Alerta da Agência Nacional de Telecomunicações

***Malware* BADBOX 2.0 em TV Boxes não homologadas**

ANATEL

Alerta da Agência Nacional de Telecomunicações

A Agência Nacional de Telecomunicações está emitindo este Anúncio de Serviço Público para alertar a sociedade sobre criminosos cibernéticos que exploram dispositivos conectados às redes de internet domésticas para realizar atividades criminosas usando a rede BADBOX 2.0. Esse tipo de *malware* pode comprometer a segurança dos dispositivos e dos dados dos usuários.

O que é a rede BADBOX 2.0

A BADBOX 2.0 é uma rede de dispositivos com sistema operacional Android conectados à internet que foram infectados com o *malware* BADBOX 2.0. Os criminosos cibernéticos usam essa rede para realizar atividades maliciosas sem que os donos dos dispositivos saibam.

Como funciona

Infecção: muitos dispositivos já vêm com o *malware* pré-instalado antes da compra, principalmente os de marcas desconhecidas. Outra forma de infecção acontece quando o usuário instala aplicativos de fontes não oficiais, que contêm códigos maliciosos.

Formação da rede: uma vez infectados e conectados à rede doméstica, esses dispositivos se tornam parte da rede BADBOX 2.0. Os criminosos podem controlar remotamente milhões desses aparelhos.

Atividades Maliciosas: A rede é usada para diversas atividades ilegais, como:

- Fraudes de anúncios: gerar cliques e visualizações falsas em anúncios para lucrar.
- Roubo de credenciais: acessar a contas usando credenciais roubadas;
- Criação de contas falsas: uso do dispositivo comprometido como *proxy* para criação de contas em diversas plataformas.
- Serviços de proxy residencial: vender o acesso a essas redes para que outros criminosos usem os endereços de IP dos usuários para esconder suas atividades.
- Distribuição de *malware* e ataques: usar a rede para lançar ataques de negação de serviço distribuídos (DDoS) ou espalhar outros tipos de vírus.

O BADBOX 2.0 é especialmente perigoso porque pode se manter nos dispositivos mesmo após reinicializações, e os cibercriminosos podem carregar novos códigos e módulos remotamente, permitindo que a ameaça evolua com o tempo.

Os criminosos cibernéticos conseguem acesso a redes domésticas usando dispositivos comprometidos. Isso inclui aparelhos de baixo custo, como:

- TV Boxes / dispositivos de *streaming*
- Tablets
- Sistemas de entretenimento de veículos
- Projetores Digitais
- Porta Retratos Digitais

Figura 1 - Imagem de TV Box apreendida pela Anatel

Dos estudos da Anatel sobre riscos cibernéticos de TV Boxes

A Anatel realizou diversos estudos e avaliações conduzidos pela equipe integrante do Plano de Ação ao Uso de Decodificadores Clandestinos do Serviço de Acesso Condicionado (SeAC), por meio de seu laboratório antipirataria, que realiza monitoramento de vários modelos de TV Boxes piratas disponibilizados ao mercado brasileiro.

Para realização do estudo pela Agência foram adotados os seguintes métodos:

- Seleção de amostra técnica de modelos não homologados com alta distribuição nacional;
- Monitoramento de tráfego em laboratório, com ênfase em conexões persistentes em modo *standby*;

- Engenharia reversa e análise de *firmware* para identificação de processos suspeitos;
- Cruzamento com Indicadores de Comprometimento (IoCs).

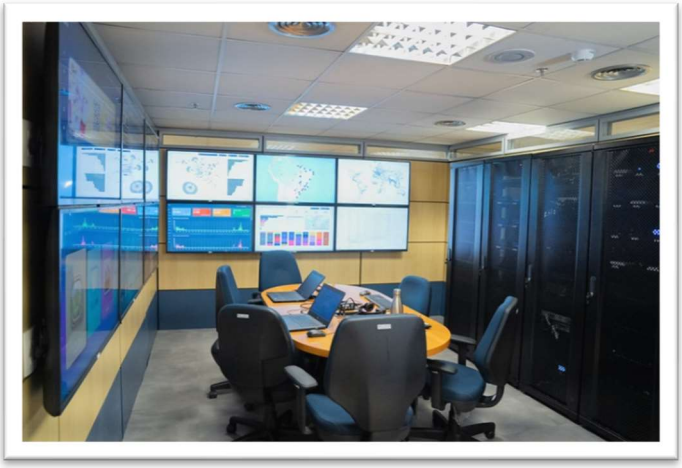

Figura 2 - Laboratório Antipirataria da Anatel

Desse estudo, constataram-se vulnerabilidades de segurança aos usuários e ameaça as redes de telecomunicações do país, levando aos seguintes resultados:

- Confirmação da presença de *malware* ativo e persistente nos dispositivos analisados (InXPlus e TouroBox);
- Identificação do processo malicioso operando com múltiplas portas abertas e conexões estabelecidas com servidores externos;
- Acesso aos mesmos domínios identificados nos estudos da empresa de segurança cibernética Human Security, disponíveis em https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/.
- Evidência de uso não autorizado como *proxy* residencial, incluindo acessos a sites de pornografia, bancos, justiça estadual e serviços públicos, sem conhecimento do usuário;
- Recebimento de arquivos suspeitos do tipo .jar através de conexões com servidores identificados;
- Indicação de que a infecção se iniciou em 2024, possivelmente via atualização remota de aplicativo.

Do aumento de dispositivos infectados no Brasil

Como forma de subsidiar seu trabalho, a equipe de inteligência da Anatel utilizou a plataforma Shadowserver Dashboard. Ela é uma plataforma da The Shadowserver Foundation que reúne e exibe, de forma visual e interativa, dados globais sobre ameaças cibernéticas 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 parcerias com provedores de serviço de acesso à internet, equipes de tratamento de incidentes cibernéticos (CSIRTs) e outras entidades.

No monitoramento da plataforma é possível verificar a evolução da contaminação do *malware* em dispositivos no Brasil, que aumentou de aproximadamente 340 mil IPs conectados entre fevereiro e maio desse ano para mais de 1,8 milhões em agosto:

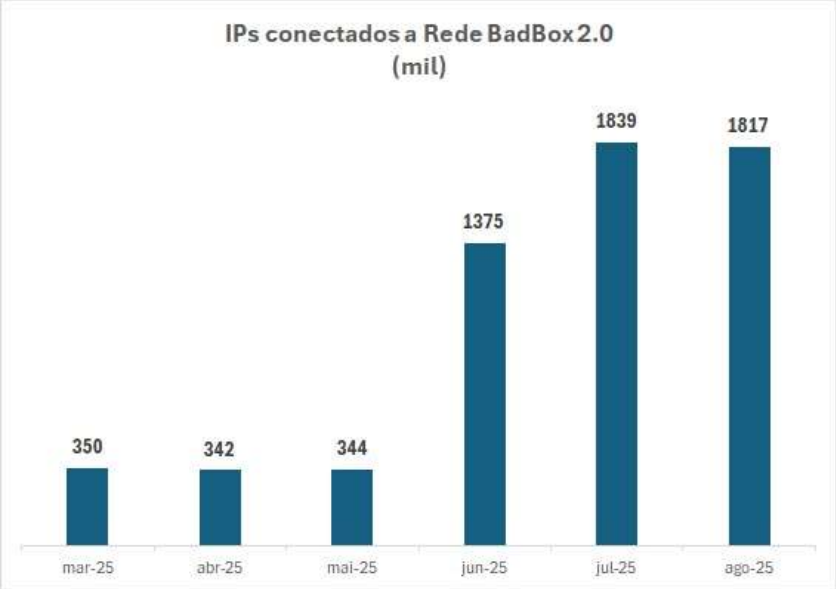

Figura 3 - IPs conectados a Rede BADBOX 2.0
Fonte: The Shadowserver Foundation 2025-Aug 25

Dos requisitos técnicos para homologação de TV Boxes

Com o intuito de conter a disseminação de TV Boxes voltadas à pirataria de obras audiovisuais, que colocam em risco as redes, serviços e usuários de telecomunicações, 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. Com o objetivo de auxiliar os usuários em uma consulta ainda mais específica sobre as TV Boxes homologadas.

Nesse sentido, a Anatel disponibilizou a relação dos modelos e demais informações relacionadas a esses produtos que foram submetidos e aprovados no processo de avaliação da Anatel, disponível no endereço https://www.gov.br/anatel/pt-br/regulado/certificacao-de-produtos/smart-tv-box-homologados.

Recomendações para controlar e mitigar os riscos das ameaças da rede BADBOX 2.0

- Verificar dispositivos conectados e tráfego de rede: avaliar todos os dispositivos na rede doméstica para detectar atividades suspeitas, como tráfego de rede incomum;
- Evitar fontes não confiáveis: não baixar e instalar software, sistemas operativos e/ou *firmware* de fontes desconhecidas ou não confiáveis;
- Efetuar atualizações de software: garantir que sistemas operativos, *software* e *firmware* estejam atualizados com os patches de segurança mais recentes;
- Desligar dispositivos suspeitos: isolar e desligar dispositivos que apresentem sinais de comprometimento, como marketplaces suspeitos, anúncios de conteúdo gratuito desbloqueado, ou ligações a servidores de comando e controle;
- Usar apenas TV Boxes certificadas pela Anatel.

Apesar da gravidade das ameaças cibernéticas causadas por TV Boxes piratas, 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 do setor público e privado, como provedores de telecomunicações e internet e a sociedade para lidar com o problema de forma eficaz.

Em Alinhamento à nova Estratégia Nacional de Cibersegurança, instituída pelo Decreto 12.753, de 4 de agosto de 2025, faz-se o presente alerta à sociedade sobre esse risco relevante na prestação de serviços digitais, possibilitando respostas rápidas e eficazes, ao mesmo tempo em que busca a conscientização dos usuários das redes de telecomunicações.

Referências:

Estratégia Nacional de Cibersegurança, instituído pelo Decreto nº 12.573, de 4 de agosto de 2025;

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

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

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

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

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;

Do monitoramento da quantidade de dispositivos infectados no Brasil:

(https://dashboard.shadowserver.org/statistics/combined/tree/?source=sinkhole&source=sinkhole6&date_range=1&data_set=count&auto_update=on).

Siga a Anatel

ANATEL