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

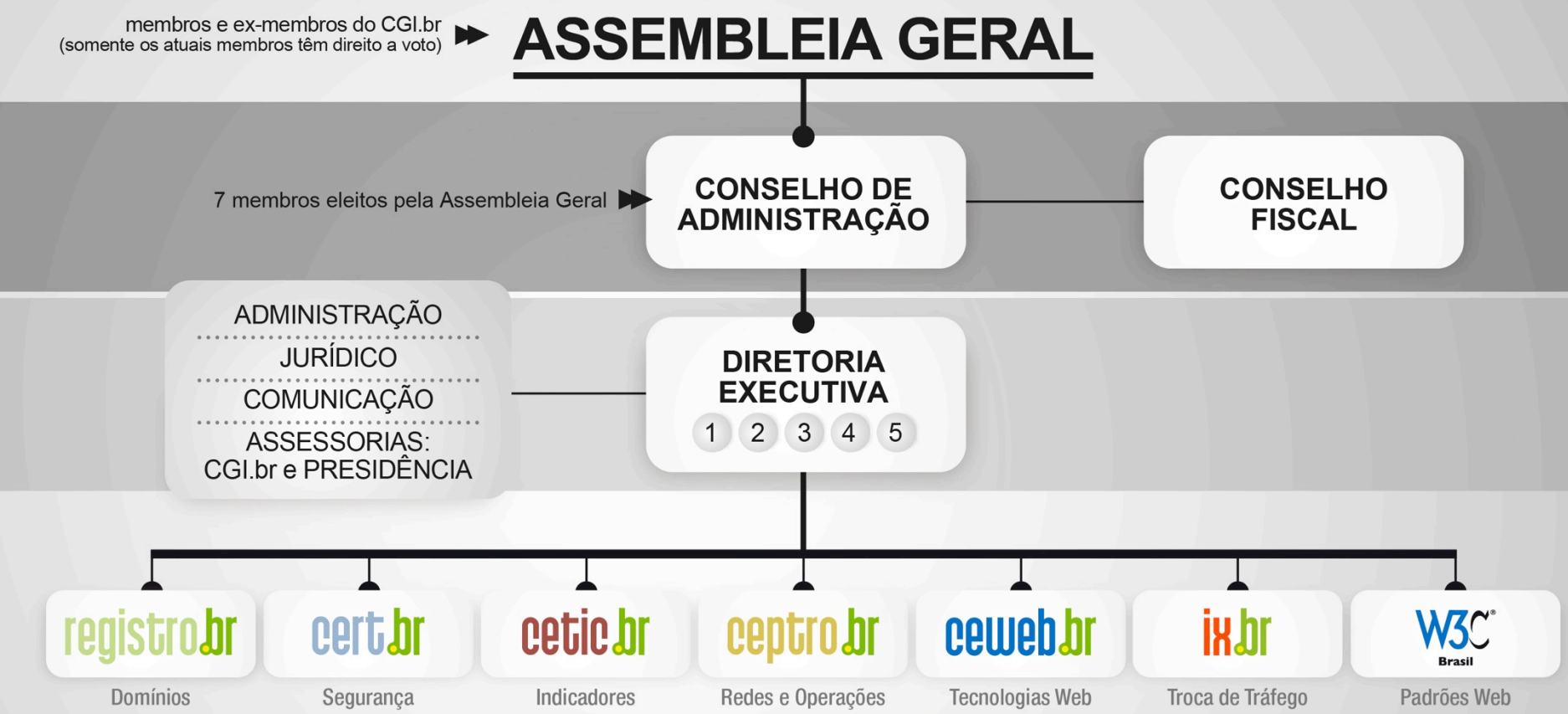
IX (PTT) Fórum 11
São Paulo, SP
04 de dezembro de 2017

Cenário de Abuso dos Sistemas Autônomos Brasileiros

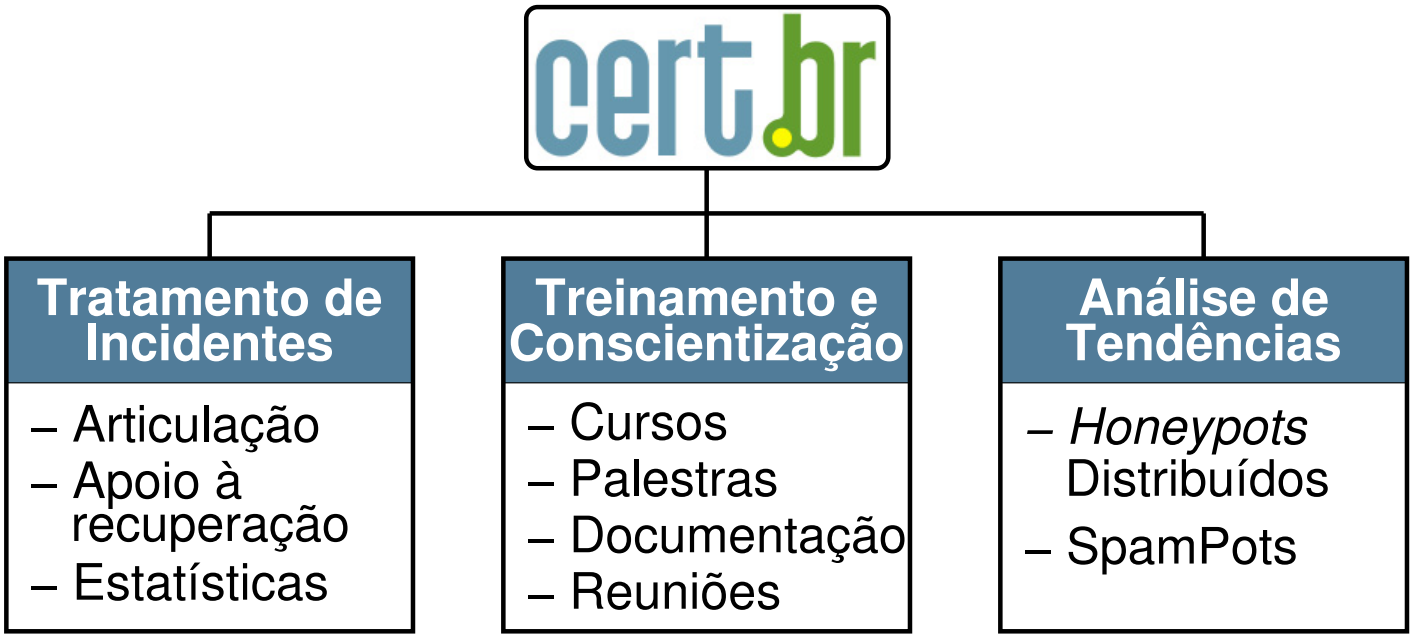
Cristine Hoepers, D.Sc.
Gerente Geral
cristine@cert.br

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

Principais atividades:

- **Tratamento de Incidentes**
  - Ponto de contato nacional para notificação de incidentes
  - Atua facilitando o processo de resposta a incidentes das várias organizações
  - Trabalha em colaboração com outras entidades
  - Auxilia novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades
- **Formação de profissionais para atuar em Tratamento de Incidentes**
- **Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências**

Métricas de Abuso dos Sistemas Autônomos: **Origem dos Dados**

Notificações de incidentes enviadas para `cert@cert.br`

- Notificações feitas de forma voluntária
- Incidentes detectados por administradores de sistemas do Brasil e do exterior

Ataques detectados na rede de *honeypots* distribuídos mantida pelo CERT.br

- Sensores passivos instalados em redes de parceiros
- Detectam
  - códigos maliciosos se propagando
  - atacantes procurando sistemas mal configurados para abusá-los

Dados fornecidos por parceiros internacionais

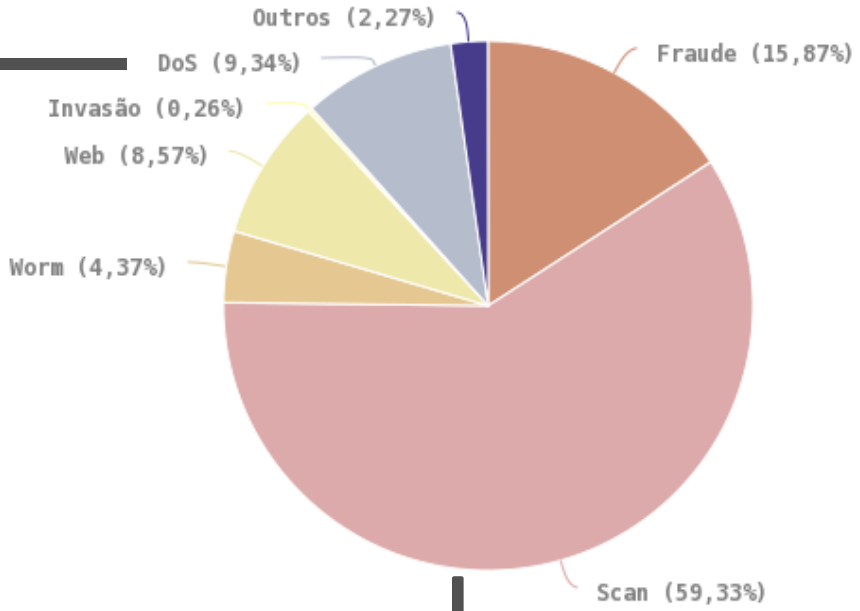
- Anonimizados
- Detectados em
  - redes de *honeypots* internacionais
  - incidentes detectados por terceiros

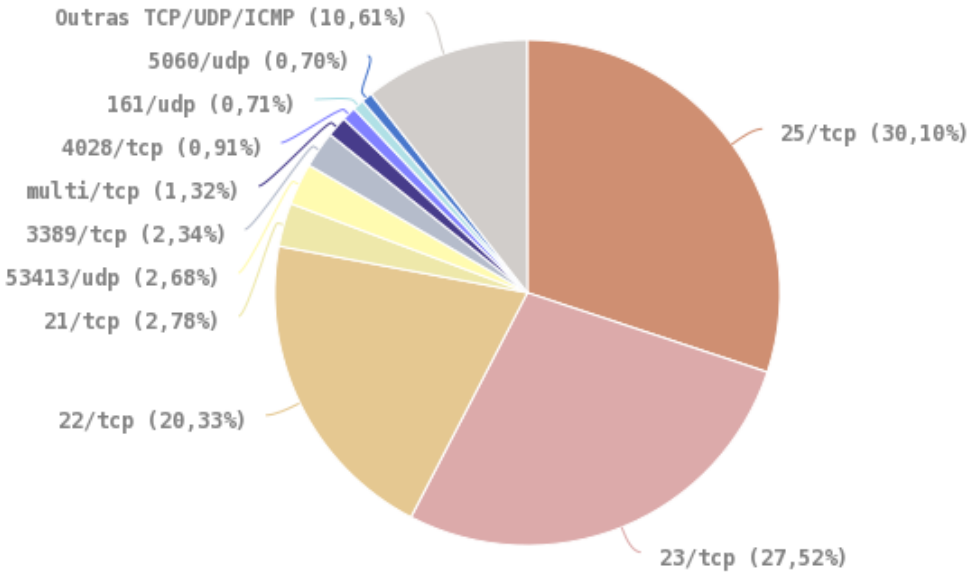
Incidentes Notificados Voluntariamente ao CERT.br

Incidentes Notificados – Destaques em 2016

DDoS – aumento de 138%

- **300Gbps é o novo "normal"**
  - Até 1Tbps contra alguns alvos
- **Tipos mais frequentes**
  - *botnets* IoT
  - amplificação de tráfego



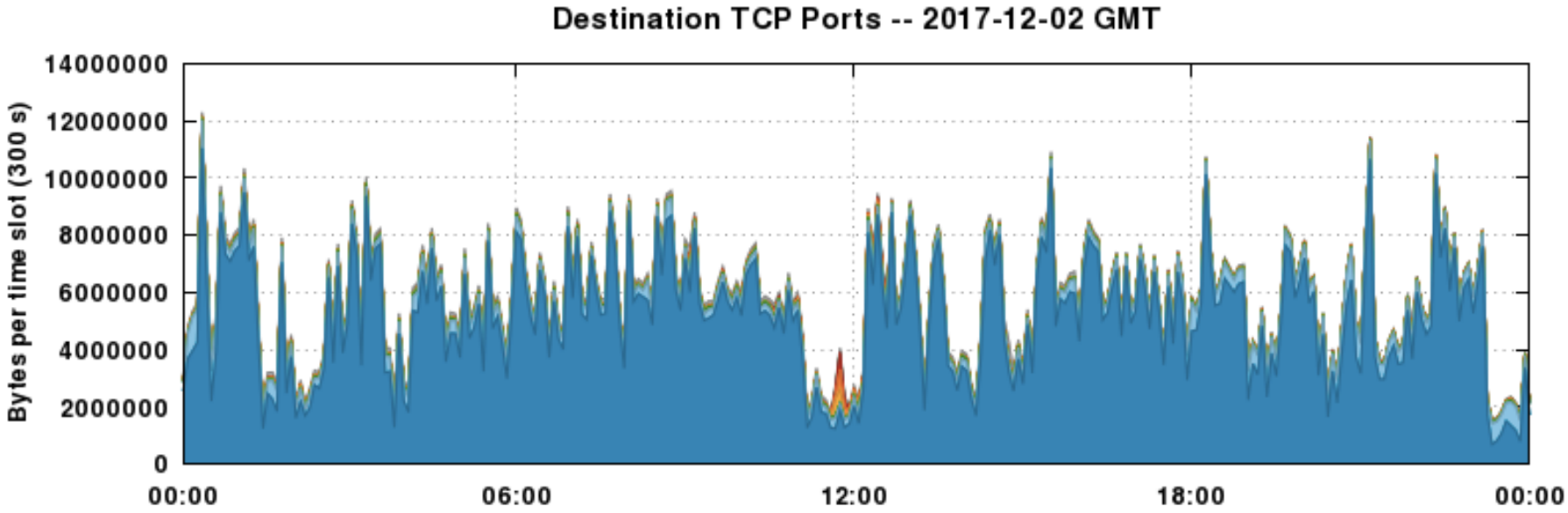


Varreduras (*Scan*)

- **Portas 22 e 23:** força bruta de senhas de:
  - servidores
  - *modems* / roteadores
  - IoT
- **Porta 25:** força bruta de senhas de *e-mail*

Atividades nos *Honeypots* Distribuídos

cert.br nic.br cgi.br



#	Key	Port	Name	Total		Max	Avg
01		23	TELNET	1.47 GB	87.90 %	36.80 KB/s	17.06 KB/s
02		22	SSH (Secure Shell)	125.07 MB	7.46 %	3.92 KB/s	1.45 KB/s
03		445	Microsoft-DS Active Directory	16.08 MB	0.96 %	415.12 B/s	186.14 B/s
04		2323	(abused by Mirai/IoT botnets)	7.84 MB	0.47 %	113.90 B/s	90.72 B/s
05		80	HTTP (Hypertext Transfer Protocol)	6.25 MB	0.37 %	1.74 KB/s	72.37 B/s
06		8080	HTTP Proxy	3.40 MB	0.20 %	2.25 KB/s	39.32 B/s
07		1433	Microsoft SQL Server	2.79 MB	0.17 %	64.26 B/s	32.32 B/s
08		8000	N/A	2.24 MB	0.13 %	1.98 KB/s	25.88 B/s
09		5555	(abused by Mirai/IoT botnets)	1.34 MB	0.08 %	27.93 B/s	15.55 B/s
10		3389	RDP (Microsoft Terminal Server)	970.71 KB	0.06 %	37.21 B/s	11.24 B/s
11		Others		36.88 MB	2.20 %	2.46 KB/s	426.88 B/s

Fonte: https://honeytarg.cert.br/stats/flows/current/

Atividades nos *Honeypots* Distribuídos: **Serviços mais Visados**

Força bruta de senhas (ataque usado por *malware* de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- Outras TCP (2323, 23231, 2222)

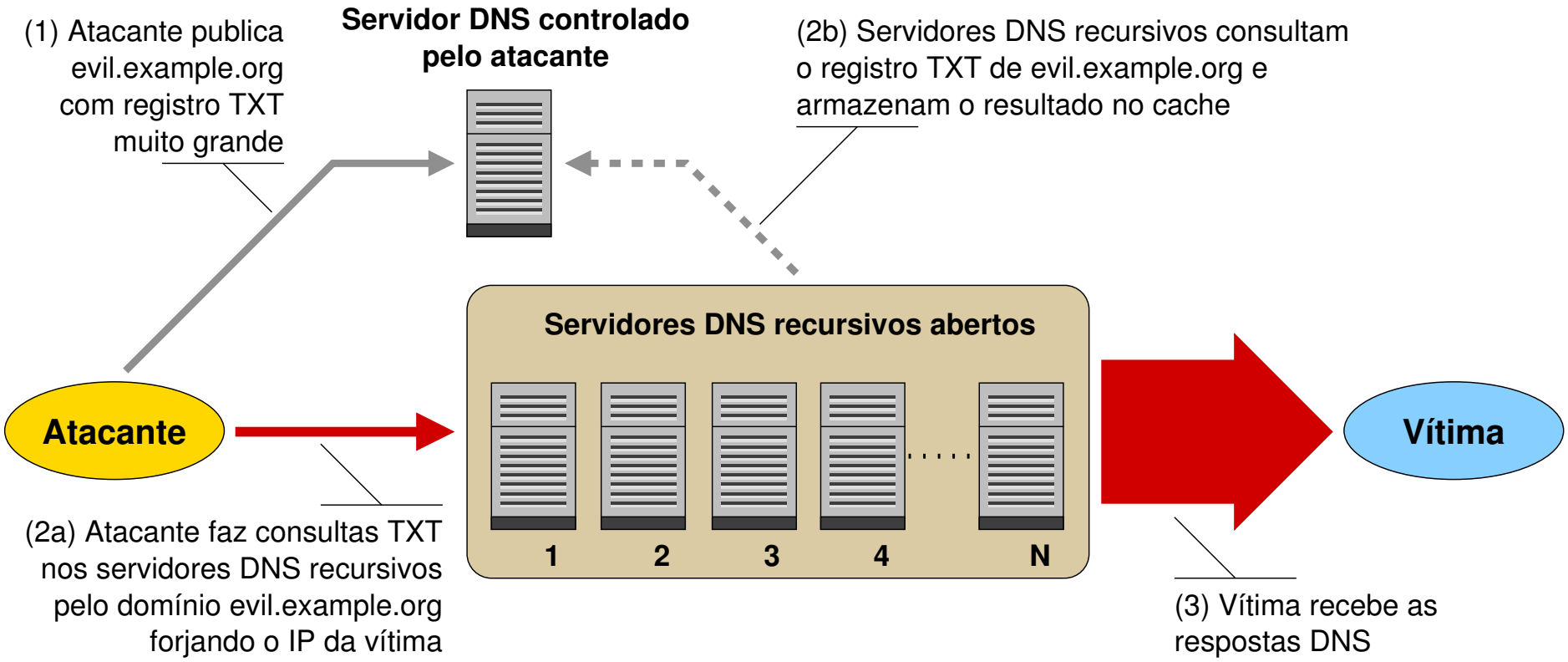
Protocolos explorados pela *botnet* Mirai, na variante para CPEs (*modems*/roteadores de banda larga)

- TCP: 7547, 5555, 37777, 6789, 81

Busca por protocolos que permitam amplificação

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Como Ocorrem Ataques DDoS com Amplificação: **Exemplo de Amplificação de Tráfego DNS**



Fonte:
Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
http://bcp.nic.br/dns-recursivo/

Dados Fornecidos por Parceiros Internacionais

Dispositivos / Serviços que Permitem Amplificação: **Total de ASNs e IPs Notificados**

ASNs e IP únicos notificados pelo CERT.br em 2017

	DNS		SNMP		NTP		SSDP	
	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

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

Obs.: Notificações realizadas após confirmar dados do ShadowServer sobre amplificadores no Brasil
http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

Outros Abusos Preocupantes

Ataques a *Modems* / Roteadores de Banda Larga: **Objetivo é Alteração de DNS para Fraudes**

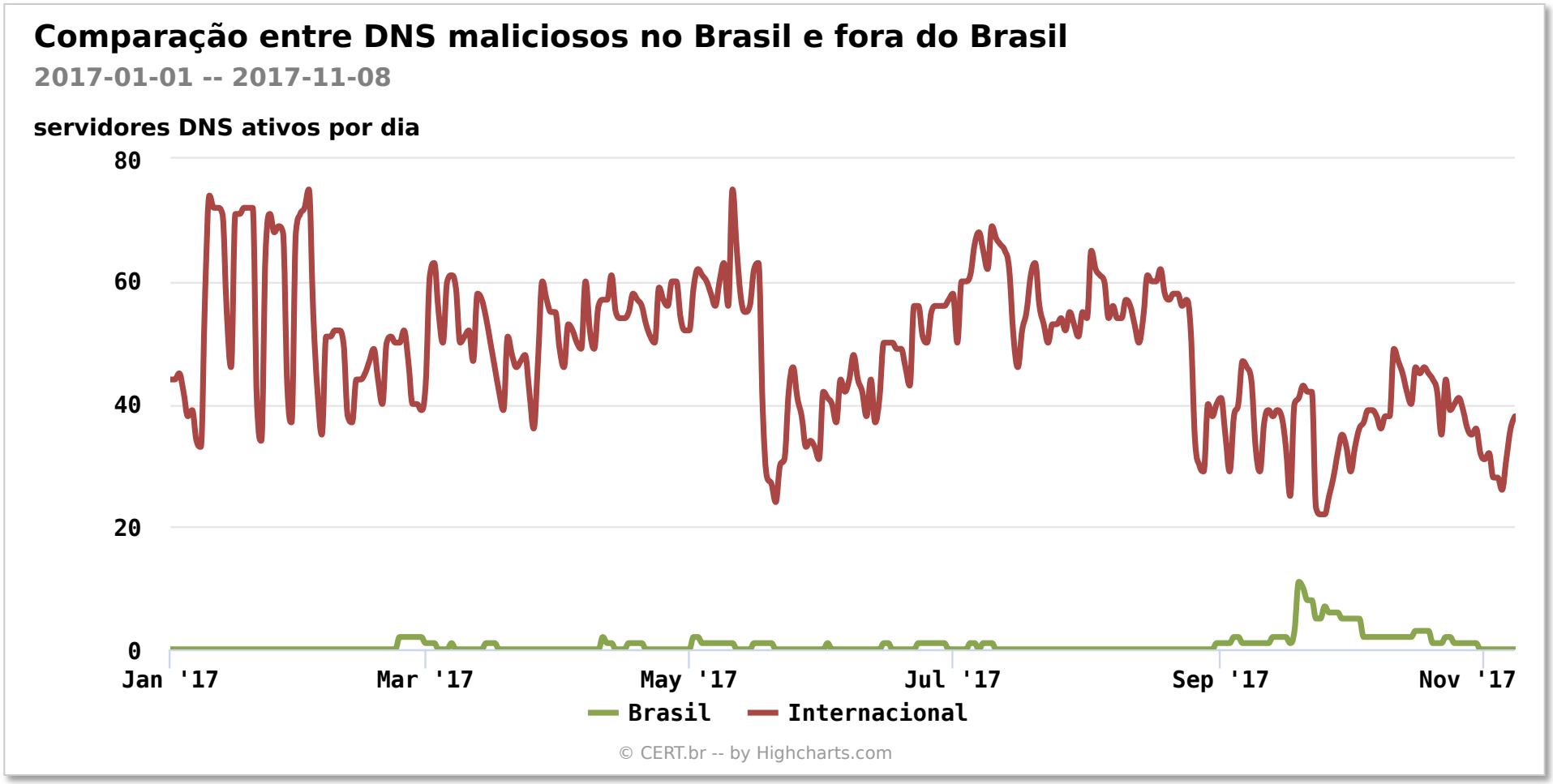
Dispositivos são comprometidos

- via força bruta de senhas (geralmente via telnet)
- explorando vulnerabilidades
- via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos
  - Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos atacantes

- **alterar a configuração de DNS dos clientes do AS, para que consultem servidores sob controle dos atacantes**
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

Servidores DNS Maliciosos *Online*/Dia: **Volume Constante Indica que é Efetivo**



Ataques de Sequestro de Rotas BGP: **Objetivo de Perpetrar Fraudes Financeiras**

Anatomia dos ataques

- Atacantes comprometem roteadores de borda de pequenos provedores
  - via força bruta de senhas de administração
- Anunciam prefixos de rede mais específicos da instituição vítima (em geral /24)
  - levantam um túnel GRE para redirecionar o tráfego destinado ao /24 sequestrado para servidor com conteúdo sob controle do atacante
- Início em março de 2017 e ainda está ocorrendo

Considerações Finais

Considerações Finais:
Resumindo os Abusos

Força bruta de senhas em

- Roteadores de borda e servidores
- *Modems* e roteadores de banda larga

Recomendações:

- senhas fortes e acesso via chaves SSH
- desabilitar telnet, ftp e outros acessos sem criptografia ou autenticação
- gerência remota e acesso somente via redes de gerência

Abuso de serviços UDP para amplificação em

- Servidores mal configurados
- *Modems* e roteadores de banda larga
  - que vem de fábrica com os serviços abertos
- Dependem de capacidade de fazer *spoofing* de IP

Recomendações:

- implementar *antispoofing* (BCP 38)
- configurar os modems e roteadores domésticos para não ter serviços abertos, não ter senha padrão, etc
- detectar proativamente ataques saindo de sua rede

Obrigada

https://cert.br/
http://bcp.nic.br/

cristine@cert.br @certbr

04 de dezembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br