MetaClean for Outlook

Security Target

V0.9

25/11/2024

Created by

Version control

Version	Comment	Date
0.1	Initial draft version	26/10/2023
0.2	Changes after CPSTIC comments	22/01/2024
0.3	Changes after CPSTIC comments	20/03/2024
0.4	Changes after CPSTIC comments	10/04/2024
0.5	Internal review	11/06/2024
0.6	Clarification in ACT.4 requirement	18/06/2024
0.7	TOE version updated	30/08/2024
0.8	Changes after Laboratory testing	24/09/2024
0.9	Changes after Laboratory non-conformities	25/11/2024

Table of contents

1 Introduction 4

1.1 Sponsor, TOE and evaluation information 4

1.2 Methodology and evaluation criteria 5

2 TOE description 6

2.1 TOE Functional description 6

2.2 Identification of the TOE secure use, installation and configuration guides 8

2.3 TOE usage description 9

2.3.1. Installation and first deployment 9

2.3.2. Additional metadata detection settings 9

2.3.3. Integration with Dashboard 9

2.3.4. TLS Cipher suites configuration 9

2.3.5. TLS Elliptic curves configuration 9

2.3.6. Safe uninstallation 9

2.3.7. Add-ins disabling 10

3 Operational environment 11

3.1 Operational environment description 11

4 Security Problem Definition 12

4.1 Operational Environment Assumptions 12

4.2 Assets to protect 13

4.3 Threat descriptions 14

4.3.1. Traceability threats/security requirements 15

5 Security Functional Requirements 16

5.1 SF. Trusted Administration 16

5.2 SF. Trusted Communications Channels 17

5.3 SF. Trusted Installation and Updates 18

5.4 SF. Audit 19

5.5 SF. Cryptography 20

5.6 SF. Anti-exploitation Capabilities 21

5.7 SF. Metadata Protection 22

6 Acronyms 23

7 Document references 24

8 Annex 25

8.1 Third party libraries used by the TOE 25

1 Introduction

This document is the Security Target for **MetaClean for Outlook**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Sponsor, TOE and evaluation information

Applicant data	Adarsus Technologies S.L.
Developer data	Adarsus Technologies S.L.
Contact information of developer	Guzmán Rejón (guzman.rejon@adarsus.com) +34 699919555 Avenida Secundino Zuazo, 95. C.P: 28055
TOE name	MetaClean for Outlook
TOE version	v.5.2.1
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE secure use, installation and configuration guides*
Taxonomy according to CCN-STIC-140	N/A

1.2 Methodology and evaluation criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE description

2.1 TOE Functional description

The TOE is a software solution that addresses file metadata management on mail attachments. It can be used for automatically deleting or modifying metadata with previous defined values, from outgoing documents in Microsoft Outlook. In order to modify metadata instead of deleting it, it is necessary to enter in the general configuration the specific data you want to modify instead of the metadata in question.

MetaClean for Outlook is a plugin for the Microsoft Outlook email desktop client that allows to automatically process the metadata of email attachments. The main functionality of the TOE is implemented by the TOE Java program called **MetaCleanMail.exe**, which deletes or modifies metadata.

The metadata processing is implemented following the next steps:

1. **Attachment inspection process:** the attachment file format is examined and if it matches with the general configuration, the file is selected to be processed by the TOE.
2. **Temporary disk copy:** attachments that meet the general configuration are copied to a temporary drive disk before metadata erasure/modification processing is performed.
3. **Invoke to MetaCleanMail.exe:** this TOE program is invoked to remove or modify metadata in the attached files. The process is synchronous and the metadata is processed during the execution of MetaCleanMail.exe and the email is not sent until the TOE has finished.

The general configuration of this solution is performed via Outlook Client interface. This solution performs the metadata processing before sending the email to the determined server that the client uses.

The TOE allows its integration with a large list of type of files (https://www.adarsus.com/formatos-de-ficheros-compatibles-con-metaclean/). A selection of them will be tested in the evaluation, which in turn are the most common ones, in order to test the correct performance of the TOE functionalities: PDF, Signed PDF, PNG, GIF, JPG, AVI, MP4, MOV, MP3, DOC, DOCX, ODT, PPT, PPTX, ODP, XLS, XLSX, ODS, ZIP and 7Z. The TOE will only process metadata from files whose format matches one of the above, with a correct extension, and which are not password protected.

In relation with the specific functionalities of the TOE, it can be defined the following:

- **SF. Trusted Administration:** The TOE does not present any role, as it is a final user solution managed by the user of the operating system in which it is installed and it does not need a differentiation of roles. The final user is able to perform different management functionalities such as select which documents will be analyzed by the TOE in search of metadata.
- **SF. Trusted Communication Channels:** The single communication channel is the one between the TOE and MetaClean Dashboard. This communication channel will be protected by HTTP over TLS v1.2 or v1.3.
- **SF. Trusted Installation and Updates:** The TOE offers the possibility of checking the current version. The TOE is able to verify the integrity of the update packages using SHA-256.
- **SF. Audit:** The TOE generates audit records when the general configuration is changed. The generated records will be deployed in the form that contain at least information related with

date and time, type of configuration that the user changed, result of the event and the user producing the event (if applies). This audit records are stored in itself. In addition, when the audit storage is full, the TOE overwrites the oldest audit logs.

- **SF. Cryptography:** The TOE uses cryptographic functions, algorithms and protocols which are included among those authorized for ENS Medium Category according to the CCN-STIC-807 guide.
- **SF. Anti-exploitation Capabilities**: The TOE shall not request the allocation of any explicit system memory address, or allocate memory with simultaneous write and execute permissions.
- **SF. Metadata Protection:** The TOE monitors attachments in outgoing emails before they are sent, being able to analyze different document formats.

2.2 Identification of the TOE secure use, installation and configuration guides

The following table lists the documents and user's guides necessary to carry out the configuration of the TOE properly:

Document's type	Document's name	Document's version (update-history-date)
Installation and configuration guide	MetaClean for Outlook Manual de Instalación y Operación -Sistemas Operativos Windows-	SHA-256 FCD2F8E7560CB204BB57E1C594F82AACAC92B5FD95914766CB34A79FF3471A47

2.3 TOE usage description

2.3.1. Installation and first deployment

The user will receive a ZIP file containing an installer executable file (*MetaClean for Outlook.msi*) which shall be executed in order to start the installation. The rest of configuration steps are described in the *MetaClean for Outlook Manual de Instalación y Operación -Sistemas Operativos Windows-* document, declared in *2.2 Identification of the TOE secure use, installation and configuration guides* section.

2.3.2. Additional metadata detection settings

On the other hand, in order to achieve a correct detection of all types of metadata detected in attached files, it is necessary to perform an additional configuration step. It is necessary to enable "Signed Included" and "Image, Audio and Video" in the Outlook Client used in the platform where the TOE is installed.

2.3.3. Integration with Dashboard

Although the TOE foresees two use cases, with and without integration with MetaClean Dashboard, the use case evaluated will be the one integrated with Dashboard, so integration with it will be required to be in compliance with security requirements.

2.3.4. TLS Cipher suites configuration

Perform the following configurations in order to configure the elliptic curves offered by the TOE in the key exchange of its TLS communications:

- Execute "Win + R" and type "gpedit.msc" with platform administrator privileges.
- Go to *Computer Configuration > Administrative Templates > Network > SSL Configuration Settings*.
- Configure "SSL Cipher Suite Order" parameter with the following value: "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256".

2.3.5. TLS Elliptic curves configuration

Perform the following configurations in order to configure the elliptic curves offered by the TOE in the key exchange of its TLS communications:

- Execute "Win + R" and type "gpedit.msc" with platform administrator privileges.
- Go to *Computer Configuration > Administrative Templates > Network > SSL Configuration Settings*.
- Configure "ECC Curve Order" parameter with the following value: "NistP256,NistP384,NistP521".

2.3.6. Safe uninstallation

Since TOE, when uninstalled, by default leaves traces of two binaries, the configuration set out in the *MetaClean for Outlook Manual de Instalación y Operación -Sistemas Operativos Windows-* guide on page 15 shall be carried out whenever the TOE is uninstalled.

2.3.7. Add-ins disabling

The TOE is confident that disabling the plugin will only be done by administrator users. In order to comply with this, it is necessary to specifically configure the "Com Add-ins" section within the Outlook client by following the steps specified in the guide *MetaClean for Outlook Manual de Instalación y Operación -Sistemas Operativos Windows-* guide on page 14. After entering this configuration, no user will be able to disable the plugin via this interface.

Apart from these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in section *5 Security Functional Requirements* of this document beyond the steps in the TOE guide.

3 Operational environment

3.1 Operational environment description

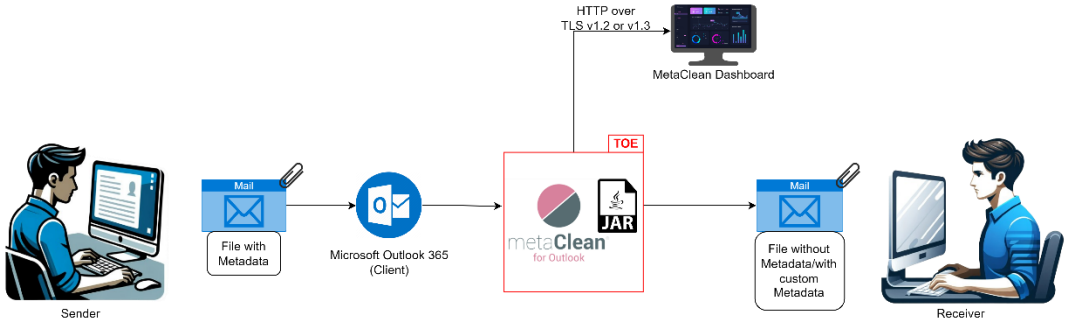

Figure 1: Operational environment.

- **Sender**: The user who sends an email with attached documents that will be analyzed.
- **Microsoft Outlook 365 (client)**: Outlook is an email and personal information management software developed by Microsoft, used for managing emails, calendars, tasks, and contacts in a unified platform. This component is where the plugin MetaClean for Outlook is installed. For the present evaluation, the OS where Microsoft Outlook is deployed is Windows 10 version 22H2 and KB5028166 security patch.
- **MetaClean Dashboard:** An internal service of MetaClean, whose objective is to update the MetaClean for Outlook plugin.
  For the present evaluation, the version of this component of the operational environment is 1.3.0 over Ubuntu 22.04.3.
- **Receiver:** The user who receives the email with attached documents that have been analyzed and whose metadata has been removed or overwritten following the general configuration.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.TRUSTED PLATFORM	The product shall run on a trusted platform, including the operating system or any runtime environment on which it is used. The platform versions shall be those recommended by the developer, being admissible but not recommended versions that are in extended support with security patch support and, in any case, unsupported versions. The product storage (binaries, configuration files, audit logs and output files) shall be protected by the trusted platform.
A.PERIODIC UPDATES	The product software will be updated as updates are released to correct known vulnerabilities.
A.TRUSTED PLATFORM ADMINISTRATION	Platform administrator shall be fully trusted members of the platform provider organization and have the best security interest of the deployed product. They shall be properly trained and free of malicious intent of conflict of interest in the management of the platform where the TOE is deployed.
A.TRUSTED PLATFORM USER	Platform users shall be fully trusted members of the platform provider organization and have the best security interest of the deployed product. They shall be properly trained and free of malicious intent of conflict of interest in the use of the platform where the TOE is deployed.

4.2 Assets to protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.COMMUNICATIONS	TOE’s communications, established between its own components and with its operational environment.	Confidentiality, Integrity and Authenticity.
AS.UPDATES	Updates that may affect TOE’s configuration and functionality.	Integrity.
AS. PSS	General configuration and audit data.	Confidentiality and Integrity.
AS.METADATA	Metadata information in the files processed or that will be processed by the TOE.	Confidentiality.

4.3 Threat descriptions

Threat	Description	Assets
T.MU MALICIOUS UPDATES	An attacker can perform a malicious update that weakens the product's security features.	*AS.UPDATES*
T.COM UNATHORIZED COMMUNICATION PROTOCOLS	Use of unauthorized protocols that allow an attacker to compromise the integrity and confidentiality of critical product communications.	*AS.COMMUNICATIONS*
T.CRYPTO – WEAK CRYPTOGRAPHIC MECHANISMS	Use of cryptographic mechanisms or weak key lengths in the product that allow an attacker to compromise it, primarily through brute force attacks.	*AS.COMMUNICATIONS* *AS. UPDATES*
T.AUD – NO DETECTED ACTIVITY	An attacker may attempt to gain access, change or modify the product's security features without the administrator's knowledge.	*AS.PSS*
T.INT – SOFTWARE INTEGRITY COMPROMISE	An attacker may attempt to compromise the integrity of the product through unprivileged software running on the same platform as the product.	*AS.PSS*
T.MEDXF – METADATA EXFILTRATION	When transferring documents between different business units of the same corporation or between different corporations, sensitive internal information contained in document metadata could be exfiltrated in an unauthorized way. This information may have been generated by users or automatically and it could include names of business members, business units, usernames, software tools or hardware systems used in an organization.	*AS.METADATA*
T.MAN MANIPULATION ATTACKS	An attacker may attempt to modify the general configuration of the TOE through manipulation attacks in the administration interface, misleading the user to change the general configuration.	*AS.PSS*

4.3.1. Traceability threats/security requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.MU	T.COM	T.CRYPTO	T.AUD	T.INT	T.MEDXF	T.MAN
ADM.2							X
COM.1		X	X				
COM.2		X					
ACT.1	X						
ACT.2	X		X				
ACT.4	X						
ACT.5	X						
AUD.1				X			
AUD.2				X			
AUD.4				X			
AUD.5				X			
CIF.1		X	X				
EXP.1					X		
MTD.1						X	
MTD.4						X	

5 Security Functional Requirements

5.1 SF. Trusted Administration

Requirement	Description

ADM.2	The TOE shall be able to locally perform the following management functionalities through the Outlook Client interface:
	• MetaClean Power ON/OFF.
	• Select the type of files (that are not password protected) that will be analyzed in search of metadata:
	  ○ PDF.
	  ○ Signed PDFs.
	  ○ Microsoft Office.
	  ○ Open Office.
	  ○ Image, Audio and Video.
	  ○ Files inside compression format files (ZIP, 7Z).
	• Select if the metadata will be removed or customed.
	• Specify excluded domains.

5.2 SF. Trusted Communications Channels

Requirement	Description
COM.1	The TOE shall establish the following communication channel: • Communication between the TOE and MetaClean Dashboard using TLS v1.2 with secp256r1, secp384r1 and secp521r1 curves, and the following cipher suites: ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
COM.2	The communication channel in which the TOE communicates with MetaClean Dashboard shall be initiated by the TOE.

5.3 SF. Trusted Installation and Updates

Requirement	Description
ACT.1	The TOE shall provide the ability to query the current software version. Also, the TOE shall be able to initiates updates automatically and check for new updates available.
ACT.2	The TOE shall receive a JSON chain from MetaClean Dashboard with the URL to download the update and SHA-256 hash of the update. The TOE shall verify the integrity of the update before installing it comparing the Hash of the JSON chain and the Hash of the ZIP. The update will start only if the hash provided by the Dashboard and the TOE calculated hash are the same.
ACT.4	The TOE shall not leave trace of its installation when is removed from the Operating System, apart from its configuration and output or audit files.
ACT.5	The TOE shall not download or modify its own binary code.

5.4 SF. Audit

Requirement	Description
AUD.1	The TOE shall generate the following audit records: • Change in product functionalities: ○ Select the type of files (that are not password protected) that will be analyzed in search of metadata: ✓ PDF. ✓ Signed PDFs. ✓ Microsoft Office. ✓ Open Office. ✓ Image, Audio and Video. ✓ Files inside compression format files (ZIP, 7Z). ○ Select if the metadata will be removed or customed. ○ Specify excluded domains.
AUD.2	Audit records shall contain at least the following information: • Date and time of the event. • Result of the event. • User producing the event (if applicable). • Type of configuration that the user changed.
AUD.4	The TOE shall be able to store the generated audit information in itself. It can be consulted in the file *MetaCleanforOutlook.log.*
AUD.5	The TOE shall rotate the MetaCleanforOutlook.log file at approximately 5MB size. Upon reaching five rotated files, it shall overwrite the oldest file.

5.5 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall exclusively use the cryptographic mechanisms authorized for ENS Medium Category according to the CCN-STIC-807 guide**:** • Cipher suites of the communication channel defined in **COM.1**. • Hash algorithm used to ensure the integrity of the updates defined in **ACT.2**

5.6 SF. Anti-exploitation Capabilities

Requirement	Description
EXP.1	When the TOE is running, it shall not request the allocation of any explicit system memory address, or allocate memory with simultaneous write and execute permissions.

5.7 SF. Metadata Protection

Requirement	Description
MTD.1	The TOE shall monitor attachments in outgoing email before they are sent and apply rules to files, such as, remove or modify with custom metadata. The process is synchronous and the metadata is processed during the execution of MetaCleanMail.exe, the email is not sent until the TOE is finished. When an attachment meets the general configuration is copied to a temporary drive disk before metadata erasure/modification processing.
MTD.4	The TOE shall remove and modify metadata files with the following formats that are not password protected: • PDF. • Signed PDFs. • Microsoft Office. • Open Office. • Files inside compression format files (ZIP, 7Z). On the other hand, in relation with Image, audio and video files, the TOE shall only provide the ability to remove metadata and not modify them.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
ENS	Esquema Nacional de Seguridad (National Security Scheme).
LINCE	Certificación Nacional Esencial de Seguridad
ST	Security Target – Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación (Security of Information and Communication Technologies).
TOE	Target Of Evaluation - Objeto a evaluar.
TLS	Transport Layer Security
URL	Uniform Resource Locator
HTTPS	Hypertext Transfer Protocol Secure
PDF	Portable Document Format
OS	Operating System
AES	Advanced Encryption Standard
GCM	Galois/Counter Mode
SHA	Secure Hash Algorithm
ECDHE	Elliptic-curve Diffie-Hellman
RSA	Rivest-Shamir-Adleman
JSON	JavaScript Object Notation

Table 1 *Abbreviations*

7 Document references

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Methodology for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2004	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Technical Report template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022 (National Security Scheme employment cryptology, May 2022).

Table 2 List of document references

8 Annex

8.1 Third party libraries used by the TOE

Library Name	Version	Vendor
org.bouncycastle.bcmail	1.38.0	BouncyCastle.org
org.bouncycastle.bcprov	1.38.0	BouncyCastle.org
org.bouncycastle.bctsp	1.38.0	BouncyCastle.org
Apache Commons Codec	1.10	The Apache Software Foundation
Apache Commons IO	2.5	The Apache Software Foundation
Commons Lang	3.1	The Apache Software Foundation
org.dom4j	1.5.1	MetaStuff Ltd.
Simple Java API for ODF	0.7-incubating	The Apache Software Foundation
ODFDOM	0.8.8-incubating	The Apache Software Foundation
jakarta.activation	2.0.0	Eclipse Foundation
jakarta.xml.bind-api	3.0.0	Eclipse Foundation
org.apache.xerces.impl.Version	2.9.1	Apache Software Foundation
org.apache.xmlbeans	2.6.0	Apache Software Foundation
Apache POI	3.15	Apache Software Foundation