Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1215

(01/2019)

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

Sécurité du cyberespace – Cybersécurité

Cas d'utilisation pour l'expression structurée d'informations sur les menaces

Recommandation UIT-T X.1215

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
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.1215

Cas d'utilisation pour l'expression structurée d'informations sur les menaces

Résumé

La Recommandation UIT-T X.1215 présente divers cas d'utilisation dans lesquels le langage STIX (expression structurée d'informations sur les menaces) peut être utilisé pour faciliter l'échange d'informations et de renseignements sur les cybermenaces.

La présente Recommandation décrit également les concepts et les fonctionnalités du langage STIX. Elle vise à tenir compte d'un éventail de cas d'utilisation relevant de la gestion des cybermenaces, dont l'analyse des cybermenaces, la spécification des schémas d'indicateurs pour les cybermenaces, la gestion des activités de réponse et l'échange d'informations sur les cybermenaces. Ce type d'informations permet de prendre une décision relative à la sécurité sur la meilleure façon de se protéger contre une menace. La présente Recommandation vise aussi bien à permettre des analyses plus efficaces qu'à faciliter l'échange continu d'informations sur les cybermenaces. La série de spécifications pour le langage STIX [b-STIX2.0] est placée sous la responsabilité de l'Organization for the Advancement of Structured Information Standards (OASIS).

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1215	30-01-2019	17	11.1002/1000/13849

Mots clés

Renseignements sur les cybermenaces, échange d'informations, sécurité, STIX.

* 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 on 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 avait 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

Recommandation UIT-T X.1215

Cas d'utilisation pour l'expression structurée d'informations sur les menaces

1 Domaine d'application

La présente Recommandation vise à présenter divers cas d'utilisation pour l'expression structurée d'informations sur les menaces (STIX), un langage structuré utilisé pour décrire les informations sur les cybermenaces. Elle vise à tenir compte d'un éventail de cas d'utilisation relevant de la gestion des cybermenaces, dont l'analyse des cybermenaces, la spécification des schémas d'indicateurs pour les cybermenaces, la gestion des activités de réponse et l'échange d'informations sur les cybermenaces. Ces cas d'utilisation sont généralement simples et ne reflètent pas toute l'expressivité ou la flexibilité du langage STIX. En règle générale, ils sont accompagnés d'un texte décrivant le cas en question, d'un contenu exprimé dans le langage STIX, et de documents présentant du contenu STIX entièrement validé. La mise en oeuvre des cas d'utilisation est présentée dans le langage de balisage extensible (XML), étant donné que la version 1.2 du langage STIX, publiée en 2016, utilise un schéma XML, tandis qu'à partir de la version 2.0, on utilise la notation des objets du langage JavaScript (JSON). Il est recommandé d'utiliser les spécifications décrites dans la version 2.0.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation. Au moment de la publication, les versions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 entité [b-STIX2.0.1]: tout élément qui a une existence pouvant être identifiée séparément (par exemple, une organisation, une personne, un groupe, etc.).

3.1.2 objet STIX [b-STIX2.0.1]: objet "domaine" STIX (SDO) ou objet "relation" STIX (SRO).

3.1.3 expression d'informations structurées sur les menaces (STIX) [b-STIX2.0.1]: langage et format de sérialisation visant à échanger des renseignements sur les cybermenaces.

3.1.4 échange sécurisé et automatisé d'informations sur les indicateurs (TAXII) [b-STIX2.0.1]: protocole de couche application pour la communication d'informations sur les cybermenaces.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CAPEC énumération et classification des schémas d'attaque courants (*common attack pattern enumeration and classification*)

COA ligne d'action (*course of action*)

CnC commande et contrôle (*command and control*)

CTI renseignements sur les cybermenaces (*cyber threat intelligence*)

CVE vulnérabilités et exposition courantes (*common vulnerability and exposures*)

C2 commande et contrôle (*command and control*)

DLL bibliothèque de liens dynamiques (*dynamic link library*)

EDR enregistreur de données d'incidents (*event data recorder*)

OS système d'exploitation (*operating system*)

SDO objet "domaine" STIX (*STIX domain object)* (un "noeud" dans un graphe)

SMBv2 bloc de messages sur serveur version 2 (*server Message Block version 2*)

SRO objet "relation" STIX (*STIX relationship object*) (un mécanisme représentant une "arête" dans un graphe)

STIX expression structurée d'informations sur les menaces (*structured threat information expression*)

TAXII échange sécurisé et automatisé d'informations sur les indicateurs (*trusted automated exchange of indicator information*)

TTP tactiques, technique et procédure (*tactics, technique, and procedure*)

TLP protocole léger de trafic (*traffic light protocol*)

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

5 Conventions

Aucune.

6 Vue d'ensemble du langage STIX

6.1 Concepts du langage STIX

Pour répondre en temps réel à une cybermenace, il convient non seulement de disposer d'un système de sécurité individuel, mais également d'un système coopératif de gestion de la sécurité au niveau mondial, compte tenu de l'existence de problèmes mondiaux qui ne peuvent être résolus par une seule entité ou dans un seul domaine. C'est pourquoi les renseignements mondiaux sur les cybermenaces sont une composante importante du programme de sécurité de toute organisation. Ils peuvent être obtenus en interne ou auprès de sources extérieures. L'une des solutions pour l'échange de renseignements et d'informations sur les cybermenaces consiste à utiliser le langage STIX, un langage structuré qui permet de décrire les informations sur les cybermenaces. Le langage STIX représente de manière structurée des informations sur les cybermenaces qui sont expressives, flexibles, extensibles, automatisables et lisibles.

6.2 Objets dans le langage STIX

6.2.1 Objets dans la version 1.2 du langage STIX

La version 1.2 du langage STIX adopte sept objets "domaine" STIX (SDO), définis comme suit:

1) *Campaign*: une "campagne" représente un ensemble de tactiques, de techniques et de procédures (TTP), d'incidents ou d'auteurs de menaces qui, pris dans leur ensemble, expriment une intention commune ou un effet souhaité.
2) *Course of action*: le composant "ligne d'action" est utilisé pour donner des informations sur les mesures qui pourraient être prises soit en réponse à une attaque, soit à titre préventif, avant une attaque.
3) *Exploit target*: une "cible exploitable" donne des informations sur une vulnérabilité technique, une faille ou une mauvaise configuration dans les logiciels, les systèmes ou les réseaux qui peut être ciblée et exploitée par un assaillant.
4) *Incident*: un "incident" donne des informations sur un incident de cybersécurité.
5) *Indicator*: un "indicateur" présente des schémas observables spécifiques associés à des informations contextuelles.
6) *Threat actor*: l'objet "auteur de la menace" donne des informations qui caractérisent ou identifient (voire les deux) un assaillant.
7) *TTP*: terme militaire qui signifie "tactiques, techniques et procédures".

6.2.2 Objets dans la version 2.0 du langage STIX

La version 2.0 du langage STIX adopte un ensemble défini d'objets "domaine" et d'objets "relation" utilisés par STIX pour représenter les informations sur les cybermenaces. La version 2.0 définit douze objets "domaine", comme suit:

1) *Attack pattern*: les "schémas d'attaque" sont un type de TTP qui décrit les différentes méthodes utilisées par les assaillants pour tenter de compromettre des cibles.
2) *Campaign*: une "campagne" est un ensemble de comportements antagonistes décrivant une série d'activités malveillantes ou d'attaques (parfois désignée par le terme de "vagues") qui se produisent pendant une durée déterminée contre un ensemble de cibles précises.
3) *Course of action*: une "ligne d'action" est une mesure prise soit pour prévenir une attaque, soit pour répondre à une attaque en cours.
4) *Identity*: les "identités" peuvent représenter des personnes, des organisations ou des groupes (par exemple, ACME, Inc.), ainsi que des catégories de personnes, d'organisations ou de groupes (par exemple, le secteur financier).
5) *Indicator*: un "indicateur" contient un schéma qui peut être utilisé pour détecter des cyberactivités suspectes ou malveillantes.
6) *Intrusion set*: un "ensemble d'intrusions" est un groupe de comportements et de ressources antagonistes ayant des propriétés communes et dont on pense qu'ils sont régis par une seule et même organisation.
7) *Malware*: un "logiciel malveillant" est un type de TTP, également désigné par le terme de "code malveillant", qui fait référence à un programme inséré dans un système, généralement en secret, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime, ou de gêner ou de perturber la victime.
8) *Observed data*: les "données observées" donnent des informations sur ce qui a été observé au niveau des systèmes et des réseaux au moyen de la spécification cyber-observable définie dans les parties 3 et 4 de la spécification de la version 2.0 du langage STIX.

9) *Report*: un "rapport" est un recueil de renseignements sur les menaces consacré à un ou plusieurs sujets, tels que la description d'un auteur de menace, d'un logiciel malveillant ou d'une technique d'attaque, comprenant des éléments contextuels et des informations détaillées connexes.

10) *Threat actor*: les "auteurs de menaces" sont des individus, des groupes ou des organisations dont en pense qu'ils sont animés d'intentions malveillantes.

11) *Tool*: les "outils" sont des logiciels légitimes qui peuvent être utilisés par des auteurs de menaces pour perpétrer une attaque. Il est important de savoir quand et comment les auteurs de menaces utilisent ces outils pour comprendre la façon dont les campagnes sont exécutées.

12) *Vulnerability* : une "vulnérabilité" est une "erreur dans un logiciel pouvant être directement utilisée par un pirate pour accéder à un système ou réseau".

La version 2.0 du langage STIX définit deux objets "relation", comme suit:

1) *Relationship*: l'objet "relation" est utilisé pour lier deux objets "domaine" afin de décrire les liens qu'ils entretiennent.

2) *Sighting*: une "observation" traduit la conviction que quelque chose a été détecté dans les renseignements sur les cybermenaces (par exemple, un indicateur, un logiciel malveillant, un outil ou un auteur de menace).

6.3 Caractéristiques et outils du langage STIX

Le langage STIX présente les caractéristiques suivantes:

– Schémas JSON/XML: la version 2.0 du langage STIX utilise un schéma JSON pour représenter les six objets et propriétés. La version 1.0 utilise un schéma XML.

– Objet "domaine" STIX: tous les objets du langage STIX sont de premier niveau. Ces objets sont désignés par le sigle SDO. Les propriétés de certains objets font directement référence à l'"ID" (identification) d'un autre objet (par exemple, "*created_by_ref*"), mais la plupart des relations sont exprimées au moyen de l'objet "relation" de premier niveau.

– Objet "relation" STIX 2.0: la version 2.0 du langage STIX introduit un objet "relation" de premier niveau, qui lie deux autres objets de premier niveau par un type de relation nommé.

Le langage STIX devrait offrir les outils suivants:

– *STIX validator*: l'outil de validation est une ressource utile pour valider que le contenu JSON est conforme à la spécification 2.0.

– *Pattern validator*: les schémas STIX sont des expressions qui représentent des objets cyber-observables dans un objet "indicateur". Ils sont utiles pour modéliser les renseignements qui indiquent une cyberactivité. Cet outil de validation de schémas s'assure simplement que la syntaxe du schéma est conforme à l'expression.

– *STIX visualization*: l'outil de visualisation contribue à convertir le schéma JSON en un diagramme plus concis et lisible.

– *STIX elevator*: l'outil de mise à niveau contribue au processus de mise à niveau et permet de convertir au mieux une version 1.x vers la version 2.0.

– *STIX pattern matcher*: l'outil de mise en concordance des schémas offre un moyen de comparer les données observées et les schémas d'indicateurs.

7 Cas d'utilisation de la version 2.0 du langage STIX

La présente Recommandation décrit divers cas d'utilisation concernant la façon dont le langage STIX peut être utilisé pour faciliter l'échange d'informations et de renseignements sur les cybermenaces. Elle vise à tenir compte d'un éventail de cas d'utilisation relevant de la gestion des

cybermenaces, dont l'analyse des cybermenaces (cas d'utilisation 1, paragraphe 7.2.1), la spécification des schémas d'indicateurs pour les cybermenaces (cas d'utilisation 2, paragraphe 7.2.2), la gestion des activités de réponse aux cybermenaces (cas d'utilisation 3, paragraphe 7.2.3) et l'échange d'informations sur les cybermenaces (cas d'utilisation 4). Ce dernier sujet (cas 4) n'est pas traité dans la présente Recommandation. La Figure 1 donne un aperçu d'un cas d'utilisation pour le langage STIX. Un cas d'utilisation pour la version 1.0 figure dans l'Annexe A.

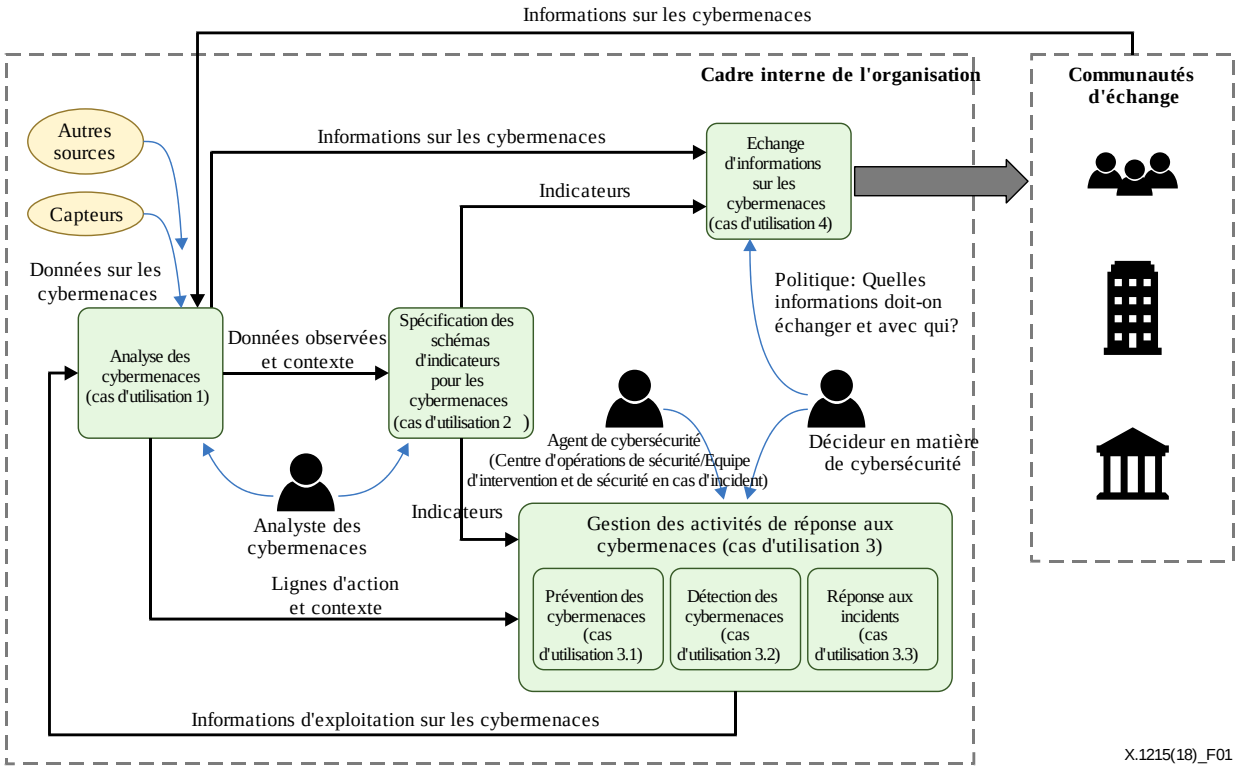

Figure 1 – Aperçu d'un cas d'utilisation pour le langage STIX

7.1 Cas d'utilisation d'un rançongiciel avec la version 2.0 du langage STIX

Un rançongiciel est un type de logiciel malveillant qui infecte les systèmes informatiques, limite l'accès aux données de la victime et exige une rançon. Dans la mesure où l'accès à son ordinateur est limité, la victime est alors forcée de payer l'entité qui a élaboré le programme malveillant pour que les restrictions soient levées. Les attaques par rançongiciel sont généralement perpétrées au moyen d'un cheval de Troie prenant l'apparence d'un fichier légitime que l'utilisateur est amené, par tromperie, à télécharger ou à ouvrir lorsqu'il le reçoit en pièce jointe d'un courrier électronique.

Récemment, le rançongiciel WannaCry a commencé à frapper les ordinateurs du monde entier, en se propageant automatiquement entre ordinateurs sans action de la part de l'utilisateur. A l'inverse des rançongiciels ordinaires, qui se diffusent en tant que pièces jointes à des courriers électroniques, le vecteur de contamination de WannaCry nécessitait uniquement que les systèmes vulnérables soient connectés à l'Internet. Le rançongiciel WannaCry chiffre divers fichiers tels que des documents, des fichiers compressés, des fichiers de bases de données et des fichiers de machines virtuelles.

Cette section décrit le cas d'utilisation d'un rançongiciel dans lequel la version 2.0 du langage STIX peut être utilisée à l'appui de la gestion des cybermenaces, face au rançongiciel WannaCry.

7.1.1 Analyse des cybermenaces

Cette section présente les informations analysées concernant un rançongiciel (WannaCrypt) qui ont été communiquées dans le cadre d'attaques par code malveillant perpétrées dans le monde entier au

moyen d'un rançongiciel exploitant une vulnérabilité relative à l'exécution du code à distance dans le protocole SMBv2 (server message block version 2).

7.1.1.1 Identité

Les informations relatives à un observateur peuvent être définies comme un objet "*identity*".

7.1.1.2 Données observées

On constate qu'un courrier électronique de notification de livraison a été reçu avec une archive contenant des fichiers au format EGG, et 52 domaines de serveur CnC (commande et contrôle) ont été observés (seuls deux domaines de serveur CnC figurent dans cet exemple).

```
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
     "0": {
     "type": "email-addr",
     "value": john@mail.com,
     "display_name" : "john"
     }
    }
}
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb2",
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
    "0: {
    "type": "email-message",
    "to_refs" : "0",
    "is_multipart": false,
    "subject" : "FedEx Shipping Information",
    "body_multipart": [
     {
     "content_type": "application/zip",
```

```
      "content_disposition": "attachment; filename=\" ipa_email_attachment_zip\"",
      "body_raw_ref": "5"
      }
    ]
   }
   }
}
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb3,
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
    "0": {
    "type":"domain-name",
    "value":" 43bwabxrduicndiocpo.net",
    "description" : "CnC server"
     }
   }
},
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb4",
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
   "0": {
    "type":"domain-name",
    "value":" dyc5m6xx36kxj.net",
    "description" : "CnC server"
     }
   }
}
```

7.1.1.3 Tactique, technique et procédure

On signale qu'une attaque par rançongiciel ciblant un ordinateur personnel a été observée; le schéma d'attaque correspond à l'activité d'une attaque ciblée par logiciel malveillant, et un objet "relation" utilisant un logiciel malveillant peut être créé par ce schéma d'attaque.

```
{
   "type": "attack-pattern",
   "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "name": " Targeted Malware ",
   "external_references": [
     {
       "source_name": "capec",
       "id": "CAPEC-542"
     }
   ]
 }

{
   "type": "malware",
   "id": "malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
   "created_by_ref" : "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2014-02-20T09:16:08.989000Z",
   "modified": "2014-02-20T09:16:08.989000Z",
   "name": "WannaCry",
   "labels": [
     "Ransomware"
   ]
}

{
   "type": "relationship",
   "id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "relationship_type": "uses",
   "source_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 },
```

7.1.1.4 Vulnérabilité

On signale que la vulnérabilité est liée à des vulnérabilités et expositions courantes (CVE), à savoir CVE-2017-0147 et CVE-2017-0143, correspondant au rançongiciel qui a exploité la vulnérabilité

relative à l'exécution du code à distance dans le protocole SMBv2 (correctif 17.3.14, MS17-010) dans Microsoft Windows. Un objet "relation" utilisant un logiciel malveillant qui cible cette vulnérabilité peut être créé.

```
{
 "type": "vulnerability",
 "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
 "created": "2016-05-12T08:17:27.000Z",
 "modified": "2016-05-12T08:17:27.000Z",
 "name": "Related CVE Information”
 "external_references": [
   {
     "source_name": "cve",
     "external_id": "CVE-2017-0147"
   },
  {
     "source_name": "cve",
     "external_id": "CVE-2017-0143"
   }
  ]
}

{
  "type": "relationship",
  "id": "relationship--6ce78886-1027-4800-9301-40c274fd472f",
  "created": "2014-06-30T09:15:17.182Z",
  "modified": "2014-06-30T09:15:17.182Z",
  "relationship_type": "targets",
  "source_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
  "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
}
```

7.1.1.5 Campagne et auteur de la menace

On définit deux objets, à savoir la campagne et l'auteur de la menace, pour décrire l'attaque par rançongiciel. Il est défini que la relation "*attributed-to*" (attribué à) peut être créée pour la campagne et l'auteur de menace, la relation "*uses*" (utilise) pour la campagne et le schéma d'attaque et la relation "*targets"* (cible) pour la campagne et la vulnérabilité.

```
{
      "type": "campaign",
      "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "created": "2017-05-12T15:50:10.983Z",
      "modified": "2017-05-13T08:33:39.001Z",
```

```
      "name": "Ransomware (WannaCrypt) Attack",
      "description": "May 12-13, 2017 infected more than 120,000 computers worldwide. Damage caused by WannaCrypt, a variant of WannaCry, which is distributed via networks in about 100 countries, including Europe and Asia.
The spread of malware is assumed by the hacker group 'Shadow Brokers' who claimed to have stolen hacking tools developed by the US National Security Agency (NSA). The attacker type is Malware Developer motivated by financial (Financial or Economic). Proficiency is Expert. The intruder's intention is Theft",
      "aliases": ["WannaCry"],
      "first_seen": "2017-05-12T04:50:40.123Z",
      "objective": "Theft"
}
{
      "type": "threat-actor",
      "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
      "created": "2017-05-08T15:50:10.983Z",
      "modified": "2017-05-08T15:50:10.983Z",
      "labels": ["hacker"],
      "roles": ["malware-author"],
     "sophistication": "expert",
     "resource_level": "team",
      "goals": ["Theft the development Tools"],
      "primary_motivation": "organizational-gain",
      "name": "Shadow Brokers”
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "attributed-to",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "uses",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5923",
```

```
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "targets",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5924",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "uses",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5925",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "attributed-to",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e"
},
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5926",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "targets",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
}
```


7.1.2 Spécification des schémas d'indicateurs pour les cybermenaces

7.1.2.1 Indicateur

L'adresse URL du site de distribution du logiciel malveillant est définie comme étant un type d'indicateur relatif à la surveillance d'adresses URL, et l'objet "relation" qui représente le logiciel malveillant peut être créé.


```
{
      "type": "indicator",
      "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
      "created": "2017-02-29T13:49:37.079000Z",
```

```
      "modified": "2017-06-29T13:49:37.079000Z",
      "labels": [
        "malicious-activity"
      ],
      "name": " Malware distribution site URL",
      "pattern":   "[url:value   =   '43bwabxrduicndiocpo.net']   OR   [url:value   =
'dyc5m6xx36kxj.net']",
      "valid_from": "2017-06-29T13:49:37.079000Z"
},
{
      "type": "relationship",
      "id": "relationship--6ce78886-1027-4800-9301-40c274fd473g",
      "created": "2017-06-30T09:15:17.182Z",
      "modified": "2017-06-30T09:15:17.182Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
      "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
}
{
   "type": "relationship",
   "id": "relationship--6ce78886-1027-4800-9301-40c274fd473h",
   "created": "2017-06-30T09:15:17.182Z",
   "modified": "2017-06-30T09:15:17.182Z",
   "relationship_type": "indicates",
   "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
   "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
}
```


7.1.3 Gestion des activités de réponse

7.1.3.1 Ligne d'action

On note qu'il y a des méthodes de réponse qui consistent à désactiver le protocole SMB ("*disable the SMB protocol"* et à corriger la vulnérabilité logicielle ("*software vulnerability patching"*), qui peuvent être définies comme des objets "*course of action*". Un objet "relation" peut être créé pour chaque objet afin d'atténuer les effets du logiciel malveillant.


```
{
   "type": "course-of-action",
   "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2016-04-06T20:03:48.000Z",
   "modified": "2016-04-06T20:03:48.000Z",
   "name": " Disable the SMB protocol ",
   "description": " Block SMB-related ports (TCP 139, TCP 445) using network firewalls
and Windows Firewall"
 }
{
```

```
   "type": "course-of-action",
   "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g",
   "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2016-04-06T20:03:48.000Z",
   "modified": "2016-04-06T20:03:48.000Z",
   "name": " Latest Windows Updates ",
   "description": " Download and apply version upgrades and latest security patches through MS update catalog site ",
"external_references": [
       {
       "url": " http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598",
       }
]
}
{
 "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
   "created": "2016-04-06T20:07:10.000Z",
   "modified": "2016-04-06T20:07:10.000Z",
   "relationship_type": "mitigates",
   "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 }
{
 "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fae",
   "created": "2016-04-06T20:07:10.000Z",
   "modified": "2016-04-06T20:07:10.000Z",
   "relationship_type": "mitigates",
   "source_ref": " course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g ",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 }
```


7.1.4 Aperçu du scénario d'attaque au moyen d'un diagramme de relation

La Figure 2 montre la relation entre tous les objets STIX utilisés pour décrire le cas d'utilisation.

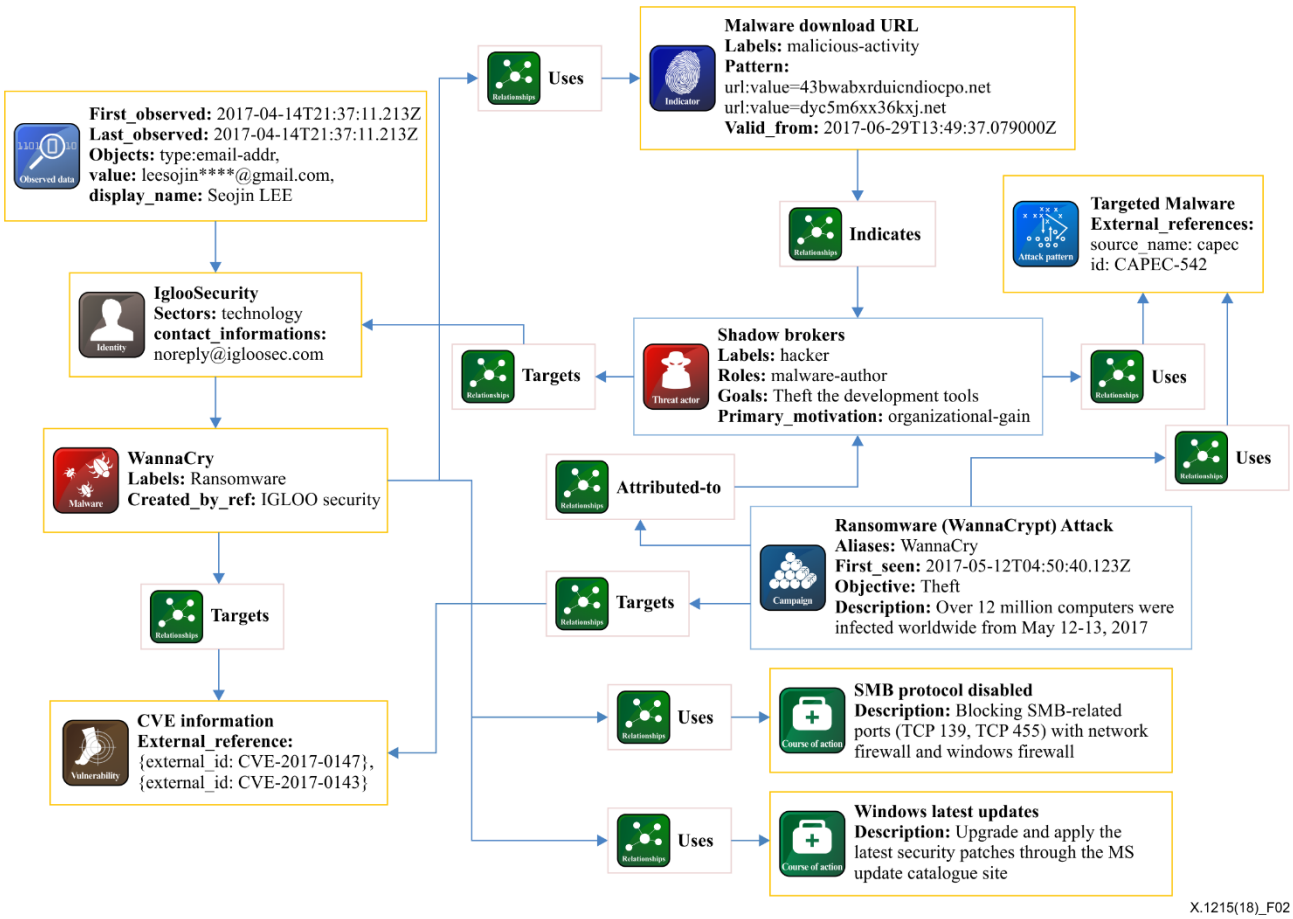

Figure 2 – Relation entre les objets STIX pour décrire le cas d'utilisation

Pour résumer, ce qui suit décrit le lot d'objets STIX qui comprend tous les objets utilisés pour détecter, analyser et contrecarrer l'attaque malveillante perpétrée au moyen du rançongiciel baptisé WannaCry.

```
{
   "type": "bundle",
   "id": "bundle--44af6c39-c09b-49c5-9de2-394224b04982",
   "spec_version": "2.0",
   "objects": [
     {
       "type": "identity",
       "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
       "created": "2017-04-14T13:07:49.812Z",
       "modified": "2017-04-14T13:07:49.812Z",
       "name": "IglooSecurity”
       "identity_class": "organization",
       "contact_information": "noreply@igloosec.com",
       "sectors": [
       "technology"
       ]
     },
```

```
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "email-addr",
          "value": john@mail.com,
          "display_name" : "john"
        }
      }
    },
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb2",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
      "number_observed": 1,
      "objects": {
      "0: {
        "type": "email-message",
        "to_refs" : "0",
        "is_multipart": false,
        "subject" : "FedEx Shipping Information",
        "body_multipart": [
        {
          "content_type": "application/zip",
          "content_disposition":  "attachment;  filename=\\  "  ipa_email_attachment_zip\
\"",
          "body_raw_ref": "5"
        }
        ]
        }
      }
    }
    {
      "type": "observed-data",
```

```
    "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb3,
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-04-14T19:37:11.213Z",
    "modified": "2017-04-14T19:37:11.213Z",
    "first_observed": "2017-04-14T21:37:11.213Z",
    "last_observed": "2017-04-14T21:37:11.213Z",
    "number_observed": 1,
    "objects": {
      "0": {
      "type":"domain-name",
      "value":" 43bwabxrduicndiocpo.net",
      "description" : "CnC server"
      }
    }
  }
  {
    "type": "observed-data",
    "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb4",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-04-14T19:37:11.213Z",
    "modified": "2017-04-14T19:37:11.213Z",
    "first_observed": "2017-04-14T21:37:11.213Z",
    "last_observed": "2017-04-14T21:37:11.213Z",
    "number_observed": 1,
    "objects": {
    "0": {
    "type":"domain-name",
    "value":" dyc5m6xx36kxj.net",
    "description" : "CnC server"
    }
    }
  },
  {
   "type": "attack-pattern",
   "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "name": " Targeted Malware ",
   "external_references": [
   {
    "source_name": "capec",
    "id": "CAPEC-542"
   }
   ]
```

```
    },
    {
     "type": "malware",
     "id": "malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
     ″created_by_ref” : "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
     "created": "2014-02-20T09:16:08.989000Z",
     "modified": "2014-02-20T09:16:08.989000Z",
     "name": " WannaCry ",
     "labels": [
      " Ransomware "
     ]
    },
    {
     "type": "vulnerability",
     "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
     "created": "2016-05-12T08:17:27.000Z",
     "modified": "2016-05-12T08:17:27.000Z",
     "name": " Related CVE Information”
     "external_references": [
      {
      "source_name": "cve",
      "external_id": "CVE-2017-0147"
      },
      {
      "source_name": "cve",
      "external_id": "CVE-2017-0143"
      }
     ]
    },
    {
     "type": "campaign",
     "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
     "created": "2017-05-12T15:50:10.983Z",
     "modified": "2017-05-13T08:33:39.001Z",
     "name": " Ransomware (WannaCrypt) Attack ",
     "description": "May 12-13, 2017 infected more than 120,000 computers worldwide. Damage caused by WannaCrypt, a variant of WannaCry, which is distributed via networks in about 100 countries, including Europe and Asia.
     The spread of malware is assumed by the hacker group 'Shadow Brokers' who claimed to have stolen hacking tools developed by the US National Security Agency (NSA). The attacker type is Malware Developer motivated by financial (Financial or Economic). Proficiency is Expert. The intruder's intention is Theft ",
     "aliases": ["WannaCry"],
     "first_seen": "2017-05-12T04:50:40.123Z",
     "objective": "Theft"
```

```
    }
    {
     "type": "threat-actor",
     "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
     "created": "2017-05-08T15:50:10.983Z",
     "modified": "2017-05-08T15:50:10.983Z",
     "labels": ["hacker"],
     "roles": ["malware-author"],
     "sophistication": "expert",
     "resource_level": "team",
     "goals": ["Theft the development Tools"],
     "primary_motivation": "organizational-gain",
     "name": "Shadow Brokers”
    },
    {
     "type": "indicator",
     "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
     "created": "2017-02-29T13:49:37.079000Z",
     "modified": "2017-06-29T13:49:37.079000Z",
     "labels": [
     "malicious-activity"
     ],
     "name": " Malware distribution site URL ",
     "pattern":   "[url:value   =   '43bwabxrduicndiocpo.net']   OR   [url:value   =
'dyc5m6xx36kxj.net’]",
     "valid_from": "2017-06-29T13:49:37.079000Z"
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "name": " Disable the SMB protocol ",
      "description":  "  Block  SMB-related  ports  (TCP  139,  TCP  445)  using  network
firewalls and Windows Firewall "
    },
    {
     "type": "course-of-action",
     "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g",
     "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
     "created": "2016-04-06T20:03:48.000Z",
     "modified": "2016-04-06T20:03:48.000Z",
     "name": " Latest Windows Updates ",
     "description": " Download and apply version upgrades and latest security patches
```

```
through MS update catalog site ",
      "external_references": [
      {
       "url": " http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598"
      }
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "uses",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
    },
    {
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5923",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "targets",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
    },
    {
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5924",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "uses",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
    },
    {
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5925",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "attributed-to",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e"
      "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
    },
    {
       "type": "relationship",
```

```
    "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5926",
    "created": "2017-08-08T15:50:10.983Z",
    "modified": "2017-08-08T15:50:10.983Z",
    "relationship_type": "targets",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
    "target_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
  },
  {
   "type": "relationship",
   "id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "relationship_type": "uses",
   "source_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
  },
  {
   "type": "relationship",
   "id": "relationship--6ce78886-1027-4800-9301-40c274fd472f",
   "created": "2014-06-30T09:15:17.182Z",
   "modified": "2014-06-30T09:15:17.182Z",
   "relationship_type": "targets",
   "source_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
   "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
  },
  {
   "type": "relationship",
   "id": "relationship--6ce78886-1027-4800-9301-40c274fd473g",
   "created": "2017-06-30T09:15:17.182Z",
   "modified": "2017-06-30T09:15:17.182Z",
   "relationship_type": "indicates",
   "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
  },
  {
   "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
   "created": "2016-04-06T20:07:10.000Z",
   "modified": "2016-04-06T20:07:10.000Z",
   "relationship_type": "mitigates",
   "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
  },
  {
```

```
      "type": "relationship",
      "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fae",
      "created": "2016-04-06T20:07:10.000Z",
      "modified": "2016-04-06T20:07:10.000Z",
      "relationship_type": "mitigates",
      "source_ref": " course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g ",
      "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
    },
    {
      "type": "relationship",
      "id": "relationship--6ce78886-1027-4800-9301-40c274fd473h",
      "created": "2017-06-30T09:15:17.182Z",
      "modified": "2017-06-30T09:15:17.182Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
      "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
    }
   ]
}
```


7.2 Cas d'utilisation pour une cyberattaque ciblant une transaction en crypto-monnaie

Cette section décrit un cas d'utilisation pour une attaque perpétrée par le groupe baptisé "Lazarus APT", l'auteur de la menace, le 20 juin 2018, contre une transaction en crypto-monnaie effectuée en Corée.

Dans ce scénario, l'auteur de la menace a envoyé un courrier électronique de hameçonnage contenant du code malveillant au personnel effectuant la transaction en crypto-monnaie. Le courrier électronique de hameçonnage était accompagné d'un document caché postscript malveillant capable de télécharger des bibliothèques de liens dynamiques (DLL) malveillantes ultérieurement. Le document a exploité la vulnérabilité du logiciel de traitement de texte Hangul pour exécuter le postscript. En conséquence, le fichier DLL malveillant a été installé sur l'ordinateur d'un utilisateur. Le fichier DLL malveillant a pris le contrôle de l'ordinateur de l'utilisateur et a accédé aux serveurs qui étaient disponibles pendant la transaction. L'attaquant a ainsi pu accéder au portefeuille contenant des crypto-monnaies utilisé pour la transaction et a retiré une importante somme d'argent.

7.2.1 Cas d'utilisation 1: Analyser les cybermenaces

Des attaques sur des transactions de crypto-monnaies ont été signalées à plusieurs reprises entre juin et juillet 2018. Dans le présent scénario, on analyse l'acte de piratage perpétré contre la transaction de crypto-monnaie d'une entreprise dénommée "BC-Company".

7.2.1.1 Identité

On peut modéliser avec l'objet "*identity*" les informations d'identification élémentaires de l'observateur. On peut modéliser sous la forme d'objets "*identity*" l'organisation qui a observé l'incident et l'endroit où l'incident s'est produit.

Pour identifier l'auteur de l'objet "*report*", les entreprises de contrôle de la sécurité, WINS et IGLOO security, sont représentées par des objets "*identity*". La cible de l'incident est représentée par un objet "*identity*" avec la propriété "*BC-Company.com*", qui est un pseudonyme. Cet objet est spécifié dans le champ "*where_sighted_refs*" de l'objet "sighting", champ qui apparaît plus loin dans

le texte, et est utilisé comme une cible d'attaque pour les schémas d'attaque et les logiciels malveillants.

```
{
    "type": "identity",
    "id": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.843Z",
    "modified": "2018-07-20T10:03:57.843Z",
    "name": "WINS",
    "identity_class": "organization",
    "sectors": [
        "technology"
    ],
    "contact_information": "sangpil@wins21.co.kr"
},
{
    "type": "identity",
    "id": "identity--650de76c-7638-4026-8900-ec7de2fc757f",
    "created": "2018-07-20T10:03:57.886Z",
    "modified": "2018-07-20T10:03:57.886Z",
    "name": "BC-Company.com – pseudonymous URL",
    "identity_class": "organization"
},
```

7.2.1.2 Données observées

Les données observées représentent des informations brutes générées par une machine et sont différentes des indicateurs, qui traduisent plutôt des renseignements exploitables. L'objet "*observed data"* contient des informations cyber-observables qui ont été recueillies sur des systèmes et des réseaux tels que des adresses IP, des fichiers et des adresses URL. Dans ce scénario, un fichier a été observé. Une autre référence, *"sighting_of_ref*", contient l'"ID" de l'objet "domaine" qui a été observé, lequel, dans ce cas, est l'objet "*observed-data*".

Dans le cadre de l'échange de crypto-monnaies, on observe un fichier envoyé par courrier électronique. Le nom du fichier et l'adresse de courrier électronique de l'expéditeur sont représentés par l'objet "*observed-data*". Les objets "*observed-data*" qui sont observés ailleurs sont représentés par des objets "*sighting*". Le lieu observé est représenté par la propriété "*where_sighted_refs*".

```
{
    "type": "observed-data",
    "id": "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
    "created": "2018-07-20T10:03:57.887Z",
    "modified": "2018-07-20T10:03:57.887Z",
    "first_observed": "2018-07-20T10:03:57.887095Z",
    "last_observed": "2018-07-20T10:03:57.887101Z",
    "number_observed": 1,
    "objects": {
        "0": {
```

```
                    "type": "email-addr",
                    "value": "****@hanmail.net"
                },
                "1": {
                    "type": "file",
                    "name": "ICT staff profile.hwp"
                }
            }
        },
        {
            "type": "sighting",
            "id": "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21",
            "created": "2018-07-20T10:03:57.896Z",
            "modified": "2018-07-20T10:03:57.896Z",
            "count": 1,
            "sighting_of_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "observed_data_refs": [
                "observed-data--45eeee3b-a455-404e-8612-613168eeb693"
            ],
            "where_sighted_refs": [
                "identity--650de76c-7638-4026-8900-ec7de2fc757f"
            ]
        }
```


7.2.1.3 Tactiques, techniques et procédures

Cette section décrit la façon dont on caractérise ce qu'est un comportement antagoniste et comment il se manifeste.

L'attaque provenait de la pièce jointe d'un courrier électronique de hameçonnage, et deux types de code malveillant ont été utilisés. Les attaques par hameçonnage, définies dans l'énumération et classification des schémas d'attaque courants (CAPEC) avec le numéro d'identification 163, sont représentées au moyen de l'objet "*attack pattern*". Le code malveillant fourni dans le courrier électronique de hameçonnage télécharge la bibliothèque DLL malveillante exploitant la vulnérabilité CVE-2015-2545. Ainsi, les objets malveillants ont pour valeur "*exploit*" ou "*dropper*". Dans le cas de bibliothèques DLL malveillantes reçues ultérieurement, le cheval de Troie activé à distance est catégorisé comme étant un code malveillant qui prend le contrôle de l'ordinateur de l'utilisateur.

La relation entre les deux codes malveillants est spécifiée comme étant de type "*related-to*", ce qui indique qu'il y a un lien entre le document malveillant et la bibliothèque DLL malveillante.

Lorsque le harponnage s'est produit, l'attaquant a utilisé un document camouflé. Dans la mesure où l'attaque est perpétrée contre une transaction de crypto-monnaies, un objet "relation" de type "*target*" est utilisé.


```
{
    "type": "attack-pattern",
    "id": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
    "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
```

```
    "created": "2018-07-20T10:03:57.851Z",
    "modified": "2018-07-20T10:03:57.851Z",
    "name": "Sphere Phishing",
    "external_references": [
{
    "source_name": "capec",
    "external_id": "CAPEC-163"
}
    ]
},
{
    "type": "malware",
    "id": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.845Z",
    "modified": "2018-07-20T10:03:57.845Z",
    "name": " malicious document (HWP file)",
    "description": "A purpose for downloading the RAT in the document file that contains the postscript in the attachment of the spear fishing e-mail",
    "labels": [
"exploit",
"dropper"
    ]
},
{
    "type": "malware",
    "id": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.847Z",
    "modified": "2018-07-20T10:03:57.847Z",
    "name": "Malicious DLL (C2 communication)",
    "description": " A tool for remote control of the attacker controls to steal the bit coin.",
    "labels": [
"exploit",
"dropper"
    ]
},
{
    "type": "relationship",
    "id": "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "targets",
    "source_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
```

```
    "target_ref": "identity--650de76c-7638-4026-8900-ec7de2fc757f"
},
{
    "type": "relationship",
    "id": "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
    "created": "2018-07-20T10:03:57.889Z",
    "modified": "2018-07-20T10:03:57.889Z",
    "relationship_type": "related-to",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "targets",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
},
```


7.2.1.4 Vulnérabilité

Dans le cas présent, on exploite une vulnérabilité, à savoir CVE-2015-2545, en dissimulant un postscript malveillant dans le logiciel de traitement de texte Hangul et en l'exécutant. L'objet "*vulnerability*" est utilisé pour représenter cette vulnérabilité. L'objet "relation" indique également la relation entre le code malveillant et la vulnérabilité.


```
{
    "type": "vulnerability",
    "id": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
    "created": "2018-07-20T10:03:57.885Z",
    "modified": "2018-07-20T10:03:57.885Z",
    "name": " CVE information",
    "external_references": [
{
    "source_name": "cve",
    "external_id": "CVE-2015-2545"
}
    ]
},
{
    "type": "relationship",
    "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
```

```
    "relationship_type": "targets",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
},
```

7.2.1.5 Campagne et auteur de la menace

Le groupe "Lazarus APT" a diffusé des courriers électroniques de harponnage contenant du code malveillant afin de voler des crypto-monnaies dans le cadre de la transaction de crypto-monnaies.

Le but recherché par l'objet "*threat actor*" est représenté par "*Steal cryptographic currency*" (voler des crypto-monnaies) dans la propriété "*goals*". Etant donné qu'un document malveillant a été créé, la propriété "*roles*" a pour valeur "*malware-author*" (auteur de logiciel malveillant). Puisque le document a été utilisé pour commettre un délit, la propriété "*label*" a pour valeur "*crime-syndicate*" (association de malfaiteurs).

L'attaque contre la transaction de crypto-monnaies est représentée au moyen de l'objet "*campaign*" et la propriété "*objective*" a pour valeur "*Theft*" (vol).

Les objets correspondant aux techniques d'attaque et au code malveillant utilisés dans les campagnes sont représentés par des objets "relation" de type "*use*".

```
        {
            "type": "campaign",
            "id": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.850Z",
            "modified": "2018-07-20T10:03:57.850Z",
            "name": " Hacking incident for the BC-Company on June 20, 2018",
            "description": "The Lazarus APT group launched a campaign to hack the BC-
Company cryptocurrency exchange. The attack method was to send the malicious code to
the target through the spear phishing technique, and then installed the DLL file
which was able to communicate with the C2 server and use them to steal the Bit
coin.",
            "objective": "Theft"
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.848Z",
            "modified": "2018-07-20T10:03:57.848Z",
            "name": "Lazarus APT Group",
            "description": "The Lazarus APT group has been known to use spear
phishing techniques to disguise social issues as document files and use them. Also,
it is widely known in Korea as an example of exploiting a vulnerability that
implements postscript in a Hangul document.",
            "roles": [
                "malware-author"
            ],
```

```
            "goals": [
                "Steal cryptographic currency"
            ],
            "primary_motivation": "organizational-gain",
            "labels": [
                "crime-syndicate"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692"
        },
        {
            "type": "relationship",
            "id": "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "attribute-to",
            "source_ref": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "target_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3"
        },
        {
            "type": "relationship",
            "id": "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        }
```


7.2.2 Cas d'utilisation 2: Spécification des schémas d'indicateurs pour les cybermenaces

7.2.2.1 Indicateur

Les objets "*indicator*" identifient des documents malveillants et des bibliothèques DLL malveillantes. Pour les documents malveillants, la propriété "*pattern"* dans un objet "*indicator*" représente soit des URL, soit des valeurs de hachage de fichiers pour le téléchargement de bibliothèques DLL malveillantes. Dans ce scénario, les schémas DLL malveillants dans l'objet "*indicator*" représentent l'URL de commande et de contrôle (C2) et la valeur de hachage du fichier,

ce qui permet l'enregistrement d'une politique. Plusieurs objets "relation" du type "*indicates*" indiquent la relation entre deux codes malveillants.


```
{
    "type": "indicator",
    "id": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.875Z",
    "modified": "2018-07-20T10:03:57.875Z",
    "name": "C2 URL",
    "pattern": "[url:value = 'https://tpddata.com/skin/skin-6.html' OR url:value =
'https://tpddata.com/skin/skin-8.html']",
    "valid_from": "2018-07-20T10:03:57.875238Z",
    "labels": [
"malicious-activity"
    ]
},
{
    "type": "indicator",
    "id": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.853Z",
    "modified": "2018-07-20T10:03:57.853Z",
    "name": " Hash value of malicious document",
    "pattern": "[file:hashes.'SHA-256' =
'e498630abe9a91485ba42698a35c2a0d8e13fe5cccde65479bf3033c45e7d431']",
    "valid_from": "2018-07-20T10:03:57.853427Z",
    "labels": [
"malicious-activity"
    ]
},
{
    "type": "indicator",
    "id": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
    "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
    "created": "2018-07-20T10:47:50.715Z",
    "modified": "2018-07-20T10:47:50.715Z",
    "name": "Hash value of malicious DLL",
    "pattern": "[file:hashes.'SHA-256' =
'5b1663d5eb565caccca188b6ff8a36291da32f368211e6437db2dc2e9cd']",
    "valid_from": "2018-07-20T10:47:50.71577Z",
    "labels": [
"malicious-activity"
    ]
},
```

```
{
    "type": "indicator",
    "id": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
    "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
    "created": "2018-07-20T10:47:50.719Z",
    "modified": "2018-07-20T10:47:50.719Z",
    "name": " a list of C2 URLs",
    "pattern":   "[url:value   =   'www.51up.com/ace/main.asp'   OR   url:value   =
'paulkaren.com/synthpop/main.asp' OR url:value = 'shieldonline.co.za/sitemap.asp']",
    "valid_from": "2018-07-20T10:47:50.719761Z",
    "labels": [
"malicious-activity"
    ]
}
{
    "type": "relationship",
    "id": "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
    "created": "2018-07-20T10:03:57.887Z",
    "modified": "2018-07-20T10:03:57.887Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
},
{
    "type": "relationship",
    "id": "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
    "created": "2018-07-20T10:47:50.725Z",
    "modified": "2018-07-20T10:47:50.725Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
    "created": "2018-07-20T10:47:50.726Z",
    "modified": "2018-07-20T10:47:50.726Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
    "created": "2018-07-20T10:03:57.887Z",
```

```
    "modified": "2018-07-20T10:03:57.887Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
}
```


7.2.3 Cas d'utilisation 3: Gestion des activités de réponse aux cybermenaces

7.2.3.1 Ligne d'action

Dans ce scénario d'attaque, la ligne d'action de l'équipe d'intervention est double: détection et réponse. Le document malveillant est d'abord exécuté, puis l'attaque commence.

La valeur de hachage du document malveillant est enregistrée dans le cadre d'une politique de sécurité dans l'outil d'analyse des logiciels malveillants, tel que YARA. L'enregistreur de données d'incident (EDR) peut détecter l'attaque lorsque le fichier avec la valeur de hachage est exécuté. En outre, le dispositif de sécurité du réseau réagit en bloquant le trafic du lien de téléchargement URL de la bibliothèque DLL malveillante, afin que les droits d'utilisateur de l'ordinateur ne soient pas volés. Si une bibliothèque DLL malveillante a été piratée, le dispositif de réseau peut bloquer l'activité malveillante en bloquant le trafic depuis l'URL de commande et de contrôle.


```
{
    "type": "course-of-action",
    "id": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
    "created": "2018-07-20T10:03:57.884Z",
    "modified": "2018-07-20T10:03:57.884Z",
    "name": "Establishment of EDR policy",
    "description": " Registration of DLL downloading URL and a list of C2 URLs as a reputation policy"
},
{
    "type": "course-of-action",
    "id": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
    "created": "2018-07-20T10:03:57.883Z",
    "modified": "2018-07-20T10:03:57.883Z",
    "name": "EDR policy establishment",
    "description": "Registration of SHA256 hash values for malicious documents and malicious DLLs as blocking policies "
},
{
    "type": "relationship",
    "id": "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "mitigates",
    "source_ref": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
},
{
```

```
    "type": "relationship",
    "id": "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "mitigates",
    "source_ref": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
}
```


7.2.4 Diagramme de relation et lot d'objets

La Figure 3 montre la relation entre tous les objets utilisés pour décrire le cas d'utilisation.

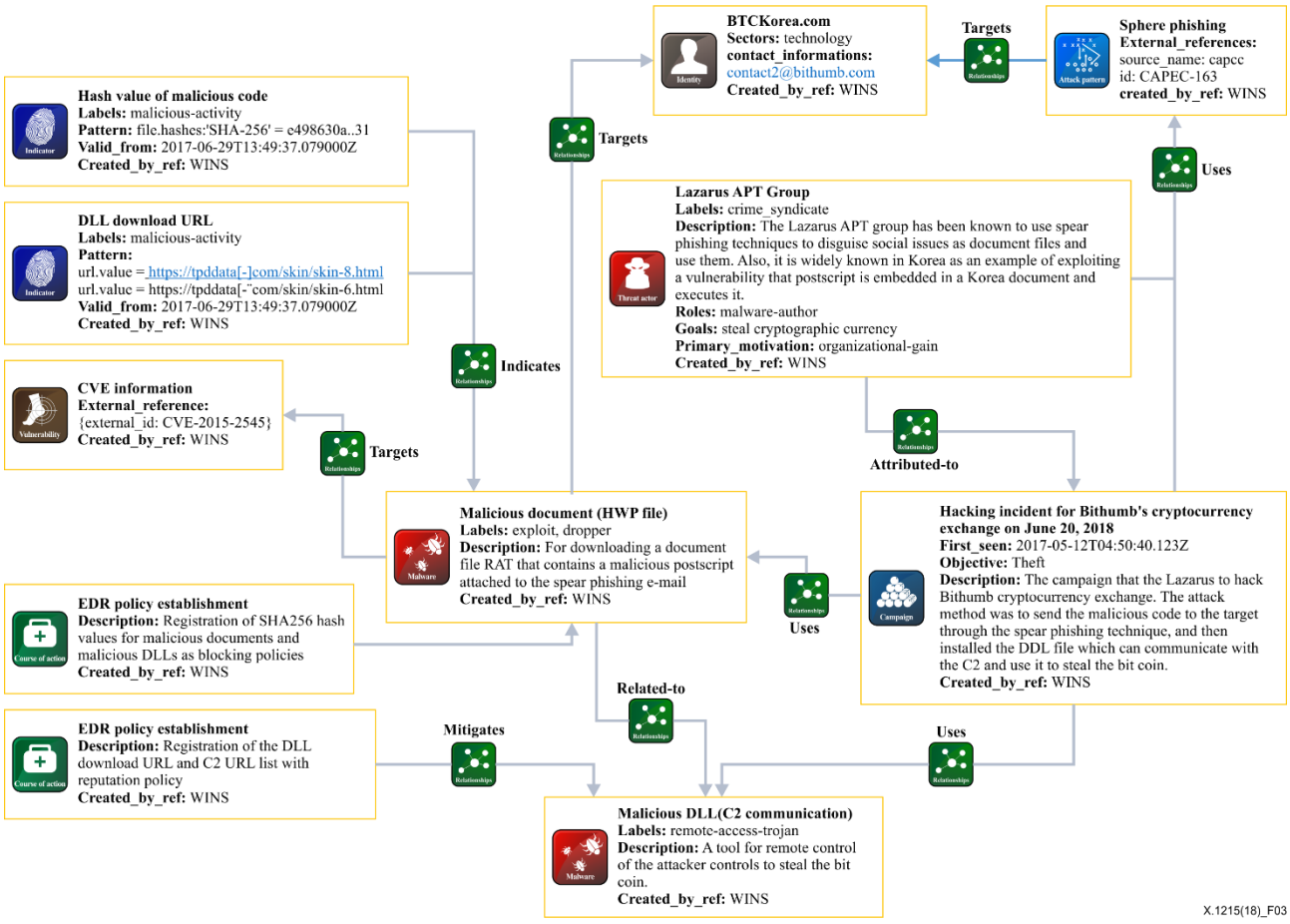

Figure 3 – Relation entre les objets STIX pour décrire le cas d'utilisation

En résumé, ce qui suit décrit un lot d'objets STIX qui comprend tous les objets utilisés pour détecter, analyser et contrecarrer les attaques malveillantes perpétrées par le groupe "Lazarus APT".


```
{
    "type": "bundle",
    "id": "bundle--42d953f0-0a5c-4b82-b223-b22ec85da222",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "campaign",
```

```
            "id": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.850Z",
            "modified": "2018-07-20T10:03:57.850Z",
            "name": "Hacking incident for BC-Company on June 20, 2018",
            "description": "The Lazarus APT group launched a campaign to hack the BC-Company cryptocurrency exchange. The attack method was to send the malicious code to the target through the spear phishing technique, and then installed the DLL file which was able to communicate with the C2 server and use them to steal the Bit coin.",
            "objective": "Theft"
        },
        {
            "type": "relationship",
            "id": "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692"
        },
        {
            "type": "course-of-action",
            "id": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "created": "2018-07-20T10:03:57.883Z",
            "modified": "2018-07-20T10:03:57.883Z",
            "name": "Establishment of EDR policy ",
            "description": "Registration of DLL downloading URL and a list of C2 URLs as a reputation policy"
        },
        {
            "type": "relationship",
            "id": "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "related-to",
            "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "malware",
            "id": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.847Z",
            "modified": "2018-07-20T10:03:57.847Z",
            "name": "Malicious DLL (C2 communication)",
            "description": "A tool for remote control of the attacker controls to
```

```
steal the bit coin.",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
            "created": "2018-07-20T10:47:50.725Z",
            "modified": "2018-07-20T10:47:50.725Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "relationship",
            "id": "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
            "created": "2018-07-20T10:47:50.726Z",
            "modified": "2018-07-20T10:47:50.726Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "report",
            "id": "report--91ed4b5a-5375-42cf-be5c-5fecff6d6da6",
            "created": "2018-07-20T10:03:57.897Z",
            "modified": "2018-07-20T10:03:57.897Z",
            "name": "Report on hacking incident for crypto currency exchange on
2018/06/20.",
            "published": "2018-07-20T10:03:57.897114Z",
            "object_refs": [
                "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
                "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
                "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
                "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
                "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
                "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
                "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
                "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
                "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
                "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
                "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
                "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
```

```
            "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
            "identity--650de76c-7638-4026-8900-ec7de2fc757f",
            "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
            "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
            "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
            "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
            "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
            "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
            "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
            "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
            "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
            "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
            "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21"
        ],
        "labels": [
            "threat-report"
        ]
    },
    {
        "type": "identity",
        "id": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
        "created": "2018-07-20T10:03:57.843Z",
        "modified": "2018-07-20T10:03:57.843Z",
        "name": "WINS",
        "identity_class": "organization",
        "sectors": [
            "technology"
        ],
        "contact_information": "sangpil@wins21.co.kr"
    },
    {
        "type": "relationship",
        "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
        "created": "2018-07-20T10:03:57.888Z",
        "modified": "2018-07-20T10:03:57.888Z",
        "relationship_type": "targets",
        "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
        "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
    },
    {
```

```
            "type": "course-of-action",
            "id": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "created": "2018-07-20T10:03:57.884Z",
            "modified": "2018-07-20T10:03:57.884Z",
            "name": "EDR policy establishment”,
            "description": "Registration of DLL downloading URL and a list of C2 URLs
as a reputation policy"
        },
        {
            "type": "relationship",
            "id": "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "mitigates",
            "source_ref": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "relationship",
            "id": "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "vulnerability",
            "id": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
            "created": "2018-07-20T10:03:57.885Z",
            "modified": "2018-07-20T10:03:57.885Z",
            "name": "CVE information",
            "external_references": [
                {
                    "source_name": "cve",
                    "external_id": "CVE-2015-2545"
                }
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "mitigates",
```

```
            "source_ref": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "indicator",
            "id": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.875Z",
            "modified": "2018-07-20T10:03:57.875Z",
            "name": "C2 URL",
            "pattern":   "[url:value   =   'https://tpddata.com/skin/skin-6.html'   OR
url:value = 'https://tpddata.com/skin/skin-8.html']",
            "valid_from": "2018-07-20T10:03:57.875238Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "attack-pattern",
            "id": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.851Z",
            "modified": "2018-07-20T10:03:57.851Z",
            "name": "Sphere Phishing",
            "external_references": [
                {
                    "source_name": "capec",
                    "external_id": "CAPEC-163"
                }
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "attribute-to",
            "source_ref": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "target_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3"
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.848Z",
```

```
            "modified": "2018-07-20T10:03:57.848Z",
            "name": "Lazarus APT Group",
            "description": "The Lazarus APT group has been known to use spear phishing techniques to disguise social issues as document files and use them. Also, it is widely known in Korea as an example of exploiting a vulnerability that implements postscript in a Hangul document.",
            "roles": [
                "malware-author"
            ],
            "goals": [
                "Steal cryptographic currency"
            ],
            "primary_motivation": "organizational-gain",
            "labels": [
                "crime-syndicate"
            ]
        },
        {
            "type": "identity",
            "id": "identity--650de76c-7638-4026-8900-ec7de2fc757f",
            "created": "2018-07-20T10:03:57.886Z",
            "modified": "2018-07-20T10:03:57.886Z",
            "name": "BC-Company.com",
            "identity_class": "organization"
        },
        {
            "type": "malware",
            "id": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.845Z",
            "modified": "2018-07-20T10:03:57.845Z",
            "name": "Malicious document(HWPfile)",
            "description": "A purpose for downloading the RAT in the document file that contains the postscript in the attachment of the spear fishing e-mail ",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
        {
            "type": "identity",
            "id": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.844Z",
            "modified": "2018-07-20T10:03:57.844Z",
            "name": "IGLOO Security",
            "identity_class": "organization",
```

```
            "sectors": [
                "technology"
            ],
            "contact_information": "noreply@igloosec.co.kr"
        },
        {
            "type": "relationship",
            "id": "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "target_ref": "identity--650de76c-7638-4026-8900-ec7de2fc757f"
        },
        {
            "type": "observed-data",
            "id": "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
"first_observed": "2018-07-20T10:03:57.887095Z",
            "last_observed": "2018-07-20T10:03:57.887101Z",
            "number_observed": 1,
            "objects": {
                "0": {
                    "type": "email-addr",
                    "value": "****@hanmail.net"
                },
                "1": {
                    "type": "file",
                    "name": " ICT staff profile.hwp"
                }
            }
        },
        {
            "type": "sighting",
            "id": "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21",
            "created": "2018-07-20T10:03:57.896Z",
            "modified": "2018-07-20T10:03:57.896Z",
            "count": 1,
            "sighting_of_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "observed_data_refs": [
                "observed-data--45eeee3b-a455-404e-8612-613168eeb693"
            ],
            "where_sighted_refs": [
```

```
                "identity--650de76c-7638-4026-8900-ec7de2fc757f"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "relationship",
            "id": "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "indicator",
            "id": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.853Z",
            "modified": "2018-07-20T10:03:57.853Z",
            "name": "Hash value of malicious document",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'e498630abe9a91485ba42698a35c2a0d8e13fe5cccde65479bf3033c45e7d431']",
            "valid_from": "2018-07-20T10:03:57.853427Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
                    "created": "2018-07-20T10:47:50.715Z",
            "modified": "2018-07-20T10:47:50.715Z",
            "name": "Hash value of malicious DLL",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'5b1663d5eb565caccca188b6ff8a36291da32f368211e6437db2dc2e9cd']",
            "valid_from": "2018-07-20T10:47:50.71577Z",
```

```
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
            "created": "2018-07-20T10:47:50.719Z",
            "modified": "2018-07-20T10:47:50.719Z",
            "name": "a List of C2 URLs",
            "pattern": "[url:value = 'www.51up.com/ace/main.asp' OR url:value = 'paulkaren.com/synthpop/main.asp' OR url:value = 'shieldonline.co.za/sitemap.asp']",
            "valid_from": "2018-07-20T10:47:50.719761Z",
            "labels": [
                "malicious-activity"
            ]
        }
    ]
}
```

Annexe A

Cas d'utilisation d'un rançongiciel avec la version 1.0 du langage STIX

(Cette annexe fait partie intégrante de la présente Recommandation.)

La présente annexe décrit le cas d'utilisation d'un rançongiciel dans lequel la version 1.0 du langage STIX peut être utilisée à l'appui de la gestion des cybermenaces, face au rançongiciel WannaCry.

A.1 Analyse des cybermenaces

Cette section présente les informations analysées concernant un rançongiciel (WannaCrypt) qui ont été communiquées dans le cadre d'attaques par code malveillant perpétrées dans le monde entier au moyen d'un rançongiciel exploitant une vulnérabilité relative à l'exécution du code à distance dans le protocole SMBv2.

A.1.1 Données observées

On constate qu'un courrier électronique de notification de livraison a été reçu avec une archive contenant des fichiers au format EGG, et 52 domaines de serveur CnC ont été observés.

```
<stix:Observables xsi:type="cybox:ObservablesType" cybox_major_version="2" cybox_minor_version="1">
    <cybox:Observable id="IGL:observable_000009392_01">
      <cybox:Event>
        <cybox:Type xsi:type="cyboxVocabs:EventTypeVocab-1.0.1">Email Ops</cybox:Type>
        <cybox:Description>Mail title: FedEx Shipping Information, Sender: john@mail, Attachment: Before decompression HBDIN_386572.egg (MD5: 447282e7c0ef3b830128476648015831) After decompression FedEx branch Information.doc (MD5: aa083dde6b58ec6e22a1dafea36f96f8), Access URL: icanhazip.com (Infection signal transmission) voh2in67mks5uygu.tor2web.cf (Ransomware private key transmission) </cybox:Description>
        <cybox:Actions>
          <cybox:Action>
            <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Receive</cybox:Type>
            <cybox:Associated_Objects>
              <cybox:Associated_Object id="IGL:object_igloo_email_000009392">
                <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
                  <EmailMessageObj:Header>
                    <EmailMessageObj:To>
                      <EmailMessageObj:Recipient category="e-mail">
<AddressObj:Address_Value>john@mail.com</AddressObj:Address_Value>
                      </EmailMessageObj:Recipient>
                    </EmailMessageObj:To>
                    <EmailMessageObj:Subject>FedEx Shipping Information</EmailMessageObj:Subject>
                  </EmailMessageObj:Header>
                  <EmailMessageObj:Attachments>
                    <EmailMessageObj:File object_reference="IGL:object_igloo_email_attachment_zip_000009392"/>
                  </EmailMessageObj:Attachments>
```

```
                </cybox:Properties>
                <cybox:Association_Type
xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-
1.0">Returned</cybox:Association_Type>
              </cybox:Associated_Object>
            </cybox:Associated_Objects>
          </cybox:Action>
        </cybox:Actions>
      </cybox:Event>
    </cybox:Observable>
    <cybox:Observable id="IGL:observable_000009392_02">
      <cybox:Description> CnC Server </cybox:Description>
      <cybox:Object id="IGL:Object-37be6630-b2df-4bf9-8750-3f45ca9e19cf">
        <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
          <URIObj:Value condition="Equals">43bwabxrduicndiocpo.net</URIObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
    <cybox:Observable id="IGL:observable_000009392_03">
      <cybox:Description> CnC Server </cybox:Description>
      <cybox:Object id="IGL:Object-827A13A8-7C90-4A6C-9FEF-F5734BE693F1">
        <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
          <URIObj:Value condition="Equals">dyc5m6xx36kxj.net</URIObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
  </stix:Observables>
```

A.1.2 Tactique, technique et procédure

On signale qu'une attaque par rançongiciel ciblant un ordinateur personnel a été observée. Le schéma d'attaque est l'activité d'une attaque ciblée par logiciel malveillant, et l'attaque a pour cible les informations de l'organisation.

```
<stix:TTPs>
    <stix:TTP xsi:type="ttp:TTPType" id="IGL:ttp_000009392">
      <ttp:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </ttp:Intended_Effect>
      <ttp:Behavior>
        <ttp:Attack_Patterns>
          <ttp:Attack_Pattern capec_id="CAPEC-542">
            <ttp:Title>Targeted Malware</ttp:Title>
          </ttp:Attack_Pattern>
```

```
        </ttp:Attack_Patterns>
        <ttp:Malware>
          <ttp:Malware_Instance>
            <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Ransomware</ttp:Type>
            <ttp:Title>WannaCry</ttp:Title>
          </ttp:Malware_Instance>
        </ttp:Malware>
     </ttp:Behavior>
      <ttp:Resources>
        <ttp:Tools>
          <ttp:Tool>
            <cyboxCommon:Type               xsi:type="stixVocabs:AttackerToolTypeVocab-
1.0">Malware</cyboxCommon:Type>
          </ttp:Tool>
        </ttp:Tools>
      </ttp:Resources>
      <ttp:Victim_Targeting>
        <ttp:Targeted_Systems      xsi:type="stixVocabs:SystemTypeVocab-1.0">Enterprise
Systems</ttp:Targeted_Systems>
        <ttp:Targeted_Information            xsi:type="stixVocabs:InformationTypeVocab-
1.0">Information Assets</ttp:Targeted_Information>
      </ttp:Victim_Targeting>
      <ttp:Exploit_Targets>
        <ttp:Exploit_Target>
          <stixCommon:Exploit_Target idref="IGL:et_000009392"/>
        </ttp:Exploit_Target>
      </ttp:Exploit_Targets>
    </stix:TTP>
  </stix:TTPs>
```

A.1.3 Cible exploitable

On signale que la vulnérabilité est liée aux vulnérabilités CVE-2017-0147 et CVE-2017-0143 du système d'exploitation Windows 10, correspondant au rançongiciel qui a exploité la vulnérabilité relative à l'exécution du code à distance dans le protocole SMBv2 dans Microsoft Windows.

```
<stix:Exploit_Targets>
    <stixCommon:Exploit_Target xsi:type="et:ExploitTargetType"
id="IGL:vulnerability_8f38ecb0-baba-4746-9f97-6ddaec989d89" timestamp="2014-02-
20T09:00:00.000000Z">
      <et:Title>SMBv2 related Vulnerability </et:Title>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0146</et:CVE_ID>
        <et:Affected_Software>
          <et:Affected_Software>
            <stixCommon:Observable>
```

```
              <cybox:Object>
                <cybox:Properties xsi:type="ProductObj:ProductObjectType">
                  <ProductObj:Product condition="Equals">Windows 10</ProductObj:Product>
                  <ProductObj:Version condition="Equals" apply_condition="ANY">1511 for
32-bit systems##comma##1511 for x64-based Systems##comma##1607 for 32-bit
Systems##comma##1607 for x64-based Systems</ProductObj:Version>
                </cybox:Properties>
              </cybox:Object>
            </stixCommon:Observable>
          </et:Affected_Software>
        </et:Affected_Software>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0147</et:CVE_ID>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0143</et:CVE_ID>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
    </stixCommon:Exploit_Target>
  </stix:Exploit_Targets>
```

A.1.4 Incident

Il est signalé que la catégorie d'incident est "*unauthorized access*" (accès non autorisé), que les ressources visées sont des informations détenues par une organisation et que les objets affectés et les réponses d'incidents correspondent à un vol "*theft*".

```
<stix:Incidents>
    <stix:Incident xsi:type="incident:IncidentType" id="IGL:incident_000009392">
      <incident:Time>
        <incident:First_Malicious_Action>2012-07-19T14:25:36+09:00
</incident:First_Malicious_Action>
```

```
        <incident:Incident_Reported>2012-10-30T00:00:00+09:00
</incident:Incident_Reported>
      </incident:Time>
      <incident:Categories>
        <incident:Category xsi:type="stixVocabs:IncidentCategoryVocab-1.0">Unauthorized
Access</incident:Category>
      </incident:Categories>
      <incident:Victim>
        <stixCommon:Name>Igloo</stixCommon:Name>
      </incident:Victim>
      <incident:Affected_Assets>
        <incident:Affected_Asset>
          <incident:Ownership_Class           xsi:type="stixVocabs:OwnershipClassVocab-
1.0">Internally-Owned</incident:Ownership_Class>
          <incident:Management_Class         xsi:type="stixVocabs:ManagementClassVocab-
1.0">Internally-Managed</incident:Management_Class>
          <incident:Location_Class             xsi:type="stixVocabs:LocationClassVocab-
1.0">Internally-Located</incident:Location_Class>
        </incident:Affected_Asset>
      </incident:Affected_Assets>
      <incident:Impact_Assessment>
        <incident:Effects>
          <incident:Effect      xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial
Loss</incident:Effect>
        </incident:Effects>
      </incident:Impact_Assessment>
      <incident:Status                        xsi:type="stixVocabs:IncidentStatusVocab-
1.0">Closed</incident:Status>
      <incident:Related_Indicators>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_01"/>
        </incident:Related_Indicator>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_02"/>
        </incident:Related_Indicator>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_03"/>
        </incident:Related_Indicator>
      </incident:Related_Indicators>
      <incident:Leveraged_TTPs>
        <incident:Leveraged_TTP>
          <stixCommon:TTP idref="IGL:ttp_000009392"/>
        </incident:Leveraged_TTP>
      </incident:Leveraged_TTPs>
      <incident:Attributed_Threat_Actors>
        <incident:Threat_Actor>
          <stixCommon:Threat_Actor idref="IGL:ta_000009392"/>
```

```
        </incident:Threat_Actor>
      </incident:Attributed_Threat_Actors>
      <incident:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </incident:Intended_Effect>
      <incident:Security_Compromise       xsi:type="stixVocabs:SecurityCompromiseVocab-
1.0">No</incident:Security_Compromise>
      <incident:Discovery_Method            xsi:type="stixVocabs:DiscoveryMethodVocab-
1.0">User</incident:Discovery_Method>
      <incident:COA_Taken>
        <incident:Course_Of_Action idref="IGL:coa_000009392"/>
      </incident:COA_Taken>
    </stix:Incident>
  </stix:Incidents>
```

A.1.5 Auteur de la menace

On signale que l'attaquant est un développeur de logiciel malveillant, "*malware developer*", que ses motivations sont d'ordre financier ou économique, "*Financial or economic*", que son niveau de maîtrise est "*expert*" et que son intention est le vol, "*theft*".

```
<stix:Threat_Actors>
    <stix:Threat_Actor id="IGL:ta_000009392" xsi:type="ta:ThreatActorType">
      <ta:Description>
       It infected more than 120,000 computers worldwide during May 12-13, 2017. Damage
       caused by WannaCrypt, a variant of WannaCry, which has spread to about 100
       countries including Europe and Asia.
       The spread of malware is assumed by the hacker group 'Shadow Brokers' who
       claimed to have stolen hacking tools developed by the US National Security
       Agency (NSA).
       The type of attacker is malware developer, the motivation is financial or
       economic, the proficiency is an expert and the intruder's intent is theft.
      </ta:Description>
      <ta:Type>
      <stixCommon:Value xsi:type="stixVocabs:ThreatActorTypeVocab-1.0"> eCrime Actor -
Malware Developer                    </stixCommon:Value>
      </ta:Type>
      <ta:Motivation>
        <stixCommon:Value   xsi:type="stixVocabs:MotivationVocab-1.1">   Financial   or
Economic </stixCommon:Value>
      </ta:Motivation>
      <ta:Sophistication>
        <stixCommon:Value          xsi:type="stixVocabs:ThreatActorSophisticationVocab-
1.0">Expert</stixCommon:Value>
      </ta:Sophistication>
      <ta:Intended_Effect>
```

```
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </ta:Intended_Effect>
      <ta:Observed_TTPs>
        <ta:Observed_TTP>
          <stixCommon:TTP idref=" IGL:ttp_000009392"/>
        </ta:Observed_TTP>
      </ta:Observed_TTPs>
    </stix:Threat_Actor>
  </stix:Threat_Actors>
```

A.1.6 Campagne

On signale que l'incident, les TTP et l'auteur de la menace correspondants ont été décrits afin de refléter l'intention de l'auteur de la menace.

```
<stix:Campaigns>
    <stix:Campaign xsi:type="campaign:CampaignType" id="IGL:campaign_000009392">
      <campaign:Title> Ransomware(WannaCrypt) Attack </campaign:Title>
      <campaign:Names>
        <campaign:Name>000009392</campaign:Name>
      </campaign:Names>
      <campaign:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </campaign:Intended_Effect>
      <campaign:Related_TTPs>
          <stixCommon:TTP idref="IGL:ttp_000009392"/>
        </campaign:Related_TTP>
      </campaign:Related_TTPs>
      <campaign:Related_Incidents>
        <campaign:Related_Incident>
          <stixCommon:Incident idref="IGL:incident_000009392"/>
        </campaign:Related_Incident>
      </campaign:Related_Incidents>
      <campaign:Related_Indicators>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_01"/>
        </campaign:Related_Indicator>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_02"/>
        </campaign:Related_Indicator>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_03"/>
        </campaign:Related_Indicator>
      </campaign:Related_Indicators>
      <campaign:Attribution>
```

```
        <campaign:Attributed_Threat_Actor>
          <stixCommon:Threat_Actor idref="IGL:ta_000009392"/>
        </campaign:Attributed_Threat_Actor>
      </campaign:Attribution>
    </stix:Campaign>
  </stix:Campaigns>
```

A.2 Spécification des schémas d'indicateurs pour les cybermenaces

A.2.1 Indicateur

Il est signalé que les indicateurs de type "*malicious e-mail*" (courrier électronique malveillant), "*exfiltration*" (extraction) et "*URL watchlist*" (liste de surveillance d'adresses URL) sont définis, et les indicateurs "*observable*", "*TTP*" et "*campaign*" sont associés.

```
<stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_01">
      <indicator:Type     xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Malicious     E-
mail</indicator:Type>
      <indicator:Description> Ransomware infection with malicious mail as one of the
indicators </indicator:Description>
      <indicator:Observable>
        <cybox:Observable_Composition operator="OR">
          <cybox:Observable idref="IGL:observable_000009392_01"/>
        </cybox:Observable_Composition>
      </indicator:Observable>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_02">
      <indicator:Type                          xsi:type="stixVocabs:IndicatorTypeVocab-
1.1">Exfiltration</indicator:Type>
      <indicator:Description> SMB  vulnerability  attack  as  one  of  the  Indicators
</indicator:Description>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
```

```
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_03">
      <indicator:Type                    xsi:type="stixVocabs:IndicatorTypeVocab-1.1">URL
Watchlist</indicator:Type>
      <indicator:Description> malicious code distribution sites as one of the
indicators                              </indicator:Description>
      <indicator:Observable>
        <cybox:Observable_Composition operator="OR">
          <cybox:Observable idref="IGL:observable_000009392_02"/>
          <cybox:Observable idref="IGL:observable_000009392_03"/>
        </cybox:Observable_Composition>
      </indicator:Observable>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    </stix:Indicators>
```

A.3 Gestion des activités de réponse

A.3.1 Ligne d'action

Il est noté que des mesures de réparation sont possibles au moyen d'un logiciel de correction des vulnérabilités, sans incidences du point de vue de la limite de connexion, avec un coût faible et une efficacité moyenne.

```
<stix:Courses_Of_Action>
    <stix:Course_Of_Action xsi:type="coa:CourseOfActionType" id="IGL:coa_000009392">
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Remedy</coa:Stage>
      <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Patching</coa:Type>
      <coa:Parameter_Observables xsi:type="cybox:ObservablesType" cybox_major_version="2"
cybox_minor_version="1">
        <cybox:Observable idref="IGL:observable_000009392_01"/>
        <cybox:Observable idref="IGL:observable_000009392_02"/>
        <cybox:Observable idref="IGL:observable_000009392_03"/>
      </coa:Parameter_Observables>
      <coa:Impact>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
```

```
1.0">None</stixCommon:Value>
      </coa:Impact>
      <coa:Cost>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Low</stixCommon:Value>
      </coa:Cost>
      <coa:Efficacy>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Medium</stixCommon:Value>
      </coa:Efficacy>
    </stix:Course_Of_Action>
    <stix:Course_Of_Action    id="IGL:coa_000009393"    xsi:type="coa:CourseOfActionType"
version="1.1">
      <coa:Title>(For users who cannot use the latest Windows security patch) Disable the
SMB protocol </coa:Title>
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Response</coa:Stage>
      <coa:Type               xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Perimeter
Blocking</coa:Type>
      <coa:Objective>
        <coa:Description> Block SMB-related ports (TCP 139, TCP 445) using network
firewalls and Windows Firewall</coa:Description>
        <coa:Applicability_Confidence>
          <stixCommon:Value                        xsi:type="stixVocabs:HighMediumLowVocab-
1.0">High</stixCommon:Value>
        </coa:Applicability_Confidence>
      </coa:Objective>
      <coa:Parameter_Observables      cybox_major_version="2"      cybox_minor_version="1"
cybox_update_version="0">
        <cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19edb">
          <cybox:Object id="IGL:Port-d5bc7186-319d-44e0-85f4-0b65f59034a3">
            <cybox:Properties xsi:type="PortObj:PortObjectType">
              <PortObj:Port_Value>139</PortObj:Port_Value>
              <PortObj:Layer4_Protocol>TCP</PortObj:Layer4_Protocol>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19asd">
          <cybox:Object id="IGL:Port-d5bc7186-319d-44e0-85f4-0b65f59034a4">
            <cybox:Properties xsi:type="PortObj:PortObjectType">
              <PortObj:Port_Value>445</PortObj:Port_Value>
              <PortObj:Layer4_Protocol>TCP</PortObj:Layer4_Protocol>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      </coa:Parameter_Observables>
    </stix:Course_Of_Action>
    <stix:Course_Of_Action    id="IGL:coa_000009394"    xsi:type="coa:CourseOfActionType"
version="1.1">
```

```
      <coa:Title> Latest Windows Updates</coa:Title>
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Remedy</coa:Stage>
      <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Patching</coa:Type>
      <coa:Objective>
        <coa:Description> Download and apply version upgrades and latest security patches
through MS update catalog site </coa:Description>
        <coa:Applicability_Confidence>
          <stixCommon:Value                    xsi:type="stixVocabs:HighMediumLowVocab-
1.0">High</stixCommon:Value>
        </coa:Applicability_Confidence>
      </coa:Objective>
      <coa:Parameter_Observables     cybox_major_version="2"     cybox_minor_version="1"
cybox_update_version="0">
<cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19adn">
          <cybox:Object id="IGL:Object-37be6630-b2df-4bf9-8750-3f45ca9e1923bb">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
              <URIObj:Value
condition="Equals">http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598</URIOb
j:Value>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      </coa:Parameter_Observables>
      <coa:Cost>
        <stixCommon:Value                    xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Low</stixCommon:Value>
      </coa:Cost>
      <coa:Efficacy>
        <stixCommon:Value                    xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Medium</stixCommon:Value>
      </coa:Efficacy>
    </stix:Course_Of_Action>
</stix:Courses_Of_Action>
```

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*

[b-RFC7159] Bray, T., Ed., The JavaScript Object Notation (JSON) (2014), *Data Interchange Format*, RFC 7159, DOI 10.17487/RFC7159. http://www.rfc-editor.org/info/rfc7159.txt

[b-STIX1.2.1] Site web de l'OASIS, spécifications STIX. https://www.oasis-open.org/standards#stix1.2.1

[b-STIX1.2.1-Part 1] Site web de l'OASIS, spécifications STIX, *Part 1: Overview*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part1-overview/stix-v1.2.1-cs01-part1-overview.html

[b-STIX2.0] Présentation de STIX https://oasis-open.github.io/cti-documentation/stix/intro.html

[b-STIX2.0-Part 1] OASIS, 2017, *STIX Version 2.0. Part 1: Part 1: STIX Core Concepts*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html

[b-STIX2.0-Part 2] OASIS, 2017, *STIX Version 2.0. Part 2: STIX Objects*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html

[b-STIX2.0-Part 3] OASIS, 2017, *STIX Version 2.0. Part 3: Cyber Observable Core Concepts*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part3-cyber-observable-core/stix-v2.0-cs01-part3-cyber-observable-core.html

[b-STIX2.0-Part 4] OASIS, 2017, *STIX Version 2.0. Part 4: Cyber Observable Objects*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part4-cyber-observable-objects/stix-v2.0-cs01-part4-cyber-observable-objects.html

[b-STIX2.0-Part 5] OASIS, 2017, *STIX Version 2.0. Part 5: STIX Patterning*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part5-stix-patterning/stix-v2.0-cs01-part5-stix-patterning.html

[b-STIX2.0 tool] Getting Started with STIX 2.0. https://oasis-open.github.io/cti-documentation/stix/gettingstarted.html

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2019