nic.br cgi.br | 20 anos cert.br

IX (PTT) Fórum Regional

São Paulo, SP

11 de agosto de 2017

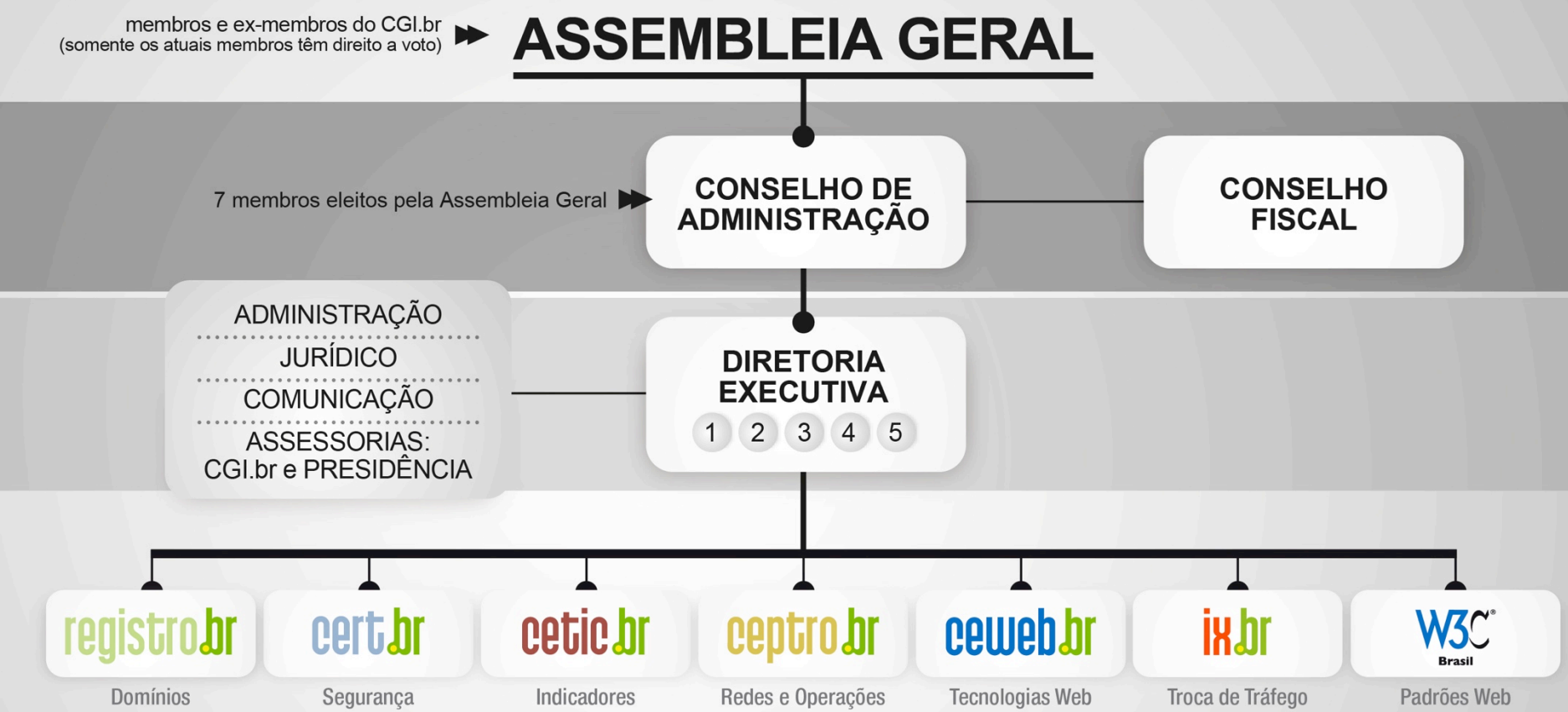
Ataques de negação de serviço e como melhorar o cenário

Miriam von Zuben
miriam@cert.br

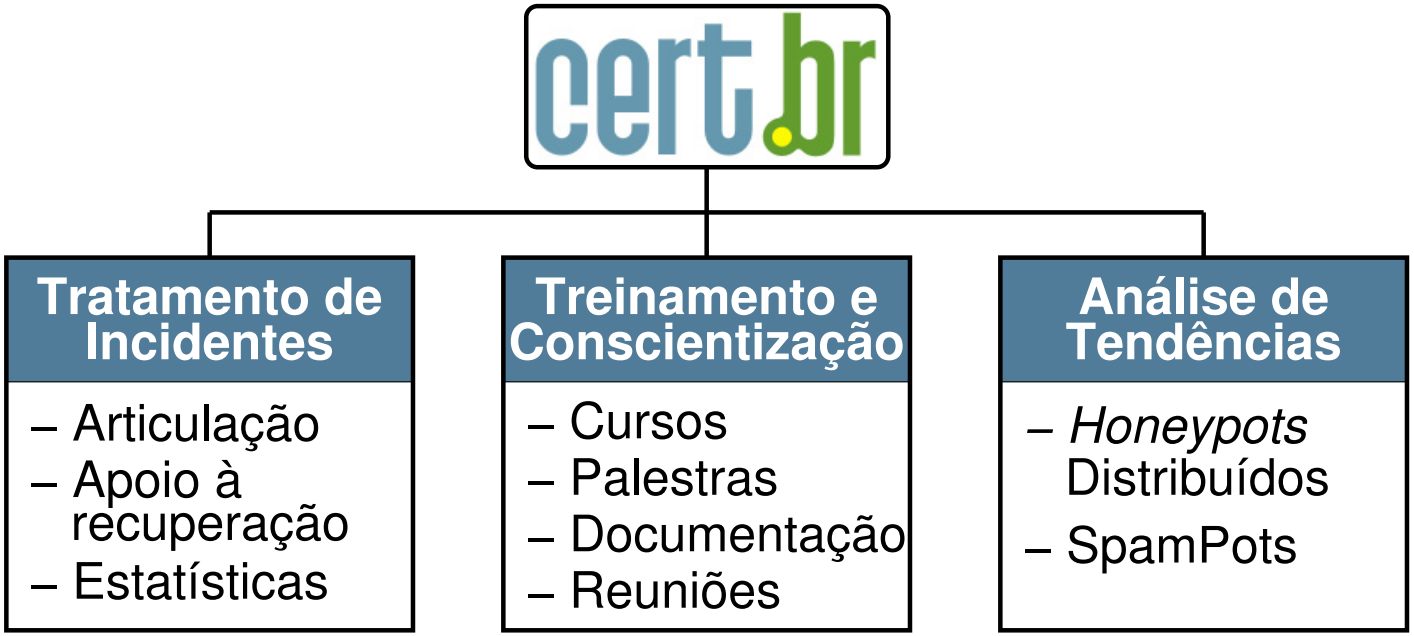
Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

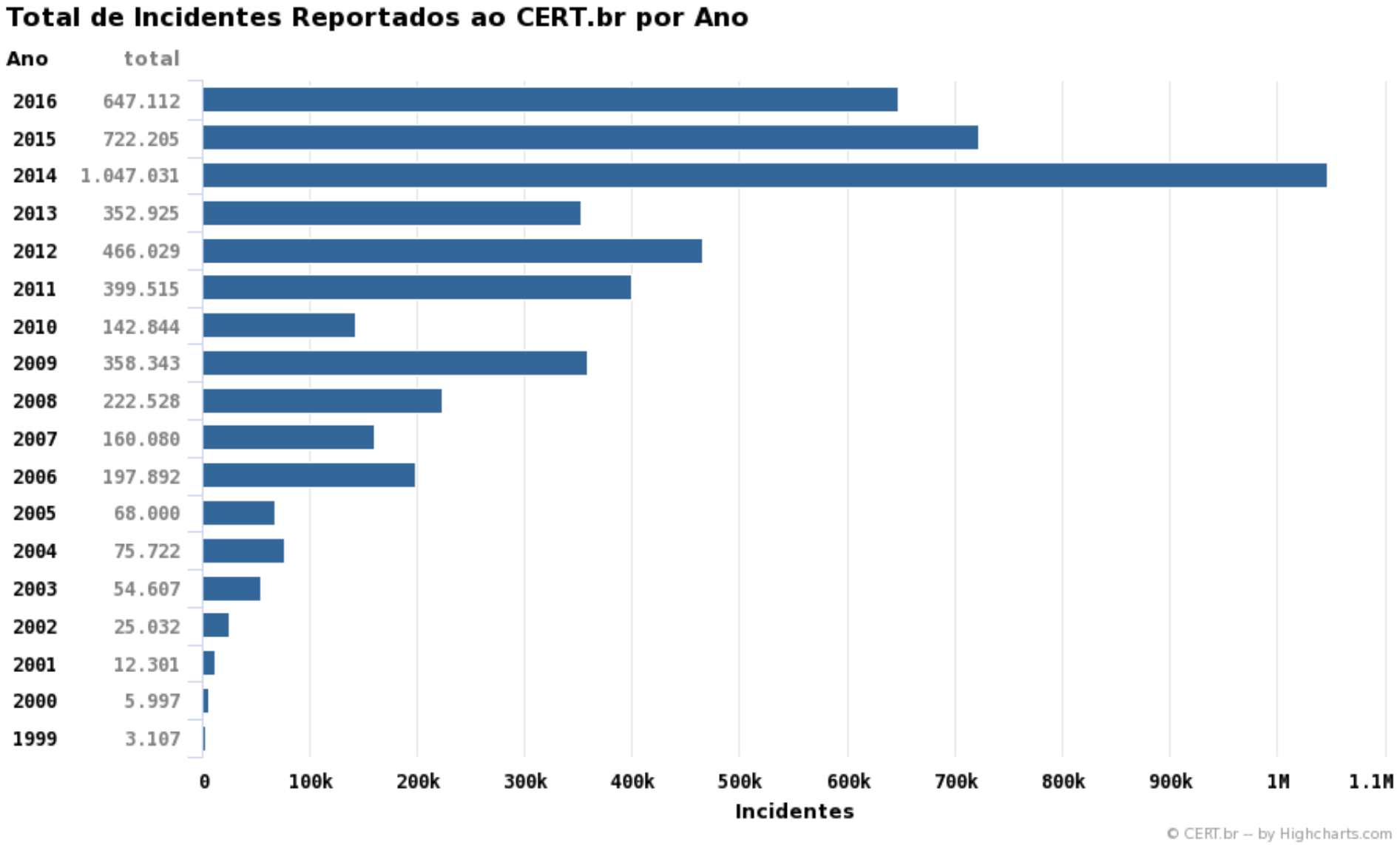
APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet
PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

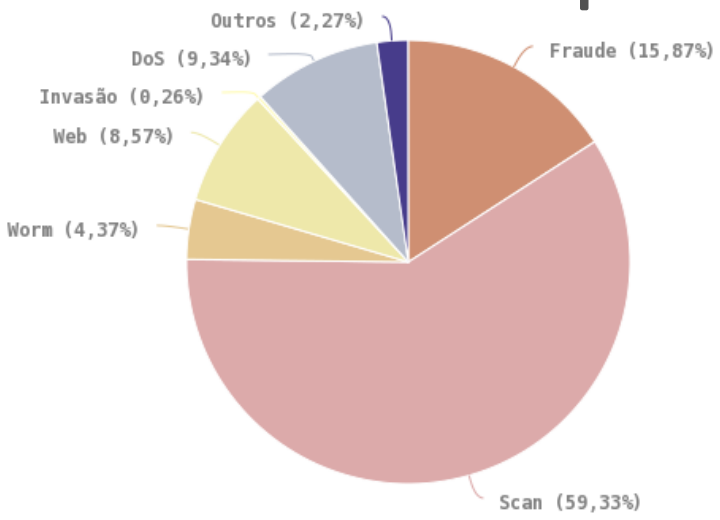
Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

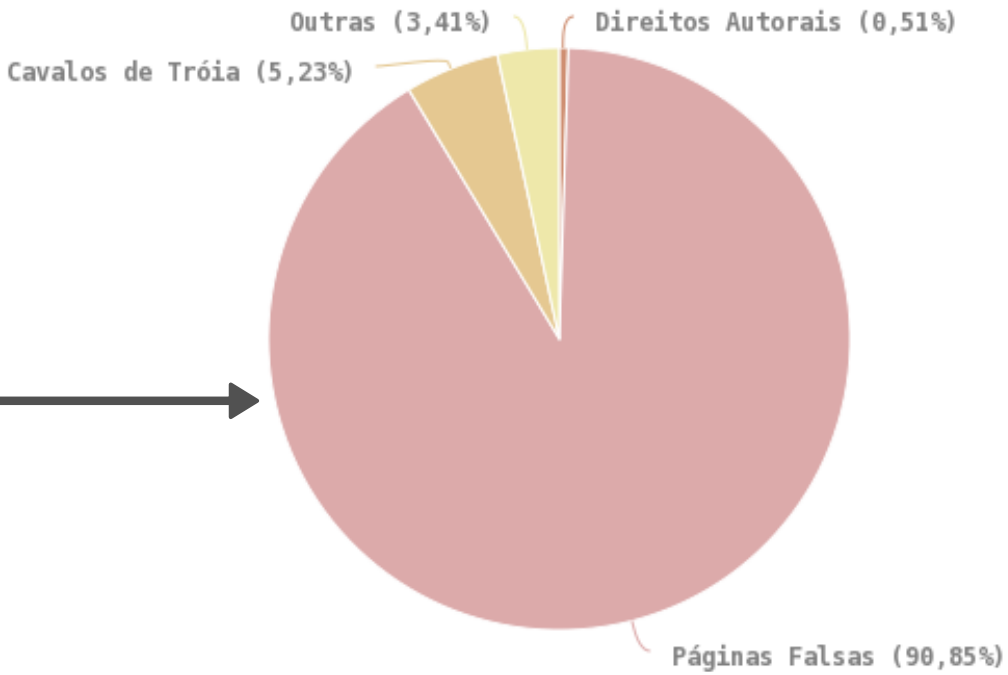


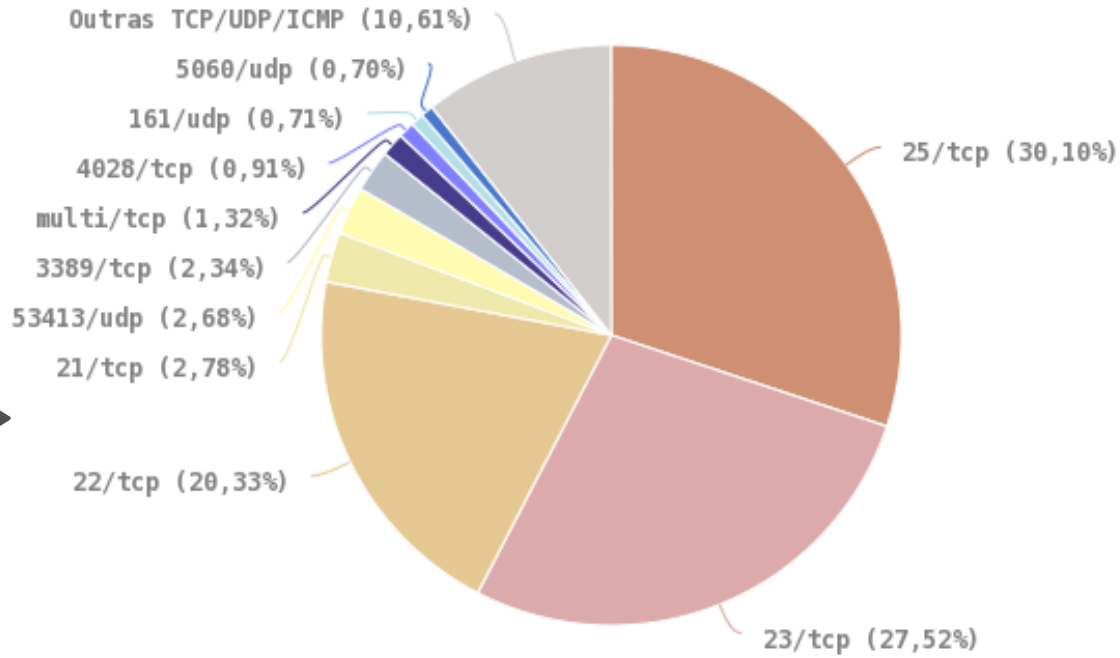
Estatísticas de notificações enviadas voluntariamente por administradores de sistemas e usuários finais para o *e-mail* cert@cert.br.

https://cert.br/stats/

Estatísticas 2016



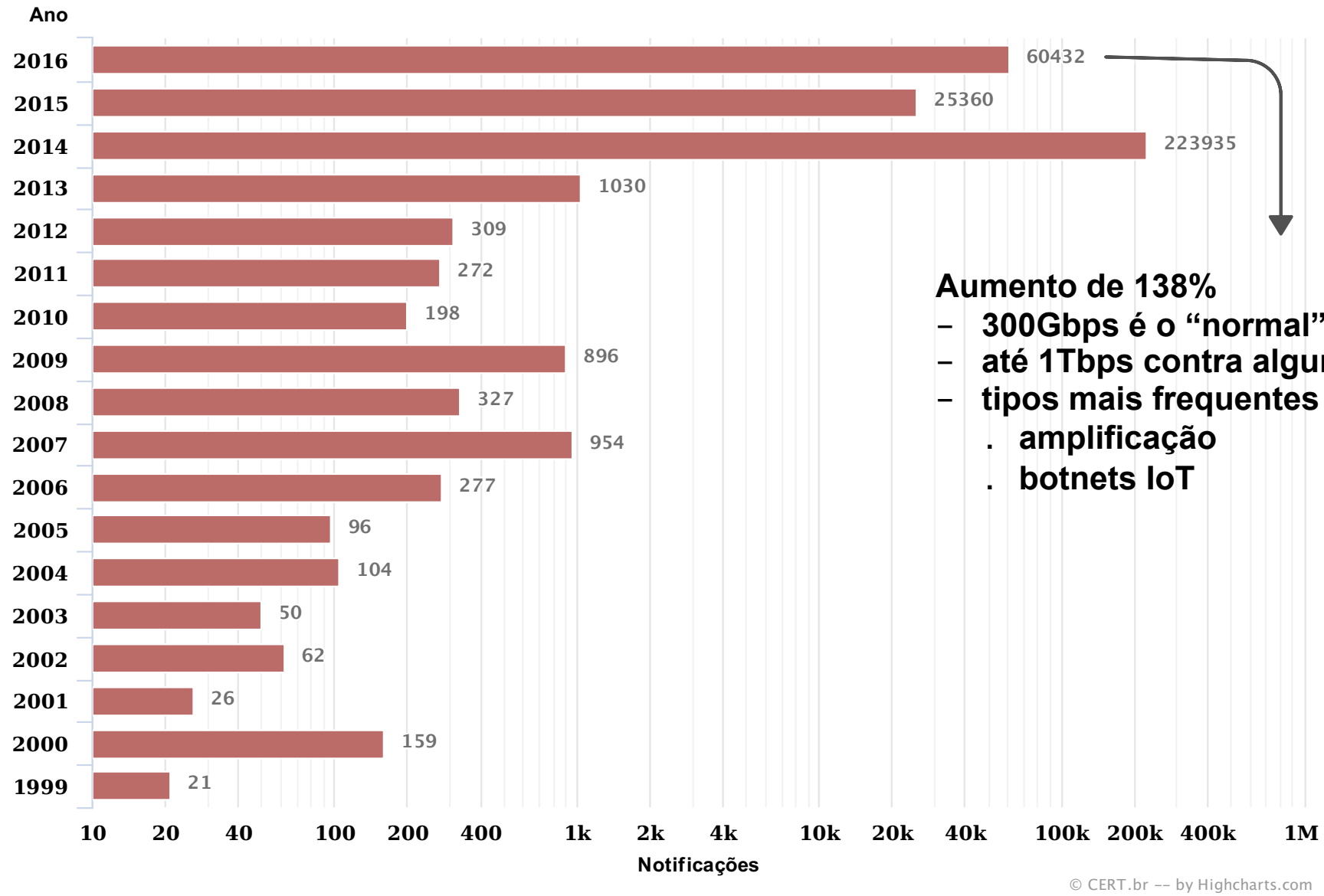




Fonte: CERT.br

Notificações sobre computadores participando em ataques de DoS

1999 -- 2016



Aumento de 138%

- 300Gbps é o “normal”
- até 1Tbps contra alguns alvos
- tipos mais frequentes
  - . amplificação
  - . botnets IoT

Fonte: CERT.br

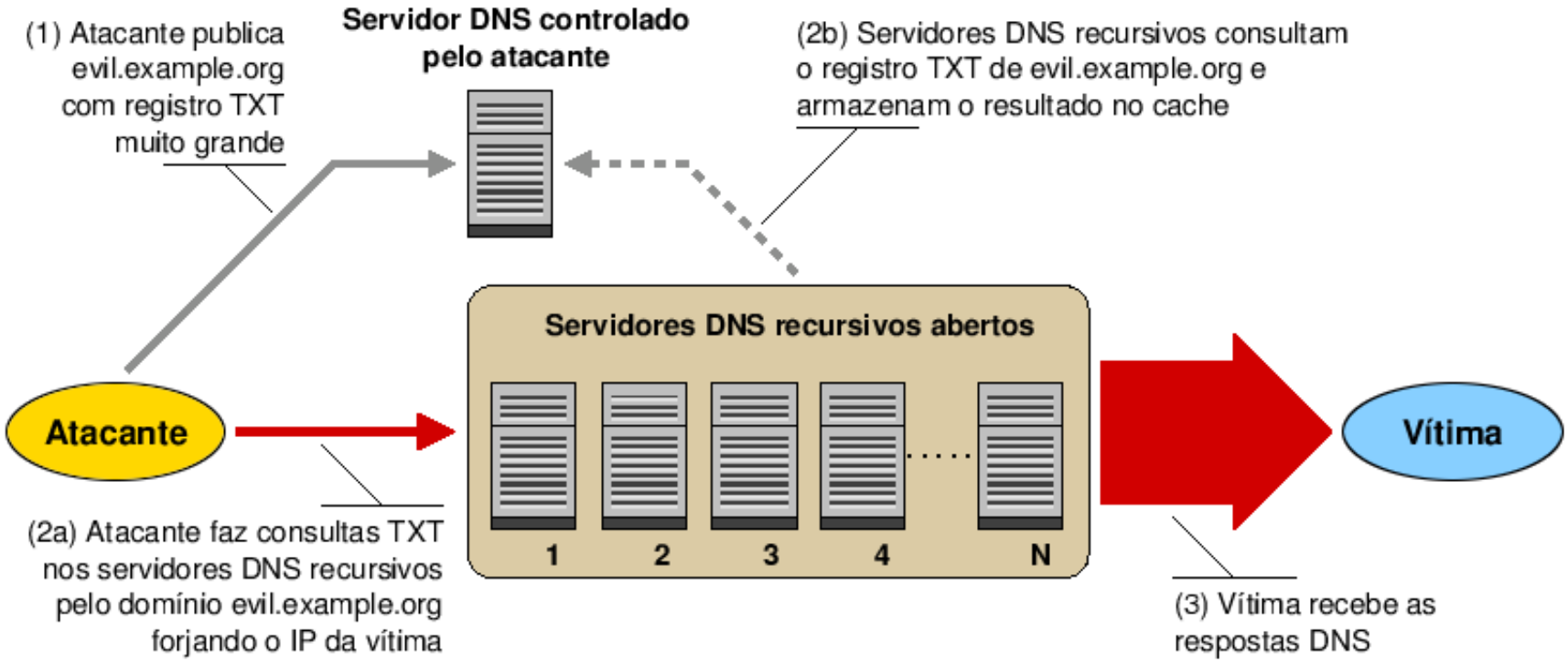
Ataques DRDoS

- ***Distributed Reflective Denial of Service***
- **Usa infraestrutura pública da Internet para amplificação**
- **Tem grande "poder de fogo"**

Protocolo	Fator de amplificação	Comando Vulnerável
DNS	28 até 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request

https://www.us-cert.gov/ncas/alerts/TA14-017A
http://www.internetsociety.org/sites/default/files/01_5.pdf

Ataques DRDoS
Exemplo de funcionamento abusando DNS



Fonte: CERT.br

Botnets de dispositivos IoT

- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**
- ***Malware* se propaga geralmente via Telnet**
  - exploram Senhas Fracas ou Padrão
    - muitas vezes são "*backdoors*" dos fabricantes
- **Foco em dispositivos com versões "enxutas" de Linux**
  - para sistemas embarcados e arquiteturas ARM, MIPS, PowerPC, etc
- **Grande base vulnerável**
  - sem gerência remota
  - sem instalação de patches
  - 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

Setembro/2016, variante Mirai é identificada

- 22 e 23/09 – 620Gbps contra o Blog do Brian Krebs
- 21/10 – DDoS contra a Dyn
- 27/11 – Surgimento da variante para CPEs

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication

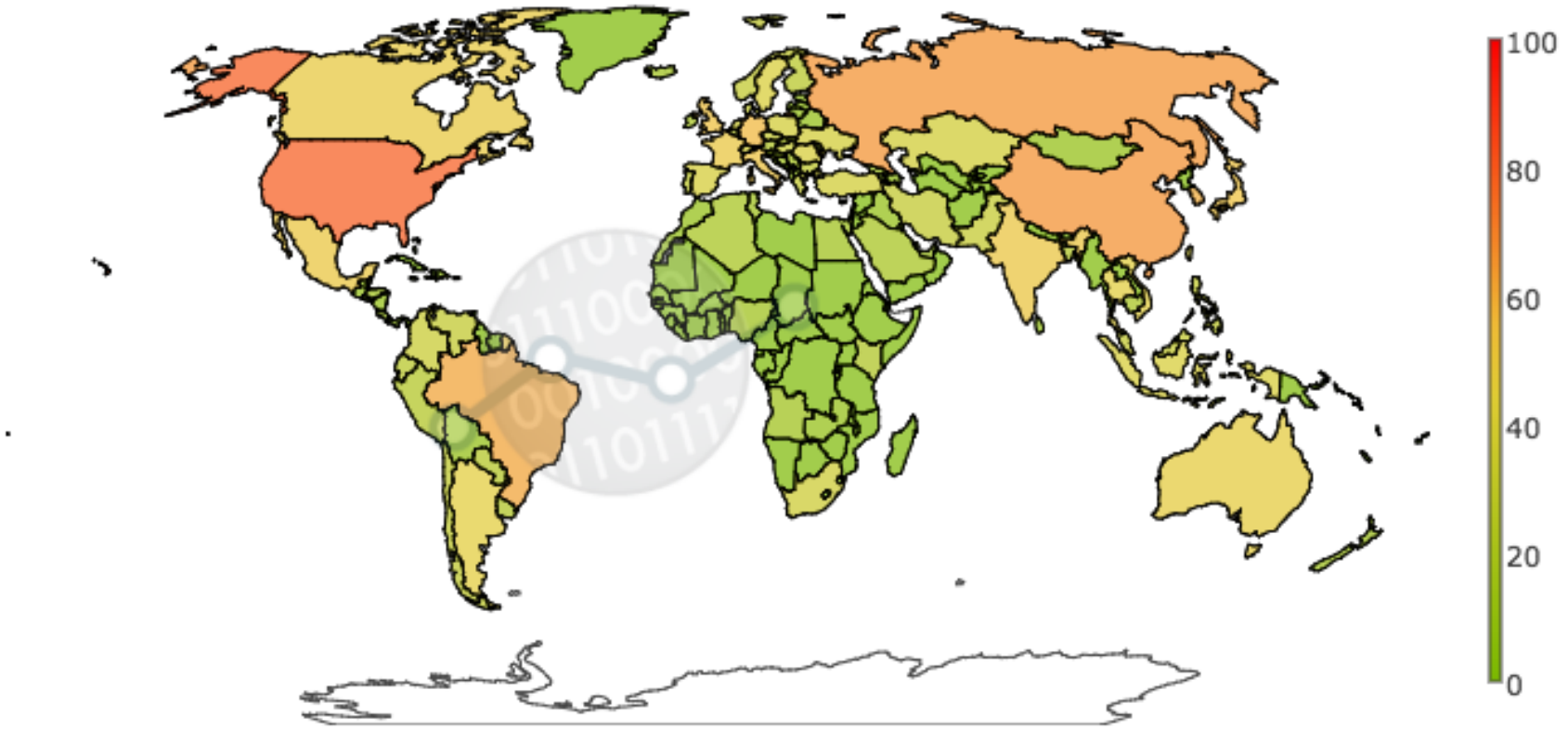
Brad Chacos | *@BradChacos* Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.bbc.co.uk/news/amp/37439513
http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html
http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

Risco potencial imposto à Internet

cert.br nic.br cgi.br

Risco potencial imposto à Internet



http://stats.cybergreen.net/

Julho/2017

Potencial ofensivo – em Tbps

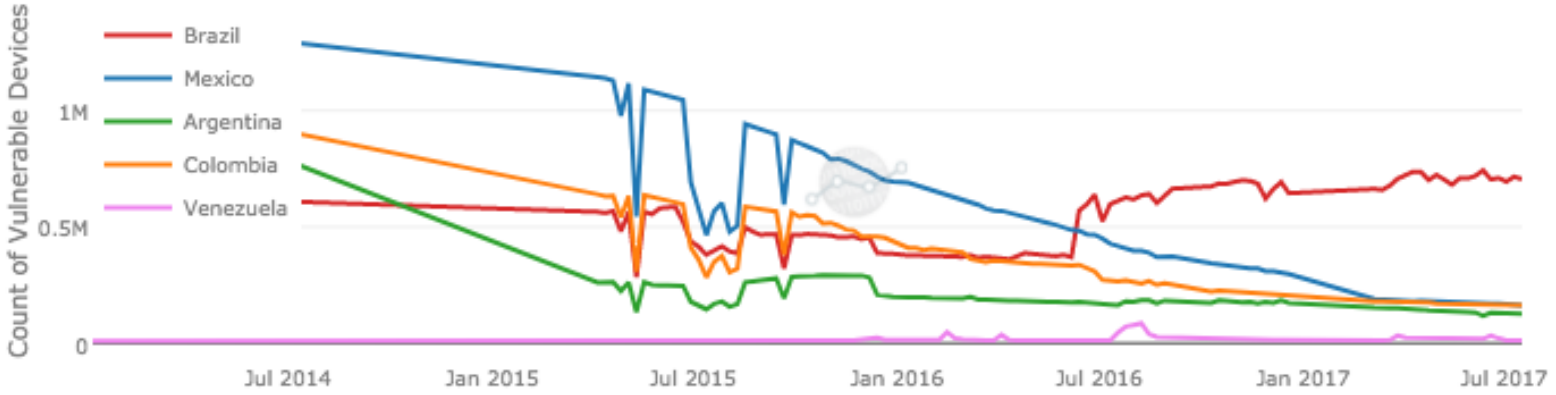
Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Mirai	DDOS Potential TBit/sec	DDOS Rank
United States	2,190,873	843,263	502,238	269,564	8,135	571	1
China	1,482,736	281,911	156,783	851,625	82,767	245	2
Russian Federation	441,759	300,671	132,920	480,070	89,994	201	3
Brazil	723,305	190,389	965,167	160,864	59,369	147	4
South Korea	321,309	221,758	279,303	189,540	4,008	144	5
India	979,519	96,387	321,609	115,567	85,398	99	6
Germany	311,630	145,350	42,220	19,984	3,560	95	7
Italy	436,750	96,707	174,792	87,731	5,759	76	8
United Kingdom	246,798	112,296	38,355	14,199	3,287	73	9
Japan	235,820	103,752	74,813	124,836	1,388	72	10

http://stats.cybergreen.net/country

Maio/2017

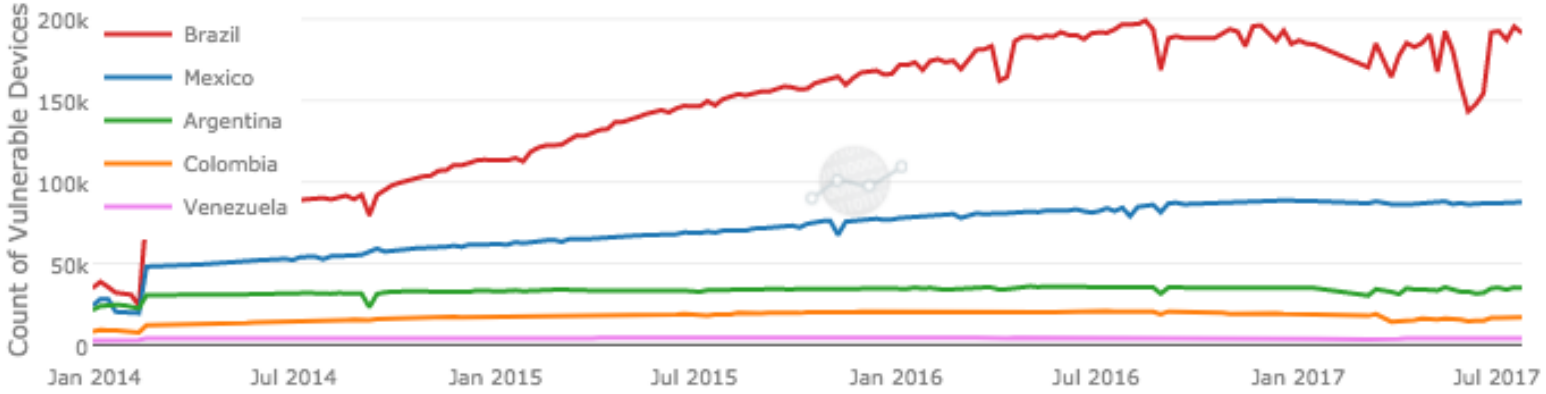
Dispositivos vulneráveis

OPEN RECURSIVE DNS



OPEN NTP

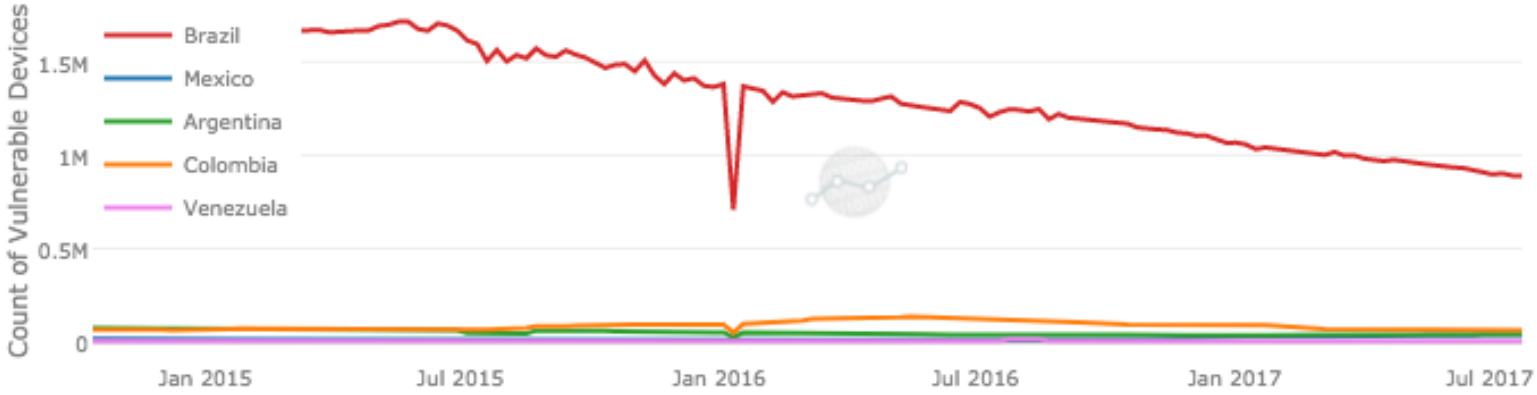
BRAZIL #4



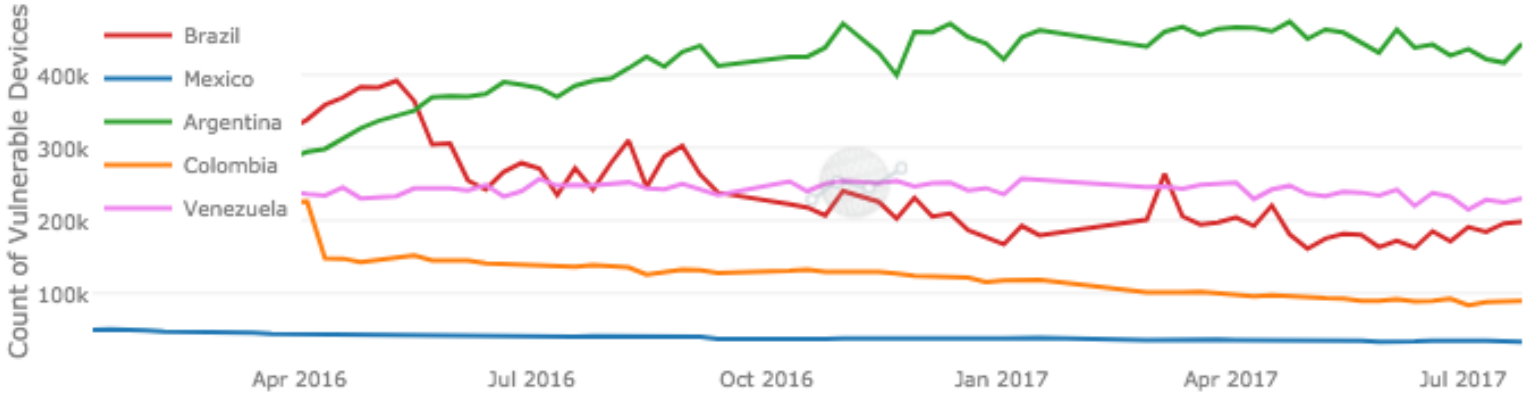
http://stats.cybergreen.net/country/brazil/

Dispositivos vulneráveis

OPEN SNMP BRAZIL #1

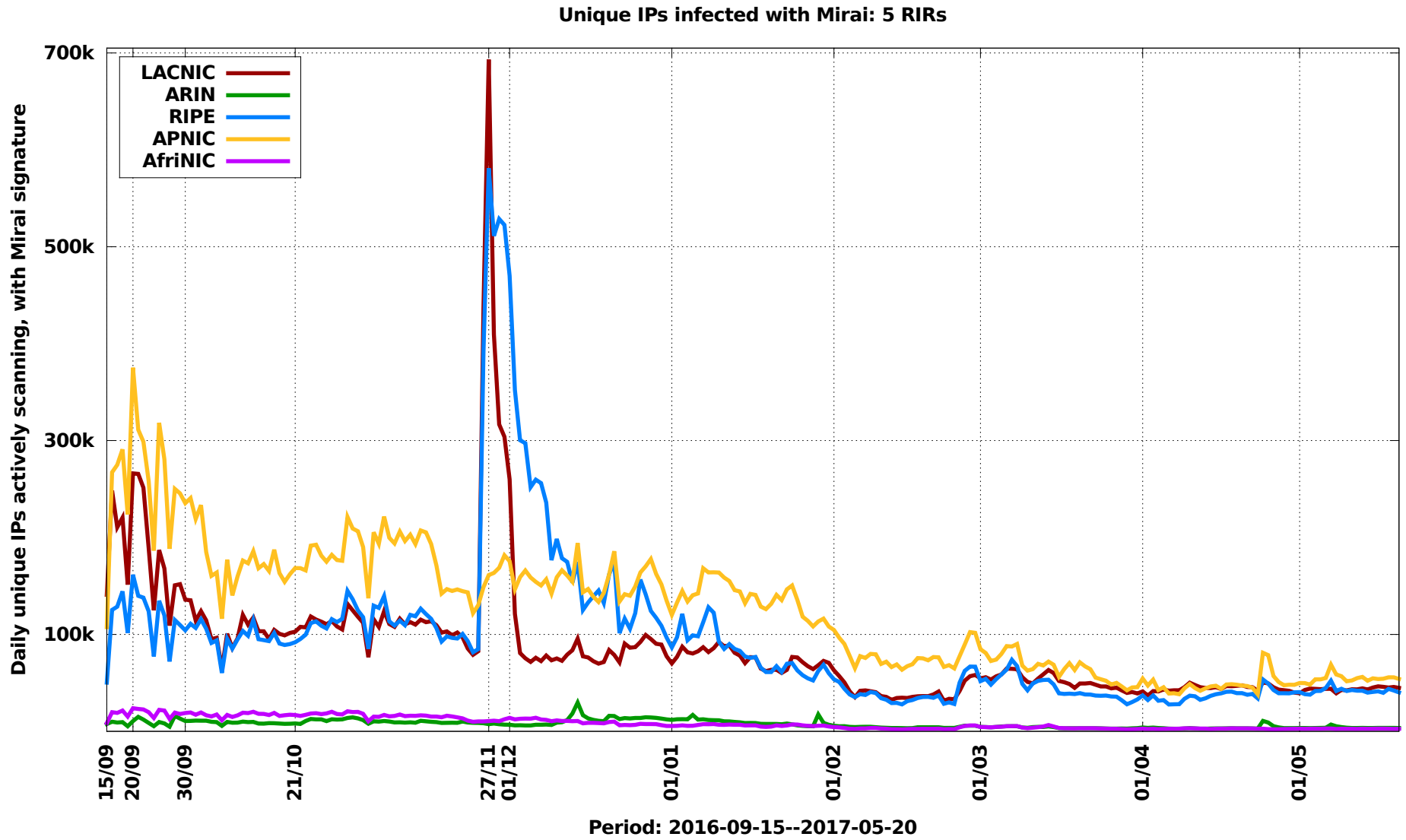


OPEN SSDP BRAZIL #6



http://stats.cybergreen.net/country/brazil/

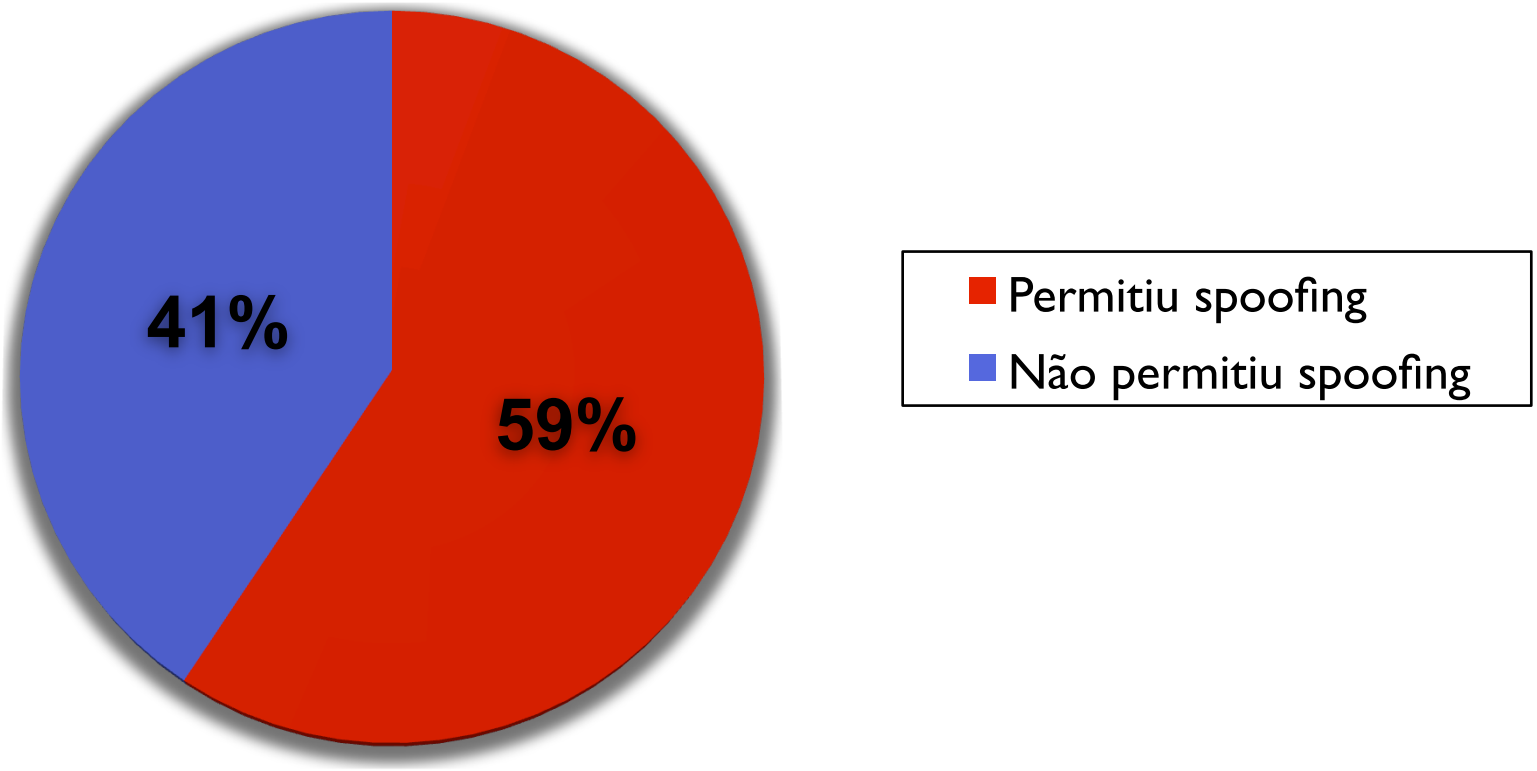
Dispositivos infectados



Fonte: CERT.br

BCP-38 – Testes SIMET Box

Testes de *spoofing* com rede de terceiros



Fonte: Projeto SIMET – NIC.br

Maio/2017

Sequestro de rotas para perpetrar fraudes financeiras

cert.br nic.br cgi.br

Ataques envolvendo sequestro de rotas BGP para perpetrar fraudes financeiras

- **Características do protocolo BGP**
  - sistemas autônomos anunciam seus blocos de rede (/16, /20, /22, etc)
  - *"peers"* aprendem e repassam esses anúncios
  - "vencem" as rotas para anúncios de blocos mais específicos
- **Anatomia dos ataques**
  - atacantes comprometem roteadores de borda de pequenos provedores
  - anunciam prefixos de rede mais específicos da instituição vítima (em geral /24)
    - "*peers*" do provedor comprometido vão aprendendo a nova rota
    - clientes das redes que aprenderam a nova rota passam a ser roteados para o local errado
  - início em março de 2017 e ainda está ocorrendo

Características dos Sequestros de Rota Detectados

Períodos:

- variando de minutos a horas
- inicialmente à noite, escalando para feriados e finais de semana

Equipamentos:

- roteadores de borda de pequenos e médios provedores
- 1 caso via rede de gerência

Prefixos sequestrados:

- /24 de serviços *Internet Banking*
- /24 de provedores de nuvem

Levantados túneis GRE:

- para destinos em provedores de *hosting*
- protocolos HTTP e DNS no destino

Como melhorar o cenário

Segurança é inerentemente multissetorial

- **Cooperação é essencial para um ecossistema saudável**
- **Nenhum grupo ou estrutura única fará sozinha a segurança**
- **Todos tem um papel importante**
  - não fazer parte do problema (contribuir para melhorar o cenário)
  - proteger-se adequadamente

Contribuir para melhorar o cenário

- **Usuários**
  - entender os riscos e seguir as dicas de segurança
  - manter seus equipamentos seguros e tratar infecções
  - adotar uma postura preventiva
- **Educadores:**
  - formar profissionais com conhecimentos de segurança
- **Desenvolvedores**
  - pensar em segurança desde as etapas iniciais de desenvolvimento
- **Gestores**
  - considerar segurança como investimento e alocar recursos adequados
  - requisitos mais rígidos para escolha de fornecedores
- **Administradores de redes e sistemas e profissionais de segurança**
  - não emanar “sujeira” de suas redes e adotar boas práticas

Contribuir para melhorar o cenário Provedores

- **Proteger os CPEs dos clientes:**
  - usar senhas bem elaboradas
  - não usar senhas padrão
  - manter o *firmware* atualizado
  - desabilitar serviços desnecessários
  - ter uma rede de gerência
- **Habilitar filtro *anti-spoofing* (BCP38)**
  - http://bcp.nic.br
- **Verificar fluxos de saída de tráfego**
  - "*extrusion detection*"
    - *flows, honeypots*, *passive* DNS
    - notificações de incidentes (contatos de whois)
    - *feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)
- **Configurar corretamente serviços que podem ser abusados**
  - https://www.cert.br/docs/whitepapers/ddos/

Preparar-se adequadamente

- **Adotar medidas pró-ativas**
  - *overprovision* (*links* com capacidade maior que os picos de tráfego
  - implementar segregação de rede para serviços críticos
  - minimizar a visibilidade de sistemas e serviços
  - verificar se os contratos permitem a flexibilização de banda em casos de ataques
  - manter contato com a equipe técnica do *upstream* para que ela ajude em caso de necessidade
  - treinar pessoal de rede para implantar medidas de mitigação

Estar preparado para o pior

- **Mitigar o ataque**
  - filtrar tráfego por IP ou porta de origem ou destino
  - usar *rate-limiting* e ACLs em roteadores e switches
  - contactar *upstream*
    - aplicar filtros
    - *nullrouting*/*sinkholing*
    - serviços de mitigação de DDoS
  - mover para CDN (*Content Delivery Network*)
  - contratar serviços de mitigação
- **Criar grupos de segurança (CSIRTs)**
  - https://cert.br/csirts/
- **Cooperação**

Latin America and Caribbean Anti-Abuse Working Group (LAC-AAWG)

- **Desenvolver uma comunidade anti-abuso na região LAC**
- **Servir como um fórum para operadores de redes e especialistas em anti-abuso**
  - promover o diálogo entre comunidades e grupos de trabalho existentes
- **Fomentar o desenvolvimento de recomendações anti-abuso e melhores práticas operacionais (BCOPs)**
  - abordar questões específicas da região e globais
  - participar e contribuir para a comunidade global
- **Coordenar atividades de conscientização contra o abusos**
  - Incentivar a adoção de melhores práticas e operações anti-abuso

lacnog

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

lacnic

http://www.lacnic.net/en/web/anuncios/2017-amenazas-en-linea-se-fortalece

Como Participar

- **Lista BCOP bcop@lacnog.org**
  - lista aberta do Grupo de Trabalho BCOP do LACNOG, destinada a discussão de melhores práticas operacionais para serviços de redes
- **Lista LACNOG lacnog@lacnog.org**
  - lista aberta para a discussão de questões do funcionamento e operações de redes em geral, não se limitando a segurança
- **Lista LAC-SEC seguridad@lacnic.net**
  - lista aberta dedicada a discussão de questões de segurança em um contexto amplo, não limitando a resposta e mitigação de incidentes de segurança
- **Lista LAC-CSIRTs lac-csirts@lacnic.net**
  - lista fechada, destinada a assuntos relacionados ao tratamento de incidentes de segurança. Participação institucional, restrita a membros de times de resposta a incidentes de segurança (CSIRT)

Como Contribuir?

- **Participar das listas de discussão**
- **Ajudar no desenvolvimento de boas práticas/BCOPs**
  - sugerir temas
  - desenvolver conteúdo técnico
  - traduzir BCPs/BCOPs existentes
  - ser editor/revisor de documentos
- **Ajudar na conscientização acerca de boas práticas existentes**
  - produzir / promover conteúdo relacionado a boas práticas
    - *newsletter*, *whitepaper*, *blogpost*, palestra, *webinar*, etc...
  - fomentar a adoção

BCOPs em Desenvolvimento

- **BCOPs**
  - *BGP Implementation*
  - ***Mitigation of attacks directed to CPE devices***
  - *First steps on IPv6 implementations*
  - *Remote Triggered BlackHole routes (RTBH)*
  - *Spanish translation of the document RIPE-631: IPv6 Troubleshooting for Residential ISP Helpdesks*

Alguns Recursos

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

  https://www.cert.br/docs/whitepapers/ddos/
- **Recomendações para Notificações de Incidentes de Segurança**

  https://www.cert.br/docs/whitepapers/notificacoes/
- **Portal de Boas Práticas para Internet no Brasil**

  http://bcp.nic.br/
- ***Project Spoofer***

  http://spoofer.caida.org/
- ***CyberGreen***

  http://www.cybergreen.net/
- ***IoT, IPv6 and the new ISP challenges for Internet security***

  https://mum.mikrotik.com/presentations/EU17/presentation_4088_1492591370.pdf
- ***M3AAWG Introduction to Reflective DDoS Attacks***

  https://www.m3aawg.org/sites/default/files/m3aawg-reflective-ddos-attack-intro.pdf
- ***M3AAWG Initial Recommendations: Arming Businesses Against DDoS Attacks***

  https://www.m3aawg.org/sites/default/files/m3aawg-arming-business-against-ddos-2017-03.pdf

Obrigada

www.cert.br

miriam@cert.br lucimara@cert.br @certbr

11 de agosto de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br