"Caça a botnets , com análise de fluxos de rede e um comparativo da superfície de ataque IPv4 x IPv6”.

Um estudo de caso com o Team Cymru Nimbus

Como aproveitar fluxos de rede (IPFIX) com a pilha ELK para o conhecimento da natureza do tráfego.

Francisco Badaró

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

francisco@itsbrasil.net & fjbvneto@gmail.com

Quem sou ?

Profissional com ampla experiência em engenharia de redes, roteamento e segurança cibernética (projeto de ambientes, hardening, computação forense, implementação e análise de dados de honeypot/honeynets, análise de vulnerabilidades e eventos, execução de pentest). Ampla experiência em análise de tráfego e contextualização com segurança cibernética. Experiência em ambiente CSIRT. Coordenação da equipe, com ampla exposição em grupos multiculturais. Atualmente gerente de telecomunicações na ITS Brasil e Professor no Centro Universitário UniRuy. Investigador e Pesquisador ativo nas áreas de roteamento, sistemas operacionais, telecomunicações, cibersegurança e programabilidade de redes/SDN.

https://www.linkedin.com/in/franciscobadaro/ | fjbvneto@gmail.com | francisco@itsbrasil.net

Quem é a ITS ?

ITS BRASIL

- ✓ **AS 28186**

  (IRR RADB::AS-ITSBRASIL)

- ✓ **ISP TIER-2 NO BRASIL**

https://as28186.peeringdb.com/

http://www.itsbrasil.net

Quem é o Team Cymru?

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

https://team-cymru.com/

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

https://team-cymru.com/company/#team

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/

- ✓ **IP REPUTATION**

https://reputation.team-cymru.com/

https://ipscore.team-cymru.com/

Agenda

1. Introdução

2. TC Nimbus - Estudo de Caso / ITS AS28186
"Caçando Atividade de Botnets em IPv4 e IPv6"

3. Conclusões e Perspectivas Futuras

Agenda

1. Introdução

2. TC Nimbus - Estudo de Caso / ITS AS28186
"Caçando Atividade de Botnets em IPv4 e IPv6"

3. Conclusões e Perspectivas Futuras

INTRODUÇÃO – CONHEÇA A SI MESMO

Conheça a si mesmo (e o contexto de seu tráfego de rede) e você vai conhecer o perfil de seu tráfego, então e somente assim, você vai entender melhor a natureza de seu inimigo.

“Conheça o inimigo e conheça a si mesmo; Em cem batalhas você nunca estará em perigo. Quando você não conhece o inimigo, mas conhecer a si mesmo, suas chances de ganhar ou perder são iguais...”

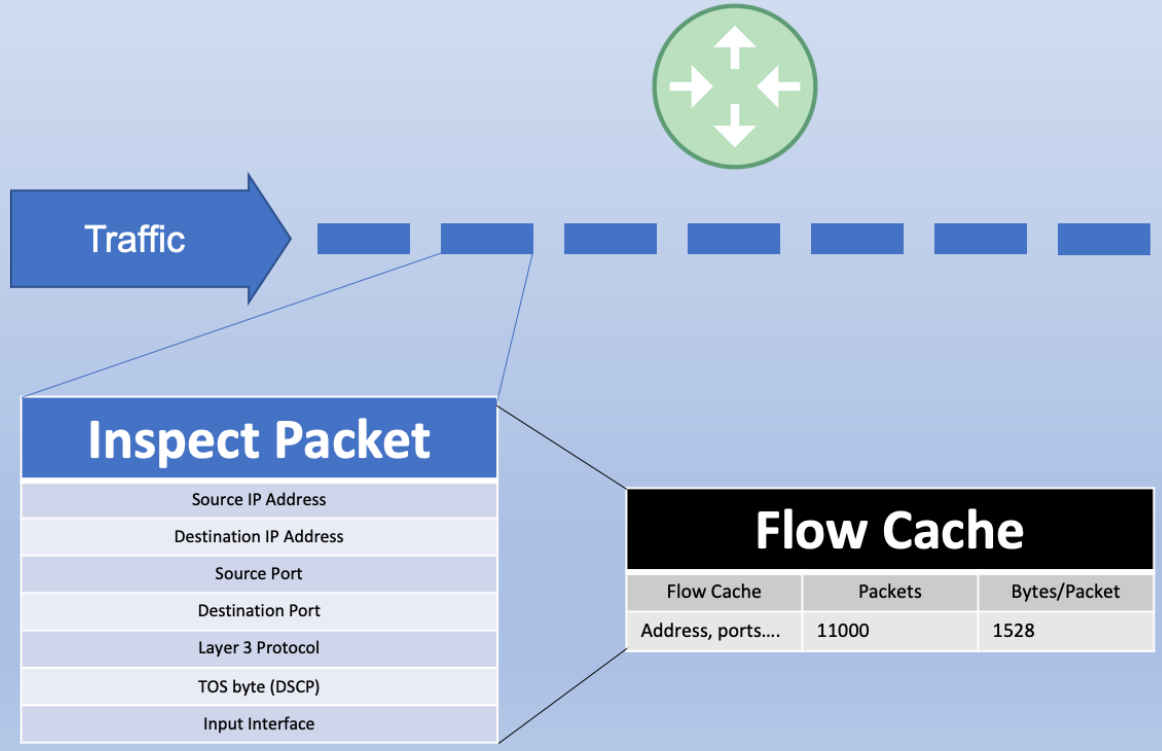
Sun Tzu

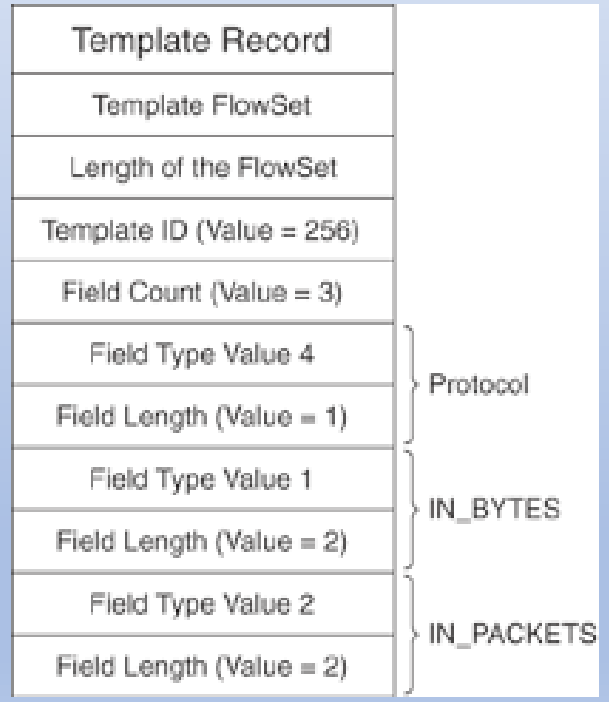
"Se você não conheçe o seu inimigo e não conheçe a sí mesmo, contará suas batalhas, pelas suas derrotas."

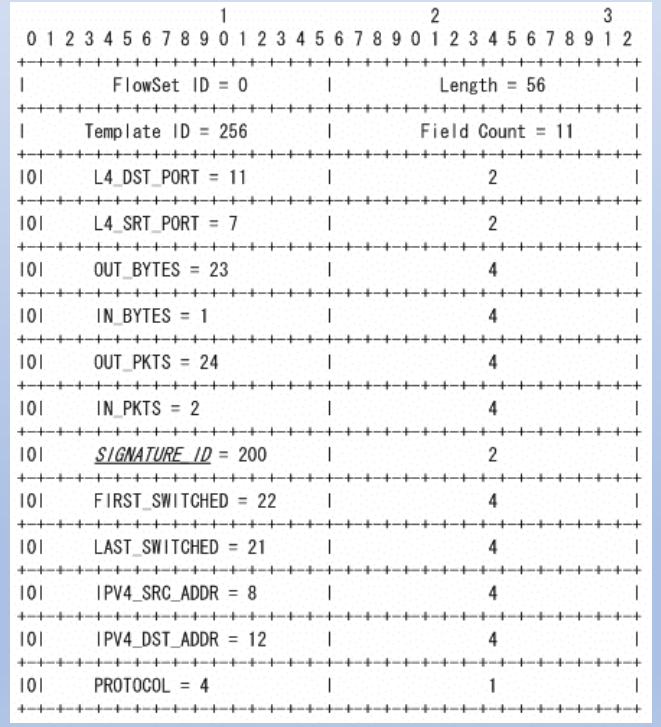
INTRODUÇÃO – ANÁLISE DE TRÁFEGO - Network Flows/IPFIX

- **Flow Protocols (Netflow, sflow, jflow, IPFIX) , *"Protocolos para coleta de metadados sobre o tráfego de rede"***

IETF RFC 7011 e 7012



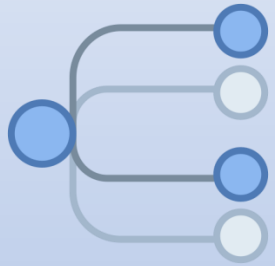




```
                    1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 1 2
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        FlowSet ID = 0         |          Length = 56          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Template ID = 256         |        Field Count = 11       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     L4_DST_PORT = 11        |              2                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     L4_SRT_PORT = 7         |              2                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     OUT_BYTES = 23          |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     IN_BYTES = 1            |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     OUT_PKTS = 24           |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     IN_PKTS = 2             |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     SIGNATURE_ID = 200      |              2                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     FIRST_SWITCHED = 22     |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     LAST_SWITCHED = 21      |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     IPV4_SRC_ADDR = 8       |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     IPV4_DST_ADDR = 12      |              4                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|     PROTOCOL = 4            |              1                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

INTRODUÇÃO – Geração de Conhecimento do Tráfego de Rede

Correlacione seus flows com os mecanismos de inteligência de sinal do Team Cymru



+

TEAM CYMRU

=

METADADOS DO SEU TRÁFEGO DE REDE
(Protocolo IPFIX)

INTELIGÊNCIA DE SINAL DO TEAM CYMRU
(IP Reputation / Controller Feed (C2) / BARS Botnet Analysis and Reporting System)

CONSTRUÇÃO DO CONHECIMENTO DA NATUREZA DO TRÁFEGO DE REDE

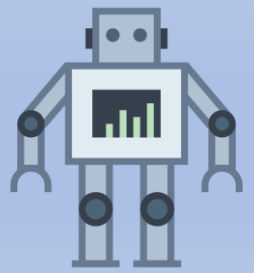
- Método de monitoramento de tráfego em nível dos flows da rede com reconhecimento de assinatura/padrão e um score de confiança associado.
- Através da análise dos flows de rede, temos eficácia na identificação da atividade de malware, analisando e correlacionando-o com comportamentos que definem seu perfil.

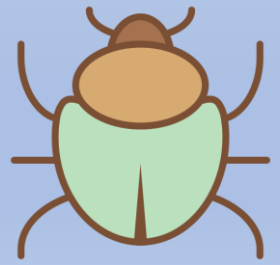
INTRODUÇÃO – Identificando o Inimigo

MISSÃO: IDENTIFICAR E COMBATER O INIMIGO



IDENTIFICAR MALWARE/BOTNETS





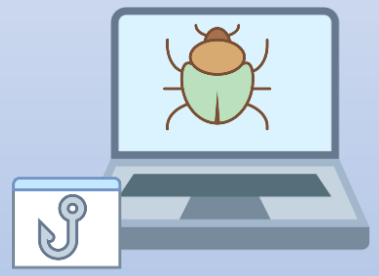
DETECÇÃO AVANÇADA DE AMEAÇAS

Identifique atividades maliciosas (possíveis roubo/exfiltração de dados, violações de políticas, ataques DDoS e outras ameaças com mais precisão), correlacionando os seus flows de rede com a inteligência avançada de ameaças do Team Cymru.

INTRODUÇÃO – Um exemplo de inimigo: BOTNETS

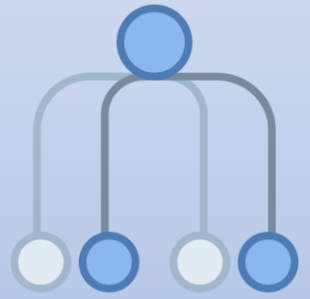
Uma Botnet é um conjunto de hosts comprometidos, rodando software malicioso controlado remotamente.

BOT



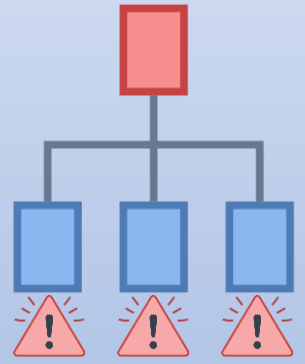
+

NETWORK



=

BOTNET



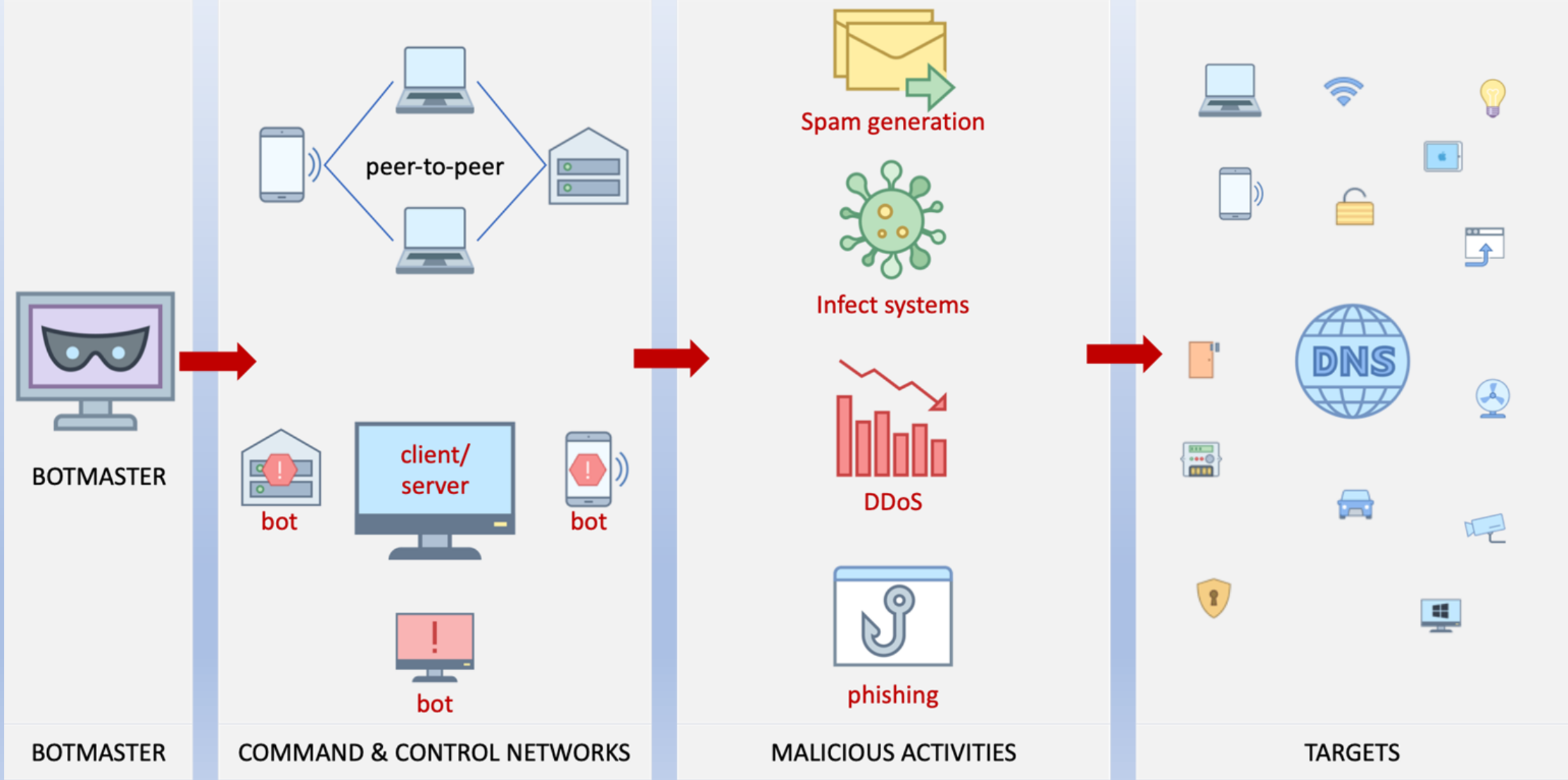
NOSSO PROPÓSITO:

- IDENTIFICAR HOSTS ENVOLVIDOS
- CORRELACIONAR MALWARE x EVENTOS
- COMBATER O CIBERCRIME

PROPÓSITO DAS BOTNETS :

- SUPORTE PARA O CIBERCRIME
- UTILIZAÇÃO EM ATAQUES, EM ESCALA

INTRODUÇÃO – C2 (Infraestrutura de Comando & Controle)



INTRODUÇÃO – Tamanho do Problema/Dados-Estatísticas Globais

The 10 Worst Botnet Countries

As of 03 May 2022 the world's worst botnet infected countries are:

1	China	Number of Bots: 787797
2	United States of America	Number of Bots: 459519
3	India	Number of Bots: 436070
4	Thailand	Number of Bots: 182863
5	Indonesia	Number of Bots: 167644
6	Algeria	Number of Bots: 128088
7	Viet Nam	Number of Bots: 127468
8	Brazil	Number of Bots: 103123
9	Pakistan	Number of Bots: 79491
10	Japan	Number of Bots: 74373

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

The 10 Worst Botnet ISPs

As of 03 May 2022 the world's worst botnet infected ISPs are:

1	amazon.com	Number of Bots: 463320
2	airtel.in	Number of Bots: 238879
3	chinanet-ah	Number of Bots: 131025
4	djaweb.dz	Number of Bots: 115037
5	chinanet-js	Number of Bots: 112116
6	telkom.net.id	Number of Bots: 91038
7	chinanet-fj	Number of Bots: 82346
8	unicom-ln	Number of Bots: 79538
9	vnpt.vn	Number of Bots: 56210
10	tot.co.th	Number of Bots: 55147

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

The 10 Worst Botnet ASNs

As of 03 May 2022 the world's worst botnet infected Autonomous System Numbers are:

1	AS4134 China_Telecom_(ChinaNet)	Number of Bots: 564971
2	AS16509 AMAZON-02	Number of Bots: 381496
3	AS45609 Bharti Airtel Ltd. AS for GPRS Service	Number of Bots: 168964
4	AS4837 China_Unicom	Number of Bots: 167507
5	AS36947 Telecom_Algeria	Number of Bots: 110681
6	AS7713 PT_Telekomunikasi_Indonesia	Number of Bots: 92300
7	AS14618 NAME_NO_LONGER_AVAILABLE	Number of Bots: 86026
8	AS24560 Bharti_Airtel_Ltd._Telemedia_Services	Number of Bots: 72835
9	AS45899 VNPT_Corp	Number of Bots: 57625
10	AS23969 TOT Public Company Limited	Number of Bots: 55193

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

INTRODUÇÃO – Tamanho do Problema/Dados - Estatísticas Locais

TOP 9 - ASes em Alerta X Pais de Origem - IPv4 – 24 H

POSIÇÃO	ASN	NOME	PAÍS
1	14061	DIGITALOCEAN	USA
2	12593	UKRCOM	UCRANIA
3	62041	TELEGRAM	REINO UNIDO (ILHAS VIRGENS)
4	209160	MITI 2000 EOOD	BULGARIA
5	50340	SELECTEL	RUSSIA
6	202425	IPVOLUME	SEYCHELLES
7	49453	GLOBAL LAYER B.V	HOLANDA
8	44446	OOO SIBIRINVEST	HOLANDA
9	16276	OVH	FRANÇA

195 K Eventos observados

TOP 9 - ASes em Alerta X Pais de Origem - IPv4 – 30 D

POSIÇÃO	ASN	NOME	PAÍS
1	50340	SELECTEL	RUSSIA
2	14061	DIGITALOCEAN	USA
3	209160	MITI 2000 EOOD	BULGARIA
4	62041	TELEGRAM	REINO UNIDO (ILHAS VIRGENS)
5	12593	UKRCOM	UCRANIA
6	50867	HOSTKEY B.V.	HOLANDA
7	202425	IPVOLUME	SEYCHELLES
8	61432	TOV VAIZ PARTNER	RUSSIA
9	49453	GLOBAL LAYER B.V	HOLANDA

1.2 M Eventos observados

TOP 9 - ASes em Alerta X Pais de Origem – IPv6 – 24 H

POSIÇÃO	ASN	NOME	PAÍS
1	62041	TELEGRAM	REINO UNIDO (ILHAS VIRGENS)
2	13335	CLOUDFLARE	USA

272 Eventos observados

TOP 9 - ASes em Alerta X Pais de Origem – IPv6 – 30 D

POSIÇÃO	ASN	NOME	PAÍS
1	62041	TELEGRAM	REINO UNIDO (ILHAS VIRGENS)
2	13335	CLOUDFLARE	USA
3	14061	DIGITALOCEAN	USA

1.4 K Eventos observados

INTRODUÇÃO – Como cumprir a missão ?

Nossa Missão: Combater as botnets para mitigar as ATIVIDADES MALICIOSAS DO CIBERCRIME.

COMO ?

1. Identificar os atores envolvidos (Rede/Hosts envolvidos).
2. Correlacionar atividade de Malware com os eventos de rede.
3. Conhecer o tráfego de sua rede e então conter a atividade de <u>C2/C&C de Botnets</u>

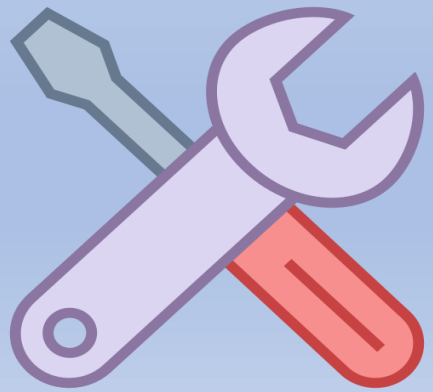
INTRODUÇÃO – Como auxiliar na missão ?

NESTES TEMPOS DE INCERTEZA?

- **Providenciando informações detalhadas sobre o seu tráfego de rede.**
- **Contextualizando com cibersegurança.**
- **Combatendo Botnets / Cortando a comunicação de C2/ Identificando atores-ameaças**

Com Estratégia, Inteligência, Ciência e

AUXILIADO POR UMA FERRAMENTA !



Agenda

1. Introdução

2. TC Nimbus - Estudo de Caso / ITS AS28186
"Caçando Atividade de Botnets em IPv4 e IPv6"

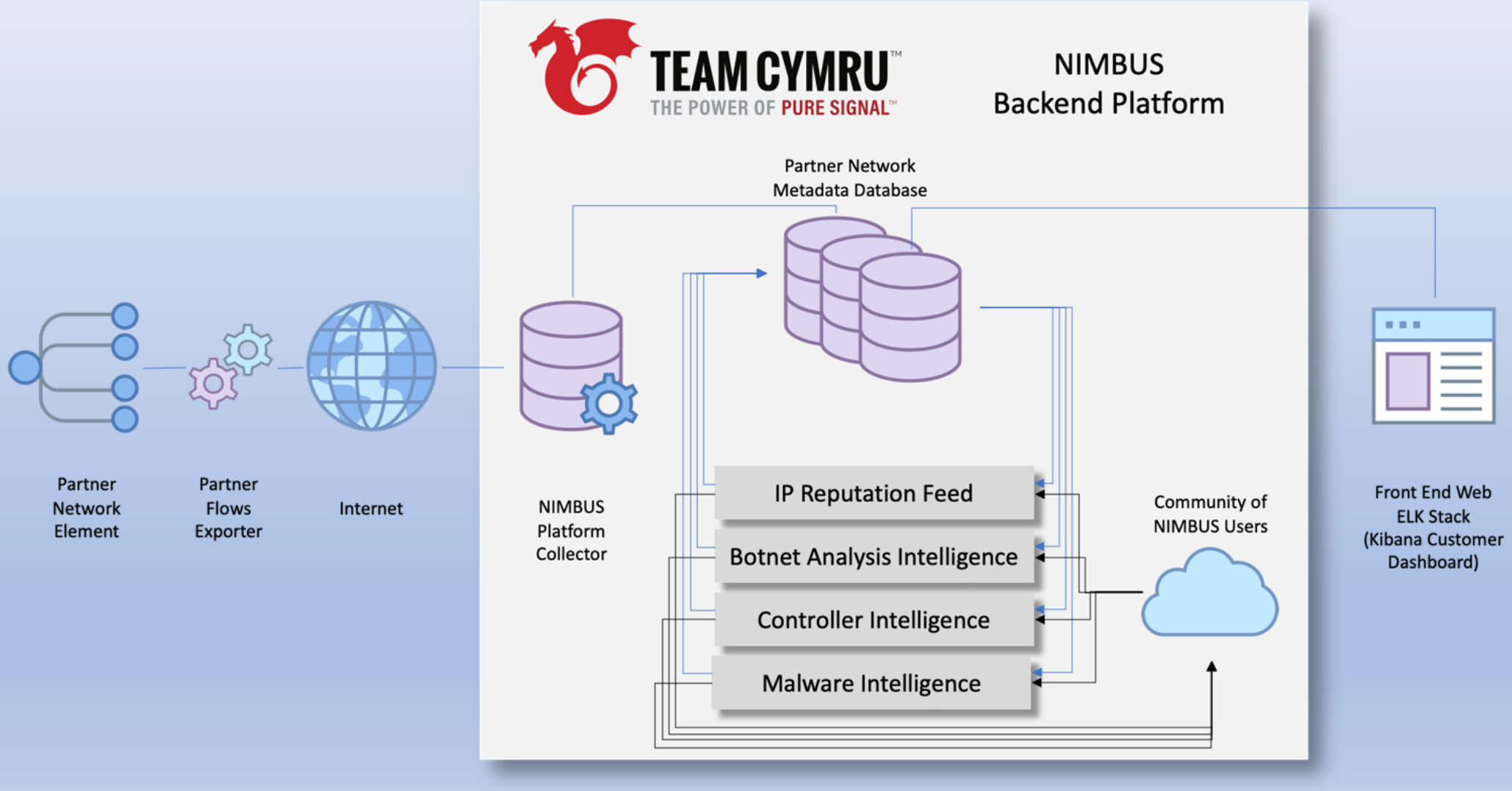
3. Conclusões e Perspectivas Futuras

NIMBUS – Monitor de Ameaças

O que é o Team Cymru Nimbus ?

- **Solução , <u>sem custos para parceiros</u>** , baseado em cloud para a análise e monitoramento de ameaças.
- Baseado em Kibana + ElasticSearch.
- Dados de reputação + O que você vê em SUA REDE (contextualizados com SEUS FLOWS).
- Externo e pró-ativo para apoiar a reação interna as ameaças.
- Dashboards para análise de tendências de tráfego, para oportunidades de peering.

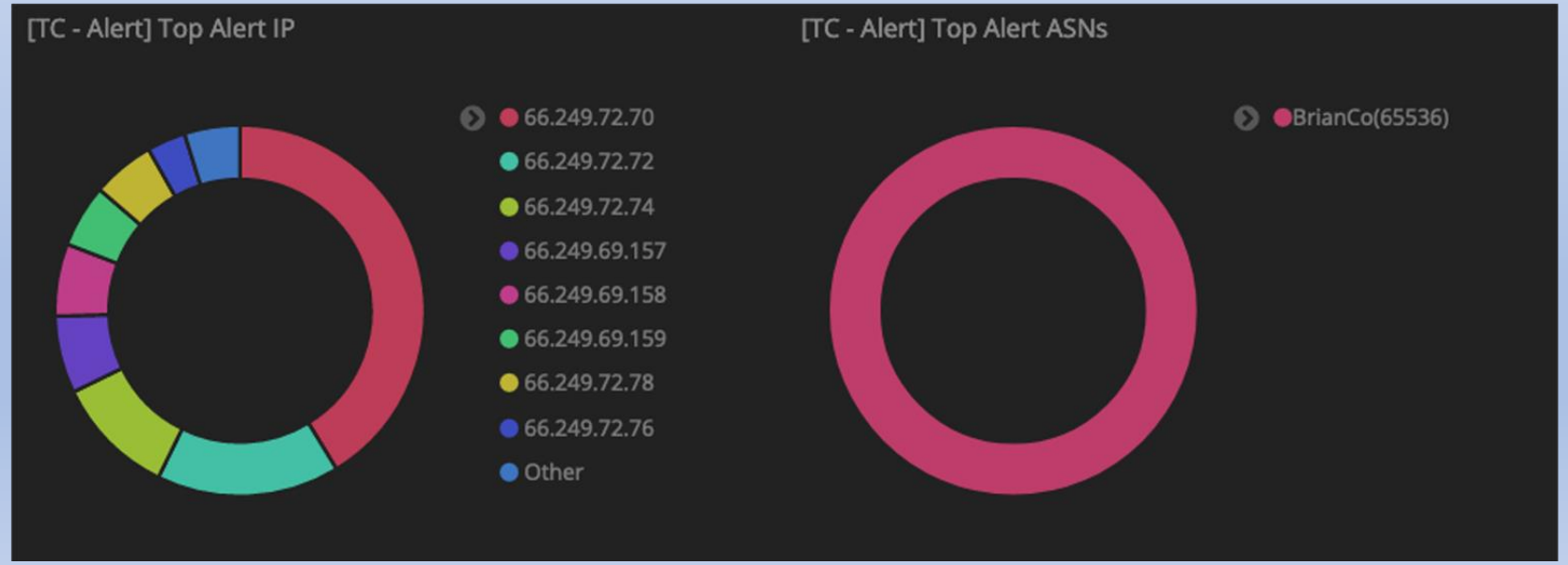
NIMBUS – Monitor de Ameaças - Arquitetura



NIMBUS – Monitor de Ameaças - Alertas

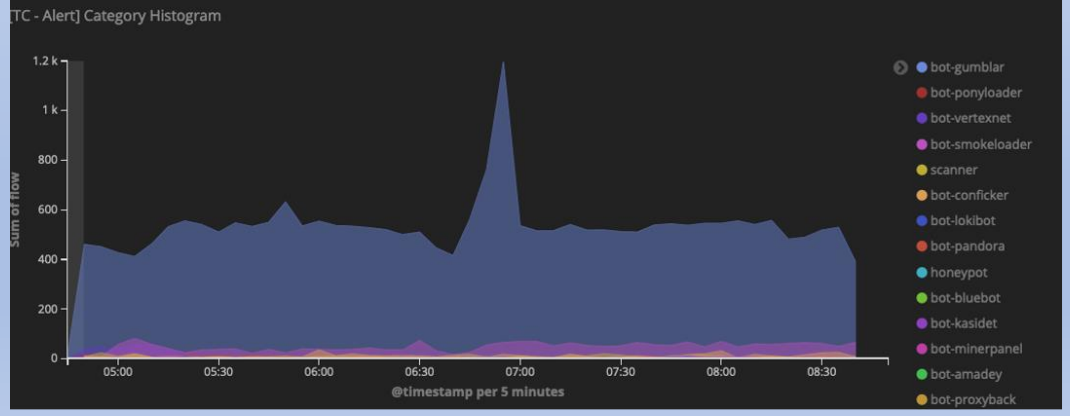
Observe as ameaças de SUA REDE

- Observe as ameaças globais , em sua rede !
- Detecção em tráfego malicioso “*Near real-time”*, categorizado, contextualizado e filtrável



NIMBUS – Monitor de Ameaças - Alertas

alert_signature: Descending	Sum of flow	Sum of bytes	Sum of pkts
bot-gumblar	25.187 k	5.869GB	3.805 m
bot-smokeloader	2.27 k	240.279MB	121.789 k
bot-conficker	553	280.31MB	220.132 k
scanner	421	28.197KB	599
bot-ponyloader	358	3.034MB	3.95 k
bot-vertexnet	306	133.275MB	79.652 k
bot-kasidet	76	57.091MB	26.485 k
bot-lokibot	72	295.552KB	663
honeypot	36	4.817KB	37
bot-amadey	18	48.864KB	161



- Filtragem simples no Kibana. Filtragem fácil (ao alcance de um clique).
- Histogramas e diversas possibilidades de filtros.
- Liste as suas ameaças ativas
- Eventos podem ser exportados via API/JSON

Como fazer parte ?

REQUISITOS

- **Ser um sistema autônomo na internet (ASN).**
- **Firmar o NDA, realizado entre você e o Team Cymru para a confidencialidade.**
- **Envio de metadados (Netflow v5/v7/v9, IPFIX, sflow, jflow e NetStream)**

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

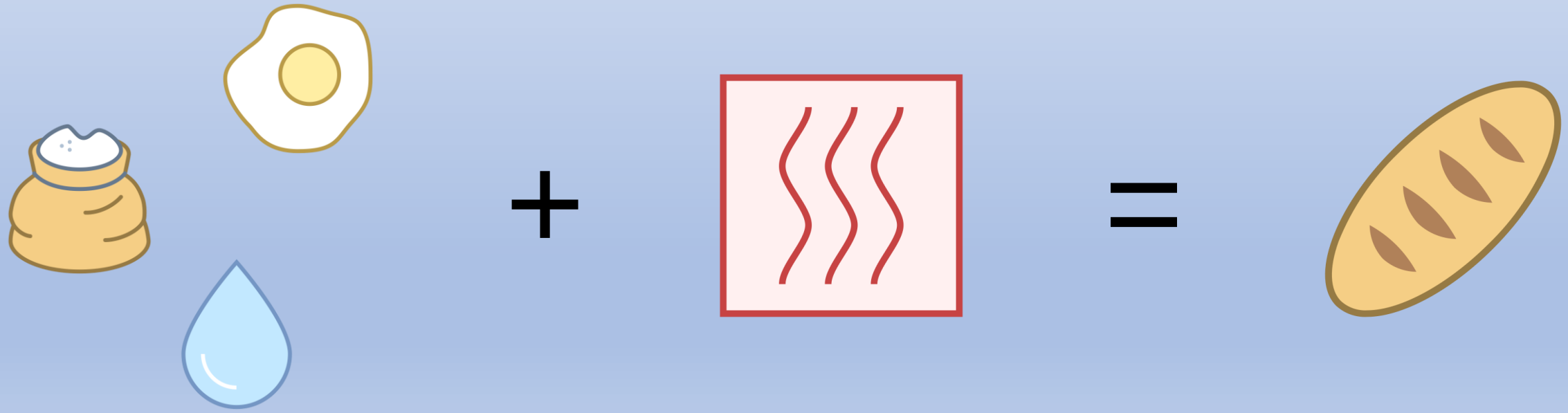
https://team-cymru.com/nimbus-contact-form/

NIMBUS – Monitor de Ameaças - Hands On

Hands on time ! Vamos ver a solução na prática !

E VERIFICAR ATIVIDADE IPv4 / IPv6 de algumas Botnets

https://team-cymru.com/wp-content/uploads/2021/08/NImbus-datasheet-2-PUBLIC.pdf



Agenda

1. Introdução

2. TC Nimbus - Estudo de Caso / ITS AS28186
"Caçando Atividade de Botnets em IPv4 e IPv6"

3. Conclusões e Perspectivas Futuras

Conclusões e Perspectivas Futuras

- **OBJETIVO: Criar conhecimento contextual de segurança cibernética a partir de metadados do tráfego.**

- **OBJETIVO: Obter conhecimento mais profundo para um controle aprimorado sobre o tráfego de sua rede.**

- **ROADMAP: Dashboards táticos oportunos e focados para lidar com ameaças específicas, entregues à sua instância pelo Team Cymru (Sob atualização constante) .**

Quando utilizado para este fim, o NIMBUS alcança grande eficiência com metadados (IPFIX) na classificação e análise de eventos

Conclusões e Perspectivas Futuras

Venha fazer parte

- ✓ **Detecção de ameaças cibernéticas quase em tempo real, contextualizados pelos dados de reputação de IP mais abrangentes do mundo.**
- ✓ **Mais de 7.000.000 (e em constante expansão) indicadores atualizados de hora em hora**
- ✓ **Filtragem personalizada para isolar atividades maliciosas por tipo, intervalos de endereços e muito, muito mais**
- ✓ **Atualmente 18 filtros de alerta (E em constante atualização)**
- ✓ **31 filtros de estatísticas de rede (E em constante atualização)**
- ✓ **Dashboard Kibana® totalmente personalizável – Com 10 Dashboards padrão e podendo ser personalizado por você !**

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

https://team-cymru.com/wp-content/uploads/2021/08/NImbus-datasheet-2-PUBLIC.pdf

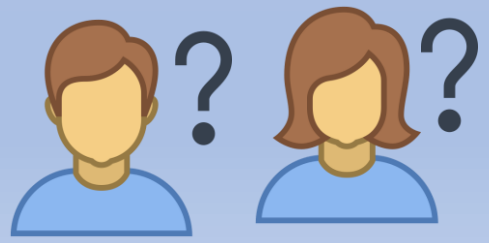
https://team-cymru.com/nimbus-contact-form/

Obrigado ITS, Team Cymru, Lacnic

MUITO OBRIGADO

FRANCISCO JOSÉ BADARÓ VALENTE NETO

fjbvneto@gmail.com ; francisco@itsbrasil.net



Q&A

SLIDES EXTRAS

Como encontramos ameaças globais ?

- Algoritmos proprietários, mas…
  - Analisando milhões de amostras de malware por dia
  - Captação de diversos sinais globalmente
  - Identificando bots em botnets e conexões com controladores
  - Executando e analisando honeypots, sinkholes e darknets
- Cada membro do Nimbus adiciona mais diversidade a dados sobre malware.
  - A comunidade de operadores usuários proporciona ajuda mútua, com o Team Cymru como parceiro.
- Com o Team Cymru, sua defesa é formada pela perspectiva global e contextualizada de ameaças.

NIMBUS – Monitor de Ameaças - Reputation Key + Score. Slide Extra

Key	Name	Description	Values
A	Days in Feed	Number of the distinct days in which the IP appeared in the feed over the past 30 days.	1-30
B	Count of Active Detections	Number of active category detections observed in the last 30 days for the given IP.	0-10000
C	Count of Passive Detections	Number of passive category detections observed in the last 30 days for the given IP.	0-10000
D	Detection Type	The detection method, as described in the next section below.	0-8
E	SSL Usage	Boolean value indicating if SSL usage was detected for the controller IP address at the time of the event.	0-1
F	Controller Instruction Decoded	Boolean value indicating if decoded instructions were available for the controller IP address at the time of the event.	0-1
G	DDoS Command Observed	Boolean value indicating if the controller IP address was associated with DDoS activity at any point in the last 30 days.	0-1
H	Non-Standard Port	Boolean value indicating if the controller or phishing IP address was using a non-standard port for the particular event. A non-standard port is any port other than: 80, 8080, 443, 6667, 6668, 6669, or 6697.	0-1
I	Number of Unique Domain Names on Same IP	Number of the distinct domains hosted on the same IP address. Value is used to identify shared hosting environments and can be used to adjust the reputation score for bots connecting to a controller operating on a shared hosting's environment on a standard port.	0-10000
J	Number of Distinct Controllers on Same IP	Number of distinct controllers or phishing instances hosted on the same IP address.	0-10000
K	Other Malicious Controller/Phishing IPs in Same /24	Number of other controllers and phishing instances hosted in the same /24.	0-256

Key	Description	Equation	Max Points	Points	Score
A31	31 days in feed in the last 30 days	(31/30) X 100	Max value for key is 100	+ 100.00	100.00
B12	12 active detections in the last 30 days	(12/1000) X 100	Max value for key is 100	+ 1.20	101.20
C211	211 passive detections in the last 30 days	(211/10000) X 100	Max value for key is 100	+ 2.11	103.31
	Score decay is applied ?			- 5.77	97.54
D0	Detection type	Not Found	Max value for key is 20	+ 0.00	97.54
E0	No SSL usage detected	0 X 2	Max value for key is 2	+ 0.00	97.54
F0	No controller instructions decoded	0 X 2	Max value for key is 2	+ 0.00	97.54
G0	No DDoS commands given in the last 30 days	0 X 2	Max value for key is 2	+ 0.00	97.54
H0	Standard port used	0 X 4	Max value for key is 4	+ 0.00	97.54
K0	0 other controller/phishing IPs in the same /24	One point per IP	Max value for key is 50	+ 0.00	97.54
J0	0 controllers on the same IP	(0 X 97.54 X .10)	Max value for key is 50	+ 0.00	97.54
I0	0 shared hosting sites on the same IP after subtracting 0 known controllers	Less than 500 shared hosting sites after subtracting controllers	Max value for key is 25	- 0.00	97.54
				Score:	98

https://reputation.team-cymru.com/

https://ipscore.team-cymru.com/

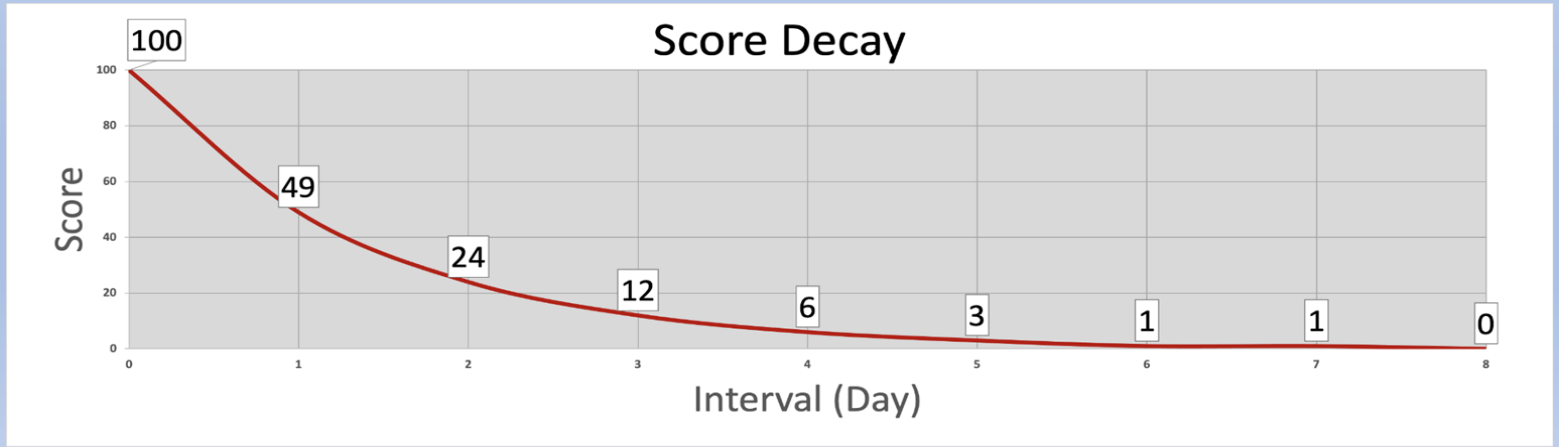
NIMBUS – Monitor de Ameaças – Decaimento do Score – Slide Extra

Explicação

O decaimento do score usa o número de minutos desde que a ameaça foi detectada pela última vez, com 0,9995 como base constante. A 'pontuação de pré-decaimento' é então multiplicada por este número.

Equação Base

Decaimento do Score == (0.9995 ^(Número de minutos desde a última detecção)) * Score de Pré-Decaimento)



Proposta de Verificação em outros mecanismos

https:/ /www.virustotal.com/
https://www.hybrid-analysis.com/
https://reputation.team-cymru.com/
https://ipscore.team-cymru.com/

MAIS INFORMAÇÕES SOBRE LISTAS DE BLOQUEIO E MECANISMOS DE CONSULTA DE REPUTAÇÃO:

https://www.linkedin.com/pulse/blocking-lists-blacklistsdenylists-ip-reputation-badar%25C3%25B3-valente-neto/

https://www.linkedin.com/pulse/listas-de-bloqueio-blacklistsblocklist-e-consulta-ip-francisco-jos%25C3%25A9/