]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.

Document Approval

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

Table Of Contents

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.

RCS installations are deployed at the Customer’s premises, thus guaranteeing to the Customer total control on its operations and security.

NOTE HackingTeam have no way of connecting to or receiving any information from the Customer’s RCS installation.

Please refer to Figure 1 for a scheme of a standard Remote Control System installation.

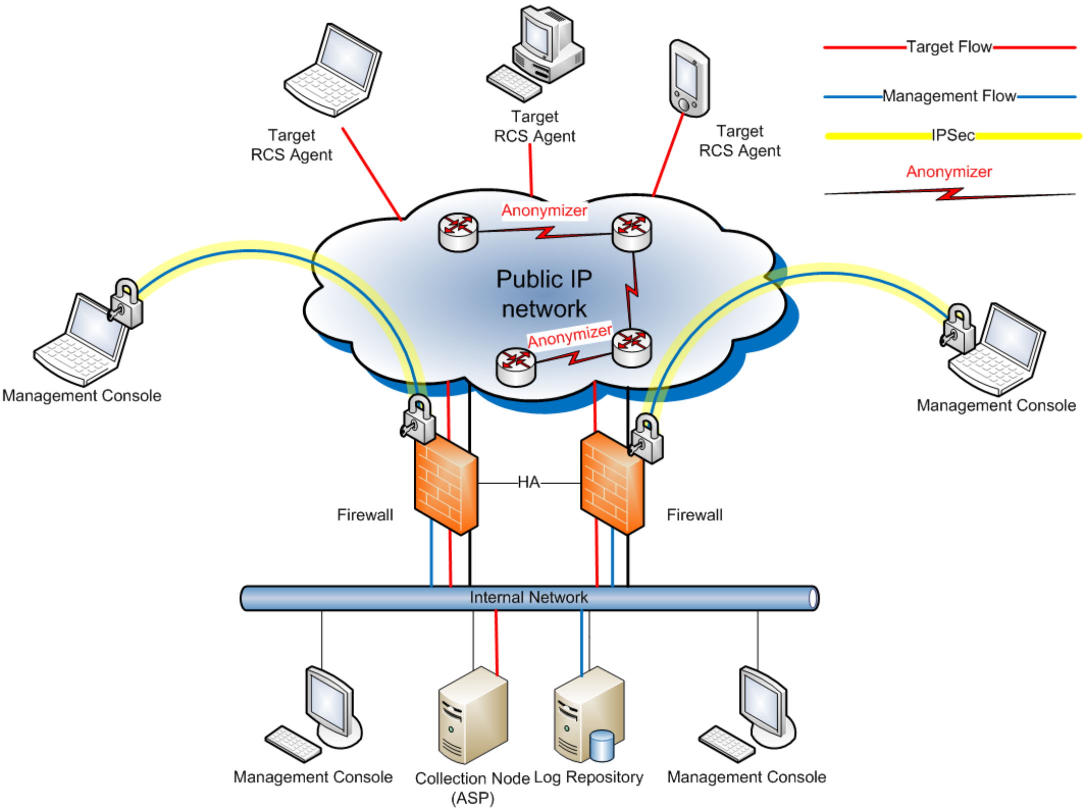

Figure 1 - Standard RCS installation

The RCS infrastructure is made of different components: one part resides at the Customer’s premises, while another part is meant to be installed on the devices to be monitored.
Furthermore, some components are intended to be installed on different networks, such as Internet Service Provider’s.

1.1 Naming conventions

Remote Control System’s main architectural components are:

- 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 sent to the Back-End for decryption and processing. When new Agents configurations are available, the Front-End sends them to 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 decryption, thus guaranteeing total security during the Agents to Front-End communication.

A Front-End must be reachable over the Internet by a public IP address: the Agents must be able to reach the Front-End from anywhere, giving you control over the devices, anywhere they could be.

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

Software requirements: Windows 2003 or 2008.

2.2 Back-End

The Backend server is the core of the whole infrastructure. It stores all the data collected from the Agents and handles the requests coming from the management Consoles.

All the RCS data is stored inside a standard relational database, thus extra capabilities, such as automatic backup and custom data mining can be implemented upon Customer request. The Backend can use a Storage Area Network (SAN) to enable redundancy and failure resistance.

Server sizing is dependent on the number of concurrent Targets and data retention policies.

Backend server must be installed inside the Customer's network.

Software requirements: Windows 2003 or 2008.

2.3 Management console

The RCS Console is the application used for accessing and controlling all the Remote Control System (RCS) functionalities.

Operators can be profiled to grants different level of access to the system:

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

A single Operator can be granted more than one privilege.

Using the Alerting panel, it is possible to setup custom alerts to warn a group of Operators when evidence of interest is received.

Operators can handle all the multimedia evidences collected, such as screenshots and phone calls, from within the Console, from which they can also be exported in their native format (e.g. jpeg images, mp3 audio files) to be processed by external equipment.

The health status of each component of the system can be monitored from the Console, and the system is capable of alerting a group of Operators in case there is a problem with any component.

All the communications between the Console and the Backend are encrypted using SSL.

The Console can be installed on any pc/workstation running Windows, OS X or Linux. If the customer needs to access the data from outside its own network, a standard VPN solution can be used to permit the Console to connect to the Backend.

The Console must be able to connect to the Internet to download some information such as satellites maps for target tracking.

NOTE A list of all the URLs that must be accessible for the Console to operate is available, in case the Customer’s network is firewalled.

Software requirements: Windows, MacOS X or Linux

3 Target Side Components

3.1 RCS Agent

The RCS Agent is the software component that monitors the target computer or smartphone. Installation of the Agent is performed by means of different installation vectors.

Once installed, the Agent sends all the collected data to the Frontend, by using any of the device's Internet connections. The Agent can be configured to collect different kind of data (e.g. screenshots, phone calls) from the target device. Data are first stored, encrypted and hidden, on the device itself, until there is an Internet connection available to send them.

Operators can reconfigure the Agents behavior at any time through the Console: a new configuration is made active upon the next time the Agent connects to the frontend.

Such an asynchronous channel of communication, and the set-and-foget configuration capabilities of the Agents were specifically designed to eliminate the need for an Operator to stay in front of the Console waiting for interesting data to be collected.

RCS Agents are autonomous and can be configured to react on specific events with different actions, allowing them to adapt to different situations that may occur on the target device, even if there is no current communication between the Agent and the Frontend.

All communications between Agents and Frontends are encrypted with strong encryption algorithms and mutually authenticated, preventing any possibility of eavesdropping or leakage of information.

The Agent for Windows and Mac systems uses standard Internet connectivity through LAN or WiFi, and it's capable of connecting even in enterprise environments, where network firewalls and/or proxies are usually in place.

The Agent for smartphones can be configured to use several methods of communication (see below) such as 3G network, Wi-Fi, BlueTooth or USB connection with a laptop or desktop system.

The RCS Agent is resistant to most endpoint security technologies available on the market, such as antiviruses, personal firewalls, antispyware, antirootkits and analysis tools, as well as restoration technologies, such as DeepFreeze, commonly found in Internet Cafes.

The Agents can be controlled and configured uniformly using the RCS Console: all the differences between the various OSs are made transparent to the Operator.

Functionalities available for each platofmr may vary (please refer to the attached Compatibility List).

3.2 Agent Deployment

RCS Agent must be installed on target devices in order to monitor them, and installation can be performed either locally or remotely.

3.2.1 Local installation

When physical access to the target device is available, local installation can be very effective. Some specific local installation vectors are available, such as bootable CDs and USB storage for desktop systems, or memory card infection and USB cable connection for smartphones.

3.2.2 Remote installation

Remote installation may require some information about the target to be already available to the Operator: information like the ISP used by the target for connecting to the Internet or his e-mail address can be of great help in preparing an effective installation vector.

3.2.2.1 Melting tool

Melting inserts an Agent inside any existing executable file, such as application installers. As soon as the file is executed on the target device, RCS Agent is installed.

3.2.2.2 Exploit portal

The Exploit Portal, by making use of unwanted security holes in common applications, allows for embedding of RCS Agents into common file formats, such as *Adobe PDF*, *Microsoft PowerPoint* and *Word documents*.
Installation of the RCS Agent is started as soon as the target opens the document.

3.2.2.3 Network Injector

The *Network Injector* (NI) installs RCS Agents over the Target's Internet connection by using a patent-pending injection technique and a proprietary streaming melting technology.

Network Injector is capable of inserting an RCS Agent into any downloaded executable file and browsed web page, without visible changes in the content.

Deployment of the Network Injector can be done inside any network: from small home WiFi networks to geographically distributed Internet Service Providers.

Multiple users can be monitored and different types of injection are available, such as injection into web pages or downloaded applications.

3.2.2.4 Remote Mobile Infection

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

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.

3.2.3 Uninstallation

Each Agent can be uninstalled remotely from the Console: uninstallation completely removes the Agent from the device.

3.2.4 Retrievable data

Evidence collected from Windows and Mac target include the following:

- 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

Evidence collected from smartphones include the following data:

- 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

3.2.5 Event/Action logic

The RCS Agent is able to recognize different events happening on the target device, reacting to them with specific actions.

For example, the following combinations of events and actions can be configured to raise the chances of collecting relevant evidence and prevent the Target from becoming aware of the Agent presence on his device.

Here is a list of common examples of specific configurations that we advice to our Customers.

- When the screen saver starts, send the collected evidence to the Frontend
- When a given GPS position is reached , start the microphone recording (we suspect our target is going to have a meeting
- If battery or disk space run too low, stop recording the audio to prevent
- When receiving a phone call, take a snapshot with the front facing camera
- 30 days after installation of the Agent, uninstall the Agent itself and stop the investigation

The Operator is free to combine events to actions to fit his needs and better address each specific investigation.

3.2.6 Communication

While Agents for Windows and Mac have better chances to find a LAN or WiFi connection available anytime during the day, the Agent for smartphone may be much more limited in the availability of an Internet connection, therefore on smartphones we made available much more methods for the Agent to communicate.

GPRS/UTMS/3G+ RCS Agent is able to use any existing data connection, eventually forcing it if it’s been actively disabled by the Target. If the Target doesn’t have a flat rate data plan on the phone, it’s possibile to configure to Agent to use a different APN, preventing any unwanted entry to appear on the Target’s billing for the connections issued by the Agent.

Wi-Fi: the Agent automatically recognizes and uses any open/preconfigured wireless Access Point (e.g. hotel and home WiFi networks).

SMS: the Agent can send an SMS containing specific information such as SIM information or GPS position to a preconfigured phone number.

NOTE It’s not possible to use SMS to send collected data to the Frontend.

USB: if the smartphone is connected to a desktop for charging or synchronization, the agent can use the desktop Internet connection to send the collected data.

3.2.7 OS compatibility

RCS Agents can be installed on:

- Windows XP, Vista, 7 (32/64 bit)
- MacOs X 10.6 Snow Leopard, 10.7 Lion
- Windows Mobile 6, 6.5
- iOS 3, 4 (iPhone/iPad)
- Symbian S60 3rd and 5th edition
- BlackBerry 4.5 or newer

4 Public Side

4.1 Anonymizers

Anonymizers are used to avoid exposing the real IP address of the Front End, by setting up a geographically distributed network capable of bouncing the connection between an Agent and its Frontend among different countries.

Since connections between anonymizers are fully encrypted and no data decryption is performed on them, they can be placed even in untrusted networks or countries.

Management of the Anonymizers is performed through the RCS Console, where chains of Anonymizers can be configured and changed at any time.