SecurityPi

Hardening your IoT endpoints in Home

@rabimba | Mozilla Tech Speaker | RICE University

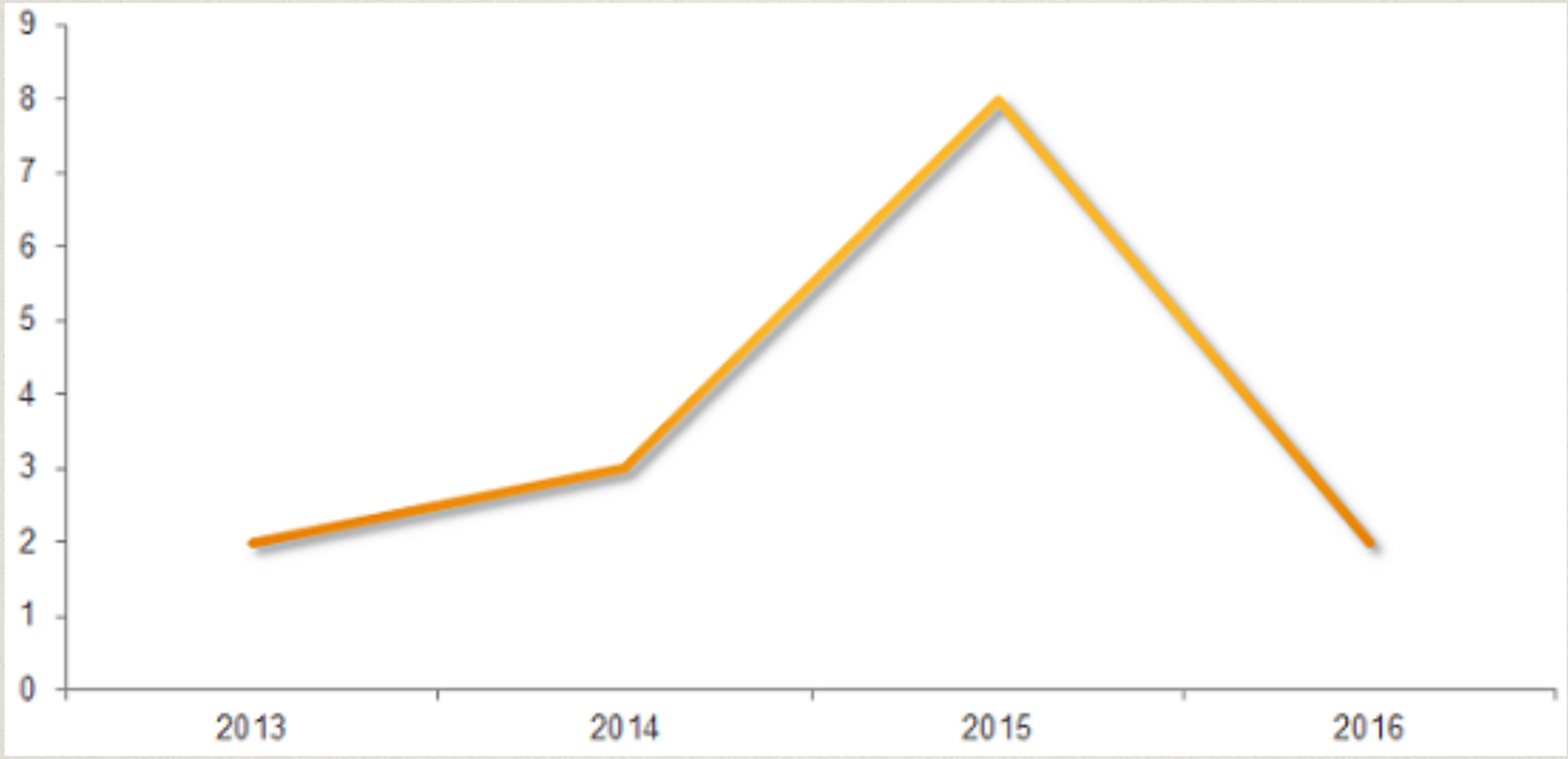
LinuxCon China 2017

Why

How

Protect the Legacy

Wait. Do we need protection?

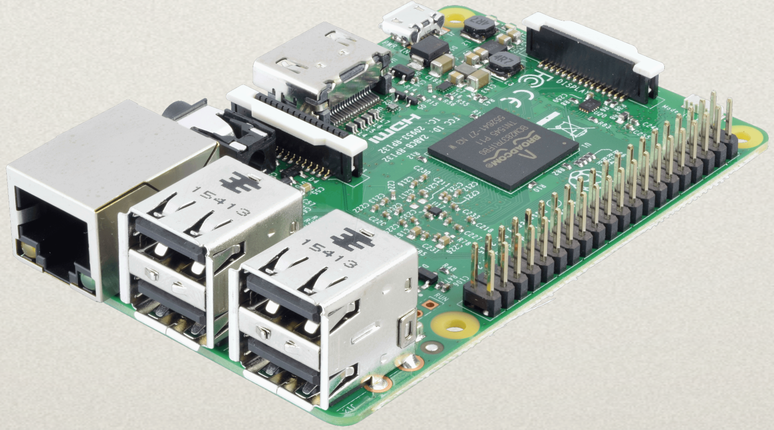


New IoT malware families by year.
The number IoT threats jumped in 2015 and many of these threats continue to be active into 2016

Source: https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

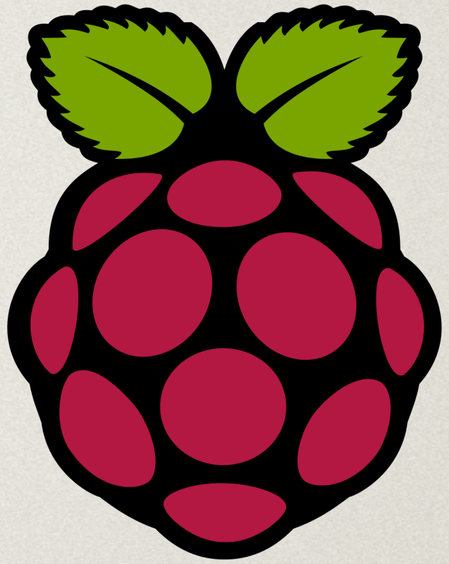
Tools for the trade

- Raspberry Pi 3 with case
- MicroSD Card
- Power Adaptor for pi (Important!)



Install Image

- Raspbian (Debian Wheezy)
- NOOBS



But what about my network?

Configure Network : Part 1

Gateway!

- Pro:
  - No additional hardware needed
  - Simple setup
- Con
  - Attackers can bypass device by connecting directly to actual gateway/router
  - Performance implications

Configure Network : Part 2

Mirror Port!

- Pro:
  - No additional hardware needed
  - All traffic will be monitored
  - Raspberry Pi isn't inline
- Con:
  - Home/SMB network equipment may not support Span/Mirror ports

Configure Network : Part 3

Grad Student Way (In-Line)

- Pro:
  - All traffic will be monitored
- Con:
  - Raspberry Pi is in-line with all network traffic
  - Performance implications

Getting BRO Onboard

Install Required Dependencies

- `$ sudo apt-get install cmake make gcc g++ flex bison libpcap-dev swig zlib1g-dev`

Download Bro Source Code

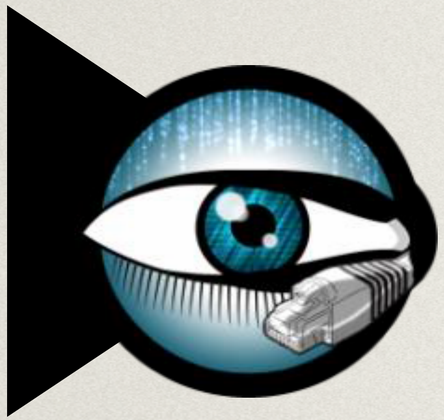
- `$ wget` https://www.bro.org/downloads/release/bro-2.4.tar.gz

Unpack

```
$ sudo ./configure —prefix=/opt/nsm/bro
$ sudo make
$ sudo make install
```

```
26  #Install Bro
27  echo "Installing Bro"
28  sudo wget https://www.bro.org/downloads/release/bro-2.4.1.tar.gz
29  sudo tar -xzf bro-2.4.1.tar.gz
30  sudo mkdir /opt/nsm
31  sudo mkdir /opt/nsm/bro
32  cd bro-2.4.1
33  sudo ./configure --prefix=/opt/nsm/bro
34  sudo make
35  sudo make install
36  cd ..
37  sudo rm bro-2.4.1.tar.gz
38  sudo rm -rf bro-2.4.1/
```

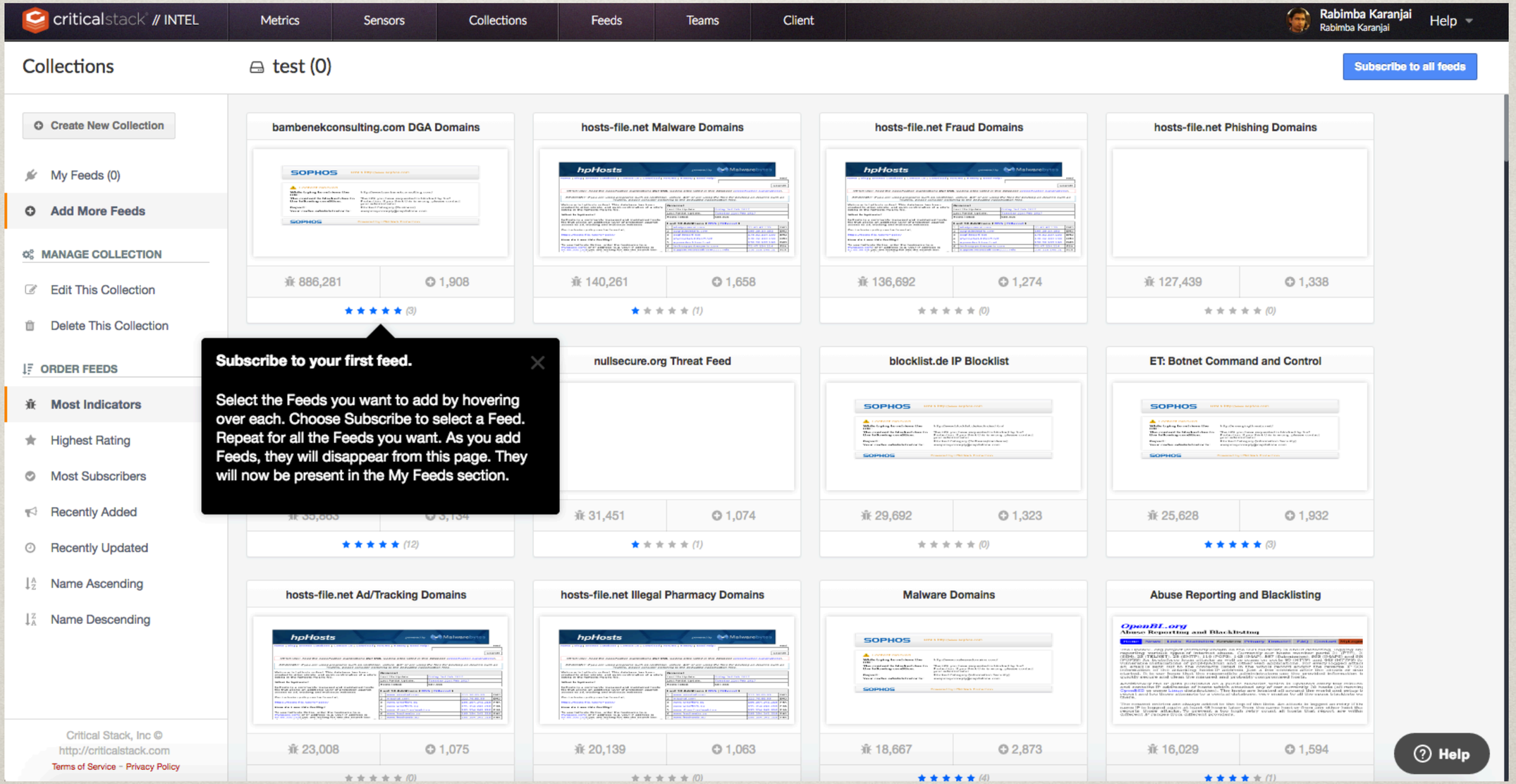
BRO Intrusion Detection System



conn.log
dhcp.log
dnp3.log
dns.log
ftp.log
http.log
irc.log
known_services.log
modbus.log
ius.log
smtp.log
snmp.log
ssh.log
ssl.log
syslog.log tunnel.log
intel.log notice.log

Make BRO Great Again

Integrate Critical Stack



Integrate Critical Stack

$ wget https://intel.criticalstack.com/client/critical-stack-intel-arm.deb
sudo dpkg -i critical-stack-intel-arm.deb

Add the API Key

- $ sudo -u critical-stack critical-stack-intel api <key>

```
41  #Install Critical Stack
42  echo "Installing Critical Stack Agent"
43  sudo wget https://intel.criticalstack.com/client/critical-stack-intel-arm.deb
44  sudo dpkg -i critical-stack-intel-arm.deb
45  sudo -u critical-stack critical-stack-intel api $cs_api
46  sudo rm critical-stack-intel-arm.deb
```

What about my logs?

Stash The Logs

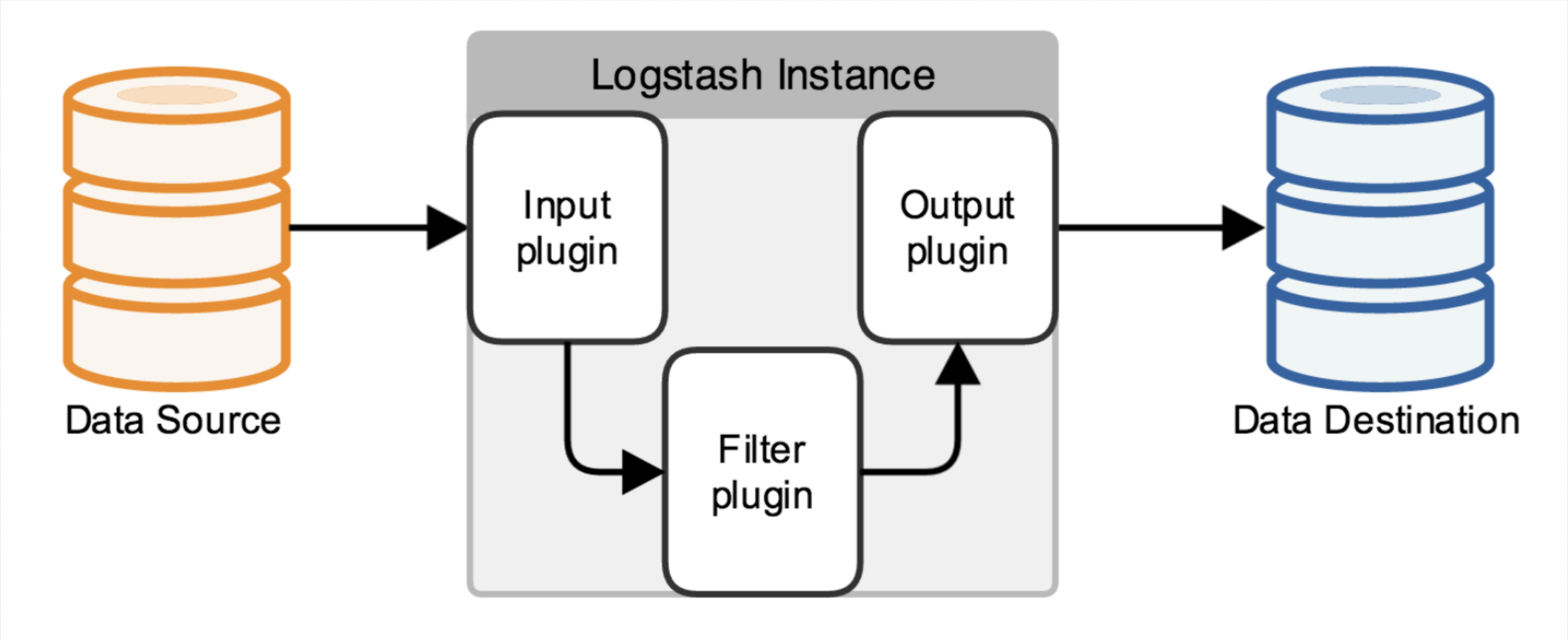
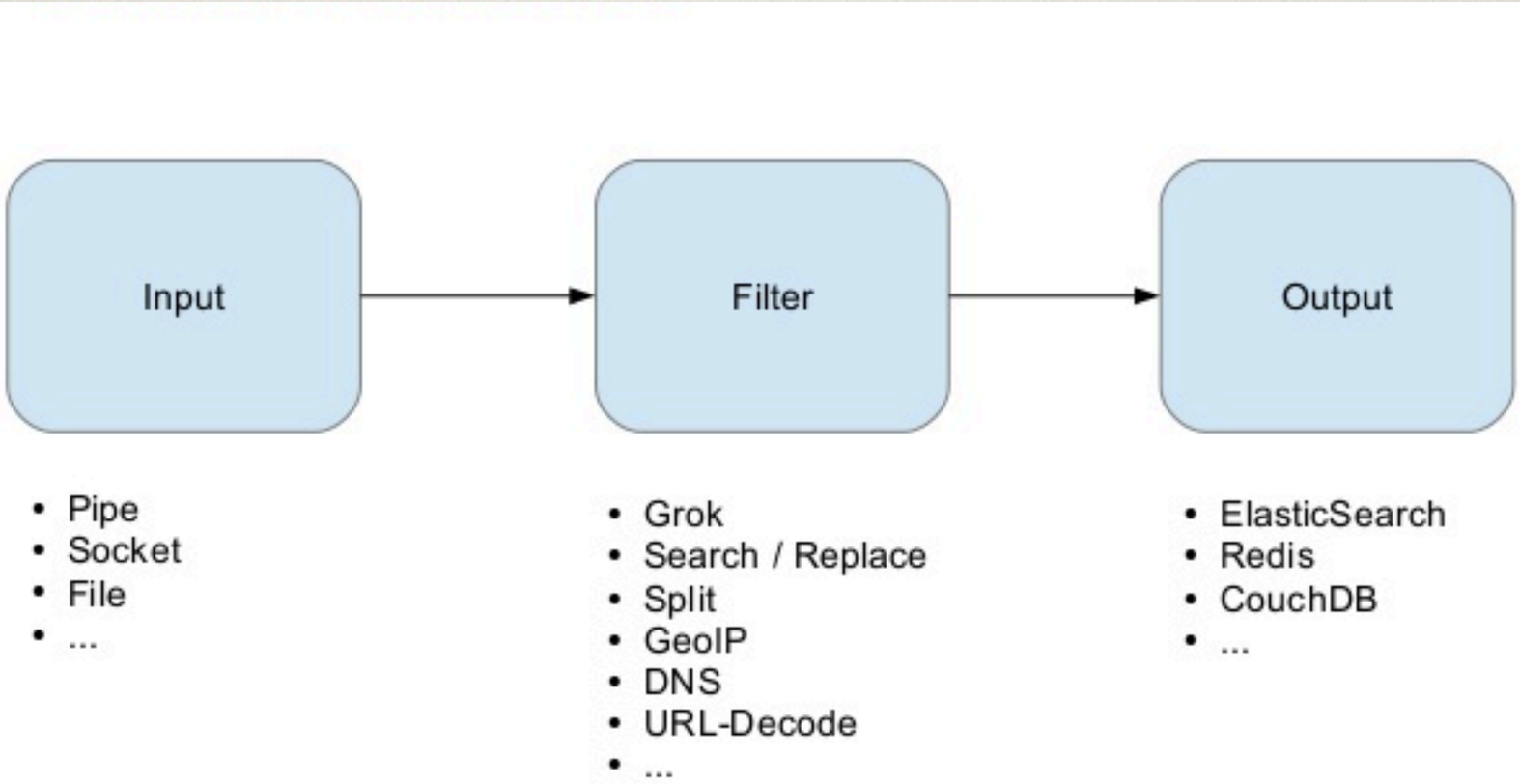


Image courtesy : http://lek-research.readthedocs.io/en/latest/LEK%20Installation.html

In Short: Logstash



What we will do!

Overview

- Utilizing Custom Patterns
- GROK Message Filtering
- Adding Custom Fields
- Adding Geo IP Data
- Date Match
- Using Translations for Threat Intel

Get LogStash

```
$ wget https://download.elastic.co/logstash/logstash/logstash-1.5.3.tar.gz

$ sudo mv /opt/logstash-1.5.3/ /opt/logstash
$ cd /opt/logstash
$ bin/logstash -e 'input { stdin { } } output { stdout { } }'
```

How do I see the logs?

elastic

Install

```
$ wget
```

https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.1.deb

```
$ sudo dpkg -i elasticsearch-1.7.1.deb
```

*Update cluster name in yml file

I wanted to “See”!

Install

```
$ wget    https://download.elastic.co/kibana/kibana/kibana-4.1.0-linux-x86.tar.gz

$ sudo mkdir /opt/kibana
$ cd /opt/kibana
$ bin/kibana
```

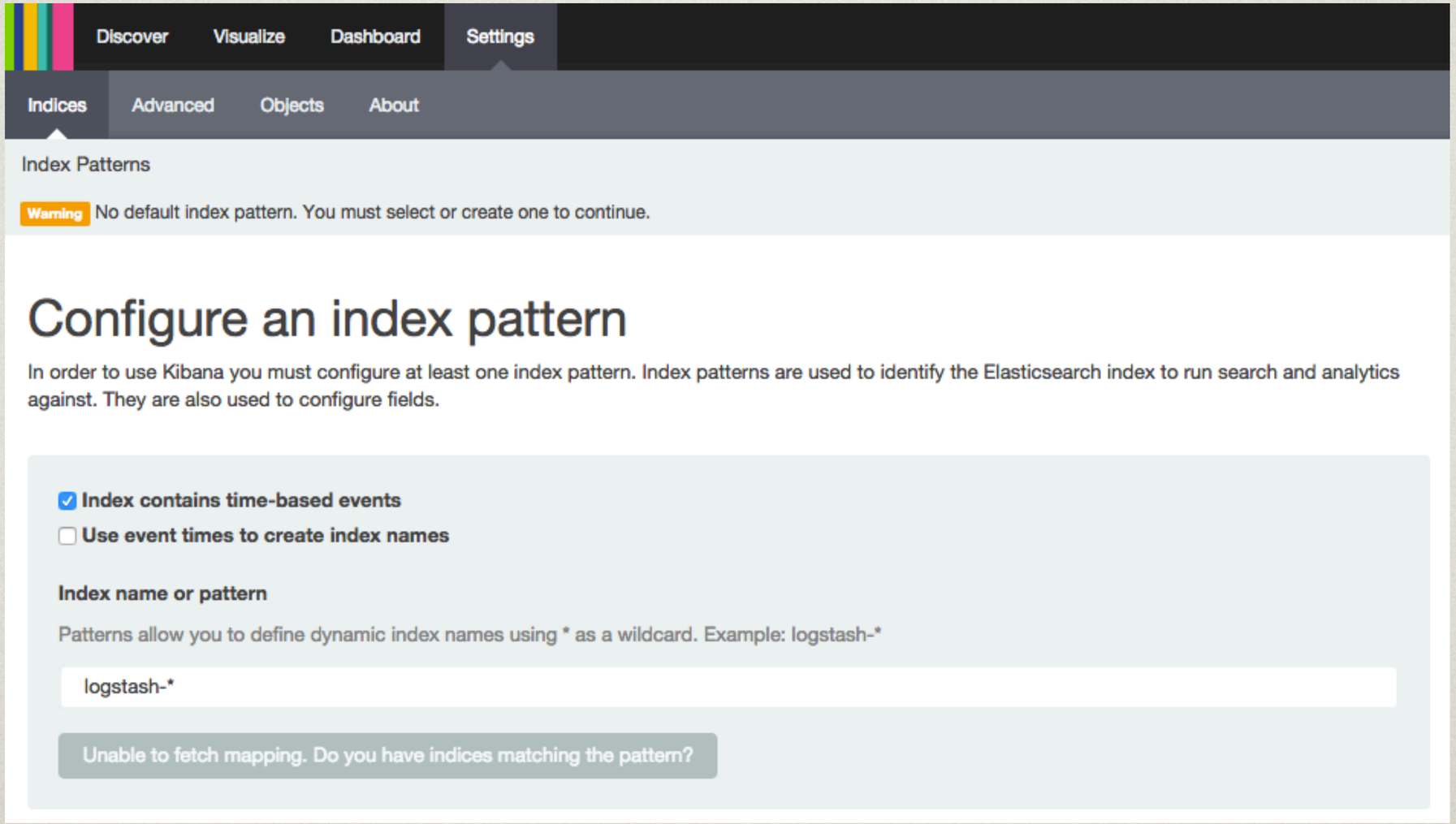
Another error?? Your node needs another ARM!

I wanted to “See”!

Custom ARM Install

```
$ wget http://node-arm.herokuapp.com/node_latest_armhf.deb
$ sudo dpkg -i node_latest_armhf.deb
$ sudo mv /opt/kibana/node/bin/node /opt/kibana/node/bin/node.orig
$ sudo mv /opt/kibana/node/bin/npm /opt/kibana/node/bin/npm.orig
$ sudo ln -s /usr/local/bin/node /opt/kibana/node/bin/node
$ sudo ln -s /usr/local/bin/npm /opt/kibana/node/bin/npm
$ /opt/kibana/bin/kibana
```

kibana


Discover
Visualize
Dashboard
Settings
Indices
Advanced
Objects
About
Index Patterns
Warning
No default index pattern. You must select or create one to continue.
Configure an index pattern
In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.
Index contains time-based events
Use event times to create index names
Index name or pattern
Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*
logstash-*
Unable to fetch mapping. Do you have indices matching the pattern?

Configuration

```
input {
 file {
 path =>                "/opt/bro/logs/current/*.lo
                                                  gs"
        start_position  "beginning
                   =>                  "
           }
           }
       output {
   elasticsearch {
 host =>   localhost

          cluster         "elasticsearch-
             =>            clustername "
 }
}
```

Configuration

```
filter {
grok {
match =>  {
"message" => "%{IP :client}%{WORD :method }
                {URIPATHPARAM: request}%{NUMBER :bytes}%{NUMBER:duration }"
                                                                    }
                                                                    }
                                                                    }
```

Sample for Apache Access log

Configuration

```
filter {
      grok {
                  patterns_dir => "/opt/logstash/custom_patterns"
                                match => {
                              message => "%{291009}"
                                }


      }
}
```

- Configuration
- Create a Rule File
- /opt/logstash/custom_patte rns/bro.rule

- 291009
(?<start_time>\d+\.\d{6})\s+(?<uid>\S+)\s+(?:(?<evt_srcip>[\d\.]+)|(?<evt_srcipv6>[\w:]+)|-
)\s+(?:(?<evt_srcport>\d+)|-)\s+(?:(?<evt_dstip>[\d\.]+)|(?<evt_dstipv6>[\w:]+)|-
)\s+(?:(?<evt_dstport>\d+)|-
)\s+(?<fuid>\S+)\s+(?<file_mime_type>\S+)\s+(?<file_description>\S+)\s+(?<seen_in
dicator>\S+)\s+(?<seen_indicator_type>[A:]+::\S+)\s+(?<seen_where>[
A:]+::\S+)\s+(?<source>\S+(?:\s\S+)*)$

Configuration

```
filter {
        if [message] =~ /^((\d{10}\.\d{6})\t([\d\.]+)([\d\.]+)\t(\d+)\t(\d+)\t(\w+))/ {
                grok {
                        patterns_dir => "/opt/logstash/custom_patterns"
                        match => {
                                message => "%{291001}“
                        }
                }
        }
}
```

291001 (?<start_time>\d{10}\.\d{6})\t(?<evt_srcip>[\d\.]+)\t(?<evt_dstip>[\d\.]+)\t(?<evt_srcport>\d+)\t…

Configuration

```
filter {
    if [message] =~ /A(\d+\.\d{6}\s+\S+\s+(?:[\d\.]+|[\w:]+|-)\s+(?:\d+|-)\s+(?:[\d\.]+|[\w:]+|
•           )\s+(?:\d+|-)\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+[A:]+::\S+\s+[A:]+::\S+\s+\S+(?:\s\S+)*$)/ {
        grok{
            patterns_dir => "/opt/logstash/custom_patterns"
            match => {
                message => "%{291009}"
            }
                add_field => [ "rule_id", "291009" ]
                add_field => [ "Device Type", "IPSIDSDevice" ]
                add_field => [ "Object", "Process" ]
                add_field => [ "Action", "General" ]
                add_field => [ "Status", "Informational" ]
            }
        }
    }
```

```
filter {
  …..all normalization code above here….
  geoip {
   source => "evt_dstip"
   target => "geoip_dst"
   database => “/opt/logstash/GeoLiteCity.dat“
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][longitude]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][latitude]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][city\_name]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][continent\_code]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][country\_name]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][postal\_code]}“
  }
  mutate {
    convert => [ "[geoip_dst][coordinates]", "float"]
  }
}
```

New ElasticSearch Template Needed

- Configuration
- filter {
- ...bro normalization stuff... translate {
- field => "evt_dstip"
- destination => "badIP" dictionary_path => '/opt/logstash/IP.yaml '
- }
- }
- But what goes in IP.yaml?

Configuration

- Dictionary Hash in standard YAML format

"1.2 .3 .4": Bad IP
"ab c123": Very Bad IP

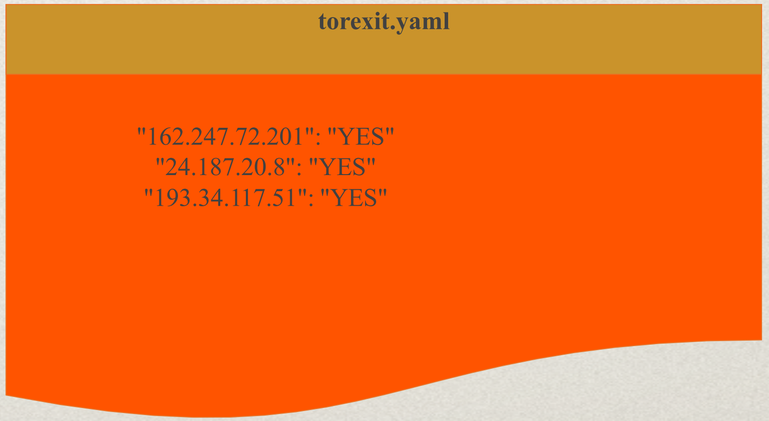
- Install the translate plugin

```
$ cd /opt/logstash
$ bin/plugin install logstash-filter-translate
```

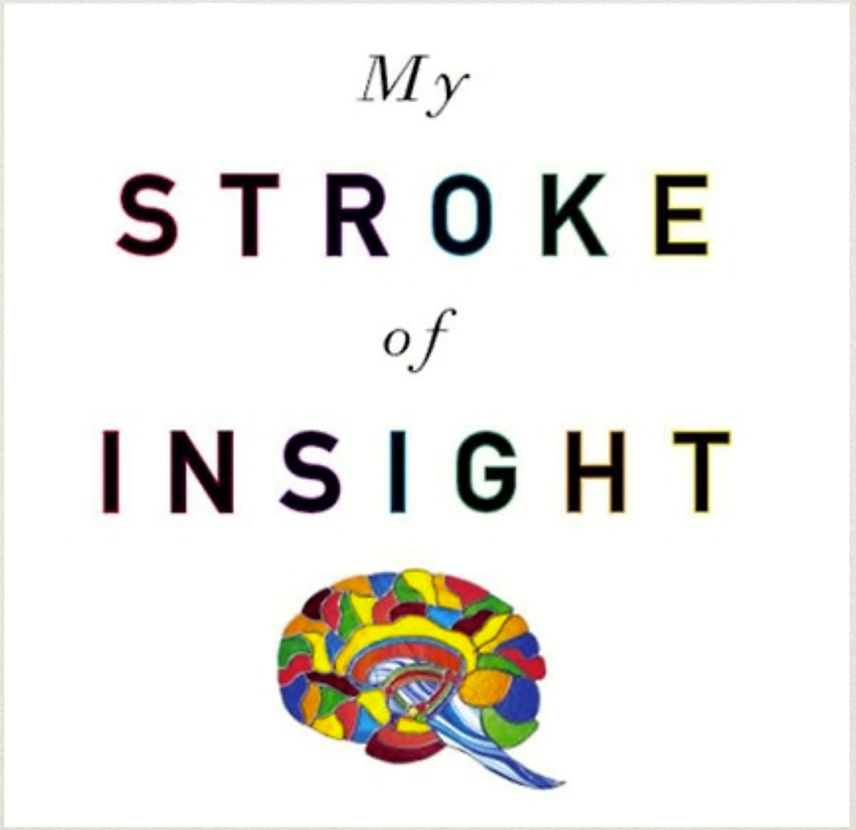
Configuration

- TOR Exit IP: https://check.torproject.org/exit-addresses
- Malicious IP: http://www.malwaredomainlist.com/hostslist/ip.txt

- Automate the scraping of available intel
- Populate the YAML Files



What do I know?



Configuration

```
if     "YES" in [tor_IP] {

email  {
options => [ "smtpiporHost", "SMTP_HOST",
from => ""port","SMTP-PORT",
"userName ","EMAIL-USER",
"password","EMAIL-PASS","authenticationType",
"plain",
"starttls","true"]
<EMAIL USER>"
subject => "Tor Exit IP Detected on Home
Network" to => "<EMAIL USER>"
via => "smtp"
htmlbody => htmlBody }}
```

There is a TOR device in my network!

Alerts

- TOR IP Addresses
- Malicious IP Addresses
- Malicious File Hashes
- Bro IDS intel.log results
- Bro IDS notice.log results
- Connections to differet countries
- Device Specific Connection seggregation

kibana

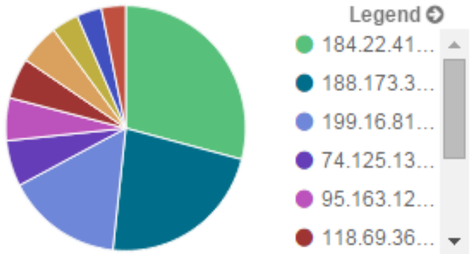
Discover | Visualize | Dashboard | Settings | Last 5 years

Logstash - Bro Base

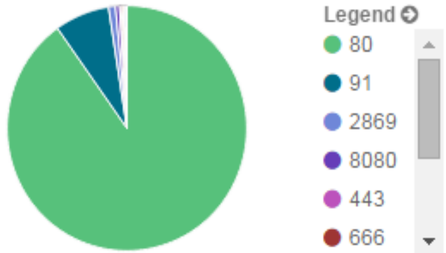
*

Date Chart of Log Sources

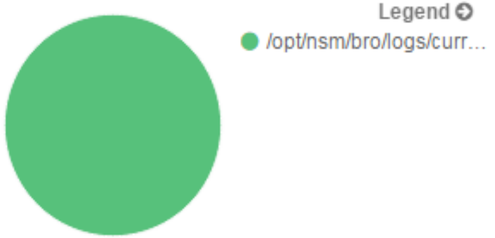
Top Destination IP



Top 10 Destination Ports



Top Log Sources

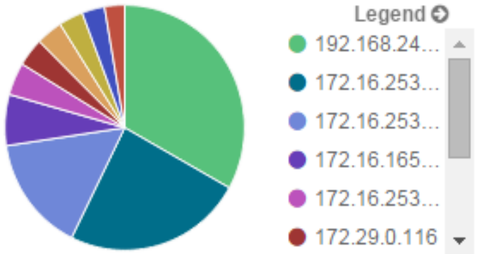


Log Count

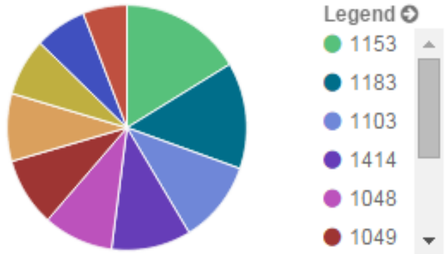
7,604

Count

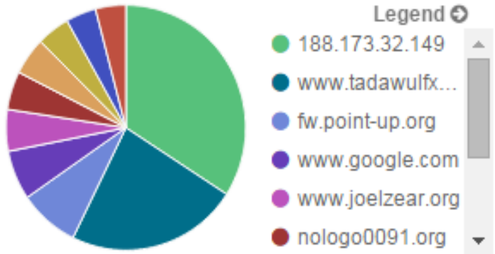
Top Source IP



Top 10 Source Ports

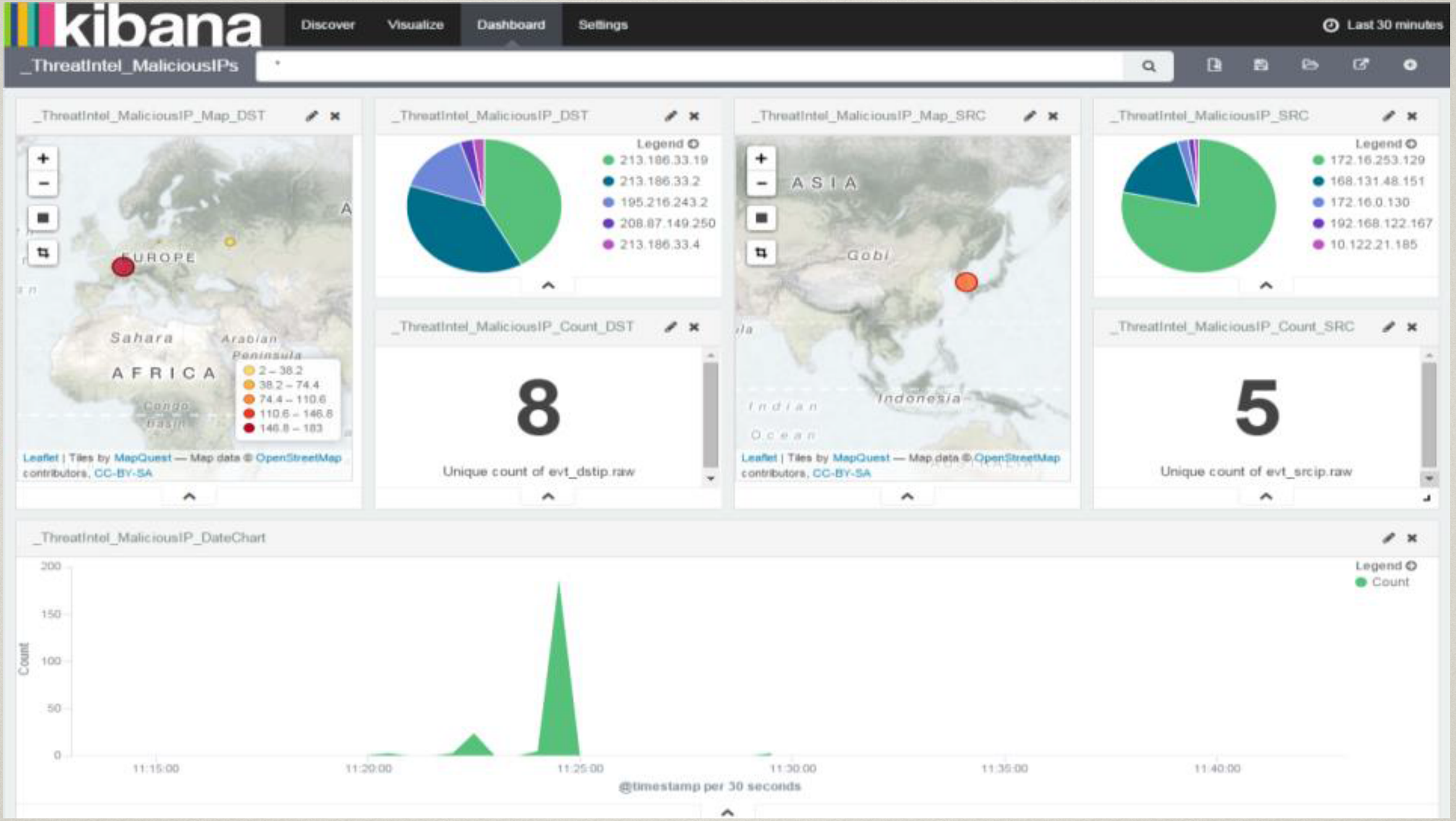


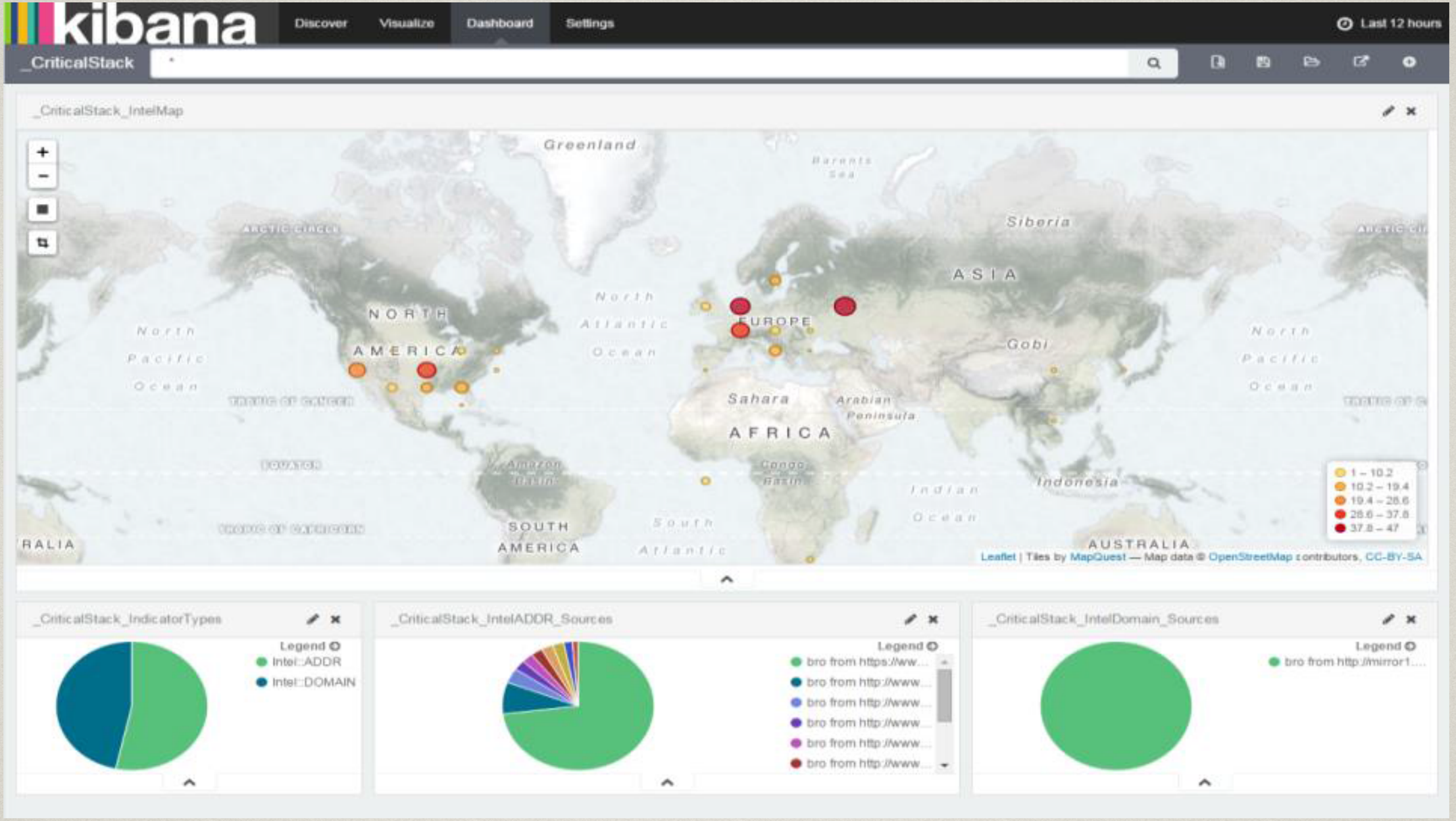
Top 10 Web Sites



Monthly Log Count

@timestamp per month	Count
December 31st 2010, 23:00:00.000	10
July 1st 2011, 00:00:00.000	99
August 1st 2011, 00:00:00.000	8


kibana
Discover
Visualize
Dashboard
Settings
Last 30 minutes
_ThreatIntel_MaliciousIPs
*
_ThreatIntel_MaliciousIP_Map_DST
EUROPE
Sahara
AFRICA
Arabian Peninsula
Congo basin
2 – 38.2
38.2 – 74.4
74.4 – 110.6
110.6 – 146.8
146.8 – 183
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_DST
Legend
213.186.33.19
213.186.33.2
195.216.243.2
208.87.149.250
213.186.33.4
_ThreatIntel_MaliciousIP_Count_DST
8
Unique count of evt_dstip.raw
_ThreatIntel_MaliciousIP_Map_SRC
ASIA
Gobi
Indian Ocean
Indonesia
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_SRC
Legend
172.16.253.129
168.131.48.151
172.16.0.130
192.168.122.167
10.122.21.185
_ThreatIntel_MaliciousIP_Count_SRC
5
Unique count of evt_srcip.raw
_ThreatIntel_MaliciousIP_DateChart
Legend
Count
200
150
100
50
0
Count
11:15:00
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
@timestamp per 30 seconds


kibana
Discover
Visualize
Dashboard
Settings
Last 12 hours
_CriticalStack
_CriticalStack_IntelMap
Greenland
Barents Sea
Siberia
ASIA
NORTH AMERICA
EUROPE
North Atlantic Ocean
North Pacific Ocean
Gobi
Sahara
Arabian Peninsula
AFRICA
Indian Ocean
Indonesia
SOUTH AMERICA
AUSTRALIA
1 – 10.2
10.2 – 19.4
19.4 – 28.6
28.6 – 37.8
37.8 – 47
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_CriticalStack_IndicatorTypes
Legend
Intel::ADDR
Intel::DOMAIN
_CriticalStack_IntelADDR_Sources
Legend
bro from https://ww...
bro from http://www...
bro from http://www...
bro from http://www...
bro from http://www...
bro from http://www...
_CriticalStack_IntelDomain_Sources
Legend
bro from http://mirror1....

What about proactivity?

NMAP

- Scheduled nmap scan of subnet
- `sudo nmap -sn 192.168.0.1/255.255.255.0 -ox nmap .xml`
- Parse XML file for new devices
  - New devices added to SQLite DB
    - IP Address & MAC Address
  - Email alerts when new devices found

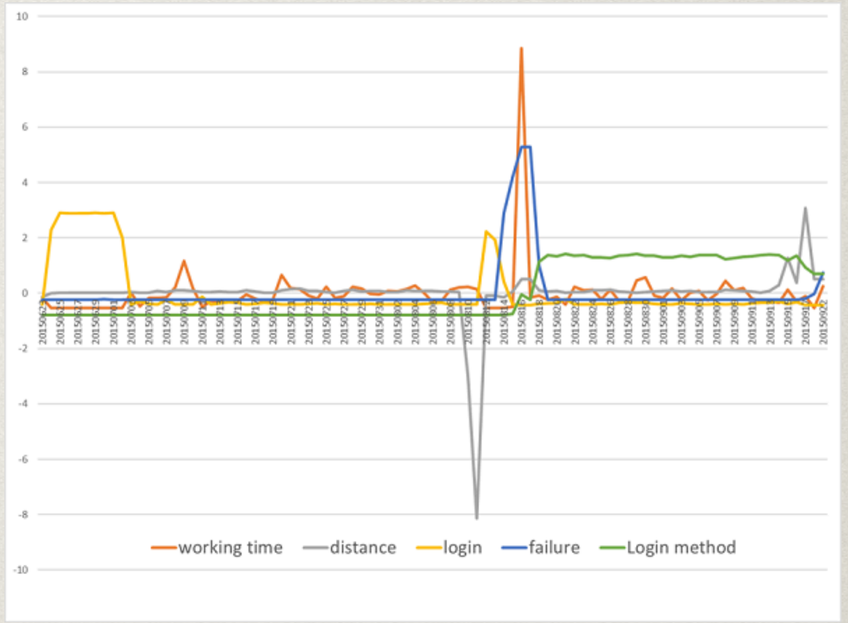
Show me the code!

https://goo.gl/ks3p9Q

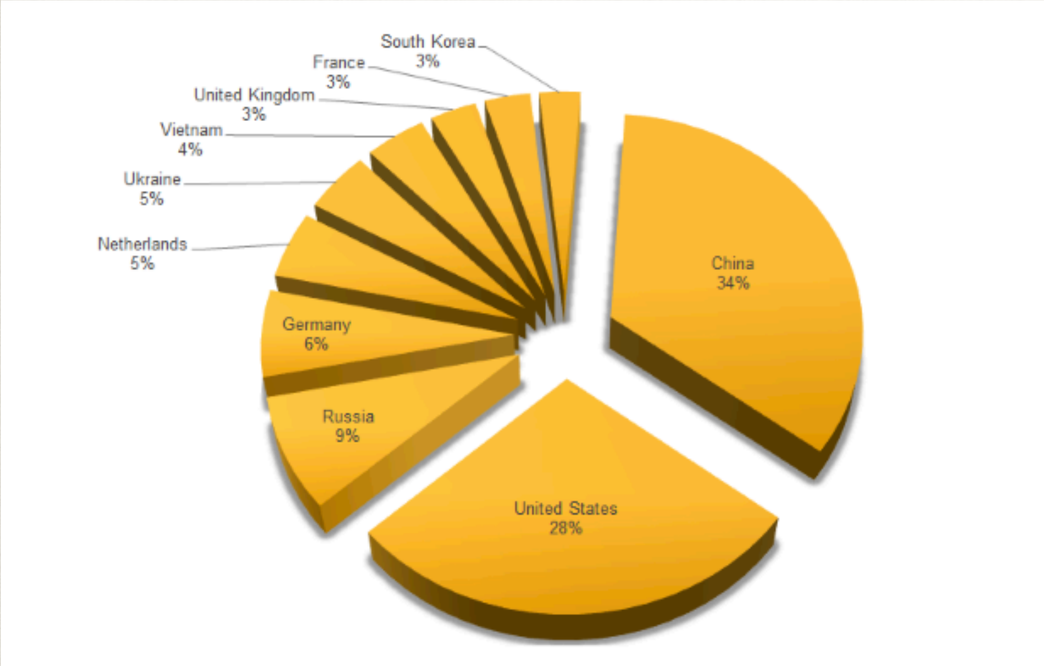
Learn more!

Extract Features from log

```
[WARN] USER user1 connected concurrently with 2228 miles different location
  - Connection1
    * IP: 162.223.5.123 (Toronto, Ontario, Canada)
    * Time: 2015-08-14 05:49:07.0 ~ 2015-08-14 08:05:27.0
  - Connection2
    * IP: 69.12.4.10 (Livermore, California, United States)
    * Time: 2015-08-14 06:03:35.0 ~ 2015-08-14 08:05:27.0


# [Rule: Concurrnet Login from different location] Finished
  * Found 4438 Warning, 0 Critical bad actions

# [Rule: Successful login from Suspicious IP]

# [Rule: Successful login from Suspicious IP] Finished
  * Found NO Bad action

# [Total Summary] Finished checking for 2 rules
  * Found 4438 Warning, 0 Critical bad actions
```



Does it work?



Top ten attack origins on monitored IoT honeypot in 2016,
by count of unique attackers

Country	Attempts number	Country	Attempts number
China	423 (23.5 %)	U.S.	800 (26.8 %)
U.S.	366 (20 %)	China	548 (18.4 %)
Brazil	123 (6.8 %)	France	162 (5.4 %)
Russia	90 (5 %)	Canada	151(5 %)
India	85 (4.7%)	Germany	141 (4.7 %)
Canada	56 (3.1%)	Brazil	135 (4.5 %)
South Korea	43 (2.4%)	Russia	106 (3.55 %)
Germany	40 (2.2%)	India	92 (3 %)
Italy	39 (2.16%)	U.K.	78 (2.61 %)
Seychelles	38 (2.11%)	Hong Kong	67 (2.2 %)

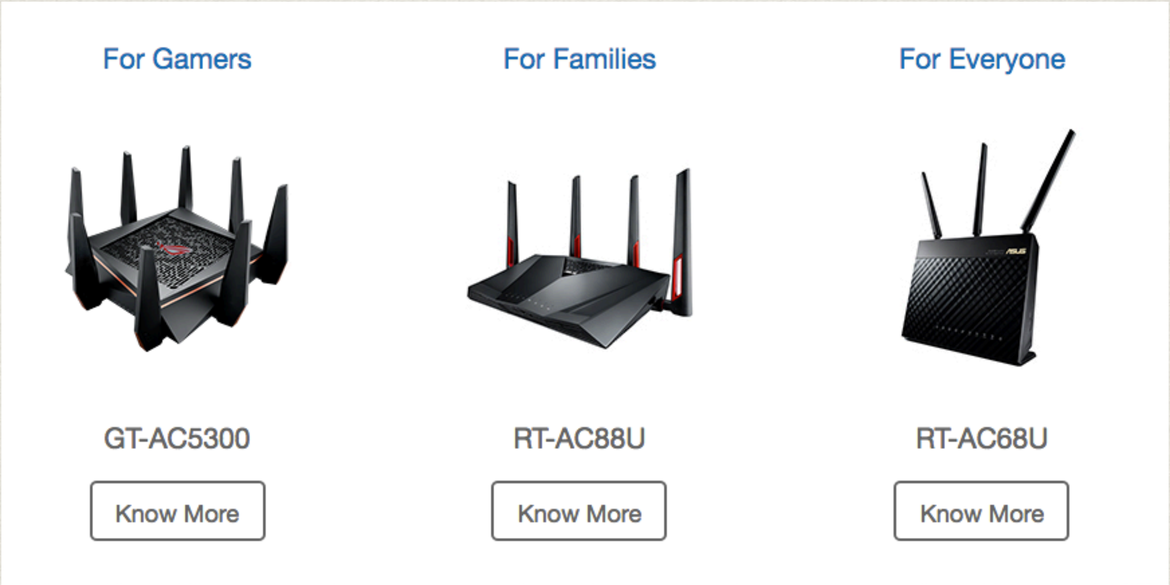
SSH brute force attempts on my RaspberryPi -_-

Data Source: https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

Show me the code again!

https://goo.gl/5ufCUF

Commercial Solutions



Has AiProtection (Costs $140 ~ $350)
By Asus and Trend Micro

Thank You!

@rabimba | karanjai.moz@gmail.com