Malware Scanning Methodology

Goal

The goal of this methodology is to test the capability of anti-malware products to accurately detect malicious files while incurring very low false positive rates.

Corpus

Malicious samples are sourced from the Anti-Malware Testing Standards Organisation (AMTSO), using the Real-Time Threat List service. The corpus contains 200 recent, highly prevalent malicious PE files. These are verified by Artifact Security independently of AMTSO for malicious behaviour and validity for this test.

The submitted query to the RTTL service is made public upon issuing certification. Best efforts are made to prevent any bias of sample selection towards a particular vendor participating in this test.

Legitimate samples are sourced from Windows files present on clean deployments of Windows systems. The total number of legitimate samples is 400.

Rating

The tested solution must clearly indicate malicious classification of each malicious sample identified and appropriately identify legitimate samples as clean. No alert or detection of legitimate samples is considered an accurate classification.

Exposure

Products can be exposed to the sample through whatever means necessary (i.e. full fledged solutions, command-line scanners etc). The scanning engine must be the same as what will be provided to the VirusTotal community.

Internet access is available to the scanners during exposure. Upon successful detection of the initial malicious 200 samples these are modified to preserve their functionality but change their appearance. Any samples that lose malicious functionality because of the modification are discarded.

The modified samples are submitted to the product where 100% detection is expected.

Feedback & Pass requirements

Upon successfully completing the initial samples exposure and modified samples the participant is issued with the full set of results. Sub-optimal results can be disputed, if evidence provided is sufficient enough to validate the claim of the product the sample will be discarded and replaced with a new sample from the RTTL.

The pass requirement for this test is 100% accuracy in malicious detection and 0% false positive rate in legitimate handling.

Change Log

10/03/2025 – v1 – Document Created – Identifier MalwareDetection2025v1.0