Project Rat-Trap: User Guide

Getting started

To start the client, simply execute the .jar file. There is no need to install or adding components. You should see now the connection manager. It looks like this:

profiles list	Profiles New Connection	Name New Connection Host Type host here	
		Path Type path here Port Type port here choose your homecountry	Connection data
buttons	New Save modified	Delete Connect	

Figure 1: Connection window

Creating a connection

To create a connection, simply click on "New Connection" in the "Profiles" list on the left and fill the following fields:

- Name: The name of the connection.
- Host: IP address or URL of your server.
- Path: The path where the servlet is stored on the server.
- Port: The port, over which client and server communicate
- Home country: Your country. Default is Zweibrücken, Germany.

While filling the fields, the "New" button becomes enabled. When finished, press the "New" button to create the new connection.

Modifying a connection

If you want to modify a connection, select it in the profiles list and change the connection data fields. Once you change something, the "Save modified" button becomes enabled and you can store the modified connection.

Connecting to the server

To connect to the server, choose a connection in the profiles list and double-click or press connect. Connecting is only possible with your own connections, not with the default "New Connection". Once the connection is established, the main window will open.

The main window

	Trojeccitat	Trap									
	Connection										
navigation	Overview World	view Chart Vie	ew								
	Identified harve	sters					Linked spam				
	ip	time	country	city	long	lat	server	country	city	long	lat
	143.93.17.28	2 Jul 2005	Germany	Frankfurt	8°41′E	50°07'N	217.252.34.193	GERMANY	null	13°25'E	52°30'N
	84.166.215.33	7 Jun 2005	GERMANY	null	13°25'E	52*30'N	195.71.11.67	GERMANY	null	13°25'E	52°30'N
	84.166.224.244	20 Jun 2005	5 GERMANY	null	13°25'E	52°30'N	not localized yet	not localized yet	not localized yet	not localiz	enot local
	84.166.225.215	5 2 Jun 2005	GERMANY	null	13°25'E	52°30'N	203.119.12.252	AUSTRALIA	null	149°08'E	35°17'S
	84.166.225.215	3 Jun 2005	GERMANY	null	13°25'E	52°30'N	12.40.51.219	United States of Am	neri Framingham	71°26W	42°18'N
	84.166.234.135	8 Jun 2005	GERMANY	null	13°25'E	52*30'N	64.236.24.12	United States of Am	neri Atlanta	84*24W	33°46'N
	84.166.246.234	9 Jun 2005	GERMANY	null	13°25'E	52°30'N	203.119.12.252	AUSTRALIA	null	149°08'E	35°17'S
	84.166.246.234	9 Jun 2005	GERMANY	null	13°25'E	52°30'N	12.40.51.219	United States of Am	neri Framingham	71°26W	42°18'N
	84 166 248 184	22 Jun 200	5 GERMANY	null	13°25'E	52°30'N	216 239 57 104	United States of Am	neri San Jose	121°52'W	37°18'N
									ana -		
							•		.11111		
							•		110		
									NUI		II.
							4		AUA		
							4				
							4				
			conter	nt window	7		<				
			conter	nt window]		د.][:

When connected correctly, the main window opens as shown below:

Figure 2: Main window

The client is able to show the following categories in the content window:

Linked connections – Overview

The tables show all linked connections between harvesters and spammers like in figure 2. Linked connections are pairs of harvesters and spammers, where a spammer has used the information of a harvester. This connection is displayed by showing the harvester on the left and the spammer on the right.

World view

This view visualizes the connections shown in the overview table. There are three visualization modes, which can be selected with the content navigation (s. figure 3):

- 1. Tracked spammers: This visualization mode shows the tracked and linked spammers. The red dots show the spammer's origin, and are connected by curves to the point, you determined, when creating your connection. One curve means one connection, many connections merge to a thicker curve.
- 2. Tracked harvesters: This visualization mode shows tracked and linked harvesters. The visualizations work the same way like described in 1) but harvesters are marked with green dots and curves.
- 3. Links between harvesters and spammers: This mode shows the origins of spammers and harvesters. Curves mark connections between the groups. A curve symbolizes one connection like shown in the overview window. The more connections in the same places appear, the more curves merge, which is shown by thicker curve lines.



Figure 3: World view

Chart view

This view shows details of the linked spammers and harvesters, using pie chart diagrams. There are four kinds of charts, which can be selected with the content navigation (s. figure 4):

- 1. Origin of spam: This chart shows the countries, where spam originates.
- 2. Origin of harvesters: This chart shows the countries, where the harvesters come from.
- 3. Harvester intelligence: This chart shows the harvesters and their intelligence. A higher intelligence means that the harvester can decipher more notations of e-mail addresses.
- 4. User agents: This chart shows the user agents, used by the harvesters.



Figure 4: Chart view