MRG

Internet Security & Solutions

Online Banking Browser Security Project - April 2010

Contents:

Introduction:

As we discussed before, in our first test, financial malware represents a significant threat to banks and their customers. An estimated 1% of PCs worldwide are infected with this malware and research shows, having an up to date antivirus only reduces the chance of infection by about 25%.

Financial malware is difficult to detect by design. It uses sophisticated techniques to evade detection, each type has thousands of unique variants and it is updated regularly.

The purpose of this project is to simulate as accurately as possible a scenario where a new piece of financial malware is released in to the wild.

MRG had developed a tool that simulates the behaviour of real financial malware. The tool once executed, permanently infects the system and is designed to capture data entered in to banking sites, bypass any firewall and send the captured data out of the system to our test page.

The tool uses some sophisticated techniques, but has some built in weaknesses, so it should be possible for it to be detected in time.

We conducted initial test on 18 April 2010 and have given feedback to vendors. As of 03 May 2010, we will re run the test every day for fourteen days or until it is detected by a good proportion of the antimalware products and the results will be published in real time on our test site.

Once the malware simulator is detected by most of the antimalware applications, we will start the test again using a more advanced test tool. Once this new tool is well detected, we will begin again with an even more sophisticated simulator. This process should represent the evolution and increase in sophistication exhibited by real malware.

Applications which have passed the initial test in each phase will obviously not be included in the remainder of the phase.

Applications which fail and do not have the ability to "learn" new threats will also be excluded. We will work with these vendors to help them improve their product.

This simulator is potentially very dangerous, therefore, we have included a safety feature which allows us to disable it instantly, should the need arise.

The simulator has never been exposed to any security applications, so accurately represents a zero day threat.

We will not provide any information about the simulator to the remaining vendors whilst the 14 day testing phase of the project is running. Vendors who have a support contract with MRG will be given feedback, along with a technical overview of the simulator and allowed remote access to it in our labs at the end of this first phase, however, we will not release the simulator itself.

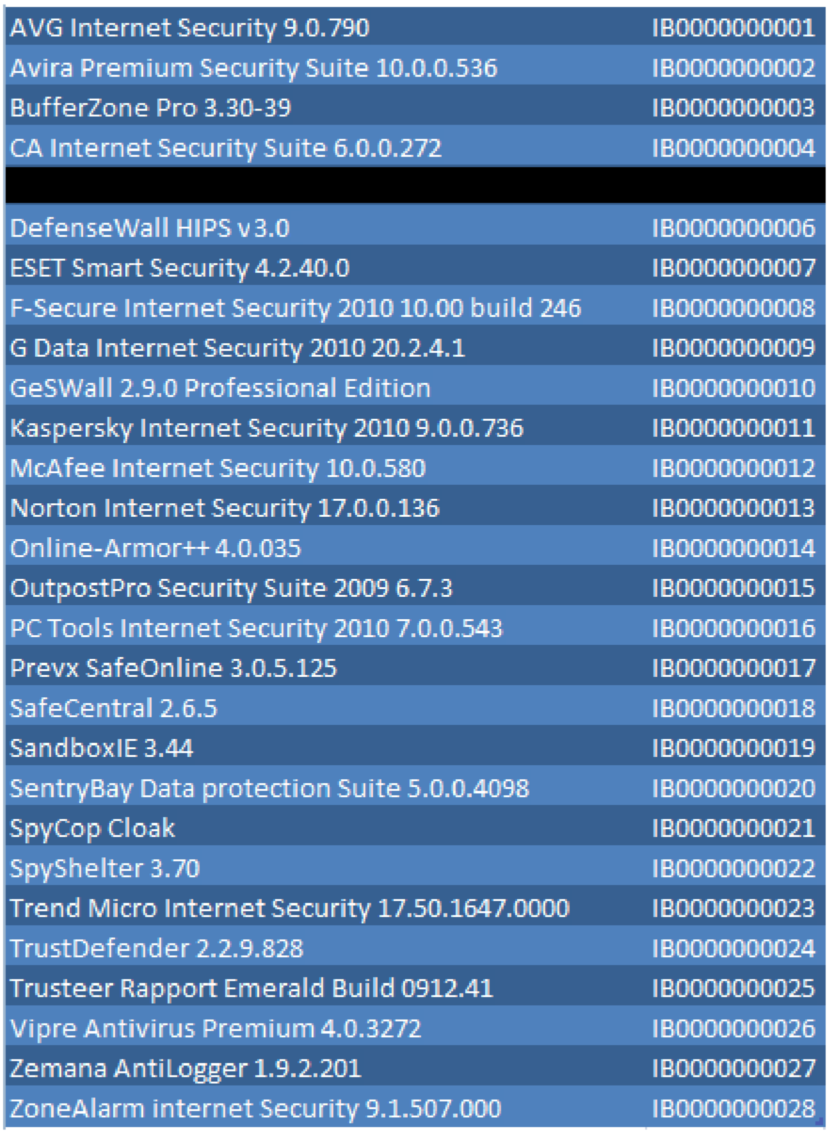
Security Applications Tested:

We have chosen 28 applications made up of full internet security suites to dedicated identity / browser security utilities. Each of these purports to provide security for online activities, or is specifically designed to secure browsers for online banking.

Because of the "live" nature of the testing in this project, with captured data being sent directly to our test page in real time, we have assigned each application a unique code.

When each of the security applications is tested, we will enter its unique code in to the User ID field on the backing site, thus we will be able to identify which applications fail the test.

The applications and their unique code are detailed below:



AVG Internet Security 9.0.790	IB0000000001
Avira Premium Security Suite 10.0.0.536	IB0000000002
BufferZone Pro 3.30-39	IB0000000003
CA Internet Security Suite 6.0.0.272	IB0000000004
[redacted]	[redacted]
DefenseWall HIPS v3.0	IB0000000006
ESET Smart Security 4.2.40.0	IB0000000007
F-Secure Internet Security 2010 10.00 build 246	IB0000000008
G Data Internet Security 2010 20.2.4.1	IB0000000009
GeSWall 2.9.0 Professional Edition	IB0000000010
Kaspersky Internet Security 2010 9.0.0.736	IB0000000011
McAfee Internet Security 10.0.580	IB0000000012
Norton Internet Security 17.0.0.136	IB0000000013
Online-Armor++ 4.0.035	IB0000000014
OutpostPro Security Suite 2009 6.7.3	IB0000000015
PC Tools Internet Security 2010 7.0.0.543	IB0000000016
Prevx SafeOnline 3.0.5.125	IB0000000017
SafeCentral 2.6.5	IB0000000018
SandboxIE 3.44	IB0000000019
SentryBay Data protection Suite 5.0.0.4098	IB0000000020
SpyCop Cloak	IB0000000021
SpyShelter 3.70	IB0000000022
Trend Micro Internet Security 17.50.1647.0000	IB0000000023
TrustDefender 2.2.9.828	IB0000000024
Trusteer Rapport Emerald Build 0912.41	IB0000000025
Vipre Antivirus Premium 4.0.3272	IB0000000026
Zemana AntiLogger 1.9.2.201	IB0000000027
ZoneAlarm internet Security 9.1.507.000	IB0000000028

Methodology used in the Test:

1. Windows XP Professional Service Pack 3 is installed and updated with all important updates.
2. An image of the Operating System is created.
3. A clone of the Imaged system is made for each of the 28 security applications to be used in the test.
4. An individual security application is installed using default settings on each of the Cloned systems and then updated.
5. A fresh clone of the clone created in 4. Is used for each test.
6. The test is conducted by:
    a. Downloading the simulator using Internet Explorer to the desktop and executing it.
    b. The unique code is entered in to the “User ID” field on the login page of www.hsbc.co.uk using the keyboard and then selecting the ”Log on” button.
7. A test is deemed to have been passed if the security application prevents the simulator from capturing data and sending it to our test site.

8. If the security application requests input from the user, it must provide a specific notice to block an action and or identify it as a specific threat. (an alert stating something is simply “unknown” or requires “elevated privileges” fails to identify specific threats or risks and so is ignored)
9. Testing is conducted with all systems having internet access.
10. Each individual test for each security application will be conducted from a unique IP address.
11. The filename, creation date etc of the simulator will be changed for each test.
12. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG.

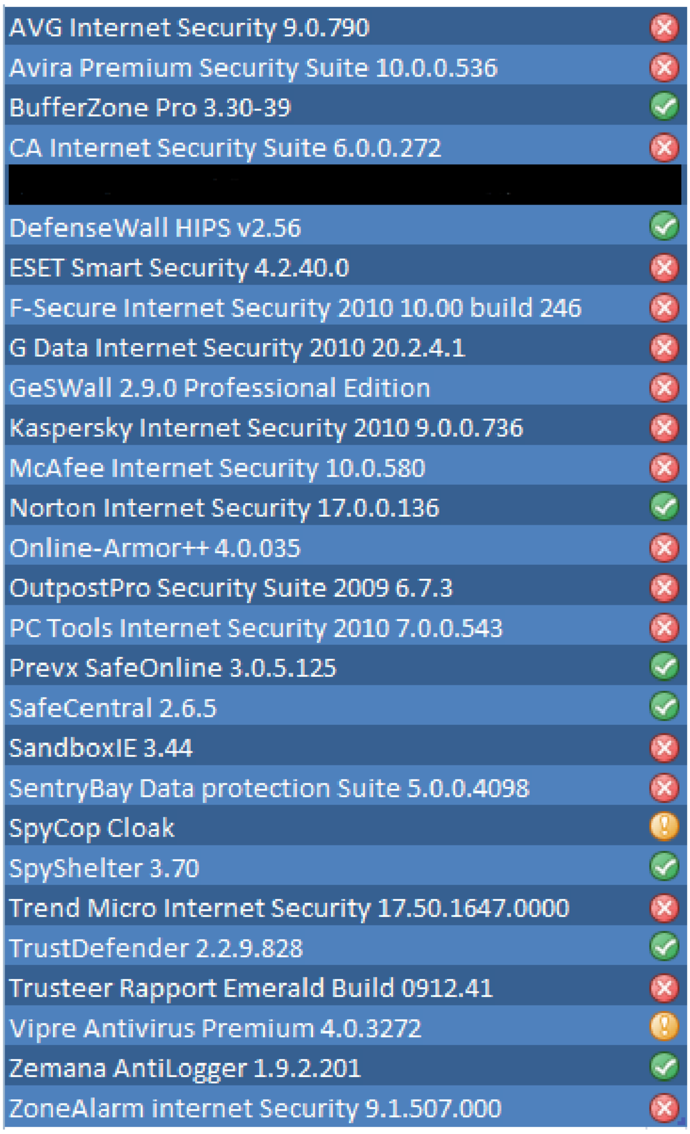
Test Results:

All live test results will be published in real time here:

www.browsersecurityproject.malwareresearchgroup.com

Detailed data will be collated periodically and provided to vendors who have a support contract with MRG.

The results of the initial test were as follows:



AVG Internet Security 9.0.790	✗
Avira Premium Security Suite 10.0.0.536	✗
BufferZone Pro 3.30-39	✓
CA Internet Security Suite 6.0.0.272	✗
[redacted]	[redacted]
DefenseWall HIPS v2.56	✓
ESET Smart Security 4.2.40.0	✗
F-Secure Internet Security 2010 10.00 build 246	✗
G Data Internet Security 2010 20.2.4.1	✗
GeSWall 2.9.0 Professional Edition	✗
Kaspersky Internet Security 2010 9.0.0.736	✗
McAfee Internet Security 10.0.580	✗
Norton Internet Security 17.0.0.136	✓
Online-Armor++ 4.0.035	✗
OutpostPro Security Suite 2009 6.7.3	✗
PC Tools Internet Security 2010 7.0.0.543	✗
Prevx SafeOnline 3.0.5.125	✓
SafeCentral 2.6.5	✓
SandboxIE 3.44	✗
SentryBay Data protection Suite 5.0.0.4098	✗
SpyCop Cloak	!
SpyShelter 3.70	✓
Trend Micro Internet Security 17.50.1647.0000	✗
TrustDefender 2.2.9.828	✓
Trusteer Rapport Emerald Build 0912.41	✗
Vipre Antivirus Premium 4.0.3272	!
Zemana AntiLogger 1.9.2.201	✓
ZoneAlarm internet Security 9.1.507.000	✗

We have been very rigorous in conducting this initial test and have already had detailed discussions with some vendors concerning results. We will be happy to discuss the results in the appropriate section of our forum.