nic.br cgi.br | cert.br

Exercício Guardião Cibernético 2.0
Abertura dos Grupos de Estudos

02 de julho de 2019 – Brasília/DF

Panorama de Ameaças e Papel do CERT.br no Brasil e no Mundo

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

TLP:WHITE

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995 (portaria MCT/MC), **responsável por coordenar e integrar as iniciativas e serviços da Internet no País**.

Dentre as **atribuições** definidas no **Decreto Presidencial nº 4.829**, de 03/09/2003, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- a **recomendação de padrões e procedimentos técnicos operacionais para a Internet no Brasil**;
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
- a promoção de estudos e padrões técnicos para a **segurança das redes e serviços no país**;
- a coordenação da atribuição de endereços Internet (IPs) e do registro de nomes de domínios usando <.br>;
- a coleta, organização e disseminação de informações sobre os serviços Internet, incluindo indicadores e estatísticas;
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet**.

https://www.cgi.br/sobre/

Composição do CGI.br

Estabelecida pelo **Decreto presidencial Nº 4.829** de 03/09/2003

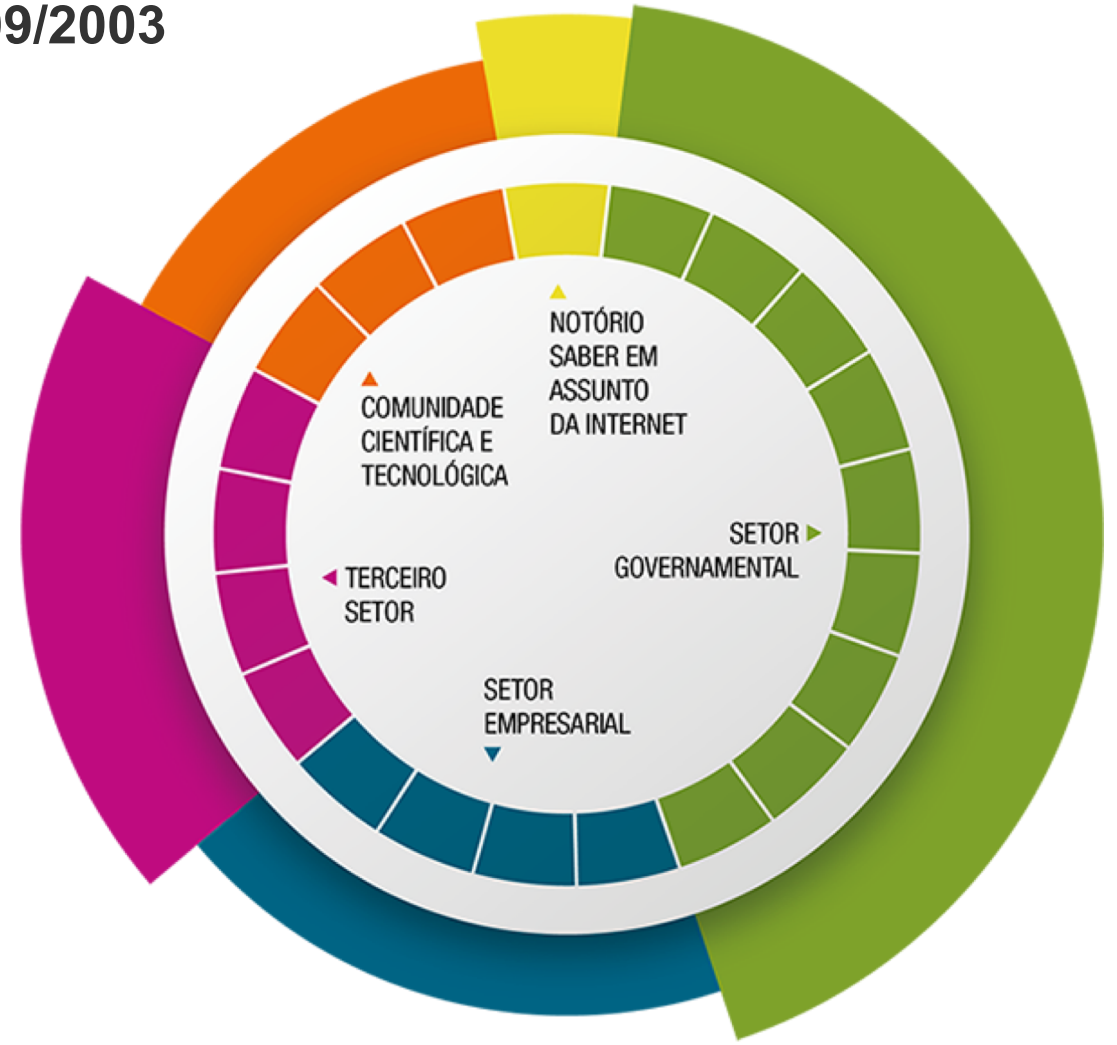
9 representantes do setor governamental

Ministério da Ciência, Tecnologia e Inovação (coordenação)
Casa Civil da Presidência da República
Ministério das Comunicações
Ministério da Defesa
Ministério do Desenvolvimento, Indústria e Comércio Exterior
Ministério do Planejamento, Desenvolvimento e Gestão
Agência Nacional de Telecomunicações
Conselho Nacional de Desenvolvimento Científico e Tecnológico
Conselho Nacional de Secretários para Assuntos de Ciência, Tecnologia e Inovação

12 representantes da sociedade civil

Setor empresarial (4)
- Provedores de acesso e conteúdo da Internet
- Provedores de infraestrutura de telecomunicações
- Indústria de bens de informática, de bens de telecomunicações e de software
- Setor empresarial usuário

Terceiro setor (4)
Comunidade científica e tecnológica (3)
Notório saber em assuntos de Internet (1)



TLP:WHITE

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

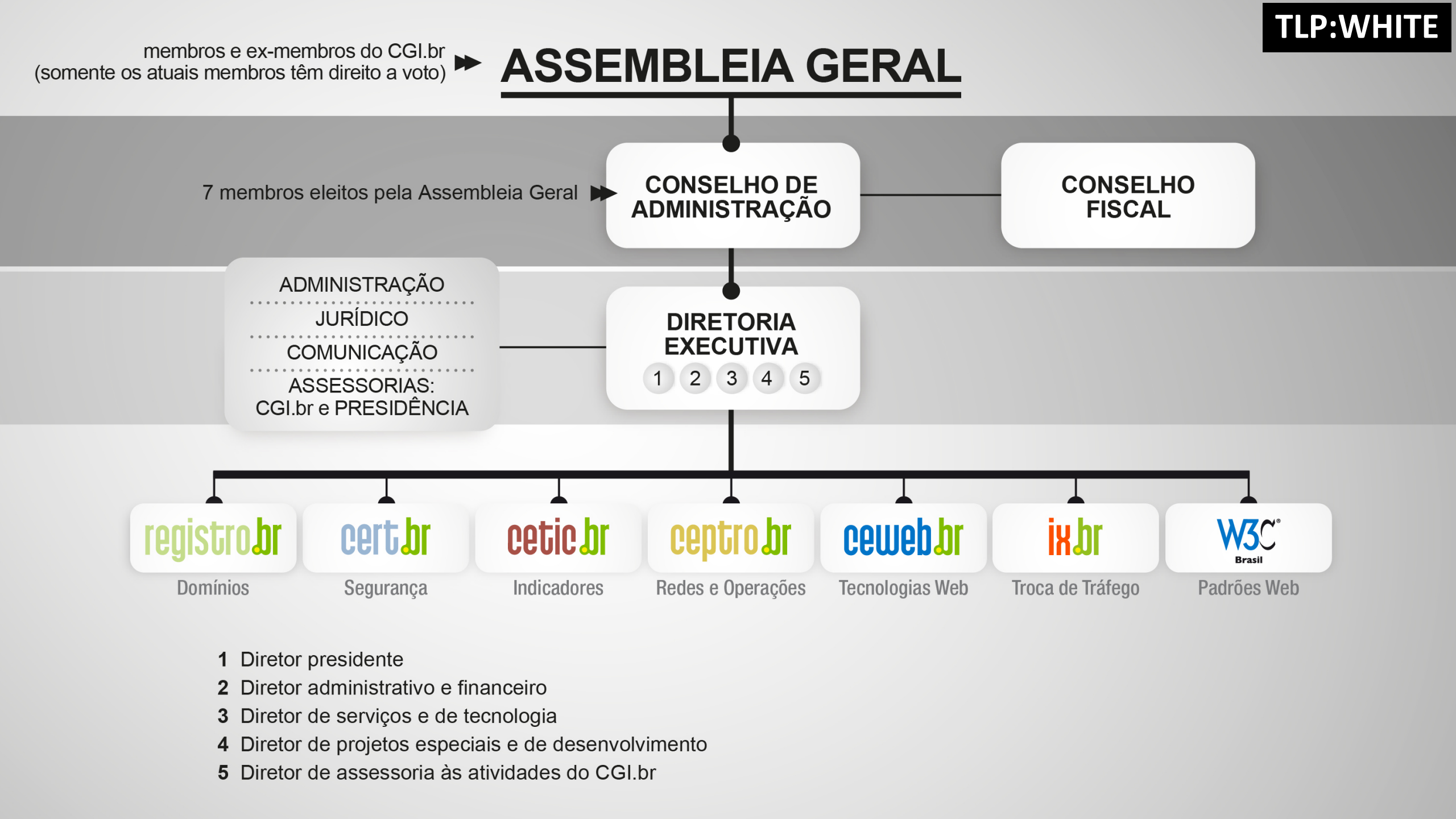
Pessoa jurídica de direito privado, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre seus objetivos estão:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- **atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis, atividades do CERT.br;**
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

https://www.nic.br/sobre/
https://www.nic.br/estatuto-nic-br/

TLP:WHITE



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

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

The Honeynet PROJECT

https://cert.br/sobre/

Criação:

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

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

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Foco das Atividades

- Atuar como ponto de contato nacional para notificação de incidentes
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências
- Transferir o conhecimento adquirido através de cursos, boas práticas e materiais de conscientização

Panorama de Ameaças

cert.br nic.br cgi.br

TLP:WHITE

Internet no Brasil em Números

TIC Provedores (Cetic.br)

- Total de ISPs (estimado): 6618
- Respondentes: 2177
- 75% tem 1000 clientes ou menos

https://www.cetic.br/pesquisa/provedores/

IX.br SP

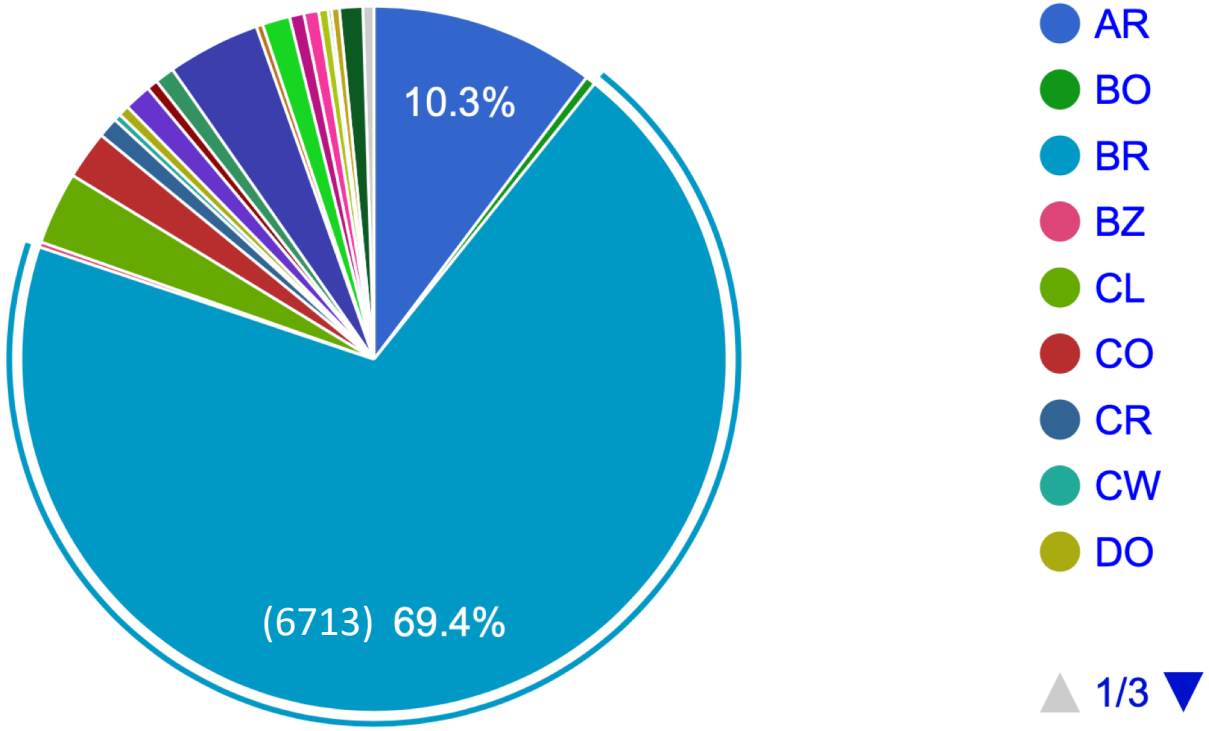
Um dos maiores *Internet eXchanges* do mundo

- #1 em participantes(1467)
- #3 em tráfego – média (3.5Tbps) e pico (5.1Tbps)

  https://www.pch.net/ixp/dir

≈700 ASNs usam MikroTik como roteador de *core*

Alocação de ASNs na Região do LACNIC

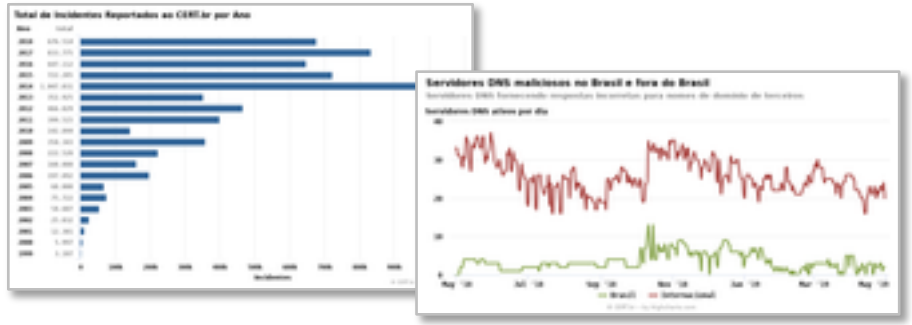


http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion

Tratamento de Incidentes e Abusos:
Fontes dos Dados e Ações/Métricas Públicas

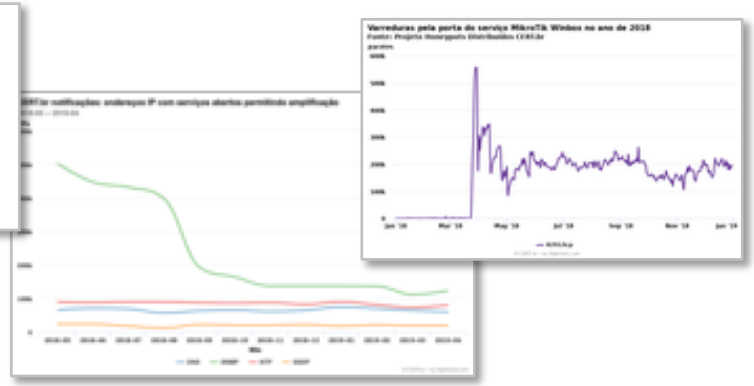
TLP:WHITE

Notificações voluntárias de incidentes enviadas para: `cert@cert.br` –
2018: 2.578.416 *e-mails* tratados



Threat feeds (*Honeypots* Distribuídos do CERT.br, Team Cymru, SpamHaus, ShadowServer, Shodan, Operações Anti-Botnet)

Notificações para os ASNs e estatísticas públicas



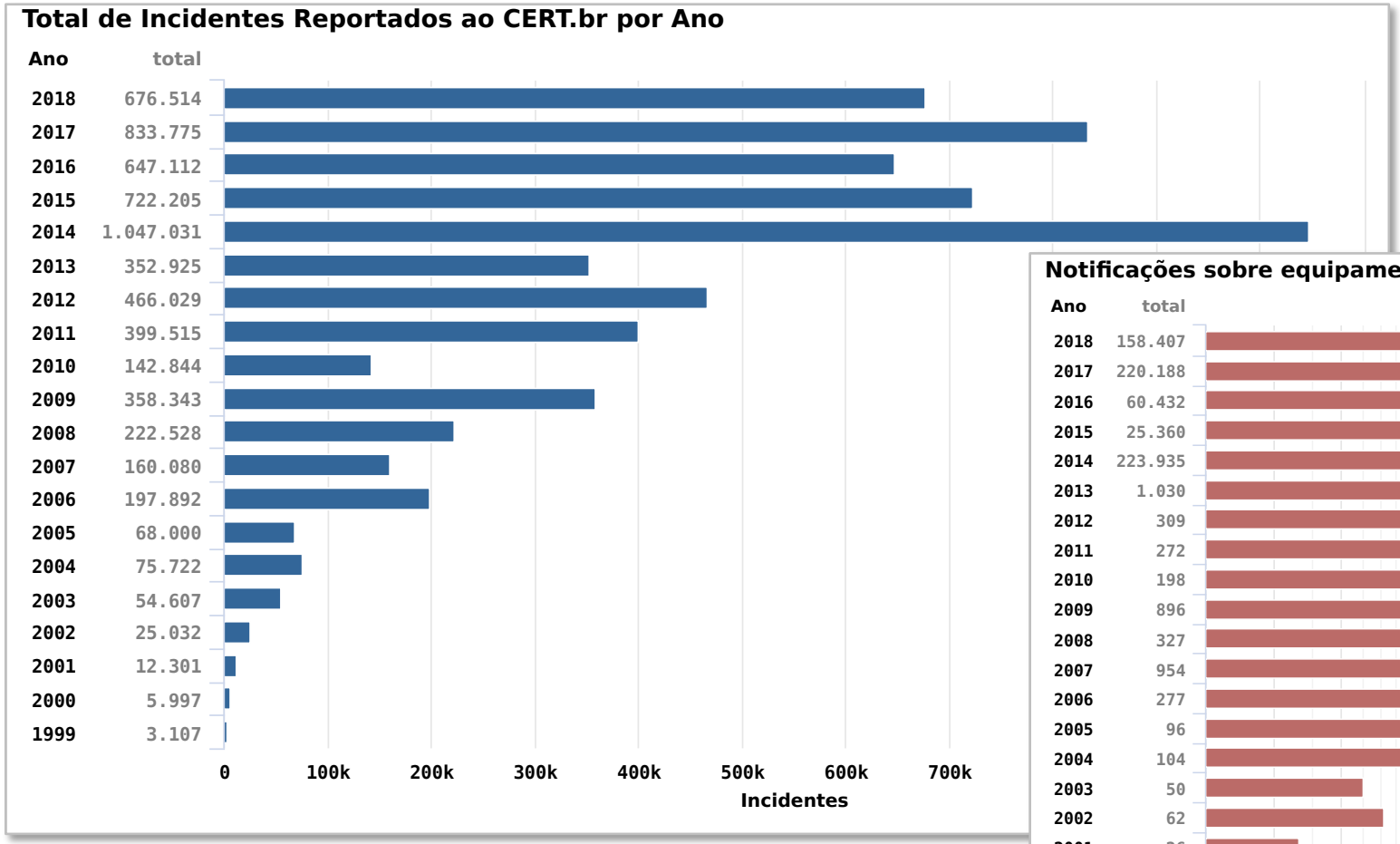
Reclamações de *spams* originados nas redes brasileiras

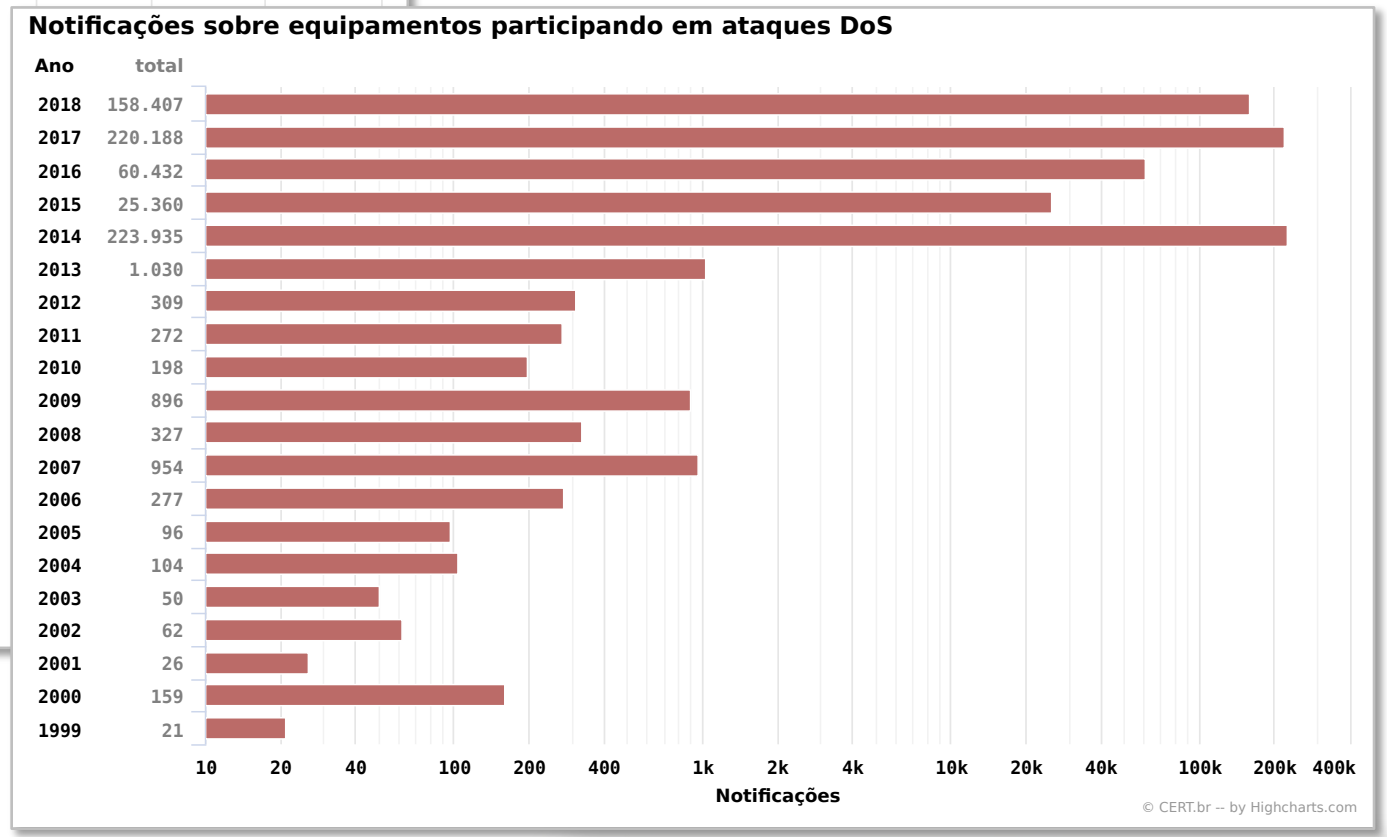
Tratados de forma automatizada – foco em identificar redes com problemas e reduzir abusos: 497.066 reclamações tratadas

https://cert.br/stats

Incidentes Reportados para o CERT.br:
Total e DDoS de 1999 a 2018

TLP:WHITE

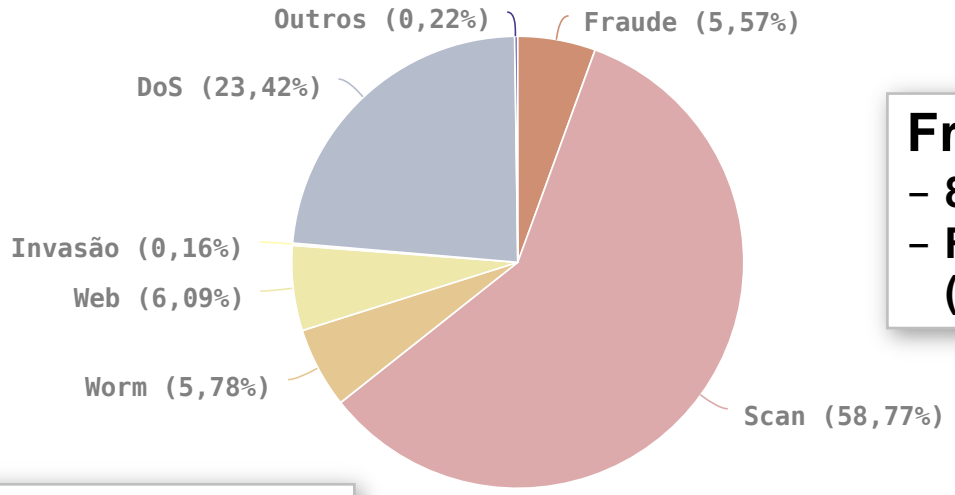




Fonte: https://www.cert.br/stats/incidentes/

TLP:WHITE

Incidentes Reportados para o CERT.br :
Detalhes sobre os tipos de incidentes vistos em 2018

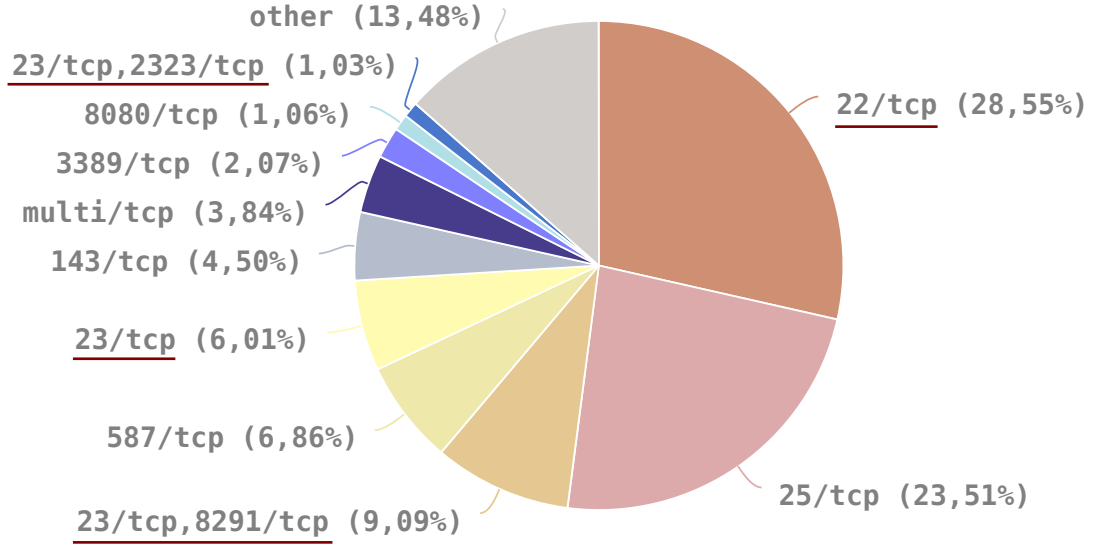


Fraude

- 84% são páginas falsas (*phishing*)
- Relacionadas com ataques em CPEs (*Rogue DNS + DNS Hijacking*)

DDoS

- Aumentou de patamar em 2014
- 300Gbps é o “normal”
- Até 1Tbps contra alguns alvos
- Tipos mais frequentes
  - *botnets* IoT
  - amplificação de tráfego



Scan

- Portas 22 e 23, 2323: força bruta de senhas de CPEs, servidores e IoT
- Portas 23, 8291: força bruta e vulnerabilidade Winbox MikroTik
- Porta 25: força bruta de senhas de *e-mail*

Ataques à Infraestrutura dos ASNs:
Incidentes Envolvendo Desvio de Tráfego

TLP:WHITE

Invasão de CPEs (roteadores domésticos) **para trocar o DNS**

Invadidos

- 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 Ataques

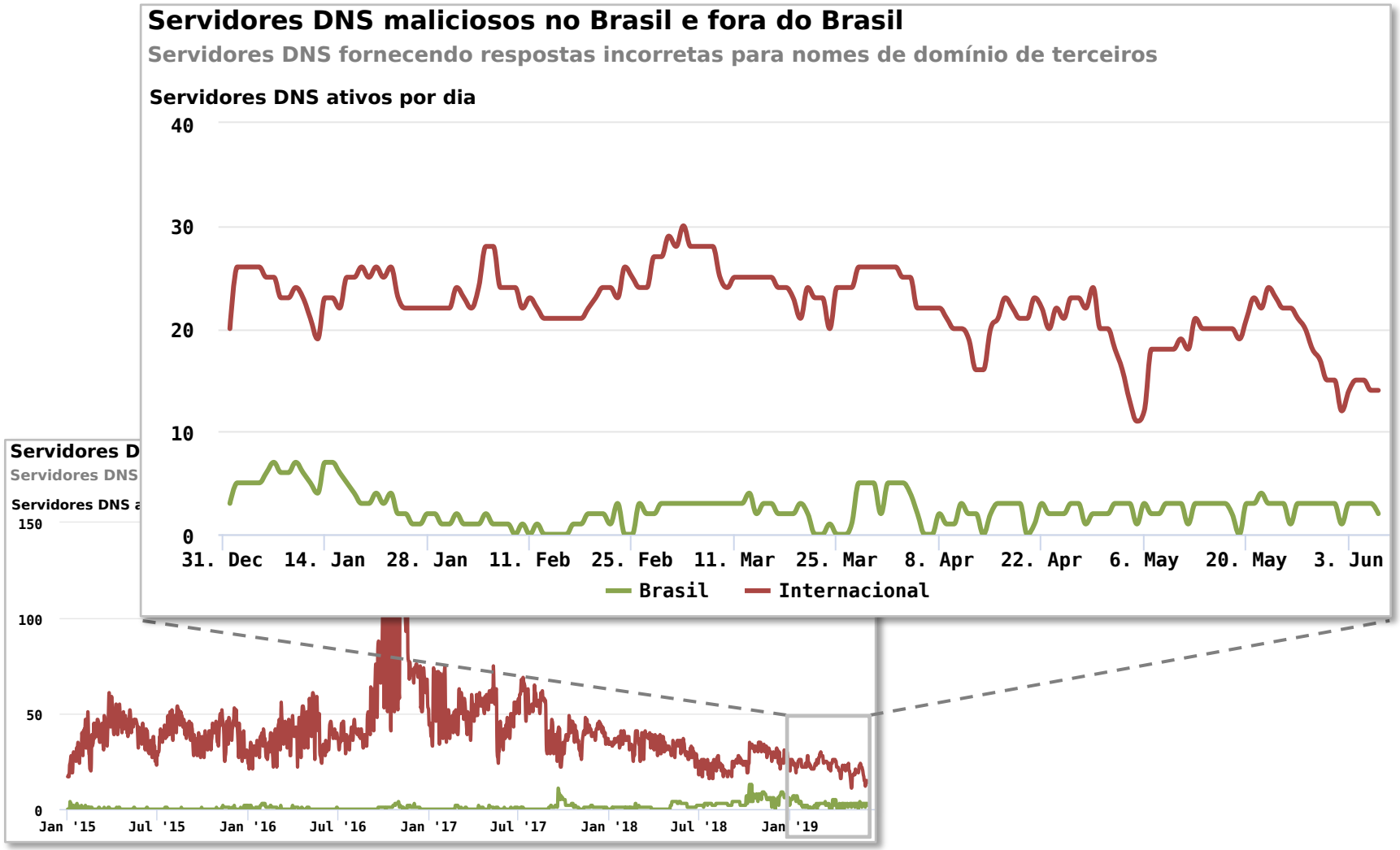
- **alterar a configuração de DNS para que consultem servidores sob controle dos atacantes**
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*

Sequestro de Rota BGP para Ataques Contra o Sistema Financeiro

- atacantes comprometem roteadores de borda de pequenos provedores
  - via força bruta de senhas (geralmente via telnet)
- 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

Servidores DNS Maliciosos Usados nos CPEs Invadidos: **Fornecem Respostas Autoritativas Erradas**

TLP:WHITE



Fonte: https://www.cert.br/stats/dns-malicioso/

Semântica é importante ao reportar incidentes ou pedir takedown!

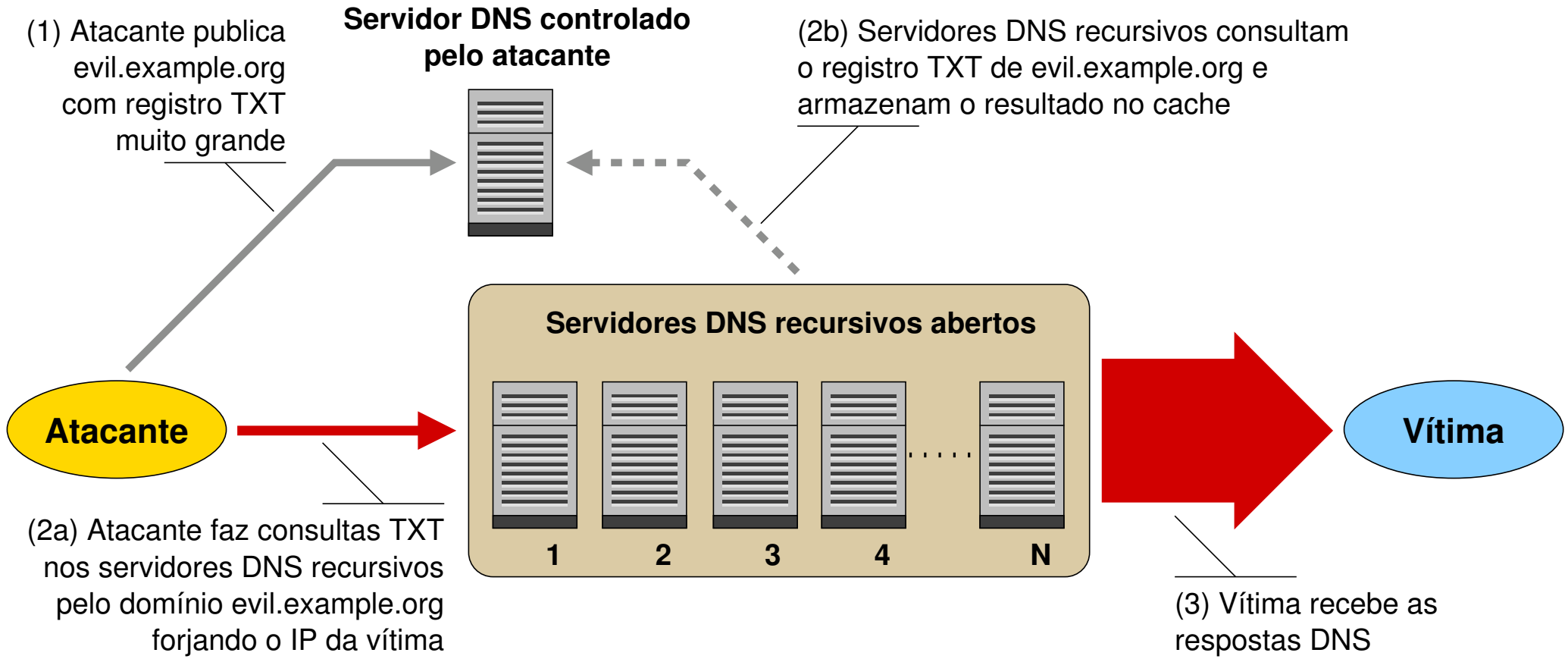
- **Isto não é um DNS invadido**
- **Isto não é envenenamento (*cache poisoning*)**
- **Isto não é sequestro de domínio (*domain hijacking*)**

Isto é um servidor DNS malicioso (*rogue*) sendo usado para sequestro de DNS (*DNS hijacking*)

- **autoritativo para os domínios das vítimas**
- **recursivo aberto respondendo ao restante das consultas**

Ataques DDoS com Amplificação: **Relembrando como Funcionam**

TLP:WHITE



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

Ataques DDoS com Amplificação:
Fatores de Amplificação

TLP:WHITE

Protocolo	Fator de Amplificação	Comando Vulnerável
DNS	28 a 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
LDAP / CLDAP	46 a 70	Malformed request
SSDP	30.8	SEARCH request
Chargen	358.8	Character generation request

Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A

TLP:WHITE

Dispositivos / Serviços que Permitem Amplificação:
Total de ASNs e IPs Brasileiros Notificados pelo CERT.br

	DNS		SNMP		NTP		SSDP		Ubiquiti	
month	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340	-	-
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255	-	-
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855	-	-
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836	-	-
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233	-	-
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124	-	-
2018-12	2.849	64.649	2.361	137.463	719	82.610	832	21.704	-	-
2019-01	2.960	74.257	2.583	137.253	923	89.567	840	17.348	-	-
2019-02	2.905	69.093	2.556	136.401	944	80.838	868	20.689	2.690	180.756
2019-03	2.933	63.895	2.661	111.561	914	72.873	847	18.837	2.042	95.974
2019-04	2.898	59.865	2.662	123.241	997	79.698	886	18.919	1.909	76.666
2019-05	3.045	68.764	2.633	103.204	1.019	77.979	953	18.564	1.797	64.729

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/

Dados disponíveis em: https://www.cert.br/stats/amplificadores/

TLP:WHITE

Abuso de MikroTik:
Varreduras Contra os *Honeypots* e *Payload* do *Exploit*

Varreduras por Winbox (8291/TCP) nos *honeypots*

- praticamente inexistentes até o dia 23/mar/2018
- atingiram um pico no dia 29 de março
- tem se mantido constantes em valores significativos

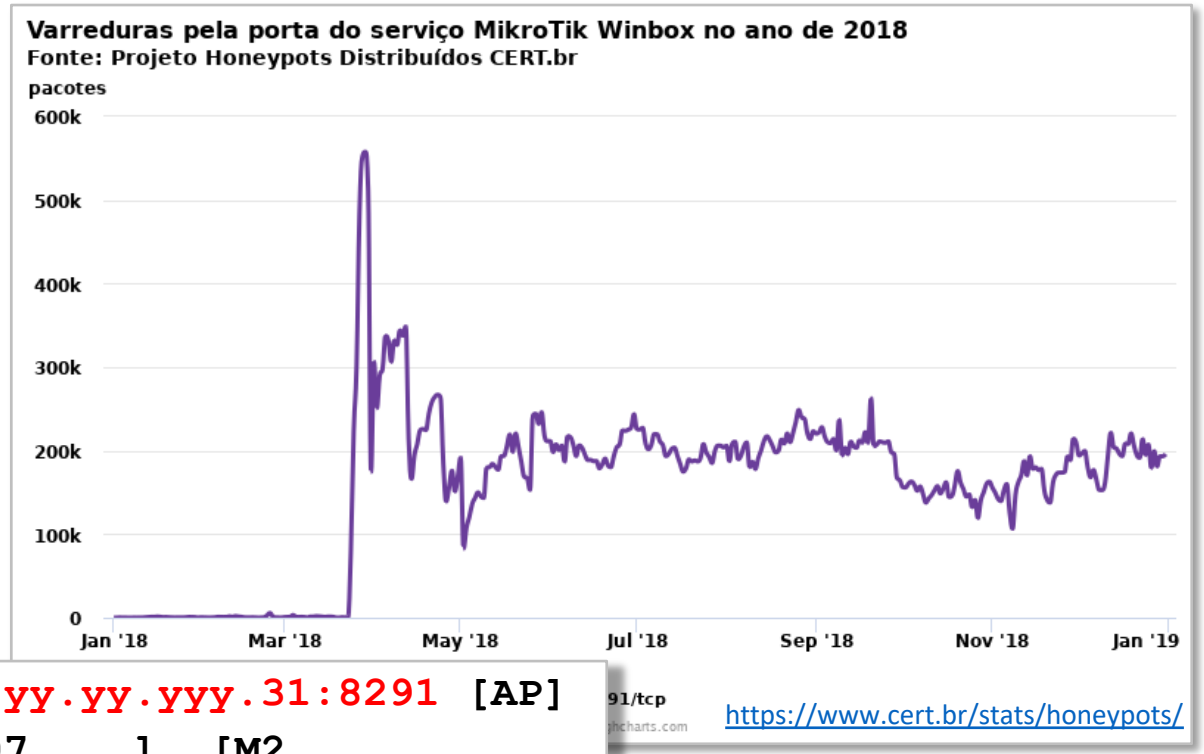
Recomendações:

- *hardening*
- manter RouterOS sempre na última versão Long-term

Referências:

https://blog.mikrotik.com/security/winbox-vulnerability.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847




```
T 2019/01/16 19:08:04.934837 xxx.xx.xx.86:51405 -> yy.yy.yyy.31:8291 [AP]
  5d 01 00 5b 4d 32 05 00    ff 01 06 00 ff 09 07 07    ]..[M2..........
  00 ff 09 07 01 00 00 21    2a 2e 2f 2e 2e 2f 2e 2f    .......!*./.././
  2e 2e 2f 2e 2f 2e 2e 2f    2e 2f 2e 2e 2f 2e 2f 2e    .././.././.././.
  2e 2f 72 77 2f 73 74 6f    72 65 2f 75 73 65 72 2e    ./rw/store/user.
  64 61 74 02 00 ff 88 02    00 00 00 00 00 08 00 00    dat.............
  00 01 00 ff 88 02 00 02    00 00 00 02 00 00 00       ...............
```

Papel do CERT.br no Brasil e no Mundo

cert.br nic.br cgi.br

TLP:WHITE

Foco do CERT.br nestes 22 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Auxiliar na análise técnica e facilitar o tratamento de incidentes por outros CSIRTs
- Ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (CSIRTs)
- Gerar massa crítica para possibilitar a cooperação e melhora na segurança das redes
- Ter uma visão sobre as principais tendências de ataques no Brasil

Comunidade Internacional

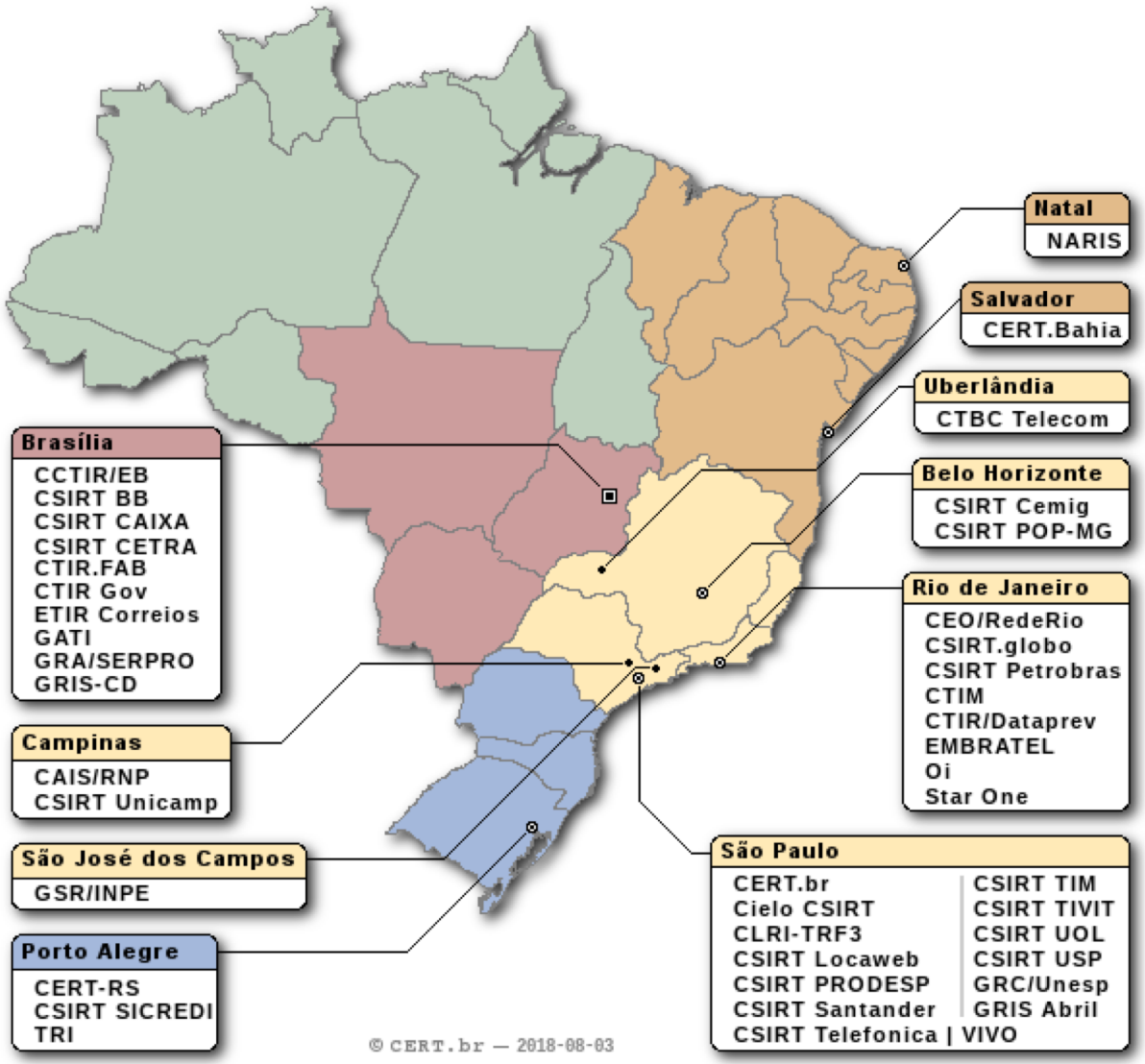
- Estabelecer relações de confiança
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes

Grupos de Tratamento de Incidentes (CSIRTs) Brasileiros: **42 times com serviços anunciados ao público**

TLP:WHITE

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, CSIRT Petrobras
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

https://cert.br/csirts/brasil/



Fóruns Internacionais de Segurança e Combate a Abusos na Internet

TLP:WHITE

FIRST – *Forum of Incident Response and Security Teams*

- Criação: 1990
- Membros: 483 CSIRTs, em 92 países, participantes de todos os setores (atualizado em 30/06/2019);

APWG – (originalmente *AntiPhishing Working Group*)

- Criação: 2003
- Membros: mais de 2.000 organizações, participantes de todos os setores, incluindo organizações internacionais;

M^{3}AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group*

- Criação: 2004
- Membros: mais de 200 membros da Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Criação: 2017
- Membros: Comunidade Internet em Geral; mantido pelo LACNOG, LACNIC e M^{3}AAWG.

TLP:WHITE

Cooperação Internacional: **Principais Fóruns**

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação:

- *Co-chair* do *Membership Committee*
- *Chair* da Conferência 2020
- Viabilizamos a parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos TCs e Simpósios na região
- Parte do grupo de especialistas do *Education Initiative*
  - atualizando a lista de serviços
  - formalizando a lista de competências

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

CERT/CC	US-CERT	CERT.at
NCSC-NL	NCSC-FI	CERT.LV
JPCERT/CC	NISC JP	HKCERT
TWCERT/CC		

LAC-CSIRTs

Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

TLP:WHITE

Trabalho desenvolvido no LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Editora: Lucimara, Chair LAC-AAWG / CERT.br

Publicação conjunta

- M³AAWG - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- LACNOG - *Latin American and Caribbean Network Operators Group*

Disponível em:

- Inglês e Japonês

Novas traduções serão publicadas em breve:

- Português, Espanhol, Francês, Alemão e Coreano

www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP

LACNOG-M³AAWG 共同作業による
顧客側通信機器 (CPE
最低限のセキュリティ
Best Current Operat
LAC-BC
May 201

この文書の原文は LACNOG の Web サイト www.
この文書の原文は M³AAWG の Web サイト www.

この文書は LACNOG[1] (Latin American and Caribbean
(Messaging, Malware and Mobile Anti-Abuse Working Gr
Current Operational Practices (BCOP)である。LACNO
AAWG[3] (Latin American and Caribbean Anti-Abuse Wor
した草案をもとに M³AAWG 会員と Senior Technical
調作業によって作成された。

目次

エグゼクティブサマリ .....
1. 用語について .....
2. 一般的要件 (General Requirements-GR) .....
3. ソフトウェアのセキュリティについての要件 (
4. アップデートと管理についての要件 (Update ar
5. 機能についての要件 (Functional Requirements-
6. 初期設定についての要件 (Initial Configuration
7. ベンダーについての要件 (Vendor Requirements
8. 略語一覧 .....
9. 謝辞 .....
10. 参考情報 .....
付録 1 – 要件の一覧表 .....

[1] Latin American and Caribbean Network Operators Group (LACNO
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M³A
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-A
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bc

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

lacnog

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition
LAC-BCOP-1

May 2019

This document is available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1
This document is available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

This is a joint Best Current Operational Practices (BCOP) document developed by LACNOG[1] (Latin American and Caribbean Network Operators Group) and M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group[4], in cooperation with M³AAWG members, Senior Technical Advisors and the M³AAWG Technical Committee.

Table of Contents

Executive Summary 2
1. Terminology 2
2. General Requirements (GR) 3
3. Software Security Requirements (SSR) 4
4. Update and Management Requirements (MR) 4
5. Functional Requirements (FR) 5
6. Initial Configuration Requirements (IR) 7
7. Vendor Requirements (VR) 8
8. List of Acronyms 8
9. Acknowledgements 8
10. Informative References 9
Annex 1 - Table of Requirements 11

[1]The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2]Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
[3]Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4]LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

TLP:WHITE

Precisamos um Ecossistema mais Saudável: **Programa por uma Internet mais Segura**

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

PROGRAMA INTERNET +SEGURA

https://bcp.nic.br/i+seg

Atuação em Incidentes Cibernéticos de Grande Envergadura

cert.br nic.br cgi.br

TLP:WHITE

Foco do CERT.br nestes 22 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Auxiliar na análise técnica e facilitar o tratamento de incidentes por outros CSIRTs
- Ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (CSIRTs)
- Gerar massa crítica para possibilitar a cooperação e melhora na segurança das redes
- Ter uma visão sobre as principais tendências de ataques no Brasil

Comunidade Internacional

- Estabelecer relações de confiança
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

The Honeynet PROJECT

Criação:

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

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

[1] https://www.nic.br/grupo/historico-gts.htm | [2] https://www.nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Foco das Atividades

- Atuar como ponto de contato nacional para notificação de incidentes
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências
- Transferir o conhecimento adquirido através de métricas, cursos, boas práticas e materiais de conscientização

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

02 de julho de 2019

nic.br cgi.br

www.nic.br | www.cgi.br