nic.br cgi.br cert.br

FIRST/TF-CSIRT Technical Colloquium
January 25th – 27th, 2016
Prague, CZ

TLP:White

Incident Handling in High Profile International Events: Lessons Learned and the Road Ahead

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

cert.br nic.br cgi.br

International Events in Brazil

2012 – Rio+20

RIO+20
United Nations
Conference on
Sustainable
Development

BRASIL 2013
FIFA
CONFEDERATIONS CUP

2013 – FIFA Confederations Cup

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

WYD
Rio2013

2014

2014 – FIFA 2014 World Cup

FIFA WORLD CUP
Brasil

Rio2016

Rio2016
PARALYMPIC GAMES

2016 – Summer Olympics

Facts to Consider

- **These events attract the attention of the world**
  - **and of the attackers as well**
  - **dates and times are well known**
- **Media coverage of attacks is a given**
- **Incidents impact the country’s image**
- **The Internet is a critical infrastructure for**
  - **TV transmission, webcast or other forms of remote participation**
  - **journalists’ communication**
  - **communication of all events’ coordination entities**
- **But the Internet does not change because of all this**
  - **we still rely on ISPs, vendors, and the events organizers’ own infrastructures, policies and partners**

Brazilian Organizational Structure

Special Secretariat for Security of Major Events

- to coordinate all security efforts for major events up until 2016 paralympic games
- part of the Ministry of Justice (MJ)
- defined that the protection of the "cyberspace" would be the mission of the Ministry of Defense (MD) Cyber Defense Center (CDCiber)

Real life is more complex

- the owner of the asset is the only one that can actually secure the asset and respond to any incident
- the international organizations are not really open for information sharing
- the events' infrastructures are not the only targets
  - [h]ac[k]tivism changed the targets

How Incident Handling Coordination Evolved

Leverage what each organization can do best

- **CDCiber changed its own mission from “protecting” to “integrating and coordinating” with all parties**
  - its focus is incident detection and coordination in the Government Security Command&Control centers
  - online intelligence gathering for physical security
- **CTIR Gov – Brazilian Federal Public Administration CSIRT**
  - focus on incidents targeting government sites
- **CERT.br**
  - training for all CDCiber personnel stationed at the CDCiber C&C
  - international coordination, takedowns
  - facilitate communication and coordination
  - situational awareness and monitoring
    - including honeypots, IRC, twitter, etc

Attacks Seen During the World Cup

“*Hacktivism*” coordinated with street demonstrations

Most targets were not related to the World Cup

- **any “`gov.br`”, universities, sponsors and political parties**
    - **information leak**
    - **defacements**
    - **DDoS using amplification (Chargen, DNS, SNMP)**
        - reports of 4Gbps peaks
- **some targets not even related to Brasil or the World Cup**
    - **as the “`elections.ny.gov`” website**
- **pictures of the stadiums wi-fi passwords**
- **phishings related to FIFA, midia outlets and the Brazilian Soccer Federation**

Midia coverage of the attacks before the event

- **this was the most intense period of attacks**

Lessons Learned: **CDCiber Perspective**

Preparation, including risk analysis, asset mapping and intelligence gathering was essential and needs to be enhanced

To increase the collaborative action and the trust relationships among the organizations is not only relevant, it is essential

Some highlights of big impact events

- **Attacks to the Army Website**
- **Federal Police twitter account compromised**
- **Leak of information from the Ministry of Foreign relations**

Source (in Portuguese):
http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf

Lessons Learned:
CTIR Gov Perspective

What worked well: Integration of CDCiber, CERT.br and CTIR Gov Teams

- Team members with technical readiness, that know each other, have a trusted relationship and focus on each teams strengths
- Proactivity was key

Some highlights of big impact events

- Government sites were targets of most hacktivism demonstrations, focusing on DDoS, Spear Phishing and leaks
- The social media monitoring performed by CDCiber and CERT.br reduced significantly the incident response time

Source (in Portuguese):
http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CTIR-Gov.pdf

Lessons Learned: **CERT.br Perspective**

Cooperation among CERT.br, CTIR Gov and CDCiber was already big, but was strengthened

- **there was information exchange and task division**

Some highlights of big impact events

- **Work load was even bigger than anticipated**
  - **had to allocate extra people to social network monitoring**
  - **extra hours**
  - **last minute requests from the Federal Police and other organizations**
- **Reaching out to international organizations, sponsors and some ISPs was a challenge**
  - **no clear point of contact**
  - **no information sharing**
    - but requests for "information giving"

Rio2016™

Rio2016™ JOGOS PARALÍMPICOS

27

weeks

Changes for the Olympic Games

The Games are more reliant on technology

Rio2016 is the not for profit local organizing organization

- Fully operational CSIRT, on-site
  - 8x5 since September/2015
  - 24/7 from March to September/2016
  - http://www.cert.br/csirts/brazil/#rio2016-csirt
- Working in coordination with CERT.br, CTIR Gov and CDCiber
- A Cyber Security Core Team, with members from several organizations, is coordinating preparation, risk analysis, incident response plans and exercises

Other coordination and cooperation structures will function in a similar model to that of the 2014 World Cup

Canais de Contato
Contact Information

Rio2016 Computer Security Incident Response Team

csirt@rio2016.com
INOC.DBA: 4230*RIO
Tel: (55) 21 2016-2986

Obrigada!
Thank you!
Děkuji!

www.cert.br

@ lucimara@cert.br   @certbr

January 26th, 2016

nic.br cgi.br

www.nic.br | www.cgi.br