RUFANDO BOMB NEWS Notícias sem rodeios

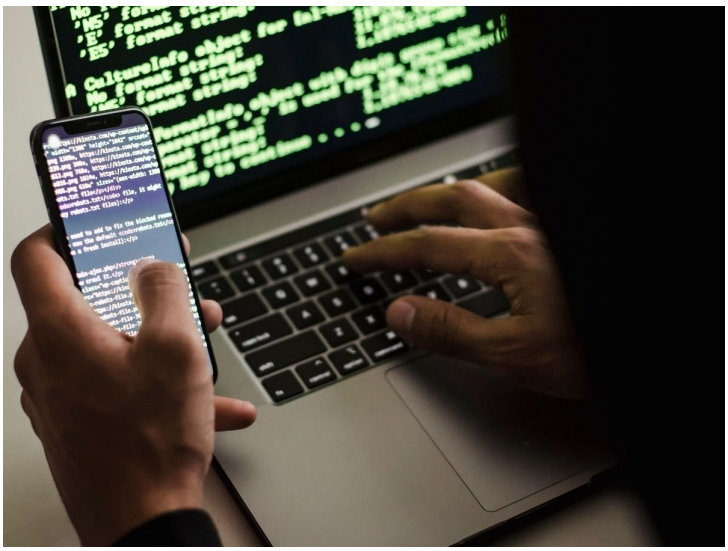
Quinta-Feira, 27 de Agosto de 2026

Invasor do Sistema de Alertas da Defesa Civil Aprendeu a Usar Plataforma em Curso Governamental

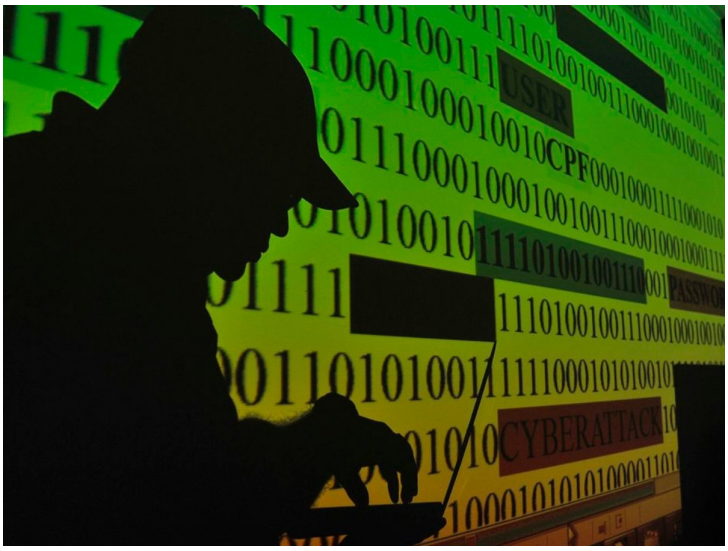
Ministério explica que hacker utilizou credenciais vazadas e conhecimento adquirido em treinamento para disparar alerta falso

O Ministério da Integração e do Desenvolvimento Regional apresentou nesta sexta-feira (10 de julho) um relatório detalhado à Câmara dos Deputados explicando as circunstâncias do incidente que comprometeu o sistema de alertas da Defesa Civil. De acordo com o documento, o criminoso responsável pelo envio do alarme fraudulento obteve seus conhecimentos técnicos por meio de cursos disponibilizados pela própria plataforma estatal.

"Um indivíduo que se identifica como Misantropi4 utilizou acesso válido à plataforma IDAP, obteve instruções através de tutoriais de capacitação presentes no portal governamental e conseguiu disparar mensagens de alerta tipo Defesa Civil para múltiplos municípios", informou a instituição em comunicado oficial.

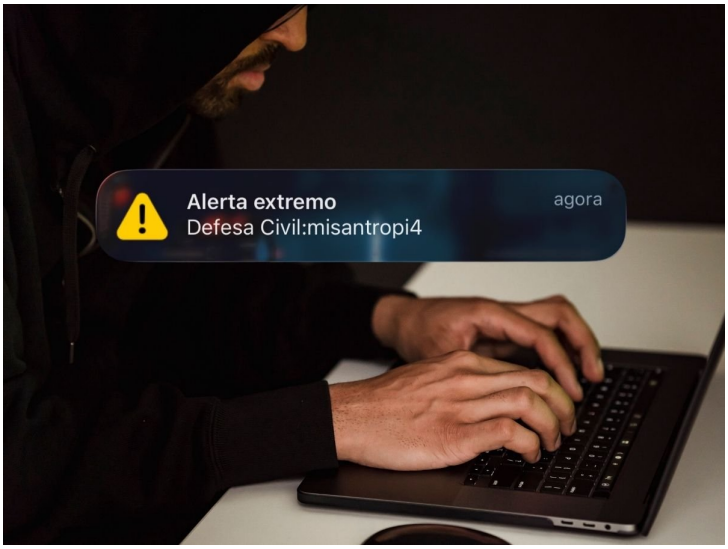


O incidente ocorreu durante a noite de 19 de junho e nas primeiras horas de 20 de junho, quando centenas de milhares de cidadãos brasileiros receberam em seus telefones móveis um aviso sonoro de nível crítico acompanhado de uma mensagem textual da Defesa Civil com referência ao apelido "Misotropi4".



A resposta ministerial foi encaminhada em atendimento a um pedido formal do deputado Gustavo Gayer (PL-GO), que havia solicitado esclarecimentos sobre o episódio através de requerimento protocolado na Casa Legislativa.

Conforme relato da pasta, a detecção do problema ocorreu às 23 horas e 59 minutos do dia 19 de junho. Após identificar a invasão, o ministério procedeu imediatamente com o bloqueio das contas comprometidas e removeu conteúdo malicioso do sistema. Investigações conduzidas pela Polícia Federal continuam em andamento para identificar e responsabilizar o autor.



O ministério revelou que as credenciais de acesso foram expostas em um canal de comunicação do Telegram e que uma falha de segurança na plataforma foi aproveitada durante a execução do ataque. Porém, segundo informações fornecidas no documento, "ambas as vulnerabilidades foram completamente remediadas".

A instituição garantiu que a infraestrutura central do ministério não sofreu qualquer comprometimento e implementou um conjunto amplo de medidas para fortalecer a proteção cibernética. As ações corretivas incluem o bloqueio permanente das contas indevidas, restrição de acesso apenas para usuários dentro da rede ministerial, ativação de autenticação em duas etapas e exigência de conexão via VPN para órgãos de Defesa Civil que utilizem a plataforma.