Keywords: unwanted software; PUA; UwS, Deceptor; Certified; test plan, AppEsteem

December 29, 2023
Published January 2, 2024

Version 1.1

UwS Handling Certification Test Plan for 2024

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version 1.3 (the "Standard"). AppEsteem Corporation is solely responsible for the content of this Test Plan.

©AppEsteem Corporation, 2023-2024. All rights reserved.

Table of Contents

©AppEsteem Corporation, 2023-2024. All rights reserved.

Uws Handling Test Plan for 2024

1. Introduction

The Internet is rife with apps that use alternative software monetization. These apps offer themselves up as various forms of "free" software (e.g., free to scan, free to try, free with ads or offers, free because they bundle offers to silently install other apps for free, free because they borrow computer resources, or freemium). Because these apps rely on large numbers of installs or high conversion rates to paid versions, a significant percentage of software monetization apps use aggressive techniques to trick consumers to download, install, accept other offers, advertise, and even pay for software. When these techniques become overly aggressive, AVs typically label the software as "Unwanted" or "Potentially Unwanted" and prevent them from downloading, installing, and running on their customers' systems.

It's not easy for AVs to keep up with software monetizers. Industry file sharing is sporadic, and since these apps rely on human, not system, vulnerabilities, automating their classification is difficult. Because of traditionally different AV standards of what's Unwanted and what's Potentially Unwanted, testing detection capabilities against overly aggressive software monetizers has been problematic.

For the past eight years, AppEsteem has worked to establish a consensus among AVs about the behaviors that make an app Unwanted Software (UwS) or a Potentially Unwanted Application (PUA). We have codified these behaviors into "ACRs", or Application Certification Requirements. We publish a freely available Deceptor® feed, which contains software monetization apps we believe are Unwanted, and a freely available Certified feed, which contains apps we have certified as clean, and that we believe should be considered neither UwS nor PUA. These feeds are widely used by many parties, including AVs.

We believe that our Deceptor and Certified feeds are a valuable tool for helping fight against consumer cybercrime and fraud committed by software monetizers. Having an agreed-upon set of behaviors that apps must avoid makes it efficient for cooperating AVs to eradicate bad behavior and protect their customers. Conversely, if the AVs do not cooperate, their workload increases, and their customers are underserved. By providing both Deceptor and Certified feeds, we help AVs and their associated automation and AI services disambiguate between good and bad behavior, which leads to better consumer protection against apps not provided in the feeds.

We believe that consumers are better served if they choose an AV that is efficient at processing our feeds, because then the AV's customers will have more Unwanted software blocked, and more clean software monetizers will run unimpeded.

The objective of this UwS Handling Certification Test is to provide consumers with information on which AV products have effectively implemented our Deceptor and Certified feeds, so they can be assured of effective protection against over-aggressive software monetizers while not getting impeded from working with "clean" software monetizers.

In the test, allowances have been taken to allow AVs to describe any deviations they have

©AppEsteem Corporation, 2023-2024. All rights reserved.

between their own UwS and PUA software policies and our ACRs. We will support AV product disputes on our test results through our portal.

This test has no significant changes in methodologies or policies from the plan we established for 2023.

We intend to follow the AMTSO Testing Protocol Standard for this UwS Handling Certification Test, and we hope all tested AVs will choose to be Participants.

2. Scope

In the test, we intend to include consumer-targeted AVs. We will focus on the most basic AVs of each vendor that we believe supports UwS protection. We will test versions that are currently available for consumers to download and install at the time of each test. To most closely replicate what its customers see, we will test each AV in its default configuration (including accepting in the affirmative when protection options are presented to the consumer at install time with no default answer pre-selected).

We plan to test AV effectiveness in detecting and automatically blocking the installation and initial execution of apps that have been listed within the previous six months on AppEsteem's Deceptor page (https://customer.appesteem.com/deceptors), and not blocking the installation and initial execution of apps that have been listed within the previous six months on our Certified page (https://customer.appesteem.com/certified). The test does not measure the AV's ability to block or allow landing pages, or the AV's ability to detect subsequent execution.

3. Methodology and Strategy

The test will measure whether AV products can effectively use AppEsteem's feeds to prevent the timely installation and initial execution of a Deceptor app, and allow the installation and initial execution of a Certified app. These installers will either be placed onto the system as part of the test, or dynamically downloaded from the official Windows and Mac app stores. We understand that this is different than other AV tests; the reason for this difference is that we have learned that the best way to influence software monetizers to change their overly aggressive behavior is to block the app from ever running.

The test samples will be OS-specific (e.g., when testing on Windows, only Windows apps will be tested.

We will publish test results monthly. Before each month's tests commence, we will obtain the latest publicly available version of each AV, and we'll attempt to update its signatures.

Note that the test is measuring the ability of the AV product to either prevent or allow the app from running. This may happen at, during, or immediately after installation. It will be considered an "allow" if the app that gets installed runs, and a "block" if it does not. Allowing a Deceptor app will be considered an FN. Blocking a Certified app will be considered an FP.

The test clients will be running Windows 11 home edition and macOS Ventura with the latest

©AppEsteem Corporation, 2023-2024. All rights reserved.

available updates as of the time of the test. Please note that the OS may receive updates during the test. The AVs will be running the latest available components for the current version at the time of the test.

The test will only test the listed samples contained in our feeds. In essence, it is an open book test designed to measure the ability of the AV to use our feeds to protect their customers.

We understand that AVs may have already been detecting the Deceptor app before we listed it, and they may continue to detect the app after we clear it.

4. Participation

All tested AVs in this test may become Participants at no cost. We charge no fee to be tested, and we offer no additional for-pay services to AVs. Participants may suggest which of their consumer-based AVs we should include in our test, and unless we have a good reason otherwise (such as not suggesting in time, or if we believe the suggestion was not made in good faith), we'll honor those suggestions. Participants can also provide us with a post-run script that we'll execute to gather up any logs. All Tested vendors will be able to audit their configuration by using our web-based portal to view a video showing the options selected during AV's install, that the components and signatures are up to date, and that there is Internet connectivity. As required by the AMTSO standard, Participants also have the ability to provide commentary on test results.

Vendors can register to use our portal as follows:

1. Create an account on our portal at https://customer.appesteem.com and log in
2. Register Vendor company
3. Click "Enroll for AV Test"
4. Enter the AV that you expect us to test and submit
5. Once we provision the account, options for providing policy deviations, requesting an API key, and managing test results will appear on the dashboard page.
6. Three web services are available to help Vendors prepare for the test:
    - https://customer.appesteem.com/api/deceptors
    - https://customer.appesteem.com/api/certified
    - https://customer.appesteem.com/api/DeceptorTest?apikey={KEY}

Opt-Out Policy: AV vendors may request to opt out of the test, and we will use factors such as the AV's market share as well as its claims of effectiveness against UwS and PUA to evaluate the request.

Conflict of Interest Disclosure: The test will use the data and samples provided through our free-to-access Deceptor and Certified APIs and websites. AV vendors who regularly access and respond to our APIs will have a significant advantage over vendors who do not.

Funding: We are self-funding this test. Our business model is based on us selling services to software monetizers about apps they wish to certify as clean. We believe that the more efficient the AVs are at detecting Deceptors and allowing Certified apps, the more valuable our certification service is for software monetizers. We expect that this test will accrete value for our customers as well as attract new customers to our certification services.

©AppEsteem Corporation, 2023-2024. All rights reserved.

5. Environment

Physical Configuration: We will test on fully updated standard consumer OS systems, running either native or virtually, connected to the Internet, that attempt to replicate typical consumer configuration. The AVs will be tested in default configuration with a paid consumer license. If any configuration questions are asked that do not supply a default answer, we will choose the answer closest to an affirmative answer. We will purchase the licenses to the AVs.

Sample Relevance: All samples used in the test will be obtained from our Deceptor and Certified feeds. No sample will be chosen if it's been posted for less than one (1) day, or for more than six months. Only samples for apps that we have not marked as inactive or resolved will be used. For Certified samples, it's possible that we have certified apps against an older set of ACRs; to avoid confusion, we will only include Certified samples for apps when they do not fail any of our current ACRs.

Note that all samples are available to be known in advance by all Tested AVs. There will be no surprises. All AV Vendors will have plenty of opportunity to dispute these samples in advance of the test, as part of their operationalization of handling our feeds or by examining them.

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

Curation Process: Samples have been curated by us as part of our ongoing Deceptor hunting and Certification business, and they are contained in our Deceptor and Certified feeds. Before, during, and after the test, all samples are available to all Tested vendors. We provide APIs for test results, and a web-based portal (instructions in the Participation section above) so all Tested Vendors can dispute the inclusion of any sample in the final results, and dispute whether the sample is relevant to them because of their own UwS and PUA policies. We will review the disputes and be the sole decider of whether the sample will be included or counted as relevant.

Distribution of Test Data: A listing of the samples used from the feed will be made available through our web-based portal. The web-based portal (instructions in the Participation section above) will show the samples tested, whether the AV blocked or allowed it, and whether this resulted in a pass or fail. Also in the portal we will provide video evidence the app running if the app was allowed, and video evidence of the app unable to run if the app was blocked. If Participants provide us with a post-run script to gather logs and auditing data, we will execute the script and provide these results as well.

6. Schedule

Start Date Range, Test Duration, and Calculated End Date: The UwS Handling test will run twice a week commencing in January 2024, and will continue throughout the calendar year. We will produce monthly Test Reports and grant earned certifications based on the test runs that were completed during the month.

©AppEsteem Corporation, 2023-2024. All rights reserved.

Milestones: Each month we plan to follow this schedule.

Sample Schedule Summary for Test Project

Index	Test Activity	Start Date Range	Dependencies
1	*Test Commencement*	*Twice weekly starting the first week of each month*	
2	*Review AV Configuration*	*Anytime during the month*	
3	*Preliminary Results and Disputes*	*Anytime during the month after the first test run is complete*	*(1), (2)*
4	*End of Testing Period*	*End of each month*	*(3)*
5	*Disputes close*	*Five business days after the end of each month*	*(4)*
6	*Final Test Report*	*Within ten business days after the end of each month*	*(5)*

Communications: We will notify all Tested vendors if there are significant deviations from this schedule (for instance, around observed holidays not listed on AMTSO).

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

7. Control Procedures

Connectivity Validation: We will run the test from VMs connected to the Internet. We will provide video evidence in our web-based portal (instructions in the Participation section above) that demonstrates that there was connectivity. Vendors can provide a post-run script that we will execute after each test run if they wish to confirm cloud connectivity themselves.

Logging: As we are replicating a typical consumer configuration, we will not turn on logging during the test. Vendors can provide a post-run script that we will execute after each test run if they wish to collect their own logs.

Updates: We will use the AV's consumer-accessible user experience to check for updates prior to each test run, and we will share the results as part of the video evidence that we will provide. Vendors can provide a post-run script that we will execute after each test run if they wish to

©AppEsteem Corporation, 2023-2024. All rights reserved.

validate the updates themselves.

8. Dependencies

Participant and Test Subject Vendors Required Actions: Tested vendors are requested to review preliminary results and provide disputes throughout the month.

9. Scoring Process

For each monthly Test Report, we will exclude samples that were successfully disputed, and we will remove samples for each AV that were deemed not relevant due to the AV's own UwS and PUA policies.

For the remaining samples, AVs who block Deceptors with less than 5% FNs, and who allow Certified apps with less than 5% FPs, will be deemed to have passed the test. Because sample size could be small, AVs will be deemed to have passed the test if they have less than 2 FNs and less than 2 FPs.

We will grant certifications to AVs who we deem have passed the test and who support at least 90% of our Deceptor-level ACRs with their own UwS and PUA policies.

10. Dispute Process

Disputes are available, at no cost, to all Participants and all Test Subject Vendors.

We provide a web-based portal (instructions in the Participation section above) that all Tested vendors can use to review the test run results, see their Test Reports, and dispute the includes of samples. We also provide a web service for receiving Test Reports. Both the portal and the web service will be continuously available throughout the test. We will accept disputes against a monthly Test Report until five business days after the end of each calendar month.

We request that each Dispute is accompanied by either an element of proof or evidence that the dispute is legitimate.

Disputes can be made as follows:

1) When the sample is bad, corrupted, or longer applicable. In such cases, successful disputes will be removed from all Tested vendors' test results.

2) When the result was misinterpreted by us. In such cases, successful disputes will be corrected by us.

3) When the test case was not executed properly, due to tester or environmental error. In such cases, successful disputes will be removed from the specific AV's test results.

4) When the Deceptor sample was not blocked because it did not violate any of the AV's UwS or PUA policies. In such cases, the Tested vendor must attest in good faith that they have reviewed the sample, and they do not generally detect any of the Deceptor-level ACRs that

©AppEsteem Corporation, 2023-2024. All rights reserved.

the Deceptor sample violates. In such cases, successful disputes will be removed from the specific AV's test results.

5) When the Certified sample was blocked because it violated the AV's additional UwS or PUA policies. In such cases, the Tested vendor must attest in good faith that they have reviewed the Certified sample, and it violates a specific, documented policy that the vendor generally enforces against. In such cases, successful disputes will be removed from the specific AV's test results, and we will attempt to "remember" this policy exception to save the Tested vendor time in future disputes. In the future, we'll consume these policies when AMTSO's USC working group starts to produce them.

6) When the AV has informed us in good faith that they needed extra time in reviewing the Deceptor or Certified sample.

©AppEsteem Corporation, 2023-2024. All rights reserved.

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for 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. All products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)

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

4. Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards. (Section 4)

5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)

6. I will disclose how the Test was funded. (Section 4)

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: 

Name: Dennis Batchelder

Test Lab: AppEsteem Corporation

AMTSO Test ID: [AMTSO-LS1-TP108]

©AppEsteem Corporation, 2023-2024. All rights reserved.