



Efficacy Assessment of Trusteer Rapport

August 2010

Contents:

Introduction	2
Version of the Application Tested	2
Penetration Test Tools used	2
Methodology used in the Test	3
Test Results	3
Conclusions	3

Introduction:

Malware Research Group published the first comparative assessment of browser security products in March 2010. Since this time, there have been several new versions of the security applications released and therefore the results of the March test are obsolete.

The purpose of this report is to provide an up to date assessment of the efficacy of the most recent version of one of the original applications tested, this being, Trusteer Rapport.

Trusteer Rapport is a dedicated browser security application, designed to prevent data theft during internet banking sessions

Version of the Applications Tested:

- Trusteer Rapport - Emerald Build 1003.9 – 23248

Penetration Test Tools used:

In order to simulate the actual mechanisms financial malware employ to capture data, we used the following test tools:

- Spy Shelter Security Test Tool 1.3 (key Logging, Screenshots – ten methods and Clipboard Monitoring), which will be referred to as **SS Key, SS Screen & SS Clip** respectively.*
- Zemana Keylogger Simulator 1.5.2.70 which will be referred to as **Z Key**.
- Zemana ScreenLogger Simulation Test v 1.0.0.33, which will be referred to as **Z Screen**
- Zemana SSL-Logger Simulation Test v 1.5.2.83, which will be referred to as **Z SSL**.
- Malware Research Group Keylogger Simulator V1.0, which will be referred to as **MRG Key**.
- Malware Research Group Screenlogger Simulator V1.0 which will be referred to as **MRG Sc**.
- Malware Research Group Financial Malware Simulator V2.0s, which will be referred to as **MRG FMS**. See below for details of this tool.
- Zemana Extreme Leak Test Runner 1.0.0.0, tests will have the suffix **(ZE)** when run via this utility. See below for explanation of its functionality.
- Amecisco Inc. Invisible KeyLogger, which will be referred to as **IKS**, an advanced kernel level keylogger.

* = All ten screen capture techniques need to be blocked to receive a pass.

The MRG Financial Malware Simulator is a tool developed by Malware Research Group to properly simulate a zero day piece of financial malware. The simulator is used to accurately model how real financial malware behaves on a system in the real world.

The simulator, once executed, infects the system and then will capture data the users in to Internet Explorer on a range of secured banking sites. This logon data, once captured, is then sent out of the system, bypassing any firewall, to the results page on the MRG website.

The Zemana Extreme Leak Test Runner (**ZE**) enhances the effectiveness of various simulation tools by faking the original path of the test tool with one that appears to come from a legitimate MS OS location and thereby bypasses most HIPS systems.

Methodology used in the test:

1. Windows XP Professional Service Pack 3 is installed and updated with all important updates.
2. A folder containing the penetration test tools detailed is copied to the desktop.
3. An image of the Operating System is created.
4. A clone of the Imaged system is made for the security application to be used in the test.
5. The security application is installed using default settings on the Cloned system.
6. The clone is cloned 18 times, thus making 18 copies of the system created in step 5.
7. The test is conducted by running one of the penetration test tools on each of the 18 copies of the system.
8. Text is entered in to the “User ID” and “Password” fields of the account login page of the <http://www.yourbankhere.com/bank/index.php> site, using either the keyboard or copying from Windows Notepad, depending on which Penetration Test Tool is used and then selecting the “Login” button.
9. A test is deemed to have been passed if the security application identifies / blocks the specific threat posed by the test tool. A security application which, for instance only detects the global hook used to instigate the SSL sniffer in the ZLL Test Tool and not the sniffer itself will be deemed to have failed that test.
10. Testing is conducted with all systems having internet access.
11. Testing was conducted on 02 August 2010 and repeated by a different tester to verify results.

Test Results:

Application Name	SS Key	SS Screen	SS Clip	SS Key (ZE)	SS Screen (ZE)	SS Clip (ZE)	MKG Key	MKG Sc	MKG Key (ZE)	MKG Sc (ZE)	MKG FMS	SSL	Z Key	Z Screen	Z Key (ZE)	Z Screen (ZE)	SSL (ZE)	IKS
Trusteer Rapport	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Trusteer Rapport passed all 18 tests. Most significant of all is that it blocks the Financial Malware Simulator. We have tested eighteen of the most popular internet security suites against this simulator and only two were able to block its action under the conditions used in this report.

Conclusions:

Malware Research Group has had regular communication with the vendor since the publication of the first test in March. We now note that Trusteer Rapport has “configurations” which are determined by the bank which provides the product to their customers. These configurations may be such that a particular protection ability of the product is disabled.

When we tested in March, we were unaware of this configuration issue and did not realise we were using a version that had elements of protection disabled. This test makes use of a version which has all protection features enabled and so gives a more accurate representation of the products performance.

Malware Research Groups recent primary focus has been on browser security and online banking. We have spent some considerable time assessing numerous security applications and various threat categories in this area and feel we are one of the leading research and assessment organisations in this field. With this in mind, we point out that we are currently unable to bypass the browser security protection provided by Trusteer Rapport, using third party or our own, proprietary penetration tools or simulators.