KECS-CR-19-20

ZERO Inspector V4.0

Certification Report

Certification No.: KECS-CISS-0927-2019

2019. 4. 23

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.04.23	-	Certification report for ZombieZERO Inspector V4.0 - First documentation

This document is the certification report for ZombieZERO Inspector V4.0 of NPCore, Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of EAL2 evaluation of ZombieZERO Inspector V4.0 with reference to the Common Criteria for Information Technology Security Evaluation (“CC”hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is software-type security product that detects malicious code coming from outside and blocks or isolates it based on pattern-based and behavioral analysis technique and it blocks internal users to access in unauthorized IP/URL (ex. malicious code distribution site).

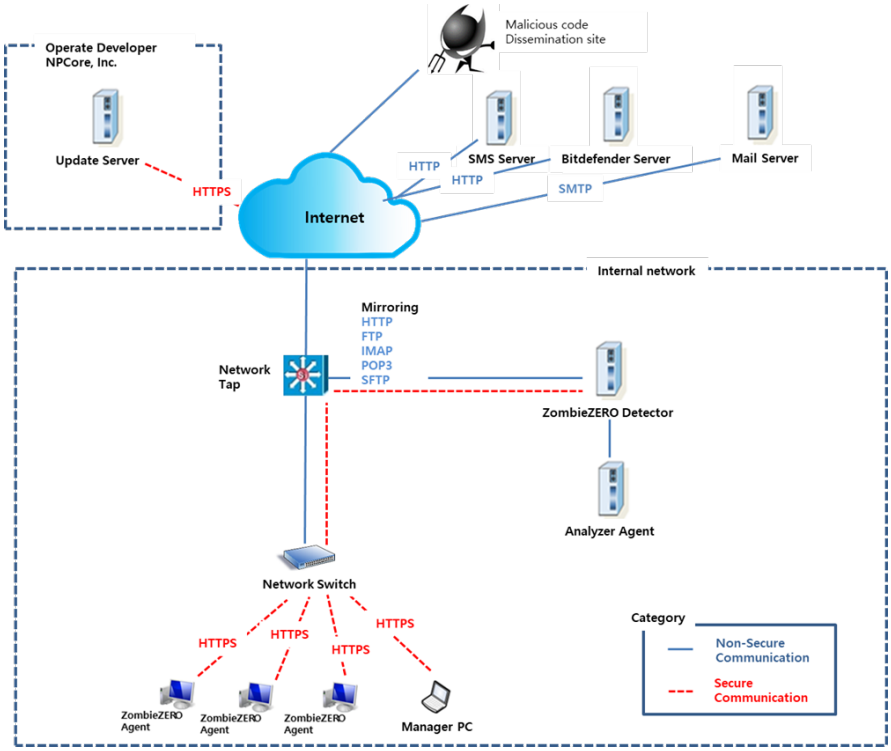
The TOE (ZombieZERO Inspector V4.0) is composed of the following components:

- ZombieZERO Detector V4.2.71 (hereafter referred to as ‘ZombieZERO Detector’),
- Analyzer Agent V4.0.0 (hereafter referred to as ‘Analyzer Agent’), and
- ZombieZERO Agent V4.0.227 (hereafter referred to as ‘ZombieZERO Agent’).

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on April 17, 2019. This report grounds on the evaluation technical report (ETR) that KTC had submitted [3] and the Security Target (ST) [4].

The ST does not claim conformance to a Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL2. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE are CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

- ZombieZERO Detector is connected to a network terminal access point (TAP) installed at a place where external and internal networks are connected, and receives port-mirrored traffic through the Network TAP.
- Analyzer Agent installed and operated on a guest OS is not connected to other external IT entities via the network, but directly connected to ZombieZERO Detector and operated.
- ZombieZERO Agent is installed and operated in internal users' PCs.
- Encryption communication between ZombieZERO Detector and ZombieZERO Agent and between an administrator PC and ZombieZERO Detector for security management are based on the Transport Layer Security (TLS) 1.2(TLS Cipher Suites in Windows 10 v1607) protocol provided by IIS10.0 installed in ZombieZERO Detector.

- An update server run by the developer NPCore, Inc. provides up-to-date information owned by the developer, and transmits updated files to ZombieZERO Detector after electronic signature. Commercial anti-virus server provides updates to the signature pattern.

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Component		Minimum Requirement
ZombieZERO Detector	CPU	Intel Xeon Quad Core 2.13 GHz or higher
	RAM	4GB or higher
	HDD	Available space of more than 1 GB required to install ZombieZERO Detector
	NIC	10/100/1000Mbps * 4 port
	OS	Windows Server 2016 Standard 64bit
	SW	- MySQL Community Server 5.6.43 - IIS 10.0 - VMware VIX API 1.14.0
Analyzer Agent	CPU	Intel Xeon Quad Core 2.13 GHz or above
	RAM	4GB or higher
	SSD	Available space of more than 50MB required to install Analyzer Agent
	NIC	10/100/1000Mbps * 1 port
	Hypervisor (Type1)	VMware ESXi 5.5.0 U3
	Guest OS	- Windows 7 Professional 32bit - Windows 7 Professional 64bit - Windows 10 Pro 32bit - Windows 10 Pro 64bit
	SW (installed on the Guest OS)	- .net framework 4.6 - Microsoft Office 2013 - Adobe Acrobat pro XI - Adobe Flash Player 16 - Hancom Office 2010

ZombieZERO Agent	CPU	Intel Celeron 2.6 GHz or above
	RAM	4GB or higher
	HDD	Available space of more than 50MB required to install ZombieZERO Agent
	NIC	10/100/1000Mbps * 1 port
	OS	- Windows 7 Professional 32bit - Windows 7 Professional 64bit - Windows 10 Pro 32bit - Windows 10 Pro 64bit

[Table 1] Hardware and software requirements for TOE

Administrator uses the PC that can operate web browser to use the security management. Administrator's PC minimum requirements are shown in [Table 2].

Component	Minimum Requirement
CPU	Intel Celeron 2.6 GHz or above
RAM	4GB or higher
HDD	500GB or higher
NIC	10/100/1000Mbps * 1 port or more
OS	- Windows 7 Professional 32bit - Windows 7 Professional 64bit - Windows 10 Pro 32bit - Windows 10 Pro 64bit
SW	- Web Browser (Internet Explorer 10, Internet Explorer 11) - VMware vSphere Client 5.5 (Used when the guest OS of Analyzer Agent is installed)

[Table 2] Hardware and software requirements for the administrator's PC

The following software is the operational environment of the TOE and out of the scope of the TOE.

- MySQL Community Server 5.6.43, IIS 10.0(including 'TLS Cipher Suites in Windows 10 v1607' library), VMware VIX API 1.14.0, VMware ESXi 5.5 U3, .net framework 4.6, Microsoft Office 2013, Adobe Acrobat pro XI, Adobe Flash Player 16, Hancom Office 2010

The following external IT entities required to operate the TOE are out of the scope of the TOE.

- Network Tap, SMS Server, Update Server, Mail Server, Bitdefender Server

For more details refer to the ST [4].

2. Identification

The TOE is identified as follows and is delivered in a DVD.

TOE	ZombieZERO Inspector V4.0	
Detailed Version	V4.0 Revision 12	
TOE Component (Software)	ZombieZERO Detector	ZombieZERO Detector V4.2.71 (ZombieZERO Detector V4.2.71.exe)
	Analyzer Agent	Analyzer Agent V4.0.0 (Analyzer Agent V4.0.0.exe)
	ZombieZERO Agent	ZombieZERO Agent V4.0.227 (ZombieZERO Agent V4.0.227.exe)
Documents (PDF)	ZombieZERO Inspector V4.0 Installation Manual V1.4 (ZombieZERO Inspector V4.0 Installation Manual V1.4.pdf)	
	ZombieZERO Inspector V4.0 Manual for Administrator V1.4 (ZombieZERO Inspector V4.0 Manual for Administrator V1.4.pdf)	

[Table 3] TOE identification

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	ZombieZERO Inspector V4.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL2
Protection Profile	N/A (ST does not claim conformance to a PP)
Developer	NPCore, Inc.
Sponsor	NPCore, Inc.
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	April 17, 2019
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [4] does not claim conformance with Protection Profile.

The TOE complies security polices defined in the ST by security Objectives and security requirements. The TOE provides security features to detect and block/isolate malicious code, to encrypt and decrypt security policy file, to block access to unauthorized IP/URLs, to verify the integrity of TSF and configuration data, to record security audit, and to provide security management. For more details refer to the ST [4].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [4], chapter 3.3):

- ZombieZERO Detector and Analyzer Agent among the TOE components shall be located in a physically secured environment where only authorized administrators can access.
- Analyzer Agent among the TOE components shall be executed and operated securely in a reliable virtual machine.
- The internal and external communications shall be done only through the network TAP to enable the TOE to perform mirroring of network traffic that is introduced to the internal network or transmission to the Internet. In addition, Analyzer Agent is directly connected with ZombieZERO Detector without a network route.

For the complete list of assumptions regarding the operational environment of the TOE, refer to the ST [4], chapter 3.3. Furthermore, some aspects of threats and organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the ST [4], chapter 3.1, 3.2 and 4.2.

This text covers some of the more important limitations and clarifications of this evaluation.

Note that:

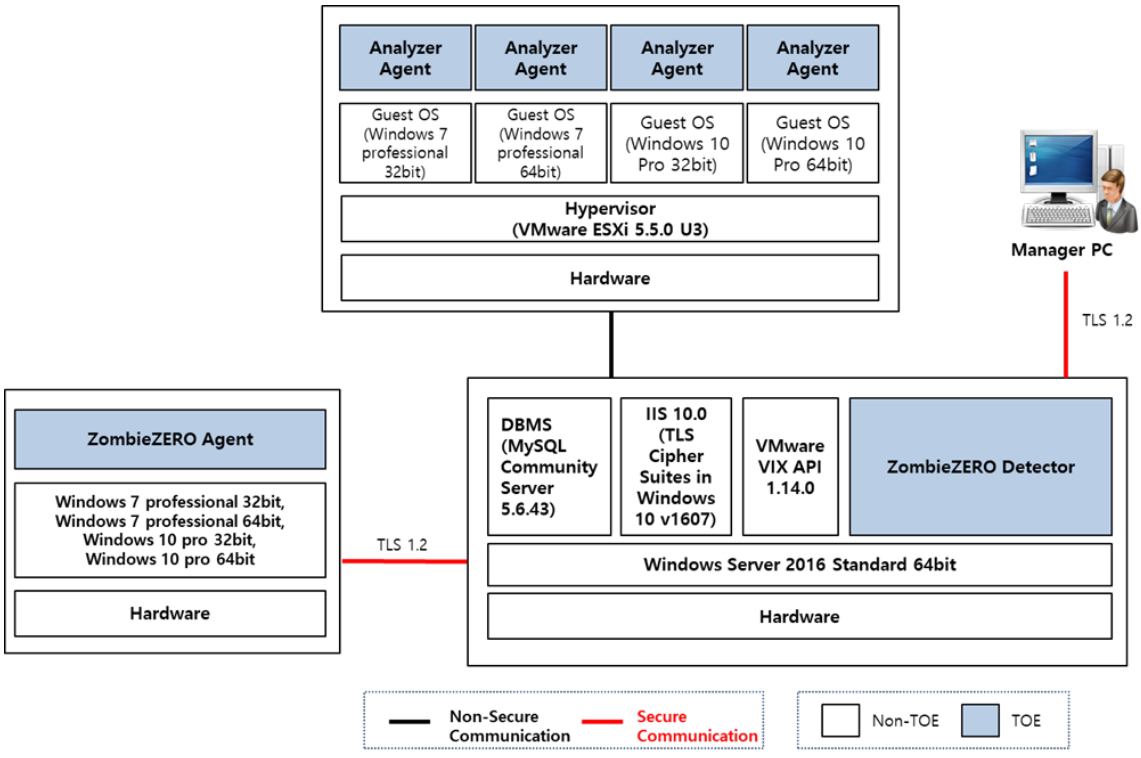
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. .(for

the detailed information of TOE version and TOE Components version refer to the [Table 2])

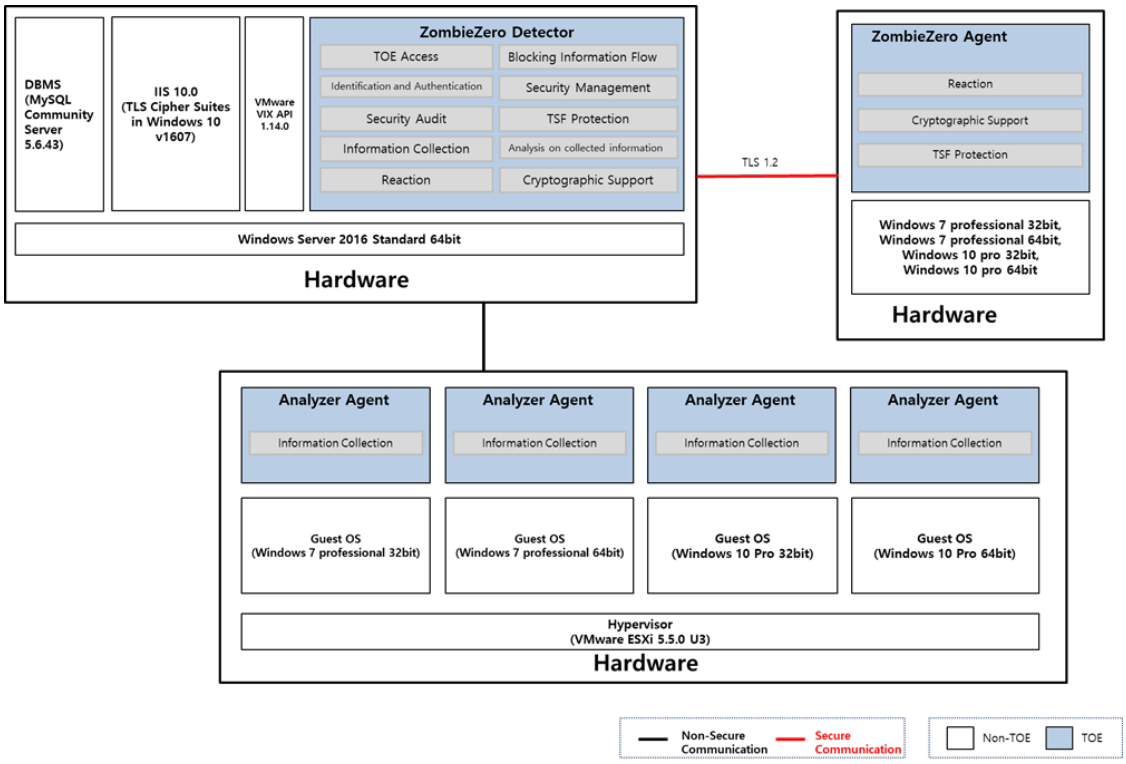
5. Architectural Information

[Figure 2] and [Figure 3] show the scope of the TOE. The TOE is software that is consisting of the ZombieZERO Detector, Anlayzer Agent, and ZombieZERO Agent. It is provided as a form of digital versatile disc (DVD). In addition, the physical scope includes the “Installation Manual” and “Manual for Administrator” distributed as a form of electronic document (DVD) to the end users (customers).

The OS, guest OS, Hypervisor, DBMS, IIS, and VMware VIX API, which are required to operate the TOE, are out of the scope of the TOE.



[Figure 2] Physical scope of the TOE



[Figure 3 Logical scope of the TOE

- ZombieZERO Detector extract and collects files from traffic coming into the internal network through HTTP/1.1, FTP, POP3, IMAP, and SMTP protocols. ZombieZERO Detector stores the behavior information of the files collected by the Analyzer Agent and the file (.exe) requested to be analyzed by ZombieZERO Agent. ZombieZERO Detector detects malicious code by comparing collected files against patterns held by ZombieZERO Detector. ZombieZERO Detector sends a security policy (blocking and isolation) for detected malicious code to the ZombieZERO Agent. ZombieZERO Detector transmits a reset packet to the corresponding internal PC and blocks the packet when the packet is transmitted to Blacklist IP/URLs.
- Analyzer Agent executes the file transmitted from ZombieZERO Detector and collects and stores the action information. (Behavior information: registry

behavior, network behavior, memory behavior, file behavior, process behavior)

- ZombieZERO Agent blocks (or isolates) the execution of files containing malicious code according to the security policy.

For the detailed description is referred to the ST [4].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Version
ZombieZERO Inspector V4.0 Installation Manual V1.4 (ZombieZERO Inspector V4.0 Installation Manual V1.4.pdf)	V1.4
ZombieZERO Inspector V4.0 Manual for Administrator V1.4 (ZombieZERO Inspector V4.0 Manual for Administrator V1.4.pdf)	V1.4

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE.

SFRs test, testing the correct implementation of the Security Functional Requirements described in the ST.

TSFIs tests, testing the functionality invoked using TSFIs.

Integrity tests, testing the integrity of security functionalities provided by the TOE.

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.1. This means that the developer tested all the TSFI defined for SFR-enforcing of the TOE, and demonstrated that the TSF behaves as described in the functional specification.

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator performed all tests provided by developer and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures, according to the guidance.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is ZombieZERO Inspector V4.0 consisting of the following components:

- ZombieZERO Detector V4.2.71,
- Analyzer Agent V4.0.0, and
- ZombieZERO Agent V4.0.227.

Administrator can identify the complete TOE reference after log in ZombieZERO Inspector V4.0. And the guidance documents listed in this report chapter 6, [Table 2] were evaluated with the TOE.

For details regarding non-TOE hardware and software required by the TOE, refer to the evaluated guidance documents.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL2.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent. Therefore the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation. Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer uses a CM system that uniquely identifies all configuration items. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE, the parts that comprise the TOE, the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation,

facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. Therefore the verdict PASS is assigned to ADV_TDS.1.

The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, for the SFR-enforcing TSFIs the developer has described the SFR-enforcing actions and direct error messages. Therefore the verdict PASS is assigned to ADV_FSP.2.

The TSF is structured such that it can not be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how

its security enforcement can not be compromised or bypassed).

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.1.

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE, don’t allow attackers prossessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
	ASE_COMP.1	ASE_COMP.1.1E	PASS	PASS	
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS		
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.1	ATE_COV.1.1E	PASS	PASS	PASS
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings :

- ZombieZERO Detector must be connected to the Network TAP for network packet monitoring between the Internet and the internal network.
- The authorized administrator should manage not to provide unnecessary services to Windows Server 2016 Standard based ZombieZERO Detector.
- The following communication uses HTTPS protocol based on TLS1.2 provided by IIS10.0. When TLS 1.2 is used, secret communication is performed using a secure encryption algorithm.
- ZombieZERO Detector ↔ ZombieZERO Agent
- Manager PC ↔ ZombieZERO Detector
- Authorized administrators should periodically perform live updates on the ZombieZERO Detector to ensure that the latest malware information is applied.
- The Analyzer Agent must connect directly to the ZombieZERO Detector to avoid communication with other IT entities via the network to prevent malicious code propagation.

11. Security Target

The ZombieZERO Inspector V4.0 Security Target V1.10 [4] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [5] according to the CCRA supporting document ST sanitising for publication [6].

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
Malicious Code	It refers to executable code created by malicious purposes. Executable code includes not only program, macro, and script but also data format using vulnerability. Malicious software is the widest concept. It can be classified to viruses, worms, Trojan horses, and spyware according to the self-replication ability and infection target.
Malicious behavior	Behavior that uses user's PC in malicious activities as malicious code is installed in user's PC with the malicious purpose.
Behavior-based	It is a technology that detect malicious code by determining whether the code is malicious based on the behavior of the executable file to respond to the malicious code effectively which is advanced daily and difficult to be detected by existing pattern methods.
Network TAP	Network TAP is an external monitoring device that

	mirrors traffic delivered between network nodes. It is a hardware device inserted to the specific spot (intrusion prevention system (IPS) and switch to monitor data.
Port Mirroring	It is a method to replicate packets to other switch ports to monitor or observe the packets that pass through the switch port in the network switch.
Blacklist	A list of malicious files and malicious code distribution sites (IP/URL) held by the developer and files that are determined as malicious files by the ZombieZERO Detector

13. Bibliography

The evaluation facility has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] CC2018-00007 ZombieZERO Inspector V4.0 Evaluation Technical Report V3.0, April 17, 2019

[4] ZombieZERO Inspector V4.0 Security Target V1.10, April 12, 2019

[5] ZombieZERO Inspector V4.0 Security Target Public Version V1.10, April 12, 2019 (Sanitized Version)

[6] ST sanitizing for publication, CCDB-2006-04-004, April 2006