**Keywords:** anti-malware; compliance; assessment; testing; test plan; template; deceptor; security; App Esteem

AppEsteem and AMTSO
Preparation Date: October 12, 2017
Documentation Source Dates : August 2017

**Version 4.0**

# AppEsteem Deceptor Test Plan for Q4 2017

**Authored by:** Dennis Batchelder, President, AppEsteem

**AMTSO Consultative Resources**: John Hawes, Scott Jeffreys

**Abstract:**

This Test Plan has been prepared by AppEsteem as part of the AMTSO Operational Pilot Implementation of the Draft 5 Standards. AppEsteem has commissioned AV Comparatives to run a comparative test to measure AV Vendor effectiveness of blocking apps it has called out as Deceptors. This Plan details the testing activities in its Deceptor Program for the Q4 2017 timeframe.

This document has been developed using Test Plan Template Version 1.1 from August 2017. Wherever conflicts might exist between this Template and the Standards, the Testing Protocol Standards will provide the prevailing rule.

Anti-Malware Testing Standards Organization

# Table of Contents

# Deceptor Test Plan

## 1. Introduction

The objective of the Deceptor Test is to measure how effective various AV products are at quickly detecting the apps called out by AppEsteem Corporation as Deceptors, especially as some of these apps attempt to evade detection. It is our desire that all AV vendors will improve their products to be able to detect all apps called out as Deceptors, which is a malware category, and not considered PUA. AppEsteem provides all AV vendors access to their Deceptor list, both on a website and available as a web API call.

AppEsteem has commissioned this test from AV Comparatives. We intend to adhere to the AMTSO Testing Protocol Standard, currently in draft form and posted here: http://amtso.org/wp-content/uploads/2017/07/Testing-Protocol-Standards-for-the-Testing-of-Anti-Malware-Solutions_APPROVED_DRAFT.pdf. We hope all vendors tested will be Voluntary Participants in this test.

## 2. Scope

In our test, we intend to include consumer-targeted AV products from vendors who are members of AMTSO. We will test with default configuration, which may mean that PUA protection is turned off. AV vendors who request to opt out before the test starts, and have attested that their consumer products have less than 1% consumer install share, will be excluded upon request.

We plan to test AV effectiveness in detecting and blocking the installation of apps that have been listed on AppEsteem's Deceptor page (https://customer.appesteem.com/deceptors).

## 3. Methodology and Strategy

The test will measure whether AV products can prevent the installation of a Deceptor app. For Windows apps, the test will validate if the AV product can successfully block the installation. For browser extensions, the test will validate if the AV product can successfully block the "developer model" installation of the extension. No MacOS Deceptor apps will be included in the test.

Note that the test is specifically against the app install packages. It will be considered a fail if the detection occurs after installation has started.

The test clients will be running Windows 10 home edition.

The test will attempt to use the originally-listed as well as the latest-available versions of each app deemed a Deceptor. We will test continuously throughout the test period, using fresh versions of the apps. We expect to refresh the apps and rerun the tests as frequently as every hour.

## 4. Participation

All participants in this test may be Voluntary. There is no cost to be voluntary.

**Opt-Out Policy**: We will honor any opt-out request for AV products who attest they have less than a 1% global consumer install share to opt out from this test. Vendors may opt out from the test up to the Test Commencement date (defined in Section 6).

**Conflict of Interest Disclosure**: The test will use the data and samples provided through AppEsteem's free-to-access Deceptor API and website. Vendors who regularly access and respond to AppEsteem's API will have a significant advantage over vendors who don't.

**Funding**: In the interests of driving urgency into protecting consumers better from unwanted and deceptive apps, AppEsteem and AV Comparatives are sponsoring this Deceptor test. AppEsteem anticipates that better Deceptor coverage will drive better behavior from app vendors, which may in turn increase AppEsteem's business.

## 5. Environment

**Physical Configuration**: We will test on standard Windows 10 Home Edition systems that attempt to replicate typical consumer configuration. The AV products will be tested in default configuration with a paid consumer license, even if this means PUA is turned off (we believe this is fine, as Deceptors are considered malware, and not PUA). We request that Voluntary Participants provide a consumer license key that can be used to test the product before Test Commencement, as defined in Section 6.

**Sample Relevance**: All samples used in the test will be obtained from the public pages listed on AppEsteem's Deceptor page. Note that some apps use forms of polymorphism, so the samples obtained for the test may be different than the samples that a vendor can download themselves.

**Geographic Limitations**: We have no geographic limitations in this test.

**Curation Process**: Samples will be obtained from the public pages listed on AppEsteem's Deceptor page. After the test is complete, the samples used will be made available to all participants. Participants may dispute the inclusion of any sample in the final results, and AppEsteem will review the disputes and be the sole decider of whether the sample will remain.

**Distribution of Test Data**: Vendors will be provided with a list of all the samples used in the test.

## 6. Schedule

**Start Date Range**: The Commencement Date of the test will occur between November 1, 2017 and November 30, 2017.

**Test Duration and Calculated End Date**: The test is anticipated to last one to two weeks from the commencement of the test.

**Milestones**: Interim milestones that can be reviewed by Participants, including the anticipated delivery of a Test Report, should be specified where applicable.  The following Sample Schedule Summary can be used as a reference.

***Sample Schedule Summary for Test Project***

| Index | Test Activity | Start Date Range | Dependencies |
|---|---|---|---|
| ***1*** | *Test Commencement* | *November 1, 2017 -<br>November 30, 2017* | |
| ***2*** | *Confirm Vendor Configuration Feedback* | *One week after Test Commencement* | |
| ***3*** | *Milestone 2 – Test Report First Edition – End of Testing Period* | *Two weeks after Test Commencement* | *(1), (2)* |
| ***4*** | *Feedback and Dispute Resolution Time – Retests as Needed* | *A period of two weeks, starting one week after Milestone 2.* | *(3)* |
| ***5*** | *Milestone 3 – Issue Final Report – End Date for Test* | *Four weeks after Milestone 2.* | *(4)* |

**Communications**: Deviations of more than one month from the above dates will trigger an updated schedule notification to all participants.

**Risks and Risk Management**: We have no specific known risks for this test.

## 7. Control Procedures

The test will attempt to verify whether the AV products were installed successfully, are logging appropriately, and can communicate to and receive updates from their appropriate backend services. At any time before Test Commencement, Participants may optionally provide instructions to validate connectivity, turn on logging, and configure to receive updates.

## 8. Dependencies

**Participant Actions**: Participants are expected to review the samples and dispute as necessary during the Feedback and Dispute Resolution Time, as defined in Section 6 and 10.

## 9. Scoring Process

AV products will be scored based on their detection rates of the Deceptor samples. The score will be the percentage of Deceptor samples successfully blocked, and this score will be calculated against three sets of samples:

1) Original samples reported by AppEsteem in its Deceptor API

2) Samples recently "harvested" from the Deceptor landing pages

3) All samples

## 10. Dispute Process

After reviewing the samples included in the test, Participants may dispute the inclusion of any sample. Participants must provide the sample hash, the reason for the dispute, and evidence as to why the sample should not be included in the test. AppEsteem will review all dispute requests that have provided evidence and make a final determination.

## 11. Attestations

I confirm that I intend to meet each of the following guidelines to the best of your ability.

1. I intend to provide public notification on the AMTSO website that has met its obligation for public notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)

2. I confirm that all products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)

3. I will disclose any anticipated imbalance or inequity in your test design to all Participants in your Test. (Section 2, Section 3)

4. I may charge for Participation in a Test, but will not charge additional fees for Participants to be Voluntary. (Section 4)

5. I confirm that any material conflict of interests or other information that could materially impact the reliability of the Test will be disclosed. (Section 4)

6. I will provide disclosure as to how the test was funded. (Section 4)

I hereby affirm that I believe this Test Plan complies with the AMTSO Testing Standards.

Signature:

Name: Dennis Batchelder, AppEsteem Corporation

Test Lab: AV Comparatives

AMTSO test ID: AMTSO-OP1-TP105