nic.br cgi.br | cert.br

IX Fórum 10

05 de dezembro de 2016
São Paulo, SP

IoT no cenário atual de ataques DDoS

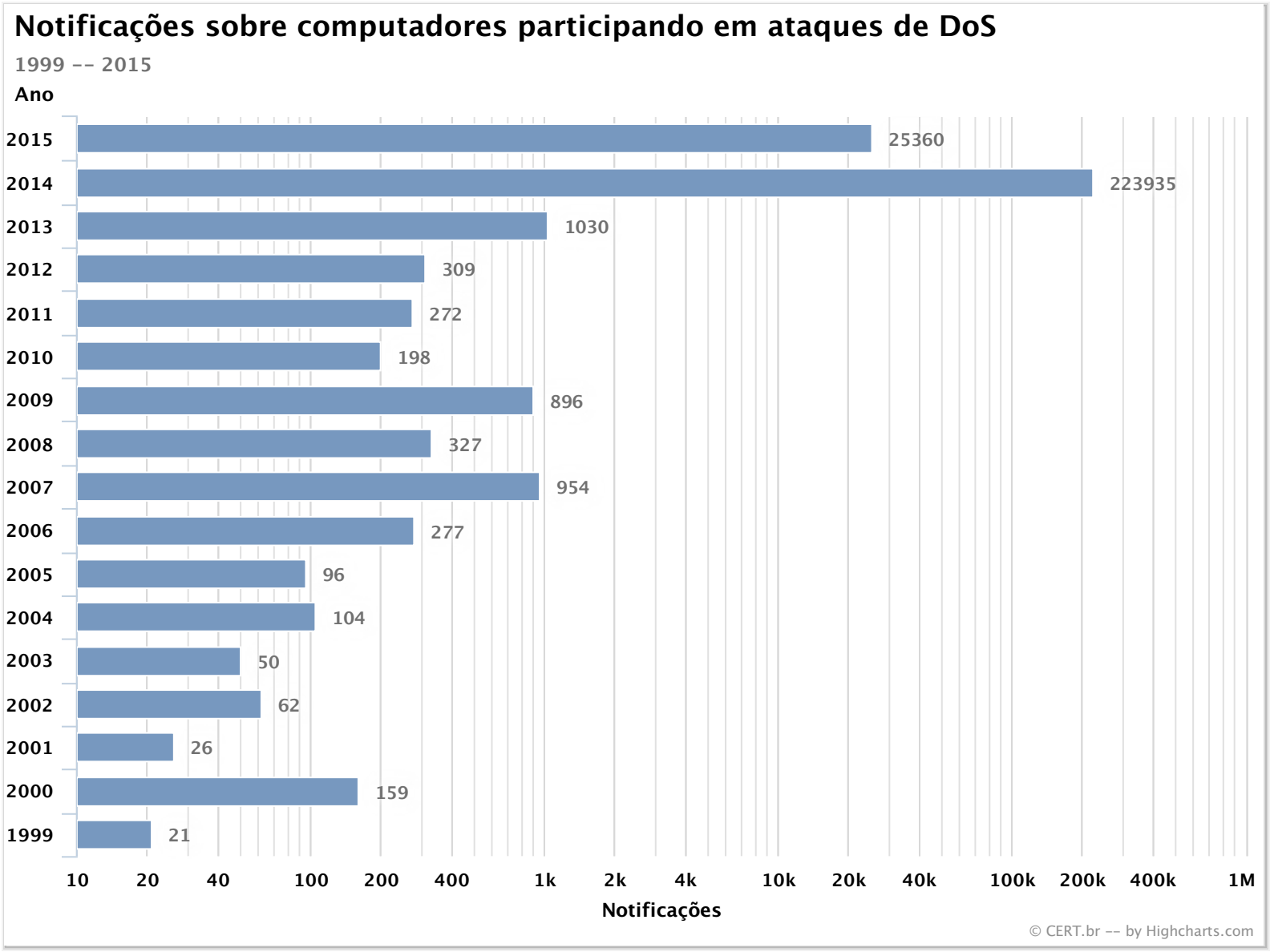
Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

Cenário atual

cert.br nic.br cgi.br

Ataques DDoS – Estatísticas CERT.br



Estatísticas CERT.br

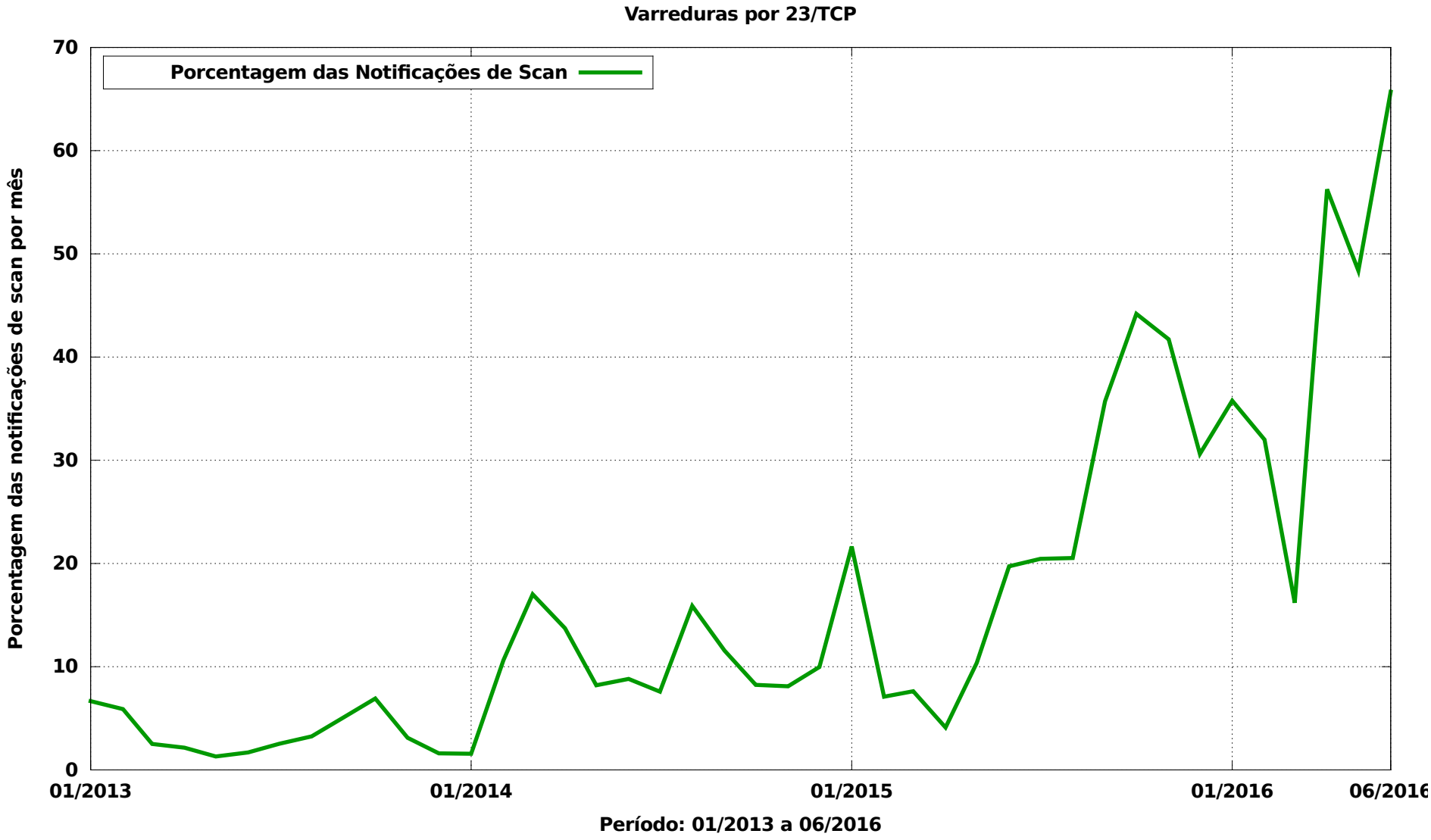
2014

- **Aumento de 217 vezes nas notificações de ataques DDoS**
- **Maior parte das notificações foram ataques DRDoS a partir do Brasil**
  - Serviços UDP permitindo abuso:
    - SNMP, SSDP, DNS recursivo aberto, etc

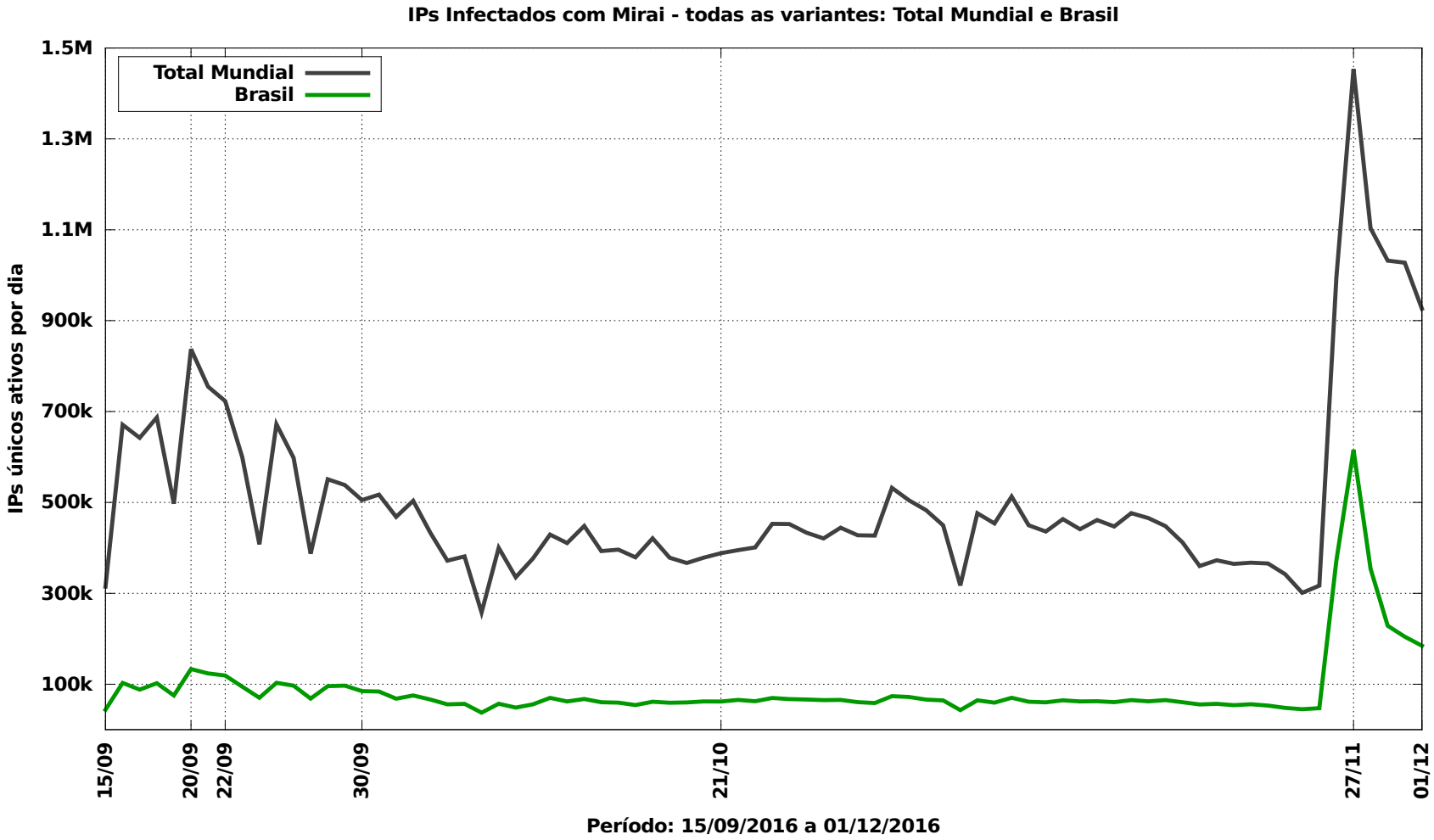
2015

- **Notificação de ataques DDoS 89% menor que 2014**
- ***Scans* por SSDP (1900/UDP)**
  - fator de amplificação de 30.8 vezes
  - 2012: posição 107
  - 2015: posição 18
- **crescimento de *scans* de Telnet (23/TCP)**
  - *scans* visando equipamentos de rede alocados às residências de usuários finais, tais como *modems* ADSL e cabo, roteadores Wi-Fi, etc

Notificações ao CERT.br:
Scans por 23/TCP – 2013 a jun/2016



Dados atualizados dos sensores do CERT.br:
Endereços IP únicos infectados com Mirai



01/08
- Primeira aparição Mirai

20 - 22/09
- Blog Brian Krebs - 620 Gbps

28/09
- OVH - 1Tbps

30/09
- Vazamento código fonte Mirai

21/10
- DynDNS

07/11
- vulnerabilidade TR pública

27/11
- Deutsch Telecom
- 900.000 roteadores banda larga

Características dos ataques recentes (1/2)

- **Foco em dispositivos com versões "enxutas" de Linux**
  - para sistemas embarcados
  - arquiteturas ARM, MIPS, PowerPC, etc
- **Grande base vulnerável**
  - sem gerência remota
  - sem instalação de *patches*
  - autenticação fraca e "*backdoors*" do fabricante
  - configurações padrão de fábrica inseguras
    - senhas padrão, do dia, "para manutenção"
    - serviços como Telnet habilitados
    - serviços UDP permitindo abuso para amplificação
      - SNMP, SSDP, DNS recursivo aberto
- ***Botnets* de dispositivos IoT**
  - CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc

Características dos ataques recentes (2/2)

- **Propagação do *malware***
  - Inicial: via Telnet (23/TCP e 2323/TCP)
    - explorando senhas fracas ou padrão
  - Variantes: via protocolos vulneráveis (7547/TCP e 5555/TCP)
    - TR-069: CPE WAN Management Protocol (CWMP)
      - TR-069 NewNTPServer vulnerability
    - TR-064: LAN-Side DSL CPE Configuration
      - acessível via WAN sem autenticação

- **Qual o limite?**
  - 1.351 câmeras de vídeo ➔ ataque 300 Gbps (sem amplificação) *
  - 1.4M de equipamentos com Mirai ➔ X (sem amplificação)
  - 1.4M de equipamentos com Mirai ➔ Y (com amplificação)

*** http://www.lacnic.net/web/eventos/lacnic25-agenda-lacsec#viernes**

Desafios para Melhorar o Cenário

cert.br nic.br cgi.br

Nos Fabricantes, Velhos Problemas (1/2)

- **Preocupação zero com segurança**
  - “alguém” fará a segurança depois...
- **Falta de Autenticação**
  - para conectar e receber comandos
  - para fazer atualizações
- **Empresas de diversos setores agora desenvolvem *software*, mas não agem como tal**
  - equipe de segurança de produto e PSIRT?
  - planejamento de atualizações no ciclo de vida do produto?
  - segurança de engenharia de *software*?

Nos Fabricantes, Velhos Problemas (2/2)

- **Desafio adicional em IoT: Um *chipset* ➔ diversos "fabricantes"**
  - Ex.: Dentre os fabricantes nacionais de câmeras, temos encontrando somente *chipsets* Dahua e Xiongmai
  - Como atualizar? *Recall* consegue ser efetivo? (vide caso Xiongmai)

- **Lições Aprendidas com a Deutsch Telecom**
  - contato pré-estabelecido com o fabricante do CPE
  - criação rápida de novo *firmware* com a correção da vulnerabilidade
  - planejamento para gerência e *update* remotos
    - maior parte do parque precisa apenas que o CPE seja desligado e ligado novamente para que inicie a busca por um novo *firmware*

Recomendações para Usuários de Equipamentos de Telecomunicações (1/2)

- **Ser criterioso ao escolher o fornecedor**
  - verificar se possui política de atualização de *firmware*
  - verificar histórico de tratamento de vulnerabilidades
  - identificar qual o *chipset*
    - verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*
  - fazer testes antes de comprar
  - checar se é possível desabilitar serviços desnecessários e trocar senhas

- **Antes de fazer a implantação, planejar**
  - algum esquema de gerência remota
  - como atualizar remotamente

Recomendações para Usuários de Equipamentos de Telecomunicações (2/2)

- **Mesmo escolhendo criteriosamente o fornecedor, assumir que os dispositivos virão com sérios problemas**
  - testar em ambiente controlado
  - assumir que terá um "*backdoor*" do fabricante
- **Desabilitar serviços desnecessários e mudar senhas padrão**
  - nem sempre é possível, vide DVRs e o caso antigo do CPE da Arris que não permitia desabilitar Telnet
- **Manter os equipamentos atualizados**
- **Utilizar sempre que possível uma rede de gerência**

Recomendações para provedores de acesso
E se IoT começar a usar amplificação?

Estatísticas de notificações enviadas pelo CERT.br para detentores de IPs brasileiros permitindo amplificação			
Mês	**Serviço**	**Endereços IP**	**ASNs**
julho e agosto	DNS	79.441	2.401
	NTP	29.176	3.945
setembro e outubro	NTP	82.594	215
	SSDP	4.902	321
	Chargen	316	70
novembro	SNMP	560.965	1.865

- **Implementar boas práticas:**
  - **BCP38/BCP84**
  - **filtrar pacotes com endereços "*spoofados*"**
  - **http://bcp.nic.br/entenda-o-antispoofing/**

Obrigada

www.cert.br

miriam@cert.br

@certbr

05 de dezembro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br