nic.br cgi.br | cert.br

5º Fórum Brasileiro de CSIRTs
23 de setembro de 2016
São Paulo, SP

Atuação do CERT.br no Tratamento de Incidentes na Rio 2016

Cristine Hoepers
cristine@cert.br

cert.br nic.br cgi.br

Cooperação:
Rio 2016, CERT.br, CTIR Gov e CDCiber

Planejamento similar ao da Copa 2014

Adição do Rio2016 CSIRT como parceiro

Divisão de tarefas

- **Rio2016 CSIRT : time 24x7 para as redes dos jogos**
- **CDCiber: atuação presencial nos Centros de Comando e Controle e foco em redes do interesse do MD e infraestruturas críticas**
- **CTIR Gov: foco nos ataques às redes do Governo**
- **CERT.br: facilitar a comunicação e coordenação com outros atores e auxiliar no acompanhamento de ameças**

Detalhes da Atuação CERT.br/NIC.br

Ajuda na identificação de

- possíveis ameaças e cenários de ataques
- necessidades de infraestrutura

Monitoramento extra de incidentes e fontes de dados sobre ataques

- notificações de incidentes
- *feeds* de dados (*Honeypots* Distribuídos do CERT.br, Team Cymru, ShadowServer, Operações Anti-Botnet)
- fontes públicas de informação (Twitter, Facebook, IRC, C&C, *defacements*)

Comunicação e coordenação com outros atores

- via a rede de contatos já estabelecida, principalmente CSIRTs
- reunião e grupo de cooperação com operadoras e empresas de *hosting*
- divulgação do planejamento nacional para parceiros internacionais

Adicionalmente

- Rede iNOC-DBA mantida pelo NIC.br
- Treinamento das equipes de tratamento de incidentes
  - Turmas especiais para CDCiber e Rio 2016

Divulgação do Rio2016 CSIRT:
Palestras e Reuniões

Pelo Rio2016 CSIRT

- **4º Fórum Brasileiro de CSIRTs**

Pelo CERT.br

- **LAC-CSIRTs Bogotá, setembro/2015**
- **FIRST TC Praga / TF-CSIRTs Meeting, Janeiro/2016**

Mensagem ao FIRST

```
Date: Mon, 4 Jul 2016 21:22:58 -0300
From: Cristine Hoepers <cristine@cert.br>
To: first-teams@first.org
Subject: Rio 2016 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.
[...]
```

Copa 2014 vs. Rio 2016: **Principais Diferenças**

Copa 2014

- Processo quase não envolveu a FIFA ou Comitê local de organização
- Sem ponto de contato para notificar incidentes envolvendo a infraestrutura dos jogos
- Manifestações de rua e *hacktivismo* intensos e com grande impacto
- Pico de DDoS reportado: 4Gbps

Rio 2016

- Comprometimento e envolvimento total do Comitê Organizador local
- Rio2016 CSIRT como ponto focal, com funcionamento 24x7
- Manifestações reduzidas, *hacktivismo* presente, mas sem tanto impacto
- Pico de DDoS: entre 300Gbps e 500Gbps

Categorias de Incidentes

cert.br nic.br cgi.br

Categorias de Incidentes Observados

- Tentativas de fraudes financeiras usando o nome dos Jogos como atrativo para infectar vítimas
- *Sites* com vendas não autorizadas de ingressos
- Desfiguração de *sites* com mensagens de protesto contra os Jogos
  - em menor número que na Copa 2014
- Supostos vazamentos de dados de *sites* de governo e de entidades envolvidas com os jogos
  - alguns dados eram públicos
  - outros dados não foi possível verificar se eram confidenciais ou se foram forjados
- Ataques Distribuídos de Negação de Serviço (DDoS) contra *sites* de governo e contra patrocinadores

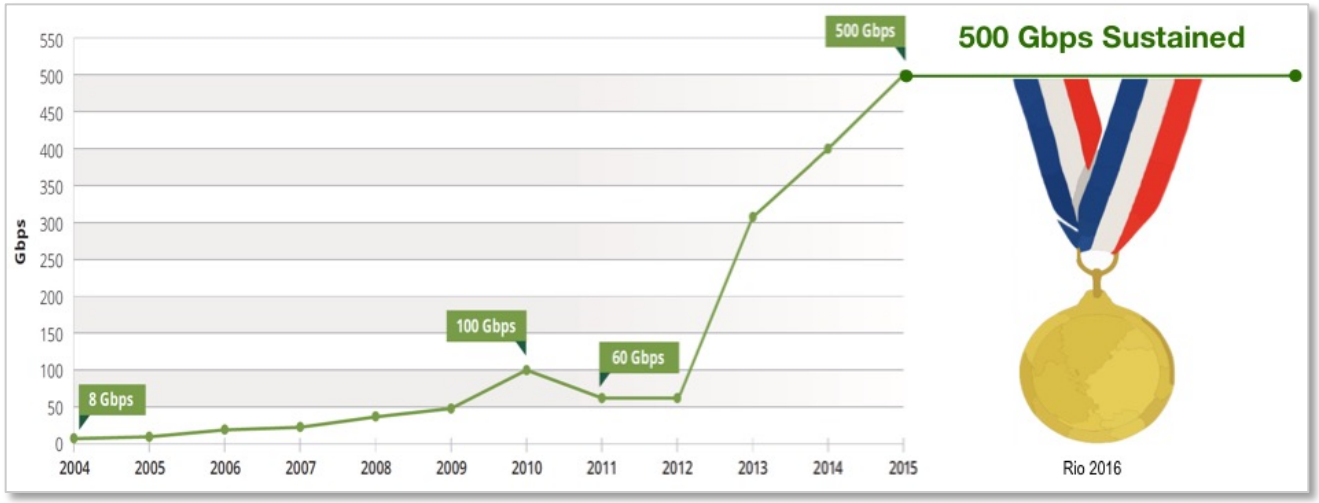
Sobre fatos divulgados na mídia

Vazamento de dados da Agência Mundial Antidoping (WADA)

- confirmado publicamente pela agência[1], apontando a causa como uma mensagem direcionada de *phishing* que levou ao comprometimento de credenciais
- infraestrutura da WADA é independente dos Jogos Rio2016

Ataques DDoS de 540Gbps, segundo Arbor ASERT

- Publicou o artigo entitulado "*Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks!*"[2], que continha este gráfico:



[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/

Comandos de Ataques DDoS vistos em C&C: **Antes do Início dos Jogos** (Testes?)

```
2016-07-12 15:41:59 CC: xx.xxx.xx.xxx:23,
     cmd: "!* HOLD [vitima1] 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 [vitima2] 80 60"

2016-07-12 16:00:23 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [vitima3] 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 [vitima4] 179 60"

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

Comandos de Ataques DDoS vistos em C&C:
Durante os Jogos

```
2016-08-03 23:37:13 CC: xxx.xxx.x.xxx:23, cmd: ". GETFLOOD
      [vitima1*] 80 / 60"
2016-08-03 23:39:21 CC: xxx.xxx.x.xxx:23, cmd: ". POSTFLOOD
      [vitima1*] 80 /?login.php&username=owned 120"

2016-08-06 20:18:58 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima3] 179 400"

2016-08-06 20:26:00 CC: xxx.xxx.x.xxx:23, cmd: "!* UDP
      [vitima3] 179 500 32 500 10"

2016-08-06 20:27:24 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima3] 179 500"

2016-08-06 20:30:10 CC: xxx.xxx.x.xxx:23, cmd: "!* HOLD
      [vitima2] 80 500"

2016-08-06 20:31:11 CC: xxx.xxx.x.xxx:23, cmd: "!* TCP
      [vitima2] 80 500 32 syn 0 10"

2016-08-06 20:35:31 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima2] 80 500"

2016-08-19 14:36:51 CC: xx.xx.xxx.xxx:23, cmd: "! GETFLOOD
      [vitima1*] / 80 30"
```

Obrigada

www.cert.br

cristine@cert.br

@certbr

23 de setembro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br