That annoying SMS phish you just got may have come from a box like this

The researchers added: “This campaign is notable in that it demonstrates how impactful smishing operations can be executed using simple, accessible infrastructure. Given the strategic utility of such equipment, it is highly likely that similar devices are already being exploited in ongoing or future smishing campaigns.”

Sekoia said it’s unclear how the devices are being compromised. One possibility is through CVE-2023-43261, a vulnerability in the routers that was fixed in 2023 with the release of version 35.3.0.7 of the device firmware. The vast majority of 572 identified as unsecured ran versions 32 or earlier.

CVE-2023-43261 stemmed from a misconfiguration that made files in a router’s storage publicly available through a web interface, according to a post published by Bipin Jitiya, the researcher who discovered the vulnerability. Among other things, some of the files contained cryptographically protected passwords for accounts, including the device administrator. While the password was encrypted, the file also included the secret encryption key used and an IV (initialization vector), allowing an attacker to obtain the plaintext password and then gain full administrative access.

The researchers said that this theory was contradicted by some of the facts uncovered in their investigation. For one, an authentication cookie found on one of the hacked routers used in the campaign “could not be decrypted using the key and IV

described in the article," the researchers wrote, without elaborating further. Further, some of the routers abused in the campaigns ran firmware versions that weren't susceptible to CVE-2023-43261.

Milesight didn't respond to a message seeking comment.

The phishing websites ran JavaScript that prevented pages from delivering malicious content unless it was accessed from a mobile device. One site also ran JavaScript to disable right-click actions and browser debugging tools. Both moves were likely made in an attempt to hinder analysis and reverse engineering. Sekoia also found that some of the sites logged visitor interactions through a Telegram bot known as GroozaBot. The bot is known to be operated by an actor named "Gro_oza," who appears to speak both Arabic and French.

Given the prevalence and massive volume of smishing messages, people often wonder how scammers manage to send billions of messages per month without getting caught or shut down. Sekoia's investigation suggests that in many cases, the resources come from small, often-overlooked boxes tucked away in janitorial closets in industrial settings.

https://arstechnica.com/security/2025/10/that-annoying-sms-phish-you-just-got-may-have-come-from-a-box-like-this/