Smishing Campaigns Exploit Cellular Routers to Target Belgium - Against

Data: 2025-10-01 11:11:40

Autor: Inteligência Against Invaders

A newly identified wave of smishing attacks has been traced to exploited Milesight Industrial Cellular

Routers.

According to research by Sekoia.io’s Threat Detection & Research (TDR) team, the routers’APIs were abused to send phishing text messages –a tactic that has repeatedly targeted Belgian users by impersonating official government services.

The malicious activity was first detected on July 222025, when honeypots recorded suspicious requests. Investigators found the routers had been manipulated to send SMS messages containing phishing links, often disguised as communications from CSAM and eBox (two widely used Belgian government platforms). Messages were written in Dutch and French and consistently featured Belgium’s +32 country code.

Sekoia noted that over 19,000 routers of this type are accessible on the public internet. Of these, at least 572 are exposed to unauthenticated access, enabling attackers to send or retrieve SMS messages. Logs suggest the technique has been used since at least February 2022.

Belgium in the Crosshairs

Although campaigns have reached France, Italy, Sweden and other countries, Belgium remains the most frequent target.

Between November 2022 and July 2025, multiple distinct operations impersonated federal authentication and digital mailbox services. In June and July 2025 alone, several new phishing domains mimicking these services were registered.

The smishing campaigns often follow a validation phase: attackers test whether a compromised router can send SMS messages by directing initial texts to numbers they control. Once confirmed, the devices are used to launch mass phishing waves.

Read more on phishing tactics targeting government platforms: Home Office Phishing Scam Targets UK Immigration Sponsors

Wide-Reaching Fraud

The infrastructure supporting these campaigns appears tied to Lithuanian hosting provider Podaon, with phishing domains frequently registered through NameSilo. Some sites even employed scripts to restrict access from non-mobile devices, limiting detection by analysts.

Sekoia.io’s findings highlight how vulnerable equipment is leveraged to conduct wide-reaching fraud. The campaigns typically impersonated services such as:

- Belgian CSAM and eBox
- French banking and postal organizations
- Telecom providers in Sweden and Denmark

A Persistent Threat

“Smishing continues to represent a significant and evolving threat,”Sekoia researchers warned.

By exploiting relatively unsophisticated devices, attackers can operate at scale, distributing fraudulent messages across multiple countries.

“In light of this, heightened vigilance remains essential. Users should be cautious of unsolicited messages – especially those containing shortened or suspicious URLs, spelling or grammatical errors or urgent calls to action,”the company explained.

“Awareness and scepticism are among the most effective defences against smishing attempts, which increasingly target both individuals and organisations on a global scale.”