By Hany Fahim
Founder and CEO
@iHandroid

VM FARMS
@vmfarms

TALES FROM THE OPS SIDE

HOW BRAZIL KEPT US UP AT NIGHT

WEDNESDAY, DECEMBER 16TH, 2015
8:00PM EST

DINER

SITE OUTAGE REPORTED

vmbot 10 seconds ago

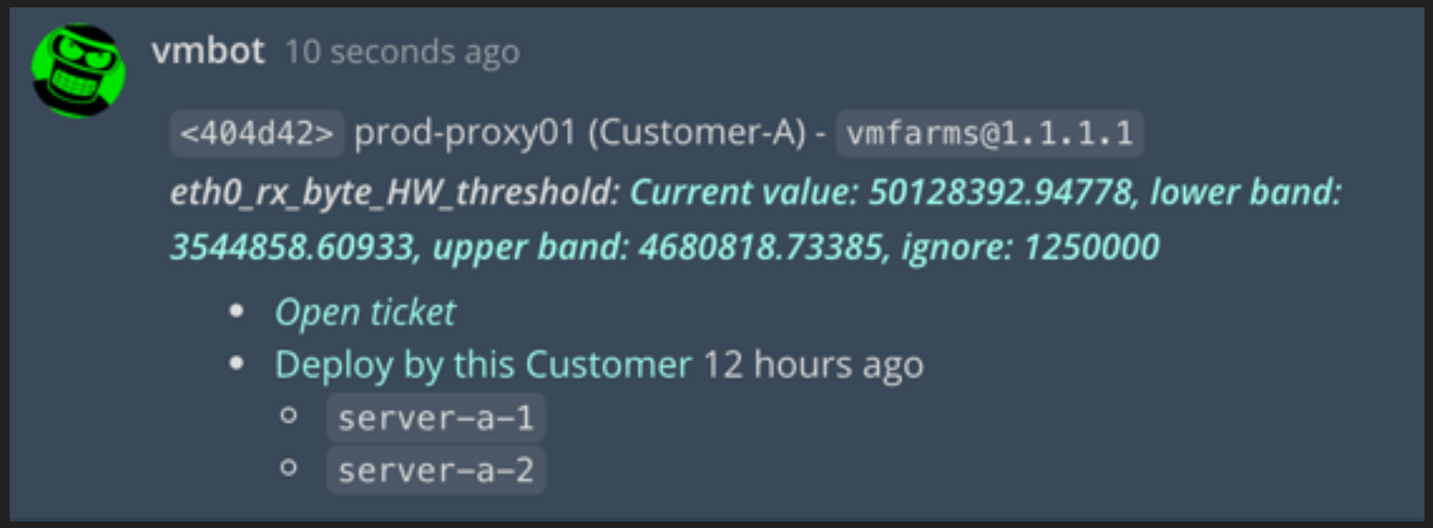
SITE OUTAGE FOR Customer-A!

API - https://api.customer-a.com/health-check is DOWN

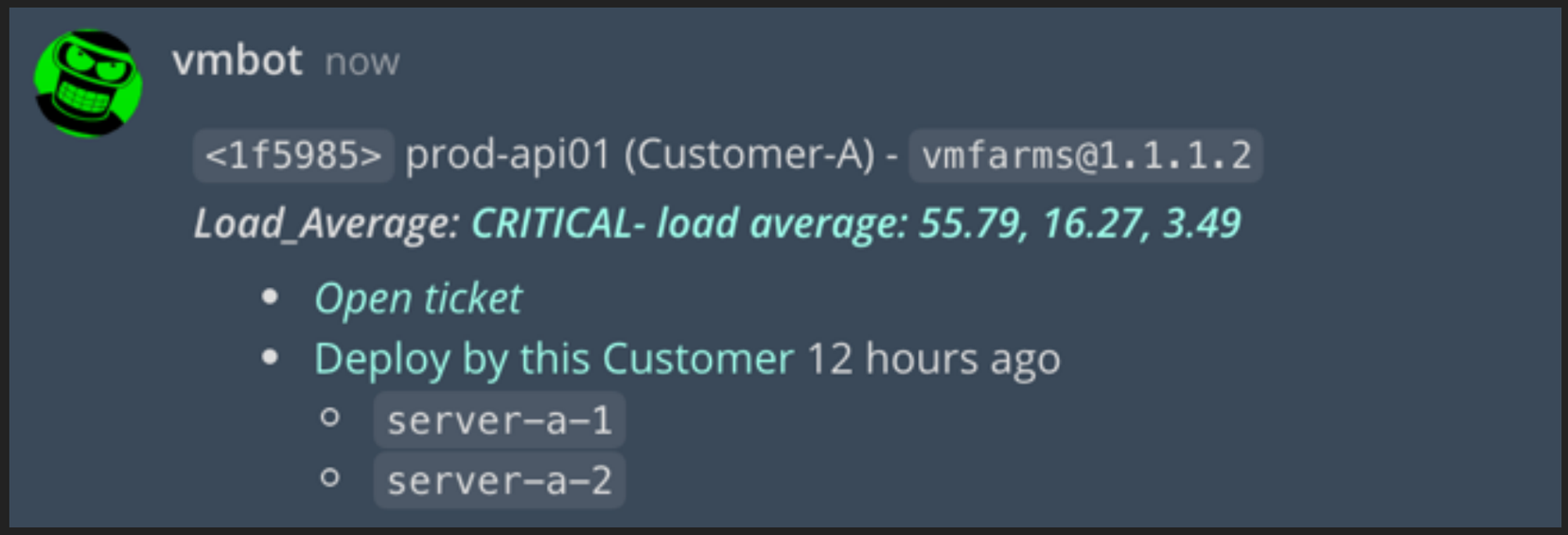
- Status: `HTTP TIMEOUT` *(down 1 minute since Dec 16th 15, 20:05:00)*
- DNS : `1.1.1.1` *(properly resolves)*
- Open ticket | Outage Report | Server Conf
- Deploy by this Customer 12 hours ago
  - `server-a-1`
  - `server-a-2`

LARGE SPIKE IN TRAFFIC

Traffic was up about **1000%**.



Load on the API servers was through the roof!



WAS THIS AN ATTACK?

- Key decision point:

  Should we defend or scale?

- Two very different paths.

  It’s important to make the right choice to avoid wasting time.

TRAFFIC ANALYSIS

- Hopped onto the load balancers and looked at the **top source IPs** to determine if there was a pattern.

```
$ tail -n 5000 haproxy.log | awk '{print $1}' | sort | uniq -c | sort -nr | head
    461 1.1.1.1
    356 1.1.1.2
    317 1.1.1.3
    308 1.1.1.4
    292 1.1.1.5
    239 1.1.1.6
    188 1.1.1.7
    177 1.1.1.8
    169 1.1.1.9
    169 1.1.1.10
```

WHOIS

- Performed a series of `whois` lookups of the **top 10 IPs**.

BRAZIL!

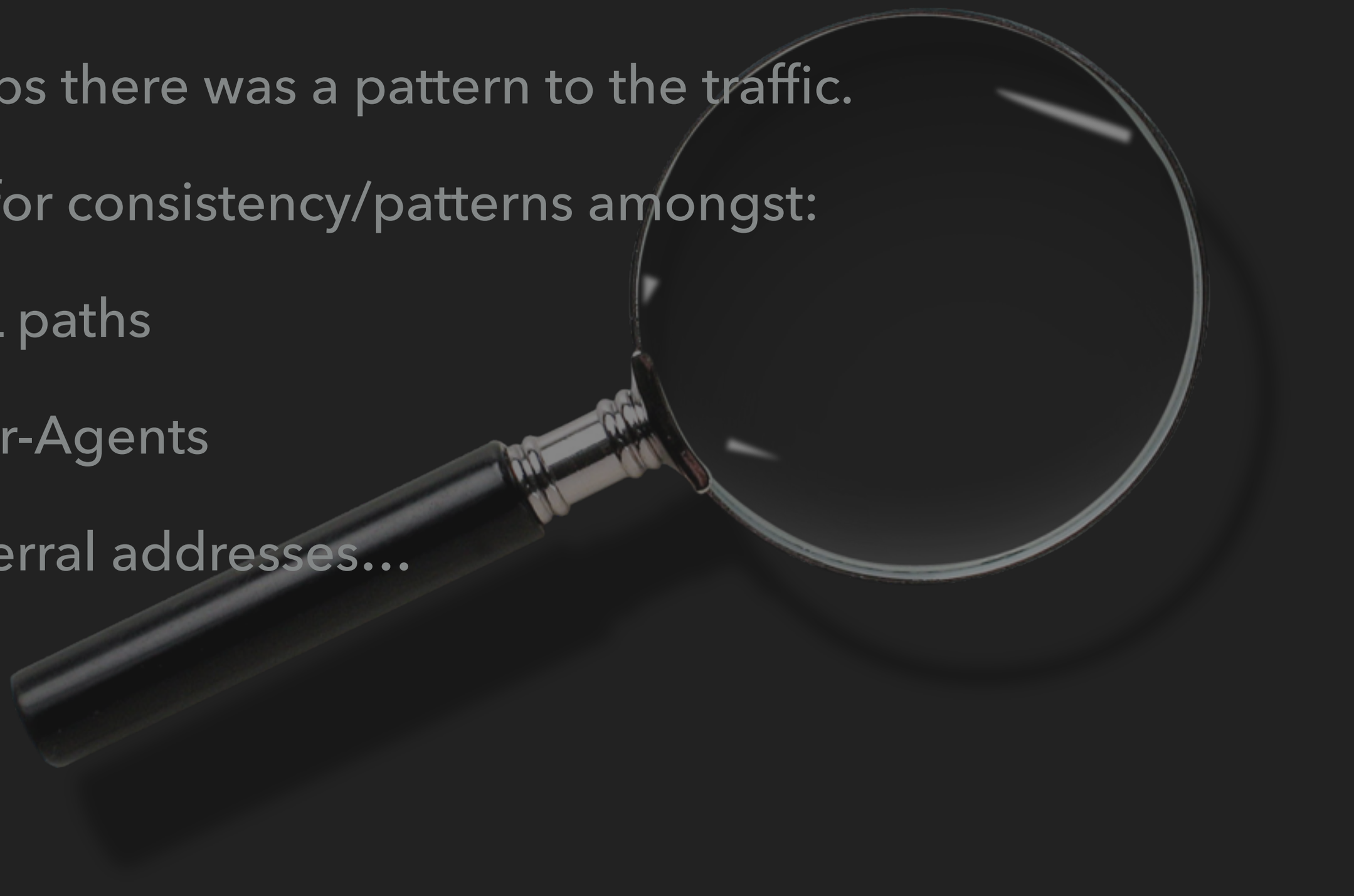
TOP ATTACKER

- According to Akamai, in 2014, **Brazil was ranked #7** in the world for source attack traffic (DDoS, exploits, etc...).
  - *Other reports place them as #2.*
- This matches our experience.
  - Based on our own observations of hacks and exploits, **Brazil is ranked in the top 5**.


LOOKING
SUSPICIOUS

HUNTING FOR PATTERNS

- Perhaps there was a pattern to the traffic.
- Look for consistency/patterns amongst:
  - URL paths
  - User-Agents
  - Referral addresses…



SITE OUTAGE REPORTED

vmbot 10 seconds ago

SITE OUTAGE FOR Customer-B!

API - https://api.customer-b.com/health-check is DOWN

- Status: `HTTP TIMEOUT` *(down 1 minute since Dec 16th 15, 20:10:00)*
- DNS : `2.1.1.1` *(properly resolves)*
- Open ticket | Outage Report | Server Conf
- Deploy by this Customer 3 hours ago
  - `server-b-1`
  - `server-b-2`

THINGS STARTED TO CLICK – SIMILAR SPACE!

- Both customers were in the **security/VPN space**.
- *Same pattern:*
  - High traffic, spread out over many IPs.
  - High load on the API servers.
  - **IPs coming from Brazil as well!**
- Where would you look to find out what's going on?

TOOK TO TWITTER

- Searched "`brazil`", immediately there were a flood of tweets:

  > "BIG BROTHER en ACCION en Brazil!!! Justicia ordena bloquear WhatsApp durante 48 horas en Brasil"

  BIG BROTHER in action in Brazil!!! Justice ordered block WhatsApp for 48 hours in Brazil

  > "El Gobierno de #Brazil ordenó bloquear #WhatsApp durante dos días!! Creo que muchos estarán en la carcel el fin de semana."

  The government ordered #Brazil #WhatsApp block for two days!! I think many will be in jail over the weekend.

IT WAS TRUE

Brazil is blocking access to WhatsApp for 48 hours

By Rich McCormick on December 16, 2015 10:52 pm Email

BRAZIL'S ROCKY RELATIONSHIP WITH WHATSAPP

- Officially, the Brazilian government claims the block was put in place due to WhatsApp's non-compliance with handing over user data which is **encrypted**.
- They know that WhatsApp is unable to retrieve such data.
- Unofficially, Brazilian telecom companies are angry at their diminishing profits as more and more users communicate over WhatsApp.

BACKGROUND ON BRAZIL AND WHATSAPP

- Apparently **93% of Brazil's** internet population uses WhatsApp.
  - Doctors use it to communicate with their patients. Businessmen use it to conduct transactions. People who cannot afford a phone plan embrace its free services.
- With an Internet population of 100 million, that's **93 million users**!
  (50% of the entire population of Brazil).
- **It is the single most used app in the country.**

“Me without WhatsApp”

TOO LEGIT

- Strong evidence this was legitimate traffic.
- Time to scale up!
- Started building out API servers in a mad frenzy.
- **Traffic kept soaring.**

BY MIDNIGHT, THINGS WERE STABLE AGAIN!

OR SO WE THOUGHT . . .

"PagerDuty Alert. You have 2 triggered incidents..."

5:30AM

- Both sites reported as down again!
- Traffic had spiked again, **this time much higher than the previous peak**.
- Brazil was waking up!
- One customer was already 5x their original size.
- **Time to scale up again!**

OTHER SYSTEMS BUCKLING

- Able to stabilize things fairly quickly.
- However, a few hours later, the API server load started to ease up?
  - *Traffic was still climbing, but load was decreasing.*
- **Sites went back down.**
  - Something else was up.

HAPROXY AND SSL

- HAProxy v1.5 added support for SSL termination (yay!).
- Noticed large connection times **during SSL handshake**.

```
$ cat ~/conn_times.txt
time_namelookup    : %{time_namelookup}\n
time_connect       : %{time_connect}\n
time_appconnect    : %{time_appconnect}\n
time_pretransfer   : %{time_pretransfer}\n
time_redirect      : %{time_redirect}\n
time_starttransfer : %{time_starttransfer}\n
                     ----------\n
        time_total : %{time_total}\n
```

```
$ curl -w @curl-format.txt -si https://customer-a.com | grep time_
time_namelookup    : 0.005
time_connect       : 0.015
time_appconnect    : 0.930  # << What is going on here?
time_pretransfer   : 0.930
time_redirect      : 0.000
time_starttransfer : 1.533
        time_total : 1.533
```

APPCONNECT

- “The time it took from the start until the SSL connect/handshake with the remote host was completed.”

HAPROXY IS SINGLE THREADED

```
$ uptime
 11:09:07 up 134 days,  7:57,  1 user,  load average: 1.17, 1.37, 1.39
```

- Load was at ~ 1.
  - Under normal circumstances, this would be OK…
  - Until you realize that HAProxy is **single process and single threaded by default!**

LOGJAM!

DO YOU REMEMBER THIS?

DO YOU REMEMBER LOGJAM?

- Was the name of a TLS exploit for a man-in-the-middle (MITM) attack.
  - Did you know that the US Government mandated weaker encryption in the 90s?
- We are still paying for it today.

2048-BITS IS EXPENSIVE

- To curb the effects of Logjam, it is recommended to increase the size of your Diffie-Hellman parameters (DH-Params) to **2048-bits**.
  - *This is very computationally expensive.*
- Our tests have shown that cutting DH-Params to 1024-bits **reduces CPU load by 50%!**

NEED MORE PROXIES!

- Started to build out more **proxies**.
- Setup DNS round-robin as a quick way to scale.
- **Had to quadruple the number of proxies before things were stable again.**

10:30AM

AND THEN IT STOPPED.

TRAFFIC CALMED

- Load subsided, traffic waned, alerts cleared.
- What just happened?
- Took to Twitter…

Brazil

Judge lifts WhatsApp ban in Brazil after ruling block punished users unfairly

Messaging service used by millions of Brazilians was meant to be blocked for 48 hours to pressure app's owner Facebook to cooperate in criminal investigation

WE NEVER SAW THE TRUE PEAK

- It was interesting to see the flurry of users circumventing the block with VPN.
- Did not see the full brunt of traffic.
- Out of curiosity, wanted to see if there was a way to figure out what the true traffic looked like.

PC CONECTADO

- In 2003, the Brazilian government launched an initiative to offer low-cost tax-free computers to anyone who wanted it.
- They mandated the use of **Linux** and **Open Source Software**, and outright rejected Microsoft's bid for OS of choice.
- This included all government ministries and state-owned systems.
- This move was widely publicized in the media.

THINK ABOUT THIS FOR A MINUTE.

LINUX AND OSS

- Linux has come a long way, but it *still* requires some **technical know-how to operate**.
- Unlike Windows and Mac, *you usually have to pop open the hood and tinker.*
- After more than a decade of this program, the result is a **highly technical population**.
  - *We've observed this effect directly.*

PUTTING IT TOGETHER

- Government enables the people by giving them **technical knowledge.**
- Then tries to block access to the **single most used app in the country.**
- **No wonder these VPN services were getting hit hard!**
- This may also explain why they are ranked #7 for source attack traffic.

LESSONS LEARNED

- **Multi-core HAProxy FTW!**
  - Careful with using features that depend on shared memory.
- **Twitter is an invaluable resource for getting up-to-date information on current events.**
  - *We may have gone the other route and blocked legitimate traffic.*

AND FINALLY...

GOVERNMENT CENSORSHIP AND BLOCKADES RARELY WORK,ESPECIALLY WHEN YOU ARM YOUR PEOPLE WITH KNOWLEDGE.

By Hany Fahim
Founder and CEO
@iHandroid

VM FARMS
@vmfarms

QUESTIONS? (PSST.. WE'RE HIRING!)

THANKS!