]HackingTeam[

RCS Remote Mobile Infection

Datasheet

THIS DOCUMENTATION IS STRICTLY CONFIDENTIAL

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.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

Remote Mobile Installation (RMI) is a module for the *Remote Control System* (RCS) platform designed to install RCS Agents on mobile phones.

Installing RCS Agents on smartphones from remote, without any help, is not an easy task. Worse yet, if remote installation fails, installation may become a tough task: it may be impossible to have physical access to the device.

Remote Mobile Infection (RMI) makes remote installation *easy*, *repeatable* and *effective*.

RMI works by sending a wap-push message to the target smartphone. When the SMS is received and accepted by the user, a browser is automatically opened and the Agent installation package is downloaded from the URL embedded in the message.

The text message can be customized, thus enabling use of *social engineering* techniques to their full extent: for example, by pretending to be the telecom operator offering promotions or updates, chances of success in installation of the Agent are dramatically increased.

Message delivery to the mobile phone is done using common cellular protocols, such as GSM, Edge, 3G or UMTS, and is supported by the vast majority of the mobile operators all over the world.

RMI is fully integrated into the RCS Console and is therefore very easy to use: to perform an installation, you just need the mobile phone number.

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.

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 and the target platform (e.g. Blackberry, Windows Mobile), the notification message is presented to the user asking for confirmation: for installation to complete, the user must confirm.

NOTE Blackberry and Symbian phones WILL ask the user how to proceed, either to install the update or discard the message.

1.1.2 Web Redirection

By forcefully starting the web browser and redirecting to the specified website, the Agent installation is downloaded and executed.

Adding carefully chosen text, the user is tricked in accepting the message, increasing the effectiveness of the attack.

1.1.3 Service Notification

This attack opens a window containing a custom message and a URL link. Once the target accepts the message, the web browser is automatically redirected to the URL, thus starting the Agent installation.

2 FAQ

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

No, RMI doesn't perform a MITM attack. It works by redirecting the 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: 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 wap-push messages, which are part of the GSM standard.

WHAT ARE THE BEST AND WORST CASE SCENARIO?

In the best case, the backdoor is automatically run on the target device, without any kind of user interaction. On the contrary, in the worst case the device asks for permission to execute the payload located at the specified URL, thus requiring some social engineering to trick the user into accepting the message.

WHICH PHONES SUPPORT RMI INFECTION?

RMI can be used on smartphones that run Windows Mobile, BlackBerry, Symbian or Android operating systems.

DOES RMI WORK ON ANY PROVIDER?

RMI works on every provider unless they are actively blocking wap-push messages.