FBI desmantela infraestrutura do grupo Handala à medida que operações cibernéticas ligadas ao Irão escalam

written by O Cidadão | 21 de Março, 2026

Como explica Gil Messing, Chief of Staff da Check Point Software: ***"Desativar os websites e canais do Handala atinge-os onde mais importa. As suas operações dependem fortemente da publicação de conteúdos para criar impacto psicológico, muitas vezes exagerando os danos para amplificar o medo. Interromper a sua capacidade de difusão compromete esse efeito. No passado, tentaram contornar estas ações criando rapidamente novos canais, mas este continua a ser um ponto crítico de pressão."***

Em paralelo, registou-se um movimento particularmente

relevante:
Durante os alertas desta manhã, enquanto civis corriam para abrigos, receberam duas mensagens SMS. Uma continha ameaças diretas de morte com ligação a um website suspeito, a outra imitava uma aplicação do Home Front Command. Esta última foi enviada enquanto as pessoas procuravam abrigo, alegando ser a melhor aplicação para proteção. **No entanto, tratava-se de uma app maliciosa que descarregava um ficheiro capaz de causar danos reais em dispositivos Android.**

Este episódio representa uma evolução significativa, combinando um ataque físico com um ataque cibernético, explorando um sistema de envio massivo de SMS, tudo isto em simultâneo com o lançamento de mísseis contra o país.

É a primeira vez que se observa esta combinação de ataque físico, sirenes e mísseis, com uma ofensiva cibernética direcionada a cidadãos através dos seus telemóveis. O facto de ocorrer de forma sincronizada, ao minuto, e com envio de mensagens ameaçadoras, torna este caso único na integração destas dimensões.

Mais detalhes da Check Point Research:

Durante a manhã em Israel, às 6h55, em paralelo com sirenes ouvidas no centro do país e noutras localizações, cidadãos israelitas receberam duas mensagens SMS enviadas por atores iranianos. As mensagens incluíam desinformação agressiva como: ***"Netanyahu está morto. A morte aproxima-se de ti e em breve os portões do inferno abrir-se-ão diante de ti"***, acompanhadas de um link para um website que provavelmente continha conteúdo malicioso, entretanto removido.

Simultaneamente, foram distribuídas mensagens que imitavam o Home Front Command, incentivando a população a descarregar uma aplicação para **"localizar abrigos"**. Segundo a análise dos investigadores da Check Point, os links direcionavam para o download da aplicação maliciosa "ShelFriend", que permite ao

atacante acesso total ao dispositivo móvel, incluindo localização, câmara, ficheiros, fotografias, lista de contactos e leitura de SMS. A página da aplicação indicava ainda ser **“alimentada pela Atraf**”, um website que já tinha sido comprometido por atores iranianos no passado.

Existem também indícios do uso sistemático de ferramentas de **inteligência artificial** para traduzir e adaptar mensagens ao público israelita, bem como para acelerar a sua distribuição, permitindo um impacto psicológico alargado num curto espaço de tempo.

A operação caracteriza-se pela imitação de linguagem oficial e pela inclusão de elementos que reforçam credibilidade, como interfaces visuais aparentemente legítimas e indicadores de confiança.

Os atacantes recorrem ainda a plataformas de distribuição existentes, incluindo sistemas de email e serviços de SMS, utilizando infraestruturas legítimas e nomes de remetentes familiares, aumentando a perceção de autenticidade das comunicações.