BroCon ’17 Lightning Talks

Blacklists Revisited

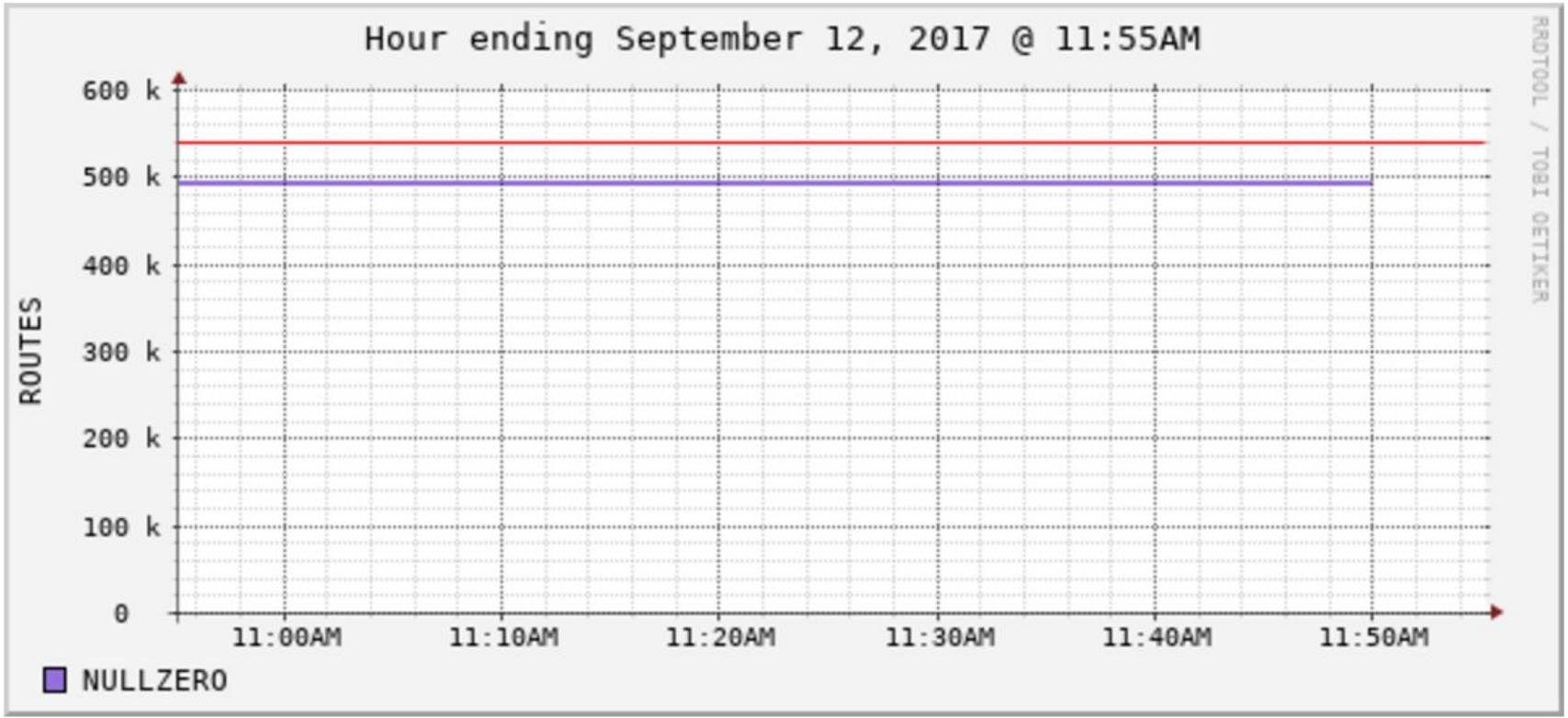
Aashish Sharma

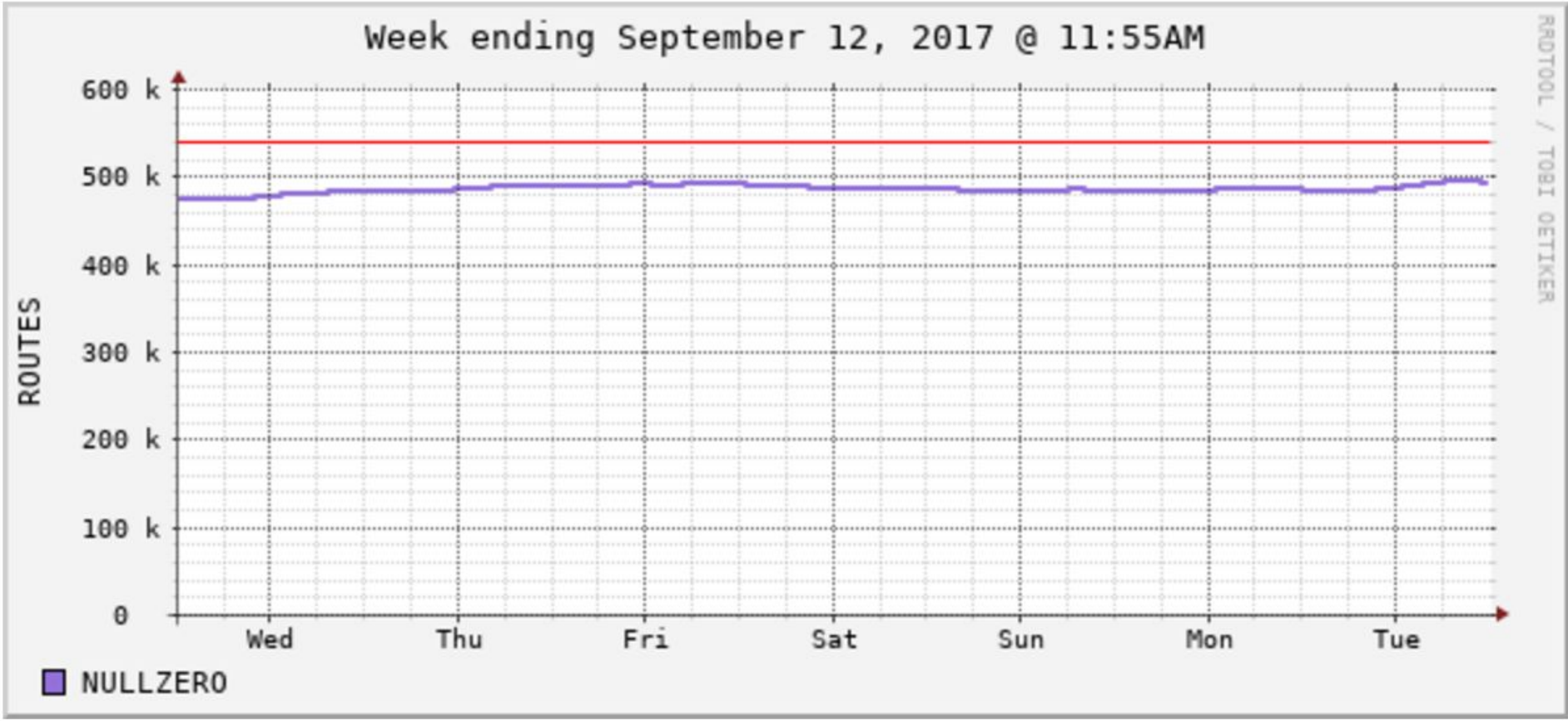
asharma@lbl.gov

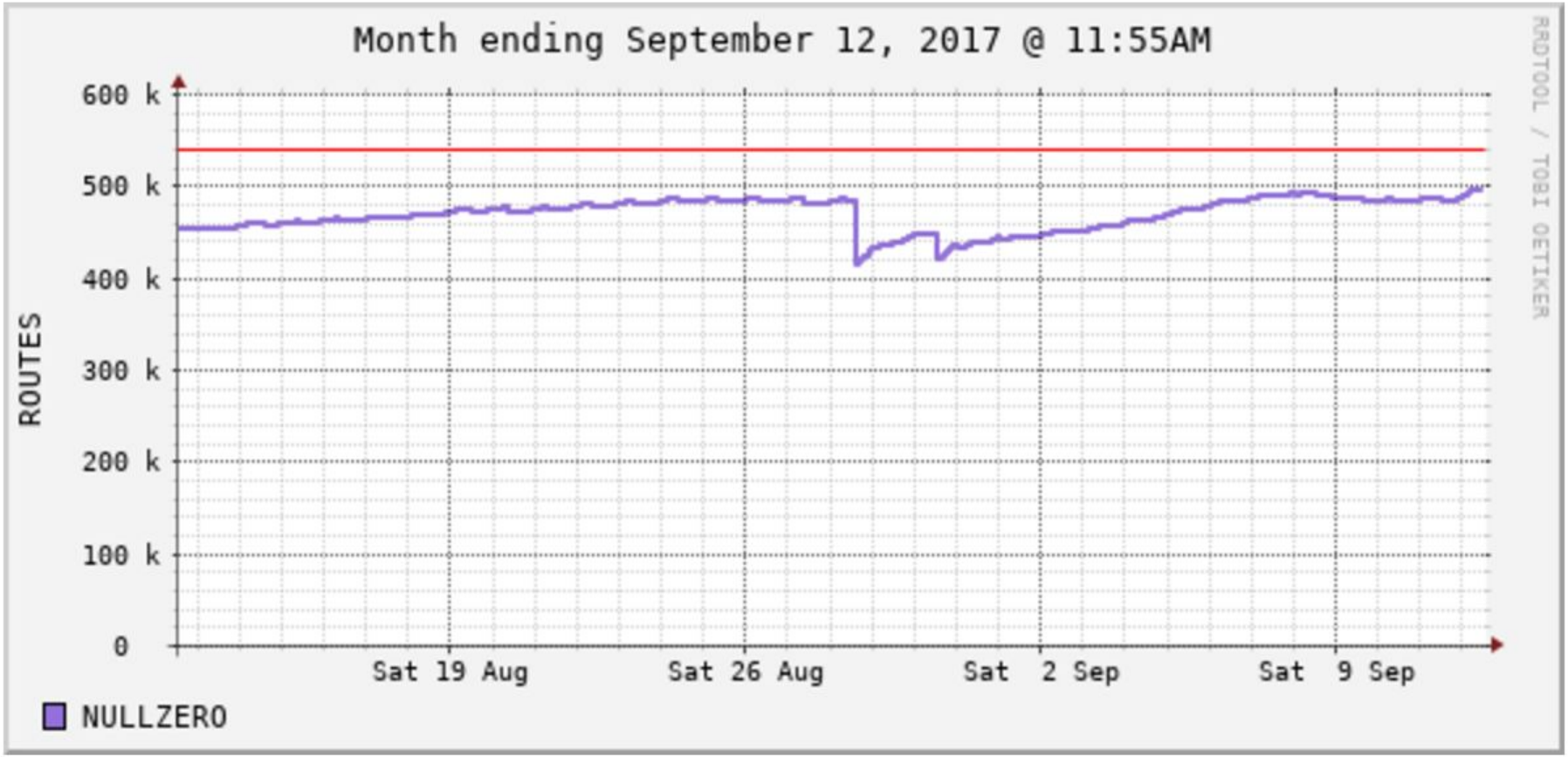
Blacklists Revisited

Lightening Talk
BroCon, 2017

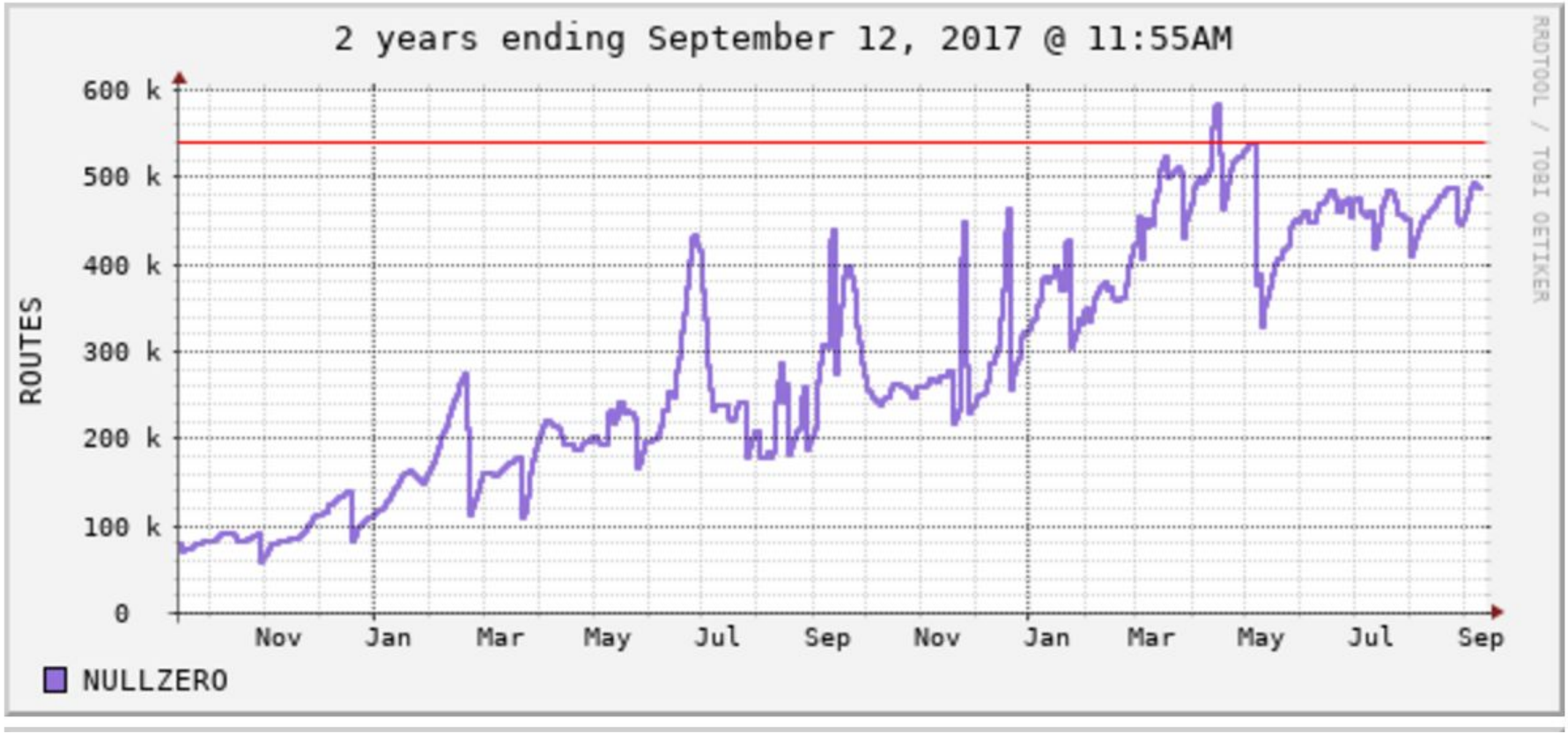
Problem

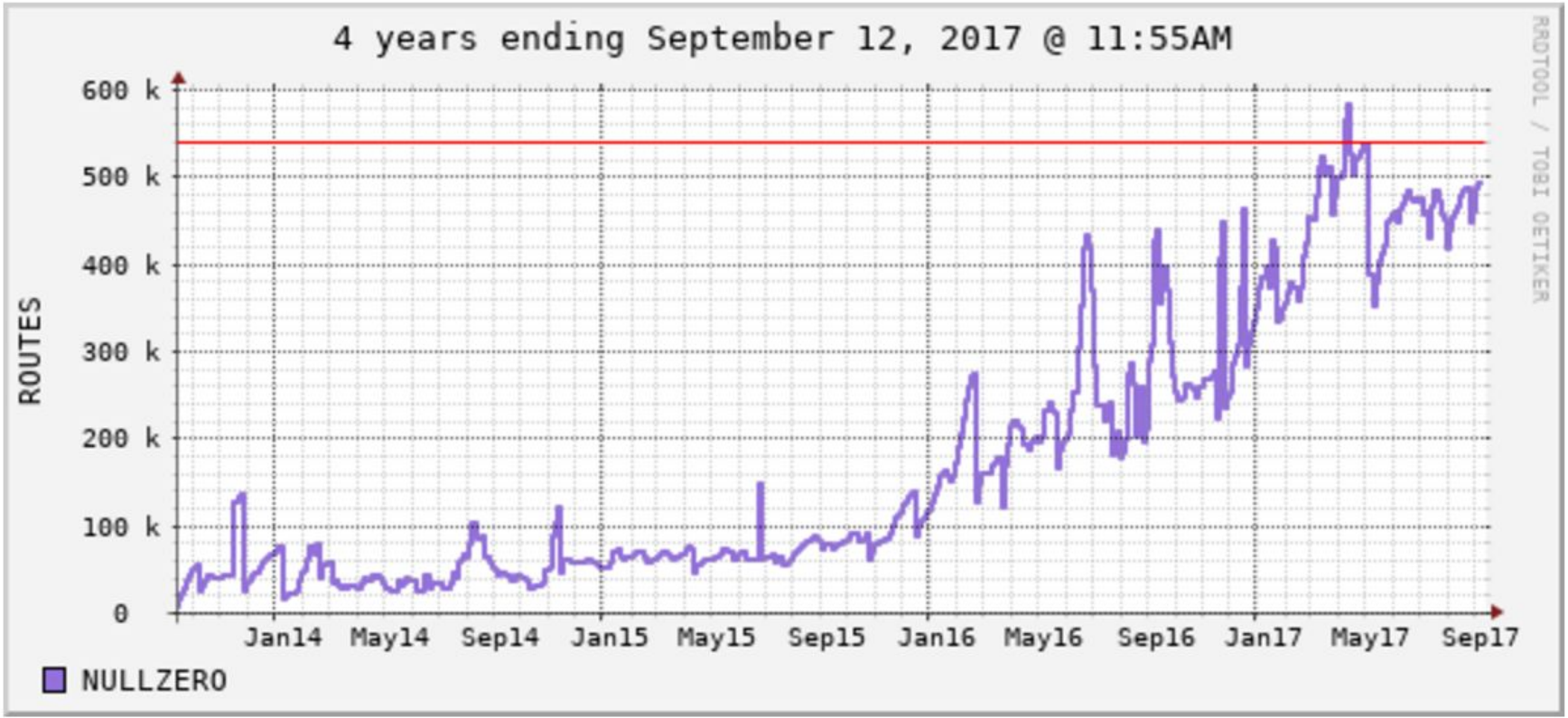

Hour ending September 12, 2017 @ 11:55AM
600 k
500 k
400 k
300 k
200 k
100 k
0
ROUTES
11:00AM
11:10AM
11:20AM
11:30AM
11:40AM
11:50AM
NULLZERO
RRDTOOL / TOBI OETIKER

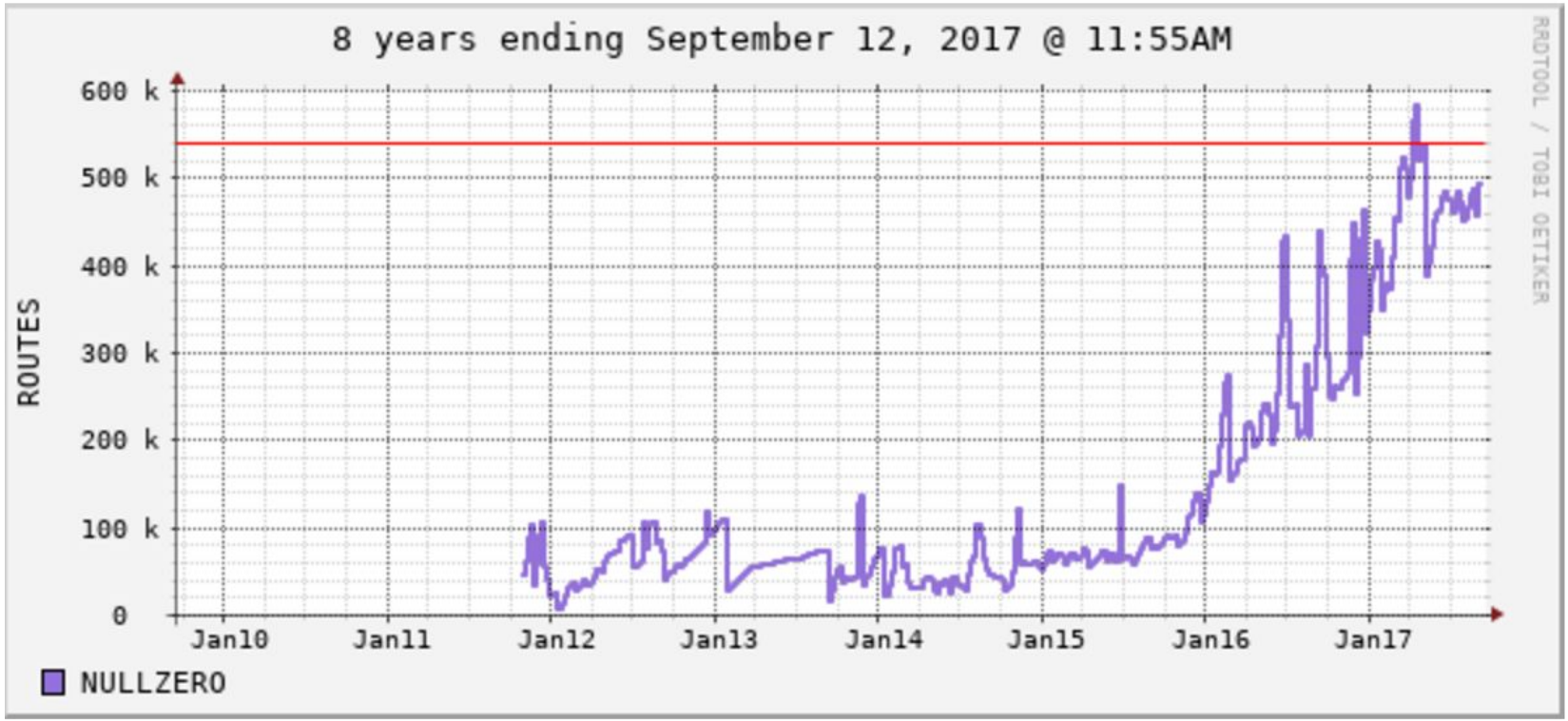

Week ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Wed
Thu
Fri
Sat
Sun
Mon
Tue
NULLZERO
RRDTOOL / TOBI OETIKER


Month ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Sat 19 Aug
Sat 26 Aug
Sat 2 Sep
Sat 9 Sep
NULLZERO
RRDTOOL / TOBI OETIKER


Year ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
NULLZERO
RRDTOOL / TOBI OETIKER


2 years ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Nov
Jan
Mar
May
Jul
Sep
Nov
Jan
Mar
May
Jul
Sep
NULLZERO
RRDTOOL / TOBI OETIKER


4 years ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Jan14
May14
Sep14
Jan15
May15
Sep15
Jan16
May16
Sep16
Jan17
May17
Sep17
NULLZERO
RRDTOOL / TOBI OETIKER


8 years ending September 12, 2017 @ 11:55AM
ROUTES
600 k
500 k
400 k
300 k
200 k
100 k
0
Jan10
Jan11
Jan12
Jan13
Jan14
Jan15
Jan16
Jan17
NULLZERO
RRDTOOL / TOBI OETIKER

Problem: Blocking Bad

Badness keeps increasing on the internet

How to manage blocking and more so unblocking

So, Can we identify……

Are blocked IPs coming back ?

How long do we block before unblock ?

Can we keep state forever

(that we can identify badness quickly)

Or, Are these one time visitors

Can we find out how many local IPs did the blacklisted IPs touched ?

How long the scan lasted ?

When was the last connection ?

Whats frequency of such connections ?

Problem 2:

We can read a million IPs using input-framework, but how to send those to 50 workers ?

Million IPs * 50 workers = 50 million Events

I want to be able to do this for 4 billion IPs

Bloomfilter

global Blacklist::m_w_add_bloom: event(val: opaque of bloomfilter);

1505245203.733616 1.2.3.4 8 128.3.x.y 0 icmp Blacklist::Drop

[ip=1.2.3.4, source=blacklist.adhoc, comment=####### 2017-03-29: Multi-Causal Drop + COUNT=8, LOOKBACK=30 + Country_Analysis, COMMIT_COUNT=2488]

Result: [block_until=<uninitialized>, watch_until=0.0, num_reblocked=0, current_interval=0, current_block_id=,
location=<uninitialized>] 1.2.3.4 128.3.x.y 0 bro Notice::ACTION_LOG 3600.000000 F

Aug 3 00:47:07	177.139.195.165	Blacklist::ONGOING	1	1501724827.167408	1501745134.319078	00-05:38:27	00-00:21:33	69	70	blacklist.adhoc
Aug 3 10:47:09	177.139.195.165	Blacklist::ONGOING	1	1501724827.167408	1501778367.997637	00-14:52:21	00-01:07:42	178	174	blacklist.adhoc
Aug 3 20:47:09	177.139.195.165	Blacklist::ONGOING	2	1501724827.167408	1501816682.763774	01-01:30:56	00-00:29:06	240	240	blacklist.adhoc
Aug 4 06:47:26	177.139.195.165	Blacklist::ONGOING	2	1501724827.167408	1501852922.704135	01-11:34:56	00-00:25:24	327	320	blacklist.adhoc
Aug 4 16:47:28	177.139.195.165	Blacklist::ONGOING	2	1501724827.167408	1501888432.024195	01-21:26:45	00-00:33:36	390	369	blacklist.adhoc
Aug 5 02:47:28	177.139.195.165	Blacklist::ONGOING	3	1501724827.167408	1501924862.984854	02-07:33:56	00-00:26:26	488	454	blacklist.adhoc
Aug 5 12:47:29	177.139.195.165	Blacklist::ONGOING	3	1501724827.167408	1501961086.496166	02-17:37:39	00-00:22:43	584	548	blacklist.adhoc
Aug 5 22:47:29	177.139.195.165	Blacklist::ONGOING	4	1501724827.167408	1501996956.381444	03-03:35:29	00-00:24:53	661	628	blacklist.adhoc
Aug 6 08:47:45	177.139.195.165	Blacklist::ONGOING	4	1501724827.167408	1502032986.136781	03-13:35:59	00-00:24:39	778	737	blacklist.adhoc
Aug 6 18:48:39	177.139.195.165	Blacklist::ONGOING	5	1501724827.167408	1502069303.080677	03-23:41:16	00-00:20:16	870	820	blacklist.adhoc
Aug 7 04:48:39	177.139.195.165	Blacklist::ONGOING	5	1501724827.167408	1502105037.713573	04-09:36:51	00-00:24:42	955	906	blacklist.adhoc
Aug 7 14:48:39	177.139.195.165	Blacklist::ONGOING	5	1501724827.167408	1502139365.973362	04-19:08:59	00-00:52:33	996	954	blacklist.adhoc
Aug 8 00:48:39	177.139.195.165	Blacklist::ONGOING	6	1501724827.167408	1502177084.343250	05-05:37:37	00-00:23:55	1068	1023	blacklist.adhoc
Aug 8 10:48:57	177.139.195.165	Blacklist::ONGOING	6	1501724827.167408	1502212184.928205	05-15:22:38	00-00:39:12	1144	1118	blacklist.adhoc

I HLHHL /YY, Y / LI1Ib	1111, j b , LI H . /H	ij	UNI:iUINU	I HI/LYIY *I*, YHH/H	I HIYYYY .:L *HbLL* / .:S	H.:S - H.:S	4j	¶¶	otacKllst.aonoc		
1502002798 . 931530	**Laci< List**	Blacklist	ONGOING	1501725596. 793429	1501999438. 493328	jL 04 02	70	118	**blackl i st .**		
	36-. - 4 , 111					jb 03-04	**adhoc**				
1502002798. 931530	18, 0.197 .180	Blacklist	ONGOING	1501732798. 361439	1502000700.131405	03-02 25 02	**00-00** 34 59	75	200	blacklist.adhoc	
1502002797 . 930819	11€ 193 . 98	Blacklist	ONGOING	1 501725587 . 861836	1501992561. 917784	03-02 09 34	00-02 50 36	**40**	70	bl ac kli st . ad hoc	
1502002797. 909702	58. , 35. 94	Blacklist	ONGOING	1501729186, 807464	1501994957 . 041549	03-01 49 30	00-02 10 41	87	149	**blacklist. adhoc**	
1502002796 . 892513	80 . 123 . 55	Blacklist	ONGOING	1 501725593 . 212484	1501997566. 643137	03-03 32 53	00-01 27 10	79	81	**blackl i st . adhoc**	
1502002796 . 892513	74. 47 . 9	Blacklist	ONGOING	1 501725592 . 419912	1501996018. 334763	03-03 07 06	00-01 52 59	37809	40930	black li st m. ast e r	
1502002796 . 892513	43. . 89 . 50	**Blacklist**	ONGOING	1 501736392 . 565320	1501997273. 002917	03-00 28 **00**	00-01 32 04	51	85	**blackl i st . adhoc**	
1502002795. 891941	94 . , 70.142	Blacklist	ONGOING	1 501725562 , 915203	1501998722, 850506	03-03 52 40	00-01 07 53	233	256	**blacklist. adhoc**	
1502002795. 891941	91. . 131. 83	Blacklist	ONGOING	1501739965. 088664	1502000317. 736456	03-00 19 13	**00-00** 41 18	146	230	blacklist. ad hoc	
1502002795 . 891941	91. . 11. 126	**Blacklist**	ONGOING	1501729171.110696	1501997352. 979105	03-02 29 42	00-01 30 43	37	61	**blackl i st . adhoc**	
1502002795. 891941	87. . 154 . 245	Blacklist	ONGOING	1 501739983 . 694479	1502001559 . 234655	03-00 39 36	00-00 20 37	1197	1212	**blackl i st . adhoc**	
1502002795 , 891941	61. 138 . 106	Blacklist	ONGOING	1 501725575 . 189671	1501989683. 077166	03-01 21 48	00-03 38 33	158	157	**blackl i st . adhoc**	
1502002795 . 891941	61. . 174 . 214	Blacklist	ONGOING	1 501725573 . 608766	1501992671. 949395	03-02 11 38	00-02 48 44	67	78	bl ac kli st . ad hoc	
1502002795 . 891941	22] 7. 154 . 75	**Blacklist**	ONGOING	1 501732792 . 434863	1502000053 . 608638	03-02 14 21	**00-00** 45 42	547	553	**blackl i st . adhoc**	
1502002795. 891941	21£ 3. 213 . 11	**Blacklist**	ONGOING	1 501725561 . 228135	1501991689. 643607	03-01 55 28	00-03 05 06	50	77	**blackl i st . adhoc**	
1502002795. 891941	21E 207. 226	Blacklist	ONGOING	1501729174, 697860	1501999666, 648398	03 - 03 08 12	**00-00** 52 09	44	65	**blacklist. adhoc**	
1502002795 . 891941	21] 0. 195 . 79	**Blacklist**	ONGOING	1 501736377 . 625080	1501995539. 874785	02-23 59 22	00-02 00 56	17	26	**blackl i st . adhoc**	
1502002795 . 891941	201 6. 215 . 162	**Blacklist**	ONGOING	1501725576, 818303	1501997957 . 574425	03-03 39 41	00-01 20 38	82	135	**blackl i st . adhoc**	
1502002795. 891941	18, 6, 195 . 65	**Blacklist**	ONGOING	1501729166, 554365	1502000455 , 788233	03-03 21 29	00-00 39 00	96	125	**blackl i st . adhoc**	
1502002795 . 891941	124 . 37. 50	**Blacklist**	ONGOING	1 501725594 . 466683	1501999716. 419462	03-04 08 42	**00-00** 51 19	115	175	**blackl i st . adhoc**	
1502002795 . 891941	12e . 137 . 174	**Blacklist**	ONGOING	1 501725566 . 317103	1502001077. 428540	03 - 04 31 51	00-00 28 38	5916	5997	**bl ac kl i st . adhoc**	
1502002795 , 891941	**10!:** 8 . 118 . 54	**Blacklist**	ONGOING	1 501732772 , 758054	1501998495 , 242517	03-01 48 42	00-01 11 41	144	146	**blacklist. adhoc**	
1502002794, 848936	87, .43.249	**Blacklist**	ONGOING	1501729164, 272415	1502000370. 963638	03 - 03 20 07	00 - 00 40 24	45	77	**blacklist. adhoc**	
150200 2794 . 848936	61. . 232 . 5	Blacklist	ONGOING	1 501725562 . 380724	1501996345 . 620671	03-03 13 03	00-01 47 29	46	48	**blacklist. adhoc**	
1502002794, 848936	59 , 23, 9	**Blacklist**	ONGOING	1501729183, 743209	1501997053, 525989	03-02 24 30	00-01 35 41	24	40	**blacklist. adhoc**	
1502002794, 848936	46 . . 105 . 12	**Blacklist**	ONGOING	1 501725566 , 429378	1502001331. 367935	03-04 36 05	00-00 24 23	387	388	**blackl i st . adhoc**	
1502002794 , 848936	45. 167 .181	**Blacklist**	ONGOING	1 501725580 , 774554	1502001048. 470458	03-04 31 08	**00-00** 29 06	21	336	TOR	
1502002794, 848936	201 0. 224. 241	Blacklist	ONGOING	1501725568, 552434	1502001 439. 124658	03 - 04 37 51	00 - 00 22 36	2445	2525	**blacklist. adhoc**	
1502002794, 848936	18t 7, 54 , 121	Blacklist	ONGOING	1 501725566 , 097575	1502000466, 261048	03-04 21 40	**00-00** 38 49	813	798	**blackl i st . adhoc**	
1502002794, 848936	171 2,201.133	**Blacklist**	ONGOING	1 501725560 , 904906	1502000181 , 894427	03 - 04 17 01	00 - 00 43 33	45	69	**blackl i st . adhoc**	
1502002794, 848936	**13!:** 0. 100. 34	Blacklist	ONGOING	1501729162, 626309	1502000427, 707746	03-03 21 05	**00-00** 39 27	34	53	**blacklist. adhoc**	
1502002794. 848936	12, 0. 243.142	Blacklist	ONGOING	1501729162. 609136	1501999847, 812804	03-03 11 25	**00-00** 49 07	113	111	**blacklist. adhoc**	
1502002794, 848936	121 4,132 , 11 0	Blacklist	ONGOING	1501725564, 109139	1502001676, 486699	03-04 41 52	**00-00** 18 38	**400**	405	blacklist,adhoc	
1502002794, 848936	11, 0. 110 . 211	Blacklist	ONGOING	1501725562, 298755	1501995268. 808754	03-02 55 07	00-02 05 26	159	161	blacklist.adhoc	
1502002794, 848936	**112** . 82 . 50	Blacklist	ONGOING	1 501736369 , 154361	1502000672 , 974104	03-01 25 **04**	**00-00** 35 22	59	60	**blackl i st . adhoc**	
1502002762. 20677	194 . 9 . 162 5. 132 . 177		ONGOIN	1501729124. 918559	1502000890. 047415	03-03 29 25	00-00 31 12	144	153	**bl ac kl i st .**	

Bro in Apache Metron

Jon Zeolla

Jon.Zeolla@SeisoLLC.com

https://github.com/apache/metron

What is Metron?

Metron integrates a variety of open source big data technologies in order to offer a centralized tool for security monitoring and analysis. Metron provides capabilities for log aggregation, full packet capture indexing, storage, advanced behavioral analytics and data enrichment, while applying the most current threat intelligence information to security telemetry within a single platform.

What is Metron?

Metron integrates a **ton** of open source big data technologies in order to offer a centralized tool for security monitoring and analysis. Metron provides capabilities for log aggregation, full packet capture indexing, storage, advanced behavioral analytics and data enrichment, while applying the most current threat intelligence information to security telemetry within a single platform.

What is Metron?

Metron integrates a **ton** of **Hadoop ecosystem** technologies in order to offer a centralized tool for security monitoring and analysis. Metron provides capabilities for log aggregation, full packet capture indexing, storage, advanced behavioral analytics and data enrichment, while applying the most current threat intelligence information to security telemetry within a single platform.

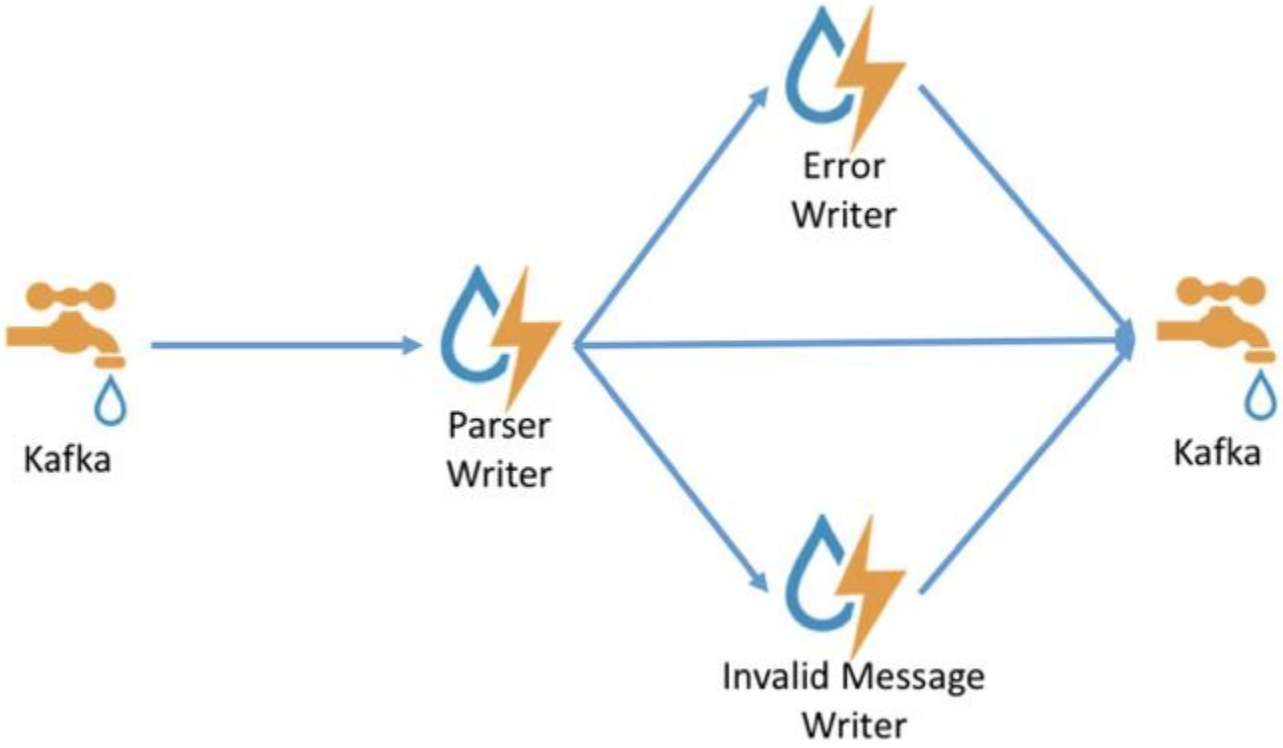
What is Metron?

Metron integrates a **ton** of **Hadoop ecosystem** technologies in order to offer a **way to use a large amount of security data (bro, snort, yaf, pcap, etc.).**

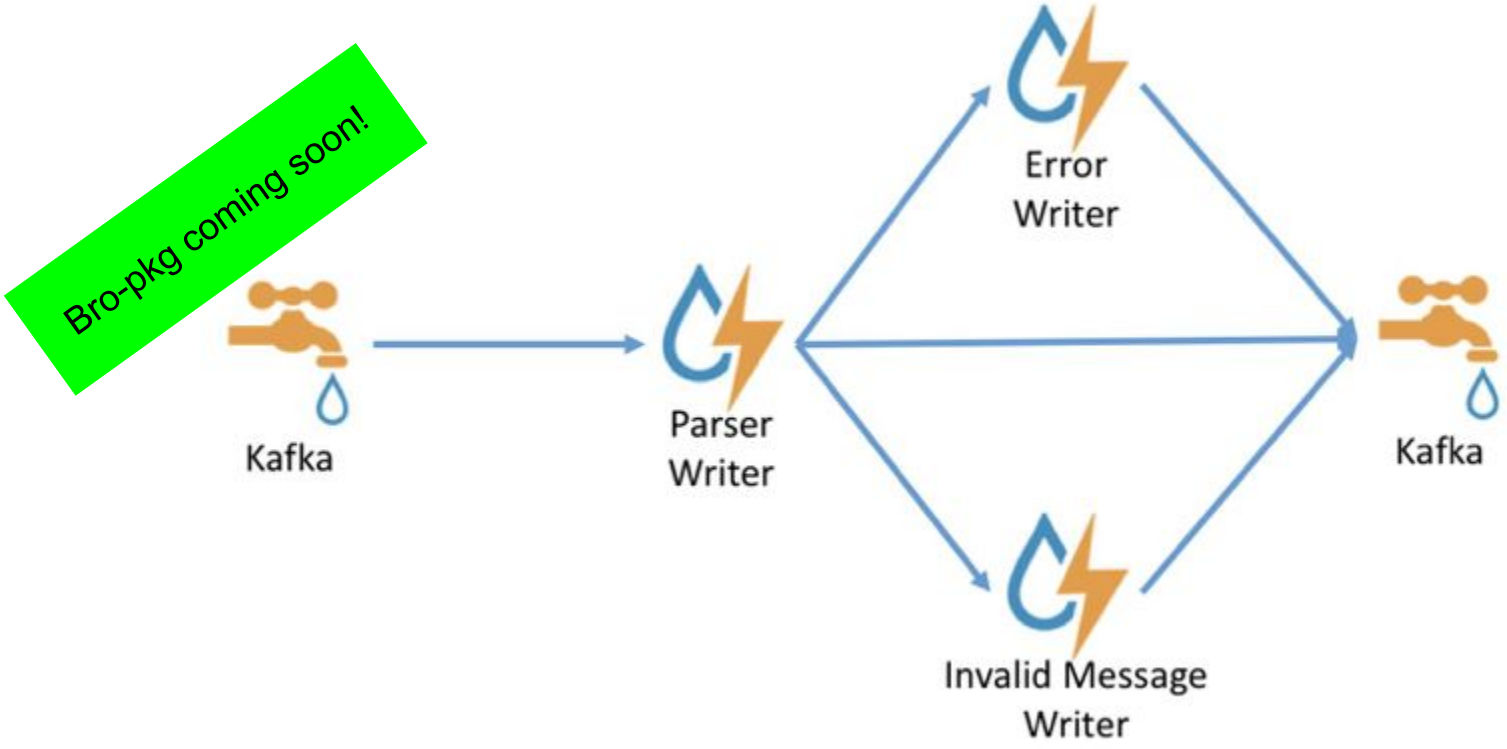
What is Metron?

Metron integrates a **ton** of **Hadoop ecosystem** technologies in order to offer a **way to use a large amount of security data (bro, snort, yaf, pcap, etc.).**

Parsing and Normalizing

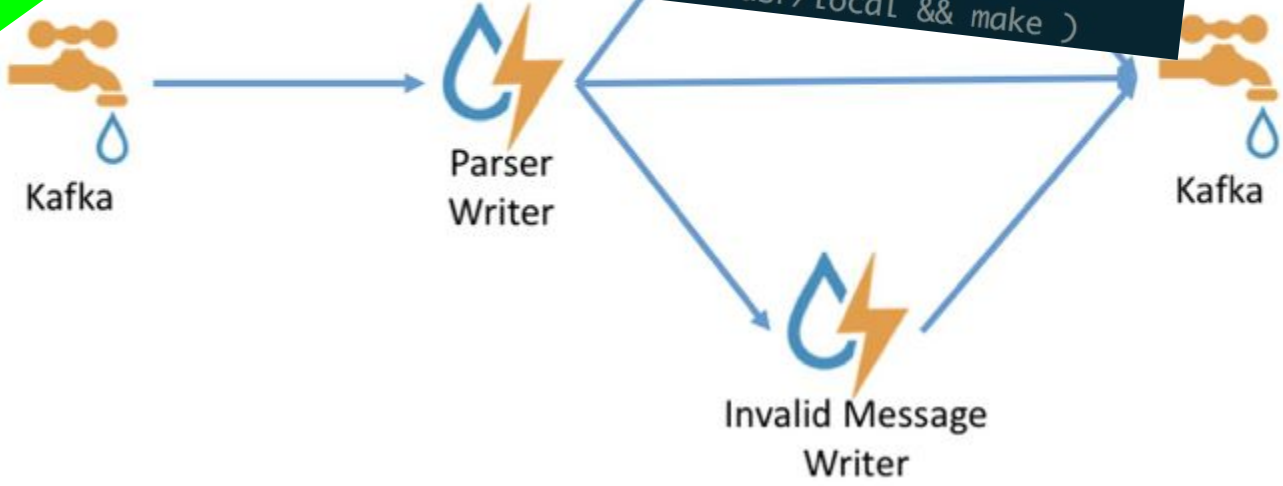


Parsing and Normalizing



```
build_command = ( if [ ! -a /usr/local/lib/librdkafka.so ]; then curl -L
https://github.com/edenhill/librdkafka/archive/v0.9.4.tar.gz | tar xvz && cd
librdkafka-0.9.4/ && ./configure --prefix=/usr/local --enable-sasl && make &&
sudo make install && cd - ; else if [ $(python -c "from ctypes import *; minver
= 0x904ff; dll = cdll.LoadLibrary(\"/usr/local/lib/librdkafka.so\"); version =
dll.rd_kafka_version(); exit(0) if minver >= version else exit(1)") ]; then
echo "At least version 0.9.4 of librdkafka is installed"; else echo "Please
manually upgrade librdkafka to at least version 0.9.4"; exit 1; fi; fi &&
./configure --bro-dist=%(bro_dist)s --with-librdkafka=/usr/local && make )
```

Bro-pkg coming



```
build_command = ( if [ ! -a /usr/local/lib/librdkafka.so ]; then curl -L
https://github.com/edenhill/librdkafka/archive/v0.9.4.tar.gz | tar xvz && cd
librdkafka-0.9.4/ && ./configure --prefix=/usr/local --enable-sasl && make &&
sudo make install && cd - ; else if [ $(python -c "from ctypes import *; minver
= 0x904ff; dll = cdll.LoadLibrary(\"/usr/local/lib/librdkafka.so\"); version =
dll.rd_kafka_version(); exit(0) if minver >= version else exit(1)") ]; then
echo "At least version 0.9.4 of librdkafka is installed"; else echo "Please
manually upgrade librdkafka to at least version 0.9.4"; exit 1; fi; fi &&
./configure --bro-dist=%(bro_dist)s --with-librdkafka=/usr/local && ma
```

Bro-pkg coming

Kafka

Parser

Writ

- **Inability to solicit user feedback during bro-pkg install**
  #11 opened 12 hours ago by JonZeolla
- **InterpolationSyntaxError when referencing a variables multiple times**
  #10 opened 12 hours ago by JonZeolla
- **bro-pkg doesn't support external library dependencies**
  #9 opened 12 hours ago by JonZeolla

valid Message

Writer

```
build_command = ( if [ ! -a /usr/local/lib/librdkafka.so ]; then curl -L
https://github.com/edenhill/librdkafka/archive/v0.9.4.tar.gz | tar xvz
librdkafka-0.9.4/ && ./configure --prefix=/usr/local
sudo make install && cd - ; else if [ $(python
= 0x904ff; dll = cdll.LoadLibrary
dll.rd_kafka_version()
echo "At
```

lizing

me to Bro-IDS

9:45 AM

Under step 6 of this documentation it shows that you can install a package with `bro-pkg install .`, but I'm having some issues doing that. I've attached a screenshot - anybody know why this would be happening?

Jon

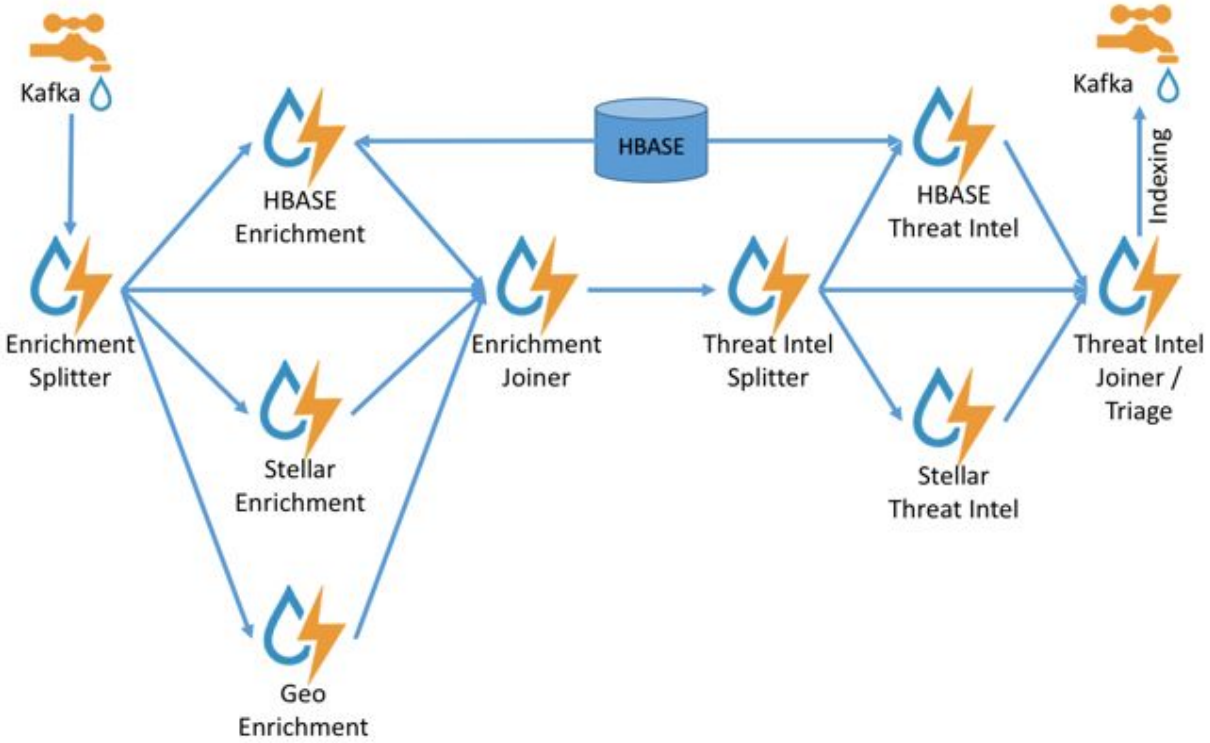
```
[root@          metron-bro-plugin-kafka]# ls
bro-pkg.meta  CHANGES  cmake  CMakeLists.txt  configure  configure.plugin  COPYING  MAINTAINER  Makefile  README.md  scripts  src  tests  VERSION
[root@          metron-bro-plugin-kafka]# git status
# On branch bro-pkg
nothing to commit, working directory clean
[root@          metron-bro-plugin-kafka]# git remote -v
origin  https://github.com/jonzeolla/metron-bro-plugin-kafka (fetch)
origin  https://github.com/jonzeolla/metron-bro-plugin-kafka (push)
[root@          metron-bro-plugin-kafka]# bro-pkg install .
error: invalid package ".": missing bro-pkg.meta metadata file
[root@          metron-bro-plugin-kafka]# bro-pkg install https://github.com/jonzeolla/metron-bro-plugin-kafka --version bro-pkg
The following packages will be INSTALLED:
  https://github.com/jonzeolla/metron-bro-plugin-kafka (bro-pkg)

Proceed? [Y/n] y
Skipping unit tests for "https://github.com/jonzeolla/metron-bro-plugin-kafka": no test_command in metadata
Installing "https://github.com/jonzeolla/metron-bro-plugin-kafka" (bro-pkg)
Installed "https://github.com/jonzeolla/metron-bro-plugin-kafka"
Loaded "https://github.com/jonzeolla/metron-bro-plugin-kafka"
[root@          metron-bro-plugin-kafka]# bro -N | grep -i kafka
Bro::Kafka - Writes logs to Kafka (dynamic, version 0.2)
[root@          metron-bro-plugin-kafka]# bro-pkg --version
bro-pkg 1.0.4
```

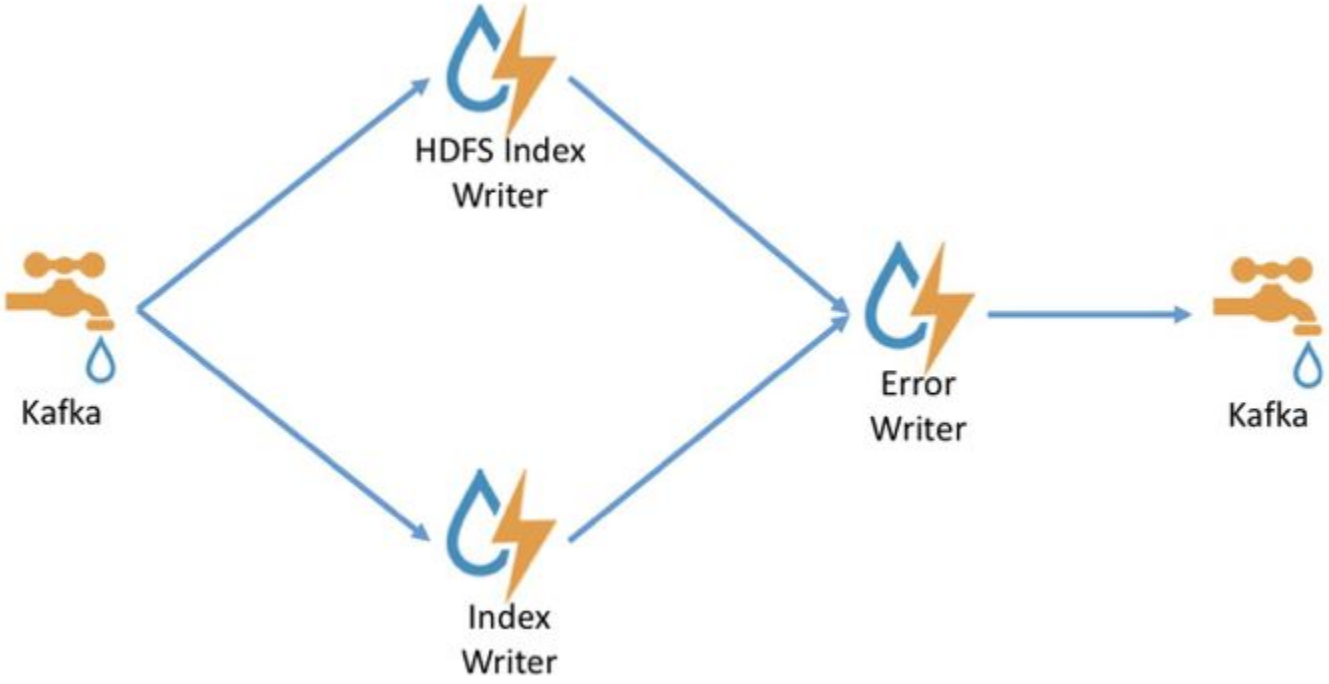
ple times

#9 ...valid Message Writer

Enriching and Triaging



Indexing



Key Features

- Streaming data normalization and cleansing
- Ultra-high scale data processing with horizontal scaling
- Canned and custom, streaming enrichments that provide data-local context
- Native Threat Intelligence Integration
- “Modeling as a Service” platform
  - Heavily leveraging the profiler for feature extraction (IPs, Users, Subnets, Applications, etc.)
- PCAP storage/retrieval

Native bro log support in 0.4.1

- Conn
- DPD
- FTP
- Files
- CertsInfo
- SMTP
- SSL
- Weird
- Notice
- DHCP
- SSH
- Software
- Radius
- X509
- DevicesInfo

Taking Bro to the BSD Community

Michael Shirk

https://github.com/shirkdog/Presentations

Detecting Fakers & Attackers via Notice/Http Logs

Fatema Bannat Wala

fatema.bannatwala@gmail.com

Detecting Fake Google-Bots - I

Q: Internet Bots pretending to be Google-Bots and mining data from your sites?
A: Detect them and block them with BRO:)

- Characteristics of legit googlebot that Google uses for web-crawling:
  1. Uses CIDR: 66.249.0.0/16
  2. DNS's ends in 'googlebot.com'
  3. Uses UA having: 'Googlebot'

```
$ cat notice.log | bro-cut -d | grep 'Scan::WebCrawler' | grep -i 'googlebot' | egrep -v "66\.249\." | awk -F'\t' '{print $1, $11, $12; system("host " $14)}'
```

ts note **msg**

2017-09-01T16:08:03-0400 Scan::WebCrawler **217.208.229.37** crawler is seen Mozilla/5.0 (**compatible; Googlebot/2.1 +http://www.googlebot.com/bot.html**) 37.229.208.217.in-addr.arpa domain name pointer **217-208-229-37-no205.tbcn.telia.com**.

2017-09-01T16:14:57-0400 Scan::WebCrawler **138.201.80.141** crawler is seen **Googlebot-Image/1.0** 141.80.201.138.in-addr.arpa domain name pointer **static.141.80.201.138.clients.your-server.de**.

Detecting Fake Google-Bots - II

Q:Have someone In-House pretending to be a Google-Bot?
A: Detect them and investigate them with BRO:)

Investigator questions:

- Is the host compromised?
- Is this user doing research?
- Is this a Proxy?

```
$ cat notice.log | bro-cut -d | grep 'Scan::WebCrawler' | grep -i 'googlebot' | egrep "128\.4\.|128\.175\." | awk -F'\t' '{print $1, $11, $12; system("host " $14)}'
```

ts note **msg**

2017-09-01T16:08:03-0400 Scan::WebCrawler **128.xx.yy.zz** crawler is seen Mozilla/5.0 **(compatible; Googlebot/2.1; +http://www.google.com/bot.html)** zz.yy.xx.128.in-addr.arpa domain name pointer **zz-yy-xx-128-aaa.bbb.ccc.**

2017-09-01T16:14:57-0400 Scan::WebCrawler **128.ss.tt.vv** crawler is seen Mozilla/5.0 **(compatible; Googlebot/2.1; +http://www.google.com/bot.html)** uu.vv.tt.128.in-addr.arpa domain name pointer **vv-tt-ss-128-ddd.eee.fff.**

Detecting ShellShock Attempts

Q: Is someone still trying to give a shell shock to your servers?
A: Unveil them with BRO

```
$ cat http.log | bro-cut -d | awk -F'\t' '{ if ($13 ~ /cmd\.exe/ || $13 ~ /\/bin\/bash/) print $1, $2, $3, $4, $5, $6, $8, $13 }' | more
```

ts uid id.orig_h id.orig_p id.resp_h id.resp_p method **user_agent**

2017-08-31T16:20:05-0400 Cjq5cD4agq22BN8cn9 31.210.47.92 58168 128.x.y.z 80 GET **() { foo;}; echo Content-Type: text/plain ; echo ; /bin/bash -c 'id ; uname -a ; whoami'**

2017-08-31T16:20:06-0400 CnGk7y4G6xBRYKlrtd 31.210.47.92 58176 128.x.y.z 80 GET **() { foo;}; echo Content-Type: text/plain ; echo ; /bin/bash -c 'id ; uname -a ; whoami'**

2017-08-31T16:20:06-0400 CdshMA2SftnrUVBEx 31.210.47.92 58175 128.x.y.z 80 GET **() { foo;}; echo Content-Type: text/plain ; echo ; /bin/bash -c 'id ; uname -a ; whoami'**

CEASE: Leveraging Bro as a Network Feed

Nick Buraglio

ESnet

ENERGY SCIENCES NETWORK

CEASE: Leveraging Bro as a network intel feed

Nick Buraglio

Network Engineer,

ESnet Network Planning Team

Lawrence Berkeley National Laboratory

09/12/2017

U.S. DEPARTMENT OF ENERGY

Office of Science

BERKELEY LAB

Correlation Evaluation And Security Enforcement

ESnet

Correlation Evaluation And Security Enforcement

- Deployed in high impact areas (public exchange points, etc.)
- Leverage existing data sets
  - Syslog
  - Netflow
  - Bro Alarms
  - Route topology
- Protect ESnet critical infrastructure
- Extend to an opt-in service for connectors

- Useful to any large network - not just ISPs

ESnet

Bro alarms tuned properly...

- ...Allows us to…
- ...correlate existing data sets to cross reference for:
  - Targeted attacks
  - Small[er] DDoS
  - Volumetric attacks
- ….over a very large, carrier grade, international network
- ….understand the topological path the given traffic may take
- ….mitigate undesirable issues that may arise very far from any given sensor

ESnet

What the heck is this “CEASE” thing?

Correlation Evaluation And Security Enforcement

…..at every transit POP

ESnet

We are hiring!!

- Do interesting things!
- Work on a **one of a kind, global scale** network!
- Learn from smart people!

Network Engineers!
https://lbl.taleo.net/careersection/engineer/jobdetail.ftl?job=83959

Software Engineers!
https://lbl.taleo.net/careersection/engineer/jobdetail.ftl?job=84046

Questions?

buraglio@es.net

ESnet

Bro and PacketSled

Technical Overview

Leo Linsky

PacketSled

Challenges

- Our own pain points — Bro script is expensive.
- Customer use cases — documenting all interesting flows that other intrusion detection systems miss.
- Long term vision — we want our sensors to do more on the same hardware.

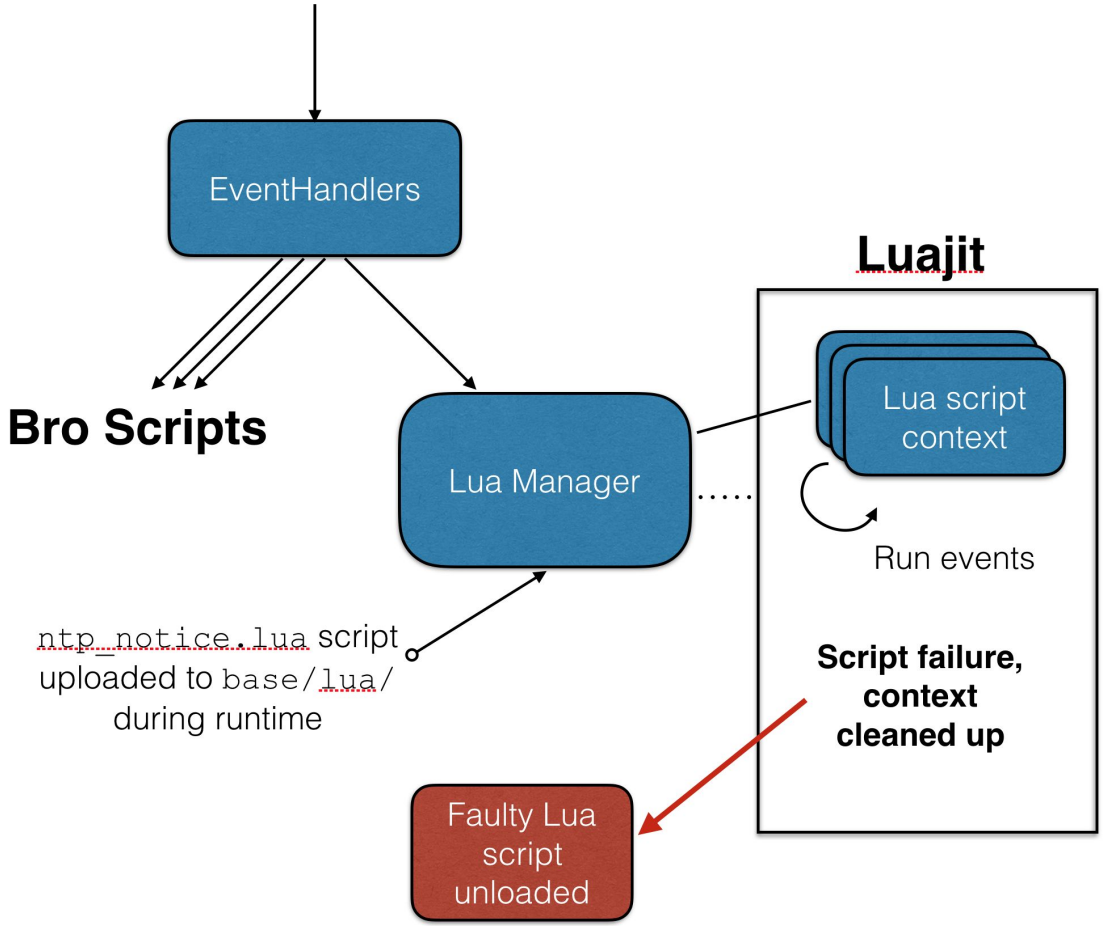
Options

- Compile Bro script and optimize the executables?
  - We want to run scripts dynamically, without restarting a sensor.
- Integrate a high performance alternative.
  - BIF’s, Binpac, and Bro plugins — need to be compiled and loaded with build, inaccessible for analysts looking to write and deploy detections.
  - LuaJIT is well supported, designed to be integrated via the Lua C API, and it gets faster as it runs.

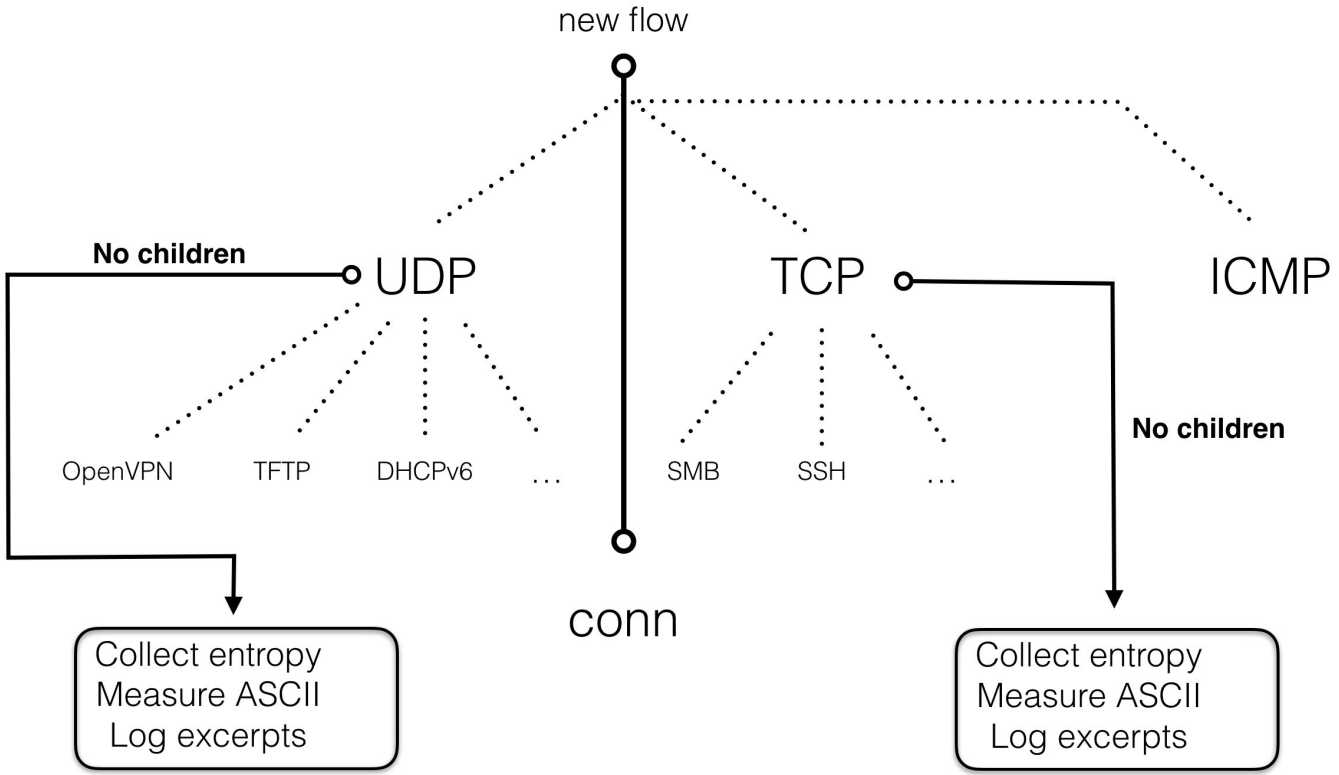
Outcomes

- Project forked from Bro 2.5 (future versioning independent from mainline Bro.)
- Introduces alternative scripting framework built into the Bro-core to support Lua scripts.
- Changes in how we handle and generate metadata for unidentified flows.
- Performance improvements and customizations

Event generation from Bro kernel and plugins



Analyzers of Last Resort



Other Additions

- Optimizing core loops (like `net_run()`) with preprocessor branch prediction macros `likely()` and `unlikely()` for ~3% speedup. We optimize for maximum load.
- UDP and TCP analyzers of last resort: modify analyzers to log the beginning of UDP and TCP flows which were not analyzed by any child analyzers. Includes entropy and ASCII counts, with thresholds that can be adjusted to identify plaintext protocols and pull an excerpt.
- General bug fixes (SMB, UID's), improvements (mostly as BIF's, such as bitwise operations), and customizations.

Next Steps...

Aaron Eppert

PacketSled

Thought Experiment

- How many of you have modified Bro?
- Are you productizing Bro?
- What does the sustainability model look like?

Challenges

- Political
- Commits
- Non-corruption of open source
- Risks as a vendor

We Want to Share

- PacketSled can share:
  - Lua
  - Analyzers of Last Resort
  - Optimizations and Bug fixes

Bro - Community?

- Vendor and Consumer Consortium
- What if we built a census roadmap balancing Vendor wants and Consumer needs with the realities of maintainers and committers?

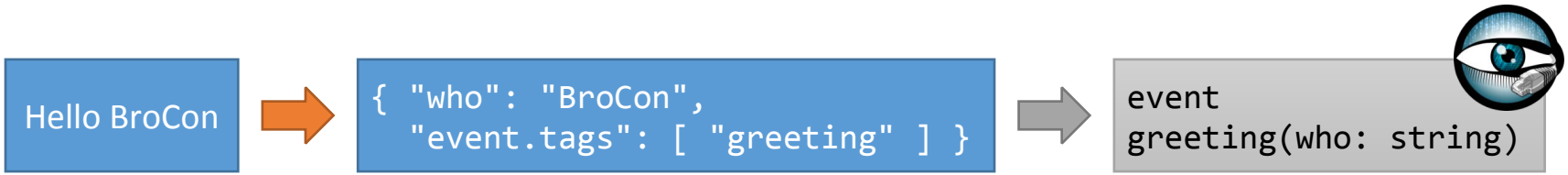
The Bro Lognorm Plug-in

Jan Grashöfer

https://github.com/J-Gras

bro-lognorm

- “Wouldn’t it be cool to parse syslog messages inside of Bro?” – Seth
- Idea: Use *liblognorm* (rsyslog)
  - matches log lines against rules: `rule=greeting:Hello %who:word%`



- Implementation:
  - Bro plugin offering the `lognormalizer` opaque type
  - Script-land interface for easy usage

bro-lognorm

Setup:

```
# test.rulebase:
# rule=greeting:Hello %who:word%

@load Bro/Lognorm
redef Lognorm::rule_files += {"test.rulebase"};

event greeting(who: string) {
    print fmt("Hi '%s'", who);
}

event Lognorm::unparsed_line(line: string) {
    print fmt("No rule for: '%s'", line);
}
```

Usage:

```
# Manually:
event bro_init() {
      Lognorm::normalize("Hello BroCon");
}

# Read files:
@load Bro/Lognorm/read_logs
redef Lognorm::log_file += {"test.log"}

#Read syslog:
@load Bro/Lognorm/read_syslog
```

github.com/J-Gras/bro-lognorm

jan.grashoefer@kit.edu

- Use cases: ¯_(ツ)_/¯
- Example-plugin implementing an opaque type