An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2506120143

NCSC Advisory

SMS Pumping

17 June 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

Description

The NCSC has received reports of SMS Pumping attacks targeting Irish organisations.

SMS Pumping, also referred to as **SMS toll fraud** or **artificial traffic inflation**, is a type of fraud where attackers exploit application SMS verification features such as One-Time Passwords (OTPs) or sign-up flows, to trigger a high volume of messages to premium or international numbers.

The attackers profit by receiving a share of the inflated SMS termination fees often by colluding with rogue telecom carriers at the expense of the victim organisation.

This can lead to significant financial loss due to excessive telecom bills, infrastructure overload from the increased traffic, reputational damage and possible fraud liability.

Here is how the attack works, how to protect your organisation and tips on how to detect a SMS Pumping attack.

How SMS Pumping Works

1. **Trigger Abuse**: Attackers deploy automated scripts or bots to exploit SMS-sending features generating large volumes of outbound messages.
2. **Number Targeting**: These messages are directed to phone numbers with high SMS termination fees, typically premium-rate or international numbers controlled by the attackers or their partners.
3. **Revenue Sharing**: Often the attackers collaborate with fraudulent or complicit telecom providers, receiving a portion of the inflated SMS termination revenue generated by the artificially increased message traffic. Sometimes the motivation could just be to cause the target org increased costs.

Prevention Measures

1. **Rate Limiting**: Enforce strict per-IP and per-user limits on SMS-triggering endpoints and implement exponential backoff for retries.
2. **Intelligence Checks**: Leverage services to:
    - Block high-risk destinations (e.g., premium-rate regions).
    - Detect and block VOIP, virtual, or premium-rate numbers.
3. **CAPTCHA Integration**: Require CAPTCHA on all public SMS-triggering forms.
4. **Geo-Fencing**: Limit SMS sending to specific countries where you operate and use allow/deny lists for country codes based on business needs.
5. **Phone Number Validation**: Enforce E.164[1] number format and use robust validation to filter out fake or malformed numbers before sending SMS.

[1] https://www.twilio.com/docs/glossary/what-e164

6. **Multi-Factor Abuse Detection**: Combine user behavior, IP reputation, velocity, and historical patterns to detect automated abuse attempts.

Mitigation Steps

1. **Shut Down the Attack Vector**: Temporarily disable or rate-limit the affected form or endpoint.
2. **Investigate Audit Logs**: Review the SMS logs, IPs, user agents, and geolocation data to understand the scope of the abuse.
3. **Coordinate with SMS Gateway Provider**: Alert your SMS provider - they may help trace fraudulent activity, apply filters, or provide chargeback support.
4. **Blacklist Numbers/Regions**: Block further traffic to affected number prefixes or country codes.
5. **Refactor SMS Flow**: Consider implementing email-based verifications for suspicious or high-risk regions.
    - Require phone verification only after CAPTCHA or account creation.
6. **Report the Abuse**: If you are the victim of an SMS Pumping attack report the incident to the Gardai and notify your telecom/SMS gateway and relevant fraud monitoring services.

Detection Tips

1. Sudden spike in SMS volume without a matching rise in new users.
2. SMS sent to low-traffic or previously unused countries.
3. Repeated requests from the same IP or IP range.
4. Clusters of random phone numbers sharing common prefixes.

Further Reading

- https://www.group-ib.com/blog/sms-pumping/
- https://www.twilio.com/docs/glossary/what-is-sms-pumping-fraud