SMS Spoofing

> > > Best Practice < < <

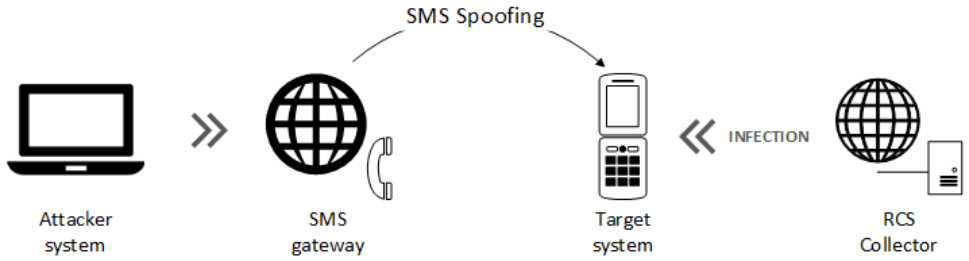
SMS Spoofing is a technique that disguises the identity of the sender of a message. The message appears to come from a sender's name rather than the sender's phone number. The sender's name, of course, will be a fake.

The RCS Remote Mobile Infection allows users to use spoofing techniques to hide the number and avoid detection.

SMS gateways are easily available for purchase on line. These permit choosing a sender name, and so SMS gateways provide an easy and effective way to disguise the true identity of the RMI.

Additionally, many mobile operators provide services that allow displaying a name instead of the number, typically for advertising purposes. Users can take advantage of this service to increase the chances of success when using social engineering to infect a suspect's mobile phone.

These techniques can be combined with services available on the Remote Control System such as Web Link. For example, the Web Link can be sent to a suspect's phone number with the origin of the message hidden.



There are many services on Internet providing such service. Here are a few examples:

- ✓ 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)

It is important to highlight that remote Agents generated through the Console (like QR Code / Web Link) can only be used one time. The first connection will trigger the backdoor download and will **delete** the file on the Collector.