]Hacking**Team**[

RCS 8.1
The hacking suite for governmental interception

Technician's Guide

Information property

NOTE: requests for additional copies of this manual or product technical information should be addressed to:

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

Contents

Glossary

The terms and their definitions used in this manual are provided below.

A

Accounting

Console section that manages RCS access.

acquisition sequence

Group of complex events, actions and acquisition modules that make up the advanced agent configuration.

Administrator

The person who enables user access to the system, creates work groups and defines operations, targets and the type of data to be collected.

Agent

Software probes installed on devices to monitor. They are designed to collect evidence and communicate it to the Collector.

alert rules

Rules that create alerts when new evidence is stored or agents communicate back for the first time.

Alerting

Console section that manages new evidence alerts.

alerting group

Group of users who receive notifications via mail whenever a system alarm is triggered (for example, when the database exceeds available free space limits). Normally this group is not linked to an operation.

Analyst

Person in charge of analyzing the data collected during operations.

Anonymizer

(optional) Protects the server against external attacks and permits anonymity during investigations. Transfers agent data to Collectors.

Audit

Console section that reports all users' and system actions. Used to monitor abuse of RCS.

B

back end

Environment designed to decrypt and save collected information. In distributed architecture, it includes Master Node and Shard databases.

BRAS

(Broadband Remote Access Server) routes traffic to/from DSLAM to the ISP network and provides authentication to the ISP subscribers.

C

Collector

Receives data sent by agents directly or through the Anonymizer chain.

console

Computer on which the RCS Console is installed. It directly accesses the RCS Server or Master Node.

D

Dashboard

Console section used by the Analyst. Used to have a quick overview of the status of the most important operations, targets and agents.

DSLAM

(Digital Subscriber Line Access Multiplexer) network device, often located in the telephone exchanges of the telecommunications operators. It connects multiple customer digital subscriber line (DSL) interfaces to a high-speed digital communications channel using multiplexing techniques.

E

evidence

Collected data evidence. The format depends on the type of evidence (i.e.: image).

evidence alerts
> Alerts, usually in the form of emails, sent to analysts when new evidence matches the set rule.

F

factory
> A template for agent configuration and compiling.

front end
> Environment designed to communicate with agents to collect information and set their configurations. In distributed architecture, it includes the Collector and Network Controller.

I

injection rules
> Settings that define how to identify HTTP traffic, what resource should be injected and what method is to be used for the injection.

M

Monitor
> Console section that monitors components and license status.

N

Network Controller
> Component that checks Network Injector and Anonymizer status and sends them new configurations and software updates.

Network Injector
> Hardware component that monitors the target's network traffic and injects an agent into selected Web resources. It comes in two versions, Appliance or Tactical: the former is for deployment at the ISP, the latter for use in WiFi environments.

Network Injector Appliance
> Rackable version of the Network Injector, for installation at ISP. See: Tactical Network Injector.

O

operation

Investigation aimed at one or more targets, whose devices will be recipients for agents.

R

RCS

(Remote Control System) the product documented hereto.

RCS Console

Software designed to interact with the RCS Server.

RCS Server

One or more computers, based on the installation architecture, were essential RCS components are installed: Shard databases, Network Controllers and Collector.

S

SSH

(Secure SHell) a network protocol for secure data communication, remote shell services or command execution.

System

Console section that manages the system.

System administrator

The person who installs the servers and consoles, updates software and restores data in case of faults.

T

Tactical Network Injector

The portable version of Network Injector, for tactical use. See: Network Injector Appliance.

TAP

(Test Access Port) a hardware device installed in a network that passively monitors the transmitted data flow.

target

The physical person under investigation.

Technician

The person assigned by the Administrator to create and manage agents.

V

VPS

(Virtual Private Server) a remote server where the Anonymizer is installed. Commonly available for rent.

Guide introduction

Presentation

Manual goals

This manual is a guide for the *Technician* on how to use the RCS Console to:

- create agents and install them on a target defined by the Administrator
- create HTTP connection injection rules for Network Injectors

Information on how to consult the manual is provided below.

Content

This section includes the following topics:

New guide features

List of release notes and updates to this online help.

Release date	Code	Software version	Description
30 June 2012	Technician's Guide 1.1 JUN-2012	8.1	Added agent functions *see "Agent page" on page 28* . Added **Idle** event *see "Idle event" on page 71* . Changed installation for **Exploit**, **WAP push** and **QR Code** vectors. Changed vectors **Offline Installation, Installation Package** *see "List of installation vectors" on page 95* . Changed Symbian certification process *see "Obtaining a Symbian certificate" on page 108* . Code Signing certificate for **Melted Application** and **Silent Installer vectors** *see "Obtaining a Code Signing certificate" on page 95* .
16 April 2012	Technician's Guide 1.0 APR-2012	8.0	First publication

Supplied documentation

The following manuals are supplied with RCS software:

Manual	Addressees	Code	Distribution format
System Administrator's Guide	System administrator	*System Administrator's Guide 1.1 JUN-2012*	PDF
Administrator's Guide	Administrators	*Administrator's Guide 1.1 JUN-2012*	PDF
Technician's Guide (this manual)	Technicians	*Technician's Guide 1.1 JUN-2012*	PDF
Analyst's Guide	Analysts	*Analyst's Guide 1.1 JUN-2012*	PDF

Print concepts for notes

Notes foreseen in this document are listed below (Microsoft Manual of Style):

WARNING: indicates a risky situation which, if not avoided, could cause user injury or equipment damages.

CAUTION: indicates a risky situation which, if not avoided, can cause data to be lost.

IMPORTANT: offers the indications required to complete the task. While notes can be neglected and do not influence task completion, important indications should not be neglected.

NOTE: neutral and positive information that emphasize or add information to the main text. They provide information that can only be applied in special cases.

Tip: suggestion for the application of techniques and procedures described in the text according to special needs. It may suggest an alternative method and is not essential to text comprehension.

Service call: the operation may only be completed with the help of technical service.

Print concepts for format

A key to print concepts is provided below:

Example	Style	Description
See "User data"	*italic*	this indicates a chapter, section, sub-section, paragraph, table or illustration heading in this manual or other publication of reference.
<ddmmyyyy>	<aaa>	indicates text that must be specified by the user according to a certain syntax. In the example <ddmmyyyy> is a date and could be "14072011".
Select one of the listed servers **[2]**.	**[x]**	indicates the object specified in the text that appears in the adjacent image.
Click **Add**. Select the **File menu, Save data**.	**bold**	indicates text on the operator interface, a graphic element (i.e.: table, tab) or screen button (i.e.: display).
Press ENTER	UPPER CASE	indicates the name of keyboard keys.

Example	Style	Description
See: Network Injector Appliance.	-	suggests you compare the definition of a word in the glossary or content with another word or content.

Product and guide addressees

Following is the list of professionals that interact with RCS.

Addressee	Activity	Skills
System administrator	Follows the HackingTeam's instructions provided during the contract phase. Installs and updates RCS servers, Network Injectors and RCS Consoles. Schedules and manages backups. Restores backups if servers are replaced. WARNING: the system administrator must have the required necessary skills. The HackingTeam is not liable for equipment malfunctions or damages due to unprofessional installation.	*Expert network technician*
Administrator	Creates authorized accounts and groups. Creates operations and target. Monitors system and license status.	*Investigation manager*
Technician	Creates and sets up agents. Sets Network Injector rules	*Tapping specialist technician*
Analyst	Analyzes and exports evidence.	*Operative*

Software author identification data

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

RCS (Remote Control System)

Presentation

Introduction

RCS (Remote Control System) is a solution that supports investigations by actively and passively tapping data and information from the devices targeted by the investigations. In fact, RCS anonymously creates, sets and installs software agents that collect data and information, sending the results to the central database to be decrypted and saved.

Content

This section includes the following topics:

Differences with previous versions

Differences with the RCS 7.6 version are described below

Glossary

RCS v. 7.6	*RCS 8.0 and higher*
Activity	Operation
Agent	Module
Anonymizer chain	Anonymizing chain
Backdoor	Agent
Backdoor Class	Factory
Collection Node (ASP)	Collector
Injection Proxy Appliance (IPA)	Network Injector Appliance
Log Repository (RCSDB)	Master Node and additional Shard
Mobile Collection Node (RSSM)	Collector
RCSAnon	Anonymizer

Infection vector glossary for desktop

RCS v. 7.6	*RCS 8.0 and higher*
EXE	Melted application
CD	Offline Installation
USB	Offline Installation
EXPL	Exploit

Infection vector glossary for mobile

RCS v. 7.6	*RCS 8.0 and higher*
SD	Local Installation
CAB	Installation Package
APP	Exploit

RCS v. 7.6   RCS 8.0 and higher

SIS	Installation Package, Symbian
COD	
APK	Installation Package WAP Push Message

RCS Console for the Technician

Presentation

The Technician's role

The Technician's role is to:
- create injection rules for each installed Network Injector
- create infection agents for the various target devices
- keep agent software updated

Technician enabled functions

To complete his/her activities, the Technician has access to the following functions:
- **Operation**
- **System**

Content

This section includes the following topics:

Starting the RCS Console

When started, RCS Console asks you to enter your credentials previously set by the Administrator.

What the login page looks like

This is what the login page looks like:
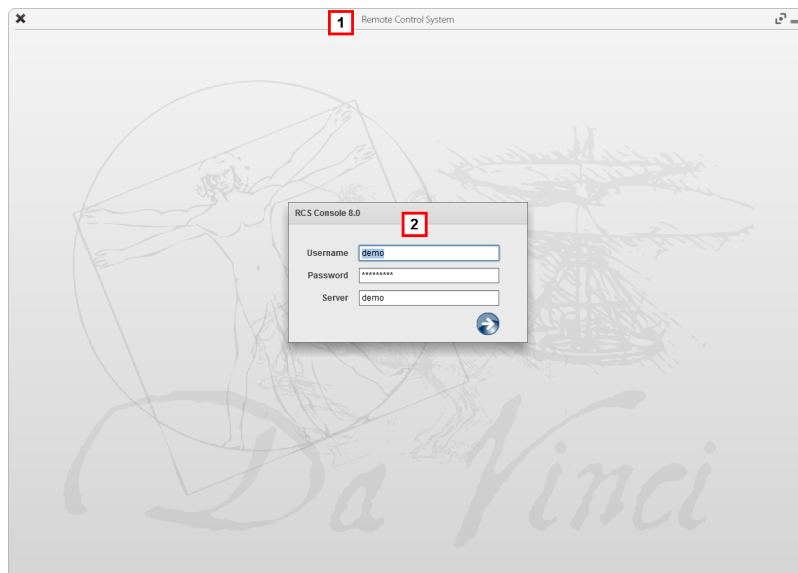
Area	Description
1	Title bar with command buttons: ✖ Close RCS Console. ⬈ Expand window button. ➖ Shrink window button.
2	Login dialog window.

Open RCS Console

To open RCS Console functions:

Step	Action
1	In **Username** and **Password,** enter the credentials as assigned by the Administrator.
2	In **Server,** enter the name of the machine or server address to connect to.

Step	Action

3

Click ![icon]: the homepage appears with the menus enabled according to your account privileges.*See "Homepage description" below* .

Homepage description

To view the homepage: | • click 🏠

Introduction

The homepage is displayed when the RCS Console is started, and is the same for all users. Enabled menus depend on the privileges assigned to the account.

What it looks like

This is what the homepage looks like, with recently opened items saved. For details on shared elements and actions:
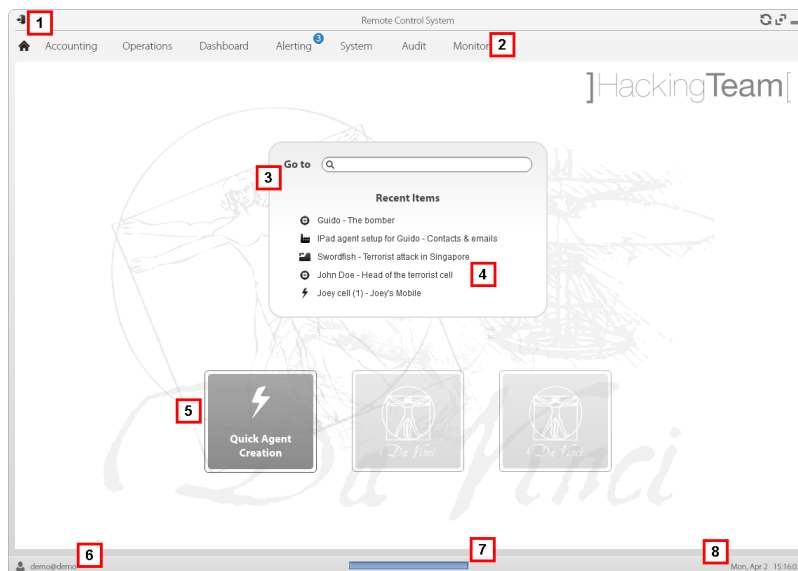
Area	Description
1	Title bar with command buttons.
2	RCS menu with functions enabled for the user.
3	Search box to search operations, targets and agents, by name or description.

Area	Description
4	Links to last five opened elements (operation, target and agent).
5	Wizard buttons
6	Logged in user with possibility of changing the language and password.
7	Download area with ability to view progress during export or compiling.
8	Current date and time with possibility of changing the time zone.

Shared interface elements and actions

Each program page uses shared elements and allows similar actions to be run.
For easier manual comprehension, elements and actions shared by some functions are described in this chapter.

What the RCS Console looks like

This is what a typical RCS Console page looks like. A target page is displayed in this example:
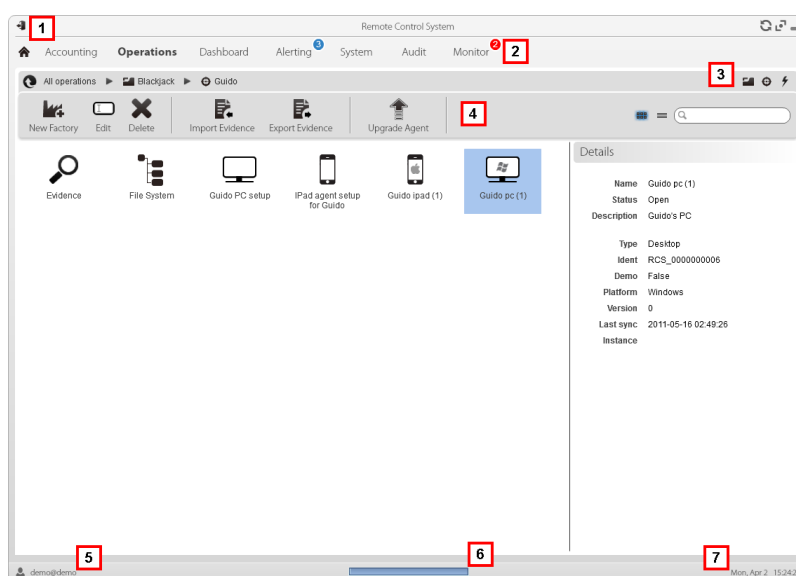
Area	Description
1	Title bar with command buttons:
	◀| Logout from RCS.
	↻ Page refresh button.
	⬈ Expand window button.
	▬ Shrink window button.
2	• 🏠 Return to homepage button
	• RCS menu with functions enabled for the user.
3	Operation scroll bar. Descriptions are provided below:

Icon	Description
◐	Back to higher level.
🗂	Show the operation page.
⊕	Show the target page.
🏭	Show the factory page.
⚡	Show the agent page.

Area	Description
4	Buttons to display all elements regardless of their group membership. Descriptions are provided below:

Icon	Description
🗂	Show all operations.
⊕	Show all targets.
⚡	Show all agents.

Area	Description
5	Window toolbar.
6	Search buttons and box:

Object	Description
🔍 John Doe	Search box. Enter part of the name to display a list of elements that contain the entered letters.
≡	Display elements in a table.
⠿	Display elements as icons.

Area	Description
7	Logged in user with possibility of changing the language and password.

Area	Description
8	Download area with ability to view progress during export or compiling. Files are downloaded to the desktop in RCS Download folder. • top bar: percent generation on server • bottom bar: percent download from server to RCS Console.
9	Current date and time with possibility of changing the time zone.

Actions always available on the interface

Change interface language or password

To change the interface language or password:

Step	Action
1	Click **[6]** to display a dialog window with the user's data.
2	Change the language or password and click ✱ to confirm and exit.

Converting the RCS Console date-time to the actual time zone

To convert all dates-times to the actual time zone:

Step	Action
1	Click **[8]** to display a dialog window with the current date-time: **UTC time**: Greenwich mean time (GMT) **Local time**: date-time where the RCS server is installed **Console time**: date-time of the console used that can be converted.
2	Change the time zone and click ✱ to confirm and exit: all displayed dates-times are converted as requested.

Table actions

The RCS Console displays various data in tables. Tables let you:

- sort data by column in increasing/decreasing order
- filter data by column

Action	Description
Sort by column	Click on the column heading to sort that column in increasing or decreasing order.

Action	Description
Filter a text	Enter part of the text you are searching for: only elements that contain the entered text appear.

The example shows elements with descriptions like:

- "my**boss**"
- "**boss**anova"

Action	Description
Filter based on an option	Select an option: the elements that match the selected option appear.

Action	Description
Filter based on several options	Select one or more options: the elements that match all selected options appear.

Action	Description
Change the column size	Select the edge of the column and drag it.

Technician procedures

Introduction

The Technician is in charge of infection rules to retrieve important information. Some typical procedures are described below with references to significant chapters. These are only simple indications. Skill and ability are essential to exploit RCS flexibility and adapt it to investigation needs.

Procedures

Injection on HTTP connections

Network Injector must be used for injections on HTTP connections:

Step	Action
1	In **System** section, **Network Injector** create the injection rules. See "*Managing the Network Injector*" on page 52

> NOTE: no agent installation is required.

Infecting a computer not connected to Internet

To infect a computer not connected to Internet

Step	Action
1	Create a factory, disabling synchronization. See "*Target page*" on page 18 .
2	Compile the factory selecting the installation vector suited to the device platform and installation method, then create the agent. See "*Compiling a factory*" on page 24 .
3	Install the agent on the target device with the selected methods. See "*List of installation vectors*" on page 95 .
4	After the required amount of time, retrieve evidence produced on the target device.
5	Import agent evidence and analyze it. See "*Agent page*" on page 28 .

Infecting a computer connected to Internet

To infect a computer connected to Internet

Tip: these steps are essential when you do not initially know which target activities to record or to avoid recording an excessive amount of data.

Step	Action
1	Create a factory: the system automatically enables synchronization. *See "Target page" on page 18*
2	Compile the factory selecting the installation vector suited to the device platform and installation method, then create the agent. *See "Compiling a factory" on page 24 .*
3	Install the agent on the target device with the selected methods. *See "List of installation vectors" on page 95 .*
4	The agent appears in the target page at first synchronization. *See "Target page" on page 18*
5	Reset the agent using the basic or advanced configuration. The agent applies the new configuration at the next synchronization. *See "Basic factory or agent configuration" on page 36* *See "Advanced factory or agent configuration" on page 41 .*

Keeping agent software updated

HackingTeam cyclically updates its software. To update installed agents:

Step	Action
1	• In **Operations** section, **Target** update agents. *See "Target page" on page 18* or • In **Operations** section, **Target** open an agent and update it. *See "Agent page" on page 28 .*

Targets

Presentation

Introduction

A target is a physical person to be monitored. Several agents can be used, one for each device owned by the target.

Content

This section includes the following topics:

Target page

To open a target	• **Operations** section, double-click an operation, double-click a target

Purpose

This function lets you:

- manage factories which, when compiled, become agents to be installed on the target device.
- open a factory for basic configuration (*see "Basic factory or agent configuration" on page 36*) or advanced configuration (*see "Advanced factory or agent configuration" on page 41*
- import target evidence
- open an installed agent
- update agent software

What the function looks like

This is what the page looks like:
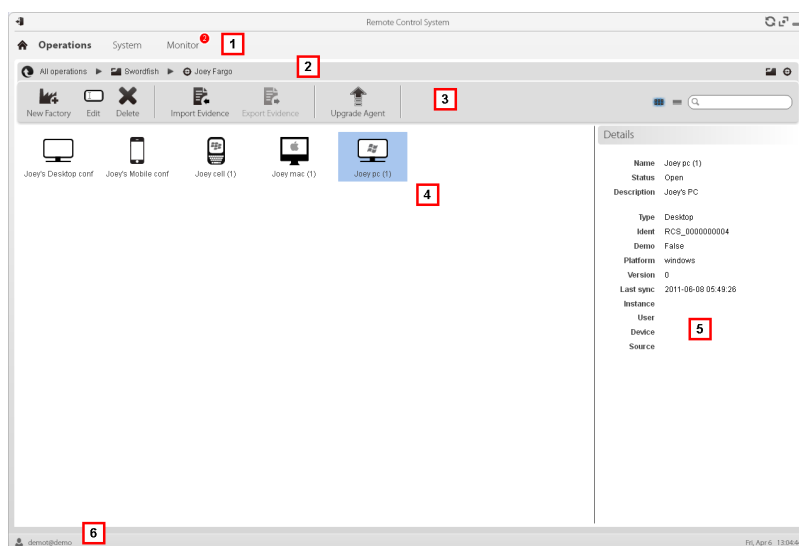
Area	Description
1	RCS menu.
2	Scroll bar
3	Window toolbar. Descriptions are provided below:

NOTE: the ▤ key displays elements in a list with their data.

Icon	Description
	Compile the configuration into one or more agents to be installed, based on selected installation vectors. *See "Compiling a factory" on page 24*
	Editing a factory or agent
	Deleting a factory or agent
	Closing the agent or factory.
	Adding the agent to the dashboard.
	Adding the agent to alerts: an alert is generated at each synchronization.
	Moving the factory or agent to a new target.
	Import target evidence physically collected on the device.
	Export target evidence in .tgz format.
	Update all agents' software to the last version received from HackingTeam support service. *CAUTION: the update does not update the configuration that is transmitted to the agent at the next synchronization.*

4	Icons/list of created factories and installed agents.

⬚ : agent in demo mode.

Area	Description
5	Selected factory or agent data.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For a description of the data in this window *see "Target page data" on page 23* .

For more information on targets *see "What you should know about Factories and Agents" on the facing page*

Creating a factory

To create a factory:

Step	Action
1	• Click **New Factory**: data entry fields appear. • Enter the name and description and in **Type** select the device type.
2	Click **Save**: the new factory with the selected name appears in the main work area.

Closing a factory or agent

To close a factory or agent:

Step	Action
1	Select a factory or agent and click **Close**.
2	Confirm close. ⚠ *CAUTION: closing an agent is irreversible and the agent is uninstalled at the next synchronization. Closing a factory makes it inaccessible. Active agents remain accessible while all agents that have not been synchronized at least once before the factory is closed will be uninstalled.*

Deleting a factory or agent

To delete a factory or agent:

Step	Action
1	Select a factory or agent and click **Delete**. Confirm the action: logs, settings and evidence are deleted. ⚠️ *CAUTION: this operation is irreversible.*

Importing target evidence

To import evidence:

Step	Action
1	Click **Import Evidence**: the import window opens. Click **Select Directory** and select the folder where the offline.ini file is saved.
2	Click **Import**: evidence is saved in the database and is available to be viewed by Analysts.

Exporting target evidence

To export evidence:

Step	Action
1	Click **Export Evidence**: the export window opens.
2	Click **Ok**: evidence is saved in the specified folder.

What you should know about Factories and Agents

Infection methods

A device can be infected via:

- **physical infection**: the device is infected by the execution of a file transmitted using USB memories, CDs or documents. Evidence can be collected physically or via Internet as soon as the device connects.
- **remote infection**: the device is infected by the execution of a file transferred via Internet connection or made available in a Web resource. Evidence can be collected physically or via Internet as soon as the device connects. Remote infection can be enhanced using Network Injector.

Infection strategy components

Components needed for correct infection include:

- **Factory**: basic agent creation template.
- **Installation vectors**: infection channels.
- **Agent**: the software to be installed on the target device.
- **Target and operation**: defined when investigations are opened by the System Administrator. Refer to the System Administrator Manual.
- **Evidence**: the types of recordings to be collected

Factories

A *factory* is a base agent creation template. The icon varies according to the type of device intended for the agent:

- : factory for desktop agent

- : factory for mobile agent

The following must be set in the factory:

- data to be acquired (basic configuration) or modules to be dynamically activated (advanced configuration)
- *installation vectors* (i.e.: CD, exploit, Network Injector)

Tip: a factory can be used to create several agents: for example, to be installed via different installation vectors (i.e.: two computers with different operating systems).

Installation vectors

Installation vectors are selected when compiling and define the installation method, physical or remote, for an agent. When compiling, available installation vectors may vary according to the device's operating system.

Several installation vectors can be used for the same agent.

NOTE: injection rules are used for injection on HTTP connections.*See "Managing the Network Injector" on page 52*

Agents

An *agent* is the result of compiling a factory with one or more installation vectors. An agent is ready to be installed on a device.

Basic configuration defines the type of data to be acquired while advanced configuration lets you dynamically and independently activate or deactivate modules.

For the types of modules available in basic and advanced configurations *see "Module list" on page 78*

Data acquisition modules

Modules trigger some activities on the target device, mainly data acquisition. They are enabled and set in the basic configuration (only some) or in advanced configuration.

Available module types also depend on the device type.

For the complete list*see "*[*Module list*](#)*" on page 78* .

Target page data

To view page data:	• **Operations** section, double-click an operation, double-click a target, click **Icon view** or **Table view**

Page elements can be viewed as icons or a table.

Icon view

Icons are described below:

Data	*Description*
	Desktop and mobile type factory in Open status.
	Desktop agent types, in Open status, for operating systems: • OS X • Windows
	Mobile agent types, in Open status, for operating systems: • Android, • BlackBerry, • iOS, • Symbian • Windows Mobile
	NOTE: icons are light grey for **CLOSED** factories and agents. This is the icon for a mobile agent for Android in Closed status: .

NOTE: icons are light grey for **CLOSED** agents. This is the icon for a mobile agent for Android in Closed status:⬛.

Table view

Data is described below:

Data	Description
Name	Factory or agent name.
Description	Factory or agent description
Status	**Open**: an open factory can be compiled to create agents. An open agent can be installed, is running and records evidence.
	Closed: a closed factory or agent cannot be reopened. Data in RCS can still be viewed.
Type	Desktop or mobile type.
Platform	(agent only) Operating system on which the agent is installed.
Version	(agent only) Agent version. A new version is created when a new configuration is created.
Last sync	(agent only) Date and time of the last agent synchronization.
Ident	(agent only) Univocal agent identification.
Instance	(agent only) Univocal identification of the device where the agent is installed.

Compiling a factory

To compile a factory:	• **Operations** section, double-click an operation, double-click a target, double-click a factory, click **Build**
	• **Operations** section, double-click an operation, double-click a target, double-click a factory, click **Advanced Config**, **Build**

Purpose

This function lets you create one or more agents (for production use or to be tested in demo) depending on the chosen installation vectors and target platforms.

NOTE: for a detailed description of each installation vector *see "List of installation vectors" on page 95*

Next steps

Creating an agent implies the subsequent installation on a target device.

What the function looks like

This is how the page is displayed for a desktop agent:
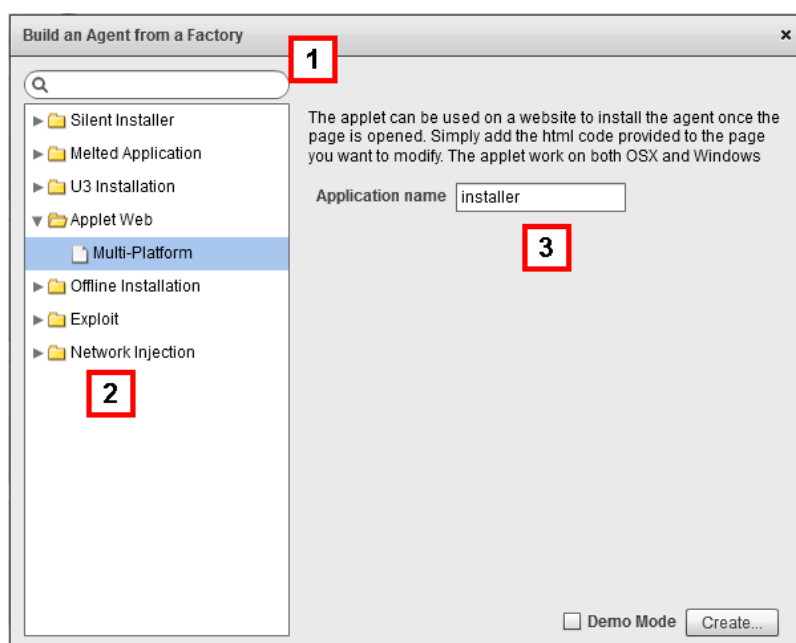
Area	Description
1	Installation vector and platform search box.
2	Vector and platform tree view.
3	Compiling settings area for the chosen vector.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For more information on factories *see "What you should know about Factories and Agents" on page 21* .

For a detailed description of each installation vector *see "List of installation vectors" on page 95*

Creating an agent

To create an agent:

Step	Action
1	Select one or more installation vectors and set the options.
2	Click **Create**: a ZIP or ISO file is created and downloaded in the RCS Download folder, ready to be installed on the device.

Creating an agent to be tested in demo mode

IMPORTANT:only use this option for tests on internal devices. Agents in demo mode are not invisible and RCS installation is not hidden.

To create an agent for test purposes:

Step	Action
1	Select one or more installation vectors and set the options.
2	Select the **Demo** combo box.
3	Click **Create**; the agent installed on the device will show its presence with audio signals and on screen messages.

Agents

Presentation

Introduction

Agents acquire data from the device on which they are installed and send it to the RCS Collectors. Their configuration and software can be updated and they can transfer files unnoticed to the target.

Content

This section includes the following topics:

Agent page

To manage agents:	• **Operations** section, double-click an operation, double-click a target, double-click an agent

Purpose

This function lets you:

- check the agent configuration log and view details for each configuration.
- transfer files to/from the target device
- import/export agent evidence
- update agent software
- display commands run by the agent
- display the IP addresses used by the agent to contact the Collector

What the function looks like

This is what the page looks like:
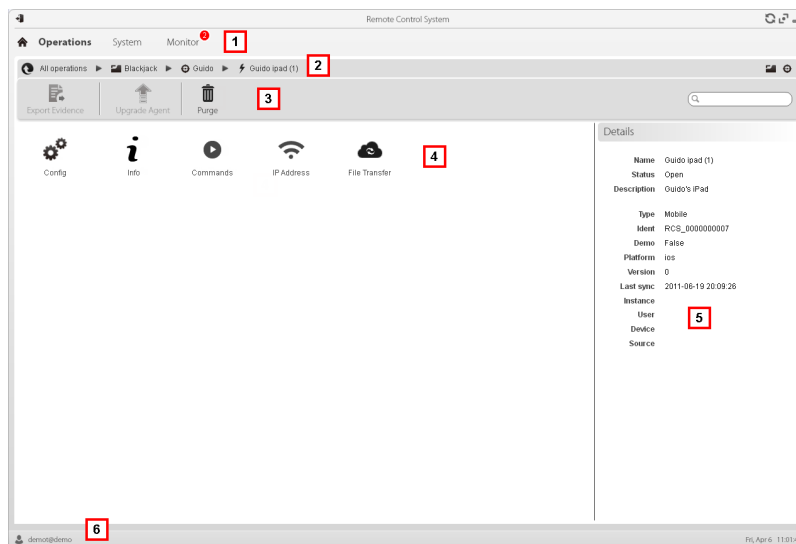
Area	Description
1	RCS menu.
2	Scroll bar

Area	*Description*
3	Window toolbar. Descriptions are provided below:

Icon	*Description*
	Export agent evidence.
	Update agent software to the last version received from HackingTeam support service. **CAUTION: the update does not update the configuration that is transmitted to the agent at the next synchronization.**
	Delete evidence on the device not yet transmitted to RCS. Parameters: • **Date before**: delete evidence saved before the set date. • **Size bigger than**: delete evidence larger than the set size.

Area	*Description*
4	Possible actions on the agent. Descriptions are provided below:

Icon	*Description*
	Show the results of commands run on the device using **Execute** actions.
	Show the agent synchronization log. *See "Agent synchronization log data" on page 32* .
	Show the agent settings log, allowing the existent settings to be edited and saved as new. *See "Agent configuration log data" on page 31* .
	Open the function to upload or download files from the target device. *See "Transferring files to/from a target" on page 32*

Area	*Description*
5	Agent details.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For more information on agents *see "What you should know about agents" below* .

What you should know about agents

Agent synchronization

An agent will perform synchronization only if:

- synchronization is enabled in the basic configuration
- a **Synchronize** type action was added to advanced settings.

First agent synchronization

Once installed, the agent appears in the target page after the first synchronization. Its icon represents the platform on which the agent is installed. For example:

- : agent installed on a Windows device

- : agent installed on a BlackBerry device

After installation succeeds, the agent starts to acquire data if appropriately set.

Offline and online agents

An agent behaves differently according to the Internet connection availability:

If the Internet connection is...	Then...
not available	if the agent has modules enabled, it starts to record data in the device.
available	if first synchronization has been run on the agent, you can:

- change settings, for example, as recording requests become more specific for that device. Resetting an agent does not change factory settings
- update its software,
- transfer files to and from the device,
- analyze sent evidence

Tip: start creating an agent and only enable synchronization and the device module. Then, once installed, and upon receiving the first synchronization, gradually enable the other modules, according to the device capabilities and the type of evidence you want to collect.

Temporarily disabling an agent

Agent activities can be temporarily suspended without uninstalling the agent by simply disabling all the modules and leaving only synchronization active.

Agent testing

To test a configuration before production use, create an agent in Demo mode (*see "Compiling a factory" on page 24*).

The agent is created in *demo* mode, behaving according to the given configuration, with the sole difference that it clearly signals its presence on the device (with audio, led and screen messages). Signaling permits easy identification of an infected device used for testing.

> NOTE: in case evidence is not received from an agent in demo mode, this may be due to a server settings error or impossibility of reaching the address of the set Collector (i.e.: due to network settings problems).

Agent configuration

Agent configuration (basic or advanced) can be repeatedly edited. When saved, a copy of the configuration is created and saved in the configuration log.

At the next synchronization, the agent will receive the new configuration (**Sent time**) and communicate successful installation (**Activated**). From that point on, any changes can only be made by saving a new configuration.

> NOTE: If **Sent time** and **Activated** are null, the current settings can still be edited.

For a description of agent configuration log data *see "Agent configuration log data" below* .

Agent configuration log data

Descriptions are provided below:

Field	*Description*
Description	User's description of the settings.
User	Name of the user who created the configuration.
Saved	Date settings were saved.
Sent time	Date settings were sent via synchronization.
	WARNING: if this value is null, the agent has not yet received the configuration.

Field	Description
Activated	New agent configuration installation date.

Agent event log data

Descriptions are provided below:

Field	Description
Acquired	Date-time of the event acquired on the device. It can be filtered. **Last 24 hours** is set by default.
Received	Date-time of the event logged in RCS. It can be filtered. **Last 24 hours** is set by default.
Content	Status information sent by the agent.

Agent synchronization log data

Descriptions are provided below:

Field	Description
Acquired	Synchronization date-time. It can be filtered. **Last 24 hours** is set by default.
IP	IP address used for synchronization.
Address	Site where connection was established.

Transferring files to/from a target

To transfer files to/from the agent:	• **Operations** section, double-click an operation, double-click a target, double-click an agent, double-click **File Transfer**

Purpose
Uploading and downloading files on the device where the agent is installed.

What the function looks like
This is what the file transfer to/from target function looks like:
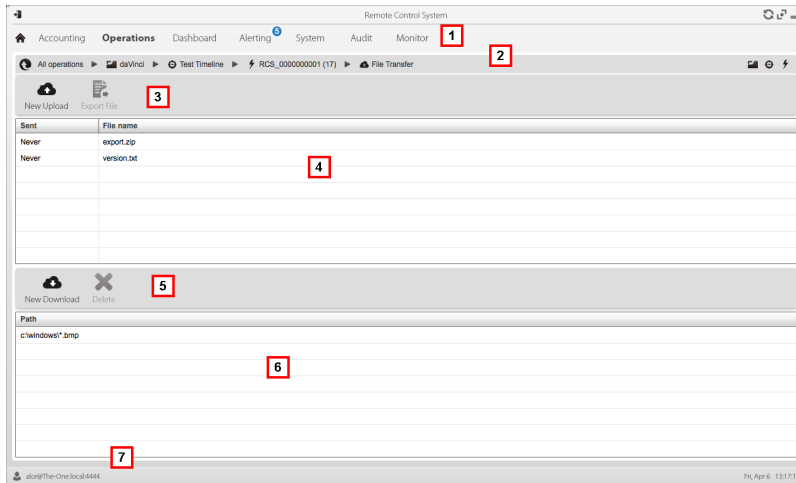
Area	Description
1	RCS menu.
2	Operation scroll bar. Descriptions are provided below:

Icon	Description
◐	Show the list of operations.
▰	Show the operation page.
⊕	Show the target page.
▦	Show the factory page.
⚡	Show the agent page.

Area	Description
3	Window toolbar. Descriptions are provided below:

Icon	Description
☁	Upload a file to the device, in the folder where the agent is installed. Each successful upload is logged with the date-time and file name.
🗎	Export upload log.

Area	Description
4	Upload log, with toolbar.

Area	Description
5	Window toolbar. Descriptions are provided below:

Icon	Description
	Download a file from the device. The path and file name must be indicated. Each successful download is logged with the file name complete with path. The file is saved in RCS Download folder on the desktop.
	Delete the selected file from the RCS Download folder.

Area	Description
6	Download log, with toolbar.
7	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .
For a description of agent data *see "Agent page" on page 28* .

Factory and agent: basic configuration

Presentation

Introduction

The basic configuration lets you add data acquisition and simple command execution modules that do not require complex settings.

Content

This section includes the following topics:

Basic factory or agent configuration

| *To set factories and agents:* | • **Operations** section, double-click an operation, double-click a target, double-click a factory |
| | • **Operations** section, double-click an operation, double-click a target, double-click an agent |

Purpose

This function lets you:

- set the factory/agent configuration indicating whether online synchronization is required and the data to be acquired
- open the factory compiling function (*see "Compiling a factory" on page 24* .
- open the advanced configuration function (*see "Advanced factory or agent configuration" on page 41*)

Next steps

After setting a factory configuration, it must be compiled to obtain an agent.

After editing the agent configuration, simply save it. If the agent is online, the new configuration will be applied at the next synchronization. Otherwise, physical installation is required.

What the function looks like
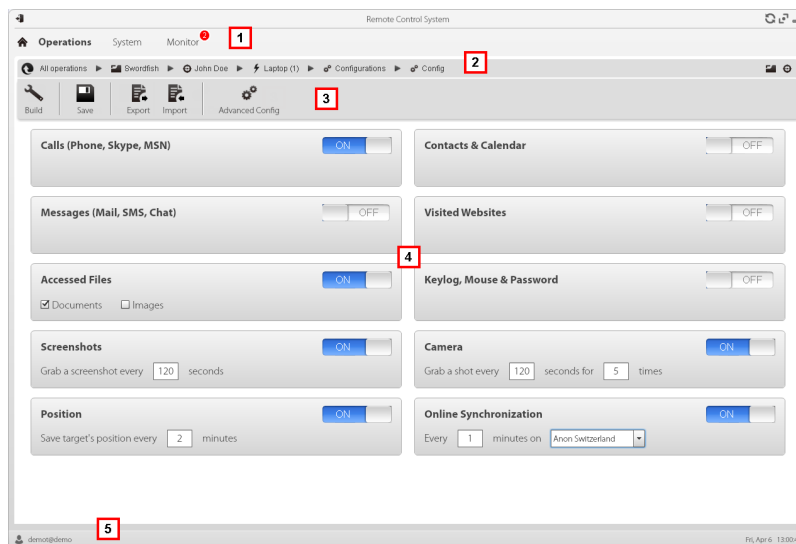
This is what the page looks like:

Area	Description
1	RCS menu.
2	Scroll bar
3	Window toolbar. Descriptions are provided below:

Icon	Description
🔧	Compile the configuration into one or more agents to be installed, based on selected installation vectors. *See "Compiling a factory" on page 24*
💾	Save the configuration: the agent configuration is logged and sent to the agent at the next synchronization. *See "Agent configuration log data" on page 31*
📤	Export the configuration to a .json file.
📥	Import the configuration from a .json file.
⚙	Open the advanced configuration window. *See "Advanced factory or agent configuration" on page 41 .* ⚠ *CAUTION: when returning from advanced configuration to basic configuration, the advanced configuration will be lost and the basic configuration will be restored.*

Area	Description
4	List of collectable evidence and relevant activation status. ℹ *NOTE: the module list varies according to device type.*
5	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11 .*
For more information on the basic configuration *see "What you should know about basic configuration" on next page .*
For a description of the data in this window *see "Basic configuration data" on next page .*
For the list of modules available in the two settings *see "Module list" on page 78*

Setting a factory or agent configuration

To activate or deactivate collectable evidence:

Step	Action
1	• Click **OFF** for the evidence to be acquired: the button turns to **ON** and configuration options, where available, may be set.
2	• In **Online Synchronization** leave **ON** if the target device can access the Internet. This lets you gradually set options. Leave **OFF** if the target device cannot access the Internet or if you want to manually acquire evidence from the target. • Click **Save** to save the current configuration.
3	Continue differently:

If you are setting...	Then...
a factory	click **Build** to compile it and obtain the agents for the different platforms. See *"Compiling a factory" on page 24* .
an agent	agent settings are automatically updated at the next synchronization.

What you should know about basic configuration

Basic configuration

The basic factory/agent configuration let you enable and quickly set evidence acquisition.

Basic configuration does not include the acquisition of some types of evidence nor detailed acquisition method options.

Default basic configuration:

- System information acquisition when the device is turned on (cannot be disabled)
- A module to run synchronization between the agent and RCS at a certain interval.

For the list of module types in base settings *see "Basic configuration data" below* .

⚠️ *CAUTION: when returning from advanced settings to base settings, all advanced settings will be lost and default base settings will be restored.*

Basic configuration data

The types of collectable evidence that can be enabled in basic factory or agent configuration are listed below.

Recording	Description
Calls	Record calls.
Messages	Record messages.
Accessed files	(desktop only) Record documents or images opened by the target. **Document, Images**: file types.
Screenshots	Record windows opened on the target display. **Grab a screenshot every**: image acquisition interval.
Position	Log the target's geographic position. **Save target position every**: position acquisition interval.
Contacts & Calendar	Record contacts and calendar.
Visited websites	Record visited website URL addresses.
Keylog	(mobile only) Log key strokes.
Keylog, Mouse & Password	(desktop only) Log key strokes, passwords saved on the system and mouse clicks.
Camera	Record webcam images. **Grab a shot every**: image acquisition interval. **for...times**: acquisition repetitions.
Online Synchronization	Enabled by default. If enabled, the agent contacts the server to send data and receives new configurations, updates, and so on. **Every**: synchronization interval **minute on**: Anonymizer or Collector name or IP address. The name or IP address can be manually entered. The chain layout can be viewed in **System** section, **Frontend** function. *See "Front end management" on page 49* . If disabled, it indicates that the device is always offline and evidence will be physically retrieved and imported into the database. *See "Target page" on page 18*

Factory and agent: advanced configuration

Presentation

Introduction

Advanced configuration lets you set advanced configuration options. Other than enabling collectable evidence, events can be linked to actions, to trigger specific agent reactions to changing conditions in the Device (i.e. screensaver is started). Actions can start or stop modules and enable or disable other events. Furthermore, all the event, action and module options can be individually set.

Content

This section includes the following topics:

Advanced factory or agent configuration

To open advanced configuration:	• **Operations** section, double-click an operation, double-click a target, double-click a factory, click **Advanced Config** • **Operations** section, double-click an operation, double-click a target, double-click an agent, click **Advanced Config**

Purpose

This function lets you:

- create module activation sequences triggered by events occurring on the target device. Each sequence can be made up of one or more sub-actions.
- Set general factory/agent configuration options.

CAUTION: when returning from advanced settings to base settings, all advanced settings will be lost and default base settings will be restored.

Next steps

For a factory, after completing its configuration, compile it to obtain the agent to be installed.*See "Compiling a factory" on page 24*

For an agent, after completing its configuration, simply save the new configuration. At the next synchronization, the new configuration will be sent to the agent.

What the function looks like
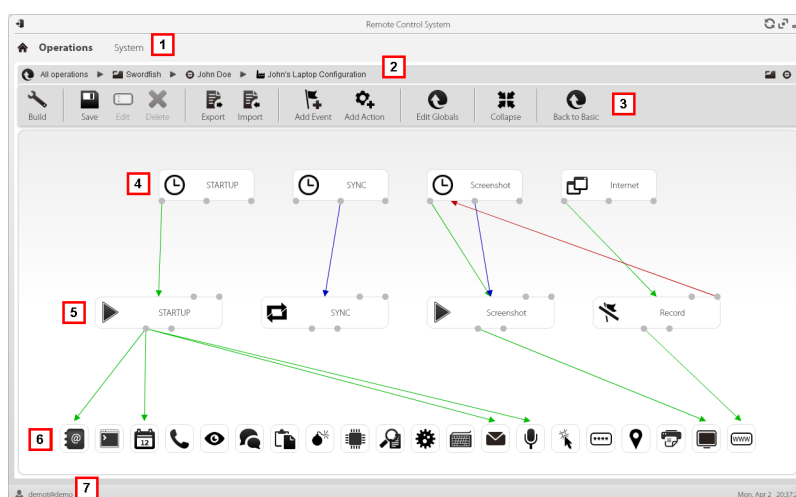
This is what the page looks like:

Area	Description
1	RCS menu.
2	Scroll bar
3	Window toolbar. Descriptions are provided below:

Icon	Description
🔧	Compile the configuration into one or more agents, based on selected installation vectors. *See "Compiling a factory" on page 24*
💾	Save the current configuration.
⌑	Edit the selected event or action.
✖	Delete the selected event, action or logical connection.
≣⚠	***CAUTION: all settings are lost when you return to the basic configuration.***
📄→	Export the configuration to a .json file.
📄←	Import the configuration from a .json file.
⚑⁺	Add an event.
⚙⁺	Add an action.
↻	Edit global agent data *see "Global agent data" on page 47 .*
⤧⤦	Shrink or expand event or action widgets to provide a better view of current settings.

4	Event area **STARTUP** and **SYNC** events are by default.
5	Action area. **STARTUP** and **SYNC** actions are enabled by default.
6	Modules area. Modules vary by desktop or mobile device.
7	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For more information on the advanced configuration*see "What you should know about advanced configuration" on the facing page* .

Creating a simple activation sequence

To create a simple sequence, to collect evidence when an event occurs:

Step	Action
1	Creating an event: • Click **Add Event**: the event selection and settings window opens. • In **Type,** select the type of event and set options. *See "Event list" on page 68* • Click **Save**: the new event is added to the work area
2	Creating an action: • Click **Add Action**: the empty action is added to the work area
3	Link the event to the action, then the action to the desired module: • Click on the **Start** event connection point, then drag the arrow to the action • Click on the **Start Modules** action connection point, then drag the arrow to the type of data to be acquired.*See "Module list" on page 78* .
4	Click **Save**: the configuration is ready to be compiled (if factory) or transmitted to the device at the next synchronization (if agent).

Creating a complex activation sequence

To create a complex sequence, to start collecting evidence, run a sub-action and enable/disable an event, when an event occurs:

Step	Action
1	Creating an event: • Click **Add Event**: the event selection and settings window opens. • In **Type,** select the type of event and set options. *See "Event list" on page 68* • Click **Save**: the new event is added to the work area

Step	Action
2	Creating an action and setting sub-actions:

- Click **Add Action**: the empty action is added to the work area
- Double-click on the action and add the sub-action in **Subaction** and set options. *See "List of sub-actions" on page 61* .

Step	Action
3	Connecting the event to the action:

- Click on one of the **Start, Repeat, End** event connection points, then drag the arrow to the action

Step	Action
4	Connecting the action to the module:

- Click on the **Start Modules** , **Stop Modules** action connection points, then drag the arrow to the module to be started or stopped. *See "Module list" on page 78* .

Tip: Drag multiple arrows if multiple modules have to be enabled.

For an action that requires an event to be enabled/disabled:

- Click on the **Enable events or Disable events** action connection points, then drag the arrow to the events to be enabled/disabled.

Step	Action
5	Click **Save**: the configuration is ready to be compiled (if factory) or transmitted to the device at the next synchronization (if agent).

What you should know about advanced configuration

Advanced configuration

Advanced factory/agent configuration lets you create complex activation sequences using a simple graphic interface.

The purpose of the sequence is to start/stop evidence collection, and/or run an action when an event occurs.

Advanced configuration always includes two basic sequences:

- At each synchronization (Loop event), acquire device information (Start module action + Device module)
- At the end of the synchronization interval (Timer-Loop event), run synchronization between the agent and RCS (Synchronize action)

Following is an image that illustrates the two basic sequences recommended for remote data acquisition:
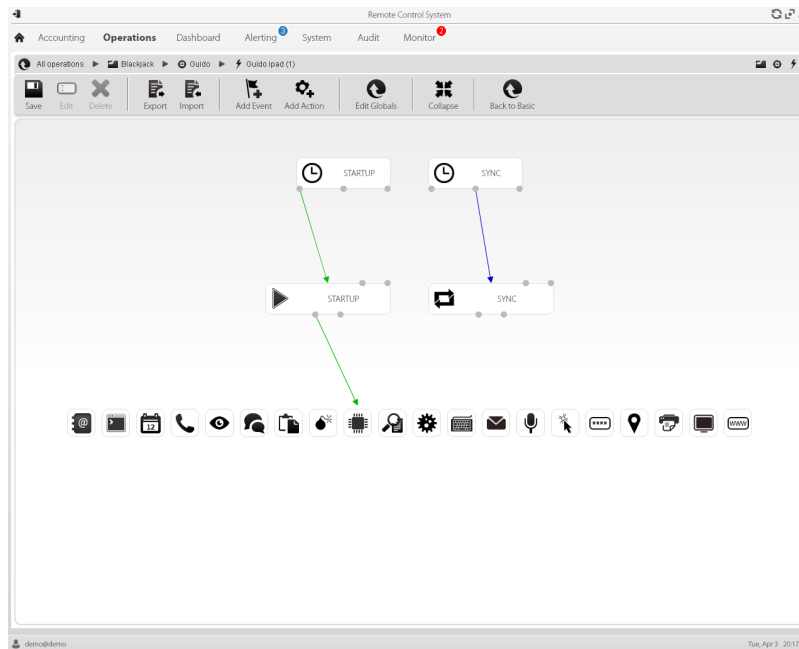
NOTE: these two basic sequences are set by default and recommended for minimum agent operations.

Advanced configuration components

Advanced configuration components are:

- *events* that trigger an action (i.e.: a call is received on the device)
- *actions* run when an event occurs (i.e.: start recording the call)
- *sub-actions* run when an event occurs (i.e.: hidden SMS sent with device position)
- *modules* which, enabled by an action, start collecting the desired evidence or trigger other actions on the device (i.e.: record call audio)
- *sequences*, used to indicate a group of events, actions, sub-actions and modules.

NOTE: some events, action and module options are only available in advanced configuration.

Reading sequences

Complex sequences can be read as follows:

- When the device is connected to the power source (event)...
- ...send an SMS (sub-action) and...

- ...start logging the position (action that triggers a module) and...
- ...disable the event occurring when the SIM is changed (action that disables an event)
- ...and so on

Possible event, action, sub-action and module combinations are infinite. Following is a detailed explanation of correct design rules.

Events

Events are monitored by the agent and can start, repeat or end an action.

NOTE: a module cannot be directly started by an event.

For example, a **Window** event (window opened on the device) can trigger an action. The action will then start/stop a module.

Various types of events are available. For the full list *see "Event list" on page 68* .

The relation between an event and one or more actions is represented by a connector:

Relation between events and actions	Description	Connector
Start	Start an action when the event occurs.	
Repeat	Repeat an action. The interval and number of repetitions can be specified.	
End	Start an action when the event is over.	

NOTE: an event can manage up to three distinct actions simultaneously. The **Start** action is started when an event occurs on the device (i.e.: **Standby** event triggers **Start** when the device enters standby mode). The **Repeat** action is triggered at the set interval for the entire duration of the event. The **Stop** action is started when the event is over (i.e.: the **StandBy** event triggers **End** when the device exits standby mode).

Actions

Actions are triggered when an event occurs. They can:

- start or stop a module
- enable or disable an event
- run a sub-action

For example, an action (empty) can disable the **Process** event (start a system process) that triggered it and enable the **Position** module (log the GPS position). If necessary, the action can also run an **SMS** sub-action (send a message to a specified phone number).

Various *sub-actions* are available and can be combined without restrictions (i.e.: run a command + create an Alert message). For the full list *see "List of sub-actions" on page 61*

Relations between actions and modules

An action can influence a module in different ways. The relation between an action and one or more modules is represented by a connector:

Relation between actions and modules	Description	Connector
Start modules	Start a module.	
Stop modules	Stop a module.	

An action can start/stop several modules simultaneously.

Relations between actions and events

The relation between an action and one or more events is represented by a connector:

Relation between action and events	Description	Connector
Enable events	Enable an event.	
Disable events	Disable an event.	

NOTE: an action can enable/disable several events simultaneously.

Modules

Each module enables the collection of a specific evidence from the target device. They can be started/stopped by an action and produce evidence.

For example, a **Position** module (log the GPS position) can be started by an action triggered by a **Call** event (a call was made/received).

Various modules are available that can be started/stopped (i.e.: start position module + stop screenshot module). For the complete list*see "Module list" on page 78* .

Global agent data

Global agent data is described below:

Field	Description
Minimum disk free	Minimum free disk space on the device.
Maximum evidence size	Maximum space occupied by evidence on the target device, up to next synchronization. 1 GB by default. When this limit is reached, the agent stops recording and waits for the next synchronization. If synchronization does not occur, no further evidence is acquired.
Wipe	If enabled, it wipes the files generated by the agent. No trace of the agent will be detected in case of forensic analysis. NOTE: this method takes longer to complete than normal file deletion.
Remove driver	Remove the driver at uninstall.
No hide	Service call: only use when requested by HackingTeam support service.
Mask	Service call: only use when requested by HackingTeam support service.

Front end management

To manage the front end: | ● **System section, Frontend**

Function scope

When RCS is running, this function lets you monitor the Anonymizers and Collectors, change the Anonymizer and chains settings and update the VPSes.

During installation, this function lets you create a new Anonymizer "object" that acts as the logical connection between the RCS Console and the software component to be installed on a VPS.

What the function looks like

This is what the page looks like:
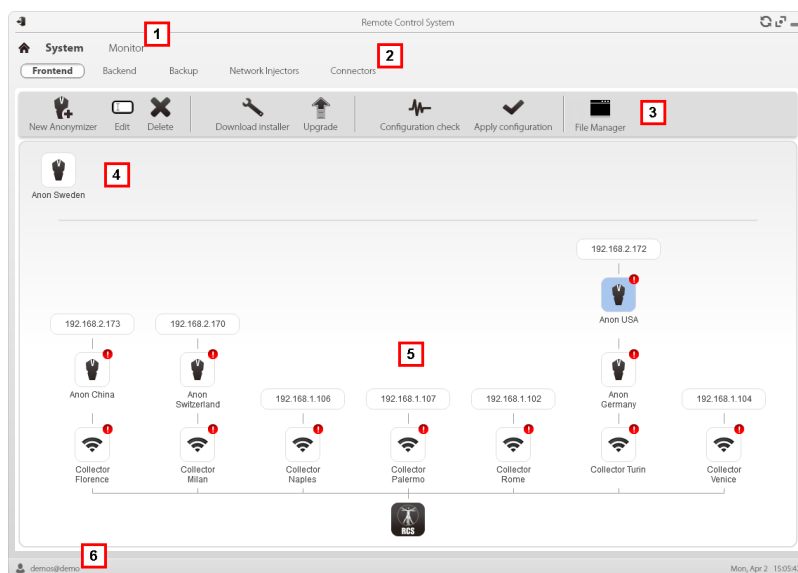
Area	Description
1	RCS menu.
2	**System** menu.
3	Window toolbar.
4	Anonymizers set but not yet included in a chain.

Area	*Description*
5	Anonymizer chains on the system with the IP address of the last element. Possible conditions:
	: Anonymizer not in chain.
	: Anonymizer in chain and running.
	: Anonymizer not monitored by the Network Controller.
	: Anonymizer with faults.
	: Collector running.
	: Collector not running.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

9

The Network Injector

Presentation

Introduction

Network Injector allows you to tap the target's HTTP connections and inject an agent on the device.

Content

This section includes the following topics:

Managing the Network Injector

To manage Network Injec-tors:	• **System** section, **Network Injector**

Purpose

When the RCS is running, this function lets you create monitoring and injection rules and send them to the Network Injector.

What you can do

With this function you can:

- create an agent's injection rule on a target and apply the rule on Network Injector.

NOTE: an agent need not be installed to create an injection rule.

What the function looks like

This is what the page looks like:

Area   Description

1   RCS menu.

Area	Description
2	**System** menu.
3	Network Injector toolbar.
4	Network Injector list.
5	Injection rule toolbar. Descriptions are provided below:

Action	Description
	Add a new rule.
	Open the window with rule data.
	Delete the selected rule.
	Update the selected Network Injector's settings.

Area	Description
6	List of selected Network Injector rules **En**: select to enable the rules to be applied.
7	RCS status bar. .

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For a description of injection rule data *see "Injection rule data" on page 55* .

For further information on injection rules *see "What you should know about Network Injector and its rules" on next page* .

Adding a new injection rule and applying it to the target

To add a new rule:

Step	Action
1	Select the Network Injector for the new rule.

Step	Action
2	• Click **Add New Rule**: data entry fields appear. • Enter the required data. If the rule is enabled, it can already be sent to the Network Injector. *See "Injection rule data" on the facing page* . • Click **Save**: the new rule appears in the main work area.
3	Enable the rule by selecting the **En** control box in the table.
4	Click **Apply rules**: RCS sends the rules to the selected Network Injector. The progress status is shown on the status bar.

Network Injector data

Selected Network Injector data is described below:

Data	Description
Name **Description**	User's descriptions.
Version	Software version.
Address	Device IP address.
Port	4444.
Monitor via NC	If enabled, Network Controller acquires the Network Injector status every 30 seconds. If not enabled, Network Injector continues sniffing and injection operations, but the Network Controller does not check its status. Used when connections to Network Injector are down for any reason once installed at ISP, or for tactical use.
Log	Last messages logged. : update the list. : delete viewed logs.

What you should know about Network Injector and its rules

Introduction

Network Injector monitors all the HTTP connections and, following the injection rules, identifies the target's connections and injects the agent into the connections, linking it to the resources the target is downloading from Internet.

Types of resources that can be infected

Resources that can be infected by RCS are any type of files.

NOTE: Network Injector is not able to monitor FTP or HTTPS connections.

How to create a rule

To create a rule:

1. define the way to identify the target's connections. For example, by matching the target's IP or MAC address.
2. define the way to infect the target. For example, by replacing a file the target is down-loading from the web or by infecting a website the target usually visits.

After identifying the target's connection and defining the attack method, enable and apply the rule.

What happens when a rule is enabled/disabled

Enabling a rule means making it available to the Network Injector injection process. Numerous rules can be created, adapting them to the target's different habits, then enabling the most efficient rule or rules according to the situations that arise during a certain time in the investigation.

A rule that is not enabled is not applicable meaning it cannot be sent to the Network Injector.

Injection rule data

Data that define the available infection rules are described below:

Data	Description
Enabled	If selected, the rule will be sent to the Network Injector. If not selected, the rule is saved but not sent.
Disable on sync	If selected, the rule is disabled after the first synchronization of the agent defined in the rule. If not selected, the Network Injector continues to apply the rule, even after the first synchronization.

Data	Description
Probability	Probability (in percent) of applying the rule after the first infected resource. **0%**: after infecting the first resource, Network Injector will no longer apply this rule. **100%**: after infecting the first resource, Network Injector will always apply this rule. Tip: if a value over 50% is applied, we recommend you return the value to 0% after successful installation is ensured (after synchronization) or use option **Disable on sync**.
Target	Name of the target to be infected.
Ident	Target's HTTP connection identification method. NOTE: Network Injector cannot monitor FTP or HTTPS connections. Each method is described below:

Data	Description
STATIC-IP	Static IP assigned to the target.
STATIC-RANGE	Range of IP addresses assigned to the target.
STATIC-MAC	Target's static MAC address, both Ethernet and WiFi.
DHCP	Target's network interface MAC address.
RADIUS-LOGIN	RADIUS user name. User-Name (RADIUS 802.1x).
RADIUS-CALLID	RADIUS caller ID. Calling-Station-Id (RADIUS 802.1x).
RADIUS-SESSID	RADIUS session ID. Acct-Session-Id (RADIUS 802.1x).
RADIUS-TECHKEY	RADIUS key. NAS-IP-Address: Acct-Session-Id (RADIUS 802.1x).
STRING-CLIENT	Text string to be identified in the data traffic from the target.
STRING-SERVER	Text string to be identified in the data traffic to the target.

Data	Description
User pattern	Target's traffic identification method. The format depends on the type of **Ident** selected.

Method	Format
DHCP **STATIC-IP** **STATIC-MAC**	Corresponding address (i.e.: "195.162.21.2").
STATIC-RANGE	Address range separated by '-' (i.e.: "195.162.21.2-195.162.21.5".
STRING-CLIENT **STRING-SERVER**	Text string (i.e.: "John@gmail.com").
RADIUS-CALLID	ID or part of the ID.
RADIUS-LOGIN	Name or part of the user name.
RADIUS-SESSID	ID or part of the ID.
RADIUS-TECHKEY	Key or part of the key (i.e.: "*.10.*").

Data	Description
Resource pattern	Identification method of the resource to be injected, applied to the Web re source URL. The format depends on the type of **Action** selected.

NOTE: leave empty if the selected action is **INJECT-UPGRADE**.

Action type	Resource Pattern Content

INJECT-EXE	URL of the executable file to be infected. Use wildcards to increase the number of matching URLs.
	Examples of possible formats:
	`*<nameExe>*.exe`
	`www.mozilla.org/firefox/download/firefoxsetup.exe`
	
	NOTE: when a full path is specified, be careful of any mirrors used by websites to download files (i.e.: "firefox.exe?mirror=it").
	
	Tip: enter *.exe* to infect all executable files, regardless of the URL.
	
	IMPORTANT: for example, if *exe* is entered without the '.' file extension separator, all the pages that accidentally contain the letters "exe" will be injected.

INJECT-HTML	URL of the website to be infected.
	Examples of possible formats:
	`www.oracle.com/`
	`www.oracle.com/index.html`
	
	NOTE: the site address must include the final '/' character if an HTML or dynamic page is not specified (i.e.: "`www.oracle.com/`").
	
	NOTE: a redirect page cannot be infected. Check the browser for the correct site path before using it in a rule.

INJECT-UPGRADE	Not used.
REPLACE	URL of a resource to be replaced.

Data	Description
Action	Infection method that will be applied to the resource indicated in **Resource pattern**:

Method	Description
INJECT-EXE	Infects the downloaded EXE file in real time. The agent is installed when the target runs the EXE file.
INJECT-HTML	Adds a Java applet to the Web page. When the target opens the page, java code execution must be accepted to install the agent. Tip: to avoid warning messages displayed by the target's system, we recommend you purchase a valid certificate to sign the Java applet. Please contact HackingTeam technicians for further details.
INJECT-UPGRADE	Notifies the Java Runtime Environment on the device that an update is available. The agent is installed when the target installs the update. Does not refer to **Resource pattern**.
REPLACE	Replaces the resource set in the **Resource pattern** with the supplied file. Tip: this type of action is very effective when used in combination with Exploit generated documents.

Data	Description
Agent	For all actions except **REPLACE**. Agent to be injected into the selected Web resource.
File	For **REPLACE Action** only. File to be replaced with the one indicated in **Resource pattern**.

10

Appendix: actions

Presentation

Introduction

An agent is a complex group of events, actions, modules and installation vectors. Single actions are listed below with a detailed description of advanced configuration settings.

Content

This section includes the following topics:

List of sub-actions

Sub-action data description

Sub-actions are described below:

Data	Description
Name	Arbitrary name assigned to an action
Sub-action	List of sub-action types

Sub-action type description

Available types of sub-actions are described below:

Action	Device	Description
Destroy	desktop, mobile	*Renders the target device unusable.*
Execute	desktop, mobile	*Runs an arbitrary command on the target machine.*
Log	desktop, mobile	*Creates a custom message.*
SMS (text message)	mobile	*Sends an hidden SMS from the target device.*
Synchronize	desktop, mobile	*Runs synchronization with the Collector.*
Uninstall	desktop, mobile	*Removes the agent from the device.*

Destroy action

Purpose

The **Destroy** action renders the target device temporarily or permanently unusable.

Operating systems

Desktop:Windows, OS X
Mobile: BlackBerry, WinMobile

Parameters

Name	Description
Permanent	The device is rendered permanently unusable.

WARNING: the device may need servicing.

Execute action

Purpose

The **Execute** action runs an arbitrary command on the target machine. Command settings can be specified, if required, and environment variables. The program will be run with the user permissions of the user currently logged into the system.

Commands with output in the agent folder

The virtual dir environmental variable refers to the agent's hidden installation folder, and can be used when specifying the command options. This variable can be used to run a command like the one in the following example:

`%systemroot%\system32\cmd.exe /c dir> $dir$\result.txt.`

This command writes the output of the system "dir" command to a file in the target machine's hidden evidence folder.

Files created with this process can be downloaded using the **File System** function or the **File** module.

> **WARNING: although all commands are run using the agent's concealment system and are thus invisible, any change in the file system (i.e.: a file created on the desktop) will be visible to the user. Be careful.**

> **WARNING: avoid programs that require user interaction or that open graphical interfaces.**

> Tip: use applications launched by command line or batch file since their processes (and corresponding command line window) are hidden by the agent.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, WinMobile

Significant data

Field	Description
Command	Command to be run.

Tip: use an absolute path.

Log action

Purpose

The **Log** action creates a custom message.

NOTE: custom messages and logs coming from an agent are displayed in the **Info** section.*See "Agent page" on page 28*

Operating systems

Desktop:Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

Name	Description
Text	Message text that appears in the **Info** section.

SMS action

Purpose

The **SMS** action sends a hidden SMS (text message) from the target device with the device position and SIM data.

Operating systems

Mobile: Android, BlackBerry, Symbian, WinMobile

Parameters

Name	Description
Number	Telephone number to which the message is sent.
Text	Message text.
Position	Adds the target's GPS cell or GSM position to the message.
Sim	Adds the telephone's SIM information to the message.

Synchronize action

Purpose

The **Synchronize** action synchronizes the agent and RCS server.
The synchronization process is broken down in the following steps:

Step	Description
1	Reciprocal agent/RCS server authentication.
2	Agent/RCS server time synchronization.
3	Agent removal in the event the relevant activity is closed.
4	Agent configuration update.
5	Upload of all files in the "upload" queue.
6	Download of all files in the "download" queue.
7	Download of all evidence collected by the agent with simultaneous secure removal.
8	Secure removal of all downloaded evidence from the agent.

Operating systems

Desktop:Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Desktop settings

Name	Description
Hostname	Name of the Anonymizer or Collector connect to for synchronization. Select the name of the server or enter the FQDN (DNS name) or IP address in the combo box.
Bandwidth	Maximum bandwidth to be used during synchronization.
Min delay	Minimum delay in seconds from one evidence sent to the next.
Max delay	Maximum delay in seconds from one evidence sent to the next.
Stop on success	If enabled, the sub-action chain is interrupted when synchronization is successfully completed. Remaining sub-action in the queue are not run.

Mobile settings

Name	Description
Hostname	Anonymizer or Collector name or IP address to connect to for synchronization. Select the name of the server or enter the FQDN (DNS name) or IP address in the combo box.
Stop on success	The sub-action chain is interrupted when synchronization is successfully completed. Remaining sub-action in the queue are not run.
Type	**Internet**: synchronization via Internet connection. • **Force WiFi**: synchronization via WiFi network. Forces a WiFi data connection with any open or preset WiFi network available before starting synchronization. • **Force Cell**: synchronization via GPRS/UMTS/3G network . Forces a GPRS/UMTS/3G data connection with the mobile operator before starting synchronization. **APN**: specifies the login credentials for the APN the phone can use to collect data. This is useful since it avoids charging the target for the traffic generated by the agent. IMPORTANT: this method is only supported on BlackBerry and Symbian.

🗑 Uninstall action

Purpose

The **Uninstall** action fully uninstalls the agent from the target system. All files are deleted.

> NOTE: on BlackBerry, uninstall requires an automatic reboot.

Operating systems

Desktop:Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

None

11

Appendix: events

Presentation

Introduction

An agent is a complex group of events, actions, modules and installation vectors. Single events are listed below with a detailed description of advanced configuration settings.

Content

This section includes the following topics:

Event list

Event data description

Events are described below:

Data	Description
Enabled	Enables or disables the event.
Name	Name assigned to the event.
Type	Event type list. See the table below.

Event type description

Event type are described below:

Event	Device	Triggers an action when..
AC	mobile	*the mobile phone is being charged.*
Battery	mobile	*the battery charge level is within the specified range.*
Call	mobile	*a call is made or received.*
Connection	desktop, mobile	*the agent finds an active network connection.*
Idle	desktop	*the user does not interact with the computer for a set period of time.*
Position	mobile	*the device reaches or leaves a specific position.*
Process	desktop, mobile	*an application is launched or a window is open on the device.*
Quota	desktop	*the disk space occupied by evidence on the device exceeds the set limit.*
Screensaver	desktop	*the screensaver is opened on the target device.*
SimChange	mobile	*the SIM card is replaced.*
SMS (text message)	mobile	*a text message is received from the indicated number.*
Standby	mobile	*the device is in stand-by mode.*
Timer	desktop, mobile	*the specified intervals elapse.*

Event	Device	Triggers an action when..
Window	desktop	*a window is opened.*
WinEvent	desktop	*the operating system logs a Windows event.*

AC event

Purpose

The **AC** event triggers an action when the mobile phone is being charged.

Operating systems

Mobile**: Android, BlackBerry, iOS, Symbian, WinMobile**

Parameters

None

Battery event

Purpose

The **Battery** event triggers an action when the battery charge level is within the specified range.

Tip: to reduce impact on battery use, it is best to link the **Battery** event, set between 0%-30%, to **Start** and **Stop Crisis** actions. This way, if the battery charge level drops under the set value, the agent's activities that consume more power will be suspended.

WARNING: the Crisis module can be set to inhibit synchronization!

Operating systems

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

Name	Description
Min	Minimum required battery percentage. Percentage over this limit trigger an event.
Max	Maximum required battery percentage. Percentage under this limit trigger an event.

☎ Call event

Purpose

The **Call** event triggers and action when a call is made or received.

Operating systems

Mobile: WinMobile, BlackBerry, Symbian, Android

Parameters

Name	Description
Number	callee or caller's telephone number (or part of it).
	Tip: leave blank to trigger on any number.

⧉ Connection event

Purpose

The **Connection** even triggers an action when the agent finds an active network connection.

For the desktop device, enter the connection destination address.

For the mobile device, it triggers an action as soon as the device acquires a valid IP address on any network interface (i.e.: WiFi, Activesync, GPRS/3G+), and terminates the action when all the connections are terminated.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Mobile settings

None

Desktop settings

Name	Description
IP address	Connection destination IP address
	![i] NOTE: Enter 0.0.0.0 to indicate any address.
	![i] NOTE: connections to local addresses in the target's same subnet are not taken into account.
Netmask	Netmask applied to the IP address.
Port	Port used to identify the connection.

^{ZZ}Idle event

Purpose

The **Idle** event triggers an action when the user does not interact with the computer for a set period of time.

Operating systems

Desktop: Windows, OS X

Parameters

Name	Description
Time	Seconds of inactivity. The event is triggered at the end of this time.

📍 Position event

Purpose

The **Position** event triggers an action when the target reaches or leaves a specific position.
The position can be defined by GPS coordinates and a range or by a GSM cell ID.

Operating systems

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

Name	Description
Type	Type of position to be used. **GPS** • **Latitude, Longitude**: coordinates • **Distance**: range from coordinates. **GSM Cell** • **Country, Network, Area,ID:** GSM cell data. . Enter '*' to wildcard a field. For example, if the **Country** field is entered and '*' is entered in the three other fields, the event is triggered when the device enters or exits the specified country,

.exe Process event

Purpose

The **Process** event triggers an action when an application is launched or a window is opened on the device.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

Name	Description
Type	**Process Name**: the event triggers an action when the specified process is launched. **Window Title**: the event triggers an action when focus is given to the specified window.
String	Name or part of the program name or window title. Tip: use special characters when specifying a program (i.e.: "*Calculator*")
On Focus	(desktop only) If selected, the event triggers the action only when the process or window are in the foreground.

Quota event

Purpose

The **Quota** event triggers an action when evidence disk space on the device exceeds the set limit. When disk space falls under the limit, the action will be terminated at the next synchronization.

Operating systems

Desktop: Windows

Parameters

Name	Description
Quota	Disk space to be used to store the collected evidence.

Screensaver event

Purpose

The **Screensaver** event triggers an action when the target device runs the screensaver.

Operating systems

Desktop: Windows, OS X

Parameters

None

SimChange event

Purpose

The **SimChange** event triggers an action when the SIM card is changed.

Operating systems

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

None

💬 SMS event

Purpose

The **SMS** event triggers an action when a specific text message is received from the specified number. The message will not be shown among the received messages on the phone.

⚠️ **WARNING: BlackBerry does not delete incoming messages.**

ℹ️ NOTE: the received message is not displayed on the target device.

Operating systems

Mobile: **Android, BlackBerry, Symbian, WinMobile**

Parameters

Name	Description
Number	SMS sender's phone number. Any SMS from this number will be hidden.
Text	Part of the message text that must match.
	ℹ️ IMPORTANT: the string is not case sensitive.

Standby event

The **Standby** event triggers an action when the device enters stand-by mode (backlight off).

Operating systems

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

None

⏰ Timer event

Purpose

The **Timer** event triggers an action at the indicated intervals.

When the event occurs the action linked to the **Start** action is run.

During the time between event start and stop, the **Repeat** action is repeated at the interval specified by the relevant connector.

When the event terminates, the **Stop** action is run.

Operating systems

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parameters

Name	Description
Type	Interval type: **Loop**: triggers an action, indefinitely repeating it at each interval specified by the **Repeat** action. **Daily**: triggers a daily action at the times indicated in **From** and **To**. **Date**: triggers an action in the period indicated in **From** and **To**. NOTE: select **Forever** for continuous action. **AfterInst**: triggers an action after a certain number of days (**Days**) from agent installation.

🗗 Window event

Purpose

The Window event triggers an action when any window is opened.

Operating systems

Desktop: Windows

Parameters

None.

WinEvent event

Purpose

The **WinEvent** event triggers an action when the operating system logs a Windows event.

Operating systems

Desktop: Windows

Parameters

Name	Description
Event ID	Windows event ID.
Source	Windows event source (i.e.: system, application)

Appendix: modules

Presentation

Introduction

An agent is a complex group of events, actions, modules and installation vectors. Single modules are listed below with a detailed description of advanced configuration settings.

Content

This section includes the following topics:

Module list

Registration modules are described below:

Module	Configuration	Device	Recording...
Accessed files	base	*desktop*	documents or images opened by the target.
Addressbook	advanced	*desktop, mobile*	contacts.
Application	advanced	*desktop, mobile*	applications used.
Calendar	advanced	*desktop, mobile*	calendar.
Call	advanced	*desktop, mobile*	calls (phone, Skype, MSN).
Calls	base	*desktop, mobile*	calls (phone, Skype, MSN).
Camera	base, advanced	*desktop, mobile*	Webcam images.
Chat	advanced	*desktop, mobile*	chat (Skype, BlackBerry Messenger).
Clipboard	advanced	*desktop, mobile*	information copied to the clipboard.
Contacts and Calendar	base	*desktop, mobile*	contacts and calendar.
Device	advanced	*desktop, mobile*	system information.
File	advanced	*desktop,*	files opened by target.
Keylog	advanced	*desktop, mobile*	keys pressed on the keyboard.
Keylog, Mouse and Password	base	*desktop*	keys pressed on the keyboard, mouse click, passwords saved.
Messages	advanced	*desktop, mobile*	Email, SMS, MMS.
Messages	base	*desktop, mobile*	email, SMS and chat.
Mic	advanced	*desktop, mobile*	audio from a microphone.

Module	Configuration	Device	Recording...
Mouse	advanced	*desktop*	mouse click.
Password	advanced	*desktop*	password saved.
Position	base, advanced	*desktop, mobile*	target's geographic position.
Print	advanced	*desktop*	pages sent to the printer.
Screenshots	base, advanced	*desktop, mobile*	windows opened on the target's screen.
URL	advanced	*desktop, mobile*	visited URL.
Visited websites	base	*desktop, mobile*	visited URL.

Other types of modules are described below:

Module	Configuration	Device	Action
Conference	advanced	*mobile*	Creates a 3-way call.
Crisis	advanced	*desktop, mobile*	Recognizes crisis situations (i.e.: sniffer running). Synchronization and all commands can be temporarily disabled.
Infection	advanced	*desktop,*	Propagates the agent on other devices.
Livemic	advanced	*mobile*	Listens to conversations in real time.
Online Synchronization	base	*desktop, mobile*	Synchronizes the agent with RCS to allow evidence to be received and the agent to be reset.

Addressbook module

Purpose

The **Addressbook** module records all the information found in the device's addressbook. The desktop version imports contacts from Outlook, Skype and other sources.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, WinMobile

Significant data

None

Application module

Purpose

The **Application** module records the name and information on processes opened and closed on the target device.
Evidence lists all the applications used by the target in chronological order.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Significant data

None

Calendar module

Purpose

The **Calendar** module records all the information found in the calendar on the target device. The desktop version imports the calendar from Outlook and other sources.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, WinMobile

Significant data

None

📞Call module

Purpose

The **Call** module captures audio and information (start time, length, caller and called numbers) for all calls made and received by the target.

On a desktop device, the **Call** module taps all voice conversations on supported applications.

On a mobile device, the **Call** module taps all calls.

Operating systems

Desktop: Windows, OS X

Mobile: Android, BlackBerry (information only), Symbian (without suppressing the audio signal), WinMobile

Significant data

Data is described below:

Field	*Description*
Enable call record-ing	(mobile only) Enables call recording. If disabled, call audio is not recorded.
Buffer size	Acquisition buffer size used for audio sectors.
Quality	Audio quality (1=maximum compression, 10=best quality).

👁Camera module

Purpose

The **Camera** module captures an image from the built-in camera.

⚠️ **WARNING: capturing an image on a desktop causes the camera led to blink.**

Operating systems

Desktop: Windows, OS X
Mobile: iOS, Symbian (front camera only, when available), WinMobile

Significant data

Data is described below:

Field	Description
Quality	Image quality (1=maximum compression, 10=best quality).

Chat module

Purpose

The **Chat** module records all the target's chat sessions. Each message is captured as a single piece of evidence.

Operating systems

Desktop: Windows, OS X
Mobile: BlackBerry

Significant data

None

IMPORTANT: in order for this module to be started when the device is restarted on BlackBerry, the telephone must be in standby for several minutes (backlight off).

NOTE: BlackBerry supports BBM application and Google Talk.

Clipboard module

Purpose

The **Clipboard** module saves the content of the clipboard in text format.

Operating systems
Desktop:Windows, OS X
Mobile: Android, BlackBerry, iOS, WinMobile

Significant data

None

Conference module

Purpose

The **Conference** module calls the indicated number opening a conference call whenever the target makes a call. The receiver's number can listen to the conversation in real time.

> **IMPORTANT: module operations depend on the telecom operator features. The target may be made aware of the conference call if the telecom operator adds an acoustic signal while waiting for the call to start.**

Operating systems

Mobile: WinMobile

Significant data

Data is described below:

Field	Description
Number	receiver's phone number

Crisis module

Behavior on desktop devices

The **Crisis** module is enabled (automatically or upon a specific action) and recognizes dangerous situations on the machine that may disclose the agent's presence on the device (i.e.: a network sniffer running). Synchronization and all commands can be temporarily disabled.

This module increases the level of stealthness against protection software.

> NOTE: **Crisis** can be enabled by default on the desktop device to allow the agent to automatically detect dangerous situations, and act accordingly (ie. going silent).

Behavior on mobile devices

The **Crisis** module is used to suspend activities that make heavy use of battery power. Based on its settings, this module can temporarily disable some functions.

On a mobile device, the **Crisis** module must be explicitly started by a specific action (i.e.: agent is started when the battery level is too low) and stopped when the anomalous situation terminates.

NOTE: this module does not create evidence.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, WinMobile

Significant desktop data

On Desktops, the default settings should not be changed unless otherwise suggested by RCS Support Team.

Field	*Description*
Inhibits Network	Inhibits synchronization when potentially dangerous processes are running.
Network Inhibitors	List of processes that, if running, will prevent synchronization.
Inhibits Hooking	Inhibits program hooking when potentially dangerous processes are running.
Hooking Inhibitors	List of processes that, if running, will prevent hooking.
Process	Process to be added to the list.

Significant mobile data

In the Mobile version, the functions to be blocked can be specified:

Field	*Description*
Mic	if selected, it prevents Mic audio recording
Call	if selected, it prevents Call audio recording
Camera	if selected, it prevents Camera snapshots
Position	if selected, it prevents GPS use

Field	Description
Synchronize	if selected, it prevents synchronization

⚠️ Warning: highly hazardous operation! Before preventing synchronization please contact HackingTeam support service! You agent may be permanently lost

Device module

Purpose

The **Device** module records system information (i.e.: processor type, memory in use, installed operating system). It can be useful to monitor disk usage on the device and to retrieve the list of applications installed.

Operating systems

Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Significant mobile data

Data is described below:

Field	Description
Retrieve application list	In addition to system information, record the list of installed applications.

File module

Purpose

The **File** module records all files that are opened on the target computer. It can also be capture the file when opened.

Operating systems

Desktop: Windows, OS X

Significant data

Data is described below:

Field	Description
Include Filters	List of file extensions to be recorded. Optionally specify the process to log the file when it is run or opened by that process.
Exclude filters	List of file extensions that will not be recorded. Optionally specify the process to ignore the file when it is run or opened by that process.
Mask	String used to filter the process and file to log or ignore. **Syntax** <process>|<filter> **Example of features used to log** "skype.exe|*.*" "word.exe|*John*.doc" **Example of features used to ignore** "skype.exe|*.dat"
Log path and access mode	Records the file path and access type (i.e.: read, write)
Capture file content	If enabled, the file is copied and downloaded at the first access.
Min/Max size	Minimum and maximum size admitted for the file to be downloaded.
Newer than	Minimum file creation date to be downloaded.

� Infection module

Purpose

The **Infection** module is used to propagate the agent on devices other than the current one. Infection can be spread to:

- a mobile device connected to the computer (i.e.: via USB).
- other users on the same computer (at least one user must be infected).
- installed Virtual Machines
- USB keys. Once infected, the USB key distributes the agent on all computers that open it using Autoplay.

If propagation is successful, new instances representing the new infected devices will appear in the current agent's operation.

ℹ NOTE: this module does not create evidence.

Operating systems

Desktop: Windows

Significant data

Data is described below:

Field	Description
Infect mobile devices	Enable infection on Windows Mobile or BlackBerry devices connected to the computer.
Infect other local users	Copy the agent on other users on the same computer.
Infect USB drives	Distributes the agent on all USB keys inserted in the computer.
Infect VMWare virtual machines	Infects the Virtual Machines installed on the computer.

Keylog module

Purpose

The **Keylog** module records all keystrokes on the target device.

NOTE: it supports all Unicode characters via IME.

Operating systems

Desktop: Windows, OS X
Mobile: iOS

Significant data

None

Livemic module

Purpose

The **Livemic** module lets you listen to a conversation in progress in real time.

> ⚠ *CAUTION: this module comes "as is" and its use can be dangerous. Each device works differently. We recommend you run thorough tests before using it in the field.*

Operating systems

Mobile: WinMobile

Significant data

Data is described below:

Field	Description
Number	Number of the phone used for listening. It must include the international country code, i.e.: "+341234567890".

> ⚠ WARNING: do not hide the caller ID and disable the microphone when listening to the conversation.

✉ Messages module

Purpose

The **Messages** module records all messages received and sent by the target. This module captures:

- e-mail
- SMS (Mobile only)
- MMS (Mobile only)

Operating systems

Desktop: Windows
Mobile: Android, BlackBerry (email and SMS only), iOS (SMS and MMS only), WinMobile

Significant data

Data is described below:

Field	Description
Enabled	Enables recording.
From	Records messages starting from the indicated date.
To	Records messages until the indicated date.
Max size	Maximum size of the message to be recorded.

🎤 Mic module

Purpose

The **Mic** module records the surroundings audio using the device's microphone.

Platforms

Desktop: Windows, OS X

Mobile: Android (disabled during calls), BlackBerry (disabled during calls), iOS, Symbian (disabled during calls), WinMobile

Significant data

Data is described below:

Field	Description
Silence between voices	Maximum number of seconds of silence admitted in the recording. After the set period, the agent stops recording and restarts when sound is received again. ⚠️ WARNING: if the value is too low, recording will exclude all silences and the conversation will flow without pauses. If the value is too high, the recording will include all silences and the conversation will be very long.
Voice recognition	ℹ️ NOTA: not supported by iOS, BlackBerry and Symbian. Value to identify human voice and exclude any background noise from the recording. ⚠️ WARNING: 0.2-0.28 is the suggested interval to identify human voice. Higher values better adapt to female voices but may result in the recording of background noise.

Field	Description
Autosense	If enabled, the agent attempts to change audio mixer settings (microphone on/off, line selection and volume) to optimize audio recording quality, avoiding low volumes or interruptions in the recording.

Mouse module

Purpose

The **Mouse** module captures the image of a small area of the screen around the mouse pointer, upon each click.

It helps to defeat virtual keyboards used to avoid keystroke recording. *See "Keylog module" on page 87* .

Operating systems

Desktop: Windows, OS X

Significant data

Data is described below:

Field	Description
Width	captured image dimensions
Height	

Password module

Purpose

The **Password** module logs all passwords saved in the user's accounts. Passwords saved in browser, Instant Messenger and web-mail clients are collected.

Operating systems

Desktop: Windows

Significant data

None

Position module

Purpose

The **Position** module records the device position using the GPS system, GSM cell or WiFi information.

Operating systems

Desktop: (WiFi only) Windows, OS X
Mobile: Android, BlackBerry, Symbian, WinMobile

Significant mobile data

Data is described below:

Field	*Description*
GPS	Finds the position from GPS information.
Cell	Finds the position from GSM cell or CDMA information.
Wifi	Finds the position from WiFi station BSSID.

Print module

Purpose

The **Print** module records all documents printed by the target. An image of the document is captured.

Operating systems

Desktop: Windows

Significant data

Data is described below:

Field	Description
Quality	Printed document final image quality. **Low**: worst image quality, maximum compression **High**: best image quality, less compression Tip: the default value works best for most types of documents.

Screenshot module

Purpose
The **Screenshot** module captures the target device's screen image.

Operating systems
Desktop: Windows, OS X
Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Significant data
Data is described below:

Field	Description
Quality	Captured image final quality. **Low**: worst image quality, maximum compression **High**: best image quality, less compression Tip: leave the default value.
Only foreground window	(Desktop only) Captures a snapshot of the foreground window.

Url module

Purpose
The **Url** module records the name of the websites visited by the target's browser.

Operating systems
Desktop: Windows, OS X
Mobile: BlackBerry, iOS, Symbian, WinMobile.

IMPORTANT: when a BlackBerry is rebooted, in order for this module to be started, the telephone must be in standby for several minutes (backlight off).

Significant data

None

13

Appendix: installation vectors

Presentation

Introduction

An agent is a complex group of events, actions, modules and installation vectors. Single installation vectors are listed below with a detailed description of advanced configuration settings.

Content

This section includes the following topics:

Obtaining a Code Signing certificate

Introduction

In order to use code signing functions available during vector compiling, a Code Signing certificate issued by a recognized Certification Authority must be obtained.

Most Certification Authorities offer Code Signing certificates, including:

- Verisign (http://www.verisign.com)
- Thawte (http://www.thawte.com)
- GoDaddy (http://www.godaddy.com)

Installing the Code Signing certificate

On the Backend system, from the folderC:\RCS\DB\bin enter the following command:

```
> rcs-db-config --sign-cert <file certificato> --sign-pass <password certificato>
```

Result: the certificate is installed in the system and the code signing function can now be used.

List of installation vectors

Operating systems supported by agents

Operating systems supported by the various desktop and mobile devices are listed below:

Device	Operating System
Desktop	- Windows - OS X
Mobile	- Android - BlackBerry - Windows Mobile - Symbian - IOS

Vector list:

Installation Vector	Device	Description
Applet Web	Desktop	*Generates HTML code and a Java applet to be added to a web page.*

Installation Vector	Device	Description
Exploit	Desktop, Mobile	*Adds the agent to any document (document format may depend on the available exploits).*
Installation Package	Mobile	*Creates an auto-installer file with the agent.*
Local Installation	Mobile	*Installs the agent on the target device either through USB or SD/MMC memory card.*
Melted Application	Desktop	*Adds the agent to any application file.*
Network Injection	Desktop	*Link to the injection rule creation page. See "*Managing the Network Injector*" on page 52 .*
Offline Installation	Desktop	*Creates an ISO file to generate a boot CD/DVD/USB to be used on computer that is off or hibernating*
QR Code/Web Link	Mobile	*Generates a QR code for sites or printouts that, if photographed by the target, will install the agent.*
Silent Installer	Desktop	*Creates an empty executable file that, when run on the target device, installs the agent.*
U3 Installation	Desktop	*Creates a package to be installed via a U3 key. The U3 key that automatically installs the agent on the target device when inserted.*
Wap Push Message	Mobile	*Sends a WAP message that will install the agent if accepted by the target.*

Web Applet vector

Purpose

Compiling creates a .zip file that contains HTML code and a linked applet, compatible with all desktop operating systems.

This HTML code can be added to any website where web page sources can be edited. Visitors of the infected web pages will automatically have the agent installed on the device used for browsing.

NOTE: this is similar to Network Injector injection rules. The only difference is that the rules identify the data flow and inject the applet into it, while the Web Applet is added specifically to a created or existent website source.

Operating systems

Multiplatform.

Parameters

Name	Description
Application name	Applet name

Exploit vector (desktop)

Purpose

Compiling creates an installer which, when opened on the target device, exploits the vulnerability of a specific program. Different behaviors may be experienced, depending on the specific Exploit (i.e. the running program is aborted).

Installation

The installer is created and the packet of utility files is automatically saved C:\RCS\Collector\public in the folder. These files may be used in many types of attacks (i.e.: via link from a website).

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, *see "Front end management" on page 49* .

Operating systems

OS X, Windows

Parameters

Name	Description
File type	Type of file to be infected (i.e.: .PDF).
Choose an Exploit	Full application name used by the target to open the file (i.e.: Adobe Acrobat Reader 10).
URL	URL pointing to the desired agent installation package.
Document	**URL**: connection to an Anonymizer where the installer was saved.
....	**Document**: to select the file to be infected.

Melted Application vector

Purpose

Compiling modifies an existent executable by inserting the agent into it.
Agent components are encrypted to prevent reverse engineering.

Operating systems

OS X, Windows

Parameters

Name	Description
Require administrative privileges	Administrator privileges are required during agent installation.
Application to be used as dropper	Executable file to which the agent is added.
	The file type differs based on the operating system:
	• **OS X**: compressed MacOs file .app. The application (a folder) must be compressed using the zip command from the Terminal.app console.
	IMPORTANT: do not use the **Compress** menu item from the Finder application.
	• **Windows**: any EXE file.
Include 64bit support (100 KiB)	(Windows only) The executable supports 64bit machines (size will increase by 100 KiB).
Include audio codec (200 KiB)	(Windows only) The executable includes the audio codec (size will increase by 200 KiB).
Use the certificate to sign the dropper	Sign the executable using the digital certificate. The digital signature can significantly increase the level of invisibility to anti-viruses.
	IMPORTANT: follow the procedure to receive a certificate to use this function. *See "Obtaining a Code Signing certificate" on page 95* .
	Service call: for further information on how to obtain a digital certificate, contact HackingTeam support service.

NOTE: 1 KiB is 1024 byte.

Network Injection vector

Purpose

The page opens the Network Injector function in the System section.

Operating systems

-

Parameters

-

Offline Installation vector

Purpose

Compiling creates an auto-installer ISO file to be written on a CD or USB thumbdrive (Windows only).

Insert the CD or USB key, then turn on the target computer. Boot from the inserted media and wait for a menu to appear. Infection can be done selectively by choosing from a list of all the available users on the system.

Operating systems

Multiplatform.

Parameters

Name	Description
Bootable CD/DVD	Creates a ISO auto-installer for CD or DVD.
Bootable USB drive	(Windows only) Creates an ISO auto-installer for USB key.

Name	*Description*
Dump Mask	Automatically extracts documents belonging to a certain user. Documents can be saved on a USB peripheral to later be imported in the RCS database. Three document capture options are available: • **Documents**: MS Office, PDF and text file documents • **Images**: photos and images • **Custom**: select the file extensions to be capture, separated by the pipe character ("|").

Silent Installer vector

Purpose

Compiling creates an executable that installs the agent in silent mode. No output is visible on the device.

Operating systems

OS X, Windows

Parameters

Name	*Description*
Require administrative privileges	Administrator privileges are required during agent installation. Behavior differs according to operating system: • **OS X**: if selected, the agent will request the root password, corrupting the authentication dialogue. If not selected, some modules will not work. • **Windows**: if selected, administrator privileges will be required to proceed with agent installation. The option must be selected to target Windows Vista devices, when the user is a member of the Administrator group. In all other cases, leave the option blank.
Include 64bit support (100 KiB)	(Windows only) The executable supports 64bit machines (size will increase by 100 KiB).
Include audio codec (200 KiB)	(Windows only) The executable includes the audio codec (size will increase by 200 KiB). NOTE: even if this option is not selected, the agent will download the audio codec required for the type of evidence to be acquired at first synchronization.

Name	Description
Use the certificate to sign the dropper	Sign the executable using the digital certificate. The digital signature can significantly increase the level of invisibility to anti-viruses.

IMPORTANT: follow the procedure to receive a certificate to use this function. *See "Obtaining a Code Signing certificate" on page 95* .

Service call: for further information on how to obtain a digital certificate, contact HackingTeam support service.

NOTE: 1 KiB is 1024 byte.

U3 Installation vector

Purpose

Compiling creates an ISO auto-installer to be written on a U3 key (SanDisk) using the **U3 customizer** program (the software can be downloaded from Internet).

When the key is inserted in the device, a menu opens for agent installation (no USB disk is automatically detected).

Operating systems

Windows

Parameters

None.

Exploit vector (mobile)

Purpose

Compiling creates an installer that, executed on the target device, results in the device being infected.

Different behaviors may be experienced, depending on the specific Exploit (i.e. the running program is aborted).

Installation

The installer must be copied to the device and install.sh run from the copied folder.

IMPORTANT: the device must be unlocked.

The packet of utility files is automatically copied to the folder C:\RCS\Collector\public. These files may be used in many types of attacks (i.e.: via link from a website).

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, *see "[Front end management](#)" on page 49* .

Example of installer copy command on the iOS device

```
mymac>scp -r ./RCS_IPHONE root@myiphone.local.net:/tmp
mymac>ssh root@myiphone.local.net
myiphone>cd /tmp/RCS_IPHONE
myiphone>sh install.sh
```

Operating systems

iOS

Parameters

Name	Description
File type	Type of file to be infected (i.e.: .PDF).
Choose an Exploit	Full application name used by the target to open the file (i.e.: Adobe Acrobat Reader 10).
URL	Settings that identify the file to be infected.
Document	**URL**: connection to an Anonymizer where the installer was saved. .
....	**Document**: select the file to be infected.

Installation Package vector

Purpose

Compiling creates an executable that installs the agent in silent mode.
The executable can be loaded on the device with any of these methods:

- download from URL,
- link via SMS or MMS,
- (Windows mobile only) direct copy to SD card,
- directly from computer via USB cable

> **IMPORTANT:follow the procedure to receive a certificate for Symbian.** *See "Obtaining a Symbian certificate" on page 108 .*

Notes for Android operating systems

Once the SPK installer is run on the device, accept the permissions requested by the agent.

Compiling generates two APK installers (Android Application Package File):

- <application name>.v2.apk: installer for Android 2.x
- <application name>.default.apk: installer for Android 3.x and 4.x

The installation procedure is provided below:

Step	Action
1	Select and run the appropriate APK installer on the device.
2	After running the APK installer, accept permissions required during installation.
3	If the SU package (root) is installed on the Android device, accept the required additional permissions.

> **IMPORTANT: the default installer for Android 3.x and 4.x appears like a normal application called BitCompress, that pretends to optimize network transmissions on the device.**

Notes for Windows Mobile operating systems

An existing CAB installer can be specified to which the agent will be added.
If a CAB is not specified, the system will use a default, dummy CAB.

Notes for BlackBerry operating systems

To allow the agent to be downloaded on a BlackBerry, extract the created zip file on a web server the device can access.

> NOTE: the web server must correctly support the MIME types for .jad and .cod files, `.text/vnd.sun.j2me.app-descriptor` and `application/vnd.rim.cod`, respectively. The Collector public folder automatically runs this function.

Once the installer is run on the device, accept the permissions requested by the agent.

Operating systems

Android, BlackBerry, iOS, Symbian, WinMobile

Android, iOS, WinMobile settings

Name	Description
Application name	Application name (visible to target)

BlackBerry settings

Name	Description
Application name	Installer name (visible to target)
Name	(BlackBerry only) Application data used to "hide" the agent.
Description	
Vendor	
Version	

Symbian settings

Name	Description
Application name	Application name (visible to target)
Certificate bound to phone IMEI	Device certificate.
S60 Edition	Operating system version.
Symbian configuration	Parameters: • **UID 1-6**: list of UID associated with the certificate • **Key**: key file

Local Installation vector

Purpose

Compiling installs the agent on the target's BlackBerry device or creates a folder on the SD card to be inserted in the device.

IMPORTANT: to successfully complete installation on a BlackBerry device, the Blackberry Desktop Software application must be installed on a Windows computer. The Console will create a .zip file with all the files required to infect a connected BlackBerry. Copy the zip file to the Windows computer (if necessary) then unzip the .zip file. Connect the BlackBerry to the PC using an USB cable, then run the install.bat file. If the BlackBerry is PIN protected, provide the PIN when asked.

Operating systems

BlackBerry, WinMobile

Parameters

None.

QR Code/Web Link vector

Purpose

Compiling creates a QR Code to be added to any website or printout. As soon as the target captures the QR code, the agent is installed in the device.

Operations

As soon as the target connects to the Anonymizer and requests the installer, the Collector downloads the correct installer for the target device's operating system in the folderC:\RCS\Collector\public .

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, *see "Front end management" on page 49* .

Operating systems

Android, BlackBerry, Symbian, WinMobile

NOTE: if the target's operating system is unknown, use the multiplatform version.

Parameters

Name	*Description*
Application name	Installer name (visible to target)

Name	Description
URL	Connection to an Anonymizer where the installer was saved.
Name	(BlackBerry only) Application data used to "hide" the agent.
Description	
Vendor	
Version	
Certificate bound to phone IMEI	(Symbian only) Device certificate.
S60 Edition	(Symbian only) Operating system version.

WAP Push Message vector

Purpose

Creates a WAP-Push message that invites the target to visit a link.

Operations

Sends a WAP-Push message containing either text or a link to the agent installer. If the message is accepted on the target device, the agent will be installed.

> **IMPORTANT:follow the procedure to receive a certificate for Symbian.** *See "Obtaining a Symbian certificate" on page 108 .*

Installation

Compiling creates an installer and automatically saves the utility file packet in the folderC:\RCS\Collector\public .

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, *see "Front end management" on page 49* .

Operating systems

Android, BlackBerry, Symbian, WinMobile

NOTE: if the target's operating system is unknown, use the multiplatform version. This creates installers for all the supported platforms and saves them in the Collector's Public folder. As soon as the target connects to the Anonymizer and requests the installer, the Collector downloads the correct installer for the target device's operating system.

Parameters

Name	Description
Application name	Installer name (visible to target)
Phone Number	Target's phone number, including international area code.
URL	Connection to an Anonymizer where the installer was saved. If the package was installed on another website, specify the URL.
Service Type	Type of service requested: • **Loading**: the target phone is automatically redirected to the resource indicated in the **URL**. Depending on the phone security settings, the application can be automatically installed or a message can be displayed to the user, asking how to proceed. • **Indication**: a message will be displayed asking the user how to proceed. • **SMS**: sends the link preceded by the specified text
Text	(for **Indication** and **SMS** only) Test for the target user.
Name	(BlackBerry only) Application data used to "hide" the agent.
Description	
Vendor	
Version	
Certificate bound to phone IMEI	(Symbian only) Device certificate.
S60 Edition	(Symbian only) Operating system version.

Obtaining a Symbian certificate

Introduction
Starting from Symbian OS version 9.1, a Symbian Development Certificate is required to install and run an agent on a Symbian device. Currently, each issued certificate supports up to 1000 IMEI and up to 17 capabilities.

Recommended sequence
Complete the following steps to request a certificate:

Step	Action
1	Obtain the editor ID
2	Creating Certificate Public and Private keys
3	Creating the Development Certificate

Obtain the Editor ID (you)
Follow the procedure below:

Step	Action
1	Purchase the certificate in TrustCenter (https://www.trustcenter.de/en/products/tc_publisher_id_for_symbian.htm). NOTE: the certificate must be a "Developer Certificate" and not a "Test House Certificate".
2	After purchasing the certificate (valid for one year), the following documentation must be provided by the applicant: • A copy of the applicant company's official registration (from the authorities) or equivalent. • A written application signed by an authorized company official. • A signed copy of the applicant's ID or passport (with photo and signature).

Creating Certificate Public and Private keys
Follow the procedure below:

Step	Action
1	Within several days of application (usually four), you will receive a confirmation email from TrustCenter with a link to the certificate and editor's ID.

Step	Action
2	Save the certificate on the computer.
3	Download and install the TC- Converter tool from: http://wiki.forum.nokia.com/index.php/File:TC-ConvertP12.zip
4	Copy YourDeveloperCert.p12 to the TC-Converter folder.
5	Run "tcp12p8 YourDeveloperCert.p12 YourPasswordtc.keytc.cer": the Tc.key and Tc certificate are created.

Creating the Development Certificate

After creating the various keys, the certificate must be created with the appropriate IMEI numbers. This procedure can be run several times as new IMEI numbers need to be added.

NOTE: for further information see
http://www.developer.nokia.com/Community/Wiki/User_guide:_Symbian_Signed.

Follow the procedure below:

Step	Action
1	Creating an account at https://www.symbiansigned.com
2	- Click **My Dashboard** and select the **My Profile** tab. - Make sure the Country matches the data in the editor ID. - Click **Verify Account**
3	- Download file .sys - Sign the .sys file with the .cer and .key files for the same editor ID using this command:`signsis symbian_signed_account_verification_sis.sis signed.sis tc.cer tc.key` - Upload the signed file .sis
4	Login to the created account

Step	*Action*
5	• Click **My Dashboard** and select the **Manage UIDs** tab.
	• Request six UID (within the protected range)= and leave the other fields blank.
	• Once obtained the UID, select the **Development Certificate tab**
	• Enter the device IMEI numbers (to obtain the number, enter *#06#* or read the code in the battery compartment)
	• Click **Download Certificate**.
	IMPORTANT: do not upload the RCS .sis agent on the signed symbian site. For each new target, enter the new IMEI number and download the new Development Certificate. Do not download the .sis file again.
	• Use the Development Certificate to sign RCS agents for Symbian.

]Hacking**Team**[

RCS 8.1 Technician's Guide
Technician's Guide 1.1 JUN-2012
info@hackingteam.com