MRG Effitas Online Banking / Browser Security Assessment Project

Q2 2013 Results

Contents:

Introduction:

MRG Effitas has published an Online Banking Browser Security report every year for the last four years. In 2013 and beyond, this single report is replaced by quarterly assessments. This report is the assessment for Q2 2013, with the programme running from start of Q2 2013 to end of Q1 2014.

Whilst, this report sits in much the same space as our previous annual reports, it is hoped that in being quarterly, we will be able to give more up to date information and assessments against threats that are prevalent during that particular period.

The Purpose of this Report:

What is at the core of our testing and on-going research is the belief that cybercrime is the most significant threat faced by nation states and the most prevalent crime affecting corporations and individuals. This fact has recently been acknowledged by the governments of all major countries and most are now implementing strategies, policies and allocating resources in order to counter these threats.

To put the scale of the problem in perspective, cybercrime is now estimated to have an annual global value of $250 billion and is set to overtake the revenues of all international drug crime which currently has the highest turnover.

Another metric we can use is the drastic increase in the volume and diversity of malware found in the wild. MRG Effitas is currently processing over 350,000 unique malicious binaries and up to 500,000 malicious URLs every day and supplying these to our clients and other testing labs in an attempt to protect against them.

Aside from supplying zero day threats to clients and labs, our belief is that the most significant way in which we can help in the fight against cybercrime is in the accurate and relevant assessment of product efficacy.

MRG Effitas has been working with the IEEE, other testing labs and universities in an attempt to devise a set of testing standards that will allow the accurate and relevant measurement of today's security products and also those that will be released in the next ten years in the new emerging computing model.

It is vitally important that protection technologies evolve and improve – but how are we to achieve this if we are unable to accurately measure their efficacy against current and emerging threats? Product improvement can't be achieved without the ability to measure real world performance.

The purpose of this and our other reports is to be part of that process of measurement for the sake of improvement and efficacy assurance.

Tests Employed:

Applied metrology is complicated and imprecise science and in the light of this, we position this and all our other work as the best assessments we can currently perform and not as an absolute or definitive determination.

In this quarters report, we ran two types of test:

Detection and blocking of Zeus. Zeus is still by far and away the most prevalent type of financial malware and is continually evolving to avoid detection and circumvent countermeasures employed by banks and security vendors.

Over the Q2 period, we tested a total of 100 Zeus samples, all from live URLs, which were in three main strains that emerged over the period.

Prevention of data exfiltration from ssl protected banking sites. Whilst detection is still a valuable metric, in itself it is not enough to determine real world efficacy as there will be instances where a system is compromised

before a security solution is installed or occasions where malware will bypass a preinstalled product. In these cases we need to be able to measure if active malware is able to perform data exfiltration or not.

MRG Effitas has a range of simulators which employ MitB attacks which have been used by financial malware and wider crimeware that we have reverse engineered.[i]

Over the Q2 period, we used our simulators to test the security products in the cohort against four unique MitB attacks.

Security Applications Tested:

- avast! Internet Security 8.0
- AVG Internet Security 2013
- BitDefender Internet Security 2013
- Emsisoft Anti-Malware 8.0
- ESET Smart Security 6.0
- F-Secure Internet Security 2013
- GFI VIPRE Internet Security 2013
- Kaspersky Internet Security 2013
- McAfee Internet Security 2013
- Microsoft Security Essentials 4.2
- Panda Internet Security 2013
- Quarri Protect on Q 3.2
- SoftSphere DefenseWall 3.22[ii]
- SourceFire Immunet Antivirus Plus 3.1
- Symantec Norton Internet Security 2013
- Threatmetrix TrustDefender Pro Gold Edition
- Trend Micro Titanium Internet Security 2013
- Trusteer Rapport Emerald Build 1208.34
- Webroot SecureAnywhere 8.02
- Wontok SafeCentral 3.0
- Zemana AntiLogger 1.92

Methodology Used in the Test:

1. Windows 7 Ultimate Service Pack 1 64 bit operating system is installed on a virtual machine and all updates are applied and third party applications installed and updated according to our "Average Endpoint Specification"[iii]
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications to be used in the test.
4. An individual security application is installed using default settings on each of the systems created in 4 and then, where applicable, is updated.
5. A clone of the system as it is at the end of 4 is created.
6. Each Simulator 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.[iv]
    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 and then the "log in" button is pressed.
7. 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 or local store location, 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.
8. 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 or local store location 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 or local store 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.
9. Each Zeus test is conducted by:
   a. Downloading the Zeus binary from its native URL using Internet Explorer to the desktop, closing Internet Explorer and then executing the binary
10. A test is deemed to have been passed by the following criteria:
   a. The security application blocks the URL where the Zeus binary is located.
   b. The security application detects and blocks the simulator whilst it is being downloaded to the desktop.
   c. 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. In the case of products that only provide a secure browser, the security application alerts that the system is compromised and will not allow the user to initiate a banking session at the location detailed in 6c above.
11. A test is deemed to have been failed by the following criteria:
   a. The security application fails to detect or block the binary at any stage in 9a and allows it to be executed.
12. A test result is deemed to be undetermined by the following criteria:
   a. In the case of products that only provide a secure browser or secure desktop, the security application does not alert that the system is compromised and will allow the user to initiate a banking session at the location detailed in 6c above.[v]

13. Testing is conducted with all systems having internet access.
14. Each individual test for each security application is conducted from a unique IP address.
15. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
16. All testing was conducted during Q2 2013.

Test Results:

The table below shows the results of testing using the simulators employing reverse engineered MitB Attacks

Security Application	FMA01	FMA02	FMA03	FMA04	Overall
Avast	P	P	P	P	
AVG	P	F	F	F	
BitDefender	P	P	P	P	
DefenseWall	P	P	P	P	
Emsisoft	P	P	P	P	
ESET	F	F	F	F	
F-Secure	F	F	F	F	
GFI	P	F	F	F	
Kaspresky	P	P	P	P	
McAfee	P	F	F	F	
Microsoft	F	F	F	F	
Panda	F	F	F	F	
Quarri	P	P	P	P	
SourceFire	P	F	F	F	
Symantec	P	F	F	P	
TrendMicro	P	F	F	P	
ThreatMetrix	F	F	F	F	
Trusteer	P	P	P	P	
Webroot	P	P	P	P	
Wontok	P	P	P	F	
Zemana	P	P	P	P	

P	The application prevented the simulator from capturing data
F	The application failed to prevent the simulator from capturing data

The graph below shows the detection / blocking results for the 100 ITW Zeus samples used

Security Application	Detection %
Avast	100
BitDefender	100
DefenseWall	100
Emsisoft	100
Kaspresky	100
Quarri	100
TrendMicro	100
Trusteer	100
Webroot	100
Zemana	100
F-Secure	98
SourceFire	98
Symantec	98
ESET	96
AVG	93
GFI	92
Panda	91
McAfee	89
Microsoft	74

Note, ThreatMetrix and Wontok are not included in this test as neither offers detection.

Certification:

In order to be attain the MRG Online Banking Browser Security Certification, a product must pass every test during the quarter. Applications which meet this specification will be given the certification for that quarter.

The MRG Effitas Online Banking Browser Security Certification for Q2 2013 is awarded to the following products:

- avast! Internet Security 8.0
- BitDefender Internet Security 2013
- SoftSphere DefenseWall 3.22
- Emsisoft Anti-Malware 8.0
- Kaspersky Internet Security 2013
- Quarri Protect on Q 3.2
- Trusteer Rapport Emerald Build 1208.34
- Webroot SecureAnywhere 8.02
- Zemana AntiLogger 1.92

Certifications for Q3 2013 will be announced in the second week of Q4 when our second report will be published.

[i] It is necessary to use simulators with reverse engineered MitB attacks as testing using real financial malware which rely on ITW C&C servers is unlawful under the Computer Misuse act in the UK as it requires that malicious code is run on a third parties computer without their knowledge or consent.
[ii] DefenseWall was tested on Windows 7 32 bit.
[iii] AES includes Adobe Flash, Reader, Microsoft Office 2007 & Firefox, all fully updated.
[iv] Where the security application offers a secured or dedicated banking browser, this is used
[v] Note, this classification does not represent a failure.