Notícia ⓘ Estadão / Brasil

Login e senha comprometidos são principal hipótese para alerta de ‘misantropia’, dizem especialistas

Profissionais de cibersegurança avaliam que credenciais vazadas ou roubadas podem ter sido usadas para o envio de alertas falsos da Defesa Civil em diferentes regiões do País; PF investiga disparos

Por Redação
20/06/2026 | 18h26 Atualização: 20/06/2026 | 19h35

Falso alerta da Defesa Civil foi recebido no Distrito Federal, Paraná, Rio de Janeiro e São Paulo e gerou uma onda de brincadeiras nas redes sociais. Crédito: Edição: Jefferson Perleberg

Credenciais comprometidas são a principal hipótese para explicar o disparo de alertas falsos atribuídos à Defesa Civil Nacional entre a noite de sexta-feira, 19, e a madrugada deste sábado, 20, segundo especialistas em cibersegurança ouvidos pelo **Estadão**. O caso chamou atenção pelo conteúdo incomum das mensagens, que chegaram a diferentes celulares com variações estranhas, **incluindo a exibição da palavra “misantropia”** e textos desconexos. O episódio levou à retirada do sistema ‘Defesa Civil Alerta’ do ar, em meio à suspeita de que o incidente tenha ocorrido a partir do uso indevido de acessos válidos ao sistema, em vez de uma falha técnica complexa ou ataque direto à infraestrutura.

Para o diretor de tecnologia da Scunna, **Ricardo Dastis**, ainda não é possível chegar a uma conclusão, mas o cenário mais provável é o de que credenciais de acesso (como login e senha) ao sistema da Defesa Civil tenham sido comprometidas por meio de um vazamento e utilizadas de forma indevida.

“Neste momento, ainda é cedo para uma conclusão definitiva, uma vez que as investigações oficiais seguem em andamento. No entanto, as informações que vêm circulando ao longo deste sábado em comunidades e canais especializados em segurança cibernética apontam para um possível comprometimento de credenciais de acesso ao sistema”, disse.

“Segundo esses relatos, os controles de autenticação existentes seriam insuficientes para proteger adequadamente um ambiente com esse nível de criticidade. A hipótese mais comentada é que o atacante tenha realizado buscas em bases de credenciais previamente vazadas na Internet, identificando combinações válidas de usuários e senhas associadas ao sistema. De posse dessas credenciais, teria simplesmente testado o acesso diretamente na aplicação e obtido sucesso na autenticação”, explica Dastis.

“Caso essa hipótese venha a ser confirmada pelas investigações, estaríamos diante de um ataque cibernético deliberado baseado em comprometimento de credenciais, e não necessariamente na exploração de uma vulnerabilidade técnica sofisticada do sistema”, afirma.

Segundo Dastis, informações como origem dos acessos, horários de conexão, padrões de uso e eventuais logins com credenciais legítimas a partir de dispositivos ou localidades incomuns são essenciais para reconstruir a sequência do incidente e determinar a forma de acesso ao sistema. Esses elementos, afirma, permitem diferenciar se houve ação indevida, falha técnica ou uso de credenciais válidas por terceiros não autorizados.

“Se as informações divulgadas até o momento se confirmarem, este caso reforça uma tendência cada vez mais comum na segurança cibernética moderna: ataques bem-sucedidos muitas vezes não dependem de técnicas avançadas de invasão, mas sim da utilização de credenciais legítimas previamente comprometidas”, diz o CTO da Scunna.

De acordo com o Ministério da Integração, 10 alertas falsos foram disparados, mas não é possível, no momento, estimar em quantos celulares soaram as notificações. Foram 9 alertas pelo sistema Cell Broadcast e 1 pelo sistema de mensagens SMS.

O Cell Broadcast é uma tecnologia de transmissão que permite o envio de alertas simultaneamente para todos os celulares conectados a antenas de uma área específica, sem precisar de internet ou do número de telefone.

Segundo **Diogo Cortis**, professor da PUC-SP e doutor em Tecnologias da Inteligência e Design Digital, o Cell Broadcast em si não aparenta ter vulnerabilidades estruturais relevantes. Ele afirma que plataformas desse tipo são amplamente utilizadas no mundo e, em geral, apresentam operação estável.

Para Cortis, os principais riscos costumam estar na camada de acesso administrativo. “O que acontece é que as vulnerabilidades, muitas vezes, podem estar mais nesse acesso administrativo. Então se existir uma falha de configuração, se a rede da onde isso está sendo operado for vulnerável, se o servidor não for bem configurado, aí você cria mais chances de acesso de ataques indevidos”, disse.

Na avaliação de **Arthur Igreja**, referência em tecnologia no Brasil, os alertas indicam que houve uso indevido de um sistema com alcance nacional e capacidade de acionar operadoras de telefonia em diferentes regiões do País. Ele afirma que o conteúdo foi enviado como se fosse legítimo, o que reforça a suspeita de uso irregular do próprio mecanismo de emissão.

“Alguém fez uso de um sistema que consegue ter esse alcance, chegou até lá e enviou a mensagem como se verdadeira fosse, mas não era o caso. A questão é essa, como que esse sistema, que faz um disparo para as operadoras, e as operadoras cumpriram isso, fizeram a entrega”, disse.

Para ele, a principal preocupação está na forma como o sistema foi acessado. “A grande vulnerabilidade que fica exposta é como que alguém conseguiu acessar esse sistema em diferentes regiões, porque o sistema é georreferenciado,