

nic.br egi.br

cert.br

GTS 27

Uberlândia, MG

13 de maio de 2016

Como melhorar o cenário de ataques DDoS

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The top and bottom sections of the slide feature this pattern, while the middle section is a solid light gray gradient.

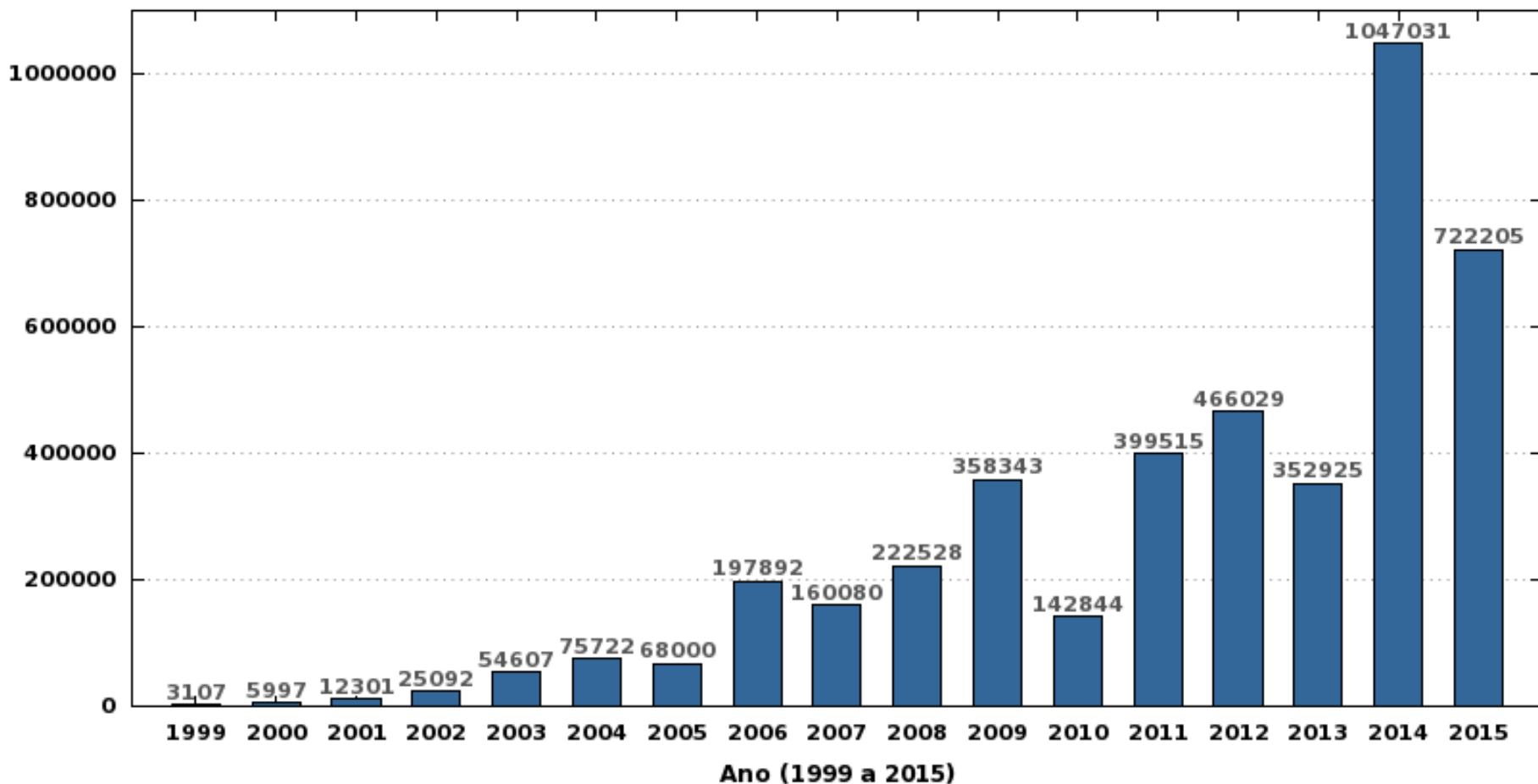
Cenário de ataques DDoS

cert.br nic.br cgi.br

Estatísticas CERT.br

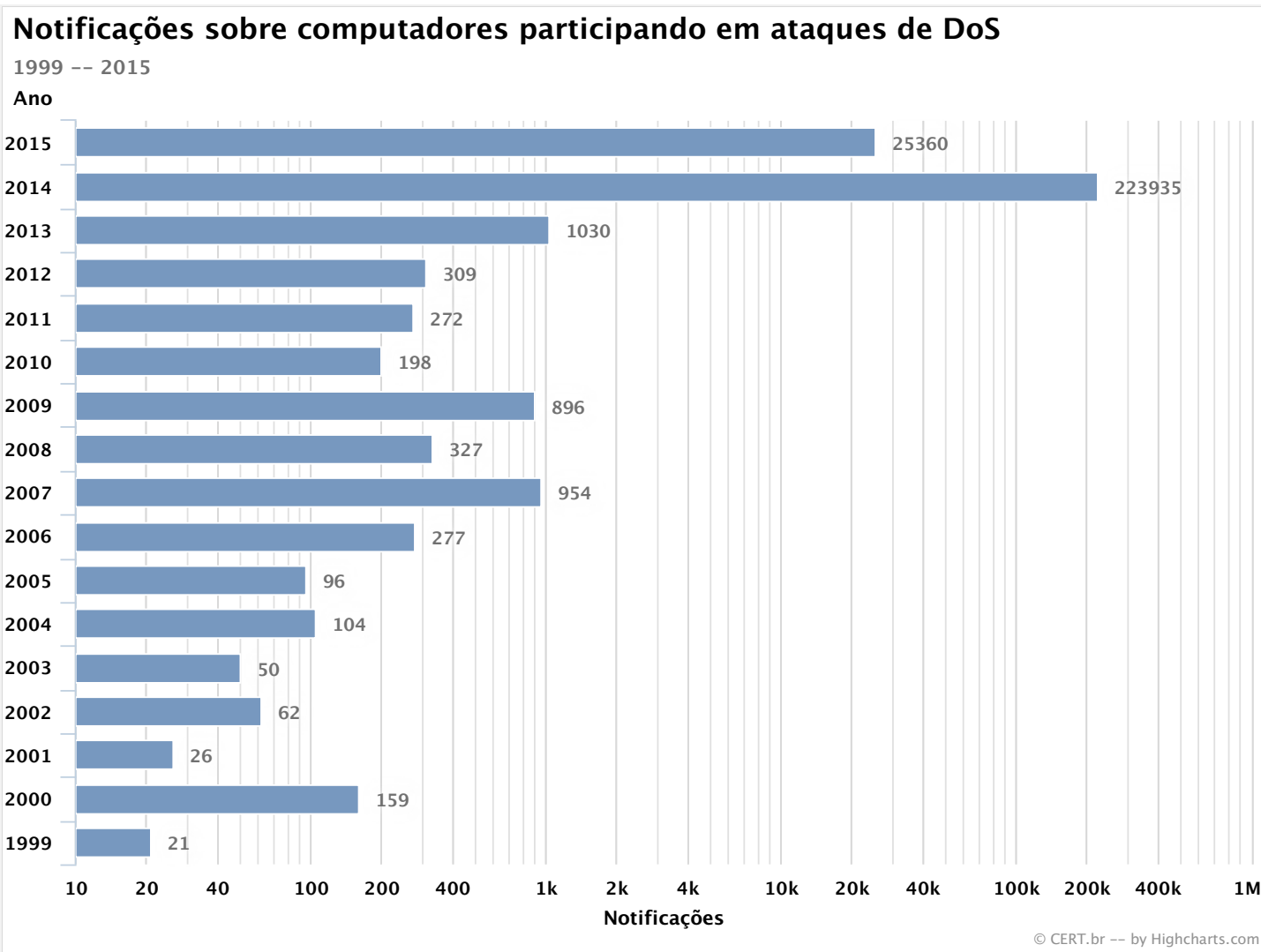
Incidentes – 1999 a 2015

Total de Incidentes Reportados ao CERT.br por Ano



Estatísticas CERT.br

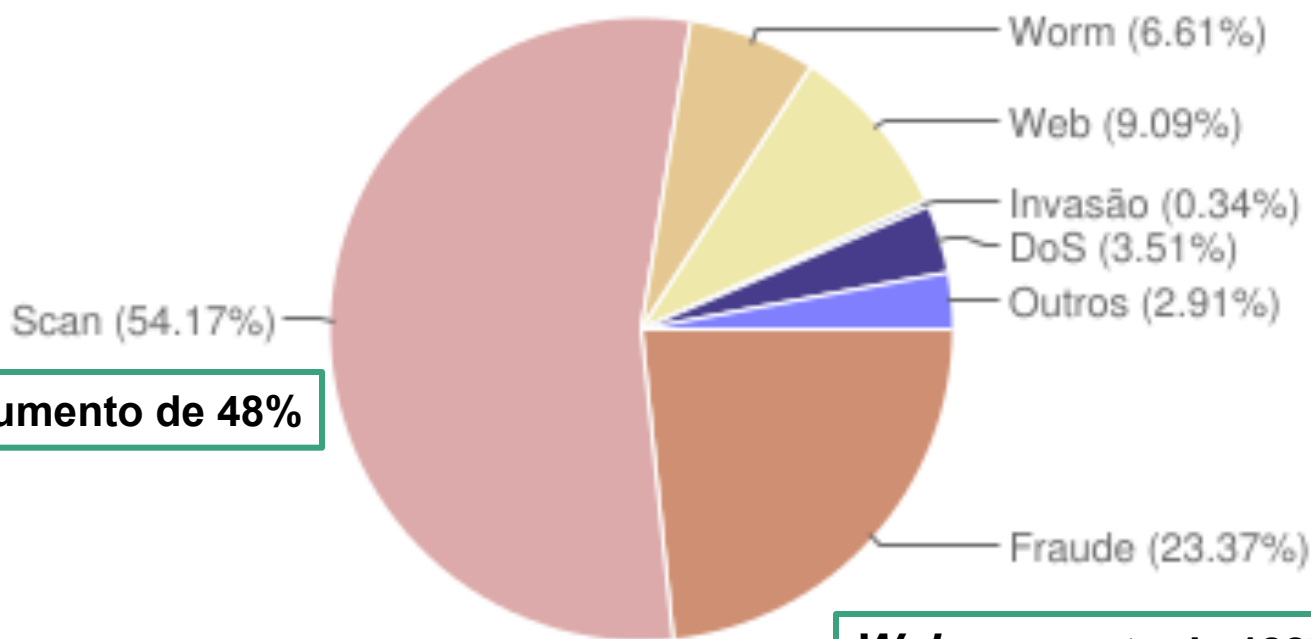
Ataques DDoS – 1999 a 2015



Estatísticas CERT.br

Tipos de ataques – 2015

Incidentes reportados
(Tipos de ataque)



scan: aumento de 48%

Web: aumento de 128%
ataque de força bruta sobre CMS

Cenário atual (1/4)

- **Brasil:**

- terceiro maior alvo de ataques do mundo
- perde para EUA e China
- antes era a Turquia (conflito com a Rússia)

* DDoS Threat Report - Reflection Attacks , Q1 2016, NexusGuard
https://www.nexusguard.com/hubfs/Threat_Report_Q1_2016_Final.pdf

Cenário atual (2/4)

- **Principais motivos**

- *hacktivismo*

- #TangoDown #DDoS

- #OpKKK, #OpISIS, #OpStopBlocking

- #OpOperadoras, #OpAnatel

- #OpOlympicHacking, #OpNimr

- #OpIcarus, #OpShutdownTheBanks, #OpDDoSBankingWebsite

- extorsão

- DD4BC, Armada Collective

- jogos

- qualquer outro

Anonymous Strikes Eight More Banks
As OpIcarus Continues

ARMADA COLLECTIVE DDOS THREATS WERE FAKE, BUT
STILL SCORED THOUSANDS OF DOLLARS

<http://www.digitaltrends.com/computing/armada-collective-fake-ddos-threats/>

<http://www.mobipicker.com/anonymous-strikes-eight-banks-opicarus-continues/>

Cenário atual (3/4)

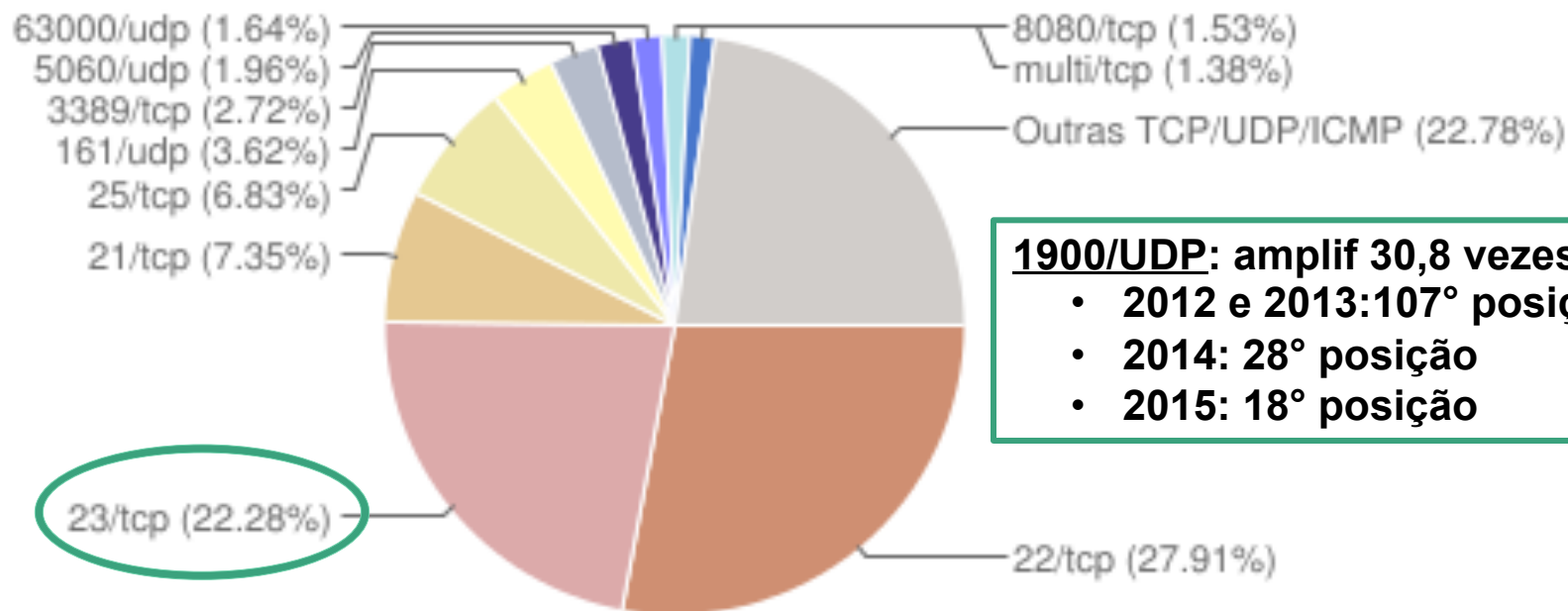
- **Diversas redes e sistemas sendo abusados para gerar ataques**
 - DNS *open resolvers*
 - falta de implementação de *antispoofing*
 - serviços desnecessários abertos
 - sistemas desatualizados
 - aplicações vulneráveis
 - senhas fracas, etc

Cenário atual (4/4)

- **Ataques cada vez mais danosos**
 - reflexão
 - técnicas combinadas
 - alvo: serviços e equipamentos de rede (*firewall*, IDS, CGN)
 - *smoke screen*
 - distrair equipes de segurança
 - dificuldade de analisar a grande quantidade de *logs*
 - objetivo real
 - comprometimento e vazamento de dados

IoT - DRDoS

Scans reportados, por porta
(Não inclui scans realizados por worms)



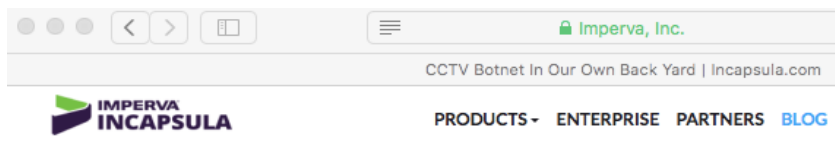
1900/UDP: amplif 30,8 vezes

- 2012 e 2013: 107° posição
- 2014: 28° posição
- 2015: 18° posição

23/TCP: em 2014 era 10%

Report: IoT-Connected Devices Leading to Rise in SSDP-based Reflection Attacks

IoT – sem amplificação (1/2)



Attack Details

As noted, this assault consisted of **HTTP GET floods** that peaked at around 20,000 RPS, with its traffic originating from roughly 900 CCTV cameras spread around the globe. Their target was a rarely-used asset of a large cloud service, catering to millions of users worldwide.

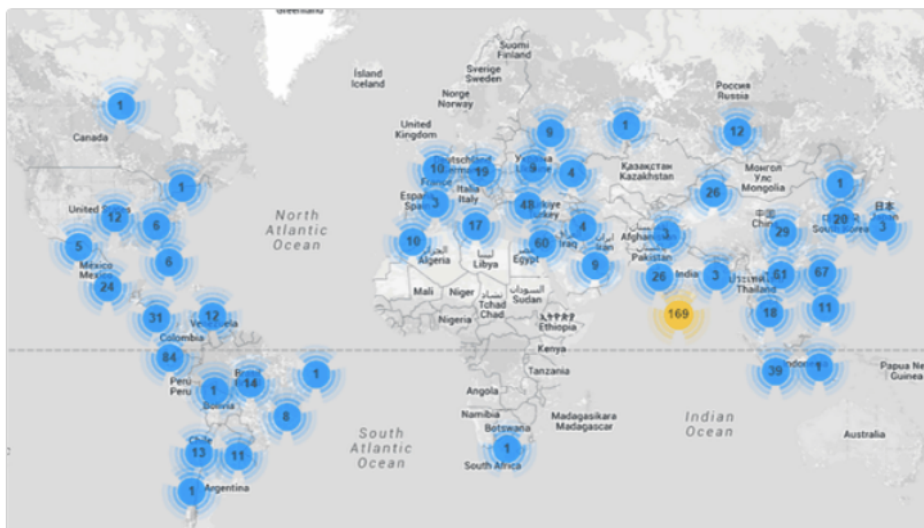


Figure 1: Geo-location of botnet devices

our network, much of it traced back to compromised CCTV cameras.

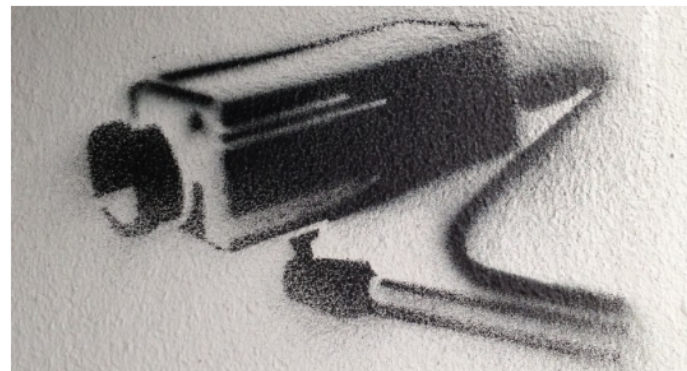
Hacked Shopping Mall CCTV Cameras Are Launching DDoS Attacks



GRAHAM CLULEY

OCT 27, 2015

IT SECURITY AND DATA PROTECTION



<https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html>

<http://www.tripwire.com/state-of-security/security-data-protection/hacked-shopping-mall-cctv-cameras-are-launching-ddos-attacks/>

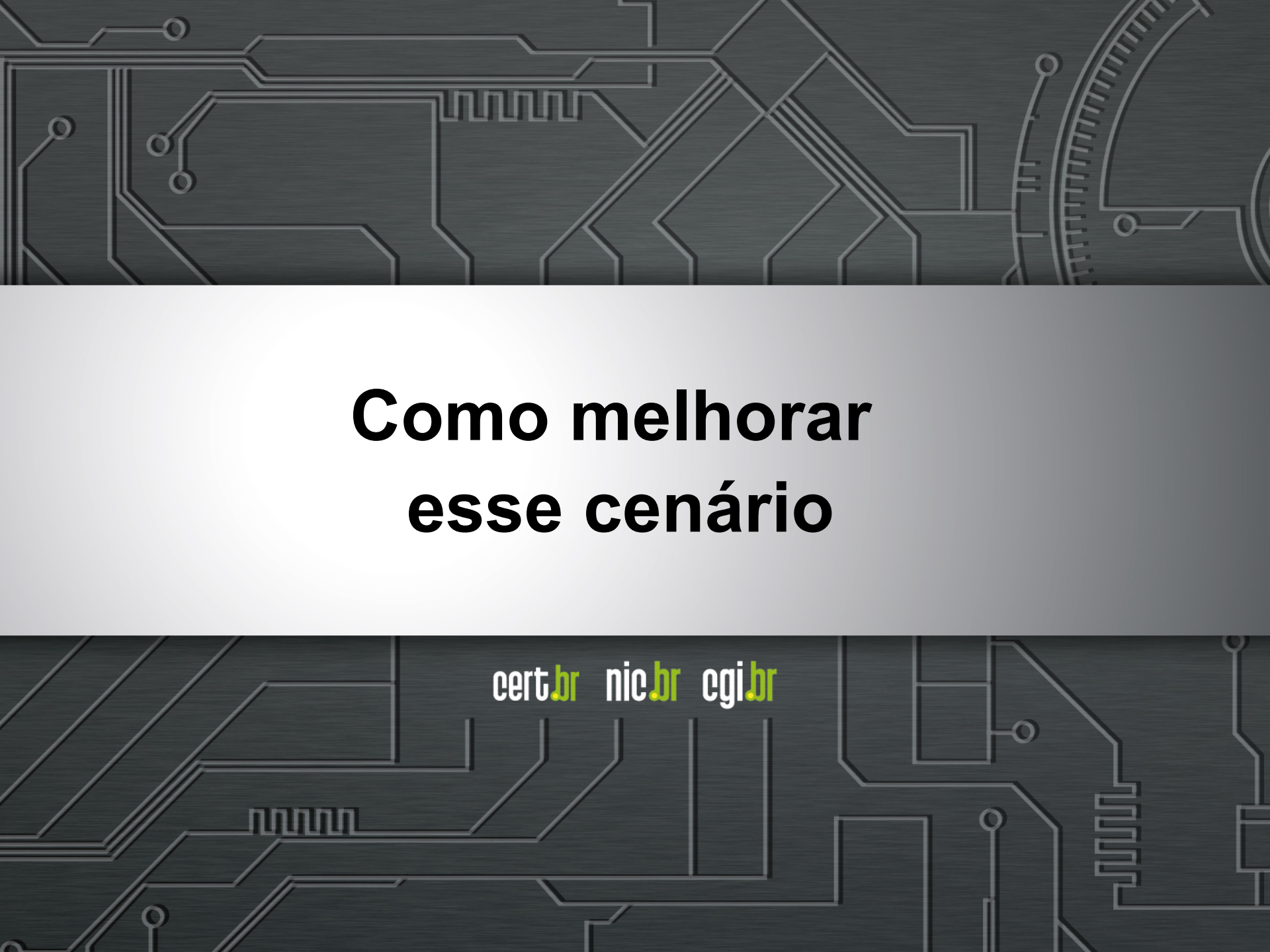
IoT – sem amplificação (2/2)

- **300 Gbps, no Brasil**
- **alvo: instituições financeiras, governamentais e ISPs**
- **câmeras comprometidas via senha de admin**
- ***scan* para achar equipamentos IoT vulneráveis**

Palestra:

WORLDWIDE INFRASTRUCTURE SECURITY REPORT

11th Annual WISR Overview – LACNIC / LACSEC – Carlos Ayala

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is symmetrical and fills the entire frame.

Como melhorar esse cenário

cert.br nic.br cgi.br

Premissa básica

- Não há como evitar ser alvo de um ataque

~~Se eu for atacado...~~

Quando eu for atacado...

Planejamento é essencial

- **“Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço”**

<http://www.cert.br/docs/whitepapers/ddos/>

- **Objetivo:**

- reunir boas práticas de segurança a serem seguidas pelos diversos setores que formam a Internet para:
 - tentar reduzir os ataques DDoS
 - minimizar os problemas por eles causados
- ajudar a entender os diferentes tipos de ataques para definir a melhor estratégia de mitigação
- fornecer lista não exaustiva de boas práticas

Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)

Autor: CERT.br

Versão: 1.0 — 19/04/2016

Sumário

1. Introdução

2. Principais alvos e motivações dos ataques DDoS

3. Como são realizados os ataques DDoS

4. Tipos de ataques DDoS

4.1 Ataques à camada de aplicação

4.2 Ataques de exaustão de recursos de *hardware*

4.3 Ataques volumétricos

5. Como evitar que suas redes e sistemas sejam abusados para gerar ataques DDoS

5.1 Usuários finais

5.2 Desenvolvedores de aplicações Web

5.3 Administradores de redes

5.4 Provedores de conectividade

6. Como tratar ataques DDoS

6.1 Preparação

6.2 Detecção e Análise

6.3 Mitigação

6.4 Após o ataque

- 1. Importância da notificação de incidentes de segurança**
- 2. O que notificar**
- 3. A quem notificar**
- 4. Buscando contatos**
 - 4.1 WHOIS**
 - 4.2 CSIRTs**
 - 4.3 *Top-Level Domains* (TLDs)**
 - 4.4 Criando e mantendo base de contatos própria**
- 5. Formas e formato de notificar**
- 6. O que incluir na notificação**
- 7. Exemplos de consultas WHOIS**
 - 7.1 Pesquisa por IP sem determinação do servidor WHOIS**
 - 7.2 Pesquisa por IP selecionando o servidor WHOIS**
 - 7.3 Pesquisa por nome de domínio**
 - 7.4 Mapeamento de IP para ASN e busca por ASN**
 - 7.5 Exemplos de indicação de contato de abuso em campos diversos**

Recomendações para Notificações de Incidentes de Segurança

Autor: CERT.br
Versão: 1.1 — 20/04/2016

Modelos para *download*: [Português] [Inglês]

Sumário

1. Importância da notificação de incidentes de segurança
2. O que notificar
3. A quem notificar

8. Modelos de notificações

8.1 Modelos para *download*

8.2 Licença de uso dos modelos de notificações

8.3 Descrição das variáveis de texto

8.4 Desfiguração de página

8.5 Domínios utilizados para fraudes

8.9 DDoS por *botnet* sem *spoofing*

8.10 Ataque de negação de serviço distribuído com uso de amplificação (DRDoS)

8.10 Ataque de negação de serviço distribuído com uso de amplificação (DRDoS)

8.11 Hospedagem de artefatos maliciosos

8.12 *Phishing* simples ou com geolocalização

8.13 *Phishing* com *Pharming*

8.14 Servidor enviando *phishing scam*

8.15 Servidor de comando e controle de RAT

9. Glossário
10. Referências
11. Agradecimentos
12. Histórico de Revisões

Próximos passos

Tradução para o espanhol e inglês

Críticas, sugestões e dúvidas da comunidade são bem-vindas

doc@cert.br

Obrigada

www.cert.br

© miriam@cert.br

© @certbr

13 de maio de 2016

nic.br cgi.br

www.nic.br | www.cgi.br