ThreatList License Agreement

The cybersecurity industry's
testing standard community

ThreatList License Agreement

I. General Information

The Anti-Malware Testing Standards Organization, Inc., a California nonprofit mutual benefit corporation ("AMTSO"), is dedicated to improving the quality, relevance and objectivity of anti-malware testing methodologies. In furtherance of this mission, AMTSO has facilitated the ThreatList system ("ThreatList") to provide the cybersecurity community with a broad and objective repository of malware samples and related metadata. AMTSO welcomes qualifying entities and individuals to contribute, access and use the information provided in the ThreatList; however, before you do, you must read and agree to the terms of this License Agreement and the exhibits hereto (collectively, this "Agreement").

All information, malware samples, metadata, and ThreatList query results (collectively, "ThreatList Data") which comprise the ThreatList is collaboratively provided by ThreatList Reporters (collectively, "Reporters"). All parties that contribute, access, and use ThreatList Data (collectively, "ThreatList Users"), have agreed to be bound by this Agreement, and by accessing or contributing any ThreatList Data, you similarly agree to be bound by this Agreement.

In general, AMTSO does not take a review, technical or editorial role in the ThreatList. This means that AMTSO does not monitor or review the ThreatList Data, and does not take any responsibility for the ThreatList Data, including whether any ThreatList Data actually constitutes malware. For the purposes for this Agreement, the term "malware" includes, without limitation, software or other electronic data designed to, or otherwise capable of, infiltrating and/or damaging a computer system. Please read the section of this Agreement titled "No Warranties; Exclusions and Limitations of Liability" carefully before accessing the ThreatList, using, or contributing any ThreatList Data.

II. Privacy Policy

AMTSO operates under the terms of a Privacy Policy, which sets forth how we collect and use your information. Please review this Privacy Policy carefully before registering with AMTSO to access the ThreatList, use, or contribute any ThreatList Data.

III. Restrictions on Access and Use of ThreatList Data

A. General Restrictions. The following restrictions apply with respect to all access and use of ThreatList Data.

1. Registration. All ThreatList Users must meet the qualifications for status as a ThreatList "Reporter" or "Beneficiary" (as defined in Exhibit A to this document and which may be modified and amended from time to time by decision of the ThreatList Oversight Board), and each individual or entity Reporter or Beneficiary must be approved by vote of the ThreatList Oversight Board, prior to being registered as a ThreatList User.

2. Each ThreatList User agrees to protect the confidentiality of all ThreatList access tools, including certificates, passwords, or other login credentials provided by AMTSO in association with the ThreatList. Each ThreatList User agrees not to provide any such access tool to any third party without explicit prior written consent from AMTSO and/or the ThreatList Oversight Board.

3. Each ThreatList User agrees to contribute, access, or use the ThreatList Data, in whole or in part, only in compliance with this Agreement, which includes the ThreatList Usage Guide and Terms and Conditions attached as Exhibit A, hereto.

4. Each ThreatList User agrees to protect the confidentiality of all data received from the ThreatList at all times. Each ThreatList User is prohibited from sharing any such data with any third party, unless such third party is:

    a. An employee of the ThreatList User who requires access to such data to perform services at the request of the ThreatList User which are permitted by the terms of this Agreement;

    b. A contractor of the ThreatList User who requires access to such data to perform services at the request of the ThreatList User which are permitted by the terms of this Agreement;

    c. A registered ThreatList User, and the access is provided pursuant to the terms of this Agreement, or

    In the interests of clarity, except as specifically set forth above, ThreatList Users shall not provide any access to any ThreatList Data to any third party including, but not limited to, any third-party multiscanning anti-malware service.

5. AMTSO respects the intellectual property rights of others, and will protect its own intellectual property rights.

    a. If any ThreatList User publicly uses, in whole or in part, any ThreatList Data, then such ThreatList User may cite AMTSO as the source for such data; which may be cited as follows:

        This data was acquired through the ThreatList system provided by the Anti-Malware Testing Standards Organization, Inc. (AMTSO), at www.amtso.org.

    b. Except as set forth in this Section, neither this Agreement nor your access or use of the ThreatList or any ThreatList Data grants any rights to use the name “AMTSO”, “ThreatList” or any third party trademarks.

B. Additional Restrictions and Obligations. Each party hereto agrees to follow the additional restrictions and obligations set forth in the ThreatList Usage Guide, set forth on Exhibit A hereto, as may be modified and amended from time to time.

1. Each ThreatList User is responsible to ensure that it and each of its employees, contractors and affiliates abide by this Agreement.

2. AMTSO does not have any obligation to monitor or review the ThreatList or ThreatList Data, including any Query Results, and does not take any responsibility for the ThreatList or ThreatList Data, including whether any ThreatList Data actually constitutes malware or whether any Query Results are accurately returned. However, AMTSO reserves the right to monitor the ThreatList and any related access points of the ThreatList, including the usage or queries and take necessary actions to terminate or prevent any violation of this Agreement.

3. Please respect all AMTSO trademarks, and the trademarks of third parties. Use of AMTSO's trade names, trademarks, service marks, logos or domain names must be in compliance with this Agreement and AMTSO's Intellectual Property Policy.

IV. Grant of Rights

A. AMTSO hereby grants (i) to each ThreatList User a revocable, personal, non-transferable, limited license to access and use the web portal and API provided by the ThreatList, for the purpose of submitting and downloading ThreatList Data, and (ii) to each Non-Member a revocable, personal, non-transferable, limited license to access and use the web portal and API provided by the ThreatList, for the sole purpose of submitting ThreatList Data.

B. Each ThreatList User who submits ThreatList Data hereby grants to each other ThreatList User a non-exclusive, irrevocable, royalty-free limited license to use the ThreatList Data submitted by the granting ThreatList User solely under the terms of this Agreement. However, for purposes of clarification, AMTSO shall have the right to terminate any ThreatList User's access to any ThreatList Data as a result of any violation of the terms of this Agreement, as determined by AMTSO in its sole discretion.

C. Each ThreatList User hereby grants to AMTSO a non-exclusive, irrevocable, royalty-free license to use, reproduce, distribute, modify, create derivative works and sublicense the ThreatList Data submitted by the granting ThreatList User, in all media currently and hereinafter known.

D. Ownership of all proprietary rights in the ThreatList Data shall remain vested in the ThreatList User contributing such ThreatList Data and its respective licensors. Each ThreatList User that contributes any ThreatList Data hereby represents that either:

1. ThreatList User is the exclusive owner of the contributed ThreatList Data; or
2. To the extent the contributed ThreatList Data contains any third party content, the ThreatList User has acquired sufficient rights to redistribute such third party content to the ThreatList and ThreatList Users pursuant to this Agreement.

V. Dispute Resolution and Complaints

A. Contributions to, and use of, all ThreatList Data is subject to this Agreement, which includes the ThreatList Usage Guide and Terms and Conditions attached as Exhibit A, hereto, and all ThreatList Users are expected to abide by these terms. There may be occasions, however, when a ThreatList User or other party may believe that these terms have been breached. In such case, the party alleging the breach is requested to send a full description of the alleged infraction or other complaint (a "ThreatList Complaint") to threatlist-admin@amtso.org.

B. Following receipt of a ThreatList Complaint, the ThreatList Oversight Board will conduct an investigation in accordance with the Complaint Procedures set forth in Exhibit A to this Agreement.

VI. No Warranties; Exclusions and Limitations of Liability

A. ACCESSING AND USING THE THREATLIST AND THREATLIST DATA IS SOLELY AT YOUR RISK. AMTSO PROVIDES THE THREATLIST AND THREATLIST DATA SOLELY ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND AMTSO EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES OF ANY KIND INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONTINUOUS OPERATION, COMPLETENESS, QUALITY, ACCURACY, AND NON-INFRINGEMENT. AMTSO MAKES NO REPRESENTATION OR WARRANTY THAT THE THREATLIST AND THREATLIST DATA WILL MEET YOUR REQUIREMENTS, BE SAFE, SECURE, UNINTERRUPTED, TIMELY, ACCURATE, OR ERROR-FREE, OR THAT YOUR INFORMATION WILL BE SECURE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM AMTSO, ANY THREATLIST USER, OR THROUGH THE THREATLIST CREATES ANY REPRESENTATION OR WARRANTY OF ANY KIND.

B. AMTSO shall have no obligation to update the ThreatList or ThreatList Data, and does not make any determination as to whether any sample actually constitutes malware or whether any Query Results are accurately returned. AMTSO has no obligation to verify or authenticate any ThreatList Data, including any Query Results, malware samples or metadata.

C. AMTSO IS NOT RESPONSIBLE TO YOU OR TO ANY THIRD PARTY FOR ANY DAMAGES OR LOSSES OF ANY KIND (INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, LOST DATA OR BUSINESS INTERRUPTION) ARISING DIRECTLY OR INDIRECTLY OUT OF THE ACCESSING OR USE OF THE THREATLIST AND/OR THREATLIST DATA, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY AND PUNITIVE DAMAGES, OR ATTORNEYS' FEES, REGARDLESS OF WHETHER ANY PERSON OR ENTITY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

D. YOU HEREBY RELEASE AND WAIVE ALL CLAIMS, DAMAGES AND LOSSES OF ANY KIND, KNOWN AND UNKNOWN, YOU MAY HAVE AGAINST AMTSO AND ANY THREATLIST USER OR NON-MEMBER, AND AGAINST EACH OF AMTSO'S AND ANY THREATLIST USER'S OFFICERS, DIRECTORS, EMPLOYEES AND AGENTS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE THREATLIST AND/OR THREATLIST DATA.

E. ANY MATERIAL UPLOADED, DOWNLOADED OR OTHERWISE ACCESSED THROUGH YOUR USE OF THE THREATLIST IS AT YOUR OWN RISK, AND YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM, NETWORK, PRODUCTS OR SERVICES THAT RESULTS THEREFROM. YOU AGREE THAT AMTSO HAS NO RESPONSIBILITY OR LIABILITY FOR THE DELETION OF, OR THE FAILURE TO STORE OR TRANSMIT, ANY THREATLIST DATA, OR TO MAINTAIN THE THREATLIST. AMTSO RETAINS THE RIGHT TO LIMIT OR TERMINATE YOUR USE OF THE THREATLIST DATA AT AMTSO'S SOLE DISCRETION AT ANY TIME WITH OR WITHOUT NOTICE.

F. ThreatList Users shall exercise caution and not upload, download or use any ThreatList Data that may result in criminal or civil liability under any applicable laws or regulations including, without limitation, the laws of the United States of America and any applicable laws and regulations in the jurisdiction where the ThreatList User lives, works or provides or accesses ThreatList Data.

G. Some states or jurisdictions do not allow the types of disclaimers in this section, so they may not apply to you either in part or in full.

VII. Other Terms

A. Termination.

1. The licenses granted herein are valid for one (1) year from the date of electronic submission of your acceptance of this Agreement. Unless otherwise terminated by AMTSO or you, these licenses shall automatically renew after the initial term expires for successive terms of one (1) year each.

2. This Agreement may be terminated in the following manner:

    a. By either party at any time upon ninety (90) calendar days written notice;

    b. By AMTSO upon any breach that is not cured within ten (10) calendar days written notice from AMTSO; or

    c. By direction of the ThreatLlist Oversight Board pursuant to resolution of a ThreatList Complaint brought pursuant to this Agreement.

3. Upon termination of this Agreement, you shall immediately cease all access to the ThreatList, and cease all access and use of ThreatList Data, including any Query Results.

B. AMTSO reserves the right to cease operation of ThreatList, permanently or temporarily, at AMTSO's sole discretion, at any time upon ninety (90) calendar days written notice to all registered ThreatList Users. Upon such cessation of operations, ThreatList will no longer be accessible. In addition, AMTSO reserves the right to cease operations of ThreatList, permanently or temporarily, to address any technical or other operational issue with ThreatList at any time, although reasonable effort will be made to notify all registered ThreatList Users such action with as much advance notice as reasonably possible.

C. This Agreement, including the exhibits hereto, together with the AMTSO Privacy Policy, AMTSO Intellectual Property Policy, as each may be applicable, contains the entire agreement and understanding between AMTSO and you as a ThreatList User with respect to the ThreatList. AMTSO may modify this Agreement at any time, which modified agreement shall be binding on all ThreatList Users thirty (30) calendar days after the earlier to occur of (i) the posting of the modified agreement on the ThreatList and AMTSO websites, or (ii) AMTSO sending written notice of the modified agreement to the ThreatList Users.

D. Neither party to this Agreement may assign this Agreement without the prior written consent of the other party. Subject to the foregoing, this Agreement shall inure to the benefit of, and be binding upon, AMTSO and each ThreatList User's permitted successors and assigns.

E. If in any circumstance AMTSO does not apply or enforce any provision in this Agreement, it is not a waiver of that provision.

F. If any provision of this Agreement is found to be unlawful, void or unenforceable, that provision of part of the provision is deemed severable from this Agreement

and will be enforced to the maximum extent possible, and all other provisions of this Agreement will remain in full force and effect.

G. All matters and disputes relating to this Agreement shall be governed by the laws of the State of California without regard to any conflicts of law provisions thereof.

H. All notices required under this Agreement shall be given electronically and in writing, and shall be addressed or delivered to AMTSO at threatlist-admin@amtso.org, and to any ThreatList User at the address for electronic delivery provided upon registration with AMTSO to use the ThreatList.

* * * *

IN WITNESS WHEREOF, this Agreement has been executed and delivered as of the later of the dates set forth below.

Applicant Name: _____

Applicant Title: _____

Applicant Company or Institution: _____

Signature:_____ Date:_____

Exhibit A to ThreatList License Agreement

ThreatList Usage Guide and Terms and Conditions

Introduction

The ThreatList acts as a spiritual successor of the WildList system, which ceased operations in December 2022. The ThreatList system is intentionally different to WildList, with a different approach to reporting and challenging samples as well as a backend service hosted and maintained by AMTSO.

Objective

The goal of ThreatList is to provide a platform for reporters to exchange critical malware that they see in the wild / on customer devices, to strengthen the collective ability to identify and detect threats while also giving independent test organizations and potentially other selected partners the ability to access a curated list of known threats. This is accomplished by leveraging the existing infrastructure of AMTSO's RTTL system. Samples can be submitted, commented on, challenged, and downloaded by any approved participant in ThreatList (collectively, "ThreatList Users"). A statistics page allows for a direct and meaningful overview of all Reporters and consumers to identify potential issues.

Reporters

The Reporters are the most important participants in ThreatList as they form the backbone and provide the content for the system. Security vendors, security researchers, and companies with a business interest in the ThreatList can apply to become Reporters to gain access to the curated list as well as freshly submitted samples with evaluation status. Any entity in this group will be referred to as a ThreatList Reporter.

Each ThreatList Reporter entity must have 1 primary reporting contact and may have up to 1 secondary reporting contact; each contact represents their Reporter entity and is responsible for sample submissions from that Reporter. For transparency of communication, a Reporter entity may include a third contact, which should be a mailing list and can thus be modified independently by the Reporter company.

To become a Reporter, a potential new entrant must contact the ThreatList operational team via threatlist-admin@amtso.org. New applicants are not required to be AMTSO members but will be required to approve legal agreements and a code of conduct. Applicants must be able and willing to provide a steady stream of samples from their own internal sources. This will be verified by employing a secondary acceptance environment which allows potential new Reporters to submit samples into the backend without adding to or accessing the official ThreatList.

Requirements to be considered (this is a non-binding list and the Oversight Board may choose to waive certain requirements in certain circumstances):

- The applicant should to have shown their ability to provide at least 20 samples per day on a rolling average

- At least 20% of the samples provided should be “fresh” and should not have been submitted previously by an existing Reporter
- Fewer than 20% of the submitted samples should be subject to challenge by existing Reporters

If any of the above-mentioned requirements are not met, the ThreatList Oversight Board may reject an application to become a Reporter (or, in the case of an existing Reporter, may revoke the Reporter's access rights and credentials).

After a trial period lasting approximately 1 month, the samples uploaded by the applicant will be evaluated by the ThreatList Oversight Board based on input from the operational team. A final vote of the Oversight Board will be held to accept the applicant as a ThreatList Reporter. The application will be approved if the total of YES votes + the total of abstentions is greater than the total of NO votes AND if the total of YES votes is greater than total number of abstentions. A vote will count as an abstention if it is returned with any empty field, or if no vote is received by the specified deadline. In case of a potential (personal) conflict of interest, the vote will be cast in a secret ballot.

Revocation of a previously-approved application will follow a similar process.

Beneficiaries

Access for non-Reporters such as testers (“Beneficiaries”) is very limited and can only be approved by the Oversight Board collectively approving an application. Appropriate candidates for Beneficiary status include testers, magazines, and other organisations engaged in testing which could make valid use of the sample set. Beneficiaries will be supplied with samples identified relative to a specific week or year.

To be accepted as a Beneficiary, the potential entrant needs to demonstrate legitimacy, state where and how the samples are going to be used, and approve the required legal agreements, prior to a vote of the Oversight Board. Such votes shall be considered passed only when only YES votes and abstentions are recorded; any NO vote shall be treated as a veto.

Besides non-Reporter Beneficiaries, all Reporters will have the ability to consume the sample/data feeds via the API.

Oversight Board

The Oversight Board has various functions to manage the success of the ThreatList. They are tasked with identifying and discussing issues and changes, communicating with reporters, and approving new Reporters and Beneficiaries. The Oversight Board shall consist of between 5-7 members who agree to serve a single-year, renewable term aligned with the AMTSO Fiscal Year (July to June).

Individuals interested in participating in the Oversight Board can notify AMTSO through threatlist-admin@amtso.org. To be eligible, a candidate needs to have been a Reporter for at least 3 years.

Should more than 7 eligible candidates express interest in serving on the Oversight Board for a given AMTSO Fiscal Year, a vote for the yearly term will be conducted through the auspices of the AMTSO Chief Operating Officer and the ThreatList operational team.

The Oversight Board has the following responsibilities:

- Creating and updating the rules and guidelines for the system

- Voting on admitting new Reporters
- Granting or removing the access to the samples to Beneficiaries
- Controlling the official messaging from and online presence of the ThreatList
- Resolving escalated disputes and repeated challenges

ThreatList Sets

A ThreatList set differs from the former WildList set in one key aspect. Since the backend is designed to provide a steady stream of samples instead of a fixed monthly set, there will be no monthly ThreatList set. Instead, Beneficiaries may choose to either access all samples, including those still open to challenge, or to download one of the weekly or daily curated sets which will be built automatically by the backend. This weekly/daily set will be identified by the current year and calendar week/day tags. Beneficiaries may to choose their preferred method depending on their use case.

To support this flexibility of usage approaches, implemented tags will identify samples/sets as 'candidate', 'release', 'obsolete', or 'removed'. Details regarding these tags in operation will be provided by the operational team overseeing the Threat List implementation.

Submissions are made by all Reporters, with each Reporter required to meet a certain minimum threshold of samples submitted per day on a rolling average. The scope of submitted samples is as follows:

- First Stage Malware (Infectors) – specification of type which should be submitted
- Second Stage Malware (Payloads)
- Malware Hosts (URLs) – clear definition required

Both "regular" and file-infector malware are eligible. Out of scope are malware artifacts, non-malware samples such as PUAs, Hacktools or similar software without specifically malicious intent, as well as damaged files.

As the service should stand out from other exchange systems or malware feeds, the target is to have Reporters submit only their most prevalent samples, important zero days, or unique samples seen by them in the wild. This translates to a big focus on quality instead of quantity, while producing decently sized sets.

As the sample submission is done in real time, so are the sample challenges. Every sample will stay in an evaluation state for 7 calendar days, during which time Reporters may submit challenges to the sample. After this period, if the sample has not been challenged, it will move into the core stage in which it be assigned to the current ThreatList set and can no longer be challenged.

Note that in isolated cases, the Oversight Board might call for a sample to be reviewed in an additional challenge period based on issues identified after the 7-calendar day window by the ThreatList Reporters.

A submitted sample should not contain any personal or inappropriate data. If a Reporter identifies such sample within the sample set, it should be reported and will be removed from the set.

Infrastructure

The existing AMTSO RTTL (Real Time Threat List) service will be used to host the ThreatList. There will be a strict separation between samples submitted as RTTL files and

those submitted by a ThreatList Reporter. RTTL contains all the required features for ThreatList:

- Backend service to submit or receive samples (incl. the usage of APIs and tools)
- Interface for permission handling
- Statistical interfaces
- Ability to challenge sample submissions and share feedback to a Reporter
- Acceptance interface for new Reporters by community approval

Priority access for Beneficiaries, which would allow exclusive sample access during an initial period of (for example) 24 hours, is possible and may be implemented at any time with the approval of the operational team and Oversight Board.