SE Labs

INTELLIGENCE-LED TESTING

www.SELabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

ADVANCED ENDPOINT PROTECTION TEST

JULY 2017

CONFIDENTIAL

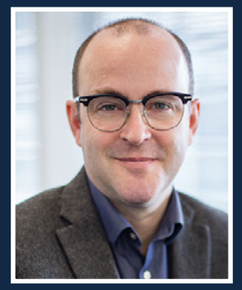
SE Labs was commissioned to test the effectiveness of **Morphisec Endpoint Security** in relation to its abilities to detect and protect against software exploits that attack vulnerable applications in memory.

The product was deployed in a realistic manner and exposed to a range of threats proven to successfully exploit vulnerabilities in software where there are no protection mechanisms provided.

The results in this report indicate how effectively the product was at detecting and/or protecting against those threats in real time.

CONTENTS

Document version 1. 0. Written 31st July 2017



SIMON EDWARDS
Director

WEBSITE www.SELabs.uk
TWITTER @SELabsUK
EMAIL info@SELabs.uk
FACEBOOK www.facebook.com/selabsuk
BLOG blog.selabs.uk
PHONE 0203 875 5000
POST ONE Croydon, London, CR0 0XT

MANAGEMENT
Operations Director Marc Briggs
Office Manager Magdalena Jurenko
Technical Lead Stefan Dumitrascu

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Gia Gorbold
Alexandru Statie
Jon Thompson
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
Colin Mackleworth

SE Labs Ltd is a member of the Anti-Malware Testing Standards Organization (AMTSO)

INTRODUCTION

It is no longer news that attackers are targeting organisations and abusing software vulnerabilities to breach networks. Or rather, it is very much news in every national media outlet. The month before we ran this test some of the world's largest organisations were attacked and infected with ransomware. The malware spread using a known vulnerability in a Microsoft network protocol and caused an unknown (but doubtless large) amount of damage.

While security updates are an effective solution against known vulnerabilities, they cannot predict new attacks that are developed specifically to bypass existing counter-measures. So-called 'zero day' attacks are unknown by the general public, including the developers of the vulnerable software. Stopping a zero day attack is notoriously hard precisely because defenders have no knowledge of its details.

Traditional anti-malware solutions typically combine malware signatures (basic information about known attacks); behavioural analysis (checking an application's behaviour and judging how suspicious it is); and reputational weightings (is this file well-known and generally considered to be 'clean', or is it widely considered to be malware?) Exploit protection is sometimes included, but in practice may still rely on signatures, behavioural analysis and reputational judgements.

We exposed **Morphisec Endpoint Security** to a range of in-memory exploits. We checked that these would succeed in successfully exploiting a target without protection and then compared the results to those gathered when the same attacks were launched against a system protected by **Morphisec**. This report contains our results.

EXECUTIVE SUMMARY

Product tested

PRODUCT	PROTECTION ACCURACY RATING	LEGITIMATE ACCURACY RATING	TOTAL ACCURACY RATING
Morphisec Endpoint Security	100%	90%	97.5%

The ratings above are weighted to take into account the different levels of detection and protection provided by the products. Negative ratings are allocated when a product misses threats or misclassifies legitimate applications.

Morphisec Endpoint Security is designed to prevent advanced attacks by stopping the exploitation of vulnerable applications. Its developers claim that the technology works by changing how applications load into memory, making things unpredictable for attackers.

The product was exposed to three sets of working exploits: 32-bit, 64-bit and threats that had been customised to evade anti-malware detection. It was also exposed to regular applications to ensure that it did not simply block every attempt to execute code on the system. A good security product will block threats without generating significant numbers of 'false positives'.

- **Morphisec Endpoint Security detected and blocked all of the known exploits.**
- **The product was also completely effective at detecting and blocking evasive malware.**
- **There was a small number of false positive results generated against free third-party applications.**

Simon Edwards, SE Labs, 31st July 2017

In-Memory Exploit Attacks

These results illustrate how each product handled the types of attacks that criminals use when attempting to compromise computers belonging to specific individuals.

Tactics typically include sending email attachments containing customised malware that appears to be a legitimate document or other innocent file.

The results below use the following terms:

Stopped – the product prevented the attack from exploiting the target

Notified – the product has detected the attack and alerted the organisation

Allowed – the product failed to prevent the attack from exploiting the target

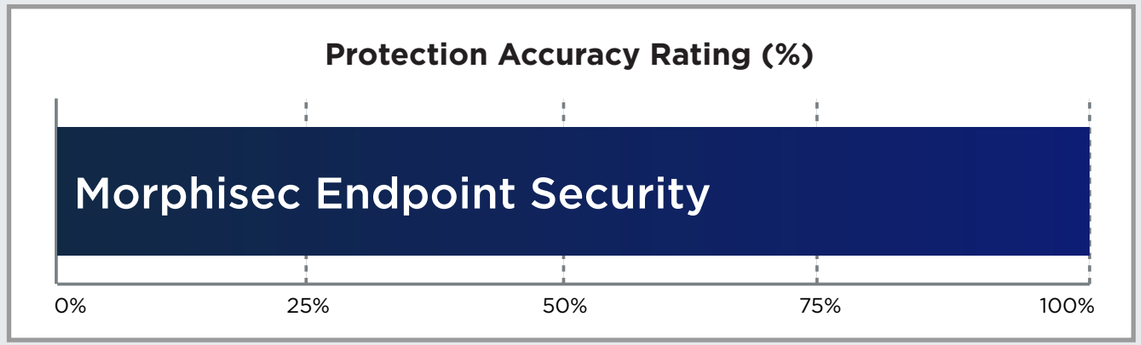
It is possible for a product to detect and notify the organisation about a threat without preventing the exploitation of the target. Products are awarded four points for stopping a threat, two for warning about it (but not blocking it) and -5 points for allowing the threat to succeed.

In-Memory Exploit Attacks (32-bit)

Product	Stopped	Notified	Inbox	Protection Accuracy Rating	Protection Accuracy (%)
Morphisec Endpoint Security	25	25	0	100	100%

In-Memory Exploit Attacks (64-bit)

Product	Stopped	Notified	Inbox	Protection Accuracy Rating	Protection Accuracy (%)
Morphisec Endpoint Security	25	25	0	100	100%



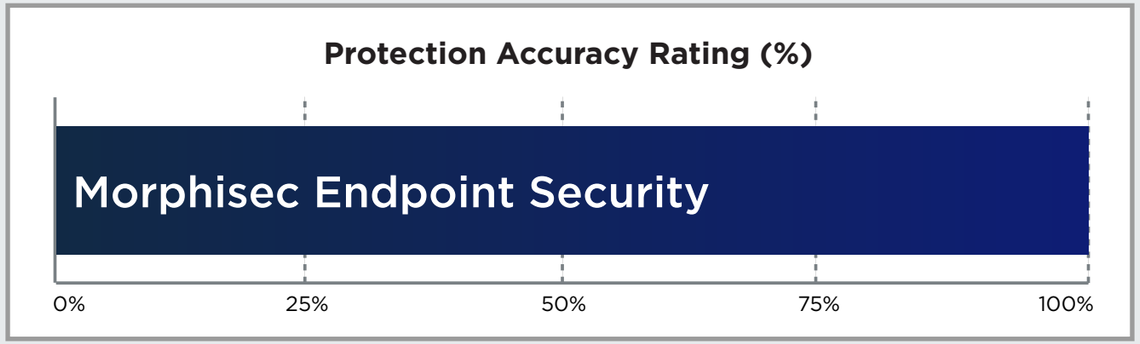
Evasion Effects

Attackers have a large range of techniques available to hide the malicious nature of their malware. This can involve using encryption, compression and other methods of 'scrambling' the code of a file to obfuscate its true nature.

In this test we used exploits to deliver stealthy payloads capable of evading anti-malware products. Techniques used included, but were not limited to, re-encoding, polymorphism and code injection.

Evasion Effects

Product	Stopped	Notified	Allowed	Evasion Effects Accuracy Rating	Evasion Effects (%)
Morphisec Endpoint Security	25	25	0	100	100%



Legitimate Applications

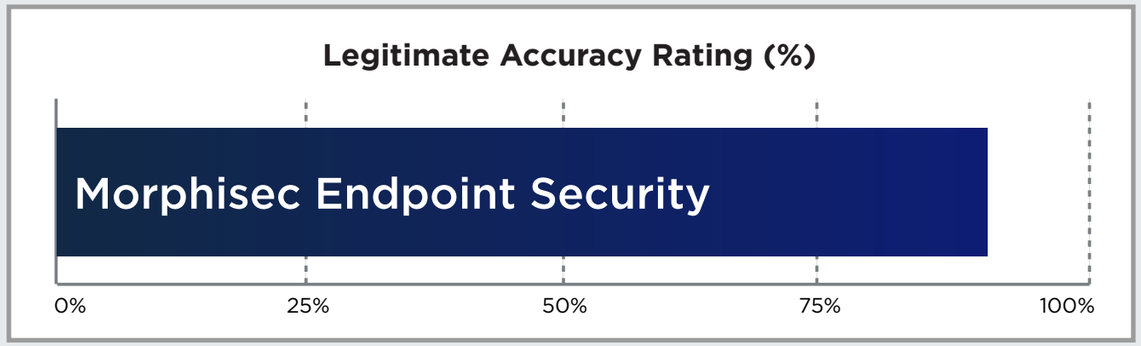
A set of legitimate files, including documents of varying formats and executable programs, were submitted to the product.

It is important to test for false positives because too many indicate a product that is too aggressive and will block useful applications as well as threats.

It would be easy to create a product that blocked all threats if it was also allowed to block all legitimate files. Finding the balance between allowing good and blocking bad is the key to almost every type of security system.

Each product is awarded two points for every legitimate file that it does not detect as malware. For each misclassification it loses eight points.

Legitimate Applications					
Product	Stopped	Notified	Allowed	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Morphisec Endpoint Security	1	0	49	90	90%



Summary

Accuracy Ratings	
Protection Accuracy Rating	100%
Legitimate Accuracy Rating	90%
Total Accuracy Rating (%)	97.5%

In-Memory Exploit Attacks	
Stopped	50
Notified	50
Allowed	0
Protection Accuracy Rating	200
Protection Accuracy (%)	100%

Evasion Effects	
Stopped	25
Notified	25
Allowed	0
Evasion Effects Accuracy Rating	100
Evasion Effects (%)	100%

Legitimate Applications	
Stopped	1
Notified	0
Allowed	49
Legitimate Accuracy Rating	90
Legitimate Accuracy (%)	90%

Conclusions

Morphisec claims that its **Morphisec Endpoint Security** product can, "Prevent advanced attacks like APTs, zero-days, ransomware and evasive malware." We tested this claim by exposing it to known exploits, new stealthy malware and regular applications. Ideally it would stop all of the threats and allow all of the legitimate programs to run.

The threats that we used are commonly used to target organisations of all sizes. Threats were changed in a number of ways to see how easy it would be to bypass the detection and blocking mechanisms of **Morphisec's** product. The methods and tools used are available to every internet user with an interest in exploiting systems. They are zero cost to obtain and uncomplicated to use, which makes them very dangerous.

Morphisec Endpoint Protection detected and blocked all of the known exploits, as well as all of the evasive malware. It allowed most legitimate applications to run unhindered. This is an excellent result for an endpoint product. In our public tests of anti-malware products we rarely see such a strong success rate.

Appendices

Appendix A: FAQs

A full methodology for this test is available from our website

- This test was commissioned and paid for by **Morphisec**. **Morphisec** had no control or insight into the selection of threats and legitimate applications used in this test.
- The test was conducted between 25th May and 31st July 2017.
- The systems used in the test had full internet access and were confirmed to have access to any required or recommended back-end systems.
- Public threats and legitimate applications were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs. They were created and managed by Metasploit Framework Edition using default and custom settings. The choice of exploits was advised by public information about ongoing attacks. One notable source was the 2017 Data Breach Investigations Report from Verizon.
- Malicious and legitimate data was provided to **Morphisec** once the full test was complete.
- SE Labs conducted this endpoint security testing on virtual machines.

Appendix B: Product Versions

Product Versions		
Vendor	**Product**	**Build**
Morphisec	Morphisec Endpoint Security	2.0