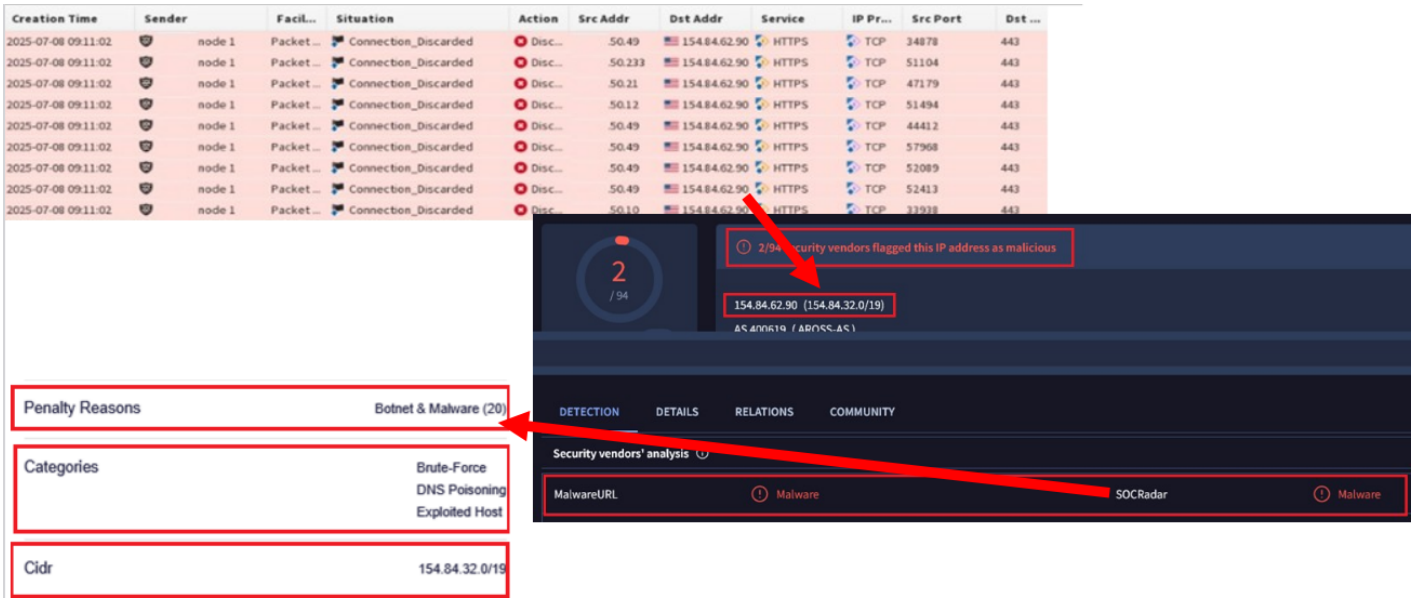
Juntando o quebra cabeças e entendendo a anatomia

Cruzamento do endereço IP suspeito, identificado como maior gerador de conexões, com as informações de inteligência da plataforma https://virustotal.com e o desenvolvimento de pensamento analítico sobre os ativos que compõe o cenário.

> **Análise de reputação do endereço IP identificado:**

VirusTotal confirmou a ligação da reputação desse CIDR do endereços IP com casos de malware, incluindo domínio maliciosos que estes IPs já foram vinculados, e através de informações indexadas em uma terceira plataforma de inteligência, apontada nos indicadores, que ao ser consultada detalhou ainda mais, como sendo um "malware" ligado a uma "Botnet".



Date resolved	Detections	Resolver	Domain
2025-05-05	1 / 94	Georgia Institute of Technology	fast-audit.com
2025-05-05	12 / 94	Georgia Institute of Technology	xzsuyuan.com
2025-05-05	1 / 94	Georgia Institute of Technology	yinpf.com
2025-05-05	1 / 94	Georgia Institute of Technology	qikankt.com
2025-05-05	1 / 94	VirusTotal	cd228.com
2025-05-05	1 / 94	Georgia Institute of Technology	k-2-i.com
2025-05-05	4 / 94	Georgia Institute of Technology	0774hz.com
2025-05-05	4 / 94	Georgia Institute of Technology	cqmilaoshu.com
2025-05-05	1 / 94	Georgia Institute of Technology	moz-kamen.com
2025-05-05	1 / 94	Georgia Institute of Technology	xckpdn.com

> **Que tipo de dispositivo da rede originou tais requisições e quais as características sistêmicas desse dispositivo?**

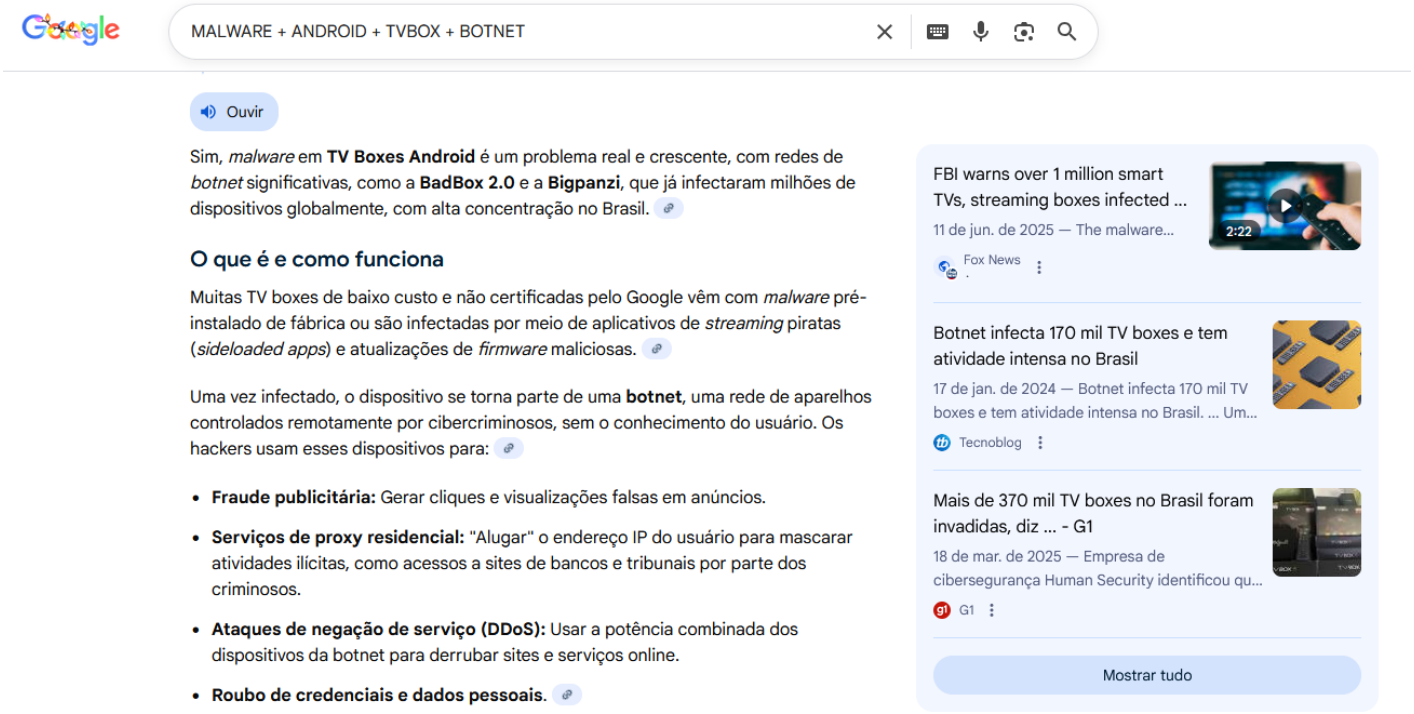
Dispositivo identificado, conforme a gestão de ativos, incluindo sua localização, como uma TvBox MXQ-PRO 4K, confirmado de forma presencial e visual. O dispositivo possui sistema operacional Android na versão 10.1.

> **Com o conjunto de informações que temos até aqui, existe algo em fontes abertas que pode refinar ainda mais nossa detecção?**

Recapitulando através de palavras-chave, quais as informações que temos até aqui?

MALWARE + ANDROID + TVBOX + BOTNET

O que podemos fazer com estas palavras-chave? Busca em fontes abertas na internet, como por exemplo o próprio buscado do Google, e.... **INFORMAÇÕES VALIOSAS!**



Com as informações obtidas em fontes abertas, foi possível identificar precisamente que o modelo da TvBox que estamos analisando, e confirmar que ele possui ligação com a Botnet "ANDROID BADBOX 2.0", pois pertencia a um grupo de dispositivos sabidamente comprometidos, com estudo detalhado por pesquisadores de segurança da informação:

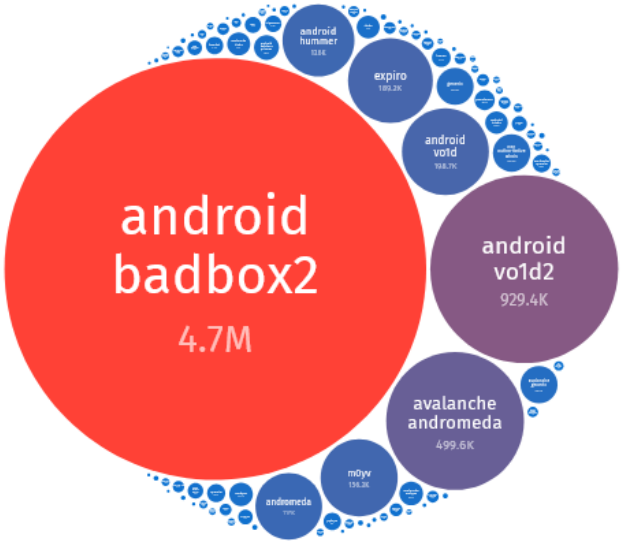
https://www.bleepingcomputer.com/news/security/badbox-malware-disrupted-on-500k-infected-android-devices/

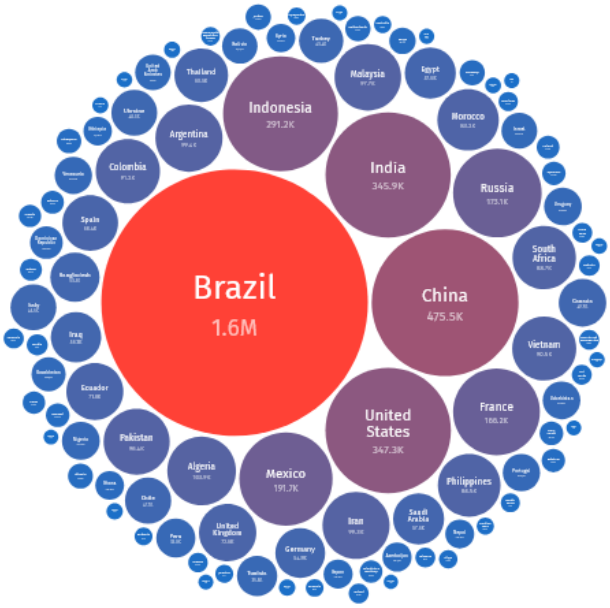
https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/

Device Model	Device Model	Device Model	Device Model
TV98	X96Q_Max_P	Q96L2	X96Q2
X96mini	S168	ums512_1h10_Natv	X96_S400
X96mini_RP	TX3mini	HY-001	MX10PRO
X96mini_Plus1	LongTV_GN7501E	Xtv77	NETBOX_B68
X96Q_PR01	AV-M9	ADT-3	OCBN
X96MATE_PLUS	KM1	X96Q_PRO	Projector_T6P
X96QPRO-TM	sp7731e_1h10_native	M8SPROW	TV008
X96Mini_5G	Q96MAX	Orbsmart_TR43	Z6
TVBOX	Smart	KM9PRO	A15
Transpeed	KM7	iSinbox	I96
SMART_TV	Fujicom-Smart	MXQ9PRO	MBOX
X96Q	[illegible]box	Mbox	R11
[illegible]	KM6	X96Max_Plus2	TV007
Q9 Stick	SP7731E	H6	X88
X98K	TXCZ		

Fonte: https://www.bleepingcomputer.com

- **Reforçando as informações colhidas - Estatística de dispositivos infectados por esta Botnet - Geral e por Países:**





Fonte: https://dashboard.shadowserver.org

Brasil liderando o número de infecções globais.

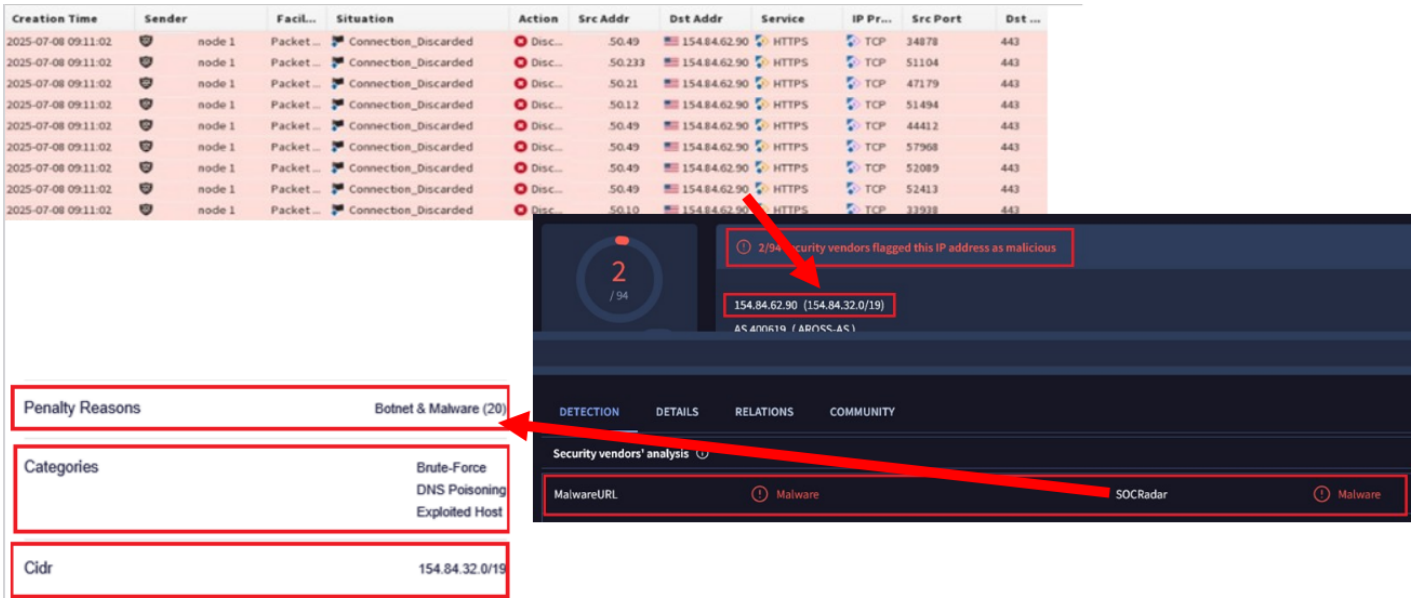
Como este dispositivo pode operar de maneira maliciosa para comprometer a infraestrutura onde estava inserido?

-

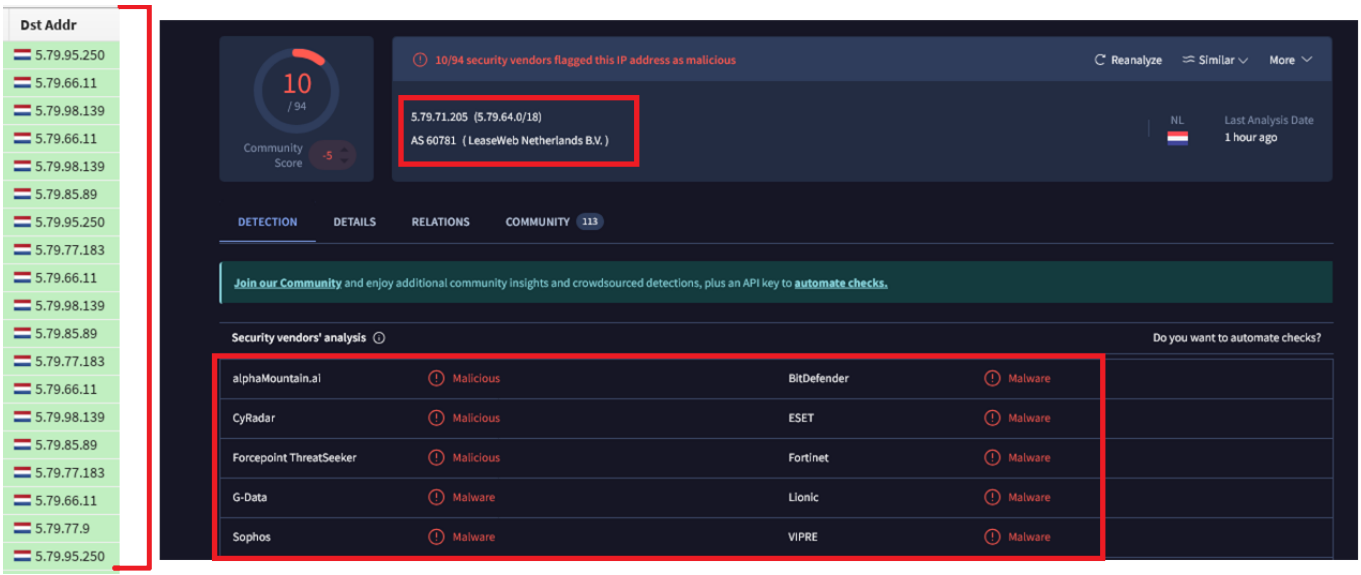
> **Indicadores de EVASÃO de defesas detectados:**

- **Durante a detecção e contenção, pode haver a alteração dos Indicadores de Comprometimento (IoC) de rede que identiicam o servidor de Comando e controle do Malware (Ip, geolocalização, ASN, Domínios, etc), como no exemplo abaixo, mas não se limitando apenas a estes:**

DE:



PARA:



- **Uso de um único dispositivo, com permissionamento excessivo, para se deslocar lateralmente na rede interna, utilizando protocolos autorizados para mascaramento e não despertar alertas/suspeitas.**
  - Dispositivos TvBox podem ser conectadas a um servidor de conteúdo para apresentação de propagandas ou conteúdos internos, nesse cenário, os dispositivos comprometidos, mantém o envio das requisições ao servidor de conteúdo que originalmente teriam permissão, mascarando o tráfego sobre

protocolos legítimo, porém, se comparado com o tráfego legítimo, tem quantidades anormais de conexões.
    - Este host interno (servidor de conteúdo), teria um cenário de vulnerabilidades em aplicações, serviços, e permissões excessivas no acesso à rede privilegiada, que permitiriam aos dispositivos maliciosos executar comandos através dele e a partir daí analisar e comprometer outros dispositivos da infraestrutura em outras redes internas (técnica de pivoting).

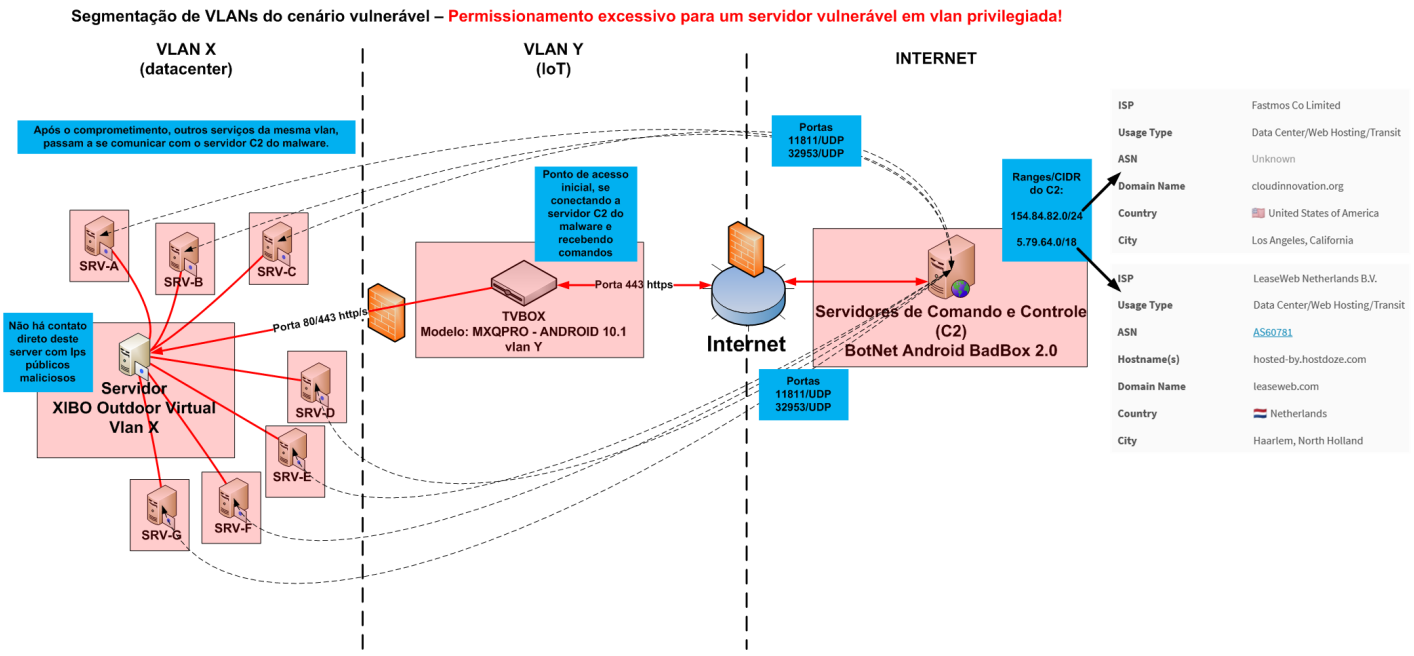
Tráfego TVBox > servidor TvBox XIBO

- **Indicadores de COMPROMETIMENTO do ambiente detectados:**
    - Em mais uma ação de evasão, horas após os primeiros indícios no ambiente analisando em *timeline*, é possível observar que para não ser detectado, o malware evitaria o tráfego para outras sub-redes, que seria inspecionado pelo firewall, comprometendo hosts/serviços da mesma sub-rede onde está inserido, possivelmente explorando vulnerabilidades de serviços desatualizados nos hosts, com comandos ordenados pelo servidor de comando e controle (C2) externo do malware, através dos dispositivos TvBox locais comprometidos, usando seu servidor legítimo local de conteúdos como pivoting para chegar a hosts da rede onde este servidor está inserido.
    - Nesse cenário de exploração interna, o tráfego ocorreu de host para host de uma mesma sub-rede, sem troca de rede e posteriormente outros hosts da mesma sub-rede passam a tentar se conectar com servidor de comando e controle de malware, externamente, sendo aqui um ponto de detecção.

Action	Src Addr	Dst Addr	Service	IP Pr...	Src P...	Dst P...
Allow	.50.3	154.84.62.128	HTTPS	TCP	40972	443
Allow	.50.64	154.84.62.128	HTTPS	TCP	33374	443
Allow	.50.233	154.84.62.128	HTTPS	TCP	34872	443
Allow	.50.24	154.84.62.128	HTTPS	TCP	41928	443
Allow	.50.53	154.84.62.128	HTTPS	TCP	40762	443
Allow	.50.21	154.84.62.128	HTTPS	TCP	36608	443
Allow	.50.44	154.84.62.128	HTTPS	TCP	37128	443
Allow	.50.12	154.84.62.128	HTTPS	TCP	37630	443
Allow	.50.49	154.84.62.128	HTTPS	TCP	35614	443
Allow	.50.51	154.84.62.128	HTTPS	TCP	60364	443
Allow	.50.10	154.84.62.128	HTTPS	TCP	53008	443
Allow	.50.38	154.84.62.128	HTTPS	TCP	54368	443
Allow	.50.20	154.84.62.128	HTTPS	TCP	55804	443
Allow	.50.3	154.84.62.90	HTTPS	TCP	54336	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40382	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40392	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40384	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40400	443
Allow	.50.3	154.84.62.90	HTTPS	TCP	54338	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40416	443
Allow	.50.3	154.84.62.90	HTTPS	TCP	54340	443
Allow	.50.3	154.84.62.90	HTTPS	TCP	54342	443
Allow	.50.3	154.84.62.90	HTTPS	TCP	54344	443
Allow	.50.233	154.84.62.90	HTTPS	TCP	42496	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40432	443
Allow	.50.24	154.84.62.90	HTTPS	TCP	40422	443
Allow	.50.233	154.84.62.90	HTTPS	TCP	42512	443
Allow	.50.233	154.84.62.90	HTTPS	TCP	42528	443
Allow	.50.233	154.84.62.90	HTTPS	TCP	42520	443

- A detecção de explorações nesta camada de uma sub-rede / host para host, poderia ser realizada com ferramentas de *Endpoint Detection and Response* (EDRs), *eXtended Detection and Response* (XDRs) com agentes de resposta ativa, *Host-based Intrusion Prevention/Detection System* (HIDS/HIPS), que monitoram o tráfego, e os hosts dentro de uma mesma sub-rede, através de agentes de resposta ativa.

- **Representação gráfica:**



Revision #34
Created 2025-12-08 16:41:28 -03 by Ado Cardoso da Silva
Updated 2025-12-15 22:04:53 -03 by Ado Cardoso da Silva