MRG Effitas 360 Assessment & Certification Programme

Q2 2014

Contents

Introduction

MRG Effitas has a core focus on efficacy assessments in the anti-financial fraud space; however, we also publish more traditional "Real World" detection tests as well. An example of such a test is our "Time to Detect Assessment Q4 2013" (Project 37).

This assessment measured security products' ability to protect an endpoint from a live infection, but also, where a system was compromised, it also measured the time taken to detect the infection and remediate the system. The time-to-detect-and-remediate component relied on each security product being manually forced to conduct a scan every thirty minutes over a twenty-four hour period.

For 2014, it was decided that a new approach was needed as the methodology applied in previous tests did not reflect how a security product would be used on an endpoint in the real world. In practice, many security applications will only detect an infection during a reboot / startup or if a scheduled scan has been set by default.

For this assessment, time-to-detect will employ a methodology based on the infected endpoint being rebooted once every eight hours during a 24 hour period.

The methodology employed in this test maps more closely to real world use and although it may not be a 100% accurate model of how an "average" system is used, it gives a more realistic assessment of a security product's ability to detect and remediate an infected endpoint.

This Programme is called a "360 Assessment" since it deals with the full spectrum of malware instead of just financial malware. In the 360 Assessments, Trojans, Backdoors, Ransomeware, PUAs, Financial Malware and "other" malware are used.

Executive summary

This Certification Programme is designed to serve as a reflection of product efficacy based on what we have previously termed "metrics that matter".

In many of our previous tests, particularly those that have focused on financial malware, we started with the assumption that the endpoint has already been compromised. Being the world's largest supplier of early life malicious binaries and malicious URLs, and from our own simulator development, we know that all endpoints can be infected, regardless of the security solution employed.

For us, the metrics that really matter are not just the product's ability to block initial infection (although this is critical in most use cases). One also needs to measure the time taken for the security product to detect malware on a system and remediate it.

When conducting these tests, we tried to simulate normal user behaviour. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how certain types of malware work, how it attacks and how such attacks could be prevented. Simulating normal user behaviour means that we paid special attention to all alerts given by security applications. A pass was given only when alerts were straightforward and clearly suggested that malicious action should be blocked.

We tested a group of internet security suits and complementary security applications. With internet security suits and complementary applications, it is very important to note that the best choice for an average user is to keep things very simple and for the product not to present many popup alerts or questions.

Out of seventeen products we tested, only three managed to meet the performance specification to attain our Q2 1014 360 certification award, these being **Emsisoft Anti-Malware**, **Kaspersky Internet Security** and **Webroot SecureAnywhere Internet Security Plus.**

A further four security applications, whilst failing to meet the criteria for certification, did achieve a pass in that they were able to detect all infections and fully remediate the system within twenty four hours (a level 3 pass). These applications were: BitDefender Internet Security, ESET Smart Security, SurfRight HitmanPro and Trend Micro Titanium Internet Security 2014.

All other security applications failed the test in that they were unable to detect the malware and/or remediate the system even after the third reboot at the end of the twenty four hour period.

Certification

In order to attain a quarterly MRG Effitas 360 certification award, a security application must either protect the system from initial infection (a level 1 pass) or detect any missed malware and fully remediate the system before the first user initiated reboot (a level 2 pass). Applications that meet this specification will be given certification for that quarter.

MRG Effitas 360 Assessment & Certification Programme awards the following products as being certified for Q2 2014:

Level 1 Certification: Emsisoft Anti-Malware, Kaspersky Internet Security

Level 2 Certification: Webroot SecureAnywhere Internet Security Plus

The purpose of this report

Since its inception in 2009, MRG Effitas has strived to differentiate itself from traditional testing houses by having its primary focus on providing "*efficacy assessments"* and not just performing *"tests"*.

Traditionally, testing of security software has centred about measuring product ability to detect malware. Testing has evolved rapidly over the last two to three years and most labs, under the guidance of AMTSO (of which MRG Effitas is a member) have strived to conduct "Real World" testing.

Although there is no absolute definition of this kind of testing, loosely speaking, it involves the introduction of malware to an endpoint through a realistic vector, such as a browser or USB memory stick. Real World testing mostly includes "dynamic testing" – i.e., the malware is executed and then the ability of the security product to block the malware is measured.

Several testing labs also conduct "System Rescue" tests. These assess a security product's ability to remediate a pre-infected endpoint.

Whilst both types of tests are useful and yield valid and meaningful data, MRG Effitas wanted to merge these tests and also take one step further by measuring the time security products take to detect infections and remediate the endpoint.

To make testing more realistic to real world scenarios, no manual scanning was conducted; instead, the system was rebooted every eight hours within a twenty four hour period (three reboots in total), thereby giving security applications the opportunity to detect infections on restart.

As we have stated before in our previous tests, all malware has one primary objective, and that is to make money for the cybercriminals.

Measuring initial detection rates and also the time taken to detect active malware is important, particularly in today's threat landscape with the mix of malware that is prevalent.

As we have repeated in our previous financial malware tests, the longer a cybercriminal can have their malware on a system, the greater the opportunity there is for them to be able to capture private user information data, such as banking passwords and social media credentials, etc.

There has been an increase in the prevalence of ransomware, such as "CryptoLocker", which once active on the system, holds the user at ransom to decrypt system data or unlock the system in some other way (interestingly, the most common way CrtptoLocker is installed on an endpoint is via Zeus infections).

For these types of malware, it is initial detection that is of the greatest importance, since the vast majority of security solutions will be unable to rescue an encrypted or locked system. (In other internal tests, we have found that Webroot SecureAnywhere was in fact able to undo the encryption performed by some ransomware.)

In providing these quarterly certifications, the MRG Effitas 360 Assessment & Certification Programme is the *de facto* standard by which security vendors, financial institutions and other corporations can attain the most rigorous and accurate determination of a product's efficacy against the full spectrum of malware that is prevalent during the period.

Tests employed

In this assessment (Q2 2014), we ran the following tests:

In the Wild 360 / Full Spectrum test

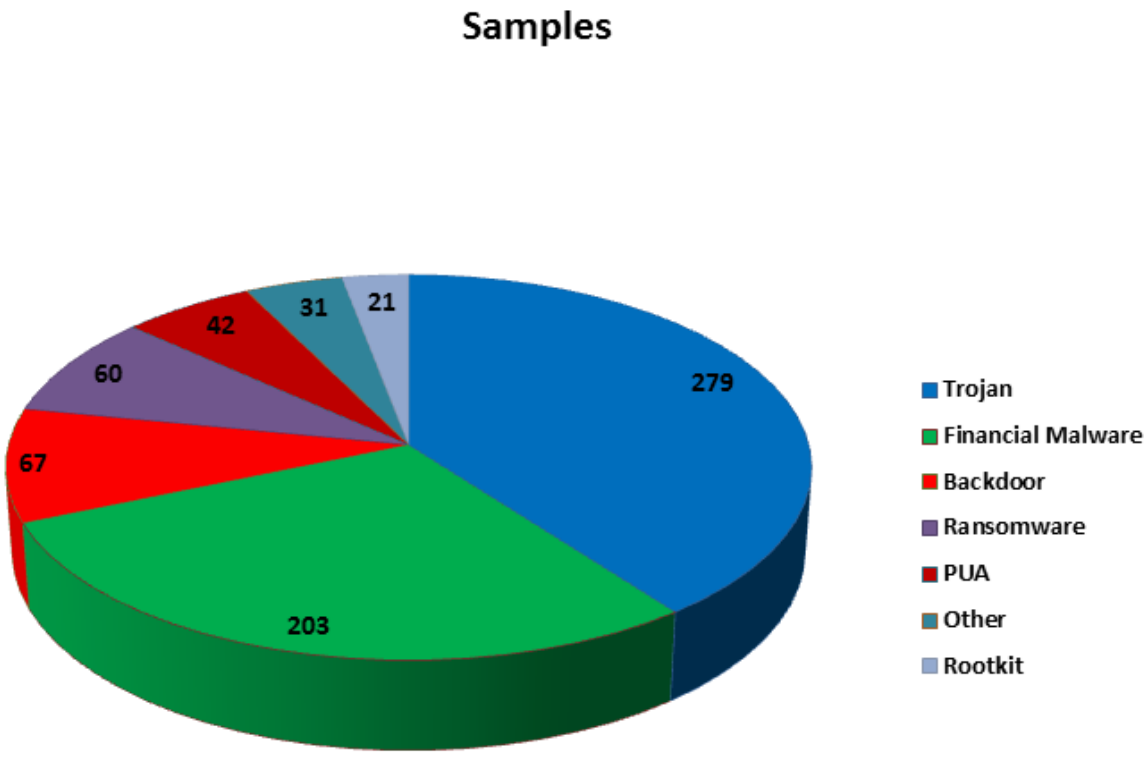
Testing was conducted as per the methodology detailed in Appendix 1.

Time to Detect and Remediate test

Testing was conducted as per the methodology detailed in Appendix 1.

Samples used

The chart below shows the makeup of the stimulus load.



Security Applications Tested

(Last program build used in the project)

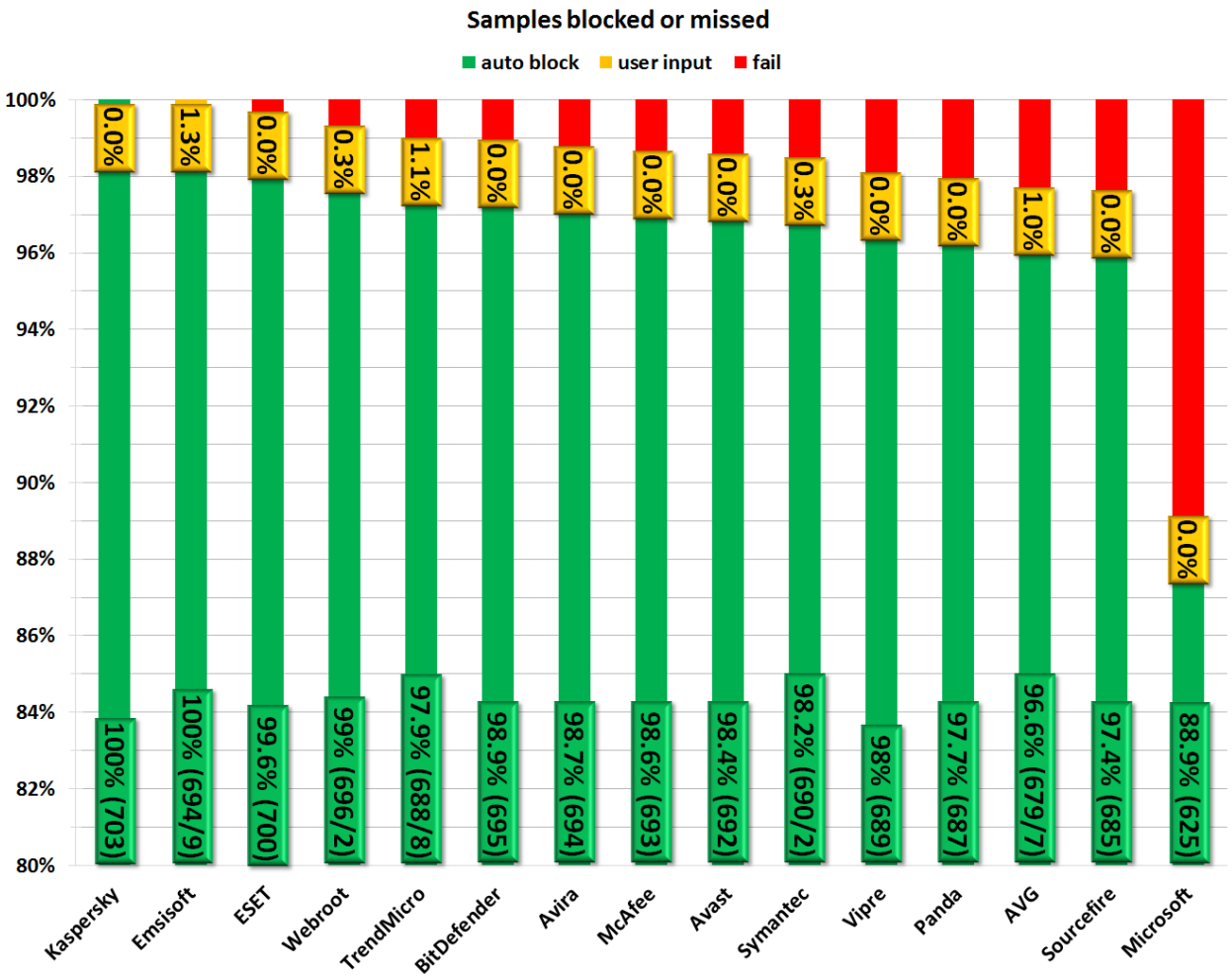
- avast Internet Security 9.0.2016.330
- AVG Internet Security 2014 14.0 Build 4569a7320
- Avira Internet Security 2014 14.0.3.350
- BitDefender Internet Security 2014 Build 17.27.0.1146
- Emsisoft Anti-Malware 8.1.0.40
- ESET Smart Security 7.0.302.26
- SurfRight HitmanPro 3.7.9 Build 216
- Kaspersky Internet Security 2014 14.0.0.5467d
- Malwarebytes Anti-Malware 2.0.1.1004
- McAfee Internet Security 2014 6.8.702
- Microsoft Security Essentials 4.5.216.0
- Panda Internet Security 2014 19.01.01
- SourceFire Immunet Antivirus Plus 3.1.8.9583
- Symantec Norton Internet Security 2014 21.2.0.38
- ThreatTrack VIPRE Internet Security 2014 7.0.4.3
- Trend Micro Titanium Internet Security 2014 7.0 Build 1151
- Webroot SecureAnywhere Internet Security Plus 2014 8.0.4.68

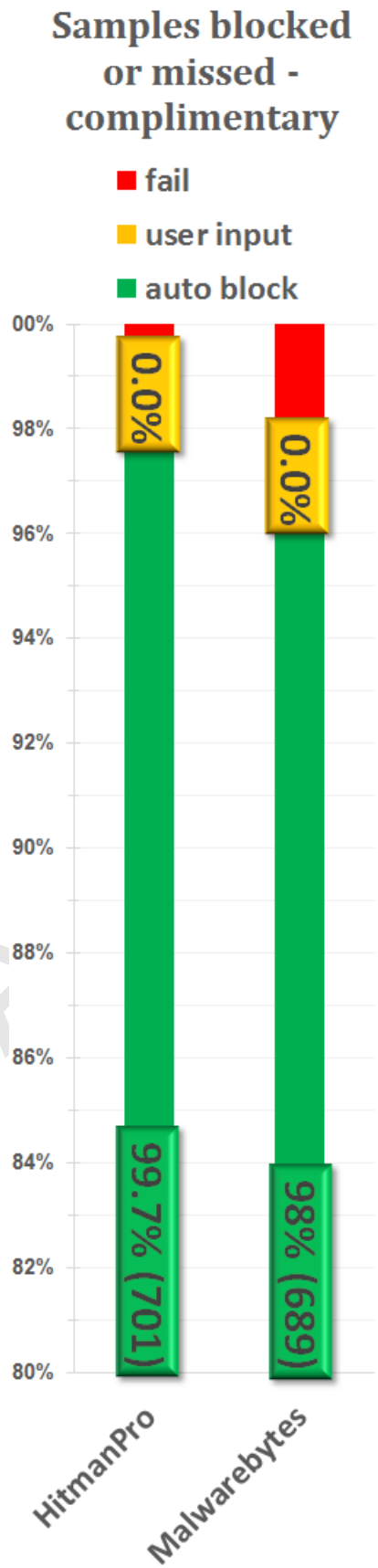
Test Results

The tables below show the results of testing in the MRG Effitas 360 Assessment Programme.

Q2 2014 In the Wild 360 / Full Spectrum test results

The table below shows the initial detection rates of the security products.





Q2 2014 Time to Detect & Remediate Test

Understanding Grade of Pass:

- **Level 1** = All threats detected on first exposure / system uncompromised

  Emsisoft Anti-Malware

  Kaspersky Internet Security

- **Level 2** = All threats detected and neutralised / system remediated before first user reboot

  Webroot SecureAnywhere Internet Security Plus

- **Level 3** = All threats detected and neutralised / system remediated within 24 hours / 3 user reboots

  BitDefender Internet Security

  ESET Smart Security

  SurfRight HitmanPro

  Trend Micro Titanium Internet Security

- **Failed** = The security product failed to detect all infections and remediate the system during the testing procedure.

  avast Internet Security

  AVG Internet Security

  Avira Internet Security

  Malwarebytes Anti-Malware

  McAfee Internet Security

  Microsoft Security Essentials

  Panda Internet Security

  SourceFire Immunet Antivirus Plus

  Symantec Norton Internet Security

  ThreatTrack VIPRE Internet Security

Appendix 1

Methodology Used in the 360 Assessment & Certification Programme Q2 2014

Methodology Used in the Assessment:

1. Windows 7 Ultimate Service Pack 1 64 bit operating system is installed on a virtual machine[i] 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. 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 and allows it to be executed.
8. Testing on infected systems continues for twenty four hours by the following process:
    a. The system is rebooted every eight hours during a 24 hour period resulting in a total of three reboots.
9. Remediation performance of an application is determined by manual inspection of the system in contrast to its pre-infected state and not by the determination of the security application itself.[iv]
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 Q2 2014.

[i] VM hardware spec is 4GB RAM & 2 core processor.
[ii] AES includes Adobe Flash, Reader, Java, Microsoft Office 20010, Internet Explorer 11 & VLC Player. All Microsoft components are fully updated, all third party components are out of date by three months.
[iii] During the installation of the security application, if an option to detect PUAs is given, it is selected.
[iv] This is because in some instances, an application will claim to have removed an infection, but has failed to do so and can be seen still active on the system.