INFORME Nº 17/2025/GR01FI2/GR01/SFI

PROCESSO Nº 53504.002905/2025-76

INTERESSADO: SUPERINTENDÊNCIA DE FISCALIZAÇÃO

1. ASSUNTO

1.1. Alerta sobre riscos relevantes da presença de *malware* BADBOX 2.0 em dispositivos do tipo *set-top box* não homologados, amplamente distribuídos no Brasil.

2. REFERÊNCIAS

2.1. Estratégia Nacional de Cibersegurança, instituido pelo Decreto nº 12.573, de 4 de agosto de 2025 ;

2.2. Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações, aprovado pela Resolução nº 715, de 23 de outubro de 2019;

2.3. Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020;

2.4. Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, aprovados pelo Ato nº 77, de 05 de janeiro de 2021 ;

2.5. Requisitos Técnicos para Avaliação da Conformidade do tipo de produto Smart TV Box, aprovados pelo Ato nº 9281, de 5 de julho de 2023,

2.6. Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC), aprovado pela Resolução Interna Anatel nº 189, de 7 de fevereiro de 2023;

3. DA CONTEXTUALIZAÇÃO

I - Da necessidade de homologação de produtos de telecomunicações

3.1. Os equipamentos para telecomunicações requerem homologação da Anatel para serem comercializados e utilizados no Brasil, conforme art. 55 do **Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações** , aprovado pela Resolução nº 715, de 23 de outubro de 2019. Esse normativo tem como um dos princípios a proteção e a segurança dos usuários dos produtos de telecomunicações, estabelecido no inciso I de seu art. 3º. Para cumprir com esse princípio, o processo de avaliação da conformidade e homologação busca garantir padrões mínimos de qualidade e segurança, e o arcabouço regulatório prevê que tanto a comercialização quanto a utilização de produtos para telecomunicações irregulares são passíveis de sanções administrativas, que podem ir de advertência a multa.

3.2. Percebe-se, no entanto, que equipamentos não homologados destinados à recepção de sinais de TV a cabo ou de vídeo sob demanda podem ser atrativos ao consumidor, por possibilitarem o acesso a conteúdos protegidos por direitos autorais de forma irregular - o que é crime. Além disso, essas TV Boxes apresentam um grande risco: elas podem conter vírus e malwares, comprometendo a segurança cibernética dos usuários e das redes.

3.3. O presente documento tem por finalidade fazer um alerta sobre os perigos da presença de *malware* BADBOX 2.0 em dispositivos do tipo *set-top box* não homologados, que são amplamente distribuídos no Brasil. Para tanto, apresenta-se-á um breve resumo sobre as medidas que a Anatel já adotou quanto ao uso desses dispositivos e as ações já efetuadas quanto ao tema em outros países para, então, tratar dos resultados do último estudo recentemente concluído pela Agência.

II - Dos primeiros estudos da Anatel sobre riscos cibernéticos de TVs Boxes não homologadas

3.4. Durante os anos de 2021 e 2022, a Superintendência de Fiscalização (SFI) da Anatel instituiu um **Grupo de Trabalho destinado a realizar estudos em dispositivos TV Box (GT TV Box)** com a finalidade de identificar as vulnerabilidades e ameaças que esses equipamentos podem trazer às redes, aos serviços e aos usuários de telecomunicações. O GT elaborou Relatórios Técnicos dos estudos de engenharia reversa em TV Box (SEI nº 7777396 e SEI nº 9580113), apontando:

a) a possibilidade de os equipamentos serem vetores de ataques do tipo de negação de serviço (*Denial-of- Service - DoS*, ou *Distributed-Denial-of-Service - DDos*);

b) a presença de um *mallware ("pandoraspear")*, cuja função é permitir controlá-los remotamente, por meio de um servidor de Comando e Controle;

c) falhas de segurança no processo de atualização dos aplicativos por meio de lojas virtuais próprias, permitindo que toda a informação trocada seja capturada e modificada por um atacante mal-intencionado, possibilitando a instalação de aplicativos maliciosos no dispositivo; e

d) essa vulnerabilidade, associada a outra em que o sistema operacional dos dispositivos permite que terceiros possam ter acesso irrestrito com privilégios de administrador (conhecido como *"root"*), o que possibilita o controle total da TV Box, incluindo o acesso a outros dispositivos que compartilham a mesma rede, tais como: computadores, televisores, roteadores, celulares, webcams, dentre outros, capturando dados e informações dos usuários, como registros financeiros, senhas, arquivos, fotos, etc.

III - Dos requisitos técnicos para homologação de TV Box

3.5. Com o intuito de conter a disseminação de TV Box voltados à pirataria de conteúdos protegidos por lei, a Anatel estabeleceu a criação de uma classificação de produto específica, passível de homologação, denominada *Smart TV Box*. Por meio do **Ato nº 9281, de 5 de julho de 2023** , foram definidos procedimentos técnicos para a verificação de requisitos de segurança cibernética para aumentar a proteção dos usuários e da rede de telecomunicações.

3.6. Com o objetivo de auxiliar os usuários a identificarem os TVs Boxes homologados, a Anatel disponibilizou a relação dos modelos e demais informações relacionadas aos produtos que foram submetidos e aprovados pela Agência, conforme lista acessível em https://www.gov.br/anatel/pt-br/regulado/certificacao-de-produtos/smart-tv-box-homologados.

IV - Do Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC)

3.7. Como as TVs Boxes piratas são amplamente distribuídas por canais informais, a Anatel buscou fortalecer suas ações de fiscalização no âmbito do Plano de Ação de Combate à Pirataria (PACP), que foi criado em 2018. Assim, a Agência intensificou a apreensão de equipamentos irregulares com apoio dos órgãos aduaneiros e de segurança pública, em portos/aeroportos, em centros de distribuição (CD) de grandes *marketplace* e em lojas do mercado popular.

3.8. Em outra iniciativa, com a finalidade de reduzir a atratividade dos dispositivos TV Box não homologados, através da **identificação e bloqueio do acesso** desses equipamentos ofertados no país, em 2023 a Anatel estabeleceu o **Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC)** aprovado pela Resolução Interna Anatel nº 189, de 7 de fevereiro de 2023 . Além desse objetivo principal, o plano traçou alguns objetivos associados, a saber: aumentar a segurança física e de dados dos usuários; reduzir os riscos às redes de telecomunicações causados por dispositivos TV Box não homologados (redução de agentes-escravos de ataques de negação distribuída de serviços); reduzir a atividade clandestina de provimento de SeAC por entidades ou pessoas físicas não outorgadas; e melhorar o equilíbrio competitivo do mercado audiovisual pela redução de ofertas irregulares de conteúdo.

3.9. Para atender aos objetivos traçados pelo **Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do SeAC**, a Anatel celebrou com a Associação Brasileira de TV por Assinatura (ABTA) o Acordo de Cooperação nº 2/2023, cujo objeto é a estruturação de laboratório para realização de análises técnicas sobre equipamentos e outros meios ilegais de oferta audiovisual pirata, com intercâmbio de informações, com uma abordagem integrada, envolvendo ações normativas, operacionais, preventivas e repressivas, para proteger a infraestrutura crítica de telecomunicações, a segurança digital dos consumidores e o equilíbrio econômico do setor regulado.

3.10. O laboratório atualmente monitora cerca de 31,8 mil endereços IPs, e mantém temporariamente bloqueado, cerca de 2,2 mil (considerando dados atualizados até 07 de agosto de 2025), por estarem diretamente ligados às atividades ilegais, incluindo atividades maliciosas de dezenas de modelos de TVs Boxes.

V - Do estudo da Human Security em março 2025

3.11. Em março de 2025, a empresa de segurança cibernética Human Security publicou um estudo sobre os riscos associados a dispositivos, incluindo TV Boxes, infectados por *malwares*, especificamente pelo BADBOX 2.0 (https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-BadBox-2-0).

3.12. De acordo com esse estudo, mais de 1 milhão de dispositivos estavam infectados, sendo que o Brasil era o país mais afetado, com 37,6% dos dispositivos observados pela Human Defense Platform, na época da publicação do estudo. Adicionalmente, identificou-se que a rede maliciosa se estabelece através de *backdoors* em equipamentos de baixo custo, permitindo que agentes de ameaças carreguem módulos de fraude remotamente. Além disso, verificou-se que esses aparelhos se comunicam com servidores de comando e controle (C2), pertencentes e operados por uma série de agentes de ameaças distintos, porém cooperativos, facilitando a execução de atividades maliciosas.

VI - Da ação judicial do Google contra a rede BADBOX 2.0

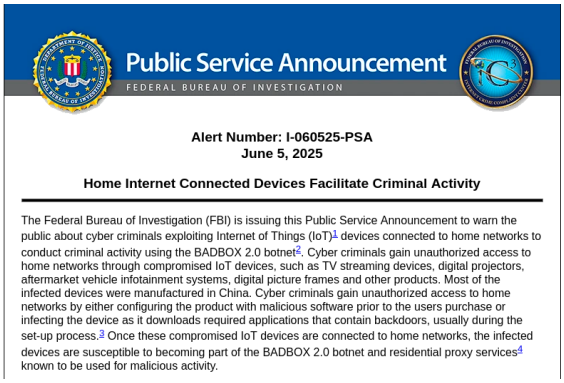
3.13. Em maio de 2025, o Google ingressou com uma ação judicial em Nova York contra os autores da rede BADBOX 2.0. Nos autos do processo, o Autor demonstrou que a rede BADBOX 2.0 ameaça a segurança da internet, incluindo as plataformas do Google, ao transmitir *malware* pela internet para configurar, implantar e operar uma *botnet*. A distribuição do *malware* em dispositivos de usuários que utilizam o sistema operacional *Android Open Source Project* ("AOSP"), criado pelo Google, mantém um papel de supervisão, comprometendo a segurança desses dispositivos, explorando-os para realizar uma variedade de fraudes publicitárias, inclusive por meio da rede de anúncios do Google, tornando esses dispositivos ferramentas para vários outros crimes cibernéticos, vendendo acesso a esses dispositivos a outros agentes de ameaças para que eles possam se conectar ao endereço IP de um dispositivo infectado e usá-lo para mascarar sua localização. O Google identificou que o *malware* comprometeu mais de 10 milhões de dispositivos no mundo e dezenas de milhares somente no *Southern District* de Nova York. (https://www.courtlistener.com/docket/70683171/google-llc-v-does-1-25)

VII - Do alerta nacional do Federal Bureau of Investigations (FBI)

3.14. No mês de junho de 2025, o Federal Bureau of Investigations (FBI) divulgou um alerta nacional sobre o *malware* BADBOX 2.0, destacando que a maioria dos dispositivos infectados foi fabricada na China. Os criminosos cibernéticos obtêm acesso não autorizado a redes domésticas configurando o produto com *software* malicioso antes da compra pelos usuários ou infectando o dispositivo enquanto ele baixa os aplicativos que contêm *backdoors*, geralmente durante o processo de configuração.

3.15. A rede maliciosa consiste em milhões de dispositivos infectados e mantém inúmeras *backdoors* para serviços de proxy que criminosos cibernéticos exploram vendendo ou fornecendo acesso gratuito a redes domésticas comprometidas para serem usadas em diversas atividades ilícitas.

3.16. O FBI destaca os principais indicadores da atividade da rede, quais sejam: sites suspeitos onde os aplicativos são baixados; solicitação que as configurações de proteção do *Google Play* sejam desativadas; dispositivos genéricos de *streaming* de TV anunciados como desbloqueados ou capazes de acessar conteúdo gratuito; Dispositivos de IoT (*Internet of Things*) anunciados por marcas desconhecidas; dispositivos *Android* que não são certificados pelo *Play Protect*; e tráfego de Internet inexplicável ou suspeito.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-060525-PSA
June 5, 2025

Home Internet Connected Devices Facilitate Criminal Activity

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement to warn the public about cyber criminals exploiting Internet of Things (IoT)[1] devices connected to home networks to conduct criminal activity using the BADBOX 2.0 botnet[2]. Cyber criminals gain unauthorized access to home networks through compromised IoT devices, such as TV streaming devices, digital projectors, aftermarket vehicle infotainment systems, digital picture frames and other products. Most of the infected devices were manufactured in China. Cyber criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to the users purchase or infecting the device as it downloads required applications that contain backdoors, usually during the set-up process.[3] Once these compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of the BADBOX 2.0 botnet and residential proxy services[4] known to be used for malicious activity.

(excerto de https://www.ic3.gov/PSA/2025/PSA250605)

VII - Do alerta do Centro Nacional de Cibersegurança de Portugal

3.17. No início do mês de julho de 2025, o Centro Nacional de Cibersegurança de Portugal (CERT.PT) também emitiu um alerta sobre o *malware* BADBOX 2.0, estimando que existem mais de 80.000 dispositivos comprometidos no ciberespaço português (https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135938/alerta-de-malware-BadBox20).

3.18. De acordo com esse alerta, o *malware* BADBOX é uma ameaça sofisticada que compromete dispositivos Android, incluindo Smart TV, aparelhos de *streaming*, tablets e projetores digitais. Identificado inicialmente em 2023, o BADBOX é frequentemente pré-instalado em dispositivos de baixo custo, maioritariamente fabricados na China, através de ataques à supply chain ou por intenção dos fabricantes. O malware estabelece backdoors que permitem a execução remota de código malicioso sem o consentimento - ou conhecimento - do utilizador.

3.19. Além disso, a variante BADBOX 2.0, identificada em 2025, expandiu o seu alcance, infetando mais de 1 milhão de dispositivos em 222 países, com maior prevalência de casos no Brasil (37,6%), Estados Unidos (18,2%), México (6,3%) e Argentina (5,3%). O *malware* pode também ser disseminado através de aplicações maliciosas descarregadas por meios não oficiais.

VIII - Do alerta do Centro Nacional de Cibersegurança da Irlanda (NCSC)

3.20. Em 18 de julho de 2025, o Centro Nacional de Segurança Cibernética da Irlanda (NCSC) publicou um estudo intitulado "Android BadBox 2.0 Malware" (https://www.ncsc.gov.ie/pdfs/AndroidBadBox2-0.pdf), no qual identificou um aumento significativo de dispositivos comprometidos no país infectados pelo *malware* BADBOX 2.0, inserido no *firmware* de diversos produtos de consumo de baixo custo, como tablets, TVs conectadas, molduras de fotos digitais e telefones.

3.21. O documento divulgado busca dimensionar o alcance e as capacidades dessas infecções, bem como detalhar seus impactos no país, destacando que *malware* é incorporado à imagem do sistema operacional ou assinado com certificados privilegiados, o que torna sua remoção consideravelmente mais difícil. Verificou-se, ademais, que uma redefinição de fábrica ou a instalação do flash do dispositivo geralmente não atenuam a infecção. Para maior persistência, algumas variantes instalam inicializadores, aplicativos de sistema ou *downloaders* ocultos, que reinstalarão o *malware* após a remoção.

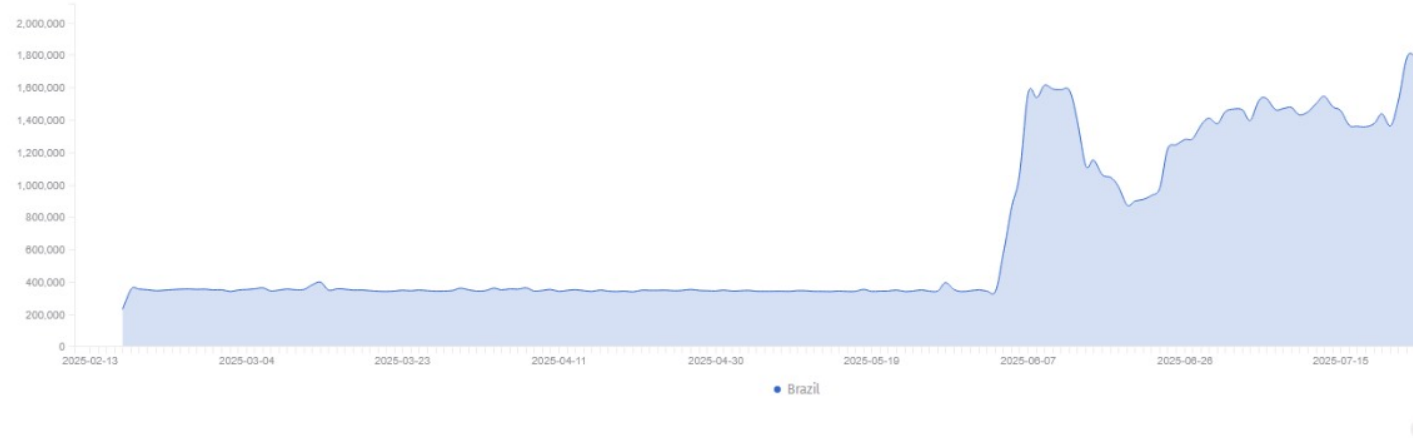
3.22. O alerta do NCSC faz parte de esforços coordenados de conscientização e remediação em todos os níveis – individual, comercial e nacional – que são essenciais para limitar o alcance e o impacto de ecossistemas de *malware* persistentes e em evolução.

VII - Do monitoramento da quantidade de dispositivos infectados no Brasil

3.23. A *The Shadowserver Foundation* é uma organização não-lucrativa fundada em 2024, que é considerada uma líder mundial em segurança e na investigação de atividade maliciosa. Seu objetivo é contribuir com uma cultura na qual a indústria de segurança é responsável por serviços e capacidades superiores.

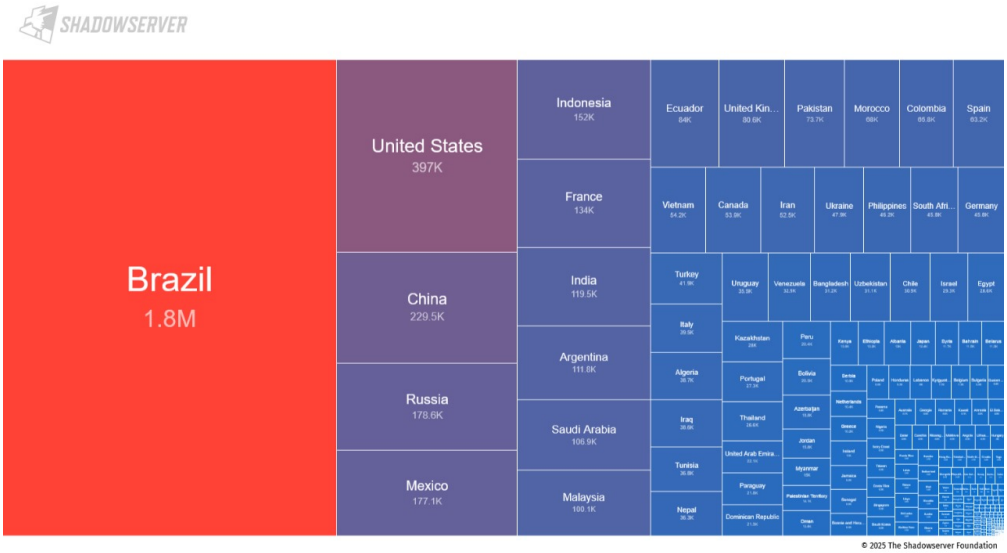
3.24. O *Shadowserver Dashboard* é uma plataforma da *The Shadowserver Foundation* que reúne e exibe, de forma visual e interativa, dados globais sobre ameaças cibernéticas. Esses dados são coletados por meio de *scanners* (vasculadores de serviços na internet), *honeypots* (servidores ou aplicações simuladas deliberadamente colocadas para serem atacadas, desviando a atenção do ataque dos servidores ou aplicações reais), *sinkholes* (sumidores de tráfego que absorvem e descartam os ataques) e emparcerias com ISPs, CSIRTs (Computer Security Incident Response Team - Equipe de Resposta a Incidentes de Segurança Informática) ou outras entidades.

3.25. No monitoramento da plataforma é possível verificar a evolução da contaminação do *malware* BADBOX 2.0 em dispositivos no Brasil, identificados a partir de endereços IP por técnicas de *sinkhole*. Nessa técnica, um recurso usado por agentes maliciosos é redirecionado para um dispositivo (ouvinte) que pode entender as conexões de dispositivos contaminados. Como se pode ver nas capturas de telas do *Shadowserver Dashboard* a seguir, observa-se que houve aumento de aproximadamente 340 mil IPs conectados entre fevereiro e junho desse ano para mais de 1,8 milhões em agosto de 2025:



(https://dashboard.shadowserver.org/pt-br/statistics/combined/time-series/?date_range=180&source=sinkhole&source=sinkhole6&tag=android.badbox2&geo=BR&dataset=unique_ips&limit=100&group_by=geo&stacking=stacked)

3.26. O gráfico abaixo compara a contaminação do *malware* BADBOX 2.0 em equipamentos no Brasil e em outros países do mundo:



(https://dashboard.shadowserver.org/pt-br/statistics/combined/tree/?date_range=1&source=sinkhole&source=sinkhole6&tag=android.badbox2&data_set=count&scale=log)

3.27. Assim, a situação brasileira é de fato preocupante.

4. DO ESTUDO DA ANATEL SOBRE O BADBOX 2.0

4.1. Desde o início de 2025, com objetivo específico de realização de estudos, investigações e avaliações para levantar subsídios e impactos na exposição do usuário a riscos relacionadas à segurança cibernética no Brasil, a equipe integrante do Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC), por meio de seu laboratório antipirataria, realiza monitoramento de vários modelos de TV Boxes piratas quanto à presença do BADBOX 2.0.

4.2. Em uma dessas investigações, dois modelos que apresentavam comportamento estranho chamaram a atenção da equipe. Esses modelos geravam tráfego de dados de *upload* mesmo estando em modo *stand-by,* indicando atividade de rede inesperada, pois a TV Box deveria estar inativa. A partir desses indícios, estabeleceu-se uma metodologia específica para estudar esse comportamento anômalo.

I - Da metodologia

4.3. Para realização do estudo, foram adotados os seguintes parâmetros metodológicos e passos de análise:

4.3.1. Os modelos de TV Boxes selecionados como amostra para testes são de modelos não homologados com grande distribuição nacional;

4.3.2. O tráfego desses modelos de TV Boxes foram monitorados em em laboratório, com ênfase em conexões persistentes em modo *standby*;

4.3.3. Foi realizada a engenharia reversa e análise de *firmware* para identificação de processos computacionais suspeitos;

4.3.4. Os resultados preliminares foram cruzados Indicadores de Comprometimento (IoCs) conhecidos. IoCs são evidências digitais que apontam para uma possível violação de segurança em sistemas ou redes, isto é, indicadores de que um ataque cibernético já foi documentado, já aconteceu ou continua acontecendo.

II - Das evidências coletadas no estudo

4.4. As avaliações conduzidas pela equipe integrante do Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do SeAC durante os estudos constataram vulnerabilidades de segurança aos usuários e ameaça às redes de telecomunicações do país, levando às seguintes evidências:

4.4.1. Foi confirmada a presença de *malware* ativo e persistente nos dispositivos analisados (InXPlus e TouroBox).

4.4.2. Foi identificado processo computacional malicioso operando com múltiplas portas abertas e conexões estabelecidas com servidores de controle externos;

4.4.3. Os TV Boxes acessavam aos mesmos domínios identificados no estudo da Human Security citado no item V da seção 3 deste relatório;

4.4.4. Foi identificado o uso não autorizado dos TV Boxes como *proxy* residencial. Isto é, a partir de uma conexão aos TV Boxes, sem consentimento dos usuários, identificaram-se acessos com potencial uso para fins maliciosos, incluindo acesso a sites de pornografia, de bancos, de tribunais estaduais e serviços públicos;

4.4.5. Arquivos suspeitos eram baixados através de conexões com servidores na internet. Esses arquivos eram do tipo .jar, que é um formato de arquivo comprimento que pode conter múltiplos arquivos relacionados ao java, tais como arquivos de classes, recursos e metadata que permitem que desenvolvedores agrupem aplicações java, bibliotecas ou módulos em um único arquivo para distribuição e instalaão simplificada;

4.4.6. Também se obteve indicação de que a infecção se iniciou em 2024, possivelmente via atualização remota de aplicativo.

III - Das riscos trazidos pela rede BADBOX 2.0

4.5. Além daquelas obtidas por evidências coletadas no estudo, destacam-se os seguintes riscos causados pela rede BADBOX 2.0:

I - Fraude publicitária: geração de cliques falsos em anúncios, aumentando custos para anunciantes;

II - Roubo de credenciais: tentativas de acesso a contas usando credenciais roubadas;

III - Criação de contas falsas: uso do dispositivo comprometido como *proxy* para criação de contas em diversas plataformas;

IV - *Proxying* residencial: uso de dispositivos comprometidos para redirecionar tráfego através de redes domésticas, a fim de mascarar atividades maliciosas;

V - Ataques DDoS e disseminação de *malware*: dispositivos podem ser usados para ataques de negação de serviço ou para instalar *malware* adicional.

IV - Das recomendações para mitigação dos riscos

4.6. Para controlar e mitigar os riscos das ameaças da rede BADBOX 2.0, **recomenda-se ao público**:

I - Verificar dispositivos conectados quanto ao uso de lojas de aplicativos com configurações do *Google Play Protect* desativadas;

II - Evitar fontes não confiáveis: não baixar e instalar software, sistemas operativos e/ou *firmware* de fontes desconhecidas ou não confiáveis;

III - Efetuar atualizações de *software*: garantir que sistemas operativos, *software* e *firmware* estejam atualizados com os patches de segurança mais recentes;

IV - Desligar dispositivos suspeitos: isolar e desligar dispositivos que apresentem sinais de comprometimento, como *appstores* suspeitos, anúncios de conteúdo gratuito desbloqueado, ou ligações a servidores de comando e controle;

V - Usar dispositivos certificados: optar por dispositivos certificados pela Anatel e pelo *Google Play Protect*, de preferência de marcas conhecidas e confiáveis, evitando produtos de marcas desconhecidas;

4.7. Desde a descoberta da atividade do *malware* em TV Box pirata durante o primeiro semestre de 2025, a Agência tem determinado às operadoras de telecomunicações, no âmbito do Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do SeAC, a realização de bloqueios de domínios e IPs utilizados pela rede BADBOX 2.0 - medida essa que também foi adotada por outris países (https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241212_BadBox_Sinkholing.html).

4.8. Apesar da gravidade das ameaças cibernéticas causadas por TV Box pirata, sua mitigação enfrenta desafios técnicos, legais e operacionais. Esses equipamentos operam em redes domésticas com IPs dinâmicos, são vendidos irregularmente em lojas de comércio popular, até mesmo em *marketplaces*. Suas atividades maliciosas são discretas, dificultando a detecção. Além disso, questões legais impedem intervenções diretas em residências sem respaldo jurídico. Por isso, é necessário um esforço conjunto e coordenado entre diferentes órgãos para lidar com o problema de forma eficaz, reforçando a ampla divulgação do presente documento.

4.9. Por fim, ressalta-se a responsabilidade direta aos provedores de telecomunicações e internet. Nesse cenário, cabe aos provedores exercer papel ativo no enfrentamento desse risco, adotando medidas técnicas e operacionais que colaborem com a mitigação do uso de dispositivos clandestinos. Isso inclui o monitoramento de tráfego anômalo, a colaboração com autoridades reguladoras, o bloqueio de domínios maliciosos e o fortalecimento de práticas de segurança em suas redes. Além de uma medida técnica, trata-se de uma obrigação regulatória prevista no art. 10º do Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020.

5. DA PROPOSTA DE ENCAMINHAMENTO

5.1. Considerando os resultados obtidos, ao tempo em que a equipe integrante do Plano de Ação para Combate ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC) alerta sobre os relevantes riscos na prestação de serviços digitais, propõe-se a ampla divulgação do conteúdo desse estudo, em alinhamento à nova Estratégia Nacional de Cibersegurança, instituída pelo Decreto 12.753, de 4 de agosto de 2025.

Documento assinado eletronicamente por **Eduardo Hiroshi Murakami**, **Coordenador de Processo**, em 12/08/2025, às 09:44, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

Documento assinado eletronicamente por **Jamilson Ramos Evangelista**, **Assessor(a)**, em 12/08/2025, às 09:45, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **13720692** e o código CRC **45F2E7F5**.