ANÁLISE DO TRÁFEGO DE REDE COM FLOWS NO CONTEXTO DE CIBERSEGURANÇA, O USO DO TC NIMBUS

FRANCISCO JOSE BADARÓ VALENTE NETO / CSIRT ITS

francisco@itsbrasil.net

fjbvneto@gmail.com

Virtual AOPF-AONOG 2020

QUEM SOU EU ?

Francisco José Badaró Valente Neto

- ❑ **Mestre em Sistemas e Computação.**
- ❑ **Especialista em Sistemas e Computação / Redes de Computadores.**
- ❑ **Diversas certificações de diversos fabricantes**

- ***Profissional da área de TI/Telecom/Redes com larga experiência na área de infraestrutura de redes/telecomunicações/internet (Roteamento, Cibersegurança, Arquitetura de Sistemas/Sistemas Operacionais).***
- ***Pesquisador Ativo e Publicador (Redes, Telecomunicações (Otimização e Roteamento)), Cibersegurança, SDN e Blockchain.***
- ***Professor do Centro Universitário UniRuy/Wyden-YDUQS.***
- ***Gerente de Telecomunicações e Treinamento - ITS Brasil***

https://www.linkedin.com/in/franciscobadaro/en

http://lattes.cnpq.br/0008999030113038

https://www.researchgate.net/profile/Francisco_Neto24

QUEM É A ITS ?

ITS BRASIL TELECOM

- ✓ **AS 28186**
  (IRR RADB::AS-ITSBRASIL)
- ✓ **ISP TIER-2 NO BRASIL**
- ✓ **INICIANDO SEU CSIRT, O CSIRT ITS**
  abuse@itsbrasil.net

“Nossa equipe é o que nos dá força”
“Valorizamos a parceria”
“Nós olhamos para o futuro”

https://www.peeringdb.com/net/3284
http://www.itsbrasil.net

QUEM É O TEAM CYMRU ?

""teem cumre""

"Entendemos toda a pilha, incluindo a camada 8 - A camada humana ".

https://team-cymru.com/

TEAM CYMRU

- ✓ **BOGONS/FULLBOGONS**

https://team-cymru.com/community-services/bogon-reference/

- ✓ **UTRS**

https://team-cymru.com/community-services/utrs/

- ✓ **NIMBUS**

https://team-cymru.com/community-services/nimbus/

AGENDA

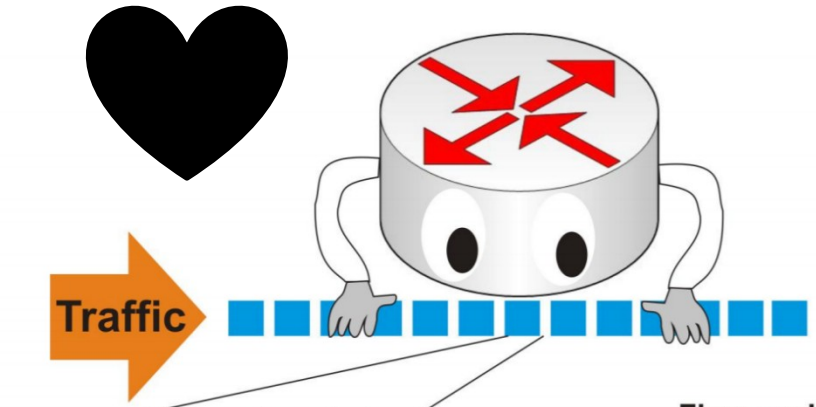
1. **Introdução**
2. Solução Abordada – Estudo de Caso CSIRT ITS
3. Conclusões e Perspectivas Futuras

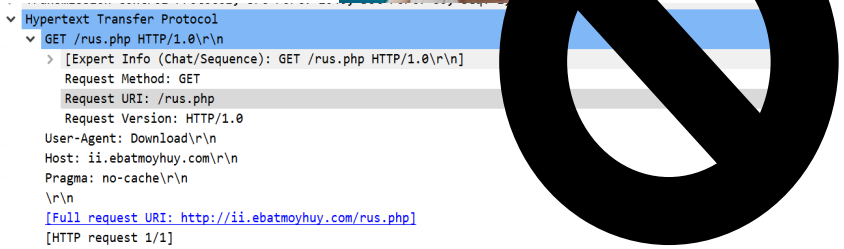
INTRODUÇÃO – Conhece-te a ti mesmo

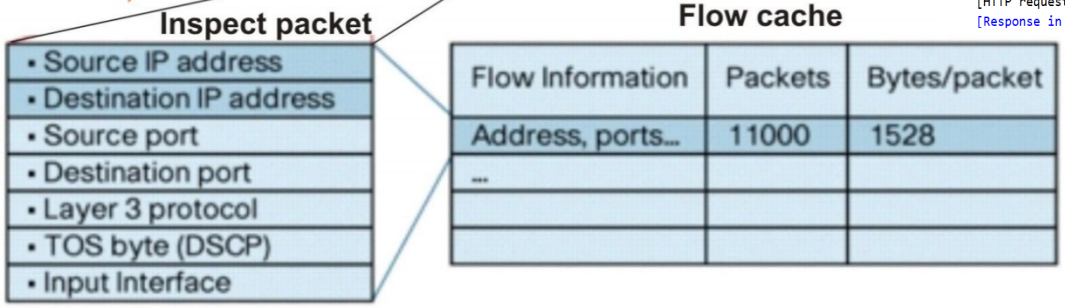
- **Conhece-te a ti mesmo (E o contexto do seu tráfego de rede) ... ... E conhecereis o perfil do seu tráfego, assim compreenderás melhor a natureza do seu inimigo ...**

INTRODUÇÃO – Análise de Tráfego/Flows

- **Protocolos de *Flows* (Netflow , sflow, jflow, IPFIX ...) fornecem detalhes sobre o tráfego (Inclusive permitindo analisar anomalias e conhecer melhor seu inimigo)).**



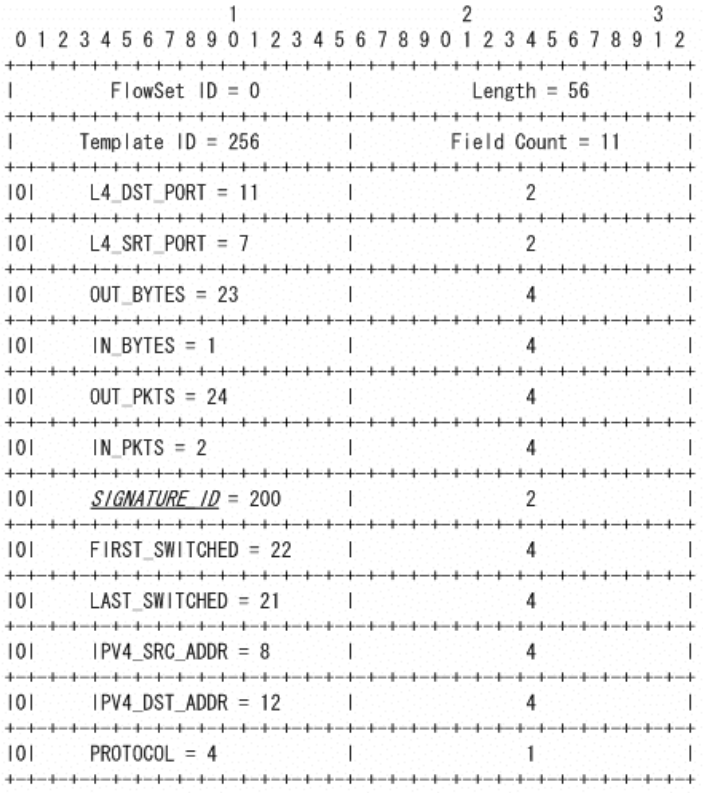




INTRODUÇÃO – Flows/IPFIX

- **Detalhamento de Tráfego com IPFIX (“*Netflow v10*”)**

IETF RFC 7011 e 7012



ATRIBUTO	DESCRIÇÃO
IP Orig.	IP de origem
Porta Orig.	Porta de origem
IP Dest.	IP de destino
Porta Dest.	Porta de destino
Protocolo	Protocolo de Transporte (ICMP, TCP, UDP)
TimeStamp	Carimbo de Tempo do Flow
Duração	Duração do Flow
Bytes (Tam)	Quantidade de Bytes transmitidos
Pacotes (Tam)	Quantidade de pacotes transmitidos
Flags	Concatenação de todas as flags dos protocolos de transporte

- ✓ **O monitoramento de tráfego é essencial para contabilizar o tráfego da rede e auxiliar na detecção de anomalias. ESSENCIAL NO COMBATE A MALIGNIDADE.**

INTRODUÇÃO – Flows/IPFIX

- **Correlação Flows x Base de Assinaturas Team Cymru**

FlowSet ID = 0	Length = 56
Template ID = 256	Field Count = 11
L4_DST_PORT = 11	2
L4_SRT_PORT = 7	2
OUT_BYTES = 23	4
IN_BYTES = 1	4
OUT_PKTS = 24	4
IN_PKTS = 2	4
SIGNATURE_ID = 200	2
FIRST_SWITCHED = 22	4
LAST_SWITCHED = 21	4
IPV4_SRC_ADDR = 8	4
IPV4_DST_ADDR = 12	4
PROTOCOL = 4	1

Dados Flows/IPFIX

+

Base Assinaturas Team Cymru

=

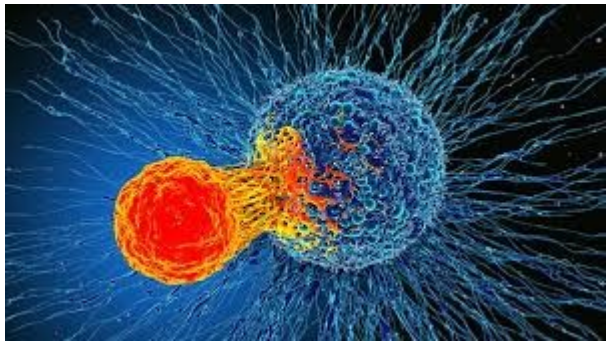
Construção do Conhecimento da Rede

- Método de monitoramento de tráfego em nível de fluxo com reconhecimento de assinatura/padrões e um score de malignidade associado.

- Através da análise de fluxos, temos efetividade na identificação de malignidades, por analisar e correlacionar com comportamentos que definem seu perfil (Assinatura).

INTRODUÇÃO – IDENTIFICAR O INIMIGO

- **MISSÃO: IDENTIFICAR E COMBATER O INIMIGO**

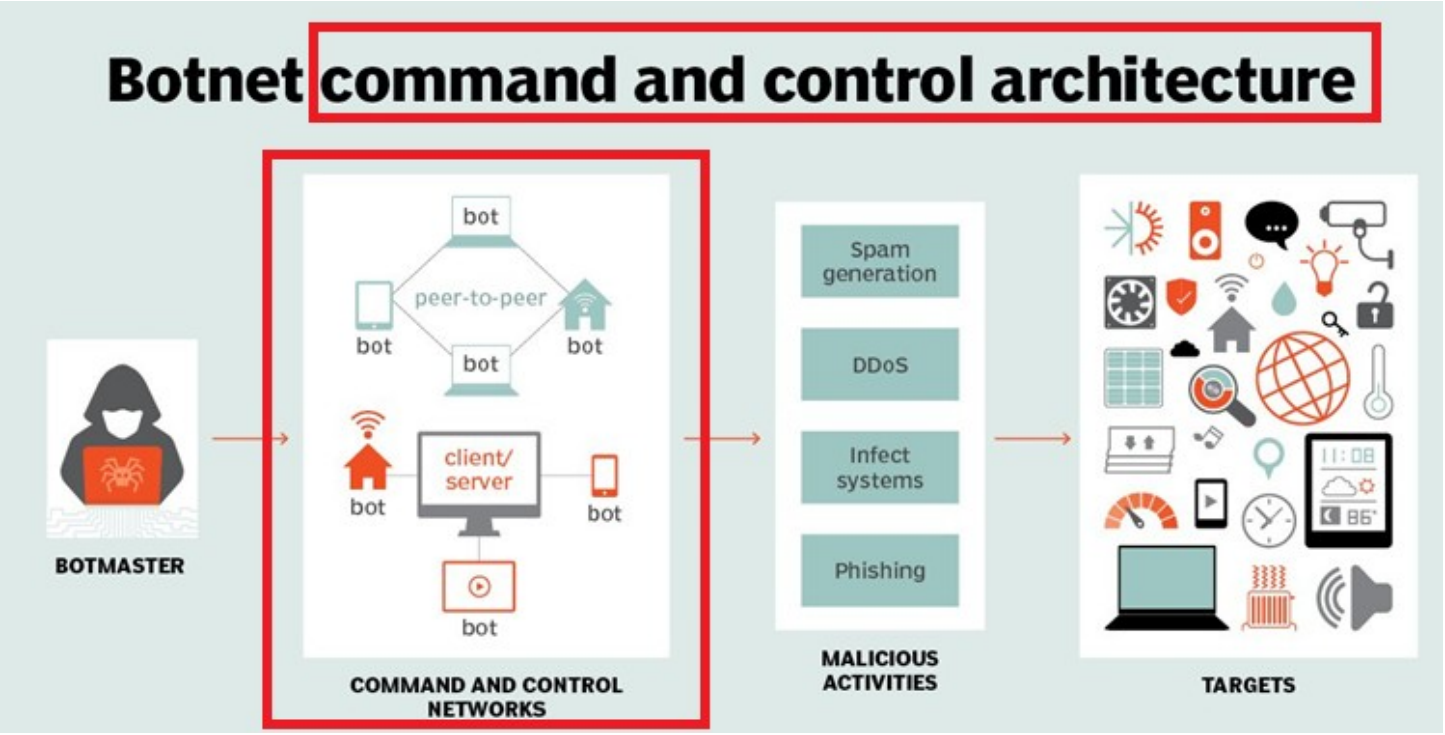


IDENTIFICAR A MALIGNIDADE

➢ **DETECÇÃO DE AMEAÇAS**

Identificar atividade maliciosa (possíveis roubos de dados, uso abusivo, violações de políticas, ataques DDoS e outras ameaças com mais precisão), correlacionando o tráfego de rede com inteligência de ameaças.

INTRODUÇÃO – O INIMIGO: Botnets



- Os cibercriminosos exercem controle remoto por meio de processos automatizados nos hosts controlados (bots) através de canais de comunicação (CnC/C2/C&C) dos mais diversos meios (IRC, HTTP ...).

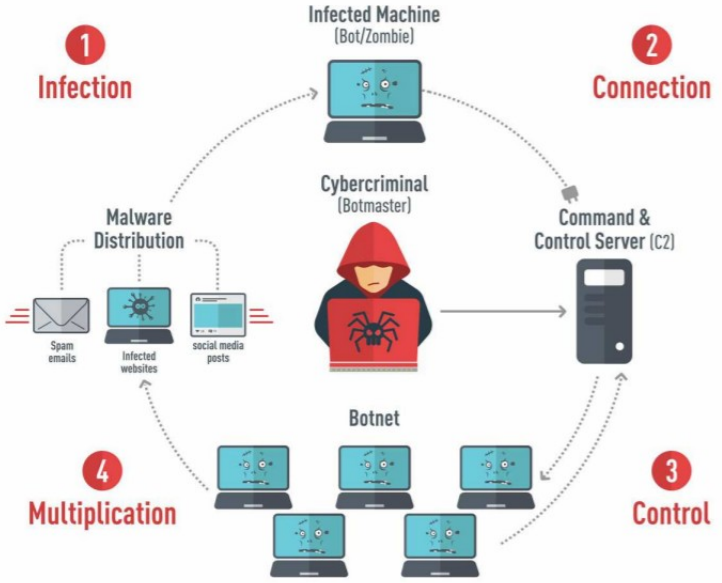
- Como todo o processo ocorre sem o conhecimento ou consentimento do usuário do computador, as botnets são, às vezes, chamados de redes zumbis.

- Uma botnet é um conjunto de hosts comprometidos que executam software maliciosos (Malignidade) controlados remotamente.

INTRODUÇÃO – O INIMIGO: Botnets

- **... O inimigo ... : Botnets !**

*ISRStealer (Information Stealer) , **proxyback,** quant/quanta, minerpanel, gumblar , conficker (W32.Downadup and W32.Conficker), pony/ponyloader, smokeloader, vertexnet (SCADA/Industrial), **mirai (SCADA/Industrial)**, lokibot, kasidet/neutrino, azorult, coresys, emotet ...*



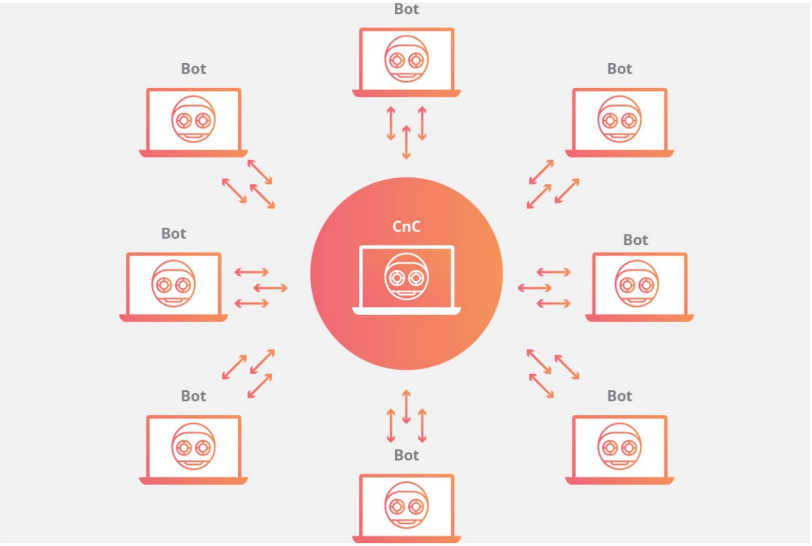
Publicação: The Botnet Reference - Um guia para o conhecer as variações destas malignidades [Informações sobre botnets, Regras YARA (quando existente) ...]

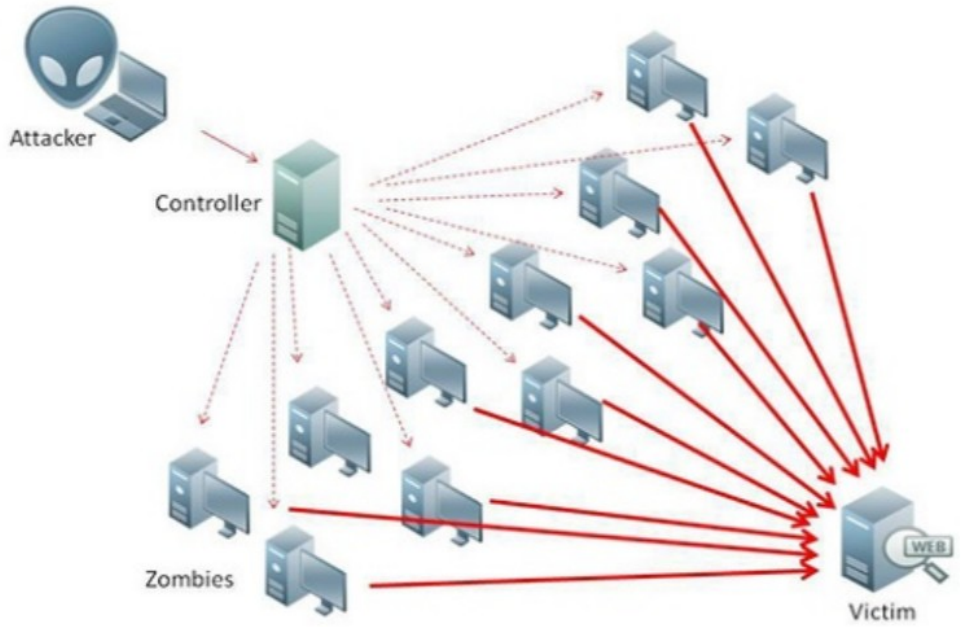
INTRODUÇÃO – O INIMIGO: Botnets

- **Nossa missão: Combate as Botnets para mitigar ATIVIDADES MALICIOSAS !!!**

✓ **IDENTIFICAR ATORES *(HOSTS ENVOLVIDOS)***

✓ **CORRELACIONAR MALIGNIDADE x EVENTO**



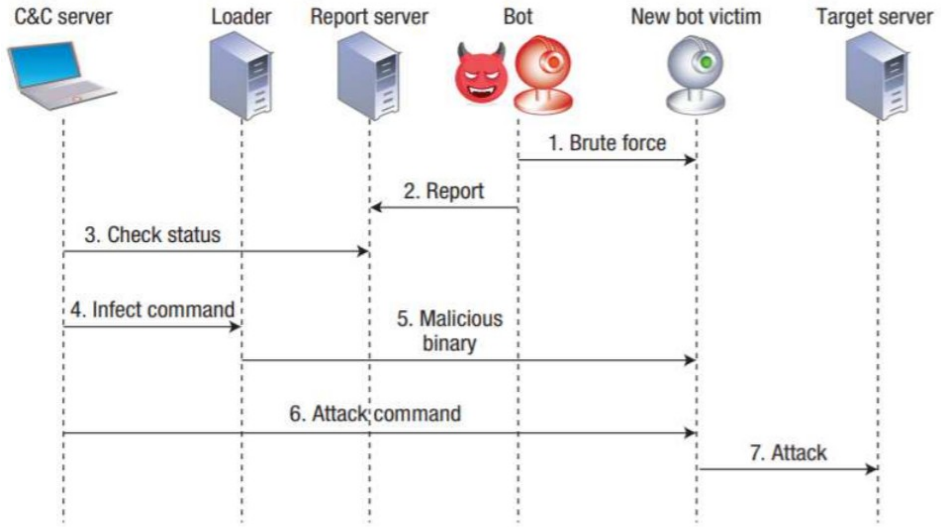


✓ **LIMPEZA DO HOST OU CORTE DA ATIVIDADE DE C2C/CnC**

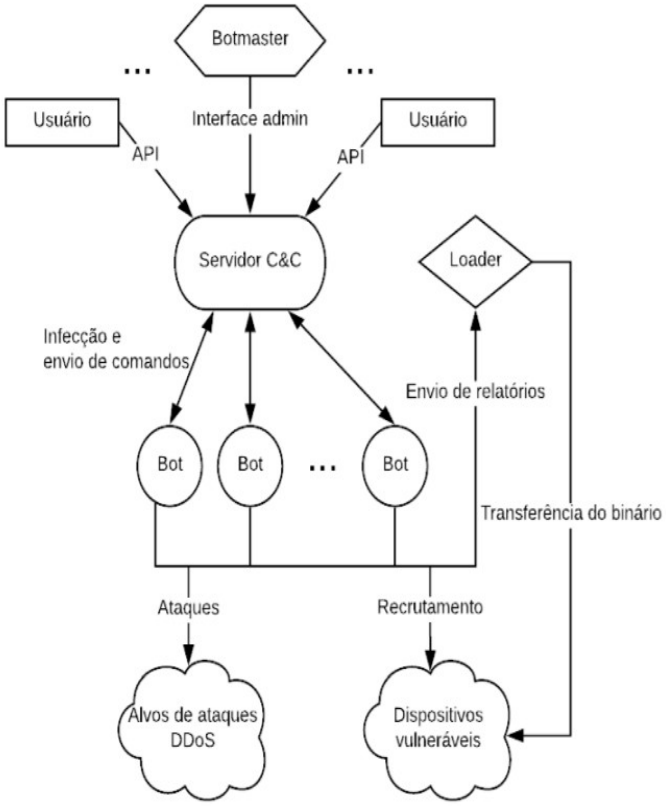
INTRODUÇÃO – O INIMIGO: Botnets

- **Botnet Mirai / Botnet Vertexnet (Botnet SCADA/Industrial | Comunicação e Operação)**

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



!! DDOS DA ORDEM DE TBPS !!



- **Mirai x OVH, 2016 = ~ 1 tbps**
- **Mirai x Akamai/Krebs on Security, 2016 = ~ 620 gbps**
- **Mirai x DynDNS , 2016 = ~ 1 tbps**

INTRODUÇÃO – OS RISCOS

–> Atividades internas maliciosas são um problema comum ("Bob pode estar ao seu lado")

–> Ataques a infraestrutura podem ser altamente prejudiciais ("Ataques as suas pernas e braços, te paralisam")

–> Um ataque à você JÁ PODE (e provavelmente esta) EM ANDAMENTO ("Como você se observa ?")

–> Desafios de conformidade e regulamentares também devem ser atendidos ("Dura Lex, Sed Lex")

–> A perda de dados confidenciais causa mais prejuízo do que perdas financeiras ("Como calcular o intangível ?")

–> Ataques DDoS podem tornar seu sistema de informação impossível de acessar ("No final, o inimigo pode furar o pneu a não conseguir roubar o carro")

Os ataques cibernéticos estão entre os riscos de negócios mais perigosos enfrentados pelo nosso setor.
Técnicas dos inimigos em constante evolução ! TEMOS QUE ESTAR PRONTOS .

INTRODUÇÃO – Tamanho do Problema DDOS

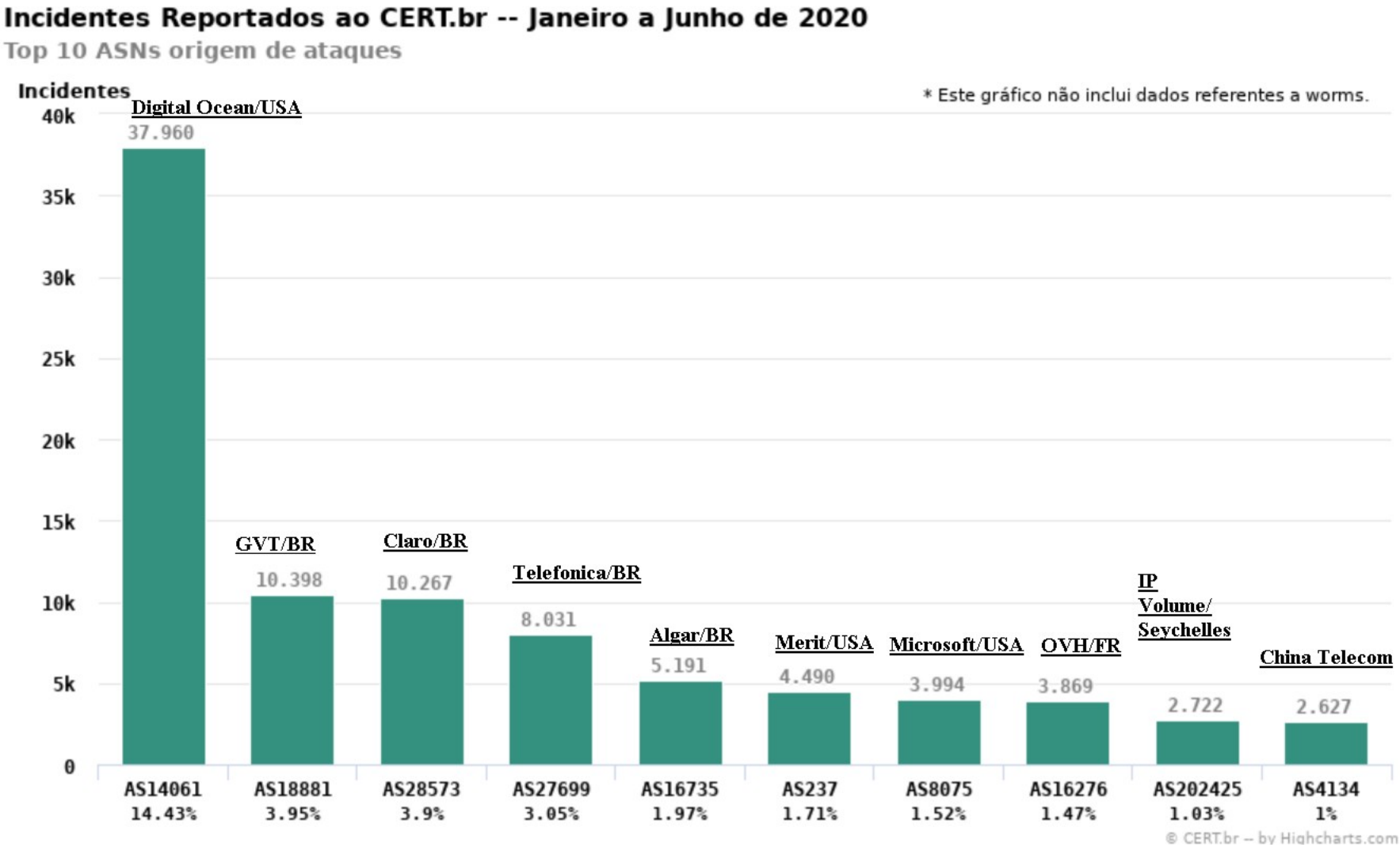
- **O Grande Problema: A AMPLIFICAÇÃO !**

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

Github | Memcached | 2018 = ~ 1.35 tbps
Google | CLDAP e outros | 2017 = ~2.5
AWS | DDOS - CLDAP | 2020 = ~ 2.3 tbps

Clássico Artigo: Amplification Hell – C.Rossow | Ref. Ataque Google
https://christian-rossow.de/publications/amplification-ndss2014.pdf
https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

INTRODUÇÃO – Tamanho do Problema/Estatísticas Nacionais



https://www.cert.br/stats/incidentes/2020-jan-jun/top-asn.html

INTRODUÇÃO – Tamanho do Problema/Estatísticas Globais

Top Countries | ASNs /Remote Code Execution

#	ASN	AS name	Country	IPs	Count
1	44050	PIN-AS	RU	213,760	2,056
2	63949	LINODE-AP	US	544,512	573
3	14061	DIGITALOCEAN-ASN	US	1,863,680	557
4	27699	TELEFÔNICA	BR	6,607,104	504
5	6939	HURRICANE	US	602,624	364
6	206791	SBY-TELECOM-AS	UA	256	355
7	45090	CNNIC-TENCENT-NET-AP	CN	4,953,856	353
8	10439	CARINET	US	121,600	342
9	4134	CHINANET-BACKBONE	CN	115,909,632	312
10	237	MERIT-AS-14	US	5,806,336	223

Top Countries/IoT Attacks

#	Country	Name	ASNs	IPs	Count
1	NL	Netherlands	896	32,114,304	84,279,871
2	US	United States	16,883	1,297,353,844	59,528,380
3	CN	China	422	440,711,680	42,609,490
4	BG	Bulgaria	632	6,040,832	27,798,657
5	FR	France	1,085	83,829,248	13,142,735
6	RU	Russian Federation	5,055	61,620,224	6,275,283
7	DE	Germany	1,857	120,647,296	4,437,352
8	BR	Brazil	6,246	154,998,400	3,356,441
9	UA	Ukraine	1,755	14,999,808	2,592,881
10	IN	India	1,692	46,648,920	2,214,277

Projeto Shadow Server 2020

https://www.shadowserver.org/

Top 20 Países e ASNs MemCached BAD !

Country	Total
South Africa	9,551
United States	8,336
China	3,559
Hong Kong	1,097
Russian Federation	948
Germany	917
France	912
Japan	857
Netherlands	672
Singapore	564
Indonesia	497
United Kingdom	442
Vietnam	420
Canada	365
Brazil	244
India	227
Ukraine	191
Poland	186
Thailand	160
Turkey	155

ASN	AS Name	Country	Total
AS37353	MacroLAN,	ZA	9,467
AS			2,389
AS35916	MULTA-ASN1	US	1,867
AS37963	CNNIC-ALIBABA-CN-NET	CN	1,673
AS18779	EGIHOSTING	US	1,290
AS16276	OVH,	FR	1,087
AS16509	AMAZON-02	US	593
AS63949	LINODE	US	568
AS54600	PEGTECHINC	US	504
AS7859	PAIR-NETWORKS	US	498
AS14618	AMAZON-AES	US	494
AS41095	IPTP,	NL	290
AS4134	CHINANET	CN	280
AS51167	CONTABO	DE	254
AS45090	CNNIC-TENCENT-NET	-	249
AS15003	NOBIS-TECH	US	249
AS24940	HETZNER	DE	226
AS20473	AS-CHOOPA	US	223
AS4837	CHINA169	CN	180
AS27589	MOJOHOST	US	162

Top 20 Countries e ASNs NTP BAD !

Country	Total
United States	459,286
Russian Federation	249,497
China	113,622
United Kingdom	103,081
Germany	87,331
Brazil	74,672
France	65,958
Italy	65,041
Mexico	46,138
Australia	44,252
Japan	42,076
Canada	40,704
Thailand	38,104
Netherlands	34,123
Korea, Republic of	30,487
India	27,351
Czech Republic	26,958
Sweden	26,719
Kazakhstan	25,496
Romania	22,717

ASN	AS Name	Country	Total
AS			65,231
AS3216	SOVAM	RU	53,415
AS4134	CHINANET	CN	38,359
AS7018	ATT-INTERNET4	US	23,915
AS5413	AS5413,	GB	23,579
AS18566	MEGAPATH5-US	US	22,073
AS3269	ASN	IT	20,572
AS4230	CLARO	BR	20,092
AS3320	DTAG	DE	19,423
AS10429	Telefonica	BR	19,224
AS4837	CHINA169	CN	19,062
AS8151	Uninet	MX	17,898
AS5588	GTSCE	CZ	17,319
AS7922	COMCAST-7922	US	16,765
AS4766	KIXS-AS	KR	15,917
AS9198	KAZTELECOM	KZ	13,923
AS1257	TELE2,	EU	12,194
AS1221	ASN	AU	12,021
AS6128	CABLE-NET-1	US	11,844
AS11172	Alestra,	MX	11,368

Projeto SISSDEN 2019

Secure Information Sharing Sensor Delivery Event Network

https://sissden.eu/

INTRODUÇÃO – Tamanho do Problema/Estatísticas Globais

The 10 Worst Botnet Countries

As of 06 August 2020 the world's worst botnet infected countries are:

1	India	Number of Bots: 1853658
2	China	Number of Bots: 1361005
3	Iran (Islamic Republic of)	Number of Bots: 921557
4	Viet Nam	Number of Bots: 885370
5	Thailand	Number of Bots: 468576
6	Brazil	Number of Bots: 463946
7	United States of America	Number of Bots: 417500
8	Egypt	Number of Bots: 404401
9	Indonesia	Number of Bots: 403589
10	Pakistan	Number of Bots: 313648

https://www.spamhaus.org/statistics/botnet-cc/

The 10 Worst Botnet ASNs

As of 07 August 2020 the world's worst botnet infected Autonomous System Numbers are:

1	AS4134 China Telecom (ChinaNet)	Number of Bots: 873990
2	AS45609 Bharti Airtel Ltd. AS for GPRS Service	Number of Bots: 824967
3	AS45899 VNPT Corp	Number of Bots: 430922
4	AS8452 TE Data, SAE	Number of Bots: 331402
5	AS7713 PT Telekomunikasi Indonesia	Number of Bots: 229390
6	AS36947 Telecom Algeria	Number of Bots: 222263
7	AS45595 Pakistan Telecom Company Limited	Number of Bots: 222070
8	AS4837 China Unicom	Number of Bots: 217138
9	AS7552 Viettel Group	Number of Bots: 214667
10	AS9829 Bharat Sanchar Nigam Limited (BSNL)	Number of Bots: 177001

https://www.spamhaus.org/statistics/botnet-asn/

INTRODUÇÃO – O que você pode fazer ?

- **Fornecimento de informações detalhadas do tráfego da rede.**
- **Estas, contextualizadas com cibersegurança.**
- **Combate as botnets / “Cortar” o C2C-C&C-CnC / Identificar atores-ameaças/malignidades**
- **Colaborar com o Ecossistema/Comunidade de Cibersegurança !**
- **(CERT.br / Projetos de impacto na internet / Grupos de P&D de Relevância e notável contribuição (Como o Team Cymru, o Projeto Shadow Server ...) .**
- **... ... ...**

INTRODUÇÃO – Como Mitigar as Necessidades ?

AGENDA

1. Introdução

2. **Solução Abordada – Estudo de Caso CSIRT ITS**

3. Conclusões e Perspectivas Futuras

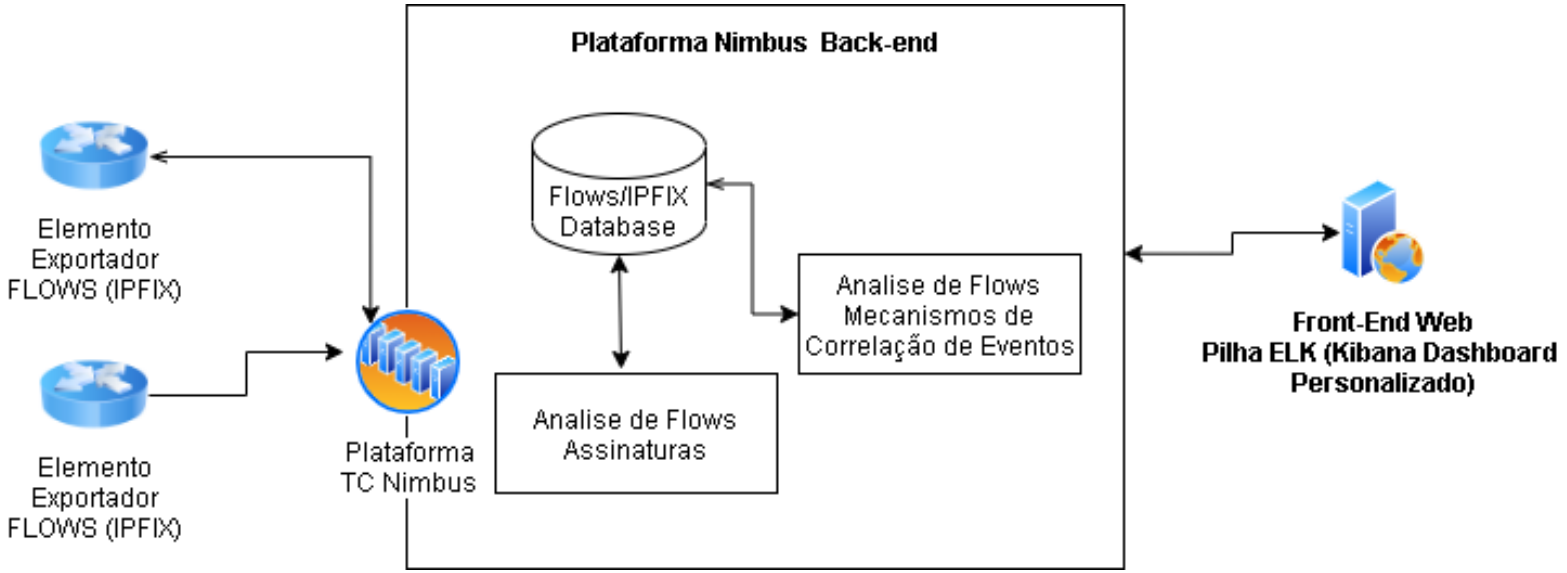
Solução Abordada – Estudo de Caso CSIRT ITS

- **ANALISE DE FLOWS, COM TC NIMBUS**

  https://team-cymru.com/community-services/nimbus-threat-monitor/

- **Contextualização da inteligência de tráfego com aspectos de cibersegurança**

Arquitetura Plataforma TC Nimbus



Solução Abordada – Estudo de Caso CSIRT ITS

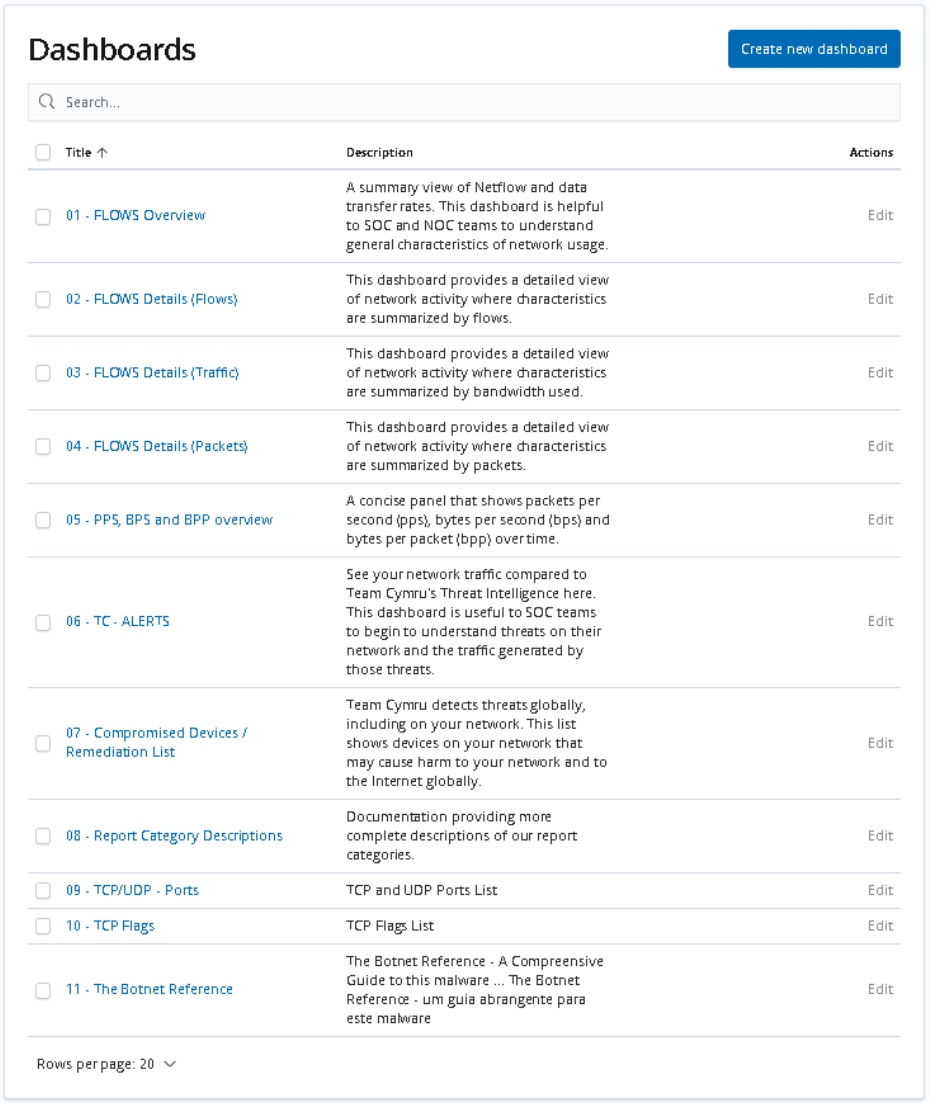
- O que é o TC Nimbus ?

- TC Nimbus = Dashboard Analítico

Pilha ELK (Elastic +

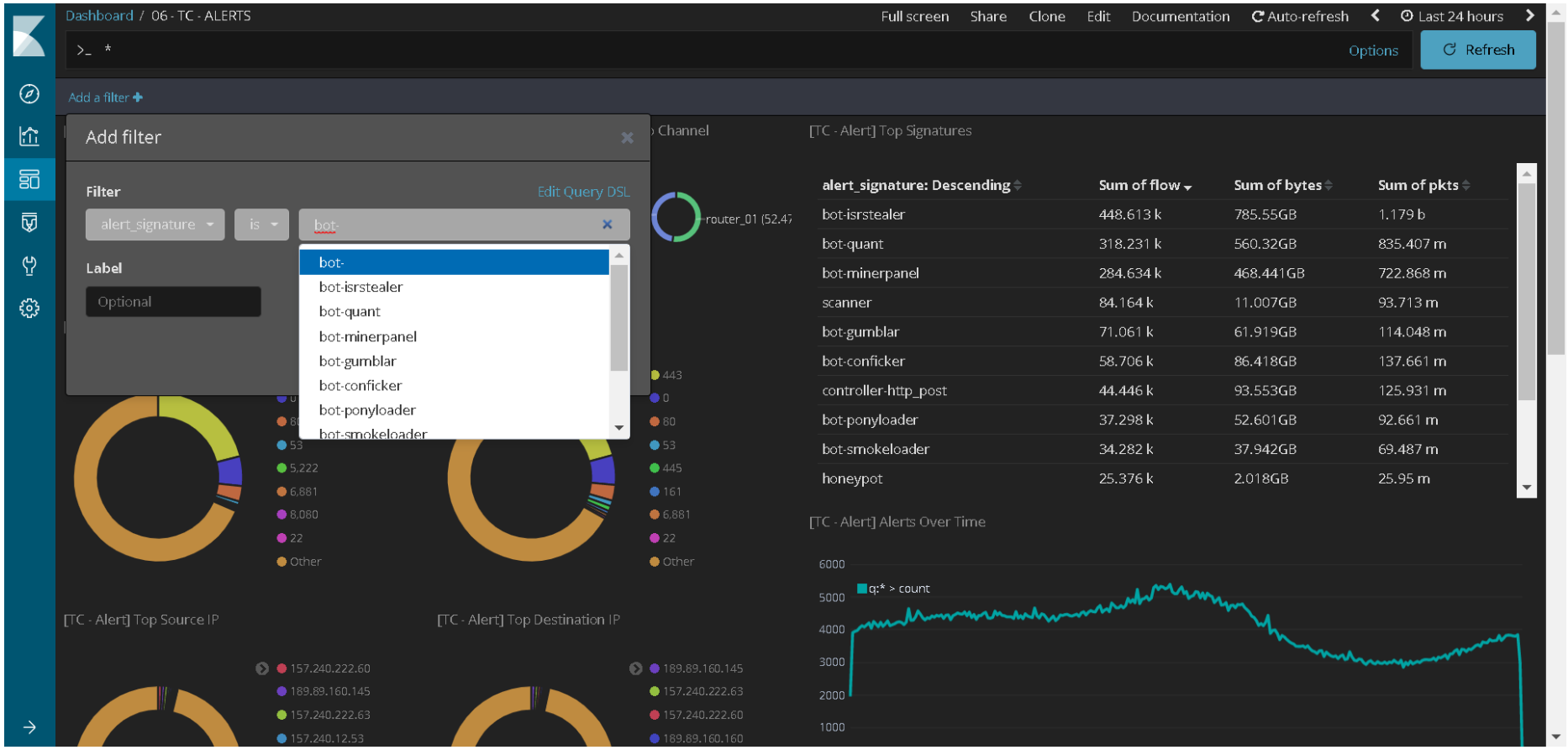
Kibana Personalizado)

~ 18 filtros possíveis para alertas
~ 31 filtros de estatísticas de rede
~ 7,000,000 + indicadores atualizados por hora
Suporte para netflow (v5/v7/v9/v10-IPFix), sflow, jflow e NetStream



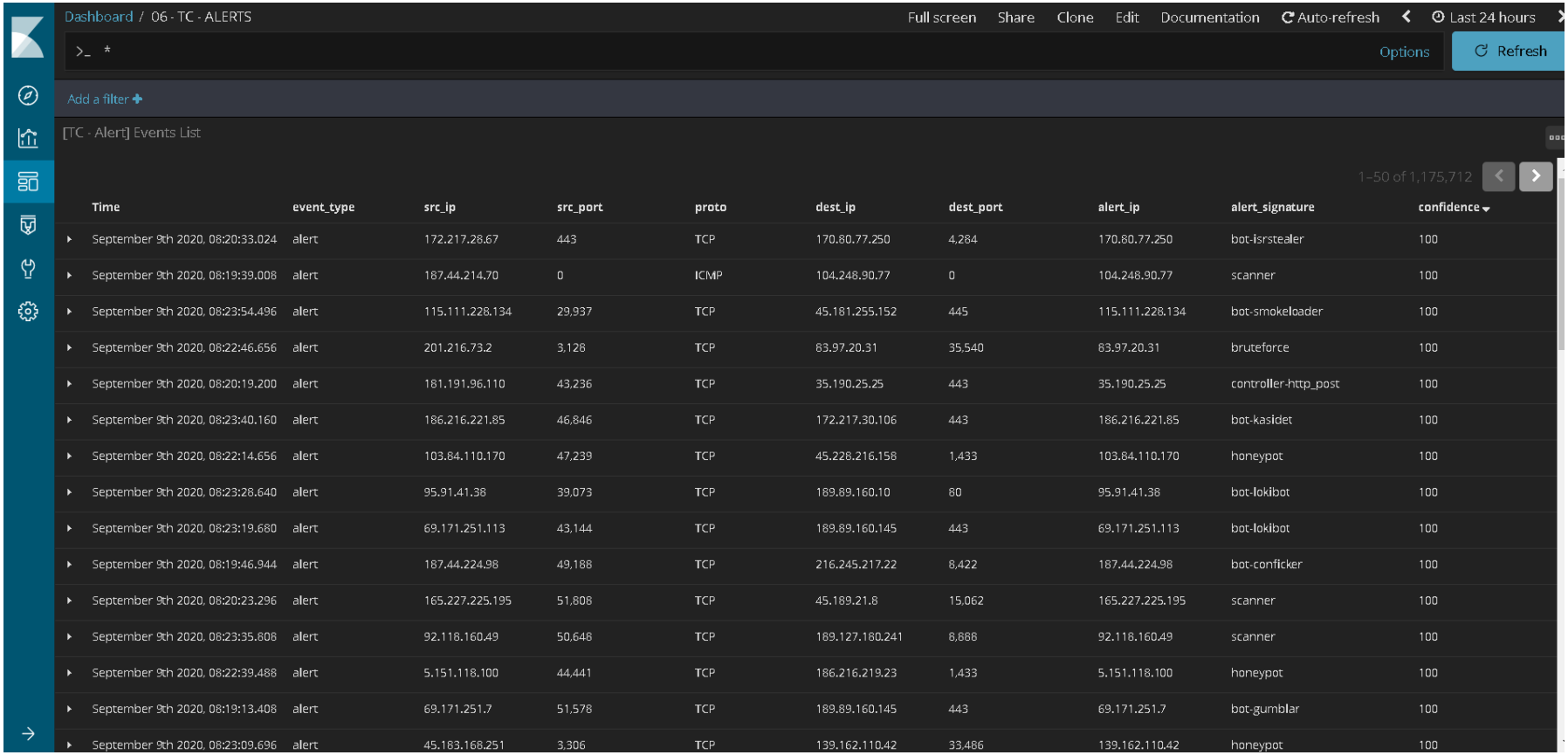
Solução Abordada – Estudo de Caso CSIRT ITS

- **TC Nimbus – Dashboards – TODO PODER AOS FILTROS !**



Solução Abordada – Estudo de Caso CSIRT ITS

- **TC Nimbus – Dashboards/Escore CONFIDENCE (“*Qualidade dos dados*”)**

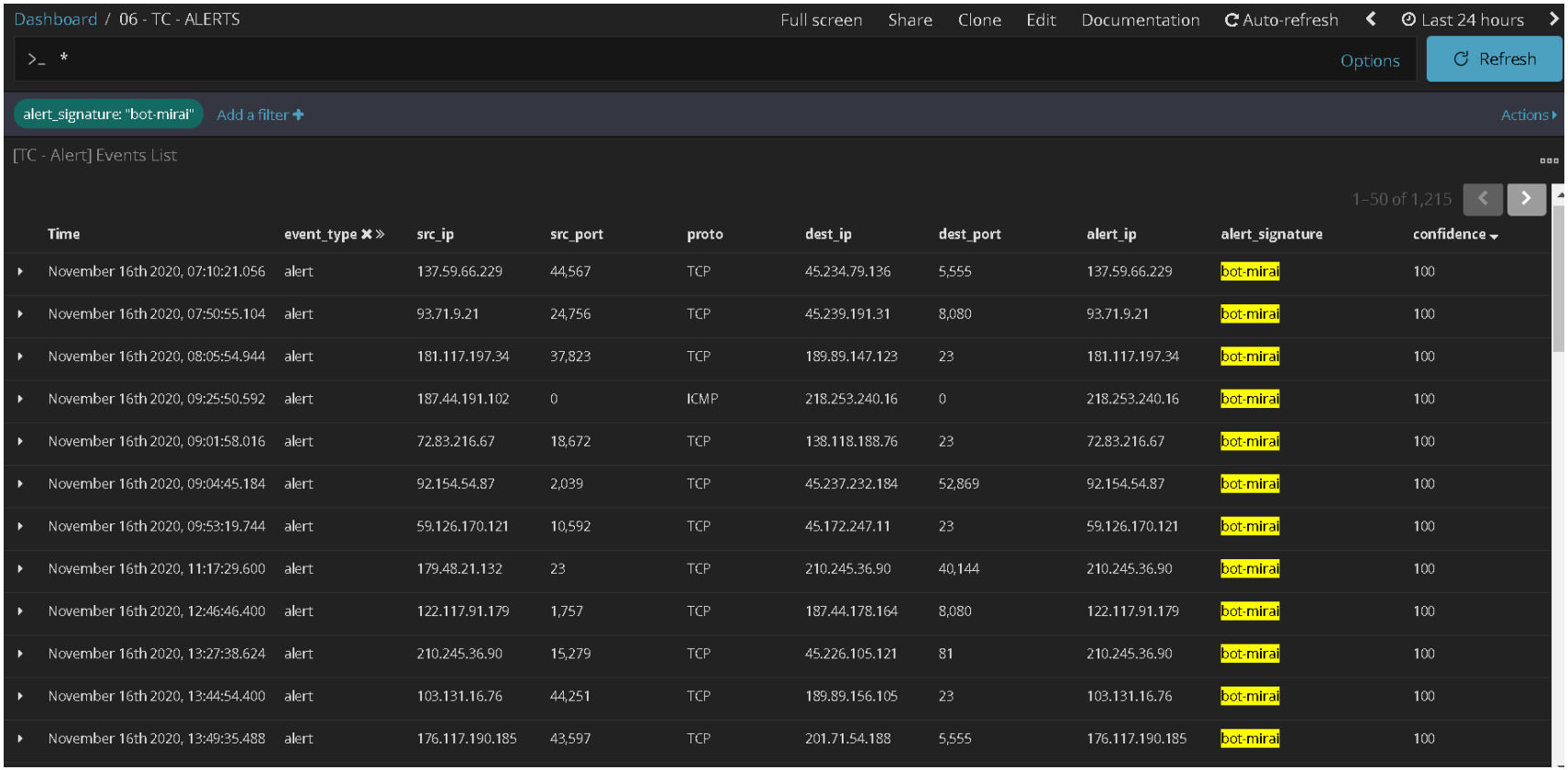


Time	event_type	src_ip	src_port	proto	dest_ip	dest_port	alert_ip	alert_signature	confidence
September 9th 2020, 08:20:33.024	alert	172.217.28.67	443	TCP	170.80.77.250	4,284	170.80.77.250	bot-isrstealer	100
September 9th 2020, 08:19:39.008	alert	187.44.214.70	0	ICMP	104.248.90.77	0	104.248.90.77	scanner	100
September 9th 2020, 08:23:54.496	alert	115.111.228.134	29,937	TCP	45.181.255.152	445	115.111.228.134	bot-smokeloader	100
September 9th 2020, 08:22:46.656	alert	201.216.73.2	3,128	TCP	83.97.20.31	35,540	83.97.20.31	bruteforce	100
September 9th 2020, 08:20:19.200	alert	181.191.96.110	43,236	TCP	35.190.25.25	443	35.190.25.25	controller-http_post	100
September 9th 2020, 08:23:40.160	alert	186.216.221.85	46,846	TCP	172.217.30.106	443	186.216.221.85	bot-kasidet	100
September 9th 2020, 08:22:14.656	alert	103.84.110.170	47,239	TCP	45.228.216.158	1,433	103.84.110.170	honeypot	100
September 9th 2020, 08:23:28.640	alert	95.91.41.38	39,073	TCP	189.89.160.10	80	95.91.41.38	bot-lokibot	100
September 9th 2020, 08:23:19.680	alert	69.171.251.113	43,144	TCP	189.89.160.145	443	69.171.251.113	bot-lokibot	100
September 9th 2020, 08:19:46.944	alert	187.44.224.98	49,188	TCP	216.245.217.22	8,422	187.44.224.98	bot-conficker	100
September 9th 2020, 08:20:23.296	alert	165.227.225.195	51,808	TCP	45.189.21.8	15,062	165.227.225.195	scanner	100
September 9th 2020, 08:23:35.808	alert	92.118.160.49	50,648	TCP	189.127.180.241	8,888	92.118.160.49	scanner	100
September 9th 2020, 08:22:39.488	alert	5.151.118.100	44,441	TCP	186.216.219.23	1,433	5.151.118.100	honeypot	100
September 9th 2020, 08:19:13.408	alert	69.171.251.7	51,578	TCP	189.89.160.145	443	69.171.251.7	bot-gumblar	100
September 9th 2020, 08:23:09.696	alert	45.183.168.251	3,306	TCP	139.162.110.42	33,486	139.162.110.42	honeypot	100

IP	Reputation Score	Days Observed	Category	Country Code
115.111.228.134	98	29	bot, darknet	
170.80.77.250	93	28	bot	
186.216.221.85	1	21	bot	

Solução Abordada – Estudo de Caso CSIRT ITS

TC Nimbus – Dashboards – INVESTIGANDO ATIVIDADE BOTNET MIRAI (APENAS Últimas 24h !)



Dashboard / 06 - TC - ALERTS — Full screen | Share | Clone | Edit | Documentation | Auto-refresh | Last 24 hours

>_ * — Options | Refresh

alert_signature: "bot-mirai" | Add a filter | Actions

[TC - Alert] Events List — 1–50 of 1,215

Time	event_type	src_ip	src_port	proto	dest_ip	dest_port	alert_ip	alert_signature	confidence
November 16th 2020, 07:10:21.056	alert	137.59.66.229	44,567	TCP	45.234.79.136	5,555	137.59.66.229	bot-mirai	100
November 16th 2020, 07:50:55.104	alert	93.71.9.21	24,756	TCP	45.239.191.31	8,080	93.71.9.21	bot-mirai	100
November 16th 2020, 08:05:54.944	alert	181.117.197.34	37,823	TCP	189.89.147.123	23	181.117.197.34	bot-mirai	100
November 16th 2020, 09:25:50.592	alert	187.44.191.102	0	ICMP	218.253.240.16	0	218.253.240.16	bot-mirai	100
November 16th 2020, 09:01:58.016	alert	72.83.216.67	18,672	TCP	138.118.188.76	23	72.83.216.67	bot-mirai	100
November 16th 2020, 09:04:45.184	alert	92.154.54.87	2,039	TCP	45.237.232.184	52,869	92.154.54.87	bot-mirai	100
November 16th 2020, 09:53:19.744	alert	59.126.170.121	10,592	TCP	45.172.247.11	23	59.126.170.121	bot-mirai	100
November 16th 2020, 11:17:29.600	alert	179.48.21.132	23	TCP	210.245.36.90	40,144	210.245.36.90	bot-mirai	100
November 16th 2020, 12:46:46.400	alert	122.117.91.179	1,757	TCP	187.44.178.164	8,080	122.117.91.179	bot-mirai	100
November 16th 2020, 13:27:38.624	alert	210.245.36.90	15,279	TCP	45.226.105.121	81	210.245.36.90	bot-mirai	100
November 16th 2020, 13:44:54.400	alert	103.131.16.76	44,251	TCP	189.89.156.105	23	103.131.16.76	bot-mirai	100
November 16th 2020, 13:49:35.488	alert	176.117.190.185	43,597	TCP	201.71.54.188	5,555	176.117.190.185	bot-mirai	100

IP	Reputation Score	Days Observed	Category	Country Code
122.117.91.179	100	29	bot, darknet, scanner	
181.117.197.34	100	27	bot, darknet	
72.83.216.67	100	29	bot, darknet, honeypot, scanner	
138.118.188.76	0	0	-	
187.44.178.164	0	0	-	
189.89.147.123	0	0	-	

Solução Abordada – Estudo de Caso CSIRT ITS

- **AÇÃO CSIRT ITS - Aviso informativo (E reforço...)**

ITS TELECOMUNICAÇÕES/DEPARTAMENTO DE MONITORAMENTO E SEGURANÇA

RELATÓRIO INFORMATIVO DE SEGURANÇA – [redacted]
RELATÓRIO – [redacted]*16*
EMITIDO EM: 11/01/2020

À [redacted]

Prezados parceiros, [redacted]

Vimos por meio deste emitir relatório informativo do e-mail enviado, comunicando o evento de segurança informado no e-mail com assunto [redacted]16 .

INTRODUÇÃO

Conforme nosso planejamento que envolve a qualidade na prestação dos serviços, mantemos equipe que fica em monitoramento constante, com contexto de segurança, analisando o nosso espaço de endereçamento (informado pública e totalmente via IRR [1] conforme a RPSL [2], sob o AS-SET AS-ITSBRASIL registrado no IRR Server RADB da Merit [3], compondo o escopo de análise da nossa equipe de monitoramento e segurança.

Nossa atuação primária, a luz da Lei Nº 12.965/2014 (Lei do Marco Civil da Internet) [4] e o regulamento da internet Brasileira conforme o marco regulatório do SCM [5], se apoia também nas boas práticas e tem como objetivo o bom atendimento ao nosso assinante. Diante disto, nossa equipe conforme a metodologia adotada descrita detalhadamente abaixo neste documento, detectou os eventos relatados no e-mail de comunicado cujo objetivo deste relatório é detalhar melhor tal e-mail informativo e os eventos contextualizados nele, com instrumentação (conjunto de software) e procedimentos, detalhados na sessão de metodologia deste documento, objetivando o levantamento de dados , para análise e informativo de eventos de segurança, do host abaixo informado pela tabela 1:

HOST ANALISADO	187.44.188.6
CLIENTE ENVOLVIDO	[redacted]

Tabela 1 – Host Analisado

Este relatório está dividido em 3 subcapítulos, assim estruturados:

1. **Fundamentação Teórica**, onde explanamos a conceituação teórica sobre os eventos relatados com uma fundamentação técnica referenciando a literatura disponível até o estado da arte, alinhando ao nosso estudo de caso prático, na operação do AS28186, o contexto do assunto tratado neste documento.
2. **Metodologia**, onde explanamos o método/procedimento utilizado para a busca, processamento/tratamento dos dados/geração de informação de inteligência conforme informativo do evento de segurança correlato.
3. **Conclusão**, onde concluímos o relatório , sugerindo com objetivo de auxiliar nosso maior patrimônio, nossos clientes/parceiros a, dentro da nossa limitação de escopo/atuação, corrigir os eventuais problemas relatados.

FUNDAMENTAÇÃO TEÓRICA

A internet atualmente é muito mais que um simples veículo, um simples ambiente. Muitos aspectos na sociedade atual são dependentes da internet, logo devemos ter uma preocupação, mesmo que básica, com o contexto de Cibersegurança. Logo o contexto da Cibersegurança é um objeto da nossa análise, neste, temos o que chamamos de malignidades que são o conjunto de vulnerabilidades de softwares que causam problemas impactando de diversas formas a fruição do serviço de fornecimento de internet, impactando na qualidade, inclusive em alguns eventos, comprometendo os dados. Segundo o Cert.br [6], Ataques de negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (DDoS - Distributed Denial of Service). Um ataque DDoS não tem o objetivo direto de invadir e nem de coletar informações, mas sim de exaurir recursos e causar indisponibilidade ao alvo.

[CSIRT-ITS] [redacted] ADVOGADOS ASSOCIADOS S/C | [redacted]6 | Serviço SNMP habilitado | SDR-SAP-[redacted] Caixa de entrada ×

[redacted]@itsbrasil.net sex., 4 de set. 14:46 (há 6 dias)
para [redacted]

Prezado [redacted] **ADVOGADOS ASSOCIADOS S/C**,

Os IPs presentes no log abaixo são de sua responsabilidade e estão com o serviço SNMP (**161/udp**) habilitado. Este serviço pode ser usado para fazer parte de **ataques distribuídos de negação de serviço**, consumindo recursos da sua rede e impactando terceiros.

O indicador no campo 'Resultados do Teste' indica o tipo de problema testado e significa:

* **snmp:** status/pacotes/bytes, onde status e' "open", e pacotes/bytes indicam o tamanho da resposta recebida, em pacotes/bytes.

IP	STATUS | DATA DO TESTE | RESULTADO DO TESTE	ALERTA
187.44.216.74	OPEN | 2020-09-04T10:12:09Z | snmp: open/1/103	Serviço SNMP habilitado

Lembramos que os endereços IP listados, além de servidores e computadores, também podem ser de dispositivos de rede com o serviço SNMP habilitado, como roteadores, impressoras, CPEs (modem ou roteador de uso domestico instalado nos clientes), entre outros.

Gostaríamos de solicitar que:

* o serviço SNMP seja configurado corretamente ou desabilitado no equipamento, caso não esteja em uso.

Uma descrição do problema e possíveis soluções podem ser encontradas no final deste e-mail.

Se você não for a pessoa correta para corrigir o problema destes equipamentos com o serviço SNMP habilitado, **por favor repasse essa mensagem para alguém de sua organização que possa faze-lo.**

* O que e' o serviço SNMP **(161/udp)**?

O SNMP (Simple Network Management Protocol) é um protocolo de rede utilizado para gerenciamento e diagnostico de dispositivos de redes.

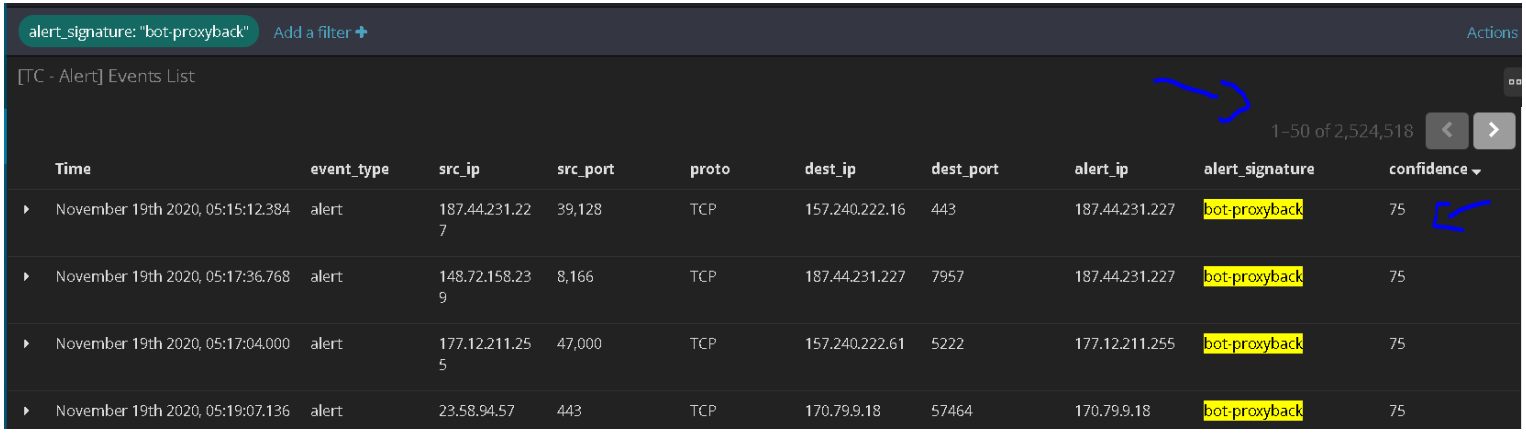
DATA MÁXIMA VENIA

Solução Abordada – Estudo de Caso CSIRT ITS

TC Nimbus – Dashboards –UM RESULTADO ! NOVA BOTNET NO RADAR.... MIRAI DIMUNIUDA !

Glória DEUS !!! kkk mirai morreu !

... houston, we have a new enemy: BOTNET PROXYBACK !



Time	event_type	src_ip	src_port	proto	dest_ip	dest_port	alert_ip	alert_signature	confidence
November 19th 2020, 05:15:12.384	alert	187.44.231.227	39,128	TCP	157.240.222.16	443	187.44.231.227	bot-proxyback	75
November 19th 2020, 05:17:36.768	alert	148.72.158.239	8,166	TCP	187.44.231.227	7957	187.44.231.227	bot-proxyback	75
November 19th 2020, 05:17:04.000	alert	177.12.211.255	47,000	TCP	157.240.222.61	5222	177.12.211.255	bot-proxyback	75
November 19th 2020, 05:19:07.136	alert	23.58.94.57	443	TCP	170.79.9.18	57464	170.79.9.18	bot-proxyback	75

Solução Abordada – Estudo de Caso CSIRT ITS

COMO FAZER PARTE NO PROJETO NIMBUS ?

https://team-cymru.com/community-services/nimbus/
https://partners.team-cymru.com/nimbus-threat-monitor?utm_source=aonog20&utm_medium=tradeshow&utm_campaign=nimbustm

GET STARTED !

Informe os dados solicitados no formulário de cadastro prévio.

REQUISITOS:

- ✓ ***SER UM SISTEMA AUTÔNOMO NA INTERNET***
- ✓ ***ACORDO DE NDA COM O TEAM CYMRU***
- ✓ ***EXPORTAR FLOWS (Netflow v5/v7/v9, IPFIX ("v10"), sflow, jflow, NetStream em IPv4 e IPv6 para os coletores do projeto !***

AGENDA

1. Introdução
2. Solução Abordada – Estudo de Caso CSIRT ITS
3. **Conclusões e Perspectivas Futuras**

Conclusões e Perspectivas Futuras

- **META: NOTIFICAR OS ENVOLVIDOS. COLABORAR COM A COMUNIDADE.**

- **ANALISAR OS DADOS, EM MAIOR PROFUNDIDADE E LARGURA POSSÍVEL.**

PARA TAL, O USO DE FLOWS (IPFIX) NA CLASSIFICAÇÃO E E ANÁLISE DE EVENTOS PERMITE GRANDE EFICACIA.

AGRADECIMENTOS

MUITO OBRIGADO

A ITS Brasil por fomentar e por incentivar a pesquisa acadêmica e o desenvolvimento interno dos seus colaboradores.

Ao Team Cymru por existir e por fomentar um ambiente de rede seguro, limpo e livre da malignidades de rede e disponibilizar conteúdo e ferramentas de grande valor a comunidade.

FRANCISCO JOSE BADARÓ VALENTE NETO

francisco@itsbrasil.net

fjbvneto@gmail.com