الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1215

(2019/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

# حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات

التوصية ITU-T X.1215

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

| | |
|---|---|
| الشبكات العمومية للبيانات | X.199–X.1 |
| التوصيل البيني للأنظمة المفتوحة | X.299–X.200 |
| التشغيل البيني للشبكات | X.399–X.300 |
| أنظمة معالجة الرسائل | X.499–X.400 |
| الدليل | X.599–X.500 |
| التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام | X.699–X.600 |
| إدارة التوصيل البيني للأنظمة المفتوحة (OSI) | X.799–X.700 |
| الأمن | X.849–X.800 |
| تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI) | X.899–X.850 |
| المعالجة الموزعة المفتوحة | X.999–X.900 |
| أمن المعلومات والشبكات | |
| الجوانب العامة للأمن | X.1029–X.1000 |
| أمن الشبكة | X.1049–X.1030 |
| إدارة الأمن | X.1069–X.1050 |
| الخصائص البيومترية | X.1099–X.1080 |
| تطبيقات وخدمات آمنة (1) | |
| أمن البث المتعدد | X.1109–X.1100 |
| أمن الشبكة المحلية | X.1119–X.1110 |
| أمن الخدمات المتنقلة | X.1139–X.1120 |
| أمن الويب | X.1149–X.1140 |
| بروتوكولات الأمن (1) | X.1159–X.1150 |
| الأمن بين جهتين نظيرتين | X.1169–X.1160 |
| أمن معرفات الهوية عبر الشبكات | X.1179–X.1170 |
| أمن التلفزيون القائم على بروتوكول الإنترنت | X.1199–X.1180 |
| أمن الفضاء السيبراني | |
| **الأمن السيبراني** | **X.1229–X.1200** |
| مكافحة الرسائل الاقتحامية | X.1249–X.1230 |
| إدارة الهوية | X.1279–X.1250 |
| تطبيقات وخدمات آمنة (2) | |
| اتصالات الطوارئ | X.1309–X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1319–X.1310 |
| أمن شبكة الكهرباء الذكية | X.1339–X.1330 |
| البريد المعتمد | X.1349–X.1340 |
| أمن إنترنت الأشياء (IoT) | X.1369–X.1360 |
| أمن أنظمة النقل الذكية (ITS) | X.1389–X.1370 |
| أمن سجل الحسابات الموزع | X.1429–X.1400 |
| أمن سجل الحسابات الموزع | X.1449–X.1430 |
| البروتوكول الأمني (2) | X.1459–X.1450 |
| تبادل معلومات الأمن السيبراني | |
| نظرة عامة عن الأمن السيبراني | X.1519–X.1500 |
| تبادل مواطن الضعف/الحالة | X.1539–X.1520 |
| تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية | X.1549–X.1540 |
| تبادل السياسات | X.1559–X.1550 |
| طلب المعلومات الحدسية والمعلومات الأخرى | X.1569–X.1560 |
| تعرف الهوية والاكتشاف | X.1579–X.1570 |
| التبادل المضمون | X.1589–X.1580 |
| أمن الحوسبة السحابية | |
| نظرة عامة على أمن الحوسبة السحابية | X.1601–X.1600 |
| تصميم أمن الحوسبة السحابية | X.1639–X.1602 |
| أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية | X.1659–X.1640 |
| تنفيذ أمن الحوسبة السحابية | X.1679–X.1660 |
| أمن أشكال أخرى للحوسبة السحابية | X.1699–X.1680 |

*لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.*

**التوصية ITU-T X.1215**

# حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات


## ملخص

تقدم التوصية ITU-T X.1215 العديد من حالات الاستعمال بشأن كيفية استخدام لغة التعبير المهيكل عن معلومات التهديدات (STIX) لدعم معلومات التهديدات السيبرانية (CTI) وتبادل المعلومات.

وتصف هذه التوصية كذلك مفاهيم اللغة STIX ووظائفها. وتهدف إلى دعم مجموعة من حالات الاستعمال التي لها علاقة بإدارة التهديدات السيبرانية، بما في ذلك تحليل هذه التهديدات، وتحديد أنماط مؤشرات التهديدات السيبرانية، وإدارة أنشطة الاستجابة، وتبادل معلومات التهديدات السيبرانية. ومع توفر هذا النوع من المعلومات، يمكن اتخاذ قرار أمني بشأن كيفية تأمين الحماية من التهديدات على نحو أفضل. وتهدف هذه التوصية إلى دعم إجراء تحليل أكثر فعالية واستمرار تبادل معلومات التهديدات السيبرانية. وتندرج مجموعة مواصفات اللغة STIX [b-STIX2.0] تحت مسؤولية منظمة النهوض بمعايير المعلومات المهيكلة (OASIS).


## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1215 | 2019-01-30 | 17 | 11.1002/1000/13849 |


## مصطلحات أساسية

معلومات التهديدات السيبرانية، تبادل المعلومات، الأمن، لغة التعبير المهيكل عن معلومات التهديدات السيبرانية (STIX).


* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

## تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

## ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، كان الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2019

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

# جدول المحتويات

**الصفحة**

**التوصية ITU-T X.1215**

# حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات

## 1 مجال التطبيق

ترمي هذه التوصية إلى تقديم مختلف حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات (STIX)، وهي لغة مهيكلة لوصف معلومات التهديدات السيبرانية. وتهدف هذه التوصية إلى دعم مجموعة من حالات الاستعمال التي لها علاقة بإدارة التهديدات السيبرانية، بما في ذلك تحليل هذه التهديدات، وتحديد أنماط مؤشرات التهديدات السيبرانية، وإدارة أنشطة الاستجابة، وتبادل معلومات التهديدات السيبرانية. وعادةً ما تكون حالات الاستعمال هذه بسيطة من حيث طبيعتها ولا تنقل التعبير الكامل للغة STIX أو مرونتها. وتتضمن حالات الاستعمال عادةً بعض المقاطع الرتيبة لوصف أنشطة حالات الاستعمال وتمثيل محتوى اللغة STIX ووثائق المحتوى STIX المتحقَّق من صحتها بشكل كامل. وتعرض عملية تنفيذ لحالات الاستعمال بلغة الوسم القابلة للتوسع (XML) في شكل الإصدار 1.2 للغة STIX الذي صدر في 2016، والذي يستعمل مخطط اللغة XML، في حين يستعمل الإصدار 2.0 ترميز الأشياء باستخدام جافاسكريبت (JSON). ويُوصى باستخدام المتطلبات الوارد وصفها في الإصدار 2.0 من اللغة STIX.

## 2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا يوجد.

## 3 التعاريف

### 1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

**1.1.3 الكيان (entity)** [b-STIX2.0-Part 1]: أي شيء يكون له وجود قابل للتحديد بشكل منفصل (كمنظمة، شخص، مجموعة، وغير ذلك).

**2.1.3 كائن اللغة STIX (STIX object)** [b-STIX2.0-Part 1]: كائن الميدان STIX (SDO) أو كائن العلاقة STIX (SRO).

**3.1.3 التعبير المهيكل عن معلومات التهديدات (STIX)** [b-STIX2.0-Part 1]: نسق اللغة والتسلسل المستعمل لتبادل معلومات التهديدات السيبرانية (CTI).

**4.1.3 التبادل المؤتمت الموثوق لمعلومات المؤشرات (TAXII)** [b-STIX2.0-Part 1]: بروتوكول طبقة تطبيق للإبلاغ عن معلومات التهديدات السيبرانية.

### 2.3 مصطلحات معرّفة في هذه التوصية

لا توجد.

## 4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

CAPEC تعداد وتصنيف أنماط الهجمات الشائعة (*Common Attack Pattern Enumeration and Classification*)

COA مسار العمل (*Course Of Action*)

CnC القيادة والتحكم (*Command and Control*)

CTI معلومات التهديدات السيبرانية (*Cyber Threat Intelligence*)

CVE مواطن الضعف والتعرّض الشائعة (*Common Vulnerability and Exposures*)

C2 القيادة والتحكم (*Command and Control*)

DLL مكتبة التوصيل الدينامي (*Dynamic Link Library*)

EDR مسجل بيانات الأحداث (*Event Data Recorder*)

JSON ترميز الأشياء باستخدام جافاسكريبت (*JavaScript Object Notation*)

OS نظام التشغيل (*Operating System*)

SDO كائن الميدان STIX ("عقدة" في رسم بياني) (*STIX Domain Object*)

SMBv2 الإصدار 2 من بروتوكول مجموعة رسائل المخدم (*Server Message Block version 2*)

SRO كائن العلاقة STIX (آلية لتمثيل "حافة" في رسم بياني) (*STIX Relationship Object*)

STIX تعبير مهيكل عن معلومات التهديدات (*Structured Threat Information Expression*)

TAXII تبادل مؤتمت موثوق لمعلومات المؤشرات (*Trusted Automated exchange of Indicator Information*)

TTP تكتيك وتقنية وإجراء (*Tactics, Technique, and Procedure*)

TLP بروتوكول بسيط للحركة (*Traffic Light Protocol*)

XML لغة الوسم القابلة للتوسع (*Extensible Markup Language*)

## 5 الاصطلاحات

لا يوجد.

## 6 لمحة عامة عن اللغة STIX

### 1.6 مفاهيم اللغة STIX

بغية الاستجابة في الوقت الفعلي للتهديدات السيبرانية، ينبغي توفير ليس نظام الأمن الفردي فحسب بل وأيضاً نظام إدارة الأمن التعاوني العالمي نظراً لأن ثمة مشاكل عالمية يتعذر حلها من خلال كيان واحد وميدان واحد. ولذلك، تمثل معلومات التهديدات السيبرانية (CTI) العالمية مكوناً مهماً لبرنامج الأمن في أي منظمة ويمكن الحصول عليها داخلياً ومن مصادر خارجية. ومن بين حلول توفير معلومات التهديدات السيبرانية وتبادلها لغة التعبير المهيكل عن التهديدات السيبرانية (STIX) وهي لغة مهيكلة لوصف معلومات التهديدات السيبرانية. وتوفر اللغة STIX تمثيلات مهيكلة لمعلومات التهديدات السيبرانية تتسم بأنها معبّرة ومرنة وقابلة للتوسع والأتمتة والقراءة.

## 2.6 الكائنات في اللغة STIX

### 1.2.6 الكائنات في الإصدار STIX 1.2

تعتمد هذه التوصية سبعة كائنات للميدان STIX (SDO) معرفة في الإصدار [b-STIX1.2.1-Part 1] على النحو التالي:

1) الحملة: تمثل حملة STIX مجموعة من التكتيكات والتقنيات والإجراءات (TTP) والحوادث أو الجهات المهدِّدة التي تعبّر معاً عن نية مشتركة أو تأثير مرغوب.

2) مسار العمل: يُستخدم مكون مسار العمل STIX لنقل معلومات حول مسارات العمل يُمكن اتخاذها إما رداً على هجوم أو كتدبير وقائي قبل الهجوم.

3) هدف الاستغلال: ينقل هدف الاستغلال STIX معلومات بشأن مواطن تعرض أو ضعف تقنية، أو تشكيل خاطئ في البرمجيات أو الأنظمة أو الشبكات التي قد تكون هدفاً للاستغلال من جانب أحد الخصوم.

4) الحادث: ينقل حادث STIX المعلومات المتعلقة بحوادث الأمن السيبراني.

5) المؤشر: ينقل مؤشر STIX أنماطاً محددة قابلة للملاحظة مقترنة بمعلومات سياقية.

6) الجهة المهدِّدة: تنقل الجهة المهدِّدة STIX المعلومات التي تصف الخصم أو تحدده (أو كلاهما).

7) TTP: مصطلح عسكري يعني "التكتيكات والتقنيات والإجراءات".

### 2.2.6 الكائنات في الإصدار STIX 2.0

تعتمد هذه التوصية مجموعة من كائنات للميدان STIX (SDO) وكائنات العلاقة التي تستعملها اللغة STIX المعرفة في الإصدار [b-STIX2.0-Part 21] لتمثيل معلومات التهديدات السيبرانية.

ويعرف الإصدار STIX 2.0 اثني عشر كائناً للميدان STIX (SDO) على النحو التالي:

1) نمط الهجوم: أنماط الهجوم هي نوع من التكتيكات والتقنيات والإجراءات التي تصف الأساليب التي يحاول بها الخصوم انتهاك الأهداف.

2) الحملة: هي مجموعة من السلوكيات العدوانية التي تصف مجموعة من الأنشطة أو الهجمات الخبيثة (التي يطلق عليها أحياناً موجات) التي تقع خلال فترة من الزمن ضد مجموعة محددة من الأهداف.

3) مسار العمل: مسار العمل هو إجراء يُتخذ إما لمنع الهجوم أو لصد هجوم قائم.

4) الهوية: يمكن أن تمثل الهويات أفراد فعليين أو منظمات أو مجموعات فعلية (مثل ACME، Inc) وكذلك فئات الأفراد أو المنظمات أو المجموعات (مثل القطاع المالي).

5) المؤشر: تحتوي المؤشرات على نمط يمكن استعماله للكشف عن الأنشطة السيبرانية المريبة أو الخبيثة.

6) مجموعة الاقتحام: الاقتحام هو مجموعة مصنفة من السلوكيات العدوانية والموارد ذات الخصائص المشتركة التي يعتقد أنها منسقة بواسطة منظمة واحدة.

7) البرمجيات الضارة: البرمجيات الضارة هي نوع من التكتيكات والتقنيات والإجراءات التي تُعرف أيضاً باسم الشفرة الخبيثة والبرمجية الضارة، وتشير إلى برنامج يدخل في نظام، بشكل سري عموماً، بهدف انتهاك سرية أو سلامة أو تيسر بيانات الضحية أو تطبيقاتها أو نظام التشغيل (OS) الخاص بها أو مضايقة الضحية أو إلحاق الضرر بها على أقل تقدير.

8) البيانات المرصودة: تنقل البيانات المرصودة معلومات رُصدت عن الأنظمة والشبكات التي تستخدم المواصفة السيبرانية القابلة للملاحظة المعرّفة في الجزأين 3 و4 من هذه المواصفة.

9) التقارير: مجموعات من معلومات التهديدات التي تركز على موضوع واحد أو أكثر، مثل وصف الجهة المهدِّدة أو البرمجية الضارة أو تقنية الهجوم، بما في ذلك السياق والتفاصيل ذات الصلة.

10) الجهة المهدِّدة: الجهات المهدِّدة هي أفراد فعليون أو مجموعات أو منظمات فعلية يُعتقد أنها تعمل بنوايا خبيثة.

11) الأدوات: الأدوات هي برمجيات مشروعة يمكن أن تستعملها الجهات المهدِّدة لتنفيذ الهجمات. ويمكن أن تكون معرفة كيف ومتى تستخدم الجهات المهدِّدة هذه الأدوات، مهمة لفهم كيفية تنفيذ الحملات.

12) مواطن الضعف: مواطن الضعف هي "خطأ في البرمجيات يمكن لأحد قراصنة الحاسوب أن يستخدمه بشكل مباشر للنفاذ إلى نظام أو شبكة".

يعرّف الإصدار [b-STIX2.0-Part 2] كائنين للعلاقة STIX (SRO) على النحو التالي:

1) العلاقة: يُستعمل كائن العلاقة لربط كائنين SDO من أجل وصف كيفية ارتباطهما ببعضهما.

2) المشاهدة: تشير المشاهدة إلى اعتقاد مشاهدة شيء في معلومات التهديدات السيبرانية (مثل مؤشر، برمجية ضارة، أداة، جهة مهدِّدة).

### 3.6 الخصائص والأدوات في اللغة STIX

ينبغي أن تراعي هذه التوصية الخصائص التالية المعرفة في الإصدار [b-STIX2.0] (و/أو الإصدار [b-STIX1.2.1]):

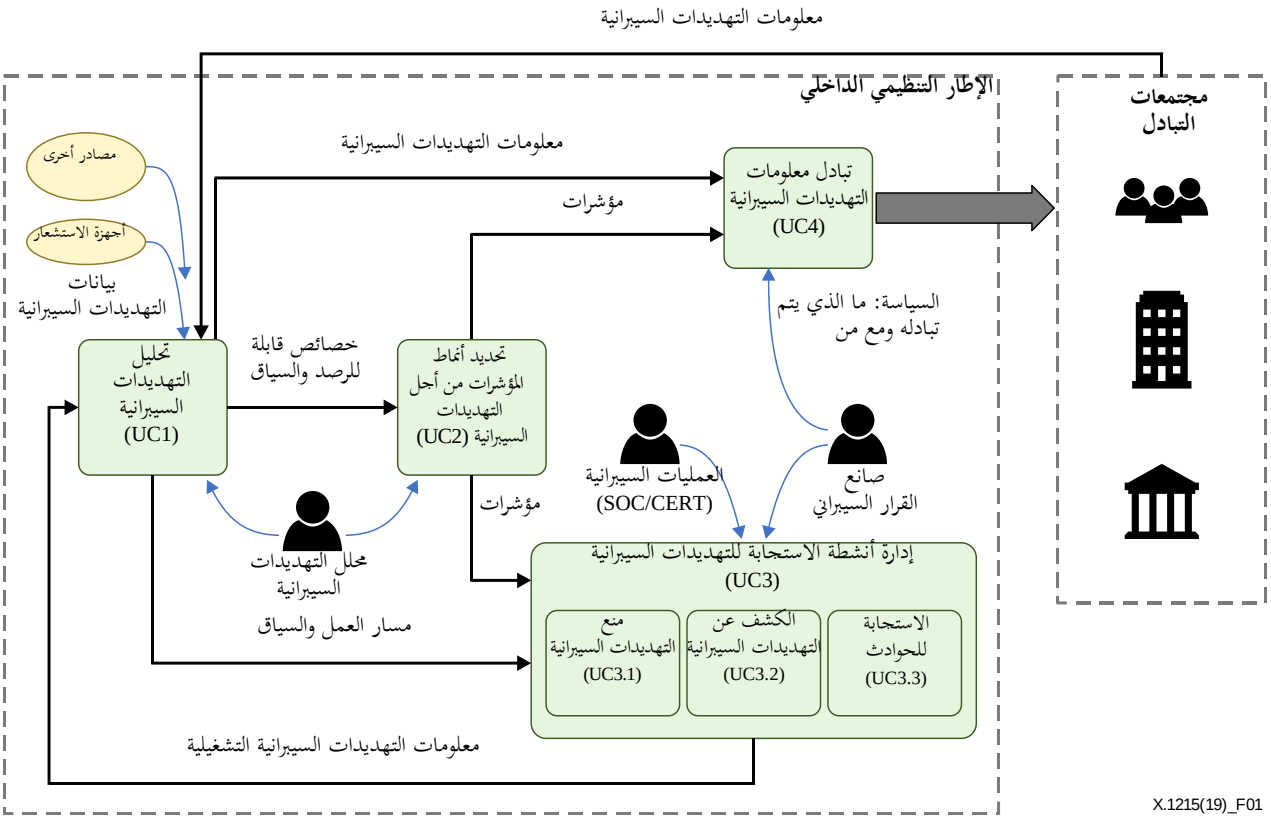
- مخططات JSON/XML: يستعمل الإصدار [b-STIX2.0] المخطط JSON [b-RFC7159] لتمثيل الكائنات والخواص الست. وبالإضافة إلى ذلك، يستعمل الإصدار [b-STIX1.2.1] مخطط XML.
- كائن الميدان STIX: تكون جميع الكائنات في اللغة STIX عالية المستوى. وتُعرف هذه الكائنات باسم STIX SDO. وتستخدم بعض خواص الكائنات إحالة إلى هوية كائن آخر مباشرة (مثل created_by_ref)، ولكن يُعبّر عن معظم العلاقات باستعمال كائن العلاقة عالي المستوى.
- كائن العلاقة STIX: يطرح الإصدار [b-STIX2.0-Part 2] كائن علاقة عالي المستوى يربط بين كائنين آخرين من الكائنات عالية المستوى بواسطة نمط علاقة مسماة.

ينبغي أن تستخدم هذه التوصية مجموعة من الأدوات المختلفة التالية المعرفة في [b-STIX2.0 tool]:

- أداة التحقق STIX: أداة التحقق STIX مورد مفيد للتحقق من مطابقة المحتوى STIX JSON لمواصفة الإصدار 2.0.
- أداة التحقق من النمط: الأنماط STIX هي تعبيرات تمثل كائنات سيبرانية يمكن رصدها ضمن الكائن SDO لمؤشر STIX. وهي مفيدة لنمذجة المعلومات التي تبين النشاط السيبراني. وتحرص هذه الأداة ببساطة على التزام قواعد تركيب النمط بتعبير النمط.
- التصور STIX: تُقدم أداة التصور STIX للمساعدة في تحويل النسق JSON إلى مخطط أكثر إيجازاً وقابلية للقراءة.
- أداة الارتقاء STIX: تساعد أداة الارتقاء على العمل كأداة للتحويل من الإصدار STIX 1.x إلى الإصدار STIX 2.0 وستوفر أفضل تحويل من 1.x إلى 2.0، حيث x = 1 و2.
- أداة مواءمة الأنماط STIX: توفر أداة مواءمة الأنماط طريقة لمقارنة بيانات STIX المرصودة بأنماط مؤشر STIX.

## 7 حالات الاستعمال المتعلقة بالإصدار STIX 2.0

تقدم هذه التوصية مختلف حالات الاستعمال بشأن الكيفية التي يمكن أن تستخدم بها اللغة STIX لدعم سياق إعداد معلومات التهديدات السيبرانية وتبادلها. وترمي إلى دعم مجموعة من حالات الاستعمال (UC) المتداولة في إدارة التهديدات السيبرانية، بما في ذلك تحليل هذه التهديدات (UC1، الفقرة 1.2.7)، وتحديد أنماط مؤشرات التهديدات السيبرانية، (UC2، الفقرة 2.2.7) وإدارة أنشطة الاستجابة للتهديدات السيبرانية (UC3، الفقرة 3.2.7) وتبادل معلومات التهديدات السيبرانية (UC4). ولا تتناول هذه التوصية تبادل معلومات التهديدات السيبرانية (UC4). ويعرض الشكل 1 مثالاً لحالة استعمال للغة STIX. ويقدم الملحق A حالة استعمال للإصدار STIX 1.2.




**الشكل 1 – لمحة عامة عن حالة استعمال للغة STIX**

### 1.7 حالة استعمال تشمل برمجية طلب الفدية (Ransomware) بالإصدار STIX 2.0

برمجية طلب الفدية (Ransomware) هي نوع من البرامج الخبيثة التي تصيب أنظمة الحاسوب وتقيد النفاذ إلى بيانات الضحية وتشترط دفع فدية. ونظراً لمحدودية النفاذ إلى الحاسوب، سوف تضطر الضحية إلى دفع فدية للكيان الذي طور البرنامج الضار من أجل إلغاء التقييد. وعادةً ما تُنفذ هجمات برمجية طلب الفدية باستخدام حصان طروادة الذي يتنكر في صورة ملف مشروع يتم خداع المستعمل لتنزيله أو فتحه عند وروده كمرفق برسالة إلكترونية.

وفي الآونة الأخيرة، بدأت برمجية طلب الفدية "WannaCry" تؤثر على الحواسيب في جميع أنحاء العالم؛ وتنتشر تلقائياً بين الحواسيب بدون تدخل من المستعمل. وعلى عكس برمجية طلب الفدية العادية التي تنتشر عبر الرسائل الإلكترونية، تستهدف البرمجية WannaCry الأنظمة المهددة المطلوبة فقط المقرر توصيلها بالإنترنت. وتقوم البرمجية WannaCry بتشفير ملفات مختلفة من قبيل ملفات الوثائق والملفات المضغوطة وملفات قواعد البيانات وملفات الآلات الافتراضية.

وتعرض هذه الفقرة الطريقة التي يمكن أن يستخدم بها الإصدار STIX 2.0 في حالة استعمال لبرمجية طلب الفدية لدعم إدارة التهديدات السيبرانية ضد برمجية طلب الفدية WannaCry.

#### 1.1.7 تحليل التهديدات السيبرانية

تقدم هذه الفقرة معلومات برمجية طلب الفدية (WannaCrypt) التي تم تحليلها والإبلاغ عنها عبر هجمات الشفرات الخبيثة على الصعيد العالمي باستعمال برمجية طلب الفدية القائمة على استغلال مواطن الضعف مع تنفيذ الشفرة عن بعد لمجموعة رسائل المخدم (الإصدار 2) (SMBv2).

##### 1.1.1.7 الهوية

يمكن تعريف معلومات المراقب بوصفها كائن هوية.

##### 2.1.1.7 البيانات المرصودة

لوحظ تلقي رسالة إلكترونية بشأن تبليغ عن شحن مع أرشيف ملفات egg و52 ميداناً من ميادين مخدم القيادة والتحكم (CnC) (يقتصر هذا المثال على ميدانيْن من ميادين المخدم CnC).

```
{
   "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"
       }
    }
}
```

**TTP 3.1.1.7**

الإبلاغ عن رصد هجوم برمجية طلب فدية استهدف حاسوباً شخصياً؛ ونمط الهجوم هو نشاط هجوم مستهدف باستعمال برمجية ضارة ويمكن إنشاء كائن علاقة يستعمل البرمجية الضارة كنمط للهجوم.

```
{
    "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"
 },
```

#### 4.1.1.7 مَواطن الضعف

يُبلّغ بأن موطن الضعف يتعلق بموطِنيْ الضعف والتعرّض الشائعين CVE-2017-0147 (CVE-)و2017-0143-CVE، وأن برمجية طلب الفدية استغلت موطن الضعف لتنفيذ الشفرة عن بعد SMBv2 (البرمجية التصحيحية 17.3.14، MS17-010) على نظام التشغيل ويندوز لشركة ميكروسوفت. ويمكن إنشاء كائن علاقة يستخدم البرمجية الضارة لاستهداف موطن الضعف هذا.

```
{
 "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"
}
```

#### 5.1.1.7 الحملة والجهة المهدِّدة

يبلَّغ بتعريف كائنيْن اثنين بوصفهما الحملة والجهة المهدِّدة من أجل المعلومات بشأن هجوم برمجية طلب الفدية. وتُحدد إمكانية إنشاء العلاقة "منسوب إلى" من أجل الحملة والجهة المهدِّدة، والعلاقة "استعمال" من أجل الحملة ونمط الهجوم والعلاقة "أهداف" من أجل الحملة وموطن الضعف.

```
{
      "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"
}
```

### 2.1.7 تحديد أنماط المؤشرات للتهديدات السيبرانية

#### 1.2.1.7 المؤشر

يُبلَّغ بأن الموقع URL الخاص بتوزيع البرمجيات الضارة يُعرَّف كنمط مؤشر للموقع URL وأنه يمكن إنشاء كائن العلاقة الذي يمثل البرمجية الضارة.

```
{
      "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"
}
```

### 3.1.7 إدارة أنشطة الاستجابة

#### 1.3.1.7 مسار العمل

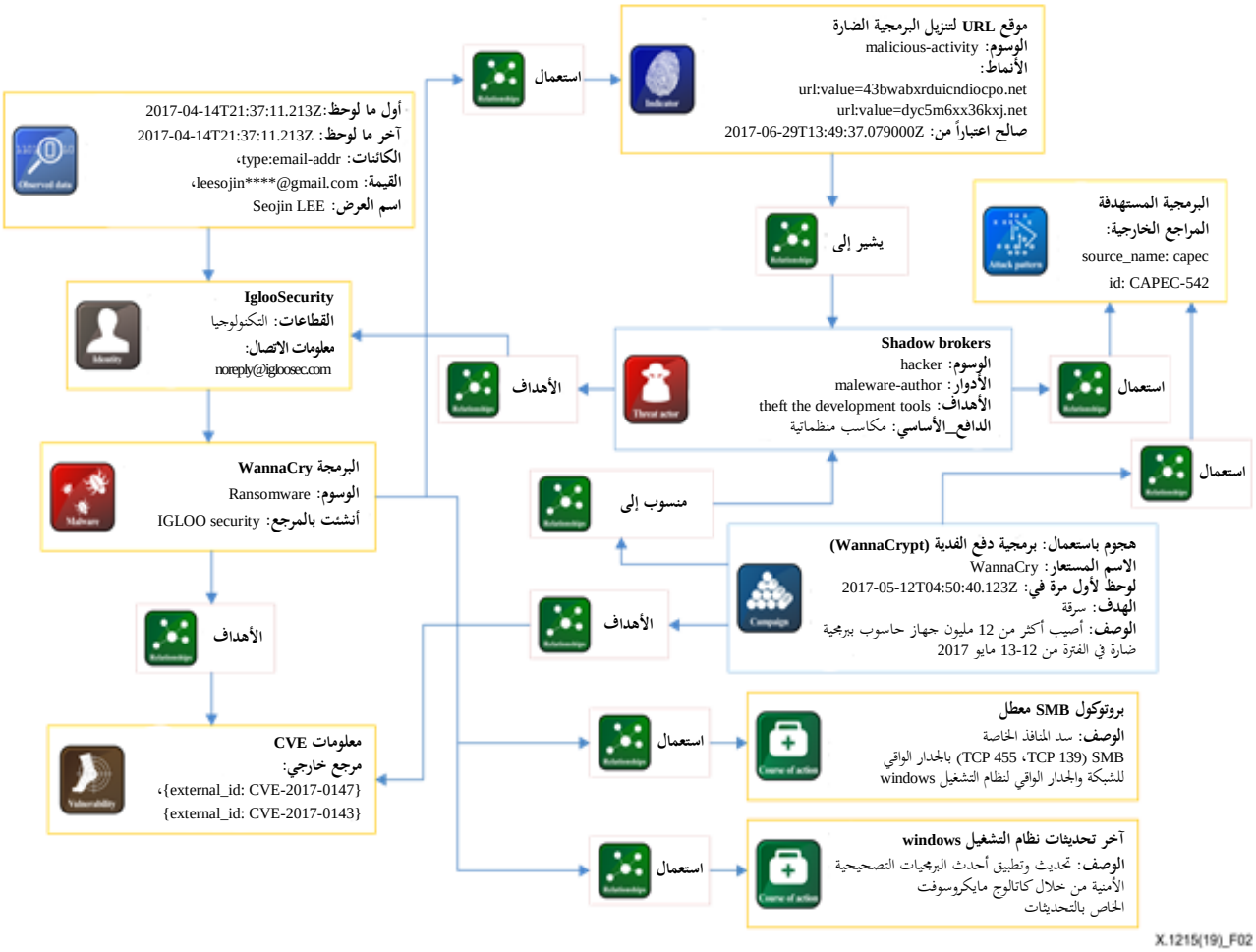
يُلاحظ أن هناك طرائق علاجية من أجل "تعطيل البروتوكول SMB" و"تصحيح موطن الضعف في البرمجية" ويمكن تعريفها بوصفها كائنات مسار العمل (COA). ويمكن إنشاء كائن علاقة لكل كائن للتخفيف من أثر البرمجية الضارة.

```
{
   "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"
 }
```

### 4.1.7 لمحة عامة عن سيناريو هجوم باستعمال مخطط العلاقة

يبين الشكل 2 العلاقة بين جميع كائنات STIX المستعملة لوصف حالة الاستعمال.




**الشكل 2 – العلاقة بين كائنات STIX من أجل وصف حالة الاستعمال**

وباختصار، يرد فيما يلي وصف للكائنات STIX المجمّعة التي تتضمن جميع الكائنات للكشف عن الهجمات الضارة التي تنفذها برمجية طلب الفدية المعروفة باسم WannaCry وتحليلها والتصدي لها.

```
{
  "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"
    }
   ]
}
```


### 2.7 حالة استعمال تتعلق بهجوم سيبراني على مكتب تغيير عملة رقمية

تصف هذه الفقرة حالة استعمال تتعلق بهجوم نفذته الجهة المهدِّدة المعروفة باسم "Lazarus APT group"، في 20 يونيو 2018 ضد مكتب تغيير عملة رقمية في كوريا.

وفي هذا السيناريو، أرسلت الجهة المهدِّدة رسالة إلكترونية احتيالية مع شفرة خبيثة لموظفي مكتب تغيير العملة الرقمية. وكانت الرسالة الإلكترونية الاحتيالية مصحوبة بملف وثائق مخفية في مرفق خبيث قادر على أن يقوم في وقت لاحق بتنزيل مكتبات توصيل دينامي (DLL) خبيثة. واستغل ملف الوثائق موطن ضعف معالج النصوص Hangul لتنفيذ المرفق ونتيجة لذلك، تم تثبيت الملف الخبيث DLL في حاسوب شخصي للمستعمل. وتمكن هذا الملف الخبيث من التحكم في الحاسوب الشخصي للمستعمل والنفاذ إلى المخدمات القابلة للنفاذ من داخل المكتب. وبالتالي، تمكن المهاجم من الوصول إلى محفظة العملات الرقمية للمكتب وسحب مبلغاً كبيراً من المال من هذه المحفظة.

#### 1.2.7 UC1: تحليل التهديدات السيبرانية

تم التبليغ عدة مرات عن هجمات على مكاتب تغيير العملات الرقمية وقعت في الفترة بين يونيو ويوليو 2018. وفي هذا السيناريو، يجري تحليل حادث القرصنة الذي تعرضت له شركة مكتب تغيير العملات الرقمية المعروفة باسم "BC-Company".

##### 1.1.2.7 الهوية

يمكن نمذجة معلومات تعرف الهوية الأساسية للمراقب بواسطة كائن الهوية. ويمكن نمذجة المنظمة التي لاحظت الحادث ومكان وقوعه ككائنات هوية.

ولتحديد مصدر كائن التقرير STIX، يتم تمثيل شركتي المراقبة الأمنية WINS وIGLOO security بوصفهما كائنيْن من كائنات الهوية. وتتم نمذجة هدف الحادث ككائن هوية مع الخاصية المعروفة باسم "BC-Company.com" وهو اسم مستعار. ويُحدد هذا الكائن في "where_sighted_refs" لكائن المشاهدة الذي سيُناقش فيما بعد، ويُستعمل كهدف للهجوم في أنماط الهجوم والبرمجيات الضارة.

```
{
"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"
},
```


### 2.1.2.7 البيانات المرصودة

تمثل البيانات المرصودة معلومات غير معالجة تولدها الآلة وهي مختلفة عن المؤشرات التي تشمل تأكيد المعلومات. ويتضمن كائن البيانات المرصودة المعلومات السيبرانية القابلة للرصد التي يتم التقاطها على الأنظمة والشبكات من قبيل عناوين بروتوكول الإنترنت والملفات والمواقع URL. وفي هذا السيناريو، تم رصد ملف. وفي مرجع آخر، تحتوي خاصية sighting_of_ref على هوية الكائن SDO الذي تمت مشاهدته والذي يمثل في هذه الحالة كائن البيانات المرصودة.

رصد مكتب تغيير العملات الرقمية ملفاً تم تسليمه عبر رسالة إلكترونية. ويُمثَّل اسم الملف وعنوان مرسِل الرسالة الإلكترونية بواسطة كائن ObservedData. وتُمثَّل كائنات البيانات المرصودة في مكان آخر في شكل كائنات مشاهدة. ويُمثل الموقع المرصود بواسطة الخاصية where_sighted_rerfs.


```
        {
            "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"
            ]
        }
```

### 3.1.2.7 التكتيكات والتقنيات والإجراءات

تصف هذه الفقرة طبيعة سلوك الخصم وكيفية تمييزه.

صدر الهجوم من مرفق برسالة إلكترونية احتيالية حيث استُخدم نوعان من الشفرات الخبيثة في الهجوم. ويتم تحديد هجمات التصيّد الاحتيالي كتعداد وتصنيف لأنماط الهجمات الشائعة (CAPEC)-163 من خلال كائن أنماط الهجمات. وتقوم الشفرة الخبيثة الصادرة من الرسالة الإلكترونية الاحتيالية بتنزيل الملف الخبيث DLL الذي يستغل موطن الضعف CVE-2015-2545. ومن ثم، توسم وسوم الكائنات الخبيثة باعتبارها وسيلة للاستغلال ونقل الفيروسات. وفي حالة الملفات DLL الخبيثة الواردة لاحقاً، يوسم remote-access-trojan كشفرة خبيثة تتحكم في الحاسوب الشخصي للمستعمل.

وتم تحديد العلاقة بين شفرتين خبيثتين كنمط "تتعلق به" للإشارة إلى وجود علاقة بين الوثيقة الخبيثة والملف DLL الخبيث.

ولتحقيق التصيّد الاحتيالي، استعمل المهاجم وثيقة مبهمة للغاية. وبما أن الهجوم يستهدف شركة تغيير العملة الرقمية، يُستخدم كائن العلاقة من النمط "الهدف".

```
{
    "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"
},
```


### 4.1.2.7 موطن الضعف

يُستعمل هنا موطن الضعف CVE-2015-2545، الذي يخفي مرفق خبيث في وثيقة معالج النصوص Hangul ويقوم بتشغيله. ويُستعمل كائن موطن الضعف لنمذجة موطن الضعف هذا. ويشير كائن العلاقة أيضاً إلى العلاقة بين الشفرة الخبيثة وموطن الضعف.


```
{
    "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"
}
```

### 5.1.2.7 الحملة والجهة المهدِّدة

قامت المجموعة Lazarus APT بنشر رسائل إلكترونية احتيالية أُدمجت فيها شفرة خبيثة لسرقة العملات الرقمية المخزنة في مكتب تغيير العملات الرقمية.

ويُمثل هدف كائن الجهة المهدِّدة في شكل "سرقة عملات رقمية" في خاصية "الأهداف". ونظراً إلى إنشاء وثيقة خبيثة، توضع خاصية "الأدوار" في خاصية الأدوار بوصفها "مؤلف البرمجية الخبيثة". وبما أنها استُخدمت لارتكاب جريمة، توضع خاصية "الوسم" في خاصية "منظمة إجرامية".

ويُمثل الهجوم على مكتب تغيير العملات الرقمية من خلال كائن الحملة وتضبط وضع خاصية "المقصد" على "السرقة".

وتُمثل تقنيات الهجوم وكائنات الشفرات الخبيثة المستعملة في حملات الهجوم من خلال كائنات العلاقات باستخدام النمط "استعمال".


```
        {
            "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"
        }
```

### 2.2.7 UC2: تحديد أنماط المؤشرات المتعلقة بالتهديدات السيبرانية

#### 1.2.2.7 المؤشر

تحدد كائنات المؤشرات الوثائق الخبيثة والملفات DLL الخبيثة. وتمثل خاصية النمط في كائن المؤشر المتعلق بالوثائق الخبيثة إما المواقع URL أو قيم الاختزال للملف من أجل تنزيل الملفات DLL الخبيثة. وفي هذا السيناريو، تمثل أنماط الملفات DLL الخبيثة في كائن المؤشر الموقع URL للقيادة والتحكم (C2) وقيمة الاختزال للملف. ويتيح ذلك التسجيل كسياسة. وتشير العديد من كائنات العلاقة من نوع "يشير" إلى العلاقة بين شفرتين خبيثتين.

```
{
    "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"
}
```


### 3.2.7 UC3: إدارة أنشطة التصدي للتهديدات السيبرانية

#### 1.3.2.7 مسار العمل

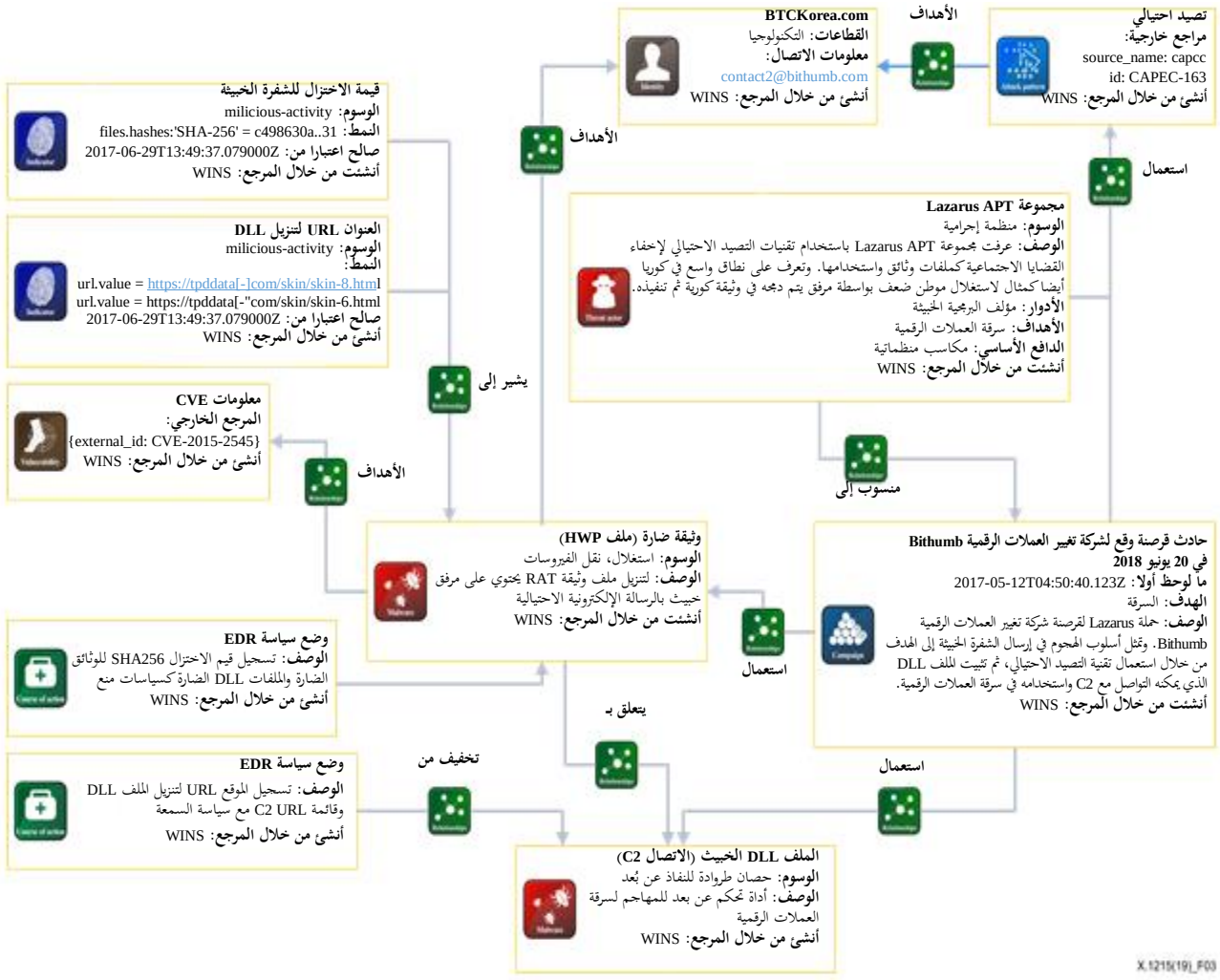
في سيناريو الهجوم هذا، يُقسم مسار العمل الذي يتّبعه فريق الاستجابة إلى الكشف والاستجابة. ويجري في البداية تنفيذ الوثيقة الضارة ثم شن الهجوم.

وتُسجَّل قيمة اختزال الوثيقة الخبيثة مع السياسة الأمنية في أداة تحليل البرمجية الخبيثة من قبيل YARA. ويمكن لمسجل بيانات الحدث (EDR) أن يكشف الهجوم عندما يُنفذ الملف مع قيمة الاختزال. وبالإضافة إلى ذلك، يبادر جهاز أمن الشبكة إلى الاستجابة عن طريق منع الحركة إلى الموقع URL لتنزيل الملف DLL الخبيث بحيث يُمنع تنزيله وبالتالي عدم سرقة حقوق التحكم للحاسوب الشخصي. وفي حال قرصنة ملف DLL خبيث، يمكن لجهاز الشبكة أن يمنع النشاط الضار بمنع الحركة إلى الموقع C2 URL.


```
{
    "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"
}
```

### 4.2.7 مخطط العلاقة والكائن المجمع

يبين الشكل 3 العلاقة بين جميع الكائنات لوصف حالة الاستعمال.




**الشكل 3 – العلاقة بين الكائنات STIX لوصف حالة الاستعمال**

وباختصار، يرد فيما يلي وصف لكائن STIX المجمّع الذي يضم جميع الكائنات اللازمة من أجل الكشف عن الهجمات السيبرانية التي تُنفذ بواسطة Lazarus وتحليلها والتصدي لها.

```
{
    "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"
            ]
        }
    ]
}
```

# الملحق A

## حالة استعمال تشمل برمجية طلب فدية بالإصدار STIX 1.2

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

يعرض هذا الملحق حالة استعمال تشمل برمجية طلب فدية لتوضيح الكيفية التي يمكن أن يستخدم بها الإصدار STIX 1.2 لدعم إدارة التهديدات السيبرانية ضد برمجية طلب الفدية WannaCry.

### 1.A تحليل التهديدات السيبرانية

تقدم هذه الفقرة معلومات محللة لبرمجية طلب الفدية (WannaCrypt) أُبلغ عنها عبر هجمات شفرات خبيثة في جميع أنحاء العالم باستعمال برمجية طلب الفدية القائمة على استغلال مَواطن الضعف عبر تنفيذ الشفرة عن بُعد لمجموعة رسائل المخدم (الإصدار 2) (SMBv2).

#### 1.1.A البيانات القابلة للرصد

رصد تلقي رسالة إلكترونية بشأن تبليغ عن شحن مع أرشيف ملفات egg و52 ميداناً من ميادين مخدم القيادة والتحكم (CnC).

```
<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>
```

**TTP 2.1.A**

أُبلغ عن رصد هجوم برمجية طلب فدية استهدف حاسوباً شخصياً؛ ونمط الهجوم هو نشاط هجوم مستهدف باستعمال برمجية ضارة، وهدف الهجوم هو خواص المعلومات في المنظمة.

```
<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>
```

### 3.1.A هدف الاستغلال

أُبلغ بأن مَوطن الضعف يتعلق بموطن الضعف (CVE-2017-0147، CVE-2017-0143) ونظام التشغيل Windows 10، وأن برمجية طلب فدية استغلت تنفيذ الشفرة عن بعد SMBv2 في نظام التشغيل Windows لشركة Microsoft.

```
<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_
010</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_
010</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_
010</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
    </stixCommon:Exploit_Target>
  </stix:Exploit_Targets>
```

### 4.1.A الحادث

أُفيد بأن التصنيف هو نفاذ غير مخول، وأن الأصول بمثابة خواص معلومات داخل المنظمة وأن الكائنات المتأثرة والتصدي للحوادث بمثابة سرقة.

```
<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>
```

### 5.1.A الجهة المهدِّدة

أُشير إلى أن المهاجم هو مطور برمجيات ضارة، وأن الدافع مالي أو اقتصادي، وأن درجة الكفاءة من مستوى خبير وأن هدف المقتحم هو السرقة.

```
<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>
```

### 6.1.A الحملة

أُشير إلى أنه تم وصف الحادث ذي الصلة والخاصية TTP والجهة المهدِّدة لتحقيق غرض الجهة المهدِّدة.

```
<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>
```

## 2.A تحديد أنماط المؤشرات من أجل التهديدات السيبرانية

### 1.2.A المؤشر

أبلغ بأنه تم تعريف مؤشرات أنماط الرسائل الإلكترونية الخبيثة والاستخلاص والعنوان URL وأن البيانات القابلة للرصد ذات الصلة والخاصية TTP والحملة مرتبطة فيما بينها.

```
<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>
```

### 3.A إدارة أنشطة الاستجابة

#### 1.3.A مسار العمل

لوحظ أن العلاج ممكن من خلال تصحيح مَواطن ضعف في البرمجية، ولا يوجد أي تأثير لتقييد التوصيل، كما أن تكلفة الاستجابة منخفضة وفعالية الاستجابة متوسطة.

```
<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</URI
Obj: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>
```

# بيبليوغرافيا


[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[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] ASIS website, *STIX specifications*. https://www.oasis-open.org/standards#stix1.2.1

[b-STIX1.2.1-Part 1] OASIS website, *STIX specifications, 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] Introduction to 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

## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

| | |
|---|---|
| السلسلة A | تنظيم العمل في قطاع تقييس الاتصالات |
| السلسلة D | مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي |
| السلسلة E | التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية |
| السلسلة F | خدمات الاتصالات غير الهاتفية |
| السلسلة G | أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية |
| السلسلة H | الأنظمة السمعية المرئية والأنظمة متعددة الوسائط |
| السلسلة I | الشبكة الرقمية متكاملة الخدمات |
| السلسلة J | الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط |
| السلسلة K | الحماية من التداخلات |
| السلسلة L | البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها |
| السلسلة M | إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات |
| السلسلة N | الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية |
| السلسلة O | مواصفات تجهيزات القياس |
| السلسلة P | نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية |
| السلسلة Q | التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما |
| السلسلة R | الإرسال البرقي |
| السلسلة S | التجهيزات المطرافية للخدمات البرقية |
| السلسلة T | المطاريف الخاصة بالخدمات التليماتية |
| السلسلة U | التبديل البرقي |
| السلسلة V | اتصالات البيانات على الشبكة الهاتفية |
| **السلسلة X** | **شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن** |
| السلسلة Y | البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية |
| السلسلة Z | اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات |

طُبعت في سويسرا
جنيف، 2019