
# MRG Effitas Time to Detect Assessment

# Q4 2013

# Contents:

**Introduction:**

Over the last five years, MRG Effitas has published a number of reports, most centring around browser security and financial malware. We will continue to operate in this same space, but as of the end of 2013, largely due to the nature of the private work we performed for clients, we decided to be more specific in focusing on what we believe are "the metrics which matter".

We have been working with the IEEE and a number of leading security vendors on a project to develop testing methodologies and metrics that will be appropriate for technologies emerging over the next fifteen to twenty years. During this time, our key slogan has been "detection is not enough" when it comes to measuring efficacy.

The two metrics MRG Effitas believes are most relevant are:

- The time taken to protect a system. There are two sub elements to this metric:
    - Time to detect
    - Time to remediate
- Assessment of data exfiltration. There are three sub elements to this metric:
    - Determination as to whether a data breach has occurred or not (uncorrupted data)
        - Calculation of what was breached
        - Measurement of how long the breach occurred

Currently, we are assessing these to metrics separately; however, as of the start of Q2 2014 we will be using a more advanced system of testing. MRG Effitas has assigned IBM as its technology partner and we will be employing their SoftLayer cloud computing technology to allow us to test using real, live botnets in such a way that imposes no risk to the public.

This current test is the second of the type of test we began in 2013 and focuses on the time to detect (as subset of the time to protect) metric only.

**The Purpose of this Assessment:**

It should be taken as a given that no security solution can detect 100% of in the wild malware all the time (malware that is active at live URLs). Exhaustive testing has shown conclusively that all security products and solutions get bypassed at some point and therefore, it is sensible to investigate product efficacy under this compromised condition.

In this report, we are assessing the ability of a cohort of security products to prevent an endpoint from being infected by live, ITW malware. If the system is infected, we measure the time the products take to detect the infection, up to a maximum of twenty four hours.

In order that testing maps closely to real world scenarios, 567 early life malware samples are used, 85% of these attempt to infect the system from live URLs via Internet Explorer and 15% via a USB stick.

## Security Applications Tested - (last version used in the test):

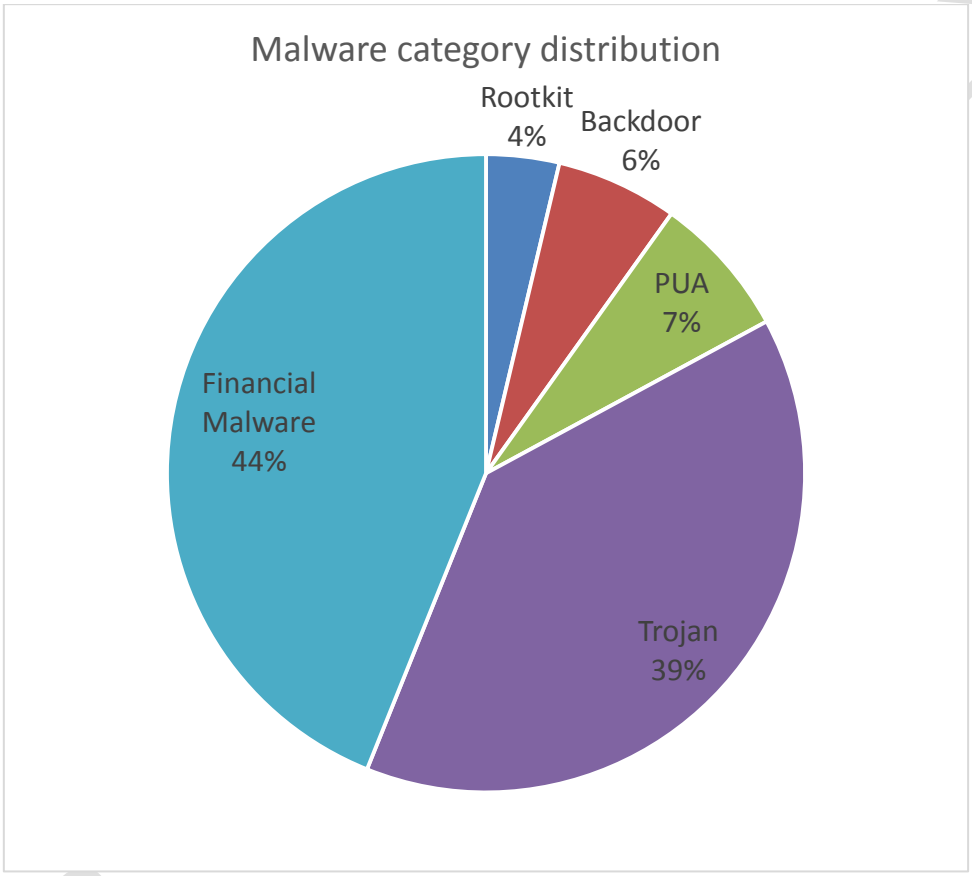
- avast Internet Security 8.0
- AVG Internet Security 2014 14.0
- Avira Internet Security 2014 14.0
- BitDefender Internet Security 2014 17.23
- Emsisoft Anti-Malware 8.1
- ESET Smart Security 7.0
- Kaspersky Internet Security 2014 14.0
- Malwarebytes Anti-Malware PRO 1.75
- McAfee Internet Security 2014 6.8
- Microsoft Security Essentials 4.4
- Panda Internet Security 2014 19.01
- SoftSphere DefenseWall 3.22
- Sourcefire Immunet Protect Plus 3.2
- SUPERAntiSpyware 5.7
- SurfRightHitmanPro 3.7
- Symantec Norton Internet Security 2014 21.1
- ThreatTrackVIPRE Internet Security 2014 7.0
- Trend Micro Titanium Maximum Security 2014 7.0
- Webroot SecureAnywhere Internet Security Plus 2014 8.0

**Methodology Used in the Assessment:**

1. Windows 7 Ultimate Service Pack 1 64 bit operating system[i] is installed on a virtual machine and all updates are applied and third party applications installed and updated according to our "Average Endpoint Specification"[ii]
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[iii] on each of the systems created in 3 and then, where applicable, is updated.
5. A clone of the system as it is at the end of 4 is created.
6. Each live URL test is conducted by:
    a. Downloading a single malicious binary from its native URL using Internet Explorer to the desktop, closing Internet Explorer and then executing the binary
    b. The security application blocks the URL where the malicious binary is located.
    c. The security application detects and blocks the malicious binary whilst it is being downloaded to the desktop.
    d. The security application detects the malicious binary when it is executed according to the following criteria:
        i. It identifies the binary 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.
7. Each USB infection test is conducted by:
    a. Downloading a single malicious binary from its native URL using a system out of the testing harness, then copying it to a USB stick.
    b. The USB stick is inserted in to the system under test and copied to the desktop using explorer and executed.
    c. The system under test is deemed to have been initially protected by the following criteria:
    d. The security application detected the malicious binary when the USB stick was inserted.
    e. The security application detected the malicious binary when it was copied to the desktop.
    a. The security application detects the malicious binary when it is executed according to the following criteria:
        i. It identifies the binary 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.
8. The system under test deemed to have been infected by the following criteria:
    a. The security application fails to detect or block the binary at any stage in 6 or 7 and allows it to be executed.
9. Testing on infected systems continues for twenty four hours by the following process:
    a. A Fast/Quick scan is performed every 30 minutes to give the security application an opportunity to detect the infection.
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. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
13. All testing was conducted during Q4 2013

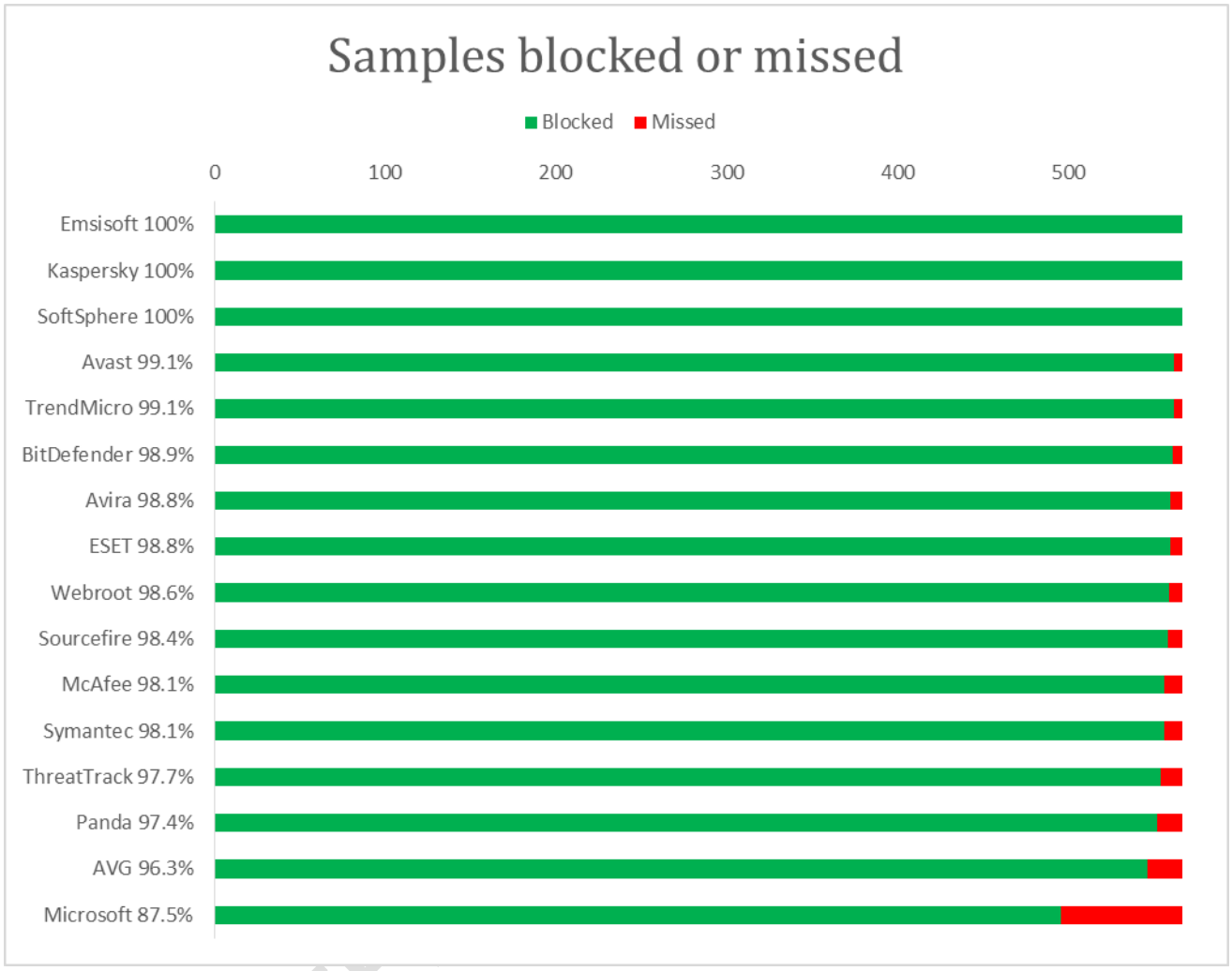
**Samples Used:**

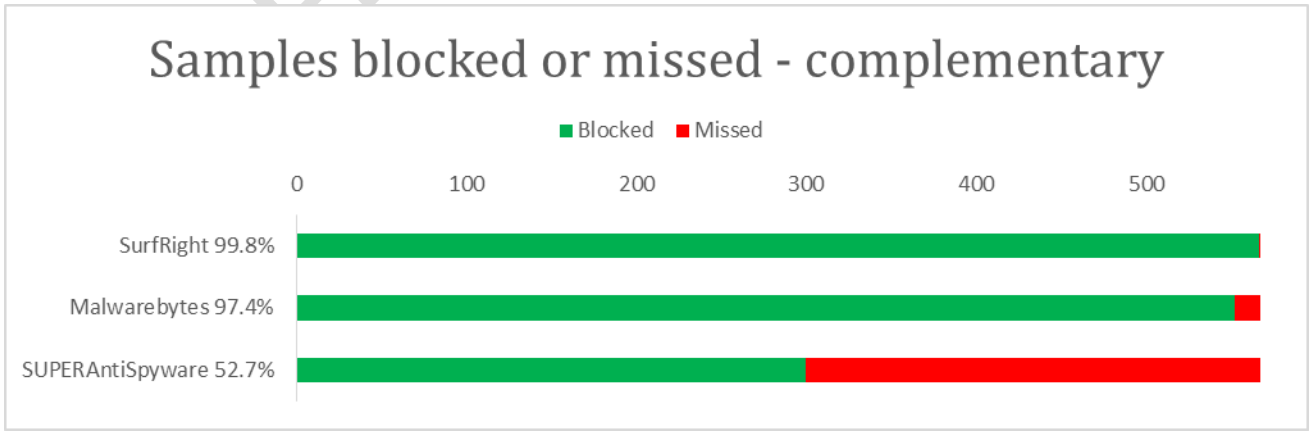
The pie chart below shows the number of each type of malware samples used:



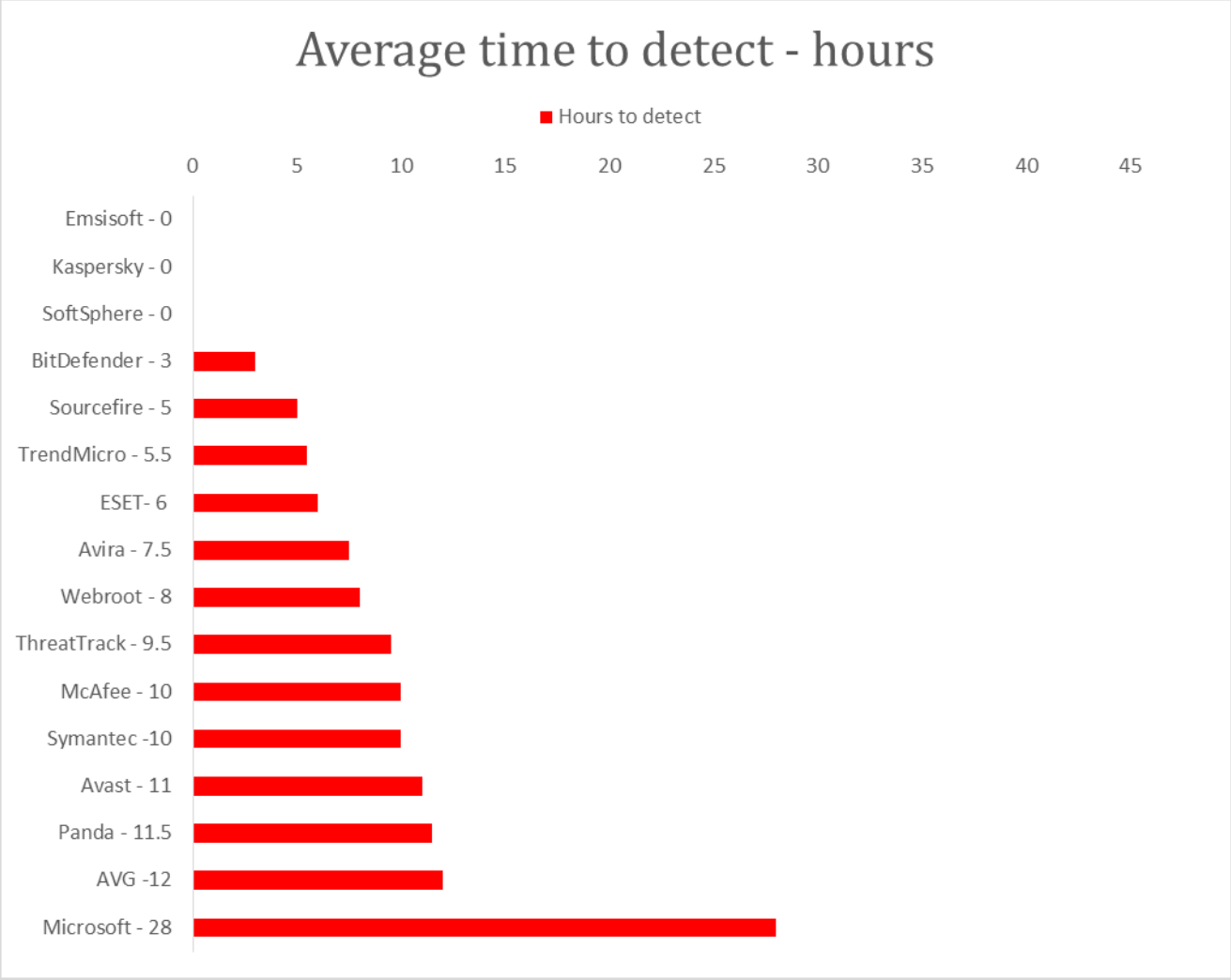
**Test Results:**

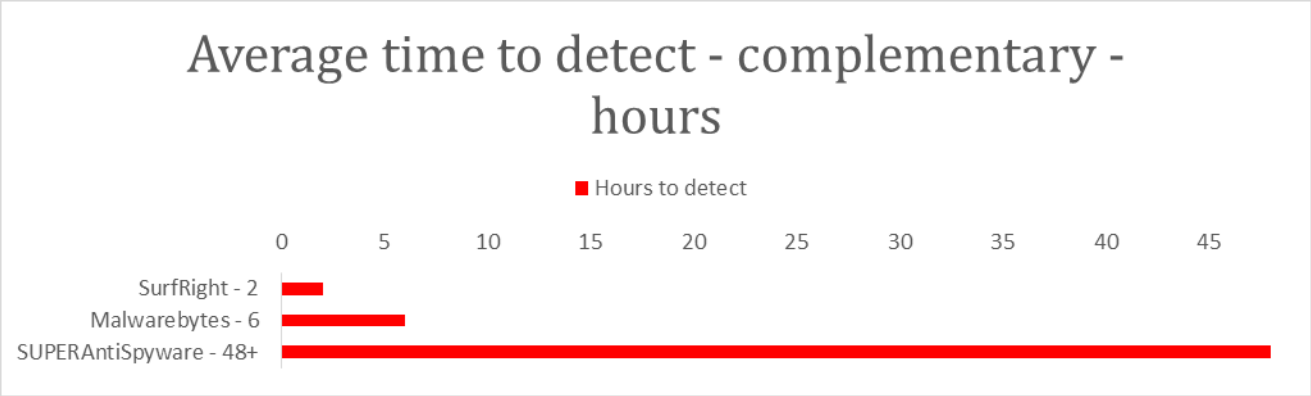
The graph below shows the initial detection rates for the security applications under test:



The graph below shows the average time to detect by the applications for the samples missed initially:



The table below shows the detail of the initial samples blocked by the applications, the numbers missed initially and the average time to detect for those samples missed initially:

| Vendor | Samples Blocked | Samples Missed | Average Time to Detect |
|---|---|---|---|
| Emsisoft | 567 | 0 | N/A |
| Kaspersky | 567 | 0 | N/A |
| SoftSphere | 567 | 0 | N/A |
| SurfRight | 566 | 1 | 2h |
| Avast | 562 | 5 | 11h |
| TrendMicro | 562 | 5 | 5.5h |
| BitDefender | 561 | 6 | 3h |
| Avira | 560 | 7 | 7.5h |
| ESET | 560 | 7 | 6h |
| Webroot | 559 | 8 | 8h |
| Sourcefire | 558 | 9 | 5h |
| McAfee | 556 | 11 | 10h |
| Symantec | 556 | 11 | 10h |
| ThreatTrack | 554 | 13 | 9.5h |
| Malwarebytes | 552 | 15 | 6h |
| Panda | 552 | 15 | 11.5h |
| AVG | 546 | 21 | 12h |
| Microsoft | 512 | 71 | 28h |
| SUPERAntiSpyware | 299 | 268 | 48h+ |



**Conclusion / Notes:**

Emsisoft, Kaspersk and SoftSphere were the only applications which successfully detected / blocked all 567malicious binaries and so protected the system under test from infection in the first instance.

It should be noted that Malwarebytes Anti-Malware, SUPERAntiSpyware and SerfRight HitmanPro are complementary tools, however all three tools are designed to protect against threats used in this test.

SuperAntiSpyware was the only application which failed to detect 100% of infections within the 48 hour period.

Whilst it is true that vast majority of infections occur when users visit malicious URLs, removable media devices also pose as a very effective delivery system for malware. We have seen this with some high profile pieces of malware in the past such as the infamous Conficker worm and various APTs. It is because of this that we chose to introduce the second infection vector to this test.

[i] DefenseWall is tested on Windows 7 32
[ii] AES includes Adobe Flash, Reader, Java, Microsoft Office 2007 & Mozilla Firefox, all fully updated.
[iii] During the installation of the security application, if an option to detect PUAs is given, it is selected.