## Background

In an effort to fight for the rights of digital consumers throughout South America, the hacktivist group Anonymous has launched OpOperadoras,[i] coordinated cyber assault against Brazilian telecommunication companies in response to a fixed broadband provision that would ban unlimited data plans in Brazil. [ii] The provision has enraged millions of Internet users[iii] throughout South America. The first organization struck was ANATEL – The National Telecommunications Agency. ANATEL suffered a large-scale DDoS attack that reached 40Gbps[iv] of traffic generated via international bots, in parallel to SQL injections that resulted in extraction of confidential information[v] regarding executives at various telecommunication companies. [vi] Hackers have posted a sample of the database on Ghostbin and are threating to release more data.

## Attack Analysis

This attack was unique as perpetrators executed it using the smoke screen technique. To create confusion and misdirection, attackers overwhelm the security personnel with irrelevant traffic, slowing down unrelated applications or filling logs with irrelevant data. While the security team is kept busy, the primary attack is launched. This time – various DDoS bursts of 4-40Gbps as well as SQL injections to infiltrate servers and extract sensitive data.

```
ANATEL - National Telecommunications Agency
Hacked & exposed

#Liberdade #Privacidade

[+] Civil Marco Internet
[+] Abuse operators
[+] Consumption limit in the fixed broadband
[+] Neglect Anatel

[+] Anonymous
[+] OpOperadoras

--------------------------------------------------------------------------------

MESSAGE TO ANATEL

We want to leave a message to the illustrious Mr. (talk shit) President of Anatel, John Rao: This is a small sample of what we can do.
The Anatel's site was hacked and we have your database in our hands. For now, let's just expose some of this information to show
we're not here to play. You may have noticed that the Anatel site also was down for a while due to DoS attacks
service (DDoS). Well, we are here to REQUIRE a decent internet, and that Anatel covers a fair service operators. Anatel must defend
consumer demand and improvements in service and infrastructure operators, as already paid dearly for a poor quality service.

"People who spend a lot of playing online internet criticizes president of Anatel"

How about playing our game, huh !?
Let the games begin...

NOTICE:

Operators, get ready, because you will be the next victims!
GVT / Live, Hi, Claro, Tim, .NET and all the others, listen: You are in our sights!

Because, after all, the boss on the Internet are we!
```

**Figure 1: Attackers respond to ANATEL's president comment "internet users spending too much time playing games"**

The attackers published a DDoS tutorial for participants[vii], explaining how to achieve a Denial-of-Service state using low and slow attacks (hack tools include: LOIC, Web Loic, SlowLoris and PyLoris).

## Targets

- www.vivo.com.br
- www.tim.com.br
- www.oi.com.br
- www.claro.com.br
- www.netcombo.com.br
- www.gvt.com.br
- www.anatel.gov.br

## Communication Channels

**Video -** https://youtu.be/gJFTrG2NzaE

**IRC -** https://kiwiirc.com/client/irc.anonymousbrasil.com/OpOperadoras

**Tutorials Suggested via Op**

- What to do with exposed? - http://pastebin.com/tv7BZjE8
- Only Privacy - http://pastebin.com/BrAnV7Bz

## How to Identify a Smoke-Screen Attack?

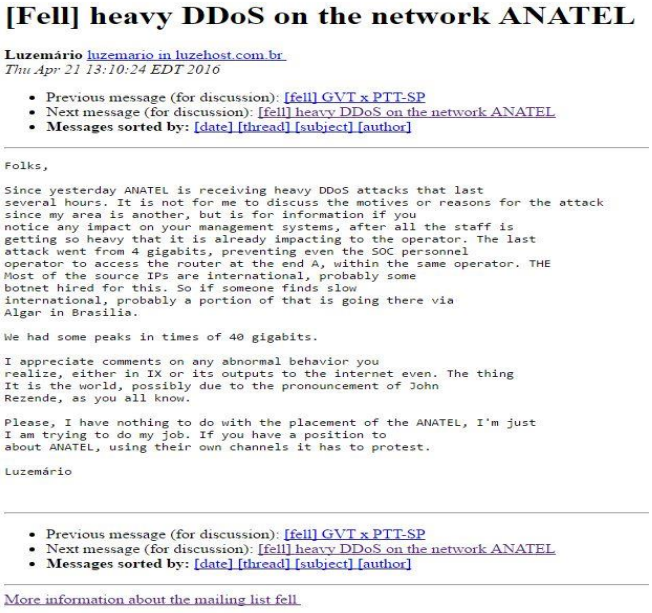
If an anomaly is identified, review the following questions:

- What is the intent?
- Is it designed to disrupt the network?
- Is the infrastructure/data center designed to handle it?
- Is it a decoy?

Then take the following steps:

1. Check logs and perhaps filter out vectors once they've been ruled them out.
2. Check additional assets and collaborate with other departments throughout the organization to ensure that nothing else appears wrong.
3. Tune the Web Application Firewall (WAF), as it can help prevent data theft and manipulation of sensitive corporate data in addition to safeguarding customer information.
4. Combining WAF with an on-premise detection and behavioral analysis solution lets you mitigate smokescreen attacks while protecting customer data.

It is absolutely critical that organizations adopt layered security models to protect their websites and databases. DDoS mitigation appliances can protect you from the smoke screens. Firewalls and a strong perimeter can secure access. Make use of the tools and forensic data that you have available. Remember: things aren't always what they seem and a smoke screen attack just might be real intent of obvious network events.



**[Fell] heavy DDoS on the network ANATEL**

**Luzemário** luzemario in luzehost.com.br
*Thu Apr 21 13:10:24 EDT 2016*

- Previous message (for discussion): [fell] GVT x PTT-SP
- Next message (for discussion): [fell] heavy DDoS on the network ANATEL
- **Messages sorted by:** [date] [thread] [subject] [author]

Folks,

Since yesterday ANATEL is receiving heavy DDoS attacks that last
several hours. It is not for me to discuss the motives or reasons for the attack
since my area is another, but is for information if you
notice any impact on your management systems, after all the staff is
getting so heavy that it is already impacting to the operator. The last
attack went from 4 gigabits, preventing even the SOC personnel
operator to access the router at the end A, within the same operator. THE
Most of the source IPs are international, probably some
botnet hired for this. So if someone finds slow
international, probably a portion of that is going there via
Algar in Brasilia.

We had some peaks in times of 40 gigabits.

I appreciate comments on any abnormal behavior you
realize, either in IX or its outputs to the internet even. The thing
It is the world, possibly due to the pronouncement of John
Rezende, as you all know.

Please, I have nothing to do with the placement of the ANATEL, I'm just
I am trying to do my job. If you have a position to
about ANATEL, using their own channels it has to protest.

Luzemário

- Previous message (for discussion): [fell] GVT x PTT-SP
- Next message (for discussion): [fell] heavy DDoS on the network ANATEL
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the mailing list fell

**Figure 2: ANATEL's acknowledges the abnormal behavior followed by a DDoS attack**

## Effective DDoS Protection Elements:

- A hybrid solution that combines on-premise detection and mitigation with cloud-based protection for volumetric attacks. It provides quick detection, immediate mitigation and prevents internet pipe saturation.
- Solution must distinguish between legitimate and malicious traffic, protect the SLA and block the attack.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.

## Effective Web Application Protection Elements

(against web intrusions, defacement and data leakage):

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time.
- Automatic and real time generation of policies to protect from zero-day, unknown attacks.
- Shortest time from deployment to a full coverage of OWASP Top-10.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report the most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

## Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

## Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://twitter.com/anonopsbrazil
[ii] https://www.facebook.com/Anonopsbrazil/photos/a.355615344512198.79166.244582758948791/1069977439742648/
[iii] http://www.zdnet.com/article/brazilians-protest-against-fixed-broadband-data-cap/
[iv] https://eng.registro.br/pipermail/caiu/2016-April/049653.html
[v] https://ghostbin.com/paste/32jjr/raw
[vi] http://pastebin.com/RhvyFmvv
[vii] http://pastebin.com/dkEMzJsr