CHECKMARK CERTIFIED

MALWAREREMEDIATION

CERTIFICATION SUMMARY

Company: Enigma
Product: SpyHunter
Version: 5.0.30.51

1st March 2019

Author(s): Scott Markle, Richard Thomas

Contents

Introduction

This document is designed to provide a high-level outline of the outcome from the latest round of testing conducted against the listed solution. Tests were conducted as per the testing requirements and procedures that form the Checkmark Certified Malware Remediation accreditation.

Results are in two sections. The first section shows the awarded certification level, the second section shows the baseline requirements that were met.

This accreditation should not be taken in isolation as an indication of a solution's malware detection capability; but is, instead, designed to illustrate a solution's ability to detect and mitigate existing malware infections/installations.

It is recommended that this accreditation be combined with that of Checkmark Certified Anti-Malware Desktop.

All information contained within this document shall remain the property of Checkmark Certified and is not for release to unauthorised third parties.

About Checkmark

The Checkmark Certified (CC) business philosophy is founded on quality and excellence with all testing activities carried out in a secure, real-world test environment and within a framework of confidentiality that ensures integrity of information and test data.

CC prides itself on its open and proactive working relationship with all its clients through ongoing and meaningful communication.

The outcome is a sound technical working relationship, which ensures the client derives maximum benefit from engaging with an independent test facility that can also act as a conduit to a global buying market for security products and services

Test Overview

Testing was conducted entirely onsite at Checkmark Certified facilities, with the exception of any offsite examination that was required for verification of the vendor's development processes.

The solution was examined for efficacy in four areas:

1. Detection and mitigation of currently running processes;
2. Detection and removal of dropped executables;
3. Detection and/or removal of secondary files, such as DLLs;
4. Detection and/or removal of registry entries.

This accreditation may result in one of three outcomes:

Less than 100% mitigation of running processes, 90% of dropped executables, 85% of secondary files, or 85% of registry entries - FAIL

Mitigation of 100% of running processes, more than 90% of dropped executables, and more than 85% of secondary files and registry entries - STANDARD CERTIFICATION

Mitigation of 100% of running processes, more than 95% of dropped executables, and more than 90% of secondary files and registry entries - PREMIUM CERTIFICATION

Test Environment & Network

The following test network diagram (Fig 1.0) depicts the test network used in this accreditation. Testing was conducted on an isolated test network, to prevent cross contamination of both the network and test results, with an active Internet connection being provided by an existing ISP.

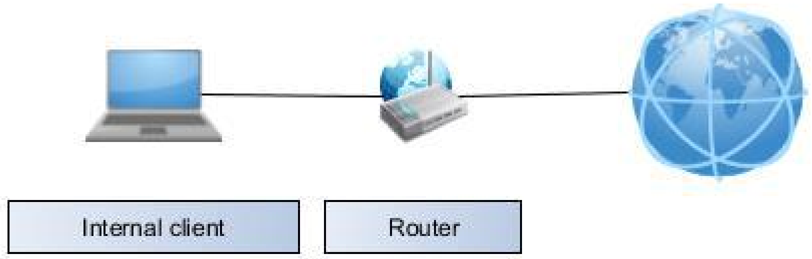

Fig 1.0 – proposed network diagram

The internal client(s) were forensically imaged prior to testing, so as to provide a viable return position.

Test Criteria – Result Overview

Universal – Development

The product outlined in this report has qualified for the following level of certification, as per the criteria outlined below. All results were correct at time of testing.

	FAIL	STANDARD	PREMIUM
Running Processes	-	-	✓
Dropped Executables	-	-	✓
Secondary Files	-	-	✓
Registry Entries	-	-	✓

Running Processes

This criteria examined the solution's ability to examine all of the system's currently running processes and accurately identify any that may be present as a result of infection.

Premium	100%	✓
Standard	97-99%	-
Fail	<97%	-

Secondary Files

This criteria requires the detection of files not otherwise included in the Dropped Executables test listed above.

Premium	>90%	✓
Standard	85-90%	-
Fail	<85%	-

Dropped Executables

This criteria is a test of the solution's ability to detect, upon scanning, the presence of any binary files that have been placed on the system after infection. Only valid, executable files are included.

Premium	>94%	✓
Standard	90-94%	-
Fail	<90%	-

Registry Entries

This criteria is intended to detect where any registry entries, resulting from previous infection, still remain.

Premium	>90%	✓
Standard	85-90%	-
Fail	<85%	-

Test Criteria – Results

Universal – Development

In order to qualify for Checkmark Certified accreditation, checks are made to determine that the vendor meets a set of standards that are designed to mitigate against outside interference with the SUT during its development phase.

UNI.DEV.1 – Access Restriction	
The SUT developer is **required** to show that access to the SUT is restricted during the development phase, so that only authorised personnel are allowed.	CHECKMARK CERTIFIED

UNI.DEV.2 – Tamper Protection	
The SUT developer is **required** to show that security policies are in place that prevent tampering with the SUT, by third parties, that would introduce a security risk on deployment.	CHECKMARK CERTIFIED

UNI.DEV.3 – Documentation Accuracy	
The SUT developer is **required** to demonstrate that accurate documentation is kept, and is reflected in the SUTs implementation.	CHECKMARK CERTIFIED

Universal – Administration

UNI.ADM.1 - Secure admin login	
The SUT **should** provide a secure means of logging into the management interface, where applicable.	CHECKMARK CERTIFIED

UNI.ADM.2 - Log accuracy	
The SUT is **required** to compile and maintain accurate log files that record any events or behaviour that trigger a security ruleset.	CHECKMARK CERTIFIED

Universal - Documentation

UNI.DOC.1 – Remediation Options	
Documentation **must** contain sufficient information on changing the actions to be taken on detection of an infection.	CHECKMARK CERTIFIED

Malware Remediation - Function

REM.FUNC.1 – Detection Report	
The SUT is **required** to provide an individual breakdown of infected files, including path, infection name/family, and severity.	CHECKMARK CERTIFIED

REM.FUNC.2 – Recommended Action	
The SUT is **required** to provide a default action recommendation on detection.	CHECKMARK CERTIFIED

REM.FUNC.3 – Process Detection Accuracy	
The SUT is **required** to accurately detect and mitigate the presence of 100% of the running processes and/or open ports associated with each individual sample.	CHECKMARK CERTIFIED

REM.FUNC.4 – Dropped Executable Detection Accuracy	
The SUT is **required** to accurately detect and mitigate the presence of 90% of the dropped files associated with each individual sample.	CHECKMARK CERTIFIED

REM.FUNC.5 – Secondary File Detection Accuracy	
The SUT is **required** to accurately detect and mitigate the presence of 85% of secondary files associated with each individual sample such as DLLs or non-executable files.	CHECKMARK CERTIFIED

REM.FUNC.6 – Registry Entry Detection Accuracy	
The SUT is **required** to accurately detect and mitigate the presence of 85% of registry entries, resulting from malware infection.	CHECKMARK CERTIFIED

Malware Remediation - Impact

REM.IMP.1 – False Positive Detection – OS Files	
The SUT is **required** to not incorrectly identify Windows critical files during detection/scanning.	CHECKMARK CERTIFIED

Disclaimer

While Checkmark Certified is dedicated to ensuring the highest standard of security product testing in the industry, it is never possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose. Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by Checkmark Certified should seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations. All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

Checkmark Certified provides detailed reporting for each product tested within the specified scope of work. The test results are relative to the test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

Appendix 1 – Test Specifications

The following pages provide a high level outline of individual procedures that are followed for specific tests.

Remediation – Testing

A number of files will be selected from the Checkmark Certified malware suite(s). Each of these files will then be, in turn, executed on a clean Windows installation and any on-screen instructions followed.

After the file has been executed, the system will be restarted. Following a successful restart, the system will be rebooted into a Linux environment so that a forensic image may be taken.

Once all forensic images are created, they will be restored individually before the SUT is installed and a number of scans conducted. Any detected files will be cleaned as per the SUTs recommended actions. The system will then be analysed for the presence of any remaining files/processes.

On completion of analysis, the results be logged for feedback to the vendor.