Resposta a Incidentes em Larga Escala

Atuação da Anatel no Combate a Botnets em Dispositivos Clandestinos

29/07/2026

Brasília – DF

Quem sou eu?

Jamilson Ramos Evangelista

marido de uma linda mulher e pai de 3 princesas

engenheiro de telecomunicações (PUC-Campinas 2006)

mestre e doutor em engenharia biomédica (Unicamp 2018 e 2021)

servidor do quadro técnico da Anatel desde 2011

coordenador de fiscalização de cibersegurança e bloqueios

Base Legal (Lei nº 9.472/1997)

União organiza e fiscaliza os serviços de telecomunicações (art. 1º).

- ✓ Inclui disciplinamento da comercialização, redes e uso.

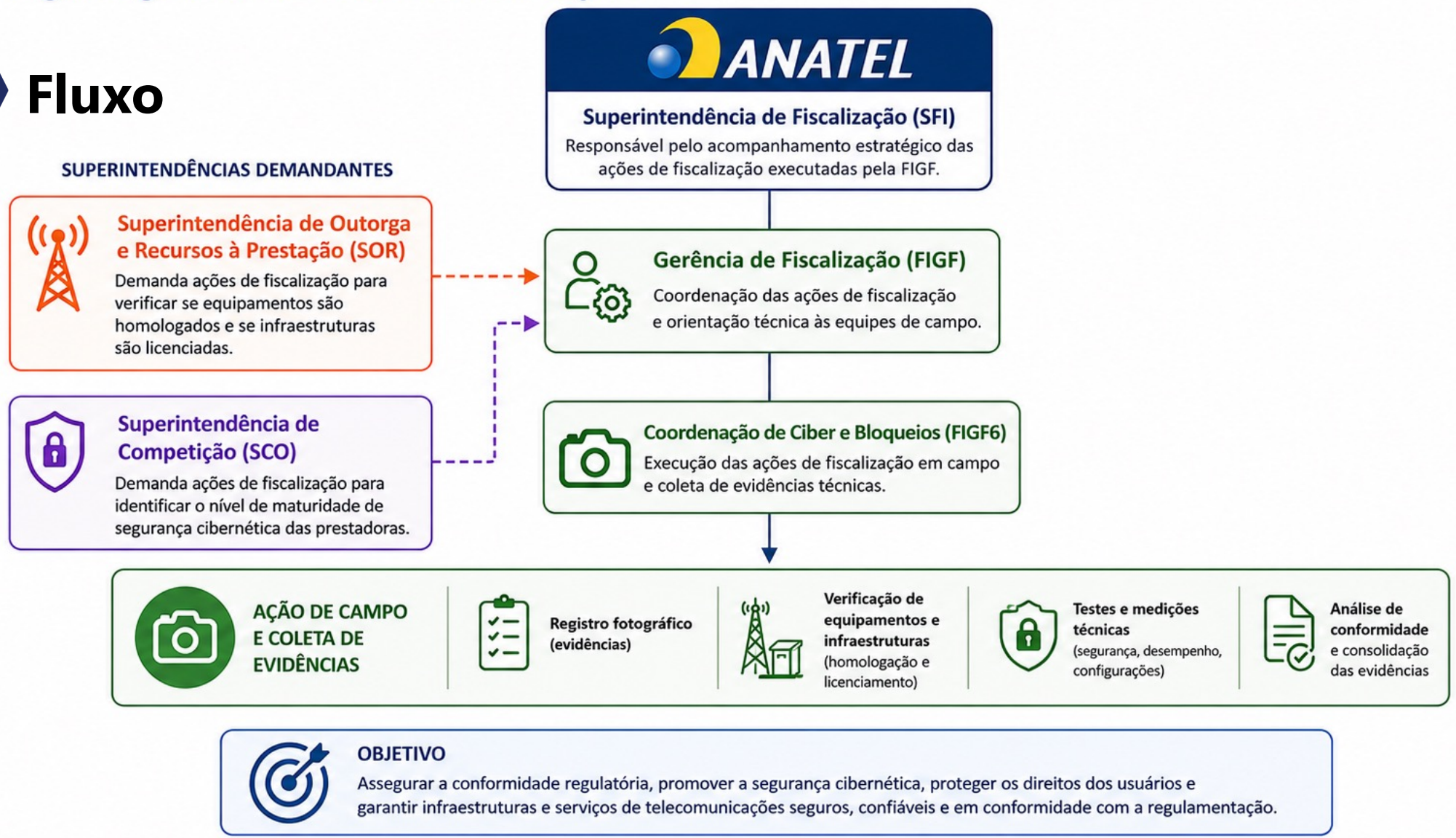
Anatel expede normas

Anatel certifica produtos de telecomunicações.

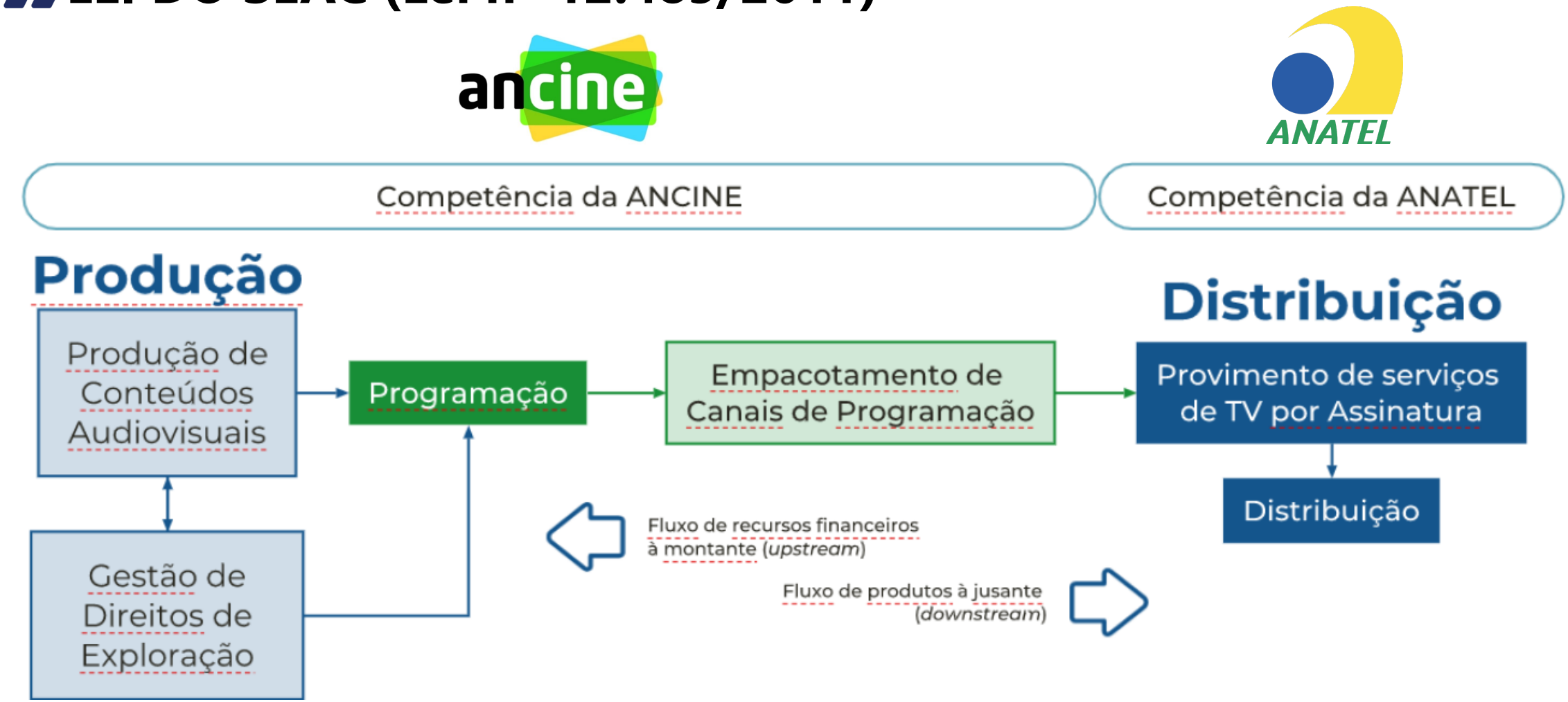
Anatel autoriza prestação de serviço.

Usuários devem utilizar adequadamente serviços e equipamentos (art. 4º).

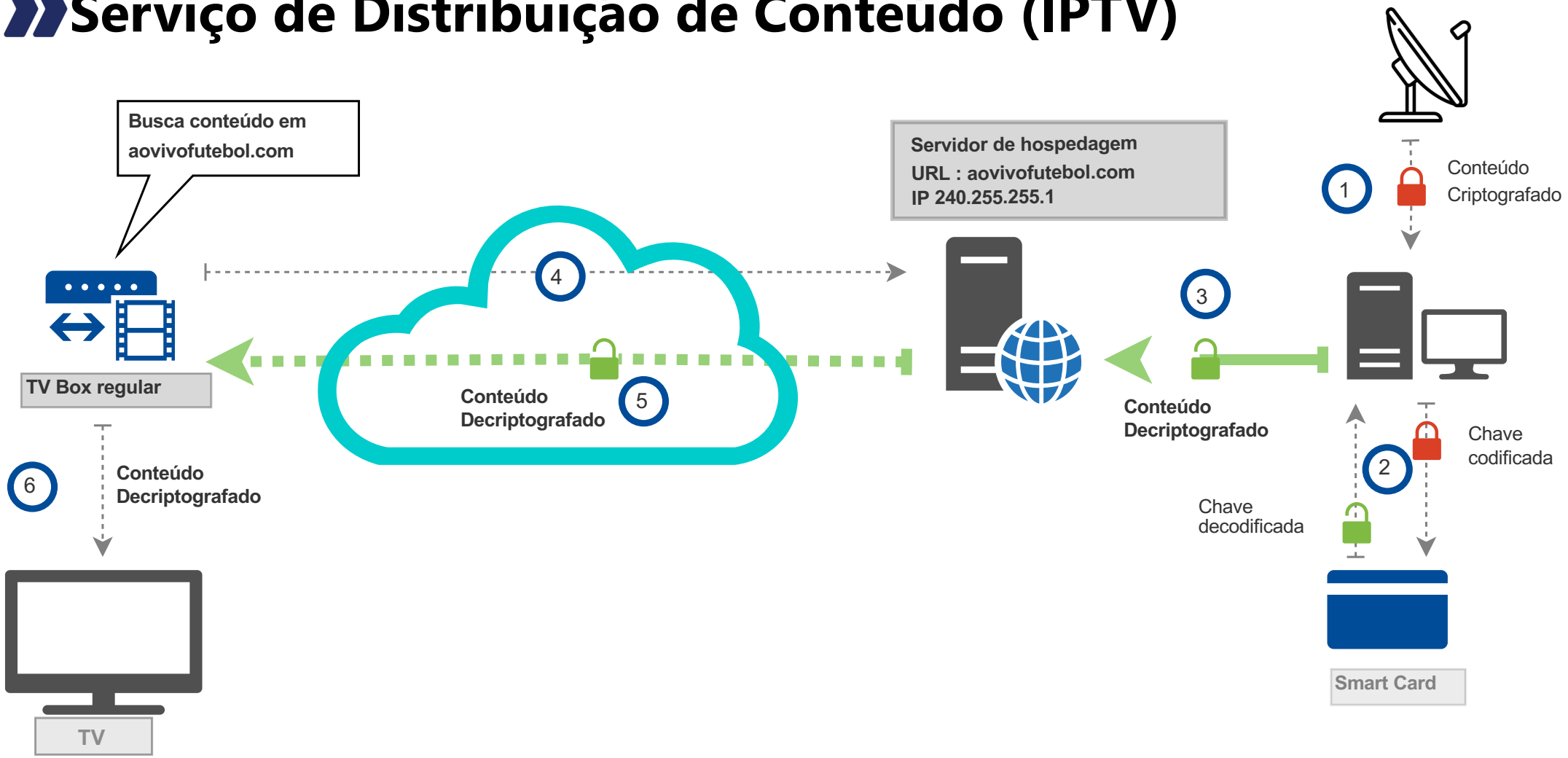
Fluxo


ANATEL
Superintendência de Fiscalização (SFI)
Responsável pelo acompanhamento estratégico das ações de fiscalização executadas pela FIGF.
SUPERINTENDÊNCIAS DEMANDANTES
Superintendência de Outorga e Recursos à Prestação (SOR)
Demanda ações de fiscalização para verificar se equipamentos são homologados e se infraestruturas são licenciadas.
Superintendência de Competição (SCO)
Demanda ações de fiscalização para identificar o nível de maturidade de segurança cibernética das prestadoras.
Gerência de Fiscalização (FIGF)
Coordenação das ações de fiscalização e orientação técnica às equipes de campo.
Coordenação de Ciber e Bloqueios (FIGF6)
Execução das ações de fiscalização em campo e coleta de evidências técnicas.
AÇÃO DE CAMPO E COLETA DE EVIDÊNCIAS
Registro fotográfico (evidências)
Verificação de equipamentos e infraestruturas (homologação e licenciamento)
Testes e medições técnicas (segurança, desempenho, configurações)
Análise de conformidade e consolidação das evidências
OBJETIVO
Assegurar a conformidade regulatória, promover a segurança cibernética, proteger os direitos dos usuários e garantir infraestruturas e serviços de telecomunicações seguros, confiáveis e em conformidade com a regulamentação.

LEI DO SEAC (Lei nº 12.485/2011)



Serviço de Distribuição de Conteúdo (IPTV)



Decodificadores Clandestinos

Fiscalização Física e Marketplace

9 Milhões
Equipamentos retirados do mercado desde 2018

Estratégia Antiga

Apreensão em comércio de rua

Estratégia Atual

Uso de **IA** para **identificar anúncios ilegais** em **marketplaces**

Parcerias com a **Receita Federal** em **Centros de Distribuição** e **Alfândega**

Foco na **desarticulação** de **grandes importadores**

TV Boxes Apreendidos
+ 1,5 milhão de unidades

Estudo GT TV Box (2021)

Botnet e malware embarcado: dispositivos se conectam automaticamente e recebem atualizações maliciosas.

Controle remoto e coleta de dados: C2 assume o dispositivo e acessa informações do usuário.

Uso em ataques cibernéticos: participação em DoS/DDoS e outras atividades maliciosas.

Risco e ilegalidade: vulnerabilidades graves, violação de direitos autorais

Estudo GT TV Box (2022)

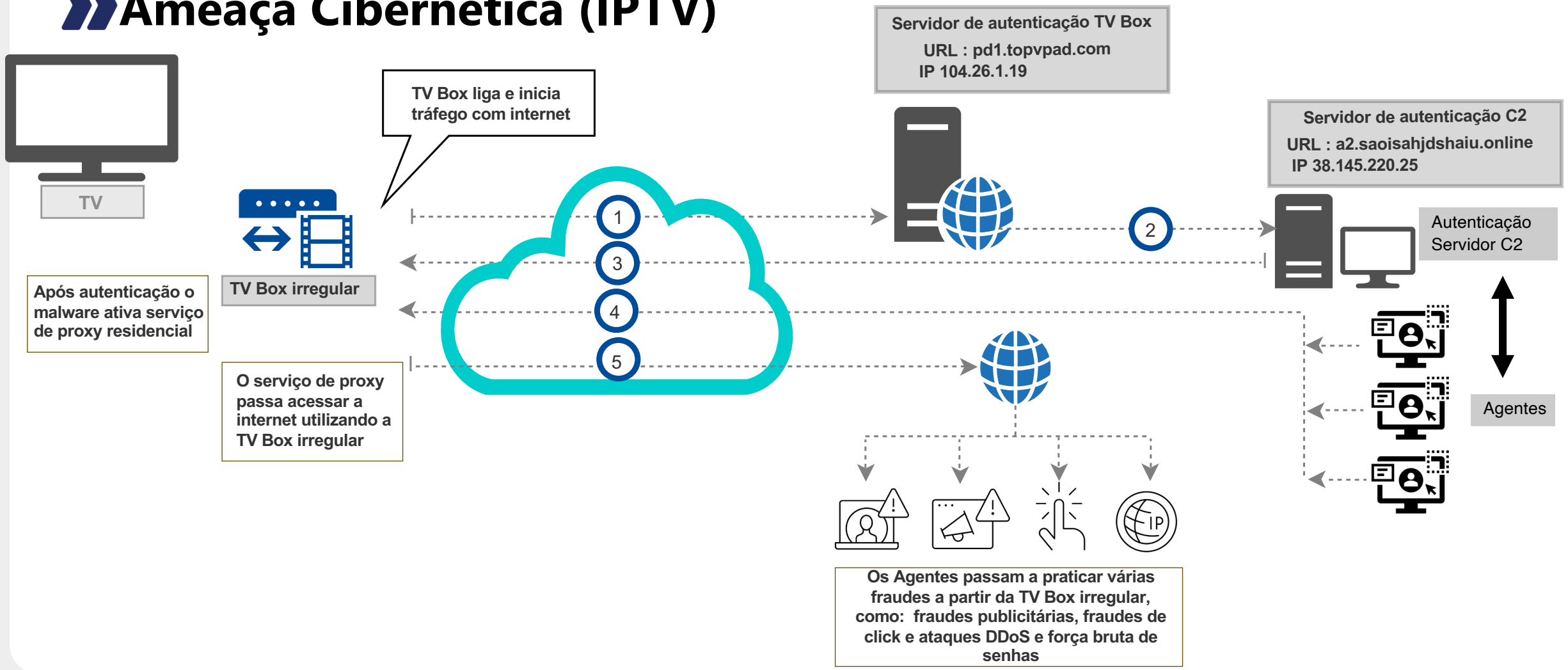
Ausência de segurança no sistema Android: dispositivos operam sem proteções essenciais.

Lojas de aplicativos não confiáveis: fora de padrões globais de segurança e sem controle adequado.

Aplicativos com indícios de malware: presença recorrente de arquivos maliciosos.

Atualizações inseguras: tráfego de atualização sem criptografia adequada, expondo o dispositivo a ataques.

Ameaça Cibernética (IPTV)



Medidas Técnicas e Regulatórias

Em 2023, a Anatel expediu o **Ato nº 9281**, criando a classificação de dispositivos denominados “*Smart TV Box*”

Requisitos de segurança cibernética

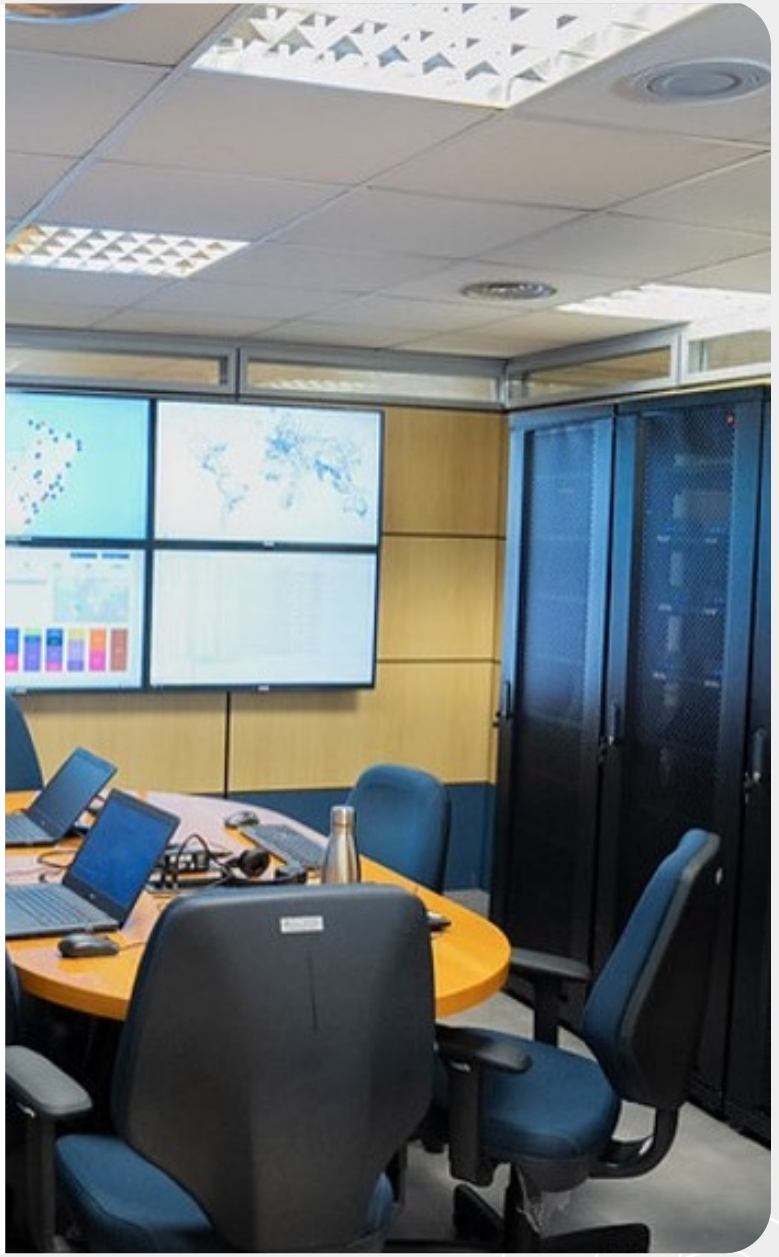
Divulgação de lista de *Smart TV Boxes* homologadas

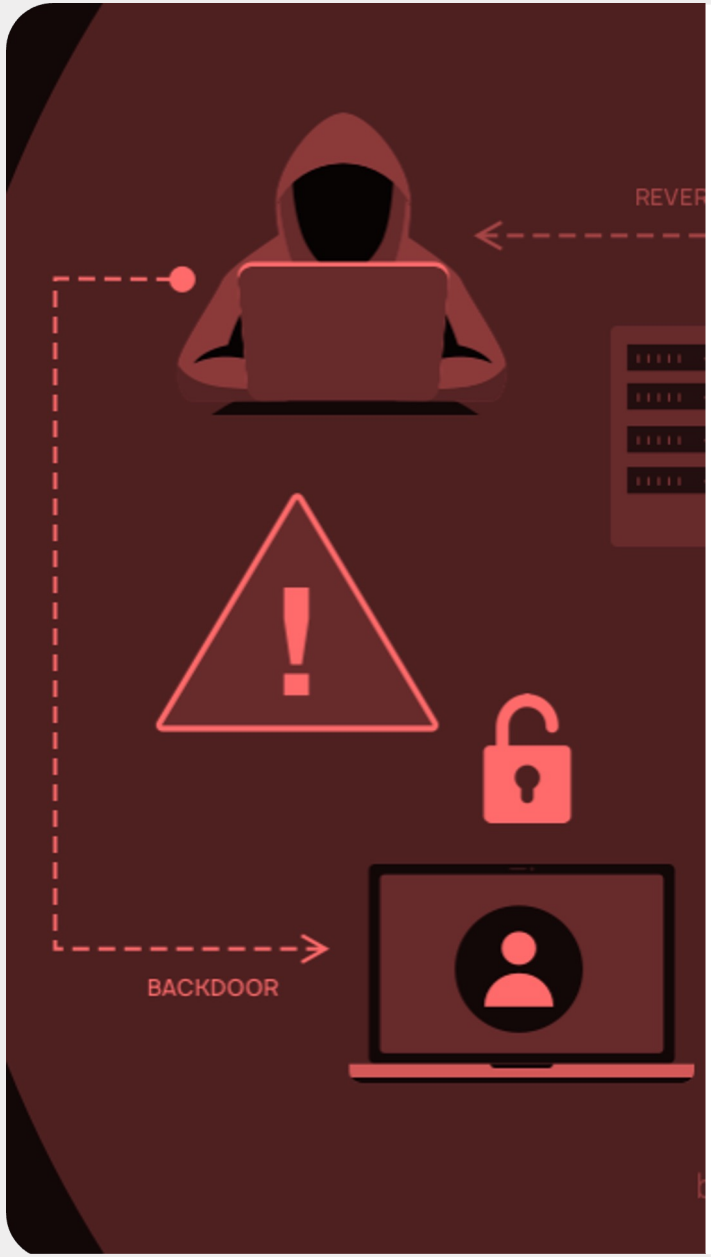
Ações de combate e cooperação

Plano de Ação contra decodificadores clandestinos (Resolução nº 189/2023)

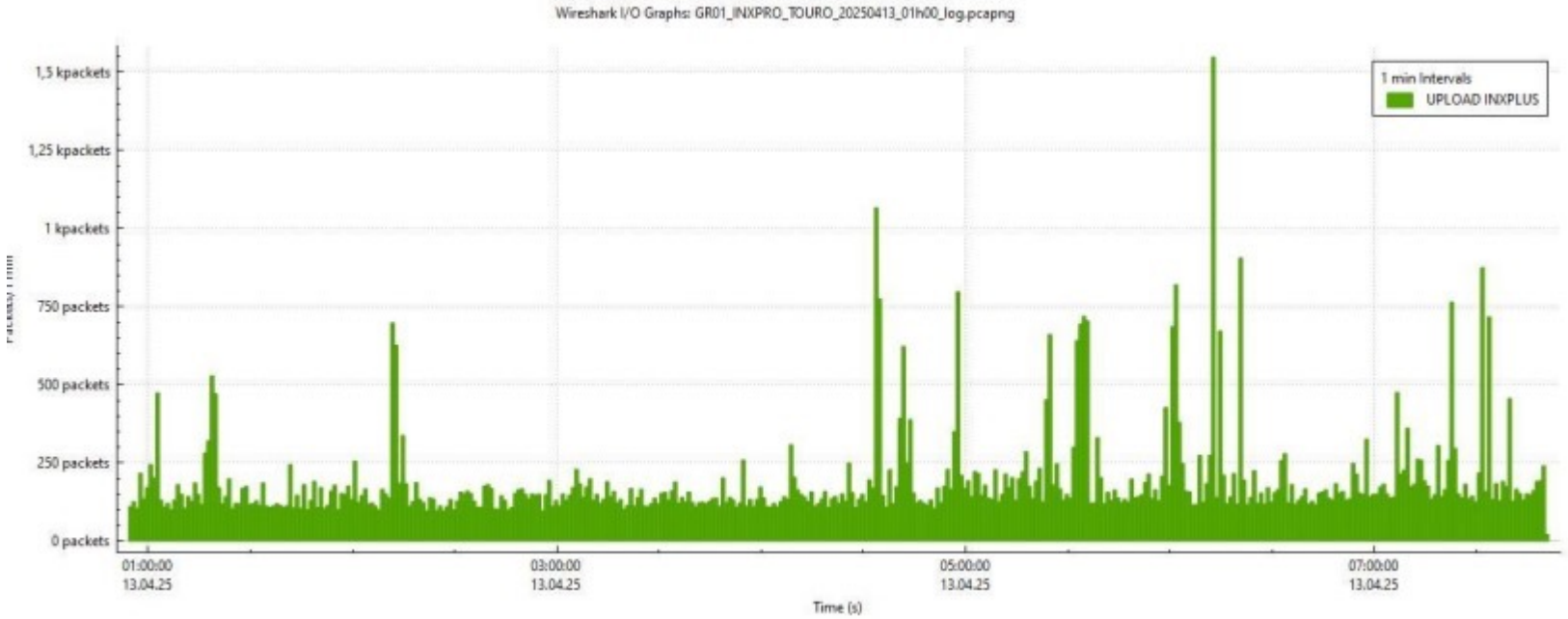
Parceria com órgãos aduaneiros e de segurança pública para apreensão

Parceria com ABTA para Laboratório Antipirataria





Estudo de caso



Comportamento anormal em dispositivos não homologados

Caracterização da Ameaça

METODOLOGIA

Análise de modelos populares e não homologados

Monitoramento de tráfego em modo *stand-by*

Engenharia **reversa** de *firmware*

Cruzamento com dados internacionais de ameaças

Caracterização da Ameaça

AMOSTRAS DE ESTUDO

NOME DO DISPOSITIVO	XPLUS	TOURO
MODELO	XPLUS_v1	TOUROBOX
PROCESSADOR	ROCKCHIP	ROCKCHIP
VERSÃO ANDROID	7.1.2	10
NÍVEL DO PATCH	5 de abril de 2017	5 de dezembro de 2019
VERSÃO DO KERNEL	3.10.104 root@ubuntu-PowerEdge-R630 #1 Fri Feb 7 09 :27 :44 CST 2025	4.9.170 #51 Fri Feb 21 16 :58 :34 CST 2025
NÚMERO DA VERSÃO	Rk322x_box-userdeug 7.1.2 XPLUS eng.root.20250207.092834 test-keys	Eros_p2-userdebug 10 QP1A.191105.004 20250221 test-keys

Caracterização da Ameaça

MONITORAMENTO

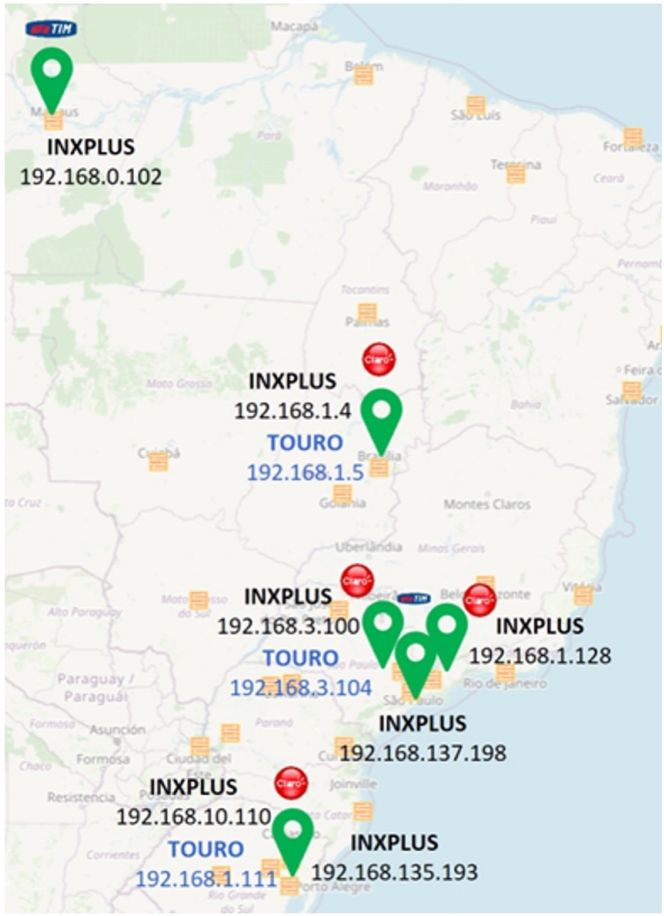
7 set-top boxes modelo InXPlus

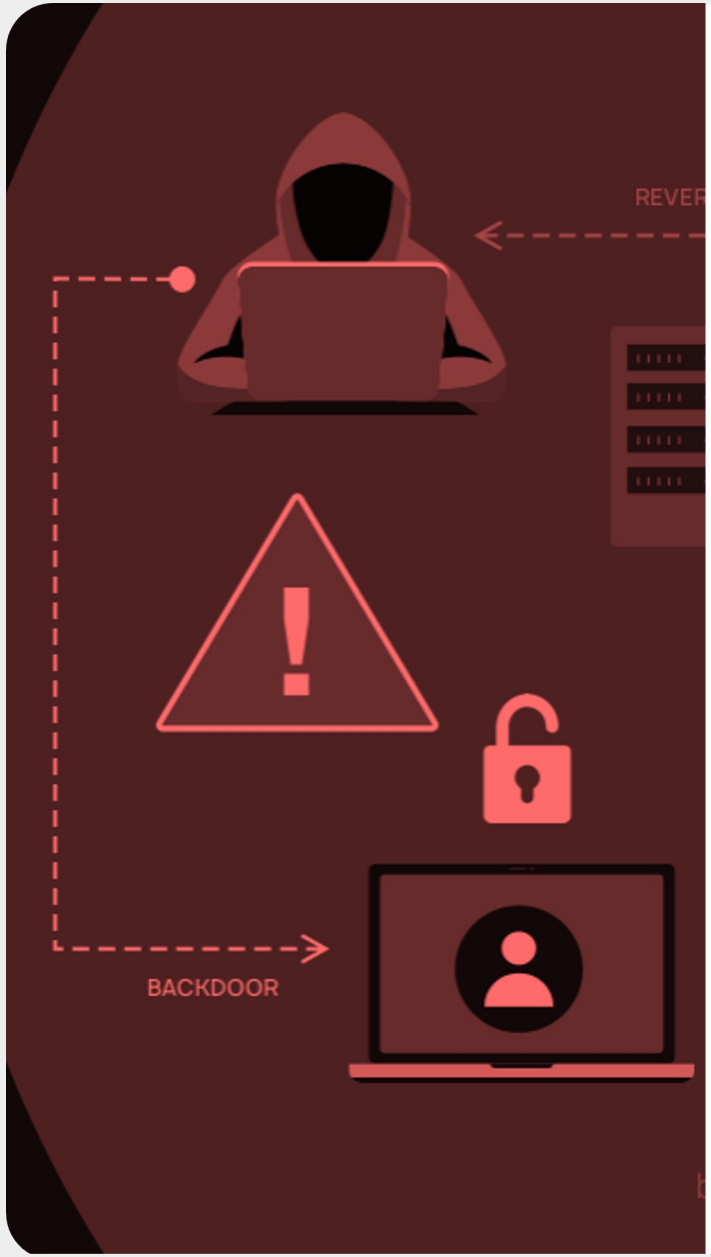
3 set-top boxes modelo TouroBox

Operadoras: TIM e Claro

Período: 8 de abril de 2025 entre às 14h00 e 16h00

Ferramenta: monitor de protocolos Wireshark



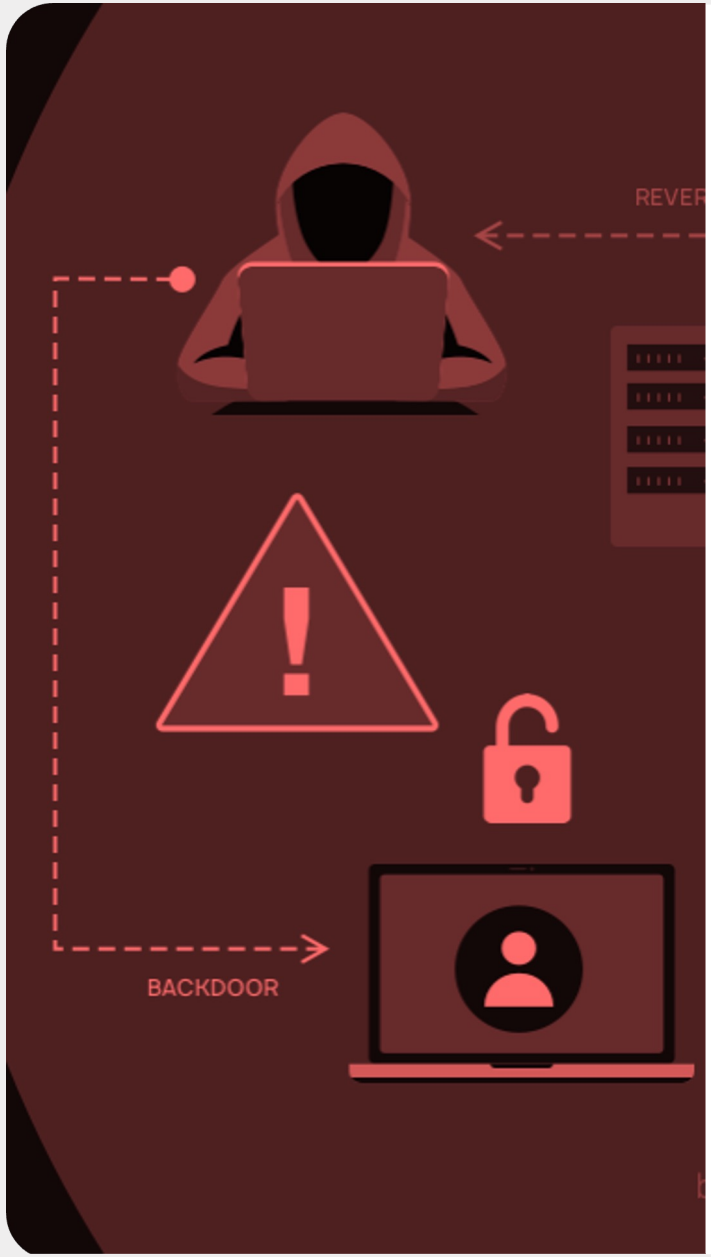


Caracterização da Ameaça

Mesmos domínios identificados pela Human Security

```
Standard query response 0xf3ba Refused A bj231211-a.bj.okamiboss.com
Standard query response 0xf3ba Refused A bj231211-a.bj.okamiboss.com
Standard query response 0xf802 Refused A bj231211-a.bj.martianinc.co
Standard query response 0xf802 Refused A bj231211-a.bj.martianinc.co
Standard query response 0xfa14 No such name A bj231211-a.bj.martianinc.co …  bindrpz.virtua.c…
Standard query response 0xfa53 Refused A bj231211-a.bj.okamiboss.com
Standard query response 0xfa53 Refused A bj231211-a.bj.okamiboss.com
Standard query response 0xfac4 A bj231211-a.bj.holadns.com A 43.135.174.111 bj231211-a.bj.ho…  43.135.174.111
Standard query response 0xfe11 Refused A bj231211-a.bj.martianinc.co
Standard query response 0xfe11 Refused A bj231211-a.bj.martianinc.co
```

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



Caracterização da Ameaça

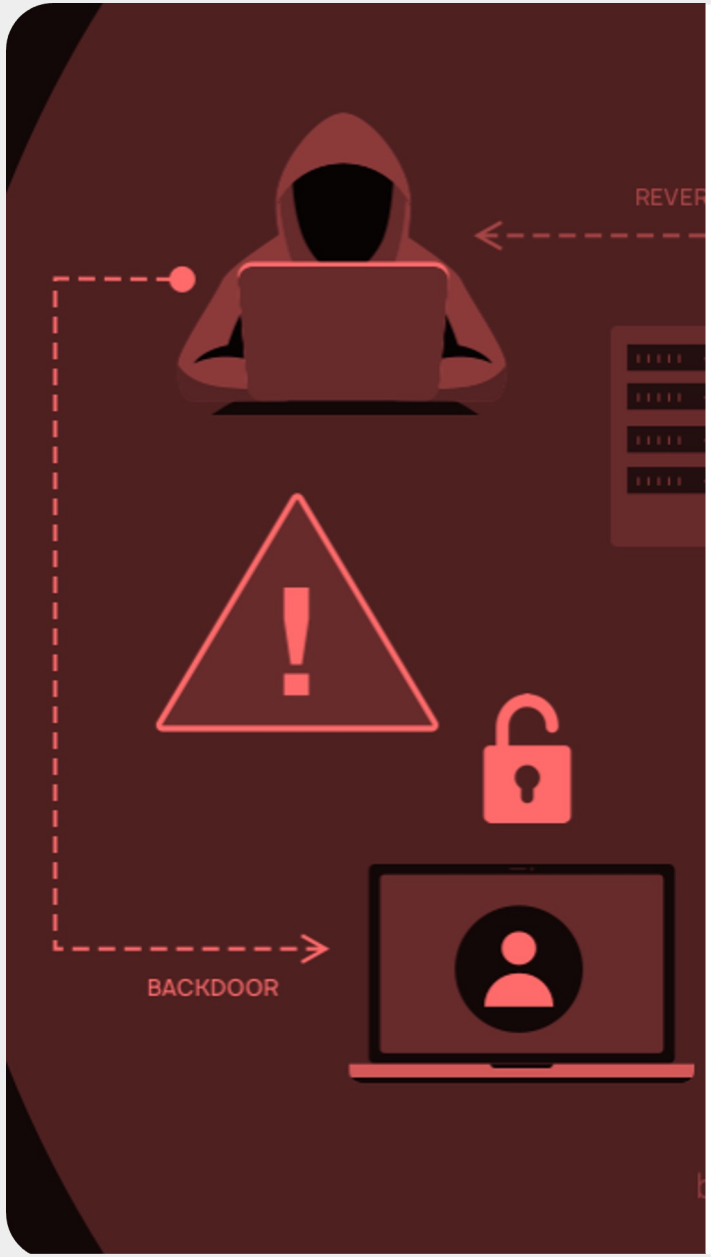
Conexão de agentes externos ao TV Box

tcp.stream eq 31

No.	Time	Source	Destination	Info
1057	2025-04-08 13:36:13,978931	192.168.3.100	43.135.174.111	34617 → 6000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=4294944854 TSecr=0 WS=64
1062	2025-04-08 13:36:14,171147	43.135.174.111	192.168.3.100	6000 → 34617 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1424 SACK_PERM TSval=452591722 TSecr=4294944854 WS=2048
1063	2025-04-08 13:36:14,172156	192.168.3.100	43.135.174.111	34617 → 6000 [ACK] Seq=1 Ack=1 Win=87616 Len=0 TSval=4294944874 TSecr=452591722
1065	2025-04-08 13:36:14,189471	192.168.3.100	43.135.174.111	34617 → 6000 [PSH, ACK] Seq=1 Ack=1 Win=87616 Len=142 TSval=4294944875 TSecr=452591722
1069	2025-04-08 13:36:14,382341	43.135.174.111	192.168.3.100	[TCP Previous segment not captured] 6000 → 34617 [FIN, ACK] Seq=259 Ack=143 Win=45056 Len=0 TSval=452591933 TSecr=4294944875
1070	2025-04-08 13:36:14,382341	43.135.174.111	192.168.3.100	6000 → 34617 [ACK] Seq=1 Ack=143 Win=45056 Len=0 TSval=452591933 TSecr=4294944875
1071	2025-04-08 13:36:14,382341	43.135.174.111	192.168.3.100	[TCP Out-Of-Order] 6000 → 34617 [PSH, ACK] Seq=1 Ack=143 Win=45056 Len=258 TSval=452591933 TSecr=4294944875
1072	2025-04-08 13:36:14,382912	192.168.3.100	43.135.174.111	[TCP Dup ACK 1063#1] 34617 → 6000 [ACK] Seq=143 Ack=1 Win=87616 Len=0 TSval=4294944895 TSecr=452591722 SLE=259 SRE=260
1073	2025-04-08 13:36:14,383327	192.168.3.100	43.135.174.111	34617 → 6000 [ACK] Seq=143 Ack=260 Win=88704 Len=0 TSval=4294944895 TSecr=452591933
1076	2025-04-08 13:36:14,395305	192.168.3.100	43.135.174.111	34617 → 6000 [FIN, ACK] Seq=143 Ack=260 Win=88704 Len=0 TSval=4294944896 TSecr=452591933
1090	2025-04-08 13:36:14,587387	43.135.174.111	192.168.3.100	6000 → 34617 [ACK] Seq=260 Ack=144 Win=45056 Len=0 TSval=452592138 TSecr=4294944896

{"os":"android","uuid":"0413BEBED66823FCBB6E190870F72259","is":"bj231211 -a","v":"v2.8.0","inf":"XPLUS#*#7.1.2#*#25#*#XPLUS#*#Android","n":"t"}
{"t":1440,"n":200,"h":10,"req_ip":"187.106.240.208","s":[" **170.106.199.84**:800,170.106.199.84:799","**107.150.105.180**:800,107.150.105.180:799","**47.85.112.181**:800,47.85.112.181:799","**43.130.169.169**:800,43.130.169.169:799"],"em":"BR-s..opaulo-itatiba-AS28573-isp"}

GR01_JR	Packets	Bytes	Total Packets	Percent Fil	Tx Packe	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
192.168.3.100	12053	2151565	187317	6.43	12053	2151565	0	0						
107.150.105.180	2961	464877	6108	48.48	0	0	2961	464877	United States	Los Angeles	340.544	-118.244	135377	UCLOUD INFORMATION TECHNOLOGY HK LIMITED
43.130.169.169	2960	464720	6935	42.68	0	0	2960	464720	United States	Ashburn	390.469	-774.903	132203	Tencent Building, Kejizhongyi Avenue
47.85.112.181	2960	464720	6025	49.13	0	0	2960	464720	United States		386.879	-772.978	45102	Alibaba US Technology Co., Ltd.
170.106.199.84	2960	464720	7213	41.04	0	0	2960	464720	United States	Santa Clara	37.353	-1.219.544	132203	Tencent Building, Kejizhongyi Avenue

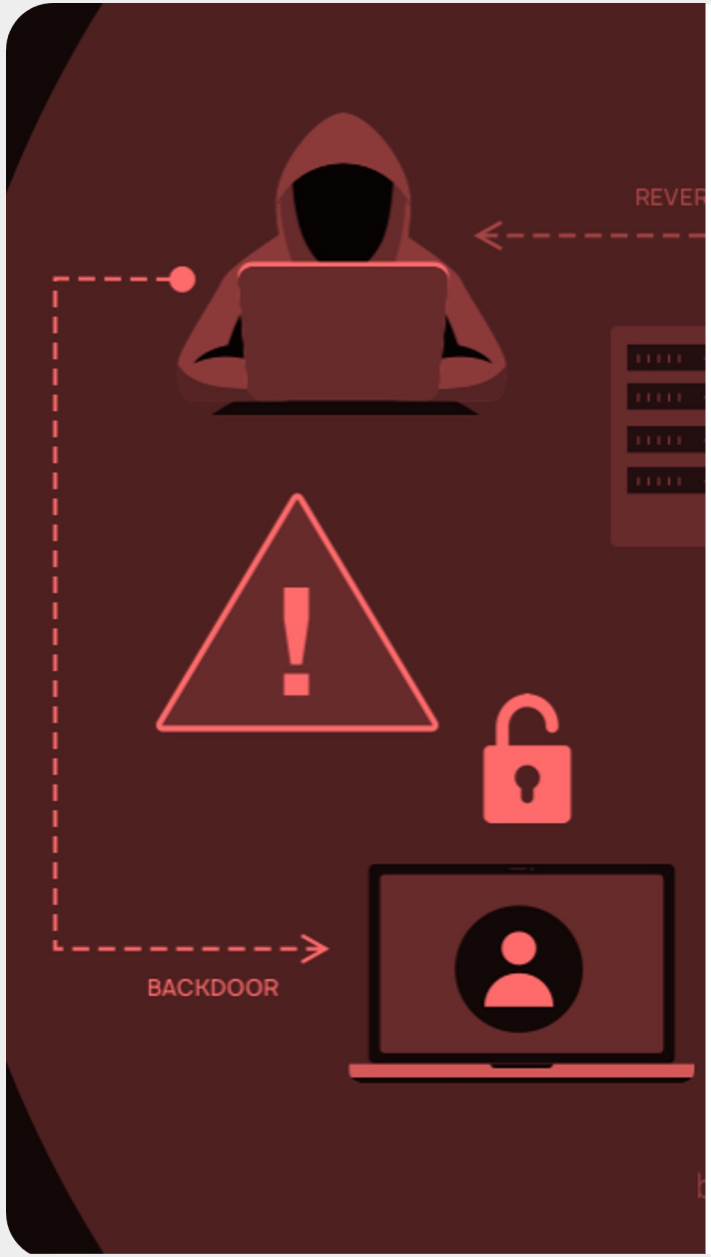


Caracterização da Ameaça

Dinâmica de acesso

	Source	Destination	Info	Name	Address
4-08 14:15:03,848357	192.168.135.93	47.85.112.244	1619f6f58a46f86d2602933f48fe65b7|ok		
4-08 14:15:03,904958	170.106.183.186	192.168.135.93	sindical.caixa.gov.br:443&1f0a0fb67621d2b9ea93cd84063fbd5d*		
4-08 14:15:03,906097	192.168.135.93	170.106.183.186	36034 → 799 [ACK] Seq=1 Ack=1 Win=87616 Len=0 TSval=162405 TSecr=3334520413		
4-08 14:15:03,936847	23.219.67.205	192.168.135.93	Application Data		
4-08 14:15:03,936880	192.168.135.93	131.162.200.96	40094 → 443 [ACK] Seq=644 Ack=3510 Win=99200 Len=0 TSval=162405 TSecr=4258…		
4-08 14:15:03,938431	192.168.135.93	170.106.183.186	1f0a0fb67621d2b9ea93cd84063fbd5d|ok		
4-08 14:15:03,948561	47.85.112.244	192.168.135.93	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message		
4-08 14:15:03,949890	192.168.135.93	152.255.34.90	56938 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=162406 TS…		
4-08 14:15:03,998747	47.85.112.244	192.168.135.93	799 → 46966 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1452 SACK_PERM TSva…		
4-08 14:15:03,998782	192.168.135.93	192.168.135.1	Standard query 0x1227 A sindical.caixa.gov.br		
4-08 14:15:04,000109	192.168.135.93	47.85.112.244	Change Cipher Spec, Encrypted Handshake Message		
4-08 14:15:04,008610	192.168.135.1	192.168.135.93	Standard query response 0x4bb1 A cluesforum.info A 135.181.45.242	cluesforum.info	135.181.
4-08 14:15:04,014184	192.168.135.93	47.85.112.244	46966 → 799 [ACK] Seq=36 Ack=518 Win=88704 Len=0 TSval=162408 TSecr=361151…		
4-08 14:15:04,085991	47.85.112.244	192.168.135.93	799 → 46960 [ACK] Seq=2622 Ack=7091 Win=43008 Len=0 TSval=3611519856 TSecr…		
4-08 14:15:04,114211	170.106.183.186	192.168.135.93	800 → 58127 [ACK] Seq=1 Ack=1275 Win=45056 Len=0 TSval=3334520401 TSecr=16…		
4-08 14:15:04,115192	170.106.183.186	192.168.135.93	799 → 36034 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1424 SACK_PERM TSva…		
4-08 14:15:04,115228	192.168.135.93	152.255.34.90	56938 → 443 [ACK] Seq=1 Ack=1 Win=87616 Len=0		
4-08 14:15:04,116701	192.168.135.93	23.219.67.205	Application Data		
4-08 14:15:04,116749	131.162.200.96	192.168.135.93	Change Cipher Spec, Encrypted Handshake Message		
4-08 14:15:04,125850	192.168.135.1	192.168.135.93	Standard query response 0x1227 A sindical.caixa.gov.br CNAME sindical.caix…	sindical.caixa.g…	152.25
4-08 14:15:04,125885	192.168.135.93	47.85.112.244	46960 → 799 [ACK] Seq=7091 Ack=3344 Win=94976 Len=0 TSval=162425 TSecr=361…		
4-08 14:15:04,131700	192.168.135.93	135.181.45.242	Client Hello (SNI=cluesforum.info)		
4-08 14:15:04,147204	47.85.112.244	192.168.135.93	799 → 46966 [ACK] Seq=1 Ack=36 Win=45056 Len=0 TSval=3611519922 TSecr=1623…		
4-08 14:15:04,147229	192.168.135.93	170.106.183.186	36034 → 799 [ACK] Seq=2860 Ack=376 Win=88704 Len=1412 TSval=162428 TSecr=3…		
4-08 14:15:04,147318	47.85.112.244	192.168.135.93	Client Hello (SNI=cluesforum.info)		
4-08 14:15:04,147331	192.168.135.93	152.255.34.90	Client Hello (SNI=sindical.caixa.gov.br)		

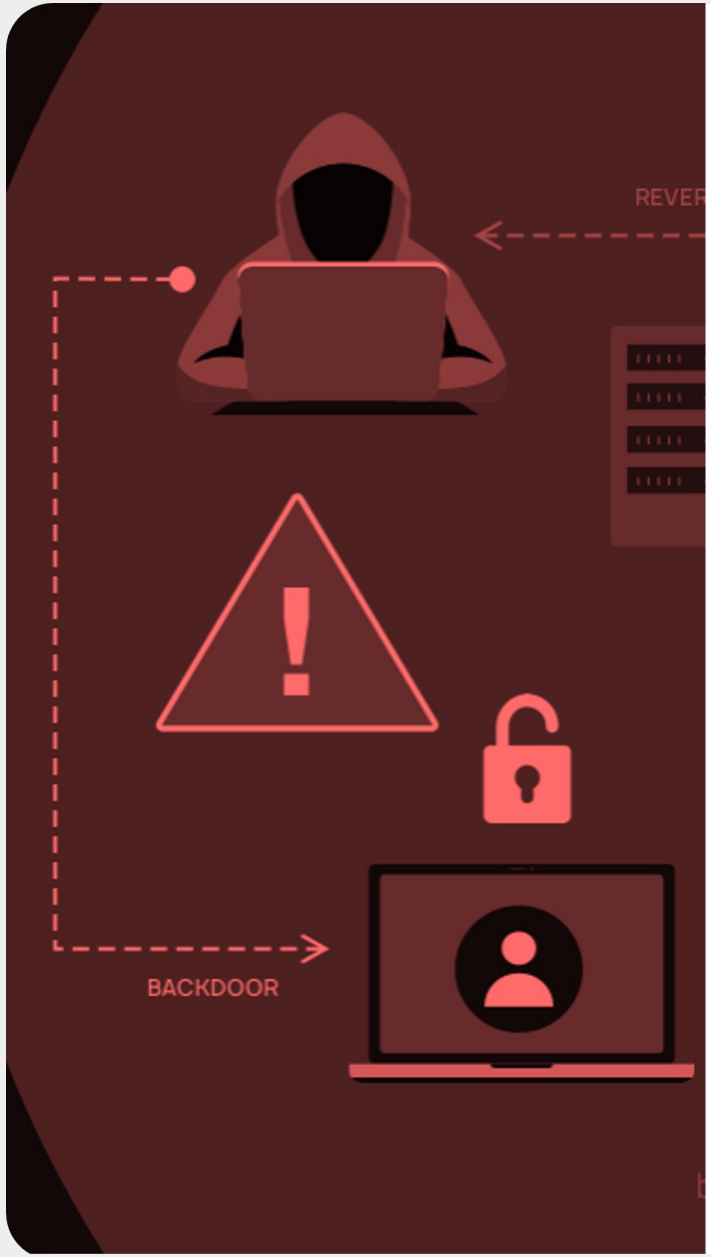
1
2
3
4



Caracterização da Ameaça

Domínios acessados através da TV Box

cdpj-api.bancointer.com.br
consulta-processual-unificada-prd.tjpa.jus.br
eproc1g.tjsc.jus.br
gol-auth-api.voegol.com.br
servicespub.prod.api.aws.grupokabum.com.br
sicmobi2.sicredi.com.br
www.bancobmg.com.br
www.trf4.jus.br
www37.bb.com.br
cassino.bet.br
api-dc-rchlo-prd.riachuelo.com.br
produto.mercadolivre.com.br
cdpj-api.bancointer.com.br

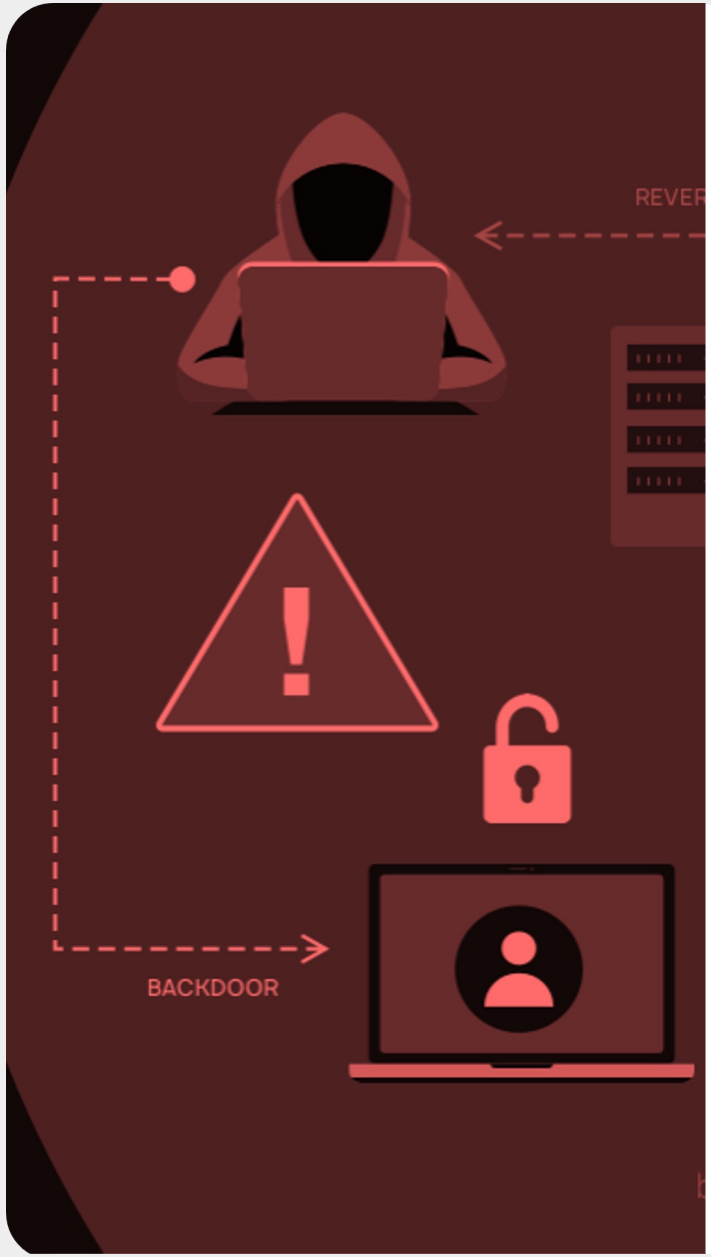


Caracterização da Ameaça

Outros tráfegos suspeitos

No.	Time	Source	Destination	Info	Source or Destination GeoIP AS Organization	Source or
338159	2025-04-08 14:12:35,620160	192.168.10.111	222.212.210.22	36154 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338195	2025-04-08 14:12:36,024694	222.212.210.22	192.168.10.111	80 → 36154 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338196	2025-04-08 14:12:36,025191	192.168.10.111	222.212.210.22	36154 → 80 [ACK] Seq=1 Ack=1 Win=87616 Len=0	CHINANET SiChuan Telecom Internet Data…	Chengdu
338198	2025-04-08 14:12:36,095863	192.168.10.111	222.212.210.22	GET /update/sdk/task_164.jar HTTP/1.1	CHINANET SiChuan Telecom Internet Data…	Chengdu
338222	2025-04-08 14:12:36,280331	222.212.210.22	192.168.10.111	[TCP Out-Of-Order] 80 → 36154 [SYN, ACK] Seq=0 Ac…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338223	2025-04-08 14:12:36,280331	192.168.10.111	222.212.210.22	[TCP Dup ACK 338196#1] 36154 → 80 [ACK] Seq=136 A…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338238	2025-04-08 14:12:36,528989	222.212.210.22	192.168.10.111	[TCP Previous segment not captured] 80 → 36154 [A…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338239	2025-04-08 14:12:36,528989	222.212.210.22	192.168.10.111	[TCP Previous segment not captured] 80 → 36154 [A…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338240	2025-04-08 14:12:36,529588	222.212.210.22	192.168.10.111	[TCP Out-Of-Order] 80 → 36154 [ACK] Seq=17668 Ack…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338241	2025-04-08 14:12:36,529588	192.168.10.111	222.212.210.22	[TCP Dup ACK 338196#2] 36154 → 80 [ACK] Seq=136 A…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338242	2025-04-08 14:12:36,529588	222.212.210.22	192.168.10.111	80 → 36154 [ACK] Seq=20516 Ack=136 Win=42240 Len=…	CHINANET SiChuan Telecom Internet Data…	Chengdu
338244	2025-04-08 14:12:36,530228	222.212.210.22	192.168.10.111	80 → 36154 [ACK] Seq=21940 Ack=136 Win=42240 Len=…	CHINANET SiChuan Telecom Internet Data…	Chengdu

No.	Time	Source	Destination	Info	Source or Destination GeoIP AS Organiza	Source or Destination GeoIP City
338198	2025-04-08 14:12:36,09…	192.168.10.111	222.212.210…	GET /update/sdk/task_164.jar HTTP/1.1	CHINANET SiChuan Telecom Interne…	Chengdu
428950	2025-04-08 14:14:13,68…	192.168.10.111	222.212.210…	GET /plg/wp/hw_wp_v12.zip HTTP/1.1	CHINANET SiChuan Telecom Interne…	Chengdu
428951	2025-04-08 14:14:13,68…	192.168.10.111	222.212.210…	GET /plg/hw_ky_bsl/hw_ky_bsl_v1.zip HTTP/1.1	CHINANET SiChuan Telecom Interne…	Chengdu
428952	2025-04-08 14:14:13,68…	192.168.10.111	222.212.210…	GET /plg/hw_earn/hw_earn_v1.zip HTTP/1.1	CHINANET SiChuan Telecom Interne…	Chengdu



Caracterização da Ameaça

Back doors e conexões da TV Box

```
rk322x_box:/data/data # netstat -tupa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp      130      0 192.168.0.4:52294       216.239.34.223:https    CLOSE_WAIT  819/com.google.andro
tcp      130      0 192.168.0.4:52516       eze04s07-in-f10.1e100.n CLOSE_WAIT  1125/com.google.andr
tcp     1094      0 192.168.0.4:34685       gru09s09-in-f138.1e100. CLOSE_WAIT  -
tcp        0      0 :::5555                 :::*                    LISTEN      182/adbd
tcp        0      0 ::ffff:192.168.0.4:3838 :::*                    LISTEN      1595/com.rockchips.m
tcp        0      0 ::ffff:192.168.0.4:3838 :::*                    LISTEN      1595/com.rockchips.m
tcp        0      0 :::10102                :::*                    LISTEN      880/com.xbs.xplus
tcp        0      0 :::10202                :::*                    LISTEN      880/com.xbs.xplus
tcp        0      0 :::12101                :::*                    LISTEN      880/com.xbs.xplus
tcp        0      0 :::10121                :::*                    LISTEN      880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:4480 :::*                    LISTEN      1565/com.rockchips.m
tcp        0      0 ::ffff:192.168.0.4:5507 ::ffff:43.135.153.199:8 ESTABLISHED 880/com.xbs.xplus
tcp        1      0 ::ffff:192.168.0.4:3468 gru09s09-in-f138.1e100. CLOSE_WAIT  1344/com.android.ven
tcp        0      0 ::ffff:192.168.0.4:5174 myshopify.com:https     ESTABLISHED 880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:5157 ::ffff:47.85.112.214:80 ESTABLISHED 880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:5555 ::ffff:192.168.0.100:33 ESTABLISHED 182/adbd
tcp        0      0 ::ffff:192.168.0.4:4171 ::ffff:47.85.112.214:79 ESTABLISHED 880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:4611 ::ffff:43.135.153.199:7 TIME_WAIT   -
tcp       24      0 ::ffff:192.168.0.4:4305 ::ffff:128.14.202.210:h CLOSE_WAIT  880/com.xbs.xplus
tcp        1      0 ::ffff:192.168.0.4:5837 ::ffff:107.151.182.82:9 CLOSE_WAIT  880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:4611 ::ffff:43.135.153.199:7 TIME_WAIT   -
tcp        0      0 ::ffff:192.168.0.4:4055 ::ffff:23.248.188.62:99 ESTABLISHED 880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:5478 ::ffff:152.32.234.128:8 ESTABLISHED 880/com.xbs.xplus
tcp        0     91 ::ffff:192.168.0.4:5024 ::ffff:43.130.169.127:8 ESTABLISHED 880/com.xbs.xplus
tcp        0      0 ::ffff:192.168.0.4:6027 ci-in-f188.1e100.net:52 ESTABLISHED 819/com.google.andro
```

MONITORAMENTO DE TRÁFEGO

- Processo de autenticação (8 domínios em proxy)

getActionStatus - Quando liga
getServerTime - De hora em hora
getApp - De hora em hora
authMacSn - De hora em hora
getAndroidFirmware - De hora em hora
getAppWhiteList - De hora em hora
getClientToken - De hora em hora
getAdvertisement - De hora em hora
getAppMarket - De hora em hora

MONITORAMENTO DE TRÁFEGO

- Confirmação de versão do .dex

Wireshark · Follow HTTP Stream (tcp.stream eq 8) · GR01_INXPLUS_20250918_10h17.pcapng

```
POST /task/getAppUpdate HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.2; XPLUS Build/XPLUS)
Host: a2.ty4523.space
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 180

{"userId":"48db410e-b1d8-32cb-b333-e38a50134df2","dexVersion":"3.58","dexType":1,"channelId":"2232","packageName
":"realplay.com.timeserver","appVersion":207,"appName":"TimeServer"}
HTTP/1.1 200
Server: nginx/1.14.2
Date: Thu, 18 Sep 2025 12:55:36 GMT
Content-Length: 77
Connection: keep-alive

{"data":{"dexUrl":"","dexVersion":3.58,"status":1},"msg":"ok","resultCode":1}
```

Packet 129. 1 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

MONITORAMENTO DE TRÁFEGO

- Atualização da versão do .dex

Wireshark · Follow TCP Stream (tcp.stream eq 0) · GR01_INXPLUS_20250911_12h41_atual.pcapng

```
HTTP/1.1 200
Server: nginx/1.14.2
Date: Thu, 11 Sep 2025 15:41:20 GMT
Content-Length: 120
Connection: keep-alive

{"data":{"dexUrl":"http://107.151.182.82/vr34der34/dex3.6.png","dexVersion":3.600,"status":0},"msg":"ok","result
Code":1}HTTP/1.1 200
Server: nginx/1.14.2
Date: Thu, 11 Sep 2025 15:41:25 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 128
Connection: keep-alive

...4..r..A.3H..T...8..;...._8...c.D3A,O.....CN.........|...........lO....o.s }..Y+.;....4...j':.S....e...r.(..!
......z....m...M
```

MONITORAMENTO DE TRÁFEGO

- Inicializa o serviço de proxy residencial

Wireshark · Follow HTTP Stream (tcp.stream eq 36) · GR01_INXPLUS_20250918_10h17.pcapng

```
GET /api/init?configVersion=3.53&rsa=1 HTTP/1.1
Accept-Language: zh-CN
Charset: UTF-8
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.10.0
Host: a2.ty54fgd435.my


HTTP/1.1 200
Server: nginx/1.14.2
Date: Thu, 18 Sep 2025 12:56:02 GMT
Content-Length: 12
Connection: keep-alive

{"code":200}
```

MONITORAMENTO DE TRÁFEGO

- Atualização domínios aplicação proxy residencial

Wireshark · Follow HTTP Stream (tcp.stream eq 9) · Ethernet (host 192.168.3.100)

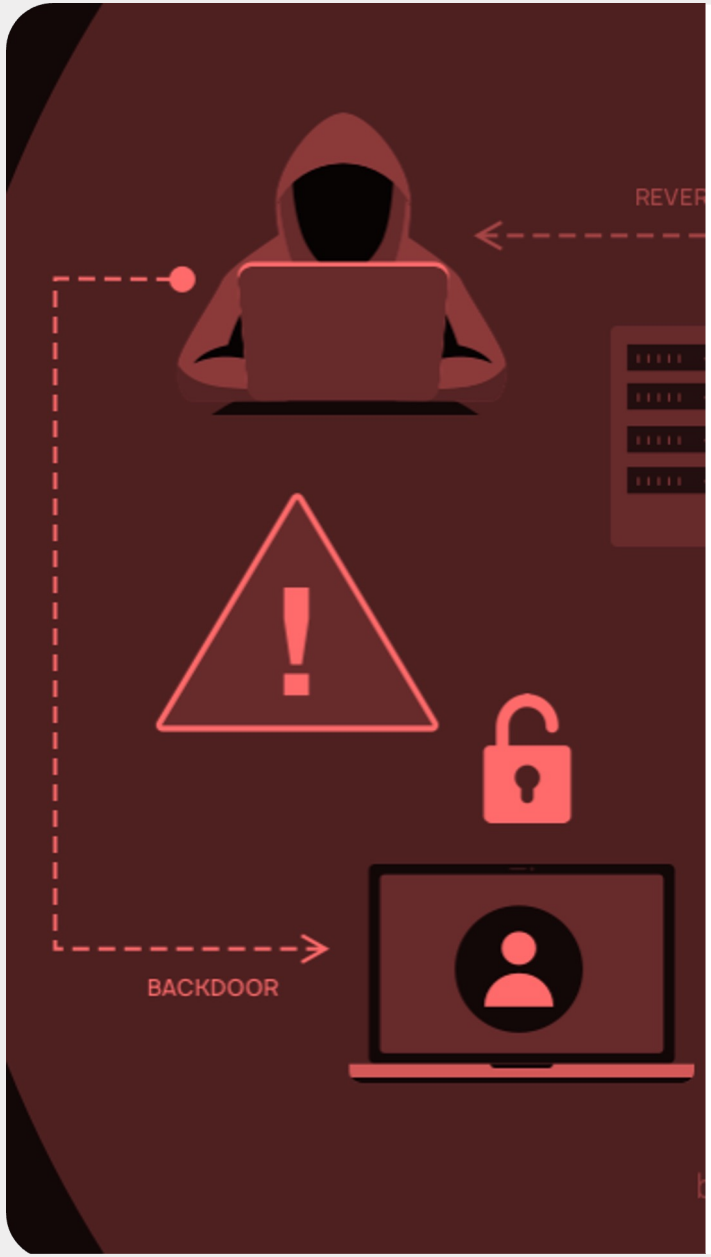
```
POST /task/getAppUpdate HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.2; XPLUS Build/XPLUS)
Host: a2.ue886578433.online
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 180

{"userId":"48db410e-b1d8-32cb-b333-e38a50134df2","dexVersion":"3.58","dexType":1,"channelId":"2232","packageName":"realplay.com.timeserver","appVersion":207,"a
ppName":"TimeServer"}
HTTP/1.1 200
Server: nginx/1.14.2
Date: Tue, 23 Sep 2025 08:38:40 GMT
Content-Length: 77
Connection: keep-alive

{"data":{"dexUrl":"","dexVersion":3.58,"status":1},"msg":"ok","resultCode":1}
GET /api/init?configVersion=3.53&rsa=1 HTTP/1.1
Accept-Language: zh-CN
Charset: UTF-8
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.10.0
Host: a2.ue886578433.online


HTTP/1.1 200
Server: nginx/1.14.2
Date: Tue, 23 Sep 2025 08:38:43 GMT
Content-Length: 487
Connection: keep-alive

{"code":100,"data":{"configVersion":3.540,"hosts":["http://t2.saoisahjdshaiu.online","http://t2.gsaksghdasbsaosydf.online","http://t2.moissahoah.site","http://
t2.sjaiosjanldnsaiuy.site","https://t2.moissahoah.site"],"interval":5500000,"reportApi":"/cpc/api/report","tagName":"config","taskApi":"/cpc/api/task","updates
":["http://a2.saoisahjdshaiu.online","http://a2.gsaksghdasbsaosydf.online","http://a2.moissahoah.site","http://a2.sjaiosjanldnsaiuy.site","https://a2.moissahoa
h.site"]}}
```



Caracterização da Ameaça

RESULTADOS

Presença de *malware* ativo e persistente

Uso como *proxy* residencial (sem consentimento)

Acessos indevidos a bancos, serviços públicos e pornografia

Infecção desde 2024, via atualização remota

Conexões com servidores da rede criminosa **BADBOX 2.0**

BADBOX 2.0

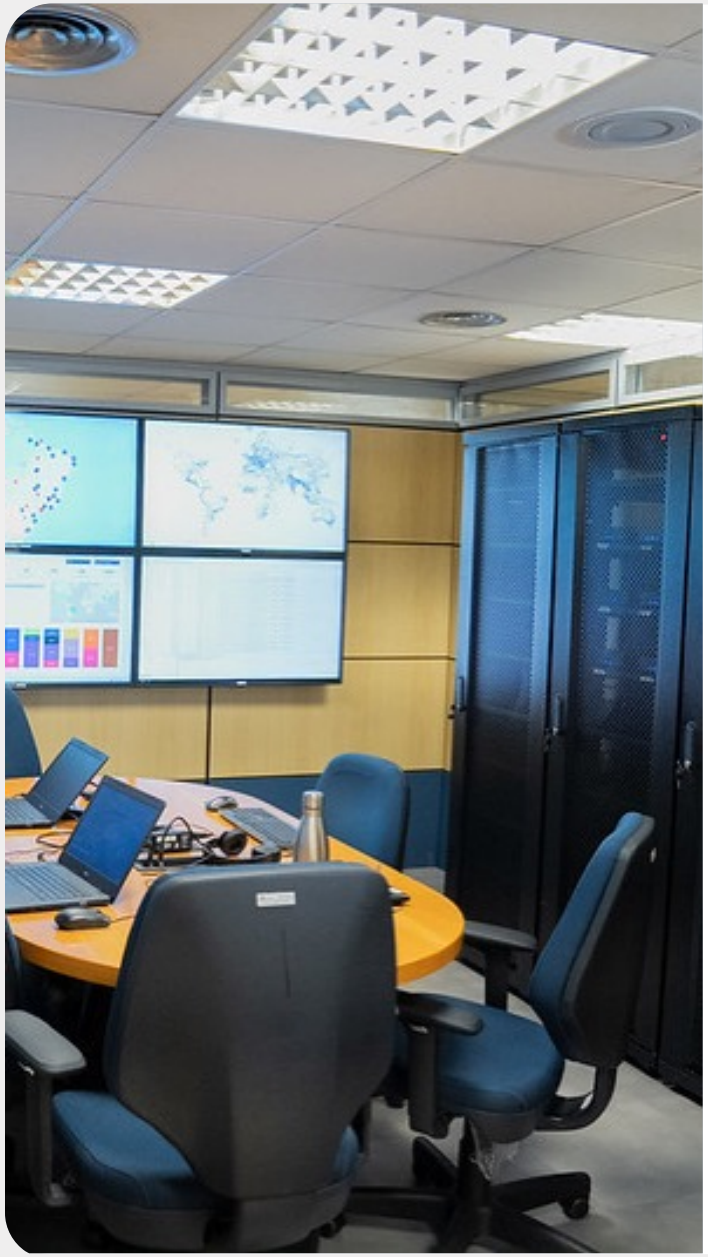
Shadowserver: milhões de dispositivos comprometidos e comunicação ativa com C2.

Google: remoção de apps maliciosos e ações contra a infraestrutura da botnet.

FBI: dispositivos infectados usados em fraudes, ataques e proxies residenciais.

Europa (Irlanda/Portugal): crescimento da botnet e alerta para infecção em larga escala.

Anatel: confirmação no Brasil e adoção de medidas de bloqueio e mitigação.



BADBOX 2.0
Ações de Combate na Anatel

Fiscalização em comércios populares e marketplaces

Monitoramento em laboratório

Cooperação com operadoras

Bloqueio de domínios e IPs maliciosos

IDENTIFICAÇÃO DE ALVOS

- Novos domínios

DOMÍNIO	WHOIS Server	Registered On	Address	city
a2.ty4523.space	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik
t2.ty4523.space	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik
a2.ty54fgd435.my	whois.dynadot.com	2025-05-08 01:58:54	PO Box 701	San Mateo
t1.ty54fgd435.my	whois.dynadot.com	2025-05-08 01:58:54	PO Box 701	San Mateo
t2.ty54fgd435.my	whois.dynadot.com	2025-05-08 01:58:54	PO Box 701	San Mateo
a1.ue886578433.online	whois.namecheap.com	2025-04-03 05:08:50	Kalkofnsvegur 2	Reykjavik
a2.ue886578433.online	whois.namecheap.com	2025-04-03 05:08:50	Kalkofnsvegur 2	Reykjavik
t1.ue886578433.online	whois.namecheap.com	2025-04-03 05:08:50	Kalkofnsvegur 2	Reykjavik
t2.ue886578433.online	whois.namecheap.com	2025-04-03 05:08:50	Kalkofnsvegur 2	Reykjavik
a1.vrr8345.site	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik
a2.vrr8345.site	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik
t1.vrr8345.site	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik
t2.vrr8345.site	whois.namecheap.com	2025-05-06 04:26:36	Kalkofnsvegur 2	Reykjavik

IDENTIFICAÇÃO DE ALVOS

- IPs associados

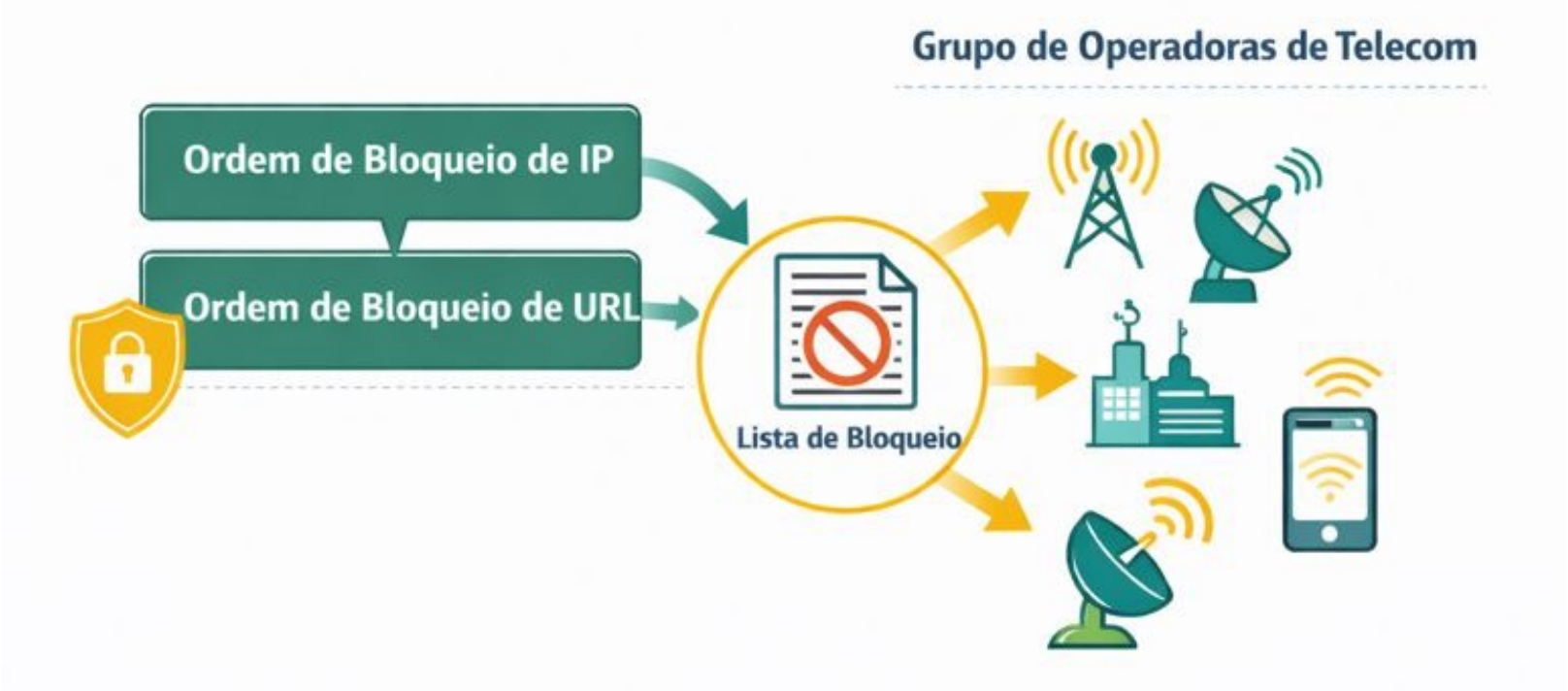
t2.ty4523.space historical A data

38.145.220.25

A | AAAA

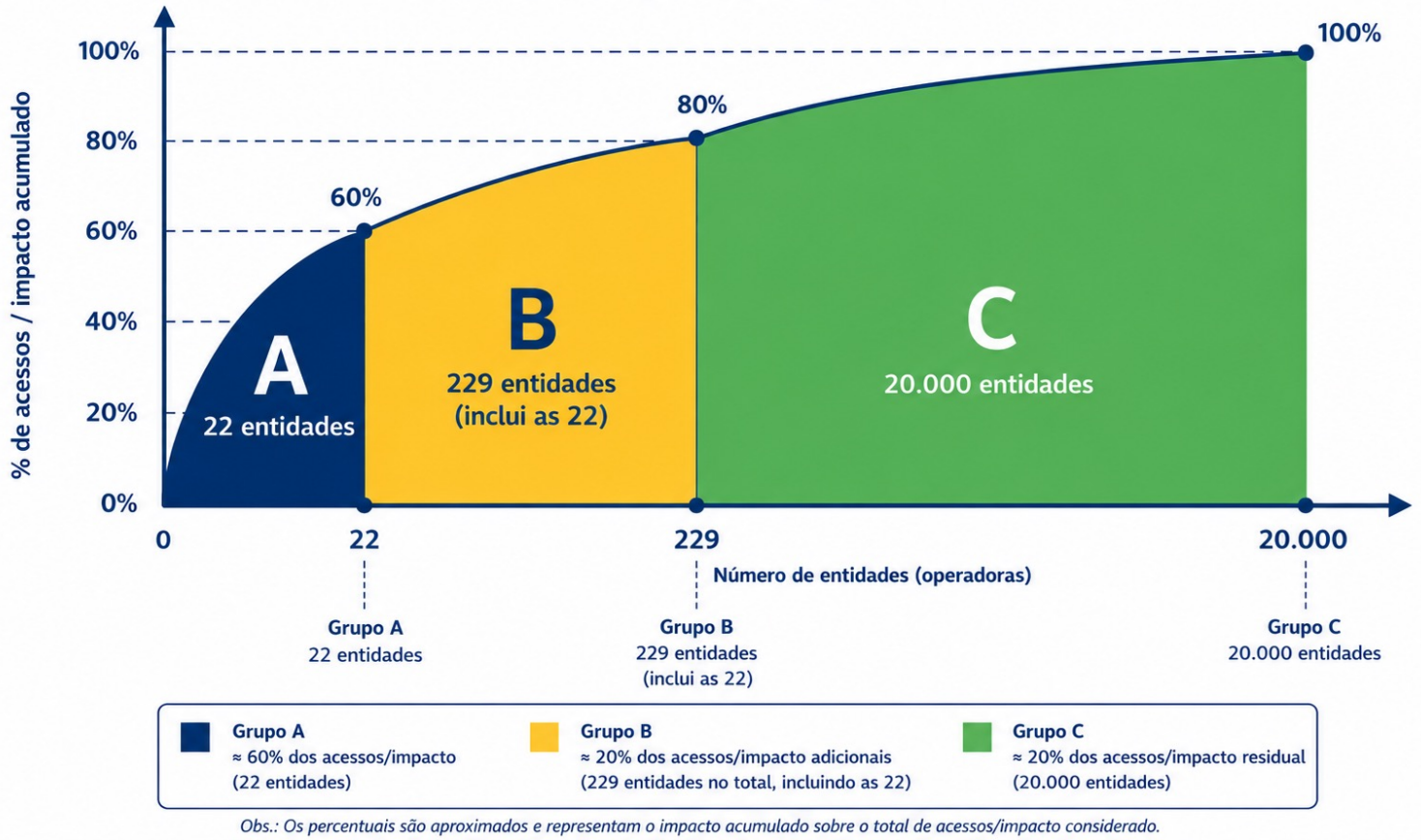
IP Addresses	Organization	First Seen	Last Seen	Duration Seen
38.34.183.220	Enzu Inc	2025-09-15 (9 days)	2025-09-23 (today)	8 days
38.34.183.212	Enzu Inc	2025-09-09 (15 days)	2025-09-15 (9 days)	6 days
45.136.119.180	Enzu Inc	2025-09-05 (19 days)	2025-09-09 (15 days)	4 days

BLOQUEIOS DE DOMÍNIO E IPS



BLOQUEIOS DE DOMÍNIO E IPS

Agrupamento de Operadoras de Telecom com Base na Curva ABC



Obs.: Os percentuais são aproximados e representam o impacto acumulado sobre o total de acessos/impacto considerado.

BLOQUEIOS DE DOMÍNIO E IPS

- Redução de IPs conectados ao malware
- Novos domínios utilizados pelo malware

SHADOWSERVER UK Government

General statistics

Time series

Date range: 1 year

Sources: sinkhole, sinkhole6

Severity: Select one or more options...

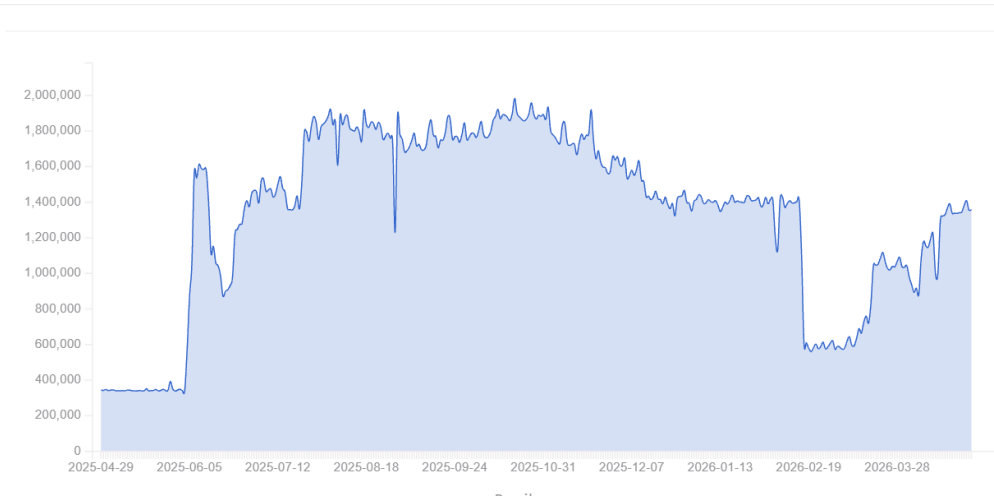
Tags: android.badbox2

Countries: Brazil (BR)

Data set: Counted IP addresses

Limit: 100

Group by: Country / Tag



REDES SEGURAS

- Redução da superfície de ataque
- Contenção da botnet
- Queda no tráfego malicioso
- Melhoria da estabilidade da rede
- Aumento da resiliência da Internet

Desafios Operacionais

A resposta a esse tipo de incidente apresenta desafios relevantes:

- escala massiva de dispositivos comprometidos;
- baixa visibilidade na rede do usuário final;
- uso de CGNAT, dificultando rastreabilidade;
- infraestrutura distribuída e dinâmica;
- uso de DNS público e CDNs;
- rápida adaptação dos agentes maliciosos.

Esses fatores exigem abordagens diferenciadas, baseadas em análise comportamental e coordenação entre múltiplos atores.

Estratégia de Mitigação e Resposta

A atuação da Anatel envolveu uma abordagem integrada, com foco em ações práticas:

- monitoramento contínuo de tráfego;
- identificação de padrões anômalos;
- bloqueio de domínios e endereços IP maliciosos;
- cooperação com prestadoras de telecomunicações;
- ações de fiscalização e apreensão de equipamentos irregulares;
- definição de requisitos de segurança para dispositivos homologados.

Essa atuação demonstra a importância da integração entre aspectos técnicos e regulatórios na resposta a incidentes de grande escala.

Resultados

Os principais resultados obtidos incluem:

- identificação de comportamento malicioso persistente em dispositivos;
- evidência de uso como proxies residenciais sem consentimento;
- detecção de conexões com infraestruturas associadas a botnets globais;
- aumento da capacidade de detecção e resposta coordenada;
- redução parcial da infraestrutura ativa por meio de bloqueios.

Lições Aprendidas

A experiência evidencia que:

- incidentes modernos são distribuídos e persistentes;
- dispositivos IoT representam vetor crítico de ataque;
- a cooperação entre atores é essencial;
- ações isoladas têm impacto limitado;
- inteligência de ameaças é fundamental para resposta

Recomendações para a Comunidade

Com base no estudo, recomenda-se:

- ampliar a visibilidade de rede (netflow, DNS, telemetria);
- investir em correlação de eventos em larga escala;
- fortalecer mecanismos de cooperação;
- adotar abordagens baseadas em risco;
- incluir dispositivos IoT na estratégia de defesa.

Conclusão

A atuação da Anatel no combate a botnets associadas a dispositivos piratas representa um exemplo prático de resposta a incidentes em larga escala, especialmente relevante no contexto brasileiro.

A integração entre regulação, análise técnica e coordenação multissetorial se mostra essencial para o enfrentamento de ameaças complexas e distribuídas.

O caso apresentado oferece subsídios práticos e replicáveis para a comunidade de CSIRTs, contribuindo para o aprimoramento das estratégias de resposta a incidentes.

figf6@anatel.gov.br