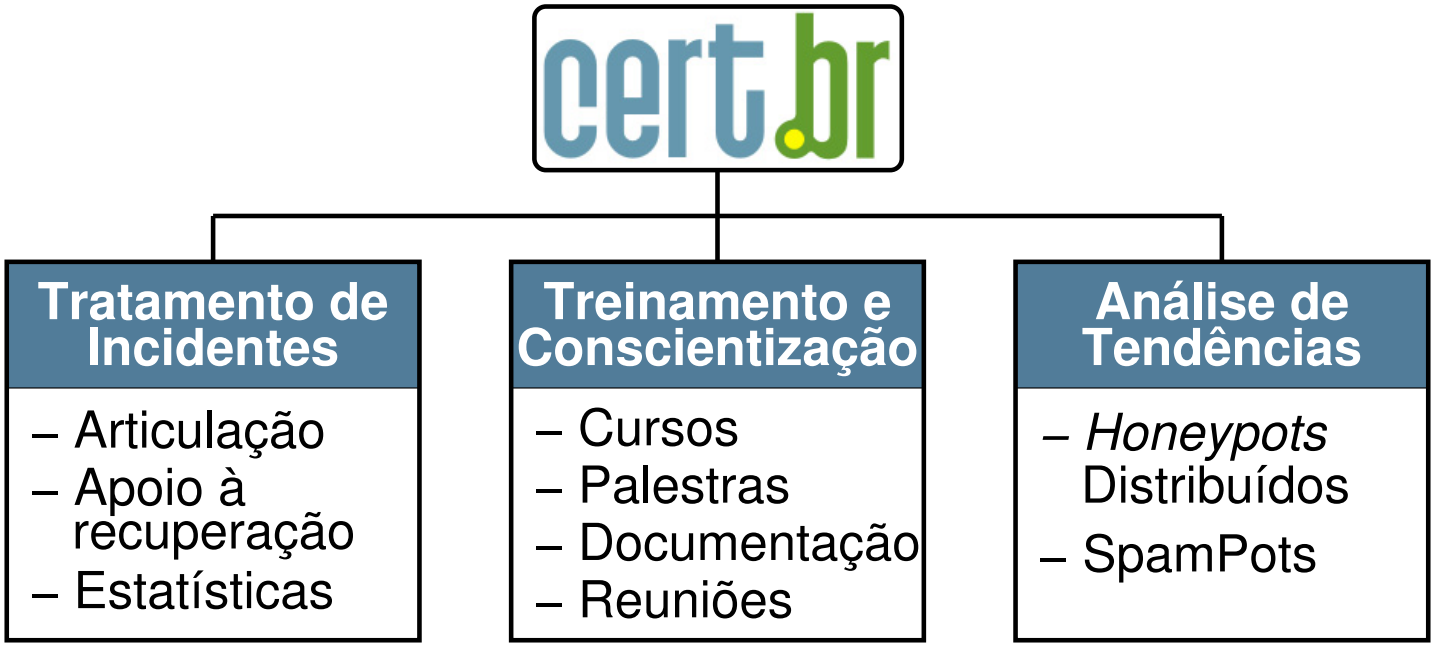
nic.br cgi.br | cert.br

Vitória, ES
21 de maio de 2015
XXXIII SBRC

Técnicas e Tendências nos Ataques de Negação de Serviços

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

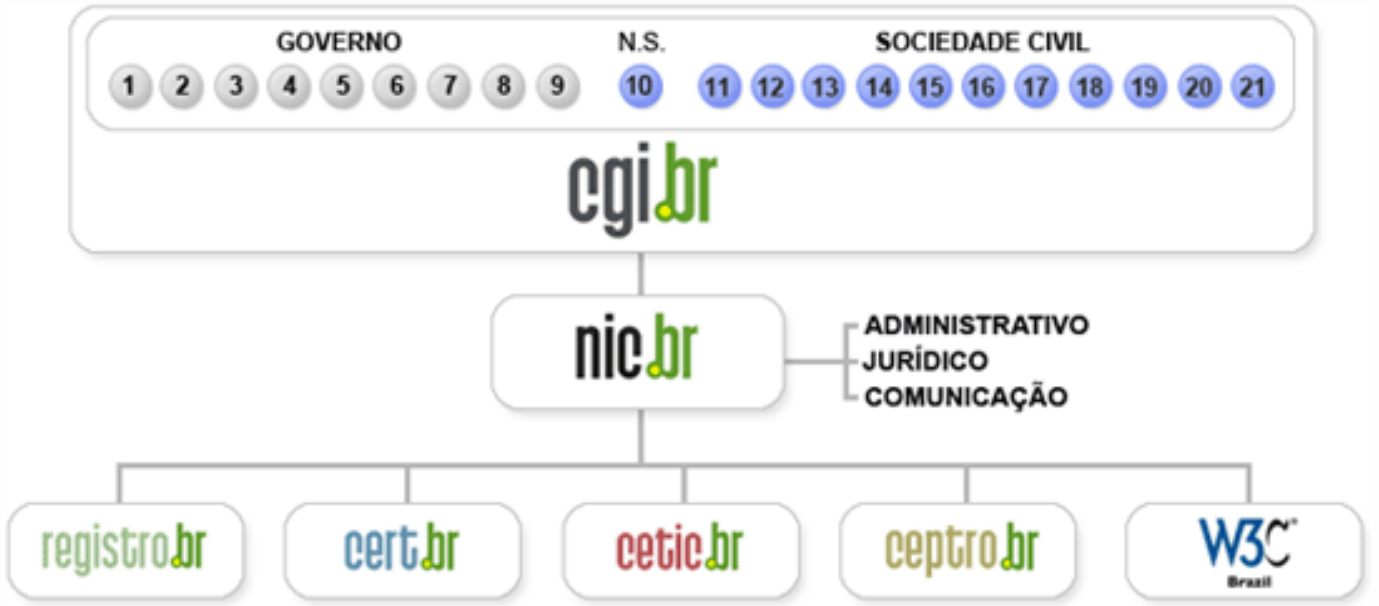
The Honeynet PROJECT

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/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Evolução da Internet no Brasil

1989	Criação e delegação do código de país (ccTLD) ".br" à FAPESP
1991	Primeira *conexão TCP/IP brasileira, realizada entre a FAPESP e o Energy Sciences Network* (ESNet) por meio do Fermilab *(Fermi National Accelerator Laboratory)*
1995	Criação do CGI.br (Portaria Interministerial MC/MCT nº 147, de 31 de maio) com a missão de coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados
1995	Criação do Registro.br
1997	Criação do CERT.br (à época NBSO)
2005	Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil

http://www.nic.br/imprensa/releases/2010/rl-2010-12.htm

Agenda

- **Ataques de negação de serviço**
  - introdução
  - objetivos
  - motivação
  - impactos
- **Tipos de Ataques**
- **Cenário Atual**
- **Prevenção**
- **Tendências e Desafios**
- **Referências**

Ataques de Negação de Serviço

cert.br nic.br cgi.br

Definições

- **DoS - *Denial of Service***
  - negação de serviço
  - técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede
- **DDoS – *Distributed Denial of Service***
  - negação de serviço distribuído
  - técnica pela qual um atacante utiliza, de forma **coordenada** e **distribuída**, um **conjunto** de computadores para tirar de operação um serviço, um computador ou uma rede
- **Objetivo:**
  - exaurir os recursos de uma rede, aplicação ou serviço de forma que usuários legítimos não possam acessá-los
- **Não é invasão**

Principais alvos

- ***Sites* de:**
  - jogos
  - comércio eletrônico
  - bancos
  - governo
  - notícias
  - partidos políticos
  - grandes eventos/patrocinadores

- **Qualquer máquina ou sistema acessível via Internet**

Moticação dos ataques

- ***Hacktivismo***
- **Retaliação**
- **Extorsão**
- **Vandalismo**
- **Concorrência desleal**
- **Tática de distração**
- **Prejudicar outros usuários**
- **Adiamento de prazos**
- **Demonstrar a capacidade a possíveis clientes**
- **Qualquer tipo de descontentamento**
- **Causas desconhecidas**

Impactos

- **Diretos:**
  - imagem
  - credibilidade
  - ameaça para a continuidade dos negócios
  - serviços e recursos legítimos não disponíveis
  - aumento de gastos

- **Colaterais:**
  - excesso de *logs*
  - problemas com *backup*
  - reflexos em outras redes (*upstream)*
  - reflexos em clientes do mesmo provedor de:
    - *hosting*
    - *clouding*

Como são realizados

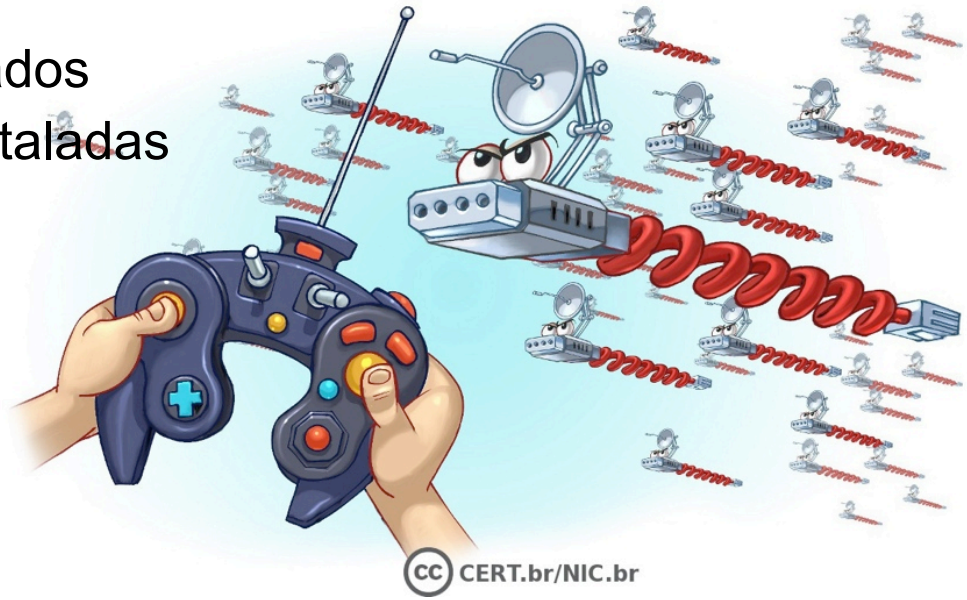
cert.br nic.br cgi.br

Participação espontânea de usuários

- **Sentimento de participação**
- **Geralmente causam poucos danos**
- **Ataques "*TANGO DOWN*" organizados por meio de:**
  - canais de IRC
  - redes sociais
- **Uso de ferramentas**
  - LOIC
  - R.U.DY (aRe yoU Dead Yet?),
  - Slowloris

Botnets (1/2)

- ***R*ede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots**
- **Servidores, computadores, dispositivos móveis e CPEs com:**
  - serviços vulneráveis
  - serviços mal configurados
  - ferramentas DDoS instaladas



Botnets (2/2)

- ***Russian Underground*** **– Serviços disponíveis**

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

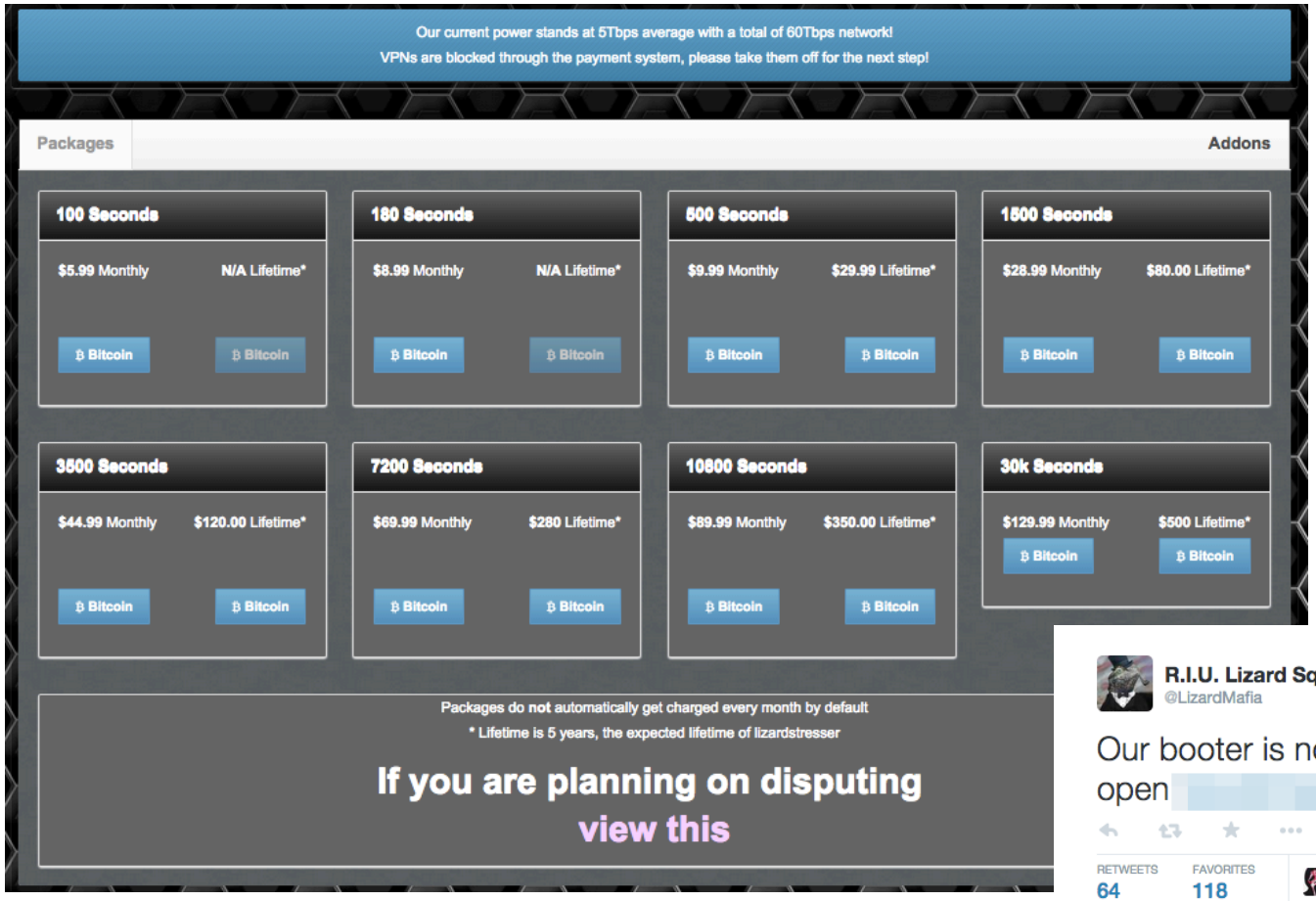
Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Booters (1/2)

- ***IP stresser*, *DDoSers*, *DDoS as a Service***
- **Serviço abertamente vendido na Internet**
- **Tentam se passar por serviços legítimos**
- **Utilizam máquinas alugadas e/ou *botnets***
- ***Front end Web***
- **Permitem ao usuário selecionar:**
  - tipo de ataque
  - duração do ataque
- **Preços muito baixos**

Booters (2/2)



http://www.theguardian.com/technology/2015/jan/12/lizard-squad-lizardstresser-hacked-home-routers

Tipos de Ataques

cert.br nic.br cgi.br

Ataques na camada de aplicação

- **Exploram características da aplicação (camada 7)**
- **Mais difíceis de serem detectados**
- **Exemplos:**
  - HTTP Flood
  - VoIP (SIP INVITE Flood)

Ataques de exaustão de protocolo

- **Tentam consumir as tabelas de conexão de estado**
- **Presentes em:**
  - servidores de aplicação
  - *firewalls*
  - IPS
- **Exemplos:**
  - fragmentação
  - TCP *Syn Flood*

Ataques volumétricos

- **Consomem banda na rede/serviço alvo ou entre a rede/serviço alvo e o resto da Internet**
- **Causam congestionamento**
- **Tipos:**
  - grande quantidade de “pequenas” máquinas
  - pequena quantidade de “grandes” máquinas
  - DRDoS

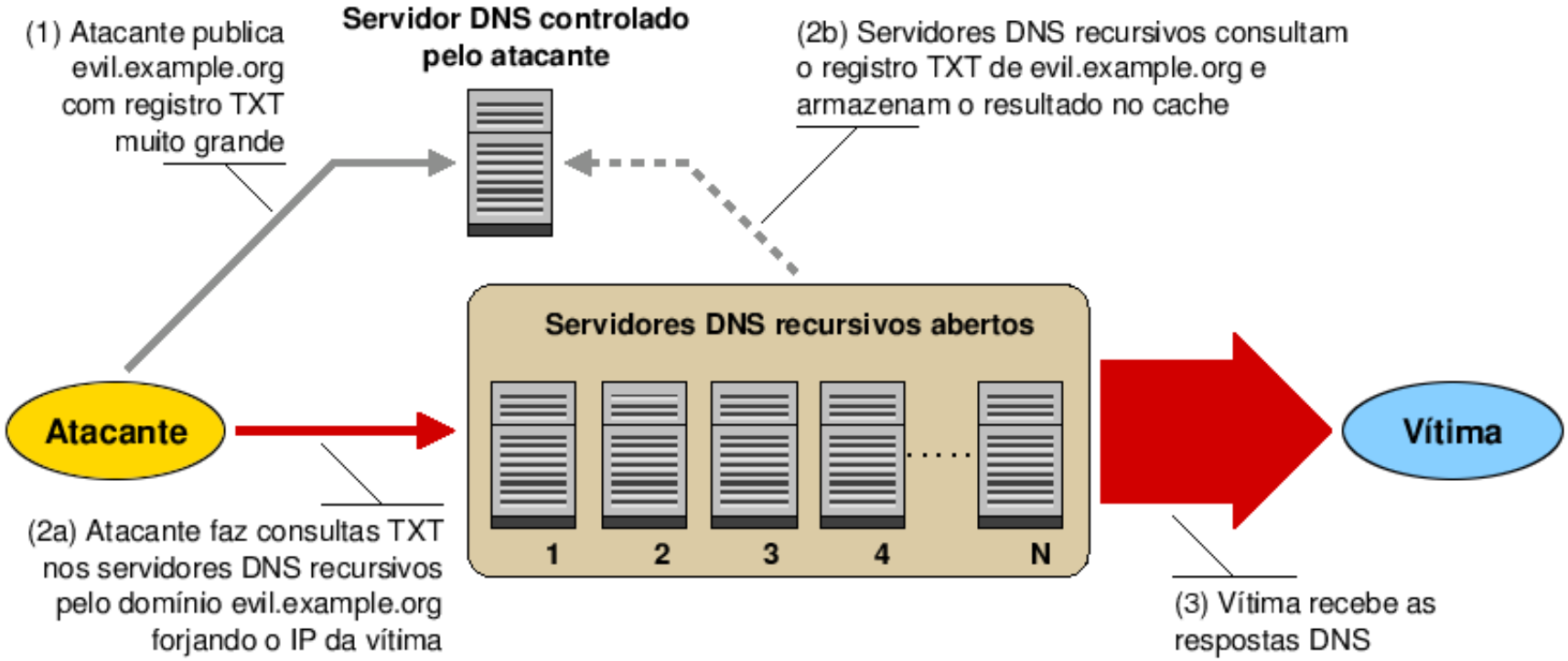
Ataques volumétricos – DRDoS

- ***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

DRDoS
Exemplo de Funcionamento Abusando DNS



Amplificação de DNS (53/UDP)

```
14:35:45.162708 IP (tos 0x0, ttl 49, id 46286, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.71, saveroads.ru.[|domain]

14:35:45.163029 IP (tos 0x0, ttl 49, id 46287, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.72, saveroads.ru.[|domain]

14:35:45.164011 IP (tos 0x0, ttl 49, id 46288, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.73, saveroads.ru.[|domain]
```

Amplificação de NTP (123/UDP)

```
19:08:57.264596 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 cca8 d704 032a  .....{c........*
     0x0020:  0006 0048 0000 0021 0000 0080 0000 0000  ...H...!........
     0x0030:  0000 0005 c6fb 5119 xxxx xxxx 0000 0001  ......Q..*x.....
     0x0040:  1b5c 0702 0000 0000 0000 0000            .\..........

19:08:57.276585 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 03a7 d707 032a  .....{c........*
     0x0020:  0006 0048 0000 000c 0000 022d 0000 0000  ...H.......-....
     0x0030:  0000 001c 32a8 19e0 xxxx xxxx 0000 0001  ....2....*x.....
     0x0040:  0c02 0702 0000 0000 0000 0000            ............

19:08:57.288489 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 e8af d735 032a  .....{c......5.*
     0x0020:  0006 0048 0000 00bf 0000 782a 0000 0000  ...H......x*....
     0x0030:  0000 0056 ae7f 7038 xxxx xxxx 0000 0001  ...V..p8.*x.....
     0x0040:  0050 0702 0000 0000 0000 0000            .P..........
```

Amplificação de Chargen (19/UDP)

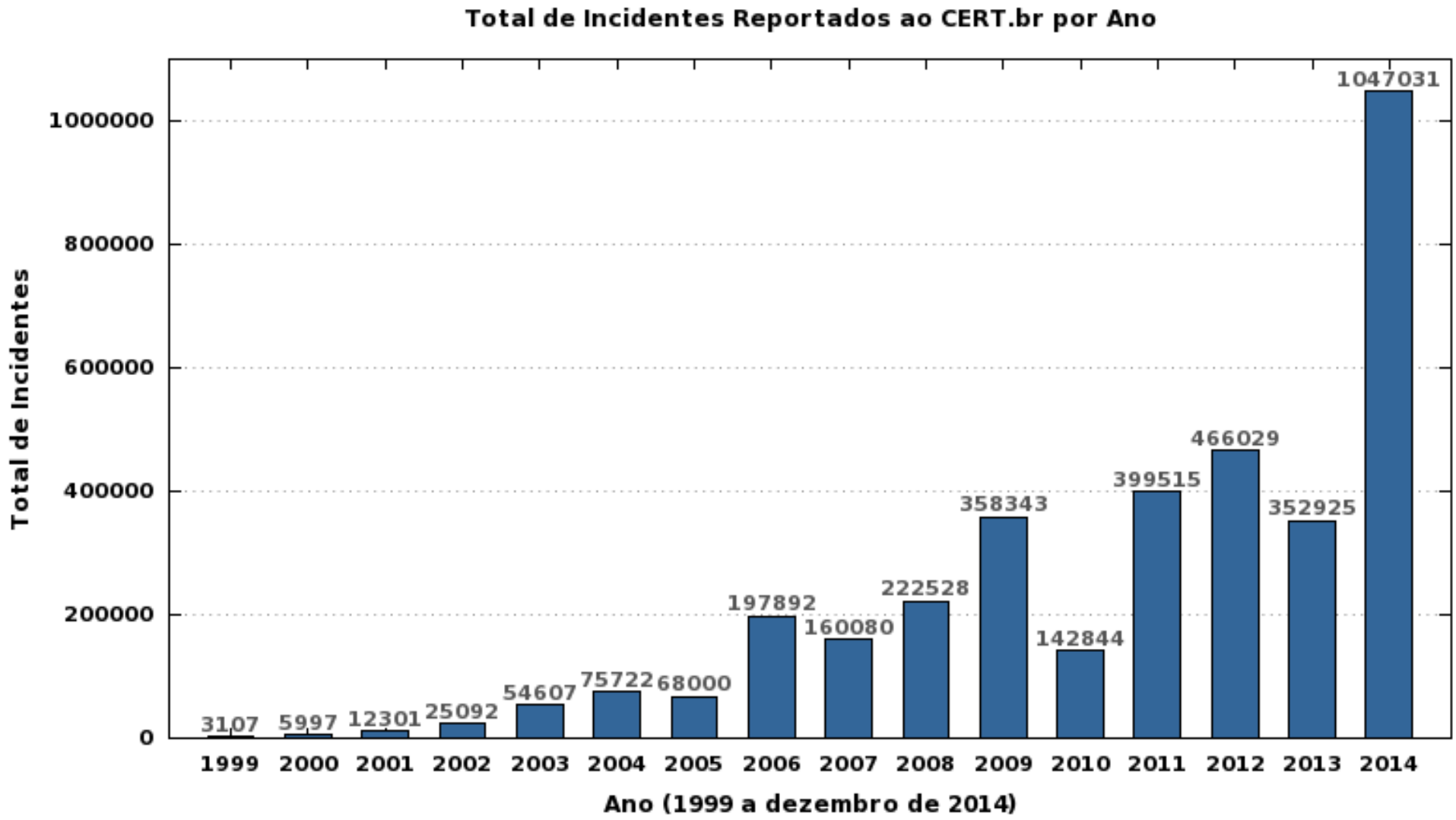
```
Nov 17 00:50:28.142388 IP vitima.32729 > IP amplificador.19: udp 1 [tos
0x2
8]
  0000: 4528 001d f1fb 0000 f411 65c4 xxxx xxxx  E(........e.....
  0010: xxxx xxxx 7fd9 0013 0009 0000 01         ..............

Nov 17 00:50:28.206383 IP amplificador.19 > IP vitima.32729: udp 74
  0000: 4500 0066 4bab 0000 4011 bff4 xxxx xxxx  E..fK...@.......
  0010: xxxx xxxx 0013 7fd9 0052 69ae 2122 2324  .........Ri.!"#$
  0020: 2526 2728 292a 2b2c 2d2e 2f30 3132 3334  %&'()*+,-./01234
  0030: 3536 3738 393a 3b3c 3d3e 3f40 4142 4344  56789:;<=>?@ABCD
  0040: 4546 4748 494a 4b4c 4d4e 4f50 5152 5354  EFGHIJKLMNOPQRST
  0050: 5556 5758 595a 5b5c 5d5e 5f60 6162 6364  UVWXYZ[\]^_`abcd
  0060: 6566 6768 0d0a                           efgh..
```

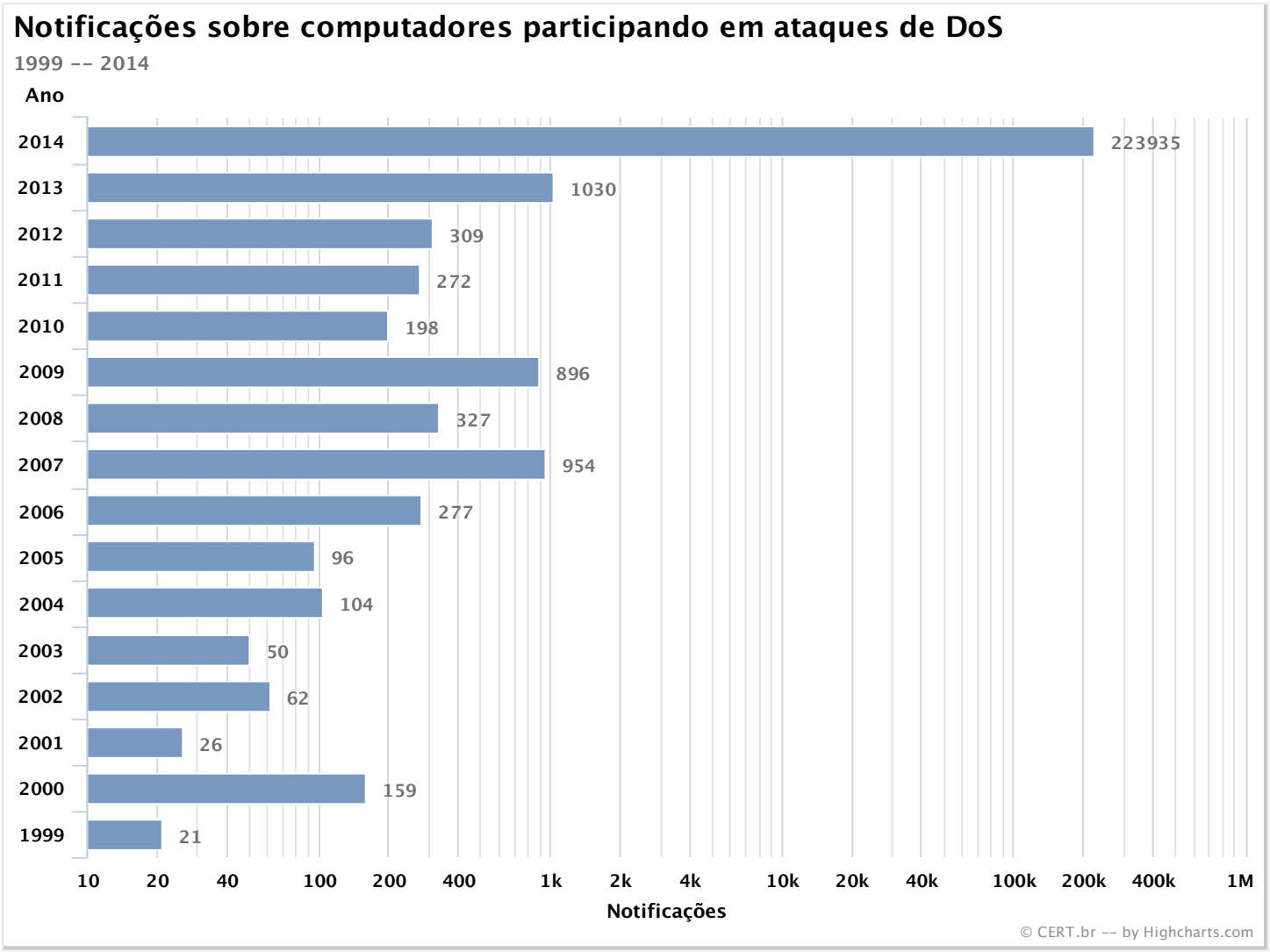
Cenário Atual

cert.br nic.br cgi.br

Estatísticas CERT.br – 2014



Estatísticas DDoS CERT.br – 2014



Estatísticas DDoS CERT.br – 2014

- **223.935 notificações sobre computadores participando em ataques DoS**
- **217 vezes maior que o ano de 2013**
- **Mais de 90% usando amplificação**
  - Protocolos mais abusados:
    - 161/UDP (SNMP)
    - 1900/UDP (SSDP)
    - 53/UDP (DNS)
    - 123/UDP (NTP)
    - 27015/UDP (protocolo da STEAM)
    - 19/UDP (CHARGEN)

Arbor Q4-2014

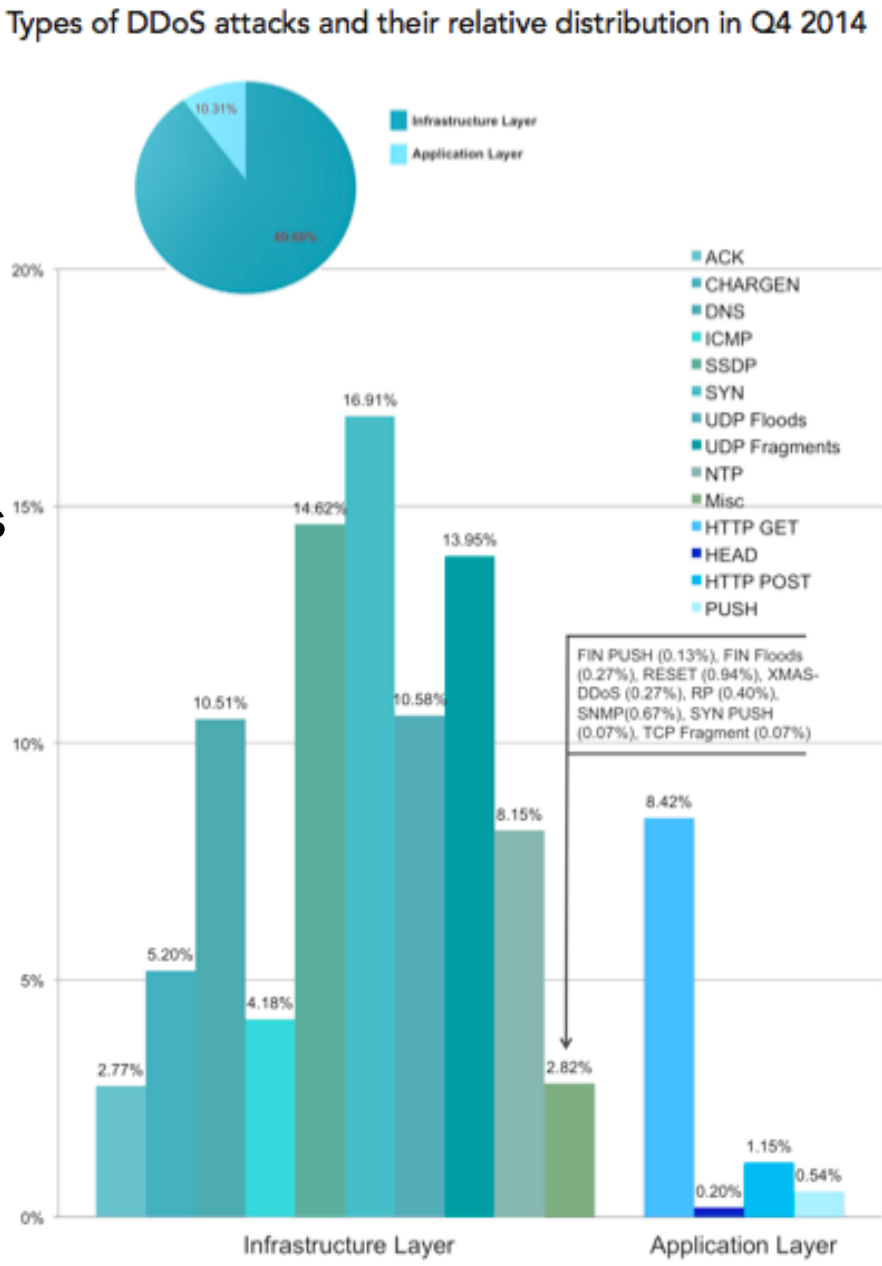
- **Maiores ataques:**
  - 400, 300, 200 e 170 Gbps
- **Principais protocolos usados DRDoS:**
  - DNS, NTP, SNMP, CharGen, SSDP
- **Tipos de ataques:**
  - 65% volumétrico
  - 20% exaustão de protocolo
  - 17% aplicação

Worldwide Infrastructure Security Report - 2014
http://www.arbornetworks.com/resources/infrastructure-security-report

Akamai Q4-2014

- Aumento de 90% nos ataques DDoS comparado a Q4-2013
- 9 ataques com +100 Gbps
- Maior 158 Gbps
- Alvo principal: empresas de jogos
- Ataques mistos
- Ataques baseados em UDP foram os mais comuns
- Protocolos mais usados
  - NTP, CHARGEN e SSDP (DRDoS)
  - SSDP flood – ataque de 106 Gbps
- *botnets* alugadas para ataques volumétricos

Akamai - The State of the Internet [security] / Q4 2014 / www.stateoftheinternet.com



DRDoS - Spamhaus

RISK ASSESSMENT / SECURITY & HACKTIVISM

Spamhaus DDoS grows to Internet-threatening size

More than 300 Gb/s of traffic aimed at the anti-spam site's hosting.

by **Peter Bright** - Mar 27, 2013 4:30pm BRT

Share Tweet 258

Last week, anti-spam organization Spamhaus became the victim of a large denial of service attack, intended to knock it offline and put an end to its spam-blocking service. By using the services of CloudFlare, a company that provides protection and acceleration of any website, Spamhaus was able to weather the storm and stay online with a minimum of service disruptions.

Since then, the attacks have grown to more than 300 Gb/s of flood traffic: a scale that's threatening to clog up the Internet's core infrastructure and make access to the rest of the Internet slow or impossible.

http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/

DRDoS - Blizzard

NOV 14, 2014 @ 1:18 PM 40,512 VIEWS

Blizzard Confirms DDOS Attack On World Of Warcraft

Dave Thier
CONTRIBUTOR

I write about video games and technology. **FULL BIO**

Opinions expressed by Forbes Contributors are their own.

FOLLOW

Blizzard encountered some of the usual launch headaches when it released Warlords of Draenor, the fifth expansion to its landmark MMO World of Warcraft: too many people trying to access the new zones at once, server traffic and the like. But the game also ran into a much larger problem when the North American Servers were hit by a Distributed Denial of Service attack last night, preventing the servers from working properly for hours. Blizzard confirmed the attack in a blog post on Battle.net:

http://www.forbes.com/sites/davidthier/2014/11/14/blizzard-confirms-ddos-attack-on-world-of-warcraft/

CPEs e *Stressers Bots*

Lizard Squad's LizardStresser booter runs on 'hacked home routers'

Security expert Brian Krebs warns that internet users who didn't change their default passwords may be unknowingly aiding hacking group

Hacking group Lizard Squad may have been using "thousands of hacked home Internet routers" to run its LizardStresser service, which helps anyone launch distributed denial of service (DDoS) attacks to knock websites offline.

"in addition to turning the infected host into attack zombies, the malicious code uses the infected system to scan the Internet for additional devices that also allow access via factory default credentials, such as 'admin/admin,' or 'root/12345'," wrote Krebs.

http://www.theguardian.com/technology/2015/jan/12/lizard-squad-lizardstresser-hacked-home-routers

Prevenção

cert.br nic.br cgi.br

Não faça parte do problema
Usuários finais

- **Manter computadores, dispositivos móveis e equipamentos de rede seguros**
  - instalar todas as atualizações disponíveis
  - manter o sistema operacional atualizado
  - utilizar mecanismos de segurança
    - antivírus
    - *firewall* pessoal
  - desabilitar serviços que não estão sendo utilizados
  - trocar as senhas padrão
  - habilitar verificação em duas etapas
  - ser cuidadoso ao clicar em *links*

Não faça parte do problema
Desenvolvedores de aplicações Web

- ***Web Application Firewall***
- **Desenvolvimento de *software* deve incluir**
  - levantamento de requisitos de segurança
  - testes de carga
  - super dimensionamento
  - balanceamento de carga
  - páginas menos pesadas
  - páginas estáticas em períodos de pico

Não faça parte do problema
Provedores/Administradores de Redes

- **Proteger os CPEs dos clientes:**
  - usar senhas bem elaboradas com grande quantidade de caracteres e que não contenham dados pessoais, palavras conhecidas e sequências de teclado
  - não usar senhas padrão
  - manter o *firmware* atualizado

Habilitar filtro *anti-spoofing* (BCP38)

http://bcp.nic.br

Não faça parte do problema
Provedores/Administradores de Redes

- **Configurar corretamente serviços que podem ser usados em amplificação**
  - DNS
    - contactar administradores de servidores vulneráveis
    - recursivos apenas para sua rede
      - considerar uso do Unbound
    - nos autoritativos:
      - desabilitar recursão
      - considerar Response Rate Limit (RRL)
  - NTP
    - considerar uma implementação mais simples
      - OpenNTPD
    - atualizar para a versão 4.2.7 ou superior
    - desabilitar a função monitor no arquivo ntpd.conf

Não faça parte do problema
Provedores/Administradores de Redes

- **Configurar corretamente serviços que podem ser usados em amplificação**
  - SNMP
    - quando possível utilizar a versão 3
    - não utilizar a comunidade Public
  - SSDP
    - desabilitar o acesso aos equipamentos via WAN
    - desabilitar UPnP, se não for necessário
  - Demais protocolos
    - Habilitar apenas quando necessário

Preparação
Provedores/Administradores de Redes

- **Adotar medidas pró-ativas**
  - possuir um sistema autônomo
    - mais de um *link* de conexão com a Internet
  - *overprovision*
    - ter *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

Detecção

- **Verificar fluxos de entrada e saída de tráfego**
  - permitem identificar:
    - mudanças de padrão
    - comunicação com C&C
- **"*Intrusion Detection*"**
  - IDS / IPS, *Firewall*, Antivírus
- **"*Extrusion Detection*"**
  - *Flows*, Honeypots, Passive DNS
  - Notificações de incidentes
  - *Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)

Como mitigar os ataques

- **Filtrar trafego por IP ou porta de origem ou destino**
  - *firewall*, IPSs, *switches* e roteadores
- **Usar *rate-limiting* e ACLs em roteadores e *switches***
- **Contactar *upstream***
  - aplicar filtros
  - *nullrouting/sinkholing*
  - serviços de mitigação de DDoS
- **Melhorar a infraestrutura**
  - mais banda, roteador com mais capacidade
- **Mover para CDN (*Content Delivery Network*)**
- **Contratar serviços de mitigação**
  - pode afetar a confidencialidade das informações

Tendências e Desafios

cert.br nic.br cgi.br

Tendências e desafios (1/3)

- **IoT**
  - cada vez mais dispositivos conectados
  - podendo participar de botnets e DDoS
- ***Botnets* formadas por:**
  - servidores *Web*
  - CPEs
  - máquinas de usuários
  - dispositivos móveis
- **Ataques cada vez mais:**
  - potentes
  - fáceis de serem realizados
  - acessíveis e baratos (para quem ataca)

Tendências e desafios (2/3)

- **Usuários não são especialistas**
  - cada vez maior o número de dispositivos vulneráveis e que precisam de manutenção
    - computadores
    - dispositivos móveis
    - CPEs
    - IoT
- **Sistemas cada vez mais complexos**
  - segurança não é parte dos requisitos
  - falta de profissionais capacitados para desenvolver com requisitos de segurança
  - pressão econômica para lançar, mesmo com problemas

Tendências e desafios (3/3)

- **Administradores de sistemas e redes**
  - tem que “correr atrás do prejuízo”
  - ferramentas:
    - de segurança não conseguem remediar os problemas
    - de ataque “estão a um clique de distância”
  - falta de pessoal treinado no Brasil para lidar com redes e com segurança em IPv4
    - falta ainda maior de pessoal com habilidades em IPv6
    - IPv6 não pode ser mais ignorado
    - http://ipv6.br

Referências

cert.br nic.br cgi.br

Referências

- **Portal de Boas Práticas para a Intenet no Brasil**
  http://bcp.nic.br
- **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**
  http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/
- **Am*plification Hell: Revisiting Network Protocols for DDoS Abuse***
  ***http*://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse**
- ***Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks***
  https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer
- ***Network DDoS Incident Response Cheat Sheet***
  https://zeltser.com/ddos-incident-cheat-sheet/
- ***Exit from Hell? Reducing the Impact of Amplification DDoS Attacks***
  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer

Revista .br

- **Ano 06 | 2015 | Edição 08**

  Mercenários Digitais

http://cgi.br/publicacao/revista-br ano-06-2015-edicao-08/

Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no site, via *Twitter* e RSS
http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- **Redes Sociais**
- **Senhas**
- **Comércio Eletrônico**
- **Privacidade**
- **Dispositivos Móveis**
- ***Internet Banking***
- **Computadores**
- **Códigos Maliciosos**
- **Verificação em Duas Etapas**
- **Redes**

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

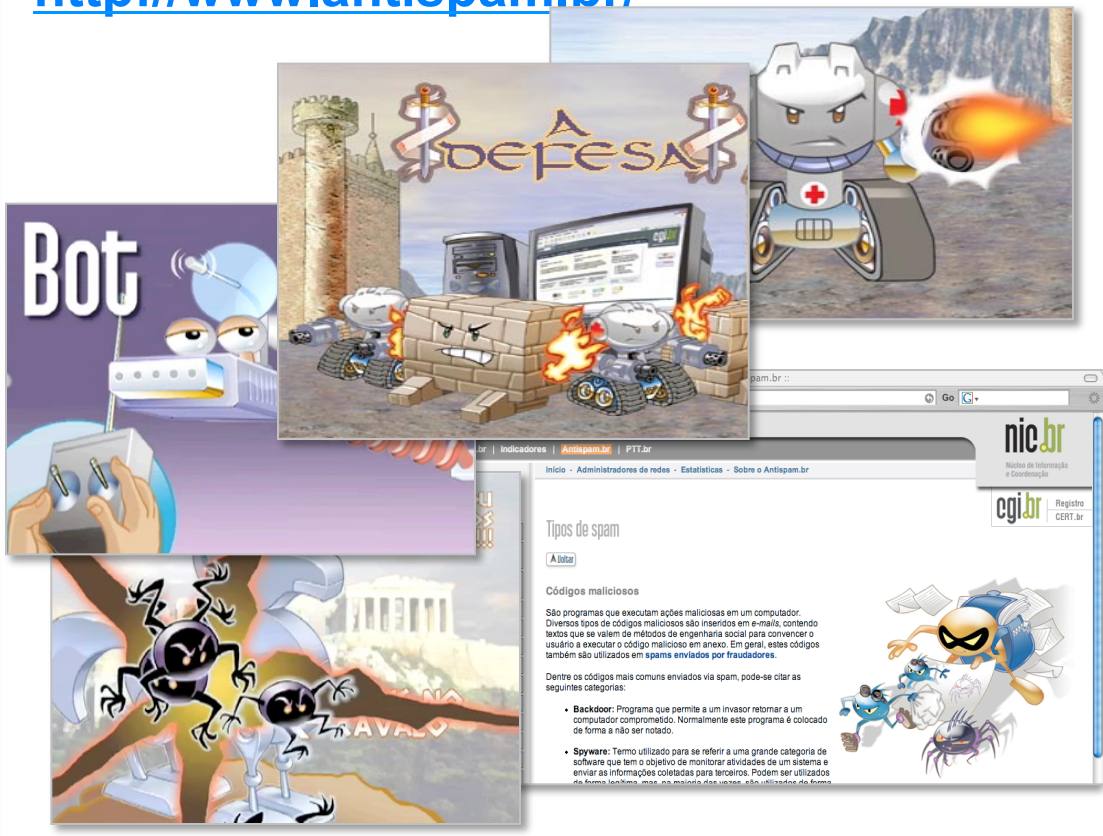
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/



Obrigada

www.cert.br

miriam@cert.br

@certbr

21 de maio de 2015

nic.br cgi.br

www.nic.br | www.cgi.br