Automating Security @

Ryan Huber
Twitter: @ryanhuber

whoami

slack

Additional Information

Breaches

How does a company know when it has been hacked?

The company’s employees notice something strange

A 3rd party contacts the company because they notice something strange

(*Krebs)

Hacker(s) contact the company because they want them to notice something strange

They don’t

How did they get in?

verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION

The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

“Pulling back from a single industry view, we find that most of the attacks make use of stolen credentials, [...]”

“[...] 95% of these incidents involve harvesting creds from customer devices, then logging into web applications with them.”


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Collecting Data
Detection
Rules
Alerts
Verification
Q&A

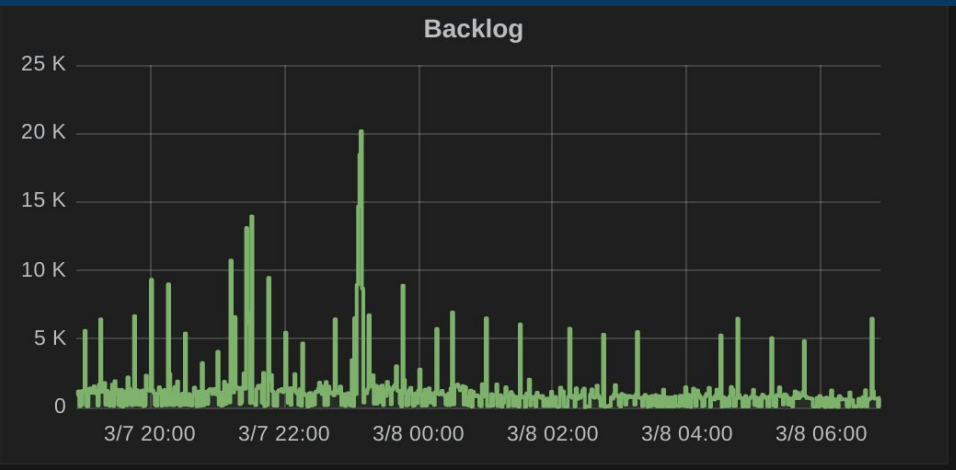
Step 1: Collecting data

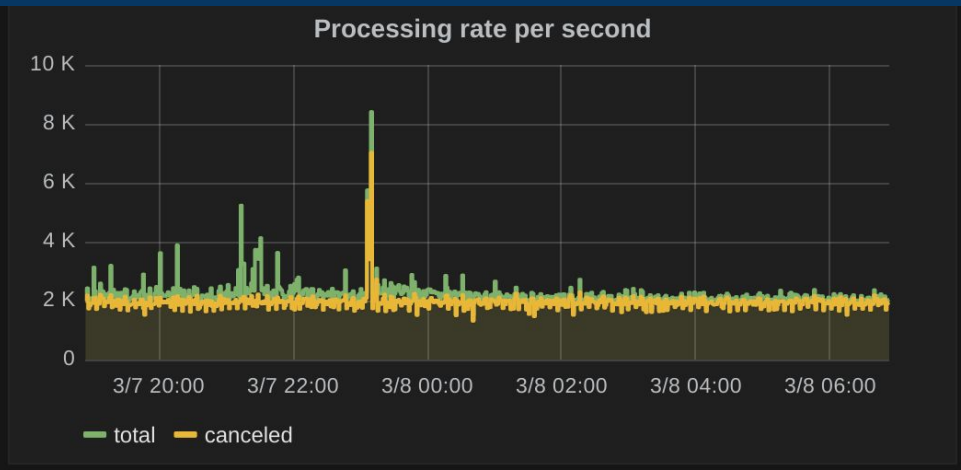
Our own AWS account

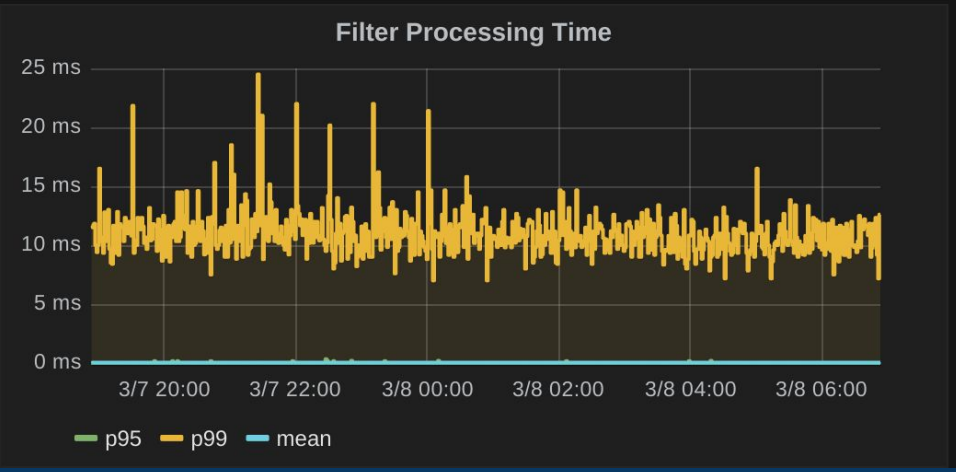
Set up a reliable logging pipeline

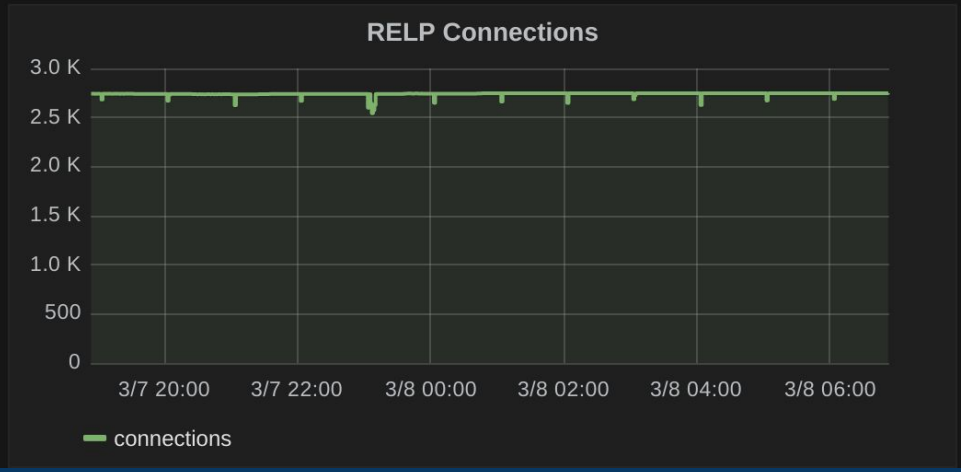
rsyslog (w/ RELP)

streamstash
(or logstash)


Backlog
25 K
20 K
15 K
10 K
5 K
0
3/7 20:00
3/7 22:00
3/8 00:00
3/8 02:00
3/8 04:00
3/8 06:00


Processing rate per second
10 K
8 K
6 K
4 K
2 K
0
3/7 20:00
3/7 22:00
3/8 00:00
3/8 02:00
3/8 04:00
3/8 06:00
total
canceled


Filter Processing Time
25 ms
20 ms
15 ms
10 ms
5 ms
0 ms
3/7 20:00
3/7 22:00
3/8 00:00
3/8 02:00
3/8 04:00
3/8 06:00
p95
p99
mean


RELP Connections
3.0 K
2.5 K
2.0 K
1.5 K
1.0 K
500
0
3/7 20:00
3/7 22:00
3/8 00:00
3/8 02:00
3/8 04:00
3/8 06:00
connections

Elasticsearch

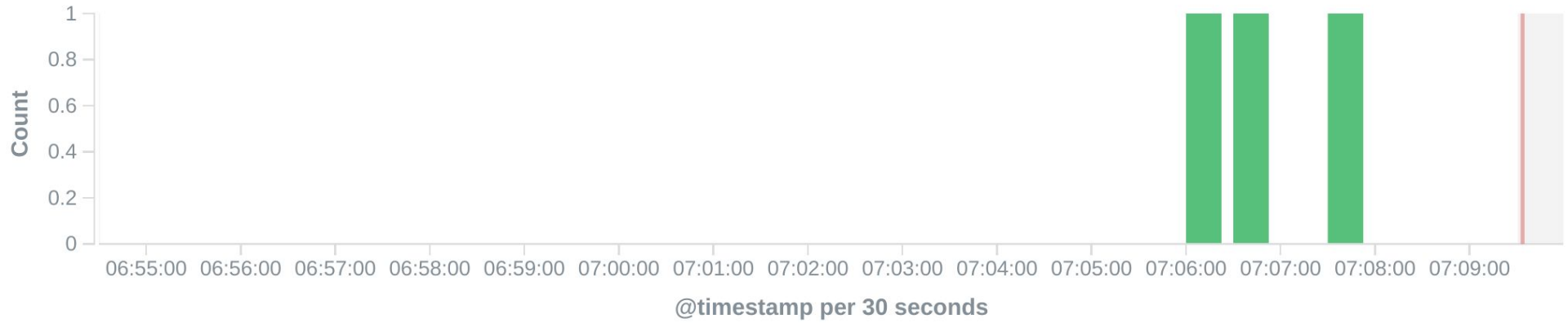
Data Sources

auditd

go-audit

```
$
$ uptime
 23:07:38 up 3 days,  8:18,  1 user,  load average: 16.24, 16.17, 16.44
$
$
$
$
$
```

March 8th 2016, 06:54:30.522 - March 8th 2016, 07:09:30.522 — by 30 seconds



Time	auid_username	command
March 8th 2016, 07:07:38.839	rhuber	uptime
March 8th 2016, 07:06:30.857	rhuber	uptime

auth logs
(ssh…)

cloudtrail

web logs

Step 2: Detection

The defender’s advantage

ZERO DAYS ARE NOT INVISIBILITY CLOAKS

The Hypothetical Malicious Insider

Off-the-shelf rulesets


MISSION CONTROL CENTER
esa
CAPCOM
PAYLOAD DEPLOY/
RETRIEVAL (PDRS)
ENVIRONMENTAL
(ECOM)
Relay Plot
MET 001:16:04:55.47
Ground
Range: 36.73
R-dot: -25.90
Y: -0.06
Y-dot: -0.22
Azimuth: -179.91
Elevation: +5.00
3D Attitude Display

Elasticsearch
or
$plunk

ElastAlert

Rules

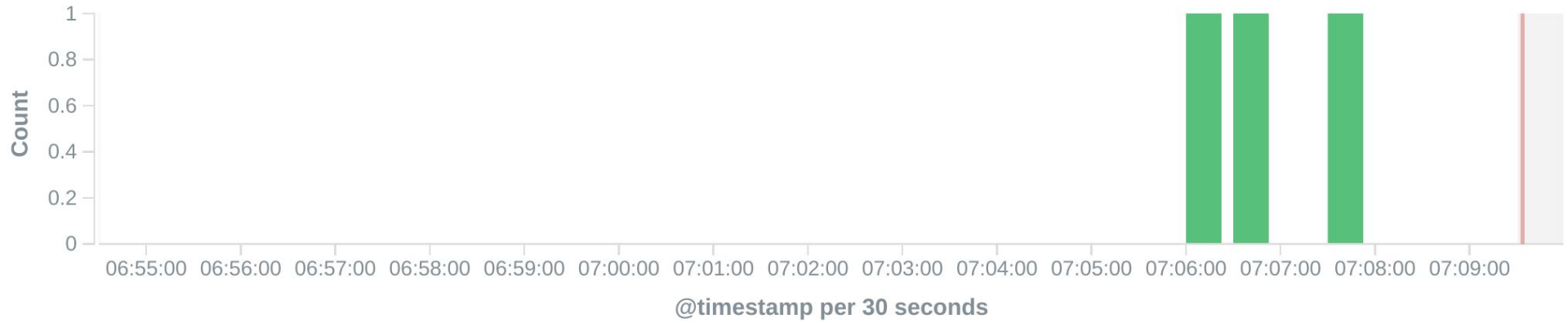
Time awake

Impossible GeoIP

IP

```
$
$ uptime
 23:07:38 up 3 days,  8:18,  1 user,  load average: 16.24, 16.17, 16.44
$
$
$
$
$
```

March 8th 2016, 06:54:30.522 - March 8th 2016, 07:09:30.522 — by 30 seconds



Time	auid_username	command
March 8th 2016, 07:07:38.839	rhuber	uptime
March 8th 2016, 07:06:30.857	rhuber	uptime

Alerts

AlertCenter

SecurityBot

securitybot BOT 12:47 PM

I see you just ran the command `flurb -export` on `accountingserver01`. This is a sensitive command, so please acknowledge this activity by typing `acknowledge`.

ryan 12:47 PM

acknowledge

securitybot BOT 12:47 PM

Acknowledging via 2fa.

Don’t overwhelm everyone

Verification

Carbon Black, anectotally..

Canaries

Red team exercises

Bonus:

What if they got in anyway?

Forensic data is there

Summary

https://goo.gl/ZAxCnH

@ryanhuber