Keywords: cryptomining, cryptojacking, test, endpoint protection, enterprise, business, corporate, NioGuard.

17.06.2019

Version 1.1

NioGuard Security Lab

Anti-Cryptojacking Test

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 [1.1] (the “Standard”). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.3]. NioGuard Security Lab is solely responsible for the content of this Test Plan.

Table of Contents

AMTSO Test Plan Template

1. Introduction

NioGuard Security Lab (Tester) tests a variety of corporate endpoint security products from the industry leaders in an effort to judge which were the most effective in detecting unauthorized cryptomining called cryptojacking. Each product is exposed to the same threats that represent cryptominers in different forms. The Test Report indicates how effectively the products were at detecting those threats in real time.

The Test Plan follows the AMTSO Testing Protocol Standard and is a subject for a compliance check by AMTSO.

2. Scope

This section clearly identifies the types of Test Subjects that will be included in the Test and an approach for selecting the version or edition that shall be tested. The actual Test Subject Vendors and Participants might not be finalized at the point of the Test Plan's publication.

We welcome the following Vendors to be Participants in this test with their corporate endpoint protection solutions.

Product Vendor	Product Name	Version Selected or Process Used
Acronis	*Acronis Backup*	*Latest version available by Test Commencement Date.*
Avast	*Avast Business Antivirus Pro Plus*	*Latest version available by Test Commencement Date.*
Avira	*Antivirus Pro*	*Latest version available by Test Commencement Date.*
BitDefender	*Bitdefender GravityZone Security for Endpoints*	*Latest version available by Test Commencement Date.*
Crowdstrike	*Falcon Endpoint Protection Enterprise*	*Latest version available by Test Commencement Date.*
ESET	*ESET Endpoint Security*	*Latest version available by Test Commencement Date.*
FireEye	*FireEye Endpoint Security*	*Latest version available by Test Commencement Date.*
F-Secure	*F-Secure Business*	*Latest version available by Test*

	Suite	*Commencement Date.*
K-7	*K-7 Endpoint Protection*	*Latest version available by Test Commencement Date.*
Kaspersky	*Kaspersky Endpoint Security*	*Latest version available by Test Commencement Date.*
Malwarebytes	*Malwarebytes Endpoint Security*	*Latest version available by Test Commencement Date.*
McAfee	*McAfee Endpoint Security*	*Latest version available by Test Commencement Date.*
Microsoft	*Microsoft Windows Defender ATP's Antivirus*	*Latest version available by Test Commencement Date.*
Sophos	*Sophos Intercept X Advanced*	*Latest version available by Test Commencement Date.*
Symantec	*Symantec Endpoint Protection*	*Latest version available by Test Commencement Date.*
Trend Micro	*Trend Micro OfficeScan*	*Latest version available by Test Commencement Date.*
VIPRE	*VIPRE Endpoint Security Cloud Edition*	*Latest version available by Test Commencement Date.*

The final list of the Test Subject Products will be published in the Test Report.

The test contains the following scenarios:

1. The publicly available cryptominers.
2. Packed and/or obfuscated versions of the cryptominers mentioned in item 1 to exclude signature-based detection.
3. Malware that start cryptominers on an infected host.
4. Negative tests that include legitimate everyday activities resulting in high CPU (GPU) load.

The test aims at testing the capabilities of endpoint security solutions to identify cryptomining activity on a host focusing on behavior blocking functions.

Configuration approach is using the default settings if other is not specified in the Test Report. A Vendor can request to use custom configuration of the Product. In such case, all custom settings will be mentioned in the Test Report.

3. Methodology and Strategy

The Test aims to verify detection capabilities of security solutions against cryptomining that may use organization's computing resources (CPUs/GPUs) for unauthorized cryptocurrency mining.

The sources of cryptominers used in the test are:

1. Public code repositories (e.g. Github) that contain the source code and/or binaries of the popular cryptominers.
2. Malware caught in the wild that unsolicitedly use a user's computer to install and run a cryptominer.

In case of running cryptominers from the public source code repositories, the compiled miners, if available, are downloaded and run under a user with regular privileges via the command line. If compiled versions of the miners are not available, the miners are compiled. If a cryptominer requires installation of addition software or framework (e.g. Java Platform), this will be installed in a test environment. The default test wallets and mining pools are used for cryptomining in the tests if available. Otherwise, a test wallet is created and an address of a mining pool is manually specified. The test environments are built on the Windows 10 with all patches available at the moment of the test.

All threats are identified, collected and analyzed independently of security vendors directly or indirectly involved in the test.

For negative tests, everyday legitimate activities were taken into account that have a significant impact on CPUs (GPUs) and may lead to potential false positives.

By default, the latest version of a product is used at the moment of running a test unless specific version is requested by a Vendor, which will be mentioned in the Test Report.

4. Participation

Participation in the test for the Test Subject Vendors is free of charge. All Test Subject Vendors may choose to adopt Participant status by notifying us.

The general process for participation in this, or any, test with NioGuard Security Lab is as follows.

- NioGuard Security Lab or Vendor approach one another in person, by email or on the call.
- Both parties will then:
  - Discuss the desired testing methodology and configuration
  - NioGuard Security Lab reserves the right that they may or may not test the product
  - Dispute processes precede
  - Report publication

Please contact us at ada@nioguard.com. We will be happy to arrange a call to discuss our methodology and the suitability of your product for inclusion.

Opt-Out Policy:

A Vendor can choose to opt out before the Test starts without providing any details regarding this decision. The Vendor will not be included in that specific Test. If a Vendor choose to opt out during the ongoing Test or after the Test completion, the Vendor must provide arguments for that decision. NioGuard Security Lab will disclose circumstances under which a Participant or Test Subject Vendor has been dropped from the public final Test Report.

Conflict of Interest Disclosure: No known conflicts of interest exist at this time. Post-test consultancy services are available to all participants for a fee.

Funding: The Test was commissioned by Acronis International GmbH. Other Test Subject Products are included in the Test at no cost to the vendor. Post-test consultancy services, rights to use our logos, and re-promote our results are made available to all Participants, subject to consultancy or licensing fees.

5. Environment

Physical Configuration:
The testing environment is as follows:

1. CPU environment

   VirtualBox Windows 10 virtual machine
   - CPU 2 (Intel Core i5-3210 2.50GHz)
   - RAM 4,00 GB
   - Windows 10 Enterprise Evaluation build 17134 64-bit
2. GPU environment
   - Intel Core i5-7600 3.50GHz
   - RAM 8 GB
   - GPU 1: GeForce GTX 1060 6GB
   - GPU 2: GeForce GTX 850M 4GB
   - GPU 3: P106-100
   - Windows 10 Pro 1803 build 17134.523 64-bit

The test environment can be changed during the test. The actual configuration of the test environment used during the test will be provided in the Test Report.

Sample Relevance: The Test includes test scenarios that run the public cryptominers that are used in many cases of cryptojacking attacks to mine cryptocurrency.

Geographic Limitations: No limitations.

Curation Process: The cryptominers selected for the test should be publicly available and run on Windows 10 (64-bit). Additional protection such as PE packers can be applied to the public cryptominers so the behavior blocking capabilities of the Products can be tested as well. The cryptominers were selected and validated by NioGuard Security Lab to be operable.

Distribution of Test Data: Test data will be provided to Partners according to the signed agreement between parties once the Test is complete. NioGuard Security Lab does not share data on one partner with other partners. Any Test Subject Vendor that has their Product tested may request logs generated by their Product.

6. Schedule

Start Date Range: Test configuration is scheduled to begin on June 17th, 2019 and the Test commencement is forecast for July 1st, 2019. Participant configuration is anticipated to take place during the intervening two-week period.

Test Duration and Calculated End Date: The anticipated duration and end date of the test should also be provided.   This will allow for Tester to notify Test Subject Vendors that the Product would need to remain operational for the needed period of time to complete the Test.

Milestones: Interim milestones that can be reviewed by Participants, including the anticipated delivery of a Test Report, should be specified where applicable. The following Sample Schedule Summary can be used as a reference.

Schedule Summary for Test Project

Index	Test Activity	Start Date Range	Dependencies
1	*Test Commencement*	*July 1, 2019*	(2)
2	*Confirm Vendor Configuration Feedback*	*June 17 - July 1, 2019*	
3	*Milestone 1 – Preliminary Results*	*July 8, 2019*	*(1), (2)*
4	*Milestone 2 – Test Report First Edition – End of Testing Period*	*July 15, 2019*	*(3)*
5	*Feedback and Dispute Resolution Time – Retests as Needed*	*July 15, 2019 - July 22, 2019*	*(4)*
6	*Milestone 3 – Issue Final Report – End Date for Test*	*July 29, 2019*	*(5)*

Communications: All Test Subject Vendors will be notified of deviations from the Schedule by four weeks or more.

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

7. Control Procedures

The Test Plan may include instructions for potential Participants to provide Specific Data regarding the Product(s) to be included in the test. These elements are included in the Control Procedures section.

Connectivity Validation: A means for confirming whether a Product's cloud connectivity or other features are functioning can be provided by the Vendor.

Logging: Products run with the default settings. Additional logging may be enabled if requested by the Vendor of the Product in question. Vendors are invited to make configuration recommendations.

Updates: All products are updated fully using the latest definitions, patches and any other available updates. These updates are made immediately prior to each exposure to a threat or legitimate application. Products may be upgraded to the latest version, if the version changes during the test period.

8. Dependencies

Participant and Test Subject Vendors Required Actions: Vendors may contact Alexander Adamov representing NioGuard Security Lab for inclusion, exclusion or to respond to an invitation, either accepting or declining.

9. Scoring Process

The following occurrences during the Test will be recorded and all contribute to the product effectiveness measure.

- Threat detection in the form of pop-up information messages or requests for action.
- Threat blocking in the form of:
    - Execution blocking.
    - Process blocking.
    - Network connection blocking.
- Details of the threat, as reported by the product (e.g. threat name; attack type).
- Unsuccessful detection of threats.
- Legitimate processes allowed to run without blocking.

Measuring Product Effectiveness: Each Target System is monitored to detect a product's ability to detect, block, or neutralize threats that are executed. As cryptominers considered by some Vendors as Potentially Unwanted Application (PUA) and their Products do not block but only notify a user, we do not distinguish product's reactions such as detection, blocking, or neutralizing cryptominers assigning them the same score for any type of reactions that help a user identify cryptomining activity. False Positives in the negative tests will result in giving a score that will be subtracted from Protection Rating (4).

The following metrics will be calculated in this Test:

- True Positive Rate (TPR)

$$TPR = \frac{TP}{TP + FN} \qquad (1)$$

- True Negative Rate (TNR)

$$TNR = \frac{TN}{TN + FP} \qquad (2)$$

- Accuracy

$$Accuracy = \frac{TP+TN}{TP + TN + FP + FN} \qquad (3)$$

- Protection Rating

$$Protection\ Rating = \sum_i \quad dw \cdot x_j^p \quad - \sum_j \quad dw \cdot x_j^n \quad , \qquad (4)$$

where

dw = 1 (detection weight),

x_i^T = {0,1} represents a product's reaction to the test *i* with the type *T*.

0: stands for no reaction from the product side;

1: a product reacts by detecting, blocking or neutralizing a specific test;

$i \in [1, N]$, where *N is* the total number of positive tests*;*

$j \in [1, M]$, where *M is* the total number of negative tests*;*

$T \in \{p, n\}$represents a type of test, thus:

x_j^p - product's reaction to a positive test,

x_j^n - product's reaction to a negative test,

where

- TP (True Positive) — correctly detected,
- FP (False Positive) — incorrectly detected,
- TN (True Negative) — correctly undetected,
- FN (False Negative) — incorrectly undetected.

Awards: NioGuard Security Lab provides badges such as AAA, AA, and others based on the Test Scoring results. Partners can use the NioGuard Security Lab awards logos for marketing purposes.

10. Dispute Process

The dispute process runs for two weeks from the end of the test. Please see Section 6 covering the Test Schedule for additional details and timing. The general Dispute Process works as follows.

1. Any disputes from a Participant or Test Subject Vendor must be accompanied by an element of proof, or evidence that the dispute is legitimate, rather than just the Vendor's statement of disagreement.

2. Test results are provided with Product's logs.

3. Vendor responds within two weeks, arguing why some test results are wrong.

4. Tester replies, accepting or denying the dispute.

Evidence Sharing Policy: Test Subject Vendors may request their Product's logs for free. Any sensitive information that will potentially help to identify samples used in the test will be removed from the logs. Test Subject Vendors should enable Testers to review and understand all logs and other data generated by their Products, to ensure no sensitive information is shared unintentionally. NioGuard Security Lab may withhold evidence if it is encrypted, obfuscated or otherwise rendered unreadable to the Tester, and may edit or otherwise modify logs and other items of evidence only to remove sensitive information if required. Participants can request more Test data according to a signed agreement after Test completion.

11. 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/ Alexander Adamov

Name: Alexander Adamov

Test Lab: NioGuard Security Lab