]HackingTeam[

Remote Control System

RCS Prerequisites

1 Overview

This document details all the prerequisites needed to perform a correct installation of *Remote Control System*. All the prerequisites must be fulfilled in order to successfully operate the system.

All the hardware must be installed and connected properly, and all the network equipments must be installed and connected following the constraints of each component.

2 RCS Components

2.1 RCS Database

OPERATING SYSTEM: *Windows Server 2008 R2* (English)
NETWORK CONNECTIONS
INBOUND: 4443/TCP
OUTBOUND: 25/TCP, normal system activity (name resolution, system updates...)

RCS Database should have a private ip address, and should not be accessible from the Internet.

If an external storage is provided, it must be mounted as folder in *C:\RCSDB* path, otherwise if a data partition is available on the internal disk, it must be mounted in *C:\RCSDB* path in order to provide data storage.

If *RCS Remote Mobile Installation* must be used, carrier signal in physical location of *RCS Database* must be available.

2.2 RCS Collector

OPERATING SYSTEM: *Windows Server 2008 R2* (English)
NETWORK CONNECTIONS
INBOUND: 80/TCP
OUTBOUND: 4444/TCP, normal system activity (name resolution, system updates...)

RCS Collector could have a public ip address, and must be directly accessible from the Internet on port 80/TCP. Using a private ip address and redirecting incoming traffic using NAT is recommended.

A network connection to *RCS Database* must be possible on port 4443/TCP.

A network connection to *RCS Injection Proxy* must be possible on port 4444/TCP.

Public ip address configured on *RCS Collector* or used for NAT must be static.

2.3 RCS Console

OPERATING SYSTEM: Any supported by *Adobe AIR* (*Windows 7* is recommended)
NETWORK CONNECTIONS
INBOUND: none
OUTBOUND: 80/TCP, normal system activity (name resolution, system updates...)

RCS Console should be located in the same network of RCS Database, and a network connection to it on port 4443/TCP must be possible. It doesn't need a public ip address.

If a distributed environment is required and RCS Console must connect from outside, creating a VPN tunnel to RCS Database network with proper equipment is recommended.

RCS Console system must support 1280x800 screen resolution or higher.

2.4 RCS Anonymizer

OPERATING SYSTEM: *Linux* (*CentOS* is recommended)
NETWORK CONNECTIONS
INBOUND: 80/TCP, 4444/TCP
OUTBOUND: 80/TCP, normal system activity (name resolution, system updates...)

RCS Anonymizer must have a static public ip address.

Normally RCS Anonymizer is installed on a VPS rent from a public provider.

A guideline about VPS is provided in *4.1*.

Due to company policy and to protect confidentiality requirements Customer must provide accounts on VPS services.

2.5 RCS Injection Proxy

OPERATING SYSTEM: *Linux* (installed by the *RCS Injection Proxy* setup procedure)
NETWORK CONNECTIONS
INBOUND: 80/TCP, 4444/TCP
OUTBOUND: full access

RCS Injection Proxy requires specific network configurations and devices in order to be able to work under different scenarios:

(a) **LAN:** two Ethernet cards must be available on the proxy computer, one needs to be connected to a mirror port, the other one to any other port: second card is required only when the

mirror port doesn't accept incoming traffic from the proxy.

(b) **Wi-Fi LAN:** two Wi-Fi cards are required, one must be able to enter monitor mode, the other one needs to join the Wi-Fi LAN.

(c) **ISP:** a tap or mirror port must be connected to the appliance, proxy must have access to the Internet and to the same network where the packets are going to be injected.

3 Additional requirements

3.1 SIM card

A SIM card with PIN code disabled must be provided to operate the *RCS Remote Mobile Installation* tool. SIM account must have data traffic and binary SMS capabilities enabled.

Due to company policy and to protect confidentiality requirements Customer must provide required SIM cards.

3.2 Symbian signing process

A *Symbian Developer Certificate* and a *Symbian Signed Account* must be provided in order to install and run *RCS* on *Symbian* devices, due to *Symbian* highly restricted architecture.

A guideline about *Symbian* certificate request process and *Symbian Signed* account creation is provided in *4.2*.

Due to company policy and to protect confidentiality requirements Customer must provide required certificates and accounts.

4 Guidelines

4.1 Virtual Private Server

VPS are being offered by many providers in any country with different operating systems and prices depending on bandwidth, CPU power and memory.

Any *Linux* VPS running recent distributions with a statically connected ip address is likely to be compatible with *RCS Anonymizer*, anyway suggested distribution is *CentOS*.

There's no particular CPU power and disk space requirement to operate *RCS Anonymizer*.

Low cost VPS with limited bandwidth and limited traffic/month usage are usually enough for small number of concurrent targets. It's usually a good idea to start with a limited VPS option and in case upgrade to a more powerful bundle.

Most VPS can administered through a web based interface application, which performs all ordinary maintenance activities (reboot, shutdown, root password change, backup…) including account management and billing.

After installation of *RCS Anonymizer* on selected VPS systems, the software can be fully configured and monitored using *RCS Console*.

Here is a list of recommended VPS providers:

- **Linode:** http://www.linode.com/ (USA and others)
- **Serverplan:** http://www.serverplan.com/ (Italy)
- **Host Europe:** http://www.hosteurope.de/ (Germany and others)

4.2 Symbian Signed account

It is required to buy a certificate from TC TrustCenter at the following address:

http://www.trustcenter.de/en/products/tc_publisher_id_for_symbian.htm

Certificate type must be “Developer Certificate” and not “Test House Certificate”.

After acquiring the certificate, valid for one year, the Certification Authority will request documentation about the developer and the company that’s asking the certificate.

Symbian Signed account can be created going to the following address:

http://www.symbiansigned.com/