



Online Banking Security Test

June 2011

FOR MRG EFFITAS

Contents:

Introduction	3
Issues with Using Financial Malware to Test Security Products	4
The Purpose of this Test	4
Security Applications Tested	5
Methodology Used in the Test	6
Test Results	7
Analysis of the Results	10
Conclusions	12

FOR MRG EFFITAS USE ONLY

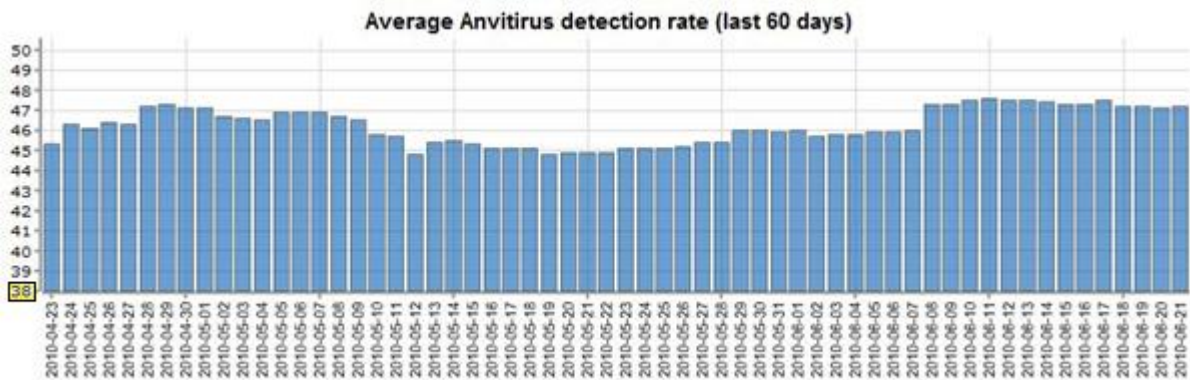
Introduction:

MRG Effitas has published several reports based on our research into online banking, financial malware and browser security. Our previous report, which was published twelve months ago, was based on a project which sought to model how a range of security applications would respond to a new, zero-day threat over a period of a month. One year on, we are publishing our latest online banking security report.

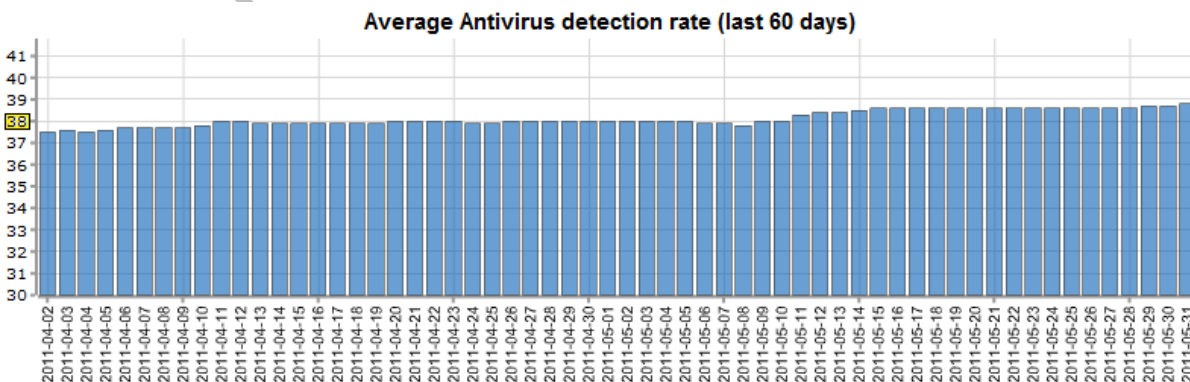
Based on evidence from our research, it has been our position for some time now that users need to employ additional security measures on top of traditional anti-virus or internet security suites, to counter threats posed by financial malware. Our previous reports and other independent research have shown that traditional security applications are, on the whole, unable to provide adequate protection against financial malware.

It is a common expectation that as a result of modern technology, products and services become relatively cheaper and more effective over time. Information technology is a prime example of this, with the cost of equipment dropping whilst performance doubles every couple of years or so. Given this trend for improved performance and decreasing cost, one would think it reasonable to expect the same pattern to manifest itself in terms of security as well – greater security for lower cost.

In the report we published in June 2010, we illustrated that Zeus, the most virulent strain of financial malware, was very stealthy; we used the graph below¹ which charted its average detection rate based on over forty anti-malware/anti-virus applications.



We can see from the graph that at that time Zeus had an average detection rate of about 46.5%. A year on, we can see from the graph below that average detection rates for Zeus have dropped to about 38.2% - a level that would hardly have even registered above the lowest value on the vertical axis of last year's graph above.



What is the reason for the low detection rate of financial malware? In the simplest terms, detection is low because it is designed that way. Since the criminals invest a lot of time and effort in infecting systems in the

¹ Zeus detection graphs reproduced by permission of ZeuS Tracker.

first instance, they want to get maximum return on this by having their malware running on a system, undetected and unimpeded, for as long as possible. They want as long an opportunity as possible to steal as much personal data as they can and for the infected system to be part of a wider botnet for the maximum length of time.

Aside from technical features such as importing many external APIs to evade heuristics, malware terminating in virtual environments, making it difficult for researchers to analyse and tens of thousands of variants being generated daily, financial malware has low detection rates because of competition.

Whilst Zeus is the most prevalent type of financial malware, there are several others: SpyEye, LdPinch, Bugat, Gozi, Clampi, etc. There is in effect a competitive free market in relation to crimeware, where developers will continually innovate, add functionality and refine their products in an attempt to increase their market share. This competition ensures financial malware is continually evolving in sophistication at an alarming rate.

Issues with Using Financial Malware to Test Security Products:

Testing financial malware is extremely complex. It is not enough to see if a security application allows a malicious sample to run or not. In order to properly assess efficacy, it is necessary to establish whether, if a sample is allowed to execute, it is able to capture a user's logon data and then successfully send this out of the system to a remote location.

One approach is to actually set up a botnet. This is an extremely complex and costly task. Any botnet used for testing purposes would need to meet our No. 1 rule: "Do No Harm". In order to ensure this, it would need to run in a very complex virtual environment and because of the virtual nature, it could be possible that the financial malware would not function properly for the reasons described earlier.

Another approach is to analyse how financial malware works and then design a simulator which operates in the same way. Although this is also complex and costly, it offers reliable, consistent results and is safer as whilst the simulator performs malicious activity, it is not weaponized and in any case will not be released from the lab.

How does financial malware work? If we look at the two most common types, Zeus and SpyEye, we can see that they both use what is called a Man in the Browser attack, or MitB attack. With these attacks the malware infects the browser/browser memory and then makes use of legitimate resources available to the browser such as BHOs, etc. In the case of SpyEye, once inside the browser, it hooks the TranslateMessage, send, HttpSendRequestA, HttpSendRequestW and InternetCloseHandle APIs and can therefore capture any username or password sent via the browser.

The MRG Effitas Financial Malware Simulators all use the same MitB attacks as real financial malware. The V2.1e version used in these tests follows very similar approaches as SpyEye and can capture usernames and passwords even when entered into SSL encrypted sites.

The simulator also has several other characteristics common to real malware which make it a valid representation of a real zero day piece of financial malware. We will provide a technical overview of this simulator to any vendor in this report on request.

There are several "logger simulators" available to the public which will capture keystrokes, record the screen and webcam, etc. These applications do not represent how real financial malware works and therefore cannot be used as a meaningful assessment of efficacy.

The Purpose of this Test:

This report and associated tests are intended to give an assessment of how a range of security applications cope against a piece of malware which uses a MitB attack to capture the user ID and password entered into a SSL protected online banking site.

In an attempt to yield as much useful data as possible and to make this as relevant to current systems as can be, testing was conducted on two different operating systems:

- 1) Windows 7, 32 bit
- 2) Windows 7, 64 bit

The reason behind choosing to test on two versions of this operating system is that whilst there has been a 64 bit version of Windows for some time now, it was not until the advent of Windows 7 that it began to gain popularity.

Windows 64 bit operating system has two main advantages. Firstly, it allows the use of more than 4GB of RAM. It is for this reason alone that many systems are now being shipped with Windows 7 64 as the standard operating system. Secondly, Windows 64 comes with a feature called Kernel Patch Protection or KPP.

The kernel is the heart of the operating system and serves as an interface between applications which run on it and the physical hardware of the computer. Patching or modifying the kernel has been practiced by malware authors and security vendors as a means to attain certain functionality in their software. With the advent of KPP, malware authors are unable to use patching to achieve these functionalities, however, this applies to the security vendors as well and consequently, on 64 bit versions of Windows, some security applications do not provide their full complement of protection.

Testing was also conducted under two different conditions:

- 1) Where the simulator attempts to infect a clean operating system which is already protected by a security application; and
- 2) Where the security application is installed on an operating system that has already been infected with the simulator.

The rationale behind using these first condition is to replicate the situation where a user with a clean protected system encounters a financial malware threat and the second condition, where a user may install a security application on a system that has already been used so could well be compromised.

Security Applications Tested:

The test cohort is made up of twenty-eight security applications. Nineteen of the applications are internet security suites or security applications which purport to offer system-wide protection. Of these nineteen, five are specifically recommended or promoted by financial institutions as being able to offer security in relation to online banking. The remaining nine applications are dedicated browser security, anti-logging or HIPS applications, which purport to provide security against financial malware and/or identity theft.

The applications tested are as follows:

Internet Security/Full Security Suites

1. Acronis Internet Security Suite 2010 Build 13.0.17.343
2. Agnitum Outpost Security Suite Pro 7.5.3701.574.1664
3. Avira Premium Security Suite 10.0.0.621
4. BitDefender Internet Security 2011 Build 14.0.29.354
5. BluePoint Security 2010 1.0.58.99
6. BullGuard Internet Security 10.0
7. ESET Smart Security 4.2.71.2
8. F-Secure Internet Security 2011 10.51 Build 106
9. G DATA InternetSecurity 2012 22.0.2.25
10. Norman Security Suite 8.00
11. Panda Internet Security 2012 17.00.00

12. Symantec Endpoint Protection 11.0.6300.803
13. Trend Micro Internet Security 2011
14. Webroot Internet Security Essentials 2011

Internet Security Suites Recommended/Promoted by Banks

1. AVG Internet Security 2011 10.0 Build 1375a3626
2. Kaspersky Internet Security 2011 11.0.2.556
3. McAfee Internet Security 2011
4. Norton 360 5.0.0.125
5. Zone Alarm Internet Security Suite 2010

Browser Security/Anti-Logging/HIPS HIPS Applications

1. Zemana AntiLogger 1.9.2.510
2. TrustWare BufferZone Pro 3.41-14
3. SentryBay Data Protection Suite 5.3.0.5872
4. SoftSphere DefenseWall 3.13
5. QFX Software KeyScrambler Personal 2.8.1.0
6. Neo's SafeKeys v3
7. Prevx v3.05.220
8. Quaresso Protect On Q v 2.3.1.2388
9. Trusteer Rapport Emerald Build 1008.42

Methodology Used in the Test:

1. Both Windows 7 Ultimate Service Pack 1 32 and 64 bit operating systems are installed on separate virtual machines and all updates are applied to each.
2. An image of each of the operating systems is created.
3. A clone of both of the imaged systems is made for each of the 28 security applications to be used in the test, thus creating 28 32-bit and 28 64-bit systems.
4. An individual security application is installed using default settings on each of the 32 and 64 bit systems created in 4 and then updated.
5. A clone of the system as it is at the end of 4 is created.
6. The post-protection infection test is conducted by:
 - a. Downloading the simulator using Internet Explorer to the desktop, closing Internet Explorer and then executing the simulator.
 - b. Starting a new instance of Internet Explorer and navigating to www.paypal.com.
 - c. Text is entered into the Account login page of www.paypal.com using the keyboard, or using a virtual keyboard if the application under test provides such functionality, in the form of "test@email.com" along with the password "password" and then the "log in" button is pressed.
7. The pre-infected system test is conducted by:
 - a. Performing steps 1-6 above with the exception of 6a, but infecting the system with the simulator at step 2.
8. A test is deemed to have been passed by the following criteria:
 - a. The security application detects the simulator whilst it is being downloaded to the desktop.
 - b. The security application detects the simulator when it is executed according to the following criteria:
 - i. It identifies the simulator as being malicious and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaits user input.

- ii. It identifies the simulator as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode and when run in this mode it meets the criteria c or d below.
 - c. The security application prevents the simulator from capturing and sending the logon data to the MRG results page, whilst giving no alerts or informational alerts only.
 - d. The security application intercepts the installation/action of the simulator and displays warnings and user action input requests that are clearly different to those displayed in response to legitimate applications, when they are executed or installed on that system.
9. A test is deemed to have been failed by the following criteria:
- a. The security application fails to detect the simulator when it is executed and then:
 - i. The security application fails to prevent the simulator from capturing and sending the logon data to the MRG results page and gives no, or informational alerts only.
 - ii. The security application intercepts the installation/action of the simulator but displays warnings and user action input requests that are indistinguishable in meaning from those displayed in response to legitimate applications, when they are executed or installed on that system.
 - b. The security application identifies the simulator as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode and when run in this mode it:
 - i. Fails to prevent the simulator from capturing and sending the logon data to the MRG results page and gives no, or informational alerts only.
 - ii. Displays warnings and user action input requests that are indistinguishable in meaning from those displayed in response to legitimate applications, when they are executed or installed on that system.
10. Testing is conducted with all systems having internet access.
11. Each individual test for each security application is conducted from a unique IP address.
12. The filename, creation date, etc. of the simulator are changed for each test.
13. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
14. All testing was conducted on 02 June 2011, within a one hour window.

Test Results:

Post-protection infection tests:

Standard Internet Security Applications	
Windows 7 (32)	Windows 7 (64)
Acronis Internet Security Suite	Acronis Internet Security Suite
Agnum Outpost Security Suite Pro	Agnum Outpost Security Suite Pro
Avira Premium Security Suite	Avira Premium Security Suite
BitDefender Internet Security	BitDefender Internet Security
Bluepoint Security	Bluepoint Security
BullGuard Internet Security	BullGuard Internet Security
ESET Smart Security	ESET Smart Security
F-Secure Internet Security	F-Secure Internet Security
G Data internetSecurity	G Data internetSecurity
Norman Security Suite	Norman Security Suite
Panda Internet Security	Panda Internet Security
Symantec Endpoint Protection	Symantec Endpoint Protection
Trend Micro Internet Security	Trend Micro Internet Security
Webroot Internet Security Essentials	Webroot Internet Security Essentials

Internet Security Applications Recommended by Banks	
Windows 7 (32)	Windows 7 (64)
AVG Internet Security Kaspersky Internet Security McAfee Internet Security Norton 360 Zone Alarm Internet Security	AVG Internet Security Kaspersky Internet Security McAfee Internet Security Norton 360 Zone Alarm Internet Security




Browser Security & Anti-Logging Applications	
Windows 7 (32)	Windows 7 (64)
Aplin Software Neo's SafeKeys Prevx Prevx QFX Software KeyScrambler Quaresso Protect On Q SentryBay Data Protection Suite SoftSphere DefenseWall Trusteer Rapport TrustWare BufferZone Pro Zemana AntiLogger	Aplin Software Neo's SafeKeys Prevx Prevx QFX Software KeyScrambler Quaresso Protect On Q SentryBay Data Protection Suite SoftSphere DefenseWall Trusteer Rapport TrustWare BufferZone Pro Zemana AntiLogger

Pre-infected system tests:

Standard Internet Security Applications	
Windows 7 (32)	Windows 7 (64)
Acronis Internet Security Suite	Acronis Internet Security Suite
Agnitum Outpost Security Suite Pro	Agnitum Outpost Security Suite Pro
Avira Premium Security Suite	Avira Premium Security Suite
BitDefender Internet Security	BitDefender Internet Security
Bluepoint Security	Bluepoint Security
BullGuard Internet Security	BullGuard Internet Security
ESET Smart Security	ESET Smart Security
F-Secure Internet Security	F-Secure Internet Security
G Data internetSecurity	G Data internetSecurity
Norman Security Suite	Norman Security Suite
Panda Internet Security	Panda Internet Security
Symantec Endpoint Protection	Symantec Endpoint Protection
Trend Micro Internet Security	Trend Micro Internet Security
Webroot Internet Security Essentials	Webroot Internet Security Essentials

Internet Security Apps Recommended by Banks	
Windows 7 (32)	Windows 7 (64)
AVG Internet Security	AVG Internet Security
Kaspersky Internet Security	Kaspersky Internet Security
McAfee Internet Security	McAfee Internet Security
Norton 360	Norton 360
Zone Alarm Internet Security	Zone Alarm Internet Security

Browser Security & Anti-Logging Applications	
Windows 7 (32)	Windows 7 (64)
Aplin Software Neo's SafeKeys	Aplin Software Neo's SafeKeys
Prevx Prevx	Prevx Prevx
QFX Software KeyScrambler	QFX Software KeyScrambler
Quareso Protect On Q	Quareso Protect On Q
SentryBay Data Protection Suite	SentryBay Data Protection Suite
SoftSphere DefenseWall	SoftSphere DefenseWall
Trusteer Rapport	Trusteer Rapport
TrustWare BufferZone Pro	TrustWare BufferZone Pro
Zemana AntiLogger	Zemana AntiLogger

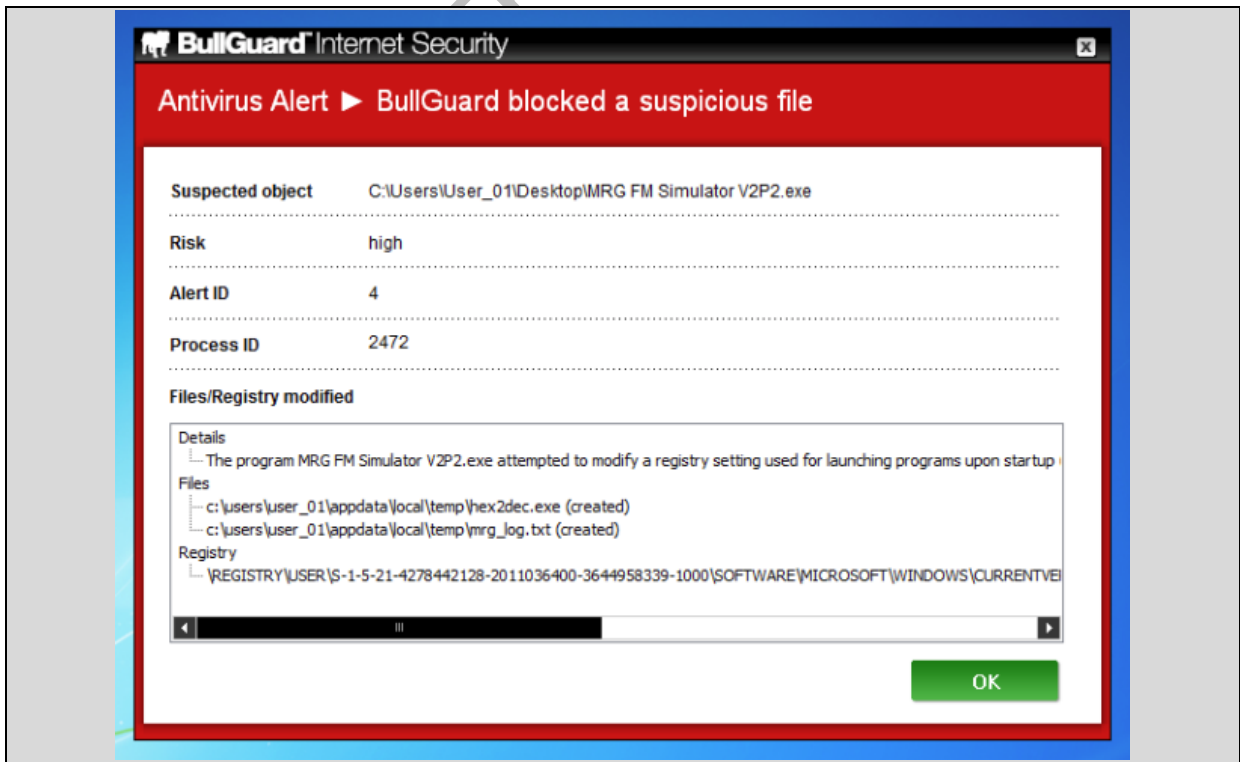
Key	
Pass	
Fail	
N/A	

Analysis of the Results:

Post-protection infection tests:

Clearly, as with our previous tests in this area, the performance of the internet security applications is extremely poor against this malicious code.

In this category, BullGuard Internet Security was the only application which passed the infection test and intercepted and blocked the execution of the simulator – and indeed, all of its components as the screenshot below shows.



Interestingly, BullGuard uses the same engine as BitDefender and yet BitDefender did not detect the simulator, which would indicate that BullGuard is using some proprietary behavioural analysis technology, not present in BitDefender

The internet security applications which had been recommended or promoted by the banks did not perform any better than those which had not, none of them being able to protect the system from the malicious activity.

BluePoint Security is not specifically marketed as an internet security application, however, its use of white listing technology is presented as a means of ensuring complete protection since if an application/piece of code is not on the white list, it will be blocked. The V2.1e financial malware simulator used in these tests was able to completely bypass the white listing technology employed by BluePoint and run unimpeded and without any alerts from the security application.

There was no difference in the internet security suites between the results on 32 and 64 bit systems; however, it must be pointed out that differences would only be expected to occur where they had actually been able to provide a positive result on the 32 bit operating system to start with.

As can be seen from the table on page 8, the dedicated browser security/anti-logging applications perform significantly better against the simulator. Zemana AntiLogger, SoftSphere DefenseWall, Prevx, Quaresso Protect On Q and Trusteer Rapport were all able to protect the system against the MitB attack and prevent the simulator from capturing the login data.

We have tested Trustware BufferZone Pro, SentryBay Data Protection Suite, QFX Software KeyScrambler Personal and Neo's SafeKeys against basic keylogging simulators and they have proved effective; however, none of these was able to protect against the MitB attack used in this test.

We can see the impact of KPP on the 64 bit version of Windows in the dedicated browser security/anti-logging applications, with neither Trustware BufferZone Pro nor SoftSphere DefenseWall being available on these operating systems.

All of the applications which failed on the 32 bit Windows also failed on the 64 bit version. In addition to this, Prevx, which had passed the test on the 32 bit operating system, failed to protect the system when run on the 64 bit version.

We have tested Prevx extensively and became aware of this vulnerability several months ago. We notified the vendor of this vulnerability at that time, so are surprised to see that it still remains.

On Windows 7 64, out of twenty-seven security applications, only BullGuard Internet Security, Zemana AntiLogger, Quaresso Protect On Q and Trusteer Rapport were able to protect the system from the infection test.

Pre-infected system tests:

The pre-infected system test yielded the same results as the post-protection infection test with the exception that BullGuard Internet Security did not detect the simulator.

SoftSphere DefenseWall was classified as "not applicable" since the product is only marketed as a prevention tool which must be used on a clean system and does not purport to offer detection or remediation functionality.

Further to the processes described in the methodology, in the case of all the internet security applications, we gave them all a chance to detect the simulator by sunning a full system scan and even rebooting the system, so they could have an opportunity to detect it as it became active during the restart. None of them was able to detect the simulator under these conditions.

We feel the above highlights the need for dedicated browser/anti-logging applications, as it is a perfectly valid possibility that a system could be compromised by financial malware with no alert from traditional security applications. In this scenario a user would be completely unaware that they and their banking details were at risk and would continue activity under the false sense of security offered by their internet security application.

Conclusions:

The first and most obvious conclusion is that a year on from our previous report, with the exception of BullGuard, the internet security applications still did not protect the system from the malicious MitB attack instigated by the simulator.

We would suggest that in the security community, it is no secret that traditional applications commonly do not provide protection against zero day and many early life financial malware threats. Given this fact, we question the wisdom of financial institutions promoting or providing traditional internet security applications as a means of securing internet banking.

Promotions such as the one shown below clearly suggest that customers will be able to “bank, shop and surf the internet with confidence” once they use the software.

The screenshot shows the MBNA website interface. At the top left is the 'mbna' logo. On the top right, there is an 'Online Card' button and a 'Log in' button. Below these are three main navigation tabs: 'Choose a credit card', 'Card services and benefits', and 'Protection and security'. A breadcrumb trail indicates the user's current location: 'You are here: Personal credit cards > Protection and security > Complimentary McAfee Online Banking Suite'.

The main content area features a sidebar on the left with 'Protection' and 'Security' categories. The 'Protection' category includes 'Payment Protection', 'Identity Protection', and 'Card & Phone SOS'. The 'Security' category includes 'Credit card security', 'Online account security', 'Computer security', 'Reporting fraud', and 'Complimentary McAfee Online Banking Suite'.

The main content area has a heading: 'Here's a special offer as a thank you just for being an Online Card Services customer...'. Below this, it states: 'To keep your PC safe and secure, we're offering the McAfee Online Banking Suite worth £59.98, completely complimentary for one year. You can bank, shop and surf the internet with confidence. McAfee offers effective online protection with:'

- **Anti Virus, spyware and adware** - within milliseconds malicious threats are blocked and removed.
- **Anti-Spam and Email Protection** - keeps your mailbox free from unwanted, fraudulent and phishing emails.
- **Two Way Firewall** - allows you to confidently use the Internet knowing hackers can't get access.
- **Online Backup** - automatic backup for your essential photos, videos and documents.
- **Site Advisor Plus** - active protection against dangerous websites and much more.
- **Additional Features** - including home network manager as well as PC optimisation.

In addition, this product will be automatically enrolled at the end of the 12 month period for a subsequent paid year at only £29.99, a discount of 50%.

On the right side of the offer, there is a McAfee logo and two sections: 'Existing Online Card Services users:' with a 'Log in' button, and 'New to Online Card Services?' with a 'Register' button. Below these is a link for 'Not an MBNA Card holder?' with a 'View our cards' link.

In this report, we detailed five internet security applications which had been promoted or highlighted by financial institutions. None of these showed any evidence of performing any better than the other internet security applications and none were able to provide any protection against the malicious MitB attack.

It is clear from these tests that on average, the dedicated browser and anti-logging applications provide better protection against these threats and would therefore be a better choice for anyone seeking increased protection.

Not all the dedicated anti-logging applications proved effective, however. There seems to be some confusion or misinformation about the nature of the threat posed by financial malware which stems from the inappropriate use of terms such as “key-loggers” when financial malware is being discussed. As has been mentioned earlier, sophisticated financial malware does not use the same methods of capturing data as the kind of key-logger simulators the public can access on various security sites.

In choosing the browser security/anti-logging applications, we ensured that the vendor had specifically positioned them as products which could provide security for online banking, prevent identity theft or provide protection against financial malware. In the case of QFX Software’s KeyScrambler Personal, for example, they use the terminology “protects your keystrokes” and talk of “keyloggers” but then go on to host endorsements on their site, which specifically suggest it is effective against financial malware.

Encrypting “keystrokes” and virtual keyboards will offer no protection against sophisticated financial malware like SpyEye – or indeed, as this report shows, our simulator.

Out of all twenty-seven applications on test, only three were able to protect the system under all conditions, these being Zemana AntiLogger, Quaresso Protect On Q and Trusteer Rapport. An interesting feature of all three of these is that they protected the system silently, never asking for any user input and with no significant impact on system performance.

Several generations ago, people would have kept their money in a cash box, then, at the end of the day, locked this cash box in a safe for security. A generation or so later, people would have taken their money to their bank, where it would have been kept in the bank’s for security.

Today, only about 3% of the money in the developed world actually exists in any material form. The money we have is not sitting inside a metal safe in the bank. Our money exists in a virtual form as a series of 1s and 0s on a bank’s server somewhere. With online banking, a user’s browser is their portal to their virtualised money on the bank’s server. Users need to keep their browsers in a safe, because, effectively, that’s where their money is.

This report has focused on financial malware in relation to online banking via browsers by end users; however, there is a far greater security risk. Increasingly, government organisations, financial institutions and large corporations are adopting Virtual Desktop Infrastructure (VDI) technologies as a way of increasing efficiency and reducing costs.

Using a variation of the technology employed in the simulator used in this test, MRG Effitas has created a simulator that allows us to compromise all the VDI solutions we have seen and gain access to an organisation’s complete virtual desktop environment. In effect, using this technology, without being detected, we can in effect access the computing environment of that organisation just as if we were sitting in front of their employee’s PC. We can access their e-mails, all their documents, their CRM and customer details – in fact, we can access anything and everything they can.

This is a serious issue and we are in discussions with providers of VDI solutions and security vendors to help counter this vulnerability. We will publish a report on Virtual Desktop Infrastructure security later in the year.