REF: 2017-16-INF-2295 v2	Created by: CERT9
Target: P	Revised by: CALIDAD
Date: 04.04.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2017-16 Panda Adaptive Defense
Applicant: B48435218

References:
[EXT-3369] Certification request of Panda Adaptive Defense
[EXT-3874] Evaluation Technical Report of Panda Adaptive Defense.
The product documentation referenced in the above documents.

Certification report of the product “Panda Adaptive Defense Protection Agent v8.0”, as requested in [EXT-3369] dated 10-05-2017, and evaluated by the laboratory “Applus Laboratories”, as detailed in the Evaluation Technical Report [EXT-3874] received on 23/02/2018.

ENAC CERTIFICACIÓN Nº 45/C-PR110
https://oc.ccn.cni.es
Email: certificacion.ccn@cni.es

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Panda Adaptive Defense Protection Agent v8.0”.

The “Panda Adaptive Defense Protection Agent v8.0” is a software that executes on a target machine upon the operative system Windows. The application provides a protection mechanism to the machine in which it is installed based on the management of the applications running on that device. It does it by recording behavioural data of other applications and then classifying them based on a correlation analysis with the aid of the developer web services.

Developer/manufacturer:	Panda Security, Edificio Miribilla Santiago de Compostela 12, 48003 Bilbao
Sponsor:	Panda Security
Certification Body:	Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
ITSEF:	“Applus Laboratories”.
Protection Profile:	None.
Evaluation Level:	EAL2+ALC_FLR.1.
Evaluation end date:	23/03/2018.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory “Applus Laboratories” assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product “Panda Adaptive Defense Protection Agent v8.0”, a positive resolution is proposed.

TOE SUMMARY

The TOE is composed of the Protection Agent, which implements the main TOE security functionality (process interception, risk analysis, audit functionality, etc), and the NDKAPI DLLs, which provide an ease-of-use API, using an encrypted channel, to other Panda processes in order to receive notifications and user logs from the Protection Agent and to manage the Protection Agent itself.
The NDKAPI DLL authenticates the loading process so that only allowed processes like the Management Agent (which receives information from the cloud management console) and the Local Console can interact with the Protection Agent.
The Protection Agent place several user and kernel hooks in the operating system to allow monitoring of every launched process and will allow or deny the execution of a process or functionality based on:

- Information obtained from the Collective Intelligence through an HTTPS connection, which has previously received the monitored processes actions.
- Malware signatures

- Exploit signatures
- Access to malicious website
- Process behaviour local risk analysis
- Whitelisted websites (Panda maintains a list of phishing or malware urls so they are blocked unless whitelisted)
- Device control configuration
- Configured risk analysis operation mode

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R4 and the CEM v3.1 R4.

Class	Family/Component
ASE: Security Target Evaluation	ASE_INT.1. ST Introduction ASE.CCL.1. Conformance claims ASE_SPD.1. Security problem definition ASE_OBJ.2. Security objectives ASE_ECD.1. Extended component definition ASE_REQ.2. Derived security requirements ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture ADV_FSP.2. Functional specification ADV_TDS.1. TOE design
AGD: Guidance documents	AGD_OPE.1. Operational user guidance AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities ALC_CMS.2. CM Scope ALC_DEL.1. Delivery ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage ATE_FUN.1. Functional tests ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria v3.1 R4:

Class	Component
FAU: Security audit	FAU_ARP.1. Security alarms FAU_GEN.1. Audit data generation FAU_SAA.1. Potential violation analysis

	FAU_SAR.1. Audit review FAU_SAR.3. Selectable audit review
FDP: User data protection	FDP_SDI.1. Stored data integrity monitoring
FIA: Identification and authentication	FIA_UAU.2. User authentication before any action FIA_UID.2. User identification before any action
FMT: Security management	FMT_MOF.1. Management of security functions behavior FMT_SMF.1. Specification of Management Functions FMT_SMR.1. Security roles
FPT: Protection of the TSF	FPT_ITC.1. Inter-TSF confidentiality during transmission FPT_ITI.1. Inter-TSF detection of modification FPT_ITT.1. Basic internal TSF data transfer protection FPT_TST.1. TSF testing

IDENTIFICATION

Product: "Panda Adaptive Defense Protection Agent v8.0"
Security Target: "Panda Adaptive Defense Protection Agent Security Target v3.0, de 23/02/2018"
Protection Profile: None.
Evaluation Level: Common Criteria v 3.1 R4 EAL2+ALC_FLR.1

SECURITY POLICIES

The use of the product "Panda Adaptive Defense Protection Agent v8.0" shall implement a set of security policies assuring the fulfilment of different standards and security demands.
The detail of these policies is documented in the Security Target, section 3.4.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.5.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product "Panda Adaptive Defense Protection Agent v8.0", although the agents implementing attacks have the attack

potential according to the “Basic” attack potential of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.
For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.
The threats covered by the security properties of the TOE are categorized below.

The detail of these threats is documented in the Security Target, section 3.3.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The detail of these security objectives for the TOE operational environment is documented in the Security Target, section 4.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is composed of two subsystems:

- The Protection Agent Core Subsystem that conforms most of the TOE and executes outside user-space.
- The NDK API ADLLs Subsystem that encompasses the separate part of the TOE that connects to the users in the user-space.

PHYSICAL ARCHITECTURE

The TOE is installed in a desktop workstation or server and automatically provides the security features it is designed for.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Panda Adaptive Defense Protection Agent Operational Guidance 2.0
- Panda Adaptive Defense Protection Agent Preparative Guidance 3.0
- Panda Adaptive Defense Protection Agent Functional Specification 2.0
- Adaptive Defense 360 Guide for network administrators 2.3.5
- Nano Development Kit (NDK) API 2.2.0.2

All guidance documentation is distributed as PDF files except for the las item, the NDK API documentation, which is a package consisting of the generated doxygen documentation.

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests previously passed in the developer premises. Likewise, he has selected and repeated all of the developer functional tests in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a test for each of the security functions of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and, in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product “Panda Adaptive Defense Protection Agent v8.0” it is necessary the disposition of the following software components:

- Windows 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit).
- Windows Server 2008(32-bit and 64-bit) , Windows Server 2008 R2 (32-bit and 64-bit), Windows Server 2012 and Windows Server 2012 R2
- VMWare ESX 3.x, 4.x, 5.x and 6.x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x, 9.x, 10.x, 11.x and 12.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008, 2008R2, 2012, 2012R2 and 2016 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer and XenApp 5.x and 6.x

Regarding the hardware components, the TOE has to run on devices (usually personal computer systems) with the following minimum requirements:

- Processor: Pentium 300 MHz or equivalent
- RAM: 256MB
- Space for installation: 650MB
- Browser: Internet Explorer 6.0 or later

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

Physical machine: Intel i5 at 3.2 GHz and 12 GB of DDR3 RAM.
Operative system: Windows 10 version 1703 with Internet Explorer 11.

EVALUATION RESULTS

The product “Panda Adaptive Defense Protection Agent v8.0” has been evaluated against the Security Target: “Panda Adaptive Defense Protection Agent Security Target v3.0, de 23/02/2018”.

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory “Applus Laboratories” assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE works together with the Panda Cloud Servers. It makes a constant connection between the servers and the TOE. In order to sanitize some problems related with communication the laboratory recommends to analyse the protocols used between the end points, using whenever is possible, the best transport protocol (TLS 1.2) rather than working on client’s demand.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product “Panda Adaptive Defense Protection Agent v8.0”, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.
[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.
[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.
[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.
[CCDB-2006-04-004] ST sanitising for publication, April 2006.

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- "Panda Adaptive Defense Protection Agent Security Target v3.0, de 23/02/2018"

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including

EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.
The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.