

nic.br egi.br

cert.br

Semana de Capacitação 2021, Ceptro.br/NIC.br
24 de junho de 2021
Evento *Online*

Segurança para Provedores

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br **nic.br** **egi.br**

Gestão de Incidentes

- ▶ Coordenação
- ▶ Análise Técnica
- ▶ Suporte à Mitigação e Recuperação

Consciência Situacional

- ▶ Aquisição de Dados
 - ▶ *Honeypots* Distribuídos
 - ▶ SpamPots
 - ▶ *Threat feeds*
- ▶ Compartilhamento das Informações

Transferência de Conhecimento

- ▶ Conscientização
 - ▶ Desenvolvimento de Boas Práticas
 - ▶ Cooperação, Eventos e Reuniões (*Outreach*)
- ▶ Treinamento
- ▶ Aconselhamento Técnico e Político

Filiações e Parcerias:



SEI
Partner
Network



Criação:

Agosto/1996: CGI.br publica o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”¹

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

¹ <https://cert.br/sobre/estudo-cgibr-1996.html> | ² <https://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 administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

<https://cert.br/sobre/>
<https://cert.br/sobre/filiacoes/>
<https://cert.br/about/rfc2350/>

Ataques Prevalentes e Problemas de Segurança

cert.br nic.br egi.br

“Hackers elegem o Brasil como alvo”?

“Metade dos ataques da América Latina” é muito ou pouco?

Hackers elegem o Brasil como alvo preferido na América Latina



Convergência Digital ... 21/06/2021 ... Convergência Digital

O Brasil sofreu mais de 3,2 bilhões de tentativas de ataques cibernéticos no primeiro trimestre de 2021. O país lidera o ranking da América Latina, que contabilizou um total de 7 bilhões de tentativas durante o período. México, Peru e Colômbia aparecem empatados em segundo lugar com 1 bilhão de ataques cada, conforme dados divulgados pela Fortinet.

abranet
Associação Brasileira de Internet

Home A Abranet Editorial Regulamento

NOTÍCIAS

Brasil sofreu metade dos ataques hackers direcionados para a América Latina

Por: Da Redação da Abranet* - 21/06/2021

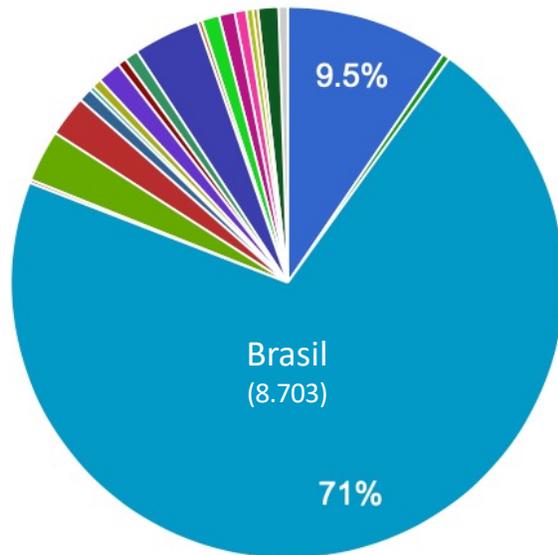
O Brasil sofreu mais de 3,2 bilhões de tentativas de ataques cibernéticos no primeiro trimestre de 2021. O país lidera o ranking da América Latina, que contabilizou um total de 7 bilhões de tentativas durante o período. México, Peru e Colômbia aparecem empatados em segundo lugar com 1 bilhão de ataques cada, conforme dados divulgados pela Fortinet.

<https://www.abranet.org.br/Noticias/Brasil-sofreu-metade-dos-ataques-hackers-direcionados-para-a-America-Latina-3431.html>

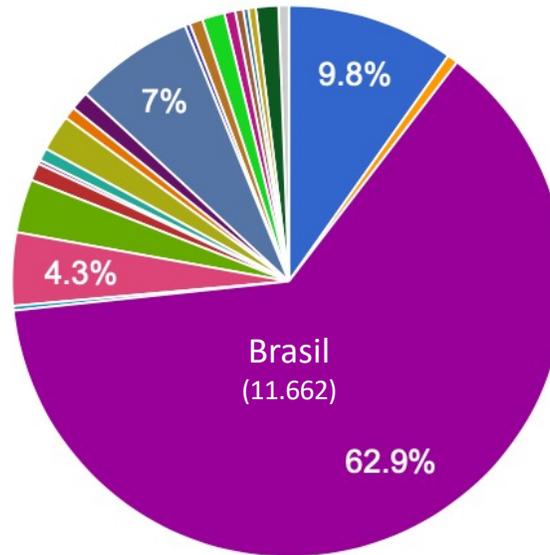
Internet no Brasil em Números: ASNs, IPs e Interconexão de Tráfego

Alocação de Sistemas Autônomos e Endereços IP na América Latina e Caribe

Distribution of ASN per country



Distribution of IPv4 blocks per country



Interconexão de tráfego

IX.br São Paulo

- nº 1 em participantes (2.326)
- nº 1 em pico de tráfego (13.2Tbps)
- nº 3 em média de tráfego (4.78Tbps)

Fonte: <https://www.pch.net/ixp/dir>

Fonte: <https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion>

Dados atualizados em 23 de junho de 2021

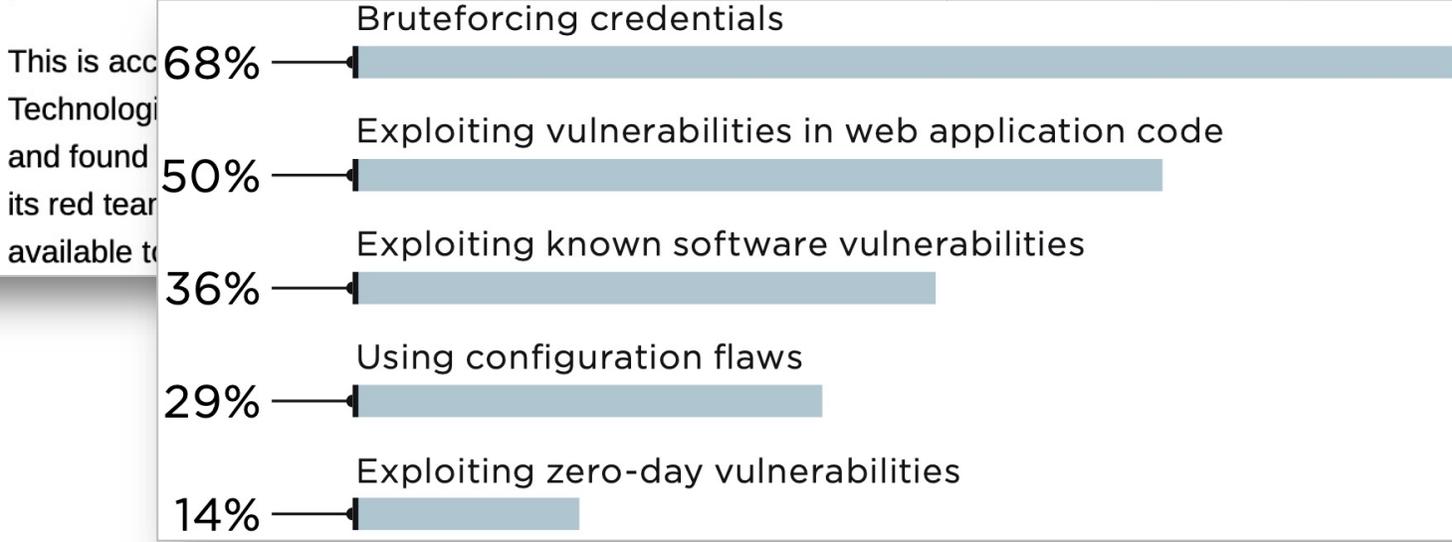
You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

Three little words: Patches, passwords, policies

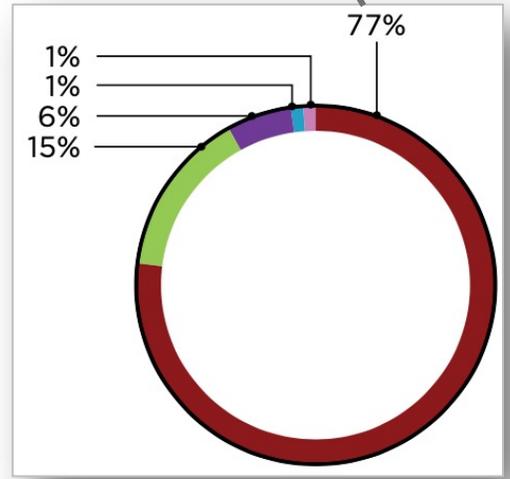
Thu 13 Aug 2020 // 07:06 UTC

Shaun Nichols in San Francisco [BIO](#) [EMAIL](#) [TWITTER](#)

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.



- Using web application protection vulnerabilities and flaws
- Bruteforcing credentials used for accessing DBMS
- Bruteforcing credentials for remote access services
- Bruteforcing domain user credentials together with software vulnerabilities exploitation
- Bruteforcing credentials for the FTP server



https://www.theregister.com/2020/08/13/pentest_networks_fail/

<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf>



Insider Threat Awareness Month Reminds Us That the Biggest Threats Can Arise from Within

Posted By **cyberinsiders**



Insider Threat Awareness Month offers a great opportunity to make organizations realize that today's modern cyberattack is no longer carried out by a dark cyber-assassin with sophisticated hacking techniques. The reality is that they no longer hack in at all, they log in using weak, stolen, or otherwise compromised passwords. And a shocking amount of the time, it is actually an insider doing the "hacking."

<https://www.cybersecurity-insiders.com/insider-threat-awareness-month-reminds-us-that-the-biggest-threats-can-arise-from-within/>

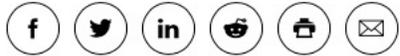
August 6, 2020

Lesson learned: Failure to patch led to password leak of 900 VPN enterprise servers



Teri Robinson

Follow @TeriRnNY



Applying a security update to a CVE released more than a year ago could have prevented a hacker from publishing plaintext usernames and passwords, as well as IP addresses, for more than 900 Pulse Secure VPN enterprise servers.

“The lesson here? Patch, patch, patch,” said Laurence Pitt, global security strategy director at Juniper Networks. “The fact that this vulnerability allowed for username/cleartext password combinations to be exposed is bad enough, but what makes it unacceptable is that this was reported in a CVE, released over a year ago and fixed in a later version of the product.”

<https://www.scmagazine.com/home/security-news/patch-fail-led-to-password-leak-of-900-vpn-enterprise-servers/>

Menu Search **Bloomberg** Sign In **Subscribe**

Bloomberg Cybersecurity < >  Hush-Hush NSA Lifts Veil on How Businesses Help Fight Hacks  John McAfee Faces U.S. Extrajudicial Arrest Over Taxes, Spanish Court...



Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By [William Turton](#) and [Kartikay Mehrotra](#)
June 4, 2021, 4:58 PM GMT-3

- ▶ Investigators suspect hackers got password from dark web leak
- ▶ Colonial CEO hopes U.S. goes after criminal hackers abroad

<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

Alert (AA20-133A)

Top 10 Routinely Exploited Vulnerabilities

Original release date: May 12, 2020



Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

Top 10 Most Exploited in 2020

Of the top 10 vulnerabilities from 2016 to 2019 listed above, the U.S. Government reported that the following vulnerabilities are being routinely exploited by sophisticated foreign cyber actors in 2020:

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
 - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
 - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting

<https://us-cert.cisa.gov/ncas/alerts/aa20-133a>

Rapid7 NICER Report 2020

Metodologia de estudo

- *“probe against all of IPv4 space to see if there’s something listening at all on a given port using Zmap”*
- *“then perform a protocol-level request against all nodes that responded to the initial probe”*
- *“Project Heisenberg is a net of honeypots Rapid7 has deployed across the [...] attacks are aggregated and sent to Rapid7 for enrichment and analysis”*

National / Industry / Cloud Exposure Report (NICER) 2020

Rapid7’s National / Industry / Cloud Exposure Report (NICER) for 2020 is the most comprehensive census of the modern internet. In a time of global pandemic and recession, the Rapid7 research team offers this data-backed analysis of the changing internet risk landscape, measuring the prevalence and geographic distribution of commonly known exposures in the interconnected technologies that shape our world.



<https://www.rapid7.com/research/report/nicer-2020/>

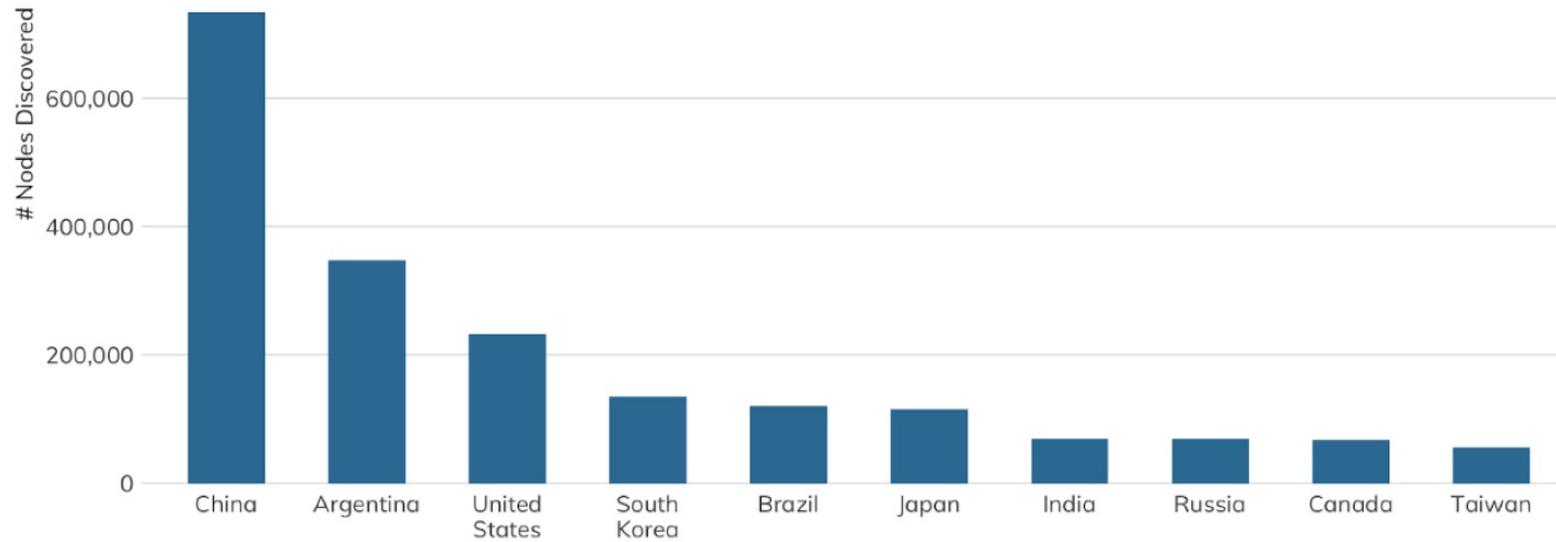
Rapid7 NICER Report 2020: Most Exposed Countries

- **Total attack surface** (i.e., number of total IPv4s in use exposing something during the study period). Rationale: More stuff = more stuff to attack.
- **Total exposure of selected services.** Specifically SMB, SQL Server, and Telnet. Rationale: These should never be exposed. Ever.
- **Distinct number of CVEs present across all services.** Rationale: More known vulnerabilities = more exposure.
- **The center of the distribution of vulnerability rates.** Vulnerability rate is defined as the number of exposed services with vulnerabilities/exposed services. Rationale: Higher vulnerability concentration across all exposed services should contribute more to the rank penalty.
- **Maximum vulnerability rate.** Rationale: To break any ties that remain after the previous steps, penalize a nation state with the highest vulnerability rate.

Rank	Country
1	United States
2	China
3	South Korea
4	United Kingdom
5	Germany
6	Brazil
7	Russia
8	Japan
9	Canada
10	Iran

Rapid7 NICER Report 2020: TELNET (23/TCP)

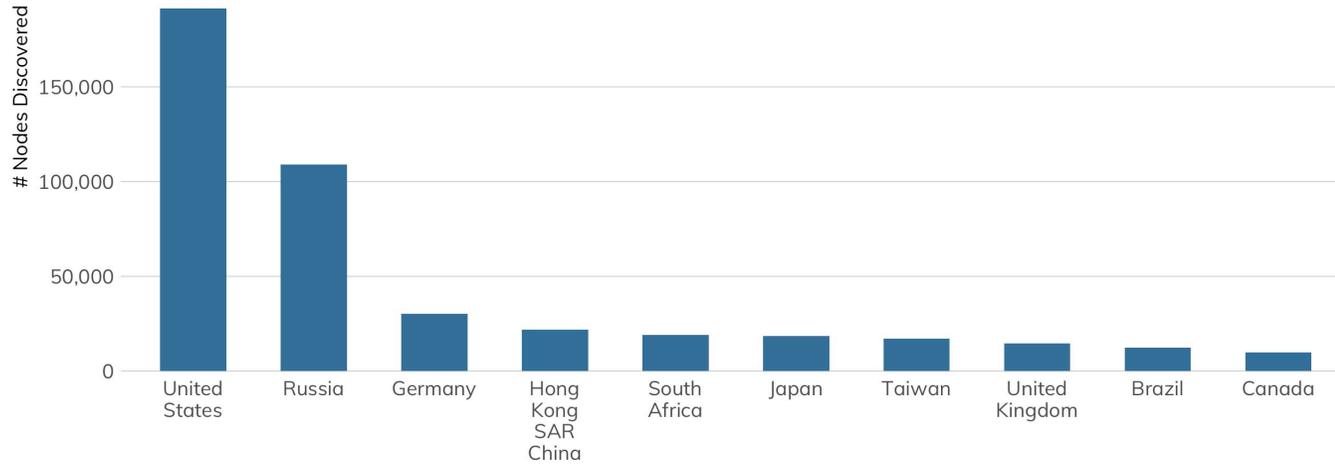
Top 10 Countries for Console Access : Telnet (23)



Vendor	Count
Cisco	278,472
Huawei	108,065
MikroTik	73,511
HP	70,821
Ruijie	17,565
ZTE	15,558

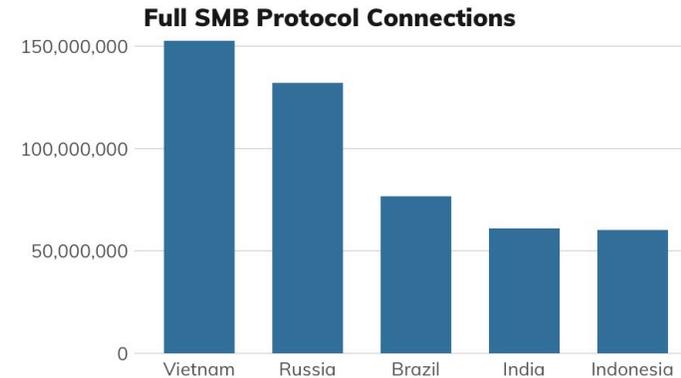
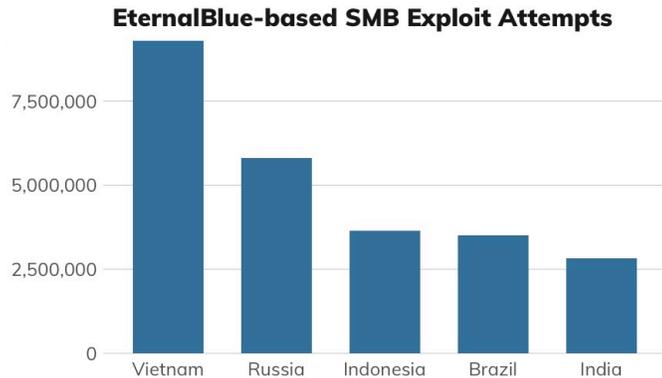
Rapid7 NICER Report 2020: SMB (445/TCP)

Top 10 Countries for File Sharing : SMB (445)



Project Heisenberg Malicious SMB Activity by Source Country (April 2020)

Note free Y scales



SMB Server Kind	Count
Windows (Server)	298,296
Linux/Unix/BSD/SunOS (Samba)	170,095
Windows (Desktop)	110,340
QNAP NAS Device	10,164
Other/Honeybot	1,914
Apple Time Capsule or macOS	1,465
Windows (Embedded)	703
Keenetic NAS	647
Printer	386

Rapid7 NICER Report 2020- RDP (3389/TCP)

Project Heisenberg RDP Activity

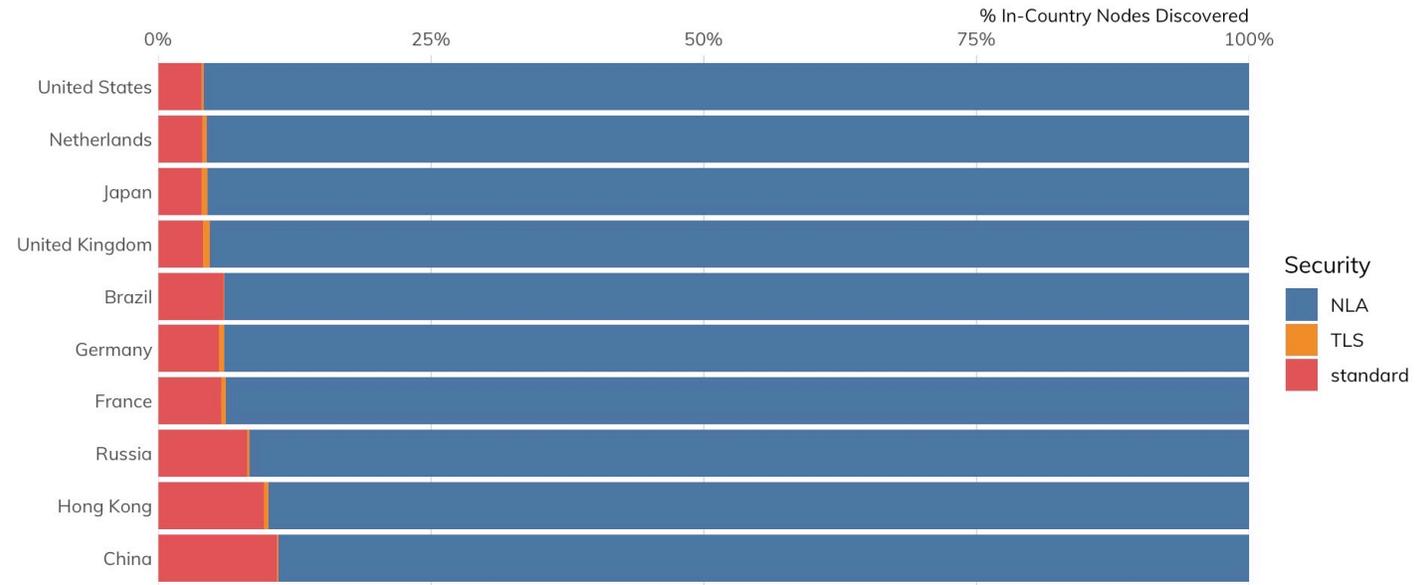
Total — Port BlueKeep Exploit Attempts



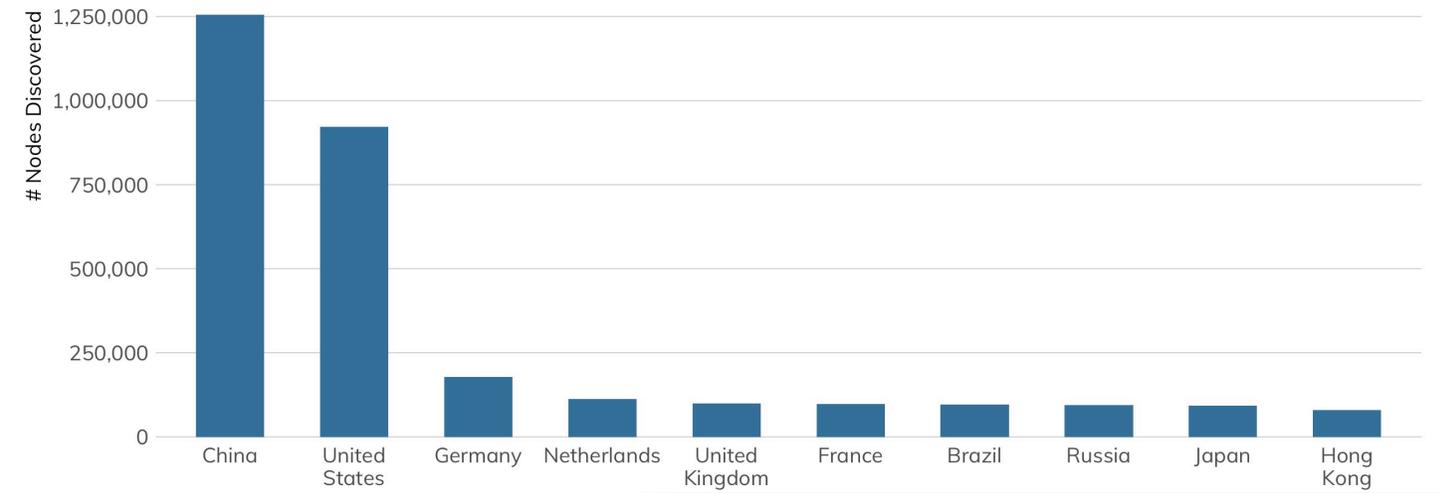
Unique — Port BlueKeep Exploit Attempts



RDP Security Used Percent by Country



Top 10 Countries for Remote Access : RDP (3389)



Projeto *Honeypots* Distribuídos do CERT.br: Top Portas TCP – 22/06/2021

#	Port	Name	Total	
01	23	TELNET	3.81 GB	94.27 %
02	445	Microsoft-DS Active Directory	60.95 MB	1.51 %
03	22	SSH (Secure Shell)	57.87 MB	1.43 %
04	3389	RDP (Microsoft Terminal Server)	19.15 MB	0.47 %
05	80	HTTP (Hypertext Transfer Protocol)	7.42 MB	0.18 %
06	8291	Mikrotik Winbox	6.43 MB	0.16 %
07	8728	Mikrotik API	5.65 MB	0.14 %
08	443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)	3.14 MB	0.08 %
09	21	FTP (File Transfer Protocol - control)	2.94 MB	0.07 %
10	1433	Microsoft SQL Server	1.78 MB	0.04 %
11	Others		66.29 MB	1.64 %

Fonte: <https://honeytarg.cert.br/stats/flows/2021/06/22/flows-2021-06-22.html>

Projeto *Honeypots* Distribuídos do CERT.br: Top Portas UDP – 22/06/2021

#	Port	Name	Total	
01	5060	SIP (Session Initiation Protocol)	276.88 MB	93.13 %
02	123	NTP (Network Time Protocol)	2.23 MB	0.75 %
03	389	LDAP (Lightweight Directory Access)	1.41 MB	0.47 %
04	53	DNS (Domain Name System)	676.86 KB	0.23 %
05	65060	N/A	610.66 KB	0.21 %
06	1900	SSDP	518.07 KB	0.17 %
07	3702	WS-Discovery	461.90 KB	0.16 %
08	6515	N/A	450.51 KB	0.15 %
09	5080	N/A	439.01 KB	0.15 %
10	5070	VTSAS (VersaTrans Server Agent Service)	409.51 KB	0.14 %
11	Others		13.22 MB	4.45 %

Fonte: <https://honeytarg.cert.br/stats/flows/2021/06/22/flows-2021-06-22.html>

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

mês	DNS		SNMP		NTP		SSDP		Portmap		Ubiquiti	
	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2020-06	3.248	59.613	3.119	87.996	1.063	69.523	705	5.859	1.647	11.302	1.388	18.746
2020-07	3.270	65.856	3.201	86.097	1.120	69.026	699	9.380	1.684	11.004	1.339	17.531
2020-08	3.261	63.398	3.191	83.327	1.131	69.764	770	15.579	1.647	10.844	1.274	15.503
2020-09	3.193	54.958	3.172	81.526	1.143	70.447	720	15.395	1.627	12.073	1.208	12.596
2020-10	3.247	54.648	3.253	86.907	1.128	70.329	818	19.746	1.654	12.264	1.147	10.771
2020-11	3.268	52.582	3.231	83.917	1.161	72.123	803	20.592	1.635	11.907	1.104	9.440
2020-12	3.253	55.852	3.200	81.773	1.186	71.765	812	21.070	1.623	11.258	1.041	8.654
2021-01	3.243	61.129	3.206	80.996	1.194	70.290	785	19.191	1.642	11.438	1.034	8.187
2021-02	3.252	64.200	3.188	78.482	1.191	71.413	771	18.584	1.614	11.134	996	7.702
2021-03	3.225	63.207	3.252	80.335	1.220	69.490	773	22.095	1.626	9.724	937	7.181
2021-04	3.259	59.877	3.305	78.657	1.221	71.816	791	19.001	1.647	9.704	902	6.361
2021-05	3.241	62.856	3.345	80.922	1.239	71.958	773	20.064	1.612	9.312	886	6.458

Obs.: Notificações realizadas após confirmar dados do ShadowServer sobre amplificadores no Brasil

<https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/>

Dados disponíveis em: <https://bcp.nic.br/i+seg/sobre/#panorama-atual>

Ataques à Infraestrutura dos ASNs: Incidentes Envolvendo Desvio de Tráfego

Sequestro de Rota BGP para Ataques Contra o Sistema Financeiro

- atacantes comprometeram roteadores de borda de pequenos e médios provedores
 - via **força bruta de senhas** (geralmente via telnet)
- anunciaram prefixos de rede mais específicos da instituição vítima (em geral /24)
- “peers” do provedor comprometido aprenderam a nova rota
- clientes das redes que aprenderam a nova rota passam a ser roteados para o local errado

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

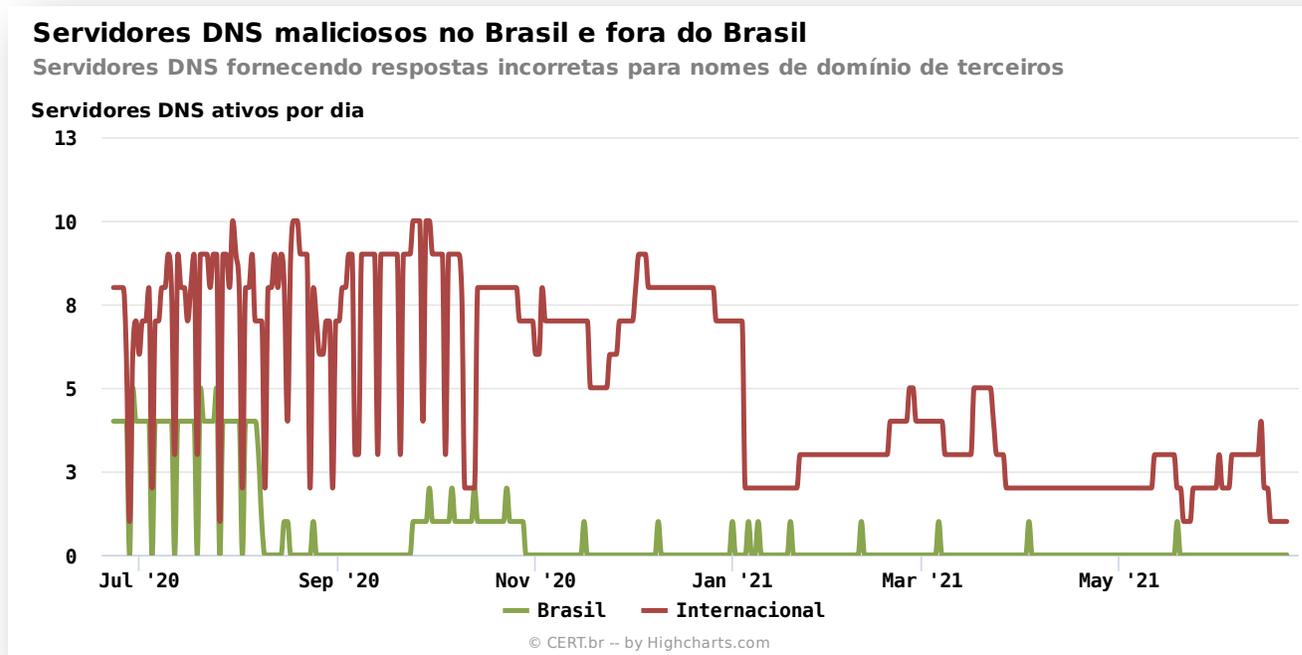
- **alterar a configuração de DNS para que consultem servidores sob controle dos atacantes**
- servidores DNS maliciosos hospedados em serviços de *hosting/cloud*

Servidores DNS Maliciosos Usados nos CPEs Invadidos: 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



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

<https://www.cert.br/stats/dns-malicioso/>
<https://team-cymru.com/blog/2020/09/08/illuminating-ghostdns-infrastructure-part-1/>
<https://team-cymru.com/blog/2020/10/07/illuminating-ghostdns-infrastructure-part-2/>
<https://team-cymru.com/blog/2021/01/26/illuminating-ghostdns-infrastructure-part-3/>
<https://cujo.com/dns-hijacking-attacks-on-home-routers-in-brazil/>

Resumo sobre os Incidentes Observados pelo CERT.br: Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores:

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
 - *e-mails* e serviços em nuvem
 - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
 - falta de aplicação de correções
 - erros de configuração
 - falta/falha de processos

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse mais atenção a erros e configurações
- todos os serviços tivessem 2FA/MFA

É necessário focar no básico

- *Patches* + configuração segura (*hardening*)
- Adotar MFA (*Multi-Factor Authentication*)
 - ex: aplicativo autenticador ou *token* (ex: Yubikey)
 - motivos usuais para não adoção
 - diminui a conveniência e pode ter custos
 - requer treinamento dos técnicos e usuários
 - medo de perder acesso aos serviços

Veja também: Principais Ataques na Internet: Dados do CERT.br
<https://youtu.be/nHh8hHaomFE?t=714>
<https://cert.br/stats/>

O que Priorizar

cert.br nic.br egi.br

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)

O mais importante:

- **Não usar somente senhas**

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

Boas Práticas para Acesso Remoto

Para todos os serviços que necessitam de autenticação

- Jamais utilizar contas e senhas padrão ou de teste
- Utilizar senhas fortes
- Considerar autenticação de dois fatores
- Aumentar monitoração

SSH

- Permitir **acesso somente via par de chaves**
- Reduzir os equipamentos com o serviço aberto para a Internet
- **Filtragem de origem**
- Mover o serviço para uma porta não padrão
- Considerar o uso de um **gateway de autenticação** (*jump host*, *host de salto*, *servidor de salto*, etc)
- **Acesso a elementos de rede somente via rede de gerência**

Estas e outras recomendações em:

- Sugestões para defesa contra ataques de força bruta para SSH
<https://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/>

Uso de SSH com par de chaves criptográficas: Gerando chaves em máquinas *UNIX-Like*

Gere o par de chaves com o comando `ssh-keygen`:

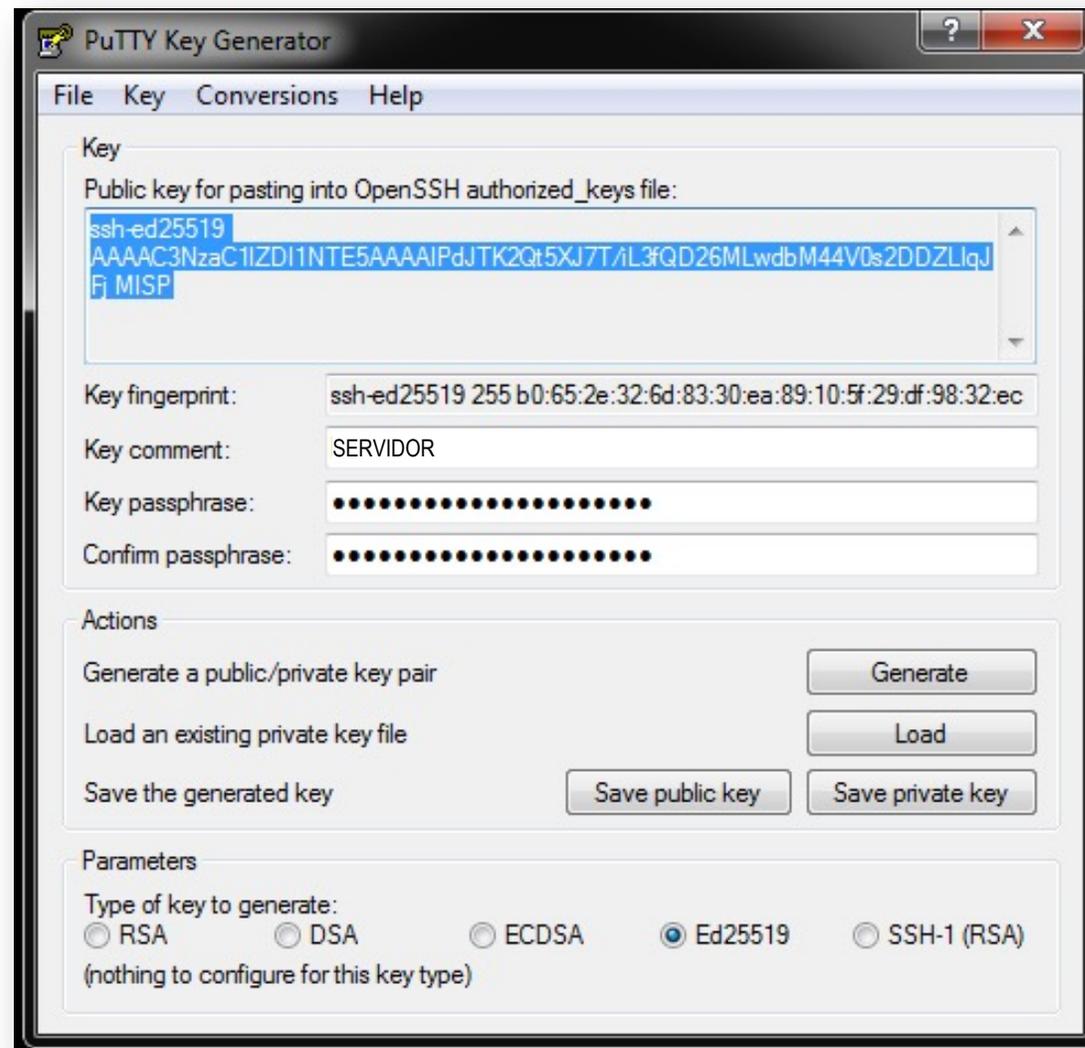
```
# ssh-keygen -t ed25519 -q -f /path/da/chave/servidor_ed25519 -C 'SERVIDOR'
```

Inclua o conteúdo do arquivo da chave pública recém gerada (`servidor_ed25519.pub`) no arquivo `/root/.ssh/authorized_keys` do seu servidor

Uso de SSH com par de chaves criptográficas: Gerando chaves em máquinas Windows

Gere o par de chaves com o aplicativo PuTTY Key Generator (`puttygen.exe`):

- Escolha o tipo `Ed25519`
- Utilize senhas fortes
- Copie o conteúdo da caixa “Public key for pasting into OpenSSH authorized_keys file” para o arquivo `/root/.ssh/authorized_keys` do seu servidor



Uso de SSH com par de chaves criptográficas:

Configurando o servidor

- Configure o *daemon* do SSH editando o arquivo `/etc/ssh/sshd_config` do servidor, alterando se necessário o conteúdo das seguintes linhas:

```
PermitRootLogin prohibit-password
```

```
PubkeyAuthentication yes
```

```
PasswordAuthentication no
```

- Reinicie o serviço do SSH com o comando:

```
# service sshd restart
```

Notificações enviadas pelo CERT.br: Como Identificar para Priorização

1. Cabeçalhos **From:** e **Return-Path:**

```
Return-Path: <cert@cert.br>  
From: "CERT.br" <cert@cert.br>
```

2. Sempre entregues pelo mesmo servidor de *e-mail*:

```
Received: from woq.cert.br (woq.cert.br [IPv6:2001:12ff:0:7000::2])  
 (using TLSv1.3 with cipher AEAD-AES256-GCM-SHA384 (256/256 bits))
```

3. Assinadas com DKIM, permitindo verificar origem:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=cert.br;  
s=certbr20200115; t=1623411839;  
bh=7LdHJ8S1GHTHez00QG00jtIWwJA5Fp68vQJmN8Qzfck=;  
h>Date:From:To:Cc:Subject:Message-ID:Reply-To:MIME-Version:  
Content-Type:Content-Transfer-Encoding:From;  
b=uxtftyG614MBjwkuAbdCMS84UXsWqrN49WoLXqaNEv6gp0Rftjk2Zn+moDKK4F3dOk  
weERFEziPO100BuOiLdL3my4TruuLwKMK2W86CdM+Y7IMi+4oZkCEqQ3cTciNYDKwi  
BSKAJhxm2tQfccGr4ecKCEh/PasEiUJSJQIbsgDE=
```

Notificações enviadas pelo CERT.br: Exemplo de Mensagem

Date: Fri, 11 Jun 2021 11:43:58 +0000
From: "CERT.br" <cert@cert.br>
To: abuse@[domínio], contato@[domínio]
Cc: cert@cert.br
Subject: Alerta: [AS XXXXX] servico Portmap habilitado

Caro responsável,

Os IPs presentes no log abaixo são de servidores sob sua responsabilidade com o serviço Portmap (111/udp) habilitado. Este serviço pode ser abusado para fazer parte de ataques distribuídos de negação de serviço, consumindo recursos da sua rede e impactando terceiros, além de poder revelar informações sensíveis armazenadas neste equipamento.

Gostaríamos de solicitar que:

* o serviço Portmap seja acessível apenas à sua rede local, ou que desabilite o serviço no equipamento, caso ele não esteja em uso.

[...]

```
=====
Endereco IP      | ASN      | Status | Data do Teste | Resultados do Teste
xxx.xx.xxx.xxx  | XXXXX   | OPEN  | 2021-06-11T10:47:12Z | portmap: open/1/188
=====
```

Mais detalhes sobre o porque do envio desta mensagem, quem é o CERT.br e como resolver este problema estão listados abaixo.

Cordialmente,

--

CERT.br
<cert@cert.br>
<https://www.cert.br/>

Como Detectar Abusos e Incidentes com *Netflows*

cert.br nic.br egi.br

Objetivos

Provavelmente você já tem habilidade de gerar *netflow* nos seus elementos de rede

- custo zero

É possível fazer tudo com *software* livre

- custo zero

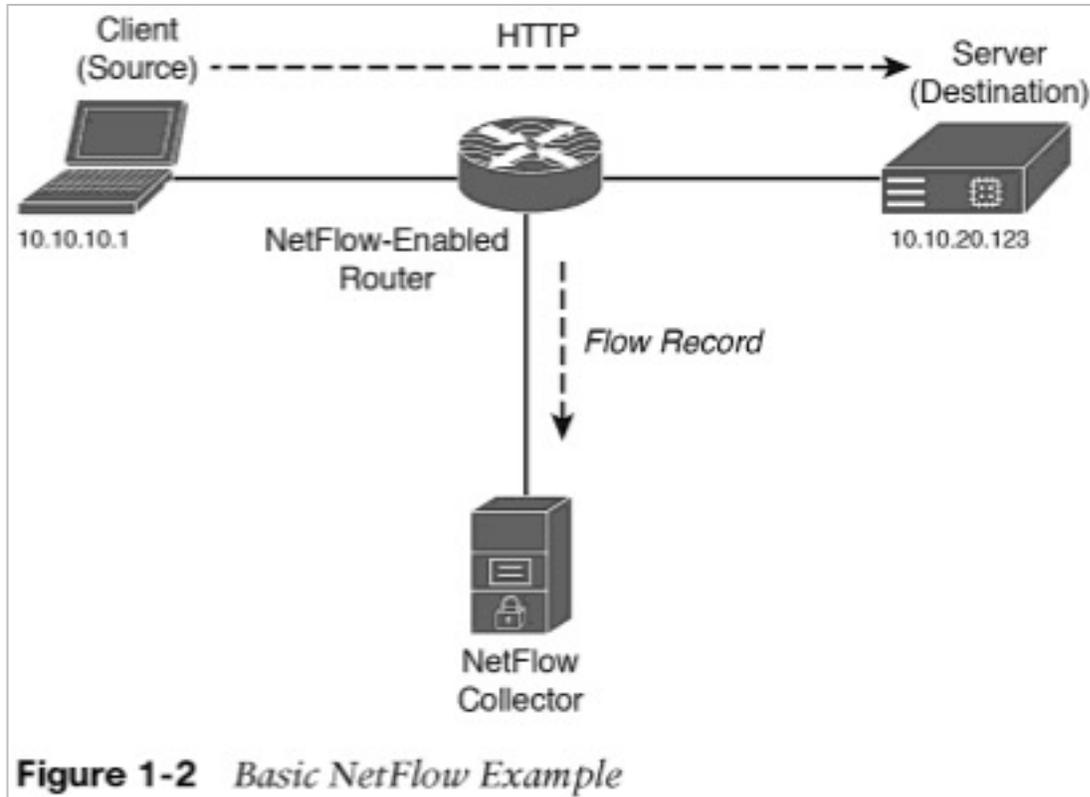
***Netflows* para segurança e não só para engenharia de tráfego**

- detectar *botnets*, DDoS saindo da sua rede, etc
- dados históricos para investigação de incidentes

Todos os exemplos utilizam

- nfcapd ou sfcapd para coleta dos *netflows*
- nfdump para consulta

O que é um *NetFlow*



Field	Value
Source IP address	10.10.10.1
Destination IP address	10.10.20.123
Source port	13578
Destination port	80
Protocol	TCP

Fontes:
Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security
<http://www.ciscopress.com/store/network-security-with-netflow-and-ipfix-big-data-analytics-9781587144387>
NetFlow – Wikipedia
<https://en.wikipedia.org/wiki/NetFlow>

Exemplo de *NetFlow*: Clientes Consultando DNS do Google

```
$ nfdump -R /var/log/flows/2017/12/06 \
```

```
'proto udp and dst port 53 and (dst host 8.8.4.4 or dst host 8.8.8.8)'
```

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port
2017-12-06 00:00:30.833	0.000	UDP	xxx.xxx.10.134:56263 ->	8.8.8.8:53
2017-12-06 00:02:04.330	0.000	UDP	xxx.xxx.77.56:54475 ->	8.8.8.8:53
2017-12-06 00:03:47.530	0.000	UDP	xxx.xxx.10.134:40439 ->	8.8.8.8:53
2017-12-06 00:03:50.097	0.000	UDP	xxx.xxx.77.56:57897 ->	8.8.8.8:53
2017-12-06 00:08:23.849	0.000	UDP	xxx.xxx.62.27:53777 ->	8.8.8.8:53
2017-12-06 00:09:02.758	0.000	UDP	xxx.xxx.10.210:55233 ->	8.8.8.8:53

```
[...]
```

2017-12-06 15:38:43.989	0.000	UDP	xxx.xxx.11.83:46347 ->	8.8.8.8:53
2017-12-06 15:38:45.134	0.000	UDP	xxx.xxx.77.56:47928 ->	8.8.8.8:53
2017-12-06 15:39:34.757	0.000	UDP	xxx.xxx.13.106:32768 ->	8.8.4.4:53
2017-12-06 15:39:36.639	0.000	UDP	xxx.xxx.11.83:35310 ->	8.8.8.8:53
2017-12-06 15:39:43.110	0.000	UDP	xxx.xxx.115.110:57283 ->	8.8.4.4:53

```
Summary: total flows: 3341, total bytes: 149035520, total packets: 1710592, avg  
bps: 21144, avg pps: 30, avg bpp: 87
```

```
Time window: 2017-12-06 00:00:00 - 2017-12-06 15:39:59
```

```
Total flows processed: 53147598, Blocks skipped: 0, Bytes read: 3409846180
```

```
Sys: 10.574s flows/second: 5025915.9 Wall: 10.563s flows/second: 5031249.4
```

Detecção de CPEs Comprometidos: Via Acessos a Servidores DNS Maliciosos

Sugestão de consulta *NetFlow*

- protocolo UDP porta destino 53 (DNS)
- origem no bloco de clientes
- cujo destino **não** seja
 - o seu recursivo
 - os servidores do Google (ou outros servidores públicos)

```
$ nfdump -R /var/log/flows/2017/12/06 'proto udp and dst port 53 and src net  
xx.xx.xx.xx/nn and not (dst host 8.8.4.4 or dst host 8.8.8.8 or dst host  
<seu-recursivo>)'
```

Como interpretar o resultado

- todo IP que aparecer no resultado consultou um DNS potencialmente malicioso
 - provavelmente está invadido
 - é necessário atuar
 - ex: atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc

Detecção de *Botnets* IoT: Via Acessos a IPs de Comando e Controle

Sugestão de consulta *NetFlow*

- destino a IPs publicamente listados como comando e controle de *botnets* IoT (que incluem *botnets* de CPEs)

<https://www.abuseat.org/iotcc.txt>

```
$ nfdump -R /var/log/flows/2017/12/06 'proto tcp and dst ip in [ @include iotcc.txt ]'
```

Como interpretar o resultado

- todo IP que aparecer no resultado acessou o comando e controle
 - provavelmente é um IoT ou um CPE invadido
 - é necessário atuar
 - se for IoT de cliente: contatá-lo para atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc;
 - se for um CPE invadido: atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc

Outra fonte de IPs maliciosos

https://urlhaus.abuse.ch/downloads/text_online/

Ataques DDoS:

Detecção de grandes geradores de tráfego (1/2)

Sugestão de consulta *NetFlow*

- procurar por todos os IPs que geraram muito tráfego
- somente em uma rede específica (CIDR)
- excluindo todos os serviços legítimos (como servidores web, vídeo conferência, etc)

```
$ nfdump -R /var/log/flows/2017/12/07 -s srcip/bytes -L 10G -n 10 'src net  
xx.xx.xx.xx/nn and not dst net xx.xx.xx.xx/nn and not ip in [ @include servers.txt ]'
```

Parâmetros da consulta:

- `-s srcip/bytes` – mostra estatísticas por IP, ordenado por *bytes*
- `-L 10G` – mostra somente os *flows* com 10 Gbytes ou mais de tráfego
- `-n 10` – mostra somente os top 10 IPs
- `xx.xx.xx.xx/nn` – deve ser o bloco CIDR de sua rede que você deseja ver se tem algum **amplificador** ou **botnet IoT**
- `src net xx.xx.xx.xx/nn` – especifica que só interessa o tráfego com origem na sua rede
- `not dst net xx.xx.xx.xx/nn` – especifica que o destino deve ser fora da sua rede (ou seja, não pega tráfego interno)
- `not ip in` – exclui todos os IPs de uma lista específica de IPs
- `servers.txt` – um arquivo ASCII que contém uma lista com todos os servidores da rede que geram muito tráfego e que você não está interessado em consultar pois já sabe que geram muito tráfego (exemplo: servidores *web*, *e-mail*, etc)

Ataques DDoS:

Detecção de grandes geradores de tráfego (2/2)

Resultado da consulta *NetFlow*

```
$ nfdump -R /var/log/flows/2017/12/07 -s srcip/bytes -L 10G -n 10 'src net xx.xx.xx.xx/nn and not dst net xx.xx.xx.xx/nn and not ip in [ @include servers.txt ]'
```

Top 10 Src IP Addr ordered by bytes:

Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
xxx.xxx.9.28	1.9 M(16.6)	983.8 M(16.6)	1.4 T(38.6)	17919	206.0 M	1436
xxx.xxx.18.85	154428(1.3)	79.1 M(1.3)	100.8 G(2.8)	1443	14.7 M	1275
xxx.xxx.62.49	128903(1.1)	66.0 M(1.1)	94.6 G(2.6)	2102	24.1 M	1432
xxx.xxx.46.36	266474(2.3)	136.4 M(2.3)	93.3 G(2.6)	2486	13.6 M	683
xxx.x.106.10	109648(0.9)	56.1 M(0.9)	80.9 G(2.2)	1126	13.0 M	1440
xxx.xxx.75.167	108737(0.9)	55.7 M(0.9)	80.5 G(2.2)	1296	15.0 M	1446
xxx.xxx.2.21	134183(1.2)	68.7 M(1.2)	80.0 G(2.2)	1251	11.7 M	1164
xxx.xxx.236.103	103314(0.9)	52.9 M(0.9)	75.2 G(2.1)	965	11.0 M	1421
xxx.xxx.10.215	73854(0.6)	37.8 M(0.6)	54.9 G(1.5)	688	8.0 M	1451
xxx.xxx.125.2	83531(0.7)	42.8 M(0.7)	46.2 G(1.3)	779	6.7 M	1080

Summary: total flows: 11587182, total bytes: 3657941800960, total packets: 5932637184, avg bps: 533034287, avg pps: 108062, avg bpp: 616

Time window: 2017-12-07 00:00:00 - 2017-12-07 15:14:59

Total flows processed: 41883344, Blocks skipped: 0, Bytes read: 2687644604

Sys: 16.990s flows/second: 2465146.9 Wall: 16.975s flows/second: 2467332.3

Como interpretar o resultado

- todo IP que aparecer no resultado potencialmente gerou um ataque DDoS para fora da rede
- necessário investigar se é um amplificador ou parte de uma *botnet*

NetFlows:

Referências

RFC 7011 / STD 77: *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

- <https://tools.ietf.org/html/rfc7011>

NetFlow version 9

- <https://www.cisco.com/c/en/us/products/ios-nx-os-software/netflow-version-9/>

NFDUMP/ NfSen

- <http://nfdump.sourceforge.net>

Mikrotik Traffic Flow

- https://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow

Juniper Flow Monitoring

- https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/services-interfaces/flow-monitoring.html

Uso de *Flows* no Tratamento de Incidentes da Unicamp

- <https://ftp.registro.br/pub/gts/gts26/01-flows-unicamp.pdf>
- <https://youtu.be/ckEX7vUFOzk>

Onde Investir Além do Básico

cert.br nic.br egi.br

Adotar Protocolos Mais Modernos

	Padrões	Vantagens da Adoção
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	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 <i>cache</i> Habilitar o uso de outras tecnologias como o DANE
Segurança de <i>e-mail</i>	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra <i>sniffing</i> (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir <i>phishing</i> 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

Is your Internet up to date? <https://internet.nl>

The screenshot shows the Internet.nl website interface. At the top left is the logo with the text "Internet.nl IS YOUR INTERNET UP TO DATE?". To the right are language options for "English" and "Nederlands". A navigation menu includes "Home", "News", "Knowledge base", "Hall of Fame", and "About Internet.nl". A central banner reads: "Modern Internet Standards provide for more reliability and further growth of the Internet. Are you using them?". Below this are three test cards:

- Test your website** (with a padlock icon): "Modern address? Signed domain? Secure connection? Security options?" with a link "about the test >". Input field: "Your domain name: www.example.nl". Button: "Start test".
- Test your email** (with an envelope icon): "Modern address? Signed domain? Anti-phishing? Secure connection?" with a link "about the test >". Input field: "Your email address: @ example.nl". Button: "Start test".
- Test your connection** (with a signal icon): "Modern addresses reachable? Domain signatures validated?" with a link "about the test >". Button: "Start test".

SSL Server Test

<https://www.ssllabs.com/sslltest/>

ssllabs.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Do not show the results on the boards

Recently Seen Recent Best Recent Worst

SSL Configuration Generator

<https://ssl-config.mozilla.org/>

The screenshot shows the Mozilla SSL Configuration Generator web application. The browser address bar displays 'ssl-config.mozilla.org'. The page features the Mozilla logo and the title 'SSL Configuration Generator'. The interface is divided into three main sections: 'Server Software', 'Mozilla Configuration', and 'Environment'. The 'Server Software' section lists various server options, with 'Apache' selected. The 'Mozilla Configuration' section offers three levels of configuration: 'Modern', 'Intermediate' (selected), and 'Old'. The 'Environment' section shows 'Server Version' as 2.4.41 and 'OpenSSL Version' as 1.1.1d. The 'Miscellaneous' section has two checked options: 'HTTP Strict Transport Security' and 'OCSP Stapling'.

moz://a

SSL Configuration Generator

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Go
- HAProxy
- Jetty
- lighttpd

- MySQL
- nginx
- Oracle HTTP
- Postfix
- PostgreSQL
- ProFTPD
- Redis
- Tomcat
- Traefik

Mozilla Configuration

- Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version	2.4.41
OpenSSL Version	1.1.1d

Miscellaneous

- HTTP Strict Transport Security
This also redirects to HTTPS, if possible
- OCSP Stapling

Padrões	Referências
Tokens em <i>hardware</i> (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em <i>software</i> (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	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

Outras Referências de Interesse para Uma Internet Melhor

cert.br nic.br egi.br

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, Abranet, Abrint, Conexis, InternetSul, RedeTelesul e TelComp

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



Conscientização: Portal InternetSegura.br



The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main content area features a large heading: `Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!`. Below this heading are six categories, each with an illustration and a label: `para Crianças` (two children), `para Adolescentes` (two young adults), `para Pais e Educadores` (a woman and a man), `para 60+` (an elderly couple), `para Técnicos` (a technician with a server rack), and `para Interesse Geral` (a diverse group of people).

Materiais sob Licença Creative Commons: Seja Parceiro de Divulgação ou de Impressão

Segurança na INTERNET

Faça sua parte e todos teremos uma Internet mais segura!

Já há muito tempo que segurança na Internet não é um assunto somente de interesse de um público especializado. Com a iniciativa InternetSegura.br, o NIC.br produz e disponibiliza gratuitamente uma série de materiais, em diversos formatos, que orientam diferentes públicos sobre o uso seguro da Internet.

www.internetsegura.br

Catálogo de materiais e iniciativas do NIC.br

Formato impresso, colorido e permite inclusão de logo de parceiros de impressão

para Crianças

Guia Internet Segura

Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios cifrados, dicas, complete a frase, caça-palavras, entre outros.



Desafios

Contém tanto os desafios do guia Internet Segura como materiais adicionais, atualizados periodicamente. internetsegura.br/desafios



para Adolescentes

Encarte #FikDik

Encarte do guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet, que apresenta os principais cuidados, riscos e consequências do uso inadequado da Internet de forma resumida.



para Pais e Educadores

Guia Internet Segura para seus filhos

Informações para pais e responsáveis sobre como proteger os filhos, seja zelando pela privacidade das crianças, ou utilizando tecnologias de controle parental.



Guia #Internet com Responsa - Cuidados e responsabilidades no uso da Internet

Orienta pais, responsáveis e educadores de adolescentes em temas sensíveis, como exposição excessiva na Internet, liberdade de expressão e dança à imagem e reputação, cyberbullying, danos e riscos da prática de rede, selfie, entre outros. Acompanha o encarte #FikDik



Guia #Internet com Responsa na sua Sala de Aula

Explica os desafios do uso da Internet a partir da exposição excessiva, dos direitos e possíveis danos à imagem dos professores e alunos, e dos limites da liberdade de expressão.



Slides: Fascículos da Cartilha de Segurança para Internet

Slides para a divulgação de boas práticas sobre o uso seguro da Internet. Há versões de apoio para professores, com notas explicativas. Disponíveis em formatos PowerPoint (.ppt), Libre-Office (.odp), PDF sem notas explicativas e PDF com notas explicativas. cartilha.cert.br/downloads



VEJA TAMBÉM

Curso de Formação de Professores Multiplicadores para o Uso Consciente e Responsável da Internet: cursointernetcomresponsa.nic.br

Materiais de referência:

TIC Kids Online Brasil
Indicadores com mapeamento de possíveis riscos e oportunidades on-line a partir dos usos que crianças e adolescentes de 9 a 17 anos fazem da Internet. Contém dados distintos para "crianças e adolescentes" e "pais e responsáveis". cetic.br/pesquisa/kids-online

TIC Educação
A pesquisa entrista alunos, professores, coordenadores pedagógicos e diretores para mapear o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) em escolas públicas e privadas de educação básica. cetic.br/pesquisa/educacao

Para quem tem 60 anos ou mais

#Internet com Responsa 60+: Cuidados e responsabilidades no uso da Internet

Apresenta cuidados específicos para essa faixa etária, pois esse ambiente repleto de informações e oportunidades também oferece alguns riscos para quem ingressou no uso das novas tecnologias recentemente.



para Técnicos

Portal BCP e Programa Por uma Internet Mais Segura

Reúne um conjunto de boas práticas operacionais para Sistemas Autônomos (ASs) conectados à Internet. São destacadas algumas práticas que, embora extremamente importantes, ainda não são adotadas amplamente pelos ASs brasileiros. O portal também disponibiliza conteúdos e iniciativas direcionadas à comunidade de operadores de redes e serviços que formam a Internet por meio do Programa por uma Internet Mais Segura. bcp.nic.br



VEJA TAMBÉM

Curso de Boas Práticas Operacionais para Sistemas Autônomos - Presencial: bcp.nic.br/course-bcoop

Curso "Fundamentals of Incident Handling": cert.br/cursos/fih/

Curso "Advanced Topics in Incident Handling": cert.br/cursos/attih/

Interesse geral

Cartilha de Segurança para Internet

Documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários. Também disponível em cartilha.cert.br e em espanhol em cartilha.cert.br



Fascículos da Cartilha de Segurança para Internet

Aborda tópicos específicos contidos na Cartilha de Segurança para Internet e complementa conteúdos que não estavam disponíveis à época da última edição da Cartilha, como Boatos, cuidados atualizados para Redes Sociais e Códigos Maliciosos. Também disponíveis em cartilha.cert.br/fasciculos e em espanhol em cartilha.cert.br/fasciculos.



Guia #Internet com Responsa Vai às Compras

Detalha os cuidados necessários para realizar compras na Internet de forma responsável, além de enfatizar a importância de exercer direitos previstos no Código de Defesa do Consumidor.



Portal Antispam.br

Fonte de referência imparcial e embasada tecnicamente sobre o spam. Contém desde informações para administradores de redes e usuários finais, incluindo vídeos que abordam de forma simples e divertida os perigos aos quais os usuários estão expostos, explicam o que é spam e dão dicas de como navegar com mais segurança na rede. antispam.br



VEJA TAMBÉM

Materiais de referência:

Caderno CGLbr "Combate ao spam na Internet no Brasil"

Histórico e reflexões sobre o combate ao spam e a gestão da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil. cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil

DISTRIBUIÇÃO DOS MATERIAIS

O NIC.br tem o compromisso de atender todos os interessados em seus materiais, da forma mais racional possível. Para que o máximo de interessados sejam atendidos, sem desperdício, limitamos o envio de materiais a lotes de 100 unidades. Caso sua instituição tenha interesse em distribuir uma quantidade maior, teremos o prazer em disponibilizar o conteúdo para que a impressão, com seu logotipo, seja realizada de acordo com sua capacidade.

SEJA UM PARCEIRO PARA A IMPRESSÃO DOS MATERIAIS!

Escreva para info@nic.br solicitando a inclusão do seu logotipo e especifique quais materiais você gostaria de imprimir.

LICENCIAMENTO

O objetivo primordial da produção dos nossos materiais é o compartilhamento do conteúdo, portanto a maioria deles está disponível gratuitamente para download e uso sob licenças Creative Commons. Sua instituição pode utilizá-los livremente, sem necessidade de autorização prévia, desde que a fonte seja mencionada, o uso do material não seja comercial (venda do material) e que o conteúdo não seja alterado. Para usos específicos fora do escopo da licença, escreva para info@nic.br.

Confira todas as nossas publicações e atividades em nic.br

nic.br cgi.br

<https://internetsegura.br/pdf/catalogo-internetsegura.pdf>

Obrigado

@ cristine@cert.br

@ jessen@cert.br

@ notificações para: cert@cert.br

@ @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br