사이버 위협 인텔리전스 공유 체계 연구

양준호[1] · 김찬진[1] · 김미연[1] · 김지혜[1] · 김종현[2] · 염흥열[1]

[1]순천향대학교 · [2]한국전자통신연구원

Cyber threat intelligence sharing system

Jun-ho Yang[1] · Chan-jin Kim[1] · Mee-yeon Kim[1] · Ji-hye Kim[1] ·

Jong-hyun Kim[2] · Heung-youl Youm[1]

[1]Soonchunhyang University · [2]ETRI

E-mail : junhos1011@naver.com / ctz_hermit@naver.com / 17kmy@sch.ac.kr /

ngswma32@naver.com / jhk@etri.re.kr / hyyoum@sch.ac.kr

요 약

첨단기술들이 실생활에 접목되면서 사이버 영역은 더욱 넓어지고 이를 대상으로 하는 사이버 위협은 크게 늘고 있다. 이러한 사이버 위협을 보다 효과적으로 방어하고 대응하기 위하여 사이버 위협 인텔리전스 공유체계가 필요하다. 사이버 위협정보 표현규격의 정의를 통하여 개별 보안관제 업체 또는 기관 등이 보유하고 있는 사이버 위협 정보의 신속한 공유와 일관된 분석, 그리고 자동화된 해석을 가능하도록 한다.

ABSTRACT

With the advent of advanced technologies in the real world, the cyber domain has become wider and cyber threats are increasing. A cyber threat intelligence sharing system is needed to more effectively defend and respond to such cyber threats. Through the definition of cyber threat information expression standard, it enables rapid sharing, consistent analysis, and automated interpretation of cyber threat information possessed by individual security control providers or organizations.

키워드

Cyber threat intelligence, Information sharing, Security, STIX 2.0

Ⅰ. 서 론

사물인터넷, 인공지능 등의 첨단기술들이 실생활에 접목되면서 사이버 영역은 더욱 넓어지고 있다. 모든 사물들이 정보를 공유할 수 있게 되면서 이를 대상으로 하는 사이버 위협 또한 크게 늘고 있다[1]. 이러한 사이버 위협을 보다 효과적으로 방어하고 대응하기 위해선 사이버 위협을 서로 공유할 필요가 있다.

본 논문에서는 고도화된 사이버 위협을 보다 효과적으로 방어하고 대응하기 위한 공유체계로서 STIX(Structured Threat Information eXpression) 2.0에 대하여 서술한다.

Ⅱ. STIX 2.0 개념 및 배경

STIX 규격은 구조화된 위협 정보 표현규격으로 사이버 위협 정보의 공유와 사이버 위협 분석이 가능하도록 사이버 위협 정보를 표현하는 규격을 정의하고 있다. 또한 개별 보안관제 업체 또는 기관 등이 보유하고 있는 사이버 위협 정보의 신속한 공유와 일관된 분석, 그리고 자동화된 해석을 가능하게 한다[2].

2017년 7월 OASIS CTI(Cyber Threat Intelligence) TC에서 채택된 STIX 2.0은 도메인 객체와 관계 객

체로 구성되어 있으며, 12가지 SDO(STIX Relationship Object)로 구조화되어 있다. 또한, 각각의 구성 객체는 다양한 세부적인 속성을 가지고 있으며 JSON으로 표현되어 있다.

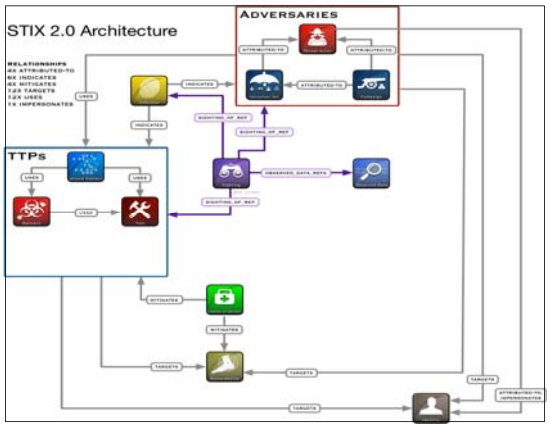

그림 1. 구조화된 위협 정보 표현(STIX 2.0) 구조

III. STIX 2.0 객체

STIX는 버전에 따라 서로 다른 스키마를 적용하고 있으며, 사이버 위협 정보 표현을 위해 STIX 2.0은 JSON을 사용한다. STIX 2.0은 도메인 객체와 관계 객체로 구성된다.

STIX 2.0 도메인 객체는 공격 패턴 객체, 캠페인 객체, 조치 객체, ID(Identity) 객체, Indicator 객체, 침입 단체 객체, 멀웨어 객체, 관측 데이터, 보고서 객체, 위협 행위자 객체, 도구 객체, 취약성 객체 등 12개로 구성되어있다[3][4][5][6].

- 공격 패턴(Attack Pattern) 객체
  공격 패턴은 악의적 사용자가 대상의 훼손을 시도하는 방법을 설명하는 TTP(Tactics, Techniques, and Procedures)의 한 형식이다.
- 캠페인(Campaign) 객체
  캠페인은 특정 목표군을 대상으로 일정 기간 동안 발생하는 일단의 악의적 활동 또는 공격을 설명하는 악의적 동작의 집합이다.
- 조치(Course of Action) 객체
  조치는 공격을 예방하거나 진행 중인 공격에 대응하기 위해 실행한 작업이다.
- ID(Identity) 객체
  ID는 실제 개인, 조직 또는 그룹은 물론 개인, 조직 또는 그룹의 부류를 표현할 수 있다.
- Indicator 객체
  Indicator는 수상한 또는 악의적 사이버 활동을 검색하는 데 사용할 수 있는 패턴을 포함하고 있다.
- 침입 단체(Intrusion Set) 객체
  침입 단체는 단일 조직이 지휘한다고 판단되는 공통 속성을 가진 악의적 동작과 리소스의 그룹화된 집합체이다.
- 멀웨어(Malware) 객체
  멀웨어는 일명 악성코드 및 악성 소프트웨어라고도 알려진 TTP의 일종이며, 피해자의 데이터, 응용 프로그램 또는 시스템에 대한 기밀성, 무결성 또는 가용성을 훼손하거나, 또는 다른 방법으로 피해자를 괴롭히거나 붕괴시킬 의도를 가지고 시스템에 삽입하는 프로그램을 가리킨다.
- 관측 데이터(Observed Data) 객체
  관측 데이터는 사이버 관측 가능 객체 사양을 사용하여 시스템과 네트워크에 대해 관측한 정보를 전달한다. 예를 들어 관측 데이터는 IP 주소, 네트워크 연결, 파일 또는 레지스트리 키의 관측 정보를 포함할 수 있다.
- 보고서(Report) 객체
  보고서는 위협 행위자, 멀웨어 또는 컨텍스트와 관련 세부 정보를 포함한 공격 기법에 대한 설명과 같이 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스의 모음이다.
- 위협 행위자(Threat Actor) 객체
  위협 행위자는 악의적인 의도를 가지고 운영된다고 판단되는 실제 개인, 그룹 또는 조직이다.
- 도구(Tool) 객체
  도구는 위협 행위자가 공격을 수행하기 위해 사용할 수 있는 합법적인 소프트웨어이다.
- 취약성(Vulnerability) 객체
  취약성은 해커가 시스템 또는 네트워크에 대한 액세스 권한을 얻기 위해 직접 사용할 수 있는 소프트웨어의 취약한 부분이다.

STIX 2.0 관계 객체는 관계성 객체와 발견 객체 등 2개로 구성되어있다[3][4][5][6].

- 관계성(Relationship) 객체
  관계성은 두 SDO가 서로 관련된 방법을 설명하기 위해 이들을 서로 연결하는 데 사용된다.
- 발견(Sighting) 객체
  발견은 Indicator, 멀웨어, 도구, 위협 행위자 등 CTI의 무언가가 발견되었다는 사실을 기술한다.

IV. STIX 2.0 유스케이스

고도화된 사이버 위협에 효과적으로 대응하기 위하여 보안 솔루션의 위협 탐지 정보를 신속히 공유하고, 대응 정책을 용이하게 수립할 수 있도록 도움을 줄 수 있는 유스케이스에 대하여 서술한다.

유스케이스는 사이버 위협 분석(UC1), 사이버

위협에 대한 지표 패턴 지정(UC2), 대응 활동 관리(UC3) 및 사이버 위협 정보 공유(UC4) 등의 4가지 유형으로 분류할 수 있다.[7]

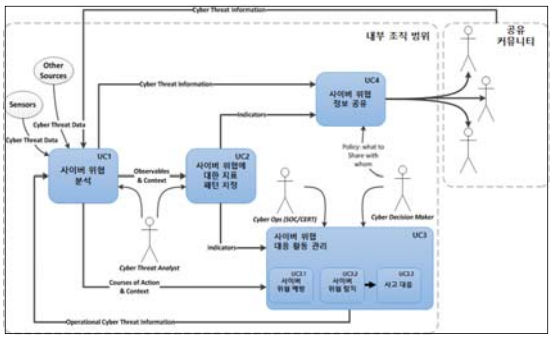

그림 2. STIX 유스케이스 개념[7]

워너크라이(Wannacry) 랜섬웨어 대응을 위한 STIX 2.0 유스케이스를 통해 각 유스케이스에 대해 서술한다[7].

일반적으로 랜섬웨어는 컴퓨터 시스템을 감염시키고 사용자의 데이터에 대한 액세스를 제한하기 위하여 암호화를 실행한 후 암호화 키에 대한 금전적 이익을 요구하는 일종의 악성 소프트웨어이다. 그러나, 워너크라이 랜섬웨어는 전자 메일 첨부 파일을 통해 확산되는 일반 랜섬웨어와는 달리 인터넷에 액세스할 때만 감염을 시도한다. 워너크라이 랜섬웨어는 문서 파일, 압축 파일, 데이터베이스 파일 및 가상 컴퓨터 파일과 같은 다양한 파일을 암호화를 한다.

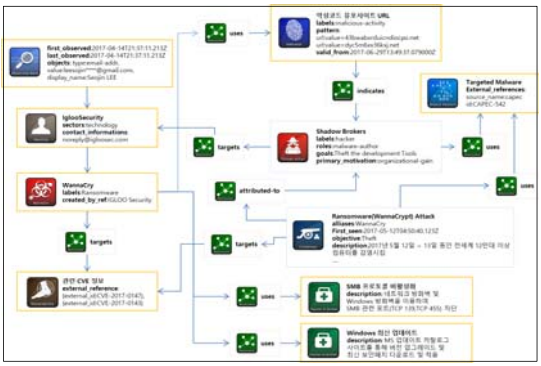

그림 3. 랜섬웨어(WannaCry) 대응을 위한 STIX 2.0 유스케이스의 다이어그램

사이버 위협 분석(UC1)은 SMBv2 원격코드실행 취약점 악용한 랜섬웨어(WannaCry) 악성코드 공격 관련 정보를 분석한다.[7]

- ID(Identity)
  관측자 정보를 Identity 객체로 정의한다.
- 관측 데이터(Observed Data)
  egg 형식의 압축 파일이 첨부된 1개의 배송 안내 메일이 수신되었으며 52개의 C&C 서버 도메인이 관측되었다.
- 공격 패턴(Attack Pattern)
  랜섬웨어 타입의 멀웨어가 수신되었으며, 공격 패턴은 랜섬웨어 워너크라이 공격 활동이다. 공격 패턴으로 멀웨어를 사용하는 관계 객체를 생성할 수 있다.
- 취약성(Vulnerability)
  Microsoft Windows의 SMBv2 원격코드실행 취약점('17.3.14 패치발표, MS17-010)을 악용한 랜섬웨어 악성코드로 CVE-2017-0147, CVE-2017-0143 취약점 정보와 연관되었으며, 멀웨어가 이 취약점을 공격대상으로 하는 관계 객체를 생성할 수 있다.
- 캠페인(Campaign), 위협 행위자(Threat Actor)
  랜섬웨어 공격에 대한 정보에 대하여 캠페인과 위협 행위자로 객체를 정의하고, 캠페인과 위협 행위자는 ‘attributed-to’ 관계를, 캠페인과 멀웨어는 ‘uses’ 관계, 그리고 캠페인과 취약성은 ‘targets’ 관계로 정의할 수 있다.

사이버 위협에 대한 지표 패턴 지정(UC2)은 멀웨어에 대한 노출을 막는 방법을 지정한다.[7]

- Indicator
  악성코드 유포 사이트 URL을 URL Watch 타입의 Indicator로 정의하고 해당 Indicator를 나타나는 관계 객체를 표현한다.

사이버 위협 대응 활동 관리(UC3)은 사이버 위협을 사전에 대응하거나 완화하는 방법을 지정한다.

- 조치(Course of Action)
  사전 대응 조치(Remedy)로는 ‘SMB 프로토콜 비활성화’, ‘Windows 최신 업데이트’ 방법이 있으며 조치 객체로 표현한다. 각각의 객체에 대해서 악성코드를 완화(mitigate)하는 관계 객체를 생성할 수 있다.

Ⅴ. 결 론

본 논문으로 stix의 개념 및 배경을 알아보았고, 객체에 따른 구조화된 위협정보를 도식화 하였다. 또한 유스케이스로서, 워너크라이 랜섬웨어에 대하여 STIX 2.0 구조로 풀어보았다.

STIX의 버전이 오를 때마다 객체들이 조금 더 상세하게 세분화되고 있다. 다만, 사이버 위협정보를 공유 받는 입장에선 발견(Sighting) 객체뿐만 아니라 이후 해당 사이버 위협이 어떻게 변경되었는지, 특이점이 추가되었는지 등에 대하여 유기적으로 사이버 위협정보를 공유할 수 있도록 진행되어야 한다.

첨단기술과 함께 사이버 영역이 계속해서 확장되고 있는 지금도 사이버 위협은 계속해서 등장하고 있다. 개별 보안관제 업체나 기관이 수많은 사이버 위협을 막기란 쉽지 않을뿐더러 한계가 존재한다. 이러한 문제를 사이버 위협 인텔리전스 공유 체계를 이용한다면 앞으로 발생할 수 있는 많은 사이버 위협에 대해서 신속한 공유와 일관된 분석, 자동화된 해석을 통해 사전 예방과 빠른 대응이 가능할 것이다.

Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00513, Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발)

References

[1] KISA. Detection Trend Report of Malicious Code Hidden Sites in the First Half of 2018 [Internet]. Available : https://www.krcert.or.kr/filedownload.do?attach_file_seq=2003&attach_file_id=EpF2003.pdf.

[2] Seongmin Bak. Structured Threat Information eXpression(STIX 2.0) part.1, TTA ICT Standardization Committee, 2018PG503-81.

[3] Nak-hyun Kim. Structured Threat Information eXpression(STIX 2.0) part.2, TTA ICT Standardization Committee, 2018PG503-82.

[4] Jong-hyun Kim. Structured Threat Information eXpression(STIX 2.0) part.3. TTA ICT Standardization Committee, 2018PG503-83.

[5] Jong-hyun Kim. Structured Threat Information eXpression(STIX 2.0) part.4. TTA ICT Standardization Committee, 2018PG503-84.

[6] Jong-hyun Kim. Structured Threat Information eXpression(STIX 2.0) part.5, TTA ICT Standardization Committee, 2018PG503-85

[7] Jong-hyun Kim. Use Cases for Structured Threat Information eXpression(STIX 2.0). TTA ICT Standardization Committee, 2018PG503-80.