The Real Time Threat List (RTTL)

AMTSO's Threat Intel Sharing Platform

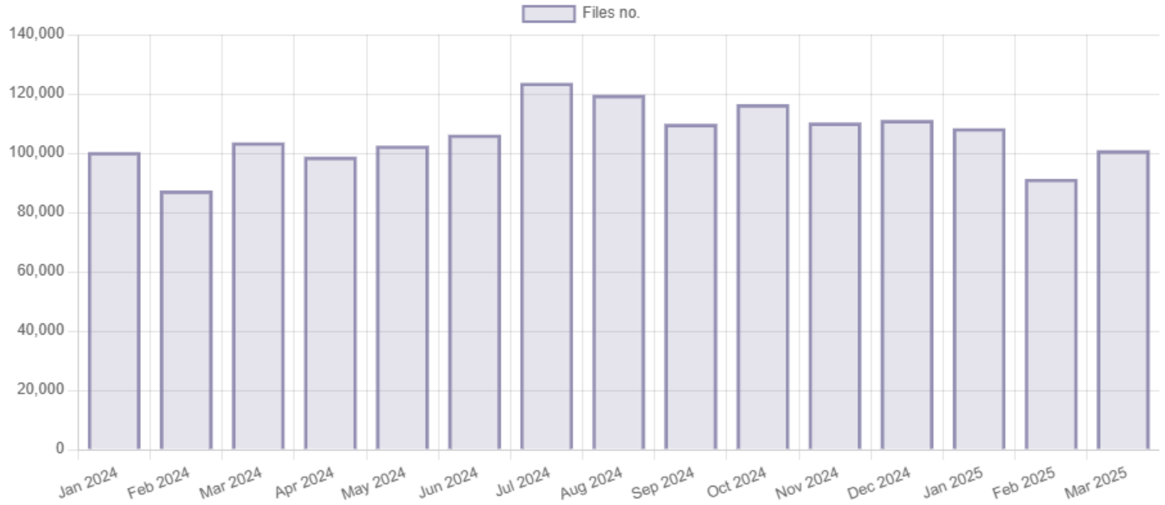
The Real-Time Threat List (RTTL) is a comprehensive initiative by AMTSO aimed at providing a broad and objective repository of malware samples and related metadata. RTTL facilitates the sharing of intelligence between AMTSO members, test labs, certification bodies, and other cybersecurity entities.

All AMTSO members can join RTTL to contribute and benefit from the malware feed. Members must upload a minimum of 200 samples per day to gain full access and benefit from the CERT and independent researcher sample feed. The RTTL platform is a vital resource for the cybersecurity community, providing a centralized platform for the submission and sharing of malware samples and threat intelligence.

With its robust features, extensive contributor network, and comprehensive sandbox integration, RTTL plays a crucial role in enhancing the quality and objectivity of anti-malware testing methodologies.

Non-members who regularly find or track malware, such as CERTs, can use the system as a single point of contact to share samples and other information to the wider security industry. Non-member security firms can also sign up to contribute samples and data, and may be granted limited download access depending on the policies of other contributors.

AMTSO members not yet signed up to the system can do so via the AMTSO member website.

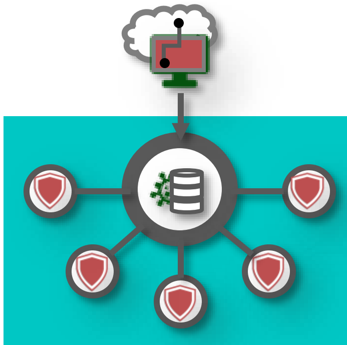


Monthly submissions in RTTL

On average, RTTL receives over 18.5k new sample submissions per week, amounting to approximately 75,000 sample submissions per month.

CERT organizations contribute between 225 and 800 new sample submissions per week, making them a vital part of the RTTL ecosystem.

Objectives RTTL



1.

Enhance the **quality**, **relevance**, and **objectivity** of anti-malware **testing methodologies**

2.

Support **test labs** and certification bodies in their efforts to evaluate and **certify security products**

3.

Provide a **centralized platform** for the submission and **sharing** of malware samples and **threat intelligence**

4.

Serve as a single point of contact to share samples and other information to the **wider security industry**

Key Features

Sample submissions
The Real-Time Threat List (RTTL) encourages members to provide at least 200 new malicious samples per day to gain access to the sample feed. This ensures a steady influx of fresh and relevant data for analysis.

CERT organizations and independent researchers can contribute and share samples without the need for membership, allowing them to reach out to all main security vendors in the industry to ensure comprehensive coverage.

Impressively, 90% of samples coming from RTTL can be considered malicious, highlighting the platform's effectiveness in identifying and combating cyber threats.
For nearly 30% of new samples submitted to RTTL, they are seen in RTTL before any other source, including other public and private feeds, exchange partnerships, and customer bases. This underscores RTTL's role as a leading source of threat intelligence. Overall, the sample quality in RTTL is very healthy. While some vendors may send in more non-malicious samples than others, RTTL frequently gets in touch with submitters of low-quality samples to resolve such issues and maintain the integrity of the platform.

Bug Fixes and Improvements

The Real-Time Threat List (RTTL) is continuously evolving and being enhanced to meet the needs of its users. New features are regularly implemented, such as quality review services, machine learning capabilities, and bug fixes. Continuous improvements are made based on requests from AMTSO members and other contributors.

It is crucial for AMTSO to maintain a reliable and high-quality service, ensuring both the quality and quantity of submissions remain at the highest standard. This commitment to excellence helps RTTL provide the best possible service to its users and the cybersecurity community.

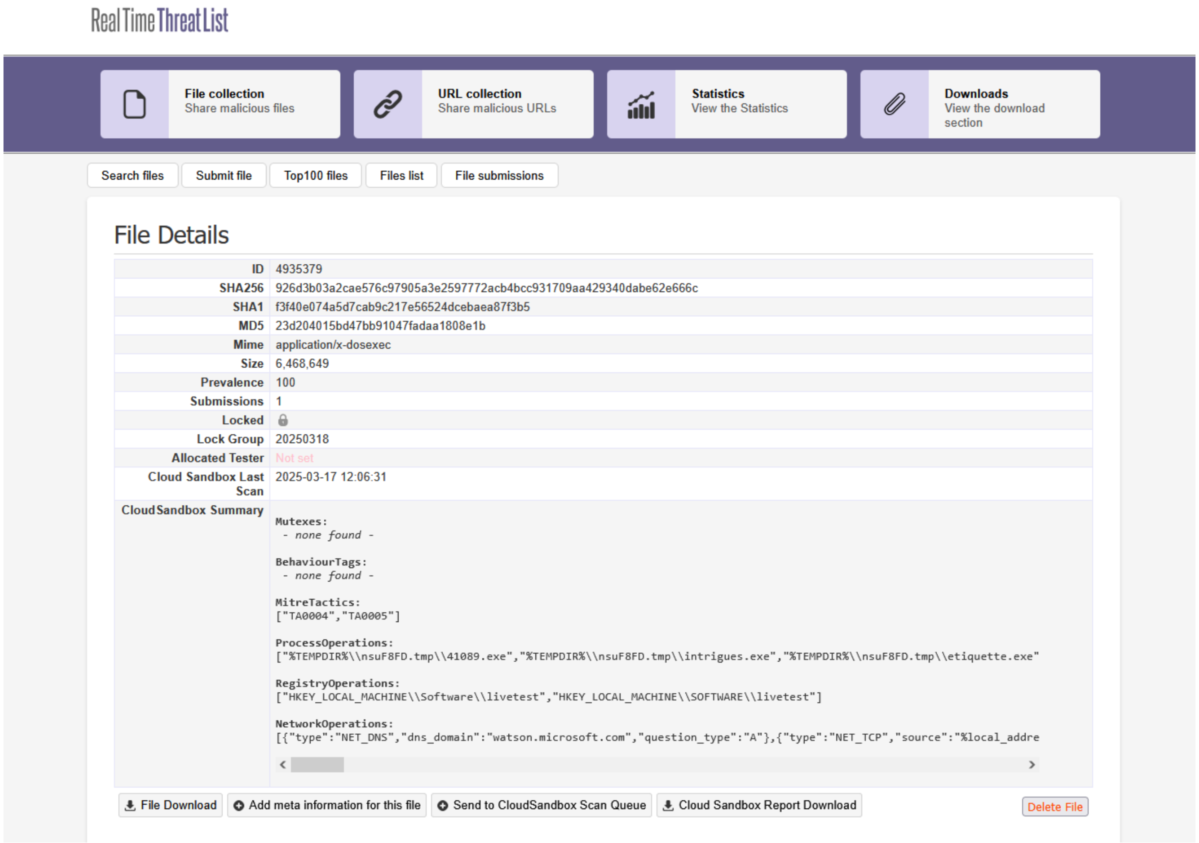
Sandbox Integration

The integration of a GDPR-compliant sandbox is a key feature of RTTL. This sandbox provides kernel- and user-mode metadata for uploaded samples, allowing for detailed analysis of malware behavior, execution trees, network operations, and more. The sandbox can process up to 5,000 samples per month, with the option to request additional analyses for a fee. RTTL members can request sandbox analysis via API or web interface, with a processing time of 2-10 minutes per sample depending on the load. The sandbox provides a full JSON report that includes all operations, network traffic, MITRE tactics, parent-child relationships, file characteristics, and more.

API and Interface

RTTL offers a comprehensive set of APIs designed to facilitate the submission, search, and download of malicious files and URLs. These APIs provide users with the ability to automate the upload processes, ensuring efficient and streamlined integration with their existing systems.

The RTTL API version 4.0 includes functions for file and URL submissions, allowing users to share malicious files and URLs seamlessly. Additionally, the API supports various operations such as searching for specific samples, downloading documents, and viewing statistics.



File Details

ID	4935379
SHA256	926d3b03a2cae576c97905a3e2597772acb4bcc931709aa429340dabe62e666c
SHA1	f3f40e074a5d7cab9c217e56524dcebaea87f3b5
MD5	23d204015bd47bb91047fadaa1808e1b
Mime	application/x-dosexec
Size	6,468,649
Prevalence	100
Submissions	1
Locked	🔒
Lock Group	20250318
Allocated Tester	Not set
Cloud Sandbox Last Scan	2025-03-17 12:06:31
CloudSandbox Summary	

```
Mutexes:
 - none found -

BehaviourTags:
 - none found -

MitreTactics:
["TA0004","TA0005"]

ProcessOperations:
["%TEMPDIR%\\nsuF8FD.tmp\\41089.exe","%TEMPDIR%\\nsuF8FD.tmp\\intrigues.exe","%TEMPDIR%\\nsuF8FD.tmp\\etiquette.exe"

RegistryOperations:
["HKEY_LOCAL_MACHINE\\Software\\livetest","HKEY_LOCAL_MACHINE\\SOFTWARE\\livetest"]

NetworkOperations:
[{"type":"NET_DNS","dns_domain":"watson.microsoft.com","question_type":"A"},{"type":"NET_TCP","source":"%local_addre
```

File Download
Add meta information for this file
Send to CloudSandbox Scan Queue
Cloud Sandbox Report Download
Delete File

RTTL interface

The RTTL interface provides full data control, allowing owners to select other members or external participants for sharing based on permissions.

This robust API infrastructure enables users to leverage RTTL's extensive repository of malware samples and threat intelligence, enhancing their cybersecurity efforts and contributing to the overall effectiveness of the platform.

“The Real-Time Threat List (RTTL) is a vital resource for the cybersecurity community, providing a centralized platform for the submission and sharing of malware samples and threat intelligence. With its robust features, extensive contributor network, and comprehensive sandbox integration, RTTL plays a crucial role in enhancing the quality and objectivity of anti-malware testing methodologies.”

– **Alexander Vukcevic, *AMTSO CTO***

Join RTTL

Already an AMTSO member? Sign up using the form at:

https://www.amtso.org/rttl/

Not a member? Sign up to contribute as a CERT or external researcher, or get in touch for more info.