Boas Práticas e Cooperação na Luta Contra Abusos de Rede

GTER 43
25 de maio de 2017
Foz do Iguaçu, PR

Christian O'Flaherty **Lucimara Desiderá**

Abuso

- Uso da rede de forma maliciosa / sem consentimento:
  - Spam
  - *Phishing*
  - Interceptação de tráfego (*Sniffing*)
  - *Spoofing*
  - Ataques de negação de serviço
  - *Malware*
  - Exploração de vulnerabilidades
  - Invasão
  - Vazamento de dados

Impactos e Desdobramentos

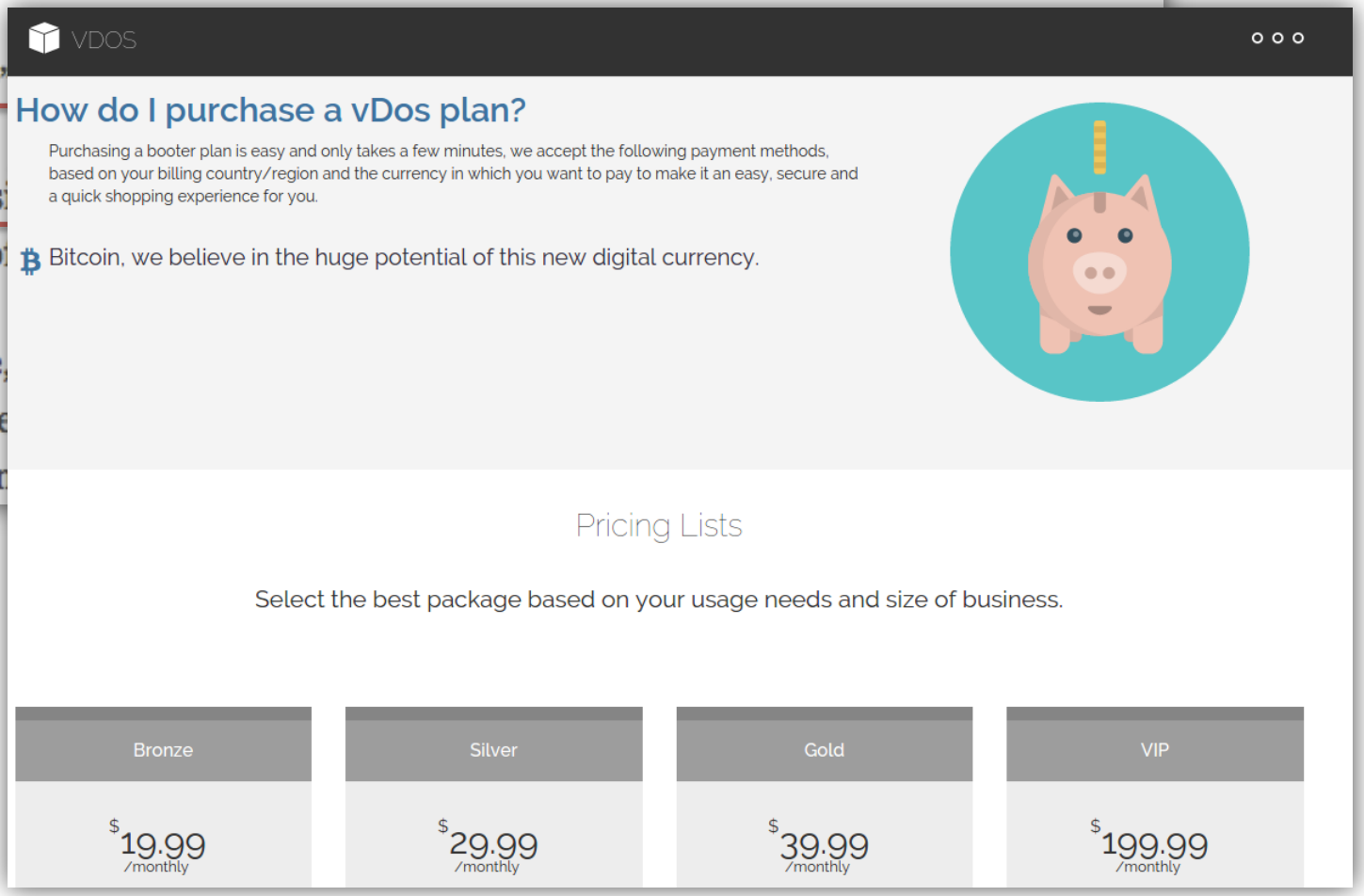
- Impactos operacionais e de negócios
  - danos à imagem
  - perda financeira
  - indisponibilidade de recursos
    - negação de serviço
    - IPs em *blacklist*
  - problemas legais

Abuso = Lucro para Criminosos

08 Israeli Online Attack Service 'vDOS' Earned
SEP 16 **$600,000 in Two Years**

vDOS — a "booter"
helping customers
(DDoS) attacks desi
secrets about tens o

The vDOS database,
young men in Israe
support services cor



https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/

Consequências do Abuso em Rede

620Gbps contra o Blog do Brian Krebs

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

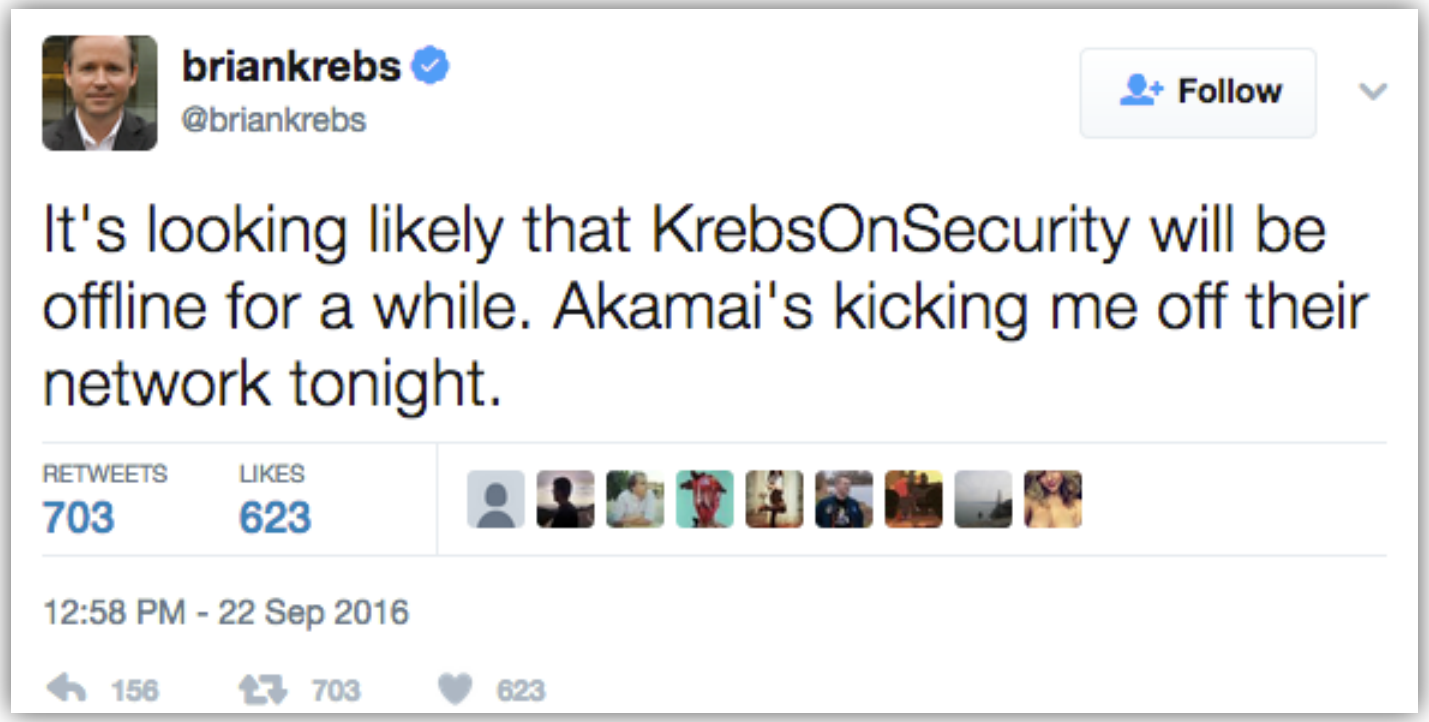
The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

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.

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

Consequências do Abuso em Rede



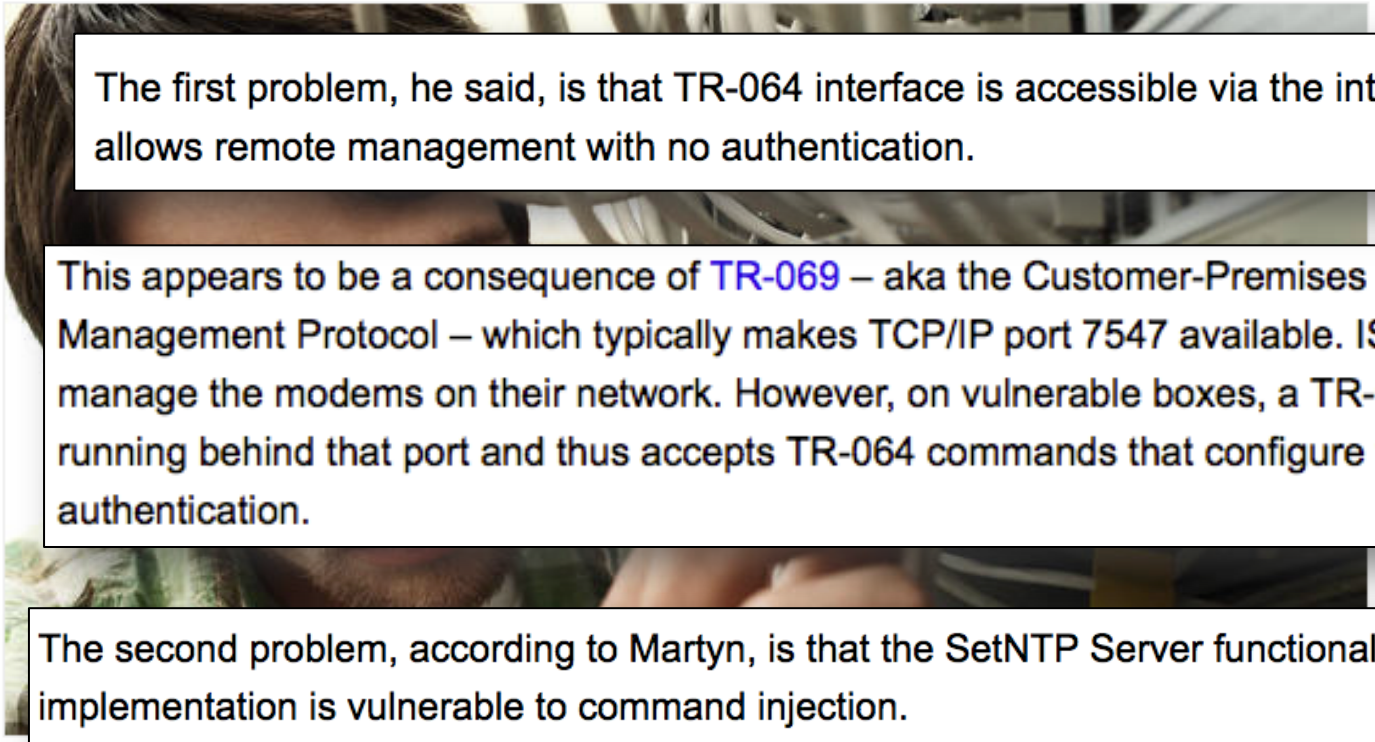
https://twitter.com/briankrebs/status/779111614226239488

In an interview with *The Boston Globe*, Akamai executives said the attack — if sustained — likely would have cost the company millions of dollars. In the hours and days following my site going offline, I spoke with multiple DDoS mitigation firms. One offered to host KrebsOnSecurity for two weeks at no charge, but after that they said the same kind of protection I had under Akamai would cost between $150,000 and $200,000 per year.

https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/

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

Malware waltzes up to admin panels with zero authentication



The first problem, he said, is that TR-064 interface is accessible via the internet-facing WAN port and allows remote management with no 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/

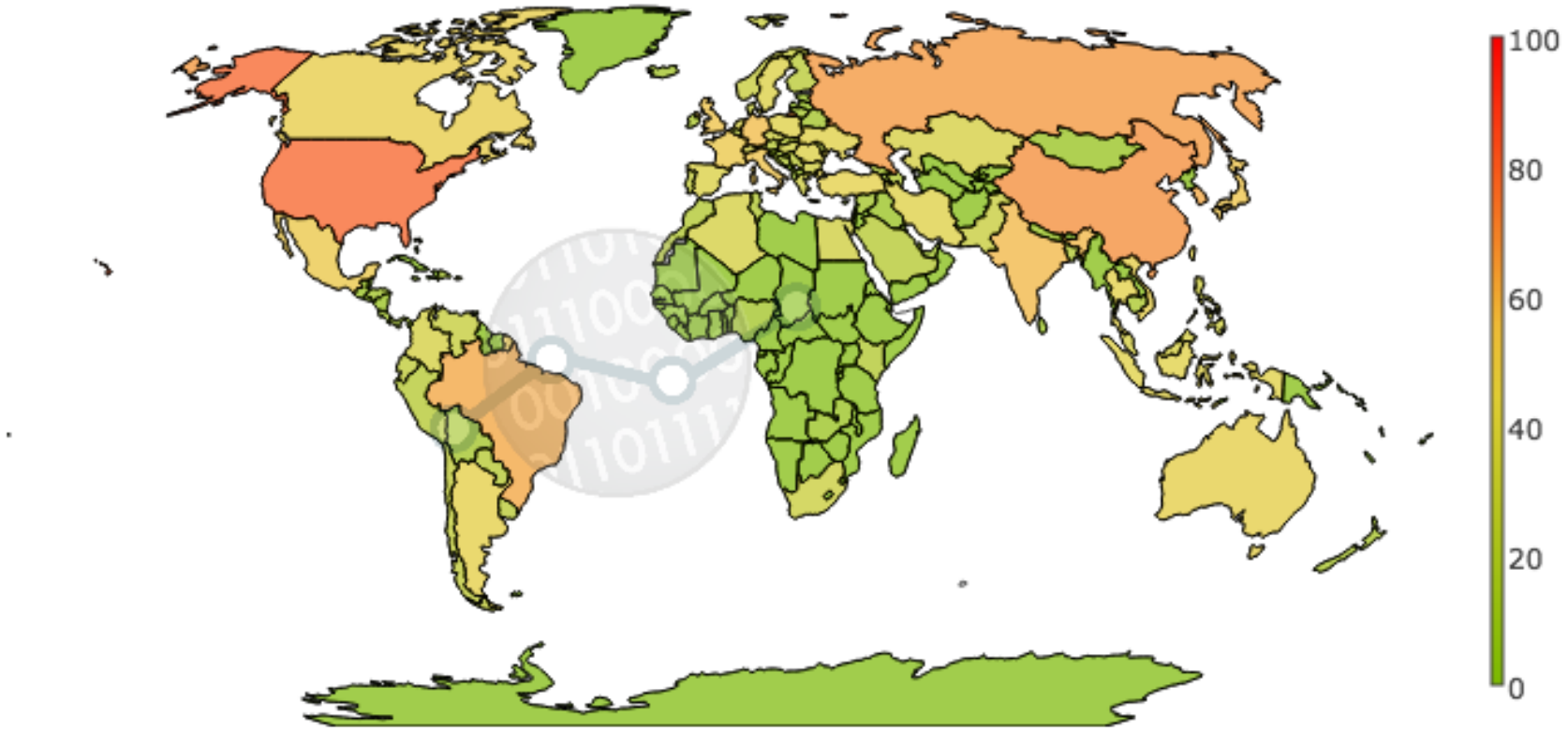
Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

Brad Chacos | *@BradChacos* Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

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

Risco Potencial Imposto à Internet



http://stats.cybergreen.net/

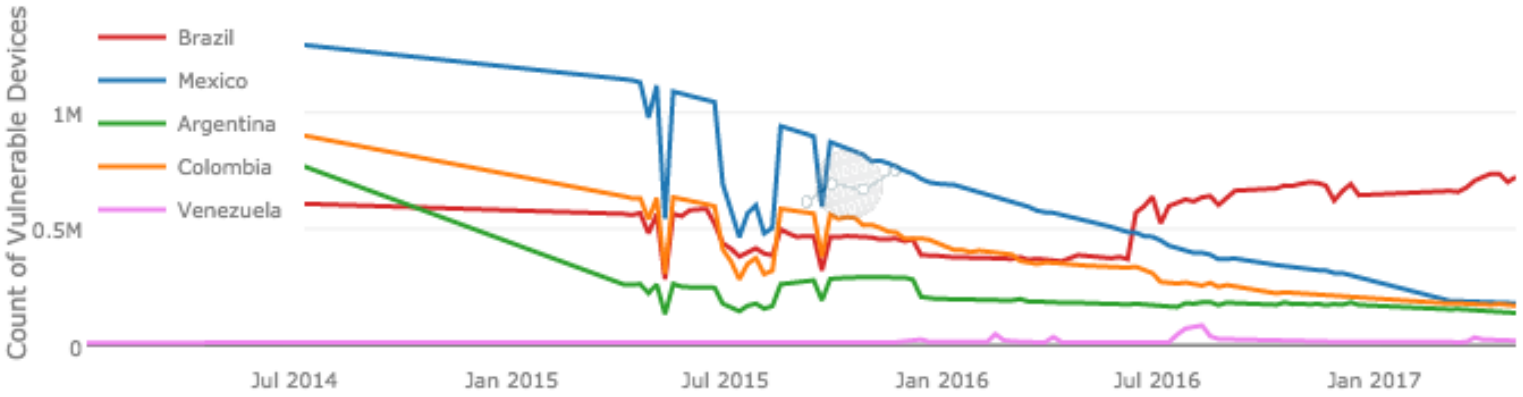
Potencial Ofensivo – em Tbps

Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Mirai	DDOS Potential TBit/sec	DDOS Rank
United States	2,190,873	843,263	502,238	269,564	8,135	571	1
China	1,482,736	281,911	156,783	851,625	82,767	245	2
Russian Federation	441,759	300,671	132,920	480,070	89,994	201	3
Brazil	723,305	190,389	965,167	160,864	59,369	147	4
South Korea	321,309	221,758	279,303	189,540	4,008	144	5
India	979,519	96,387	321,609	115,567	85,398	99	6
Germany	311,630	145,350	42,220	19,984	3,560	95	7
Italy	436,750	96,707	174,792	87,731	5,759	76	8
United Kingdom	246,798	112,296	38,355	14,199	3,287	73	9
Japan	235,820	103,752	74,813	124,836	1,388	72	10

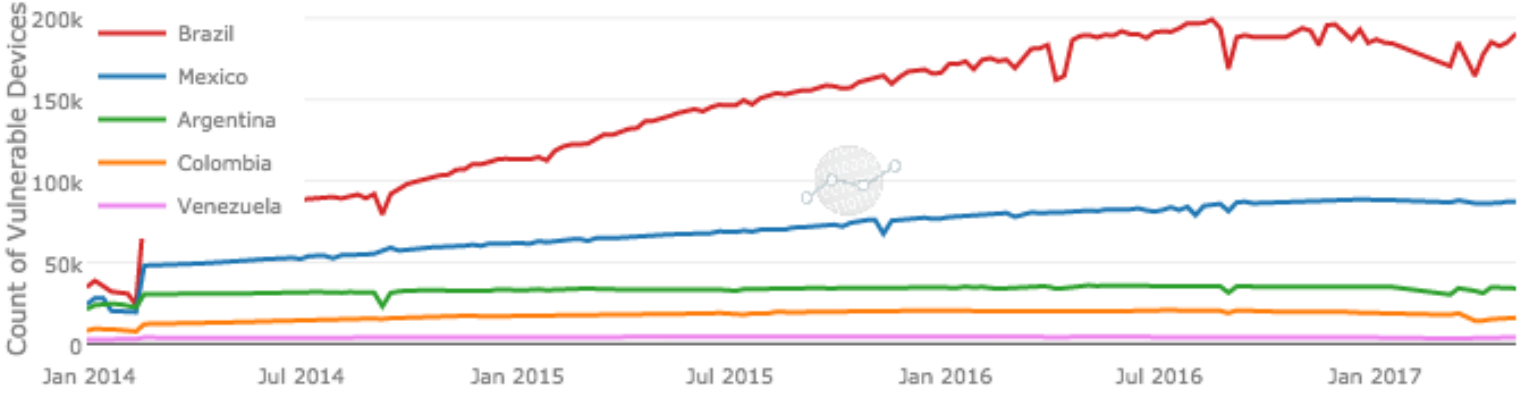
http://stats.cybergreen.net/country

Dispositivos Vulneráveis

OPEN RECURSIVE DNS BRAZIL #4



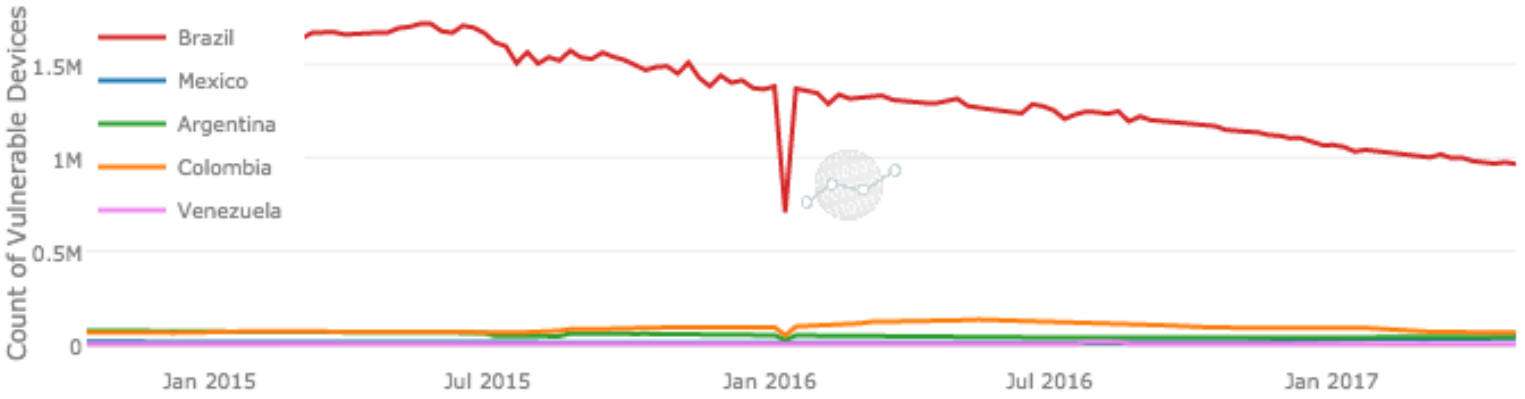
OPEN NTP BRAZIL #5



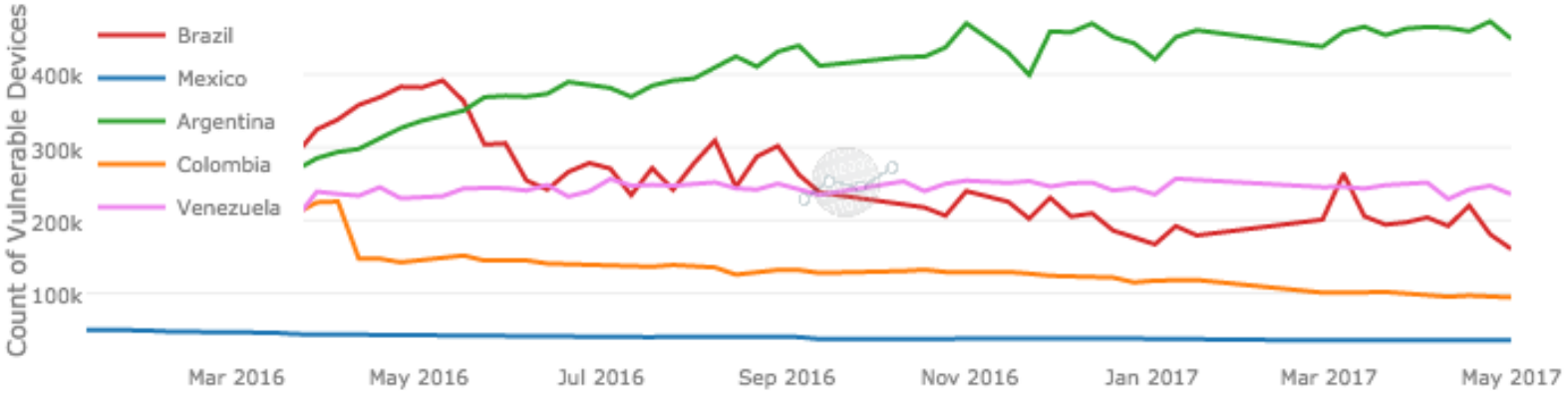
http://stats.cybergreen.net/country/brazil/

Dispositivos Vulneráveis

OPEN SNMP BRAZIL #1

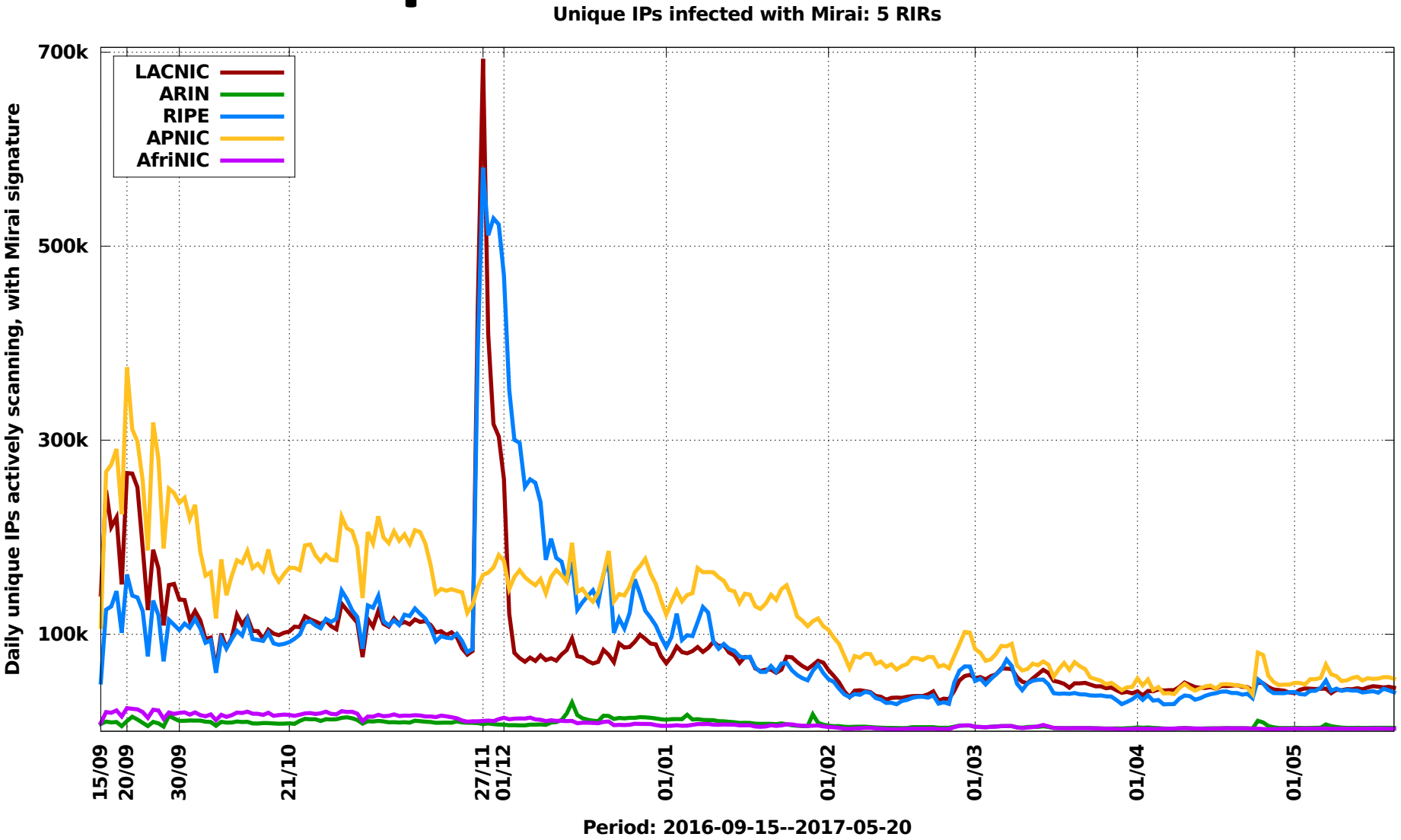


OPEN SSDP BRAZIL #11



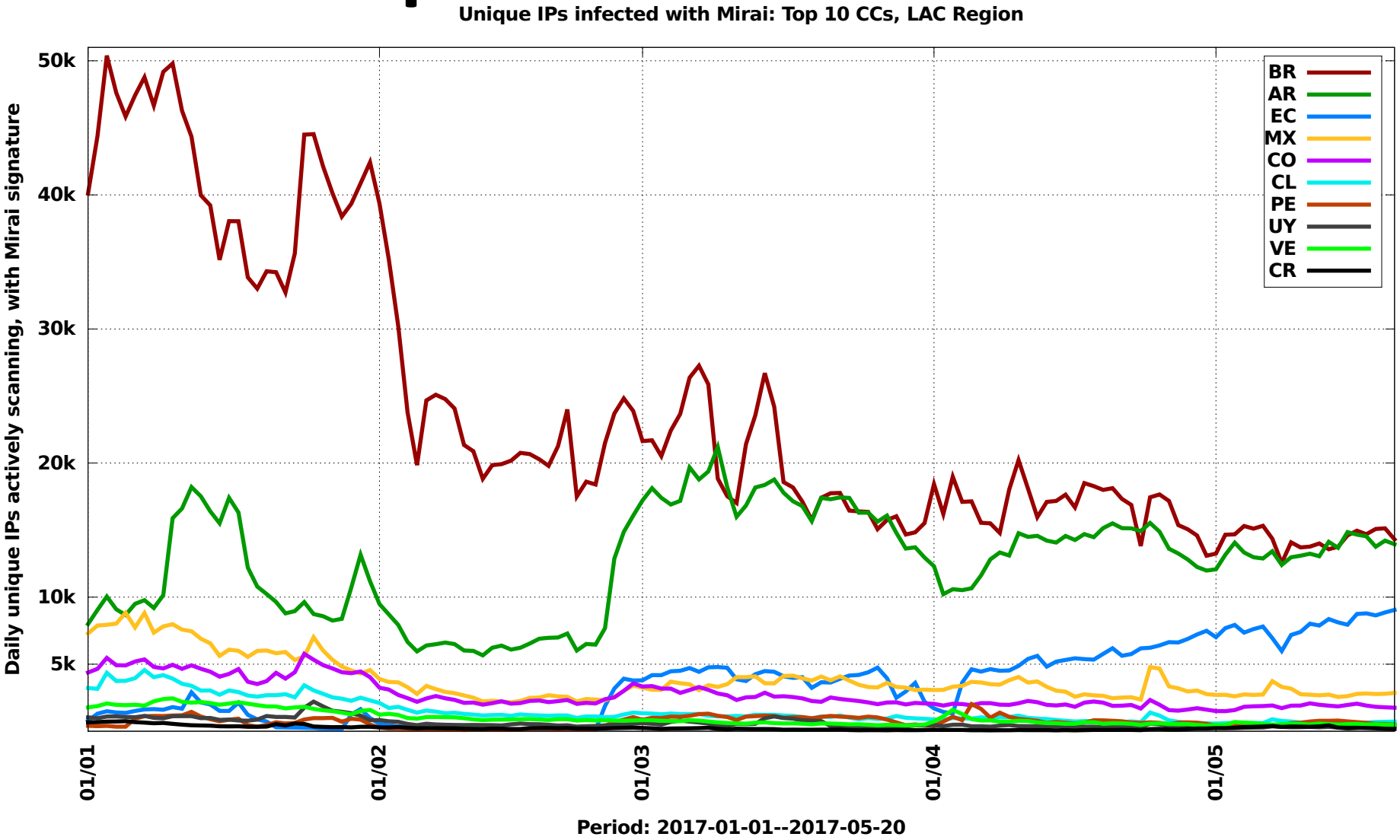
http://stats.cybergreen.net/country/brazil/

Dispositivos Infectados



Fonte: CERT.br

Dispositivos Infectados



Fonte: CERT.br

Podemos Melhorar o Cenário?

LACNIC, the Latin America and Caribbean Network Information Center, and M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, have the support of a new partner: LACNOG, the Latin America and Caribbean Network Operators Group.

On February 8th 2017, LACNOG ratified the charter for the Latin America and Caribbean Anti-Abuse Working Group. LAC-AAWG combines knowledge and expertise from LACNIC, LACNOG, and M3AAWG to develop a self-sustaining anti-abuse community in the LAC region.

LAC-AAWG will serve as a convening forum for network operators and anti-abuse experts. LAC-AAWG's mission is to foster dialog among existing communities and working groups, fomenting the development of anti-abuse recommendations and best current operational practices (BCOPs) that address region-specific and global issues. LAC-AAWG will also act as the voice of the LAC region in the global anti-abuse community, further cementing the exchange of anti-abuse ideas, knowledge, and best practices between the LAC region and M3AAWG's global community.

LAC-AAWG will also coordinate regional anti-abuse awareness activities like presentations and tutorials targeting Latin America and Caribbean relevant communities. These engagements aim to educate the LAC operator community on, and foster adoption of, regional and global anti-abuse best practices and operations.

The founding co-chairs of LAC-AAWG are Christian O'Flaherty from ISOC and Lucimara Desiderá from CERT.br/NIC.br. The first face-to-face LAC-AAWG community meetings will take place during LACNIC 27, in Foz do Iguaçu, Brazil, on May 22-26, 2017. In partnership with M3AAWG, these activities will comprise presentations, BOFs, and tutorials on anti-abuse best practices.

www.lacnic.net/en/web/anuncios/2017-amenazas-en-linea-se-fortalece

LAC-AAWG

- Desenvolver uma comunidade anti-abuso na região LAC;
- Servir como um fórum para operadores de redes e especialistas em anti-abuso;
  - promover o diálogo entre comunidades e grupos de trabalho existentes
- Fomentar o desenvolvimento de recomendações anti-abuso e melhores práticas operacionais (BCOPs)
  - abordar questões específicas da região e globais.
  - participar e contribuir para a comunidade global
- Coordenar atividades de conscientização contra o abusos
  - Incentivar a adoção de melhores práticas e operações anti-abuso

Como Participar

- Lista **BCOP** bcop@lacnog.org
  - lista aberta do Grupo de Trabalho BCOP do LACNOG, destinada a discussão de melhores práticas operacionais para serviços de redes;
- Lista **LACNOG** lacnog@lacnog.org
  - lista aberta para a discussão de questões do funcionamento e operações de redes em geral, não se limitando a segurança;
- Lista **LAC-SEC** seguridad@lacnic.net
  - lista aberta dedicada a discussão de questões de segurança em um contexto amplo, não limitando a resposta e mitigação de incidentes de segurança;
- Lista **LAC-CSIRTs** lac-csirts@lacnic.net
  - lista fechada, destinada a assuntos relacionados ao tratamento de incidentes de segurança. Participação institucional, restrita a membros de times de resposta a incidentes de segurança (CSIRT).

Como Contribuir?

- participar das listas de discussão
- ajudar no desenvolvimento de boas práticas/ BCOPs
  - sugerir temas
  - desenvolver conteúdo técnico
  - traduzir BCPs/BCOPs existentes
  - ser editor/revisor de um documentos

Como Contribuir?

- ajudar na conscientização acerca de boas práticas existentes
  - produzir / promover conteúdo relacionado a boas práticas
    - *newsletter*, *whitepaper*, *blogpost*, palestra, webinar, etc...
  - fomentar a adoção

BCOPs em Desenvolvimento

- BCOPs
  - BGP Implementation
  - **Mitigation of attacks directed to CPE devices**
  - First steps on IPv6 implementations
  - *Remote Triggered BlackHole routes* (RTBH)
  - Spanish translation of the documentRIPE-631: IPv6 Troubleshooting for Residential ISP Helpdesks.

Documentos

- M^{3}AAWG tem atualmente 42 artigos disponíveis
  (For the Industry -> Best Practices)

  https://www.m3aawg.org/published-documents

- Essas melhores práticas e tutoriais abordam tanto os desafios emergentes como os atuais de combate ao abuso, como métodos para combater o monitoramento indiscriminado, os processos para abuse desk, as técnicas anti-phishing e antispam, as melhores práticas para remetentes de e-mail e outros tópicos relevantes.

Algumas BCPs de M³AAWG

- M³AAWG Introduction to Reflective DDoS Attacks
- M³AAWG Initial Recommendations: Arming Businesses Against DDoS Attacks
- M³AAWG Multifactor Authentication Recommendations
- M³AAWG Password Recommendations for Providers
- Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction (December 01, 2005)

Obrigada!

Perguntas?
Voluntários?!!?

lucimara@cert.br
oflaherty@isoc.org