

]HackingTeam[

## Remote Control System

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.

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.

All contents of this document are: Copyright © 2010 HT s.r.l. All rights reserved.

## Document Approval

Revision	Author(s)	Release Date
1.0	Valeriano Bedeschi	10/01/2011

## Table Of Contents

1	Overview .....	1-5
1.1	Naming conventions .....	1-5
2	Customer Side Components .....	2-7
2.1	Front-End .....	2-7
2.2	Back-End .....	2-7
2.3	Management console .....	2-8
3	Target Side Components .....	3-9
3.1	RCS Agent.....	3-9
3.1.1	Agent Deployment .....	3-10
3.1.1.1	Local installation.....	3-10
3.1.1.2	Remote installation.....	3-10
3.1.1.3	Uninstallation.....	3-11
3.1.2	Retrievable data.....	3-12
3.1.3	Event/Action logic .....	3-13
3.1.4	Communication .....	3-13
3.1.5	OS compatibility .....	3-14
4	Public Side .....	4-15
4.1	Anonymizers.....	4-15

# 1 Overview

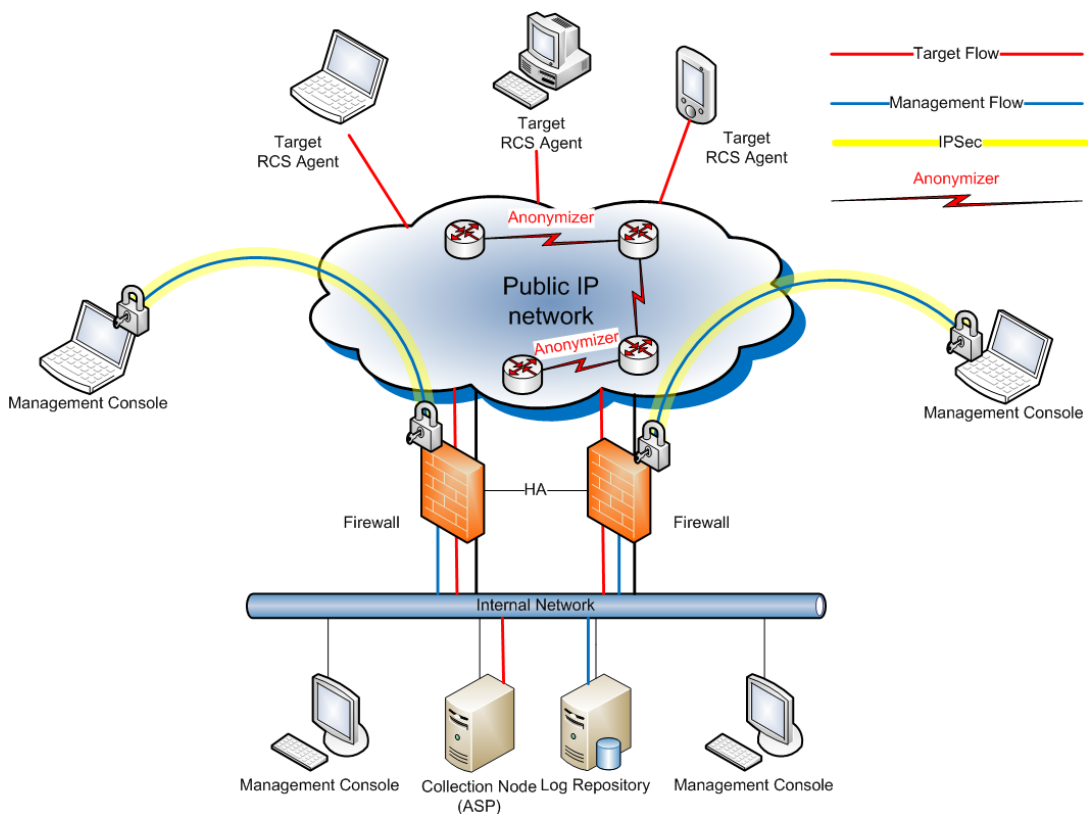
In modern digital communications, encryption is widely employed to protect users from eavesdropping.

Unfortunately, encryption also prevents law enforcement and intelligence agencies from being able to monitor and prevent crimes and threats to the country security.

Remote Control System (RCS) is a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable.

An RCS installation is totally deployed at the customer site, thus guaranteeing total control on its operations and security.

A simple scheme of a standard RCS installation follows.



The RCS infrastructure is made up of different components: some of these sit inside the customer's network, while others are meant to be installed on the devices to be monitored. Others again can be placed anywhere on the internet, to increase the stealthness and untraceability of the connections coming from the monitored devices.

In the following sections each component is explained in detail.

## 1.1 Naming conventions

Remote Control System's main architectural components are:

## Remote Control System

- Front End (Collection Node – ASP)
- Back End (Database – Log Repository)
- Management Console
  - Admin User
  - Tech User
  - Log Viewer User
- Target
- Anonymizer

## 2 Customer Side Components

---

### 2.1 Front-End

The Front-End receives connections from Agents running on intercepted devices. It acts as an isolation barrier for the Back-End, augmenting the security of the installation.

Data received by the Front-End is directed to Back-End for decryption and processing. When new Agents configurations are available, the Front-End sends them to all the interested devices.

All connections entering and leaving the Front-End are encrypted and authenticated, and can be decrypted only by the Agents. No other component is capable of doing the decryption, thus guaranteeing total security during the whole Agents to Front-End communication that happens over the Internet.

A Front-End needs a public IP address that must be reachable globally: this way the Agents can reach the Front-End from anywhere, giving you control over the devices even when they're on the other side of the world.

At least one Frontend is needed in order to receive data from the Agents.

**Software requirements:** Windows 2003 or 2008.

### 2.2 Back-End

Backend server is the core of the whole infrastructure. It contains all the data collected from the targets, handles requests coming from management consoles for controlling targets and browsing data.

All RCS data are inside a standard relational database, so it can be provided with extra capabilities such as automatic backup, custom data mining and so on.

Server dimensioning is dependent on the number of concurrent targets' and operators' sessions. In some very large installations more than one server could be needed. Data can also reside on an external data storage device.

Backend server must be placed inside customer's trusted network.

**Software requirements:** Windows 2003 or 2008.

## 2.3 Management console

Management console is the only graphic user interface for accessing and controlling all RCS's functionalities.

Depending on the credentials used for logging in, it grants different level of privileges to each user:

- **Admin:** can create users and groups, grant privileges, manage investigations, audit the system.
- **Technician:** can create vectors for targets infection and configure/re-configure agents behavior.
- **Viewer:** can browse evidences coming from the targets, classify and/or export them.

A single user can be granted with more than one privilege at a time.

Using the alerting panel, it is possible to setup custom alerts to warn the user in real time when evidences of interest arrive to the database.

The console allows the handling of all the multimedia evidences that can be collected.

The console also permits to constantly monitor the health status of each component of the system, with an integrated failure alerting module.

All the communications between the consoles and the database are SSL encrypted.

The console can be installed on any pc/workstation inside the customer's trusted network (the same network as the Back-End). If the customer needs to access the data from a different physical location, a standard VPN solution can be used to remotely access customer's network.

All the console machines should also be able to reach the internet in order to permit some functionalities such as browsing satellites maps for target tracking.

**Software requirements:** Windows, MacOS X or Linux



## 3 Target Side Components

---

### 3.1 RCS Agent

It is the software that has to be installed on the target PCs/smartphones to monitor. Installation can occur by means of different "infection vectors" (see below). It sends all the collected data to the frontend network collector, even though it doesn't require a permanent internet connection in order to work. It can be configured to collect different kind of data on the target machine (see below). Data are stored (encrypted and hidden) on the target machine until the agent has the opportunity to send them to the network collector.

Operators can reconfigure targets' behavior at any time through the console: the new configuration will be active next time the agent will connect to the frontend; it's an asynchronous way of interacting with the backdoor, designed to allow targets control and data retrieving without the need of an interactive operator on the console when RCS targets are online.

This way of interaction is possible since RCS agent can be configured with an inner logic based on an event/action paradigm (see below) that lets them to react to different situations that may occur on the target machine even when they are offline.

All connections between agents and frontends are encrypted with strong algorithms and mutually authenticated.

Desktop version uses standard internet connectivity (wired or wireless) to synchronize with the frontend and it works both in home and enterprise environments (where network firewalls and/or proxies could be in use); mobile version can be configured to use several methods of communication (see below) such as 3G/Wi-Fi/BlueTooth/USB.

Installation process and standard agents operations are hidden from the user perspective.

The Target software is guaranteed to be resistant to most endpoint security technologies available on the market (antivirus, personal firewalls, antispysware, antirootkits, and analysis tools).

It is also resistant to some image-restoring software (e.g.: Deepfreeze).

All RCS client modules, for all architectures, can be controlled and configured in an uniformed way using the RCS Console: all the differences between the various OSs are transparently handled by RCS client code itself. All RCS client modules, on all OSs, are also fully compatible with any existing RCS network infrastructure.

Each RCS client module has its own peculiar agents, with functionalities that may vary from OS to OS (please refer to the attached compatibility grid).

In the near future, some functionality from an OS will be ported to other OSs, where they are not already present; some other functionality will never be ported due to hardware limitations.

## 3.1.1 Agent Deployment

RCS Agent must be installed on target devices in order to monitor them. It can be installed either locally or remotely, depending on the scenario.

### 3.1.1.1 Local installation

If physical access to the target device is granted, local installation can be very effective. Some local installation vectors, for desktop and mobile platforms, follows:

- Booting/Running from USB/CD-ROM device (desktop platforms)
- Hard Disk physical connection (desktop platforms)
- SD/MMC Card infection (mobile platforms)

### 3.1.1.2 Remote installation

Remote installation usually requires some information about the target (eg: used ISP, e-mail address, etc). Depending on the information available about the target, identify the most effective installation vector among the following:

#### **Melting tool**

It allows the insertion of RCS software inside any existing executable file. As soon as the file is executed on the target device, RCS Agent is installed.

#### **Exploit portal**

It allows the automatic creation of exploits containing RCS agent as the payload. It creates "malformed" versions of common file formats

(eg: .pdf, .doc, .html) that triggers a specific vulnerability in the program used on the target machine to open the file. HT constantly provides exploit for vulnerabilities that are public available or "zero-day". The exploit repository resides on HT's servers in Milan: each time an operator logs into the console, it downloads from HT's servers the updated exploit list and the exploiting code itself.

Each exploits is attached with a brief description, platforms it has been tested on and vulnerable versions of the triggered application.

There are four different exploit categories:

- *Social*: they don't trigger vulnerabilities in any application, but in the users' behaviors. eg: an executable file that pretends to be an office document.
- *Public*: The vulnerability is known, and maybe already patched on latest program versions. The exploit code is publicly available.
- *Private*: The vulnerability is known, but the exploit code is not publicly available.
- *Zero-Day*: The vulnerability is not known in the wild, latest program versions are vulnerable. HT provides 3 working zero day exploits at any given time during the year. If one of them is patched (rated as private), HT will provide a new one.

### **Injection proxy**

It allows to automatically insert RCS Agent inside any executable file downloaded by the target (e.g.: a software installer) or by an application (e.g.: an automatic software update). If used in conjunction with the exploit portal, it can also insert RCS Agent payload in other kind of downloaded contents (e.g.: web pages, documents). It can be positioned as a standard network passive probe in any way that allows targets' traffic inspection, for example:

- Between DSLAM ADSL concentrator and ISP core network
- On the core switch of target's enterprise network
- Associated with target's wireless network

It does NOT require being in-line (physically in the middle of the communication)

It allows automatic target recognition by different parameters:

- IP address
- DHCP
- Radius account/parameters
- String matching (e.g.: e-mail, Facebook accounts)

It can be bought as software or as an appliance with dedicated network cards to handle hi-speed traffic analysis.

### **Remote Mobile Infection**

By sending a special crafted SMS message it is possible to trigger the automatic installation of the RCS agent on smartphones devices. It is strongly dependent on the device model and can be more effective if a mobile operator cooperates.

### **Infection Agent**

Already infected Desktop PC can automatically infect any mobile phone that is connected via USB for data synchronization or battery charging.

#### **3.1.1.3 Uninstallation**

RCS Agent can be uninstalled from remote with a simple click on the Console. Once uninstalled, the backdoor cannot be reactivated.

## 3.1.2 Retrievable data

### Desktop

Evidences acquired by client module include, but are not limited to:

- Opened files (documents, images, data, etc.)
- Screen snapshots
- Web Browsing
- Mouse clicks
- Application passwords recovery (Outlook, MSN, Internet Explorer, Firefox, etc.)
- Keystrokes (any language settings)
- Clipboard
- Printed documents
- E-mails
- Location tracking (Wi-Fi info)
- Remote Audio Spy (Microphone)
- File system explorer
- Software/OS/Hardware information
- Camera Snapshots
- VOIP calls (Skype, MSN, Yahoo)
- Chat/IM (Skype, MSN, Yahoo, ICQ, etc.)
- Execute commands of operator's choice
- Upload and download files of operator's choice

### Mobile

Evidences acquired by client module include, but are not limited to:

- Phone calls
- Organizer/Address book
- SMS/MMS
- E-mails
- Screen snapshots
- Location tracking (cell signal info, Wi-Fi info, GPS info if available)
- Remote audio Spy
- Camera Snapshots
- SIM Information

### 3.1.3 Event/Action logic

The RCS Agent can recognize different situations that happen on the target device and can react with a customizable list of actions. For example:

- When the screen saver starts → Send data
- A given GPS position is reached → Start recording audio
- Battery or disk space is too low → Stop recording audio
- Receiving a phone call → Take a camera snapshot
- After 30 days → Uninstall

Any event can be linked with any action, it's up to the operator to configure it in a way that fits his needs.

### 3.1.4 Communication

Desktop version uses standard internet connectivity (wired or wireless) to synchronize with the frontend and it works both in home and enterprise environments (where network firewalls and/or proxies could be in use).

Mobile version can be configured to use different ways of communication (each connection type can be triggered by different events):

**GPRS/UTMS/3G+** RCS Agent can use an existing data connection or can force a creation of a new one. The new connection can be established using a custom APN (if available) that could allow free of charge data sending for the target (only for RCS data).

**Wi-Fi:** RCS Agent can automatically recognize any open/preconfigured wireless Access Point (e.g.: airport, hotel, home) and connect with it in order to reach the front end

**BlueTooth:** Mobile Mediation Node is a small device (it's a sub module of the network collector) that is able to retrieve data from RCS Agents using Bluetooth. An operator with this device must be near the target in order to retrieve the data.

**SMS:** RCS Agent can send invisible SMS containing small amount of data (such as SIM information or GPS position).

**USB:** RCS Agent can use Desktop PC internet connection when attached via USB for data synchronization or battery charging.

### 3.1.5 OS compatibility

RCS Agents can be installed on:

- Windows XP, Vista, 7 (32/64 bit)
- MacOS X 10.5, 10.6
- Windows Mobile 6, 6.5
- iPhone(iPad) 3, 4
- Symbian S60 3<sup>rd</sup> e 5<sup>th</sup> edition
- BlackBerry 4.5 and newer

## 4 Public Side

---

### 4.1 Anonymizers

Anonymizers are used to avoid exposing real IP address of the Front End in the connections coming from the targets. Anonymizing nodes can be spread anywhere in the internet (see annex) and connections from the targets are routed through each of them before reaching the real Front End.

They can be placed in untrusted networks since each connection is fully encrypted from the target to the frontend (no decryption is performed by the anonymizer).

Anonymizers can be linked into one or more chains that can be fully controlled and monitored by the integrated RCS Management Console.