



















RCS Console User Manual

]HackingTeam[

INDEX

General concepts	4
Activity, Target and Backdoor	4
Getting started.....	5
THE CONSOLE SECTION	8
Users	8
Privileges	12
Groups.....	13
Activities	17
Blotter.....	21
Target	22
Backdoors.....	25
 Summary	28
   Webcam, Snapshot, Mouse Click.....	33
 Keylog.....	35
 Url.....	36
 Chat.....	37
 Print	38
 Clipboard	39
 Password.....	40
 Fileopen.....	41
 Filecap	41
  Download, Upload.....	42
 Addressbook	43
 Calendar	44
 Messages	45
 Device.....	48
THE DASHBOARD SECTION	49
Activities balloon.....	50
Targets balloon.....	50
Backdoors balloon	51
THE AUDIT SECTION	52
THE MONITOR SECTION.....	54
Components balloon	54
Components summary	55
License description.....	55
Alerting via email	55
THE ALERTING SECTION	56
Setting up an alert	57
Reviewing matching logs.....	57
HOWTO	58
Create an activity.....	58
Create a target.....	60

Create a backdoor 61
View and search log 62
Export log 63
Create an user 64
Create a group 66
Assign privileges to users 68
Create and manage blotter 69

General concepts

Activity, Target and Backdoor

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

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

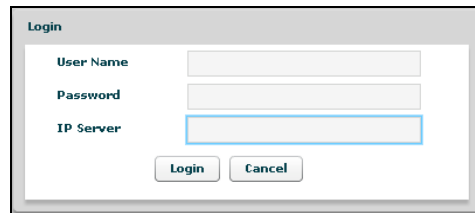
Targets in turn can be grouped in "Activities".

A single Activity represents an "investigation".

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:



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

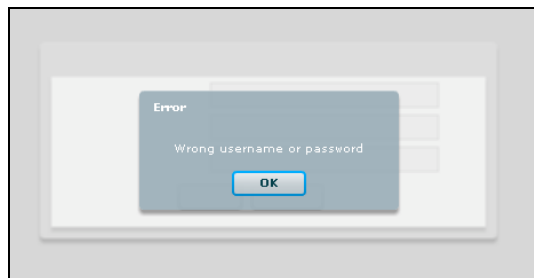
To logon you need to specify the following information:

- 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.

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

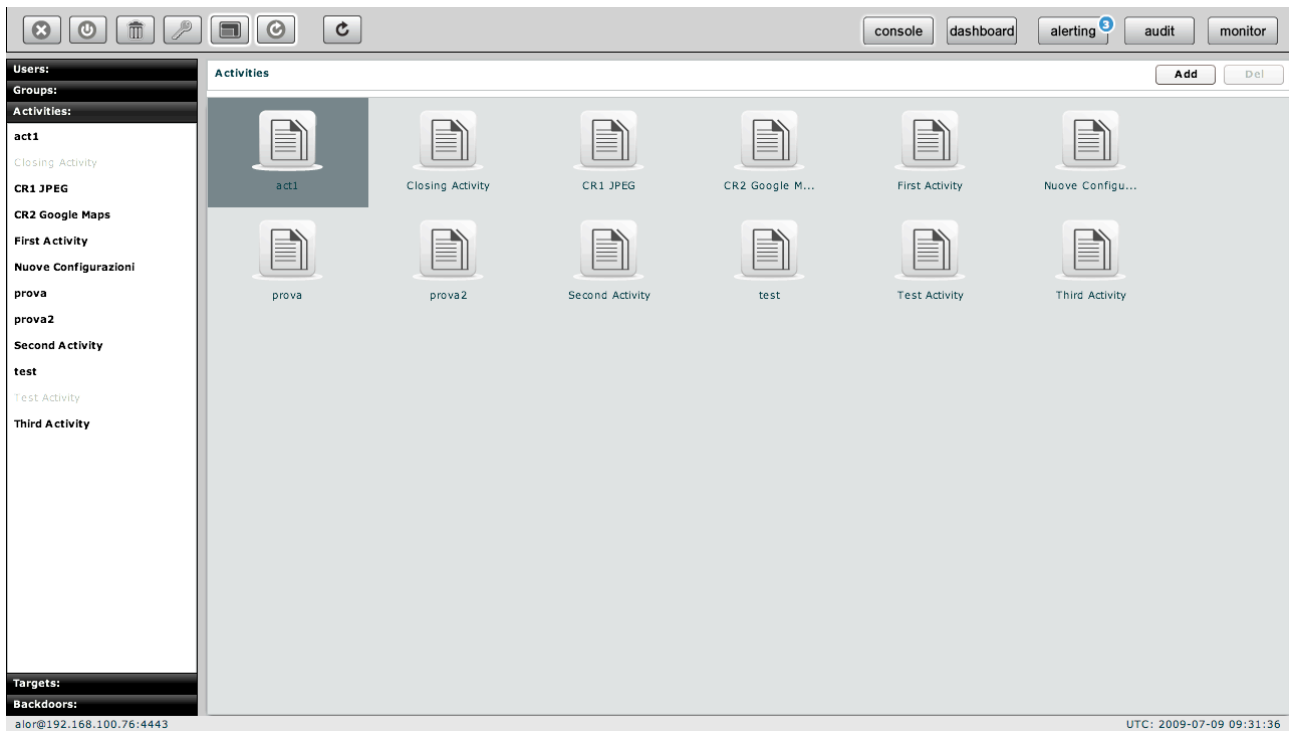
If you fail to logon the application shows an error message:



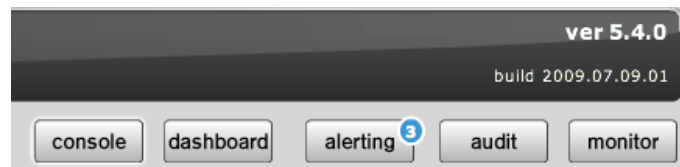
press “OK” button to close this window and return to initial logon screen.

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

After login successfully the application shows this windows:



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



Selected button has a white border.

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

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



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.

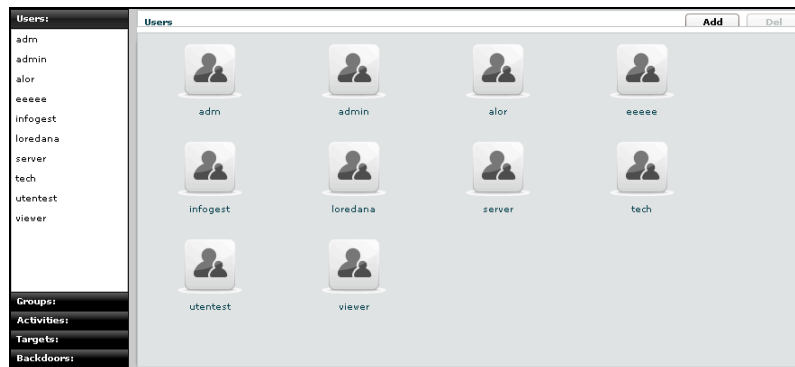
A white border appears around the selected button.

THE CONSOLE SECTION

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

Users

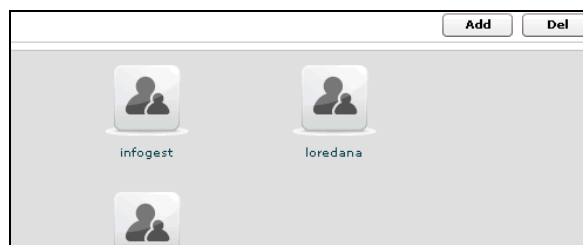
Users Menu is available only for users with *Admn* privileges.



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

At this point you can:

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



then fill all the fields and assign privileges:

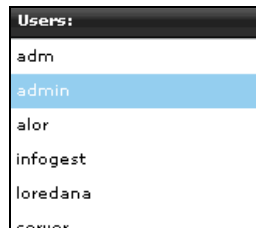
- ADMN is the admin: can manage users, group activity and target
- TECH is the technician: can create and configure backdoors
- VIEW is the viewer: can see the backdoors log and perform queries on them
- SERV is reserved for the server user (used by ASP servers)

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

	Name:	Alberto	Description:	
	Contact:		Confirm:	
	Password:		Disabled:	<input type="checkbox"/>
	Privileges:	<input checked="" type="checkbox"/> Admn <input checked="" type="checkbox"/> Tech <input checked="" type="checkbox"/> View <input type="checkbox"/> Serv		
	<input type="button" value="Save"/>			

click “Save” button to save data.

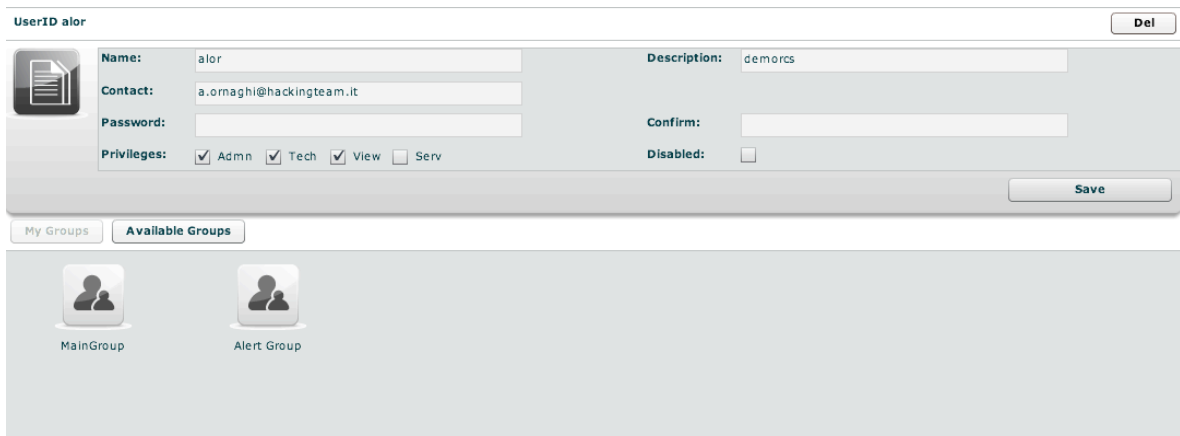
- Select an user, either by:
 1. clicking on the user in menu-list:



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

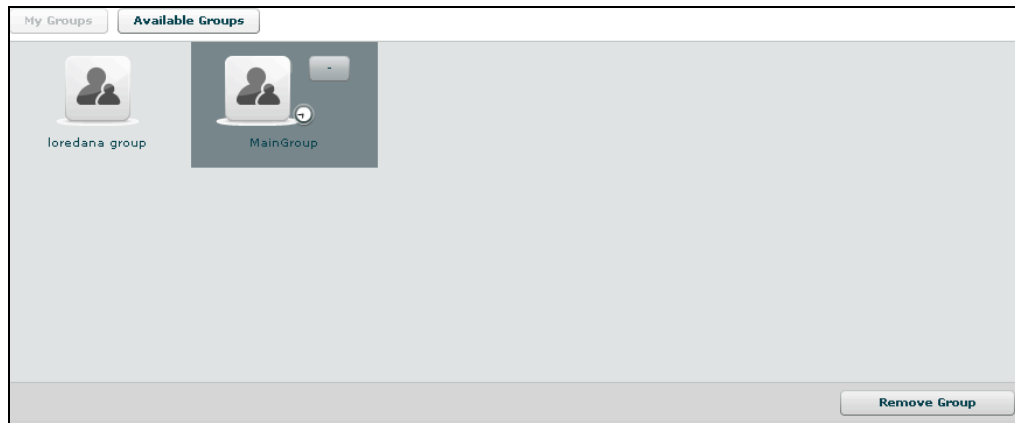


- Edit an user: after selecting an user at the top of the window you can edit fields and save them clicking “Save” button.
At the bottom, you can view all groups the selected user belongs to:

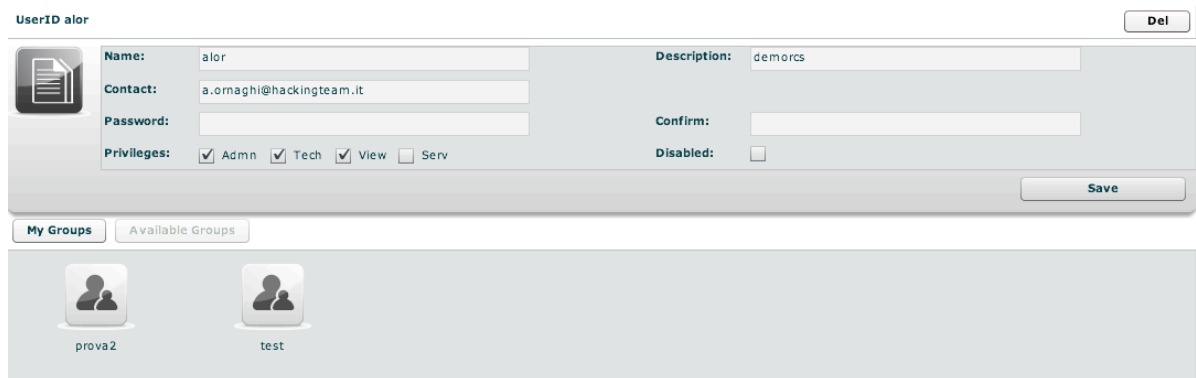


you can see group's details by double clicking group's icon.

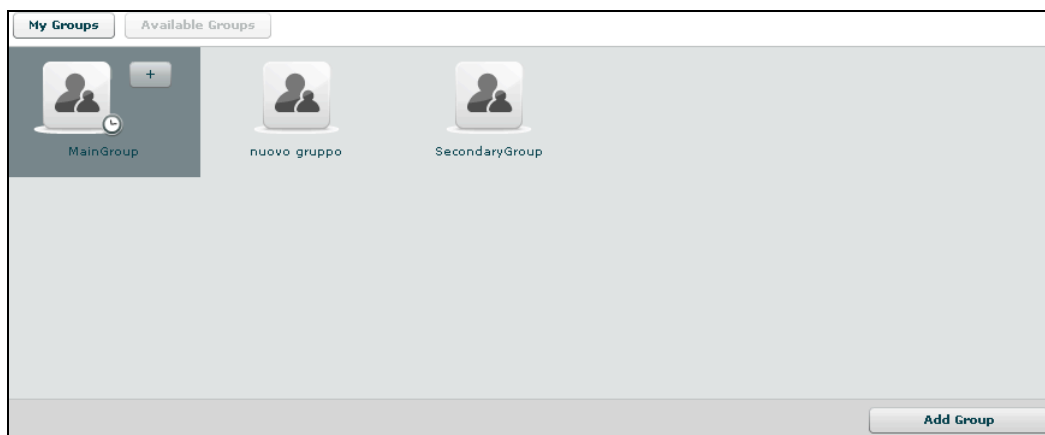
You can remove a group from selected user: select the group to remove and then click on the “-” button or click on the “Remove Group” button below.



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



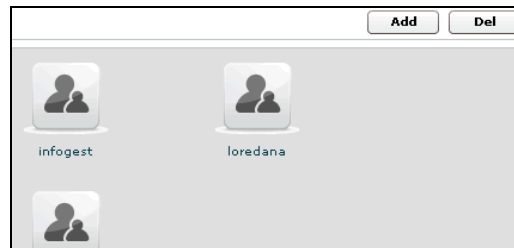
you can see group’s details by double clicking group’s icon.
To add a group to the selected user, select a group with a single click:



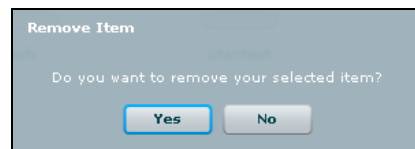
then either by:

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

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



you must confirm the action to proceed:



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

CHANGING USER PASSWORD

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

the button bar.



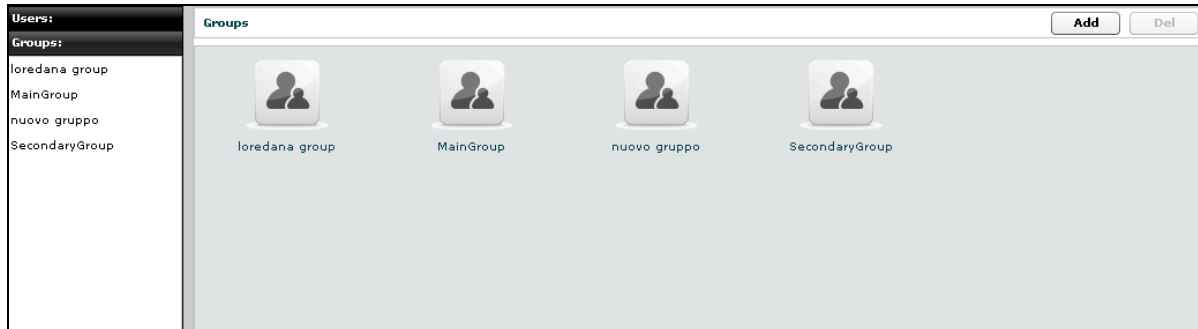
CHANGING USER CONTACT

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

Privileges

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

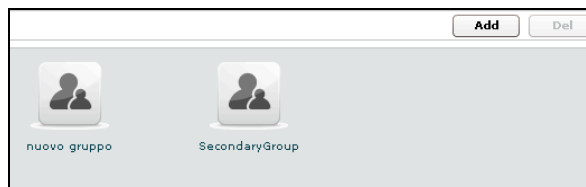
Groups



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

At this point you can:

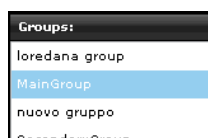
- Add new group: click “Add” button on the right at the top of the icons-list:



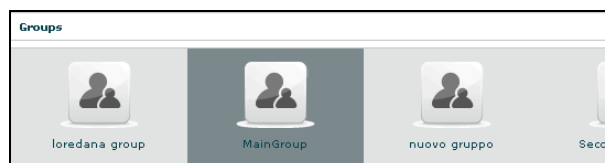
then fill fields:

click “Save” button to save data.

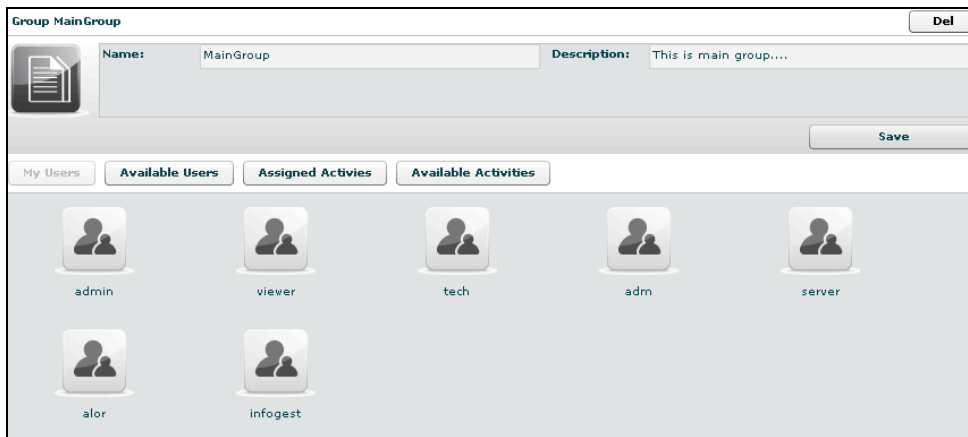
- Select a group: either by:
 1. clicking on the group in menu-list:



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

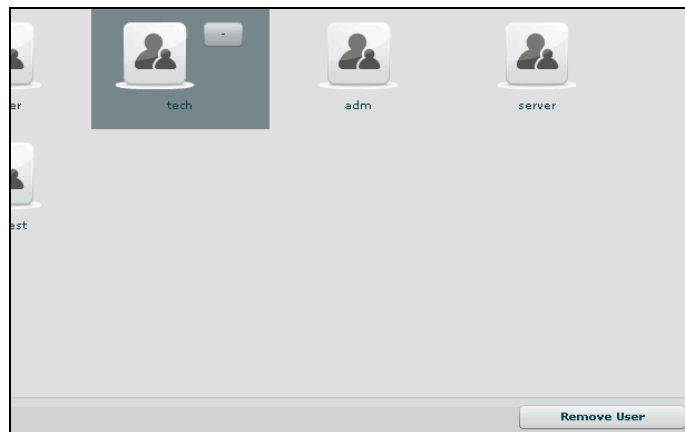


- Edit a group: after selecting a group: at the top of the window you can edit fields and save them clicking “Save” button.
At the bottom, you can view all users the selected group belongs to:

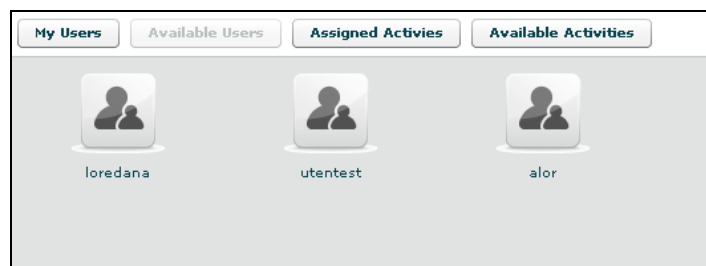


you can see user's details by double clicking user's icon.

You can remove a user from selected group: select the user to remove and then click on the “-” button or click on the “Remove User” button below.

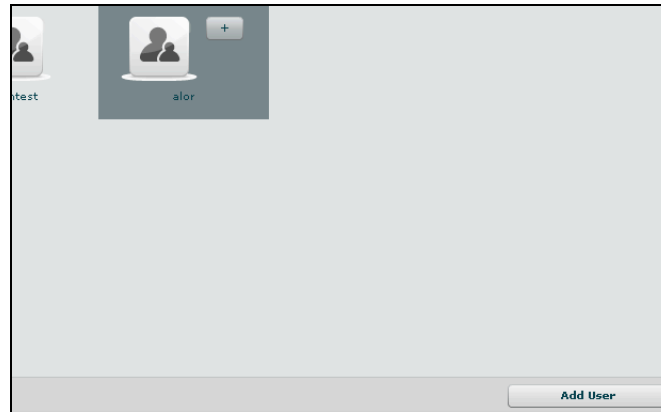


Clicking on “Available Users” button you can view all users available to be added to the selected group:



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

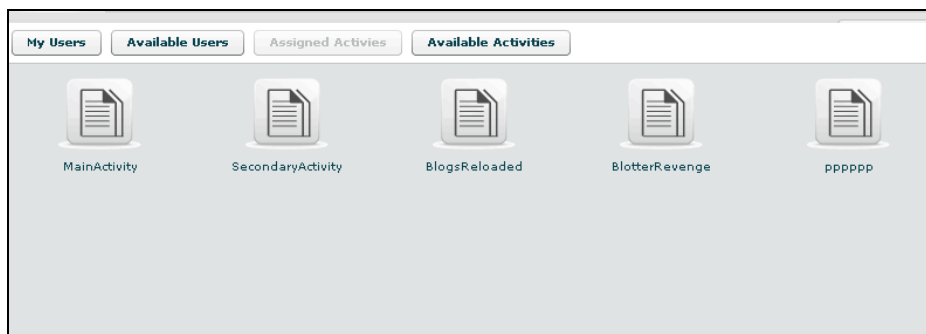
To add a user to the selected group, select a user with a single click:



then either by:

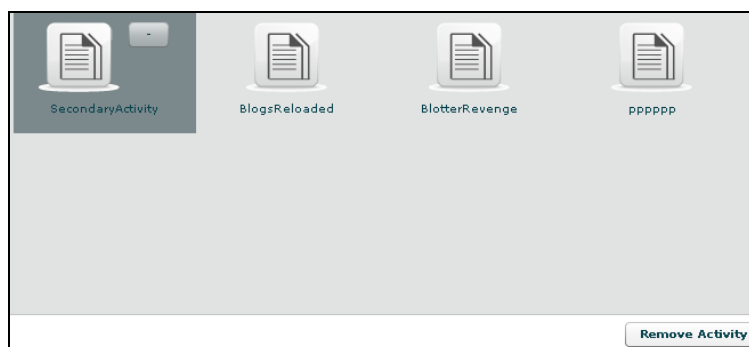
1. click “Add User” button on the left at the bottom of the window;
2. click “+” button next the user’s icon.

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

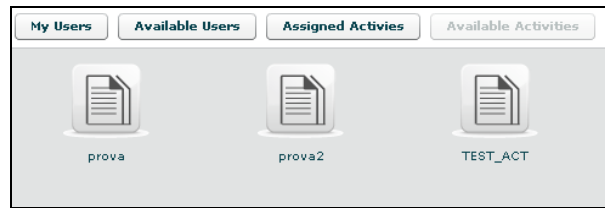


you can see activity’s details by double clicking activity’s icon.

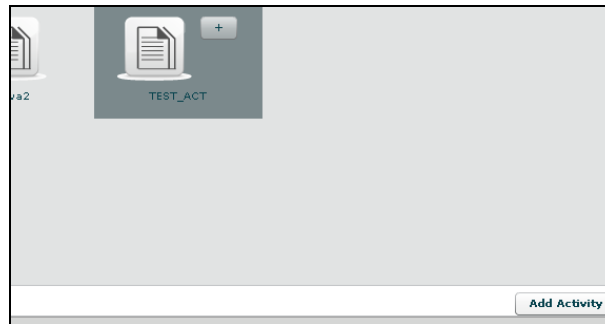
You can remove an activity from the selected group: select the activity to remove and click on the “-” button or click on the “Remove Activity” button below.



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

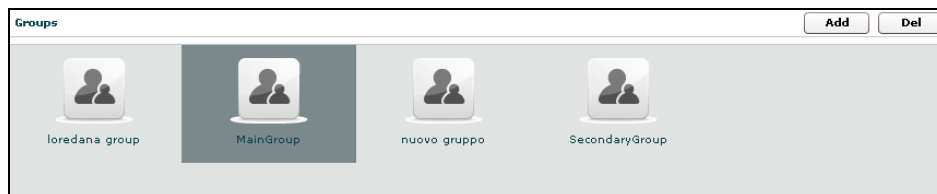


you can see activity's details by double clicking activity's icon.
To add an activity to the selected group, select an activity with a single click:

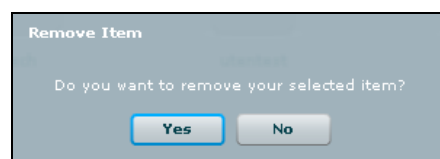


then either by:

1. click "Add Activity" button on the left at the bottom of the window;
 2. click "+" button next the icon's activity.
- Delete a group: after selecting a group, "Del" button on the top of list of icons is enabled, press the button to delete the group:

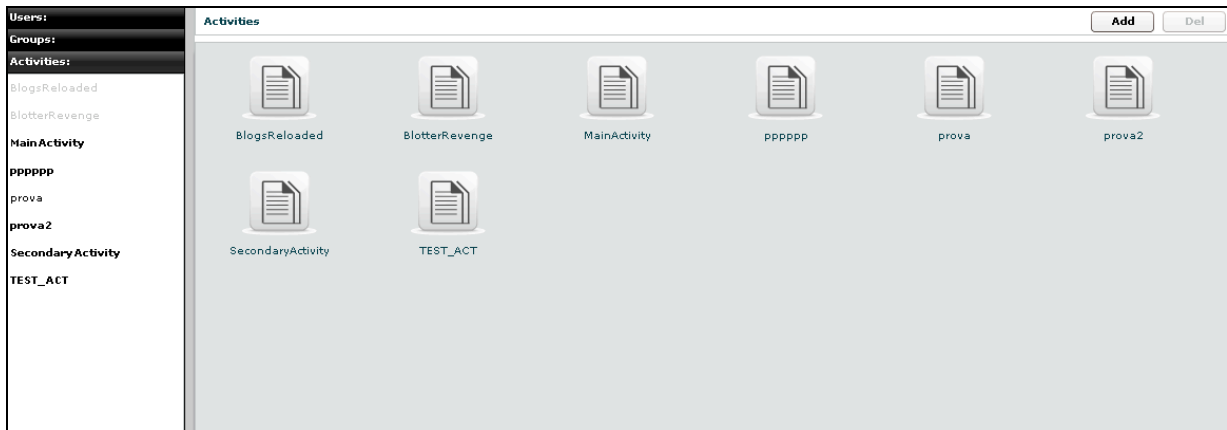


you must confirm the action to proceed:



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

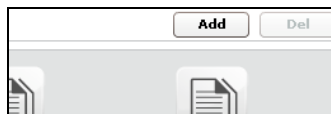
Activities



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

At this point you can:

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



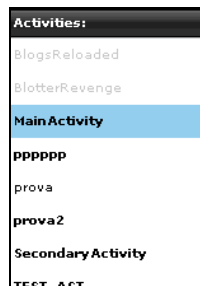
then fill fields and select “Status” OPEN:

	Name:	<input type="text"/>	Description:	<input type="text"/>
	Contact:	<input type="text"/>	Status:	OPEN <input type="button" value="v"/>
				<input type="button" value="Save"/>

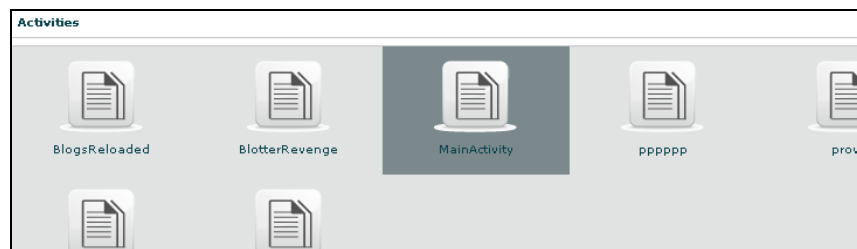
Click “Save” button to save data.

- select an activity, either by:

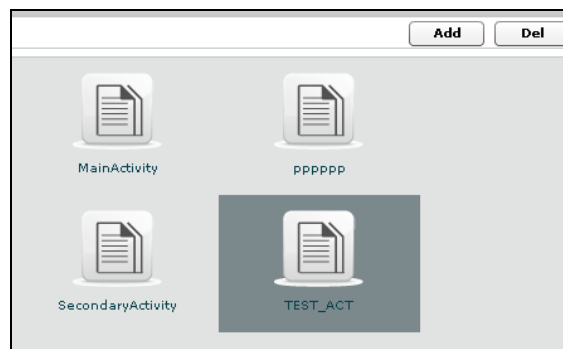
1. click on the activity in menu-list:



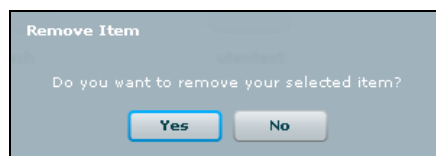
2. or double clicking on activity's icon in icons-list:



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



you must confirm the action to proceed:



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

NOTE: Deleting an Activity, will delete recursively all of its targets, backdoors and logs.

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

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

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

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

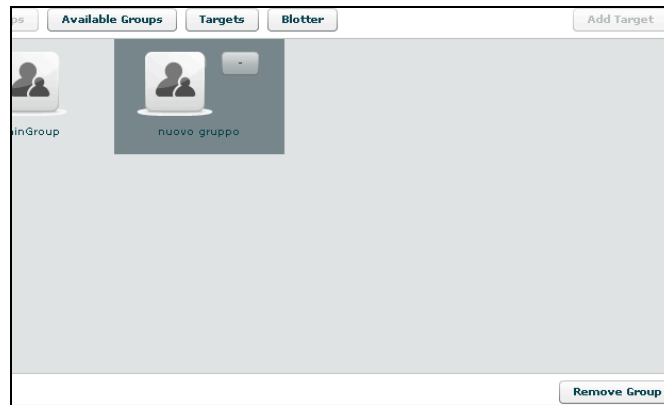
To add a new target to the selected activity, click “Add Target” button on the right:

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

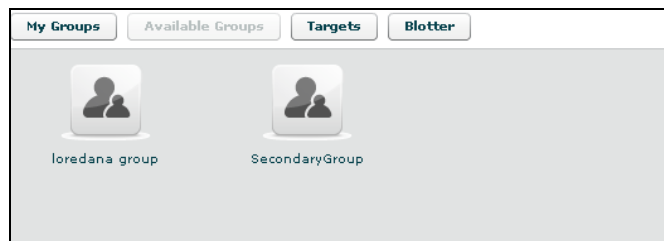
Clicking on “My Groups” button you can view all groups the selected activity belongs to:

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

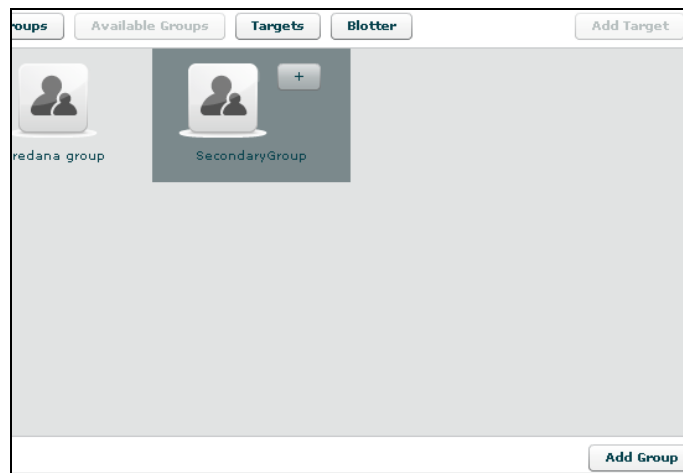
You can remove a group from selected activity: select the group to remove and then click on the “-“ button or click on the “Remove Group” button below.



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



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

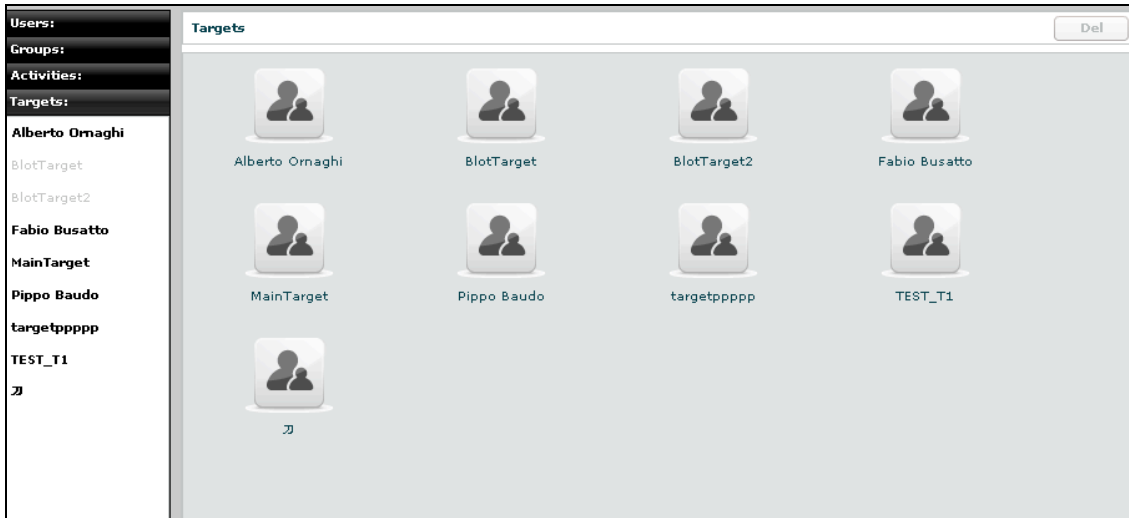


then either by:

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

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

Target



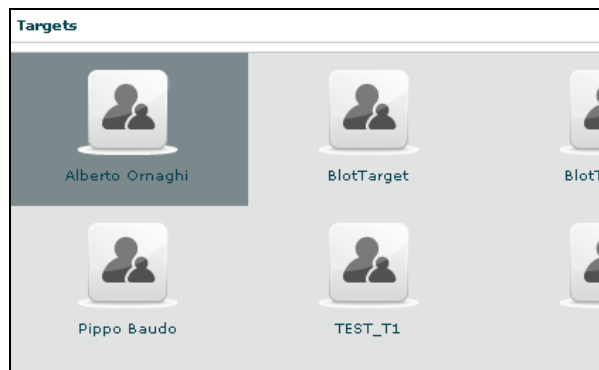
You can view a list of all targets on the left under the tab “Targets” and also on the right pane when you click on the Targets tab title.

At this point you can:

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

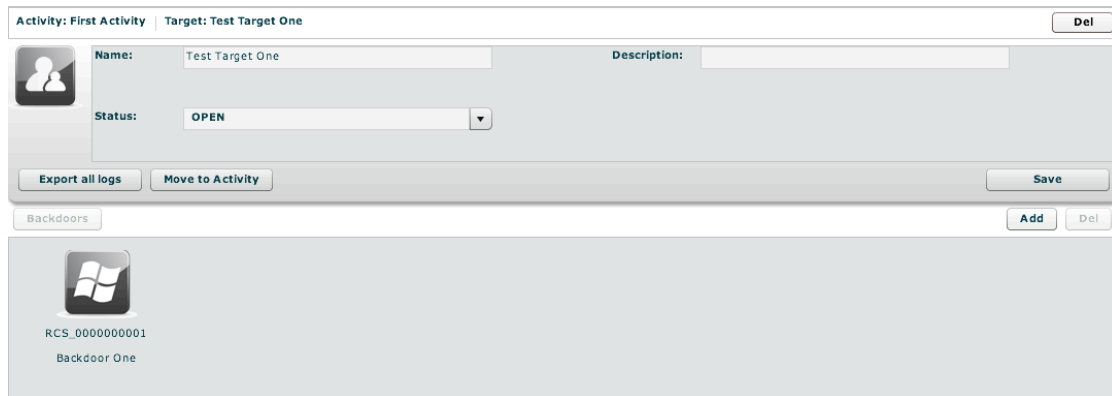


2. or double clicking on target's icon in icons-list:

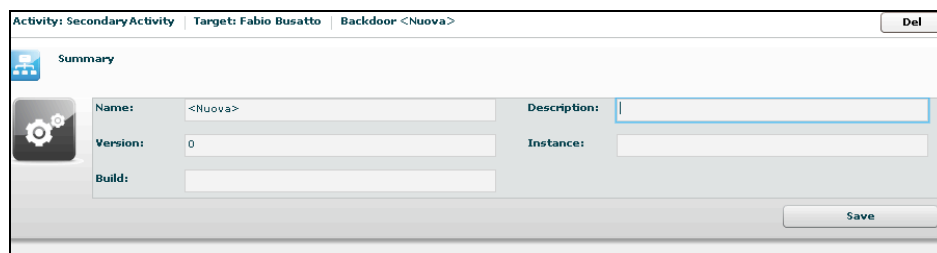


- Edit a target: after selecting a target at the top of the window you can edit fields and save them clicking “Save” button.

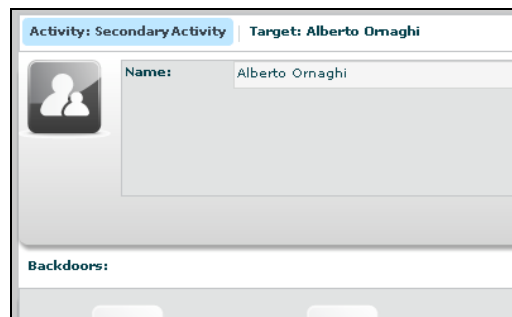
At the bottom, you can view all backdoors the selected target belongs to:



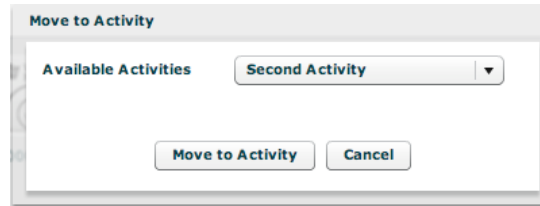
you can see backdoor's details by double clicking backdoor's icon.
To add a new backdoor to the selected target clicking "Add" button on the right:



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

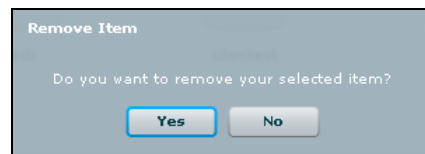


- **Close a Target:** Select Status CLOSE and press the SAVE button. Closing a target is an irreversible operation that should only be used in the appropriate case. All the backdoors related to a closed target will be automatically uninstalled upon the next synchronization.
- **Move a target,** you can move a target from one activity to another. This can be useful if you open a new investigation and the target has to be into that investigation. Instead of closing the target and reinstall a new backdoor, you can keep the backdoor installed and move it to the new investigation. When a target is moved the original one will remain in place and will be closed (no new logs will arrive). The moved target will receive all the new logs as if it was there already from the beginning.



you can only move a target to an open activity.

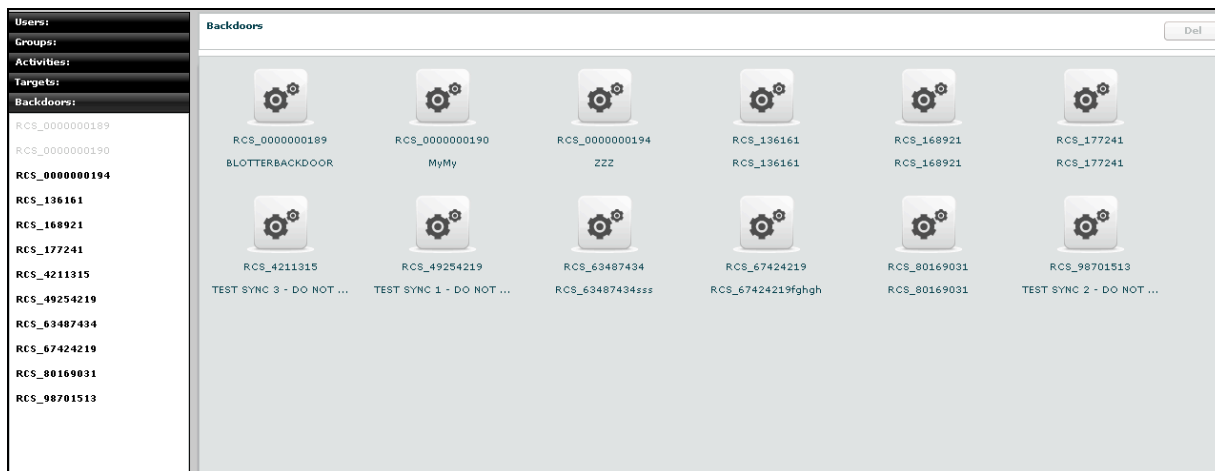
- Remove a target: after selecting a target, press “Del” button on the top of details of the selected target, you must confirm the action to proceed:



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

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

Backdoors



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

Here you can see all the backdoor created within targets and all of their instances.

You can find different types of backdoors identified by different icons. Each operating system has its own icon.

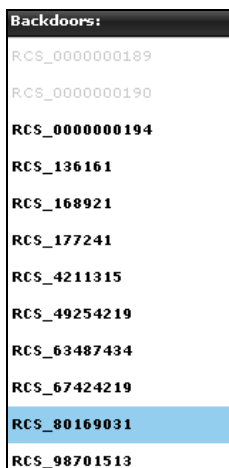
NOTE:

Backdoor installed on different systems (or users) will create different instances. Each instance stands for an installation. First installation will 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.

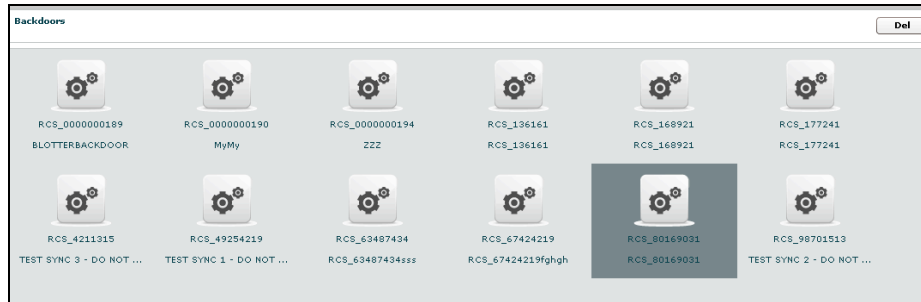
Instances can be moved under other targets if needed. Let’s say you install a backdoor on a system with 5 users. Every user will generate a different instance of the backdoor. Then you can create targets and move the instances under the correct target.

At this point you can:

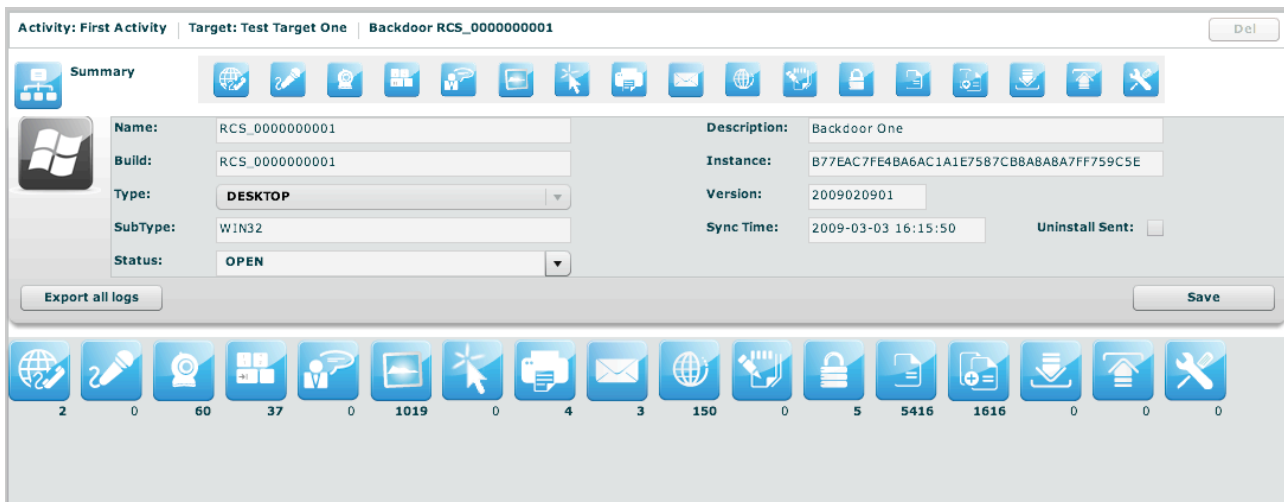
- select a backdoor, either by:
 1. clicking on the backdoor in menu-list:



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



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



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

Activity: MainActivity Target: MainTarget Backdoor RCS_136161

and near the link to open target of selected backdoor:

Activity: MainActivity Target: MainTarget Backdoor RCS_136161

under the links: on the left the summary icon and on the right a list of log's detail's icons.

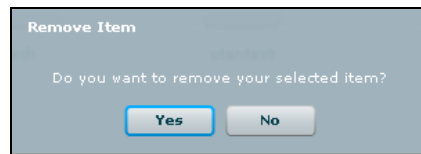
You can edit field "Description" and the "status", all the other field are read only and filled automatically by the database.

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



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

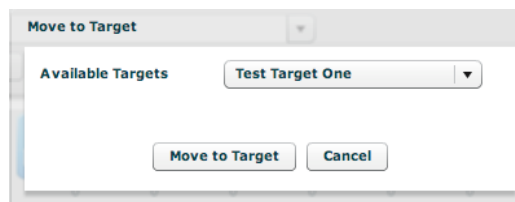
- Delete a backdoor, after selecting a backdoor, press “Del” button at the top of details of the selected target, you must confirm the action to proceed:



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

NOTE: Deleting a Backdoor will recursively delete all of its logs. Deleted backdoors will be automatically uninstalled from the target machine upon next synchronization.

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



you can only move a backdoor to an open target.

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

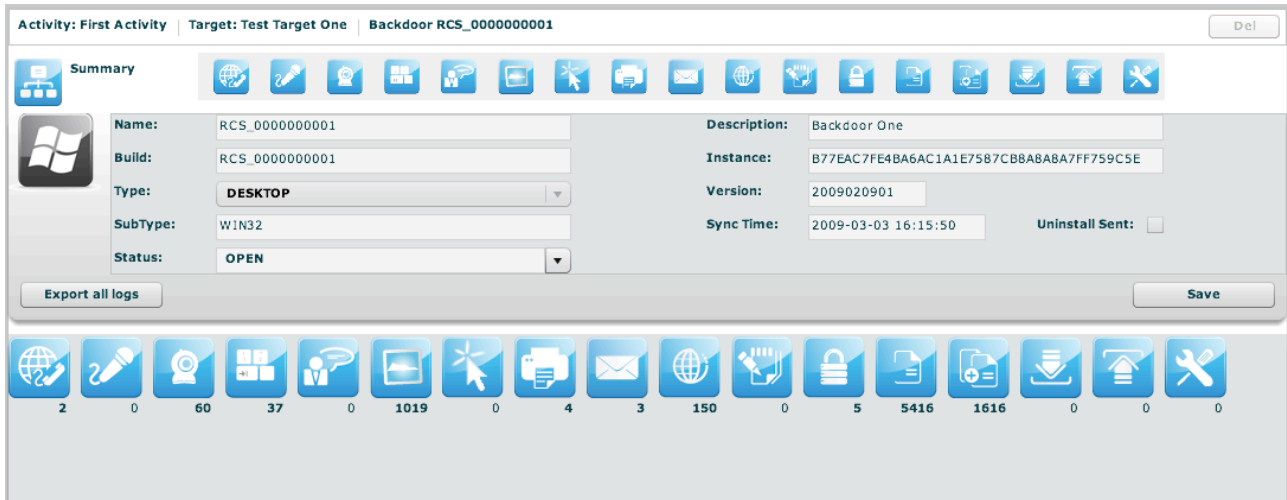


If you press the button the backdoor will be automatically upgraded to the latest version the next time it synchronize with the server.

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

Summary

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



Activity: First Activity | Target: Test Target One | Backdoor RCS_000000001

Summary

Name: RCS_000000001
Build: RCS_000000001
Type: DESKTOP
SubType: WIN32
Status: OPEN

Description: Backdoor One
Instance: B77EAC7FE4BA6AC1A1E75B7CB8A8A8A7FF759C5E
Version: 2009020901
Sync Time: 2009-03-03 16:15:50
Uninstall Sent:

Export all logs | Save

Log Type Counters: 2, 0, 60, 37, 0, 1019, 0, 4, 3, 150, 0, 5, 5416, 1616, 0, 0






For each log there is a counter:

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

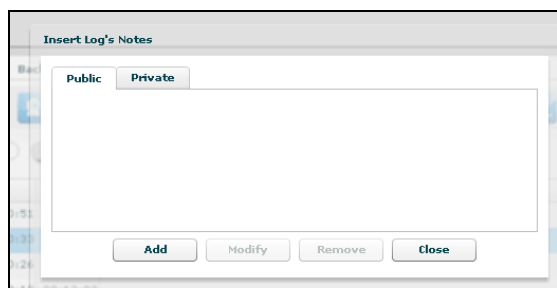
You can select more than one backdoor at a time. In this case the counters will show cumulative values.

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

Note can be public and private:



Insert Log's Notes

Public Private

Add Modify Remove Close

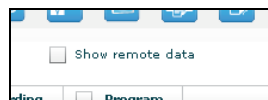
Then Tag Bar (priority), let you change priority of selected logs and is visible only when one or more row is selected.

Id	Tag	Notes	Date	Resource	Service
1934	<input type="radio"/>	0	29/08/2008 09:12:24	c4903be410c8d:	service
864	<input type="radio"/>	1	04/08/2008 15:48:56	b5d3ad899f700:	service
837	<input checked="" type="radio"/>	0	04/08/2008 15:48:31	f89c3e51ae1975	service
630	<input checked="" type="radio"/>	0	17/07/2008 11:46:14	08c48adc90c852	service

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

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

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



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

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

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

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

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

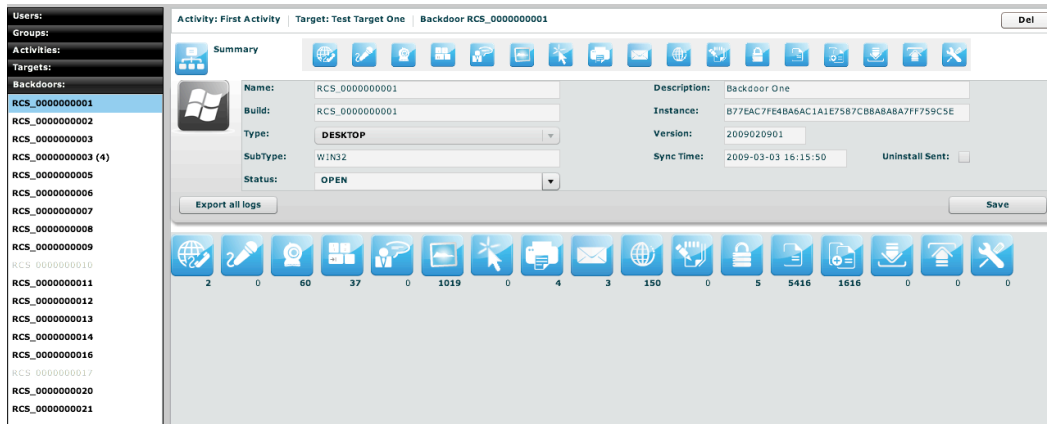
Change number of logs per page:	<input type="text" value="20"/>	<input type="button" value="Ok"/>	<input type="button" value=" <<"/>	Pag. 1 of 1	<input type="button" value=" >>"/>
---------------------------------	---------------------------------	-----------------------------------	--	-------------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

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

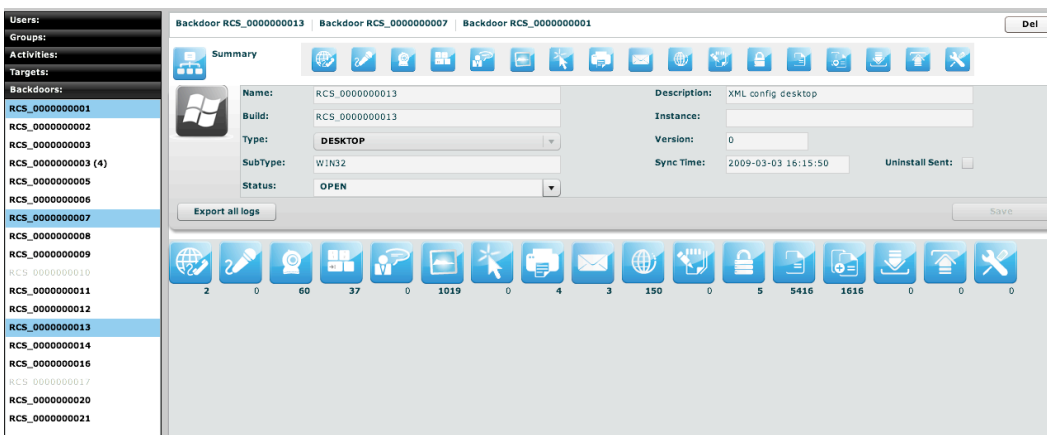
You can select more than one backdoor at a time. In this case the counters will show cumulative values and the agents log view will show log detail originating from any of the selected backdoor.

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

One backdoor selected:



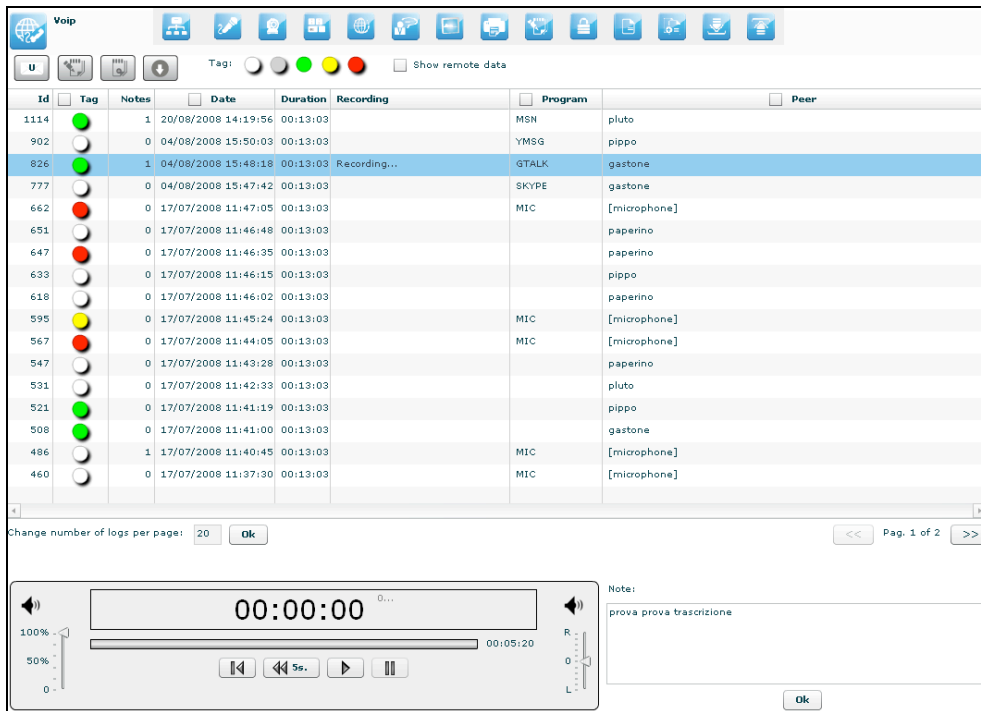
with more backdoors selected the counters show cumulative values for any type of log:



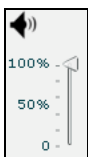
if you want to select consecutive backdoors, select first backdoor then press and hold "Shift" button while selecting the last backdoor.

 **Call, Mic**

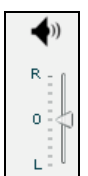
Select this agent view to show a list of all recordings of kind “call list”, “call” or “mic”.



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



this control let you change the volume;



move this arrow to change balance, zero is default.

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




There are four buttons to interact with the audio player:



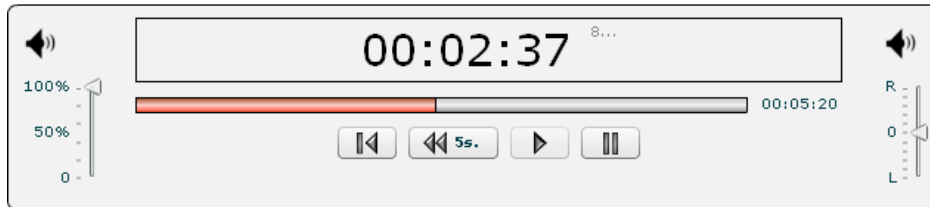
to start player from begin;

]HT[

RCS Console

-  to go back five seconds;
-  to play audio;
-  to pause audio.

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



“-“ 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.

Url

This agent viewer let you browser through logs of kind “url”. It will show you all the visited URLs. The URL is recorded only once and it doesn’t report the automatically loaded sub-URLs. Only the URLs actually visited by the target will be displayed.

If the capture option was configured you can also have a snapshot of the page in the list and it will be displayed as the snapshot visualization.

Activity: alor | Target: alor | Backdoor RCS_000000169

Url 

Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Browser	<input type="checkbox"/> Url	<input type="checkbox"/> Window	<input type="checkbox"/> Size	<input type="checkbox"/> Keywords	<input type="checkbox"/> OCR
172040		0	2009-07-13 07:26:39	IE Explorer	http://mail.google.com/mail/?shva=1	Gmail - Inbox (39) - testth			
172039		0	2009-07-13 07:26:30	IE Explorer	http://mail.google.com/mail/?shva=1	Gmail - New Guide: Underst			
172042		0	2009-07-13 07:26:25	IE Explorer	http://mail.google.com/mail/?shva=1	Gmail - Inbox (39) - testth	137 Kb		
172038		0	2009-07-13 07:26:25	IE Explorer	http://mail.google.com/mail/?shva=1	Gmail - Inbox (39) - testth			
172037		0	2009-07-13 07:26:20	IE Explorer	http://mail.google.com/mail/?shva=1	Gmail - Windows Internet E			
172036		0	2009-07-13 07:26:19	IE Explorer	https://www.google.com/accounts/S	Reindirizzamento - Windows			
172041		0	2009-07-13 07:26:10	IE Explorer	https://www.google.com/accounts/S	Gmail: l'email di Google - W	93 Kb		
172035		0	2009-07-13 07:26:10	IE Explorer	https://www.google.com/accounts/S	Gmail: l'email di Google - W			
172034		0	2009-07-13 07:26:01	Mozilla Firefox	http://www.youtube.com/	YouTube - Broadcast Yourse			
172033		0	2009-07-13 07:25:47	Mozilla Firefox	http://www.facebook.com/	Welcome to Facebook! Fac			
171972		0	2009-07-13 07:25:28	Opera	http://europa.wsj.com/home-page	Corriere della Sera - Opera			
171971		0	2009-07-13 07:24:59	Opera	http://www.corriere.it/	Libero - Opera			
171970		0	2009-07-13 07:24:50	Opera	http://www.libero.it/	Opera Web Browser Faster			
171969		0	2009-07-13 07:24:43	Opera	http://www.opera.com/browser/	Opera			
171968		0	2009-07-13 07:24:31	Mozilla Firefox	http://www.microsoft.com/events/se	Digital Blackbelt Series: Def			
171967		0	2009-07-13 07:24:22	Mozilla Firefox	http://msdn.microsoft.com/en-us/sec	Security Developer Center -			
171966		0	2009-07-13 07:24:01	Mozilla Firefox	http://www.microsoft.com/en-us/def	Microsoft Corporation - Mozi			
171961		0	2009-07-13 07:23:37	IE Explorer	http://www.ibm.com/us/en/	IBM - United States - Windo	55 Kb		

Change number of logs per page:

Pag. 1 of 2



Print

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

The screenshot shows the 'Print' view in the RCS Console. At the top, there are tabs for 'Activity: Main Activity', 'Target: MainTarget', and 'Backdoor RCS_138161'. Below the tabs is a toolbar with various icons and a 'Print' button. A table lists log entries with columns for 'Id', 'Tag', 'Date', 'Spool', and 'Size'. Two entries are visible: ID 1926 and ID 1912, both dated 28/08/2008. To the right of the table, a preview of the log content is shown, including a Base64-encoded string. Below the table is a grid of 10 document thumbnails, each with a small preview of the document's content. At the bottom, there are controls for 'Change number of logs per page' (set to 20) and 'Page 1 of 1'.

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

This screenshot shows a detailed view of a log entry. The main area displays a code snippet from a log file, including Base64 decoding and a server call to 'backdoor.identify'. On the right side, there is a zoom control panel with four buttons: 'Fit', '1:1', '+', and '-'. Below the zoom panel, there is a 'Close' button. The interface also shows the 'Id' (1912), 'Size' (3916930), and 'Date' (28/08/2008 12:36:46) for the selected log entry.

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_138181

Clipboard

Show remote data

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

Change number of logs per page: 20

<< Pag. 1 of 2 >>

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



Password

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

Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Resource	<input type="checkbox"/> Service	<input type="checkbox"/> UserId	<input type="checkbox"/> Password
105231		0	2009-05-28 09:16:08	Trillian	yahoo	testth@yahoo.it	...
105230		0	2009-05-28 09:16:08	Trillian	msn	testth@hotmail.com	...
105229		0	2009-05-28 09:16:08	Trillian	aim	419764929	ht...
105228		0	2009-05-28 09:16:08	Trillian	aim	aol	1...
105227		0	2009-05-28 09:16:08	Google Talk	GTALK	default.talk.google.com	...
105226		0	2009-05-28 09:16:08	Windows Live M	imap.gmail.com	testth	h...
105225		0	2009-05-28 09:16:08	Outlook Express	imap.gmail.com	testth	ht1...
105224		0	2009-05-28 09:16:08	Thunderbird	mailbox://proc.test@pop.mail	proc.test	ht...
105223		0	2009-05-28 09:16:08	Thunderbird	mailbox://%B7%CE%D3@pop	%B7%CE%D3	ciac...
105222		0	2009-05-28 09:16:08	Thunderbird	imap://testth@imap.gmail.co	testth	ht1...
105221		0	2009-05-28 09:16:08	Opera	https://login.libero.it	testシノビ	shir...
105220		0	2009-05-28 09:16:08	Opera	https://www.google.com	testシノビ	shir...
105219		0	2009-05-28 09:16:08	Opera	https://www.google.com	testth	ht1...
105218		0	2009-05-28 09:16:08	IE Explorer	https://login.libero.it/	testしのび	shir...
105217		0	2009-05-28 09:16:08	IE Explorer	https://www.google.com/acco	シノビ	shir...
105216		0	2009-05-28 09:16:08	IE Explorer	https://www.google.com/acco	testth	ht1...
105215		0	2009-05-28 09:16:08	IE Explorer HTTP	192.168.100.100:4443/phpMy	root	ro...
105214		0	2009-05-28 09:16:08	Firefox	https://www.google.com	testシノビ	shir...

Change number of logs per page:

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”. This is the list of opened files. If you want the real file you have to capture it or download it with the download command.

Activity: MainActivity | Target: Test Alor | Backdoor RCS_000000005

Opened Files Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Process	<input type="checkbox"/> Size	<input type="checkbox"/> Mode	<input type="checkbox"/> File
22755		0	2009-01-16 08:25:06	ieexplore.exe	0 B	---D	C:\Documents and Settings\Admin\Cookies\admin@msn[1].txt
22754		0	2009-01-16 08:25:06	ieexplore.exe	997 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@msn[2].txt
22753		0	2009-01-16 08:25:06	ieexplore.exe	997 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@msn[2].txt
22752		0	2009-01-16 08:25:06	ieexplore.exe	997 B	---D	C:\Documents and Settings\Admin\Cookies\admin@msn[2].txt
22751		0	2009-01-16 08:25:06	ieexplore.exe	0 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@msn[1].txt
22750		0	2009-01-16 08:25:06	ieexplore.exe	0 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@msn[1].txt
22749		0	2009-01-16 08:25:06	ieexplore.exe	104 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@p.live[1].txt
22748		0	2009-01-16 08:25:06	ieexplore.exe	104 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@p.live[1].txt
22747		0	2009-01-16 08:25:04	ieexplore.exe	0 B	---D	C:\Documents and Settings\Admin\Cookies\admin@live[1].txt
22746		0	2009-01-16 08:25:04	ieexplore.exe	2 Kb	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt
22745		0	2009-01-16 08:25:04	ieexplore.exe	2 Kb	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt
22744		0	2009-01-16 08:25:04	ieexplore.exe	281 B	R---	C:\Documents and Settings\Admin\Cookies\admin@www.live[1].txt
22743		0	2009-01-16 08:25:01	ieexplore.exe	0 B	---D	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt
22742		0	2009-01-16 08:25:01	ieexplore.exe	2 Kb	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[1].txt
22741		0	2009-01-16 08:25:01	ieexplore.exe	2 Kb	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[1].txt
22740		0	2009-01-16 08:25:01	ieexplore.exe	2 Kb	---D	C:\Documents and Settings\Admin\Cookies\admin@live[1].txt
22739		0	2009-01-16 08:25:01	ieexplore.exe	0 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt
22738		0	2009-01-16 08:25:01	ieexplore.exe	0 B	-W--	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt

Change number of logs per page: 20 Pag. 1 of 1083

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

Filecap

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

Activity: MainActivity | Target: Test Alor | Backdoor RCS_000000005

Captured Files Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Size	<input type="checkbox"/> File
22772		0	2009-01-16 08:25:06	104 B	C:\Documents and Settings\Admin\Cookies\admin@p.live[1].txt
22770		0	2009-01-16 08:25:04	281 B	C:\Documents and Settings\Admin\Cookies\admin@www.live[1].txt
22773		0	2009-01-16 08:24:23	262 B	C:\Documents and Settings\Admin\Cookies\admin@windowsmarketplace[2].txt
22778		0	2009-01-16 08:24:22	997 B	C:\Documents and Settings\Admin\Cookies\admin@msn[2].txt
22776		0	2009-01-16 08:24:22	104 B	C:\Documents and Settings\Admin\Cookies\admin@zune[1].txt
22775		0	2009-01-16 08:24:22	234 B	C:\Documents and Settings\Admin\Cookies\admin@zune[2].txt
22769		0	2009-01-16 08:24:22	118 B	C:\Documents and Settings\Admin\Cookies\admin@windowsmarketplace[1].txt
22768		0	2009-01-16 08:24:22	905 B	C:\Documents and Settings\Admin\Cookies\admin@login.live[2].txt
22780		0	2009-01-16 08:24:09	170 B	C:\Documents and Settings\Admin\Cookies\admin@get.live[1].txt
22777		0	2009-01-16 08:23:54	2 Kb	C:\Documents and Settings\Admin\Cookies\admin@live[1].txt
22781		0	2009-01-16 08:23:53	809 B	C:\Documents and Settings\Admin\Cookies\admin@login.live[1].txt
22774		0	2009-01-16 08:23:40	2 Kb	C:\Documents and Settings\Admin\Cookies\admin@live[2].txt
22771		0	2009-01-16 08:23:36	83 B	C:\Documents and Settings\Admin\Cookies\admin@doubleclick[1].txt
22782		0	2009-01-16 08:23:35	280 B	C:\Documents and Settings\Admin\Cookies\admin@apple[1].txt
22779		0	2009-01-16 08:23:35	174 B	C:\Documents and Settings\Admin\Cookies\admin@apple[2].txt
22767		0	2009-01-16 08:23:07	105 B	C:\Documents and Settings\Admin\Cookies\admin@mail.google[1].txt
22305		0	2009-01-15 13:12:32	296 B	C:\Documents and Settings\Admin\Cookies\admin@yahoo[2].txt
22308		0	2009-01-15 09:17:11	2 Kb	C:\DOCUME~1\Admin\LOCALS~1\Temp\dd NET Framework30 Setup1CE0.txt

Change number of logs per page: 20 Pag. 1 of 9



Download, Upload

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

Downloaded file will show you the files that were downloaded from the backdoor with the download command. It will not show you files downloaded by the target from the internet.

The same rule applies for uploaded file.

In order to capture downloaded or uploaded file by the target you have to use the filecapture agent.

Activity: alor | Target: test | Backdoor RCS_000000023

Downloaded Files

Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	Notes	<input type="checkbox"/> Date	Size	<input type="checkbox"/> File
27438		0	2009-02-06 14:09:46	6 B	c:\New Text Document.txt
27437		0	2009-02-06 14:09:46	4 B	c:\Copy of New Text Document.txt
27436		0	2009-02-06 14:09:45	3 B	c:\Copy (3) of New Text Document.txt
27435		0	2009-02-06 14:09:44	5 B	c:\Copy (2) of New Text Document.txt
27434		0	2009-02-06 14:09:37	507 B	c:\windows\win.ini
27433		0	2009-02-06 14:09:36	37 B	c:\windows\vbaddin.ini
27432		0	2009-02-06 14:09:36	36 B	c:\windows\vb.ini
27431		0	2009-02-06 14:09:35	231 B	c:\windows\system.ini
27430		0	2009-02-06 14:09:34	466 B	c:\windows\PGPfone.INI
27429		0	2009-02-06 14:09:34	4 Kb	c:\windows\ODBCINST.INI
27428		0	2009-02-06 14:09:33	1 Kb	c:\windows\msdfmap.ini
27427		0	2009-02-06 14:09:32	2 B	c:\windows\desktop.ini
27426		0	2009-02-06 14:09:23	6 B	c:\New Text Document.txt
27425		0	2009-02-06 14:09:22	4 B	c:\Copy of New Text Document.txt
27424		0	2009-02-06 14:09:21	3 B	c:\Copy (3) of New Text Document.txt
27423		0	2009-02-06 14:09:21	5 B	c:\Copy (2) of New Text Document.txt
27419		0	2009-02-06 14:08:12	6 B	c:\New Text Document.txt
27418		0	2009-02-06 14:08:11	4 B	c:\Copy of New Text Document.txt

Change number of logs per page:

<< Pag. 1 of 4 >>







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



Addressbook

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

Activity: MainActivity | Target: Target | Backdoor RCS_000000033

Addressbook      

Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> Contact	<input type="checkbox"/> Info	<input type="checkbox"/> Extended Info
3963	<input type="checkbox"/>	0	29/12/2008 15:51:30	P750, Asus	3355865863	Company Name: HT S.r.l. Business TelephoneNumber: 3355865863
3964	<input type="checkbox"/>	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	<input type="checkbox"/>	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 PostalCode: 21121 Business Address Country: Italia
3966	<input type="checkbox"/>	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

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 information like address, company name, address, webpage of the contact.

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



Calendar

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

Activity: MainActivity | Target: Target | Backdoor RCS_0000000033

Calendar

Tag: Show remote data

Id	Tag	Notes	Date	Event	Type	Start	Finish	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 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 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 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 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 versio	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 >>

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: alor | Target: test | Backdoor RCS_000000163

Messages

Show remote data

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

Change number of logs per page: 20

<< Pag. 1 of 129 >>

These are the main fields available in this view:

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

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



Location

This agent viewer let you browser through logs of kind “gps” or “cell id”. You will be able to know the geographic position of the target.

Location

U

Show remote data

Id	Tag	Notes	Date	Latitude	Longitude	Type	Error Range
9451		0	2009-05-19 12:48:34	CC:222 NC:1 AC:47204		CELL	
9450		0	2009-05-19 12:48:14	CC:222 NC:1 AC:47204		CELL	
9420		0	2009-04-02 12:37:34	CC:222 NC:1 AC:25784		CELL	
9419		0	2009-04-02 12:05:35	CC:222 NC:1 AC:25784		CELL	
9418		0	2009-01-26 14:09:07	CC:222 NC:88 AC:10060		CELL	
9417		0	2009-01-26 14:07:50	CC:222 NC:88 AC:10060		CELL	
9416		0	2009-01-26 14:06:34	CC:222 NC:88 AC:10060		CELL	
9415		0	2009-01-26 14:05:22	CC:0 NC:0 AC:10060 CI		CELL	
9414		0	2009-01-26 13:33:10	CC:222 NC:88 AC:10060		CELL	
9413		0	2009-01-26 13:31:53	CC:222 NC:88 AC:10060		CELL	
9412		0	2009-01-26 13:30:37	CC:222 NC:88 AC:10060		CELL	
9411		0	2009-01-26 13:29:28	CC:0 NC:0 AC:0 CID:0		CELL	
9449		0	2009-01-23 17:49:27	45.430630	9.179358	GPS	20
9448		0	2009-01-23 17:48:26	45.430807	9.178182	GPS	20
9447		0	2009-01-23 17:31:11	45.477713	9.184695	GPS	20
9446		0	2009-01-23 17:30:10	45.477553	9.185727	GPS	20
9445		0	2009-01-20 21:39:41	45.431890	9.180192	GPS	20
9444		0	2009-01-20 21:39:10	45.431902	9.179993	GPS	20

Change number of logs per page:

Pag. 1 of 3

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 (if the phone can fix a gps position) or cell_id (based on gsm cell information);
- Error range: possible errors in the position, expressed in meter.

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

The screenshot shows the RCS Console interface. At the top, there is a 'Location' header and a toolbar with various icons. Below the toolbar, there are controls for 'Tag' (radio buttons for white, grey, green, yellow, red) and a checkbox for 'Show remote data'. A table displays log entries with columns for Id, Tag, Notes, Date, Latitude, Longitude, Type, and Error Range. The first entry (Id: 9420) is highlighted. Below the table, there is a 'Change number of logs per page' control set to 20. The main area features a map with a selected point (Id: 9420) and a sidebar on the right showing the selected point's details: Id: 9420, Latitude: 45.476373, Longitude: 9.192394, and Error Range: 509. The map includes navigation controls and a 'Close' button.

Id	Tag	Notes	Date	Latitude	Longitude	Type	Error Range
9420	<input checked="" type="radio"/>	0	2009-04-02 12:37:34	CC:222 NC:1 AC:25784		CELL	
9419	<input type="radio"/>	0	2009-04-02 12:05:35	CC:222 NC:1 AC:25784		CELL	

You can perform some operations on the map:



move over all the map with the direction cross;



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



zoom in and zoom out on the map image.

If you select more than one log you will see all the logs on the same map indicating the path of the target.

 **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_000000094 (98)

Device

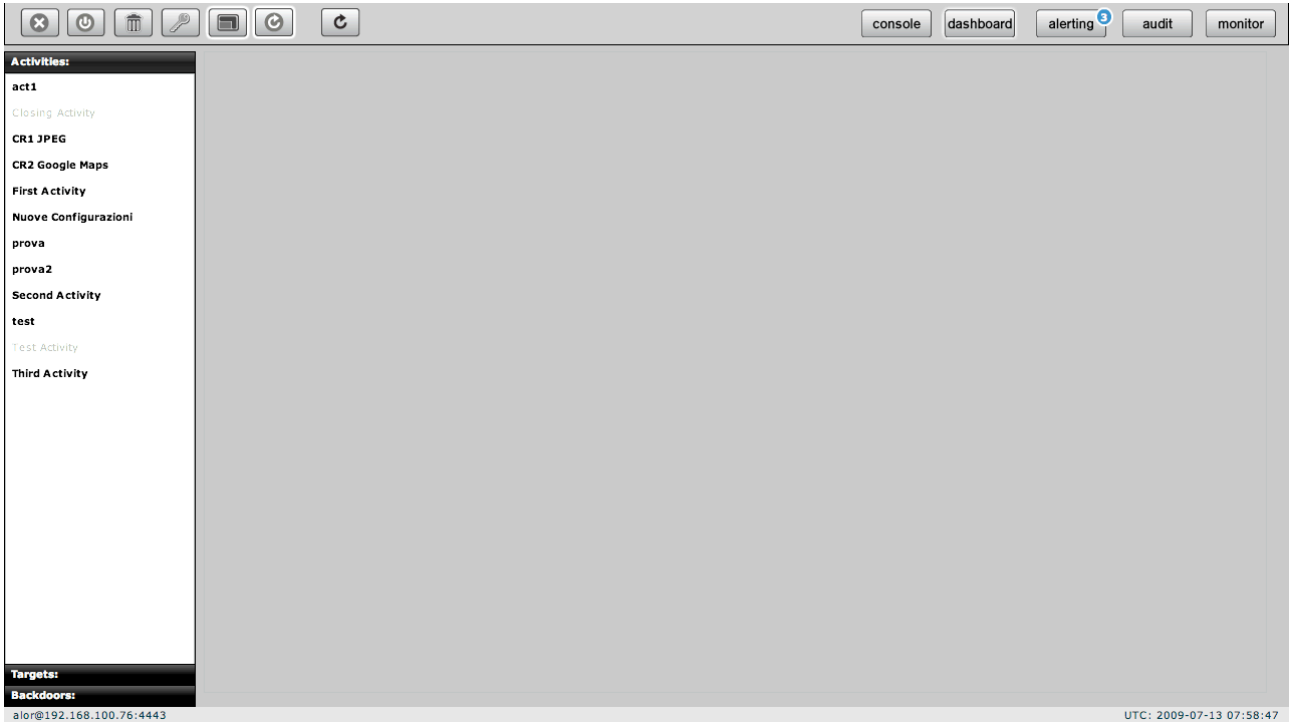
Show remote data

<input type="checkbox"/> Id	<input type="checkbox"/> Tag	<input type="checkbox"/> Notes	<input type="checkbox"/> Date	<input type="checkbox"/> 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)

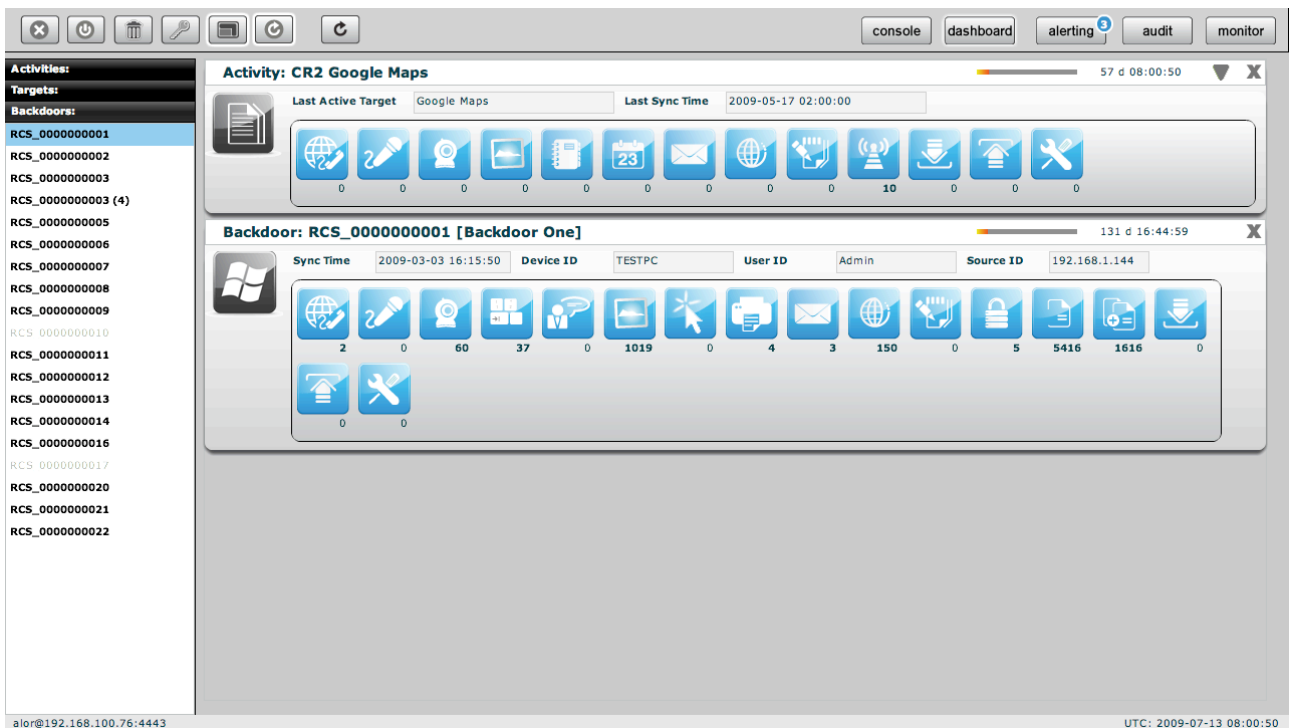
You can also retrieve the list of the applications installed on the target system.

THE DASHBOARD SECTION

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



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



Selected items will be monitored continuously (if automatic refresh is enabled) and newer (hottest) one will be placed on the top of the screen.

For all type of item: activities, targets, backdoors, there is a progress bar and a timer both showing the time elapsed from last received update:



1

▼ to expand a balloon, only for activities, to see its targets, and for targets to see its backdoors;

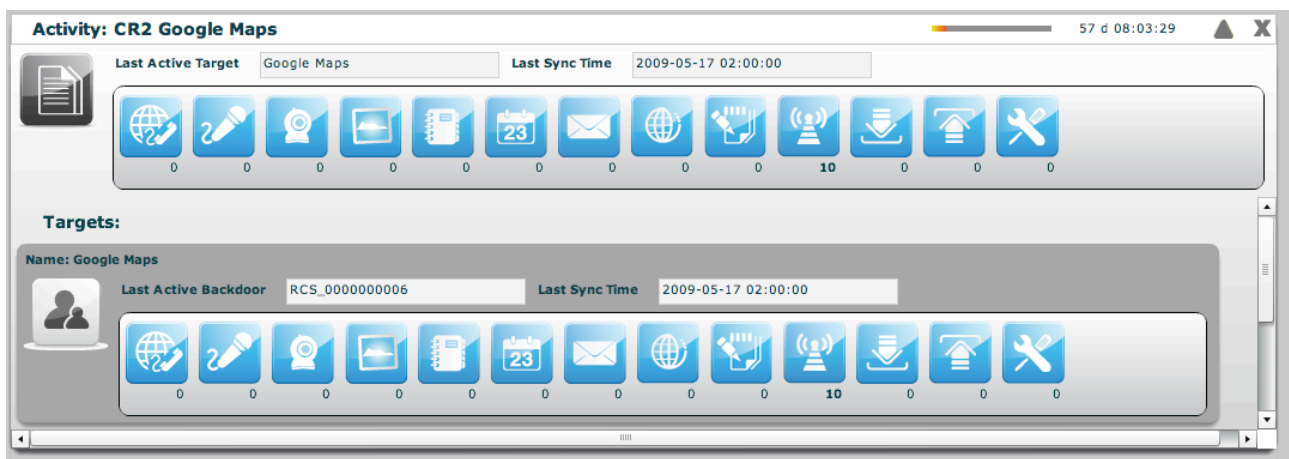
▲ to compress an expanded balloon;

✕ 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 in red until logs are viewed.

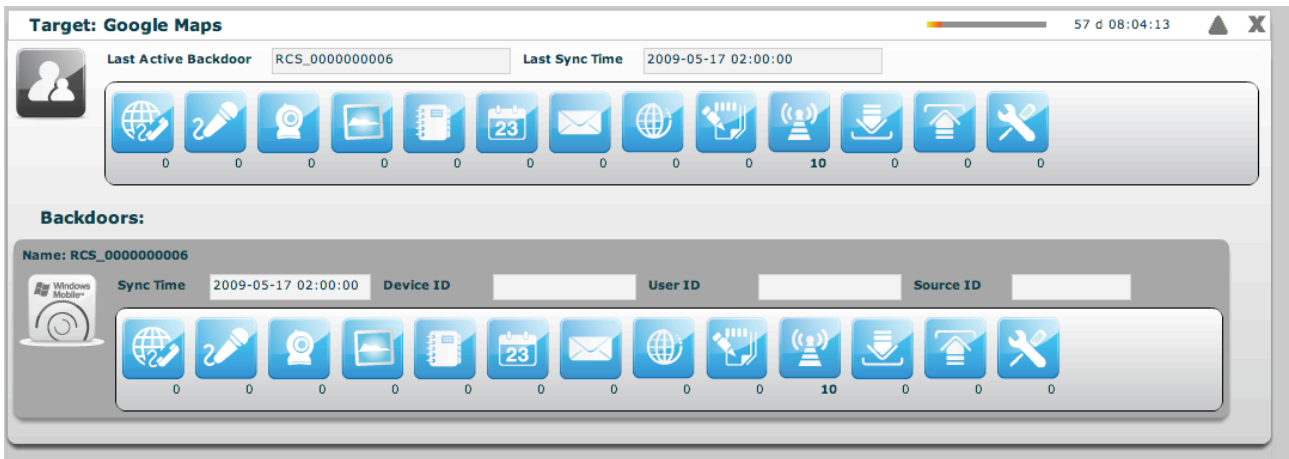
To view the logs just click on its detail icon, then you will switch to the console view.

Activities balloon



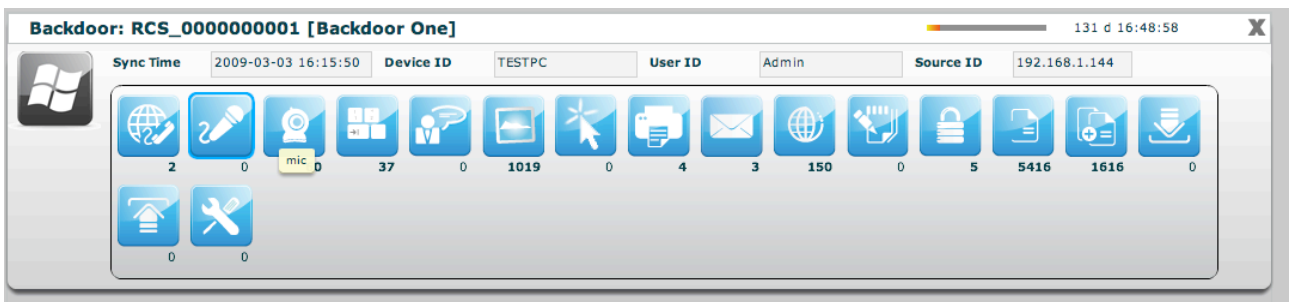
double click on target's panel to see its details. The id of the last seen target and last sync time is showed. In expanded form last sync time, and seen backdoor for each target are also displayed.

Targets balloon



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

Backdoors balloon



THE AUDIT SECTION

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="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' => '',)
14/01/2009 10:41:33	admin	member.add	admin	MainGroup				NULL
14/01/2009 10:41:34	admin	member.add	alor	MainGroup				NULL
14/01/2009 10:41:35	admin	member.add	que	MainGroup				NULL
14/01/2009 10:41:36	admin	member.add	tech	MainGroup				NULL
14/01/2009 10:41:37	admin	member.add	viewer	MainGroup				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					
14/01/2009 10:42:32	alor	backdoor.add			MainActivity	TestTarget	RCS_0000000001	array ('desc' => 'Asus', 'type' => 'WINMOBILE', 'target_id' => 1,)

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

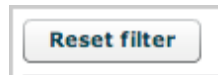
²

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.

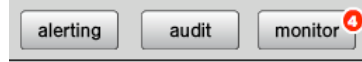
So if you select an used in the sidebar, the filter will be applied on the “user” column and not on the “actor” one.

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



THE MONITOR SECTION

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



the red number indicates the number of failed components.

The monitor section is as follow:

Monitor Summary

Monitored components: 4
 CRITICAL component(s): 0
 WARNING component(s): 0
 OK component(s): 4

License

Start Date: Unlimited
 End Date: Unlimited
 Serial: off
 Users: Unlimited
 Admn: Unlimited
 Tech: Unlimited
 View: Unlimited
 Backdoor: 19 / Unlimited
 Desktop: 13 / Unlimited
 Mobile: 6 / Unlimited
 Alerting: true

Version

Database: -1
 Console: -1
 Core WIN32: 2009020901
 Core WINMOBILE: 2009020901

Monitor: ASP::RLD 127.0.0.1 00 d 00:00:37

Cpu Process	Cpu Total	Disk free	Description:
0 %	0 %	96 %	Idle...

Monitor: ASP::RSS 127.0.0.1 00 d 00:00:35

Cpu Process	Cpu Total	Disk free	Description:
0 %	0 %	96 %	Idle...

Monitor: ASP::RSSM 127.0.0.1 00 d 00:00:28

Cpu Process	Cpu Total	Disk free	Description:
0 %	7 %	96 %	Idle...

Monitor: DB localhost 00 d 00:00:27

Cpu Process	Cpu Total	Disk free	Description:
2 %	2 %	96 %	Running queries: 0

Components balloon

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

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

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

Alerting via email

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

A rectangular button with rounded corners, containing the text "Set Alert Group" in a blue font. The button has a light gray border and a subtle gradient.

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

THE ALERTING SECTION

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

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



The alerting section is as follow:

Alerting Summary

- Open Activities: 10
- Open Targets: 11
- Open Backdoors: 17
- Alert Queries: 4
- Triggered Alerts: 3
- Matching Logs: 3

Alert Queries:

Activity	Target	Backdoor	Type	Alert Type	Supp	Keywords
First Activity	Test Target One	RCS_0000000001	CALL	LOG	0	123414
CR2 Google Maps	Google Maps	*	LOCATION	LOG	0	23
act1	*	*	*	LOG	0	ciao
Third Activity	Test Target Three	RCS_0000000003	DEVICE	LOG	0	1934

Triggered Alerts:

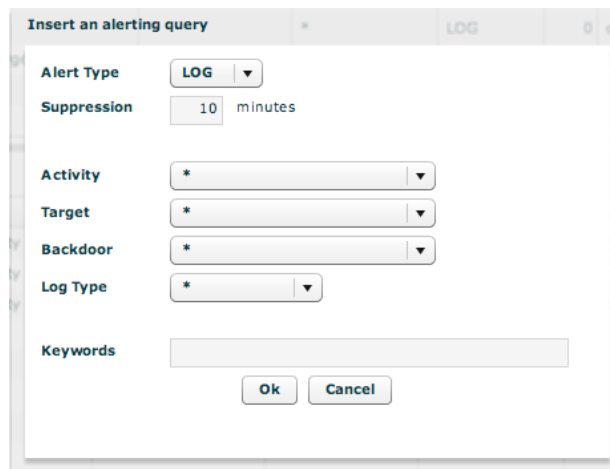
Date	Activity	Target	Backdoor	Type	Keywords	Logs
2009-07-07 10:15:00	First Activity	Test Target One	RCS_0000000001	MAIL	subject	12038
2009-07-02 15:38:00	First Activity	Test Target One	RCS_0000000001	URL	corriere.it	9186
2009-07-02 15:37:41	First Activity	Test Target One	RCS_0000000001	SNAPSHOT	corriere.it	9407

the page is divided in two sections:

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

Setting up an alert

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



You can specify the type of the alert: MAIL or LOG. MAIL will use the “contact” field of the user description and LOG will only log the alert in the database. Mailed alert will also be logged in the database for later review.

The suppression time is the time frame in which you will not be warned again for the same query. Useful if you don't want to receive multiple email for the same matching criteria.

Keywords will be searched in all the possible fields of the log, you don't have to worry about the name. You can also use wildcard: the percentage symbol (%) is used to match any word.

Reviewing matching logs

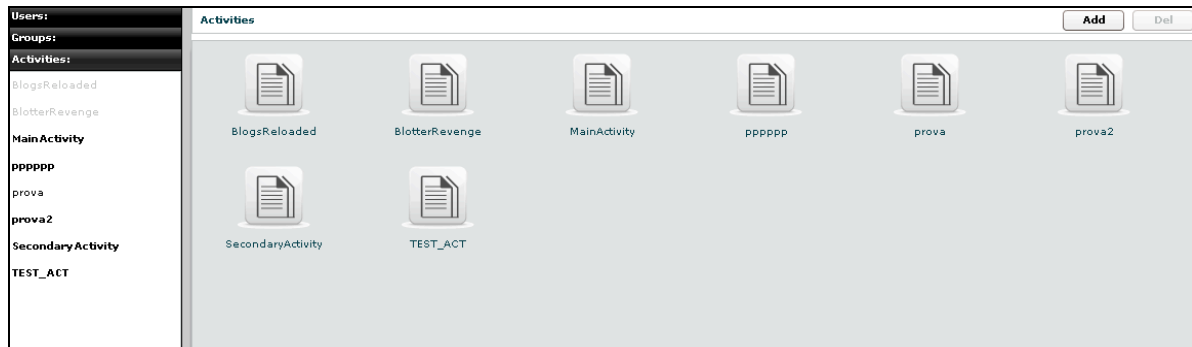
In the bottom part you have the list of logs that matched a query. Multiple logs are collapsed into the same alert log within the suppression time. So you can have multiple log_id separated by commas in the “Logs” field. Double clicking on an entry will forward you to the logs with a preset filter to let you review only those logs.

Once an alert log has been reviewed it is suggested to delete it to decrement the alert log count on the button bar.

HOWTO

Create an activity

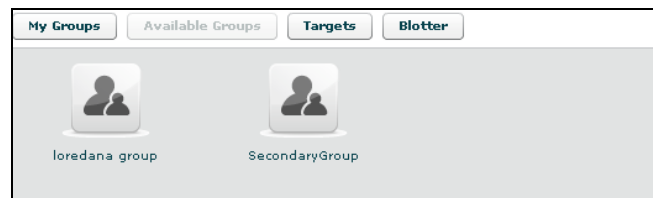
You need to be logged with Admn profile. Start application and after successfully login, click “Add” button on left menu:



fill fields and select “Status” OPEN:

click “Save” button to save data.

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



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

An activity will only be available to users belonging to groups assigned to it. Thus, in order to give access to the newly created activity, its targets and its backdoors you need to assign groups to it.

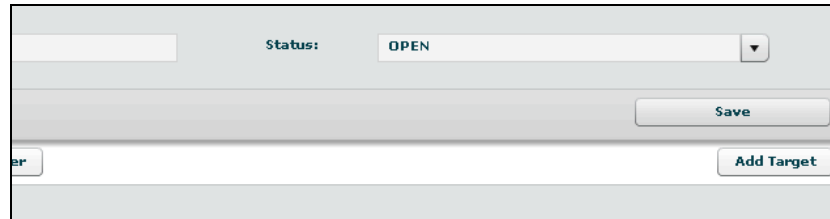
Select group with a single click:



then either by:

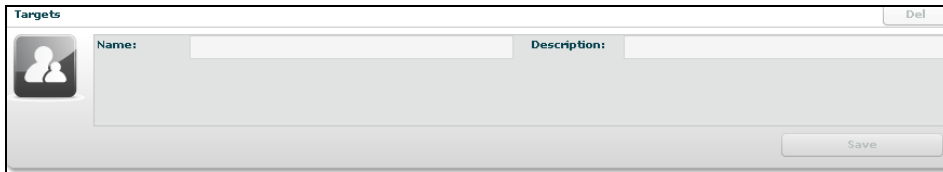
1. click “Add Group” button on the left at the bottom of the window;
2. click “+” button next the group’s icon.

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



A screenshot of a web form. At the top, there is a 'Status:' label followed by a dropdown menu showing 'OPEN'. Below this is a 'Save' button. At the bottom right of the form is an 'Add Target' button.

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



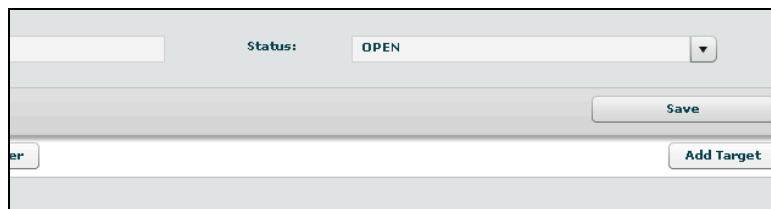
A screenshot of a window titled 'Targets'. It contains two input fields: 'Name:' and 'Description:'. A 'Save' button is located at the bottom right. There is also a 'Del' button in the top right corner and a small icon of two people in the top left corner.

Create a target

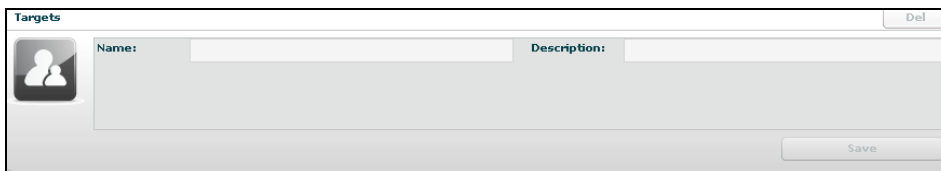
You need to be logged with Admn profile. Start application and after successfully login, click tab “Activities” on left menu:



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



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

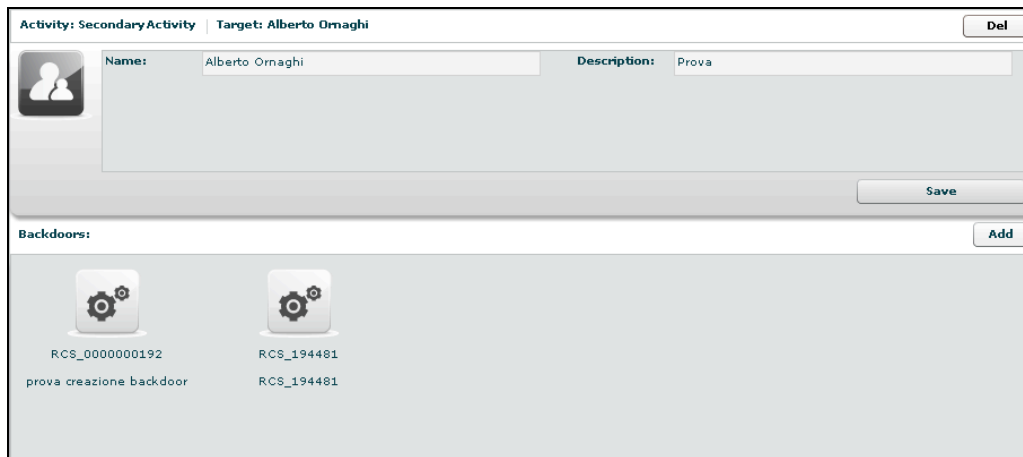


Create a backdoor

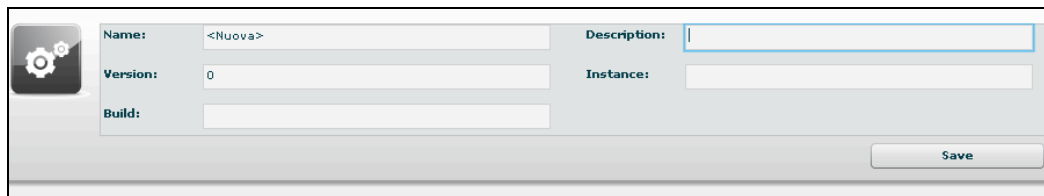
You need to be logged with Tech profile. Start application and after successfully login, click tab "Targets" on left menu:



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



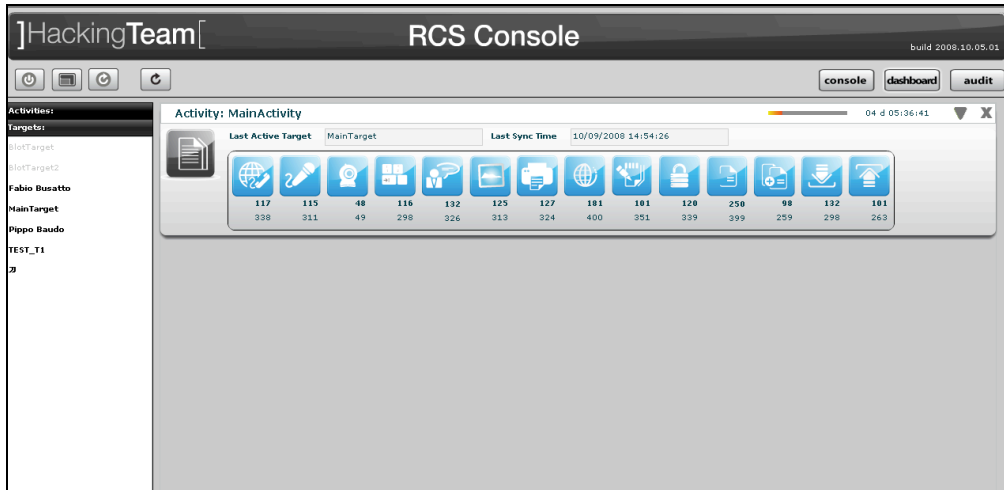
fill field "Description" and click "Save" button to save data:



View and search log

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

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

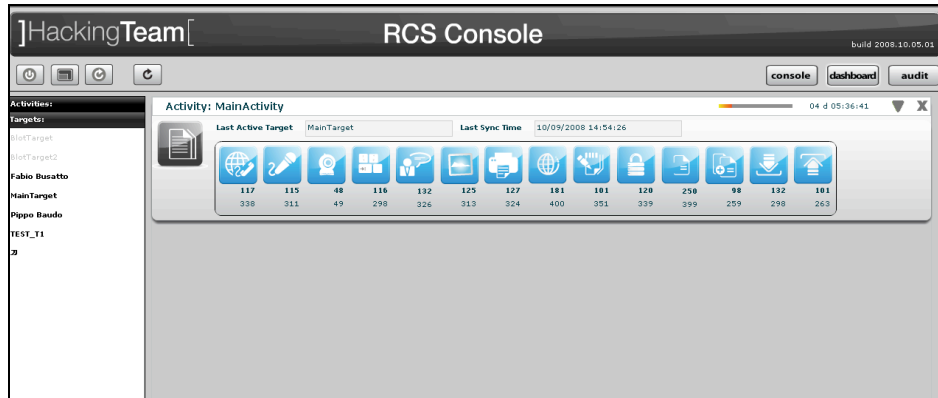


then click log's icon to see log's details.

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

Export log

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



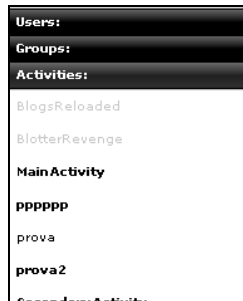
then select one or more log's rows:

Id	Tag	Notes	Date	Resource	Service	UserId	Password
1937	0	0	29/08/2008 09:12:26	If4be5aac180c4920caae2c75e77076d	service	user	pass
1934	0	0	29/08/2008 09:12:24	c4903be410c8d3e3e66c5ddd2126daca	service	user	pass
1216	0	0	20/08/2008 14:21:16	ac6d3309a61190ccce91186c045cc6dc	service	user	pass
1211	0	0	20/08/2008 14:21:14	6f2fed8e626e7d1238e8d15a3104a42b	service	user	pass
1157	0	0	20/08/2008 14:20:34	4ff7d09f18c920302462b55847e16b2	service	user	pass
1158	0	0	20/08/2008 14:20:34	69783ee76a92567d446143b811519068	service	user	pass
894	0	0	04/08/2008 15:49:49	f0eefcbdb4afc1b3fbae0018e0773a0	service	user	pass
878	0	0	04/08/2008 15:49:17	bbe3a23611885241d4f2622e39f29a95	service	user	pass
872	0	0	04/08/2008 15:49:04	86ad2abe9aa87efa03c4bbe3fb005b2	service	user	pass
864	1	0	04/08/2008 15:48:56	b5d3ad899f70013367f24e0b1fa75944	service	user	pass
837	0	0	04/08/2008 15:48:31	f89c3e51ae1979d52092d5e64fe06f5f	service	user	pass
819	0	0	04/08/2008 15:48:14	4b8cf49e7c73a1e8e2d67cdf4eaa304	service	user	pass
788	0	0	04/08/2008 15:47:58	0ede7c7ae62e005507fc15cd016c3fdf	service	user	pass
780	0	0	04/08/2008 15:47:55	ca2d05e1c5b3d2b271fb96df2e7f4cda	service	user	pass
638	0	0	17/07/2008 11:46:28	c73151b0d36ad644d5f57c87ae8c05e3	service	user	pass
630	0	0	17/07/2008 11:46:14	08c48adc90c8525f8ca1f8d727b5780c	service	user	pass
582	0	0	17/07/2008 11:45:14	5e49108f885e8c3c6b5ff3c019679af	service	user	pass

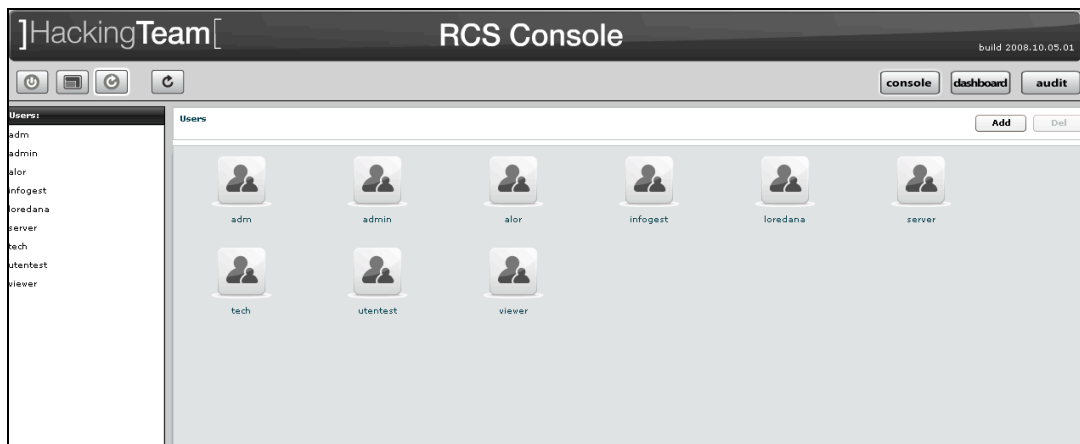
“Download” button is now enabled, click it to download selected logs.

Create an user

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



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

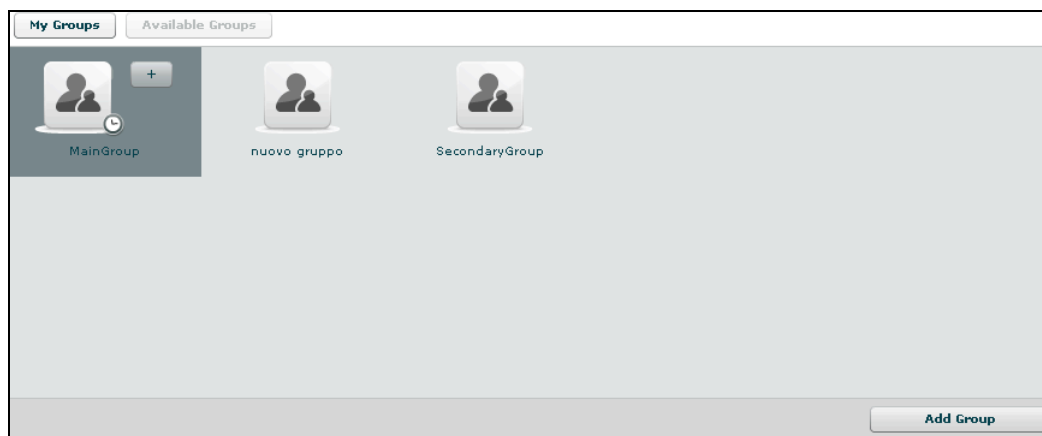


fill fields and assign privileges:

click “Save” button to save data.

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

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

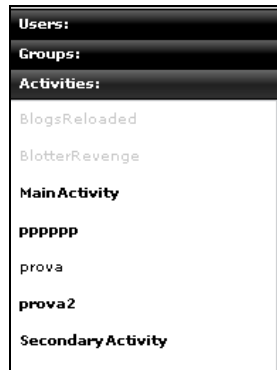


then either by:

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

Create a group

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



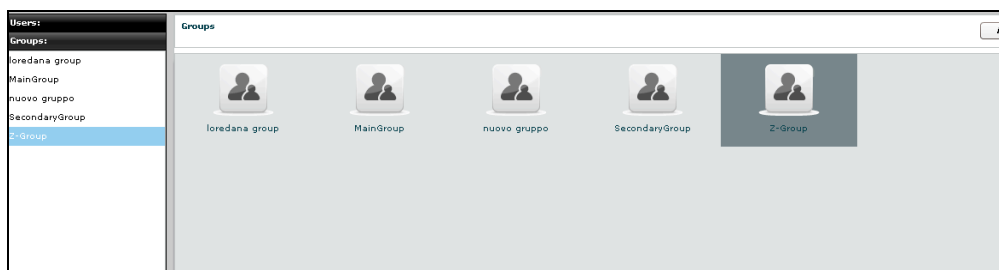
click “Add” button on the right at the top of the icons-list:



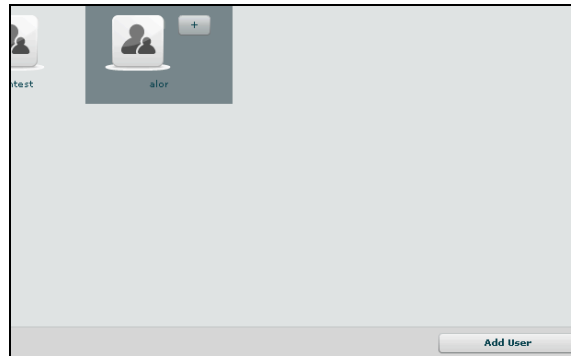
fill fields:

click “Save” button to save data.

Open new group:



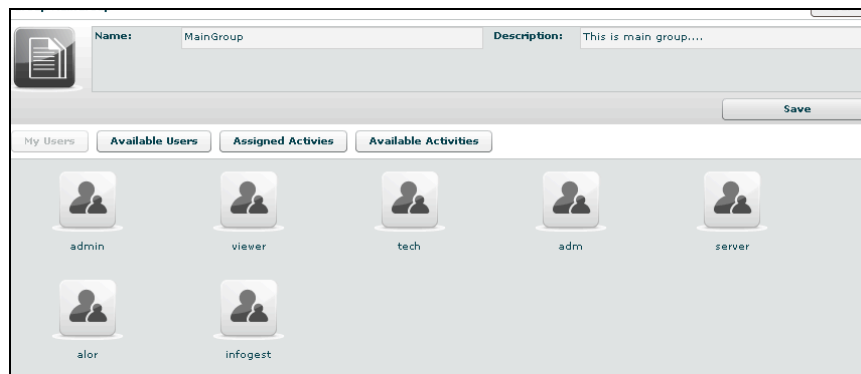
and to add a user to the new group, select user with a single click:



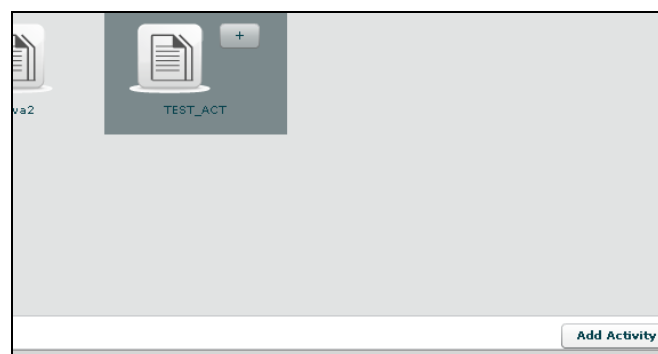
then either by:

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

Click “Available Activities” button to add activities



select activity with a single click:

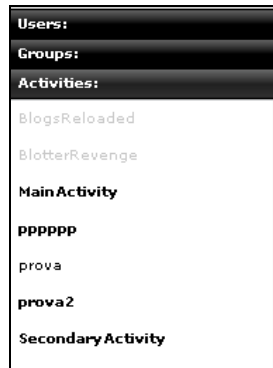


then either by:

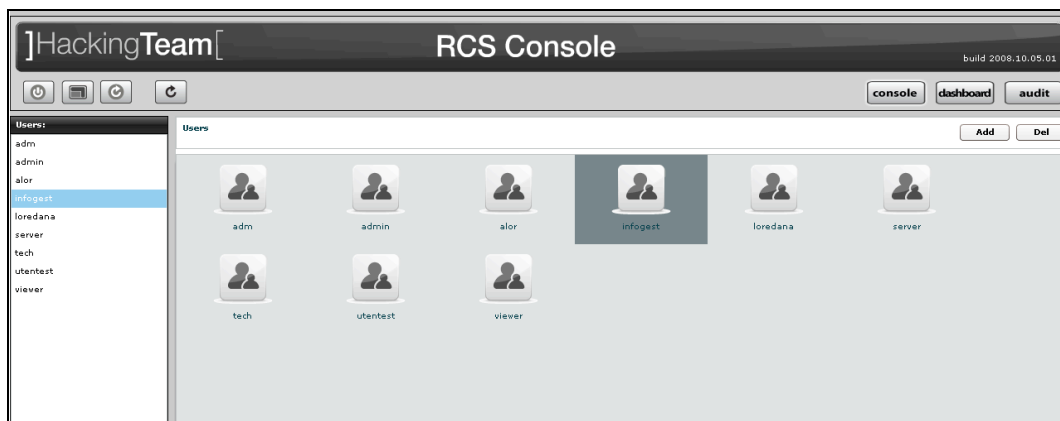
1. click “Add Activity” button on the left at the bottom of the window;
2. click “+” button next the icon’s activity.

Assign privileges to users

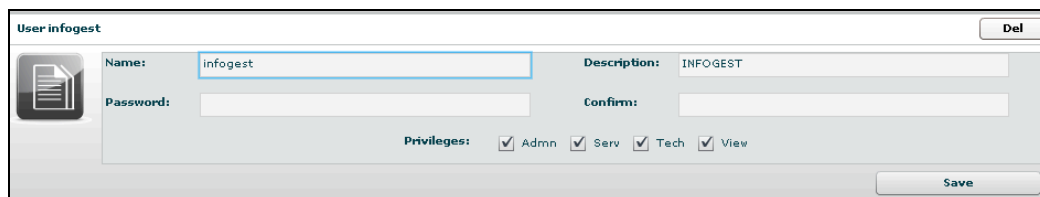
You need to be logged with Viewer profile. Start application and after successfully login, click tab “Users” on left menu:



and select an user:



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



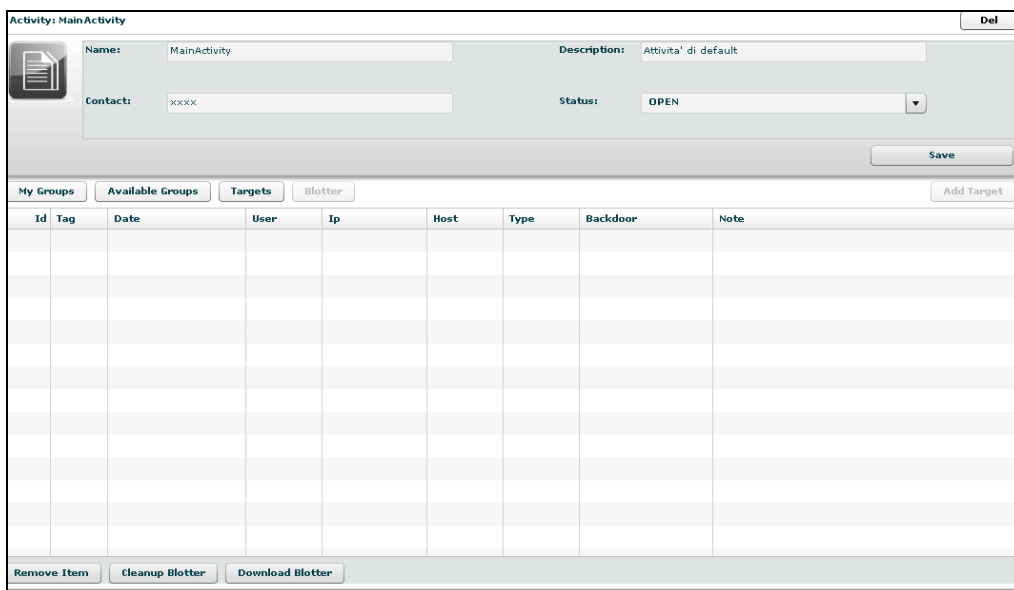
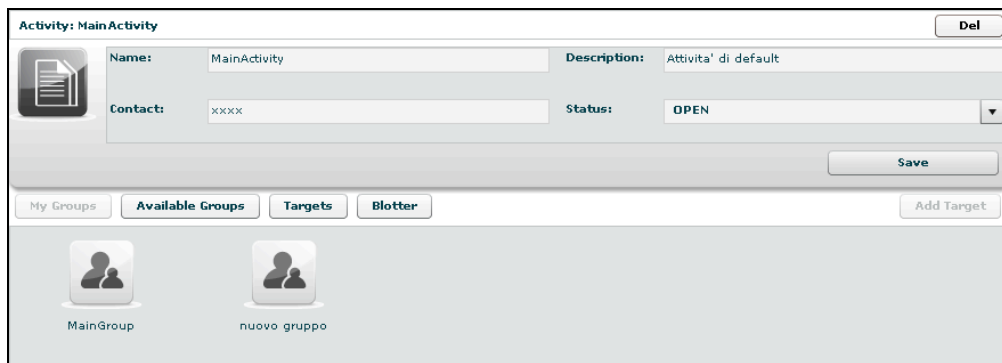
- Admn: this is the super user. It is the only one that can create users, groups, activity and targets;
- Serv: reserved role for the server components that require access to XML-RPC methods;
- Tech: this role can create, modify and reconfigure backdoors associated with a target, however the target can 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.

Create and manage blotter

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



then click "Blotter" button:



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

Id	Tag	Notes	Date	Resource	Service	UserId	Password
1937	<input checked="" type="radio"/>		29/08/2008 09:12:26	If4be5aac180c4	service	user	pass
1934	<input type="radio"/>		29/08/2008 09:12:24	c4903ba410c8d	service	user	pass
1216	<input type="radio"/>		20/08/2008 14:21:16	ac6d309a6119	service	user	pass
1211	<input type="radio"/>		20/08/2008 14:21:14	6f2fed8e62e67d	service	user	pass
1157	<input type="radio"/>		20/08/2008 14:20:34	4ff7d09f18c920	service	user	pass
1158	<input type="radio"/>		20/08/2008 14:20:34	69783ee76a925	service	user	pass
894	<input type="radio"/>		04/08/2008 15:49:49	f0eefcb44fc11	service	user	pass
878	<input type="radio"/>		04/08/2008 15:49:17	bbe3a23611885	service	user	pass
872	<input type="radio"/>		04/08/2008 15:49:04	86ad2abe9aa87	service	user	pass
864	<input type="radio"/>	1	04/08/2008 15:48:56	b5d3ad899f700	service	user	pass
837	<input type="radio"/>		04/08/2008 15:48:31	f89c3e51ae1975	service	user	pass
819	<input type="radio"/>		04/08/2008 15:48:14	4b8df49e7c73a1	service	user	pass
788	<input type="radio"/>		04/08/2008 15:47:58	0ede7c7ae62e0f	service	user	pass



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:

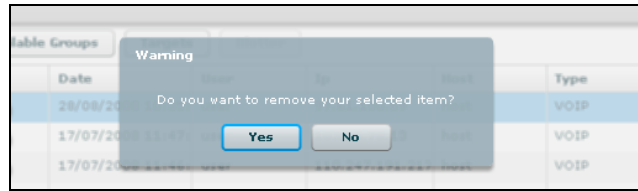
Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note
1992	<input type="radio"/>	10/09/2008 12:37:28	user	1.1.1.1	host	CLIPBOARD	RCS_136161	
1937	<input checked="" type="radio"/>	29/08/2008 09:12:26	user	201.61.41.240	host	PASSWORD	RCS_168921	
1157	<input type="radio"/>	20/08/2008 14:20:34	user	166.89.165.171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

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:

Id	Tag	Date	User	Ip	Host	Type	Backdoor	Note
1890	<input type="radio"/>	28/08/2008 10:35:11	user	97.61.150.69	host	VOIP	RCS_136161	
662	<input checked="" type="radio"/>	17/07/2008 11:47:00	user	103.16.78.13	host	VOIP	RCS_136161	
647	<input type="radio"/>	17/07/2008 11:46:00	user	110.247.191.217	host	VOIP	RCS_136161	

then click "Remove Item" button:

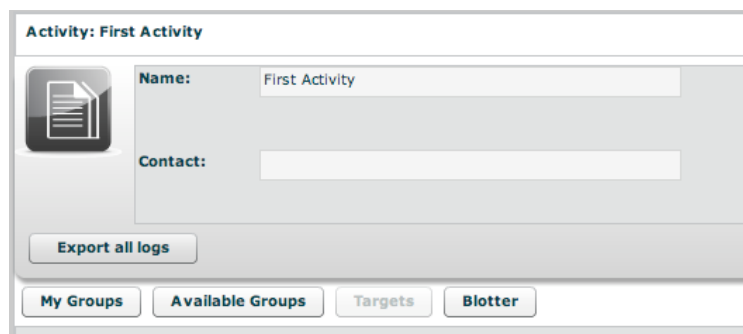


click "Yes" to confirm or "No" to exit.

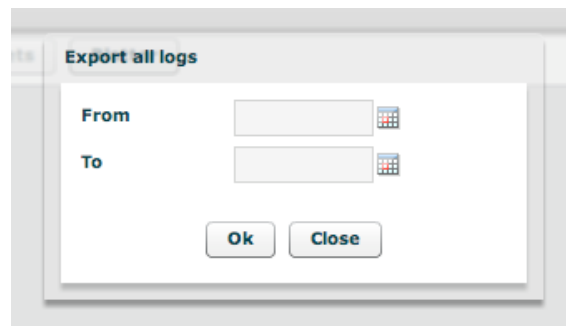
Click "Cleanup Blotter" button to clear blotter.

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

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



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



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