nic.br cgi.br

cert.br

FIRST Technical Colloquium
September 26th, 2016
San José, CR

Lessons Learned from the Rio2016 Summer Olympic Games

Lucimara Desiderá, M.Sc.
lucimara@cert.br

cert.br nic.br cgi.br

International Events in Brazil

2012 – Rio+20

2013 – FIFA Confederations Cup

World Youth Day 2013 (including the Pope’s visit)

2014 – FIFA 2014 World Cup

2016 – Summer Olympics

Cooperation

Similar to that of the World Cup, plus the Rio2016 team

- **Rio2016 CSIRT**
  - 24x7 dedicated team for the event networks
  - A Cyber Security Core Team, with members from several organizations
- **CDCiber**
  - physical presence at the Command&Control centers with focus on Ministry of Defense’s interest networks and critical infrastructure
- **CTIR Gov – Brazilian Federal Public Administration CSIRT**
  - focus on incidents targeting government sites
- **CERT.br**
  - facilitate communication and coordination
  - situational awareness and monitoring
    - including honeypots, IRC, Twitter, etc

CERT.br/NIC.br activities

Help in identifying

- possible threats and attacks
- infrastructure and processes needs

Focused monitoring of incidents and other data sources

- incident notifications
- data feeds (CERT.br Distributed Honeypots, Team Cymru, ShadowServer, Anti-Botnet operations)
- public sources of information (Twitter, Facebook, IRC, C&C, defacements)

Communication and coordination with other actors

- previously established network of contacts, especially CSIRTs
- meetings and cooperation with Telcos, ISPs and hosting companies
- announcement of the incident handling plans to international partners

Additionally

- iNOC-DBA VoIP network maintained by NIC.br
- Delivered training for incident handling teams
    - Especial classes for CDCiber and Rio2016

Announcement of the Rio2016 Plans to FIRST teams

Date: Mon, 4 Jul 2016 21:22:58 -0300
From: Cristine Hoepers <cristine@cert.br>
To: first-teams@first.org
Subject: Rio2016 Olympic Games - Incident Handling Contacts

Dear FIRST Teams,
[...]
As part of the coordinated efforts to prevent and respond to incidents related to the games we'll have 4 teams working in cooperation:

- Rio2016 CSIRT <csirt@rio2016.com> - 24/7 team, onsite at the games, that will handle incidents related to the games infrastructure (they are also handling all cases involving phishing of the Games' Oficial sites and sites selling fake tickets).

- CERT.br <cert@cert.br> - will coordinate and facilitate communication with external parties, situational awareness and network monitoring. You can copy CERT.br in any notification, this will help situational awareness and will allow us to pull in anyone else needed for coordination.

- CTIR Gov <ctir@ctir.gov.br> - will handle all incidents targetted to .gov.br networks.

- CDCiber <abuse@cdciber.eb.mil.br> - 24/7 personnel at the Games' Security Command and Control Centers, with special focus on national critical infrastructure.

[...]

World Cup 2014 vs. Rio2016: **Main Differences**

2014 World Cup

- Almost no engagement from FIFA or the local committee on the plans
- Lack of focal point for notifications
- Public demonstrations and intense hacktivism
- DDoS peak: 4Gbps

Rio2016

- Full commitment and engagement from the local Organizing Committee
- Rio2016 CSIRT as focal point and 24x7 operation
- Reduced street demonstrations and hacktivism with less impact
- DDoS peak: 300Gbps to 500Gbps

Some observations and anecdotes

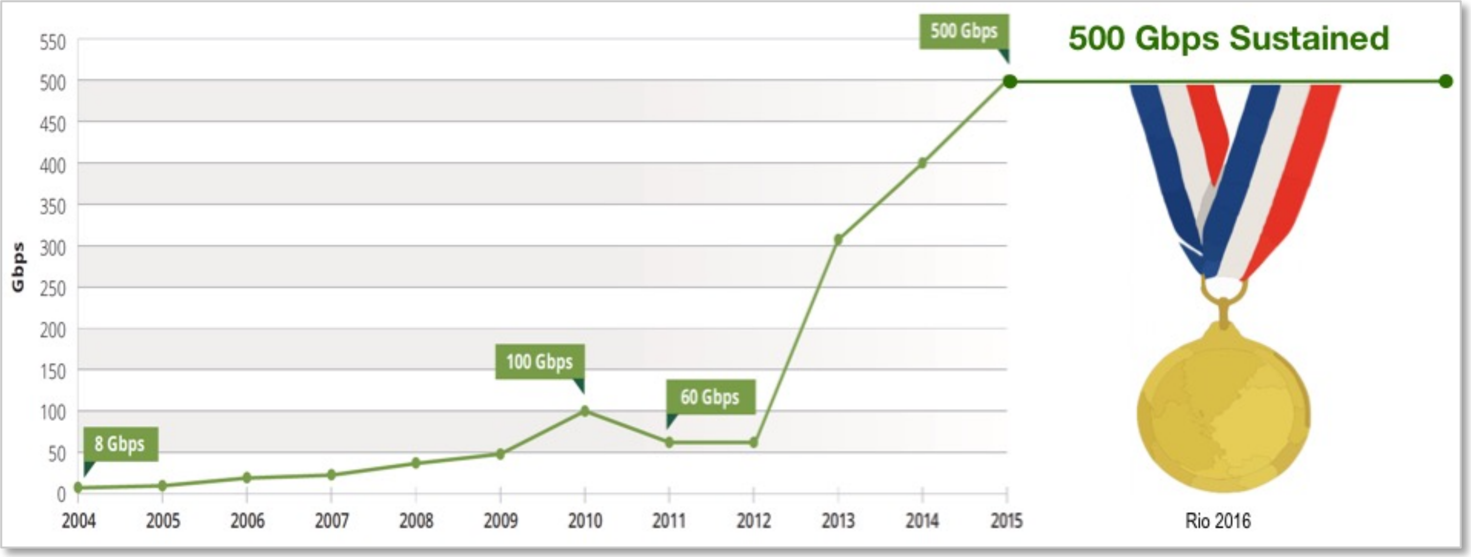
cert.br nic.br cgi.br

Incident Categories Observed

- Financial fraud attempt using the games to attract victims
- Fake websites for unauthorized ticket selling
- Defacements to protest against the games
  - much less than during the 2014 World Cup
- Supposedly data leaks from government websites and organizations related to the games
  - in some cases data was publicly available
  - in some cases was not possible to verify whether the data was really confidential or not
- DDoS against government and sponsors’ websites

About incidents with media coverage

- WADA (Anti doping agency) data leak
  - publically confirmed by the agency[1] pointing to a spear phishing that led to the compromise of credentials as the root cause
  - WADA infrastructure is totally independent from the Rio2016
- DDoS attacks of 540Gbps, according to Arbor ASERT
  - Published the article "*Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks!*"[2], with this graphic:



[1] https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group
[2] https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/

Attack commands seen at C&C: **Before the beginning of the games** (Tests?)

```
2016-07-12 15:41:59 CC: xx.xxx.xx.xxx:23,
     cmd: "!* HOLD [victim1] 443 300"

2016-07-12 15:43:22 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK“

2016-07-12 15:56:20 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [victim2] 80 60"

2016-07-12 16:00:23 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [victim3] 179 60"

2016-07-12 16:01:25 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK"

2016-07-12 16:02:02 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [victim4] 179 60"

2016-07-12 16:02:39 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK"
```

Attack commands seen at C&C:
During the games

```
2016-08-03 23:37:13 CC: xxx.xxx.x.xxx:23, cmd: ". GETFLOOD
      [victim1*] 80 / 60"
2016-08-03 23:39:21 CC: xxx.xxx.x.xxx:23, cmd: ". POSTFLOOD
      [vvictim*] 80 /?login.php&username=owned 120"

2016-08-06 20:18:58 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [victim3] 179 400"

2016-08-06 20:26:00 CC: xxx.xxx.x.xxx:23, cmd: "!* UDP
      [victim3] 179 500 32 500 10"

2016-08-06 20:27:24 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [victim3] 179 500"

2016-08-06 20:30:10 CC: xxx.xxx.x.xxx:23, cmd: "!* HOLD
      [victim2] 80 500"

2016-08-06 20:31:11 CC: xxx.xxx.x.xxx:23, cmd: "!* TCP
      [victim2] 80 500 32 syn 0 10"

2016-08-06 20:35:31 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [victim2] 80 500"

2016-08-19 14:36:51 CC: xx.xx.xxx.xxx:23, cmd: "! GETFLOOD
      [victim1*] / 80 30"
```

Rio2016 CSIRT
Point of View

cert.br nic.br cgi.br

Lessons Learned (1/3)

- Cooperation is everything
  - information exchange
  - task division (well defined responsibilities)
  - it’s possible to have competing vendors working together toward a major goal

Lessons Learned (2/3)

- **Documentation is extremely necessary**
  - centralized (wiki)
  - the tool does not matter
  - don’t forget your processes

Lessons Learned (3/3)

- **Simulations and training (non stop)**
  - wargames and rehearsals (live)
  - training
  - awareness
  - make yourself known to your constituency and partners

Obrigada!
Thank you!
¡Gracias!

www.cert.br

@ lucimara@cert.br   @certbr

September 26th, 2016

nic.br cgi.br

www.nic.br | www.cgi.br