

Testing Rapport 912.25 against specified Keyloggers & Screen Capture

FINAL REPORT

- Spy Shelter security test tool
- Zemana keylogger simulation test tool
- Zemana screenlogger simulation test tool
- Zemana SSL-Logger test tool
- Zemana Extreme Leak Test Runner
- Amecisco Invisible Keylogger

22ND MARCH 2010

VERSION: 1.0

RLR UK LTD.

© 2010 RLR UK Ltd. This report may only be reproduced or stored in full with the disclaimer and disclosure included.

DISCLAIMER

Access to or use of this report is subject to the following conditions:

1. The information in this report is subject to change by RLR UK without notice.
2. The information in this report is believed to be correct by RLR UK at the time of publication.
3. No guarantee of the accuracy of the information in this report is given.
4. RLR UK is not liable or responsible for any damages, losses or expenses incurred from any error or omission in this report. All use and reliance on this report are at the reader's sole risk.
5. No warranties, express or implied, are given by RLR UK.
6. In no event shall RLR UK be liable for any consequential, incidental or indirect damages, or for any loss of profit, revenue, data, computer programs or other assets.
7. All trademarks contained in this report are the trademarks of their respective owners.
8. This report does not imply any endorsement, sponsorship or affiliation with any organisation or product contained within.

FULL DISCLOSURE

This report was commissioned by Trusteer, but no commercial affiliation exists between Trusteer and RLR UK.

EXECUTIVE SUMMARY

This report shows the findings of a test of Rapport version 912.25 against specified spyware. Not all possible test scenarios have been undertaken and, due to this, there may be other issues not covered here.

In the tests performed, Trusteer's Rapport did protect against keylogging and screen capture of the specified spyware. Rapport also blocked the capturing of the SSL session. The results are summarised below.

Rapport	OS	Spy Shelter	Zemana Key	Zemana Screen	Zemana SSL	Extreme + Shelter	Extreme + Key	Extreme + Screen	Extreme + SSL	Amecisco
912.25	XP SP1a									
912.25	XP SP3									

Zemana Extreme Leak Test Runner appeared to have no effect on using the above tools against Rapport.

Some digital leakage is possible, in that the same character will always appear as the same letter in the keylogged data, e.g. if the user's PIN is '1111' then the output in the keylogger would be 'aaaa', showing that all four digits are the same. In addition, Zemana KeyLogger and Amecisco picked up the use of the SHIFT key, therefore revealing whether password characters are in upper or lower case. This does not reveal the actual passwords or PIN numbers though, it only reduces the search space slightly in most cases. No other issues were observed.

CONTENTS

DISCLAIMER.....	2
FULL DISCLOSURE	2
EXECUTIVE SUMMARY	3
CONTENTS	4
ABOUT RLR UK LTD.....	5
CONTACT DETAILS	5
METHODOLOGY	6
The Test Machine	6
The Tested Sites	6
Keyloggers & Screen Capture Software Used	7
TEST RESULTS	8
XP SP1a IE 6.....	8
XP SP3 IE 8.....	9
Zemana SSL-Logger Test Tool.....	9
Conclusions	11

ABOUT RLR UK LTD

RLR UK is a private, independent specialist secure IT services company, focusing on providing complete and end-to-end solutions in the information security market. RLR UK provides a range of specialist Consulting, Professional, Research and Bespoke Training Services.

As a specialist in information security, our expertise lies in identifying, analysing and minimising network and system security risks and offering comprehensive solutions that address the total IT requirements of our customers, allowing them to grow and achieve their business goals securely.

CONTACT DETAILS

Web: <http://www.rlr-uk.com>

Email: enquiries@rlr-uk.com

Tel: +44 (0)20 3137 0372

METHODOLOGY

The purpose of this test was to determine the level of protection that Emerald Build 0912.25 of Trusteer's Rapport provides to users against a set of keyloggers and screen capture malware. The default installation with all 13 security controls enabled was used for both Rapport installations.

RLR UK employs scientific methodologies when conducting any tests and all information is meticulously recorded during the tests. Every effort is made to avoid mistakes.

The Test Machine

In order to test Rapport against various malware it is essential that the starting point for every test be identical. All the tests were carried out on the same machine and Comodo's Time Machine was used to roll back the configuration of the test machine between each test, so that a fresh install of the malware and Rapport was performed each time.

Every test was performed consecutively from a fresh install. Other than Comodo's Time Machine, Trusteer's Rapport and the malware in question, no other software was installed on the machine that isn't part of a standard installation of the Operating System and browser. Operating Systems and browsers were installed with their default options and no additional components were installed. There was no anti-malware installed or configured on the test machine.

The machine was rebooted when required by the logging software and after installation of Rapport. Installation of Rapport and the logging software was controlled, such that in one set of tests Rapport was installed first and the logging software afterwards and in the second set of tests the logging software was installed first and Rapport afterwards.

The Tested Sites

Two of Trusteer's customers' sites were tested with the malware and machine configurations: NatWest's Online Banking (<https://www.nwolb.com>) and HSBC's Personal Internet Banking (<http://www.hsbc.co.uk/1/2/HSBCINTEGRATION/CAM10>). The test data entered into each site was as follows:

NatWest

Customer Number: 1203631234

PIN: 123

Password: XYZ

HSBC

Internet Banking User ID: IB1234567890

Date of Birth: 120363

Security number: 124

Rapport was not tested against any other sites and its personal site protection was not tested. All tools used successfully logged www.google.co.uk where standard searches for the two bank websites were completed to ensure that the loggers were working.

Keyloggers & Screen Capture Software Used

A variety of tools were used to test Rapport, with a mixture of test tools and commercial spy software. The selection of tools was based on reports received of possible successful logging when running Rapport and those specified by Trusteer.

- Spy Shelter security test tool
- Zemana Keylogger simulation test tool
- Zemana ScreenLogger simulation test tool
- Zemana SSL-Logger test tool
- Zemana Extreme Leak Test Runner
- Amecisco Invisible Keylogger

All but the final one in the list are test tools and do not require installation. The final one requires installation. All tools were used with default settings in this test. Zemana Extreme Leak Test Runner is not a leak testing tool itself, but can be used to run other tools with potentially greater success.

TEST RESULTS




Tests were performed on two versions of Windows XP Professional, namely SP1a and SP3. Also, two different versions of Internet Explorer were used: IE 6 on XP SP1a and IE 8 on XP SP3. This was done to show two extremes of usage on Windows XP – SP1a is the minimum requirement for Rapport to install. Tests were run with Rapport being installed both before and after Amecisco, to test whether order was important.

XP SP1a IE 6

The first set of tests was performed on Windows XP SP1a running Internet Explorer 6.0.2800.1106 with the Automatic Phishing Filter turned off. Tests were run using the UK keyboard locale only, UK as default and US as an additional locale and US only. The results of the tests are summarised in the table below. The 'Order' column specifies whether Rapport was installed first, before the spyware, or second, after the spyware.

Locale	Order	Spy Shelter	Zamana Key	Zamana Screen	Extreme + Shelter	Extreme + Key	Extreme + Screen	Amecisco
UK	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
UK	2 nd	-	-	-	-	-	-	✓ ↑
UK (US)	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
UK (US)	2 nd	-	-	-	-	-	-	✓ ↑
US	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
US	2 nd	-	-	-	-	-	-	✓ ↑

Key

-  Rapport blocks spyware
-  Rapport blocks spyware, but there is an issue
-  Rapport does not block spyware or only partially blocks the spyware
- ↑ Use of SHIFT key detected




As can be seen from the table above, Rapport blocks the specified spyware and spyware testing tools in this configuration.

XP SP3 IE 8

The second set of tests was performed on Windows XP SP3 running Internet Explorer 8.0.6001.18702 installed with 'Express Settings', including SmartScreen Filter. As before, Rapport was put through the same tests with the same results. The results of the tests are summarised in the table below. The 'Order' column specifies whether Rapport was installed first, before the spyware, or second, after the spyware.

Locale	Order	Spy Shelter	Zamana Key	Zamana Screen	Extreme + Shelter	Extreme + Key	Extreme + Screen	Amecisco
UK	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
UK	2 nd	-	-	-	-	-	-	✓ ↑
UK (US)	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
UK (US)	2 nd	-	-	-	-	-	-	✓ ↑
US	1 st	✓	✓ ↑	✓	✓	✓ ↑	✓	✓ ↑
US	2 nd	-	-	-	-	-	-	✓ ↑

Key

-  Rapport blocks spyware
-  Rapport blocks spyware, but there is an issue
-  Rapport does not block spyware or only partially blocks the spyware
- ↑ Use of SHIFT key detected

These results are the same as the previous version of Rapport

Zemana SSL-Logger Test Tool

This application is designed to extract the secure plaintext traffic from an SSL encrypted session and displays common login details contained within the requests. The SSL-Logger tool was used on the system before Rapport was installed to test functionality. The testing was slightly different for this tool.

The same two partner websites were tested (i.e. NatWest and HSBC), but Google login was also tested as a third unprotected 'control' site. Without Rapport installed, Zemana SSL-Logger will see Google, NatWest and HSBC connections. It lifts Google credentials and the

HSBC Internet Banking User ID as identified login credentials. Zemana SSL-Logger is looking for specific common control names for login credentials. HSBC uses 'userId', which is picked up, they also use 'password' as a control name and the final control contains '_dob' at the end. These will be picked up automatically. NatWest uses "ct100\$mainContent\$LI5TABA\$DBID_edit", which is not automatically picked up, but could be extracted if all the information were dumped. NatWest use similar naming conventions for their PIN and Password entry input fields. Google uses 'Email' and 'Passwd', which are automatically picked up.

Zemana SSL-Logger was then used on its own and with Zemana Extreme Leak Test Runner against Rapport, logging into the three sites mentioned above. The results are summarised in the table below, but it can be seen that Rapport successfully protected all three sites and absolutely no data was retrieved by Zemana SSL-Logger.

OS	Locale	Zemana SSL-Logger			Zamana Extreme + SSL-Logger		
		Google	NatWest	HSBC	Google	NatWest	HSBC
XP SP1a	UK						
XP SP3	UK						
XP SP1a	UK (US)						
XP SP3	UK (US)						
XP SP1a	US						
XP SP3	US						

Key

- Rapport blocks spyware
- Rapport blocks spyware, but there is an issue
- Rapport does not block spyware or only partially blocks the spyware

One notable observation is that with Rapport installed on the XP SP3 machine running IE 8, on exiting the web browser and the Zemana SSL-Logger tool, explorer.exe crashed and had to be restarted. This did not happen if Rapport was not installed, nor did it happen under XP SP1a with IE 6. This is not considered an issue as Rapport in itself does not cause this to happen.

Conclusions

Rapport appears to combat many different spyware applications, which will increase the security of those installing it. Rapport was able to successfully defeat all the specified spyware in these tests.

Rapport protected the SSL sessions of all sites in the test, whether they are protected partner sites or 'unprotected' other sites. This will keep users' credentials safe on all sites, not just these banks.

This test has only included two very specific OS configurations and one browser type. In order to fully test Rapport, additional testing would be required under different browsers and OSes. Most notably of these would be the need to test Firefox and both Windows Vista and Windows 7.