nic.br cgi.br | cert.br

Live Intra Rede – Principais Ataques na Internet

30 de setembro de 2020

Evento *Online*

Principais Ataques na Internet: Dados do CERT.br

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br 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	

Filiações e Parcerias:

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.

Público Alvo (*Constituency*)

Redes que utilizam recursos alocados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br).

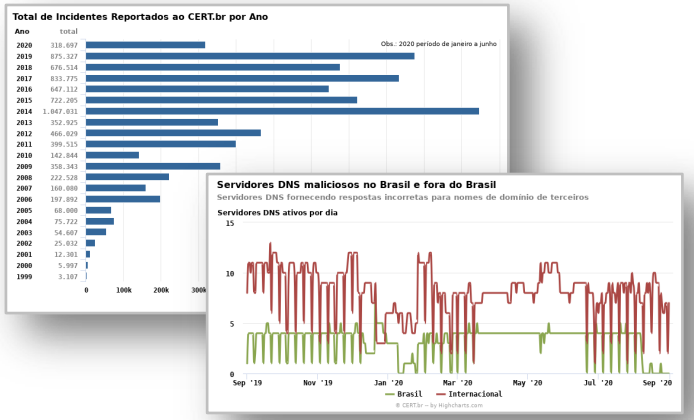
Foco das Atividades

- Ponto de contato nacional
- Trabalho colaborativo com outras entidades
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Tratamento de Incidentes:
Dados, Métricas e Compartilhamento

Notificações voluntárias de incidentes enviadas para: cert@cert.br

- 2019: 4.086.406 de *e-mails* tratados, relativos a 875.327 incidentes notificados ao CERT.br



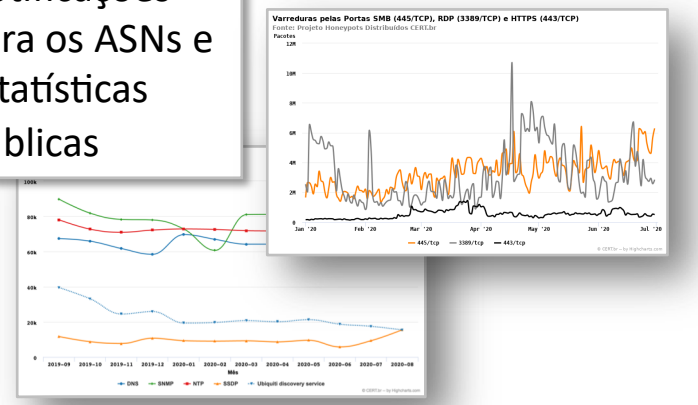
Compartilhamento via MISP

- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

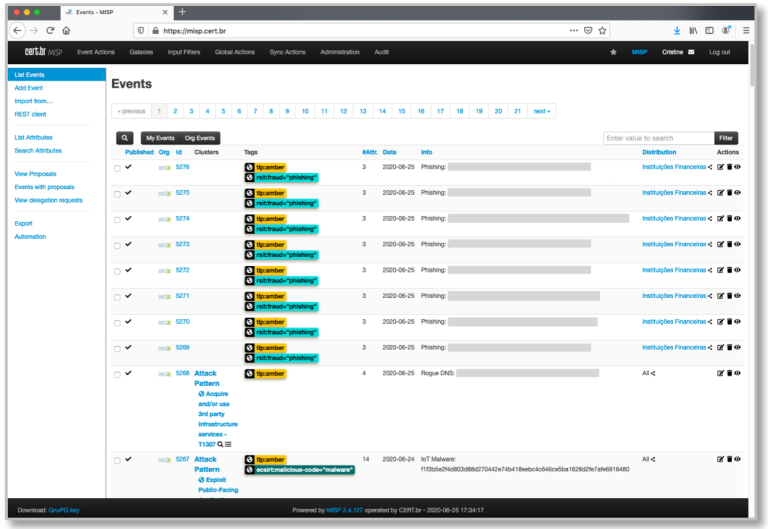
Threat feeds

- *Honeypots* Distribuídos do CERT.br
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)

Notificações para os ASNs e estatísticas públicas

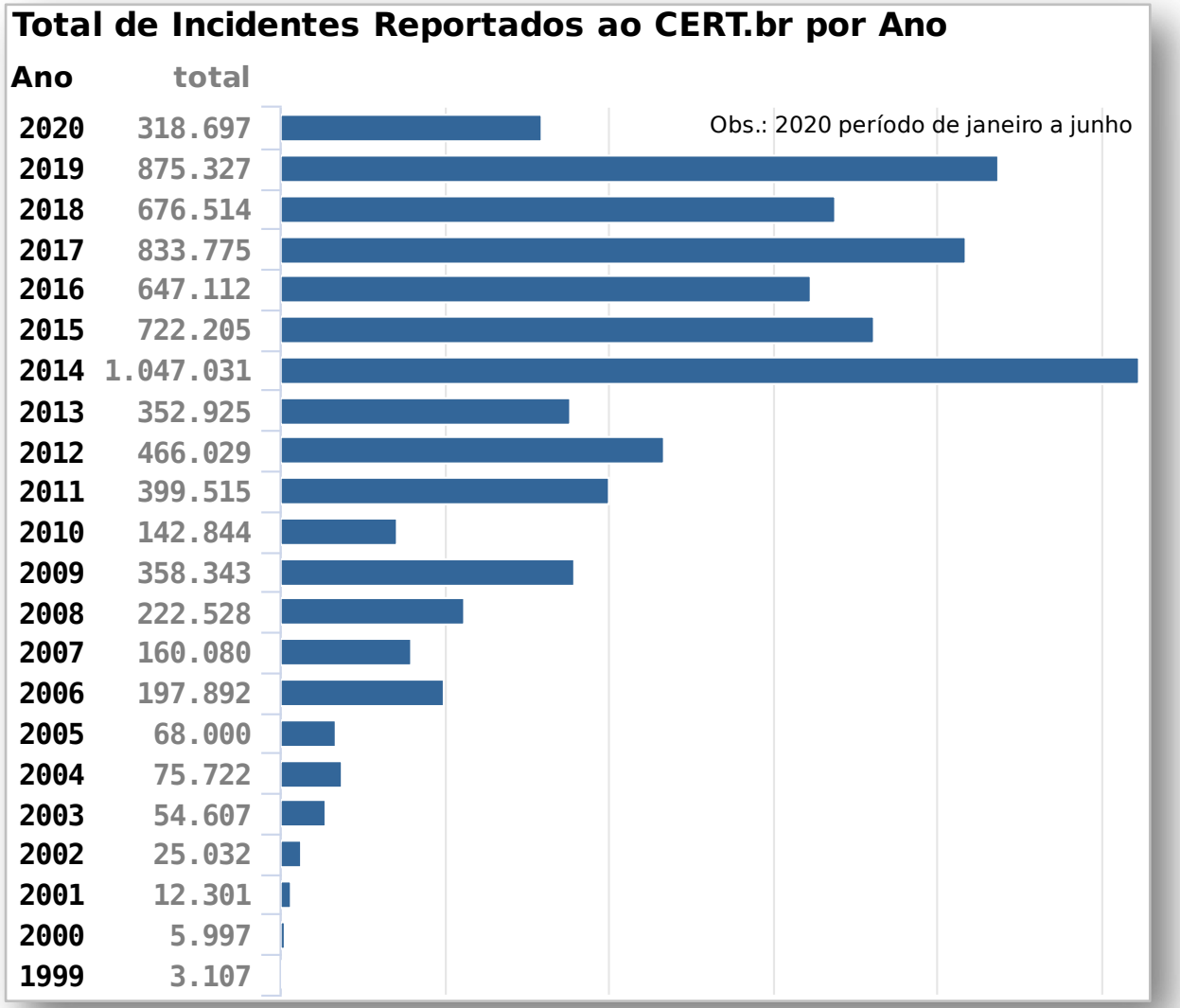


https://cert.br/stats/



https://cert.br/misp/

Incidentes Reportados para o CERT.br:
Dados Totais de 1999 ao 1º Semestre de 2020

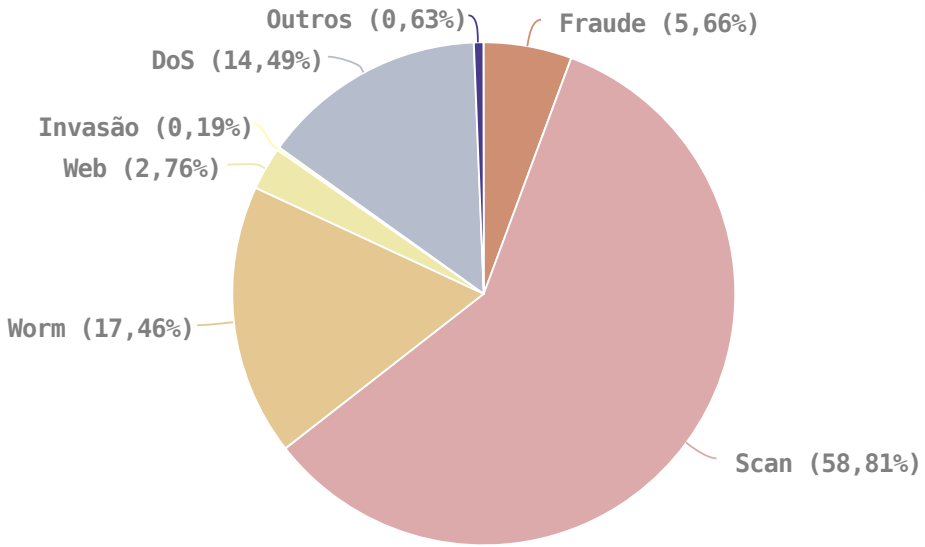


Fonte: https://cert.br/stats/incidentes/

Ataques mais comuns no último semestre

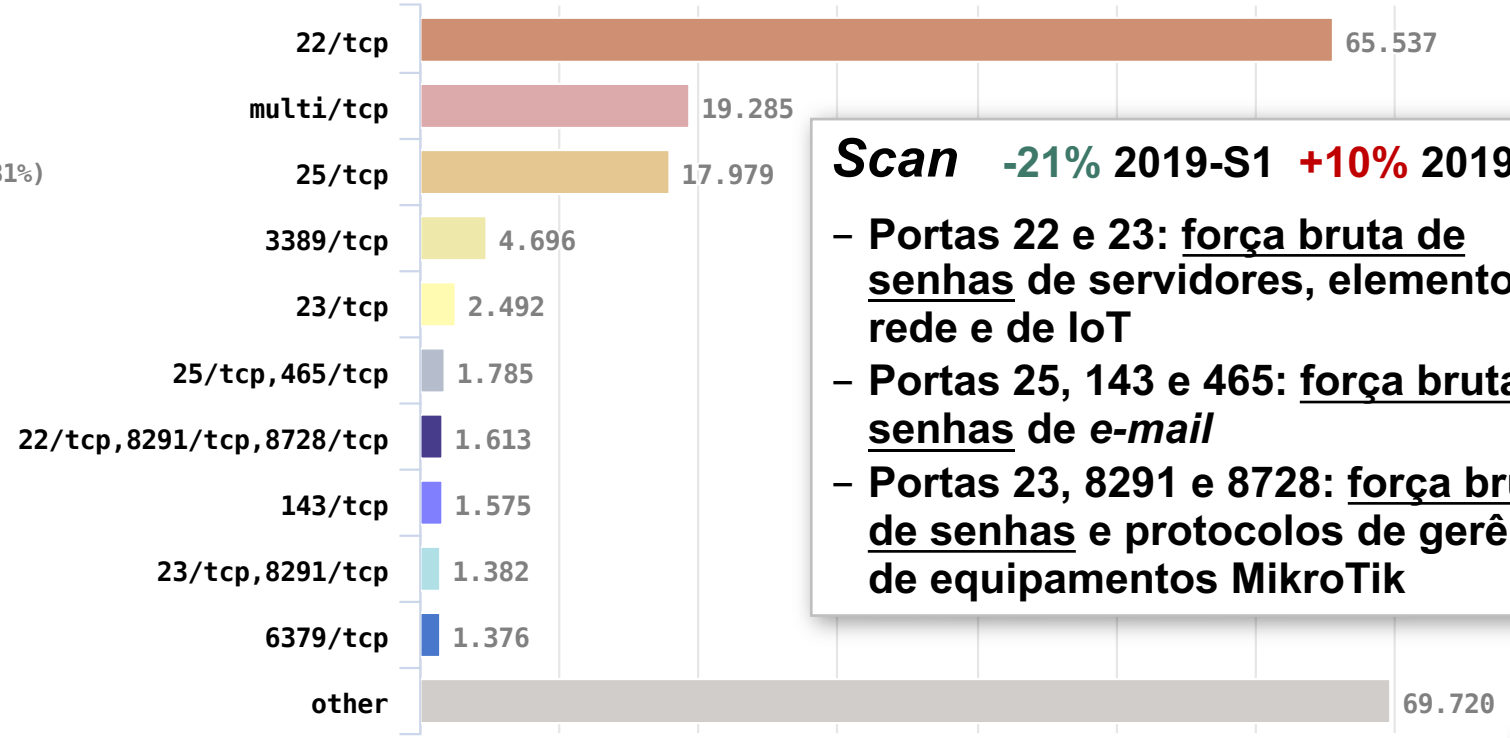
- Busca por serviços com credenciais fáceis e sem MFA
  - *e-mails* (IMAP, SMTP e SMTPS)
  - SSH e TELNET
    - elementos de rede e servidores
    - IoT e roteadores de banda larga
- Internet das coisas
  - Câmeras, *Smartphones*, TVs, Roteadores e *Modems* de banda larga/Wi-Fi
    - DDoS (UDP *flood*)
    - modificar DNS como parte de fraudes
    - minerar criptomoedas

Incidentes Reportados para o CERT.br:
Tipos de incidentes – 1º semestre de 2020



Fraude +54% 2019-S1 -35% 2019-S2

- 96% são páginas falsas (*phishing*)
- Relacionadas com invasão de CPEs para alterar o DNS



Scan -21% 2019-S1 +10% 2019-S2

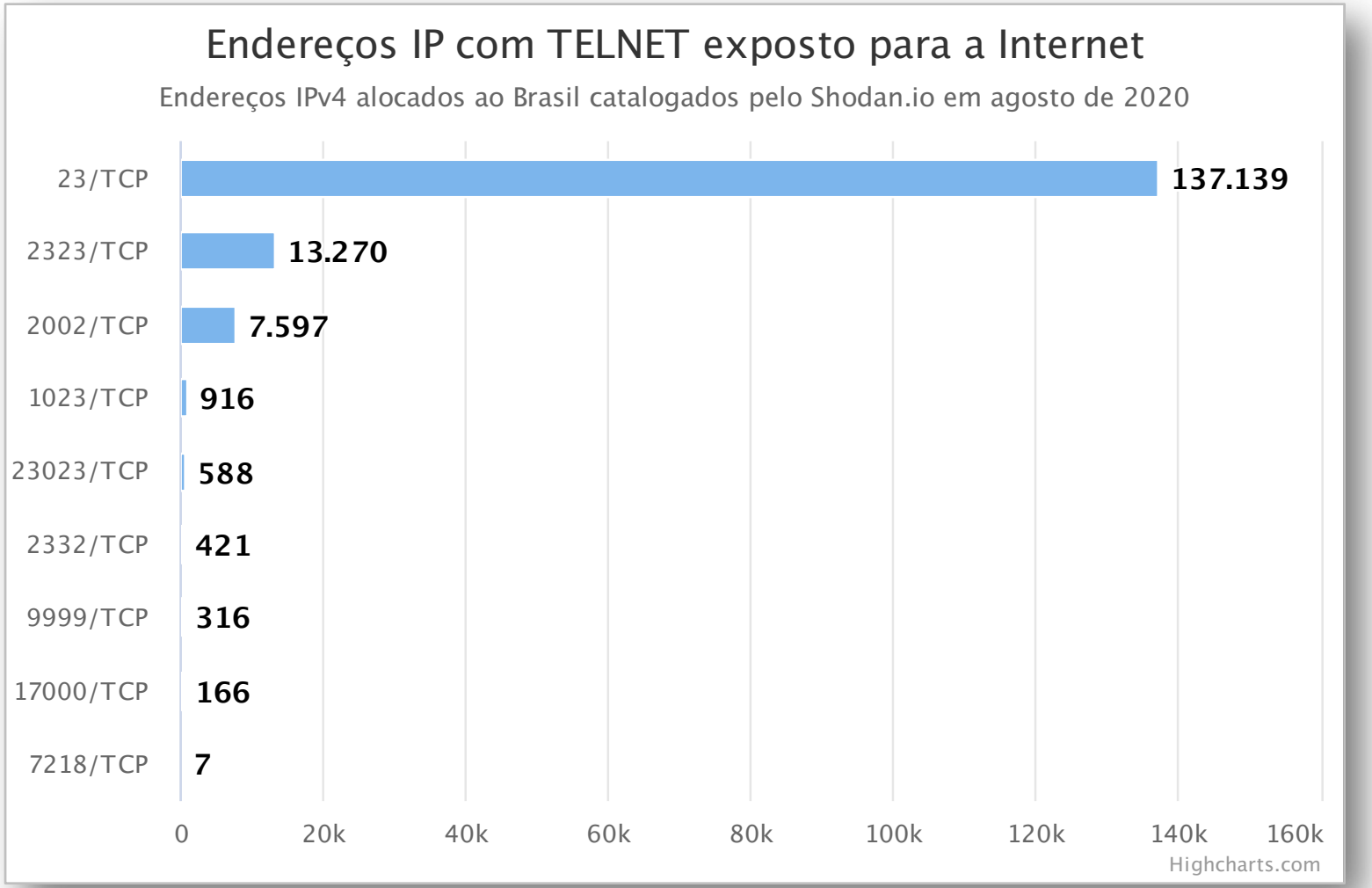
- Portas 22 e 23: força bruta de senhas de servidores, elementos de rede e de IoT
- Portas 25, 143 e 465: força bruta de senhas de *e-mail*
- Portas 23, 8291 e 8728: força bruta de senhas e protocolos de gerência de equipamentos MikroTik

DDoS -81% 2019-S1 -17% 2019-S2

- Tipos mais frequentes
  - *botnets* IoT
  - amplificação de tráfego
- Aumentou de patamar em 2014
- Número recorde foi em 2019

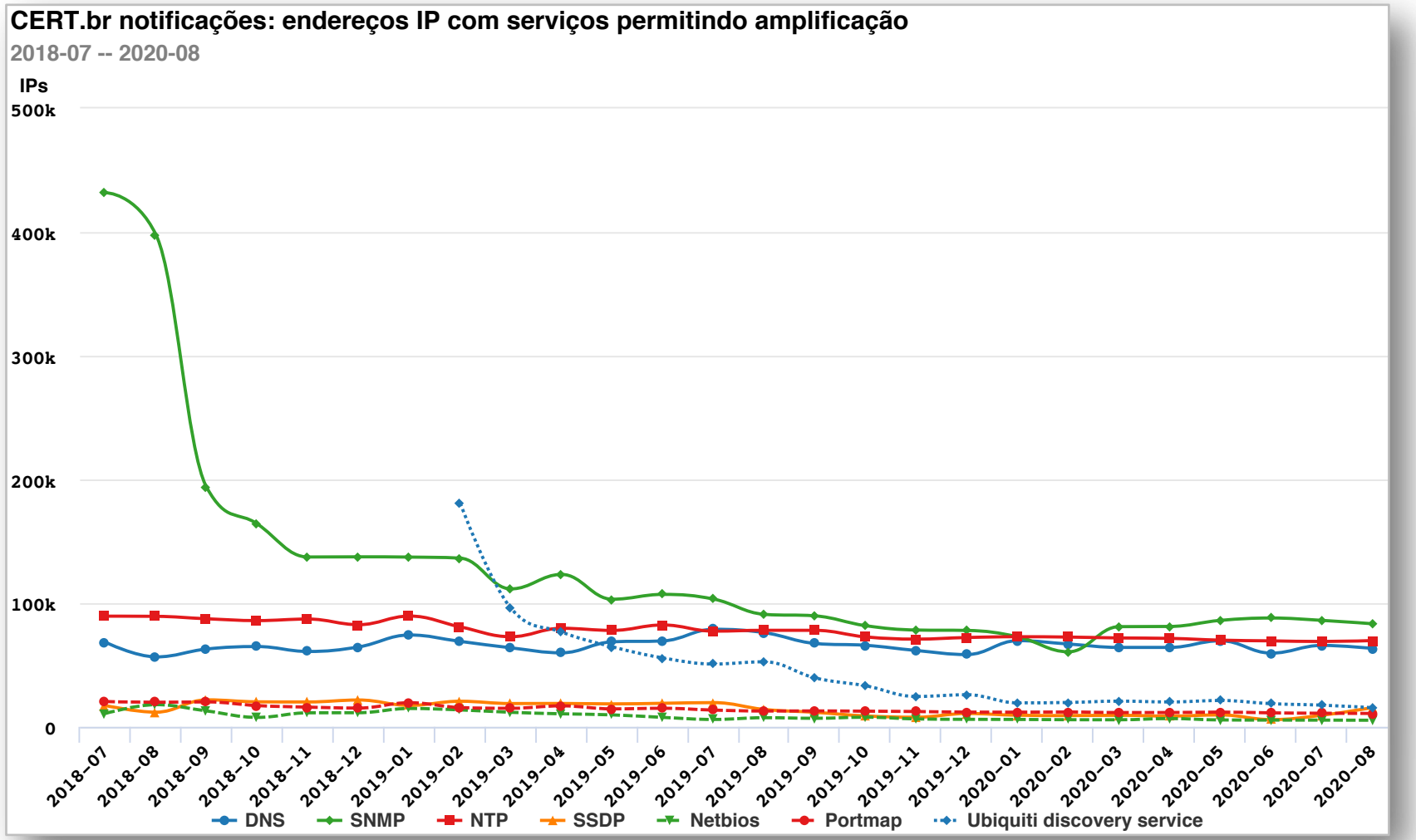
Varreduras TCP:
Honeypots (2020-S1) e TELNET no Shodan.io

#	Porta TCP	Pacotes	Bytes	Flows
01	23/tcp	30,1 G	1,5 TB	452,8 M
02	22/tcp	1,2 G	99,0 GB	250,2 M
03	445/tcp	595,2 M	43,5 GB	362,3 M
04	3389/tcp	574,4 M	28,0 GB	172,8 M
05	80/tcp	280,0 M	14,6 GB	200,6 M
06	1433/tcp	202,3 M	8,4 GB	174,0 M
07	443/tcp	95,6 M	4,1 GB	74,8 M
08	8080/tcp	77,2 M	3,9 GB	54,1 M
09	110/tcp	54,5 M	2,3 GB	12,0 M
10	81/tcp	47,1 M	1,8 GB	45,4 M
11	5900/tcp	44,7 M	2,1 GB	17,2 M
12	5555/tcp	41,8 M	1,6 GB	39,8 M
13	8545/tcp	37,9 M	1,4 GB	37,7 M
14	8291/tcp	37,6 M	1,6 GB	36,5 M
15	21/tcp	35,2 M	1,4 GB	12,5 M



Fonte: https://cert.br/stats/honeypots/

Estatísticas de Amplificação:
Notificações do CERT.br vs. *Honeypots*



#	Porta UDP	Pacotes	Bytes	Flows
01	5060/udp	637,5 M	361,9 GB	396,7 M
02	1900/udp	16,3 M	1,9 GB	16,3 M
03	123/udp	15,4 M	1,6 GB	15,2 M
04	161/udp	11,6 M	828,3 MB	7,3 M
05	389/udp	9,0 M	694,1 MB	9,0 M
06	53/udp	8,6 M	541,5 MB	8,5 M
07	1324/udp	7,8 M	816,9 MB	1,7 M
08	11211/udp	5,9 M	354,9 MB	5,8 M
09	53413/udp	4,9 M	716,5 MB	4,9 M
10	137/udp	4,9 M	361,0 MB	4,7 M
11	5353/udp	3,5 M	281,5 MB	3,5 M
12	1434/udp	3,5 M	104,6 MB	3,4 M
13	111/udp	3,4 M	232,9 MB	3,4 M
14	3283/udp	3,3 M	106,9 MB	3,3 M
15	19/udp	3,2 M	101,4 MB	3,2 M

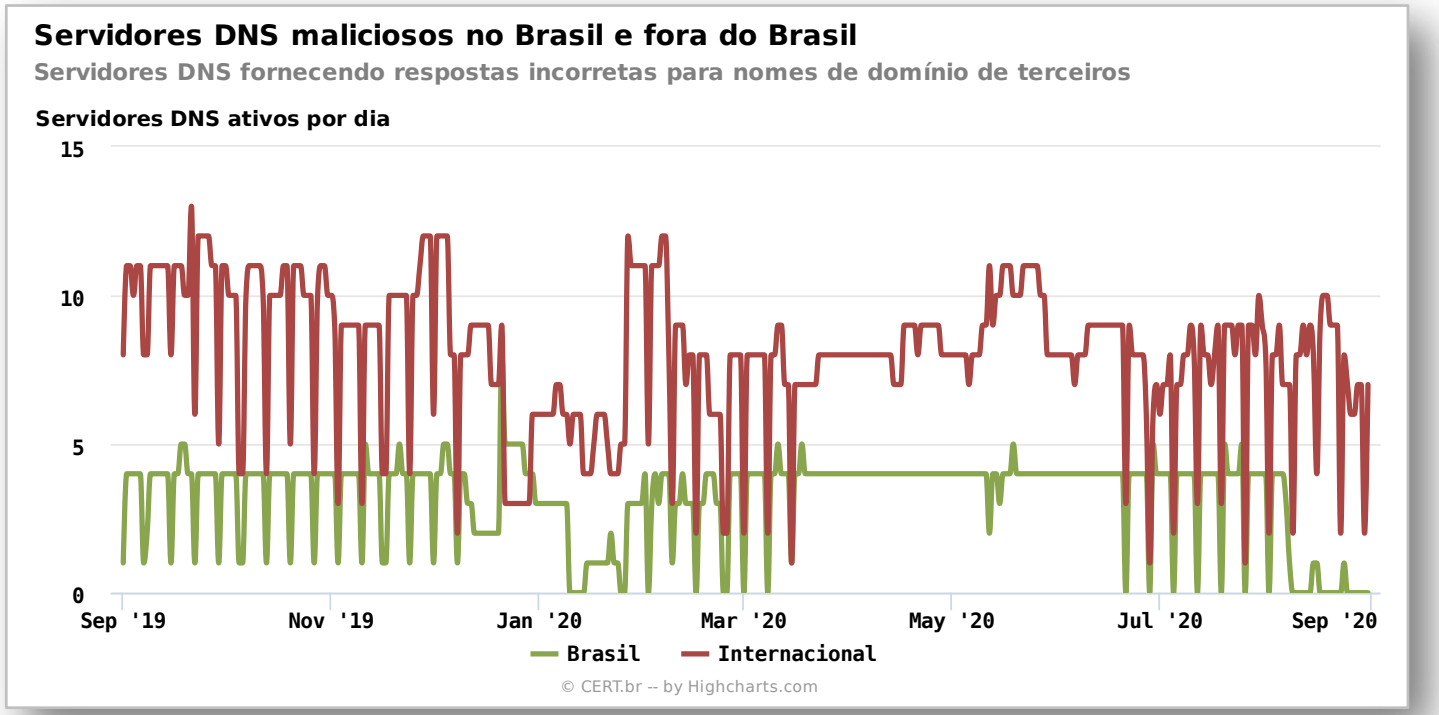
Fontes: https://cert.br/stats/amplificadores/ | https://cert.br/stats/honeypots/

CPEs Invadidos com DNS alterado:
Fornecem Respostas Autoritativas Erradas

Hospedagem em serviços de *cloud* e CDN

Domínios afetados dos seguintes setores:

- Bancos, Serviços de Pagamento, Serviços de *Streaming*, Mobilidade, Redes Sociais, *Webmail*, Comércio Eletrônico, entre outros



Fonte: https://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**

Como Melhorar o Cenário:
Investir no Básico

Manter Sistemas Atualizados

- Acompanhe todos os fabricantes do seu parque
- Atualize **TODOS** os sistemas e aplicações
  - mesmo que sejam “só internos”
- Defina regras para priorizar a aplicação de correções de segurança
  https://www.first.org/cvss/

Múltiplos Fatores de Autenticação

- Impede sucesso de força bruta de senhas
- Reduz impacto do comprometimento de credenciais

Tecnologias:

- Chaves criptográficas / certificados
- *Tokens*
  - em *hardware* (FIDO2/U2F)
  - em *software* (HOTP/TOTP)

Receber e Tratar Notificações

Acompanhar todas as notificações enviadas para

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

Considere que:

- Outras organizações e CSIRTs tem dados relevantes a passar
- Geralmente informações que podem utilizadas gratuitamente

Depois de Investir no Básico:
Adotar Protocolos Mais Modernos

	Padrões	Vantagens da Adoção
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
Segurança de *e-mail*	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra *sniffing* (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou • novas redes só terão IPv6	Mais estabilidade • Não depender de CGN ou tradução v6 → v4 • Redes móveis tendem a ter IPv6 nativo no futuro Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

Padrões	Referências
Tokens em *hardware* (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em *software* (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org https://letsencrypt.org/
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki

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

PROGRAMA INTERNET +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

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

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br