**Keywords:** anti-malware; compliance; assessment; testing; test plan; Testing Ground Labs; ransomware protection

Initial Release: May 6th, 2023
Reviewed and Public Notification: May 8th, 2023

**Version 1.1**

# Ransomware Protection Test Plan 2023 May (Windows Platform & Consumer Product)

## 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"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.4]. TGL is solely responsible for the content of this Test Plan.

The cybersecurity industry's
testing standard community

## Table of Contents

## 1. Introduction

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

MStarting as early as 1989 with the first documented ransomware known as the AIDS trojan, the use of ransomware scams has grown internationally. There were 181.5 million ransomware attacks in the first six months of 2018. This record marks a 229% increase over this same time frame in 2017. In June 2014, vendor McAfee released data showing that it had collected more than double the number of ransomware samples that quarter than it had in the same quarter of the previous year. CryptoLocker was particularly successful, procuring an estimated US$3 million before it was taken down by authorities, and CryptoWall was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over US$18 million by June 2015. In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. The losses could be more than that, according to the FBI. According to a report by SonicWall, there were around 623 million ransomware attacks in 2021.

Above words are taken from https://en.wikipedia.org/wiki/Ransomware

This test is designed to independently assess how well security solutions can protect consumer PCs against ransomware.

## 2. Scope and Participants

This test is designed to independently assess how well security solutions can protect consumer PCs against ransomware. As a result of the test, certification mark will be granted to security solutions depending on their results. Testing Ground Labs plans to examine consumer security solutions for Windows OS from the following companies (Test Subjects). Specific Test Subject Vendors and Participants will be determined after the Public Test Notification has been issued.

| Vendor | Product Name |
|---|---|
| **AhnLab** | AhnLab V3 Internet Security |
| **Avast** | Avast Premium Security |
| **Avira** | Avira Internet Security |
| **Bitdefender** | Bitdefender Internet Security |
| **ESET** | ESET Internet Security |
| **G DATA** | G DATA Internet Security |
| **Kaspersky** | Kaspersky Standard for Windows |
| **Malwarebytes** | Malwarebytes Premium |
| **McAfee** | McAfee Internet Protection |
| **NortonLifeLock** | Norton Security |
| **Sophos** | Sophos Home Premium |
| **Trend Micro** | Trend Micro Internet Security |
| **Webroot** | Webroot Secure Anywhere |
| **Microsoft** | Windows Defender |

## 3. Methodology

Detailed process is as follows.

1. ~100-200 ransomware samples are selected from TGL's collection (part of them are sourced from TGL's 1 million daily spam collection). Each sample is validated manually to make sure the sample is fully functional in the testing environment.
2. Platform: Windows 11.
3. A broad set of user-files of different types will be prepared and placed in different folders through the File System, their state (filename and checksum) will be recorded by our script. And they will also be used for sorting out the functional ransomware samples.
4. Install selected security applications on the prepared VMware OS image in default configuration.
5. Update the security applications and their antivirus bases.
6. Copy the sample set to a system with a security application and make a record about the detected\deleted samples.
7. Run each missed ransomware sample and take every action suggested by security solution. Compare the file system and check if the user-files are fully protected or been recovered.
8. Detection from on access scan, protection after sample is executed (all user-files are in their initial state), failure to protect file system, are recorded.

## 4. Participation

Testing Ground Labs chooses security solutions of interest to include into this test. Additionally, any vendor may submit request to participate in the test. Testing of either security solution (both chosen by Testing Ground Labs and submitted by a Vendor directly) is free of charge to the Vendor. Every Vendor will be provided with the feedback process, which means that the test lab will share test results with Vendors and they will have chance to investigate the results and submit disputes in case of any.

**Opt-Out Policy**: If any Vendor manages to supply sufficient reason as to why Testing Ground Labs should not include their products in an upcoming or on-going test, Testing Ground Labs will review this request and make the correspondent decision.

**Conflict of Interest Disclosure**: No known conflicts of interest exist at this time.

**Funding**: This test is free of charge. Any Vendor who would like to get post-test service or any other extra service, can email us. Results (reference or direct use of the test report or seals) would be allowed to use only in case of marketing rights agreement between Testing Ground Labs and the interested Vendor.

## 5. Environment

**Physical Configuration**: Windows 11 running on VMware

**Sample Relevance**: Ransomware samples are selected from TGL's collection (part of them are sourced from TGL's 1 million daily spam collection).

**Curation Process**: Each sample is validated manually to make sure the sample is fully functional in the testing environment.

**Distribution of Test Data**: Malicious sample data with non-optimal results are provided to vendor once the full test is complete. Testing Ground Labs does not share data on one vendor with other vendors. Any security vendor whose product was tested, may request hashes of their missed samples/false positives.

## 6. Schedule

**Start Date Range**: Test configuration is scheduled to begin on 6th May, 2023 and the Test commencement is forecast for 22nd May, 2023

**Test Duration and Calculated End Date**: The final Test Report is anticipated during the week of June 12, 2023.

**Milestones**: Interim schedule milestones are listed below.

***Sample Schedule Summary for Test Project***

| Index | Test Activity | Start Date Range | Dependencies |
|---|---|---|---|
| ***1*** | *Test Commencement* | *May 22 2023* | |
| ***2*** | *Confirm Vendor Configuration Feedback* | *May 15 2023 – May 22 2023* | |
| ***3*** | *Milestone 1 – Preliminary Results* | *May 29 2023* | *(1), (2)* |
| ***4*** | *Milestone 2 – Test Report First Edition – End of Testing Period* | *June 2 2023* | *(3)* |
| ***5*** | *Feedback and Dispute Resolution Time – Retests as Needed* | *June 9 2023* | *(3)* |
| ***6*** | *Milestone 3 – Issue Final Report – End Date for Test* | *June 12 2023* | *(5)* |

**Communications**: All Participants will be notified when the schedule changes by two weeks or more.

**Risks and Risk Management**: No additional risks are known at this time.

## 7. Control Procedures

**Connectivity Validation**: All the security solutions in the test will be granted access to their cloud reputation and other services, which is the way how it works for end-users in real life.

**Logging**: Instructions for enabling logging within the Product must be provided by the Participant upon request to Testing Ground Labs.

**Updates**: Any configuration information needed for product updates to take place during the Testing Period should be disclosed by the Participant.

## 8. Scoring Process

For each security solution, a Final Score is calculated once the full test is performed:

**Final Score = (Protection rate%) *100**

**Protection= on access scan protection plus protection during sample execution**

Basing on the Final Score, the correspondent rating is grated to each participating security solution, in accordance with the tab below:

| final score | monthly award |
|---|---|
| **98.00 - 100.00** | 5-star rating |
| **95.00 - 97.99** | 4-star rating |
| **90.00 - 94.99** | 3-star rating |

## 9. Dispute Process

The dispute process runs for eight business days commencing from the end of the test. Refer to Section 6 covering the Test Schedule for additional details and timing. The general Dispute Process works as follows.

1. Testing Ground Labs provides Vendors with results their security solution with hash values associated with any sub-optimal results.

2. Vendor responds within eight business days to Testing Ground Labs, providing fact-based disagreements with any sub-optimal results, in case of any.

3. Testing Ground Labs responds with decision, if the dispute is accepted or denied.

## 10. 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: /s/

Name: Jeffrey Wu

Test Lab: Testing Ground Labs

Email: jeff@testingground.io

AMTSO Test ID: [AMTSO-LS1-TP077]