SMS Spoofing

>>> Best Practice <<<

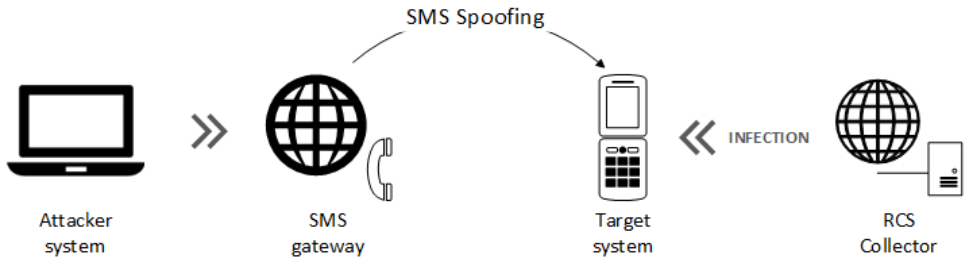
SMS spoofing is a technique to set who a message appears to come from, by replacing the originating mobile number (Sender ID) with a different one, or with an alphanumeric text.

It is not possible to change the Sender ID parameter while sending a message through RCS RMI 3G modem, but it is possible to mask it applying SMS spoofing through external services.

Some mobile operators provide special services that allow displaying a name instead of the number, typically for advertising purposes. This is a common social engineering technique and it can succeed by verifying one by one all mobile operators within the country, asking for this kind of service.

Another good alternative is to use external SMS gateways that allow changing the Sender ID.

Several software and online platforms provide this type of service. You will be able to modify the Sender ID field and the text message field, pointing to the backdoor created by Remote Control System (QR Code / Web Link).



There are many services on Internet providing such service. Just search Google for "**sms gateway sender id**".

It is important to highlight that remote Agents generated through RCS Console (like QR Code / Web Link) are **one shot**: the first connection will trigger the backdoor download and will **delete** the file on the Collector.

SMS spoofing online services

- ✓ Atomic SMS Sender (http://www.massmailsoftware.com/bulksmsandpager)
- ✓ CM Telecom (http://www.smsgateway.to)
- ✓ DiGi Messaging (http://www.digimessaging.com)
- ✓ fm SMS (http://www.fmsms.com)
- ✓ My Cool SMS (http://www.my-cool-sms.com)
- ✓ SMS Country (http://www.smscountry.com)
- ✓ SMS Gateway Center (http://www.smsgatewaycenter.com)
- ✓ SMS Global (http://www.smsglobal.com)