Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1546

(01/2014)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange concernant les événements/les incidents/l'heuristique

Enumération et caractérisation des attributs de logiciels malveillants

Recommandation UIT-T X.1546

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	**X.1540–X.1549**
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1546

Enumération et caractérisation des attributs de logiciels malveillants

Résumé

Le langage d'énumération et de caractérisation des attributs de logiciels malveillants (MAEC) comprend des énumérations d'attributs de logiciels malveillants et un comportement qui fournit un vocabulaire commun. Ces énumérations sont à des niveaux d'abstraction différents: données observables de bas niveau, comportements de niveau intermédiaire et taxonomies de haut niveau. La Recommandation UIT-T X.1546, qui est la version initiale du langage MAEC, porte essentiellement sur la création de l'énumération des attributs de logiciels malveillants de bas niveau et s'appuie sur des travaux analogues, encore peu nombreux, déjà effectués dans ce domaine. En conséquence, cette Recommandation permettra de caractériser dans un premier temps les types de logiciels malveillants les plus répandus, comme les chevaux de Troie, les vers informatiques et les outils de dissimulation d'activité (rootkits), mais elle s'appliquera à terme aux types de logiciels malveillants plus spécifiques.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1546	24-01-2014	17	11.1002/1000/12038

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

La Recommandation UIT-T X.1546 relative à l'utilisation de l'énumération et des caractéristiques des attributs de logiciels malveillants (MAEC) est une norme communautaire internationale en matière de sécurité de l'information qui vise à promouvoir des contenus de sécurité ouverts et publiquement accessibles, sur les logiciels et les comportements malveillants. Cette Recommandation a également pour objet de normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité pouvant être utilisés pour contrôler et gérer les dispositifs de protection contre les logiciels malveillants. Le langage MAEC sert à coder des renseignements précis sur les logiciels malveillants.

Le langage MAEC vise: 1) à améliorer la communication de personne à personne, de personne à outil, d'outil à outil et d'outil à personne en ce qui concerne les logiciels malveillants; 2) à réduire tout risque de double emploi dans les activités menées par les chercheurs pour analyser les logiciels malveillants; et 3) à accélérer la mise en place de contre-mesures en offrant la possibilité de tirer parti des solutions apportées aux problèmes de logiciels malveillants observés précédemment. L'analyse des menaces, la détection des intrusions et la gestion des incidents sont des processus qui permettent de traiter les cybermenaces sous toutes leurs formes. Le langage MAEC, grâce au codage uniforme des attributs des logiciels malveillants qu'il permet, constitue un format normalisé pour l'intégration d'informations décisionnelles concernant les logiciels malveillants lors de ces processus.

Les logiciels malveillants, égalements appelés "maliciels", existent sous diverses formes depuis l'apparition du premier virus informatique en 1971. Ils sont aujourd'hui à l'origine d'une multitude d'activités délictueuses, qui vont de la plupart des courriers électroniques non sollicités (spams) distribués par l'intermédiaire de réseaux "botnets" au vol de données sensibles par le biais d'attaques d'ingénierie sociale ciblées. Agissant en effet comme agent autonome au nom de l'attaquant, un logiciel malveillant est capable d'effectuer toute opération pouvant être exprimée sous la forme d'un code et représente à ce titre une menace considérable pour la cybersécurité.

La protection des systèmes informatiques contre les logiciels malveillants constitue donc actuellement pour les organisations et les particuliers l'une des préoccupations les plus importantes en matière de sécurité de l'information, dans la mesure où une seule instance de logiciel malveillant non détectée peut endommager des systèmes et compromettre des données. Ce risque d'infection ne disparaît pas totalement en cas de déconnexion d'un réseau informatique, comme en témoigne l'exemple de logiciels malveillants qui ont recours à des clés USB comme vecteur d'insertion. C'est pourquoi la plupart des mesures prises à ce jour pour lutter contre les logiciels malveillants ont essentiellement consisté à empêcher ces logiciels de produire leurs effets dommageables grâce à la détection rapide.

Il existe actuellement plusieurs méthodes couramment utilisées pour détecter les logiciels malveillants, qui reposent principalement sur les signatures physiques et l'analyse heuristique. Ces méthodes sont efficaces en raison de leur portée circonscrite, encore qu'elles présentent par nature certains inconvénients, par exemple le fait que les signatures ne permettent pas de lutter contre les infections résultant de l'exploitation de vulnérabilités inconnues ("zero-day"), les attaques ciblées, les virus polymorphes et d'autres formes de logiciels malveillants. De même, il arrive que la détection heuristique permette de détecter de manière générique certains types de logiciels malveillants, mais ne décèle pas ceux pour lesquels elle ne dispose pas de mécanismes adaptés, par exemple les outils rootkits au niveau du noyau. En conséquence, il serait plus prudent de dire que l'on ne peut s'en remettre exclusivement à ces méthodes, aussi utiles soient-elles, pour faire face à la profusion actuelle de logiciels malveillants.

L'énumération et la caractérisation des attributs de logiciels malveillants (MAEC) visent à éliminer l'ambiguïté et l'inexactitude qui existent actuellement dans les descriptions de logiciels malveillants et à réduire la dépendance à l'égard des signatures. Ainsi, MAEC a pour but d'améliorer la communication de personne à personne, de personne à outil, d'outil à outil et d'outil à personne en ce qui concerne les logiciels malveillants, de réduire tout risque de double emploi dans les activités menées par les chercheurs pour analyser les logiciels malveillants et d'accélérer la mise en place de contre-mesures en offrant la possibilité de tirer parti des solutions apportées aux problèmes de logiciels malveillants observés précédemment. Comme nous le verrons sur les figures ci-après, le langage MAEC permet la corrélation, l'intégration et l'automatisation pour le partage d'informations structurées sur les logiciels malveillants sur la base d'attributs tels que les comportements, les effets parasites et les configurations des attaques.

Ainsi qu'il ressort de la Figure 1, MAEC comprend un modèle de données qui s'étend sur plusieurs schémas interconnectés, représentant ainsi la grammaire qui définit le langage. Ces schémas permettent de générer différentes formes de produits MAEC, que l'on peut considérer comme des utilisations spécifiques de la grammaire précitée.

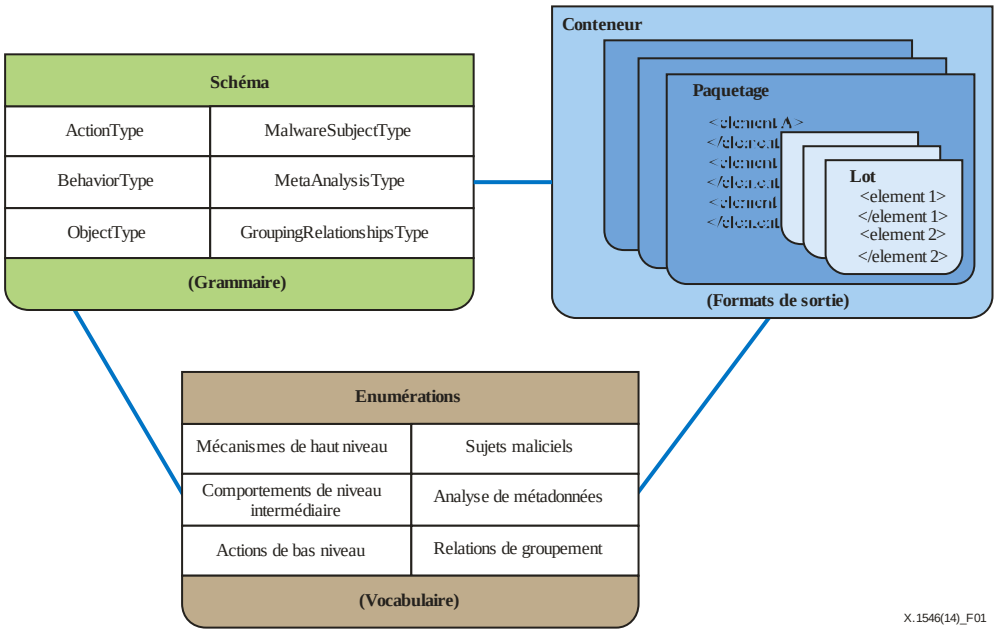

Figure 1 – Aperçu de haut niveau du langage MAEC

Les schémas du conteneur MAEC, du paquetage MAEC et du lot MAEC s'appliquent à différents cas de figure et saisissent de ce fait différents types d'informations relatives aux logiciels malveillants.

Le langage MAEC se rapporte à la fois au langage d'expression cyberobservable (CybOX) et au format d'échange de métadonnées sur les logiciels malveillants de l'IEEE ICSG (MMDEF).

Le langage CybOX est un langage normalisé permettant la spécification, la saisie, la caractérisation et la communication d'événements ou de propriétés à états qui sont observables dans le domaine opérationnel. Les données cyberobservables s'appliquent à de nombreux domaines: évaluation et caractérisation des menaces (configurations d'attaque détaillées), caractérisation des logiciels malveillants, gestion opérationnelle des événements, établissement de journaux, cyberperception de la situation, intervention en cas d'incident, expertise numérique et échange de renseignements sur les cybermenaces.

Dans le langage CybOX, presque tous les domaines sont facultatifs, si bien que l'on peut utiliser ce qui est approprié sans tenir compte du reste. Le langage CybOX peut être utilisé pour spécifier et caractériser une large gamme de cyberobjets et pour définir des compositions relationnelles et logiques d'objets, d'actions, d'événements ou de données observables multiples.

La caractérisation des logiciels malveillants à l'aide de MAEC s'appuie sur le mécanisme commun (structure et contenu) que fournit le langage CybOX pour examiner des données cyberobservables dans la gamme complète des scénarios d'utilisation. Alors que MAEC fournit un contexte d'analyse, des indicateurs, des comportements et des mécanismes, le langage CybOX fournit des actions générales et des objets utilisés dans le cyberdomaine opérationnel. Une donnée cyberobservable est un *événement mesurable* ou une *propriété à états* du cyberdomaine. Comme exemples d'événements mesurables, on peut citer la création de clés de référentiel, la suppression de fichiers et la réception d'une demande HTTP GET. Comme exemple de propriétés à états, on citera le hâchage MD5 d'un fichier, la valeur d'une clé de référentiel et l'existence d'un mutex (*mutual exclusion object*).

MAEC importe et élargit l'objet et l'action du langage CybOX. On trouvera sur la Figure 2 un aperçu extrêmement simplifié du schéma CybOX. Les composants CybOX qu'utilise MAEC sont indiqués en vert.

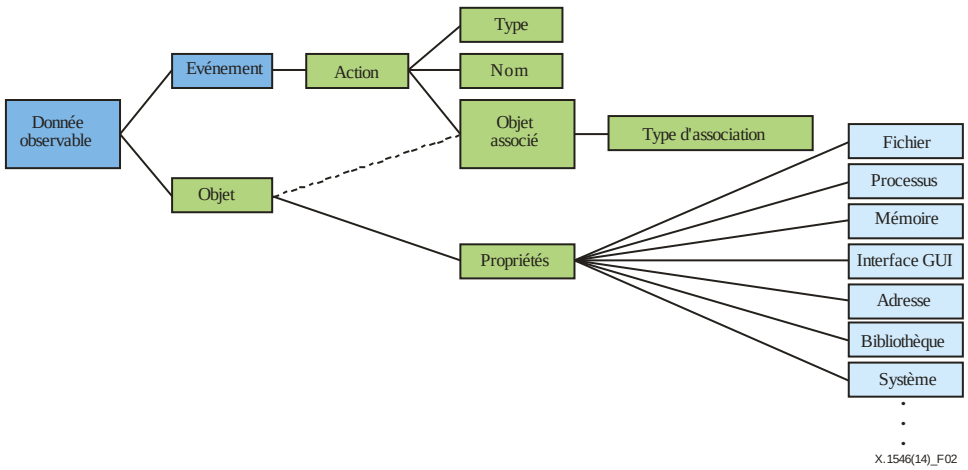

Figure 2 – Aperçu simple du schéma d'expression cyberobservable (CybOX)

La structure des propriétés du langage CybOX est une ébauche abstraite pour divers schémas de types d'objets prédéfinis (par exemple fichier, processus, mémoire) qui peuvent être instanciés à sa place. Les schémas des propriétés, indiqués en bleu clair, sont maintenus indépendamment du schéma principal CybOX.

Le format MMDEF est actuellement mis au point par le groupe ICSG (*Industry connections security group*) de l'IEEE (*Institute of electrical and electronics engineers*). Le schéma d'origine avait été élaboré principalement sous la direction d'un groupe de fournisseurs de produits antivirus (AV), afin de disposer d'un moyen de compléter par des métadonnées additionnelles les échantillons de logiciels malveillants partagés. En outre, ce format permet la caractérisation de certaines fonctions caractéristiques statiques comme le hâchage et les noms de fichier, ainsi que de certaines caractéristiques comportementales de base.

La communauté chargée de la sécurité de l'information contribue à la mise au point de MAEC en participant à la création du langage MAEC sur les listes de discussion et le portail de collaboration des concepteurs de MAEC et en intégrant le langage MAEC dans leurs outils et fonctionnalités de répertoire. La communauté MAEC comprend des représentants d'un large éventail d'entreprises, d'établissements universitaires et d'organisations gouvernementales du monde entier, qui supervisent le langage MAEC ainsi que les services et outils MAEC par l'intermédiaire du répertoire MAEC

publiquement accessible et collaborent dans ce domaine. Par conséquent, MAEC tient compte des idées, mais aussi des compétences spécialisées de l'éventail de professionnels le plus large possible dans le domaine de l'analyse et de la prévention des logiciels malveillants.

La présente Recommandation a été élaborée en collaboration avec la MITRE Corporation, étant donné qu'il est important d'assurer, dans la mesure du possible, la compatibilité technique entre la Recommandation UIT-T X.1546 et la version 1.1 de la norme intitulée "Prescriptions et recommandations concernant la compatibilité MAEC", publiée le 7 juillet 2013 [https://maec.mitre.org/compatible/Requirements_for_MAEC_Compatibility_V1.1.pdf].

Recommandation UIT-T X.1546

Enumération et caractérisation des attributs de logiciels malveillants

1 Domaine d'application

La présente Recommandation offre un moyen structuré de promouvoir des contenus de sécurité ouverts et publiquement accessibles sur les logiciels malveillants et les comportements des logiciels malveillants. Elle a également pour objet de normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité pouvant être utilisés pour contrôler et gérer les dispositifs de protection contre les logiciels malveillants.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[ISO/CEI 19757-3] ISO/CEI 19757-3:2006, *Technologies de l'information – Langages de définition de schéma de documents (DSDL) – Partie 3: Validation de règles orientées – Schematron*.

[W3C XML Schema] W3C XML Schema Part 2 (2004), *W3C XML Schema Part 2: Datatypes, Second Edition*. <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 propriétaire [b-UIT-T X.1520]: détenteur (personne réelle ou entreprise) qui est responsable de la capacité.

3.1.2 utilisateur [b-UIT-T X.1520]: consommateur ou consommateur potentiel de la capacité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 capacité: fonction(s) spécifique(s) d'un produit, d'un service ou d'un répertoire.

3.2.2 résultats de la vérification de capacité: données représentant les résultats de la vérification d'adoption correcte.

3.2.3 contenu: tout type d'entité relative à l'énumération et aux caractéristiques des attributs des logiciels malveillants (MAEC), y compris les documents au format de sortie MAEC ainsi que les éléments/types intégrés.

3.2.4 vérification d'adoption correcte: processus permettant de déterminer si un outil a correctement mis en oeuvre MAEC.

3.2.5 groupe MAEC: type normalisé de donnée de sortie MAEC permettant de saisir toutes les caractéristiques provenant de l'analyse pour une seule instance de logiciel malveillant, y compris tous les comportements ou toutes les actions MAEC observés et tous les objets MAEC connexes.

3.2.6 conteneur MAEC: type normalisé de donnée de sortie MAEC permettant de saisir un ou plusieurs paquetages MAEC.

3.2.7 format de sortie MAEC: l'un des trois types normalisés de données de sortie MAEC, y compris le conteneur, le paquetage ou le lot MAEC.

3.2.8 paquetage MAEC: type normalisé de donnée de sortie MAEC permettant de caractériser toutes les données connues pour un ou plusieurs sujets de logiciels malveillant, y compris les caractéristiques provenant de leur analyse (par l'intermédiaire de lots MAEC) et toute analyse associée ou d'autres métadonnées.

3.2.9 instance de logiciel malveillant: exemple spécifique de logiciel malveillant.

3.2.10 élément de logiciel malveillant: comportement, attribut, exploitation, charge utile, etc., qui se rapporte à une instance de logiciel malveillant spécifique, à une famille de logiciels malveillants ou à une classe d'instances de logiciels malveillants.

3.2.11 schéma de logiciel malveillant: concept qui découle de l'existence d'un certain nombre d'attributs communs à un ensemble d'instances de logiciels malveillants (familles ou classes). Un même schéma de logiciel malveillant peut être associé à de nombreuses instances de logiciels malveillants différentes.

3.2.12 sujet de logiciel malveillant: entité MAEC qui saisit tous les détails concernant une seule instance de logiciel malveillant, y compris les métadonnées correspondantes de l'analyse, le contenu de l'analyse et les informations sur les relations.

3.2.13 produit: outil, service ou répertoire antilogiciels malveillants présentant une ou plusieurs capacités.

3.2.14 répertoire: recueil implicite ou explicite d'éléments ou de schémas de logiciels malveillants qui vient à l'appui d'un outil ou d'un service de création de contenus, par exemple une base de données ou des schémas de comportement, l'ensemble d'instances de logiciels malveillants analysées par un outil dit "bac à sable" (sandbox) ou le résultat composite d'un outil d'analyse binaire statique ou dynamique. Un répertoire peut également être un ensemble de documents au format de sortie MAEC.

3.2.15 examen: processus permettant de déterminer si une capacité est compatible avec MAEC.

3.2.16 autorité d'examen: entité qui procède à une vérification d'adoption correcte et est autorisée à reconnaître officiellement qu'une capacité est compatible avec MAEC.

3.2.17 échantillon d'examen: exemple de résultat d'une capacité fourni à une autorité d'examen afin d'être utilisé pour déterminer si la capacité est compatible avec MAEC.

3.2.18 version de l'examen: version datée de MAEC utilisée pour déterminer la compatibilité d'une capacité avec MAEC.

3.2.19 service: activité d'analyse, de détection ou de correction de logiciel malveillant mettant en œuvre une ou plusieurs capacités.

3.2.20 outil: application ou dispositif logiciel qui met en œuvre plusieurs fonctionnalités. Un outil analyse, détecte ou corrige un logiciel malveillant à l'aide de différentes méthodes, par exemple un outil d'analyse statique, un outil d'analyse dynamique, un scanner basé sur les signatures, un scanner basé sur l'analyse heuristique, etc. Un outil peut également procéder à la conception de contenu.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

AV antivirus

CybOX expression cyberobservable (*cyber-observable expression*)

ID identificateur

MAEC énumération et caractérisation des attributs de logiciels malveillants (*malware attribute enumeration and characterization*)

MMDEF format d'échange de métadonnées de logiciels malveillants (*malware metadata exchange format*)

SIM gestion des informations de sécurité (*security information management*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

L'abréviation MAEC est utilisée comme substantif dans la présente Recommandation.

6 Prescriptions de haut niveau

Les points suivants définissent les concepts, les rôles et les responsabilités associés à cinq capacités différentes, chacune ciblant un usage différent du langage MAEC, qui permettent une bonne utilisation de ce langage. Ces capacités permettent aux membres de la communauté MAEC de mieux comprendre comment un produit donné emploie le langage MAEC et est susceptible de répondre à leurs besoins.

Les prescriptions suivantes s'appliquent à toutes les capacités qui prennent en charge MAEC, quelle que soit la fonctionnalité particulière qui est mise en oeuvre (les prescriptions applicables aux fonctionnalités font l'objet du § 10 ci-dessous, intitulé "Prescriptions spécifiques en matière de compatibilité"). S'il est démontré qu'une capacité satisfait à toutes les prescriptions applicables, le propriétaire de la capacité recevra de l'autorité d'examen une attestation de reconnaissance officielle de la compatibilité avec MAEC.

Conditions préalables

6.1 Le propriétaire de la capacité doit être une entité juridique autorisée, c'est-à-dire un organisme ou un particulier avec un numéro de téléphone, une adresse électronique et une adresse postale valides.

6.2 Le propriétaire de la capacité doit accepter de se soumettre à toutes les prescriptions obligatoires en matière de compatibilité MAEC, notamment celles qui sont applicables à une fonctionnalité spécifique.

6.3 Le propriétaire de la capacité doit communiquer à l'autorité d'examen un point de contact technique qui est qualifié pour répondre aux questions concernant toute fonctionnalité de la capacité relative à MAEC et pour coordonner la préparation de la capacité en vue de la vérification d'adoption correcte.

6.4 Le propriétaire de la capacité doit faire parvenir à l'autorité d'examen un "Questionnaire relatif à la compatibilité MAEC" dûment rempli. Ce formulaire sera transmis au propriétaire de la capacité, une fois que le "Questionnaire relatif à la compatibilité MAEC" aura été traité par l'autorité d'examen.

6.5 Le propriétaire de la capacité doit collaborer avec l'autorité d'examen, afin de mettre à disposition le produit, le service ou le répertoire pour vérification d'adoption correcte.

6.6 Le propriétaire de la capacité doit faire en sorte que l'autorité d'examen ait librement accès aux éléments nécessaires à la vérification d'adoption correcte, notamment aux résultats des tests et/ou aux échantillons d'examen, afin de déterminer la conformité à toutes les prescriptions en matière de compatibilité.

6.7 En vue de recevoir une attestation de reconnaissance officielle de la compatibilité MAEC, le propriétaire de la capacité doit accepter d'apporter son appui à l'autorité d'examen lors du suivi des activités de test dans les cas où des types appropriés de fichiers seront échangés avec d'autres organismes afin d'essayer de prouver l'adoption correcte de leur capacité. Cette tâche sera gérée par l'autorité d'examen et n'exigera que des efforts raisonnables de la part de toutes les parties intéressées.

6.8 La capacité doit être accessible au public ou à un ensemble de consommateurs.

6.9 La capacité doit clairement indiquer la ou les versions de MAEC et le ou les schémas associés avec lesquels MAEC est compatible.

Divers

Les présentes prescriptions traitent des aspects divers de la compatibilité MAEC.

6.10 Si la capacité ne satisfait pas à toutes les prescriptions applicables indiquées ci-dessus (§ 6.1 à 6.9), le propriétaire de la capacité ne doit pas annoncer que la capacité est compatible avec MAEC.

6.11 Si la capacité ne satisfait pas aux prescriptions se rapportant expressément à sa fonctionnalité (définies aux § 10.1 à 10.27), le propriétaire de la capacité ne doit pas annoncer que la capacité est compatible avec MAEC.

6.12 Le propriétaire de la capacité doit obtenir l'approbation formelle de l'aurorité d'examen avant d'annoncer que la capacité est compatible avec MAEC.

7 Adoption correcte

Les présentes prescriptions traitent des erreurs relevées dans l'adoption correcte concernant la compatibilité MAEC, y compris, sans toutefois s'y limiter, des erreurs relatives à la validation du schéma et aux utilisations non valables de telle ou telle structure ou de tel ou tel élément MAEC.

7.1 Le propriétaire de la capacité doit prévoir un moyen permettant à l'utilisateur de soumettre les erreurs reflétant une adoption incorrecte qu'il a repérées dans l'utilisation de MAEC et dans un quelconque contenu MAEC fourni par la capacité.

7.2 Le propriétaire de la capacité doit prévoir un plan lui permettant de remédier aux erreurs reflétant une adoption incorrecte qui lui sont signalées.

7.3 Le propriétaire de la capacité doit rectifier les erreurs reflétant une adoption incorrecte qui lui sont signalées dans un délai raisonnable à compter du signalement initial de l'erreur.

8 Documentation

Les prescriptions suivantes s'appliquent à la documentation qui est fournie avec une capacité compatible avec MAEC.

8.1 La documentation relative à la capacité doit comporter une description succincte de MAEC et de la compatibilité avec MAEC, qui peut contenir des parties reprises mot pour mot de documents placés sur le site web de MAEC.

8.2 La documentation relative à la capacité doit clairement indiquer si elle s'applique à MAEC ainsi qu'aux schémas associés, y compris ceux qui sont importés suite aux efforts de la communauté concernant le langage d'expression cyberobservable (CybOX) et le format d'échange de métadonnées de logiciels malveillants (MMDEF), par l'intermédiaire des éléments ou des objets individuels CybOX qu'il ne prend pas en charge, ou par l'intermédiaire des éléments et des objets CybOX qu'il

prend en charge. Par exemple, si une capacité demande la reconnaissance officielle de la compatibilité avec MAEC en tant qu'outil ou service de création de contenus par analyse dynamique et qu'elle ne prend pas en charge l'objet du fichier CybOX et/ou les actions associées à l'objet du fichier CybOX, alors la documentation relative à la capacité doit expressément faire mention de cette incompatibilité.

8.3 La documentation relative à la capacité doit clairement indiquer la procédure qu'un utilisateur doit suivre pour présenter les erreurs reflétant une adoption incorrecte qu'il a repérées dans un quelconque contenu MAEC fourni par le produit.

8.4 Si la documentation accompagnant la capacité comprend un index, celui-ci doit contenir des références, en regard de la rubrique "MAEC", à la documentation relative à MAEC.

9 Validité

Les prescriptions ci-après découlent de la nécessité, pour les capacités compatibles avec MAEC, de travailler avec des documents valides. Ces prescriptions permettent de veiller à ce que les informations soient correctement formatées et à ce que la structure du document soit conforme au langage MAEC.

9.1 La capacité doit, au moyen de la validation selon le schéma XML du W3C (voir le document [W3C XML Schema]), valider tout contenu MAEC (tant produit que consommé) en le comparant à la version du langage MAEC à laquelle il a déclaré être conforme.

9.2 La capacité doit signaler à l'utilisateur toute erreur de validation dans le cadre du schéma XML du W3C.

9.3 La capacité doit, au moyen de la validation Schematron (voir la norme [ISO/CEI 19757-3]), valider tout contenu MAEC (tant produit que consommé) en le comparant à la version du langage MAEC à laquelle il a déclaré être conforme.

9.4 La capacité doit signaler à l'utilisateur toute erreur de validation dans le cadre du Schematron.

10 Prescriptions concernant des capacités spécifiques

Les prescriptions suivantes ne s'appliquent qu'à des capacités pour lesquelles les propriétaires de capacité cherchent à obtenir la compatibilité MAEC en ce qui concerne la fonctionnalité associée. Une capacité compatible avec MAEC doit fournir au moins une fonctionnalité spécifique: création de contenu, stockage de contenu ou consommation de contenu.

Création de contenu	Outil ou service qui crée ou facilite le processus de création de nouveaux fichiers MAEC, y compris ceux qui regroupent les documents existants au format de sortie MAEC en un seul fichier. Les sous-types suivants de la fonctionnalité de création de contenu sont définis: • Création de contenu par analyse statique: Outil ou service qui effectue une analyse statique d'une ou de plusieurs instances de logiciels malveillants à l'entrée et qui présente les résultats dans un document au format de sortie MAEC. • Création de contenu par analyse dynamique: Outil ou service qui effectue une analyse dynamique (c'est-à-dire une exécution instrumentale) d'une instance de logiciel malveillant à l'entrée et qui présente les résultats dans un document au format de sortie MAEC. • Création de contenu par outil ou service auteur: Outil ou service qui prend en charge la création et l'édition manuelles de documents au format de sortie MAEC.
Stockage de contenu	Répertoire de contenus MAEC mis à la disposition de la communauté (gratuitement ou non).

Consommation de contenu	Outil ou service qui accepte les documents au format de sortie MAEC à l'entrée et présente leur contenu à l'utilisateur ou les utilise pour exécuter une action (correction, gestion des informations de sécurité (SIM), etc.).

Création générale de contenu

Les présentes prescriptions s'appliquent à tous les outils et services qui se proposent de fournir un contenu MAEC en sortie.

10.1 Un outil ou service qui fournit un contenu MAEC génère au moins un type de format de sortie MAEC (lot, paquetage ou conteneur MAEC).

10.2 Chaque outil ou service qui envisage de fournir en sortie une seule instance de logiciel malveillant et n'envisage pas de saisir des informations relatives à ses propres attributs devrait générer un lot MAEC unique pour cette instance de logiciel.

10.3 Un outil ou service qui envisage de fournir en sortie une seule instance de logiciel malveillant et/ou envisage de saisir des informations relatives à ses propres attributs devrait générer un ou plusieurs paquetages MAEC avec un ou plusieurs sujets de logiciels malveillants MAEC intégrés pour chaque instance de logiciel malveillant qu'il analyse. S'il ne génère pas de paquetages MAEC, il doit alors générer des conteneurs MAEC contenant des paquetages MAEC intégrés.

10.4 Un outil ou service qui envisage de fournir en sortie plusieurs ensembles ou groupes d'instances de logiciels malveillants devrait générer un ou plusieurs conteneurs MAEC avec un ou plusieurs paquetages MAEC intégrés pour chaque ensemble ou groupe d'instances de logiciels malveillants qu'il analyse.

10.5 Un outil ou service qui envisage de saisir des informations relatives à ses propres attributs doit documenter, au moins, son nom, sa version et son fournisseur en utilisant les entités appropriées du sujet du logiciel malveillant MAEC et doit en conséquence générer des paquetages MAEC ou des conteneurs de paquetages MAEC intégrés.

10.6 Un outil ou service qui génère des paquetages MAEC doit être capable de générer des lots MAEC autonomes.

10.7 Un outil ou service qui génère des conteneurs MAEC doit être capable de générer des paquetages MAEC autonomes.

10.8 Un outil ou service doit employer sa propre partie constante et unique d'espace de nom de l'identificateur (ID) dans l'ensemble des contenus MAEC qu'il génère.

Création de contenu par analyse statique

Les présentes prescriptions s'appliquent à tous les outils et services d'analyse statique qui se proposent de créer des contenus MAEC.

10.9 Lorsqu'il génère un fichier au format de sortie MAEC, un outil ou service d'analyse statique doit communiquer ses conclusions en utilisant les entités MAEC les plus appropriées (y compris, sans toutefois s'y limiter, les actions, les objets et les comportements MAEC et/ou les classifications AV) ainsi que le format de sortie MAEC le mieux adapté.

Création de contenu par analyse dynamique

Les présentes prescriptions s'appliquent à tous les outils et services d'analyse dynamique qui se proposent de créer des contenus MAEC.

10.10 Lorsqu'il génère un fichier au format de sortie MAEC, un outil ou service d'analyse dynamique doit communiquer ses conclusions en utilisant les entités MAEC les plus appropriées (y compris, sans toutefois s'y limiter, les actions et comportements MAEC) ainsi que le format de sortie MAEC le mieux adapté.

Création de contenu par outil ou service auteur

Les présentes prescriptions s'appliquent à tous les outils et services qui se proposent de créer des contenus MAEC, ou de contribuer à faciliter la création ou la modification de contenus MAEC.

10.11 Un outil ou service auteur devrait encourager la réutilisation des sujets, des comportements, des actions, des objets et des indicateurs candidats des logiciels malveillants.

10.12 Un outil ou service auteur devrait permettre à l'utilisateur de demander la validation d'un document écrit pour le langage MAEC et signaler à l'utilisateur toutes les erreurs relatives au schéma XML du W3C et au Schematron.

10.13 Un outil ou service auteur devrait permettre à l'utilisateur d'importer et d'éditer des contenus MAEC existants (y compris tous les formats de sortie MAEC).

10.14 Un outil ou service auteur doit permettre à l'utilisateur d'exporter les contenus créés en tant que documents en format de sortie MAEC valides.

10.15 Un outil ou service auteur devrait signaler les contenus en double à l'utilisateur.

10.16 Un outil ou service auteur doit fournir la valeur et la capacité au-dessus et au-delà de la capacité d'un éditeur XML suivant la décision prise par l'autorité d'examen.

Stockage de contenu

Les présentes prescriptions s'appliquent à tous les répertoires qui envisagent de fournir un ensemble de contenus MAEC.

10.17 Chaque conteneur, paquetage, sujet de logiciel malveillant, analyse, lot, action, objet, comportement, indicateur candidat, ensemble de comportements, ensemble d'actions, ensemble d'objets et ensemble d'indicateurs candidats MAEC doit contenir un identificateur (ID) unique vis-à-vis de tous les autres conteneurs, paquetages, sujets de logiciel malveillant, analyses, lots, actions, objets et comportements, indicateurs candidats MAEC et des ensembles de comportements, d'actions, d'objets et d'indicateurs candidats MAEC du répertoire.

10.18 Chaque action et objet MAEC devrait contenir un identificateur vis-à-vis de toutes les autres actions et de tous les autres objets MAEC, lorsque cet identificateur est unique vis-à-vis de toutes les autres actions et de tous les autres objets MAEC du répertoire.

10.19 La partie d'espace de nom de l'identificateur doit être constante dans l'ensemble des contenus MAEC et devrait être propre au répertoire.

10.20 Chaque conteneur, paquetage, sujet de logiciel malveillant, analyse, lot, action, objet, comportement et indicateur candidat MAEC et ensemble de comportements, d'actions, d'objets et d'indicateurs candidats MAEC conserve le même identificateur tout au long de son existence. Un élément existant ne devrait pas être réécrit à d'autres fins puisque les utilisateurs peuvent y faire référence dans leur propre contenu.

10.21 Le propriétaire du répertoire doit décrire la procédure au moyen de laquelle un utilisateur peut récupérer des mises à jour de contenus.

Consommation de contenu

Les présentes prescriptions s'appliquent à tous les outils et services qui envisagent de consommer des contenus MAEC. Il convient d'établir une distinction entre la "consommation" (qui consiste à traiter l'information d'une manière intelligente) et l'"analyse" (qui consiste à extraire un contenu donné d'un document plus volumineux).

10.22 Un outil ou service qui consomme un contenu MAEC doit consommer au moins un type de format de sortie MAEC (lot, paquetage ou conteneur).

10.23 Un outil ou service qui consomme un contenu MAEC doit prendre en charge l'analyse de chaque type de format de sortie MAEC, afin d'extraire tout type intégré qu'il consomme, quel que soit l'emplacement du type dans le document au format de sortie. Ainsi, un outil ou service qui ne consomme que des lots doit également pouvoir analyser des paquetages et des conteneurs pour extraire le lot.

10.24 Si un outil ou service n'a besoin que d'informations d'analyse technique associées à une instance de logiciel malveillant, il devrait consommer des lots MAEC.

10.25 Si un outil ou service a besoin d'informations d'analyse technique associées à une instance de logiciel malveillant ainsi que de métadonnées d'analyse et d'information de relations, il devrait consommer des paquetages MAEC.

10.26 Si un outil ou service a besoin d'informations d'analyse associées à de multiples ensembles ou groupes d'instances de logiciels malveillants, il devrait consommer des conteneurs MAEC.

10.27 Si l'outil ou le service ne consomme pas de fichiers au format de sortie MAEC pendant l'exécution, le propriétaire de la capacité doit décrire la procédure au moyen de laquelle un utilisateur peut lui soumettre des fichiers au format de sortie MAEC pour interprétation par l'outil ou le service. Il convient d'indiquer dans la documentation avec quelle rapidité les fichiers présentés au propriétaire de la capacité sont mis à la disposition de l'outil ou du service.

11 Prescriptions concernant l'autorité d'examen

Une autorité d'examen doit satisfaire aux prescriptions ci-après concernant la compatibilité MAEC.

11.1 Une autorité d'examen doit clairement identifier la version d'examen de la capacité et la version du document énonçant les exigences en matière de compatibilité MAEC et la version du langage MAEC qui a été utilisée pour déterminer s'il a été satisfait officiellement aux prescriptions en matière de compatibilité MAEC pour chaque capacité.

11.2 L'autorité d'examen doit préciser le ou les types de fonctionnalités de la capacité (création de contenu, stockage de contenu ou consommation de contenu).

11.3 Une autorité d'examen doit définir et publier des exemples de matériels de test.

11.4 L'autorité d'examen doit diffuser des informations sur la manière de participer à la vérification d'adoption correcte, de manière que les organisations puissent se préparer le plus possible à l'avance.

11.5 L'autorité d'examen doit fournir un point de contact en vue d'organiser la vérification d'adoption correcte pour les capacités déclarant prendre en charge MAEC pour lesquelles le "Questionnaire relatif à la compatibilité MAEC" a été rempli.

11.6 Il est loisible à l'autorité d'examen de soumettre à nouveau à un test une capacité qui a été officiellement reconnue comme étant compatible avec MAEC.

12 Révocation

Si une autorité d'examen a approuvé la compatibilité MAEC d'une capacité, mais qu'elle a la preuve par la suite que les prescriptions ne sont plus respectées, elle peut révoquer son approbation et la capacité ne sera plus officiellement reconnue comme étant compatible avec MAEC. On trouvera ci-après les prescriptions auxquelles l'autorité d'examen doit satisfaire en vue de révoquer la reconnaissance.

12.1 L'autorité d'examen doit adresser au propriétaire de la capacité un avertissement de révocation au moins deux (2) mois avant la date prévue pour la révocation.

12.2 L'autorité d'examen peut reporter la date de révocation.

12.3 Si l'autorité d'examen constate que les actions ou déclarations du propriétaire de la capacité sont intentionnellement de nature à induire en erreur, elle peut ne pas tenir compte de la période de préavis. L'autorité d'examen peut interpréter l'expression "intentionnellement de nature à induire en erreur" comme elle l'entend.

12.4 Si l'autorité d'examen détermine que les actions du propriétaire de la capacité, en ce qui concerne les prescriptions en matière de compatibilité, sont intentionnellement de nature à induire en erreur, la durée de la révocation sera d'au moins un an.

12.5 L'autorité d'examen doit identifier les prescriptions spécifiques qui ne sont pas respectées.

12.6 Si le propriétaire de la capacité estime qu'il est satisfait aux prescriptions, il doit répondre à l'avertissement de révocation en fournissant des détails précis indiquant pourquoi la capacité satisfait auxdites prescriptions.

12.7 Si au cours de la période de préavis, le propriétaire de la capacité modifie la capacité afin qu'elle soit conforme aux prescriptions en question, l'autorité d'examen devra mettre un terme au processus de révocation pour la capacité.

12.8 L'autorité d'examen doit rendre public le fait que la reconnaissance officielle de la compatibilité MAEC correcte a été révoquée pour la capacité.

12.9 L'autorité d'examen peut rendre publics les motifs de la révocation.

Bibliographie

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2011) – *Vulnérabilités et expositions courantes*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2014