

LIVE
INTRAREDE
2022

ATAQUES DE NEGAÇÃO DE SERVIÇO (DoS E DDoS): O QUE FAZER?

16/11 às 10h (UTC-3)
intrarede.nic.br

REALIZAÇÃO
ceptro.br nic.br cgi.br

 solintel

 VLSM

 MOGA

 TARS

 OPA!

 conectados
coworking

 telefonarnet

Profº. Lacier Dias

- ✓ Mestrando em Administração - FDC
- ✓ MBA em Gerenciamento de Projetos – FGV
- ✓ Pós-Graduado em Segurança de Rede de Computadores - UNIC
- ✓ Sócio e Diretor na Solintel, MOGA, OPA, TARS e VLSM, coordenando as áreas de Tecnologia e Ciência de Dados, auxiliando na concepção de projetos, produção e aprimoramento dos produtos da organização, com foco em projetar soluções completas para os clientes com base em produtos da organização ou projetando soluções sob medida a partir de projetos especiais.
- ✓ Com 20 anos de experiência no setor de telecom e como Professor de arquitetura, design e roteamento para redes, consultor para provedores de internet e palestrante em eventos do setor e workshops nacionais e internacionais.



SITES DE ATAQUE GRATUITO

The screenshot shows the homepage of a website titled "Free Stresser". The background is dark blue with a network diagram and binary code. The navigation menu at the top includes "Free Stresser", "Home", "Best Paid Booter List", "About", "Terms of Service", and "Telegram Channel". The main heading is "Free Stresser" in large white text. Below it, a sub-heading reads "1Gbps Spoofed UDP floods, No Accounts, No Logs, No Price." and a link to a Telegram channel is provided: "Receive Updates At Telegram Channel: <https://t.me/freestresser>". The form contains four input fields: "IP Address", "Port", "Seconds", and "Enter Captcha" (with the value "31685" entered). A large blue button labeled "Launch Stress Test" is positioned below the form. At the bottom, status information is displayed: "All tests delete in exactly 0 days, 18 hrs, 55 mins", "Your Tests Today: 0/15 | Global Tests Today: 779 | Global Running Tests: 6/15 | Users Online: 213", and a link to a tutorial: "How to boot IPs offline? [See this tutorial](#)".

Free Stresser

Home Best Paid Booter List About Terms of Service Telegram Channel

Free Stresser

1Gbps Spoofed UDP floods, No Accounts, No Logs, No Price.

Receive Updates At Telegram Channel: <https://t.me/freestresser>

IP Address Port Seconds Enter Captcha 31685

Launch Stress Test

All tests delete in exactly 0 days, 18 hrs, 55 mins

Your Tests Today: 0/15 | Global Tests Today: 779 | Global Running Tests: 6/15 | Users Online: 213

How to boot IPs offline? [See this tutorial](#)

Shodan



SHODAN

[Explore](#)

[Downloads](#)

[Pricing](#)

|country:BR



TOTAL RESULTS

11,260,614

[View Report](#)

[Browse Images](#)

[View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TOP CITIES

São Paulo	2,720,624
Rio de Janeiro	704,788
Campinas	296,640
Fortaleza	249,427
Belo Horizonte	185,731

[More...](#)

TOP PORTS

7547	2,010,886
161	1,364,262
80	1,272,437
443	1,011,319

168.196.117.208

Globo Comunicação e Participações SA

Brazil, Rio de Janeiro

BGP:

Message #1:

Type: OPEN

Length: 29

Version: 4

Hold Time: 90

ASN: 64604

BGP Identifier: 10.126.3.84

Message #2:

Type: NOTIFICATION

Length: 21

Error Code: Cease

Error Subcode: Connection Rejected

Copagril

179.188.11.47

copagril.com.br

hm8912.locaweb.com.br

[Locaweb Serviços de](#)

SSL Certificate

Issued By:

|- Common Name:

HTTP/1.1 200 OK

Date: Mon, 14 Nov 2022 20:07:05 GMT

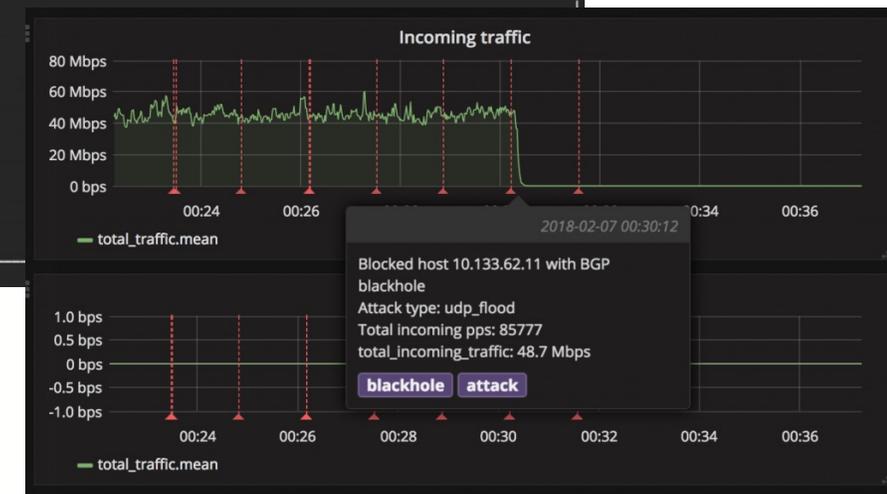
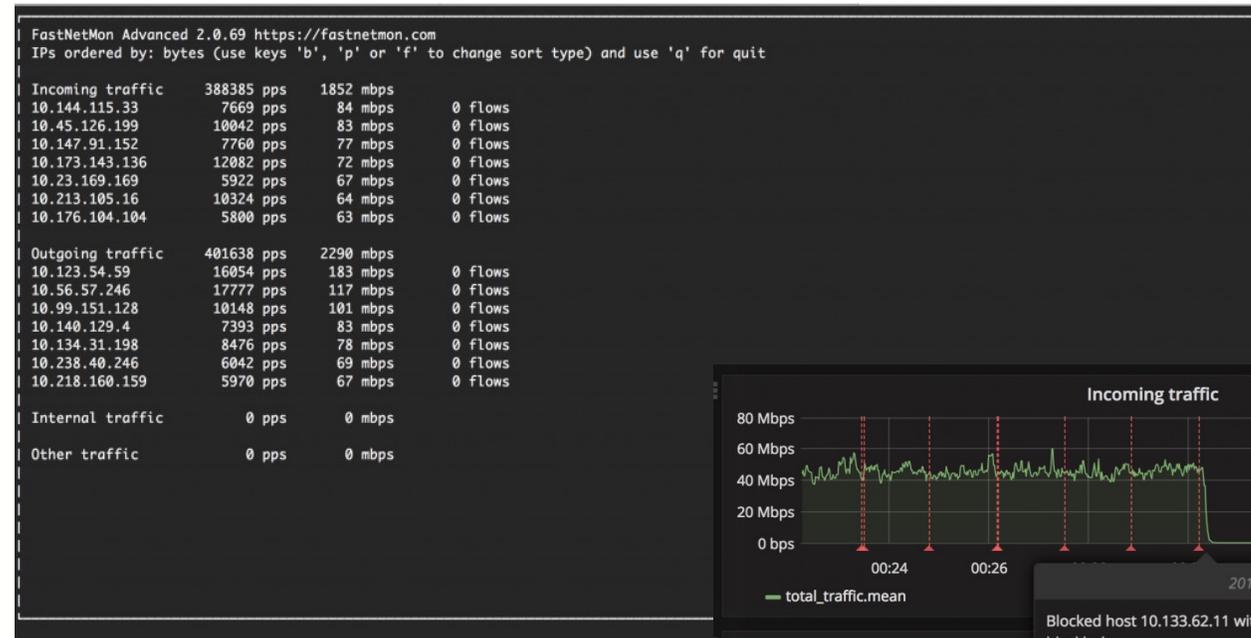
Server: Apache



FASTNETMON

O fastnetmon é comumente utilizado para identificar anomalias de tráfego e automatizar o processo de blackhole a partir de coletas de netflow, é possível definir alguns parâmetros de análise como:

- Número de pps;
- mbps;
- Flow/s;
- Pacotes TCP por segundo;
- Pacotes UDP por segundo;
- Pacotes ICMP por segundo;
- Pacotes TCP SYN por segundo;
- TCP mbps;
- TCP SYN mbps;
- UDP mbps;
- ICMP mbps.



SPAMHAUS

A Spamhaus possui diversas ferramentas baseadas em listas de nomes de domínios e IP's com má reputação. Essas reputações de domínio são calculadas a partir de muitos fatores e mantidas em um banco de dados que, por sua vez, alimenta as ferramentas

SPAMHAUS THE SPAMHAUS PROJECT

SBL XBL PBL DBL DROP ROKSO

Blocklist Removal Center About Spamhaus | Contacts | Official Statements | FAQs | News Blog

Protect your users properly today with Spamhaus ZEN+DBL+RPZ

With a 20 year history, vast internet data traffic visibility and protecting over 3 Billion users, Spamhaus is the industry leader in realtime actionable highly accurate threat intelligence

Blocklists
Safe DNSBLs for Safe Filters

Blocklist Removal
Blocked? To check, get info and resolve listings go to
▶ Blocklist Removal Center

Documents
▶ Email Marketing Guide
▶ The Definition of "Spam"
▶ Consumer Protection

ROKSO
▶ Register of Known Spam Operations
▶ ROKSO Policy & FAQs

Spamhaus News
Poor sending practices trigger a tidal wave of informational listings
The recent spate of informational listings from our researchers has highlighted some pretty poor sending practices.... (>)

SBL Advisory

XBL Advisory

PBL Advisory

DBL Advisory

ZEN

Blocklist Use
▶ DNSBL Usage Terms
▶ How Blocklists Work

Datafeed
▶ Datafeed service for ISPs and commercial users

ISP Area
▶ ISP Area
▶ ISP Abuse Desk FAQs

Spamhaus Datafeed 30-day Free Trial
▶ more info

TOP 10 World's Worst Spam Problem Networks
▶ charts



NMAP/Zenmap

Outra ferramenta normalmente presente no kit de especialistas da área é o nmap.

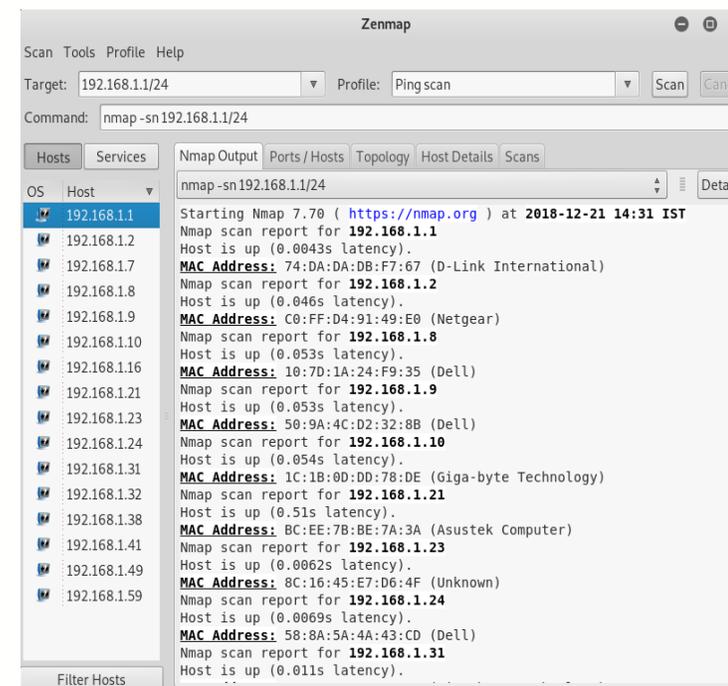


```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.38 cpe:/o:linux:linux_kernel:3 cpe:/o:netgear:raidiorator:4 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.38 (94%), Linux 3.0 (92%), Linux 2.6.32 - 3.0 (91%), Linux 2.6.18 (91%), Linux 2.6.39 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.38 - 3.0 (90%), Linux 2.6.38 - 2.6.39 (89%), Linux 2.6.35 (88%), Linux 2.6.37 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1 14.21 ms  151.217.192.1
2 5.27 ms   ae10-0.mx240-iphh.shitty.network (94.45.224.129)
3 13.16 ms  hmb-s2-rou-1102.DE.eurorings.net (134.222.120.121)
4 6.83 ms   blnb-s1-rou-1041.DE.eurorings.net (134.222.229.78)
5 8.30 ms   blnb-s3-rou-1041.DE.eurorings.net (134.222.229.82)
6 9.42 ms   as6939.bcix.de (193.178.185.34)
7 24.56 ms  10ge10-6.core1.ams1.he.net (184.105.213.229)
8 30.60 ms  100ge9-1.core1.lon2.he.net (72.52.92.213)
9 93.54 ms  100ge1-1.core1.nyc4.he.net (72.52.92.166)
10 181.14 ms 10ge9-6.core1.sjc2.he.net (184.105.213.173)
11 169.54 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
12 164.58 ms router4-fmt.linode.com (64.71.132.138)
13 164.32 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```



GVM (OpenVas)

- OpenVAS (Open Vulnerability Assessment System), em português Sistema Aberto de Avaliação de Vulnerabilidade, é um framework de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

Pontos de destaque

- Usa o Greenbone Community Feed para executar mais de 50.000 testes de vulnerabilidade;
- Código aberto;
- Desenvolvido e mantido gratuitamente pela Greenbone Networks;
- Suporta mais de 44.000 CVEs.



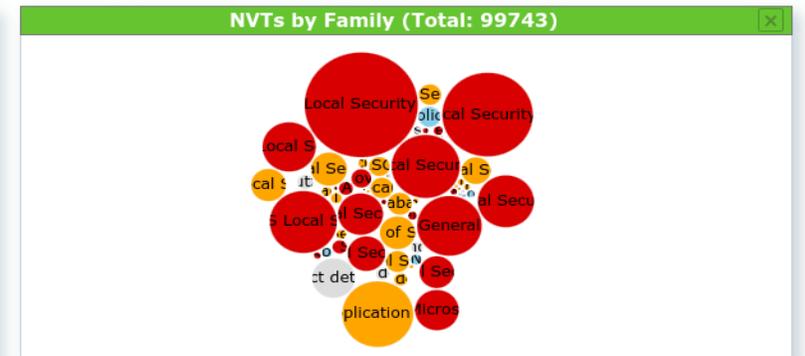
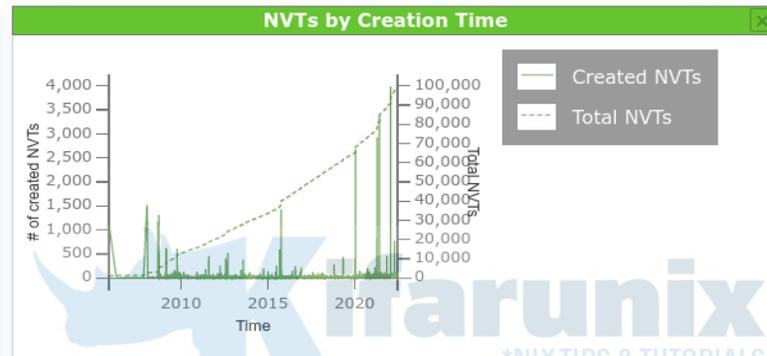
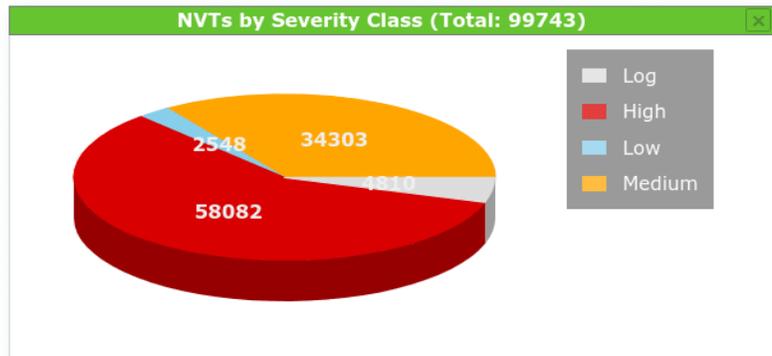
GVM (OpenVas)



Filter



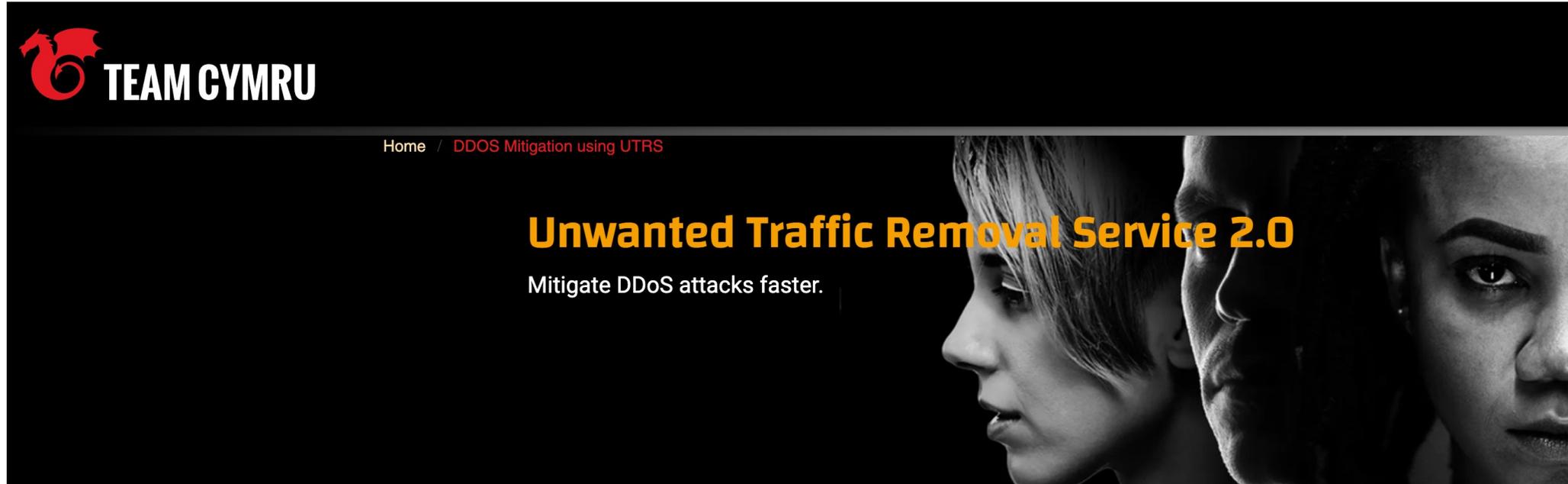
NVTs 99743 of 99743



1 - 10 of 99743

Name	Family	Created	Modified	CVE	Severity	QoD
Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2566) - Windows	Web application abuses	Fri, Jun 24, 2022 6:58 AM UTC	Fri, Jun 24, 2022 6:58 AM UTC	CVE-2022-34174	5.0 (Medium)	80 %
Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2566) - Linux	Web application abuses	Fri, Jun 24, 2022 6:51 AM UTC	Fri, Jun 24, 2022 6:56 AM UTC	CVE-2022-34174	5.0 (Medium)	30 %
Jenkins 2.335 < 2.356 Information Disclosure Vulnerability (SECURITY-2777) - Windows	Web application abuses	Fri, Jun 24, 2022 6:48 AM UTC	Fri, Jun 24, 2022 6:49 AM UTC	CVE-2022-34175	4.0 (Medium)	80 %
Jenkins 2.335 < 2.356 Information Disclosure Vulnerability (SECURITY-2777) - Linux	Web application abuses	Fri, Jun 24, 2022 6:41 AM UTC	Fri, Jun 24, 2022 6:47 AM UTC	CVE-2022-34175	4.0 (Medium)	30 %
Jenkins 2.340 < 2.356 Multiple Vulnerabilities (SECURITY-2776, SECURITY-2780) - Windows	Web application abuses	Fri, Jun 24, 2022 6:39 AM UTC	Fri, Jun 24, 2022 6:40 AM UTC	CVE-2022-34172 CVE-2022-34173	4.9 (Medium)	80 %
Jenkins 2.340 < 2.356 Multiple Vulnerabilities (SECURITY-2776, SECURITY-2780) - Linux	Web application abuses	Fri, Jun 24, 2022 6:01 AM UTC	Fri, Jun 24, 2022 6:37 AM UTC	CVE-2022-34172 CVE-2022-34173	4.9 (Medium)	30 %
Jenkins 2.321 < 2.356, 2.332.1 LTS < 2.332.4 LTS XSS Vulnerability (SECURITY-2761) - Windows	Web application abuses	Fri, Jun 24, 2022 5:52 AM UTC	Fri, Jun 24, 2022 5:53 AM UTC	CVE-2022-34171	4.9 (Medium)	80 %

UTRS - Unwanted Traffic Removal Service



UTRS 2.0, é um serviço baseado em BGP que é uma ferramenta para ajudar a mitigar ataques DDoS, exclusivamente para proprietários de ASN globalmente exclusivo, o UTRS 2.0 adiciona suporte para FlowSpec, IPv6, aumenta os tamanhos de anúncio de IPv4 e IPv6, confiabilidade aprimorada com sessões de emparelhamento redundantes e ROA's são honrados.

Reduza os ataques DDoS como uma comunidade:

O UTRS v2.0 usa técnicas como buracos negros acionados remotamente (RTBH), mas globalmente. Juntos, permitimos que você se proteja enquanto ajudamos a proteger a Internet.

Você ajuda seu próximo e ele te ajuda.



RadAr Qrator

AS



7909th place in IPv4 connectivity rating

Last month: 0 positions

2160th place in IPv6 connectivity rating

Last month: 0 positions

Overview >

Graph >

Whois >

IPv4 Connectivity ▾

Providers	5
Customers	18
Peerings	3
Unspecified	0
Prefixes	24

IPv6 Connectivity ▾

Providers	4
Customers	15
Peerings	1
Unspecified	0
Prefixes	15

Security Issues ▾

Route Leaks	583
Hijacks	0
Bogons	2
Routing Loops	77
Vulnerable Ports	19
DDoS amplifiers	2

Overview

IPv4 Connectivity Rate



IPv6 Connectivity Rate



Security Issues



Krill (RPKI)

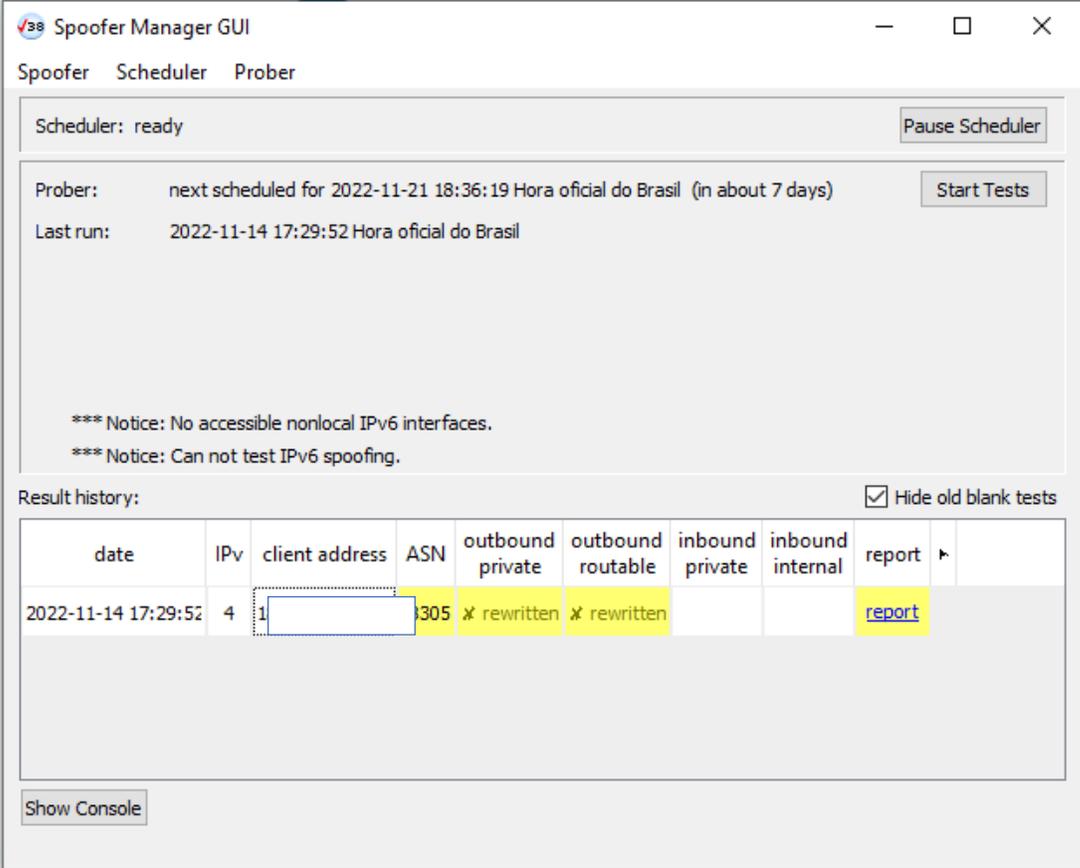
- O Krill é utilizado para gerenciar e manter as ROAs (Routing origin authorization) publicadas de forma correta, auxiliando no processo de validação de origem dos blocos IP.

The screenshot shows the Krill web interface. At the top, there is a red header with the Krill logo, a language dropdown set to 'English', and user profile icons. Below the header, there are input fields for 'Certificate Authority' and 'Current Certificate Authority'. The main content area has tabs for 'ROAs', 'Parents', and 'Repository'. A search bar is present with the text 'Search for ASN, prefix, state...'. To the right of the search bar is a 'Download CSV' button. Below the search bar, there are three columns: 'ASN', 'Prefix', and 'State'. The 'State' column contains four rows, each with a green 'SEEN' label and a '1' in a box, followed by a red trash icon. At the bottom left, there is an 'Add ROA' button. At the bottom right, there is a pagination control showing '25/page' and a red '1' in a box, followed by a red 'Analyse my ROAs' button. On the right side of the interface, there is a form with three rows labeled 'asn', 'v4', and 'v6', each with an input field.



Spoofers Caida

- O Spoofer é utilizado para validação da correta aplicação da política de anti-spoofing.



Spoofers Manager GUI

Spoofers Scheduler Probers

Scheduler: ready Pause Scheduler

Prober: next scheduled for 2022-11-21 18:36:19 Hora oficial do Brasil (in about 7 days) Start Tests

Last run: 2022-11-14 17:29:52 Hora oficial do Brasil

*** Notice: No accessible nonlocal IPv6 interfaces.
*** Notice: Can not test IPv6 spoofing.

Result history: Hide old blank tests

date	IPv	client address	ASN	outbound private	outbound routable	inbound private	inbound internal	report
2022-11-14 17:29:52	4	1 [redacted]	305	✗ rewritten	✗ rewritten			report

Show Console



WalledGarden.Global

O Walled Garden coloca no seu roteador de BGP milhares de rotas de lixo IPv4 e IPv6, central de controle, vírus, route leaks, bots usados para DDOS, phishing dentre outros.

Um ferramenta eficaz para ajudar a prevenir e mitigar ataques DDoS.



The screenshot shows the Walled Garden website interface. At the top left is the logo 'WG WALLED GARDEN'. To its right are navigation links: 'SOBRE', 'A SOLUÇÃO', 'COMO FUNCIONA', 'CONTATO', and 'PT EN ES'. Further right are input fields for 'E-Mail' and 'Nome', followed by 'Cadastrar' and 'ENTRAR' buttons. The main content area features a dark background with a city map. On the left, it displays statistics: '33 ATAQUES POR SEGUNDO', '117.572 POR HORA', and '84.652.096 POR MÊS'. Below these, it states: 'Estes ataques foram registrados na América Latina durante os últimos 6 meses. Proteja sua rede e seus clientes. Cadastre-se.' In the center, there is a dark box titled 'CONSULTE SEU NÍVEL DE SEGURANÇA' containing a 'Digite seu ASN' input field, an 'Ok' button, and labels for 'INSTITUIÇÃO:' and 'NÍVEL DE SEGURANÇA:'.



WalledGarden.Global



Pedir proteção

Ajuda



Selecione o seu AS

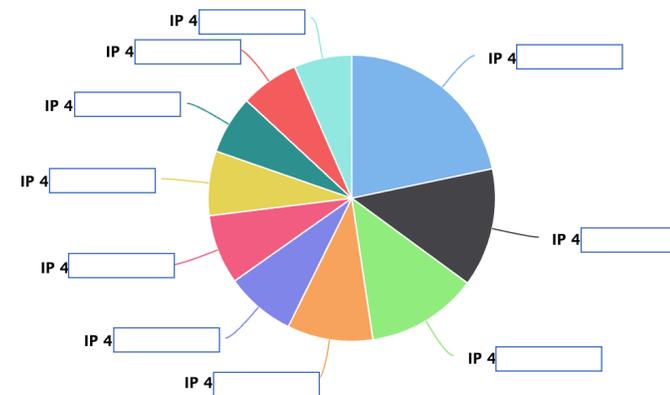
2

Data/Hora	Alerta	Proto	IP origem	Porta origem	IP destino	Porta destino
16/11/2022 10:39:42	bruteforce	TCP	4	60695	1	445
16/11/2022 10:39:42	scanner	TCP	4	4899	1	36830
16/11/2022 10:39:38	bruteforce	TCP	4	23	1	40206
16/11/2022 10:39:38	honeypot	TCP	4	23	1	55265
16/11/2022 10:39:31	honeypot	TCP	12	23634	4	23
16/11/2022 10:39:28	bruteforce	TCP	4	62406	4	23
16/11/2022 10:39:27	honeypot	TCP	14	50634	4	23
16/11/2022 10:39:25	scanner	TCP	4	8014	1	45636
16/11/2022 10:39:24	honeypot	ICMP	4	0	7	0
16/11/2022 10:39:23	scanner	TCP	4	23	5	43807
16/11/2022 10:39:21	bruteforce	TCP	1	56355	4	23
16/11/2022 10:39:21	controller-http_post	TCP	1	443	4	56636



Meus IPs que estão realizando ataques

1 Apenas os 10 IPs que realizaram mais ataques

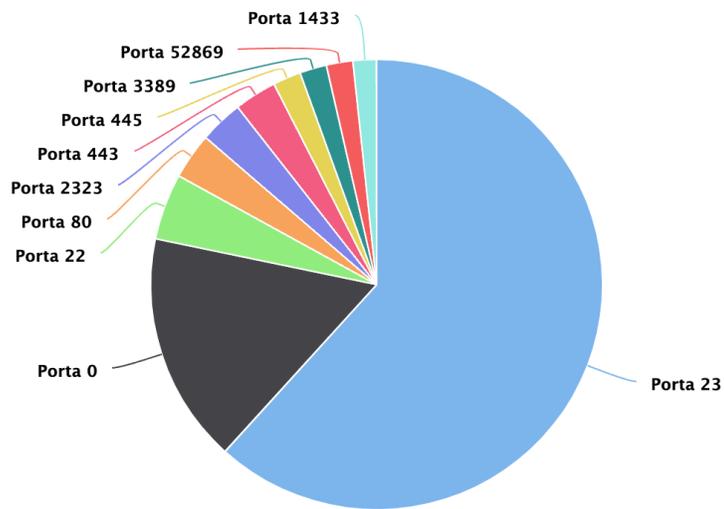


WalledGarden.Global

Minhas portas que estão realizando ataques

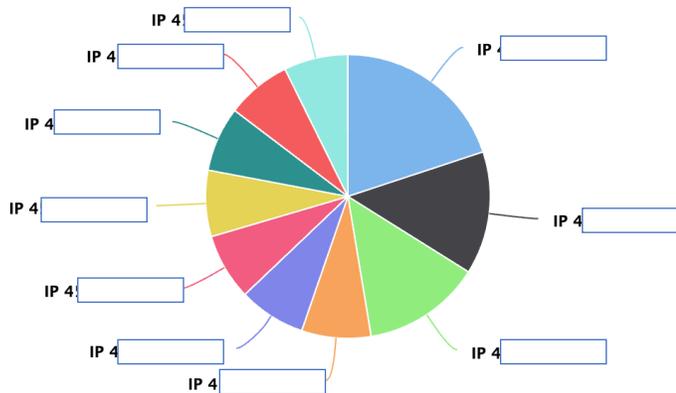


i Minhas portas que estão realizando ataques



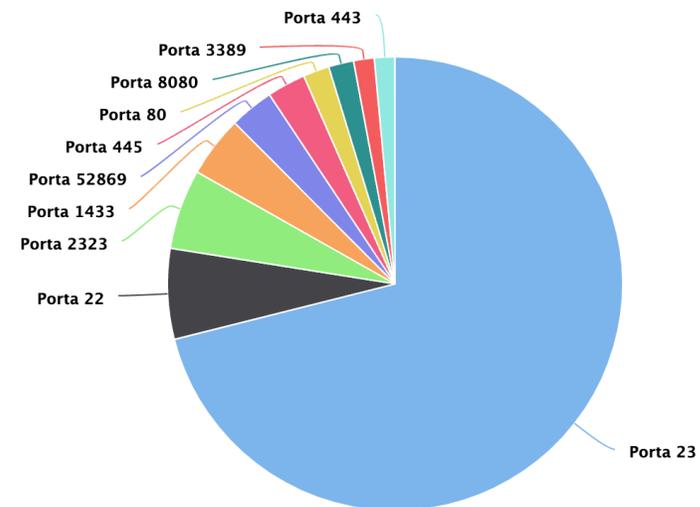
Meus IPs que estão sofrendo ataques

i Apenas os 10 IPs que sofreram mais ataques



Minhas portas que estão sofrendo ataques

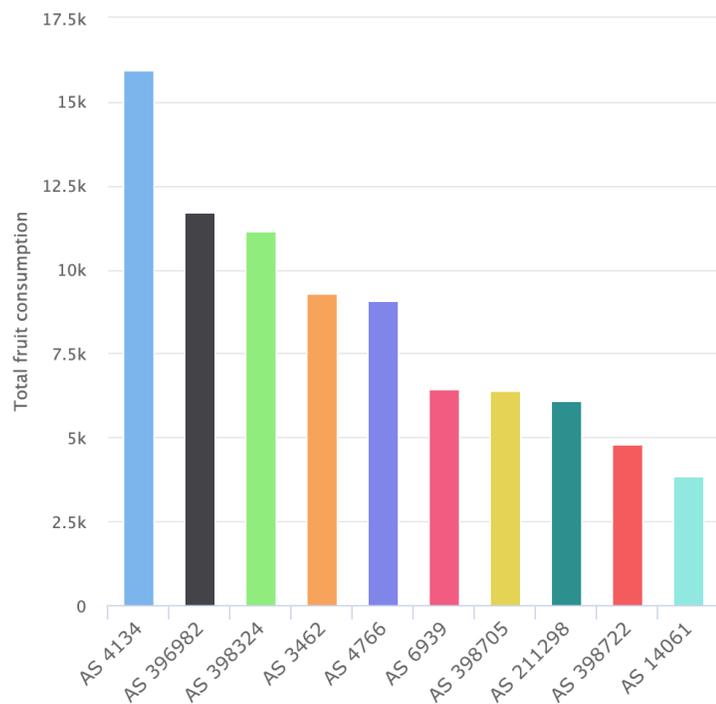
i Apenas as 10 portas que sofreram mais ataques



WalledGarden.Global

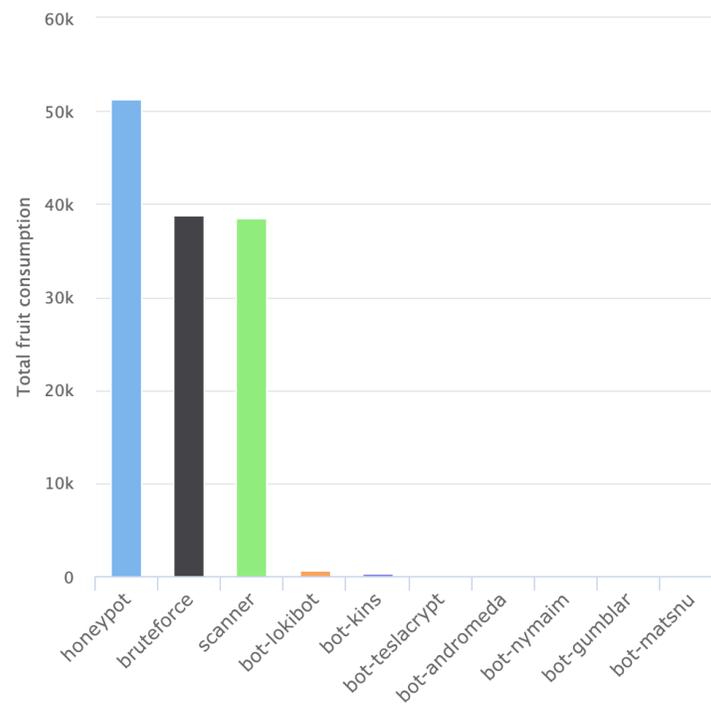
Top alerta de ASs atacantes

Top 10 dos ASs que estão me atacando



Assinatura dos alertas

Distribuição das assinaturas dos alertas



Pensar fora da Caixa...

Easter morning 1900: 5th Ave, New York City. Spot the automobile.



Source: US National Archives.



Pensar fora da Caixa...

Easter morning 1913: 5th Ave, New York City.
Spot the horse.



Source: George Grantham Bain Collection.



Conclusão....

- Teste sua rede com equipes sérias.
- Prevenção é sempre a melhor solução.



Dúvidas?????



Obrigado



Prof. Lacier Dias



lacier@solintel.com.br



(043) 99185-5550



<https://www.linkedin.com/in/lacierdias>



<https://www.facebook.com/lacier.dias>



<https://www.instagram.com/lacierdias/>

