An Analysis of AppEsteem's Certification Process

July 2024

Executive Summary

Recently, in response to several concerns shared with the Clean Software Alliance (CSA), a review into AppEsteem Corporation's (AppEsteem) certification process was conducted.

The findings indicate that overtime AppEsteem has diverted its "app services" in a way that appears to show more leniency towards its paying applications compared to others. This shift seems to be partially based on the addition of the AppEsteem 'deceptor' list.

Additionally, new ACR requirements set forth by AppEsteem appear to be arbitrary and lack alignment with existing *potentially unwanted application* (PUA) guidelines. This discrepancy has the potential, and in certain instances, does result in adverse business and financial consequences for software application developers who opt not to engage with AppEsteem's services. Conversely, vendors who pay a premium appear to be shielded from such repercussions, and even certain behaviors may be overlooked if additional payment is made.

Moreover, AppEsteem's positioning in the Anti-Malware Testing Standards Organization (AMTSO) seems to enable it to serve as both a regulator and a judge.

Background

Established in 2016, AppEsteem's premise was providing certification services for software vendors, to ensure the compliance and security of software applications, as part of its mission to "clean up the software monetization industry"[1]. The company had positioned itself as a regulator in the software certification process, offering paid certification and monitoring services to software applications and "access to certified app disclosures and telemetry" (also known as the 'certified' list[2] which lists AppEsteem 'certified' software) to anti-malware companies[3].

In early 2017, AppEsteem created and deployed a 'deceptor'[4] program: "*It took us almost a year to figure it out and get it working, but now that we've seen what our Deceptor program can do, we've decided to embed it deep into our app certification operations.*"[5].

The 'deceptor' program identifies software applications that are not aligned with certain AppEsteem requirements by publicly listing them via the AppEsteem website and recommending anti-malware

[1] https://blog.appesteem.com/post/2016/11/18/our-first-certified-app-takes-a-bow
[2] https://customer.appesteem.com/certified
[3] https://blog.appesteem.com/file.axd?file=/AppEsteem%20Vision%20and%20Plan%20August%202016.pdf
[4] https://customer.appesteem.com/home/checklist?minbar=y
[5] https://blog.appesteem.com/post/2017/05/17/helping-our-security-partners

companies to detect them ('deceptor'[6] list). The 'Deceptor' list is actively compiled through AppEsteem's proactive "hunting" process: *"We hunt for Deceptor candidates based on consumer sentiment, indications of deceptive activity in their web presence, and advertising spend. Deceptor candidates are also provided by security companies and submitted by our customers and the public."* [7]

The 'deceptor' program offers anti-malware companies an additional API stream of software application files to detect. The creation of the 'deceptor' program created two levels to AppEsteem's requirements, which came with two levels of "protection" for software developers[8]:

1. **The AppEsteem 'certification' requirements[9] (ACRs)** – "If app passes our full requirements, it's a TRUSTED APP and we don't want AVs to detect trusted apps";
2. **The AppEsteem 'deceptor' requirements[10] (29 "minbar" requirements of the total ACRs)** – "If app violates Deceptor requirements, it's a DECEPTIVE APP and we want AVs to detect all Deceptive apps."

The inception of the 'deceptor' program prompted a heated debate among industry members; some of which raised concerns regarding its validity and applicability. Such concerns were partially covered by the first CSA report[11] published in May 2018, which concluded that the 'deceptor' program lacks integrity in its design and implementation and is overly aggressive.

It was brought to the CSA's attention by several industry and anti-malware members as well as non-member vendors that the concerns covered by the first CSA report, seem to have since materialized, and a current 'deceptor' listing leads to multiple anti-malware detections for a software application. These detections may incur reputational and financial repercussions for said application developer.

The collection of the aforementioned concerns, together with previous findings, has led CSA's review into AppEsteem's actions and practices in recent months.
The findings and the conclusions of the review are detailed below.

[6] https://customer.appesteem.com/deceptors
[7] https://customer.appesteem.com/Home/DeceptorFix
[8] https://blog.appesteem.com/file.axd?file=/increasing%20av%20effectiveness%20caro%20may%202017.pdf
[9] https://customer.appesteem.com/home/checklist
[10] https://customer.appesteem.com/home/checklist?minbar=y
[11] https://www.cleansoftware.net/appesteem-program-review

Approach/Methodology

The CSA took the following measures to gather information in its current review:

- Reviewing AppEsteem-produced materials;
- Frequent reviews of software applications included in the 'deceptor' and 'certified' lists on AppEsteem's website;
- Reviewing online materials;
- Outreach to industry members and antimalware companies to gather input and feedback;
- Direct conversations with AppEsteem.

At all times, the CSA has made clear its desire to hear all feedback, and anonymity was assured for all conversations.

CSA Findings

1. Double Positioning as a Regulator and a Stakeholder

Anti-malware testing involves assessing how well security products detect and handle various threats, including false positives and false negatives. Testing companies perform these evaluations using sets of samples that may include both malicious and benign applications.

As of 2016, Dennis Batchelder, Co-Founder and President of AppEsteem[12], took the position of President and CEO of AMTSO[13].

AMTSO is an international non-profit association that "focuses on addressing the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies"[14]. AMTSO provides a framework for its members (both anti-malware vendors and anti-malware testers) to adopt fair and transparent testing practices. Test results published on the testing companies and/or vendors' websites are also displayed on the AMTSO website. These test results play a significant role in consumer and enterprise business decisions, such as selecting or validating anti-malware vendors' solutions.

In 2017, AppEsteem started testing anti-malware products for alignment with the AppEsteem program through AMTSO. Initially AppEsteem tested anti-malware companies to verify their consumption rates

[12] https://appesteem.com/team.html
[13] https://www.amtso.org/
[14] https://www.amtso.org/about-amtso/

of its 'detector' list[15].

In 2019 AppEsteem also began testing anti-malware companies' consumption rates of its 'certified' list[16] and in Batchelder's own words: "*The AVs were very happy with our Deceptor feed, but our big breakthrough on stopping their flags on certified apps came when we started testing them. We had to find how to leverage the existing momentum of our partners*[17]."

AppEsteem states that it encourages an independent and objective review of its recommendations by the anti-malware companies. In reality, test results and scores seem to be dependent on the degree by which the anti-malware companies implement AppEsteem's 'certified' and 'deceptor' lists (see "Conflict of Interest Disclosure" under section 4 included in footnotes 15 and 16).

2. Lack of Software Industry Input

In 2018 Mr. Batchelder resigned from CSA's advisory board. Following which, he "*incorporated CleanApps.org (CleanApps)*[18] *and recruited its first board from some of our (AppEsteem's) customers*"[19], a "Business Association for App Makers and Marketers" aiming to foster transparency and industry engagement.

Mr. Batchelder further explained: "we realized that AppEsteem had to find a way to get the vendor's voice and to reassure them that we're doing things fairly".

While the fact that Mr. Batchelder incorporated CleanApps.org is missing from the organization's Formation History page[20], there are numerous clear connections between CleanApps and AppEsteem:

Mr. Batchelder holds a seat on the CleanApps advisory board[21];

AppEsteem's program is referenced in all of CleanApps' press publications[22].

AppEsteem is the only certification company named and explicitly endorsed by CleanApps on its website: *"Whichever route you choose, the paid or unpaid route, it's foolhardy to go to market with an app that doesn't meet the full AppEsteem criteria. Public concern over privacy and security on the internet is growing, and the security companies aren't immune. They're likely to get even stricter over time. It's not only better for consumers if you make sure your software meets the highest security and privacy standards – it's just smart business."*[23]

---

[15] https://amtso.org/wp-content/uploads/2017/09/AMTSO-Test-Plan-AppEsteem-Deceptor-V4-1.pdf ;
[16] https://www.amtso.org/wp-content/uploads/2019/12/AMTSO-Test-Plan-AppEsteem-UwS-2020-V1-1.pdf
[17] https://web.archive.org/web/20221204184236/https://blog.appesteem.com/post/2021/04/16/our-fifth-year-the-longest-one-ever
[18] https://www.cleanapps.org/
[19] https://www.securityweek.com/behind-scenes-deceptive-app-wars/
[20] https://www.cleanapps.org/formation-history/
[21] https://www.cleanapps.org/advisory-board/
[22] https://www.cleanapps.org/press/
[23] https://www.cleanapps.org/cleanapps-org-news/how-anti-virus-companies-can-impact-your-app-business/

Moreover AppEsteem's 'Premium Services' plan includes membership with CleanApps: *"CleanApps.org Membership: During the time your company has subscribed to at least one Premium Services app, if you have chosen to become a basic member of CleanApps.org, AppEsteem will pay at the annualized rate of $1,000/year for that membership.[24]"*

This may suggest that AppEsteem provides funding for CleanApps, and even though this funding also appears on the CleanApps.org membership page[25], it is missing from the "sponsors" page[26] on the CleanApps website.

Lastly, CleanApps members with an option to participate in Exclusive Chairman's Circle meetings, meaning to possibly make an influence[27], must be AppEsteem certified: *"...any body that's on our Charter member list or Corporate membership list, and to be a Charter member or Corporate member which is higher donation levels, they have to be certified by Appesteem"*[28].

3. Out of Consensus Requirements

The AppEsteem Certification requirements (ACRs) were initially mostly based on the CSA guidelines[29] which cover the "common ground" violations agreed upon by most anti-malware companies. A good example is ACR-048 'deceptor' requirement[30] which is identical to the CSA's guideline "Products must not hide and/or limit the user's ability to close, delete, disable or uninstall the program"[31]. Over time, AppEsteem's new certification requirements moved from covering the mutual consensus, to include more requirements which are not in consensus. This is evident by the fact that not all anti-malware companies enforce all requirements.

Several ACRs are very specific and are typically part of the software developer's domain; such as ACR-004 'deceptor' requirement[32] which sets specific requirements for a trial period such as a 24 hour time frame for a fully functional free trial.

Several new ACRs prohibit commonly accepted industry practices utilized by many software vendors, including ones from the anti-malware community, streaming services such as YouTube and smart TVs. A

[24] https://archive.org/details/appesteem-certification-fee-schedule
[25] https://www.cleanapps.org/membership-level/
[26] https://www.cleanapps.org/supporters/
[27] https://www.cleanapps.org/membership-level/ "Charter Membership Benefits"
[28] https://www.youtube.com/watch?v=g95xIExQsBM&t=1040s
[29] https://www.cleansoftware.net/guidelines
[30] https://customer.appesteem.com/home/checklist?minbar=y "ACR-048 Does not hide and/or limit the consumer's ability to close, delete, disable, or uninstall the app".
[31] https://www.cleansoftware.net/guidelines
[32] "ACR-004...app provides free fixes, either during an immediate, fully functional free trial of at least 24 hours for all free scan results shown, or when the fix is not anticipated to be permanent. Free trial does not pre-collect payment details or use negative options to charge consumer unless free trial is an immediate, fully-functional trial lasting at least seven days."

good example is ACR-013 'deceptor' requirement[33] which requires an additional offer screen to be presented to the end user in addition to already existent and agreed upon user disclosures.

Moreover, it is the CSA's opinion that several new ACRs lack actual applicability, such as ACR-060 'deceptor' requirement[34] which requires software developers to disclose to the end user the name of the network used, while in practice most software developers utilize their own installer and monetization without using any network.

Most importantly, while AppEsteem claims that its ACRs are meant to cover Potentially Unwanted Software (PUA) which is a lower risk and subjective detection criteria "They are our attempt at objectivity to assess when an app is "unwanted"[35], AppEsteem's AMTSO test plans prompts anti-malware companies to treat 'deceptors' as a malware category (see Section 1 "Introduction" in footnote 15):*"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."*

4. Inconsistent Application of Criteria

The CSA's review findings of AppEsteem's 'certified' application list are attached as **Exhibit A**[36].

During the CSA's review, Appesteem reviewed and added more than 150 software applications to its 'deceptor' list, suggesting that AppEsteem focuses its efforts on "hunting" for its 'deceptor' list rather than "policing" its own certified application's behavior. Reviewing the 'certified' application list reveals that numerous certified applications are in clear violation of the AppEsteem's certification and 'deceptor' requirements. These findings suggest that AppEsteem's standards differ when applied to software applications offered by AppEsteem paying customers versus other software applications.

A YouTube video of an interview with AppEsteem's Co-Founder and President Mr. Batchelder reveals that while certified applications may lose certification and be placed on the 'deceptor' list, they can always regain certification status by paying an increased certification fee and applying changes to their

[33] "ACR-013 Don't interrupt the consumer with unrelated interstitials when the consumer is already performing another task for you. Either wait until they know the task is complete; remove the interruption by eliminating the need for the user to wait or answer your offer/ad; or obtain explicit, informed user consent to interrupt with offers/ads immediately prior to the interruption. Consent must be standalone, disclose offer provider, state risks and mitigations, and have a statement that the consent isn't required to complete the workflow."

[34] "ACR-060 If your app bundles offers from an offer provider, make sure you disclose the public name of this provider, with a link to their site for more details, in each offer."

[35] https://customer.appesteem.com/home/checklist?minbar=y

[36] It should be noted that to avoid unnecessarily harming certified software vendors, identifying elements and additional ACR violations are excluded from the public Exhibit A.

software. This may be seen by some as a penalty for the violation of certification requirements[37]: *"if you get more violations, we raise the rate of our certification*".

Discussion and Conclusions

The anti-malware industry is trusted by many consumers and enterprises globally. This trust is largely based on its integrity of being fair and transparent. It is the CSA's opinion that the certification and testing processes should be and remain independent, fair and transparent for the continued trust in this industry.

The CSA finds AppEsteem's conflict of interest troubling and one that may potentially harm the integrity of the anti-malware industry. AppEsteem's decision to utilize AMTSO's services is flawed, especially considering the fact that AppEsteem is a tester that also drafts and controls the standards (ACRs) by which it performs its tests to the different anti-malware vendors.

The CSA further finds the existence and increase in non-consensus-based certification/'deceptor' requirements concerning. Not certifying or labeling as a 'deceptor' may lead to serious business implications for software applications. These concerns are amplified due to the lack of categorization of violations according to severity. Software applications with objectively minor compliance PUA issues, suffer consequences in a manner similar to applications performing malware-like behavior.

It is also the CSA's view that the practice of testing anti-malware companies' consumption of the AppEsteem 'deceptor' list, has significantly amplified the impact of the 'deceptor' list and the overall AppEsteem program. The "encouragement" of anti-malware companies to 'detect' applications as 'deceptors' leads to an increased "flagging" of legitimate software vendors who are not paying nor aligned with Appesteam.

Moreover, the fact that many of the 'certified' applications are actually in violation of AppEsteem's 'deceptor' guidelines, may hint to the fact that being a premium paying member "shields" from being flagged as a 'deceptor'.

Lastly, the funding relationship between AppEsteem and CleanApps, combined with AppEsteem's dissociation from other vendor/industry organizations, raises questions about the industry's involvement and oversight in AppEsteem's certification process.

Contrary to the impression held by various anti-malware companies and shared with the CSA often, AppEsteem does not collaborate with industry inputs. For example, while AppEsteem appeared to publicly accept[38] some of the CSA's feedback regarding the implementation of ACR-013, in practice

[37] Interview with the CEO of AppEsteem (featuring Jim Browning) see min 50:10.
https://twitter.com/NeePscambaiting/status/1311257319192354816; https://twitter.com/NeePscambaiting/status/1306659790773518339

[38] https://blog.appesteem.com/post/2023/02/09/acr-013-is-coming-soon-are-you-ready

AppEsteem hasn't changed its policy.

This setting and these practices often lead to a reality where software developers who are not paying members of AppEsteem's services suffer a negative impact on their business, which, in extreme cases, may even result in termination of their operations, and in the words of CleanApps.org:

"...something "unwanted" can get your app labeled as a "deceptor" and make you unqualified to exist in the business community."[39]

[39] https://www.cleanapps.org/cleanapps-org-news/app-reputation-the-only-path-to-prosperity/

The Next Steps: CSA's Proposal

The CSA recommends the following actions to address the issues identified and restore integrity to the software certification process:

1. Mitigate the conflict of interest and enhanced influence arising from Dennis Batchelder's roles in both AppEsteem and AMTSO;
2. Review and revise the certification and 'deceptor' requirements to ensure objectivity, clarity and fairness while shifting the focus back to the certification process;
3. Establish a mechanism for distinguishing between the severity of violations to appropriately address compliance issues;
4. Establish regular channels of communication between AppEsteem and industry stakeholders for feedback and concerns to ensure transparency and real collaboration;
5. Embrace actual third-party oversight and dispute resolution mechanisms, restoring anti-malware companies' autonomy.

These recommendations aim to address the fundamental concerns raised in this report and ensure that the software certification process remains fair, transparent, and accountable to all stakeholders involved. The CSA remains committed to fostering a healthy and trustworthy software ecosystem and calls for collaborative efforts to achieve these goals.

About the Clean Software Alliance

The Clean Software Alliance (CSA) is a champion of sustainable, consumer-friendly practices within the software distribution ecosystem. This report is produced by the CSA, and the views expressed herein were prepared exclusively by the CSA and not by any individual, officer, director, or member of the CSA.

The CSA works to advance the interests of the software development community through the establishment and enforcement of guidelines, policies, and technology tools that balance the software industry's needs while preserving user choice and user control.
A 501(c)(6) nonprofit trade association, the CSA works inclusively across its constituents of online security vendors, software distribution & monetization firms, installer platform companies, browser providers, computer platform developers, and others to find consumer-friendly solutions to the challenges of economically sustainable software distribution.