]HackingTeam[

RCS 9

The hacking suite for governmental interception

Technician's Guide

Information ownership

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.

BSSID
(Basic Service Set IDentifier) Access Point and its client identifier.

C

Carrier
Collector Service: sends data received from Anonymizers to shards or the Master Node.

Collector
Collector Service: receives data sent by agents, via 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 cus-

tomer digital subscriber line (DSL) interfaces to a high-speed digital communications channel using multiplexing techniques.

E

Elite agent
Agent installed on secure devices. Lets you collect all types of available evidence.

entity
Group of intelligence information linked to the target and people and places involved in the investigation.

ESSID
(Extended Service Set IDentifier) Known as SSID, identifies the WiFi network.

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.

Exploit
Code which, exploiting a bug or vulnerability, runs an unforeseen code. Used to infect target devices.

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.

G

Group
Intelligence entity that groups several entities.

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
Collector Service: 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 on the field.

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.

P

Person
Intelligence entity that represents a person involved in the investigation.

Position
Intelligence entity that represents a place involved in the investigation.

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

Scout agent
Replaced the agent sent to the device to check the security level before installing actual agents (elite or soldier).

Soldier agent
Agent installed on not fully secure devices. Only lets you collect some types of evidence.

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. It is represented by the Target entity in the intelligence section.

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

V

Virtual
Intelligence entity that represents a virtual location (i.e.: website) involved in the investigation.

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

W

WPA
(WiFi Protected Access) WiFi network protection.

WPA 2
(WiFi Protected Access) WiFi network protection.

1

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*
19 February 2014	Technician's Guide 1.6 FEB-2014	9.2	Removed information on operating systems that support each action, module and event in advanced settings. If necessary, contact technical support. Added **Money** module *see " **Money module**" on page 139* . Updated installation vector documentation, *see "**Appendix: installation vectors**" on page 142* . Added soldier level agent, *see "**What you should know about agents**" on page 39* . Added remote access settings to Tactical Control Center and Appliance Control Center applications,*see "**Tactical Control Center** " on page 91 , "**What you should know about Control Center remote access**" on page 82* Added network test on Appliance Control Center, *see "**Appliance Control Center** " on page 85* . Removed INJECT-UPGRADE rule, *see "**Injection rule data**" on page 71* . Added what you should know about **Wireless Intruder**, *see "**What you should know about identifying the WiFi network password**" on page 81* . Added description of terminal commands for Tactical Control center and Appliance Control Center applications, *see "**Tactical Control Center and Appliance Control Center commands**" on page 84*
30 September 2013	Technician's Guide 1.5 SEP - 2013	9	Added Windows Phone platform, *see " **Installation Package vector**" on page 146* Updated documentation to manage root privileges for Android devices, *see "**What you should know about Android**" on page 144* . Updated Network Injector management documentation, *see "**The Network Injector**" on page 66* . Updated documentation due to improvements to the user interface. Improved the contents.

Release date	*Code*	*Software version.*	*Description*
8 July 2013	Technician's Guide 1.4 JUL-2013	8.4	The chance to test network connections, select an additional dictionary to attack a WPA or WPA 2 protected network and display installed rules were added on Tactical Control Center. Network signal power is now always visible. *See "**What you should know about Tactical Control Center**" on page 76 .* A public IP address can be mapped on a private IP address set on the network interface and installed rules viewed on Appliance Control Center. *See "**What you should know about Appliance Control Center**" on page 76 .* Removed the INJECT-HTML-JAVA rule and added INJECT-HTML-FILE and INJECT-HTML-FLASH rules. *See "**Injection rule data**" on page 71 .* Deleted the **Applet Web** vector and deprecated the **Infection** module. Added note to **Uninstall** action on Android. *See "**Uninstall action**" on page 118 .* For Android, the limit of root privileges necessary for Chat, Messages and Screenshot modules has been extended to all operating system versions. *See "**Chat module**" on page 132 , "**Messages module**" on page 137*
15 March 2013	Technician's Guide 1.3 MAR-2013	8.3	Changed Tactical Control Center use. *See "**Tactical Control Center** " on page 91 .* Changed Appliance Control Center use. *See "**Appliance Control Center** " on page 85 .* Added possibility of creating a factory on the operation level. *See "**Operation page**" on page 24 .* Changed **Installation Package and Melted application vectors** *see "**List of installation vectors**" on page 143 .* Added possibility of disabling screenshot evidence in the scout agent. *See "**What you should know about agents**" on page 39 .* Added license management to exclude file upload and command execution on the target device. *See "**File transfer to/from the target**" on page 46 .*

Release date	*Code*	*Software version.*	*Description*
15 October 2012	Technician's Guide 1.2 OCT 2012	8.2	Added basic or advanced configuration save as template. *See "What you should know about the basic configuration" on page 51* and *See "What you should know about advanced configuration" on page 57* . Added quick investigation creation wizard. *See "Wizards in the homepage" on page 13* Added scout agent management. *See "What you should know about agents" on page 39* .
30 June 2012	1.1 JUN 2012 Technician's Guide 1.1 JUN 2012	8.1	Added agent functions *see "Agent page" on page 42* . Added **Idle** event *see "Idle event" on page 123* . Changed installation for **Exploit**, **WAP push** and **QR Code** vectors. Changed vectors **Offline Installation, Installation Package** ***see "List of installation vectors" on page 143*** **.** Changed process to obtain Symbian certificate . Code Signing certificate for **Melted Application** and **Silent Installer vectors** *see "Obtaining a Code Signing certificate" on page 145* .
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 1.5 FEB-2014*	PDF
Administrator's Guide	Administrators	*Administrator's Guide 1.5 FEB-2014*	PDF
Technician's Guide (this manual)	Technicians	*Technician's Guide 1.6 FEB-2014*	PDF
Analyst's Guide	Analysts	*Analyst's Guide 1.5 FEB-2014*	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

2

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 between RCS 8.0 and RCS 7.6 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

3

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

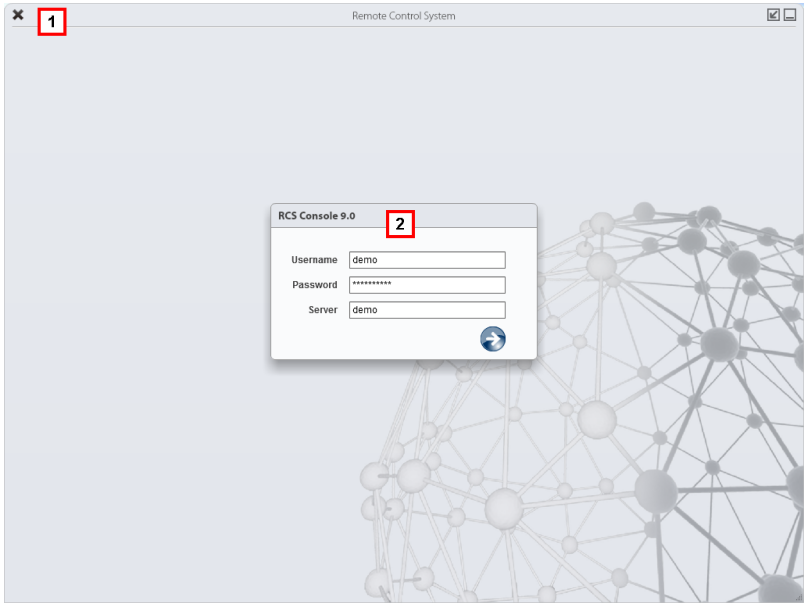
This section includes the following topics:

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 : the homepage appears with the menus enabled according to your account privileges. *See "**Homepage description**" below .*

Homepage description

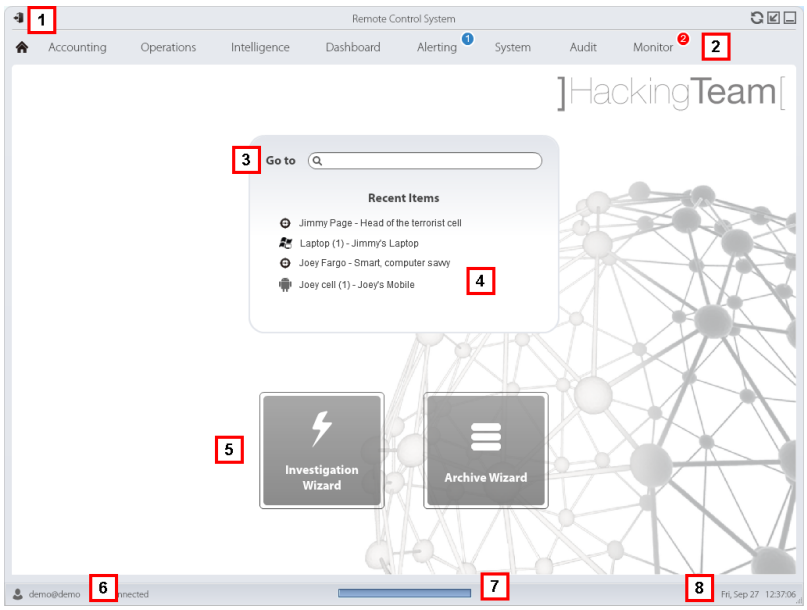
To view the homepage:	• click

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, agents and entities, by name or description.

Area	*Description*
4	Links to the last five elements opened (operation in the Operations section, operation in the Intelligence section, target, agent and entity).
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.

Wizards in the homepage

To view the homepage:

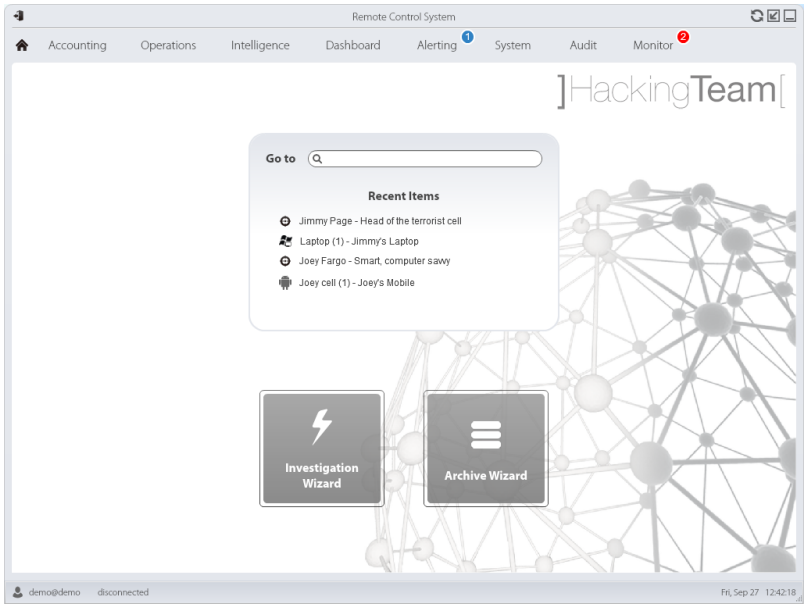
- click 

Introduction

For users with certain privileges, RCS Console displays buttons that run wizards.

What it looks like

This is how the homepage is displayed with enabled wizards:



Button	*Function*
	Open the wizard to quickly create an agent. NOTE: the button is only enabled for users with Administrator and Technician privileges.
	Open the wizard to quickly save operation and target data. NOTE: the button is only enabled for users with Administrator and System Administrator privileges.

Investigation Wizard

This wizard quickly creates an agent. The wizard asks you to enter the name (i.e.: "SmartSpy") and type of agent to be created (desktop or mobile) and creates, in the following order:

1. a "SmartSpy" operation
2. a "SmartSpy" target
3. a "SmartSpy" factory
4. a "SmartSpy" user group in which the current user is the sole member

and directly opens the factory configuration page. *See "Basic factory or agent configuration" on page 51*

Other elements can be added to this operation, target or user group by simply using the detail page.

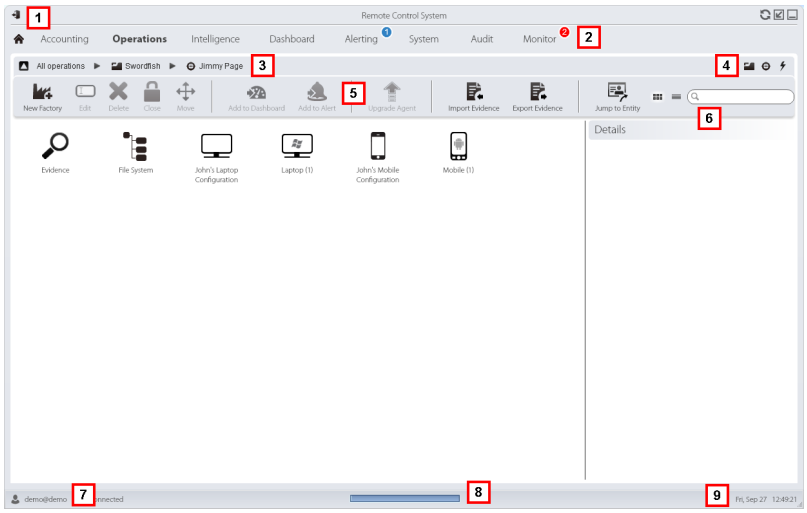
Shared interface elements and actions

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 (Operations section).
	Show the target page.
	Show the factory page.
	Show the agent page.
	Show the operation page (Intelligence section).
	Show the entity 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.
	Show all entities.

5	Window toolbar.
6	Search buttons and box:

Object	*Description*
	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.

7	Logged in user with possibility of changing the language and password.
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 **[7]** to display a dialog window with the user's data.
2	Change the language or password and click **Save** to confirm and exit.

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

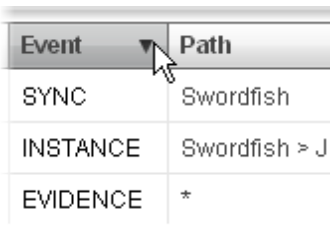
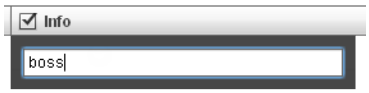
To convert all dates-times to the actual time zone:

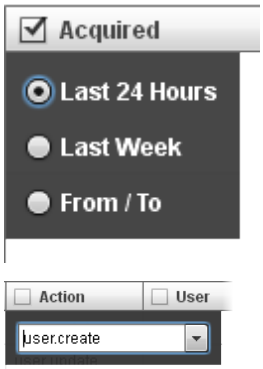
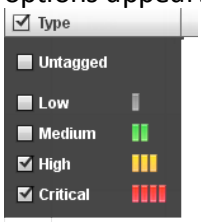
Step	*Action*
1	Click **[9]** to display a dialog window with the current date-time: **UTC time**: Greenwich mean time (GMT) **Local Time**: date-time where the RCS server is installed **Console time**: date-time of the console used and which can be converted.
2	Change the time zone and click **Save** 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. 
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. 
Filter based on several options	Select one or more options: the elements that match all selected options appear. 
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 the **System**, **Network Injector** section, create identification and injection rules for Network Injector Appliance and Tactical Network Injector. *See "**Managing the Network Injector**" on page 68* NOTE: no agent installation is required.
2	When using Network Injector Appliance, the system applies the identification rules to traffic data. Once target devices are found, they are infected with the injection rules. Or they can be automatically or manually identified and infected using Tactical Network Injector. *See "**Tactical Control Center** " on page 91 .*

Infecting a computer not connected to Internet

To infect a computer not connected to Internet

Step	Action
1	Create a factory by disabling synchronization on the operation level, *see "**Operation page**" on page 24 .* Or create a factor on the target level always without synchronization, *see "**Target page**" on page 28*
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 35 .*
3	Install the agent on the target device with the selected methods. *See "**List of installation vectors**" on page 143 .*
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 42 .*

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 "**Operation page**" on page 24*
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 35 .*
3	Install the agent on the target device with the selected methods. *See "**List of installation vectors**" on page 143 .*
4	The agent appears in the target page at first synchronization. *See "**Target page**" on page 28*
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 51* *See "**Advanced factory or agent configuration**" on page 60 .*

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 28* or • In **Operations** section, **Target** open an agent and update it. *See "**Agent page**" on page 42 .*

Operation and target

Presentation

Introduction

Managing operations sets the targets to be tapped.

Content

This section includes the following topics:

What you should know about operations

What is an operation

An operation is an investigation to be conducted. An operation contains one or more targets meaning the physical individuals to be tapped. The Technician assigns one or more agents, *desktop* or *mobile,* to the target. Thus the agent can be installed on a computer or mobile phone.

What you should know about targets

What is a target

A target is the physical person to be investigated. The Technician assigns one or more agents, desktop or mobile, to the target. Thus the agent can be installed on a computer or mobile phone.

Operation management

To manage operations:	• **Operations** section

Purpose

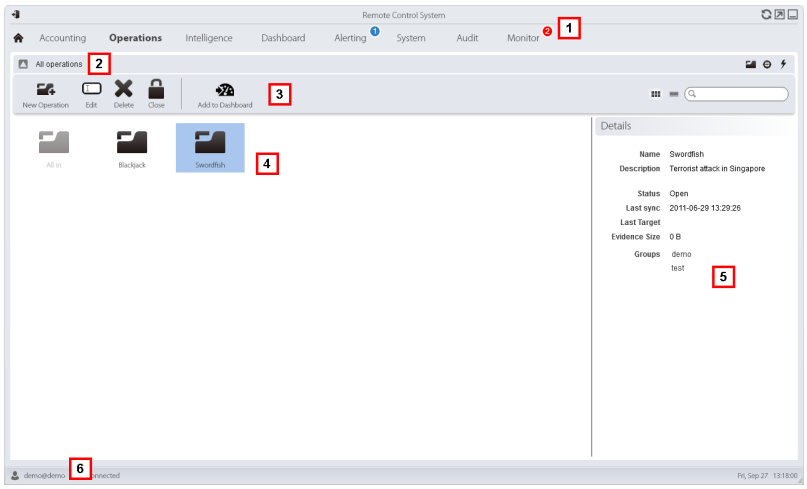
This function lets you:

- view and manage targets linked to an operation

NOTE: the function is only enabled if the user has **Operation management** authorization.

What the function looks like

This is what the page looks like:



Area	*Description*
1	RCS menu.
2	Scroll bar
3	Window toolbar.
4	List of created operations:  Open operation. If targets were set and agents correctly installed, collected evidence is received.  Closed operation. All targets are closed and agents uninstalled. All its targets and evidence can still be viewed.
5	Selected operation data.
6	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*

For a description of the data in this window *see "**Operation data**" on the facing page .*

For more information on operations *see "**What you should know about operations**" on the previous page .*

Viewing operation targets

To view operation targets:

Step	*Action*
1	Double-click an operation: the target management page opens. *See "**Operation page**" below*

Operation data

Selected operation data is described below:

Data	*Description*
Name	Operation name.
Description	User's description
Contact	Descriptive field used to define, for example, the name of a contact person (Judge, Attorney, etc.).
Status	Operation status and close command: **OPEN**: the operation is open. If targets were set and agents correctly installed, the RCS receives the collected evidence. **CLOSED**: the operation is closed and can not be re-opened. Agents no longer send data but evidence already received can still be viewed.
Groups	Groups that can see the operation.

Operation page

To view an operation:	• **Operation** section, double-click an operation

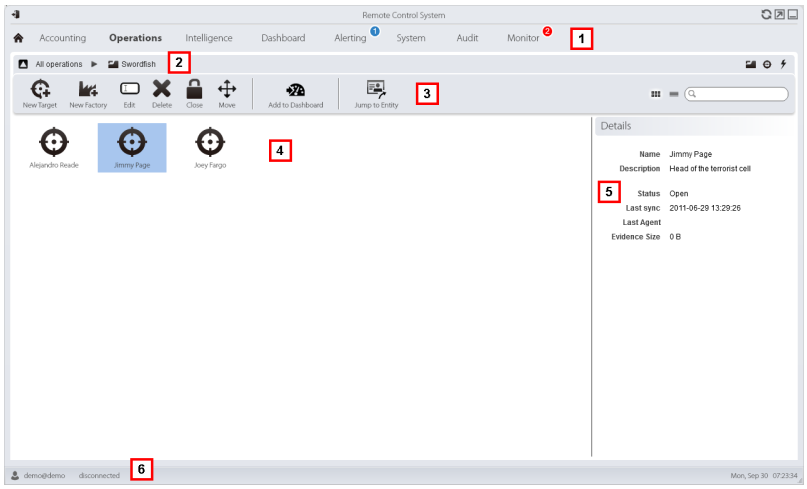
Purpose

This function lets you:

- manage factories which, once compiled, become agents to be installed on devices*see "**Advanced factory or agent configuration**" on page 60*

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	*Function*
	Create a factory.

NOTE: the function is only enabled if the user has **Factory creation** authorization.A factory can also be created on the target level, ***see "Operation page" on the previous page .***

4	Target list:

Open target

Closed target

5	Selected target data.
6	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*
For more information on operations *see "**What you should know about operations**" on page 22 .*
For more information on factories *see "**What you should know about Factories and Agents**" on page 33 .*
For a description of the data in this window *see "**Operation page data**" below .*
To quickly manage operation data*see "**Wizards in the homepage**" on page 13 .*

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.

Operation page data

Selected target data is described below:

Data	*Description*
Name	Target name.
Description	User's description
Status	Defines the target's status:  Open. If the Technician correctly installs agents, RCS receives the collected evidence.  Closed, it can no longer be opened.

4

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

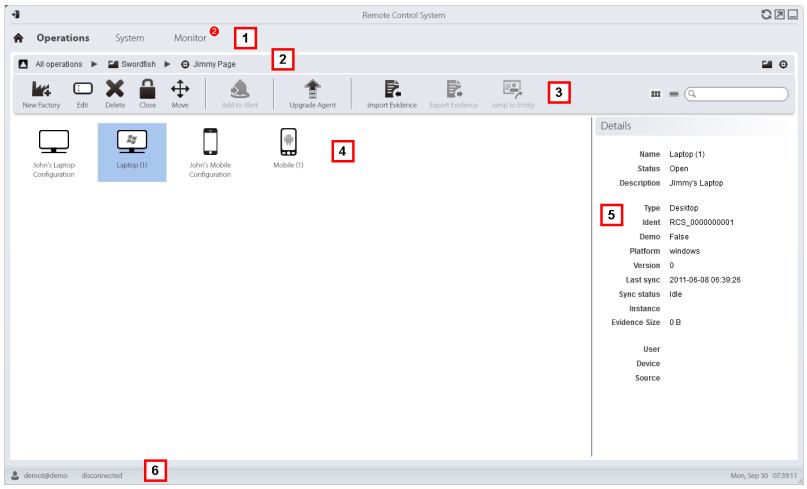
Purpose

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 51*) or advanced configuration (*see "**Advanced factory or agent configuration**" on page 60*
- 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.

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

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

Icon	*Function*
	Create a factory.

NOTE: the function is only enabled if the user has **Factory creation** authorization.
A factory can also be created on the operation level, *see "Operation page" on page 24* .

	Editing a factory or agent
	Deleting a factory or agent
	Closing the agent or factory.
	Moving the factory or agent to a new target.
	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.

IMPORTANT: for Android, root privileges must be obtained to update the agent.*See "What you should know about Android" on page 144 .*

	Import target evidence physically collected on the device.

NOTE: the function is only enabled if the user has **Import evidence** authorization.

Area	Description
4	Icons/list of created factories and installed agents.  : agent in demo mode.  : scout agent awaiting verification.  : soldier agent installed.  : elite agent installed.
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 14* .
For a description of the data in this window *see "**Target page data**" on the facing page* .
For more information on targets *see "**What you should know about Factories and Agents**" on page 33*
To quickly manage target data*see "**Wizards in the homepage**" on page 13* .

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**.

Step	Action
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.

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 type factory in Open status.
	Example of scout agent installed on a desktop Windows device, in Open status.
	Example of soldier agent installed on a desktop Windows device, in Open status.
	Example of elite agent installed on a desktop Windows device, in Open status.
	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.
Level	(agent only) Agent level: scout, soldier, elite.
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.

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**: agent model.
- **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

The *factory* is a model to be used to create agents to be installed. 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 configuration can be saved as a template to load it the next time you create a similar agent.

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).

How to create factories

Factories are templates that can be created on two different operation-target-agent hierarchical levels:

- *on the operation level*: the factory, after installation and first synchronization, automatically creates an agent and target for each device
- *on the target level*: the factory, after installation and first synchronization, automatically creates an agent for that target

The *operation level* mode ensure that collected evidence is assigned separately. In fact, it creates as many agents as there are devices. Later, if two or more devices belong to the same target, the agent can be moved to the right target.

The *target level* mode, if incorrectly used, may create a factory which is used to create several agents.

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 68*

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 129*

For more information on agents *see "**What you should know about agents**" on page 39* .

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 129* .

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 143*

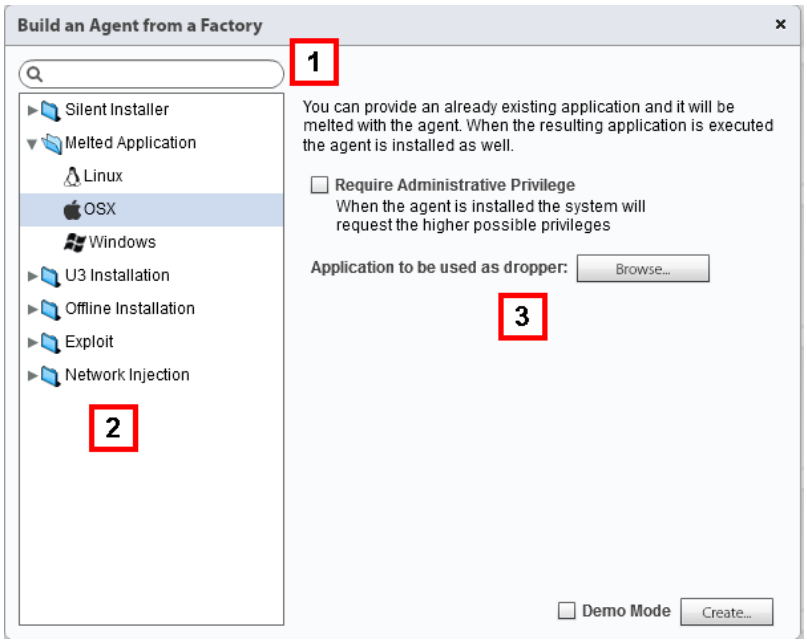
NOTE: the function is only enabled if the user has **Installation vector creation** authorization.

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 14 .*

For more information on factories *see "**What you should know about Factories and Agents**" on page 33 .*

For a detailed description of each installation vector *see "**List of installation vectors**" on page 143*

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.

5

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:

What you should know about agents

Introduction

The agent can be exposed and identified if installed in environments with antivirus or in environments managed by expert technicians.

Three different agent levels were included to prevent this from happening:

- scout
- soldier
- elite

The*scout agent* is a replacement for the agent sent at the beginning of the installation phase to analyze the level of target device security.

The *soldier agent* and *elite agent* are actual agents. The *soldier agent* is installed in environments that are not fully secure and thus only allow some types of evidence to be collected. The *elite agent* is installed in secure environments and can collect all types of available evidence.

Agent installation process

Phase	*Description*
1	The technician installs the scout agent on the target device.
2	The scout agent collects evidence from the device to check the level of security.
3	The Technician updates the agent:

If the environment is...	*Then...*
secure	the system installs the elite agent.
not fully secure	the system installs the soldier agent.
unsecure	the agent cannot be updated.

Agent icon

The agent icon provides the following information:

- level (scout, soldier, elite)
- device type (desktop or mobile)
- operating system where it is installed

Following are the three agent level icons, for example, for a Windows desktop device:

-  : scout
-  : soldier
-  : elite

Scout agent

Once installed, the scout agent appears in the target page after the first synchronization.
The scout agent acquires evidence:

- **Screenshot** type to help identify the target device
- **Device** type to help understand whether the environment to be infected is ok or whether there are applications that could compromise agent integrity.

IMPORTANT: Screenshot type evidence is only collected if the module is enabled in the configuration. If necessary, remember to enable it before sending the agent.

Soldier agent

The soldier agent lets you collect evidence defined by the base configuration modules except for **Call** and **Accessed file** modules.

IMPORTANT: the advanced settings are not enabled for soldier agents.

Tip: once the soldier agent is installed, check the settings defined in the initial phase to make sure they meet investigation needs and agent characteristics.

Elite agent

The elite agent lets you collect all types of evidence using both the base and advanced configuration

Agent synchronization

An agent will perform synchronization only if:

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

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 35*).

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" on page 44* .

Agent page

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

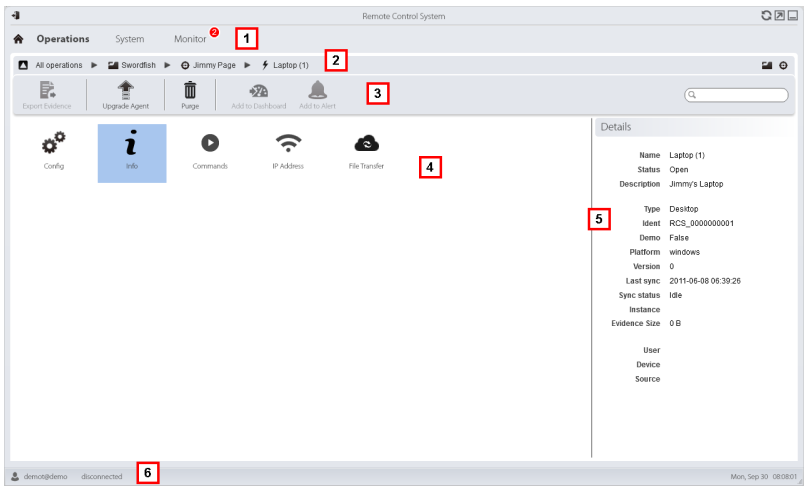
Purpose

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
- replace the scout agent with an actual agent (elite or soldier) and update the 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.

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

Icon	Description
	send the actual agent (elite or soldier) to the scout agent or update the agent software with the last version received from the HackingTeam.  ***CAUTION: the update does not update the configuration that is transmitted to the agent at the next synchronization.***  **IMPORTANT: for Android, root privileges must be obtained to update the agent.*See "What you should know about Android" on page 144 .***
	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.

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

Icon	Description
	Show the agent settings log, allowing the existent settings to be edited and saved as new. *See "Agent configuration log data" on the facing page .*
	Show the agent event log (info). *See "Agent event log data" on the facing page*
	Show the results of commands run on the device using **Execute** actions. *See "Command page" on page 45 .*
	Show the agent synchronization log. *See "Agent synchronization log data" on the facing page .*
	Open the function to upload or download files from the target device. *See "File transfer to/from the target" on page 46*

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

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*
For more information on agents *see "**What you should know about agents**" on page 39 .*

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.
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.

Command page

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

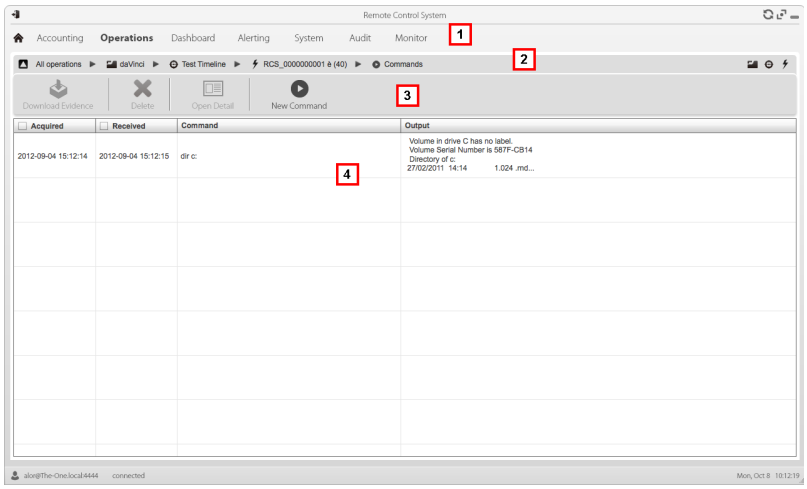
Purpose

This function lets you:

- check the results of commands run with the **Execute** action set on the agent
- check executable file results run during file transfer to/from the agent
- run one or more command on an 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*  Export the selected command to a .txt file.  Show selected command details.  Open a window to enter one or more command strings. All commands are sent to the agent at the next synchronization and the results are displayed at the next receipt.  NOTE: the function is only enabled if the user had **Command execution on agents** authorization.
5	Command list based on set filters.
6	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*

File transfer to/from the target

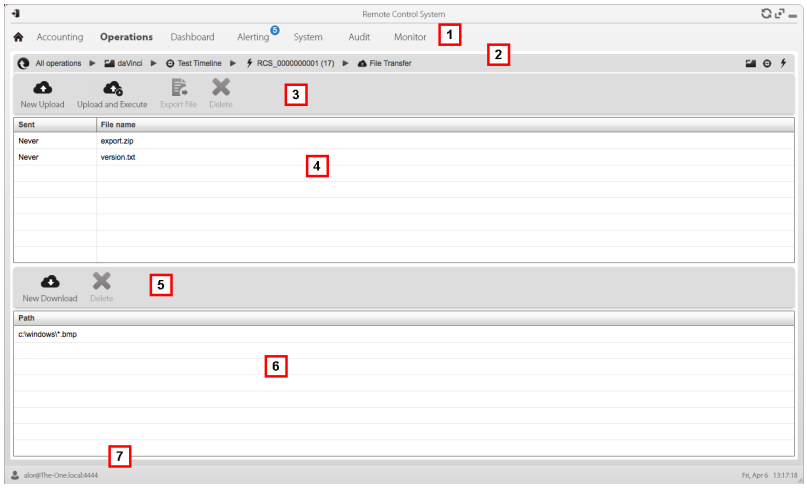
To transfer files to/-from the agent:	• **Operations** section, double-click an operation, double-click a target, double-click an agent, double-click **File Transfer**

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.

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.  NOTE: the function is only enabled if the user had **Upload files to agent** authorization.
	Load an executable file in the device folder where the agent is installed and run it (using **Execute**). Execution results appear in the **Commands** page. *See "Command page" on page 45 .* Each successful upload is logged with the date-time and file name.  **IMPORTANT: this function can be inhibited if the user does not have the relevant permissions or if not permitted by the user license.**
	Export upload log.
	Delete the selected upload Any deleted command results are saved.

4	Upload log, with toolbar.
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 14 .*
For a description of agent data *see "**Agent page**" on page 42 .*

6

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:

What you should know about the 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 available in the basic configuration *see "Basic configuration data" on page 54* .

CAUTION: when returning from advanced configuration to basic configuration, the advanced configuration will be lost and the default basic configuration will be restored.

Exporting and importing configuration settings

Base or advanced configuration settings are exported/imported to reuse the settings on other RCS systems.

The base or advanced configuration settings are exported in a .json file that can be transferred to another system and imported when creating an agent.

Saving the configuration settings as a template

Base or advanced configurations settings are saved as a template to have other users on the same RCS system reuse the configuration.

The base or advanced configuration settings are saved as a template in the database, accompanied by a description and the name of the user. When creating another target, another user can load it and thus it becomes the configuration for that agent.

IMPORTANT: base and advanced configuration templates are saved separately in the database. Base configuration templates thus appear when creating an agent with a base configuration, advanced configuration templates appear when creating an agent with an advanced configuration.

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 35* .
- open the advanced configuration function (*see "**Advanced factory or agent configuration**" on page 60*)

NOTE: the function is only enabled if the user has **Agent configuration** authorization.

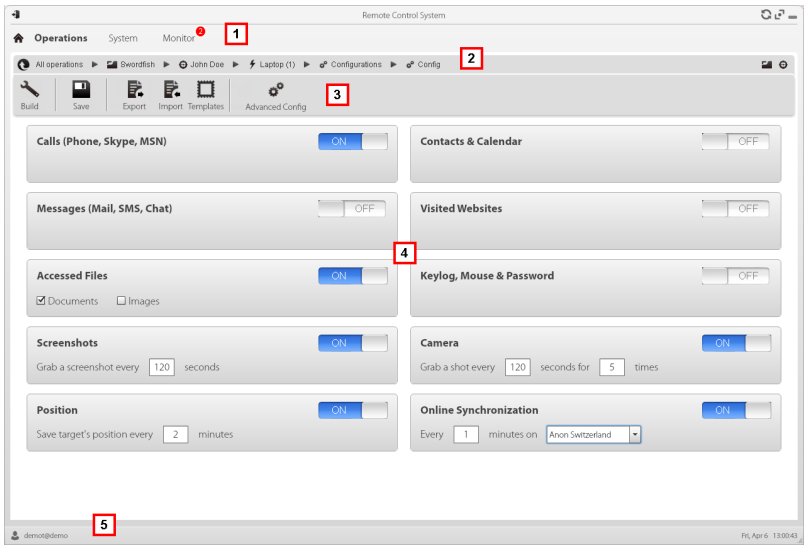
Next steps

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

Area	Description
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 35*
	Save the configuration: the agent configuration is logged and sent to the agent at the next synchronization. *See "**Agent configuration log data**" on page 44*
	Export the configuration to a .json file.
	Import the configuration from a .json file.
	Load the basic configuration template or save the current configuration as a template. *See "**What you should know about the basic configuration**" on page 51 .*
	Open the advanced configuration window. *See "**Advanced factory or agent configuration**" on page 60 .*  *CAUTION: when returning from advanced configuration to basic configuration, the advanced configuration will be lost and the basic configuration will be restored.*

4	List of collectable evidence and relevant activation status.  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 14 .*

For more information on the basic configuration*see "**What you should know about the basic configuration**" on page 51 .*

For a description of the data in this window *see "**Basic configuration data**" on the facing page .*

For the list of modules available in the two configurations *see "Module list" on page 129*

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 35* .
an agent	agent settings are automatically updated at the next synchronization.

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. NOTE: not available for the soldier level agent.
Messages	Record messages.
Accessed files	(desktop only) Record documents or images opened by the target. **Document, Images**: file types. NOTE: not available for the soldier level agent.

Recording	*Description*
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.

7

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:

What you should know about advanced configuration

Advanced configuration

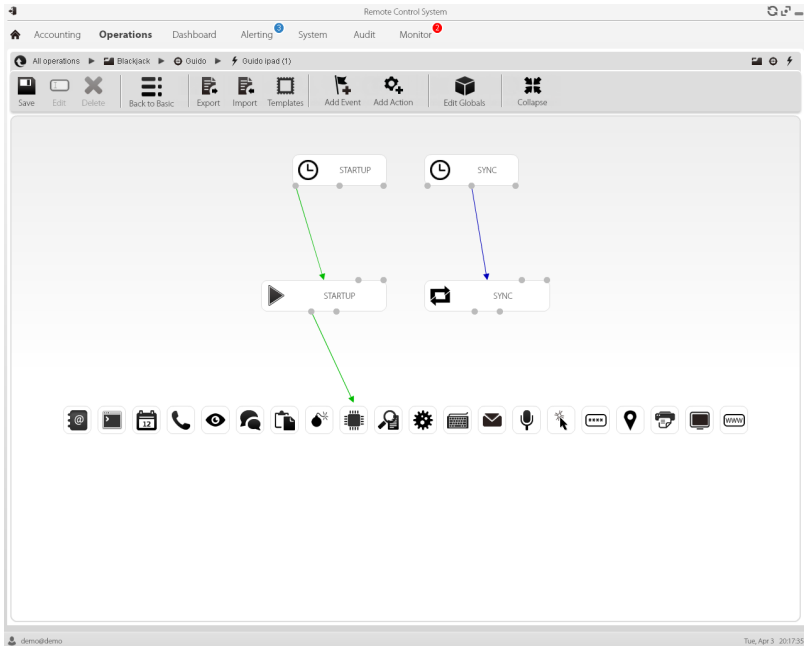
Advanced factory/agent configuration lets you create complex activation sequences using a simple graphic interface.

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 120 .*

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 114*

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 129* .

Exporting and importing configuration settings

Base or advanced configuration settings are exported/imported to reuse the settings on other RCS systems.

The base or advanced configuration settings are exported in a .json file that can be transferred to another system and imported when creating an agent.

Saving the configuration settings as a template

Base or advanced configurations settings are saved as a template to have other users on the same RCS system reuse the configuration.

The base or advanced configuration settings are saved as a template in the database, accompanied by a description and the name of the user. When creating another target, another user can load it and thus it becomes the configuration for that agent.

IMPORTANT: base and advanced configuration templates are saved separately in the database. Base configuration templates thus appear when creating an agent with a base configuration, advanced configuration templates appear when creating an agent with an advanced configuration.

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.

NOTE: the function is only enabled if the user has **Agent configuration** authorization.

NOTE: the advanced configuration is not available for the soldier level agent.

CAUTION: when returning from advanced configuration to basic configuration, the advanced configuration will be lost and the default basic configuration will be restored.

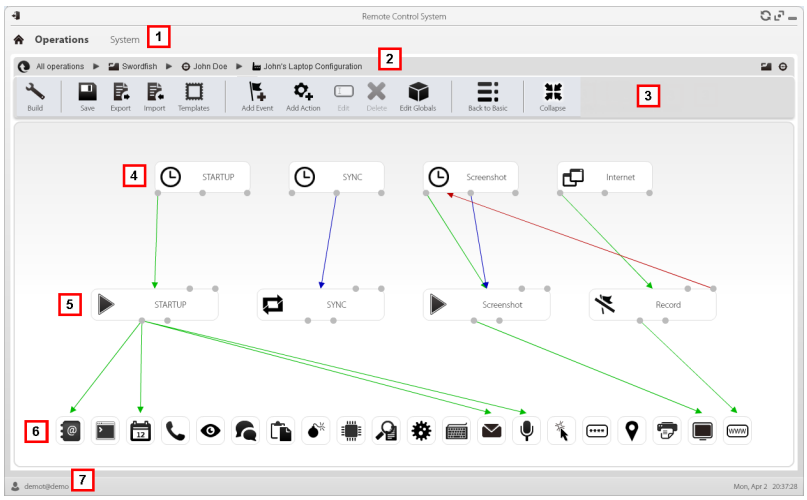
Next steps

For a factory, after completing its configuration, compile it to obtain the agent to be installed.*See "Compiling a factory" on page 35*

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

Area	*Description*
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 35*
	Save the current configuration.
	Export the configuration to a .json file.
	Import the configuration from a .json file.
	Load the advanced configuration template or save the current configuration as a template. *See "**What you should know about advanced configuration**" on page 57 .*
	Add an event.
	Add an action.
	Edit the selected event or action.
	Delete the selected event, action or logical connection.
	Edit global agent data *see "**Global agent data**" on page 64 .*
 	***CAUTION: all settings are lost when you return to the basic configuration.***
 	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.

Area	Description
7	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*
For more information on the advanced configuration*see "**What you should know about advanced configuration**" on page 57 .*

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 120* • 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 129 .*
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 120* • Click **Save**: the new event is added to the work area
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 114* .
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
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 129* .  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.
5	Click **Save**: the configuration is ready to be compiled (if factory) or transmitted to the device at the next synchronization (if agent).

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.

Field	*Description*
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.

8

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:

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.

Network Injector types

There are two Network Injector types:

- Appliance: network server for installation in an intra-switch segment at an Internet service provider.
- Tactical: laptop for tactical installation on LAN or WiFi networks

Both Network Injectors let you automatically identify the target devices and infect them according to the set rules via their control software (Appliance Control Center or Tactical Control Center). Tactical Network Injectors also allow for manual identification.*See "**What you should know about Appliance Control Center**" on page 76 ,"**What you should know about Tactical Control Center**" on page 76*

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. Or let the Tactical Network Injector operator select the device.
2. define the way to infect the target. For example, by replacing a file the target is downloading from the web or by infecting a website the target usually visits.

Automatic or manual identification rules

If information is already known on target devices, 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.

If no information is known on target devices, use Tactical Network Injector which allows operators to observe the target, identify the device used and infect it since on the field.

For this type of manual control specify **TACTICAL** in the **User patterns** field in the injection rule.

What happens when a rule is enabled/disabled

Enabling a rule means making it available to the Network Injector injection process. RCS routinely communicates with Network Injector to send rules and acquire logs. The operator is in charge of enabling this synchronization for Tactical Network Injector.

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

Starting the infection

After Network Injector receives the infection rules, it is ready to start an attack.

During the sniffing phase, it checks whether any of the devices in the network meets the identification rules. If so, it sends the agent to the identified device and infects it.

Managing the Network Injector

To manage Network Injectors:	• **System** section, **Network Injector**

Purpose

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

NOTE: the function is only enabled if the user has **Injector rules management** authorization.

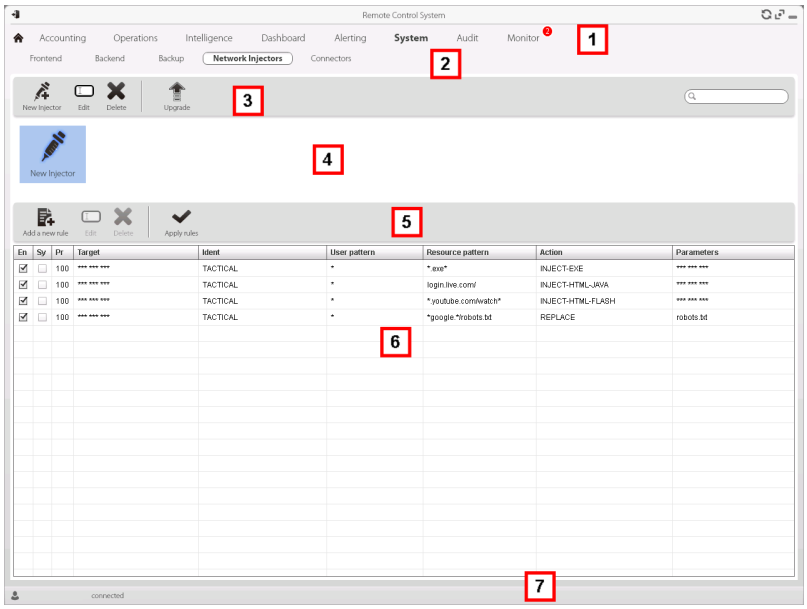
What you can do

With this function you can:

- create an agent injection rule on a target
- send the rules to Network Injector

What the function looks like

This is what the page looks like:



Area	*Description*
1	RCS menu.
2	**System** menu.
3	Network Injector toolbar.
4	Network Injector list.
5	Injection rule toolbar.

NOTE: the functions are only enabled if the user has **Injector rules management** authorization.

Descriptions are provided below:

Action	*Description*
	Add a new rule.
	Open the window with rule data.
	Delete the selected rule.
	Send rules to the selected Network Injector. Appliance automatically updates at the next synchronization provided an infection process is running. While the operator must select whether the rules should be updated with Tactical.

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 14* .

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

For further information on injection rules *see "**What you should know about Network Injector and its rules**" on page 67* .

Adding a new injection rule

To add a new rule:

Step	Action
1	Select the Network Injector for the new rule: rule commands and table appear.
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 next page* . • Click **Save**: the new rule appears in the main work area.

Send the rules to Network Injector

To send the rules to Network Injector:

Step	Action
1	Enable the rule to be sent to Network Injector by selecting the **En** control box in the table.
2	Click **Apply rules**: RCS receives the request to send the rules to the selected Network Injector . The progress bar in the download area shows operation progress. **NOTE: Network Injector only receives the updated rules when is synchronizes with the RCS server. *See "Checking Network Injector status " on page 75***

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.
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 selected, we recommend you use the **Disable on sync** option.
Target	Name of the target to be infected.

Data	*Description*
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.
TACTICAL	The target is not automatically identified but can be identified by the operator on Tactical Network Injector. Only after the device is identified by the operator is the **Ident** field customized with the data received from the device.

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

Method	*Format*
DHCP	Corresponding address (i.e.: "195.162.21.2").
STATIC-IP	
STATIC-MAC	
STATIC-RANGE	Address range separated by '-' (i.e.: "195.162.21.2-195.162.21.5".
STRING-CLIENT	Text string (i.e.: "John@gmail.com").
STRING-SERVER	
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.*").
TACTICAL	A value cannot be set. The correct value will be set by the field operator.

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.

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-FILE	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-HTML-FLASH	Preset for Youtube and read-only by the user.
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	*Function*
INJECT-EXE	Infects the downloaded EXE file in real time. The agent is installed when the target runs the EXE file.
INJECT-HTML-FILE	Lets you add the HTML code provided in the file in the visited web page. Please contact HackingTeam technicians for further details.
INJECT-HTML-FLASH	Blocks videos on youtube and requires the user to install a fake Flash update to view them. The agent is installed when the target installs the update.
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.

Factory	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**.

Checking Network Injector status

Introduction

Network Injector synchronizes with the RCS server to download updated control software versions, identification and injection rules and send their logs.

Network Injector status can be monitored from RCS Console.

Specifically:

- in the **Monitor** section: to identify when Network Injector is synchronized and thus available for data exchanges.

Identifying when Network Injector is synchronized

The procedure is described below:

Step	*Action*
1	In the **Monitor** section, select the Network Injector object row to be analyzed. Check the **Status** column: if flagged green, the Network Injector is synchronized. This situation occurs when on Control Center software (Appliance or Tactical): • **Config** was clicked, the operator manually queued for new rules or updates; • **Start** was clicked or an infection is in progress. **IMPORTANT: applied rules and updates can only be received from RCS when Network Injector is synchronized.**

What you should know about Appliance Control Center

Introduction

Appliance Control Center is an application installed on Network Injector Appliance.

Synchronization with RCS server

Appliance Control Center synchronizes with RCS to receive the updated infection rules and to check whether a new version of Appliance Control Center is available and send logs.

Synchronization can occur in two ways:

- manually, at least the first time, to receive injection rules, using the Appliance Control Center Network Injector function.
- automatically with an infection in progress.

During synchronization, RCS communicates with Network Injector Appliance at set intervals of time (about 30 sec.).

Injection interface IP address

For infection to be successful, the infection interface must have a public address, otherwise the target will never be able to see it.

In an initial phase you can use the preset address on the interface with Appliance Control Center (with **Public IP**= "auto"), wait for a message that indicates that the address is private and, in that case, set a public address to re-route the private address (**Public IP** = "xxx.xxx.xxx.xxx").

Sniffing, on the other hand, can be run via the network interface with a private IP address.

What you should know about Tactical Control Center

Introduction

Tactical Control Center is an application installed on a notebook, called Tactical Network Injector.

It can connect to a protected WiFi network, infect devices thanks to RCS identification and injection rules or infect manually identified devices.

The identification and infection rules are the same as those used for Network Injector Appliance, with the sole difference that Tactical Network Injector provides an additional "manual" identification rule. Thus the operator identifies the device to be infected and applies the injection rules to that device.

Tactical Control Center operations

With Tactical Control Center you can:

- Enable synchronization with RCS to receive updated identification and injection rules and send logs.
- Update Tactical Control Center, essentially to update agents on devices.
- Automatically identify devices in a wired or WiFi network and infect them according to the RCS identification and injection rules.
- Manually identify devices in a wired or WiFi network and infect them according to the RCS injection rules. The operator is in charge of identification.
- Connect to a protected WiFi network to obtain its password.
- Emulate a WiFi network Access Point normally used by the target.

NOTE: the injection network can be external or an open WiFi network simulated by the Tactical Control Center.

Synchronization with RCS server

Tactical Control Center synchronizes with RCS to receive the updated infection rules and to check whether a new version of Tactical Control Center is available and send logs.

Synchronization can occur in two ways:

- manually, the first time to receive injection rules.
- automatically with an infection in progress.

Updating infection rules

If traffic generated by the target cannot be infected with the current rules, request operator assistance on RCS Console to generate new rules and update Network Injector. Receive the new rules the next time Tactical Control Center is synchronized to view them.

Using network interfaces

Two different network interfaces are available during an attack, one for sniffing and one for injection. Using two separate interfaces is indicated to guarantee continuity, especially for sniffing.

Only the sniffing interface is used when emulating the Access Point and acquiring network passwords.

Sniffing interfaces can be internal or external: external interfaces are indicated for sniffing because transmission speed is higher.

Infection via automatic identification

The steps needed to infect devices automatically identified by RCS rules are described below. The attack can be run on wired or WiFi networks:

Phase	*Description*	*Where*
1	Prepare identification and injection rules for known targets to be attacked. Send the rules to Tactical Network Injector.	*RCS Console, System, Network Injector*
2	Enable synchronization with RCS to receive updated rules.	*Tactical Network Injector, Network Injector*
3	If target devices are connected to a protected WiFi network, acquire the password.	*Tactical Network Injector, Wireless Intruder*
4	The system sniffs, traffic, identifies target devices thanks to identification rules and infects them thanks to injection rules.	*Tactical Network Injector, Network Injector*
5	If necessary, force re-authentication on devices not identified by the rules.	

Infection via manual identification

Following are the steps required to infect manually identified devices. The operator's goal is to identify target devices.

The attack can be run on wired or WiFi networks:

Phase	*Description*	*Where*
1	Prepare identification rules that include manual identification and injection rules for all the target devices to be attacked. Send the rules to Tactical Network Injector.	*RCS Console, System, Network Injector*
2	Enable synchronization with RCS to receive updated rules.	*Tactical Network Injector, Network Injector*
3	If target devices are connected to a protected WiFi network, acquire the password.	*Tactical Network Injector, Wireless Intruder*

Phase	*Description*	*Where*
4	If target devices can connect to an open WiFi network, try emulating an Access Point known by the target.	*Tactical Network Injector,Fake Access Point*
5	The system proposes all devices connected to the selected network interface. Use filters to search for target devices or check the web chronology for each device.	*Tactical Network Injector, Network Injector*
6	Select devices and infect them.	

Enable synchronization with RCS

Tactical Control Center receives the updated software and identification and injection rules from RCS and sends logs.

In this communication, RCS will attempt to communicate with Tactical Network Injector at set intervals (about 30 sec.). In Tactical Control Center, decide when to enable synchronization using the **Network Injector** function.

Protected WiFi network password acquisition

If the target device is connected to a protected WiFi network, the access password must be obtained to login.

The **Wireless intruder** function lets you connect to a WiFi network and crack the password. For WPA and WPA 2 protected networks, an additional dictionary can be loaded in addition to the standard dictionary. The password is displayed and the operator can copy it to use it with the sniffing and injection function (**Network Injector** function).

Infection via automatic identification

This work mode is suited for situations when some target device information is known (i.e.: IP address).

In this case, RCS injection rules include all the data required to automatically identify target devices.

Starting automatic identification using the **Network Injector** function gradually displays target devices that are immediately infected by the injection rules.

Forcing unknown device authentication

You may not be able to connect to some devices in a password protected WiFi network. These types of devices appear in the list as unknown.

In this case, their authentication can be forced: the device will disconnect from the network, reconnect and be identified.

Infection via manual identification

Manual identification can be indicated in RCS identification rules. This procedure is frequently run when there is no information on the device to be infected and it must be identified on the field.

In this case, a series of functions to select devices connected to the network is available to the operator:

- filters can be set on tapped traffic: only devices that meet this criteria are infected.
- each device chronology can be checked to decide which device should be infected.

Once target devices are identified, simply select them to start infection; the identification rules are "customized" with the device data to allow injection rules to be applied.

NOTE: devices that were already infected via automatic identification can be manually infected.

Setting filters on tapped traffic

When manually identifying targets, some targets may not be identified among those connected to the network. In this case, use the **Network Injector** function to set filters on tapped traffic.

Tactical Control Center provides to types of filters:

- regular expressions
- Network BPF (Berkeley Packet Filter)

Filter with regular expression

Regular expressions are broad filters. For example, if our target is visiting a Facebook page and talking about windsurf, simply enter "facebook" or "windsurf".

Tactical Network Injector taps all traffic data and searches for the entered words.

For further information on all admitted regular expressions, see https://en.wikipedia.org/wiki/Regular_expression .

BPF (Berkeley Packet Filter) network filter

This is used to more accurately filter devices using BPF syntax (Berkeley Packet Filter). This syntax includes key words accompanied by qualifiers:

- *type qualifiers* (i.e.: **host**, **net**, **port**), indicate the type of object searched for
- *direction qualifiers* (i.e.: **src**, **dst**) indicate the direction of the data searched for
- *protocol qualifiers* (i.e.: **ether**, **wlan**, **ip**) indicate the protocol used by the object searched for

For example, if our target is visiting a Facebook page, enter "**host** facebook.com"

For further details on syntax qualifiers, see http://wiki.wireshark.org/CaptureFilters.

Identifying a target by analyzing the chronology

Another way to filter and shorten the list of possible targets is to analyze device web traffic to identify it as the target.

Emulating an Access Point known by the target

In certain scenarios target devices must be attracted to tap their data, indentify and infect them.

To do this, Tactical Network Injector emulates an Access Point already known to the target device.

This way, if the device is enabled to automatically connect to available WiFi networks, it automatically connects to the Access Point emulated by Tactical Network Injector as soon as it enters the WiFi area. .

What you should know about identifying the WiFi network password

Introduction

Tactical Control Center includes three types of attacks to identify protected WiFi network passwords (**Wireless Intruder**):

- WPA/WPA2 dictionary attack
- WEP bruteforce attack
- WPS PIN bruteforce attack

WPA/WPA2 dictionary attack

To run this attack, the system identifies handshakes between the client and the access point and tries to discover the password using a dictionary of common words.

The handshake is saved in folder/opt/td-config/run/besside/wpa.cap. If necessary, you can copy the handshake and try the attack with another more powerful machine.

Once the system identifies the handshake, the attack can continue without remaining near the WiFi network.

The attack may take a long time, proportionate to the size of the dictionary. The attack fails if the password is not found in the dictionary of common words.

WEP bruteforce attack

To run this attack, the system makes an injection simulating one of the clients connected to the network and collects data to force the encrypted password. A least one client must be connected to the network.

The attack lasts from 10 to 15 minutes and the notebook must remain in the WiFi network coverage range the entire time.

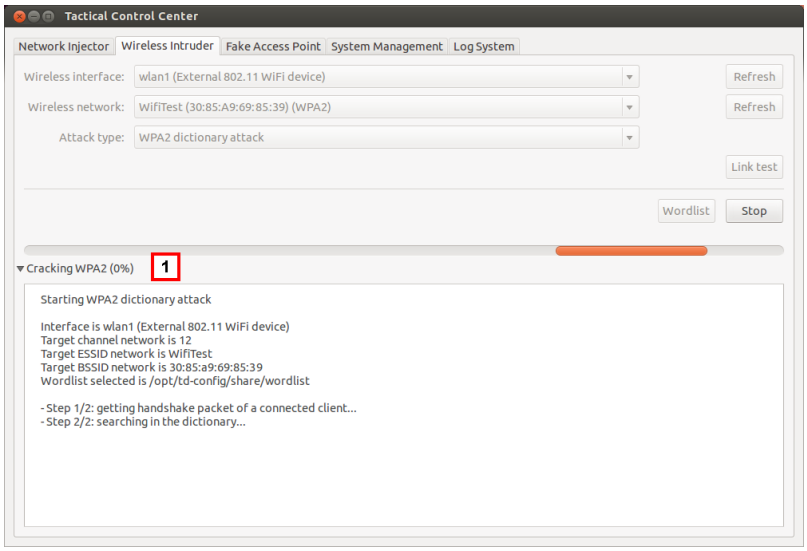
WPS PIN bruteforce attack

To run this attack, the system tries all the possible combinations to recover access point settings via a WiFi Protected Setup protocol.

The attack may take a long time and the notebook must remain in the WiFi network coverage range the entire time.

Attack progress

The percent attack progress **[1]** (WPA/WPA2 and WPS) or captured Initialization Vectors (WEP) can be seen in the **Tactical Control Center Wireless Intruder** tab.

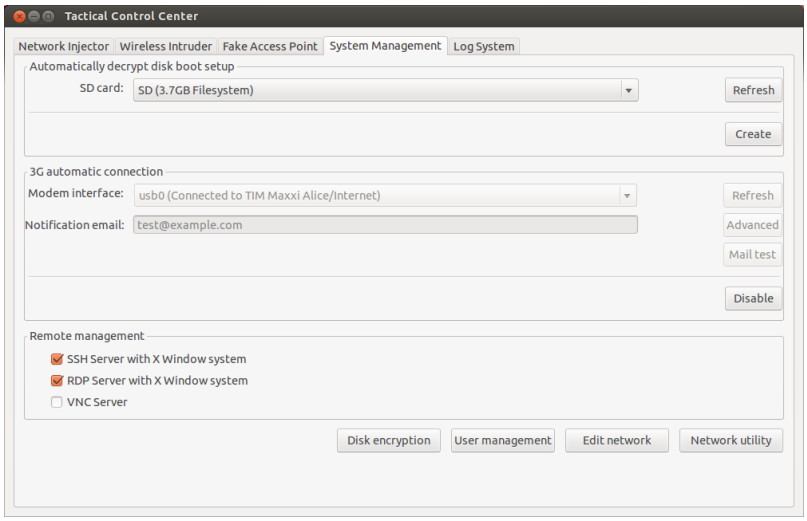


What you should know about Control Center remote access

Introduction

You can access Tactical Control Center and Appliance Control Center from remote. The applications' **System Management** tab lets you set this option.

For example, this is what the Tactical Control Center tab looks like.



Specifically, the following are required for remote access:

- Encrypted disk password (Tactical Control Center only)
- 3G Modem for the connection
- Device IP address
- Network protocol

Disk password (Tactical Control Center only)

The Tactical Network Injector notebook has an encrypted disk and the disk password is required whenever it is turned on. To avoid manually entering the password, you can save it on an SD memory card and leave the card in (preferable in the SD slot built into the notebook).

NOTE: the password is not the system password. Thus, the SD card does not contain information that can used by third parties to access the operating system.

To change the password, simply generate a new one.

3G Modem for the connection

The 3G modem set in **Modem Interface** is used to connect the device to the network.

If the system disconnects or reboots with the modem enabled, the connection is automatically re-established.

Tip: for higher security, use the 3G modem built into the notebook rather than an external modem.

Device IP address

If set, the system sends an email to the address specified in **Notification email** with the device IP address each time it connects.

If the IP address is dynamic, wait until an email is sent with the address to be used for the connection.
If the IP address is static, you can set whether the email is sent to be informed when the device is connected.

Email send mode with IP address

To send the email, you can either use the automatic settings that uses the device mail server or manually specify a mail server.
If automatic settings are used, the sender's email address is `root@hostname.local`, where `hostname` is the device host. Otherwise, it will be the one specified.
To check whether communications are correctly established, send a test email.

Network protocol

Communications are via the network protocol specified in the **Remote Management** section.

Tactical Control Center and Appliance Control Center commands

Introduction

Some terminal commands are available to manage Tactical Control Center and Appliance Control Center applications.

NOTE: Administrator privileges are required to run commands.

Commands

Commands available for Tactical Control Center and Appliance Control Center are described below:

Tactical Control Center command	*Appliance Control Center command*	*Function*
`tactical`	`appliance`	Starts the application.
`tactical -d` or `tactical --desync`	`appliance -d` or `appliance --desync`	Disconnects the system from the currently synchronized RCS server.
`tactical -l` or `tactical --log`	`appliance -l` or `appliance --log`	Displays current infection process logs. NOTE: the application window must be open.

Tactical Control Center command	*Appliance Control Center command*	*Function*
`tactical -s` or `tactical --show-logs`	`appliance -s` or `appliance --show-logs`	Displays all log files saved in file system.
`tactical - r` or `tactical --report`	`appliance - r` or `appliance --report`	Creates a system report and saves it in the user's Home folder.
`tactical - v` or `Tactical --version`	`appliance - v` or `appliance --version`	Displays the application version.
`tactical -h` or `tactical --help`	`appliance -h` or `appliance --help`	Displays available commands.

Appliance Control Center

Purpose

Appliance Control Center lets devices be infected:

- **automatically**, by applying the identification rules based on known device information (i.e.: IP address)

What you can do

With Appliance Control Center you can:

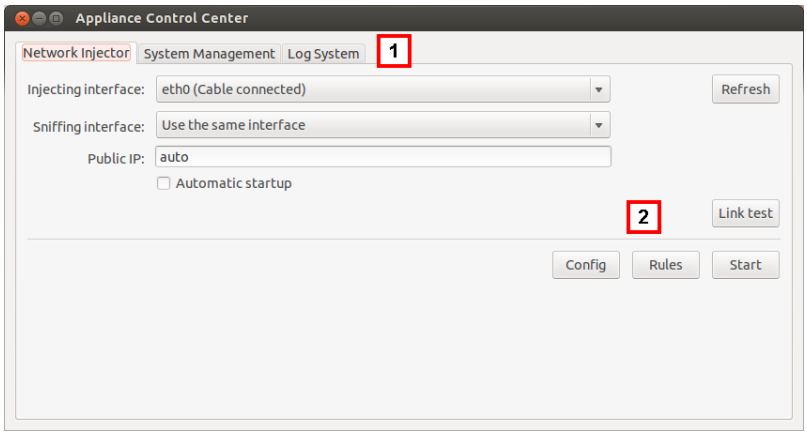
- Enable synchronization with RCS server to receive updated identification and injection rules and send logs.
- Update Appliance Control Center, essentially to update agents on devices.
- Automatically identify connected devices and infect them through identification and injection rules.
- Setting remote application access.

Password request

When Appliance Control Center opens, a password must be entered, the same as the notebook on which it's running.

What the function looks like

This is what the page looks like:



Area	*Description*
1	Single application access tabs. Descriptions are provided below:

Function	*Description*
Network Injector	It manages target device sniffing and infection, synchronizes RCS rules and updates Appliance devices.
System Management	Setting remote application access.
Log System	Lists logs in real time.

2	Area with the buttons to reload the device list, start network connections, enable synchronization, enable automatic reboot after boot and enable Network Appliance update.

To learn more

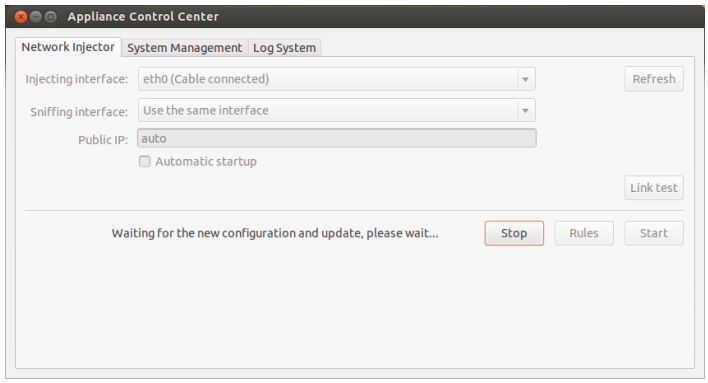
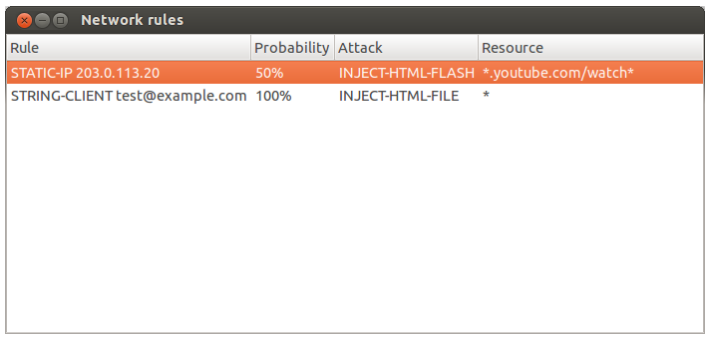
To learn more about Appliance Control Center *see "What you should know about Appliance Control Center" on page 76* .

For a description of Appliance Control Center data *see "Appliance Control Center data" on page 90*

Enabling synchronization with RCS server to receive new rules

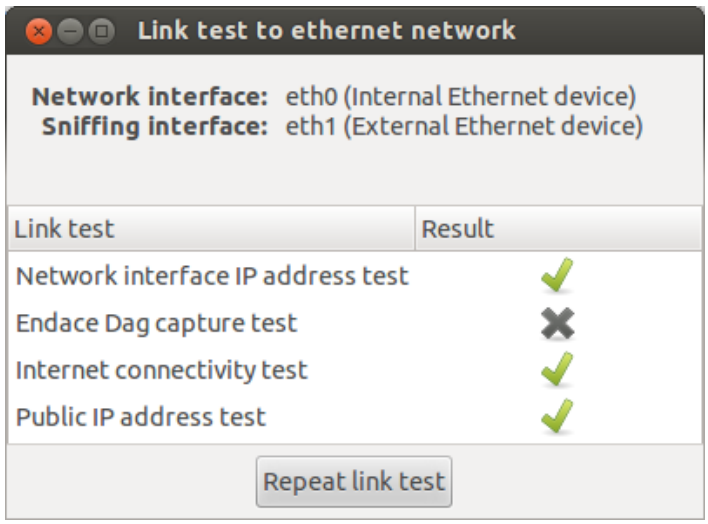
Following is the procedure on how to enable synchronization with RCS server to receive updated rules:

NOTE: if an infection is in progress, Network Injector is already synchronized with RCS server and thus rules are automatically uploaded; skip to step 4.*See "Checking Network Injector status " on page 75*

Steps	***Result***
1. In the **Network Injector** tab, click **Config**: synchronization is enabled.	
2. During synchronization, RCS queries Network Injector every 30 seconds. Sent injection rules will be received at the end of the first interval. IMPORTANT: updates are only received if sent from RCS Console.*See "Managing the Network Injector" on page 68* IMPORTANT: routinely enable synchronization to guarantee constant operating center updates and infection success.	
3. To stop synchronization, click **Stop**.	
4. To view the rules received from RCS Console click **Rules**: all rules for Network Injector appear IMPORTANT: make sure rule synchronization is successful after requesting updated from RCS Console.	

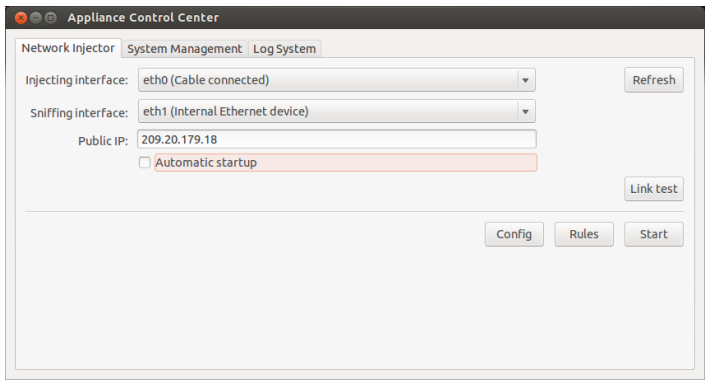
Running a network test

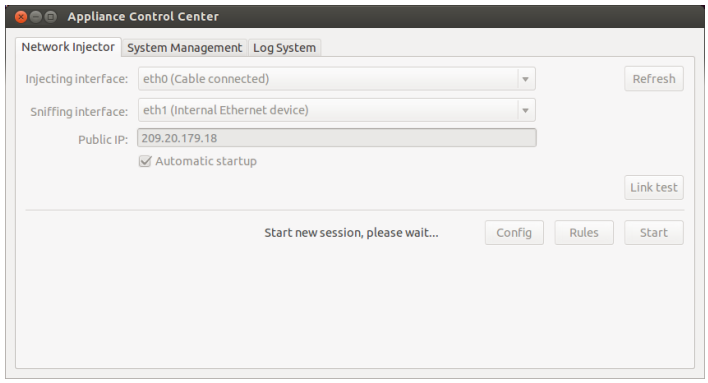
The network test procedure for sniffing and/or injection is provided below:

Steps	*Result*
1. In the **Network Injector** tab, select the network interface. 2. Click **Link test**: a window appears where test results are displayed. 3. If the test fails, review the required network settings and repeat the test. IMPORTANT: attack will not be successful if the test fails.	

Infecting targets using automatic identification

To start automatic identification and infection:

Steps	*Result*
1. In the **Network Injector** tab, select the network interface for injection in the **Injecting Interface** list box. 2. In the **Sniffing interface** list box, select a different network interface to be used for sniffing or select the same interface used for injection. Tip: use two different interfaces to guarantee better device identification. NOTE: Endace interfaces (DAG), meaning sniffing interfaces, appear in **Sniffing Interface**.	

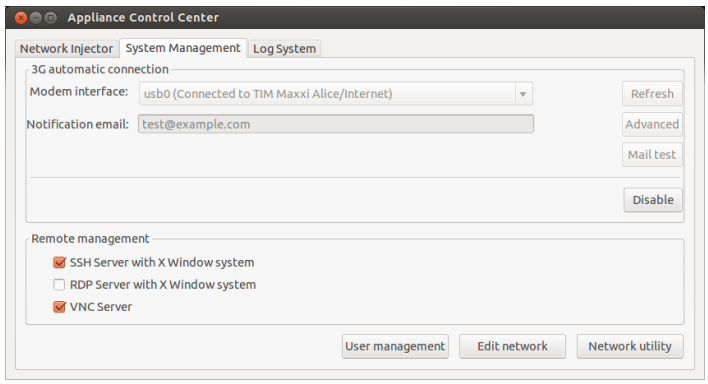
Steps	*Result*
3. Click on **Automatic Startup** to automatically restart the infection without any human intervention even after Appliance Network Injector reboot or shutdown. 4. Click **Start**. IMPORTANT: Appliance Control Center lets you set up, start an infection and close Appliance Control Center leaving the infection running. The next time it is opened with the infection running, the **Stop** button will appear instead of the **Start** button. This lets you re-configure and start a new infection. 5. To stop infection, click **Stop.** or close the window to leave the infection running. Tip: close the window to allow the system to automatically run any Appliance Control Center updates.	 -

Setting remote application access

To remotely access Appliance Control Center:

Steps	*Result*

1. Connect the modem to the device.
2. In the **System Management** tab click **Refresh**: the system recognizes the model and displays it in **Modem Interface**.
3. If several modems are installed, select the required modem from the **Modem Interface** list box.
4. To enable email delivery with the device IP address at each connection, follow the steps below:
   a. In **Notification email** enter the email address where the email will be sent.
   b. Click **Mail test** to send a test email
   c. If the email is not received, click **Advanced** to manually set the mail server: the **Email advanced configuration** window appears.
   d. Enter the required data and click **Save.**
   e. Click **Mail test** to send a test email with the set server.



5. To enable automatic connection with the selected modem, click **Enable**
6. Select the network protocol to be used for remote access.

NOTE: you can directly open some helpful operating system windows using the buttons at the bottom of the screen.

Viewing infection details

To view data recorded in the current session, select the **Log System** tab.

NOTE: all log files are saved in the file system in /var/log/td-config .

Appliance Control Center data

Network Injector data tab

Data is described below:

Data	*Description*
Injecting interface	List of connected network interfaces. Select the injection interface connected to the network on which the device to be attacked is connected.
Sniffing interface	Like **Injecting Interface** or another network interface to only be used for sniffing. NOTE: If the system includes an Endace DAG card for Gigabit connections, the card will be detected and displayed in this list.
Public IP	Lets you specify a public IP address to be mapped on the injection interface private IP address. If "auto" is entered, the system uses default IP address on the injection interface and send a message indicating that it is a private IP address.
Automatic Startup	It automatically restarts the infection without any human intervention even following Appliance Network Injector reboot or shutdown. IMPORTANT: If this option is not selected, infection will not be automatically started.

System Management data tab

Data is described below:

Data	*Description*
Modem interface	3G Modem for device connection.
Notification email	Email address where the device IP is sent whenever it connects to the network. IMPORTANT: mandatory field for dynamic IP addresses.
Remote management	Remote access network protocol.

Tactical Control Center

Purpose

Tactical Control Center lets you identify and infest devices:

- **automatically**, by applying the identification rules based on known device information (i.e.: IP address)
- **manually**, through a series of attempts to identify the target device and infect it.

The identification method should be agreed with the operating center.

What you can do

With Tactical Control Center you can:

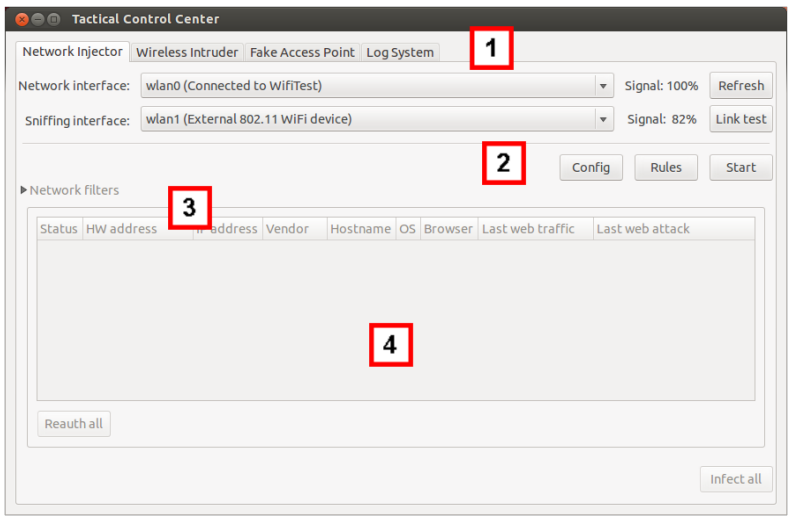
- Enable synchronization with RCS to receive updated identification and injection rules and send logs.
- Updating Tactical Control Center
- Connect to a protected WiFi network to obtain its password.
- Apply device identification rules and infect them
- Force new authentication on devices not identified upon the first attempt
- Select devices based on filters or chronological information
- Emulate an Access Point to attract target devices
- Setting remote application access.

Password request

When Tactical Control Center opens, a password must be entered, the same as the notebook on which it's running.

What the function looks like

This is what the page looks like:



Area	*Description*
1	Single application access tabs. Descriptions are provided below:

Function	*Description*
Network Injector	It manages target device sniffing and infection, synchronizes RCS rules, updates Tactical devices and displays current Tactical Network Injector rules.
Wireless Intruder	Enters a protected WiFi network by identifying the password.
Fake Access Point	Emulates an Access Point.
System Management	Setting remote application access.
Log System	Lists logs in real time.

2 Area with buttons to reload the device list, start network connections and enable synchronization

3 Filters to filter internet traffic on devices.

4 Device list area.

To learn more

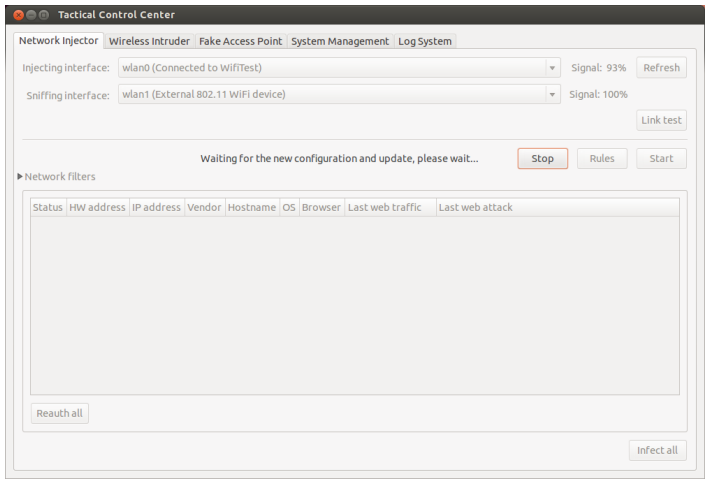
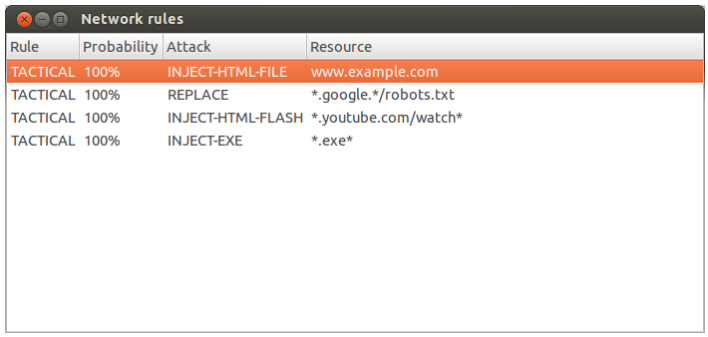
For a description of Tactical Control Center data *see "Tactical Control Center data" on page 105* .

To learn more about Tactical Control Center *see "What you should know about Tactical Control Center" on page 76* .

Enabling synchronization with RCS server to receive new rules

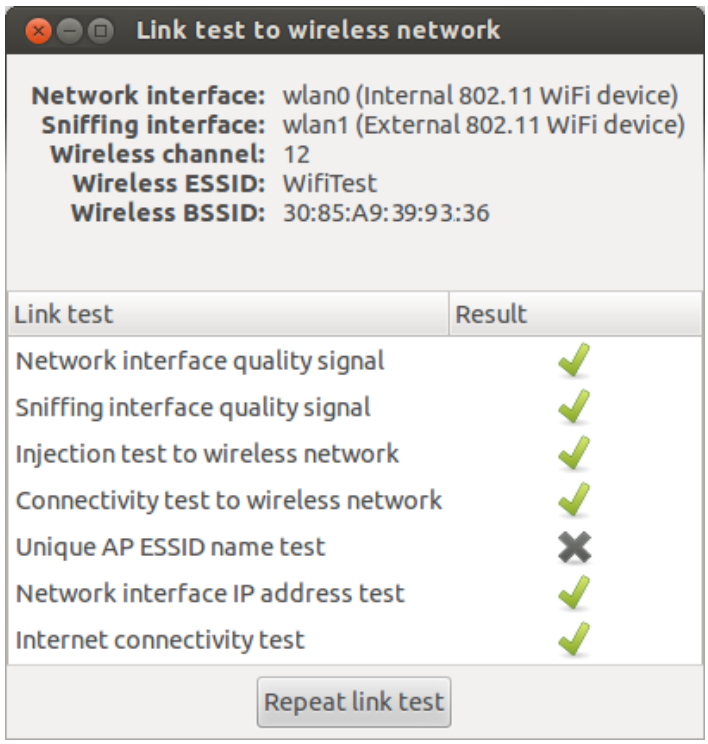
Following is the procedure on how to enable synchronization with RCS to receive updated rules:

NOTE: if an infection is in progress, Network Injector is already synchronized with RCS server and thus rules are automatically uploaded; skip to step 4.*See "Checking Network Injector status " on page 75*

Steps	*Result*
1. In the **Network Injector** tab, click **Config**: synchronization is enabled. 2. During synchronization, RCS queries Network Injector every 30 seconds. Sent injection rules will be received at the end of the first interval. IMPORTANT: updates are only received if sent from RCS Console.*See "**Managing the Network Injector**" on page 68* IMPORTANT: routinely enable synchronization to guarantee constant operating center updates and infection success.	
3. To stop synchronization, click **Stop**. 4. To view the rules received from RCS Console click **Rules**: all rules for Network Injector appear IMPORTANT: make sure rule synchronization is successful after requesting updated from RCS Console.	

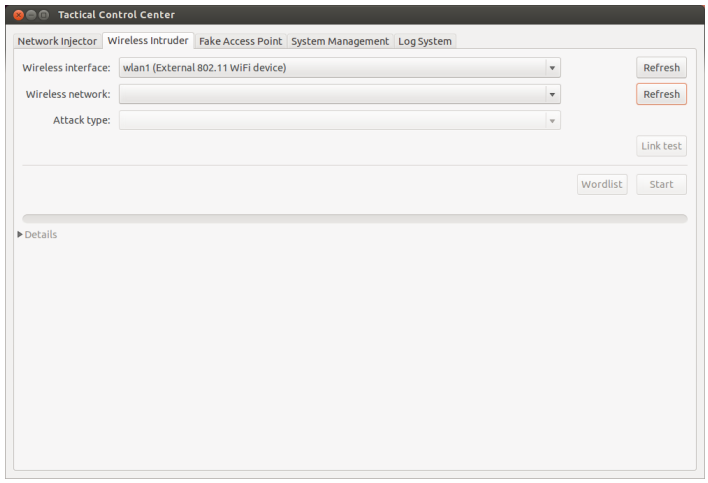
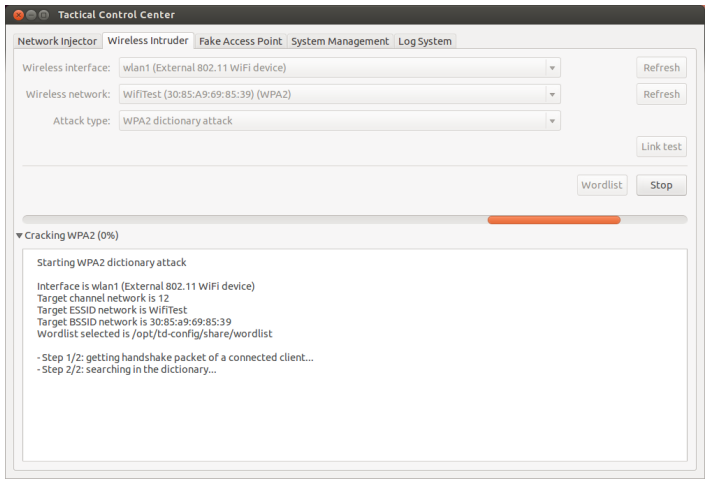
Running a network test

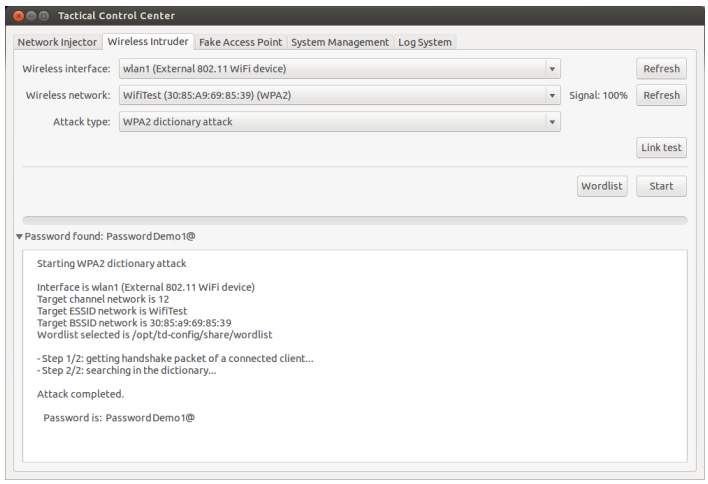
The network test procedure for sniffing and/or injection is provided below:

Steps	*Result*
1. In the **Network Injector** tab or **Wireless Intruder** tab or **Fake Access Point** tab, select the network interface. 2. Click **Link test**: a window appears where test results are displayed. 3. If the test failed, move to a better position where the signal is stronger and repeat the test.  IMPORTANT: attack will not be successful if the test fails.	

Acquiring a protected WiFi network password

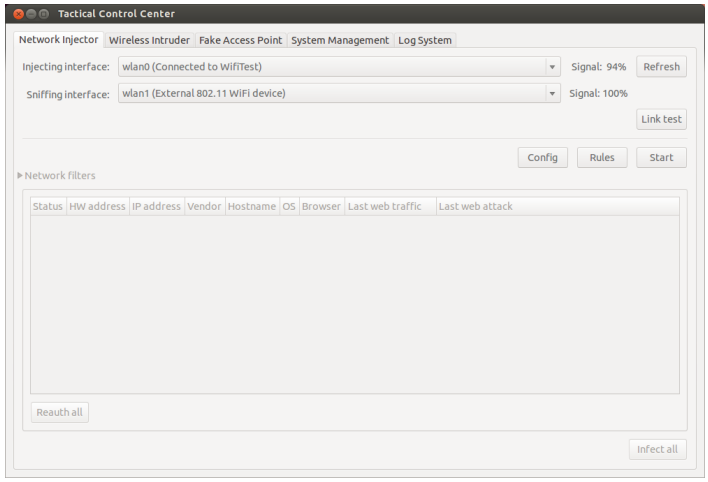
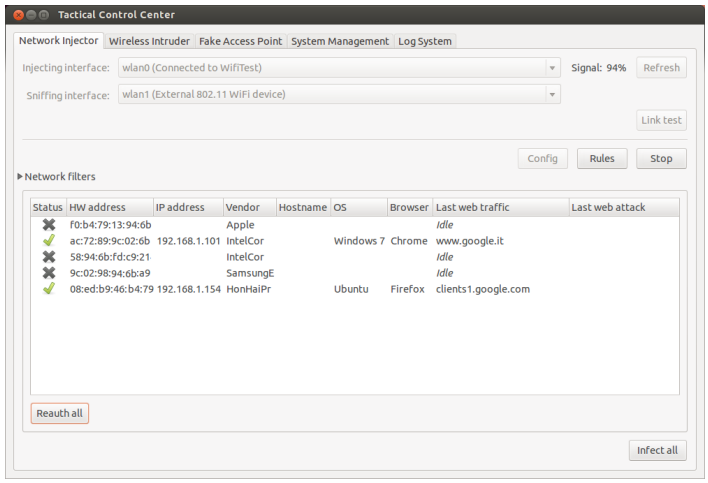
How to acquire a protected WiFi network password is described below:

Steps	*Result*
1. In the **Wireless Intruder** tab, select the WiFi network interface in **Wireless interface** 2. In **ESSID network,** select the network whose password is to be identified. NOTE: manage network interface connections/disconnections from the operating system and click **Refresh.** 3. In **Attack type** select the type of attack. 4. If necessary, click **Wordlist** to load an additional dictionary to attack WPA or WPA 2 protected networks IMPORTANT: the additional dictionary must be loaded at each attack.	
5. Click **Start**: the system launches various attacks to find the access password. 6. Click **Stop** to stop the attack.	

Steps	*Result*
7. If attacks are successful, the password appears over the status indicator.	
8. Using the operating system **Network Manager** use the password to connect to the WiFi network. The password is saved by the system and no longer needs to be entered.	-
9. Open the **Network Injector** section to start identification and infection.	

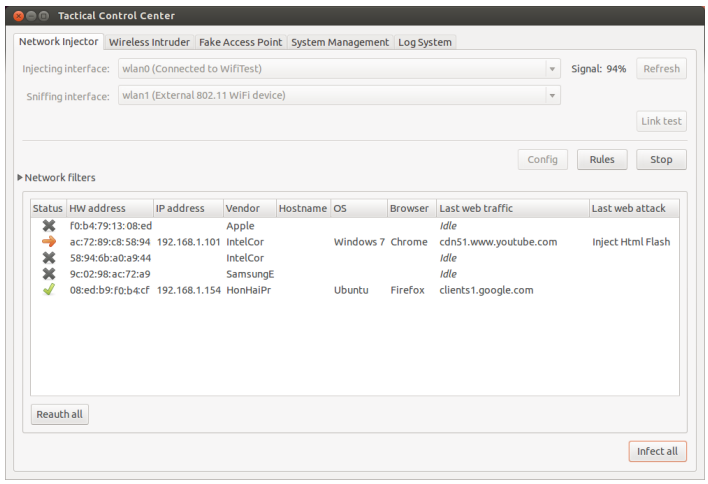
Infecting targets using automatic identification

To start automatic identification and infection:

Steps	*Result*
1. In the **Network Injector** tab, select the network interface for injection in the **Injecting Interface** list box. 2. In the **Sniffing interface** list box, select a different network interface to be used for sniffing or select the same interface used for injection. NOTE: manage network interface connections/disconnections from the operating system and click **Refresh.** Tip: use two different interfaces to guarantee better device identification. 3. Check signal power and, if necessary, run the network test (**Link test** key). NOTE: signal power must be at least 70%. A single value will be returned if the same network interface is used for injection and sniffing.	
4. Click **Start**. 5. The network sniffing process starts and all devices identified as targets appear. The **Status** column displays identification status. WARNING: verify identification status.*See "Tactical Control Center data" on page 105 .* 6. Target devices begin to be infected. Infection start is recorded in the log. NOTE: non target devices don't appear in the list and are thus excluded from automatic infection.	
7. To stop infection, click **Stop.**	-

Forcing unknown device authentication

To force an unknown device authentication:

Steps	*Result*
1. In the **Network Injector** tab, select unknown devices from the list (status ✖)	
2. Click **Reauth selected**: devices are forced to re-authenticate. Tip: in certain cases, all devices must be authenticated. To do this, click **Reauth All**.	-
3. If re-authentication is successful, automatic identification is started: device status will be ✔ and can be infected from now on.	-

Infecting targets using manual identification

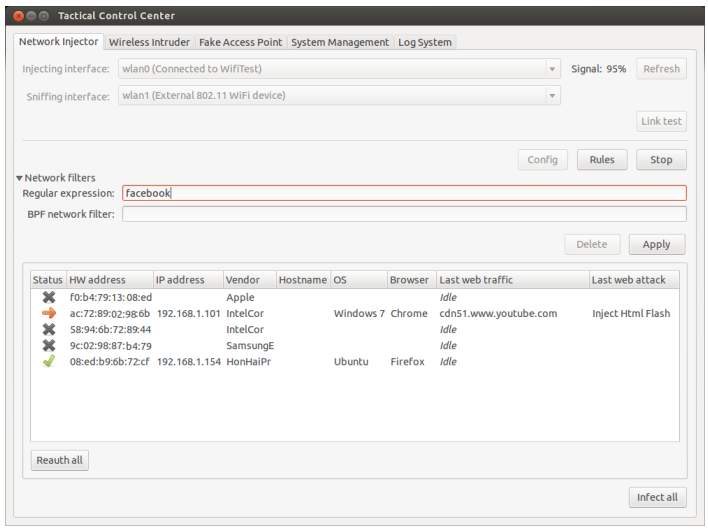
To manually infect network devices:

Steps	*Result*
1. In **Network Injector,** select one or more devices to be infected from the device list and identify them using the displayed data. Tip: if there are a lot of devices in the list, filter the selection.*See "**Setting filters on tapped traffic**" on the facing page* .	-

Steps	*Result*
2. Click **Infect selected**: all injection rules are "customized" with the device data and applied. Device attacks will be displayed in the logs. IMPORTANT: this operation requires a special rule in RCS. Tip: in certain cases, all connected devices must be infected, even non target devices or those not yet connected. To do this, click **Infect All**. **Result** : if the infection was successfully started, device status is .	-

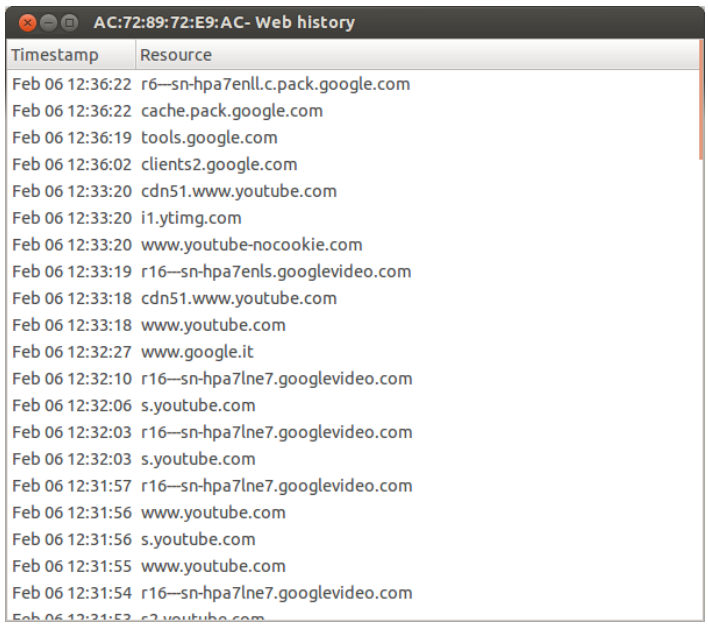
Setting filters on tapped traffic

To select target devices using data traffic filters:

Steps	*Result*
1. In the **Network Injector** tab, click **Network filters.** 2. For a wider search, enter a regular expression in the **Regular expression** text box. 3. Or, to refine the search, enter a BPF expression in the **BPF Network Filter** text box. **Result** : the system only displays filtered devices in the list.	
4. Manually infect devices as described in the procedure*see "**Infecting targets using manual identification** " on the previous page .*	-

Identify the target by analyzing web chronology

To identify a target:

Steps	*Result*
1. In the **Network Injector** tab, double-click the device to be checked: a window opens with the chronology of the websites visited by the browser.	
2. If the device is the target device, close the chronology and run procedure *"**Infecting targets using manual identification** " on page 99* .	-

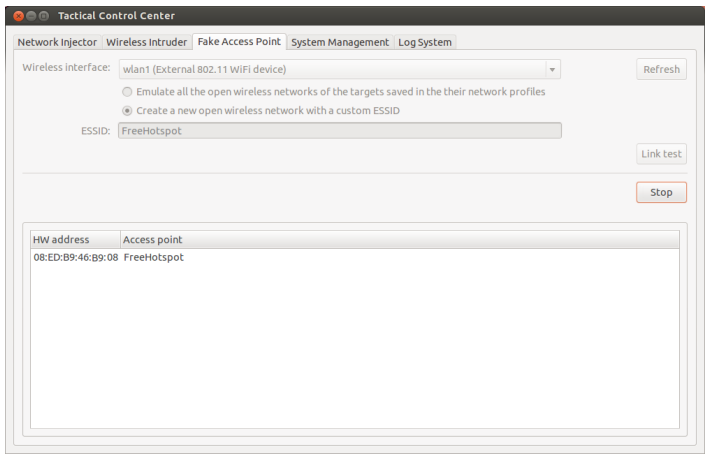
Cleaning erroneously infected devices

To remove an infection from a device, the agent must be closed on the RCS Console.

Emulating an Access Point known by the target

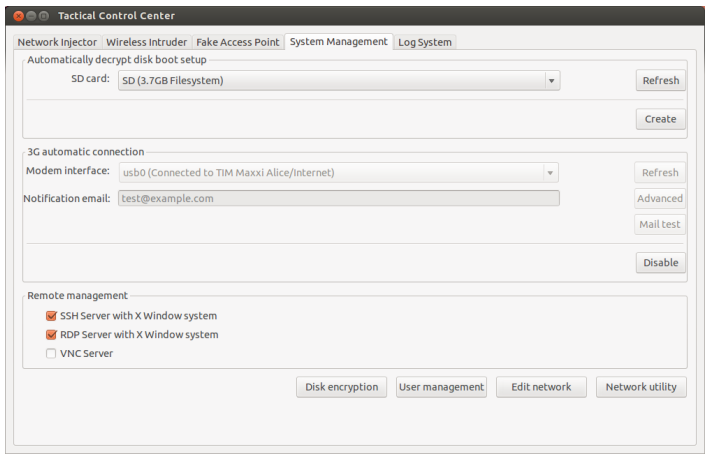
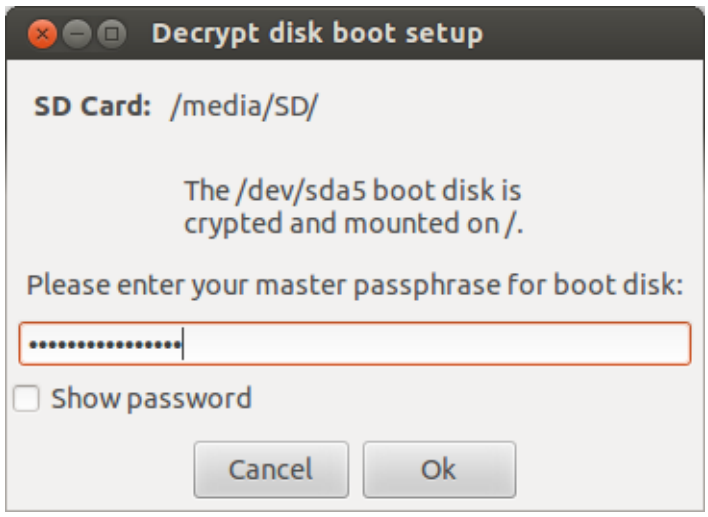
IMPORTANT: before emulating an Access Point, stop any current attacks in the Network Injector tab.

To transform Tactical Network Injector into an Access Point known by targets:

Steps	*Result*
1. In the **Fake Access Point** tab, select the network interface to listen to in the **Wireless Interface** list box.	
2. Select the type of Access Point emulation	
3. Click **Start**: Tactical Network Injector recovers the names of the WiFi networks devices usually connect to and displays them.	
4. At the same time, it establishes communications with the single devices, emulating the access point for each network.	-
5. In **Network Injector**, select the same network interface displayed as the access point in the **Injecting interface** list box	
6. Click **Start**: connected devices are displayed	-
7. Manually infect devices as described in the procedure*see "Infecting targets using manual identification " on page 99 .*	-

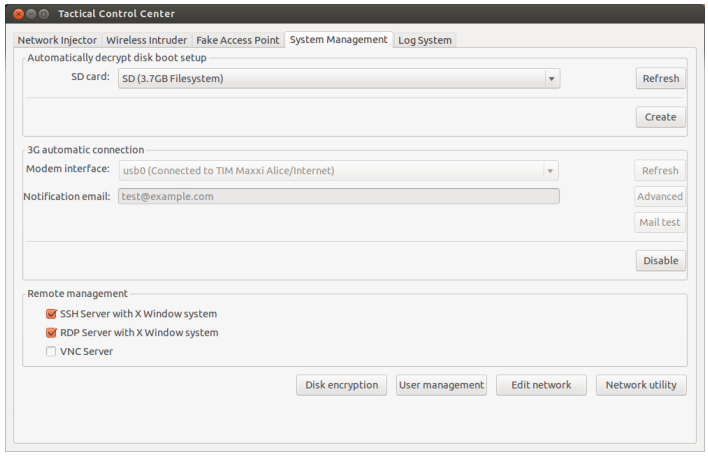
Setting remote application access

To remotely access Tactical Control Center:

Steps	*Result*
1. Insert an SD memory card in the notebook slot. 2. In the **System Management** tab, click **Refresh**: the system recognizes the SD card and displays it in **SD card**. 3. If several SD cards are installed, select the required card from the **SD card** list box and click **Create**.	
4. Enter the system administrator password and click **OK**: the system generates a new password and saves it on the SD card.	

Steps	*Result*

5. Connect the modem to the device.
6. In the **System Management** tab click **Refresh**: the system recognizes the model and displays it in **Modem Interface**.
7. If several modems are installed, select the required modem from the **Modem Interface** list box.
8. To enable email delivery with the device IP address at each connection, follow the steps below:
   a. In **Notification email** enter the email address where the email will be sent.
   b. Click **Mail test** to send a test email
   c. If the email is not received, click **Advanced** to manually set the mail server: the **Email advanced configuration** window appears.
   d. Enter the required data and click **Save.**
   e. Click **Mail test** to send a test email with the set server.



9. To enable automatic connection with the selected modem, click **Enable**

NOTE: the modem enabled in this tab also appears in the **Network Injector** tab, in the **Injecting Interface** list box and will be used to infect agents.

10. Select the network protocol to be used for remote access.

NOTE: you can directly open some helpful operating system windows using the buttons at the bottom of the screen.

Turn off Tactical Network Injector

No special procedure is foreseen. Normal computer shutdown.

Viewing infection details

To view data recorded in the current session, select the **Log System** tab.

NOTE: all log files are saved in the file system in /var/log/td-config .

Tactical Control Center data

Network Injector data tab

Data is described below:

Data	*Description*
Injecting Interface	List of connected network interfaces. Select the injection interface connected to the network on which the device to be attacked is connected. When simulating an Access Point, the interface used in the **Fake Access Point** tab also appears. The set 3G modem and enabled for remote access in the **System Management** tab also appears here.
Sniffing interface	Like **Injecting Interface** or another network interface to only be used for sniffing.
Regular expression	Expression used to filter devices connected to the network. It is applied to all data transmitted and received by the device via network, of any kind. *See "What you should know about Tactical Control Center" on page 76 .*
BPF network filter	This is used to more accurately filter devices using BPF syntax (Berkeley Packet Filter). This syntax includes key words accompanied by qualifiers: *See "What you should know about Tactical Control Center" on page 76 .*

Found device data

Data is described below:

Data	*Description*
Status	Connected network device status:  : unknown device. It cannot be infected due to problems tied to authentication. Forcing authentication.  : device being identified.  : device identified and can be infected.  : infected device.

Data	*Description*
HW address	Device network card hardware address.
IP address	Device's network IP address.
Vendor	Network card brand (rather reliable).
Hostname	Device name.
OS	Device operating system.
Browser	Web browser used by the device.
Last web Traffic	Last sites visited by the device detected and analyzed in the last five minutes. NOTE: if the device no longer generates web traffic at the end of the five minutes, the message **Idle** will appear. This usually occurs when no one is using the device.
Last web attack	Last attack type and results. To check additional details, see the **Log System** tab.

Wireless Intruder data tab

Data is described below:

Data	*Description*
Wireless interface	List of non connected network interfaces. Select the interface to connect to the protected WiFi network to be opened.
ESSID network	Name of the local network to be opened.
Attack type	Types of available password identification. **WPA/WPA2 dictionary attack** **WEP bruteforce attack** **WPS PIN bruteforce attack** ***See "What you should know about identifying the WiFi network password" on page 81 .***

Fake Access Point data tab

Data is described below:

Data	*Description*
Wireless interface	List of non connected network interfaces. Select the interface to be displayed as the WiFi network.
ESSID	ESSID network name to be created.
HW address	Device network card hardware address.
Access point	Name of the Access Point expected by the device.

System Management data tab

Data is described below:

Data	*Description*
SD card	Memory card to manage the encrypted disk password.
Modem interface	3G Modem for device connection.
Notification email	Email address where the device IP is sent whenever it connects to the network.  IMPORTANT: mandatory field for dynamic IP addresses.
Remote management	Remote access network protocol.

System monitoring

Presentation

Introduction

System monitoring guarantees constant control of component status and license usage.

Content

This section includes the following topics:

System monitoring (Monitor)

To monitor the system:	• **Monitor** section

Purpose

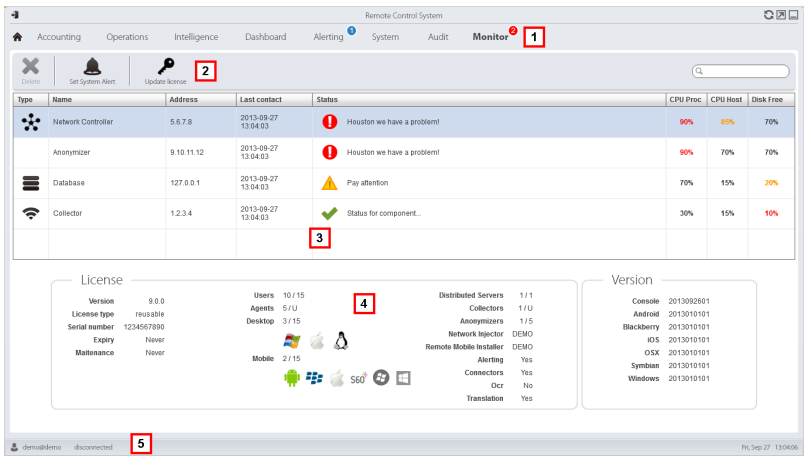
This function lets you:

- monitor system status in both hardware and software terms
- monitor license used compared to those purchased

Service call: Contact your HackingTeam Account Manager if additional licenses are required.

What the function looks like

This is what the page looks like:



Area	*Description*
1	RCS menu. Monitor 1 : indicates the current number of system alarms triggered.
2	Window toolbar.

Area	*Description*
3	List of RCS components and their status:  Alarm (generates an e-mail sent to the alerting group)  Warning  Component running
4	License status.
5	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 14 .*
For a description of the data in this window *see "**System monitoring data (Monitor)**" below .*

System monitoring data (Monitor)

System component monitoring data

System monitoring data is described below:

Data	*Description*
Type **Name**	Monitored component type and name:  Anonymizer  Carrier  Collector  Database  Network Controller
Address	Component's IP address.

Data	*Description*
Last contact	Last synchronization date-time.
Status	Component status at last synchronization:  Alarm: the component is not running, contact the alerting group for immediate service.  Warning: the component signals a risky situation, contact the system administrator for necessary checks.  Component running.
CPU	% CPU use by the single process.
CPU Total	% CPU use by server.
Disk Free	% free disk space.

License monitoring data

License monitoring data is described below: For restricted licenses, the format is "x/y" where x is the amount of licenses currently used by the system and y the maximum amount of licenses.

 ***CAUTION: if all the licenses are in use, any new agents will be put in queue until a license is freed or new ones purchased.***

Data	*Description*
License type	Type of license currently in use for agents. **reusable**: an agent's license can be reused after it is uninstalled. **oneshot**: an agent's license is only valid for one installation.  NOTE: the license can only be updated if the user has **License modification** authorization.
Users	Amount of users currently used by the system and maximum admitted quantity.
Agents	Amount of agents currently used by the system and maximum admitted quantity.
Desktop Mobile	Amount of desktop and mobile agents currently used by the system and maximum admitted quantities respectively.
Distributed server	Amount of database currently used by the system and maximum admitted quantity.

Data	*Description*
Collectors	Amount of Collectors currently used by the system and maximum admitted quantity.
Anonymizers	Amount of Anonymizers currently used by the system and maximum admitted quantity.

9

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

NOTE: some sub-actions may be missing since not supported by some operating systems.

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.

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.

Any command output can be viewed in the **Commands** page. *See "Command page" on page 45 .*

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.

Reference to the agent's folder

The dir virtual environment variable that refers to the agent's installation folder (hidden) can be added to the command string.

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 42*

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.

Parameters

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

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.

Step	*Description*
7	Download of all evidence collected by the agent with simultaneous secure removal.
8	Secure removal of all downloaded evidence from the agent.

Desktop settings

Name	*Description*
Host	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.
Band	Maximum bandwidth to be used during synchronization.
Minimum delay	Minimum delay in seconds from one evidence sent to the next.
Maximum delay	Maximum delay in seconds from one evidence sent to the next.
Stop is successfully completed	If enabled, the sub-action chain is interrupted when synchronization is successfully completed. Remaining sub-actions in the queue are not run.

Mobile settings

Name	*Description*
Host	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 is successfully completed	If enabled, the sub-action chain is interrupted when synchronization is successfully completed. Remaining sub-actions in the queue are not run.

Name	*Description*
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.

Connection type selection criteria (Windows Phone)

For Windows Phone, the system internally defines the type of connection to be used regardless of set parameters.

If the device is set to support both WiFi and 3G/4G and there is a set and running WiFi connection, the system will use the 3G/4G network when the device screen is off and not charging or the WiFI network in other cases.

Uninstall action

Purpose

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

NOTE: on BlackBerry, removing the agent requires an automatic restart.

NOTE: if the device does not have root privileges on Android, the user must authorize uninstall. To learn how to check whether you have root privileges,*see "**What you should know about Android**" on page 144 .*

NOTE: on Windows Phone, removing the agent deletes all files generated by the agent but the application icon remains in the program list.

Parameters

None

10

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

NOTE: some events may be missing since not supported by some operating systems.

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.*

Event	*Device*	*Triggers an action when..*
Timer	desktop, mobile	*the specified intervals elapse.*
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.

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!

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.

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.

Desktop settings

Name	*Description*
IP address	Connection destination IP address NOTE: Enter 0.0.0.0 to indicate any address. 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.

Mobile settings

None

Idle event

Purpose

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

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.

Parameters

Name	*Description*
Type	Type of position to be used. **GPS** • **Latitude, Longitude**: coordinates • **Distance**: range from coordinates. **GSM Cell (all operating systems except Windows Phone)** • **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,

Process event

Purpose

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

Parameters

Name	*Description*
Type	**Process name**: the event triggers an action when the specified process starts. **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*")
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 the device's disk space used to store the collected evidence exceeds the set limit.

When disk space falls under the limit, the action will be terminated at the next synchronization.

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.

Parameters

None

SimChange event

Purpose

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

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: incoming messages are only deleted on BlackBerry OS 5.x.

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

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. IMPORTANT: the string is not case sensitive.

Standby event

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

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.

Parameters

Name	*Description*
Type	Interval type: • **Loop**: triggers an action, indefinitely repeating it at every interval, as 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.

Parameters

None.

WinEvent event

Purpose

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

Parameters

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

11

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

NOTE: some modules may be missing since not supported by some operating systems.

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 (i.e..: GSM and VoIP).
Calls	base	*desktop, mobile*	calls (i.e.: phone, Skype, MSN).
Camera	base, advanced	*desktop, mobile*	Webcam images.
Chat	advanced	*desktop, mobile*	chat (i.e.: 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*	e-mail, SMS, MMS.
Messages	base	*desktop, mobile*	e-mail, SMS and chat.

Module	*Configuration*	*Device*	*Recording...*
Mic	advanced	*desktop, mobile*	audio from a microphone.
Money	advanced	*desktop*	Information on the cryptocurrency digital wallet (i.e.: Bitcoin)
Mouse	advanced	*desktop*	mouse click.
Password	advanced	*desktop, mobile*	password saved.
Position	base, advanced	*desktop, mobile*	target's geographic position.
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*	Deprecated as of RCS version 8.4.
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.

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.

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.

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 (GSM and VoIP).

Significant data

Data is described below:

Field	*Description*
Enables call recording	(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.

Significant data

Data is described below:

Field	*Description*
Quality	Image quality (low, medium, high).

Chat module

Purpose

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

IMPORTANT: for Android, root privileges are required to capture chat. ***See "What you should know about Android" on page 144 .***

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).

Significant data

None

Clipboard module

Purpose

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

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.

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.

Significant desktop data

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

Field	*Description*
Inhibit network	Inhibits synchronization when potentially dangerous processes are running.
Inhibitors (network)	List of processes that, if running, will prevent synchronization.
Inhibit Hooking	Inhibits program hooking when potentially dangerous processes are running.
Inhibitors (Hooking)	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*
Microphone	if selected, it prevents Mic audio recording
Calls	if selected, it prevents Call audio recording
Camera	if selected, it prevents Camera snapshots
Position	if selected, it prevents GPS use
Synchronization	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, root privileges). It can be useful to monitor disk usage on the device and to retrieve the list of applications installed.

NOTE: for Android, if the device has root privileges, **Device** type evidence indicates **root:yes.**

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.

Significant data

Data is described below:

Field	*Description*
Filter inclusions	List of file extensions to be recorded. Optionally specify the process to log the file when it is run or opened by that process.
Filter exclusions	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.

Field	*Description*
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"
Records the access path and method	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.
Minimum/maximum size	Minimum and maximum size admitted for the file to be downloaded.
More recent than	Minimum file creation date to be downloaded.

Keylog module

Purpose

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

NOTE: it supports all Unicode characters via IME.

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.

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)

 **IMPORTANT: root privileges are required for Android.** ***See "What you should know about Android" on page 144 .***

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.
Maximum size	Maximum size of the message to be recorded.

Mic module

Purpose

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

IMPORTANT: do not turn on the microphone to record data calls (i.e.: Skype, Viber) without having fully tested the phone model with the same operating system version. You may disable the client's audio, making the relevant application unusable..

IMPORTANT:the module is not enabled during calls for some mobile operating systems.

NOTE: for Windows Phone, recording start and end may be accompanied by an audio signal on some device models.

Significant desktop 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	NOTE: not supported by iOS, BlackBerry, Android and Symbian, Windows Phone. 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.
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.

Money module

Purpose

The **Money** module records information in the target's cryptocurrency digital wallet (i.e: Bitcoin). Specifically, it records:

- the target's address(es)
- list of transactions completed
- address book with transaction target addresses
- balance

Significant data

None

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 136 .*

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.

Significant data

None

Position module

Purpose

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

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.

NOTE: for Windows Phone, the system internally sets the most efficient way to find the device position at a given time, regardless of set parameters.

Screenshot module

Purpose

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

IMPORTANT: for Android, root privileges are required to capture screenshots. ***See "What you should know about Android" on page 144 .***

Significant data

Data is described below:

Field	*Description*
Quality	Captured image final quality. **Low**: worst image quality, maximum compression **High**: best image quality, minimum 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.

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).

Significant data

None

12

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:

List of installation vectors

Following is a list of vectors with supported device types and operating systems:

Installation Vector	*Device*	*Operating system*	*Description*
Exploit	Desktop, Mobile	*OS X, Windows* *iOS*	Adds the agent to any document (document format may depend on the available exploits).
Installation Package	Mobile	*Android, BlackBerry, iOS, Symbian, Windows Phone WinMobile*	Creates an auto-installer file with the agent.
Local Installation	Mobile	*BlackBerry, iOS, WinMobile*	Installs the agent on the target device either through USB or SD/MMC memory card.
Melted Application	Desktop Mobile	*Linux, OS X, Windows* *Android, Symbian, WinMobile*	Adds the agent to any application file.
Network Injection	Desktop Mobile	*Linux, OS X, Windows* -	Link to the injection rule creation page. *See "**Managing the Network Injector**" on page 68 .*
Offline Installation	Desktop	*Multiplatform*	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	*Multiplatform, Android, BlackBerry, Symbian, WinMobile*	Generates a QR code for sites or printouts that, if photographed by the target, will install the agent.

Installation Vector	*Device*	*Operating system*	*Description*
Silent Installer	Desktop	*Linux, OS X, Windows*	Creates an empty executable file that, when run on the target device, installs the agent.
U3 Installation	Desktop	*Windows*	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	*Multiplatform, Android, BlackBerry, Symbian, WinMobile*	Sends a WAP message that will install the agent if accepted by the target.

What you should know about Android

Root privileges

The Android operating system requires root privileges to run some operations on its devices.

An Android device agent requires root privileges to:

- capture chat, *see "**Chat module**" on page 132*
- capture e-mail, *see "**Messages module**" on page 137*
- capture screenshots, *see "**Screenshot module**" on page 140*
- keep updated, *see "**Agent page**" on page 42 , "**Target page**" on page 28*

Obtaining root privileges

Root privileges can be automatically obtained without any interaction on the device.

However, automatic acquisition is not always guaranteed. If automatic acquisition fails and **Required Administrative Privilege** was selected during agent compilation, the agent requests the user manually obtains privileges from the device if permitted by the operating system.

Checking for root privileges

To check for root privileges on the target device, enable the **Device** module.

Root status is indicated in **Device** type evidence; if root privileges were obtained, **root:yes** appears.

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 folder C:\RCS\DB\bin enter the following command:

```
> rcs-db-config --sign-cert CertificateFile --sign-pass CertificatePassword
```

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

Exploit vector

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).

Desktop device installation

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

Mobile device 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).

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
```

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, in **System, Frontend** section.

Parameters

Name	*Description*
File type	Type of file to be infected (i.e.: .PDF).
Select 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**: to 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, MMS or email,
- directly from computer via USB cable,
- (Windows Mobile only) direct copy to SD card,
- (Windows Phone only) attachment via email.

Notes for Android operating systems (vector preparation)

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

- *ApplicationName*.v2.apk: vector for Android 2.x
- *ApplicationName*.default.apk: vector for Android 3.x and 4.x

Notes for Android operating systems (installation)

The installation procedure is provided below:

Step	Action
1	Enable the **Unknown origins** option in the device settings (typically under **Settings, Applications**). The option can be disabled after installation. NOTE: if this option is not enabled, a request to authorize an application not in the Android Market appears during installation.
2	Device root privileges must be obtained if the vector includes Screenshot, Chat and Messages modules. *See "**What you should know about Android**" on page 144*
3	Run the appropriate APK vector on the selected device.
4	During APK vector installation, accept the permissions requested by the agent. For Android 3.x and 4.x, click **Open** to start the vector, otherwise the vector will not be installed**.** **IMPORTANT: the default APK vector for Android 3.x and 4.x appears as a normal application called DeviceInfo, that displays device information.**
5	A request to obtain root privileges could appear when the vector is running if the **Require Administrative Privilege** option was enabled.

Notes for Windows Phone operating systems (vector preparation)

Compiling a factory with the Installation Package vector for Windows Phone operating system creates .zip *FactoryName*_winphone_silent.zip in folder RCS Download that contains two files:

- *ApplicationName*.xap: packet with applications to be installed on the target device
- *ApplicationName*.aetx: company certificate to install the application

IMPORTANT: in order for compiling to be successfully completed, follow the procedure to load the necessary files in RCS. *See "Installation Package preparation for Windows Phone" on page 150*

Notes for Windows Phone operating systems (installation)

The MyPhoneInfo application, used to install the agent, is included in the packet with .xap applications. Installation does not require phone unlock.

.xap and .aetx files can be sent to the target device:

- as attachments in an email;
- as links sent via email, sms or in a web page

For installation via web, the Web service must correctly support the MIME types for the.xap and .aetx files; the following instructions must be found in the mime.types files:

- `application/x-silverlight-app xap`
- `application/x-aetx aetx`

Run the following procedure for both modes:

Step	*Action*
1	Open file *`ApplicationName`*`.aetx`. **IMPORTANT: this is the certificate that must always be opened first.**
2	Answer the displayed questions by clicking **Add.**
3	Open file *`ApplicationName`*`.xap`.
4	Answer the displayed questions by clicking **Install**: the MyPhoneInfo application will be installed on the phone**.**
5	From the application list, open the MyPhoneInfo application at least once.
6	Close MyPhoneInfo: the agent is ready. **IMPORTANT: if you exit the application without closing it, the application, and thus the agent, are suspended. The agent only starts when the application is closed or the phone is turned back on.**

The agent communications with the RCS server if and as long as the MyPhoneInfo application is installed on the device and the device is on. If a mobile data connection is not available, the agent can only communicate with the RCS server when the user uses the phone or the phone is connected to a computer or battery charger.

NOTE: when the device is turned on, it takes 30 minutes for the agent to restore communications with the RCS server. The 30 minutes are guaranteed if mobile data and Wi-Fi connections are running on the device. Otherwise, it could take longer.

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.

Notes for Symbian operating systems

IMPORTANT: the certificate is required for Symbian.

Android, WinMobile, Windows Phone parameters

Name	*Description*
Application name	Application name (visible to target)
Requires Administrator privileges	(Android only) If automatic acquisition fails, this option enables the user request to manually obtain root privileges from the device. **WARNING: the request is displayed on the target device.**

BlackBerry settings

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

Symbian settings

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

Installation Package preparation for Windows Phone

Introduction

For Windows Phone devices, the agent is installed on the target device through a Windows Phone application. The following files must be on the RCS server to successfully complete agent installation:

- a .pfx file to sign the Windows Phone .xap installation packet
- an .aetx file as a Windows Phone application certificate

Recommended sequence

Complete the following steps to generate the .pfx and .aetx files and load them on the RCS server:

Step	*Action*
1	Obtain a Symantec ID code to be used to purchase the certificate required to distribute a Windows Phone application.
2	Obtain the Symantec certificate required to distribute Windows Phone applications.
3	Install the Symantec certificate required to distribute Windows Phone applications.
4	Generate the .pfx and .aetx files
5	Load the .pfx and .aetx files on the RCS server

How to read these instructions

NOTE: links to web pages in the procedures were working when the manual was written. If the link does not work, find the right web page..

In the event of discrepancies between that indicated in the manual and the instructions received directly from the concerned organizations, follow the organizations' instructions.

Obtaining a Symantec ID code

Proceed as follows to obtain it:

Step	*Action*
1	Register a Microsoft account in https://signup.live.com/signup.aspx?lic=1.
2	Register an account in Windows Phone Dev Center logging in with your Microsoft account in https://dev.windowsphone.com/en-us/join/

Step	*Action*
3	• Click **Join Now**: the Windows Phone Dev Center account registration page appears. • Select **Company** as **Account Type**. • Click **Next**. • In the **Account Info** section, enter your data and contacts. • In the **Publisher Info** section, enter the name to be displayed as the application distributor during installation as the **Publisher Name.** **WARNING: the user who installs the** .xap **packet and** .aetx **certificate on his phone sees this name.** • In the **Approver Info** section, enter the data and contact information for the company manager who can approve the registration request. • Complete registration following the on-screen instructions. **IMPORTANT: prove a correct email address and phone number since they will be used to validate registration and provide the Publisher ID.**
4	After registering, you will receive an email from Symantec, the Microsoft partner that validates companies registered with Windows Phone Dev Center, to validate registration. Additional communications may also occur by phone. **IMPORTANT: have the Approver promptly respond to the Symantec email.**
5	After validation, you will receive an email with account data: • Publisher ID • Publisher Name

NOTE: to learn more, visit
http://msdn.microsoft.com/library/windowsphone/help/jj206719(v=vs.105).aspx

Obtaining a Symantec certificate

The Enterprise Mobile Code Signing Certificate is required to distribute Windows Phone applications.

Proceed as follows to obtain it:

Step	*Action*
1	Purchase a Enterprise Mobile Code Signing Certificate from Symantec at https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do.

Step	Action
2	• Enter the **Publisher ID** you received and the email indicated in the **Account Info** section during Windows Phone Dev Center registration. • Complete the purchase following the on-screen instructions.
3	When finished, you will receive a couple of emails from Symantec indicating: • order confirmation • the list of enabled functions according to the order • the certificate and instructions on how to import it on your computer

NOTE: to learn more, visit https://knowledge.verisign.com/support/code-signing-support/index?page=content&id=SO20770&actp=search&viewlocale=en_US

Installing the Symantec certificate

To complete Enterprise Mobile Code Signing Certificate installation, first install:

- Enterprise Mobile Root;
- Enterprise Mobile CA certificate.

IMPORTANT: always use the same browser to download certificates. The Firefox browser is referred to in the described procedure.

Follow the procedure below:

Step	Action
1	Open Firefox.
2	Copy and paste the URL received in the email in the address bar to install Microsoft Enterprise Mobile Root Certificate.
3	In the **Download certificate** dialog window, select all three check boxes and click **OK.**
4	Copy and paste the URL received in the email in the address bar to install Microsoft Enterprise CA Root Certificate.
4	In the **Download certificate** dialog window, select all three check boxes and click **OK.** NOTE: to check whether certificates were installed, select the certificate in the **Firefox** menu, **Options**, and select **Advanced**. Next select the **Certificates** tab and click on **Show Certificates:** the names of the installed certificates appear in the certificate list in the **Authorities .**
5	Install Enterprise Mobile Code Signing Certificate from the link in the email you received and click **Continue**.

Generate the .pfx and .aetx files

The .pfx and .aetx files required to sign and distribute Windows Phone applications can be generated with Enterprise Mobile Code Signing Certificate.

IMPORTANT: the procedure requires Windows Phone Software Developer Kit 8.0, available at http://www.microsoft.com/it-it/download/windows.aspx to be installed on the computer. The AET Generator tool included in this kit lets you create the .aetx file.

IMPORTANT: use the same browser used to install the certificates to run the procedure. The Firefox browser is referred to in the described procedure.

Follow the procedure below:

Step	*Action*
1	Open Firefox.
2	In the **Firefox** menu, select **Options**. Next, select **Advanced**, and then the **Certificates tab.**
3	Click **Show**. **certificates**.
4	• In the **Personal certificates** tab, select the *Publisher name* certificate and click **Export** • Save the file with the .p12 extension • Enter the certificate export password: "password" **IMPORTANT: enter this and not other passwords.**
5	Rename the file with the .pfx extension
6	From the Windows command prompt, open the folder where the .pfx file is saved and run the following command: **"%ProgramFiles (x86)%\Microsoft SDKs\Windows Phone\v8.0\Tools\AETGenerator\AETGenerator.exe" *FileName*.pfx password** where *FileName* is the name of the .pfx file. **Result**: three files are generated in the folder where the .pfx file is saved: • AET.aetx • AET.aet • AET.xml

NOTE: to learn more, visit http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj206943%28v=vs.105%29.aspx

Load the .pfx and .aetx files on the RCS database server

Follow the procedure below:

Step	*Action*
1	Copy the files to the RCS database server
2	From the Windows command prompt, run the following command to use the .pfx file to sign Windows Phone applications: `rcs-db-config --sign-pfx-winphone FilePath\FileName.pfx` where *FilePath* is the .pfx file path on the RCS server
3	From the Windows command prompt, run the following command to use the .aetx file as a Windows Phone application certificate: `rcs-db-config --sign-aetx-winphone FilePath\FileName.aetx` where *FilePath* is the .aetx file path on the RCS server

Local Installation vector

Purpose

Compiling directly installs the agent on the target's 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.

IMPORTANT: to successfully complete installation on an iOS device, the iTunes application must be installed on the computer.

Parameters

None.

Melted Application vector

Purpose

Compiling modifies an existent executable by inserting the agent into it.

Agent components are encrypted to prevent reverse engineering.

Parameters

Name	*Description*
Application to be used as dropper	Executable file in which the agent is added. The file type differs based on the operating system: **Desktop devices** • **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**: EXE file • **Linux**: DEB file **Mobile devices** • **Android**: third party APK application.  IMPORTANT: test the final application. In fact, some applications run additional runtime security controls. • **Symbian**: .sisx file • **WinMobile**: .cab file
Requires Administrator privileges	(Android, WinMobile, OS X only) If automatic acquisition fails, this option enables the user request to manually obtain root privileges from the device.  **WARNING: the request is displayed on the target device.**

Network Injection vector

Purpose

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

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.

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.
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 captured, separated by the pipe character ("|").

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 .

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

Deleting no longer used files

Packets saved in the folder C:\RCS\Collector\public can be deleted using the **File Manager** function, in **System, Frontend** section.

Parameters

Name	*Description*
Application name	Installer name (visible to target)
URL	Connection to an Anonymizer where the installer was saved.
Requires Administrator privileges	(Android only) If automatic acquisition fails, this option enables the user request to manually obtain root privileges from the device.  **WARNING: the request is displayed on the target device.**
Application to be used as dropper	(Android only) Third party APK applications where the agent is to be added.  IMPORTANT: test the final application. In fact, some applications run additional runtime security controls.
Name	(BlackBerry only) Application data used to "hide" the agent.
Description	
Vendor	
Release	
Certificate tied to IMEI	(Symbian only) Device certificate.
Key tied to the certificate	(Symbian only) Certificate key.
S60 Edition	(Symbian only) Operating system version.

Silent Installer vector

Purpose

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

Parameters

None

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).

Parameters

None.

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: the certificate is required for Symbian.

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.

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, in **System, Frontend** section.

Parameters

Name	*Description*
Application name	Installer name (visible to target)
Telephone number	Target's phone number, including international area code.
URL	Connection to an Anonymizer where the installer was saved. If the package was saved 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.
Requires Administrator privileges	(Android only) If automatic acquisition fails, this option enables the user request to manually obtain root privileges from the device. **WARNING: the request is displayed on the target device.**
Application to be used as dropper	(Android only) Third party APK applications where the agent is to be added. IMPORTANT: test the final application. In fact, some applications run additional runtime security controls.
Name	(BlackBerry only) Application data used to "hide" the agent.
Description	
Vendor	
Release	
Certificate tied to IMEI	(Symbian only) Device certificate.
Key tied to the certificate	(Symbian only) Certificate key.
S60 Edition	(Symbian only) Operating system version.

]HackingTeam[

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

RCS 9 Technician's Guide
Technician's Guide 1.6 FEB-2014

info@hackingteam.com