]HackingTeam[

RCS Remote Mobile Infection

Whitepaper

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Document Approval

Revision	Author(s)	Release Date
1.0	Valeriano Bedeschi	10th January 2012

Table Of Contents

1 Overview

RMI is a *Remote Control System* (RCS) module designed to install RCS agents on mobile phones.

Installing RCS agents on smartphones from remote is not an easy task. Worse yet, the requirement of having physical access to the device greatly decreases the effectiveness of the solution for smartphones.

Remote Mobile Infection (RMI) makes the task *easy*, *repeatable* and *effective*.

A special SMS is sent to the remote device by means of a GSM modem. When the SMS is received, upon acceptance of the message by the user a browser is automatically opened and a payload downloaded from the URL embedded in the message.

Since the text of message can be customized, *social engineering* techniques can be applied to their full extent: by pretending to be the telecom operator offering promotions or updates, chances of success are increased by a relevant margin.

RMI ease of use make it the most effective way of deploying RCS on smartphones form remote.

Message delivery to remote targets is done using common cellular protocols, such as GSM, Edge, 3G or UMTS, and is supported by most mobile carriers around the world.

Following the choice of having an unified management, RMI is fully integrated into the RCS Console and is very easy to use: to perform an installation, only the target mobile phone number is required.

1.1 Types of messages

RMI supports different methods for sending messages, each differing in the way the message is presented to the target user once received.

1.1.1 Update Notification

By using a dedicated GSM modem an update request can be crafted and sent to a remote mobile device.

According to mobile device security settings (i.e. strict) and the platform targeted (e.g. Blackberry, Windows Mobile), the notification message is presented to the user asking for confirmation: for installation to complete, the user have to confirm.

NOTE Blackberry and Symbian phones WILL notify the user asking how to proceed, either installing update or discarding the message.

1.1.2 Web Redirection

By forcing startup of a web browser and forcing redirection to a specified website, an installation package for an RCS agent will be downloaded and executed.

Adding carefully chosen text, the user can be tricked in accepting the message, increase the effectiveness of the attack.

1.1.3 Service Notification

This attack delivers an active notification to remote devices which pops-up a window containing a custom message and URL link. Once the message is accepted, mobile phone's browser is automatically redirected to the specified URL and the infection takes place.

2 FAQ

DOES RMI PERFORM A MAN-IN-THE-MIDDLE ATTACK?

No, RMI doesn't perform a MITM attack. Its only function is to redirect target's browser toward a URL where a RCS backdoor is located.

DOES RMI ACT LIKE A FAKE BTS?

No, RMI is not an active tool like a BTS, for this reason there's no need to be close to the target device.

DOES RMI USE A FAKE APN?

No, RMI doesn't use a fake APN.

DOES RMI RELY ON ANY VULNERABILITY?

No, RMI takes advantage of some features of the GSM standard to craft a special message.

WHAT ARE THE BEST AND WORST CASE SCENARIO?

Best case: the backdoor is automatically run on the target device, without any kind of user interaction. Worst case: target's browser asks for permission to install the backdoor.

WHICH PHONES SUPPORT RMI INFECTION?

Windows Mobile, BlackBerry, Symbian and Android.

DOES RMI WORK ON ANY PROVIDER?

RMI works on every provider unless they are actively filtering this type of messages.