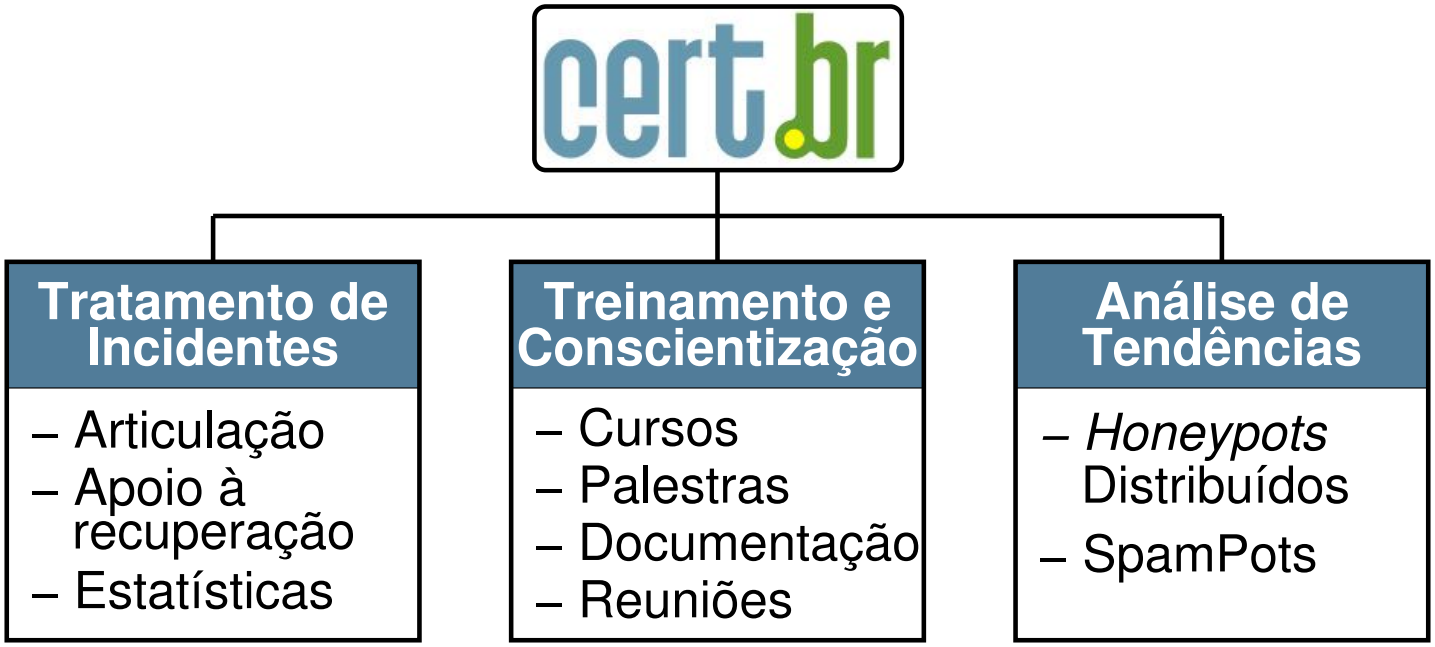
INFOESTE 2018
Presidente Prudente, SP
17 de maio de 2018

Ataques DDoS:
Das origens aos dias atuais

Marcus Vinícius Lahr Giraldi
marcus@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
MEMBER

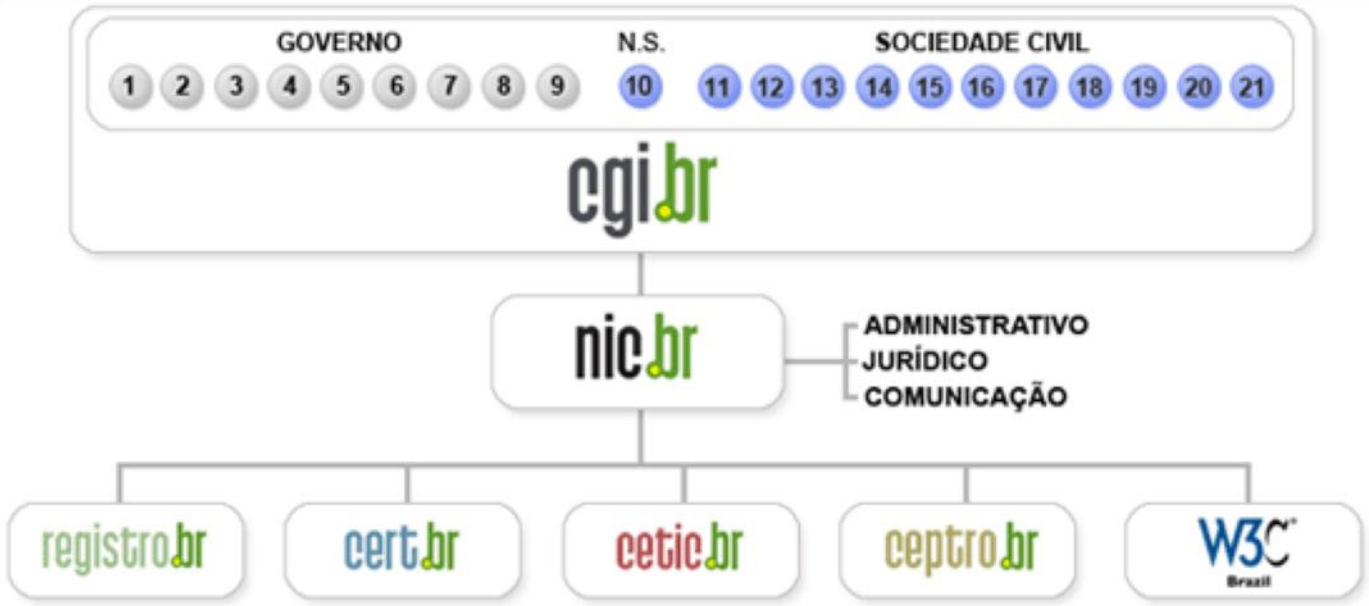
APWG
RESEARCH PARTNER
www.antiphishing.org

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**

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

https://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**

Motivação dos ataques (1/2)

- ***Hacktivismo***
- **Retaliação**
- **Extorsão**
- **Vandalismo**
- **Concorrência desleal**

Motivação dos ataques (2/2)

- **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**

Impactos 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
  - HOIC
  - 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

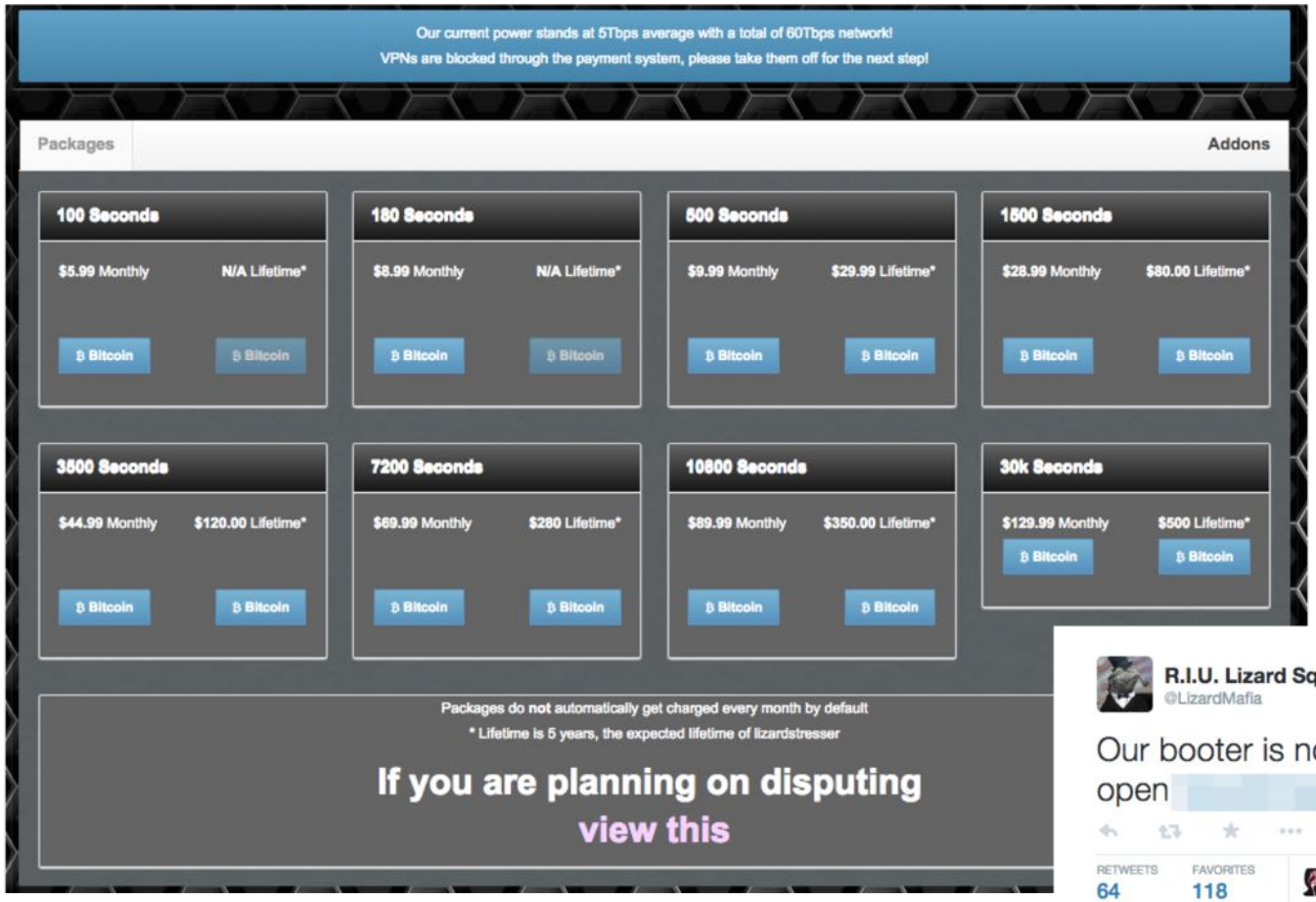
Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

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

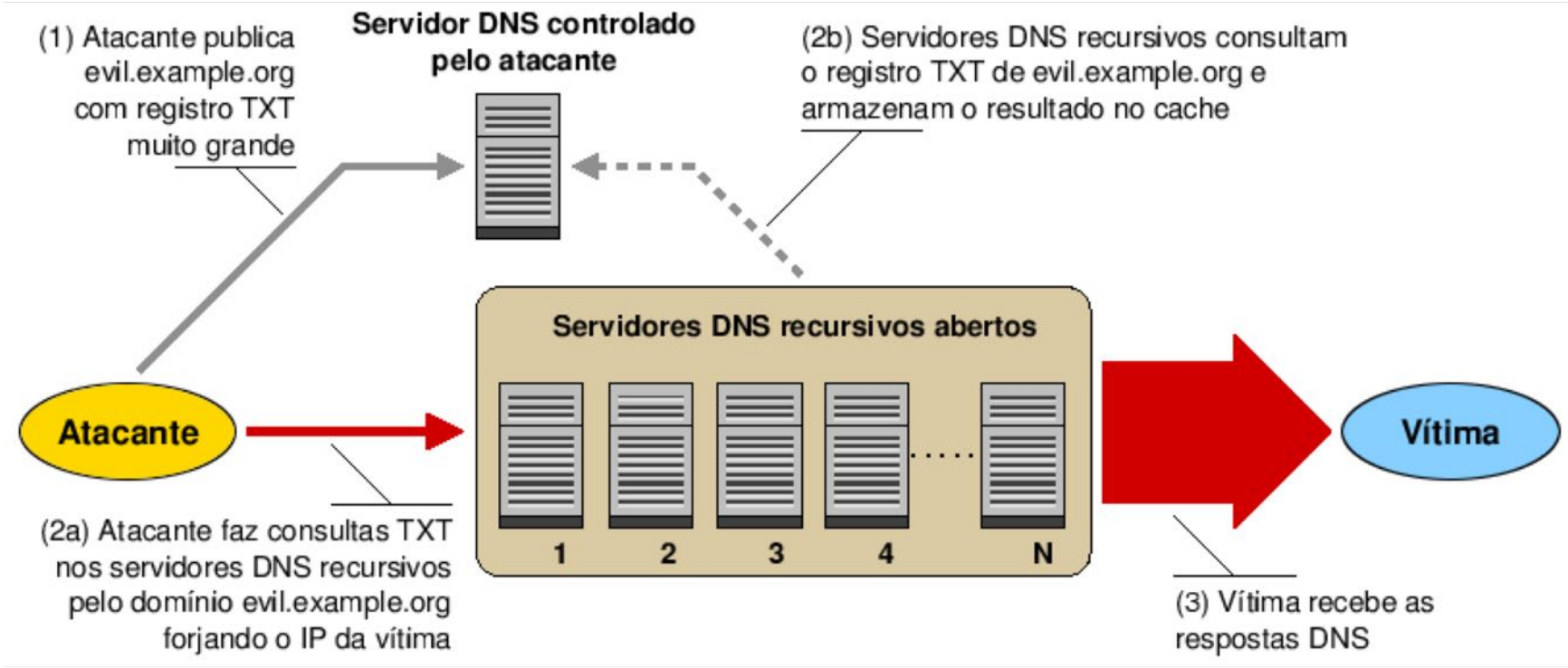
Ataques volumétricos – DRDoS

- ***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

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..
```

Amplificação de memcached (11211/UDP)

```
00 00 00 00 00 02 00 00 53 54 41 54 20 70 69 64 |........STAT pid|
20 37 32 32 38 0D 0A 53 54 41 54 20 75 70 74 69 | 7228..STAT upti|
6D 65 20 39 33 39 35 32 34 37 0D 0A 53 54 41 54 |me 9395247..STAT|
20 74 69 6D 65 20 31 35 32 36 34 38 33 31 34 33 | time 1526483143|
0D 0A 53 54 41 54 20 76 65 72 73 69 6F 6E 20 31 |..STAT version 1|
2E 35 2E 34 0D 0A 53 54 41 54 20 6C 69 62 65 76 |.5.4..STAT libev|
65 6E 74 20 32 2E 30 2E 32 31 2D 73 74 61 62 6C |ent 2.0.21-stabl|
65 0D 0A 53 54 41 54 20 70 6F 69 6E 74 65 72 5F |e..STAT pointer_|
73 69 7A 65 20 36 34 0D 0A 53 54 41 54 20 72 75 |size 64..STAT ru|
73 61 67 65 5F 75 73 65 72 20 36 30 34 39 30 2E |sage_user 60490.|
37 38 32 30 30 33 0D 0A 53 54 41 54 20 72 75 73 |782003..STAT rus|
61 67 65 5F 73 79 73 74 65 6D 20 34 37 30 33 32 |age_system 47032|
2E 30 31 33 30 34 37 0D 0A 53 54 41 54 20 6D 61 |.013047..STAT ma|
78 5F 63 6F 6E 6E 65 63 74 69 6F 6E 73 20 31 30 |x_connections 10|
...

31 35 37 39 33 0D 0A 53 54 41 54 20 6D 6F 76 65 |15793..STAT move|
73 5F 77 69 74 68 69 6E 5F 6C 72 75 20 31 38 39 |s_within_lru 189|
31 35 34 0D 0A 53 54 41 54 20 64 69 72 65 63 74 |154..STAT direct|
5F 72 65 63 6C 61 69 6D 73 20 32 30 37 32 30 0D |_reclaims 20720.|
0A 53 54 41 54 20 6C 72 75 5F 62 75 6D 70 73 5F |.STAT lru_bumps_|
64 72 6F 70 70 65 64 20 30 0D 0A 45 4E 44 0D 0A |dropped 0..END..|
```

Histórico

cert.br nic.br cgi.br

1996 - Panix

HACKERS STRIKE AT N.Y. INTERNET ACCESS COMPANY

By Elizabeth Corcoran September 12, 1996

Normally, Panix's computers -- like many others on the Internet -- can hold fewer than a dozen such packets. But on Friday, several of Panix's computers began receiving as many as 50 of such packets per second. Like Lucy and Ethel working in a candy factory on an "I Love Lucy" episode, the Panix computers soon were overwhelmed by a flood of bogus messages.

To try to shield their system from the attack, Panix managers were forced to block all incoming messages for hours at a stretch.

Fonte: https://www.washingtonpost.com/archive/business/1996/09/12/hackers-strike-at-ny-internet-access-company/7db752cc-03f9-4aab-95e2-a0fe70eab609/?utm_term=.b24fe1aa3130

2007 - Estônia

Estonian DDoS Attacks – A summary to date

Jose Nazario on May 17, 2007.

Time sure flies. I looked up from working and noticed I hadn't blogged in a while. And I noticed that I hadn't been analyzing the Estonian DDoS attacks in a week or two.

Attacks	Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11

Attacks	Date
17	less than 1 minute
78	1 min – 1 hour
16	1 hour – 5 hours
8	5 hours to 9 hours
7	10 hours or more

Attacks	Bandwidth measured
42	Less than 10 Mbps
52	10 Mbps – 30 Mbps
22	30 Mbps – 70 Mbps
12	70 Mbps – 95 Mbps

Fonte: https://asert.arbornetworks.com/estonian-ddos-attacks-a-summary-to-date/

2013 - Spamhaus

The attackers were quiet for a day. Then, on March 22 at 18:00 UTC, the attack resumed, peaking at 120Gbps of traffic hitting our network. As we discussed in the previous blog post, CloudFlare uses Anycast technology which spreads the load of a distributed attack across all our data centers. This allowed us to mitigate the attack without it affecting Spamhaus or any of our other customers. The attackers ceased their attack against the Spamhaus website four hours after it started.

Fonte: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

2013 - 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

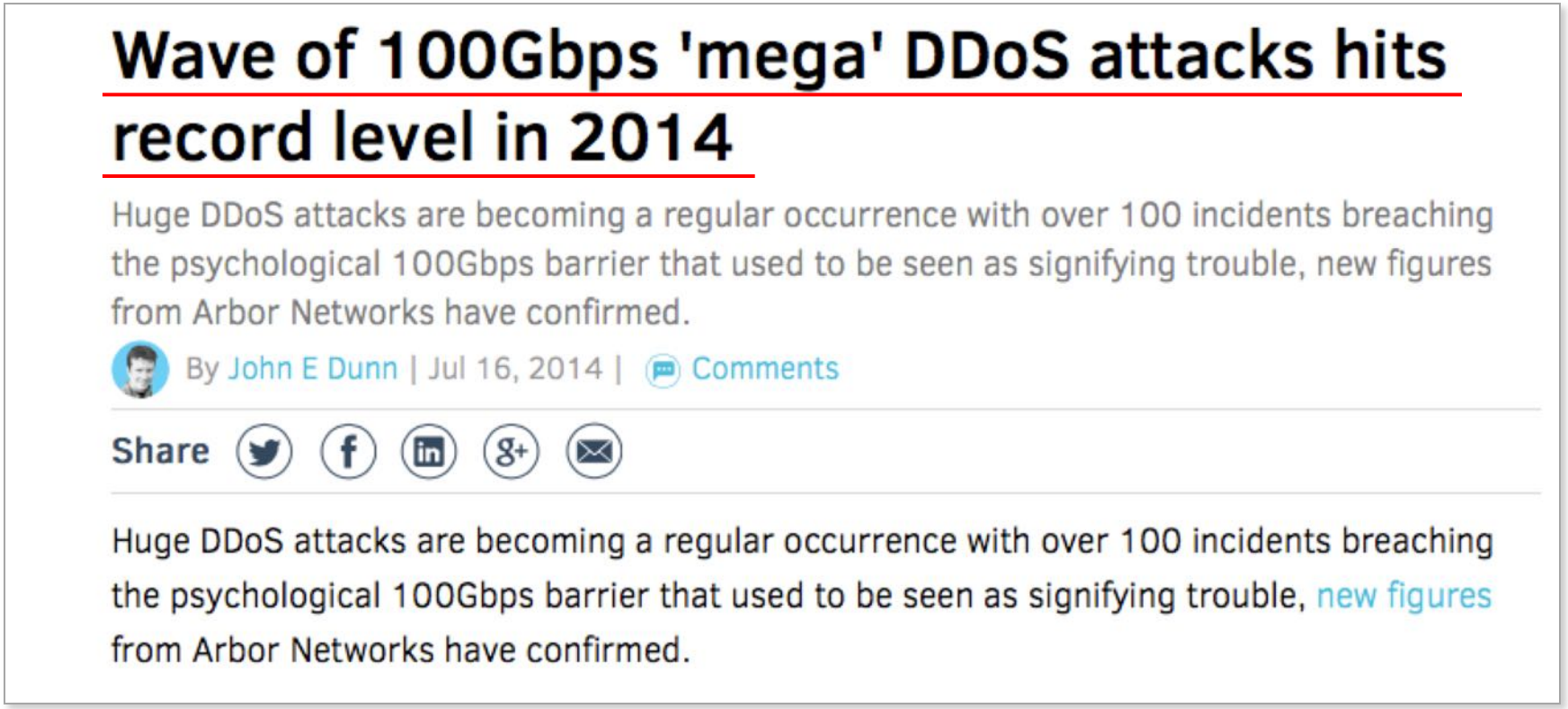
Share Tweet 258

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/

2014 - Múltiplos alvos



Wave of 100Gbps 'mega' DDoS attacks hits record level in 2014

Huge DDoS attacks are becoming a regular occurrence with over 100 incidents breaching the psychological 100Gbps barrier that used to be seen as signifying trouble, new figures from Arbor Networks have confirmed.

By John E Dunn | Jul 16, 2014 | Comments

Share

Huge DDoS attacks are becoming a regular occurrence with over 100 incidents breaching the psychological 100Gbps barrier that used to be seen as signifying trouble, new figures from Arbor Networks have confirmed.

Fonte: http://www.techworld.com/news/security/wave-of-100gbps-mega-ddos-attacks-hits-record-level-in-2014-3531040/

2014 - CloudFlare

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

13 Feb 2014 by Matthew Prince.

On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web. Monday's attack serves as a good case study to examine how these attacks work.

Fonte: https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

2015 - 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.

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

2016 - Blog do Brian Krebs

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

Fonte: http://www.bbc.co.uk/news/amp/37439513

2016 - Dyn DNS

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

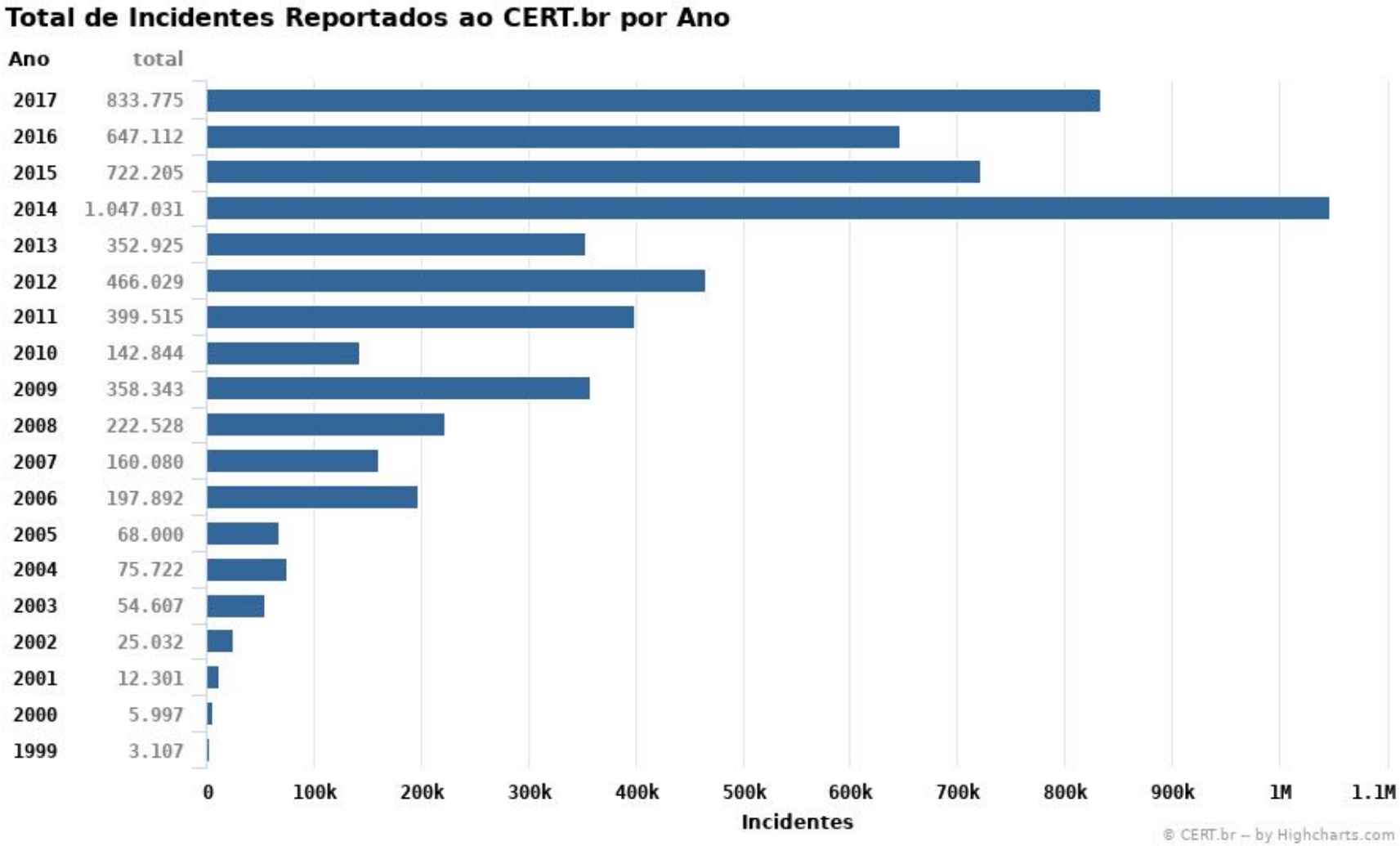
The sound of silence.

Fonte: http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html

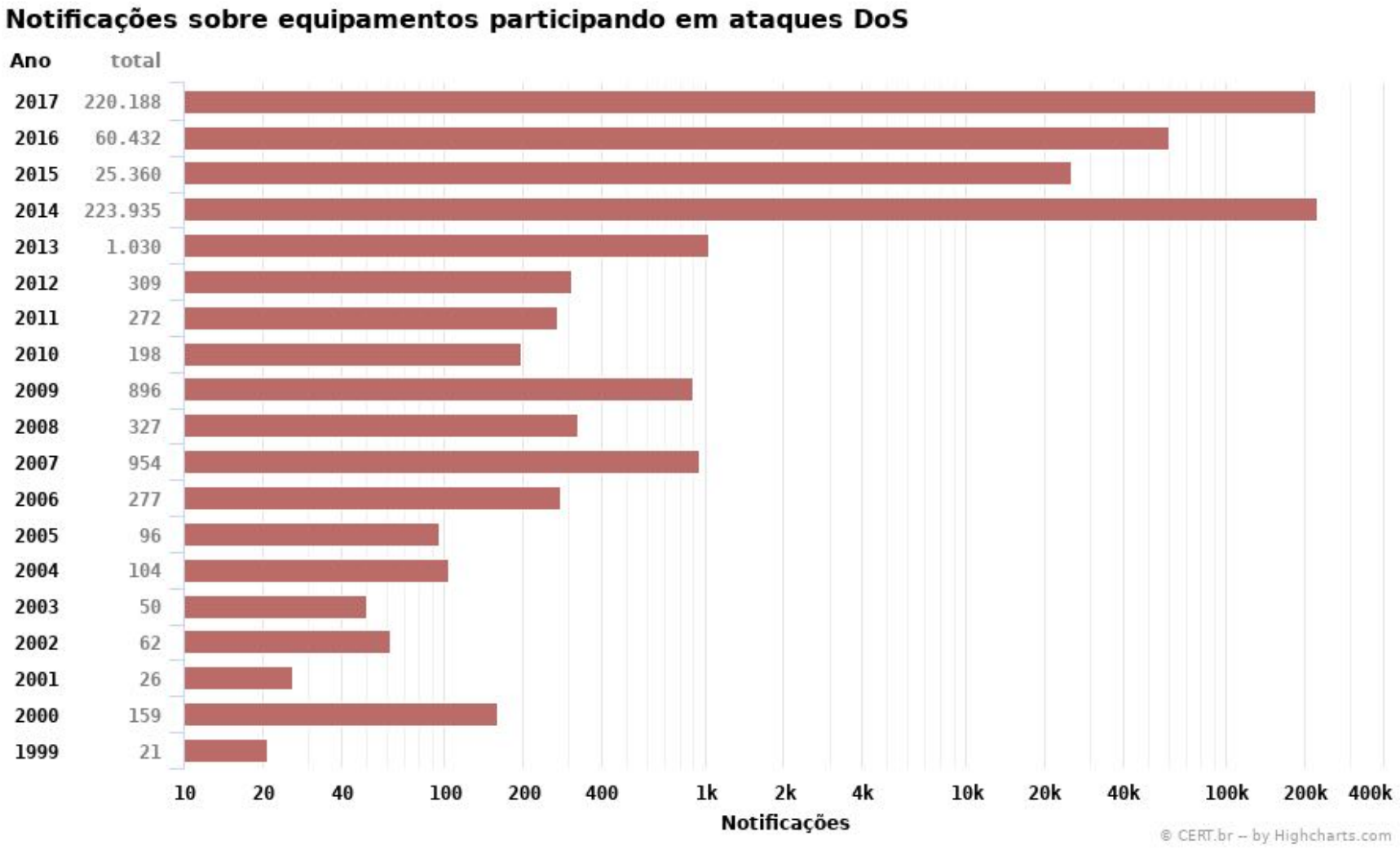
Cenário Atual

cert.br nic.br cgi.br

Estatísticas CERT.br – 2017

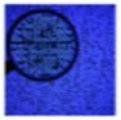


Estatísticas DDoS CERT.br – 2017



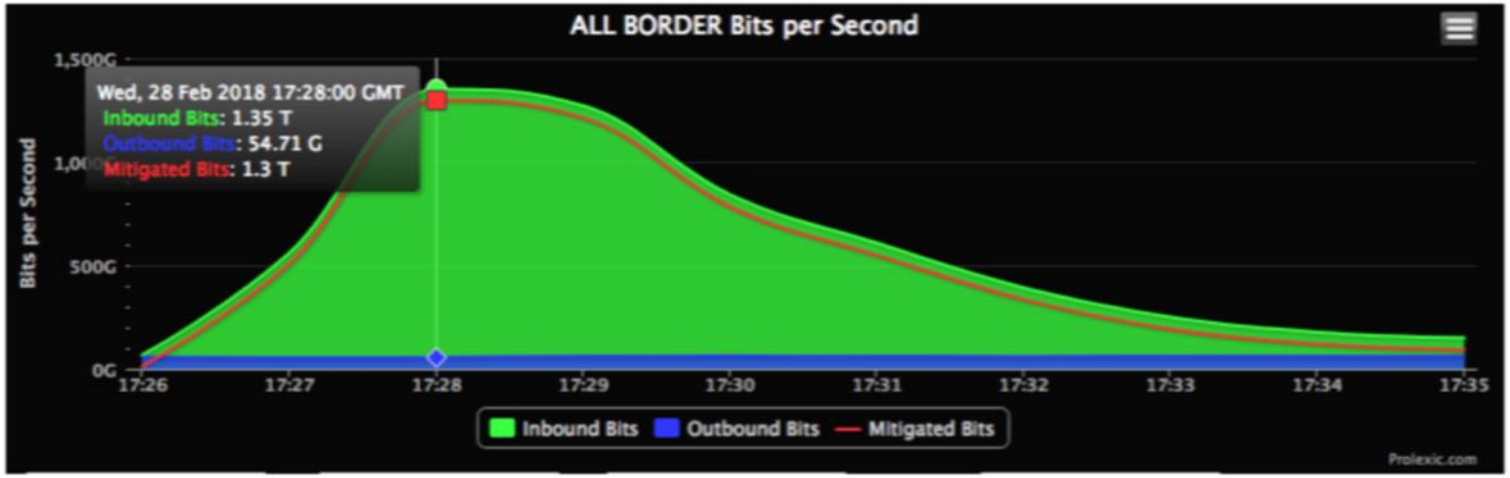
2018 - Akamai

MEMCACHED-FUELED 1.3 TBPS ATTACKS



By Akamai SIRT Alerts **March 1, 2018 7:54 AM**

At 17:28 GMT, February 28th, Akamai experienced a 1.3 Tbps DDoS attack against one of our customers, a software development company, driven by memcached reflection. This attack was the largest attack seen to date by Akamai, more than twice the size of the September, 2016 attacks that announced the Mirai botnet and possibly the largest DDoS attack publicly disclosed. Because of memcached reflection capabilities, it is highly likely that this record attack will not be the biggest for long.



Fonte: https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html

Dispositivos / Serviços que Permitem Amplificação: **Total no Brasil de ASNs e IPs Notificados**

	DNS		SNMP		NTP		SSDP	
2017	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.133	87.953	–	–	981	97.423	–	–
Fevereiro	2.066	67.159	1.681	573.373	–	–	805	37.459
Março	–	–	1.805	604.805	915	104.665	–	–
Abril	2.191	72.124	–	–	861	92.120	812	27.233
Maio	2.280	69.957	1.869	573.400	–	–	839	40.814
Junho	2.183	64.179	1.948	596.348	860	91.257	812	33.805
Julho	–	–	1.963	551.953	841	107.097	–	–
Agosto	2.347	72.677	2.018	554.457	872	108.168	891	27.209
Setembro	2.307	62.283	1.791	406.015	800	89.603	–	–
Outubro	2.328	67.066	1.886	343.674	845	108.605	902	32.056
Novembro	2.279	61.281	–	–	–	–	863	26.999
Dezembro	2.436	62.758	2.001	460.519	–	–	845	27.828
2018	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.412	61.875	2.130	479.247	823	97.075	888	25.982
Fevereiro	2.438	72.185	2.324	559.784	849	93.801	778	20.210
Março	2.476	63.811	2.278	515.345	844	84.483	544	11.431

Legenda: “–” significa que não foi realizada notificação desta categoria no referido mês

Prevenção

Não faça parte do problema!!!

cert.br nic.br cgi.br

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*

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

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)

https://bcp.nic.br

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

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
    - https://ipv6.br

IPv6

by Mark Mayne

February 28, 2018

'First true' native IPv6 DDoS attack spotted in wild

First in-the-wild DDOS IPV6 attack hits servers, with portents of more to come. The DNS dictionary attack originated from around 1,900 different native IPv6 hosts, on more than 650 different networks.

The first documented native IPv6 DDoS attack has been spotted in the wild over the weekend.

The DNS dictionary attack originated from around 1,900 different native IPv6 hosts, on more than 650 different networks and targeted authoritative DNS service Neustar's network.

The distributed attack demonstrates that that hackers are deploying new methods for IPv6 attacks, as widely predicted, not simply replicating IPv4 attacks using IPv6 protocols, according to Neustar.

DDoS

Fonte: https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-in-wild/article/747217/

Referências

cert.br nic.br cgi.br

Referências

- **Portal de Boas Práticas para a Intenet no Brasil** https://bcp.nic.br
- **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos** https://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

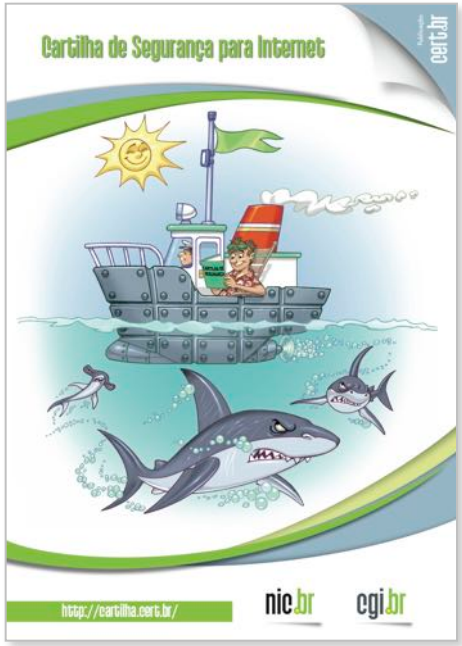
Revista .br

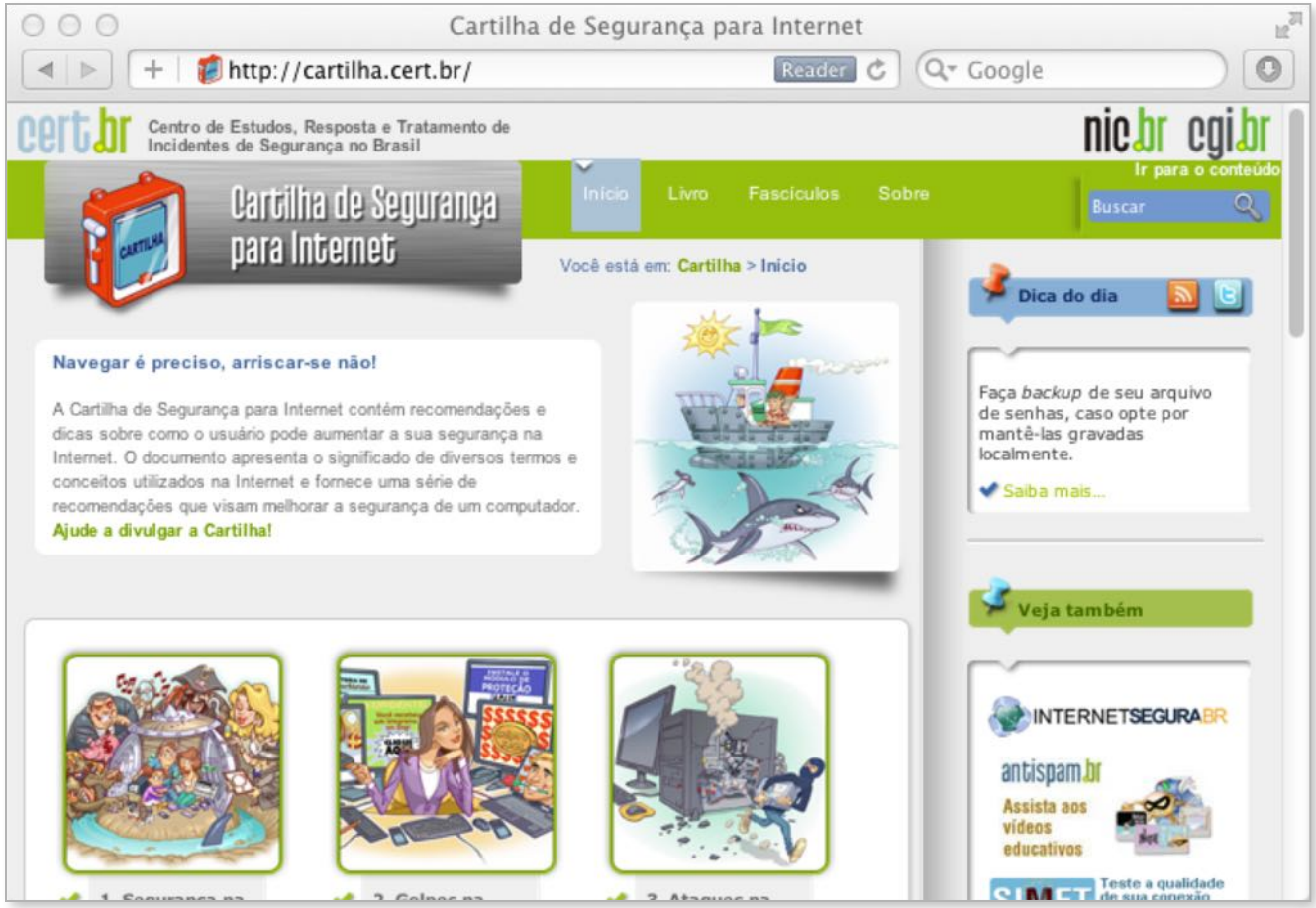
- **Ano 06 | 2015 | Edição 08**
  Mercenários Digitais

https://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
https://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
- Backup
- Boatos

Acompanhados de *Slides* de uso livre para:

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

Outros Materiais para Usuários Finais

Portal Internet Segura

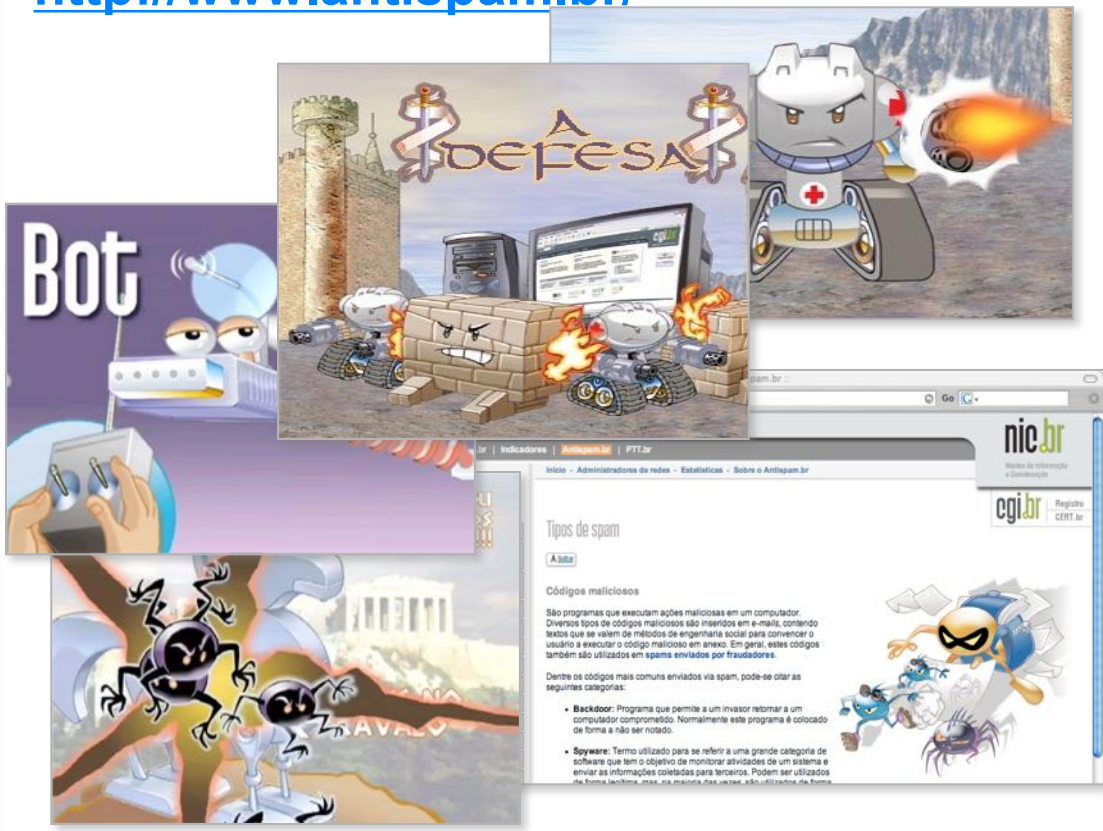
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/



Obrigado

www.cert.br

marcus@cert.br

@certbr

17 de maio de 2018

nic.br cgi.br

www.nic.br | www.cgi.br