Trusteer Rapport

# Malware Assessment Using Banking Trojans

March 15th 2012

MANDIANT®

INTELLIGENT INFORMATION SECURITY

## Table of Contents

# Executive Summary

Trusteer contracted Mandiant to perform a security assessment of Rapport, a client software security solution. The purpose of this assessment was to see how Rapport performed against 25 Trojans that steal financial-based credentials from a victim. The tests were conducted on a non-virtualized computer network connected to the Internet. All tests were carried out in Mandiant’s lab using Mandiant equipment. The victim machine was a non-virtualized 32-bit Windows 7 machine. Additional details of the test environment are detailed below. During February 2012, Mandiant independently collected all malware samples used for testing as described below. The final test of Trusteer Rapport took place on March 1, 2012.

## Results

Trusteer Rapport neutralized[1] all 25 banking Trojans tested by Mandiant. Trusteer did not have access to the malware before Mandiant performed the test.  Rapport remained functional after each malware test.

[1] Neutralized means that the malware is blocked, terminated and not started again on system reboot.

## About Rapport

Mandiant tested Trusteer Rapport Emerald Build 1108.70. Rapport was connected to the Internet, so that it could update its configuration if needed.

Additional information about the Rapport product is found at:

- http://www.trusteer.com/product/trusteer-rapport

# Malware

## Origin of Malware

Mandiant's malware analysis team has an extensive collection of labeled and organized malicious code samples. For malware samples not found in the Mandiant collection, Mandiant reached out to its extensive list of contacts within the private and public sectors of the security community. Mandiant works with two large organizations that have access to millions of labeled samples.

All samples were obtained during February 2012. Trusteer did not have access to the malware before Mandiant performed the test.

## Malware Validation

Mandiant analyzed all 25 malware samples prior to conducting any test of the Rapport security tool. There are two reasons for performing analysis before the test:

1. To confirm the family of each malware sample.
2. To determine the malware's network- and host-based indicators.

Network- and host-based indicators help Mandiant validate the success or failure of individual tests of Trusteer Rapport. These indicators are checked before each test to confirm that the malware was installed properly without Rapport installed. These indicators are checked again during a test to see if the Rapport successfully neutralizes the malware.

Network-based indicators: This includes beacon packets and DNS requests.  These indicators are discovered using Wireshark.

Host-based indicators: This consists of live memory byte signatures in the form of YARA signature. YARA[2] is a malware analysis tool that allows you to quickly scan live memory to find evidence of active malware on a host.

## Malware Samples

For the assessment, Mandiant selected 5 of the most common Trojans that attack the browser in an attempt to steal a user's financial information.

### Zeus

Zeus is a Trojan that steals banking information via keylogging and form grabbing. It is spread by phishing schemes and deceptive browser pop-ups. Zeus has infected millions of machines worldwide. Zeus has had two major revisions which are classified here as Zeus1 and Zeus2.

### SpyEye

SpyEye is a banking Trojan similar to Zeus. It captures keystrokes, performs form grabbing, and sends the captured data to a remote attacker. SpyEye is notable for its ability to inject new fields into a webpage.

### Bugat

Bugat is a banking Trojan that targets Internet Explorer and Firefox browsers to harvests information from victims during online banking sessions.

[2] http://code.google.com/p/yara-project/

### Carberp

Carberp is a banking Trojan that hooks network function calls within WININET.DLL to monitor browsing activities on an infected system. It covertly launches by injecting into common Windows processes like explorer.exe and svchost.exe to launch its main functionality.

### Shylock

Shylock is a banking Trojan that steals users credentials. It is packaged with many hiding mechanisms to avoid anti-virus detection.

The following table lists the 25 samples collected and used for the test:

| Malware Name | MD5 Checksum | Size |
|---|---|---|
| Bugat.A | 7802ff069a31dbebcdfbfc0858788aa2 | 53760 |
| Bugat.B | e92de5cc06a361575d24adbde4bf0e81 | 186609 |
| Carberp.A | f27e1e157b3964544aeb58b4de2cbe54 | 154112 |
| Carberp.B | 2b36b49baec741ba8e82ae32dca19906 | 92160 |
| Carberp.C | 4797452fc398ed98dc3b862e3d312865 | 462848 |
| Shylock.A | a8ff900f5f3134a1f04d9217ab2d5dd0 | 385592 |
| Shylock.B | 598621d8fbc21d766b6f416823df2db9 | 167936 |
| Shylock.C | 9e49bc5d094906d43b22d8fd677fe633 | 167936 |
| Shylock.D | d212e1c4c69ac9cc49b37105b31715d3 | 167936 |
| SpyEye.A | df04c2cd2b5f7e471cb0435fdb9b3014 | 115200 |
| SpyEye.B | 2dd9f7a8235fd17b33029b1471fb054a | 181760 |
| SpyEye.C | d69b970afe781b385b9c4856dd1690ea | 134656 |
| SpyEye.D | c38ae7bddb66c01af896f47bd27666ef | 290816 |
| SpyEye.E | 81b2eb00c162d35299f4ba5ad8298541 | 307200 |
| Zeus1.A | d030e469eb57187b051e06dd32429235 | 47104 |
| Zeus1.B | 772bfaa05a24fa07fe4c9a671984b0ed | 45056 |
| Zeus1.C | 82a9679951d0afeeb7d7de659b9ca7b3 | 44032 |
| Zeus1.D | cd0d3e4d6377729263419d558937b684 | 44544 |
| Zeus1.E | 9a66c30a771874314ec105be5e3b0972 | 51200 |
| Zeus1.F | 9a66c30a771874314ec105be5e3b0972 | 45056 |
| Zeus2.A | 90f22b1876df149aee86d3eb3ee16b84 | 42496 |
| Zeus2.B | 5576c826d454b69ade7617f1cb228de0 | 1882624 |
| Zeus2.C | ffa8bcce9732db6d47e50f7715d10562 | 230912 |
| Zeus2.D | 29b906dfbc0783225ea68286673cb52f | 152576 |
| Zeus2.E | 734a1f720d3d64b1f1bd53b9afc738aa | 159232 |

**Table 1 – List of 25 samples used for testing Rapport**

## Methodology

Mandiant set up a dedicated testing network and connected it directly to the Internet. All malware samples were validated prior to testing as described in the previous section.

### Network

The Mandiant test network consisted of two workstations setup as seen in the following diagram:

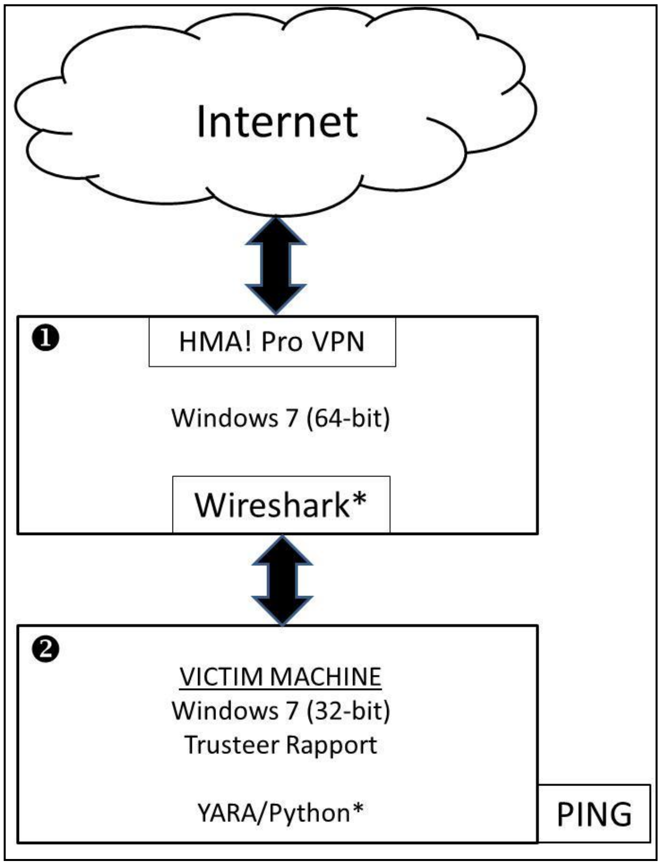


**Figure 1 – Mandiant malware assessment network**

The two machines consist of a router machine ❶ and victim machine ❷ connected to the Internet.

The router machine ❶ runs Windows 7 (64-bit) and is dual homed: one interface is connected to the Internet and the other is directly connected to the victim machine. The router machine acts as a router for the victim machine to access the Internet. The router machine runs HMA! Pro VPN[3] which allows the test network to remain anonymous on the Internet. HMA! Pro VPN hides the IP address of the router machine and encrypts all of its network traffic. This connection is shared with the victim machine. The router machine runs Wireshark to capture all network traffic leaving or destined for the victim machine. This enables Mandiant to quickly see the network-based indicators of active malware on the victim machine.

The malware is run on the victim machine ❷. This machine runs Windows 7 (32-bit) and has only Trusteer Rapport installed for malware protection. The victim machine was re-imaged after each test using PING[4] (Partimage Is Not Ghost). PING is a live Linux ISO that enables Mandiant to quickly

[3] http://hidemyass.com/vpn/
[4] http://ping.windowsdream.com/

reimage the victim machine after each test. The victim machine has Python and YARA installed. YARA is a malware analysis tool that allows us to quickly scan live memory to find evidence of active malware on the victim machine.

Wireshark and YARA provide us two ways to quickly detect malware activity. The majority of the malware samples used in this test had solid network-based indicators and live memory signatures to identify active samples. Neither Wireshark nor YARA interfere with how malware operates on the victim machine.

### Test Workflow

Before Rapport Installation:

1. Launch malware on victim machine
2. Confirm malware network- and host-based indicators are seen with YARA and Wireshark
3. Re-image the victim machine using PING
4. Repeat 1-3 for each of the 25 malware samples

With Rapport Installed:

1. Launch the Rapport console to confirm that it is running
2. Launch malware on victim machine
3. Check to see if Rapport reports or logs the infection
4. See if Rapport neutralizes the malware by looking for network- and host-based indicators
5. Confirm that Rapport and the system are still functional
6. Re-image the victim machine using PING
7. Repeat 1-3 for each of the 25 malware samples

## Final Results

The results are shown in the following table:

| Malware Name | Neutralized? |
|---|---|
| Bugat.A | Success |
| Bugat.B | Success |
| Carberp.A | Success |
| Carberp.B | Success |
| Carberp.C | Success |
| Shylock.A | Success |
| Shylock.B | Success |
| Shylock.C | Success |
| Shylock.D | Success |
| SpyEye.A | Success |
| SpyEye.B | Success |
| SpyEye.C | Success |
| SpyEye.D | Success |
| SpyEye.E | Success |
| Zeus1.A | Success |
| Zeus1.B | Success |
| Zeus1.C | Success |
| Zeus1.D | Success |
| Zeus1.E | Success |
| Zeus1.F | Success |
| Zeus2.A | Success |
| Zeus2.B | Success |
| Zeus2.C | Success |
| Zeus2.D | Success |
| Zeus2.E | Success |

**Table 2 – Rapport Test Results**

Trusteer Rapport neutralized[5] all 25 malware samples tested by Mandiant.  Rapport notified the user or logged the exact name of the Trojan in the vast majority of the tests. Rapport remained fully functional after each malware test.

[5] Neutralized means that the malware is blocked, terminated and not started again on system reboot.

## About Mandiant

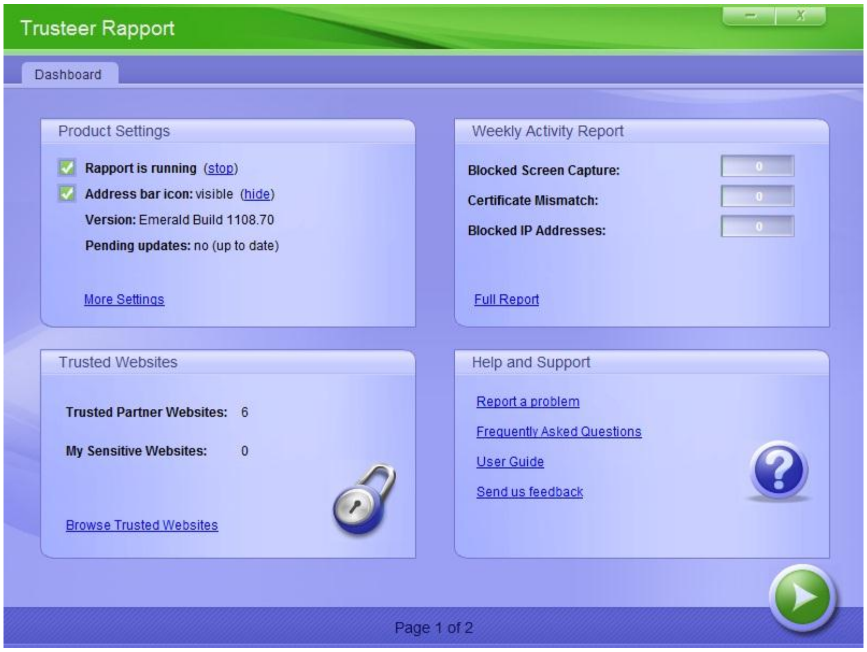
Mandiant provides industry leading information security services to help our customers overcome their most challenging problems. Our team is equally adept at building strong programs that minimize disturbances as well as helping clients rapidly respond to incidents and resume business.  Our services are a blend of proactive efforts required to build secure network environments as well as reactive services that enable you to respond to events and intrusions in a timely and effective manner.

Mandiant has extensive experience in dealing with malware. As one of the largest incident response organizations, Mandiant has analyzed thousands of pieces of malware, ranging from targeted malware as used by the APT to non-targeted malware such as the financial malware included in the scope of this engagement. Mandiant has a dedicated team of malware analysts. The members of this group are responsible for tracking, reverse engineering, and analyzing malware; and conducted this test.

## Appendix A – Example Test Flow

The following is an example of a single malware test. In this instance, we used `SpyEye.A` (described in Table 1). We start with a clean baseline image (32-bit Windows 7) with Rapport installed.

1. We launch the Rapport console to confirm that it is running and up to date as seen in Figure 2. "Rapport is running" and "no" pending updates are seen in the console. We also check that the machine has a valid connection to the Internet by launching a web browser.



Trusteer Rapport

Dashboard

Product Settings

☑ **Rapport is running** (stop)

☑ **Address bar icon:** visible (hide)

**Version:** Emerald Build 1108.70

**Pending updates:** no (up to date)

More Settings

Weekly Activity Report

| | |
|---|---|
| **Blocked Screen Capture:** | 0 |
| **Certificate Mismatch:** | 0 |
| **Blocked IP Addresses:** | 0 |

Full Report

Trusted Websites

| | |
|---|---|
| **Trusted Partner Websites:** | 6 |
| **My Sensitive Websites:** | 0 |

Browse Trusted Websites

Help and Support

Report a problem

Frequently Asked Questions

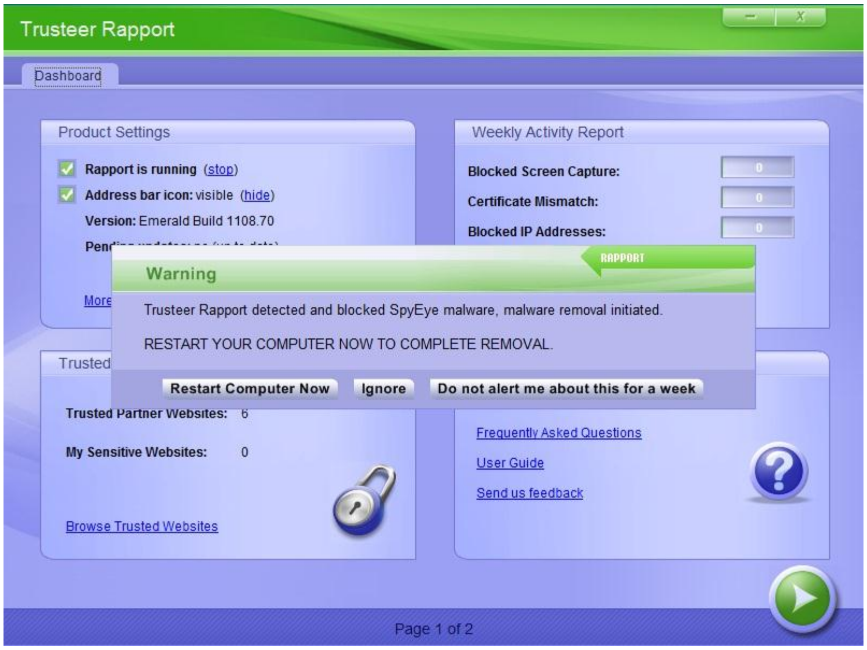
User Guide

Send us feedback

Page 1 of 2

**Figure 2 – Active Rapport console**

2. Next, we launch `SpyEye.A` as an administrator user on the victim machine.
3. We wait a short amount of time to see if Rapport reports or logs the infection. After a short duration we see the alert "Trusteer Rapport detected and blocked SpyEye malware" as seen in Figure 3. Rapport is requesting a system reboot, so we click "Restart Computer Now" to force a system reboot.



☑ Rapport is running (stop)
☑ Address bar icon: visible (hide)
Version: Emerald Build 1108.70

Blocked Screen Capture: 0
Certificate Mismatch: 0
Blocked IP Addresses: 0

Warning

Trusteer Rapport detected and blocked SpyEye malware, malware removal initiated.

RESTART YOUR COMPUTER NOW TO COMPLETE REMOVAL.

Trusted Partner Websites: 6
My Sensitive Websites: 0

**Figure 3 – Rapport alerting on SpyEye and requesting to reboot**

4. After the system reboot, we check to see if Rapport prevented the malware from launching by looking for network- and host-based indicators. We don't see any network traffic in Wireshark from `SpyEye.A`. We also scan live memory using our Yara signatures and we don't find any of our host-based signatures for `SpyEye.A`. We conclude that Rapport prevented the `SpyEye.A` malware from running on the system.
5. Next, we confirm that Rapport and the system are still functional by launching the console and launching a web browser on the local system.
6. Finally, we re-image the victim machine using PING so that we can start with a clean baseline image for the next malware test.