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

Painel Telebrasil 2018

Brasília, DF

22 de maio de 2018

Segurança cibernética: onde estamos e onde deveríamos estar?

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

cert.br nic.br cgi.br

Cenário Nacional: Grupos de Tratamento de Incidentes de Segurança

cert.br nic.br cgi.br

Evolução do Tratamento de Incidentes no Brasil: **Criação do CERT.br**

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo **CGI.br**[1]

- Levantamento da situação no País
- Definição de prioridades
- Levantamento do melhor modelo para agir como facilitador para o tratamento de incidentes de segurança
  - grupo autônomo e neutro, para atuar como ponto de contato nacional
  - orientar tecnicamente sobre prevenção e resposta a incidentes
  - fomentar treinamento, atualização e cooperação
  - fomentar a criação de novos CSIRTs no País

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm

Evolução do Tratamento de Incidentes no Brasil: **Primeiros CSIRTs**

Agosto/1997
–a RNP cria seu próprio CSIRT (CAIS)[1], seguida pela rede acadêmica do Rio Grande do Sul (CERT-RS)[2]

1999
–outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs

2003/2004
–grupo de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal

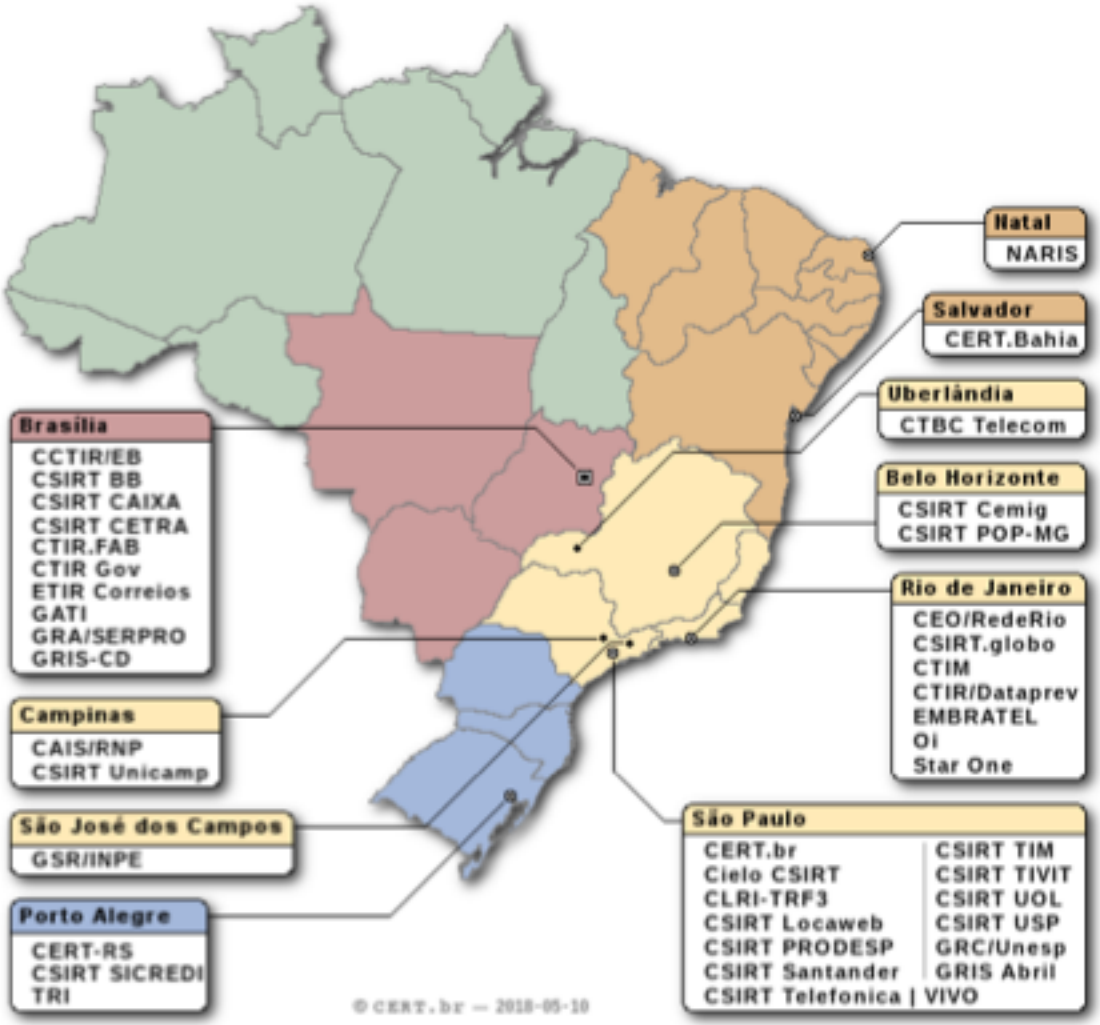
2004
–o CTIR Gov foi criado, com a Administração Pública Federal como seu público alvo[3]

[1] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[2] http://www.cert-rs.tche.br/cert-rs.html
[3] http://www.ctir.gov.br

CSIRTs Brasileiros - https://cert.br/csirts/brasil/

Lista 41 times com serviços anunciados ao público

Setor	CSIRTs
Nacional – domínios .br, ASNs ou IPs alocados ao Brasil.	CERT.br
Nacional – Administração Pública Federal	CTIR Gov
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energia	CSIRT Cemig
Sistema Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Provedores Operadoras Hospedagem	CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Outros	CSIRT.globo, GRIS Abril



Resiliência das Organizações:
Papel dos CSIRTs na Mitigação e Recuperação

Tratamento de Incidentes é só um de vários processos essenciais

- Gestão de Risco, Segurança da Informação, Continuidade de Negócios, Segurança de Desenvolvimento, Gestão de Atualizações e de Configuração

A redução do impacto de um incidente é conseqüência da

- agilidade de resposta
- redução no número de vítimas

O sucesso depende da confiabilidade

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O papel de um CSIRT é

- auxiliar a proteção da infraestrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas

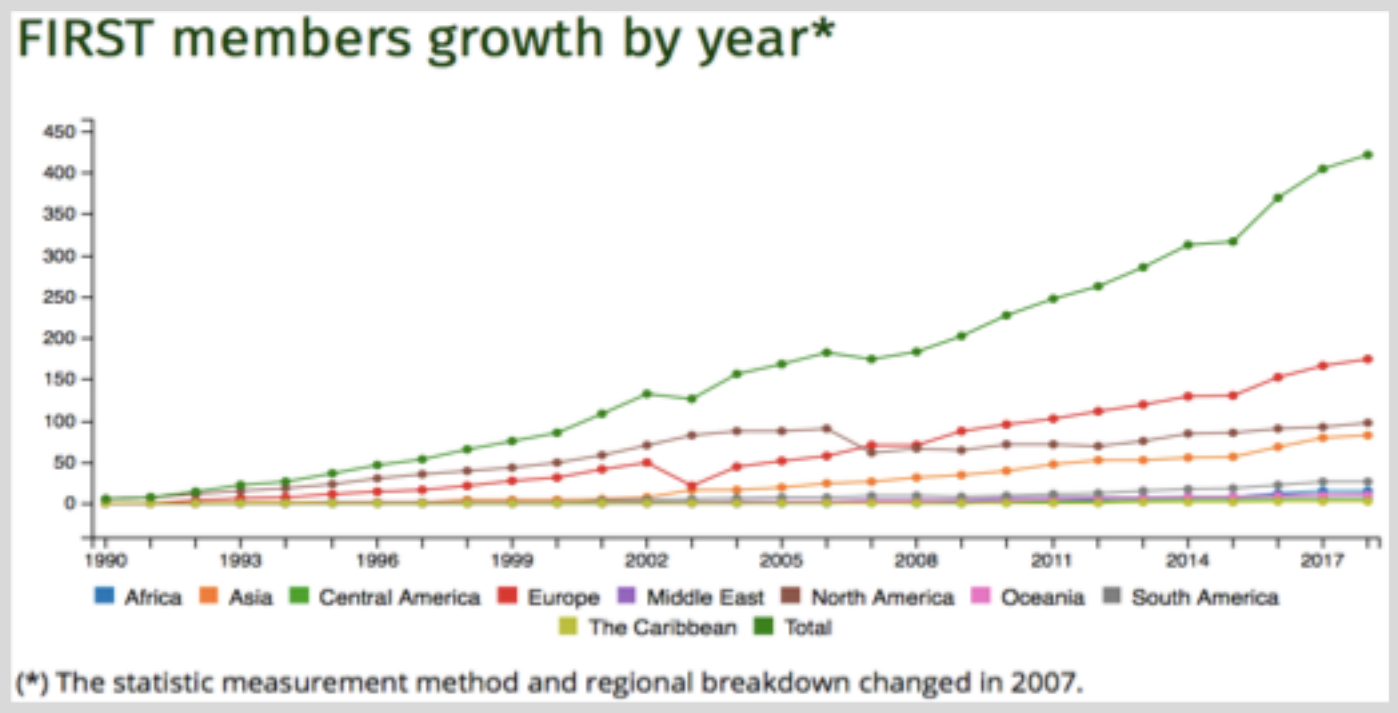
O CSIRT não é um investigador

- A decisão de levar um caso à justiça deve ser da vítima
- Em uma organização, leia-se: alta administração e setor jurídico

Cooperação Nacional e Internacional:
Criar Relações de Confiança é a Base de Tudo

Participar de Fóruns de Cooperação é essencial

- https://first.org/members/
- https://cert.br/forum2018/
- https://www.first.org/global/governance/
  - https://www.first.org/global/governance/bpf-csirt-2015-outcome.pdf
  - https://www.first.org/global/governance/bpf-csirt-2015-report.pdf



Fonte: https://www.first.org/about/history

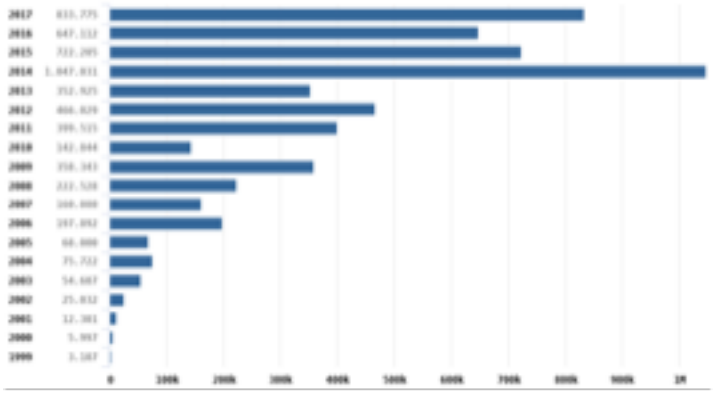
Cenário Nacional: Incidentes

Métricas de Abuso dos Sistemas Autônomos do Brasil: **Fontes dos Dados**

Notificações voluntárias de incidentes

enviadas para: `cert@cert.br`

- https://www.cert.br/stats/incidentes/



Data feeds (Honeypots Distribuídos do CERT.br, Team Cymru, Arbor Atlas, SpamHaus, ShadowServer, Shodan, Operações Anti-Botnet)

Responsáveis pelos ASNs são notificados, com dicas sobre como identificar os ataques e se recuperar

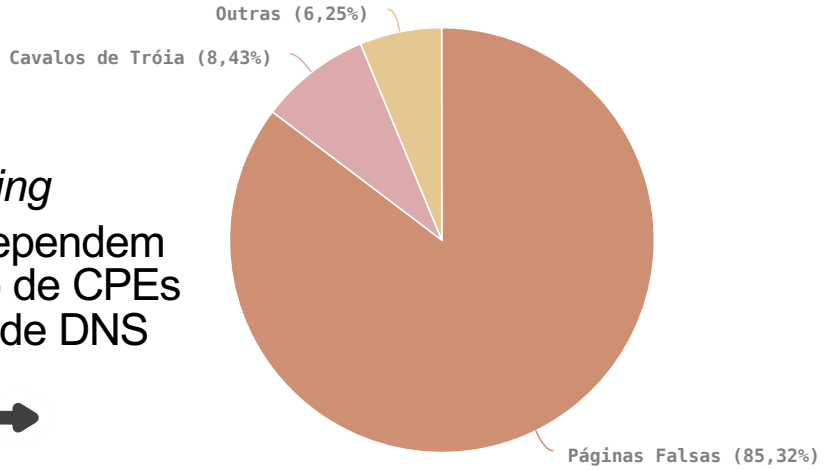
Incidentes Notificados em 2017 – Destaques

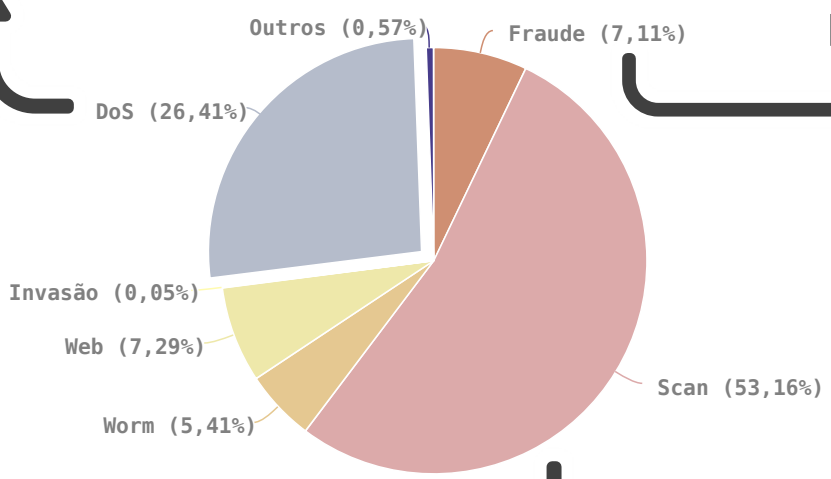
DDoS – aumento de 3.6 vezes

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

Fraude

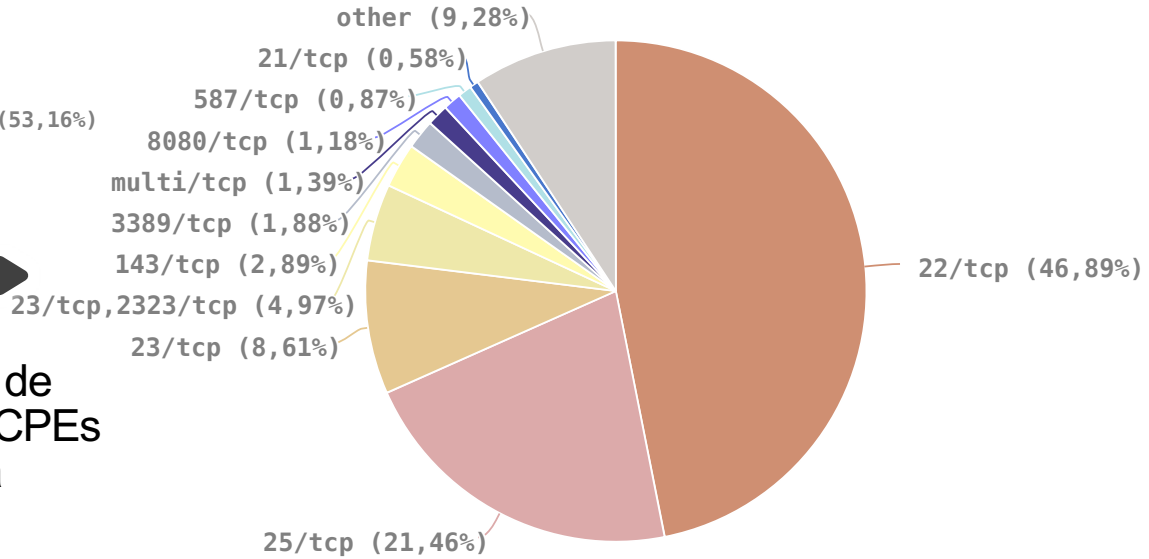
- 85% *phishing*
- Ataques dependem da invasão de CPEs para troca de DNS





Varreduras (*Scan*)

- Portas 22 & 23: força bruta de senhas de servidores, IoT, CPEs
- Porta 25: força bruta contra servicores de e-mail



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

Força bruta de senhas (usado por *malwares* de IoT/CPEs 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

- TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869

Busca por protocolos que permitam amplificação

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

Port	Name	Total	
23	TELNET	2.72 GB	95.44 %
22	SSH (Secure Shell)	72.09 MB	2.53 %
445	Microsoft-DS Active Directory	15.53 MB	0.55 %
80	HTTP (Hypertext Transfer Protocol)	9.06 MB	0.32 %
8080	HTTP Proxy	3.75 MB	0.13 %
8291	Mikrotik Winbox	2.30 MB	0.08 %
7547	(abused by Mirai/IoT botnets)	1.80 MB	0.06 %
8000	N/A	1.07 MB	0.04 %
1433	Microsoft SQL Server	1.04 MB	0.04 %
5555	(abused by Mirai/IoT botnets)	1.02 MB	0.04 %
Others		22.13 MB	0.78 %

Flows de tráfego dos *honeypots* em 19/05/2018
https://honeytarg.cert.br/stats/flows/2018/05/19/flows-2018-05-19.html

Projeto *Honeypots* Distribuídos
https://honeytarg.cert.br/honeypots/

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

Cenário Nacional:
Onde Deveríamos Estar

Segurança é inerentemente multissetorial: **Cooperação para um ecossistema saudável**

Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel

Universidades

- precisam incluir questões de segurança em todas as disciplinas
- desenvolvimento seguro precisa ser prioridade desde o início

Desenvolvedores / empresas de *software* e *hardware*

- precisam pensar em segurança desde as etapas iniciais de desenvolvimento

Gestores

- precisam considerar segurança como um investimento e alocar recursos adequados

Provedores de acesso, operadoras, administradores de redes em geral

- não emanar “sujeira” de suas redes
- adotar boas práticas

Usuários

- entender os riscos e seguir as dicas de segurança
- manter seus dispositivos atualizados e tratar infecções

Desafios para o Futuro

Qualificação profissional

- redes, administração de sistemas, segurança, desenvolvimento de *software* seguro

Certificação de dispositivos/*hardware* não faz mais sentido

- não há como certificar *software* (*firmware* é *software*)

Vulnerabilidades sempre vão existir

- o importante é tratá-las de forma rápida

Precisamos discutir, em nível global, a definição de requisitos de maturidade em segurança para fabricantes, incluindo

- possuir ciclo claro de atualização de *software/firmware*
- possuir um PSIRT (*Product Security Incident Response Team*) ou ao menos um contato claro para tratar problemas de segurança no produto
  - referências:
    - *FIRST PSIRT Services Framework*
      https://first.org/education/Draft_FIRST_PSIRT_Service_Framework_v1.0
    - *The Building Security In Maturity Model*
      https://www.bsimm.com/

Boas Práticas Operacionais para Sistemas Autônomos: **Ações da Comunidade para Melhorar a Internet**

Boas práticas para aumentar a resiliência e estabilidade das redes:

- Segurança de roteamento
- *Antispoofing*
- Redução e mitigação de DDoS

Parte da Iniciativa "*Por uma Internet mais Segura*"

Trabalho de organizações internacionais:

- ISOC – MANRS.org
- IETF – BCP 38 (*antispoofing*)
- M^{3}AAWG, LAC-AAWG, LACNOG and LACNIC: BCOP para compra e especificação de CPEs

https://bcp.nic.br/

“A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.”

– Princípio 8: Funcionalidade, segurança e estabilidade
Princípios para a Governança e Uso da Internet, CGI.br

Obrigada

www.cert.br

cristine@cert.br

@certbr

22 de maio de 2018

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br