

RCS Console

User Manual

INDEX

General concepts	4
Activity, Target and Backdoor	4
Getting started.....	5
THE CONSOLE VIEW	7
Users	7
Privileges	11
Groups.....	12
Activities	16
Blotter.....	20
Target	21
Backdoors.....	23
 Summary	25
Multiple selection of Backdoors	27
 Webcam, Snapshot, Mouse Click.....	31
 Keylog.....	33
 Url	34
 Chat.....	35
 Print	36
 Clipboard	38
 Password.....	38
 Fileopen.....	39
 Filecap	40
 Download, Upload.....	41
 Addressbook	42
 Calendar.....	43
 Messages	44
 Location.....	45
 Device.....	47
THE DASHBOARD VIEW	48
Activities balloon.....	49
Targets balloon.....	49
Backdoors balloon	50
AUDIT	51
MONITOR	53
Components balloon	53
Components summary	53
License description.....	54
HOWTO	55
Create an activity.....	55
Create a target.....	57
Create a backdoor.....	58

View and search log	59
Export log	60
Create an user.....	61
Create a group.....	63
Assign privileges to users.....	65
Create and manage blotter.....	66

General concepts

Activity, Target and Backdoor

RCSConsole is the gui to manage and browse data collected on the RCSServer. Data is gathered on the server that is captured by several backdoors configured to point to that server.

A single backdoor is a software tool that is injected on a target device to collect several kind of information in order to conduct an investigation.

A target device can be 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. Targets in turn can be grouped in "Activities".

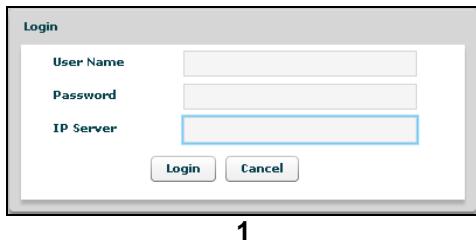
A single Activity represent an "investigation".

Backdoor can be configured to collect several kind of information, i.e. it has different agents enabled.

Each agent is responsible of collecting a single kind of information.

Getting started

When RCSConsole starts the initial logon screen is displayed:



1

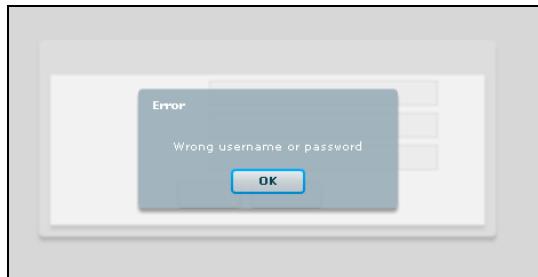
You need to logon to an RCSServer in order to have access to any data and to the rest of the application.

To logon you need to specify the following information:

- Your username
- Your password
- The RCSServer address URL¹. The URL must be preceded by protocol specification (http:// or https://). Encrypted channel (https) is active on port 4443.
Eg: https://192.168.0.1:4443

and press the "Login" button.

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

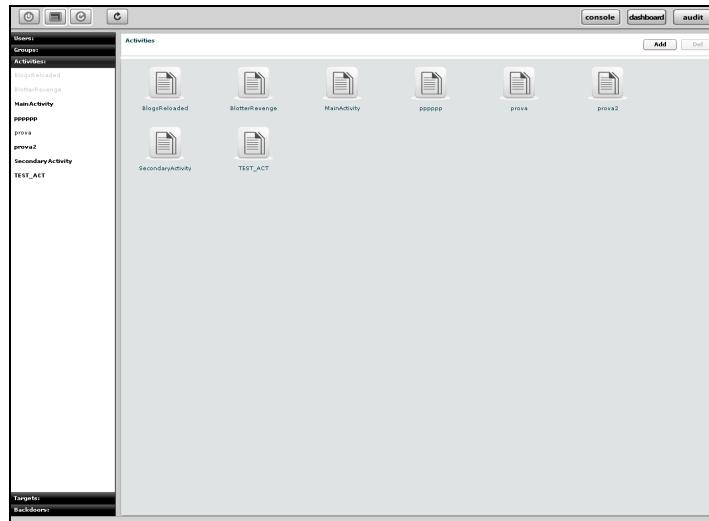


2

press "OK" button to close this window and return to initial logon screen.

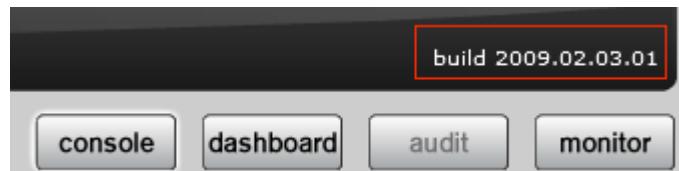
After login successfully the application shows this windows:

¹ Ask your RCSServer administrator if you don't know the server address URL or your username and password.



3

At the top on the right you see the current version, highlighted in red in next figure, and buttons to change modality: **console**, **dashboard**, **audit** and **monitor**; the default selected modality is **console**.



4

Selected button has a white border.

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



5

1. Close: to close the application;
2. Logout: to go back to login screen;
3. Clear cache: to wipe local log cache;
4. Change the current user password;
5. Fullscreen: to switch between fullscreen and resized window;
6. Automatic Refresh: to enable or disable automatic refresh;
7. Refresh: to start manual refresh.

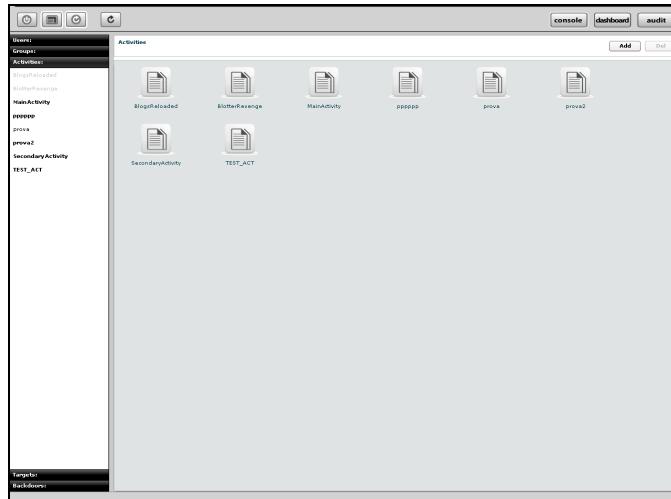
A white border appears around the selected button.

The view below the header is the same for any modality, splitted in two parts:

- on the left the object browser menu, let you navigate through all the resources accessible on the server,
- on the right the content/detail viewer

THE CONSOLE VIEW

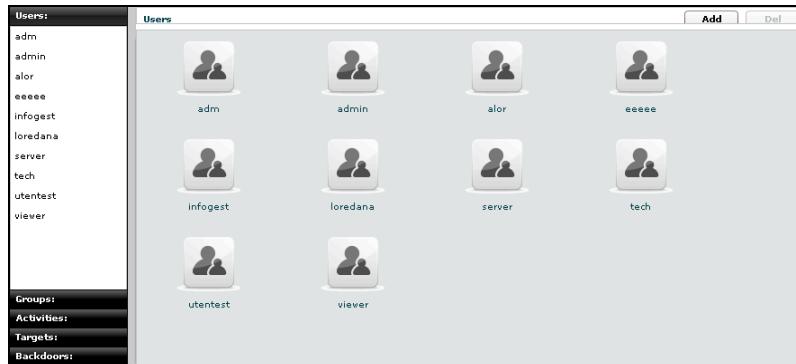
The console view let you browse through any object that your profile has access to and to manage and edit them.



6

Users

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



7

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:



8

then fill fields and assign privileges:

The image shows a dialog box titled "User infogest". It has fields for "Name" (infogest), "Description" (INFOGEST), "Password" (empty), "Confirm" (empty), and "Privileges" (Admin, Serv, Tech, View checked). At the bottom are "Save" and "Del" buttons.

9

click “Save” button to save data.

- select an user, either by:
 1. clicking on the user in menu-list:



10

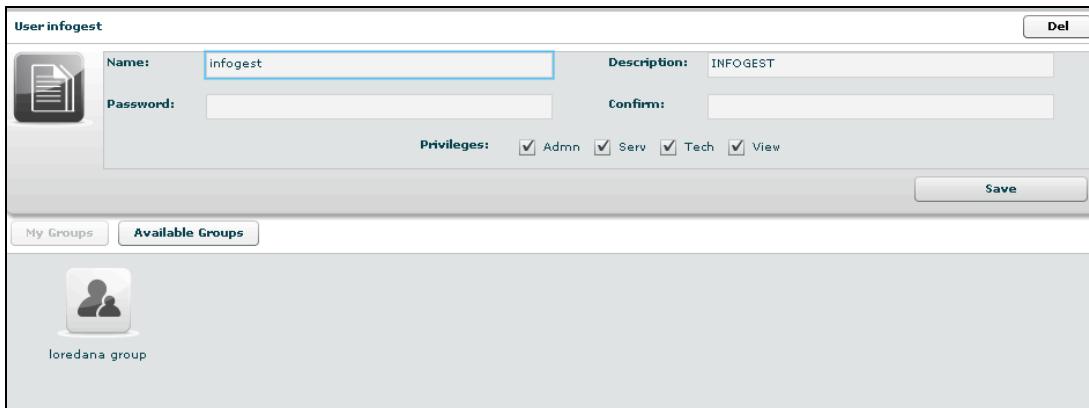
2. or double clicking on user's icon in icons-list:



11

- Edit an user: after selecting an 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:



12

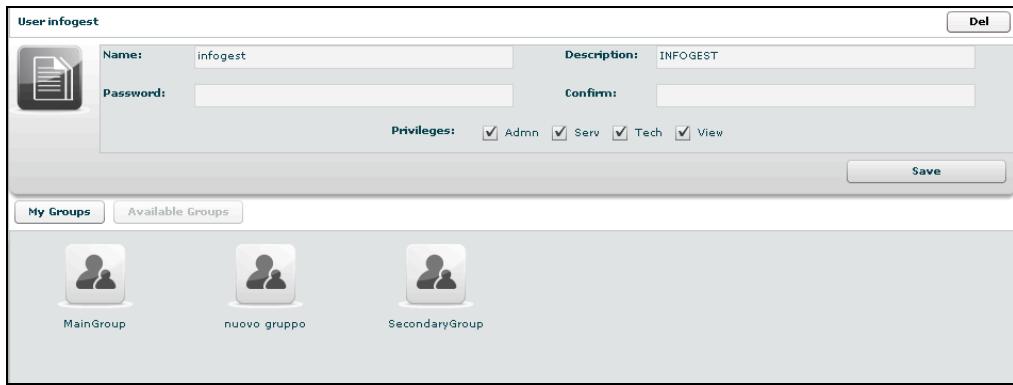
you can see group's details by double clicking group's icon.

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.



13

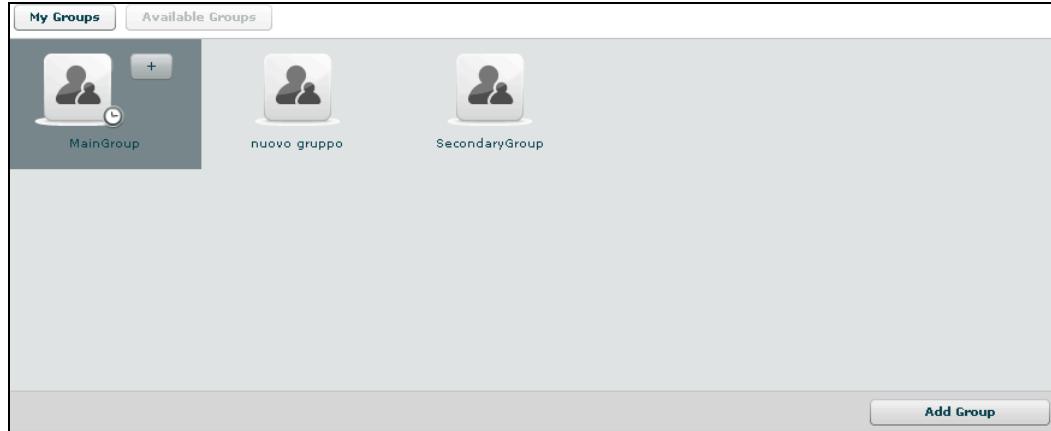
Clicking on “Available Groups” button you can view all groups available to be added to the selected user:



14

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:



15

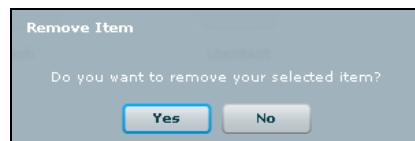
then either by:

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:



16

you must confirm the action to proceed:



17

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.

Privileges

- Admn: this is the super user. It is the only one that can create users, groups, activity and targets;
- Serv: reserved role for the server components that require access to XML-RPC methods;
- 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



18

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:



19

then fill fields:

The screenshot shows a form for adding a new group. It includes a file icon, fields for 'Name:' and 'Description:', and a 'Save' button at the bottom right.

20

click “Save” button to save data.

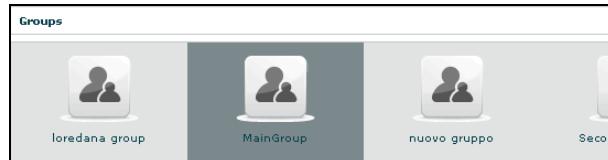
- Select a group: either by:

1. clicking on the group in menu-list:



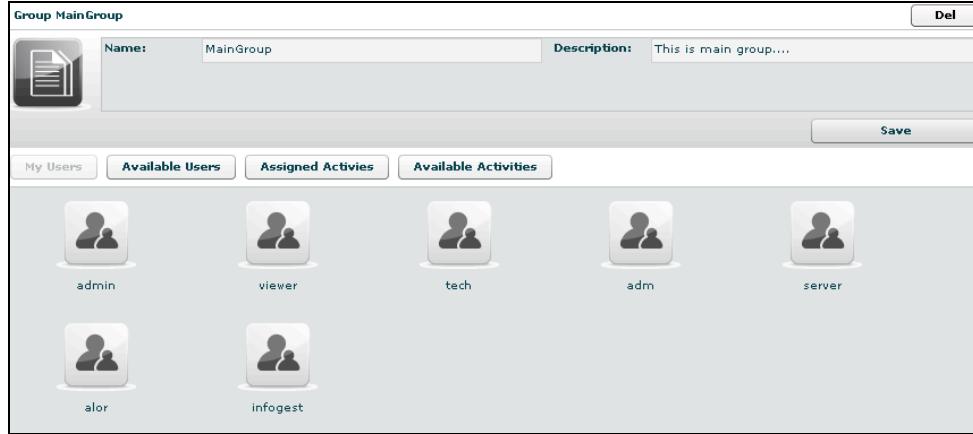
21

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



22

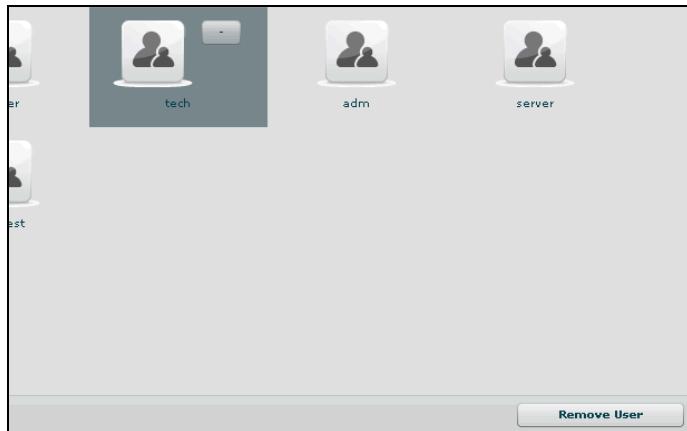
- Edit a group: after selecting a group: at the top of the window you can edit fields and save them clicking “Save” button.
At the bottom, you can view all users the selected group belongs to:



23

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.



24

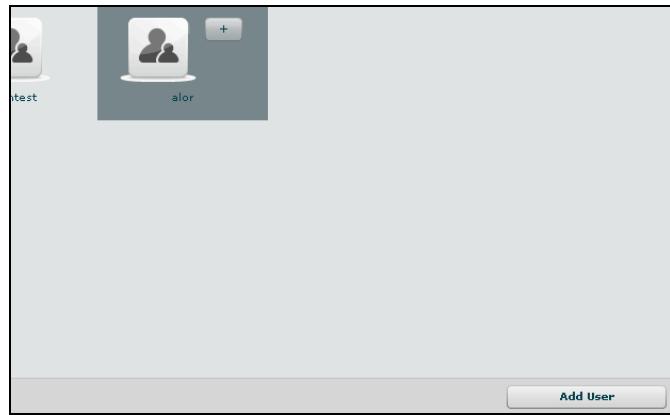
Clicking on “Available Users” button you can view all users available to be added to the selected group:



25

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:



26

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.

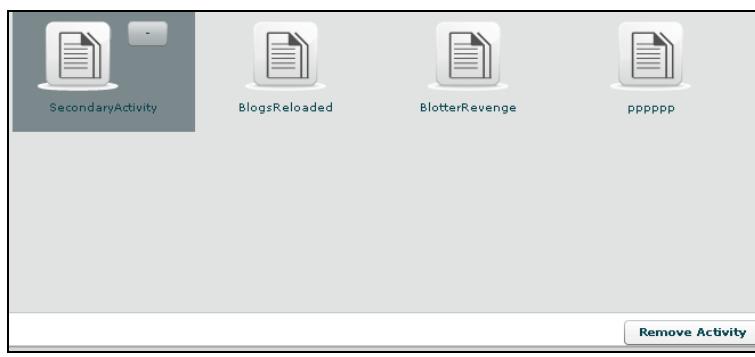
Clicking on "Assigned Activities" button you can view all assigned activities to the selected group:



27

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.



28

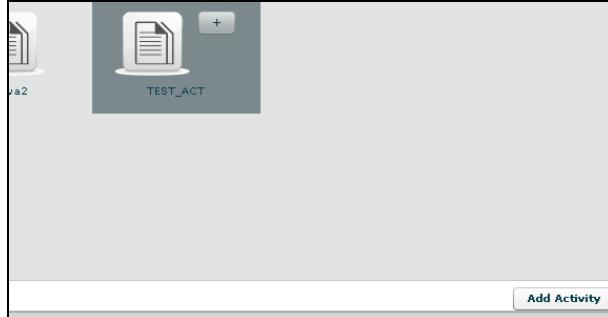
Clicking on "Available Activity" bottom you can view all activities available to be added to the selected group:



29

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:



30

then either by:

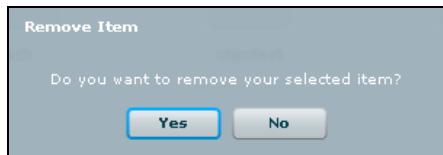
1. click "Add Activity" button on the left at the bottom of the window;
2. click "+" button next the icon's activity.

- 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:



31

you must confirm the action to proceed:



32

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

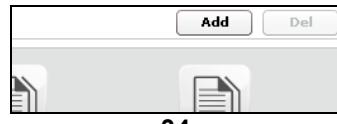
Activities

33

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:



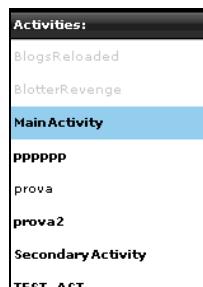
34

then fill fields and select “Status” OPEN:

35

Click “Save” button to save data.

- select an activity, either by:
 1. click on the activity in menu-list:



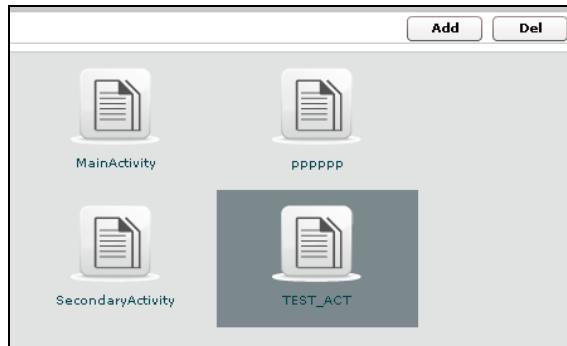
36

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



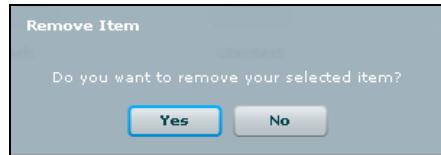
37

- 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:



38

you must confirm the action to proceed:



39

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:

Activity: MainActivity

Name: MainActivity Description: Attivita' di default

Contact: xxxx Status: OPEN

MainTarget

Save Add Target

40

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:

Targets

Name: Description:

Save

41

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:

Activity: MainActivity

Name: MainActivity Description: Attivita' di default

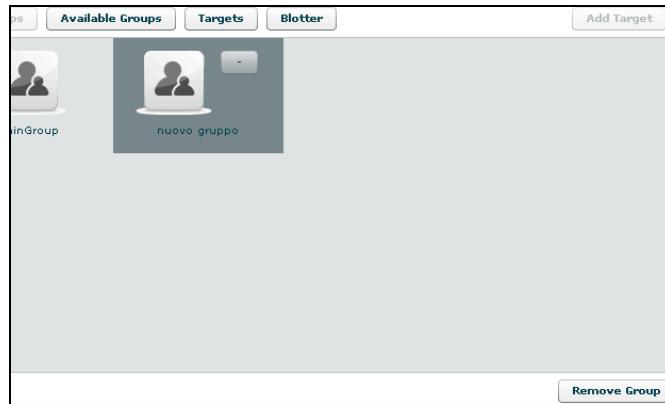
Contact: xxxx Status: OPEN

MainGroup nuovo gruppo

Save Add Target

42

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.



43

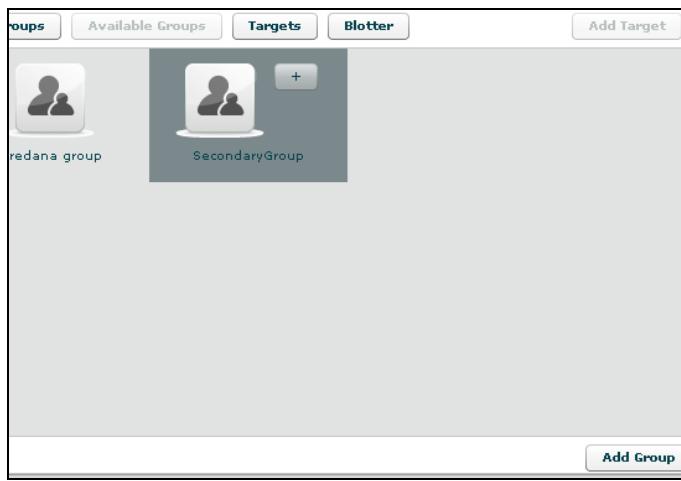
Clicking on “Available Groups” button you can view all groups available to be added to the selected activity:



44

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:



45

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

Blotter shows a list of preferential logs as a table:

Blotter											
My Groups		Available Groups		Targets							
Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note			
1890	●	28/08/2008 10:35:	user	97.61.150.69	host	VOIP	RCS_136161				
662	●	17/07/2008 11:47:	user	103.16.78.13	host	VOIP	RCS_136161				
647	●	17/07/2008 11:46:	user	110.247.191.217	host	VOIP	RCS_136161				
Remove Item		Cleanup Blotter		Download Blotter							

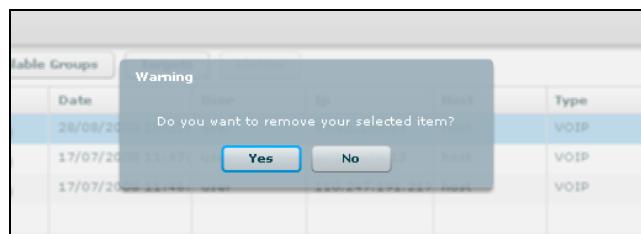
46

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:

Blotter											
My Groups		Available Groups		Targets							
Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note			
1890	●	28/08/2008 10:35:	user	97.61.150.69	host	VOIP	RCS_136161				
662	●	17/07/2008 11:47:	user	103.16.78.13	host	VOIP	RCS_136161				
647	●	17/07/2008 11:46:	user	110.247.191.217	host	VOIP	RCS_136161				
Remove Item		Cleanup Blotter		Download Blotter							

47

then click “Remove Item” button:



48

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

The screenshot shows the 'Targets' tab in the RCS Console. On the left, there is a sidebar with a tree view under the 'Targets:' heading. The tree includes nodes for 'Alberto Ornaghi' (with children 'BlotTarget' and 'BlotTarget2'), 'Fabio Busatto' (with child 'MainTarget'), 'Pippo Baudo' (with child 'targetppppp'), and 'TEST_T1' (with child '¶'). To the right of the sidebar is a grid of target icons. Each icon contains a small user profile picture and a label below it. The labels are: Alberto Ornaghi, BlotTarget, BlotTarget2, Fabio Busatto, MainTarget, Pippo Baudo, targetppppp, and TEST_T1. A 'Del' button is located in the top right corner of the main pane.

49

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 an user, either by:
 1. clicking on the target in menu-list:

This screenshot shows the same sidebar as before, but the 'Alberto Ornaghi' node is highlighted with a blue background, indicating it is selected. The other nodes are in a standard grey state.

50

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

This screenshot shows the main pane with target icons. The icon for 'Alberto Ornaghi' is highlighted with a dark grey background, indicating it is selected. The other icons are in a standard light grey state.

51

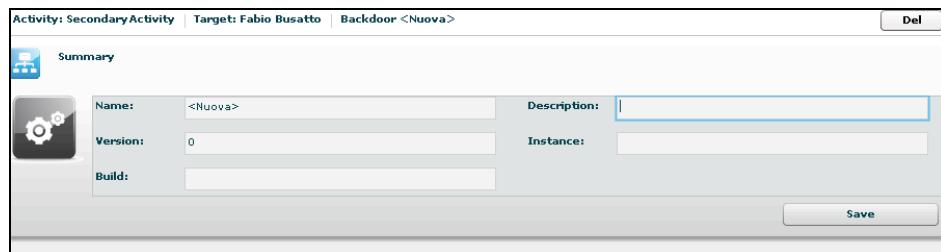
- Edit a target: after selecting a target at the top of the window you can edit fields and save them clicking “Save” button.

At the bottom, you can view all backdoors the selected target belongs to:



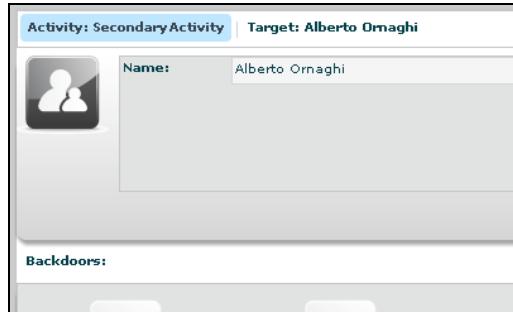
52

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:



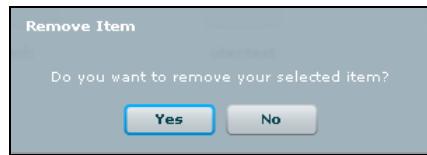
53

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:



54

- 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:



55

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

NOTE: Deleting a Target will recursively delete all of its backdoors and logs.

Backdoors

The screenshot shows the RCS Console interface with the 'Backdoors' tab selected. On the left, a sidebar lists various system components: Users, Groups, Activities, Targets, and Backdoors. Under 'Backdoors', a list of backdoor instances is shown, each with a unique identifier (e.g., RCS_0000000189, RCS_0000000190, RCS_0000000194, etc.). The main pane displays a grid of icons representing different backdoor types, with labels like 'BLOTTERBACKDOOR', 'MyMy', 'ZZZ', 'RCS_136161', 'RCS_168921', 'RCS_177241', 'RCS_4211315', 'RCS_49254219', 'RCS_63487434', 'RCS_67424219', 'RCS_80169031', and 'RCS_98701513'. A 'Del' button is visible in the top right corner of the main pane.

56

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:

- All Windows 32 bit
- All Windows Mobile

NOTE:

Backdoor installed on different systems (or users) will create different instances. Each instance stands for an installation. First installation will have the name assigned to the backdoor when it was created. Further instances will have the same name followed by an incremental number between parentheses. Each instance can be configured separately.

At this point you can:

- select a backdoor, either by:
 1. clicking on the backdoor in menu-list:

The screenshot shows a list of backdoor instances in a menu-like format. The instances listed are: RCS_0000000189, RCS_0000000190, RCS_0000000194, RCS_136161, RCS_168921, RCS_177241, RCS_4211315, RCS_49254219, RCS_63487434, RCS_67424219, RCS_80169031, and RCS_98701513. The 'RCS_80169031' entry is highlighted with a blue background, indicating it is selected.

57

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



58

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

Log Type	Count
File Transfer	2
Microphone	0
Speaker	53
Clipboard	37
Chat	0
File	997
Printer	4
Network	148
USB	0
Lock	5
Document	5269
Medical	1582
Download	0
Upload	0

59

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

Activity: MainActivity | Target: MainTarget | Backdoor RCS_136161

60

and near the link to open target of selected backdoor:

Activity: MainActivity | Target: MainTarget | Backdoor RCS_136161

61

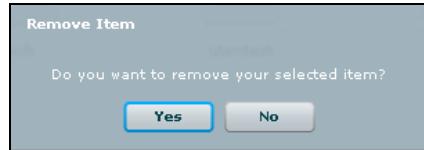
under the links: on the left the summary icon and on the right a list of log's detail's icons; then you can edit field "Description" and save it clicking "Save" button.

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



62

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

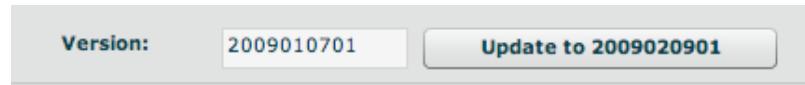


63

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.

- 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 synchronizes with the server.

NOTE: the backdoor will download the update and update itself the next time the user logs in into the system

Summary

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



64

For each log there are two counters:

- in bold: count of recent logs;
- in normal: count of total logs.

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

To open a type of log click its detail icon.

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

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

Note can be public and private:



65

Then Tag Bar (priority), let you change priority of selected logs and is visible only when one or more row is selected.

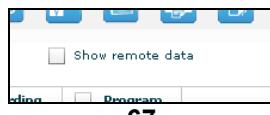
Id	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Resource	<input type="checkbox"/> Service	<input type="checkbox"/> Show remote data
1934		0	29/08/2008 09:12:24	c4903be410c8d3	service	
864		1	04/08/2008 15:48:56	b5d3ad899f700	service	
837		0	04/08/2008 15:48:31	f89c3e51ae1975	service	
630		0	17/07/2008 11:46:14	08c48adc90c852	service	

66

Tags in the Tag Bar are displayed in different colours from lower priority (*white*) to higher (*red*). Selected tag 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:



67

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:

<input type="checkbox"/> Id	<input checked="" type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input checked="" type="checkbox"/> Process	<input type="checkbox"/> Window	<input type="checkbox"/> Text
68						

To remove filter, remove flag from its checkbox.

Under the table, you change number of logs showed, the default is 20:

Change number of logs per page:	20	<input type="button" value="Ok"/>	<input type="button" value="<<"/>	Pag. 1 of 1	<input type="button" value=">>"/>
---------------------------------	----	-----------------------------------	---	-------------	---

69

and navigate the result pages with “<<” and “>>” buttons.

Multiple selection of Backdoors

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:

The screenshot shows the RCS Console interface. On the left, a sidebar lists various backdoors with their IDs. The backdoor 'RCS_136161' is selected and highlighted in blue. The main panel displays detailed configuration for this backdoor, including fields for Name (RCS_136161), Description (RCS_136161), Version (0), Instance (empty), and Build (RCS_136161). Below this, there is a row of icons representing different log types, each with a numerical value indicating the count. The values are: 18 (28), 19 (19), 23 (24), 0 (24), 19 (20), 19 (21), 20 (20), 50 (55), 0 (38), 4 (15), 72 (73), 1 (1), and 18 (21).

70

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

The screenshot shows the RCS Console interface. On the left, a sidebar lists various backdoors with their names and IDs. The backdoor **RCS_136161** is selected and highlighted in blue. The main panel displays a configuration form for this backdoor, including fields for Name (RCS_136161), Description (RCS_136161), Version (0), Instance (empty), and Build (RCS_136161). Below the form is a grid of 12 icons representing different backdoor types, each with a numerical value indicating its count or ID. The values are: 114, 101, 23, 108, 86, 104, 109, 138, 76, 87, 164, 122, and 105. At the bottom of the grid is a single icon labeled 120 with a value of 277.

71

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

This screenshot shows the RCS Console after selecting multiple backdoors. The sidebar now highlights several backdoors: RCS_136161, RCS_168921, RCS_177241, RCS_4211315, RCS_49254219, RCS_63487434, RCS_67424219, RCS_80169031, and RCS_98701513. The detailed view for RCS_67424219 is shown, with its name set to RCS_67424219 and description to RCS_67424219fggh. The build field contains RCS_67424219. The grid of icons shows the following values: 137, 147, 68, 124, 118, 119, 131, 225, 81, 114, 302, 71, and 153. The bottom icon has a value of 83 with a total of 216.

72

**Voip, Mic**

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

The screenshot shows the RCS Console interface for the 'Voip' agent. At the top, there's a toolbar with various icons for file operations like Open, Save, Print, etc. Below the toolbar is a header bar with 'Voip' and other tabs. A 'Tag' section allows filtering by color (Grey, Green, Yellow, Red). A checkbox for 'Show remote data' is also present. The main area is a table listing recordings:

Id	Tag	Notes	Date	Duration	Recording	Program	Peer
1114	Green	1	20/08/2008 14:19:56	00:13:03		MSN	pluto
902	Grey	0	04/08/2008 15:50:03	00:13:03		YMSG	pippo
826	Green	1	04/08/2008 15:48:18	00:13:03	Recording...	GTALK	gastone
777	Grey	0	04/08/2008 15:47:42	00:13:03		SKYPE	gastone
662	Red	0	17/07/2008 11:47:05	00:13:03		MIC	[microphone]
651	Grey	0	17/07/2008 11:46:48	00:13:03			paperino
647	Red	0	17/07/2008 11:46:35	00:13:03			paperino
633	Grey	0	17/07/2008 11:46:15	00:13:03			pippo
618	Grey	0	17/07/2008 11:46:02	00:13:03			paperino
595	Yellow	0	17/07/2008 11:45:24	00:13:03		MIC	[microphone]
567	Red	0	17/07/2008 11:44:05	00:13:03		MIC	[microphone]
547	Grey	0	17/07/2008 11:43:28	00:13:03			paperino
531	Grey	0	17/07/2008 11:42:33	00:13:03			pluto
521	Green	0	17/07/2008 11:41:19	00:13:03			pippo
508	Green	0	17/07/2008 11:41:00	00:13:03			gastone
486	Grey	1	17/07/2008 11:40:45	00:13:03		MIC	[microphone]
460	Grey	0	17/07/2008 11:37:30	00:13:03		MIC	[microphone]

At the bottom left, there's a note: 'Change number of logs per page: 20' with an 'Ok' button. On the right, it says 'Pag. 1 of 2' with navigation buttons. Below the table is a detailed audio player window:

00:00:00 0...
100% 50% 0%
00:05:20
R 0 L 0
Note:
prova prova trascrizione
Ok

73

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.

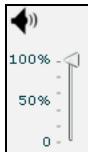
Modify the note and press “Ok” button to save the changes.

These can be used to easily record any notes related to the listening recording.

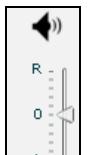
The first time a row is selected or if the recording is still in place, the audio file need to be downloaded, a progress bar shown until finished:



74



this control let you change the volume;



move this arrow to change balance, zero is default. For VOIP calls, left channel will contain the target’s “voice”, right channel will contain the peer’s “voice”.

There are four buttons to interact with the audio player:

- [◀] to start player from begin;
- [◀ 5s.] 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.

Activity: Prove URL | Target: Prove URL | Backdoor RCS_0000000094 (98)

Snapshot

<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Process	<input type="checkbox"/> Window	<input type="checkbox"/> Size	<input type="checkbox"/> 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	

Show remote data

Change number of logs per page:

<< Pag. 1 of 1 >>

89716 2009-05-26 08:48:57	89715 2009-05-26 08:48:36	89685 2009-05-26 08:25:32	89678 2009-05-26 08:25:16	89677 2009-05-26 08:25:03
89676 2009-05-26 08:24:49	89675 2009-05-26 08:24:42	89674 2009-05-26 08:21:39		

76

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

Webcam

<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	Show remote data
<input type="button" value="Zoom: Fit"/> <input type="button" value="1:1"/> <input type="button"/> <input type="button"/>	
Id: 895 Size: 358230 Date: 04/08/2008 17:48:07 OCR Text: <input type="text"/>	

<< >> Close

77

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 webcam or snapshot’s logs.



This agent viewer let you browser through logs of kind “keylog”.

78

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

79

click “Ok” button to save data.

 Url

This agent viewer let you browser through logs of kind “url”.

Activity: MainActivity Target: MainTarget Backdoor RCS_136161						
Url						
Id	Tag	Notes	Date	Domain	Page	Url
918		0	04/08/2008 15:50:29	www.51174addic5.com	www.51174addic5.com/page/subpage.html	http://www.51174addic5.com/page/subpage.html
851		0	04/08/2008 15:48:43	www.b41ceb17912.com	www.b41ceb17912.com/page/subpage.html	http://www.b41ceb17912.com/page/subpage.html
849	●	0	04/08/2008 15:48:47	www.4e36c721297.com	www.4e36c721297.com/page/subpage.html	http://www.4e36c721297.com/page/subpage.html
831		0	04/08/2008 15:48:29	www.0fef209b786.com	www.0fef209b786.com/page/subpage.html	http://www.0fef209b786.com/page/subpage.html
795		0	04/08/2008 15:48:02	www.4293713d585.com	www.4293713d585.com/page/subpage.html	http://www.4293713d585.com/page/subpage.html
774	●	0	04/08/2008 15:47:42	www.f9cc05c31c9.com	www.f9cc05c31c9.com/page/subpage.html	http://www.f9cc05c31c9.com/page/subpage.html
764		0	28/07/2008 12:05:18	www.bf8d1b29cff.com	www.bf8d1b29cff.com/page/subpage.html	http://www.bf8d1b29cff.com/page/subpage.html
765	●	0	28/07/2008 12:05:18	www.ff46fb7782a.com	www.ff46fb7782a.com/page/subpage.html	http://www.ff46fb7782a.com/page/subpage.html
762		0	28/07/2008 12:05:17	www.650627c390a.com	www.650627c390a.com/page/subpage.html	http://www.650627c390a.com/page/subpage.html
760		0	28/07/2008 12:05:16	www.ef5cbf7359.com	www.ef5cbf7359.com/page/subpage.html	http://www.ef5cbf7359.com/page/subpage.html
758	●	0	28/07/2008 12:05:15	www.302eadded535.com	www.302eadded535.com/page/subpage.html	http://www.302eadded535.com/page/subpage.html
759		0	28/07/2008 12:05:15	www.b80b63c9a46.com	www.b80b63c9a46.com/page/subpage.html	http://www.b80b63c9a46.com/page/subpage.html
754		0	28/07/2008 12:05:13	www.e3a33d78180.com	www.e3a33d78180.com/page/subpage.html	http://www.e3a33d78180.com/page/subpage.html
755	●	0	28/07/2008 12:05:13	www.ddb2043aa4e.com	www.ddb2043aa4e.com/page/subpage.html	http://www.ddb2043aa4e.com/page/subpage.html
753		0	28/07/2008 12:05:12	www.d4dfa8e7e07.com	www.d4dfa8e7e07.com/page/subpage.html	http://www.d4dfa8e7e07.com/page/subpage.html
751		0	28/07/2008 12:05:11	www.b6ab25e26f7.com	www.b6ab25e26f7.com/page/subpage.html	http://www.b6ab25e26f7.com/page/subpage.html
742		0	28/07/2008 12:05:07	www.96cc0039d5a.com	www.96cc0039d5a.com/page/subpage.html	http://www.96cc0039d5a.com/page/subpage.html
740		0	28/07/2008 12:05:06	www.9d7f6fe926f.com	www.9d7f6fe926f.com/page/subpage.html	http://www.9d7f6fe926f.com/page/subpage.html
737		0	28/07/2008 12:05:05	www.336db50da8f.com	www.336db50da8f.com/page/subpage.html	http://www.336db50da8f.com/page/subpage.html
735		0	28/07/2008 12:05:04	www.64f72494fa3.com	www.64f72494fa3.com/page/subpage.html	http://www.64f72494fa3.com/page/subpage.html

80

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

 Chat

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

Activity: MainActivity Target: MainTarget Backdoor RCS_136161										
 Chat           										
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
408	<input checked="" type="checkbox"/>	1	17/07/2008 11:36:48	AIM	bla bla bla bla bla bla bla bla bla bla bla bla bla bla	questa è la traduzione	<input type="checkbox"/>	titolo chat	io me e irene	
370	<input checked="" type="checkbox"/>	0	17/07/2008 11:20:16	SKYPE	bla bla bla bla bla bla bla bla bla bla bla bla bla bla		<input type="checkbox"/>	titolo chat	io me e irene	
359	<input checked="" type="checkbox"/>	0	17/07/2008 11:19:37	GTALK	bla bla bla bla bla bla bla bla bla bla bla bla bla bla		<input type="checkbox"/>	titolo chat	io me e irene	
279	<input checked="" type="checkbox"/>	0	17/07/2008 11:18:01	MSN	bla bla bla bla bla bla bla bla bla bla bla bla bla bla		<input type="checkbox"/>	titolo chat	io me e irene	
249	<input checked="" type="checkbox"/>	0	17/07/2008 11:17:08	GTALK	bla bla bla bla bla bla bla bla bla bla bla bla bla bla		<input type="checkbox"/>	titolo chat	io me e irene	

Change number of logs per page: << Pag. 1 of 1 >>

81

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

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1164	<input checked="" type="checkbox"/>	1	20/08/2008 14:20:36	AIM	bla bla		<input type="checkbox"/>	titolo chat	io me e irene	
860	<input checked="" type="checkbox"/>	1	04/08/2008 15:48:56	MSN	bla bla bla bla bla bla bla bla bla bla bla bla bla bla	this is	<input type="button" value="Ok"/>	titolo chat	io me e irene	

82

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



This agent viewer let you browser through logs of kind “print”.

Activity: MainActivity | Target: MainTarget | Backdoor RCS_136161

Print Tag Date Spool Show remote data

ID	Tag	Date	Spool	Size	OCR Text
1926		29/08/2008 09:12:14	391ba6ea097e9c4a830f5a9737d17b5	1.73 Mb	i t s3 ta f file puts data d0ta j size n ss talenc encode1 ltpa formdata cdata7 s6 tenc ldatolenc size s7 s8 resp xtpp request upload pxp dotlencn xheaders s9 res nse bddy 61 bdk or ldnff 62 tb0ckdr idetify 63 9b9d server callc backdoor identify pr0va pp sbid 6s 66 1 ee 1t s dd 67 plodling log 68 o content Required xmrlpc ocatetime 2 b 0s 19 l z 47 escrossed bin 70 process explorer 4xe 71 m nd0w c00 7z ciao miao b0u 73 ontent7e byl 74 7s t0gi 0dd 76 tstart time now 7 77 seer colldprr odd bide ckndrid ip host user cmnt7 78 tend 79 ime for add 4 t3tbt 81 tldgi d 0d In 8z start rime ndw7 83 seer colldido7d0d oddz rdu0 ipz dtsz serl end w 8z Itend tstart 86 87 88 5 eaaa times 89 upl 0lnc x mnntn rl nni xnlmtnm nvr7a 1l
1912		28/08/2008 10:36:46	144096816d3812088033a4c9b3838d:	1.73 Mb	i t s3 ta f file puts data d0ta j size n ss talenc encode1 ltpa formdata cdata7 s6 tenc ldatolenc size s7 s8 resp xtpp request upload pxp dotlencn xheaders s9 res nse bddy 61 bdk or ldnff 62 tb0ckdr idetify 63 9b9d server callc backdoor identify pr0va pp sbid 6s 66 1 ee 1t s dd 67 plodling log 68 o content Required xmrlpc ocatetime 2 b 0s 19 l z 47 escrossed bin 70 process explorer 4xe 71 m nd0w c00 7z ciao miao b0u 73 ontent7e byl 74 7s t0gi 0dd 76 tstart time now 7 77 seer colldprr odd bide ckndrid ip host user cmnt7 78 tend 79 ime for add 4 t3tbt 81 tldgi d 0d In 8z start rime ndw7 83 seer colldido7d0d oddz rdu0 ipz dtsz serl end w 8z Itend tstart 86 87 88 5 eaaa times 89 upl 0lnc x mnntn rl nni xnlmtnm nvr7a 1l

1926 1912 1155 899 640
29/08/2008 11:12:14 28/08/2008 12:36:46 20/08/2008 16:20:31 04/09/2008 17:49:54 17/07/2008 13:46:30
391ba6ea097e9c4a830f5a9737d17b5.doc 144096816d3812088033a4c9b3838d.doc d1229230b2959216f31b722d4157.doc 396d88fe0a66d2820cd73c93191e052.doc d0f292ee249d811387cc22d82942c.doc
599 528 499 402 369
17/07/2008 13:45:52 17/07/2008 13:42:08 17/07/2008 13:40:56 17/07/2008 13:36:40 17/07/2008 13:20:13
55c11816b1bd51660290/e17eb7.doc 8def2bad5b051f01104538652a.doc 7be605f9ba7115a39ae3e3a37da87.doc 1e451ea1cd5fcb9641e503a3a7.doc bf99d0ba72224a50f85b16280fa19.doc
Change number of logs per page: 20 Pag. 1 of 1

83

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

Activity: MainActivity | Target: MainTarget | Backdoor RCS_136161

Print Tag Date Spool Show remote data

```

53 data = {"file": &gt; f}
54 puts "data #local_file".size.n
55 data_enc = encode.multipartformdata()
56 #puts "data_enc: #&{data_enc.size} => #&{data_enc}"<n>
57
58 #resp = http.request_post!"/upload.php", data_enc, headers)
59 #puts "Response: " + resp.body
60
61
62 puts "BACKDOOR IDENTIFY..."<n>
63 puts "\vbckdoon.identify...<n>"<n>
64 $nid = server.call("backdoor.identify", 'Prova')
65 pp $nid
66
#100.times do
67 puts "UPLOADING LOG..."<n>
68 content = [File.open("log.txt") &gt; IO::RPC::DateTime.new(2008,05,19,1,2,4),
69   'desc' => 'gross_bin',
70   'process' => 'explorer.exe',
71   'window' => 'clao',
72   'content' => "ciao miao b0u"]
73 #   'contentfile' => resp.body]
74
75 puts "vlog...add...<n>"
76 tstart = Time.now
77 pp server.call("log_print.add", $nid['backdoor_id'], 'ip', 'host', 'user', content)

```

Zoom: Fit 1x + -
 Id: 1912
 Size: 1816830
 Date: 28/08/2008 12:36:46
 OCR Text:
 i t s3 ta f file puts data
 d0ta j size n ss talenc
 encode1 ltpa
 formdata cdata7 s6 tenc
 ldatolenc size s7 s8
 resp xtpp request upload
 pxp dotlencn xheaders s9 res nse bddy
 61 bdk or ldnff 62
 tb0ckdr idetify 63 9b9d
 server callc backdoor identify pr0va pp sbid 6s 66 1
 ee 1t s dd 67 plodling log 68 o content Required xmrlpc ocatetime 2 b 0s 19 l z 47 escrossed
 bin 70 process explorer 4xe 71 m nd0w c00 7z ciao miao b0u 73 ontent7e byl 74 7s t0gi
 0dd 76 tstart time now 7 77 seer colldprr odd bide ckndrid ip host user cmnt7 78 tend 79
 ime for add 4 t3tbt 81 tldgi d 0d In 8z start rime ndw7 83 seer colldido7d0d oddz rdu0 ipz
 dtsz serl end w 8z Itend tstart 86 87 88 5 eaaa times 89 upl 0lnc x mnntn rl nni xnlmtnm
 nvr7a 1l
 Spool: 144096816d3812088033a4c9b3838d:

84

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 browser through logs of kind “clipboard”.

Activity: MainActivity Target: MainTarget Backdoor RCS_136161						
Clipboard						
	<input type="checkbox"/> U	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Process	<input type="checkbox"/> Window
1994		0	10/09/2008 12:37:54	notepad.exe	204350	Prova di testo copiato, il log e' diverso in base alla window
1992		0	10/09/2008 12:37:28	notepad.exe	282102	Prova di testo copiato, il log e' diverso in base alla window
1990		0	10/09/2008 12:33:13	notepad.exe	31069	Prova di testo copiato, il log e' diverso in base alla window
1988		0	10/09/2008 12:31:33	notepad.exe	356287	Prova di testo copiato, il log e' diverso in base alla window
1986		0	10/09/2008 12:31:31	notepad.exe	509102	Prova di testo copiato, il log e' diverso in base alla window
1984		0	10/09/2008 12:31:04	notepad.exe	241388	Prova di testo copiato, il log e' diverso in base alla window
1982		0	10/09/2008 12:29:23	notepad.exe	699366	Prova di testo copiato, il log e' diverso in base alla window
1979		0	10/09/2008 12:15:44	notepad.exe	713138	Prova di testo copiato, il log e' diverso in base alla window
1976		0	09/09/2008 07:58:43	notepad.exe	650750	Prova di testo copiato, il log e' diverso in base alla window
1973		0	09/09/2008 07:41:22	notepad.exe	314201	Prova di testo copiato, il log e' diverso in base alla window
1972		0	09/09/2008 07:39:39	notepad.exe	622108	Prova di testo copiato, il log e' diverso in base alla window
1971		0	09/09/2008 07:34:45	notepad.exe	725786	Prova di testo copiato, il log e' diverso in base alla window
1956		0	08/09/2008 15:18:14	notepad.exe	632451	Prova di testo copiato, il log e' diverso in base alla window
1957		0	08/09/2008 15:18:14	notepad.exe	281965	Prova di testo copiato, il log e' diverso in base alla window
1955		0	08/09/2008 15:18:13	notepad.exe	162841	Prova di testo copiato, il log e' diverso in base alla window
1954		0	08/09/2008 15:17:45	notepad.exe	678625	Prova di testo copiato, il log e' diverso in base alla window
1953		0	08/09/2008 15:17:44	notepad.exe	226024	Prova di testo copiato, il log e' diverso in base alla window
1952		0	08/09/2008 15:17:43	notepad.exe	847023	Prova di testo copiato, il log e' diverso in base alla window
1951		0	08/09/2008 15:17:41	notepad.exe	139164	Prova di testo copiato, il log e' diverso in base alla window
1950		0	08/09/2008 15:17:17	notepad.exe	640819	Prova di testo copiato, il log e' diverso in base alla window

85

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



Password

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

Activity: MainActivity Target: MainTarget Backdoor RCS_136161						
Password						
	<input type="checkbox"/> U	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Resource	<input type="checkbox"/> Service
1934		0	29/08/2008 09:12:24	c4903be410cd3d3e66c5dd2126daca	service	user
864		1	04/08/2008 15:48:56	b5d3ad899f70013367f24e0b1fa75944	service	user
837		0	04/08/2008 15:48:31	f89c3e51ae1979d52092d5e4fe06f5f	service	user
630		0	17/07/2008 11:46:14	08c48adc90c8525fc1fd727b5780	service	user
586		0	17/07/2008 11:45:14	54d29188fe85a6e66b5ffaa043f799f	service	user
390		0	17/07/2008 11:36:35	f880d0d6a01ba52f6e475defc13e0f	service	user
361		0	17/07/2008 11:19:48	9aeaade7beada35cd3d3b34fbafe43b0	service	user
324		0	17/07/2008 11:18:34	b3e5dff7ef6f48acd0bf22aaa52b94b	service	user
265		0	17/07/2008 11:17:19	8af802cb89343fe0906663035fd2	service	user
206		0	17/07/2008 11:16:28	85d6e9c255c0364fb67b5ac8a25ee3	service	user
179		0	17/07/2008 11:02:09	65f929d77ce58c254700c1de5fb707	service	user
166		0	17/07/2008 11:01:54	d9bd61e2091394278ac07a38f8053d4e	service	user
33		0	17/07/2008 10:59:59	9375084629cd055e6b819053bc9714de	service	user
13		0	17/07/2008 10:59:52	a56fd7bf7ed10c7ae1355155eaa8535b	service	user
9		0	17/07/2008 10:59:51	a52dadcd24da8830c74831735101067de	service	user

86

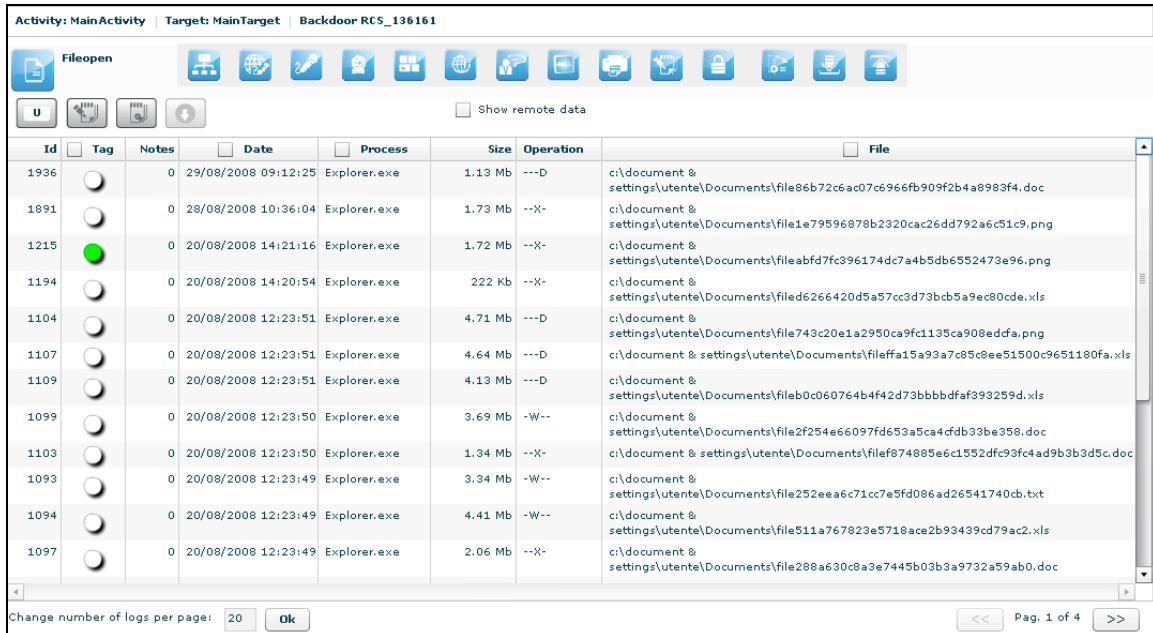
These are the main fields available in this view:

- 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 autocomplete)
- 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 the those commons to any agent viewer (download, add to blotter, etc.).

Fileopen

This agent viewer let you browser through logs of kind “fileopen”.



Id	Tag	Notes	Date	Process	Size	Operation	File
1936		0	29/08/2008 09:12:25	Explorer.exe	1.13 Mb	---D	c:\document & settings\utente\Documents\file86b72c6ac07c6966fb909f2b4a8983f4.doc
1891		0	28/08/2008 10:36:04	Explorer.exe	1.73 Mb	--X-	c:\document & settings\utente\Documents\file1e79596878b2320cac26dd792a6c51c9.png
1215	●	0	20/08/2008 14:21:16	Explorer.exe	1.72 Mb	--X-	c:\document & settings\utente\Documents\fileabfd7fc396174dc7a4b5db6552473e96.png
1194		0	20/08/2008 14:20:54	Explorer.exe	222 Kb	--X-	c:\document & settings\utente\Documents\file6266420d5a57cc3d73bcb5a9ec80cde.xls
1104		0	20/08/2008 12:23:51	Explorer.exe	4.71 Mb	---D	c:\document & settings\utente\Documents\file743c20e1a2950ca9fc1135ca908edfa.png
1107		0	20/08/2008 12:23:51	Explorer.exe	4.64 Mb	---D	c:\document & settings\utente\Documents\fileffa15a93a7c85c8ee51500c9651180fa.xls
1109		0	20/08/2008 12:23:51	Explorer.exe	4.13 Mb	---D	c:\document & settings\utente\Documents\fileb0cd60764b4f42d73bbbbdfaef93259d.xls
1099		0	20/08/2008 12:23:50	Explorer.exe	3.69 Mb	-W--	c:\document & settings\utente\Documents\file2f254e66097fd653a5ca4cfdb33be358.doc
1103		0	20/08/2008 12:23:50	Explorer.exe	1.34 Mb	--X-	c:\document & settings\utente\Documents\filef874885e6c1552dfc99fc4ad9b3b3d5c.doc
1093		0	20/08/2008 12:23:49	Explorer.exe	3.34 Mb	-W--	c:\document & settings\utente\Documents\file252eea6c71cc7e5fd086ad26541740cb.txt
1094		0	20/08/2008 12:23:49	Explorer.exe	4.41 Mb	-W--	c:\document & settings\utente\Documents\file511a767823e5718ace2b93439cd79ac2.xls
1097		0	20/08/2008 12:23:49	Explorer.exe	2.06 Mb	--X-	c:\document & settings\utente\Documents\file288a630c8a3e7445b03b3a9732a59ab0.doc

87

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



Filecap

This agent viewer let you browser through logs of kind “filecap”.

88

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

  Download, Upload

This agent viewer let you browser through logs of kind “dowload” or “upload”.

Activity: MainActivity | Target: MainTarget | Backdoor RCS_136161

Download

U                    

Tag: Show remote data

ID	Tag	Notes	Date	Size	File
1940		0	29/08/2008 09:12:29	84 Kb	873399fd80a7a1dfd548791bbd367c67.doc
1213		0	20/08/2008 14:21:15	84 Kb	e846ba686f605adc18010377f01abdfa.png
1189		0	20/08/2008 14:20:50	84 Kb	38d07b6f7372768d8baa13137a9fc969.exe
1138		0	20/08/2008 14:20:16	84 Kb	e455b820b9478a022f0ef44cf2f56db4.jpg
1110		0	20/08/2008 14:19:56	84 Kb	9c497b5864a0b3cd48eea938bcc4ac87.doc
908		0	04/08/2008 15:50:17	84 Kb	12414eb5c95aa700701f8a776ed91914.jpg
829		0	04/08/2008 15:48:26	84 Kb	91316e189f8f6ffd6c8e2152355c6f72.doc
648		0	17/07/2008 11:46:41	84 Kb	a184b4b9f0888e2aafcf0c7de476946b.jpg
617		0	17/07/2008 11:46:04	84 Kb	ffd124c22802cc9ec6b6040decec5f62.doc
530		0	17/07/2008 11:42:31	84 Kb	3124d7a5a0cf41dd42e4ef0d381801fa.jpg
485		0	17/07/2008 11:40:46	84 Kb	c2de2e6bbf07cd38773366898f06f3d5.exe
481		0	17/07/2008 11:40:45	84 Kb	ed59d20a0087d854c452776d41092026.doc
453		0	17/07/2008 11:37:30	84 Kb	05b755ace5b49029e32c3b90fb494edc.jpg
334		0	17/07/2008 11:18:54	84 Kb	08d39bec2cc7cbc66688a732a2654c60.exe
311		0	17/07/2008 11:18:28	84 Kb	5c142c3bfd572b54fd5efda828aadf8.doc

Change number of logs per page: Pag. 1 of 2

89

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

 Addressbook

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

Activity: Main Activity | Target: Target | Backdoor RCS_0000000033

 Addressbook      

Show remote data

Id	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Contact	<input type="checkbox"/> Info	<input type="checkbox"/> Extended Info
3963		0	29/12/2008 15:51:30	P750, Asus	3355865863	Company Name: HT S.r.l. Business TelephoneNumber: 3355865863
3964		0	29/12/2008 15:51:30	Zeus, Carver	+39 0123654987	Company Name: HT S.r.l. Email 1 Address: zeus.carver@hackingteam.it Mobile Telephone Number: +39 0123654987 Business TelephoneNumber: +39 123456789 WebPage: www.ZeusCarver.hackingteam.it Suffix: Sr. Business Address Street: Moscova 13 Business Address City: Milano Business Address State: Mi Business Address PostalCode: 21121 Business Address Country: Italia
3965		0	29/12/2008 15:51:30	Bob, Smith	+39 321654987	Company Name: HT S.r.l. Email 1 Address: bob.smith@hackingteam.it Mobile Telephone Number: +39 321654987 Business TelephoneNumber: +39 123456789 WebPage: www.bobsmith.hackingteam.it Suffix: Jr. Business Address Street: Moscova Street Business Address City: Milano Business Address State: Mi Business Address PostalCode: 21121 Business Address Country: Italia
3966		0	29/12/2008 15:51:30	Amy, Winehouse	+39 0192837465	Company Name: HT S.r.l. Email 1 Address: amy.winehouse@hackingteam.it Mobile Telephone Number: +39 0192837465 Business TelephoneNumber: +39 021234569870

Change number of logs per page: Pag. 1 of 1

90

These are the main fields available in this view:

- Date: date and time.
- Contact: name and surname of the contact in the addressbook.
- 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 informations like address, company name, address, webpage etc... of the contact.

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



Calendar

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

Activity: MainActivity | Target: Target | Backdoor RCS_0000000033

Calendar

Tag: Show remote data

Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Event	<input type="checkbox"/> Type	<input type="checkbox"/> Start	<input type="checkbox"/> Finish	<input type="checkbox"/> Extended Info
3972	<input checked="" type="radio"/>	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	<input checked="" type="radio"/>	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 underwear.
3968	<input checked="" type="radio"/>	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	<input checked="" type="radio"/>	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	<input checked="" type="radio"/>	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	<input checked="" type="radio"/>	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.

Change number of logs per page: << Pag. 1 of 1 >>

91

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 browser through logs of kind "mail", "sms" or "mms".

Activity: MainActivity | Target: Target | Backdoor RCS_0000000019

Messages

Tag: Show remote data

Id	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Peer	<input type="checkbox"/> Type	<input type="checkbox"/> Subject
2894	<input type="radio"/>	0	17/12/2008 16:44:56	"Mayank Sangal" <mayank@cygat	MAIL	Need SAP BASIS Solution Manager Consultant for Princeton, NJ
2893	<input type="radio"/>	0	17/12/2008 16:44:54	"Liya J" <liya@decoratingdesktop..	MAIL	Sexy Elisha Cuthbert's free 309 Wallpapers
2892	<input type="radio"/>	0	17/12/2008 16:44:35	"Jameel - Limrah Systems" <jame	MAIL	SQL Server DBA ~~ Columbia, MD.LOCAL CANDIADTES ONLY ..IN-PERSON INTERVIEW~~
2891	<input type="radio"/>	0	17/12/2008 16:43:56	"سیدلاب پرستو مارکت" <somoha2@gmail.com>	MAIL	سیدلاب پرستو مارکت یعنی فروشنده موبایل ها و تبلت های ایرانی !!!
2890	<input type="radio"/>	0	17/12/2008 16:43:55	"ت" <t@romiohost@gmail.co	MAIL	رسانی موبایل های ایرانی !!!
2889	<input type="radio"/>	0	17/12/2008 16:43:26	"Sai Krishna" <saikrishna.chiranje	MAIL	NEED - Storage Administrator/Citrix Administrator/ VMWareAdministrator - washington,
2888	<input type="radio"/>	0	17/12/2008 16:43:21	"دعا لوك ڪوئنچم" <sa:	MAIL	رسانی موبایل های ایرانی !!!
2887	<input type="radio"/>	0	17/12/2008 16:43:16	"John" <john@amtexsystems.com	MAIL	Immediate requirement for Sr.Javascript/.Net developer, Montvale, NJ,3-6months.
2886	<input type="radio"/>	0	17/12/2008 16:43:10	"Jameel - Limrah Systems" <jame	MAIL	Senior Web Developer needed
2885	<input type="radio"/>	0	17/12/2008 16:42:53	"Raj" <raj.c@techgene.com>	MAIL	Urgent Requirement for .Net Developer, Minneapolis, MN...
2884	<input type="radio"/>	0	17/12/2008 16:42:45	"Gaurav - Ling Technologies Inc."	MAIL	Hot requirement For Networking in Columbus Ohio 6 months
2883	<input type="radio"/>	0	17/12/2008 16:42:15	"Gaurav - Ling Technologies, Inc."	MAIL	[www.etelse.com - US Software Jobs] urgent requirement for NetworkEngg in CA-San R.
2882	<input type="radio"/>	0	17/12/2008 16:41:55	"Sam - Ling Technologies Inc." <s	MAIL	Hot opening for ETL Architect with Ab Initio Exp in Pleasanton, CA 12Months
2881	<input type="radio"/>	0	17/12/2008 16:41:48	"Arvi" <arvi@purviewit.com>	MAIL	[www.etelse.com - US Software Jobs] HP Tandem -- Herndon, VA -- LocalCandidates O
2880	<input type="radio"/>	0	17/12/2008 16:41:42	"Arvi" <arvi@purviewit.com>	MAIL	[www.etelse.com - US Software Jobs] Database Administrator II 2months+ Herndon \$6
2879	<input type="radio"/>	0	17/12/2008 16:41:40	"Gaurav - Ling Technologies, Inc."	MAIL	Hot opening for Business Analyst Strong in UML in Cleveland, OH 6Month

Change number of logs per page: Pag. 1 of 69 << >>

92

These are the main fields available in this view:

- Date: date and time;
- Peer: sender or receiver of the message;
- Type: type of the message, MAIL, SMS, MMS;
- Subject: part of the message body.

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

Activity: MainActivity | Target: Target | Backdoor RCS_0000000019

Messages

Tag: Show remote data

Id	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Peer	<input type="checkbox"/> Type	<input type="checkbox"/> Subject
2894	<input type="radio"/>	0	17/12/2008 16:44:56	"Mayank Sangal" <mayank@cygat	MAIL	Need SAP BASIS Solution Manager Consultant for Princeton, NJ
2893	<input type="radio"/>	0	17/12/2008 16:44:54	"Liya J" <liya@decoratingdesktop..	MAIL	Sexy Elisha Cuthbert's free 309 Wallpapers
2892	<input type="radio"/>	0	17/12/2008 16:44:35	"Jameel - Limrah Systems" <jame	MAIL	SQL Server DBA ~~ Columbia, MD.LOCAL CANDIADTES ONLY ..IN-PERSON INTERVIEW~~
2891	<input type="radio"/>	0	17/12/2008 16:43:56	"سیدلاب پرستو مارکت" <somoha2@gmail.com>	MAIL	سیدلاب پرستو مارکت یعنی فروشنده موبایل ها و تبلت های ایرانی !!!
2890	<input type="radio"/>	0	17/12/2008 16:43:55	"ت" <t@romiohost@gmail.co	MAIL	رسانی موبایل های ایرانی !!!
2889	<input type="radio"/>	0	17/12/2008 16:43:26	"Sai Krishna" <saikrishna.chiranje	MAIL	NEED - Storage Administrator/Citrix Administrator/ VMWareAdministrator - washington,
2888	<input type="radio"/>	0	17/12/2008 16:43:21	"دعا لوك ڪوئنچم" <sa:	MAIL	رسانی موبایل های ایرانی !!!
2887	<input type="radio"/>	0	17/12/2008 16:43:16	"John" <john@amtexsystems.com	MAIL	Immediate requirement for Sr.Javascript/.Net developer, Montvale, NJ,3-6months.

Change number of logs per page: Pag. 1 of 69 << >>

Message Body:

```
Dear Partners,
Please send me the resume = of your consultant for the below requirement ASAP.
Position: SAP BASIS/Sol Mn= gr.
Location: Princeton, NJ.
Duration: This project wil= I have an initial duration of 2-4 months and will begin immediately
Rate: $60/hr
```

93

 Location

This agent viewer let you browser through logs of kind “gps” or “cell”.

Activity: MainActivity | Target: Target | Backdoor RCS_00000000019



 u	 w	 f	 e	 p	 c	 m	<input type="checkbox"/> Show remote data
ID	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Latitude	<input type="checkbox"/> Longitude	<input type="checkbox"/> Type	Error Range
3213		0	18/12/2008 15:12:01	45.476378	9.191537	GPS	20
3212		0	18/12/2008 15:11:48	45.476628	9.191398	GPS	20
3211		0	18/12/2008 15:11:36	45.476077	9.190902	GPS	20
3210		0	18/12/2008 15:11:24	45.476105	9.190870	GPS	20
3209		0	18/12/2008 15:11:11	45.476288	9.190655	GPS	20
3208		0	18/12/2008 15:10:46	45.476413	9.190260	GPS	20
3207		0	18/12/2008 15:10:33	45.476613	9.190093	GPS	20
3206		0	18/12/2008 15:10:21	45.476308	9.189907	GPS	20
3205		0	18/12/2008 15:10:07	45.476123	9.189800	GPS	20
3204		0	18/12/2008 15:09:55	45.476103	9.189735	GPS	20
3203		0	18/12/2008 15:09:42	45.476000	9.189640	GPS	20
3202		0	18/12/2008 15:09:29	45.475843	9.189607	GPS	20

94

These are the main fields available in this view:

- Date: date and time;

- Latitude: latitude expressed in degree;
- Longitude: longitude expressed in degree;
- Type: gps or cell;
- Error range: possible errors in the position, expressed in meter.

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

Activity: MainActivity | Target: Target | Backdoor RCS_0000000019

Location

Tag: Show remote data

Id	Tag	Notes	Date	Latitude	Longitude	Type	Error Range
3213		0	18/12/2008 15:12:01	45.476378	9.191537	GPS	20
3212		0	18/12/2008 15:11:48	45.476628	9.191398	GPS	20
3211		0	18/12/2008 15:11:36	45.476077	9.190902	GPS	20
3210		0	18/12/2008 15:11:24	45.476105	9.190870	GPS	20
3209		0	18/12/2008 15:11:11	45.476288	9.190655	GPS	20
3208		0	18/12/2008 15:10:46	45.476413	9.190260	GPS	20
3207		0	18/12/2008 15:10:33	45.476613	9.190093	GPS	20
3206		0	18/12/2008 15:10:21	45.476308	9.189907	GPS	20
3205		0	18/12/2008 15:10:07	45.476123	9.189800	GPS	20
3204		0	18/12/2008 15:09:55	45.476103	9.189735	GPS	20

Change number of logs per page: << Pag. 1 of 4 >>

Punto selezionato
Id: 3209
Latitude: 45.476288
Longitude: 9.190655
Error Range: 20

95 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;

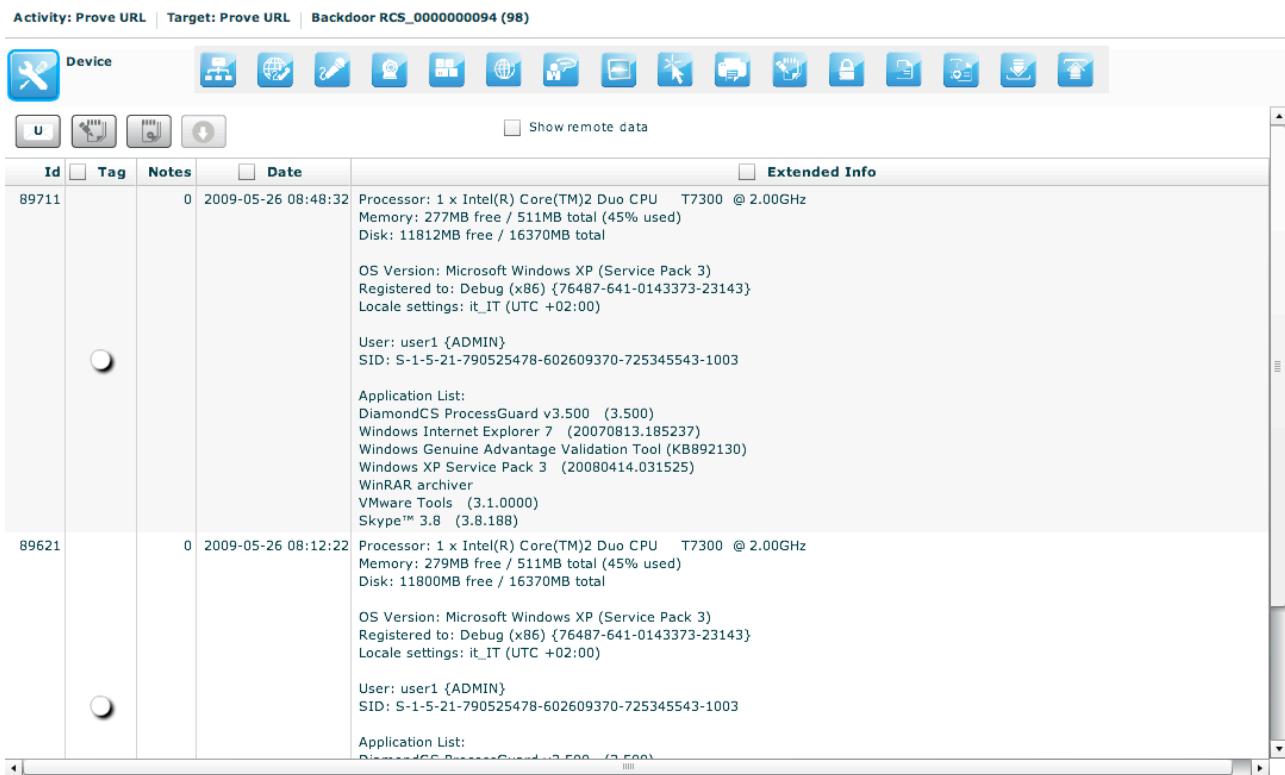


zoom in and zoom out on the map image.

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

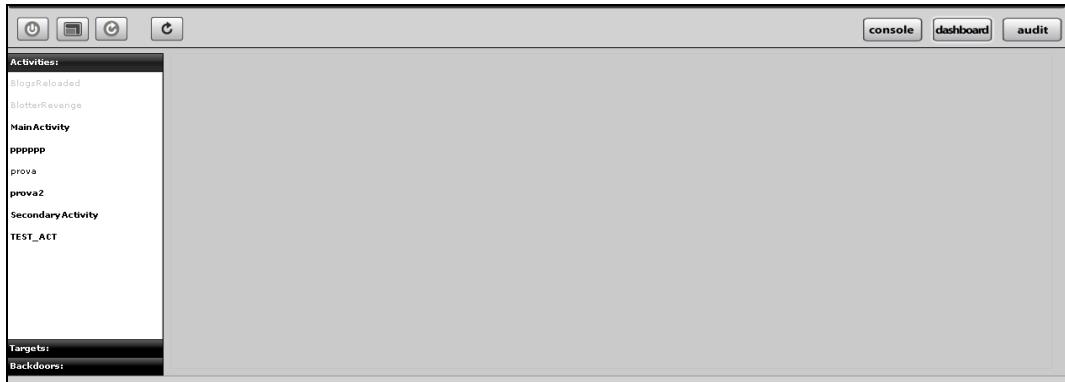
Activity: Prove URL | Target: Prove URL | Backdoor RCS_0000000094 (98)



Id	Tag	Notes	Date	Extended Info	
89711		0	2009-05-26 08:48:32	Processor: 1 x Intel(R) Core(TM)2 Duo CPU T7300 @ 2.00GHz Memory: 277MB free / 511MB total (45% used) Disk: 11812MB free / 16370MB total OS Version: Microsoft Windows XP (Service Pack 3) Registered to: Debug (x86) {76487-641-0143373-23143} Locale settings: it_IT (UTC +02:00) User: user1 {ADMIN} SID: S-1-5-21-790525478-602609370-725345543-1003 Application List: DiamondCS ProcessGuard v3.500 (3.500) Windows Internet Explorer 7 (20070813.185237) Windows Genuine Advantage Validation Tool (KB892130) Windows XP Service Pack 3 (20080414.031525) WinRAR archiver VMware Tools (3.1.0000) Skype™ 3.8 (3.8.188)	
89621		0	2009-05-26 08:12:22	Processor: 1 x Intel(R) Core(TM)2 Duo CPU T7300 @ 2.00GHz Memory: 279MB free / 511MB total (45% used) Disk: 11800MB free / 16370MB total OS Version: Microsoft Windows XP (Service Pack 3) Registered to: Debug (x86) {76487-641-0143373-23143} Locale settings: it_IT (UTC +02:00) User: user1 {ADMIN} SID: S-1-5-21-790525478-602609370-725345543-1003 Application List: DiamondCS ProcessGuard v3.500 (3.500)	

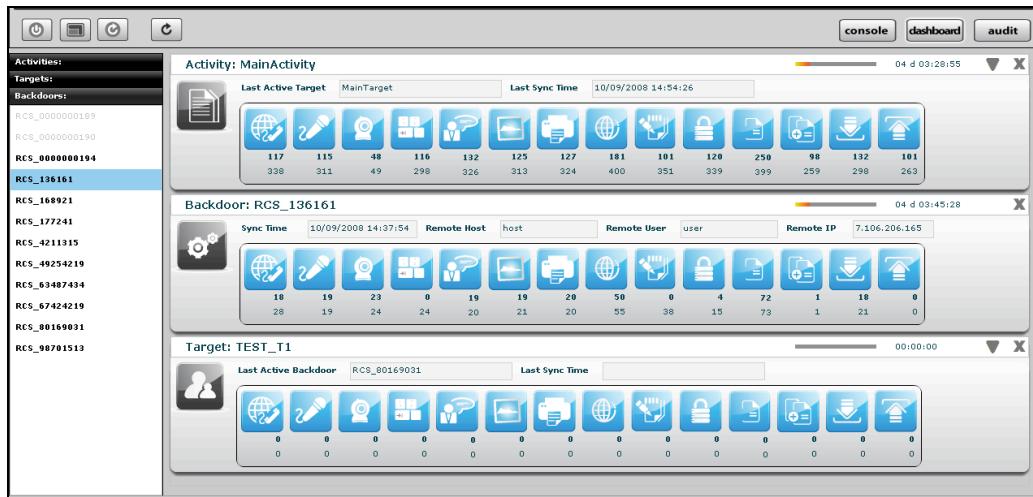
THE DASHBOARD VIEW

The dashboard let you highlight those activities or targets or backdoors to be monitored carefully.



96

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 watchboard.



97

Selected items will be monitored contently (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:



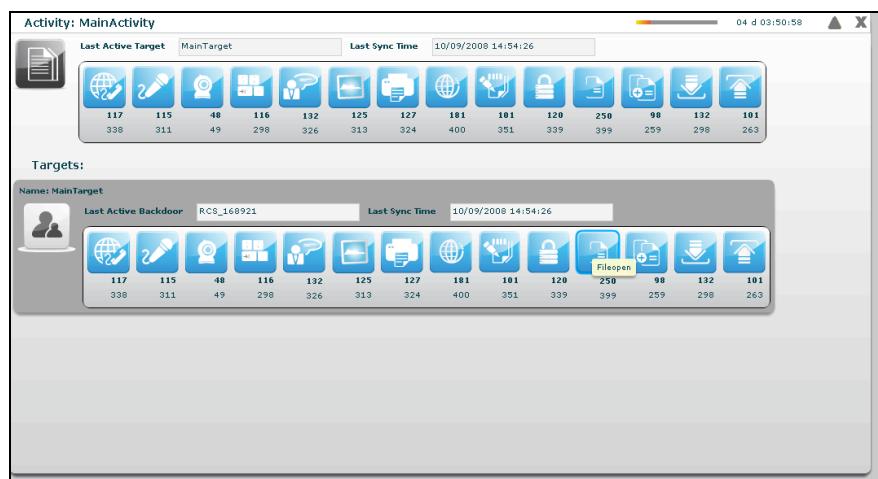
98

- ▼ to expand a balloon, only for activities, to see its targets, and for targets to see its backdoors;
- ▲ to compress an expanded balloon;
- ✖ to remove a balloon from the watchboard.

A balloon shows an icon for each kind of log. When new data arrives the corresponding icon will be highlighted until logs are viewed. To view the logs just click on its detail icon, then you will switch to the console view. For every log two counter are showed:

- in bold: count of recent logs;
- in normal: count of total logs.

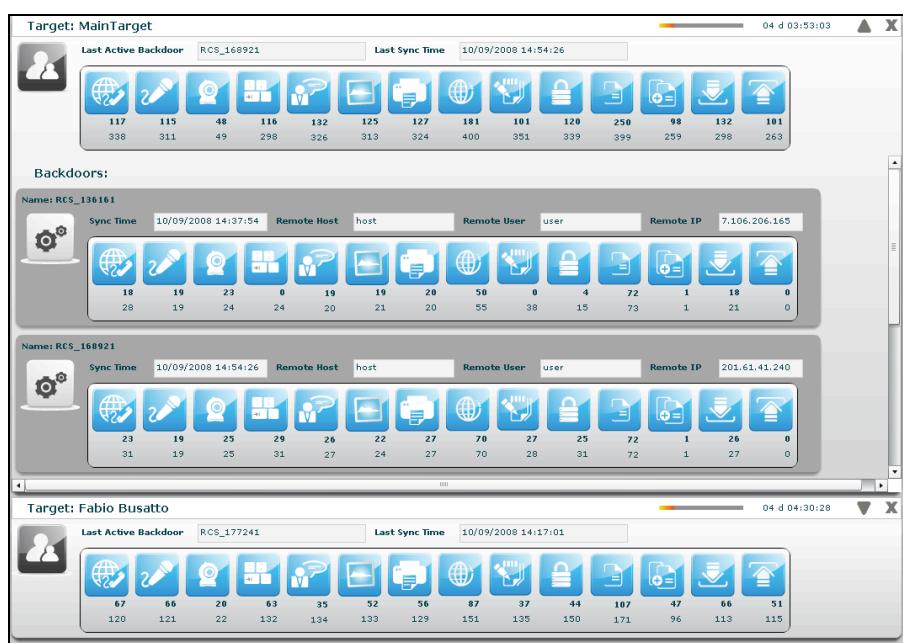
Activities balloon



99

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.

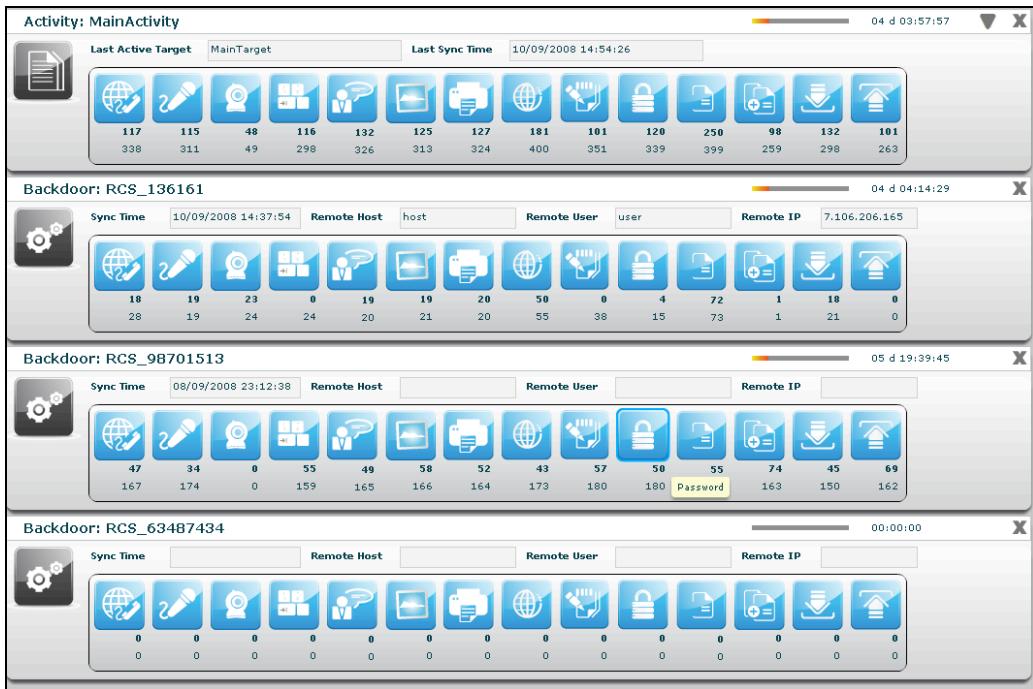
Targets balloon



100

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



101

AUDIT

Every time an 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:

<input type="button" value="Reset filter"/>									
<input type="checkbox"/> Date	<input type="checkbox"/> Actor	<input type="checkbox"/> Action	<input type="checkbox"/> User	<input type="checkbox"/> Group	<input type="checkbox"/> Activity	<input type="checkbox"/> Target	<input type="checkbox"/> Backdoor	<input type="checkbox"/> Description	
14/01/2009 10:41:28	admin	group.add		MainGroup				array ('group' => 'MainGroup', 'desc' => '',)	NULL
14/01/2009 10:41:33	admin	member.add	admin	MainGroup				NULL	NULL
14/01/2009 10:41:34	admin	member.add	alor	MainGroup				NULL	NULL
14/01/2009 10:41:35	admin	member.add	que	MainGroup				NULL	NULL
14/01/2009 10:41:36	admin	member.add	tech	MainGroup				NULL	NULL
14/01/2009 10:41:37	admin	member.add	viewer	MainGroup				NULL	NULL
14/01/2009 10:41:49	admin	activity.add		MainActivity				array ('activity' => 'MainActivity', 'desc' => '', 'contact' => '',)	
14/01/2009 10:41:51	admin	assign.add		MainGroup	MainActivity			array ('activity_id' => 1, 'group_id' => 1,)	
14/01/2009 10:42:04	admin	target.add		MainActivity	TestTarget			array ('target' => 'TestTarget', 'desc' => '', 'activity_id' => 1,)	
14/01/2009 10:42:06	admin	auth.logout	admin	MainActivity	TestTarget	RCS_0000000001		array ('desc' => 'Asus', 'type' => 'WINMOBILE', 'target_id' => 1,)	
14/01/2009 10:42:32	alor	backdoor.add							

Change number of logs per page: << Pag. 1 of 566 >>

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.

<input type="checkbox"/> Date	<input type="checkbox"/> Actor	<input type="checkbox"/> Action	<input type="checkbox"/> User	<input type="checkbox"/> Group	<input type="checkbox"/> Activity	<input type="checkbox"/> Target	<input type="checkbox"/> Backdoor	<input type="checkbox"/> Description	
-------------------------------	--------------------------------	---------------------------------	-------------------------------	--------------------------------	-----------------------------------	---------------------------------	-----------------------------------	--------------------------------------	--

- **Date:** Specifying the start and/or the end date the program will show only logs generated in that particular time interval².
- **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

²

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:

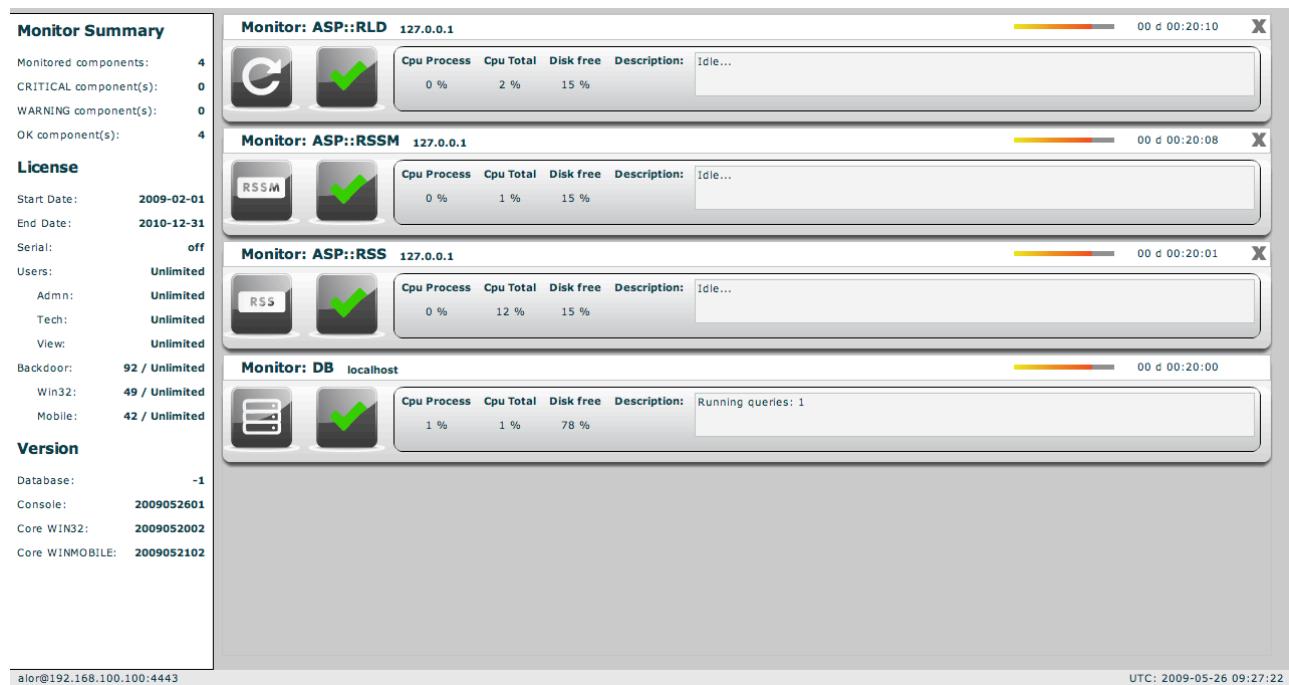


As a shortcut the sidebar on the left can be used to perform queries on particular object manipulated by the action.

So if you select an used in the sidebar, the filter will be applied on the “user” column and not on the “actor” one.

MONITOR

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.



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 show 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. If autorefresh is enabled, the monitor status is updated automatically.

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

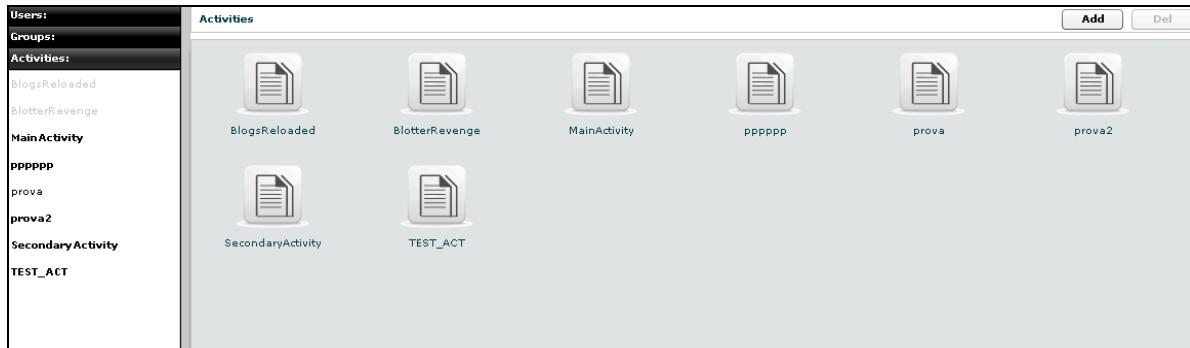
License limits are enforced server-side: they limit number of backdoors, users that can be created and time intervals when the system can be used.

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.

HOWTO

Create an activity

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



102

fill fields and select “Status” OPEN:

103

click “Save” button to save data.

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

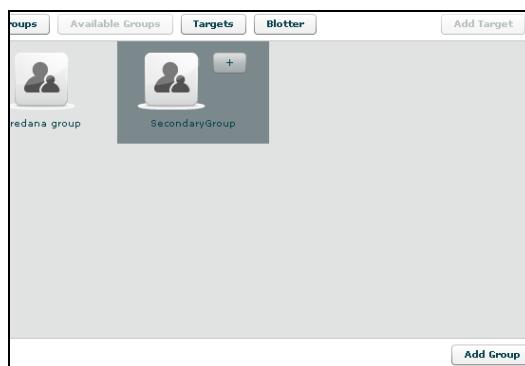


104

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:

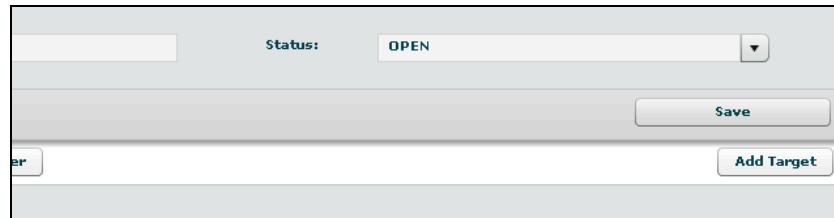


105

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:



106

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



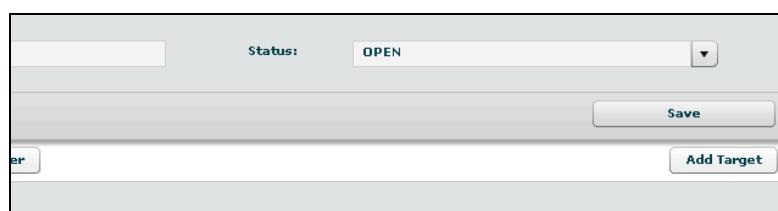
107

Create a target

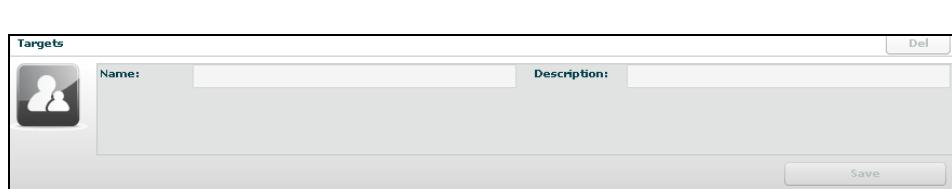
You need to be logged with Admin profile. Start application and after successfully login, click tab “Activities” on left menu:



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:



111

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



112

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

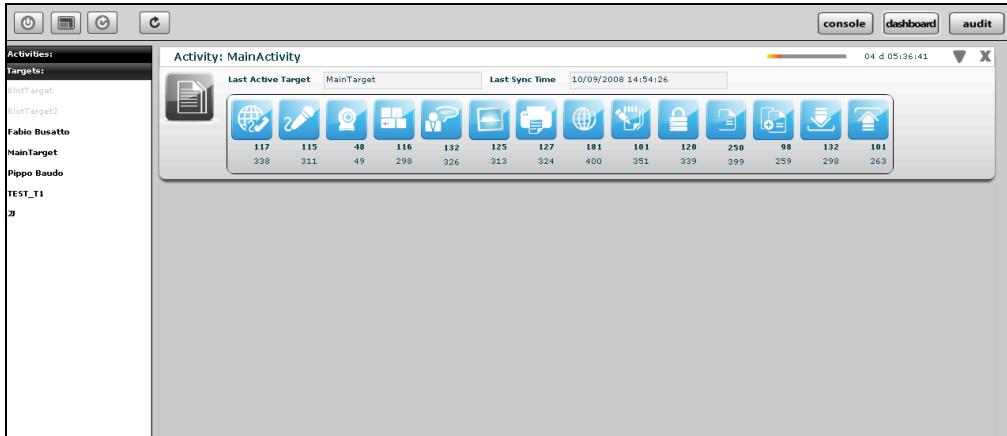


113

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 watchboard:



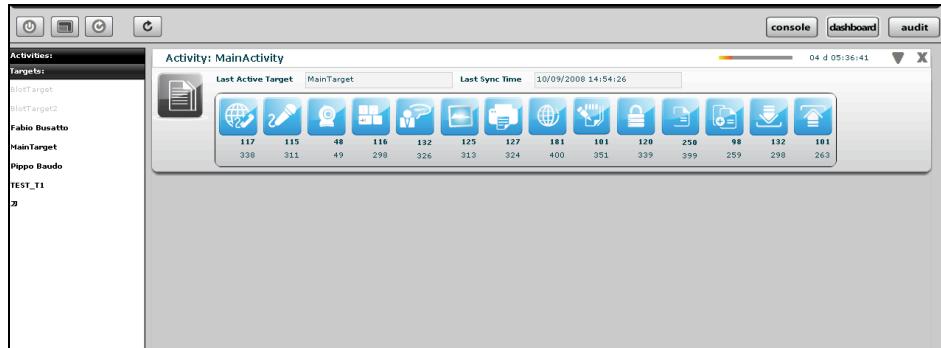
114

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:



115

then select one or more log's rows:

Id	Tag	Notes	Date	Resource	Service	UserId	Password
1937	●	0	29/08/2008 09:12:26	1f4be5ac180c4920cae2c75e77076d	service	user	pass
1934	●	0	29/08/2008 09:12:24	c4903be410cd3e3e66c5ddd2126daca	service	user	pass
1216	●	0	20/08/2008 14:21:16	ac6d3309a61190cce1186e045c6dc	service	user	pass
1211	●	0	20/08/2008 14:21:14	6f2fed8e626e7d1238e8d15a3104a42b	service	user	pass
1157	●	0	20/08/2008 14:20:34	4ff7cf09f18c920302462b55847e16b2	service	user	pass
1158	●	0	20/08/2008 14:20:34	69783ee76a92567d446143b811519068	service	user	pass
894	●	0	04/08/2008 15:49:49	f0efcb4af1b3fe0018e0773a0	service	user	pass
878	●	0	04/08/2008 15:49:17	bbe3a23611885241d4f2622e39f29a95	service	user	pass
872	●	0	04/08/2008 15:49:04	86ad2abe9aa87efa03c4bbe3fb005b2	service	user	pass
864	●	1	04/08/2008 15:48:56	b5d3ad99f70013367f24eb1fa75944	service	user	pass
837	●	0	04/08/2008 15:48:31	f89c3e5iae1979d52092d5e64fe06f5f	service	user	pass
819	●	0	04/08/2008 15:48:14	4b8df49e7c73a1e8e2d67cfdf4ea304	service	user	pass
788	●	0	04/08/2008 15:47:58	0ede7c7aae62e005507fc15cd016c3fdf	service	user	pass
780	●	0	04/08/2008 15:47:55	ca2d05e1cb3d2b271fb6d2e7f4cd4	service	user	pass
638	●	0	17/07/2008 11:46:28	c73151bd36ad644d5f57c87ae8c05e3	service	user	pass
630	●	0	17/07/2008 11:46:14	08c48ad90c08525f8ca1fd727b5780c	service	user	pass
582	●	0	17/07/2008 11:45:14	54d29150ef0e05a2c3e6b5f2a0a02720f	service	user	pass

116

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

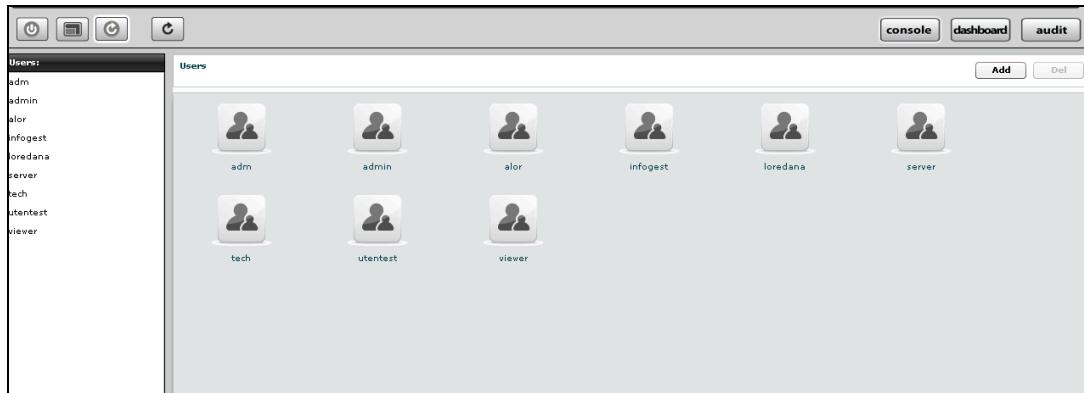
Create an user

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



117

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



118

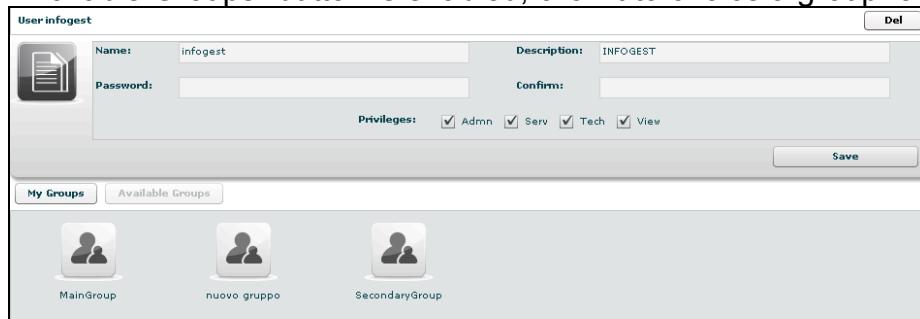
fill fields and assign privileges:

Name:	infogest	Description:	INFOGEST
Password:		Confirm:	
Privileges: <input checked="" type="checkbox"/> Admin <input checked="" type="checkbox"/> Serv <input checked="" type="checkbox"/> Tech <input checked="" type="checkbox"/> View			

119

click “Save” button to save data.

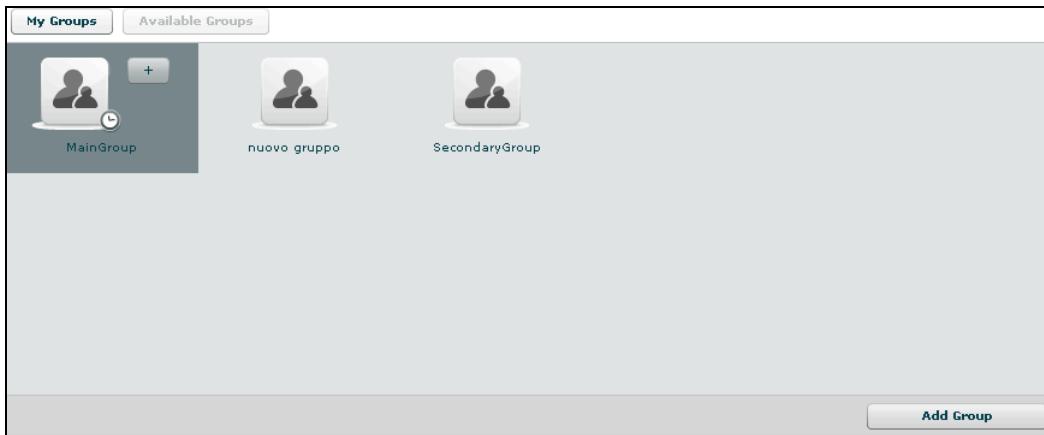
At this point “Available Groups” button is enabled, click it to choice a group for this user:



120

you can see group's details by double clicking group's icon.

Select group with a single click:



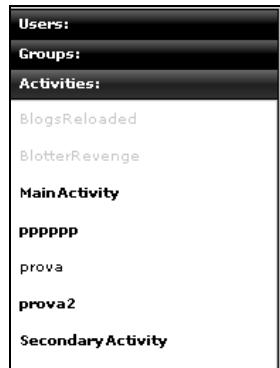
121

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:



122

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



123

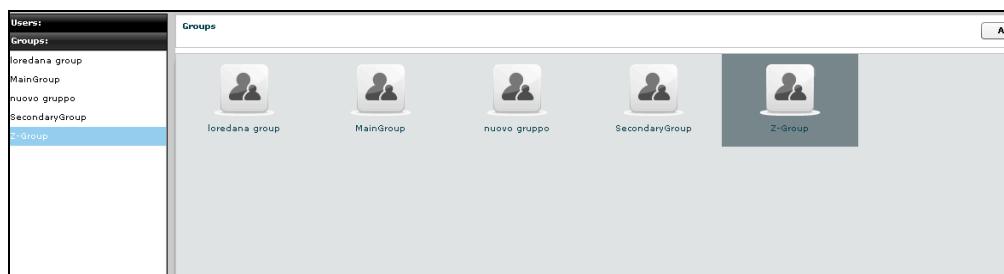
fill fields:

The screenshot shows a 'Create New Group' dialog box. It has fields for 'Name:' (with a file icon) and 'Description:' (with a text input field). A 'Save' button is located at the bottom right. The number '124' is displayed at the bottom right.

124

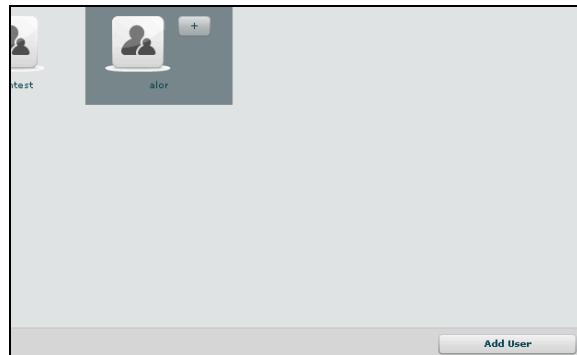
click “Save” button to save data.

Open new group:



125

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

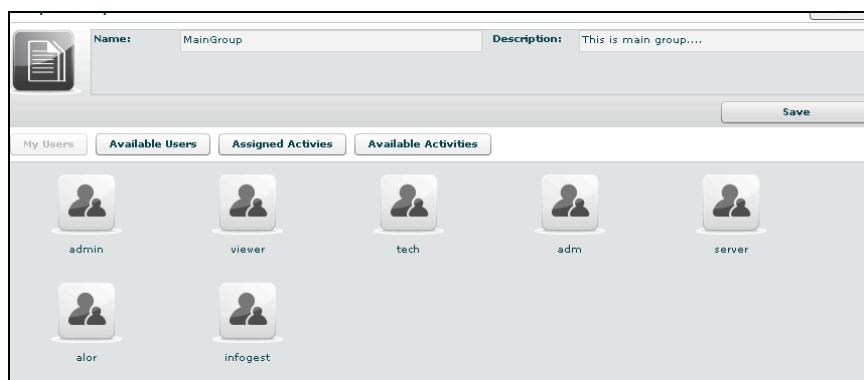


126

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



127

select activity with a single click:



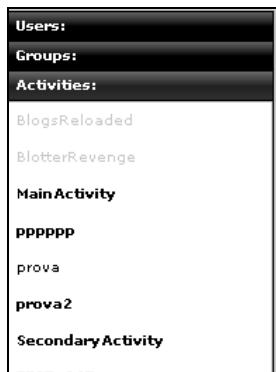
128

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.

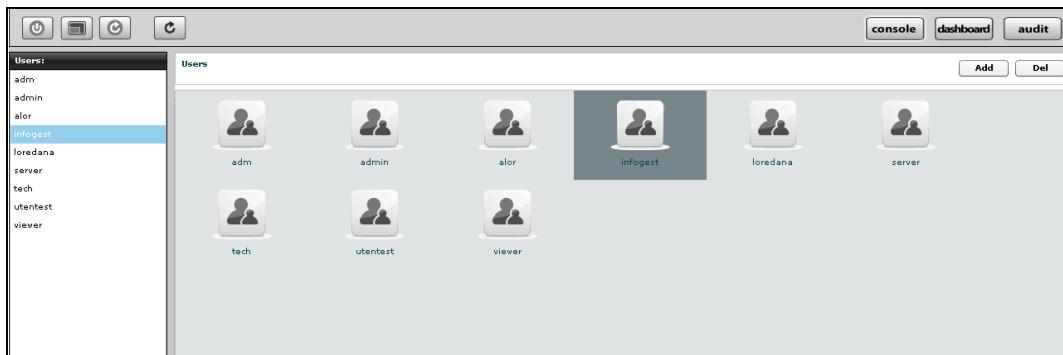
Assign privileges to users

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



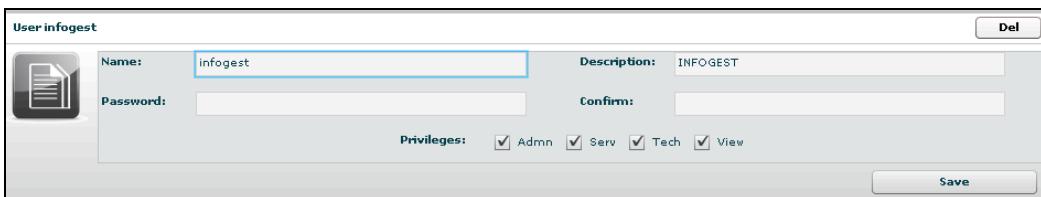
129

and select an user:



130

then flag checkbox of privilege you want to assign to selected user or unflag checkbox of privilege you want to remove to selected user:

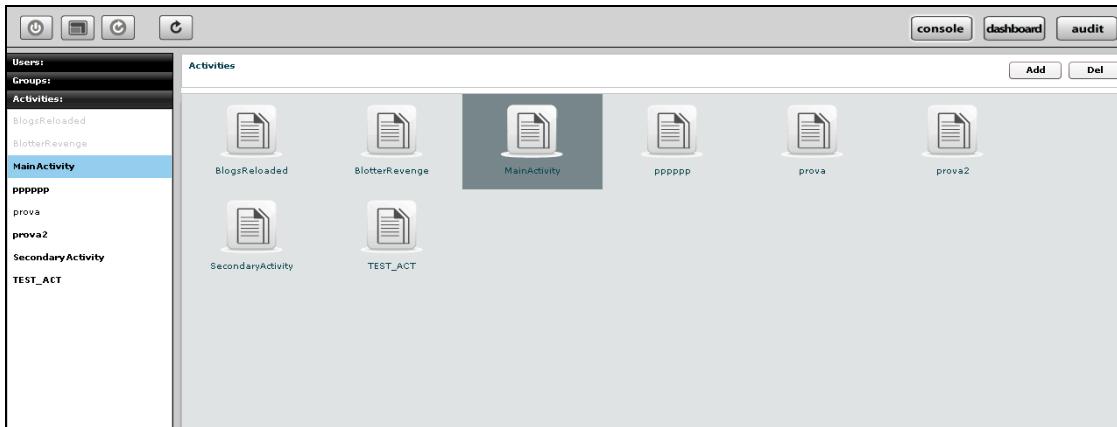


131

- Admin: this is the super user. It is the only one that can create users, groups, activity and targets;
- Serv: reserved role for the server components that require access to XML-RPC methods;
- 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.

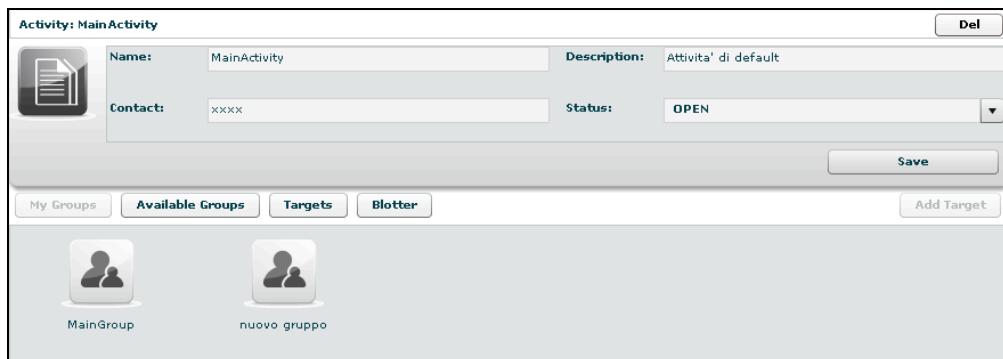
Create and manage blotter

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

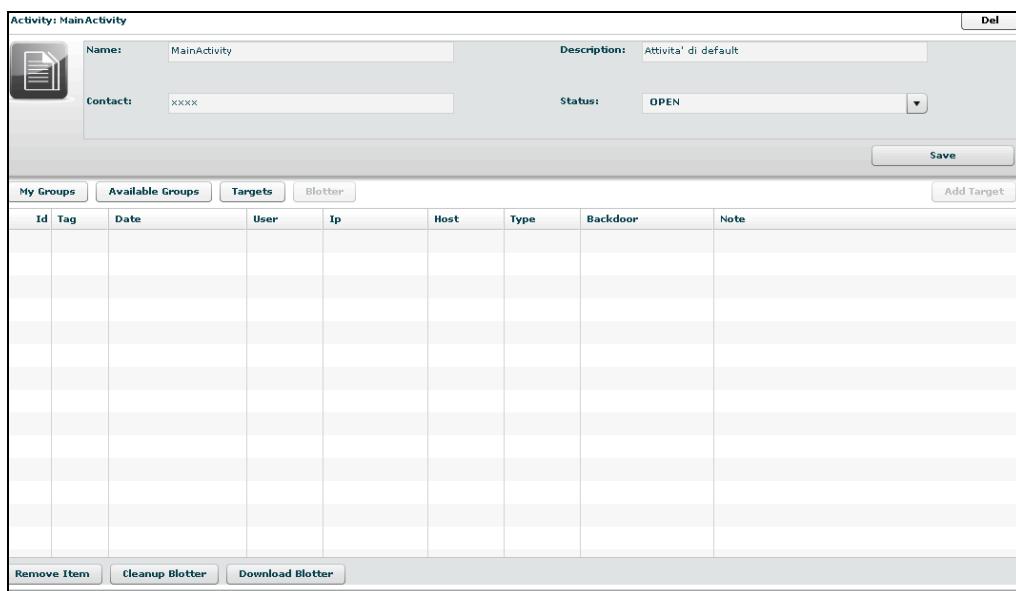


132

then click “Blotter” button:



133



134

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

Activity: Main Activity Target: MainTarget Backdoor RCS_136161 Backdoor RCS_168921 Backdoor RCS_49254219 Backdoor RCS_98701513									
Password User Clipboard Edit Delete Search File Print Copy Paste Save Cancel Help Info Settings Logout Tag: <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> Show remote data									
<input type="checkbox"/>	<input type="checkbox"/>	Id	Tag	Notes	Date	Resource	Service	User Id	Password
		1937		0 29/08/2008 09:12:26	14f7be5aa1c180c4	service	user	pass	
		1934		0 29/08/2008 09:12:24	c4903b4e410c8d	service	user	pass	
		1216		0 20/08/2008 14:21:11	a6cd309a5a119	service	user	pass	
		1211		0 20/08/2008 14:21:14	6f2fed8ee52e7ed	service	user	pass	
		1157		0 20/08/2008 14:20:34	4ff7d09f18c920	service	user	pass	
		1158		0 20/08/2008 14:20:36	69783ee76a925	service	user	pass	
		894		0 04/08/2008 15:49:49	f0aefcd9d4afc1	service	user	pass	
		878		0 04/08/2008 15:49:17	bbe3a23611885	service	user	pass	
		872		0 04/08/2008 15:49:04	86ad2dab9a87	service	user	pass	
		864		1 04/08/2008 15:48:56	b5d3ad899f700	service	user	pass	
		837		0 04/08/2008 15:48:31	f893e351ae1975	service	user	pass	
		819		0 04/08/2008 15:48:14	4b8d49e7c73a1	service	user	pass	
		788		0 04/08/2008 15:47:58	0eda7c7ae62e01	service	user	pass	

135

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:

My Groups Available Groups Targets Blotter										
<input type="checkbox"/>	<input type="checkbox"/>	Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note
		1992		10/09/2008 12:37:28	user	1.1.1.1	host	CLIPBOARD	RCS_136161	
		1937		29/08/2008 09:12:26	user	201.61.41.240	host	PASSWORD	RCS_168921	
		1157		20/08/2008 14:20:34	user	166.89.165.171	host	PASSWORD	RCS_168921	
		904		04/08/2008 15:50:04	user	227.50.46.182	host	MIC	RCS_136161	904 note
		890		04/08/2008 15:49:26	user	40.94.41.240	host	MIC	RCS_168921	
		837		04/08/2008 15:48:31	user	78.216.197.155	host	PASSWORD	RCS_136161	
		818		04/08/2008 15:48:11	user	160.113.198.14	host	MIC	RCS_168921	

136

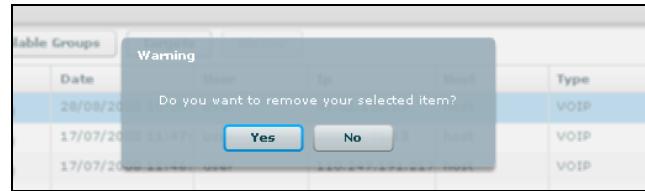
Double click mouse on detail's row to view log's detail

If you want to remove a row, select it with a single click:

My Groups Available Groups Targets Blotter Add Target										
<input type="checkbox"/>	<input type="checkbox"/>	Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note
		1890		28/08/2008 10:35:1	user	97.61.150.69	host	VOIP	RCS_136161	
		662		17/07/2008 11:47:0	user	103.16.78.13	host	VOIP	RCS_136161	
		647		17/07/2008 11:46:0	user	110.247.191.217	host	VOIP	RCS_136161	

137

then click “Remove Item” button:



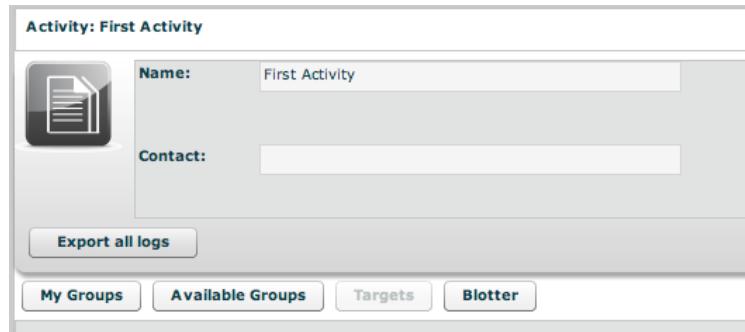
138

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

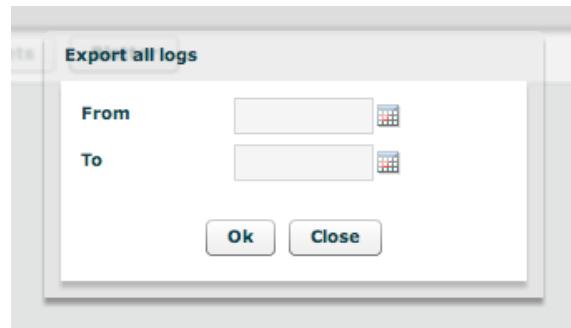
Click “Cleanup Blotter” button to clear blotter.

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 will ALL the logs in that time frame will be generated.