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

IX Fórum Regional
São Paulo, SP
10 de novembro de 2017

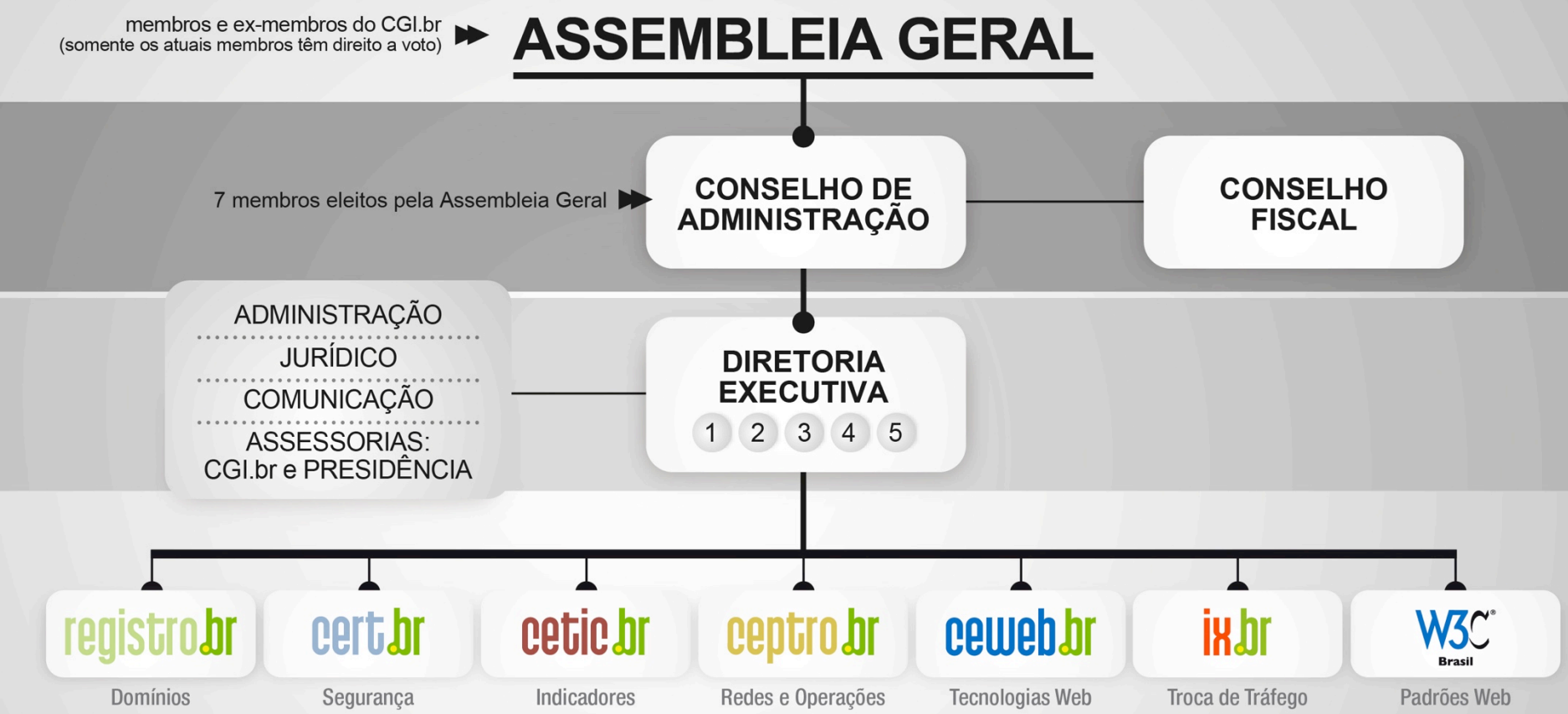
Ataques Mais Significativos e Como Melhorar o Cenário

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

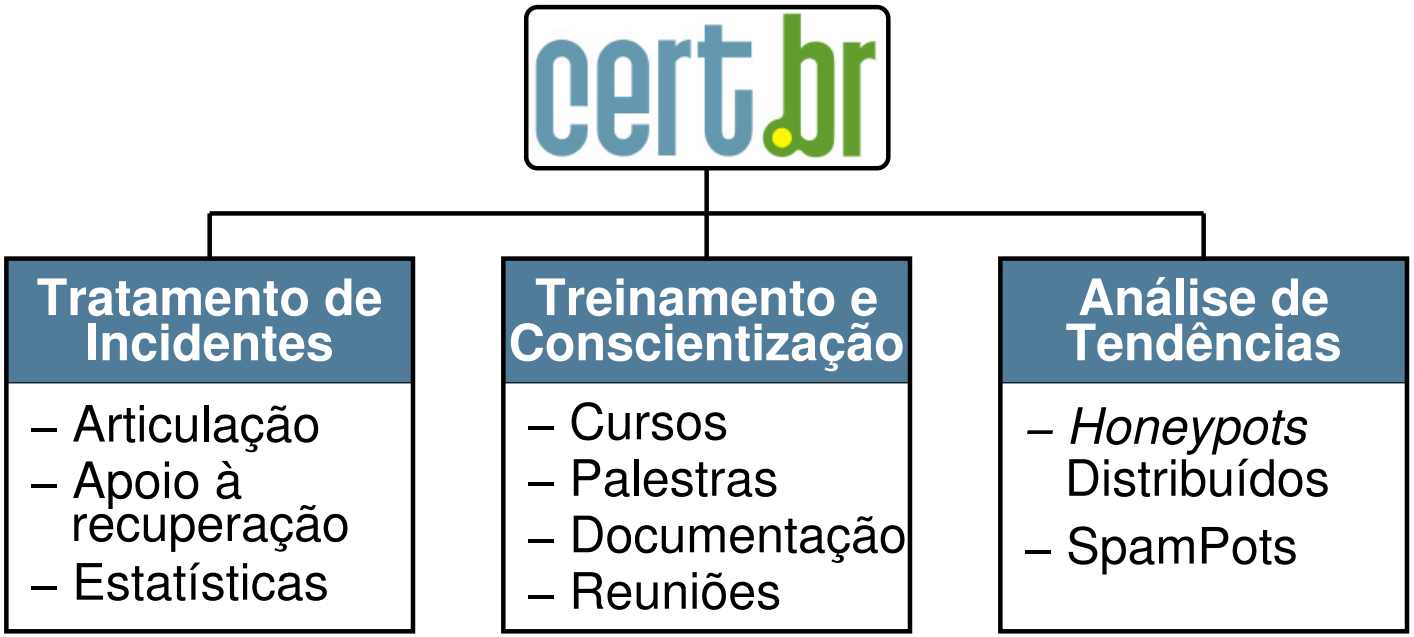
Klaus Steding-Jessen, D.Sc.
Gerente Técnico
jessen@cert.br

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**

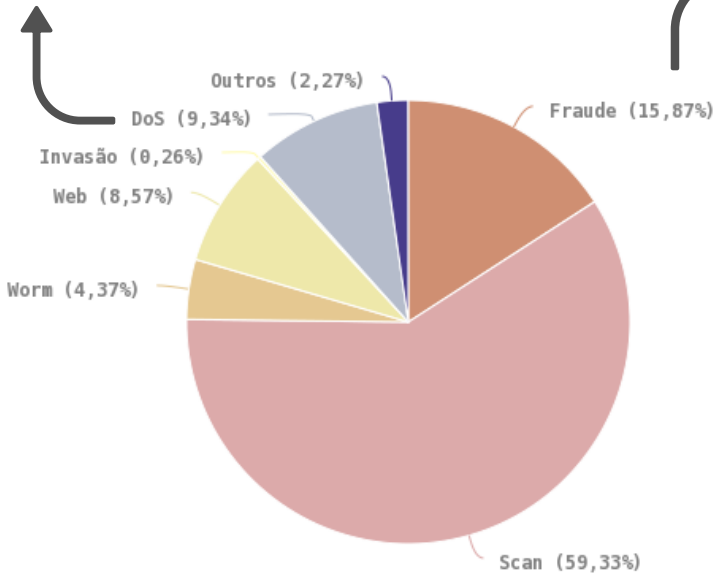
Alguns Problemas de Segurança mais Significativos no Brasil

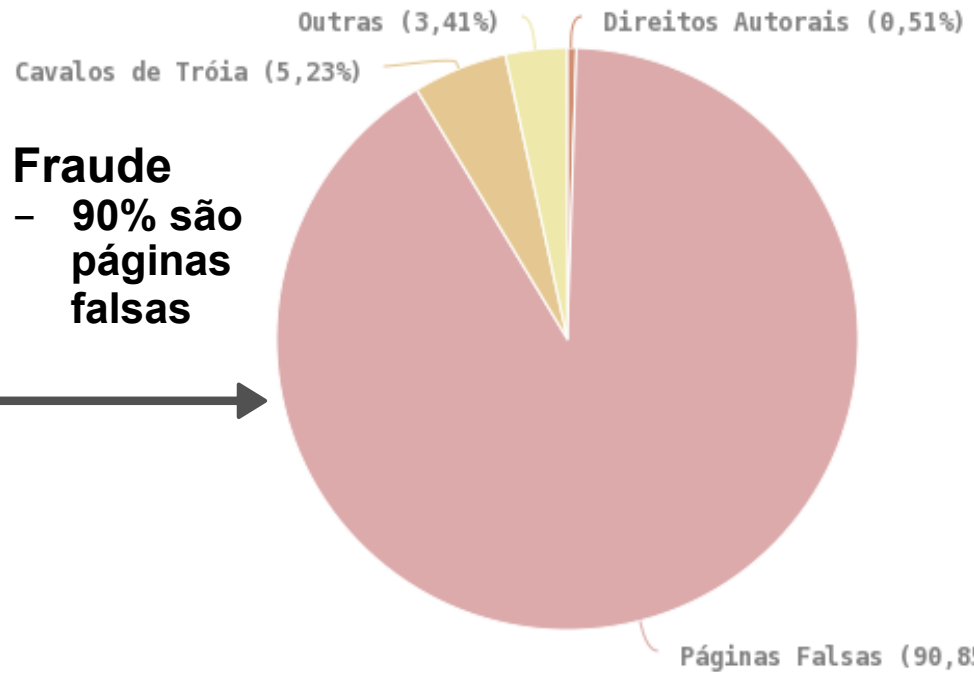
cert.br nic.br cgi.br

Estatísticas 2016

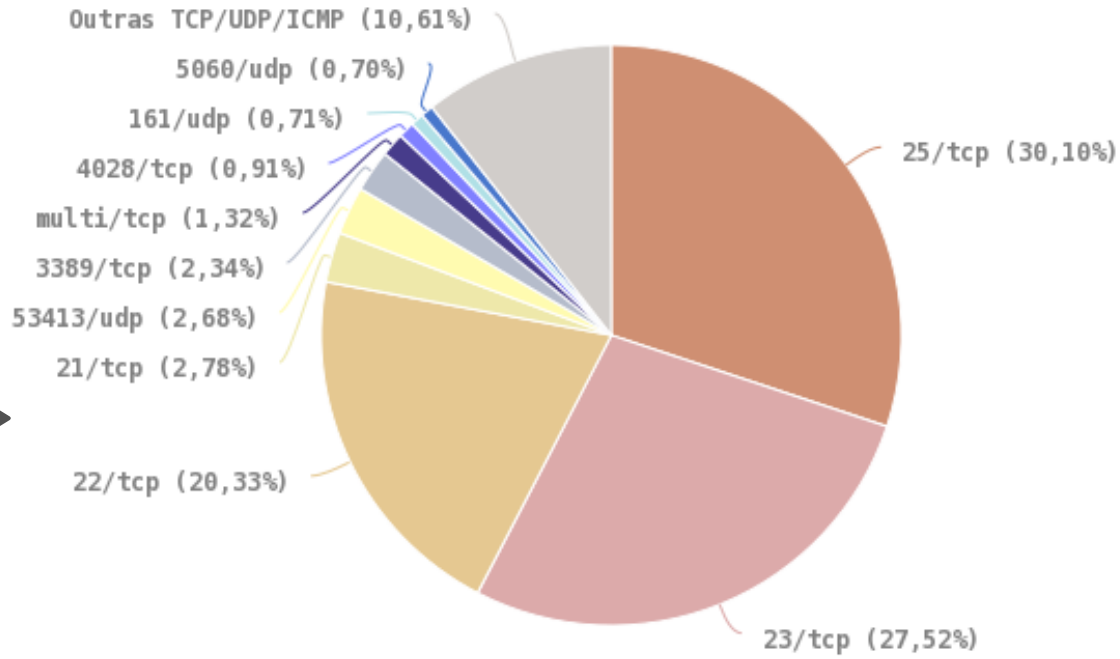
DDoS – aumento de 138%
- 300Gbps é o “normal”
- Até 1Tbps contra alguns alvos
- Tipos mais frequentes
  - botnets IoT
  - amplificação

Fraude
- 90% são páginas falsas





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



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

Força bruta de senhas (usado por malwares de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- RDP (3389/TCP)
- POP3 (110/TCP)
- Outras TCP (2323, 23231, 2222)

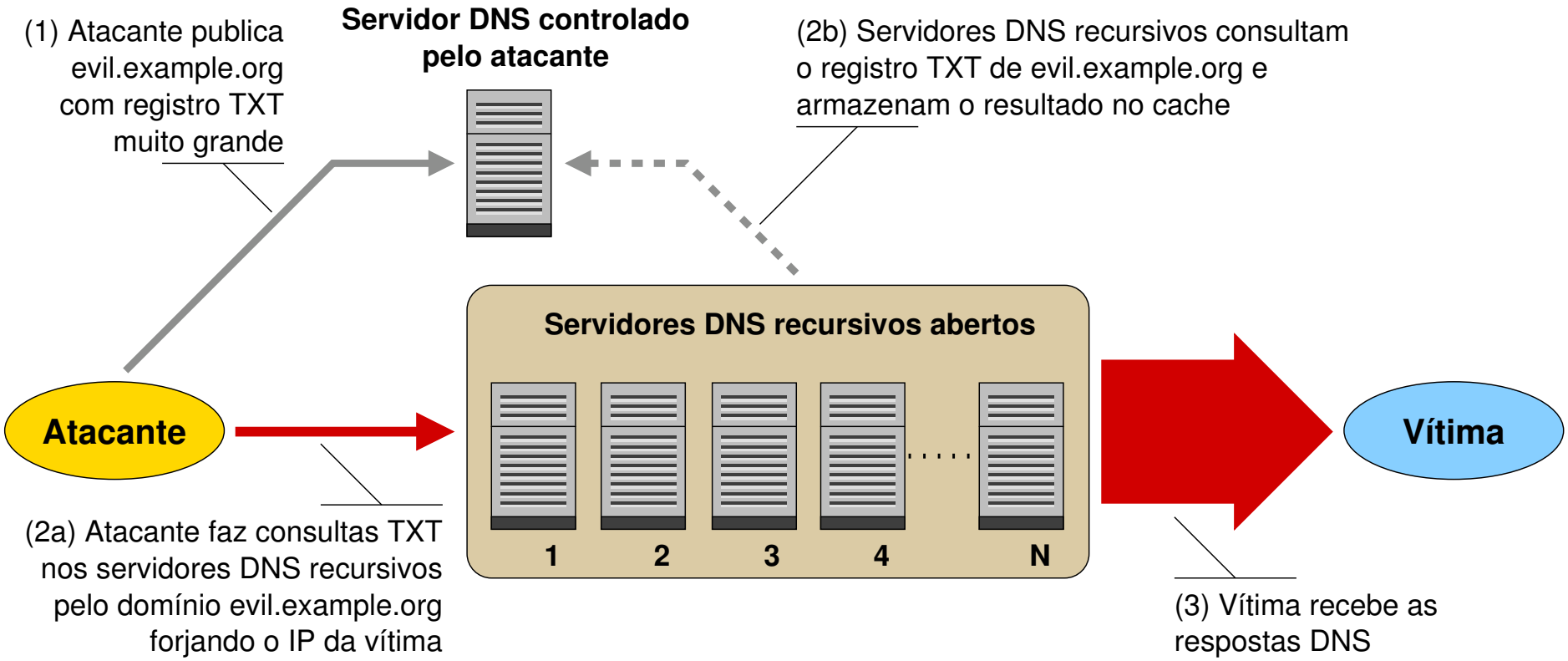
Protocolos explorados pela botnet Mirai, na variante para CPEs (roteadores de banda larga)

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

Busca por protocolos que permitam amplificação

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

Relembrando como Funcionam Ataques DDoS com Amplificação



Fonte:
Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
https://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Total de Notificações de IPs com Serviços Mal Configurados que Permitem Amplificação

Número de Sistemas Autônomos e Endereços IP únicos notificados pelo CERT.br em agosto e setembro de 2017

	Agosto		Setembro	
	ASNs	IPs	ASNs	IPs
SNMP	2.018	554.457	1.791	406.015
DNS	2.347	72.677	2.307	62.283
NTP	872	108.168	800	89.603
SSDP	891	27.209	⦸	⦸

Legenda:

⦸ não foi realizada notificação desta categoria no referido mês

Artigo do ShadowServer sobre os testes de amplificadores:
http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

Ataques Envolvendo CPEs para Alteração de DNS

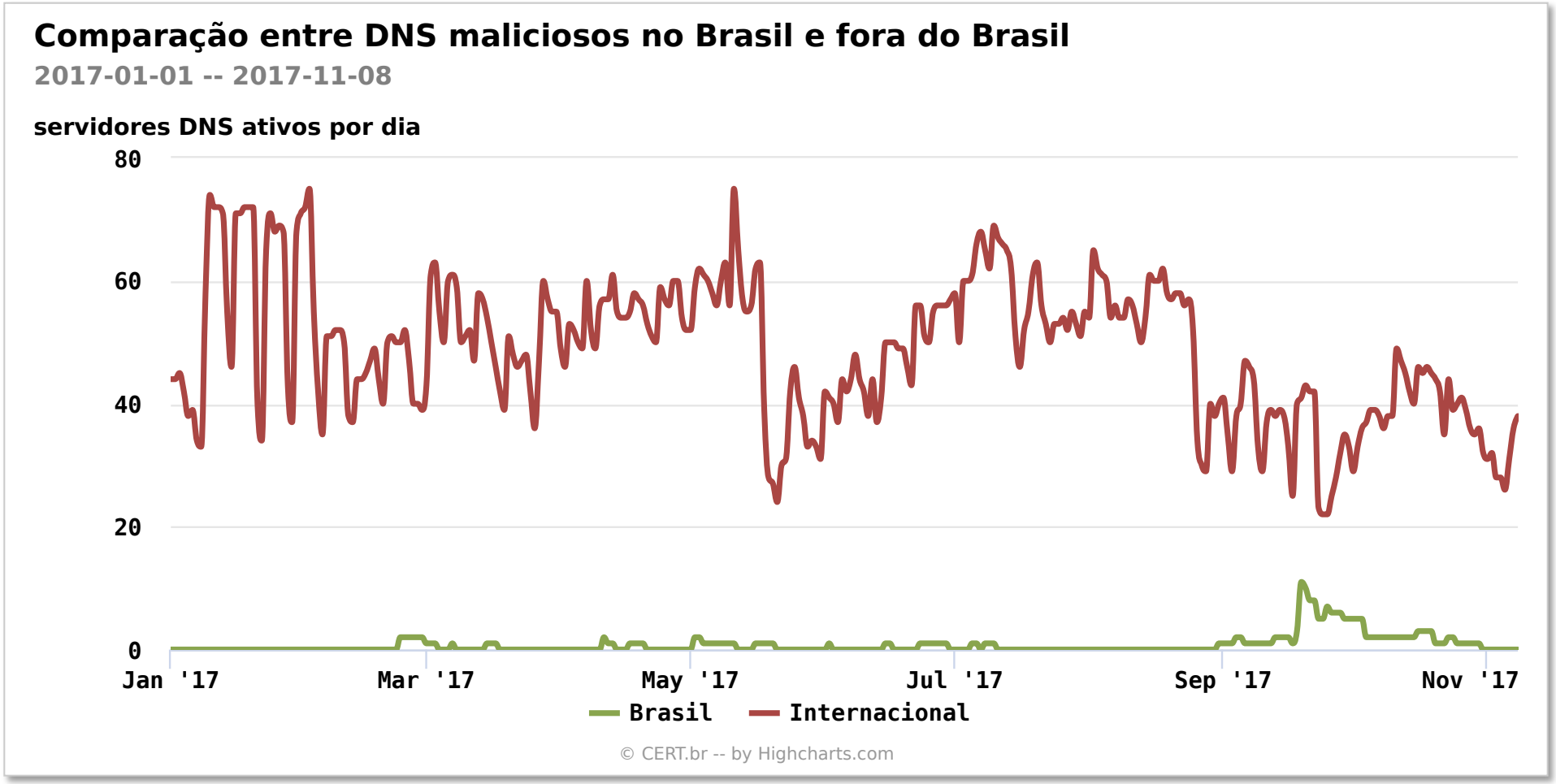
Comprometidos

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

Objetivos dos ataques

- **alterar a configuração de DNS 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*, por Dia



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 ou com caminho (*AS path*) menor

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

Passos Simples para Mudar a Situação

Recomendações

Fazer *hardening* de roteadores e elementos de rede

- senhas fortes e acesso via chaves SSH
  - desabilitar `telnet`, `ftp` e outros acessos sem criptografia ou autenticação
- rede de gerência
- desativar serviços desnecessários/não utilizados

Ativar *netflows*

- ótimas opções de *software* livre (`nfdump`/`nfsen`)
- usos reativos e pró-ativos
  - como consultas DNS para servidores maliciosos

Reduzir ataques DDoS saindo de sua rede

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

Receber e tratar notificações, que são enviadas para:

- *e-mail* do contato `abuse-c` do ASN no serviço whois
- *e-mail* de abuse ou do grupo de tratamento de incidentes

Obrigado

www.cert.br

cristine@cert.br jessen@cert.br @certbr

10 de novembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br