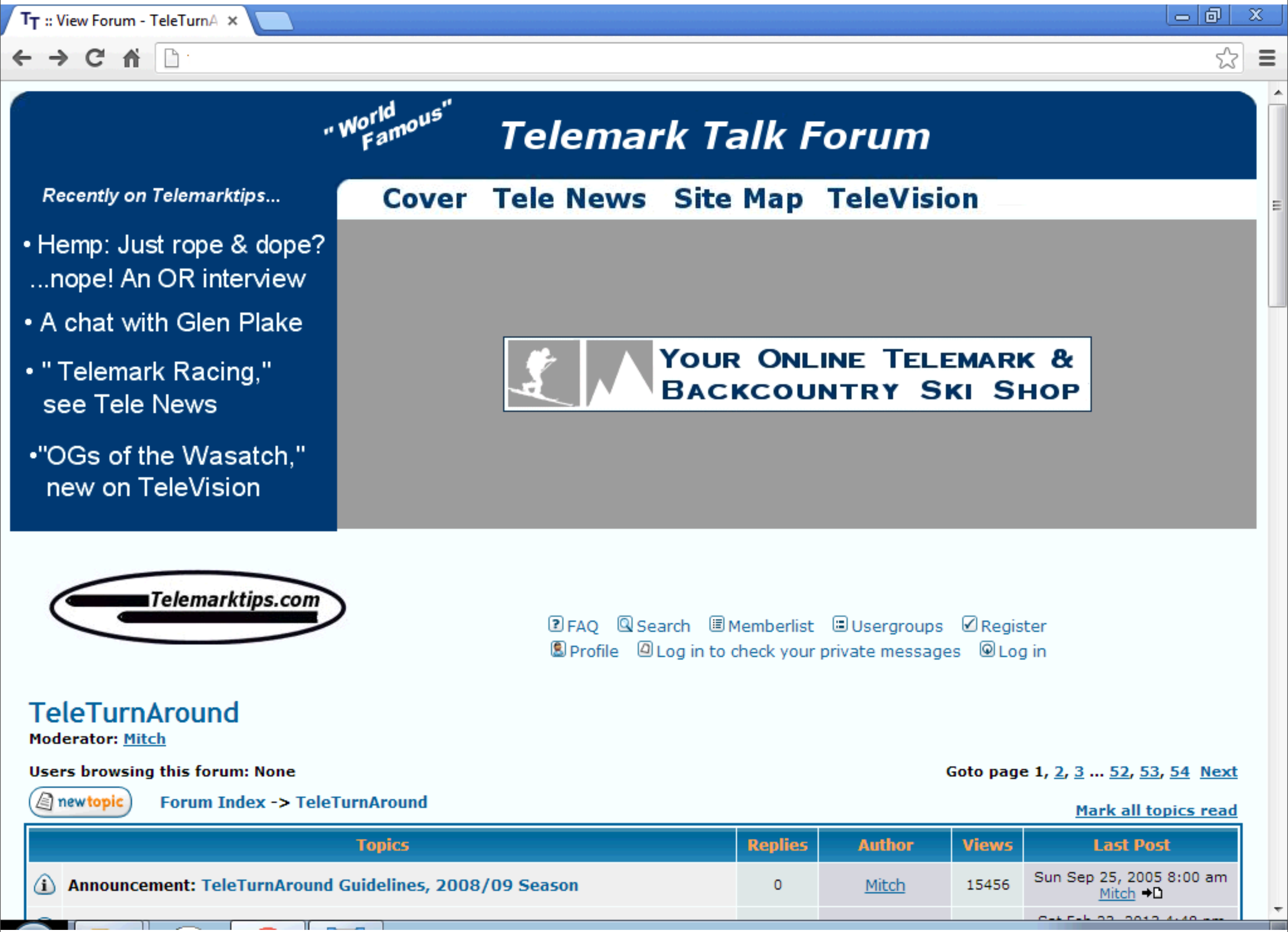


"World Famous"

Telemark Talk Forum

Recently on Telemarktips...

- Hemp: Just rope & dope? ...nope! An OR interview
- A chat with Glen Plake
- " Telemark Racing," see Tele News
- "OGs of the Wasatch," new on TeleVision

Cover Tele News Site Map TeleVision

Telemarktips.com

FAQ Search Memberlist Usergroups Register
Profile Log in to check your private messages Log in

TeleTurnAround

Moderator: Mitch

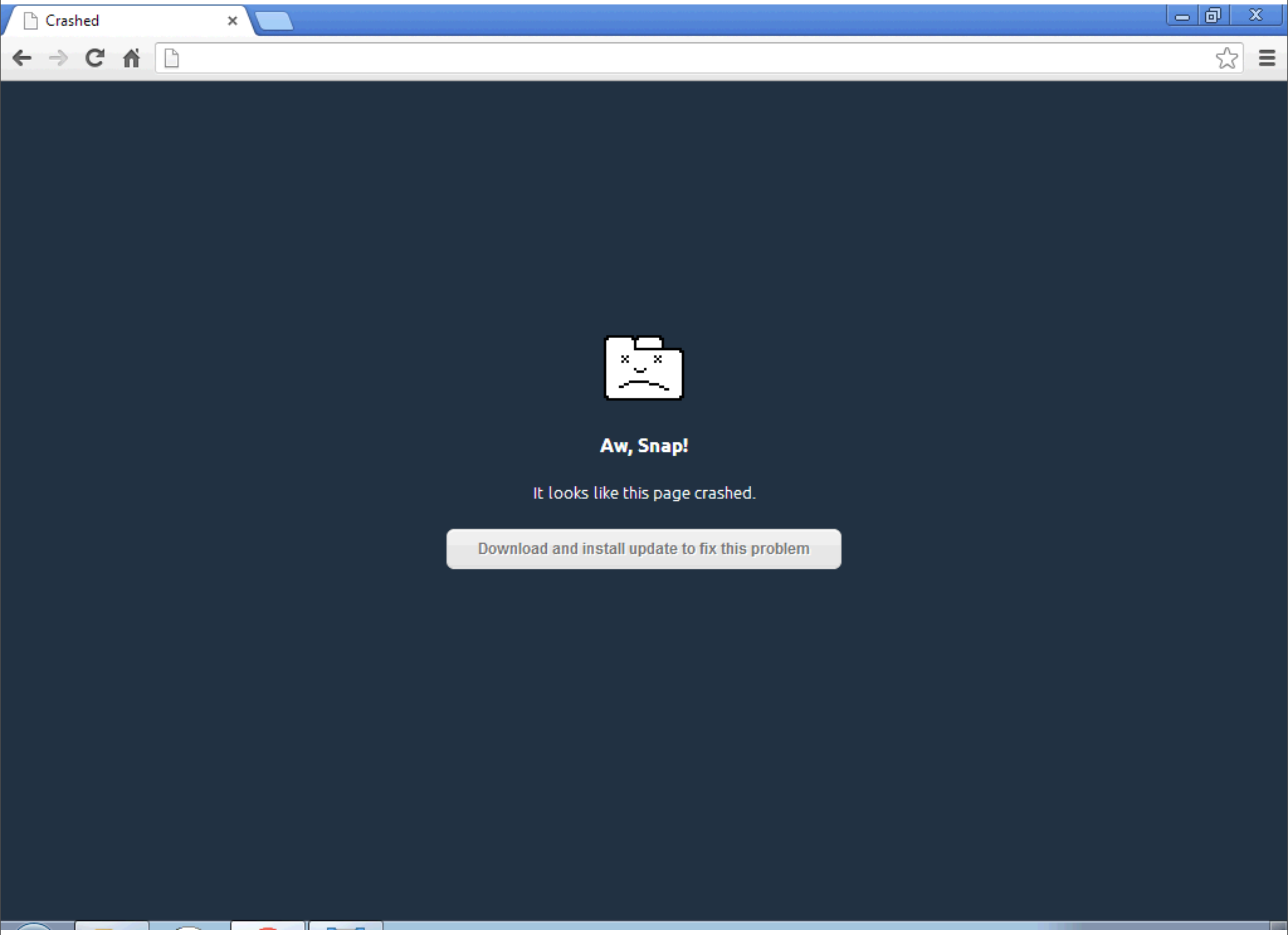
Users browsing this forum: None

Goto page 1, 2, 3 **...** 52, 53, 54 Next

new topic Forum Index -> TeleTurnAround

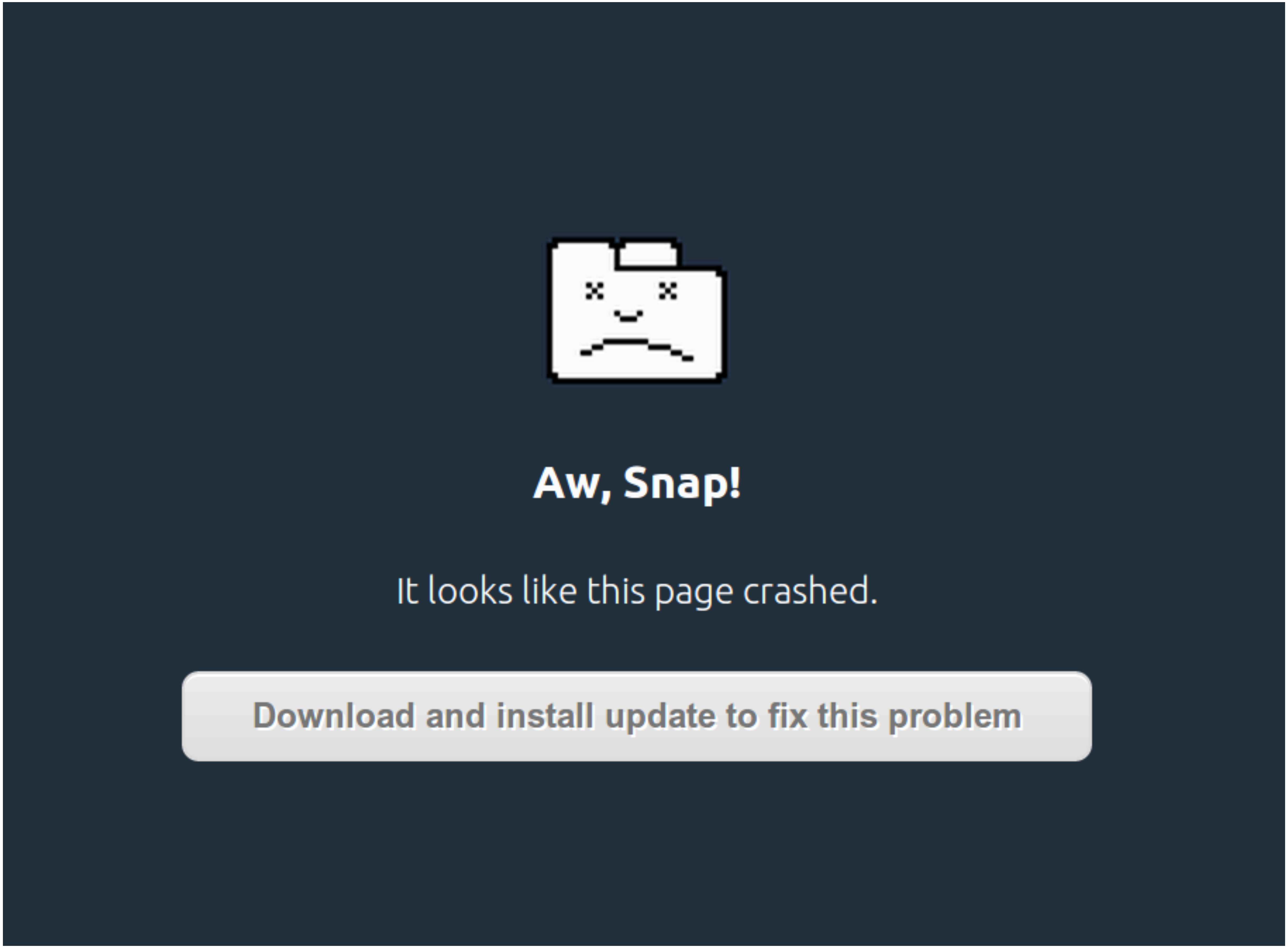
Mark all topics read

Topics	Replies	Author	Views	Last Post
Announcement: TeleTurnAround Guidelines, 2008/09 Season	0	Mitch	15456	Sun Sep 25, 2005 8:00 am Mitch



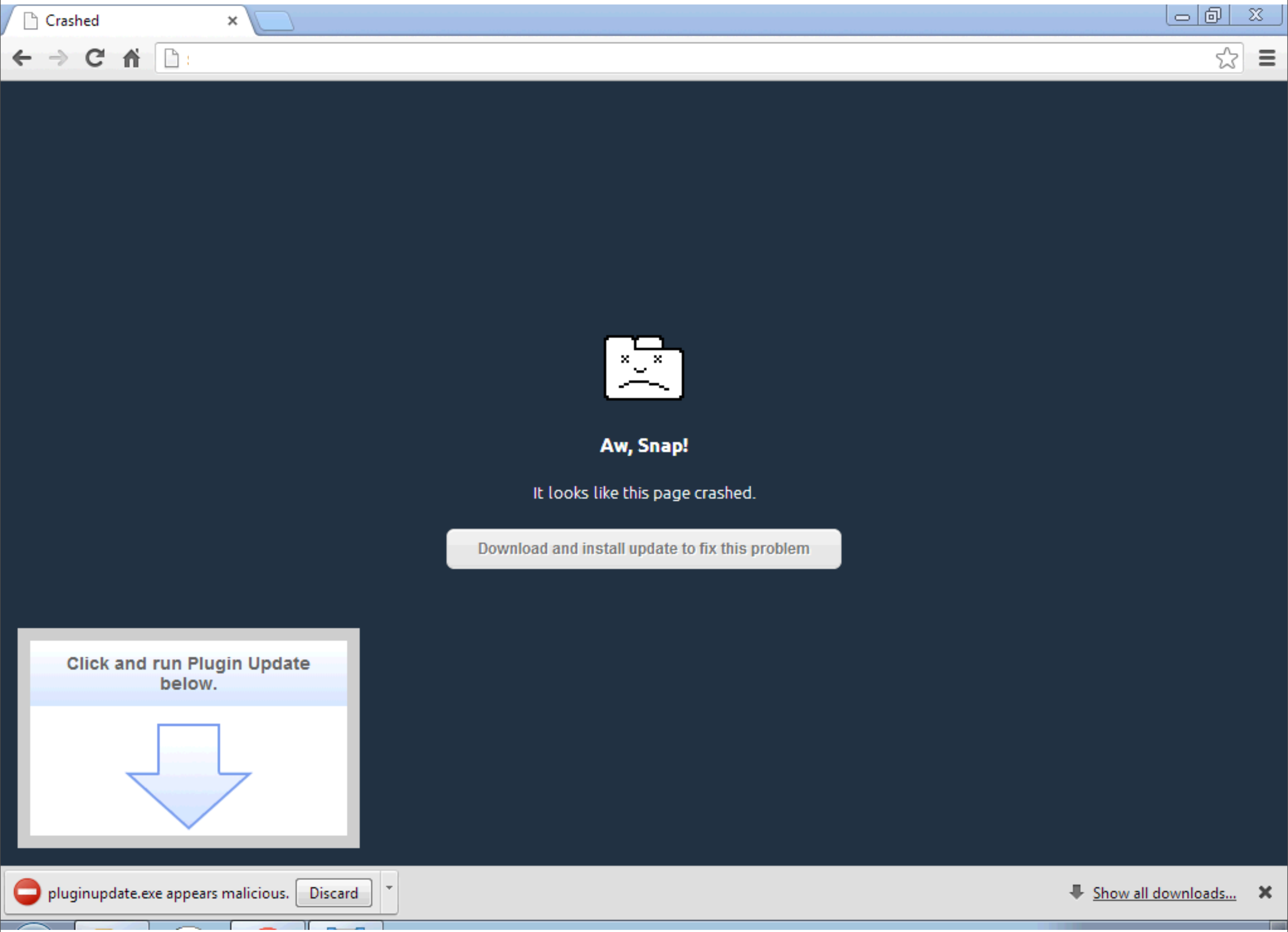
Aw, Snap!

It looks like this page crashed.



Aw, Snap!

It looks like this page crashed.



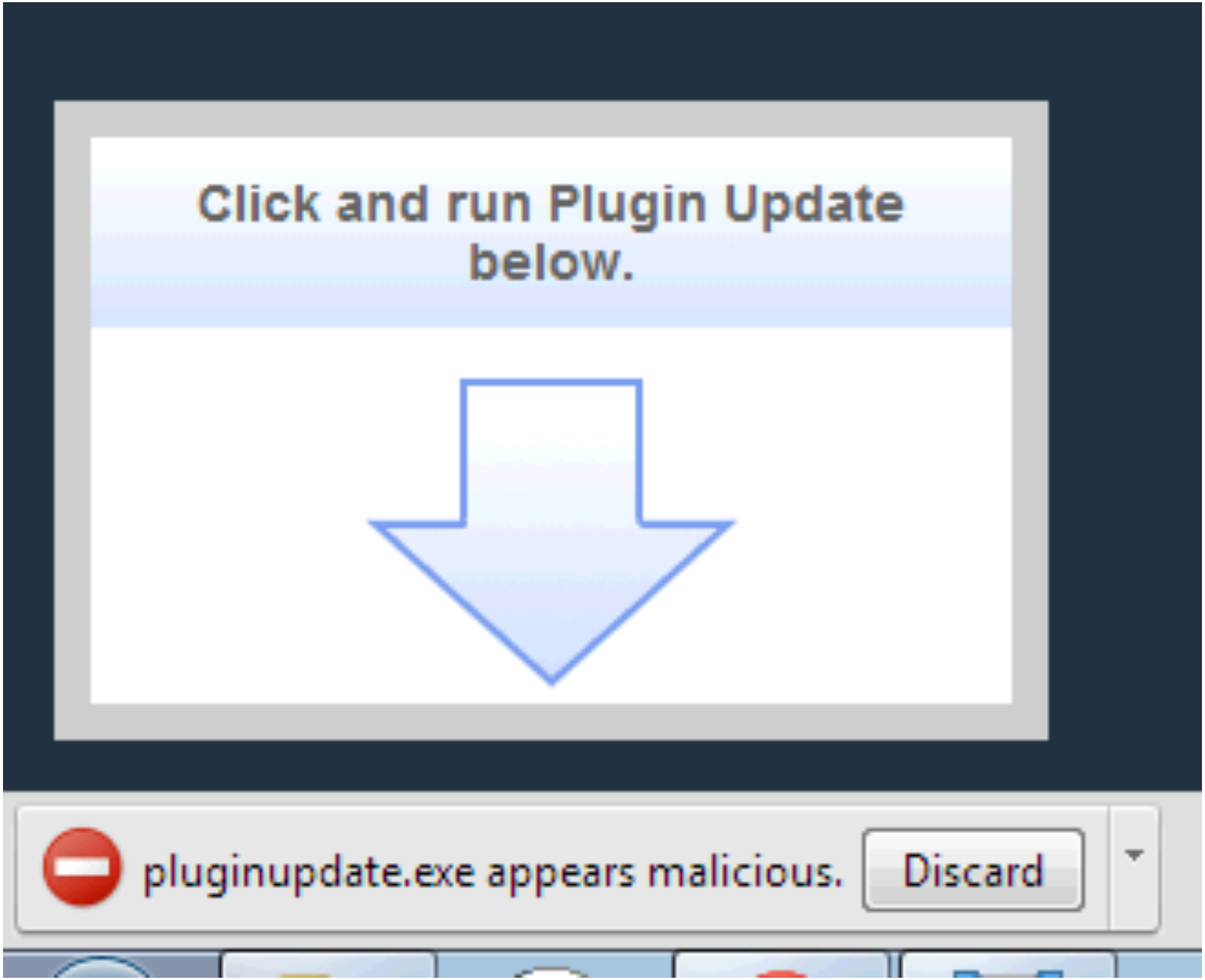
Aw, Snap!

It looks like this page crashed.

Download and install update to fix this problem

Click and run Plugin Update below.

pluginupdate.exe appears malicious. Discard



Click and run Plugin Update below.

pluginupdate.exe appears malicious.

CAMP

Content Agnostic Malware Protection

Moheeb Abu Rajab, Lucas Ballard, Noé Lutz,
Panayiotis Mavrommatis and Niels Provos

Google Safe Browsing Team

Current Situation

- Web still used for malware distribution
- Browsers and plug-ins are more secure
- Drive-by-downloads become challenging
- Social Engineering attacks on the rise

Challenges

- Exploit detection mechanism fail
- URL malware lists can be ineffective
- AVs struggle with polymorphic binaries
- Binary whitelists do not scale

Objective

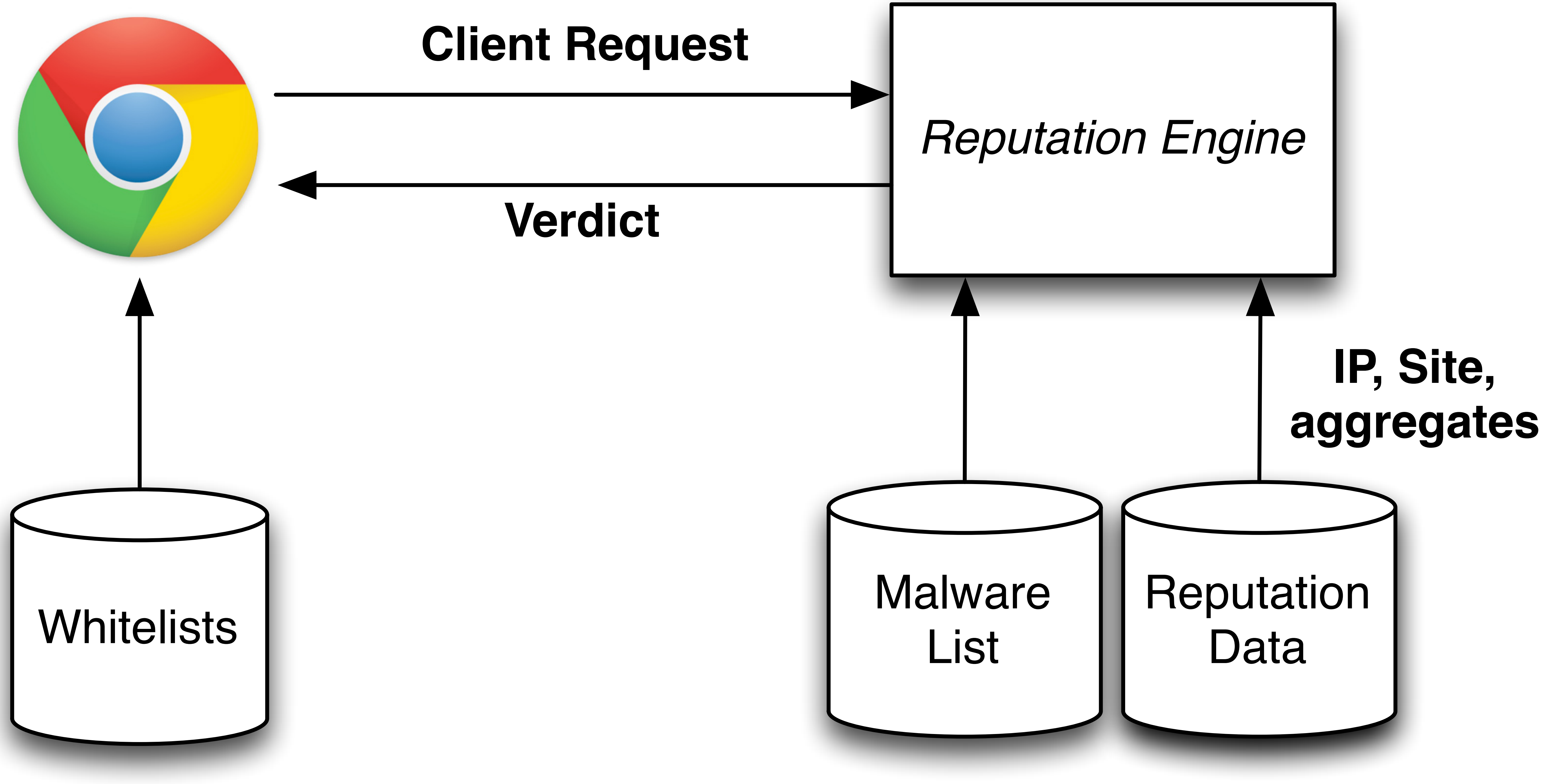
Contributions

- Content agnostic malware protection
- Real-time detection of malware
- Hybrid detection approach
- 6 month evaluation with 200M users

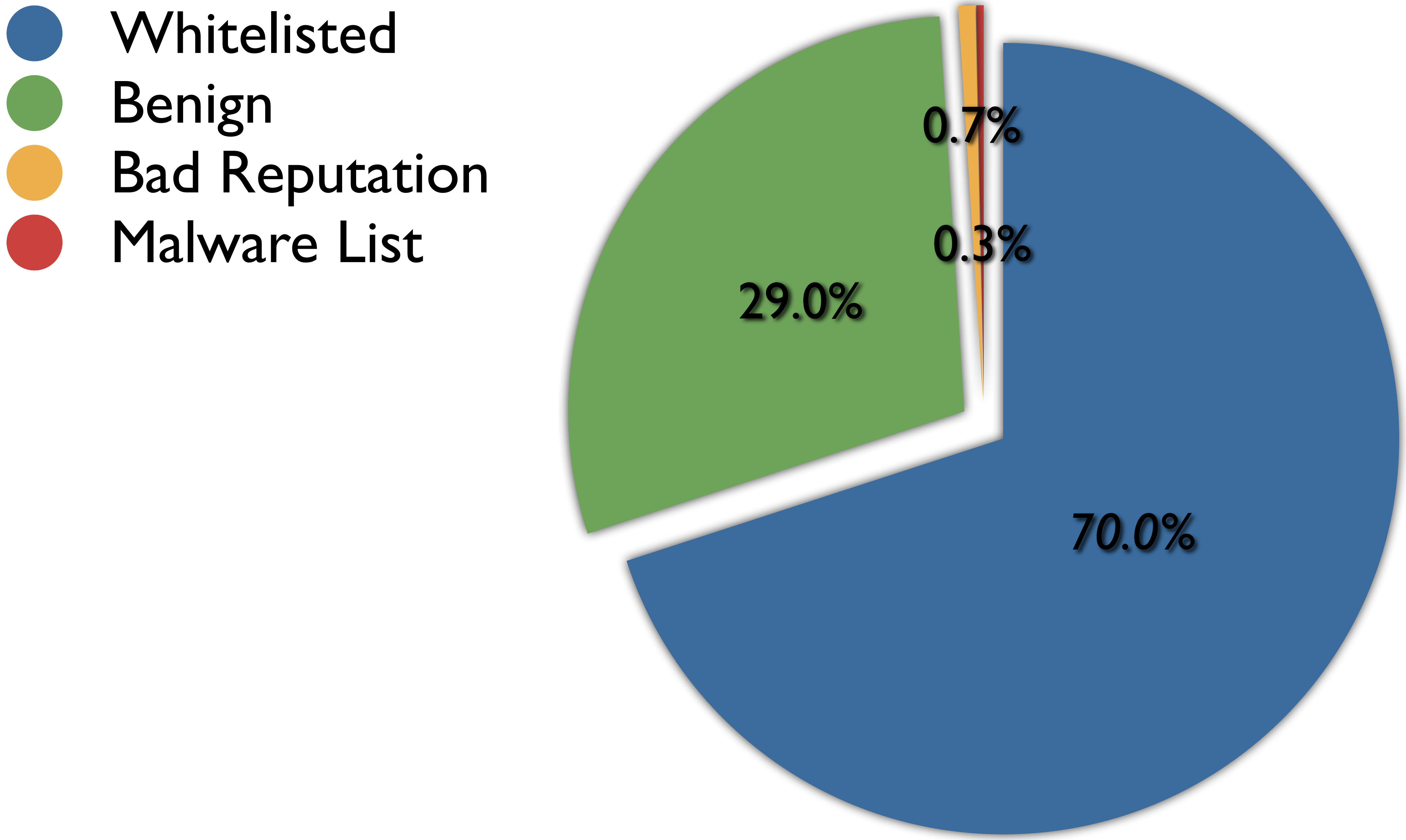
Overview

- System Architecture
- Evaluation
- Case study
- Conclusion

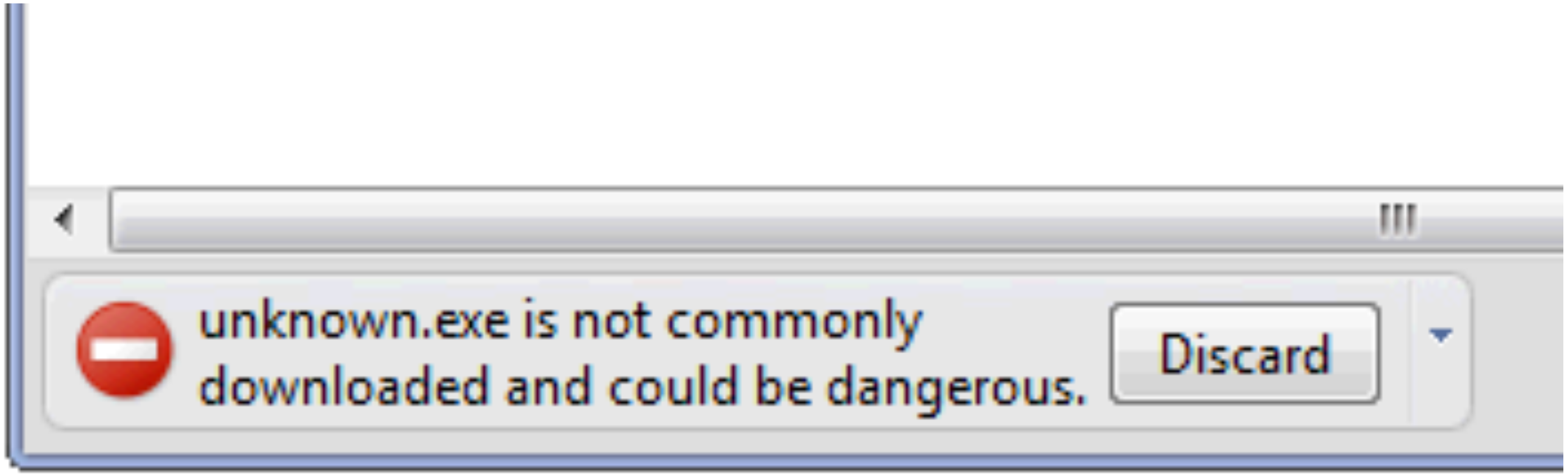
System Architecture



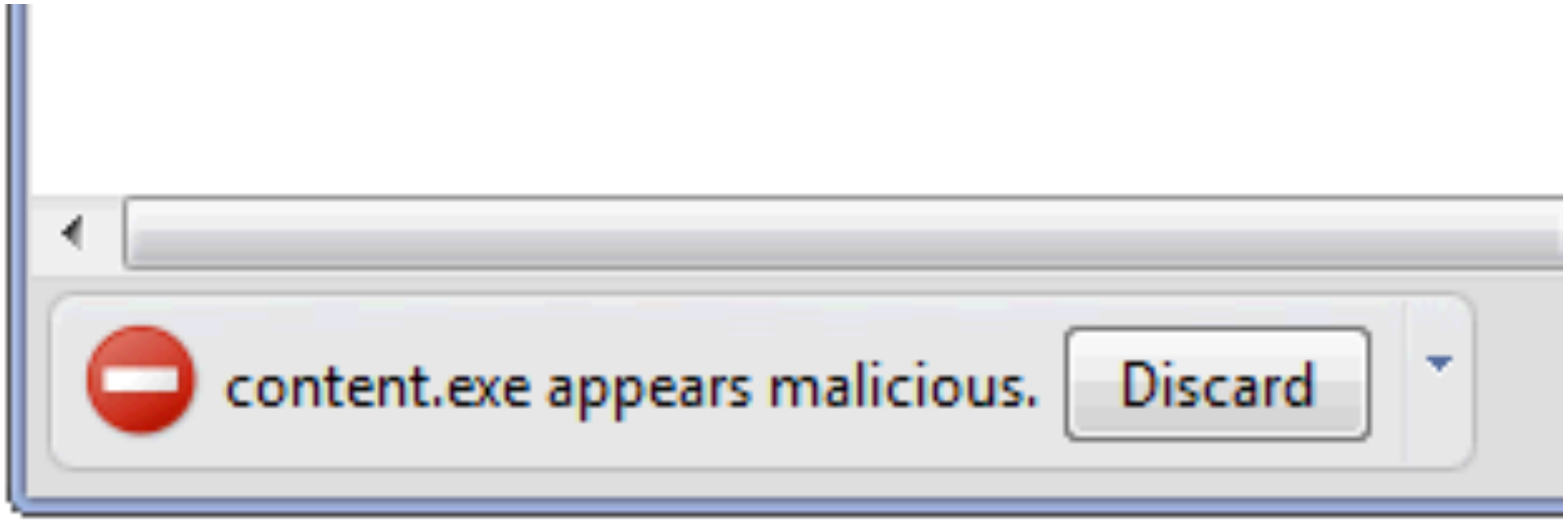
Hybrid Approach



Verdict in Chrome

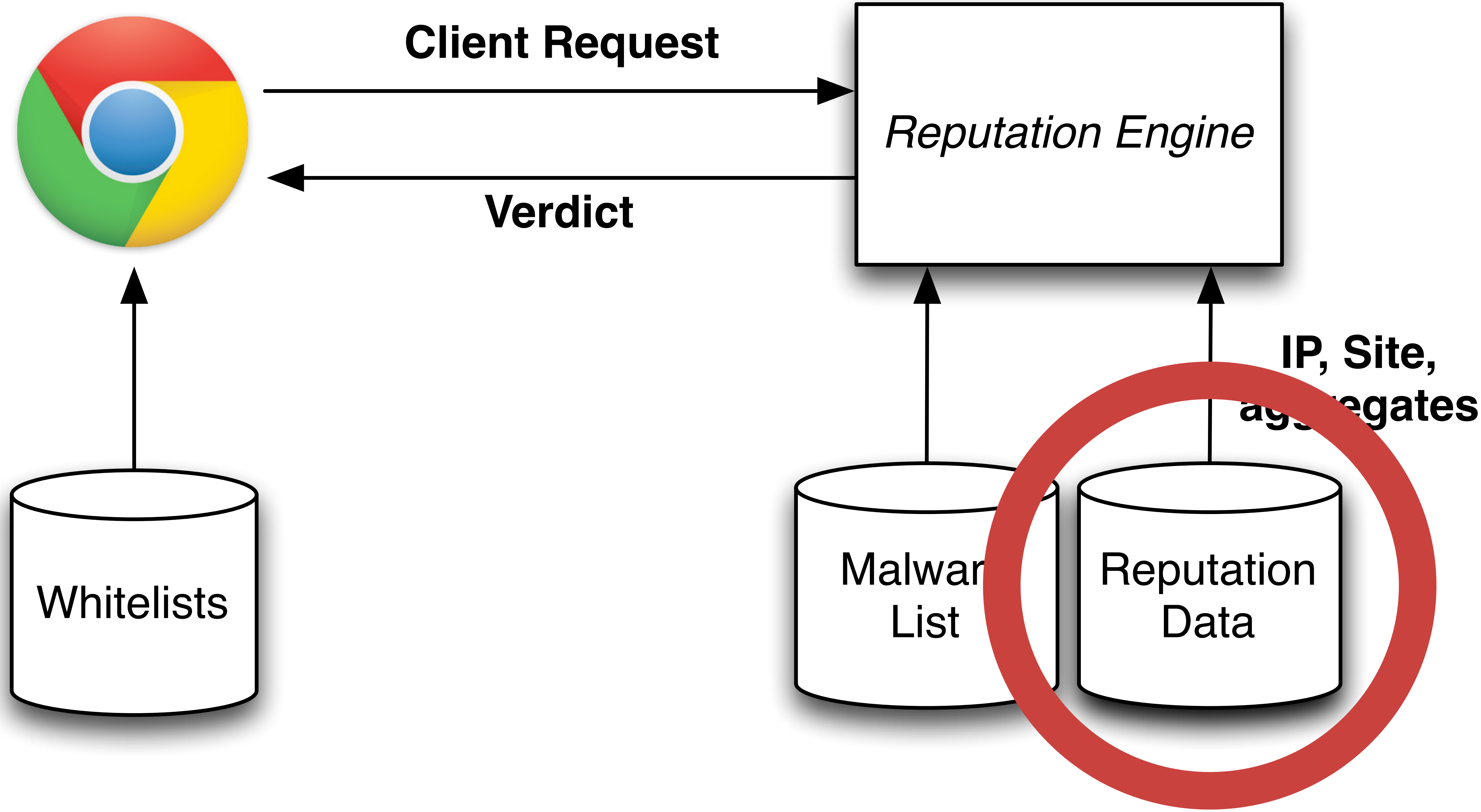


unknown.exe is not commonly downloaded and could be dangerous.



content.exe appears malicious.

System Architecture



Client Request

Reputation Engine

Verdict

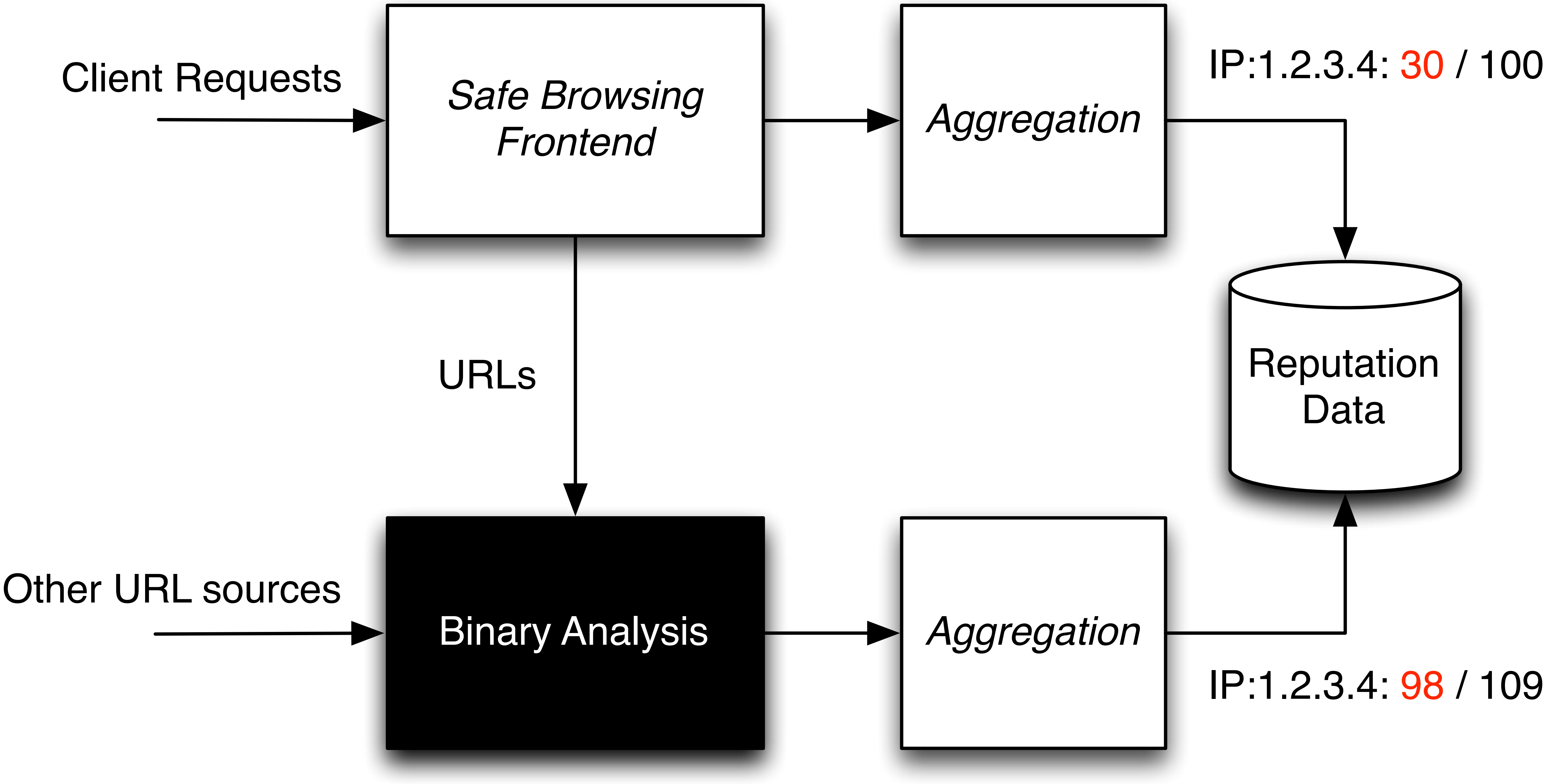
IP, Site, aggregates

Whitelists

Malwar List

Reputation Data

Reputation Data



Reputation Engine

Aggregate: # bad / # total events

Feature / Aggregation Key	Baseline Aggregates
IP:1.2.3.4	98 / 109
site:foo.com/	1039 / 5694
host:a.foo.com/	0 / 0

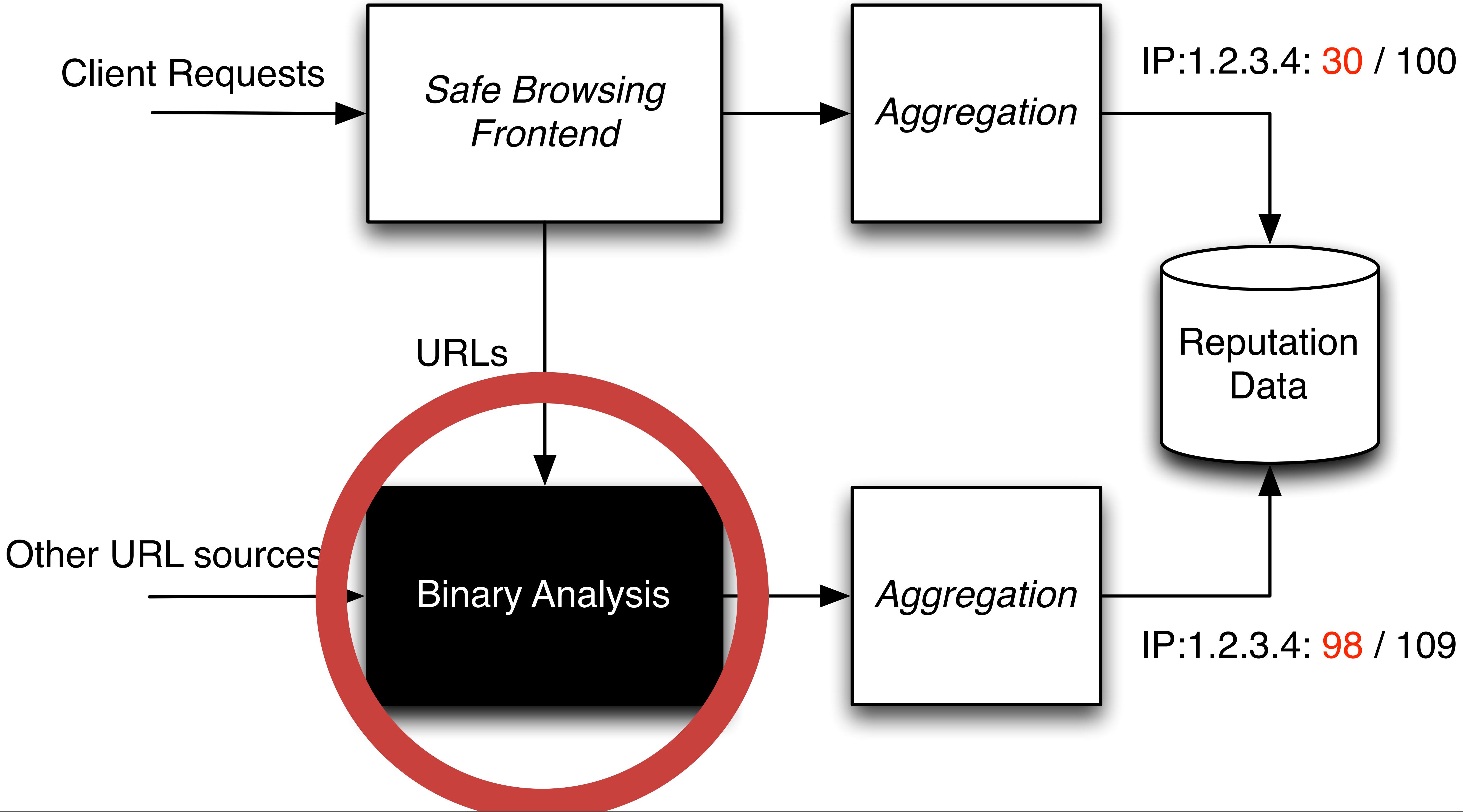
Overview

- System Architecture
- Evaluation
- Case study
- Conclusion

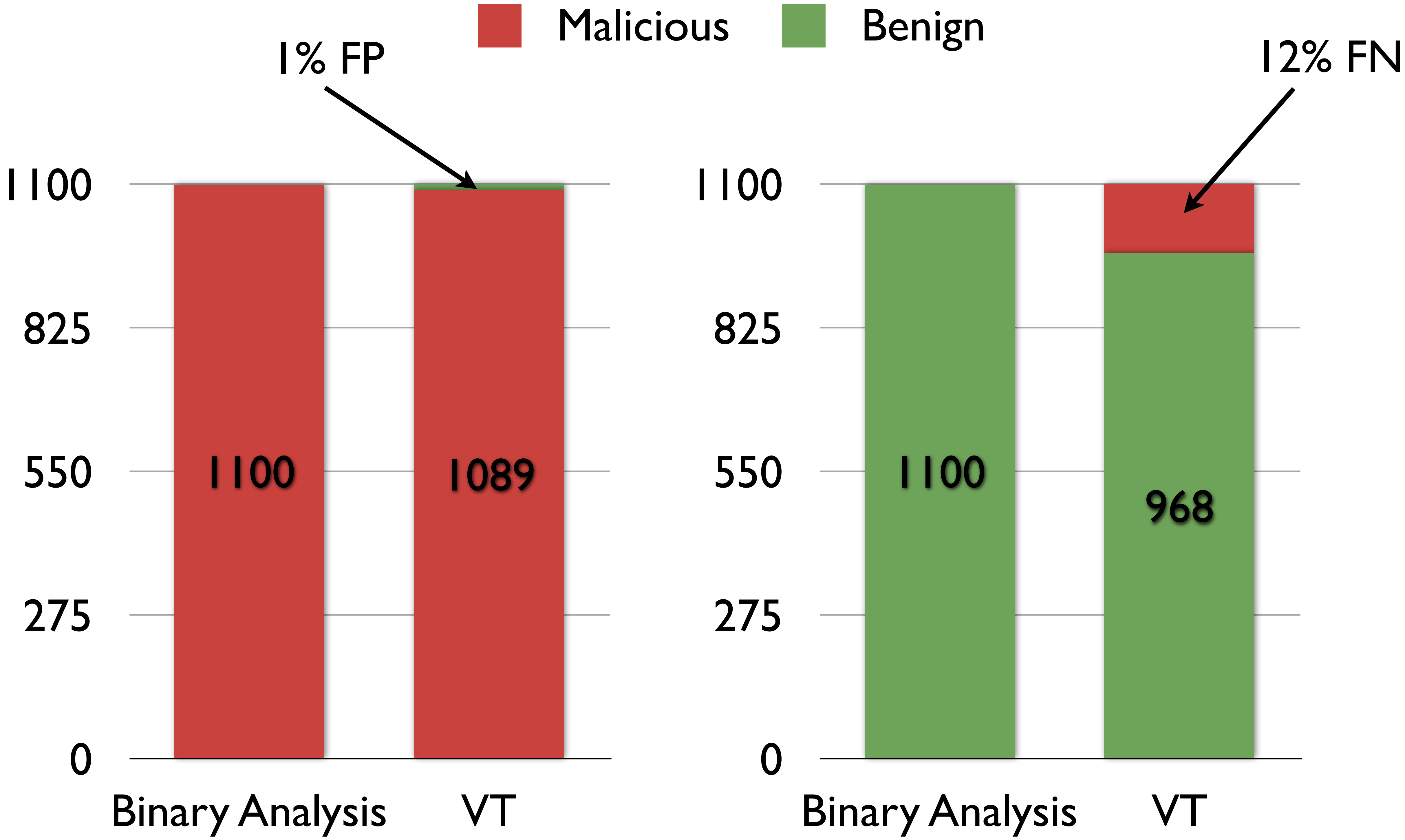
Evaluation

- 6 month evaluation, 200M Chrome users
- 15M download requests / day
- 500K warnings shown / day

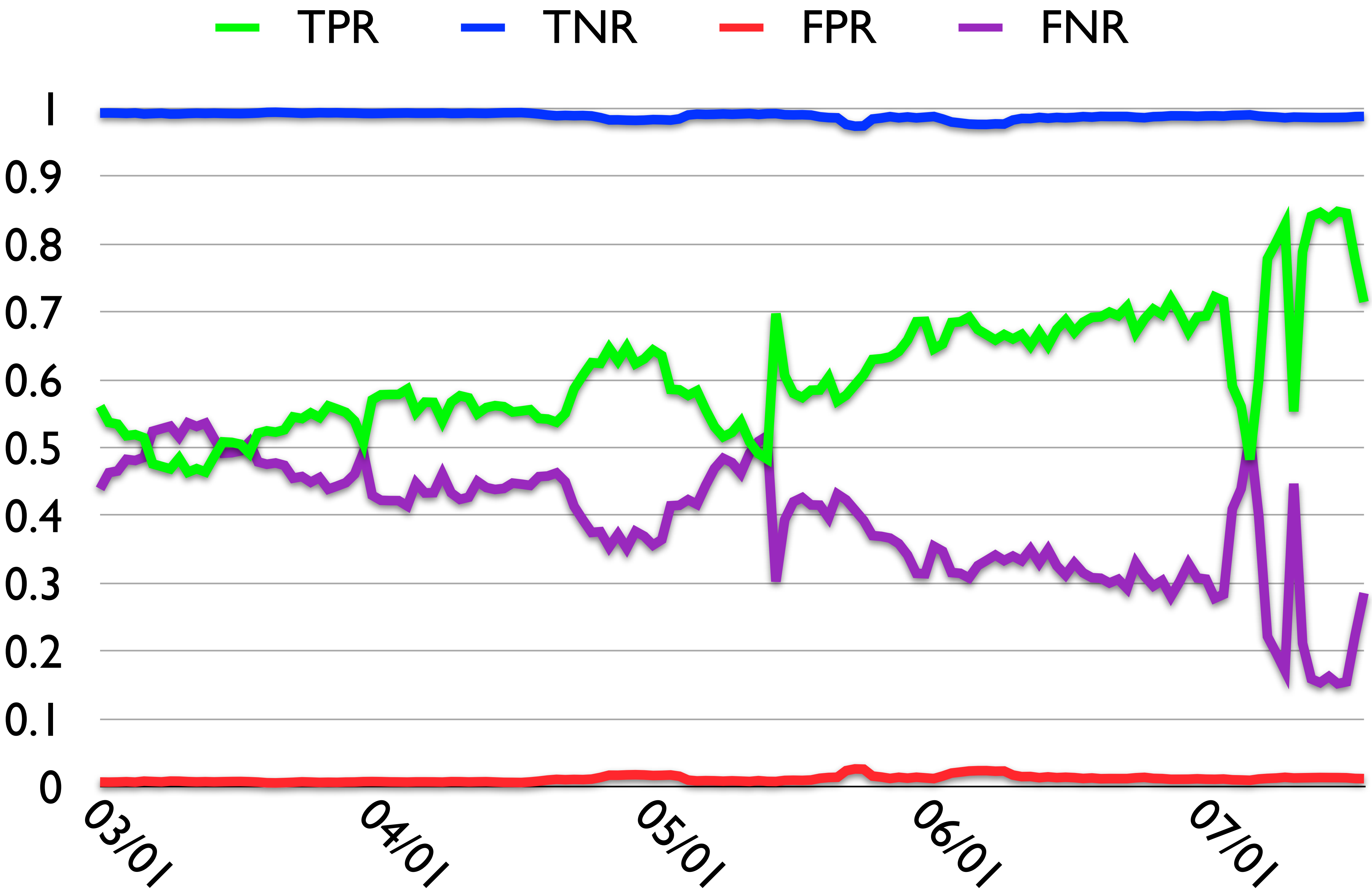
Evaluation - Labeling



Evaluation - Labeling



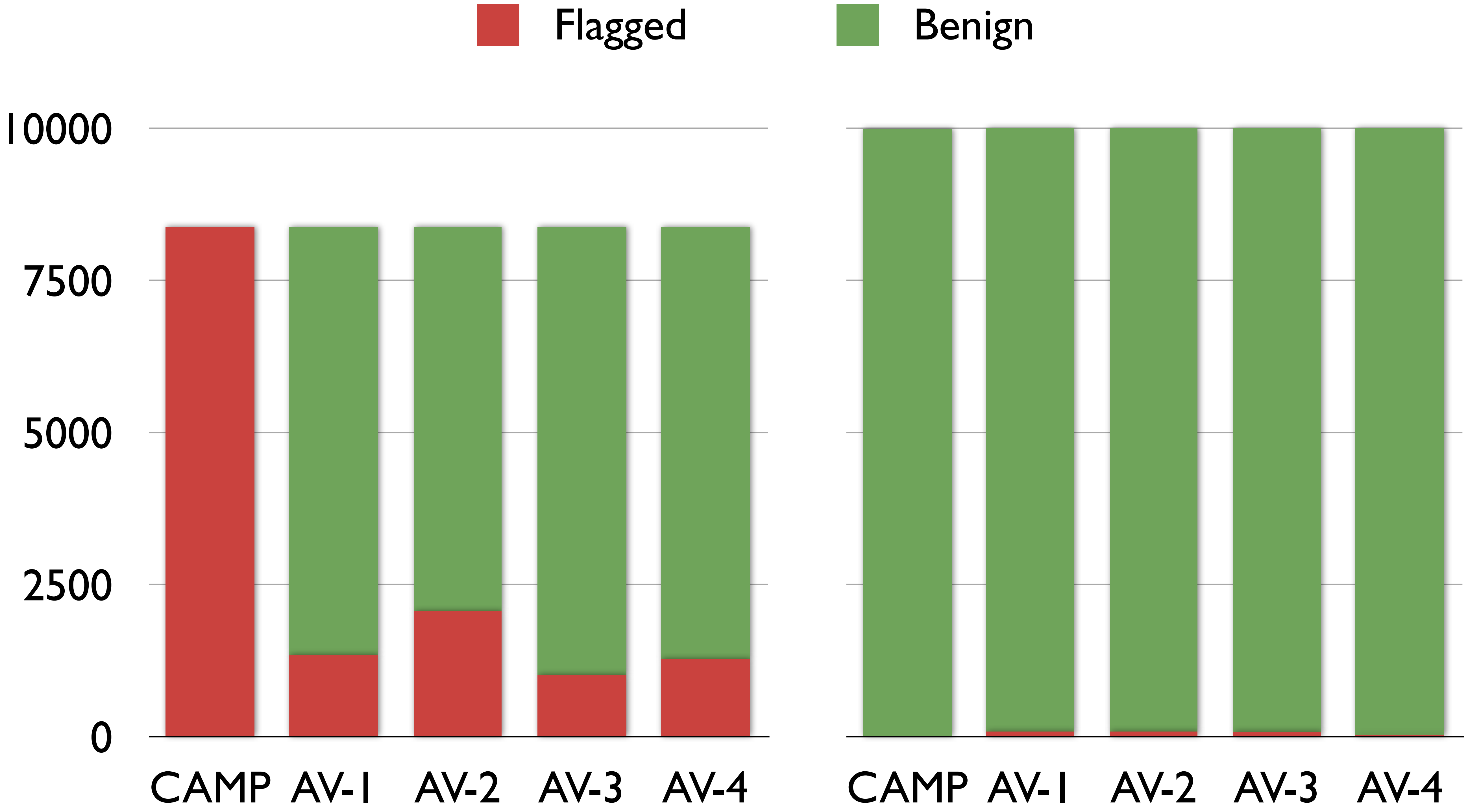
Evaluation - Reputation



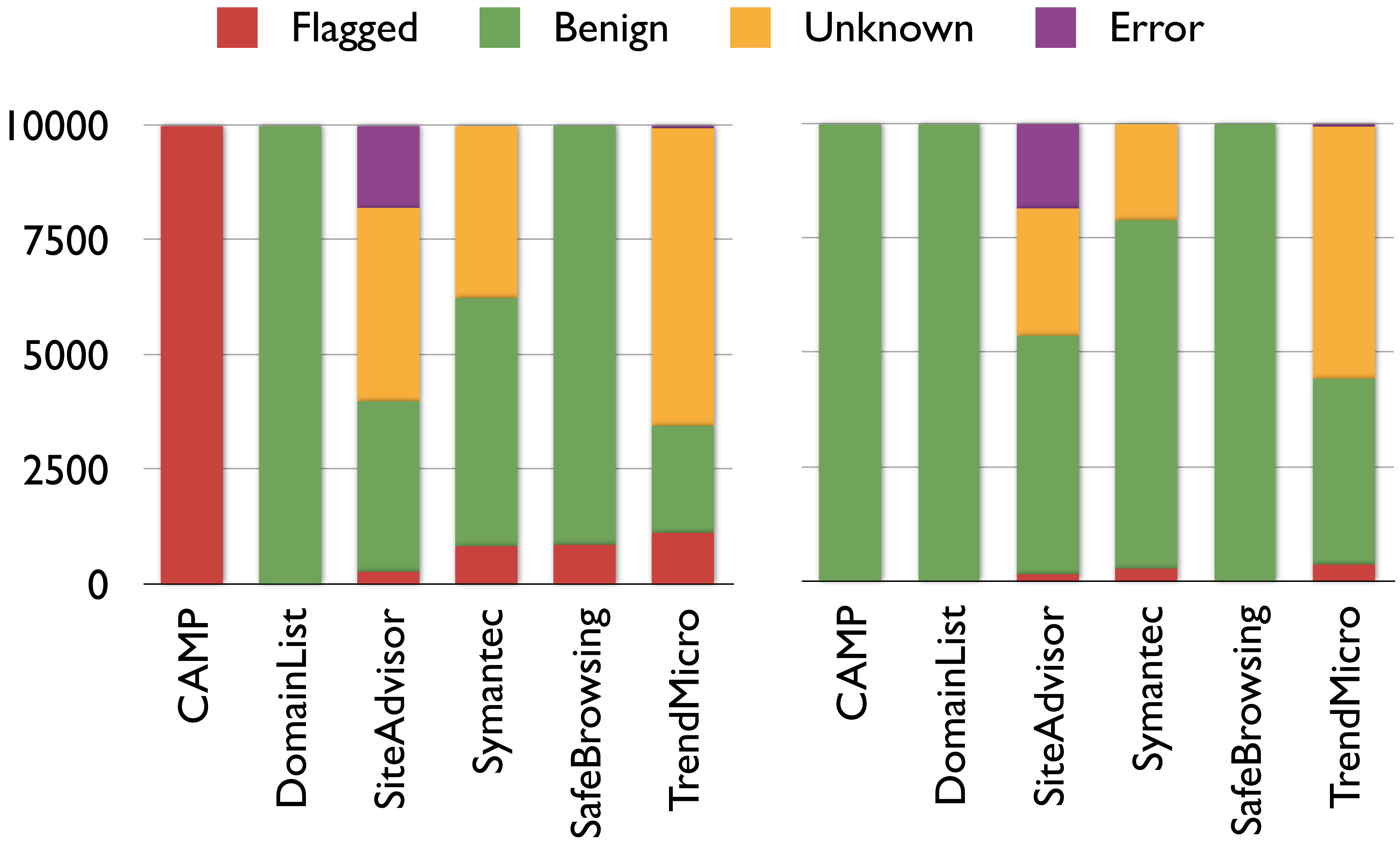
Overall Accuracy

	Reputation Engine	Overall
Accuracy	98%	99.5%
FPR	2%	0.6%

CAMP Reputation vs. AVs



CAMP Reputation vs. URL lists



Overview

- System Architecture
- Evaluation
- Case study
- Conclusion

Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- 13K unique hostnames over 2 week period
- Domain rotation every 7 minutes

Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- 13K unique hostnames over 2 week period
- Domain rotation every 7 minutes

⇨ URL Malware lists didn’t work here

Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- Binary changed roughly every 10 minutes
- Saw >900 distinct content hashes
- Only 1/40 Virus Total AV flagged binary

Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- Binary changed roughly every 10 minutes
- Saw >900 distinct content hashes
- Only 1/40 Virus Total AV flagged binary

➡ Content based approaches didn’t work here

Overview

- System Architecture
- Evaluation
- Case study
- Conclusion

Summary

- Content agnostic reputation approach
- Scalable to 200M users
- High accuracy with low false positive rate

??