MRG Effitas Real Time Protection Test Project, First Quarter

(Q2 2013)

Contents:

Introduction:

The MRG Effitas Real Time Protection Testing Project is a replacement for and an evolution of the "Flash Tests" conducted to date.

For those unfamiliar with the Flash Tests, their purpose was to give an indication of product efficacy against live, ITW threats applied to the System Under Test (SUT) using a valid, real world infection vector and process.

Despite using live ITW malware and realistic infection vectors, we always added the caveat that due to the small malware sample size used, the individual Flash Tests should not be used as a rigorous assessment of product efficacy and that their purpose was to give an indication of efficacy over time.

The MRG Effitas Real Time Protection Testing Project is designed to overcome the limitation of the Flash Tests by using greatly increased number of malware samples and higher testing frequency. The project will run for twelve months commencing at the start of Q2 2013 and finishing at the end of Q1 2014 – in line with all our other projects.

Testing is conducted weekly, using approximately fifty unique samples (no sister files) and results will be published at the end of each quarter. We are publishing this quarter's results early as it affords us the opportunity to liaise with vendors before commencement of the first full quarter testing starting the first week of July 2013.

Security Applications Tested:

1. avast! Internet Seucirty 8.0
2. AVG Internet Security 2013
3. Avira Internet Security 2013
4. BitDefender Internet Security 2013
5. Emsisoft Anti-Malware 7.0
6. ESET Smart Security 6.0
7. GFI VIPRE Internet Security 2013
8. Kaspersky Internet Security
9. Malwarebytes Anti-Malware 1.75 *
10. McAfee Internet Security 2013
11. Microsoft Security Essentials 4.2
12. Norton Internet Security 2013
13. Panda Internet Security 2013
14. SoftSphere DefenseWall 3.21
15. SourceFire Immunet Antivirus Plus 3.0
16. SUPERAntiSpyware 5.6 *
17. Trend Micro Titanium Premium Security 2013

* Denotes a complementary application.

Methodology Used in the Test:

1. Windows 7 Service Pack 1 32 bit operating system is installed on a virtual machine and all updates are applied. A variable range of third party applications are added, appropriate for any specific exploit testing that may be conducted.
2. An image of the operating systems is created.
3. A clone of the imaged system is made for each of the 17 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 step 3 and then, where relevant is updated.
5. A clone of the system as it is at the end of 4 is created.
6. Testing is conducted by:
    a. Downloading the sample using Internet Explorer to the desktop, closing Internet Explorer, conducting a context menu scan or where unavailable a system scan and then executing the sample.
7. A test is deemed to have been passed by the following criteria:
    a. The security application blocks the URL where the sample is located, thus preventing its download.
    b. The security application detects the sample whilst it is being downloaded to the desktop.
    c. The security application detects the sample during the context or system scan.
    d. The security application detects the sample when it is executed according to the following criteria:
        i. It identifies the sample as being malicious and either automatically blocks it or pauses its execution and advises the user not to execute it and awaits user input.
8. A test is deemed to have been failed by the following criteria:
    a. The security application fails to detect the sample under conditions 7a, 7b, 7c or 7d.
9. Testing is conducted with all systems having internet access.
10. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.

Samples used:

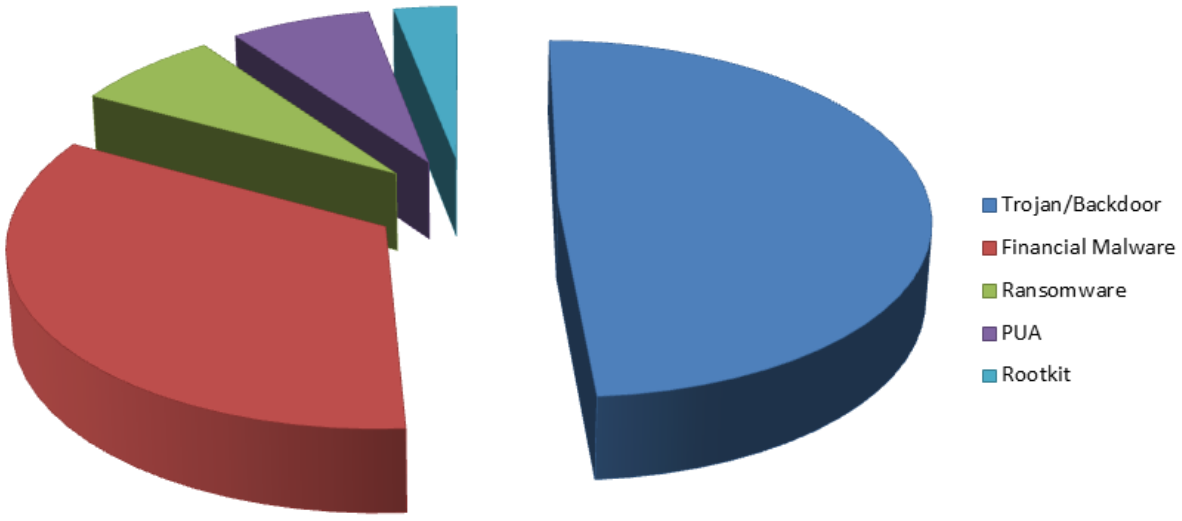
Sample selection is of fundamental importance to this and all similar tests. In the case of the Real Time Protection Project, all samples used are “live” and “in the wild”, by which we mean they are residing at the URLs selected or created by the cybercriminals and they are not from a time lagged ITW list.

As these are live ITW samples, they represent current zero day threats which can present an issue with sample verification. There is no effective and reliable way to verify samples before testing that does not introduce possible artificial sample submission or delay, so all verification is conducted after testing. Tests conducted using samples which are later proven to be invalid are excluded from the results.

The type and ratios of samples used is decided by MRG Effitas on the basis of a mixture of criteria, centering about key relevancies:

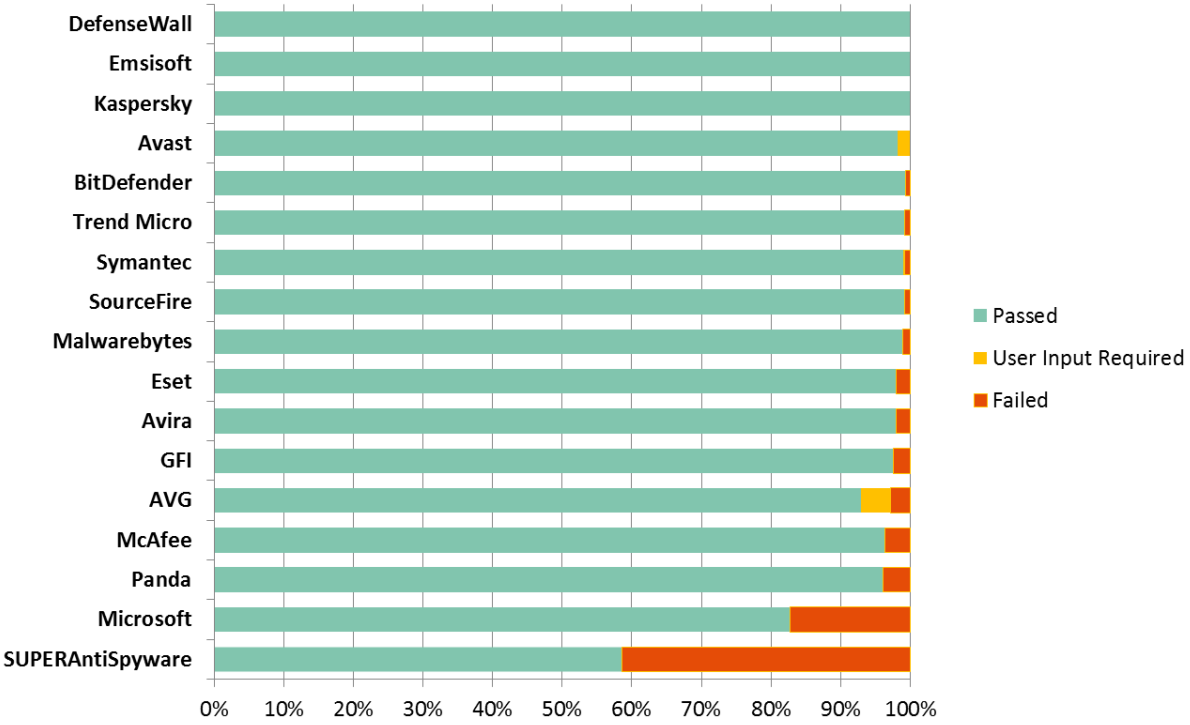
1. Prevalence – they are widespread and so represent the most common threats.
2. Growth – they may be few now, but our research shows they are rapidly expanding.
3. Innovation – they are employing innovative techniques to counter security measures.

In total, 585 live ITW samples were used in testing. The chart below shows the proportions of each category of malware:



Test Results:

The table below details the performance of each security application tested in order of efficacy.



The granular test results are detailed in the table below:

Vendor	Passed	Valid UIR	Failed	Total %
DefenseWall	585	0	0	100
Emsisoft	585	0	0	100
Kaspersky	585	0	0	100
Avast	582	11	0	100
BitDefender	581	0	4	99.3
SourceFire	580	0	5	99.1
Symantec	580	1	5	99.1
Trend Micro	580	0	5	99.1
Malwarebytes	579	0	6	99
Avira	573	0	12	97.9
Eset	573	0	12	97.9
GFI	571	0	14	97.6
AVG	568	26	17	97.1
McAfee	564	0	21	96.4
Panda	562	0	23	96.1
Microsoft	484	0	101	82.7
SUPERAntiSpyware	343	0	242	58.6

Conclusions:

In this first quarter, Kaspersky, Emsisoft and SoftSphere attained exceptional results, each achieving 100% efficacy without relying on user input requests, thus demonstrating effective and risk free protection against these threats. These three applications are awarded our highest five star rating.

Avast scored 100% but misses out on the top five star rating as it relied on user input requests to achieve this, so is awarded four and a half stars along with BitDefender, TrendMicro, Symantec, SourceFire, Malwarebytes, Eset, Avira and GFI who all performed well.

Special mention is made of Malwarebytes as it is a "complementary" antimalware product and so one should reasonably expect it to perform below its full antimalware counterparts, but it does not. Our congratulations go to them on their exceptional performance in this test cohort.

AVG, McAfee and Panda performed reasonably well with failure rates below four percent, but clearly have room for improvement and so are awarded four stars.

Microsoft had a failure rate of over seventeen percent and so is awarded three stars.

SUPERAntiSpyware, like Malwarebytes is a complementary antimalware and had a failure rate of over forty one percent and is awarded two and a half stars.

The table below details the star ratings awarded to the products for the first quarter of testing:

Kaspersky Emsisoft SoftSphere	★★★★★
Avast, BitDefender, TrendMicro, Symantec, SourceFire, Malwarebytes, Eset, Avira, GFI	★★★★½
AVG McAfee Panda	★★★★☆
Microsoft	★★★☆☆
SUPERAntispyware	★★½☆☆