]HackingTeam[

Remote Mobile Infection

Different techniques are available for carrying out a remote installation of Remote Control System against target mobile devices connected to mobile networks.
Most commonly available mobile networks are supported, such as GSM, Edge, 3G, Umts.

How it works?
By using a GSM modem connected to RCS environment our product is capable of forging custom messages which are being delivered to remote targets.
Such messages, according to specific attack techniques (described below) may contain commands or payloads which eventually infects a remote target.

How much is difficult to use?
By using our integrated RCS Console application it's very easy to deliver such attacking messages to remote phones. There's no need to perform complex manual activities.

Remote Update Notification

By using a dedicated GSM modem device an update request is being forged and notified to a remote mobile device.
According to Mobile device security settings and Mobile platform chosen, the notification message will execute the update remotely.

Please note: Blackberry and Symbian will notify the user asking how to proceed (install update or discard).

Remote Web Redirection

By using a dedicated GSM modem device a URL forced redirection is being delivered and executed (browser is opened and automatically redirected to chosen URL).
Such attack takes advantage of social engineering techniques in order to increase the impact rate.

Remote Service Notification

A variant of the above attack techniques is also available within Remote Control System.
Such attack will deliver an active notification to remote devices which it will popup a window containing a custom message and URL link.

Once the message has been accepted, mobile phone is automatically redirected to the specified URL and infection takes place, according to device security settings.

]HackingTeam[

Injection Proxy for Mobile Networks

A different approach for remotely installing RCS to mobile devices is also available by setting up Injection Proxy Appliance over WIFI or APN GSM network.

By using the same technology used for Injection Proxy on fixed networks, it's possible to remotely attack mobile devices over wireless networks or GSM networks.

In order to perform the attack it is required to be on the same network segment of the mobile device under attack.

The attack will replace the content downloaded by the user with RCS installation payload.

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?
Not strictly. 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 intervention. Worst case: target's browser will ask permission to install the backdoor package.

Which factors affect the scenario outcome?
It depends both on the policies embedded into the device itself and on the default browser. Generally speaking the execution always works, even tough on Symbian devices, due to system constraints, the user will always be asked to confirm the installation.

Which phones support RMI infection?
Windows Mobile, BlackBerry, Symbian, Android but not iPhone.

Do I need some information on the device before performing the attack?
The only information needed at this point is the operating system type, that is: Windows Mobile, BlackBerry or Symbian.

Does RMI work on any provider?
RMI works on every provider unless they are actively filtering this type of messages.

]HackingTeam[