RUFANDO BOMB NEWS Notícias sem rodeios

Quinta-Feira, 06 de Agosto de 2026

Antenas Falsas Interceptam Sinais de Celulares em São Paulo e Rio para Aplicar Golpes por SMS

Criminosos usam equipamentos ilegais que bloqueiam 4G e forçam queda para 2G, disparando 100 mil mensagens fraudulentas diariamente

Mensagens sobre ganhos em apostas, ofertas de crédito e confirmação de compras falsas chegam aos celulares de vítimas através de um método sofisticado: antenas ilegais que interceptam sinais genuínos das operadoras e bloqueiam o serviço de dados moderno.

Desde o início de 2025, a Agência Nacional de Telecomunicações (Anatel) apreendeu 11 equipamentos ilegais, sendo nove instalados em São Paulo e dois no Rio de Janeiro. Porém, investigações indicam que essas infraestruturas criminosas operam também em outras localidades brasileiras.

A maioria desses aparelhos estava posicionada em zonas de alta concentração populacional, como os bairros paulistas de Pinheiros e Moema. **O motivo é estratégico: cada equipamento consegue disparar aproximadamente 100 mil mensagens fraudulentas por dia**, aumentando significativamente o número de possíveis vítimas.

Por meio dessas antenas ilegais, também conhecidas como ERBs fakes (estação rádio-base), os criminosos conseguem capturar o sinal da operadora e transmitir SMS maliciosos para usuários dentro de um raio aproximado de 2 quilômetros do aparelho. Essa exploração se baseia em uma vulnerabilidade de segurança presente na rede 2G, tecnologia mais antiga e menos protegida.

Segundo a superintendente de Fiscalização da Anatel, Gesiléa Teles, esses equipamentos representam um investimento substancial para os criminosos.

"Estamos falando de equipamentos que podem custar mais de R$ 100 mil. O que a gente acredita é que há criminosos especializados e com poder financeiro para comprar esse tipo de equipamento e treinar quem vai operá-lo", explicou.

Geralmente, as operadoras de telefonia denunciam essas atividades ilegais quando identificam interferências anormais em seus sinais. A Anatel mantém uma investigação conjunta com a Polícia Civil para rastrear os pontos de operação dessas ERBs fakes e compreender como elas chegam ao Brasil.

"Já teve caso em que encontramos um homem que estava montando a ERB fake. Ele pegava os componentes, montava e colocava no mercado ilegal. Foi uma investigação que envolveu as polícias do Rio de Janeiro e de São Paulo", relatou Gesiléa.

No Brasil, o uso de bloqueadores de sinal é autorizado apenas para determinados órgãos públicos, particularmente aqueles responsáveis pela administração de unidades prisionais. Essas instituições necessitam de autorização específica da Anatel para manter tal tipo de equipamento.

Operar antenas falsas é considerada atividade criminosa clandestina. Os infratores podem receber condenação de dois a quatro anos de detenção. Esse período pode ser aumentado em até 50% caso haja comprovação de dano a terceiros, além de multa de dez mil reais.

Método de localização das antenas ilegais

Após receber uma denúncia, a Anatel mobiliza uma equipe para a região indicada com o objetivo de localizar a antena ilegal. Os técnicos utilizam **analisadores de espectro**, instrumentos especializados na detecção de perturbações de sinal.

Esses aparelhos orientam a busca para os pontos onde as interferências atingem maior intensidade, facilitando a identificação do local exato. No entanto, essa etapa frequentemente exige vários dias, pois a antena falsa permanece propositalmente oculta da vista de transeuntes.

De acordo com as informações da agência, os indivíduos por trás desses crimes costumam alugar imóveis em andares elevados localizados em bairros movimentados. Permanecem nesses locais por períodos reduzidos, na tentativa de permanecer despercebidos pelas autoridades.

"Os criminosos tentam colocar esses equipamentos em lugares de grande movimento e, geralmente, com uma situação um pouco mais desenvolvida", comentou Gesiléa.

Após identificar o local preciso, a Anatel comunica à Polícia Civil, que solicita à Justiça autorização para adentrar o local. Em uma operação anterior, descobriu-se que uma antena havia sido instalada dentro de um veículo, utilizado para enviar mensagens em ruas congestionadas da capital paulista.

O esquema fraudulento compreende três componentes principais: a antena falsa propriamente dita, uma caixa preta que funciona como transmissor, e um computador portátil com software responsável por gerar e enviar as mensagens para pessoas situadas na zona de cobertura do equipamento.

Estratégias de proteção contra antenas falsas

A vulnerabilidade explorada nesse tipo de fraude está presente na rede 2G, conforme explicou Daniel Nunes, docente do Instituto Nacional de Telecomunicações. Essa tecnologia antiga permite que o celular se conecte a qualquer antena capaz de estabelecer comunicação com o aparelho.

"Nas gerações modernas, como 4G para cima, há uma autenticação de mão dupla: a rede autentica o dispositivo, e o dispositivo autentica a rede. No caso do 2G, a rede autentica o dispositivo, mas o dispositivo não autentica a rede", afirmou o especialista.

Aproveitando-se dessa falha, os criminosos interceptam o 4G e o 5G e forçam o telefone do usuário a "retroceder" para o 2G. Dessa forma, mesmo em regiões com grande fluxo de pessoas, o dispositivo recebe a impressão equivocada de estar em uma zona remota, com cobertura de sinal limitada.

"Isso é praticamente impossível de ser feito em móveis que estão do 4G para cima", destacou o professor, recomendando que os usuários mantenham seus celulares conectados exclusivamente a redes mais recentes e bloqueiem o acesso por intermédio de antenas 2G.

No Android, essa opção geralmente está disponível em um caminho similar a: **Configurações > Conexões > Redes móveis**. Posteriormente, desative a opção "**Permitir serviço 2G**" – os termos podem diferir conforme o fabricante do aparelho.

No iPhone, acesse: **Ajustes > Privacidade e Segurança > Modo de Isolamento**. Selecione "**Ativar o Modo de Isolamento**" e confirme – embora esse recurso aumente a proteção, pode limitar o funcionamento de outros aplicativos.

Para se resguardar contra fraudes via SMS, recomenda-se evitar clicar em links ou atender a solicitações de download de programas recebidas nesses tipos de mensagem. Igualmente importante é manter o sistema operacional constantemente atualizado, garantindo acesso às proteções de segurança mais recentes.