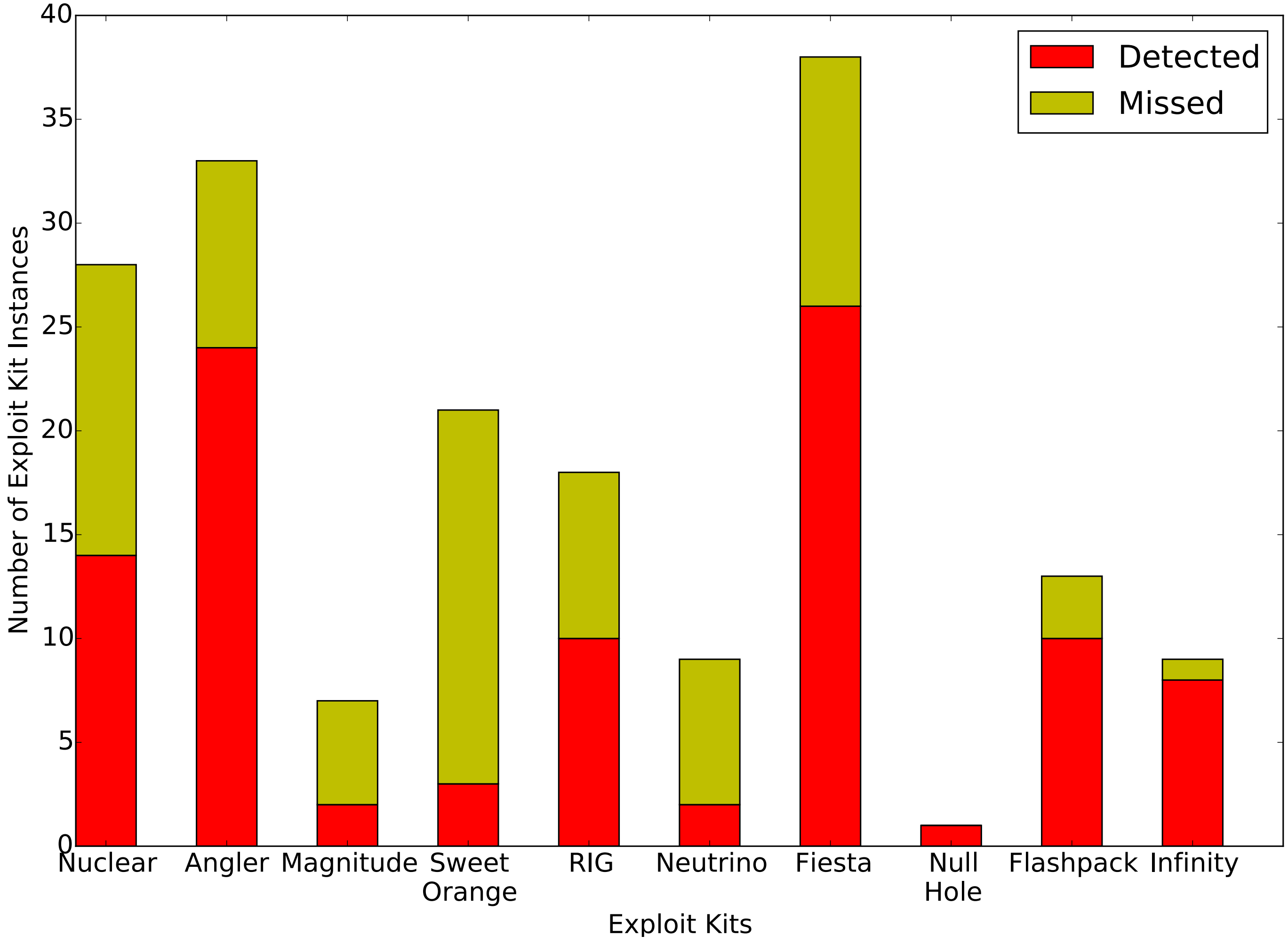
Evaluation – H1 Results



92% True Positive Rate

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

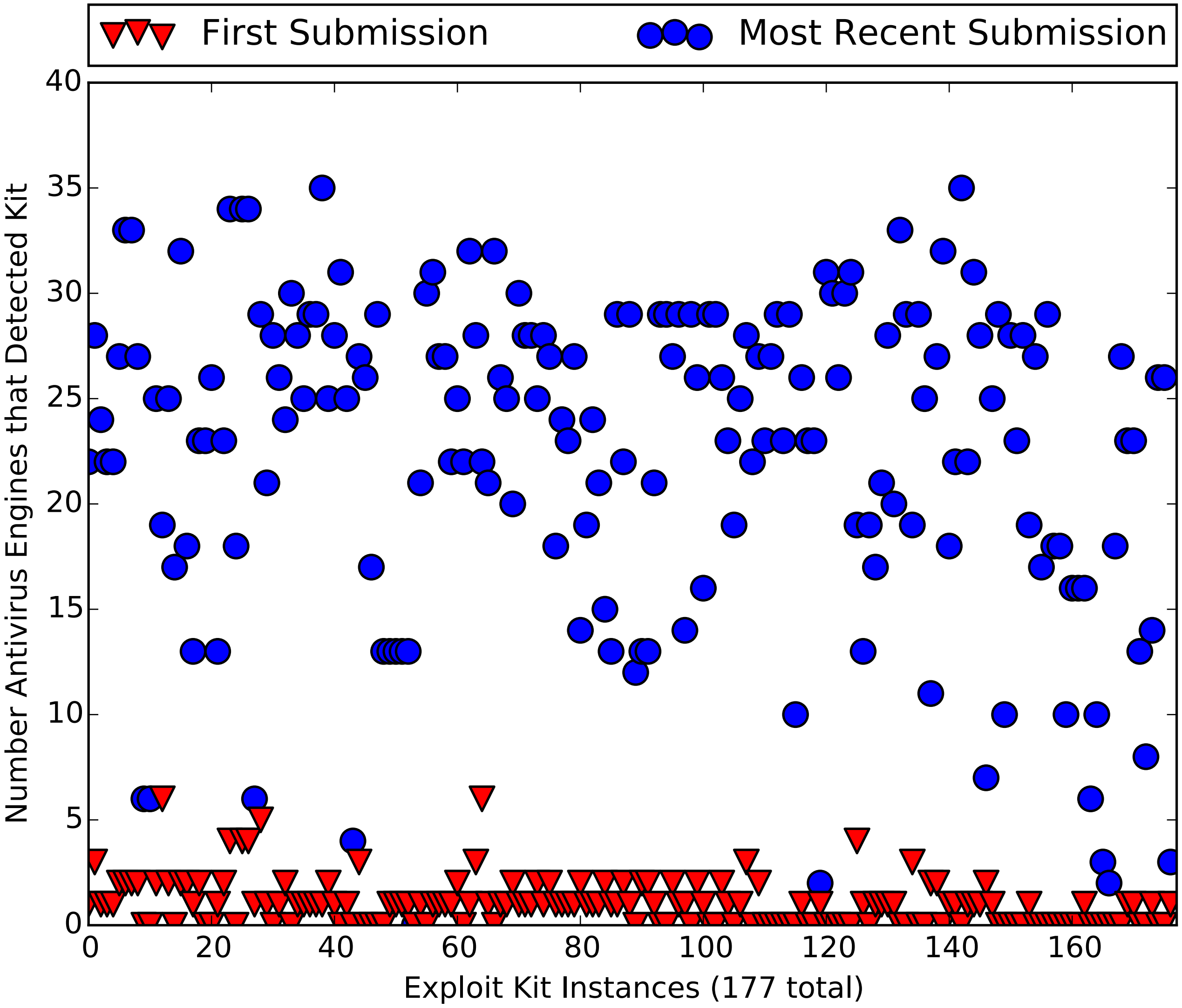
Evaluation – H2 Results



56% True Positive Rate

H1 & H2 Combined: 100% True Positive Rate

Evaluation – Comparison – VirusTotal



61 % True Positive Rate

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL