TRAPMINE ThreatScore Machine Learning Engine Malware Detection Certification

2018

Contents

Introduction

ThreatScore is a machine learning-powered malware detection engine, a part of TRAPMINE which is an endpoint protection platform combining proven technologies such as machine learning, behaviour monitoring and endpoint deception techniques.

This assessment measured the protection capabilities of TRAPMINE ThreatScore static machine learning (ML) engine by testing against in-the-wild malware attacks.

The methodology employed in this test maps: scanned statically with PE EXE files, as there is no URL protection feature implemented.

This test deals with large spectrum of malware like trojans, backdoors, ransomware, financial malware and "other" malware are used.

MRG Effitas is a member of AMTSO (Anti-Malware Testing Standards Organization, Inc.)

Executive Summary

TRAPMINE ThreatScore Machine Learning Engine 3.0 was tested in this report.

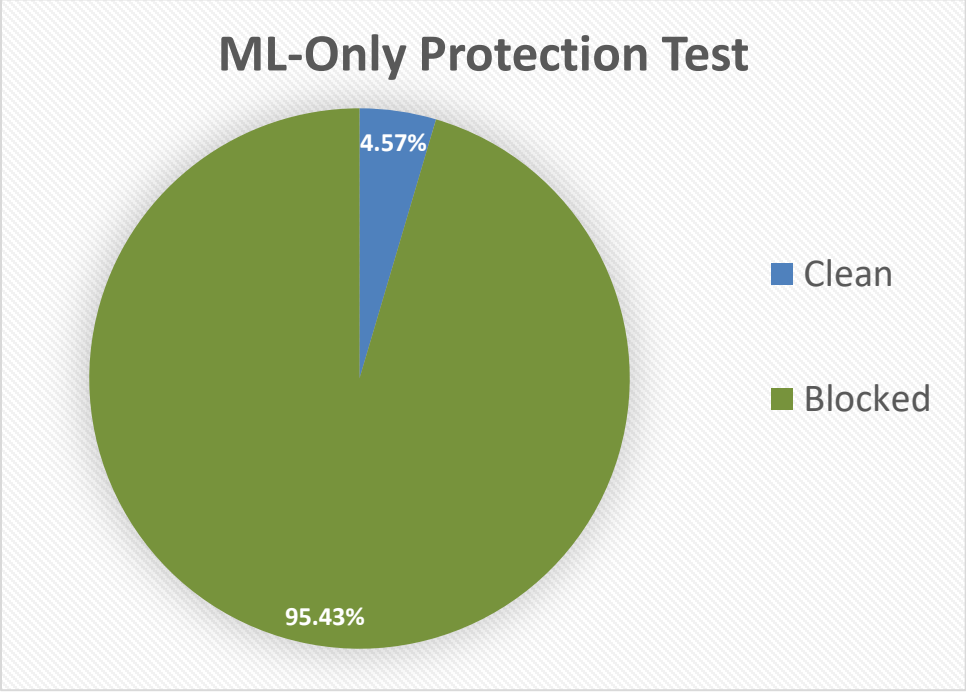
In total, 350 fresh in-the-wild malware has been tested.

MRG Effitas certifies the ability of TRAPMINE ThreatScore Machine Learning Engine to detect malware.

Test date: 25 July 2018 – 30 July 2018.

Certificate number: 2018073001

This certificate is valid until: 2019 July 30



Tests Employed

When conducting these tests, we scanned statically ITW samples, as there is no URL protection feature implemented. A pass was given only when alerts were straightforward and clearly suggested that malicious file should be blocked.

In this assessment, we ran the following test:

In the Wild Test

Most of the malicious files used in this test were compromised legitimate websites which served malware. Some of the files come from various fresh spam campaigns or fake porn websites. The remaining files come from our regular honeypots or, in case of ransomware and financial malware in particular, we used files from newly discovered distribution sites.

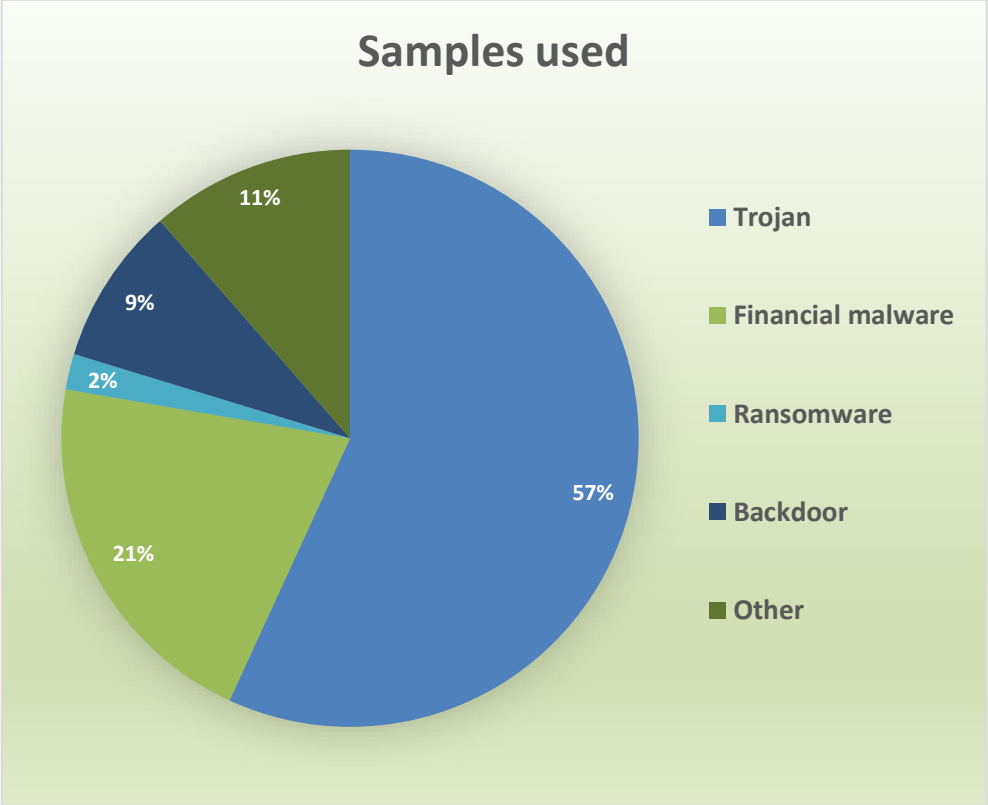
Malware used in this test can be considered as Zero Day in the true meaning of that phrase. This posed a great challenge to all participants as new variant samples such as GandCrab (Ransomware), Emotet (Banking Trojan) and many others caused most damage.

It is our opinion that Emotet currently poses the greatest threat to users, for this reason we choose to use more files than before.

Because of the wide spectrum of malware used in this project and the freshness of the samples, we used a smaller set than usual.

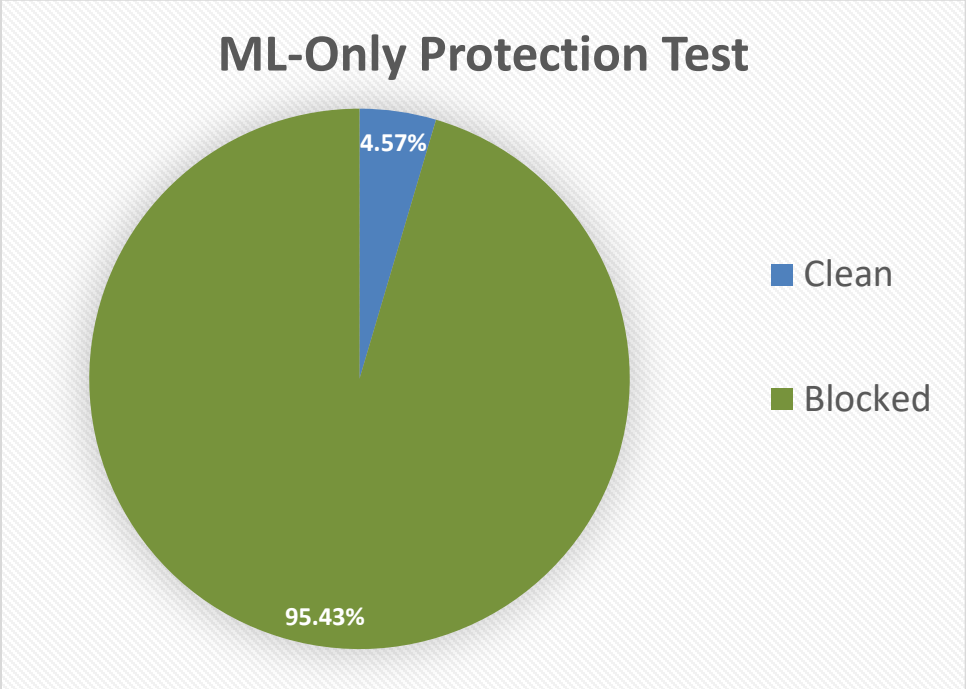
Testing was conducted as per the methodology detailed in Appendix 1. In total, 350 live ITW samples were used. The stimulus load comprised the following: 199 trojans, 31 backdoors, 73 financial malware samples, 7 ransomware samples, and 40 others.

Malware sample types used to conduct the test.



Test Results

The table below shows the initial detection rates of machine learning engine of the security product.



Appendix 1
Methodology Used in the TRAPMINE ThreatScore Machine Learning Engine Certification

Methodology used in the assessment:

1. All samples were scanned statically.
2. The malware was not executed.
3. A test is deemed to have been passed based on the following criteria:
    a. In the result, the security application clearly states that the sample is malicious and considered as a threat.
4. A test is deemed to have been failed based on the following criterion:
    a. The security application fails to detect the sample under condition 4a.
5. All testing was conducted during Q3 2018.