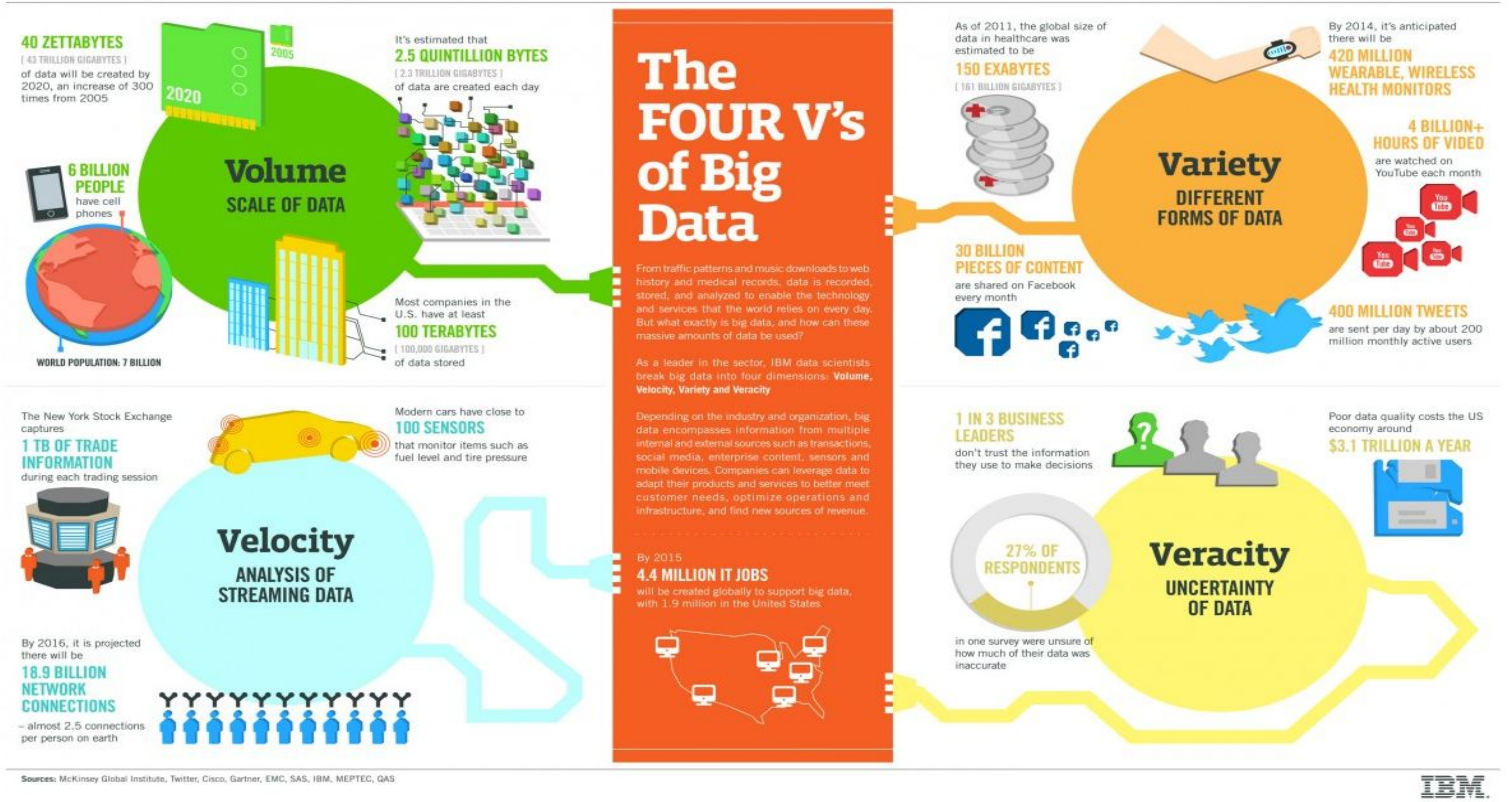
Big Data Analysis Applied to Network Security

Email Team@bnshosting.net for more

Website: www.bnshosting.net



The FOUR V's of Big Data

From traffic patterns and music downloads to web history and medical records, data is recorded, stored, and analyzed to enable the technology and services that the world relies on every day. But what exactly is big data, and how can these massive amounts of data be used?

As a leader in the sector, IBM data scientists break big data into four dimensions: **Volume, Velocity, Variety and Veracity**

Depending on the industry and organization, big data encompasses information from multiple internal and external sources such as transactions, social media, enterprise content, sensors and mobile devices. Companies can leverage data to adapt their products and services to better meet customer needs, optimize operations and infrastructure, and find new sources of revenue.

By 2015
4.4 MILLION IT JOBS
will be created globally to support big data, with 1.9 million in the United States

Volume
SCALE OF DATA

40 ZETTABYTES
[43 TRILLION GIGABYTES]
of data will be created by 2020, an increase of 300 times from 2005

It's estimated that
2.5 QUINTILLION BYTES
[2.3 TRILLION GIGABYTES]
of data are created each day

6 BILLION PEOPLE
have cell phones

WORLD POPULATION: 7 BILLION

Most companies in the U.S. have at least
100 TERABYTES
[100,000 GIGABYTES]
of data stored

Velocity
ANALYSIS OF STREAMING DATA

The New York Stock Exchange captures
1 TB OF TRADE INFORMATION
during each trading session

Modern cars have close to
100 SENSORS
that monitor items such as fuel level and tire pressure

By 2016, it is projected there will be
18.9 BILLION NETWORK CONNECTIONS
– almost 2.5 connections per person on earth

Variety
DIFFERENT FORMS OF DATA

As of 2011, the global size of data in healthcare was estimated to be
150 EXABYTES
[161 BILLION GIGABYTES]

By 2014, it's anticipated there will be
420 MILLION WEARABLE, WIRELESS HEALTH MONITORS

4 BILLION+ HOURS OF VIDEO
are watched on YouTube each month

30 BILLION PIECES OF CONTENT
are shared on Facebook every month

400 MILLION TWEETS
are sent per day by about 200 million monthly active users

Veracity
UNCERTAINTY OF DATA

1 IN 3 BUSINESS LEADERS
don't trust the information they use to make decisions

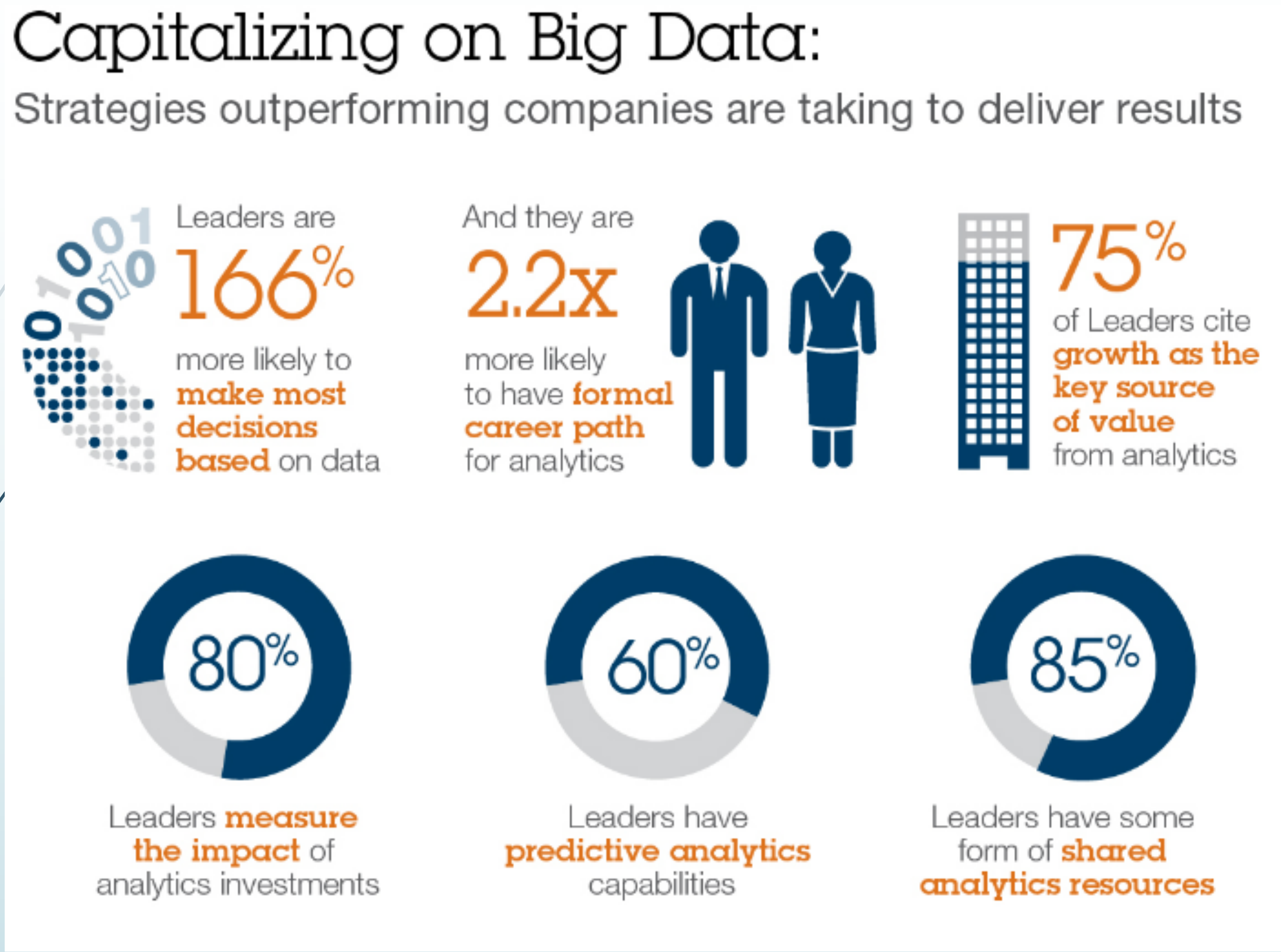
Poor data quality costs the US economy around
$3.1 TRILLION A YEAR

27% OF RESPONDENTS
in one survey were unsure of how much of their data was inaccurate

Sources: McKinsey Global Institute, Twitter, Cisco, Gartner, EMC, SAS, IBM, MEPTEC, QAS

IBM

Types of Big Data Analytics



Capitalizing on Big Data:

Strategies outperforming companies are taking to deliver results

Leaders are **166%** more likely to **make most decisions based** on data

And they are **2.2x** more likely to have **formal career path** for analytics

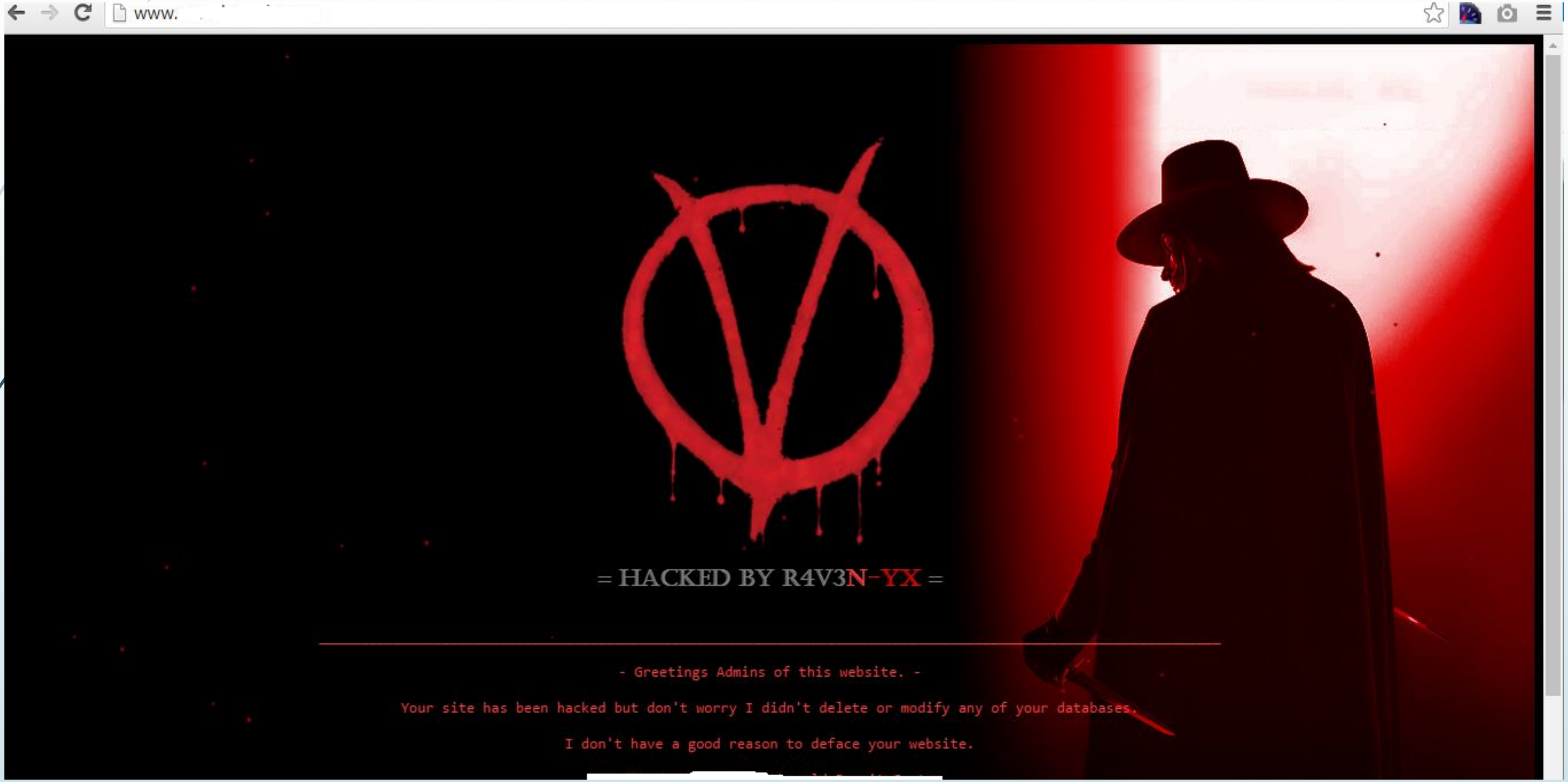
75% of Leaders cite **growth as the key source of value** from analytics

80% Leaders **measure the impact** of analytics investments

60% Leaders have **predictive analytics** capabilities

85% Leaders have some form of **shared analytics resources**

1st Benefit: Faster Forensics



www.[redacted]

= HACKED BY R4V3N-YX =

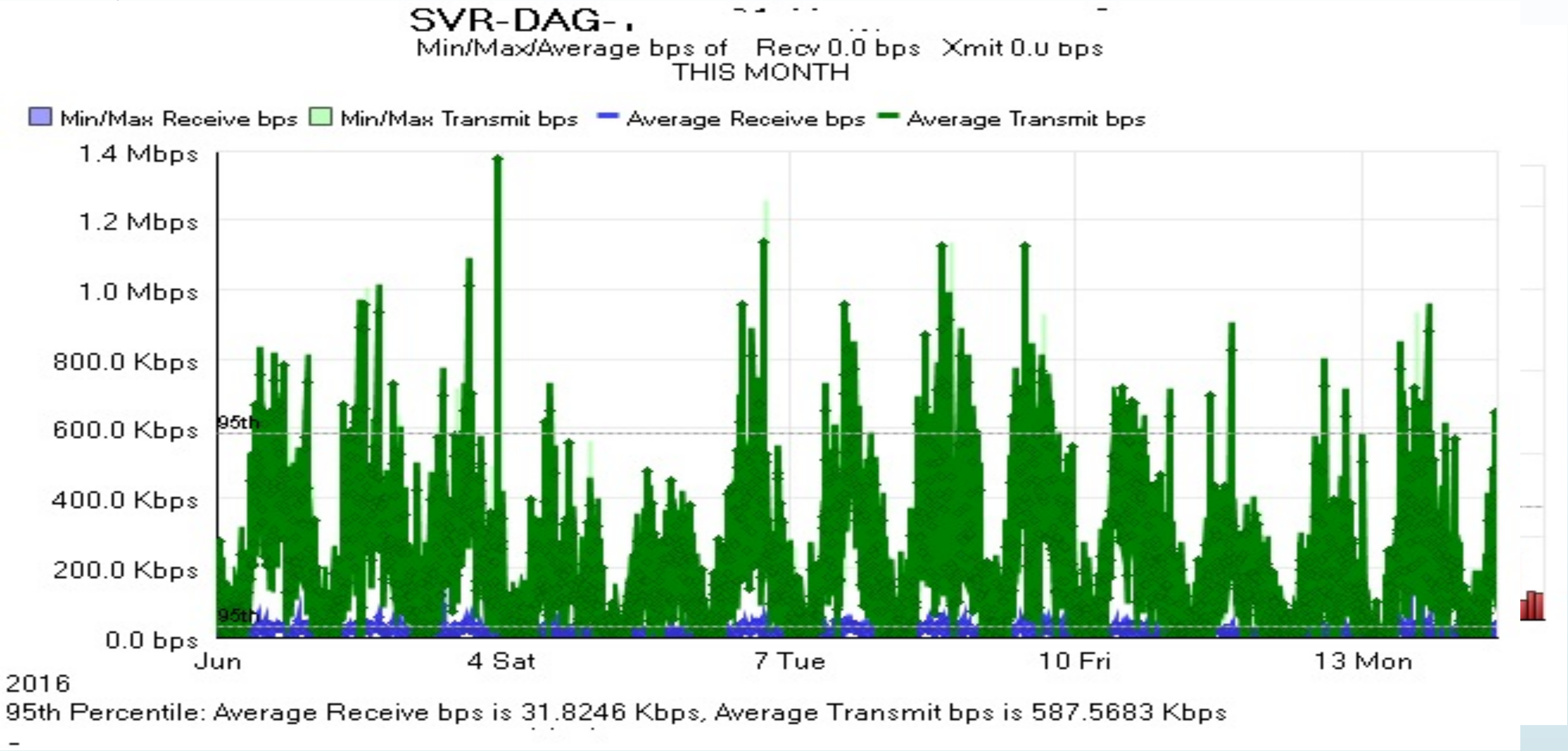
- Greetings Admins of this website. -

Your site has been hacked but don't worry I didn't delete or modify any of your databases.

I don't have a good reason to deface your website.

[redacted]

Traditional Monitoring is useless

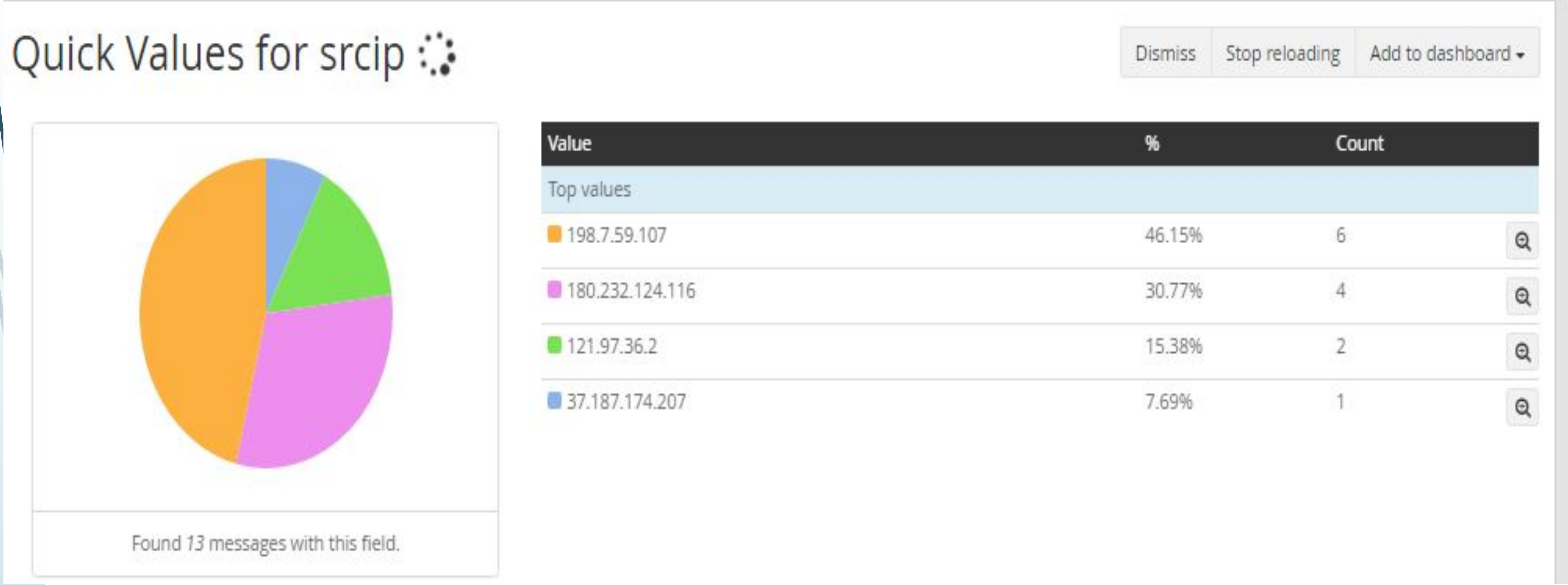


SVR-DAG-.
Min/Max/Average bps of Recv 0.0 bps Xmit 0.u bps
THIS MONTH

95th Percentile: Average Receive bps is 31.8246 Kbps, Average Transmit bps is 587.5683 Kbps

Website: www.bnshosting.net

Big Data Query: POSTs to Victim IP in the last x Days

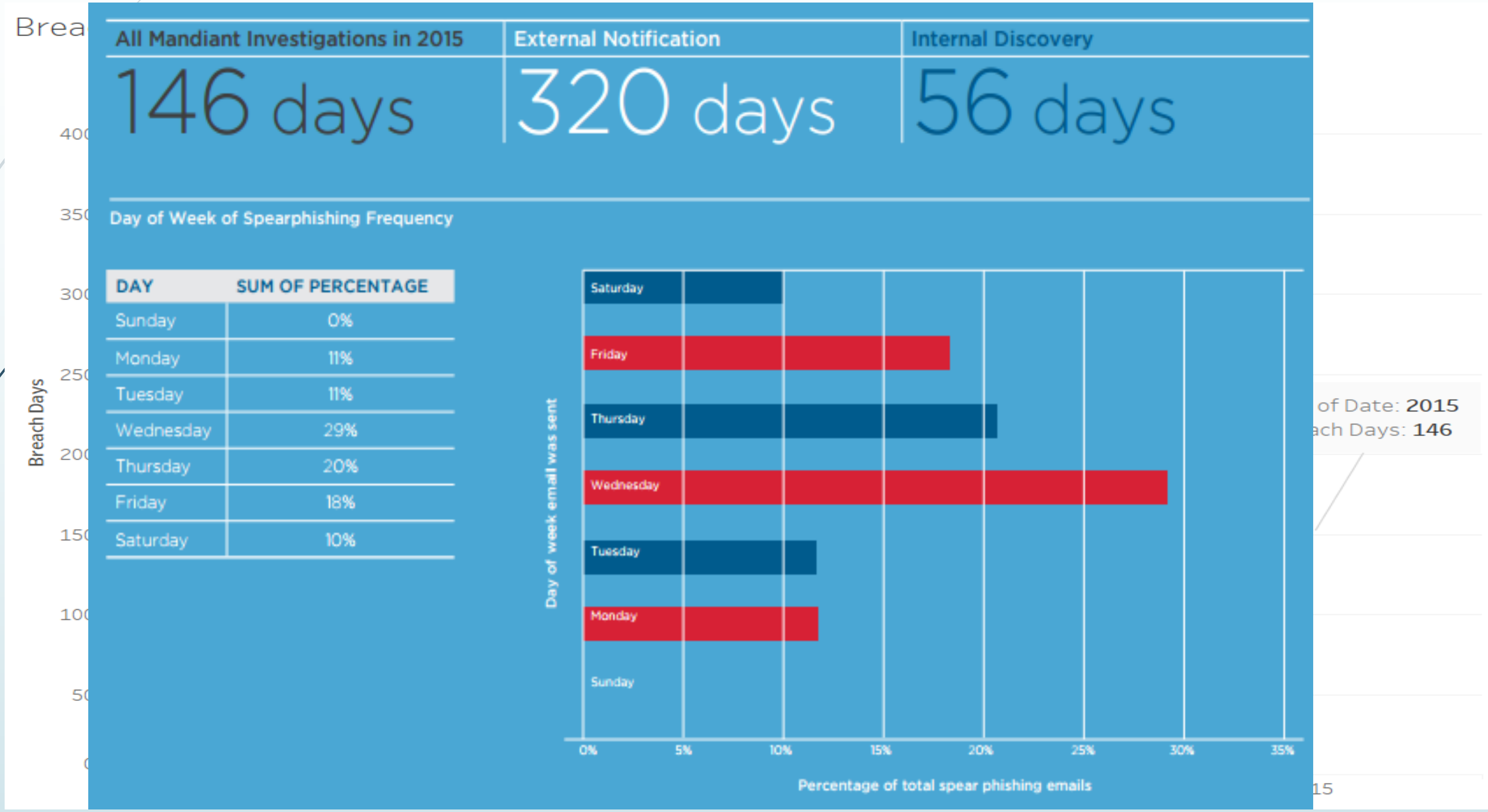


Quick Values for srcip

Value	%	Count
Top values		
🟧 198.7.59.107	46.15%	6
🟪 180.232.124.116	30.77%	4
🟩 121.97.36.2	15.38%	2
🟦 37.187.174.207	7.69%	1

Found 13 messages with this field.

2nd Benefit: Shorten Breach Detection Time

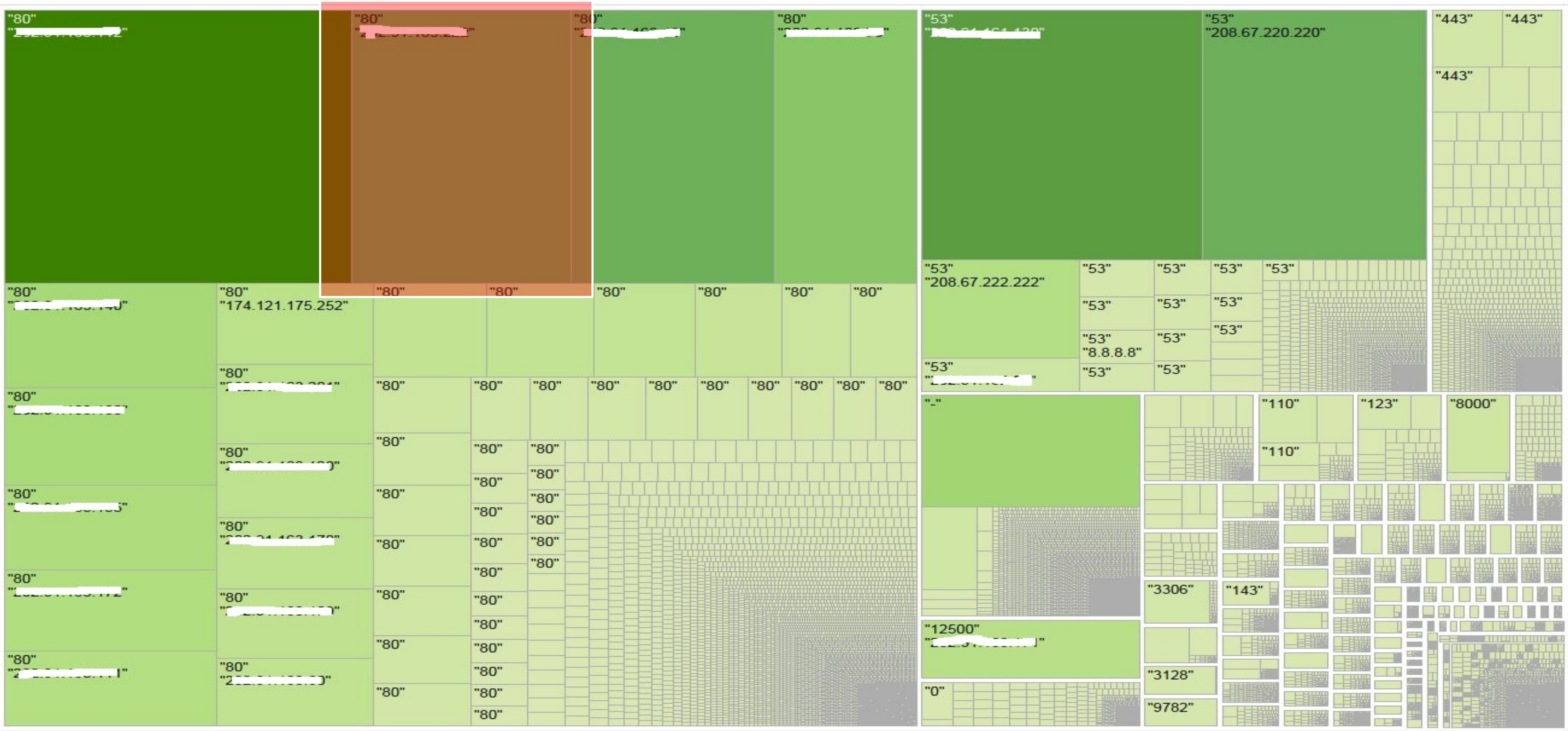


All Mandiant Investigations in 2015	External Notification	Internal Discovery
146 days	320 days	56 days

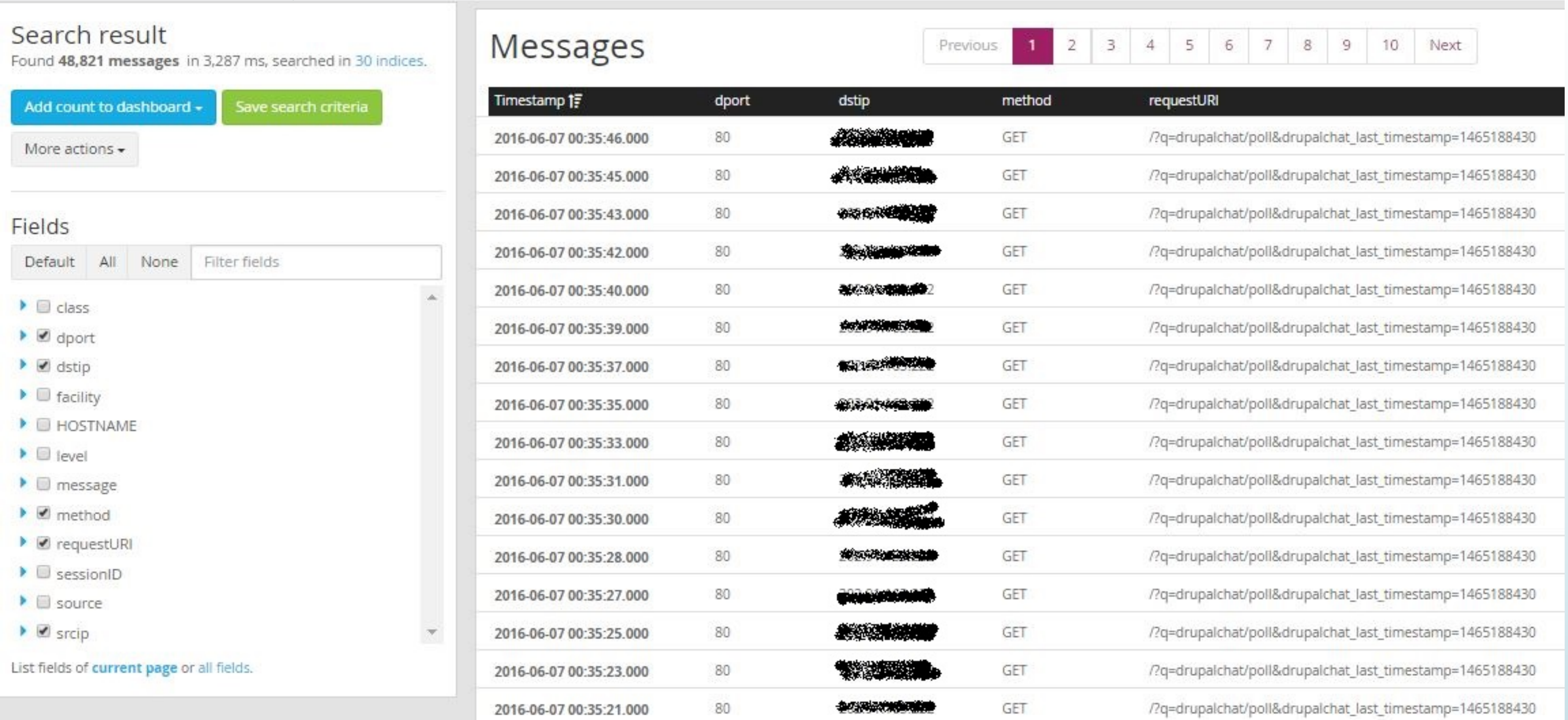
Day of Week of Spearphishing Frequency

DAY	SUM OF PERCENTAGE
Sunday	0%
Monday	11%
Tuesday	11%
Wednesday	29%
Thursday	20%
Friday	18%
Saturday	10%

Case1: Using Volume of Activity



Results show Unauthorized App



Search result

Found **48,821 messages** in 3,287 ms, searched in 30 indices.

Fields

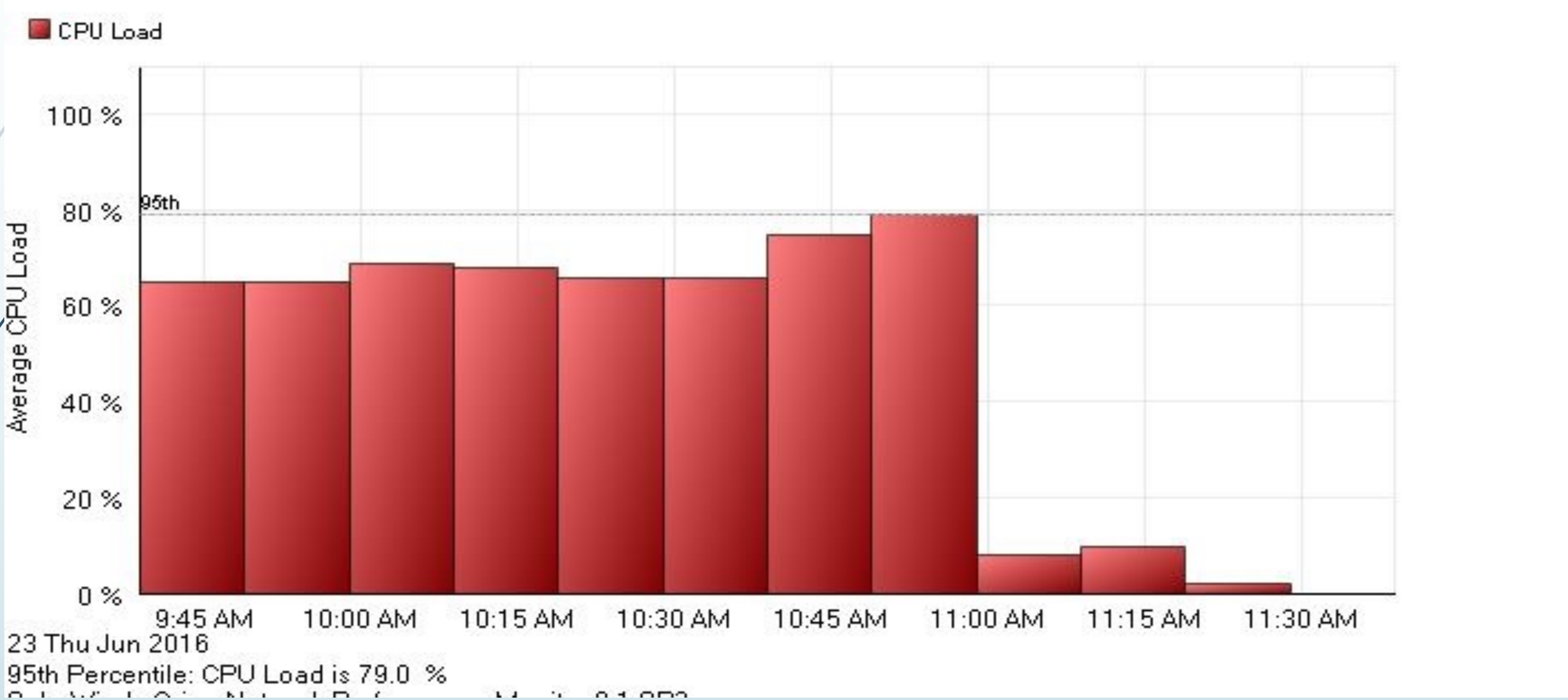
- □ class
- ☑ dport
- ☑ dstip
- □ facility
- □ HOSTNAME
- □ level
- □ message
- ☑ method
- ☑ requestURI
- □ sessionID
- □ source
- ☑ srcip

List fields of **current page** or all fields.

Messages

Timestamp	dport	dstip	method	requestURI
2016-06-07 00:35:46.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:45.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:43.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:42.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:40.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:39.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:37.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:35.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:33.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:31.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:30.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:28.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:27.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:25.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:23.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430
2016-06-07 00:35:21.000	80	[redacted]	GET	/?q=drupalchat/poll&drupalchat_last_timestamp=1465188430

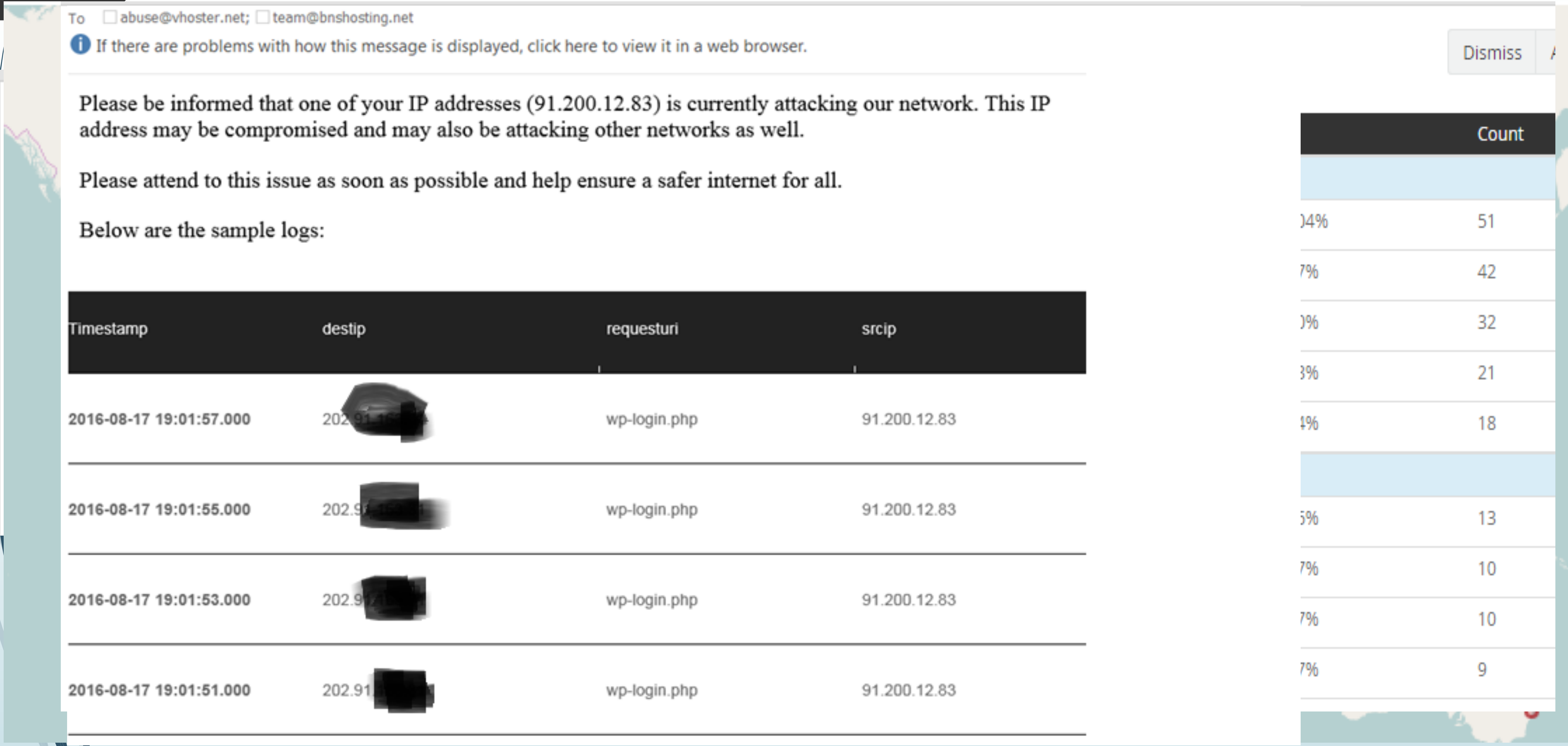
CPU Drops after client disables this.



23 Thu Jun 2016

95th Percentile: CPU Load is 79.0 %

Case 2: Using Fumbling Data



To □ abuse@vhoster.net; □ team@bnshosting.net

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Please be informed that one of your IP addresses (91.200.12.83) is currently attacking our network. This IP address may be compromised and may also be attacking other networks as well.

Please attend to this issue as soon as possible and help ensure a safer internet for all.

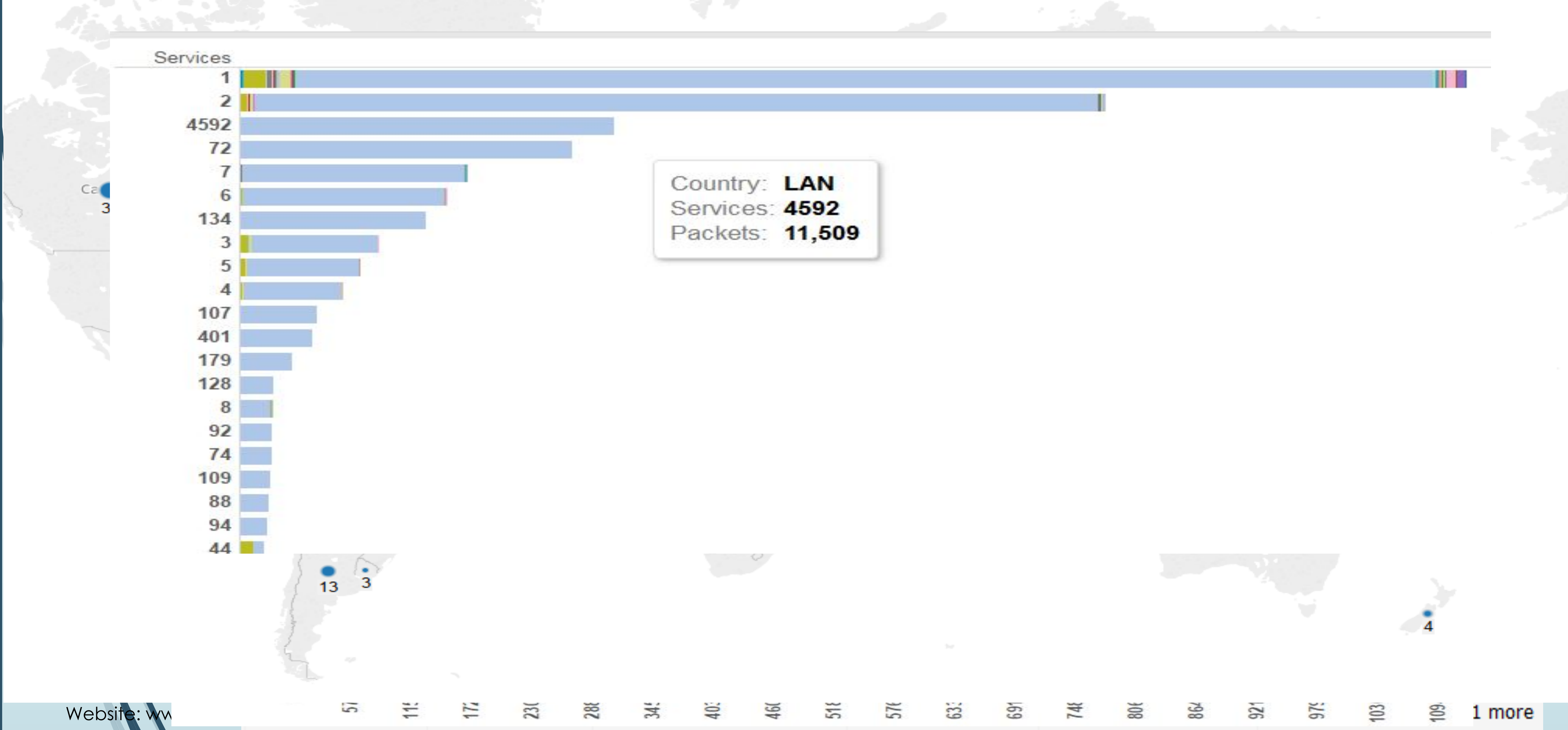
Below are the sample logs:

Timestamp	destip	requesturi	srcip
2016-08-17 19:01:57.000	202[redacted]	wp-login.php	91.200.12.83
2016-08-17 19:01:55.000	202.9[redacted]	wp-login.php	91.200.12.83
2016-08-17 19:01:53.000	202.9[redacted]	wp-login.php	91.200.12.83
2016-08-17 19:01:51.000	202.91[redacted]	wp-login.php	91.200.12.83

	Count
04%	51
7%	42
0%	32
3%	21
4%	18
5%	13
7%	10
7%	10
7%	9

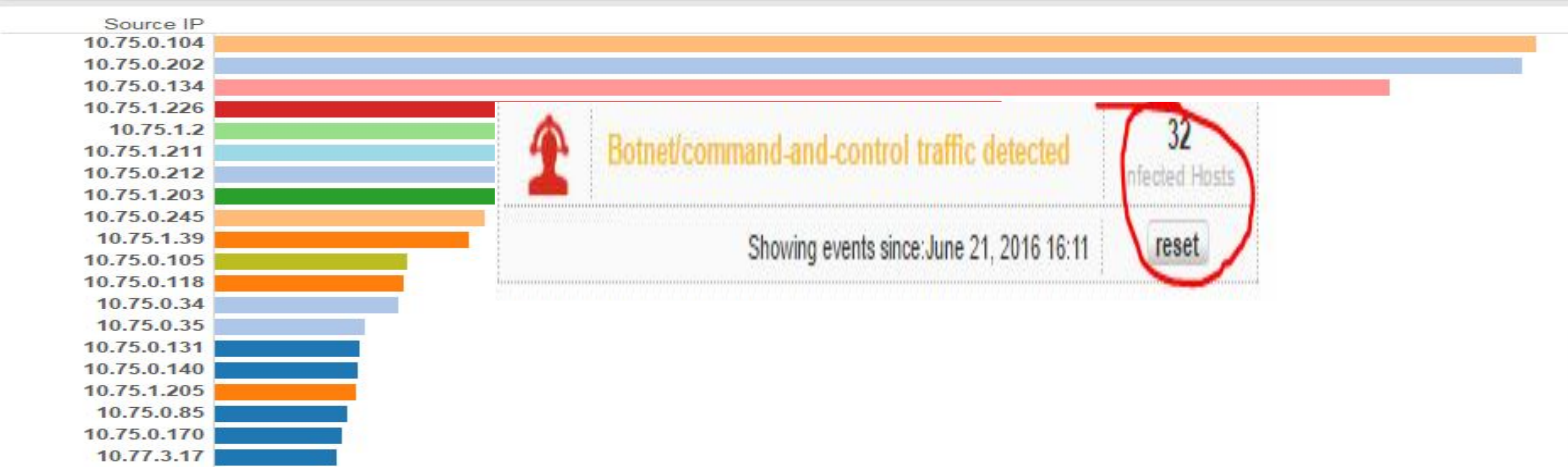
Bitstop Network Services Hosting Solutions

Case 3: Using Packet Size



Country: LAN
Services: 4592
Packets: 11,509

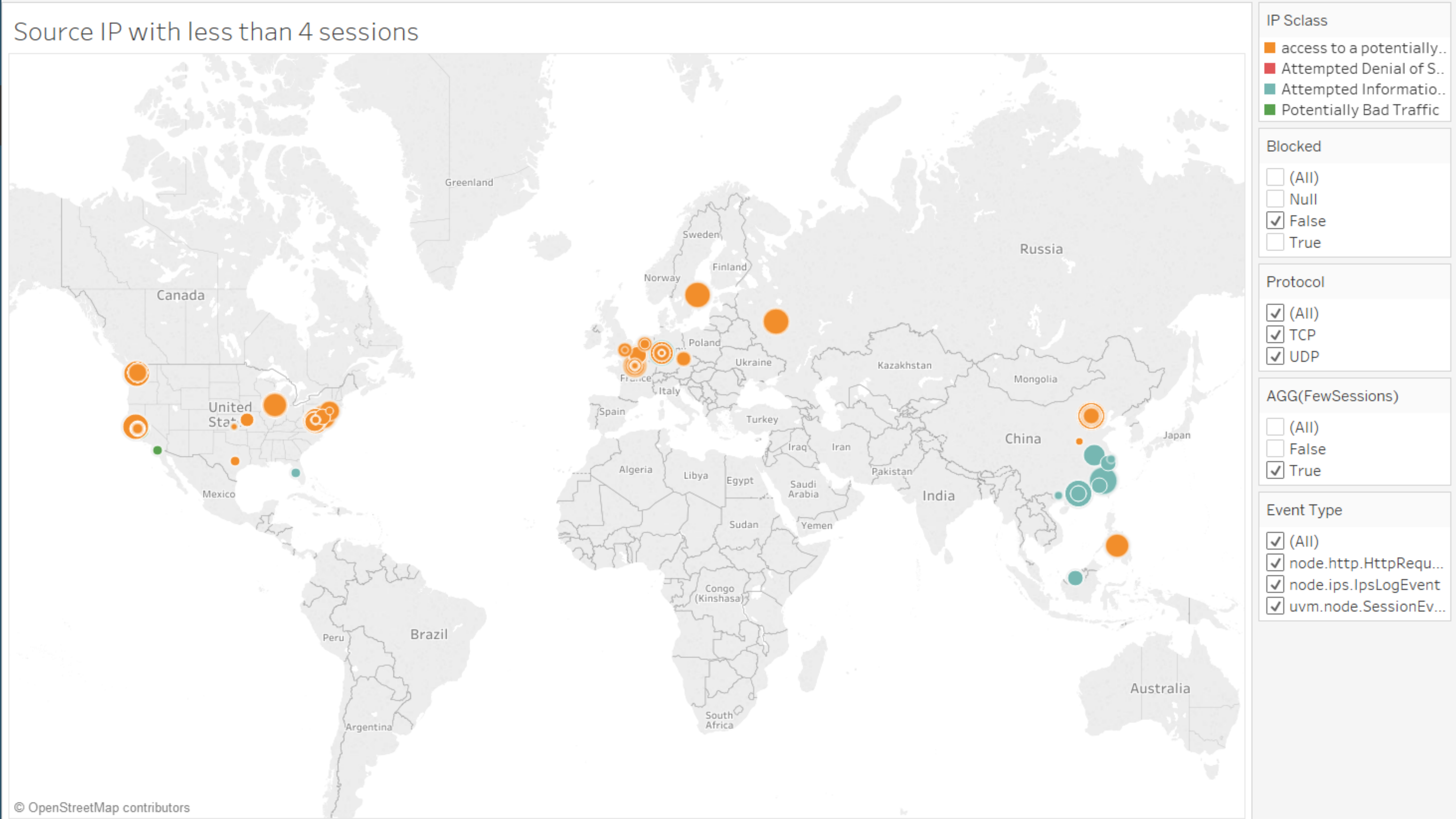
Internal Traffic Distribution by IP



Botnet/command-and-control traffic detected

32 Infected Hosts

Showing events since:June 21, 2016 16:11



Source IP with less than 4 sessions

IP Sclass

🟧 access to a potentially..
🟥 Attempted Denial of S..
🟦 Attempted Informatio..
🟩 Potentially Bad Traffic

Blocked

☐ (All)
☐ Null
☑ False
☐ True

Protocol

☑ (All)
☑ TCP
☑ UDP

AGG(FewSessions)

☐ (All)
☐ False
☑ True

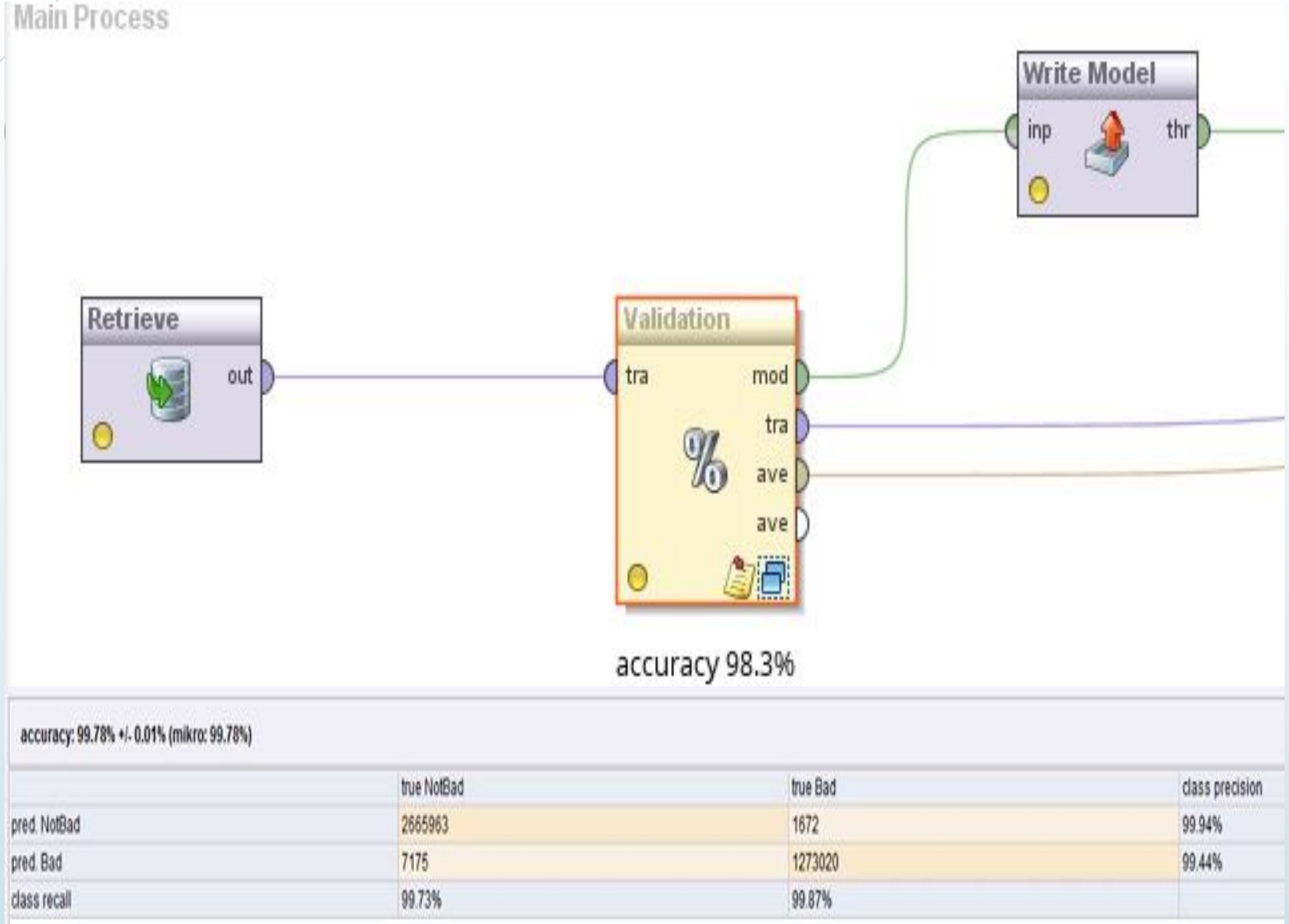
Event Type

☑ (All)
☑ node.http.HttpRequ...
☑ node.ips.IpsLogEvent
☑ uvm.node.SessionEv...

Case 5: Predictive Model Using Naïve Bayes

- Training set of known ‘Bad’ IPs
- Perform Supervised Machine Learning
- Create Model to predict ‘Bad’ IPs
- Put predicted ‘Bad’ IPs in ‘Watch List’ or ‘Hot’ Lists

Predictive Analytics Model Creation

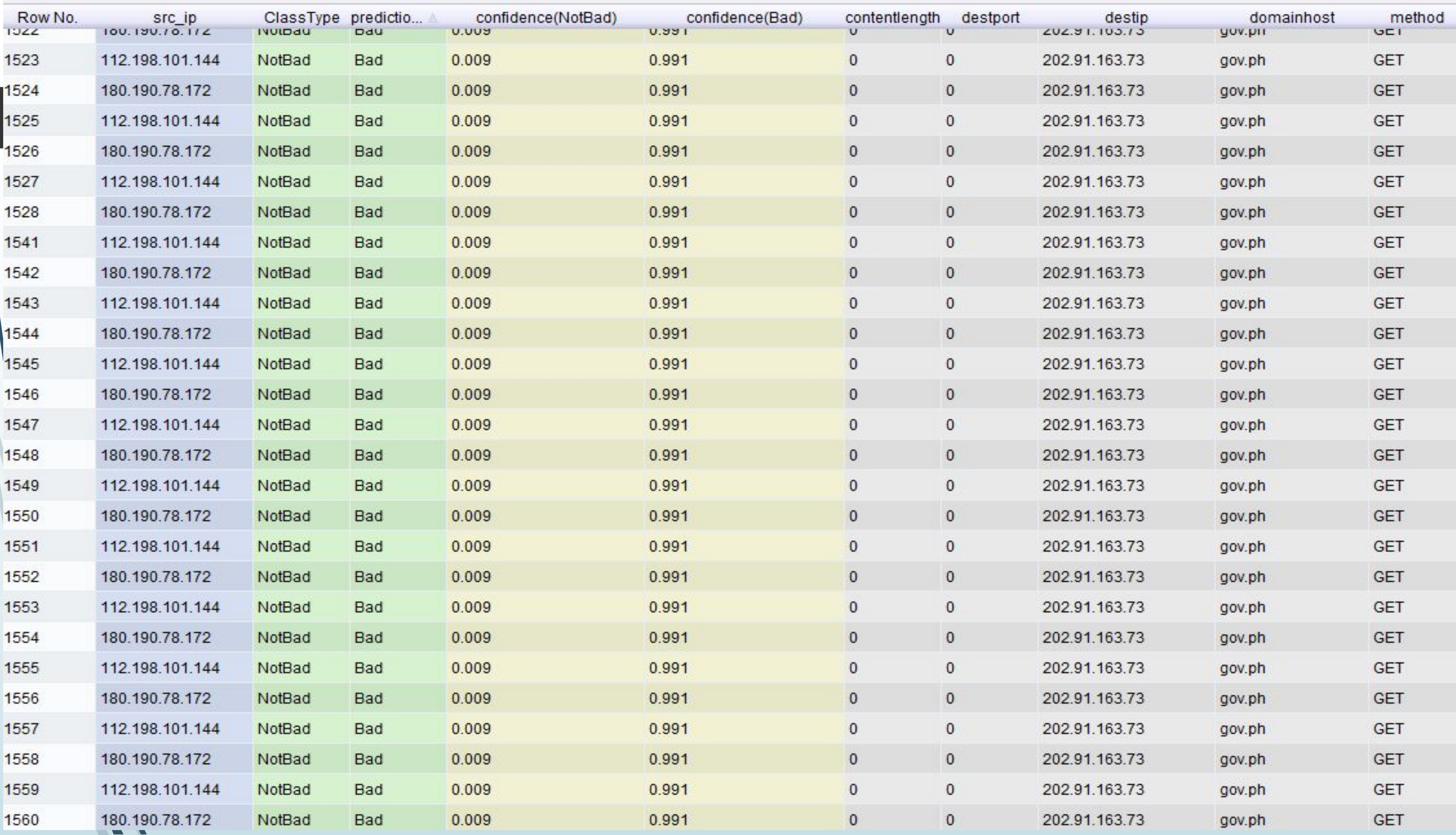


accuracy 98.3%

accuracy: 99.78% +/- 0.01% (mikro: 99.78%)

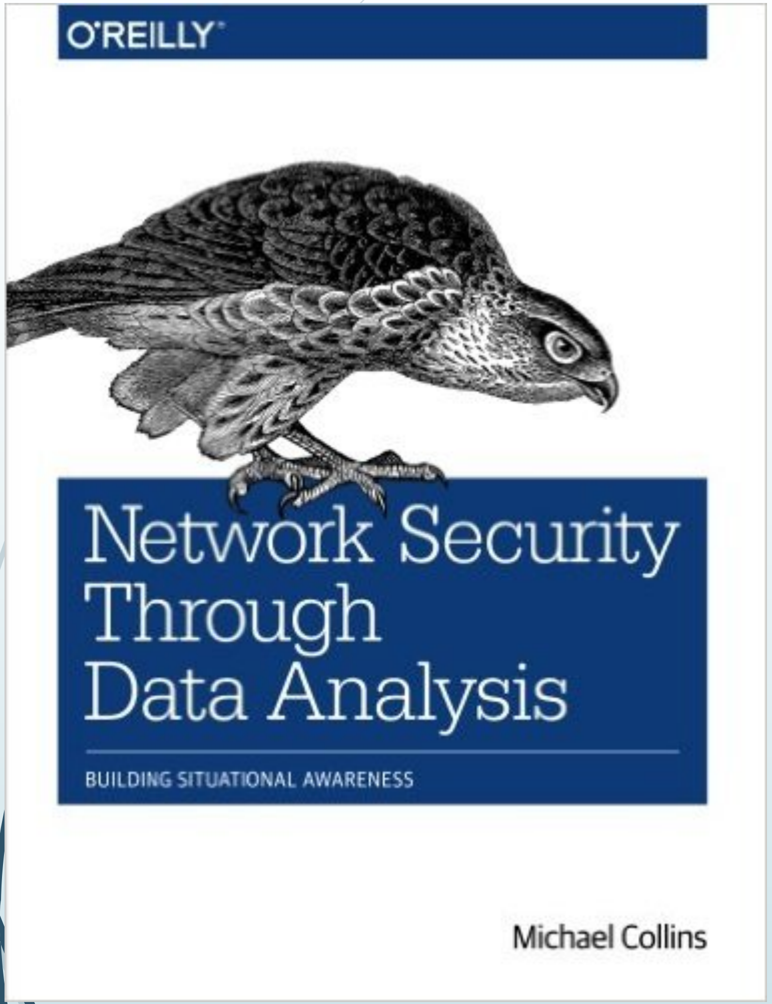
	true NotBad	true Bad	class precision
pred. NotBad	2665963	1672	99.94%
pred. Bad	7175	1273020	99.44%
class recall	99.73%	99.87%	

Website: www.bnshosting.net



Row No.	src_ip	ClassType	predictio...	confidence(NotBad)	confidence(Bad)	contentlength	destport	destip	domainhost	method
1522	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1523	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1524	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1525	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1526	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1527	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1528	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1541	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1542	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1543	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1544	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1545	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1546	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1547	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1548	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1549	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1550	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1551	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1552	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1553	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1554	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1555	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1556	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1557	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1558	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1559	112.198.101.144	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET
1560	180.190.78.172	NotBad	Bad	0.009	0.991	0	0	202.91.163.73	gov.ph	GET

Tools & Resources



O'REILLY

Network Security Through Data Analysis

BUILDING SITUATIONAL AWARENESS

Michael Collins

graylog

splunk>

Qlik

elastic

hadoop

neo4j

Gephi

KNIME

rapidminer

tableau

Additional Links:

- http://tabsoft.co/2bKiXpo
- www.bnshosting.net
- https://www.facebook.com/bnshosting/
- https://www.facebook.com/groups/PHInternet/
- https://www.facebook.com/groups/108560036239757/