사물인터넷융복합논문지 Vol. 9, No. 4, pp. 1-8, 2023 https://doi.org/10.20465/KIOTS.2023.9.4.001

사물인터넷 환경에서 침해사고 발생시 Malware에 대한 침해지표 데이터 생성 방법

이형우*
한신대학교 컴퓨터공학부 교수

Indicators of Compromise Data Generation Method for Malware on Cyber Incident Occurrence in IoT Environments

Hyung-Woo Lee*
Professor, School of Computing and Artificial Intelligence, Hanshin University

요 약 사이버 공격이 지능화·고도화됨에 따라 사물인터넷(IoT) 기기 등 이기종 시스템을 대상으로 한 사이버 공격이 발생하였을 경우 해당 침해사고 공격에 대한 상세 위협 정보를 공유할 수 있는 기법이 필요하다. 침해사고 발생시 이기종 IoT 기기로부터 수집된 디지털 포렌식 아티팩트를 침해지표(Indicators of Compromise : IoC)로 표현하고 이를 공유할 수 있는 기법이 구축되어야 한다. 특히 각종 IoT 기기를 대상으로 악성코드가 실행될 경우 사이버 위협 정보를 표현하고 CTI 시스템 간에 공유하기 위한 효율적인 침해지표 생성 방법이 제시되어야 한다. 이에 본 연구에서는 기존의 침해지표 생성 방식 및 표현 방식에 대해 분석하여 Malware에 대한 침해지표 데이터를 생성하기 위한 분류체계 및 효율적이고 규격화된 표현 방식을 제시하였다. 앞으로 제시된 침해지표 표현 및 규격화 방안을 토대로 사고관리 프레임워크 구축 시 지능화된 공격에 능동적으로 대응할 수 있을 것을 기대된다.

주제어 : 사물인터넷, 멀웨어, 침해사고, 침해지표, 사이버 공격 인텔리전트.

Abstract As cyber attacks become more intelligent and advanced, cyber attacks targeting heterogeneous systems such as Internet of Things (IoT) devices are increasing. There is a need for a technique to share detailed threat information about the incident attack. In the event of an infringement incident, a technique that can express digital forensic artifacts collected from heterogeneous IoT devices as indicators of compromise (IoC) and share them must be established. In particular, when malicious code is executed targeting various IoT devices, an efficient IoC generation method to express cyber threat information and share it among CTI systems must be presented. Therefore, in this study, the existing IoC creation method and expression method were analyzed. A classification system for generating IoC for malware and an efficient and standardized expression method were presented. Based on the proposed IoC expression and standardization method, it is expected that it will be able to actively respond to intelligent attacks when establishing an accident management framework.

Key Words : IoT, Malware, Cyber Incident, Indicators of Compromise, Cyber Threat Intelligence.

*이 논문은 한신대학교 학술연구비 지원에 의하여 연구되었음
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2023년 6월 2일 수정일 2023년 7월 24일 심사완료일 2023년 7월 28일

1. 서론

최근 사이버 공격이 지능화·고도화됨에 따라 이기종 시스템을 대상으로 한 침해사고가 발생하였을 경우 해당 공격에 대한 상세 정보를 공유할 수 있는 기법이 필요하다. APT 공격 방식 등을 이용하여 각종 IoT 기기를 대상으로 한 사이버 공격이 증가하고 있다[1-3]. 따라서 IoT 기기 등을 대상으로 한 사고관리 프레임워크 구축시 지능화된 공격에 능동적으로 대응할 수 있는 기법이 제공되어야 한다. 이를 위해서는 이기종 IoT 기기로부터 수집된 각종 디지털 포렌식 아티팩트를 침해지표(Indicators of Compromise : IoC)로 생성하고 이를 공유할 수 있는 기법이 구축되어야 한다[4-7].

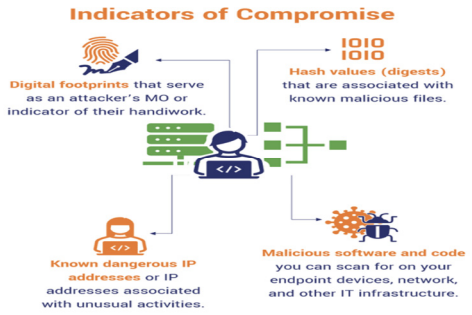
일반적으로 침해사고 발생 시 시스템 IP 주소, 도메인, URL, 해시, 이메일 주소 또는 파일 이름 등과 같은 아티팩트 들이 기본적으로 해당 공격에 대한 침해지표에 포함되는 내용이다. 그리고 이와 더불어 상세 공격 정보에 대한 내용 등이 침해지표 내에 포함되어야 한다. 따라서, 이와 같은 IoC 지표를 통해 해당 IoT 기기에서 발생한 침해사고를 명확하게 파악하고 이를 공유하여 앞으로 발생하게 될 잠재적인 위협 행위에 선제적으로 대응할 수 있게 된다[2,8,9].

이를 위해 본 논문에서는 사고관리 프레임워크 구축 개발 시 IoT 등을 대상으로 사이버 침해사고 발생시 이를 표현할 수 있는 방식인 침해지표(IoC)에 대한 표현 방식과 분류체계 및 규격화 과정을 제시하였다. 이를 통해 최근 급격히 증가하고 있는 IoT 기기를 대상으로 수집된 각종 아티팩트들을 규격화된 형태로 표현하고 이를 공유할 수 있는 체계를 제공할 수 있을 것으로 기대된다.

2. 침해지표 표현 및 분류체계

2.1 침해지표(Indicators of Compromise) 표현

침해지표(IoC)는 “여러 가지 형태의 침해사고의 흔적들을 일정한 포맷으로 정리해 놓은 문서 또는 파일” 또는 “각종 침해 혹은 감염 여부를 확인할 수 있는 디지털 포렌식 아티팩트”로 정의할 수 있다. IoC에는 일반적으로 IP 주소, 악성코드 해시 값, Host 정보 및 Internet 접속 정보, Cache 파일 정보 등이 포함되며, 정적/동적 분석을 통해 악성코드 등의 실행 흔적을 탐지하거나 조직 내부 망에서의 추가적인 감염 시스템을 찾아내는데 활용될 수 있다[7,8,10].



[Fig. 1] Representation and definition of IoC

따라서, 침해사고 대응 기능을 제공하는 CTI(Cyber Threat Intelligence) 시스템에서는 침해사고 발생시 침해지표 정보인 IoC 정보를 수집 및 저장하고 이를 지속적으로 모니터링 하고 있다. 이렇게 함으로써 최근 급증하고 있는 사이버 공격을 효율적으로 탐지하고 신속하게 탐지 및 대응 조치를 취하여 유출 발생을 방지하거나 초기 단계에서 공격을 차단/중지시키는 등 해당 기관/조직 내 피해를 최소화 할 수 있다. 결국, 침해지표(IoC)에 대한 수집, 분석 및 연관성 분석 과정을 통해 해당 조직 내에서 운영하고 있는 다른 도구로는 탐지하지 못했던 각종 보안 사고를 더욱 더 신속/정확하게 식별할 수 있고, 이를 통해서 디지털 포렌식 분석 과정을 수행하는 데 필요한 상세 리소스를 수집 및 제공할 수 있다.

2.2 침해지표(Indicators of Compromise) 예시

각종 컴퓨터 시스템 및 IoT 기기를 대상으로 랜섬웨어 공격이 발생하였을 경우 이를 침해지표(IoC)로 표현하면 아래 그림과 같다. IoC 표현 정보 내에는 해당 랜섬웨어 공격시 수집/획득된 각종 아티팩트 정보에 대한 세

Batch Scripts	
Filename	**MD5 Hash**
CheckVuln.bat	f5ef5142f044b94ac5010fd883c09aa7
Create-share-RunAsAdmin.bat	84e3b5fe3863d25bb72e25b10760e861
LPE-Exploit-RunAsUser.bat	9f2309285e8a8471fce7330fcade8619
RCE-Exploit-RunAsUser.bat	6c6c46babac6713c94debbbd454d34ef09
est.bat	e7ee8ea6fb7530d1d904cdb2d97745899
runav.bat	815bb1b0c5f0f35f064c55a1b640fca5

Executables and DLLs	
Filename	**MD5 Hash**
http_x64.exe	6c2874169fdfb30846fe7ffe34635bdb
spider.dll	20855475d20d252dda21287264a6d860
spider_32.dll	82db4c04f5dcda3bfcd75357adf98228
powershell.dll	fcf3a6eeb9f836315954dae03459716d
rpcdump.exe	91625f7f5d590534949ebe08cc728380
Filename	**SHA1 Hash**
mimikatz.exe	d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
run.exe	4831c1b113df21360ef68c450b5fca278d08fae2
zakrep_plink.exe	fce13da5592e9e120777d82d27e06ed2b44918cf
beacon.exe	3f85f03d33b9fe25bcfac611182da4ab7f06a442
win1999.exe	37178dfaccbc371a04133d26a55127cf4d4382f8
[compromised company].exe	1b2a30776df64fbd7299bd588e21573891decbe
Additional Observed Filenames	
test.exe	xxx.exe
Mim.exe	xxxw.exe
crackmapexec.exe	Services.exe
plink.exe	Systems.exe
PsExec64.exe	

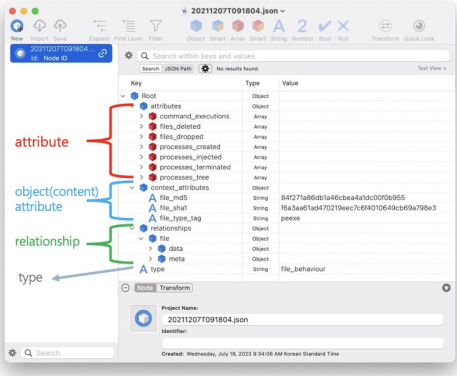
BlackCat Ransomware SHA256 Hashes:
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
731adcf2d7fb61a8335e23dbee2436249e5d575397?ec465754c6b699e9bf161
80dd44226f60ba5403745ba9d18490eb8ca12dbc9be0a317dd2b692ec041da28

C2 IPs:			
89.44.9.243	142.234.157.246	45.134.20.66	185.220.102.253
37.120.238.58	152.89.247.207	198.144.121.93	89.163.252.230
45.153.160.140	23.106.223.97	139.60.161.161	146.0.77.15
94.232.41.155			

[Fig. 2] IoC of Ransomware attack on IoT devices

부 정보를 포함하고 있다. 해당 시스템 내에서 실행된 파일의 이름, 해당 파일의 해시 값, 컴퓨터 시스템 내부 정보 등을 포함하여 And/Or 논리 구조로 침해사고에 대한 상세 정보를 표현하게 된다[10,11].

이를 좀더 상세히 설명해 보면 아래 그림과 같이 멀웨어 공격으로부터 수집된 각종 아티팩트 정보를 JSON 파일 구조를 활용하여 침해지표(IoC) 내에 포함되어 저장된다. 침해사고 관련 아티팩트는 IoC 내에는 다양한 형태와 포맷으로 표현될 수 있으며, 일반적으로 IoC 정보 내에는 침해사고 공격과 관련 속성(attribute) 정보, 상세 내용 정보와 연관성 및 데이터 타입 정보 등을 포함하고 있다.



[Fig. 3] Example of IoC Representation

2.3 악성코드 중심 침해지표 분류체계

최근 복합적이며 다형성 형태의 악성코드로 인한 공격이 증가하고 있다. 따라서 침해지표 내에 해당 악성코드에 대한 정보를 최대한 많이 포함할 필요가 있으며, 악성코드의 목적과 동작 절차에 따라서 해당 악성코드에 대한 상세 정보를 침해지표로 표현하고 이를 규격화하는 방안이 제공되어야 한다.

침해지표 표현 시 가장 중요하게 포함되어야 하는 내용 중 하나는 해당 악성코드의 수행 결과를 중심으로 하여 이를 침해지표로 표현할 필요가 있다. 일반적으로 악성코드에 대해 절차적 중심으로 과정을 살펴보면 정찰/탐색/접근/실행 및 추가작업의 5단계를 거치게 된다. 따라서 각 단계별로 발견된 아티팩트 정보를 IoC 내에 포함할 필요가 있다. 하지만, 실제로 IoT 기기에서 발견된 정보에는 악성코드가 실행된 이후 해당 기기에서 남아 있는 흔적 또는 실행 결과를 획득하게 된다. 그러므로 침해사고 발생시 결과적으로 획득되는 디지털 포렌식 아티팩트 정보를 침해지표로 표현하는 방식을 사용하는 것이 바람직하다.

멀웨어를 통해 침해사고가 발생할 경우 아래 그림과 같이 단계적으로 분류체계를 제시할 수 있다. 기존의 악성코드는 기능에 따라, 바이러스, 웜, 트로이목마, PUP로 구분할 수 있고 목적에 따라 다운로더, 드로퍼, 런처 등으로 구분할 수 있다. 또한 악성코드가 자주 사용하던 IP 주소, 포트 번호 등이 존재하며 악성코드에 대한 상세 설명 정보, 악성코드의 종류(바이러스, 웜, 트로이목마 등) 등의 정보가 IoC 내에 포함될 수 있다.

Classification

Malware
Virus
Worm
Trosan Horse
PUP

Objective

Malware
Downloader
Dropper
Launcher
Adware
Spyware
Ransomware
Backdoor
Exploit
Bot
Scareware

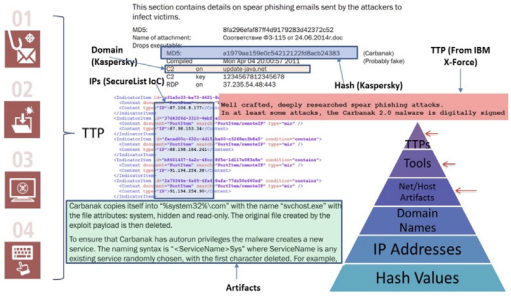
Network Port

Port #	Malware	Port #	Malware
21	trojanFore	1080	winhole
23	tiny telnet server(TTS)	1090	xtreme
25	naebiHappy	1150	orion
31	agent.paradisemasters	1234	ultors trojan
41	deepthroat foreplay	1243	backdoor G
80	www tunnel	1245	voodoo doll
119	happy99	1257	frenzy 2000
133	farnaz	1272	the matrix
137	chodemsinit (UDP)	1441	remote storm
514	RPCBackdoor	1524	trin00
555	seven eleven	1999	sub seven
666	serveU	2140	deep throat 1.3
667	snipernet	2255	nirvana
777	AIM spy	2583	wincrash
808	winHole	2773	sub seven gold 2.1
999	deep throat	3459	eclipse 2000
1001	silencer	5400	blade runner
1016	doly trojan	5880	Y3K rat
1024	netSpy	8787	backorifice 2000

Infection Symptom

Category	Sub Category
System	System Modification
	FAT Delete
	CMOS Modify
	CMOS Delete
	Memory Modify
	System Speed Down
	Auto-Execution
	Process Termination
	Rebooting
Network	e-mail transmission
	Information leakage
	Slow Network
	Message generation
	Port Open
HDD	Format
	Boot Sector Destroy
File	File Creation
	File Delete
	File Infection
	File Modification
	File Encryption
ETC	Blue Screen
	Alert
	Pop-up Window
	None

[Fig. 4] IoC Taxonomy for Malware Representation

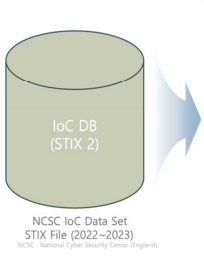


[Fig. 5] TTP related IoC Representation

3. 기존 방식의 특징 및 문제점 분석

3.1 기존 침해지표 표현의 특징 분석

우선 기존 침해지표 내에 포함된 정보에 대한 분석 과정을 수행하였다. 영국의 국립 사이버 안보 센터인 NCSC(National Cyber Security Centre)에서 제공하는 2022~2023년 사이에 침해지표(STIX 포맷) 파일을 대상으로 침해지표 내에 포함된 정보에 관하여 대략적인 통계 분석 과정을 진행하였고 그 결과는 아래 그림과 같다. 분석 결과 일반적으로 침해지표 내에는 파일 해시, URL, 파일 관련 정보 및 레지스트리 및 네트워크 관련 정보가 저장되어 있는 것을 확인할 수 있었다.



Items	Entries	%
File hash	file:hashes.MD5: 93 file:hashes.SHA-256: 90 file:hashes.SHA-1: 90	50.1%
IP/Domain/URL	ipv4-addr:value: 76 domain-name:value: 51 url:value: 40	31.3%
File Related	file:name: 57 directory:path: 4 file:parent_directory_ref.path: 5	12.3%
Registry	windows-registry-key:key: 9 windows-registry-key:values[*].name: 5	2.7%
Network Info	network-traffic:dst_ref.type: 2 #Domain & IP network-traffic:dst_ref.value: 2 network-traffic:dst_port: 1	1.1%
Etc	x509-certificate:issuer: 2 x509-certificate:serial_number: 2 mutex:name: 5 #multi thread mutex info	2.5%

[Fig. 6] Contents Frequency Analysis of NCSC IoC Data Set

이와 함께 어떤 형태의 속성 정보가 IoC에 포함되는지를 분석하기 위해 국내 주요 기관에서의 IoC 표현 체계에 대해 분석해 보았다. 아래 그림과 같이 KISA의 C-TEX, 금융보안원의 침해지표 표현 그리고 NCSC에서 정의한 IoC 표현 방식을 대상으로 공통적인 침해지표 항목을 도출해 보았다. 분석 결과 C-TEX와 금융보안원, NCSC 모두 침해지표의 표현에서 네트워크, 파일 , 페이로드, 레지스트리 및 기타 지표가 공통적으로 포함된다는 것을 확인할 수 있었다.

FBI에서 공개한 BlackCat 랜섬웨어의 침해지표 등과 같이 기존에 사용되고 있는 침해지표 표현 방식의 특징을 분석해 보면 앞서 분석한 내용과 같이 주로 파일의 이름, 해시값 등 파일 관련 정보가 IoC 내에 포함되어 있으며, 페이로드 관련 정보 및 C&C 서버의 IP 주소 정보 등 네트워크 관련 정보가 IoC에 포함된다고 볼 수 있다.

- 파일 정보: 파일명, 해시값(md5, sha1 etc), 파일 사이즈 등
- 페이로드 정보: 페이로드의 이름, 페이로드의 해시값, 사이즈 등
- 네트워크 정보: IP 주소, PORT 주소, 도메인 등
- 레지스트리: 레지스트리 키/값
- 기타: 이메일 관련 정보, yara, snort 등

type	Malware Related	Contents	OpenCTI (STIX2.1)	C-TAS	FSEC
AS	O	ASN, Network Info	O	X	O
ip-dst	O	IP address Info (C&C IP address)	O	O	O
ip-src	O	IP address Info (Attacker IP address)	O	O	O
port	O	port number (ex: 443)	O	O	O
domain	O	Domain	O	O	O
domain | ip	O	Domain | IP address	O	O	O
url	O	url	O	X	O
url	O	url	O	O	O
filename	O	File Name	O	O	O
filename-pattern	O	File Name Pattern (Directory)	X	O	X
attachment	O	Attached File	O	O	X
size-in-bytes	O	File Size (Byte)	O	X	O
md5	O	Hash	O	O	O
sha1, sha256, etc.	O	Hash	O	O	O
malware-sample	O	Malware Sample	O	O	X
malware-type	O	Malware Type	X	O	O
pattern-in-file	O	Hard-coded data	X	X	O
pattern-in-memory	O	Memory data, AES key, etc	X	X	O
pattern-in-traffic	O	Hard-coded endpoint info	X	X	O
pdb	O	pdb file	X	X	O
regkey	O	Registry Key	O	X	X
regkey | value	O	Registry Key|Value	O	X	X
http-method	O	Activated HTTP method. (ex: POST, GET...)	O	X	X
email	O	email address	O	O	O
email-attachment	O	email attached filename	O	X	O
email-body	O	email body	O	O	X
email-dst	O	email receiver (ex: ransomware)	O	O	O
email-src	O	email sender	O	O	O
vulnerability	O	CVE	O	O	O

type	Malware Related	Contents	OpenCTI (STIX2.1)	C-TAS	FSEC
target-machine	O	target info	X	X	O
cpe	O	SW info	X	O	X
Detection pattern	O	Yara, snort detection rule	O	X	O
ssdeep	O	ssdeep	O	O	X
float	O	File entropy (ex : geolocation)	X	O	O

[Fig. 7] Common Attribute on IoC Representation

3.2 기존 침해지표 표현의 문제점

기존의 침해지표 표현 체계는 침해사고의 발생 시 관측되었던 데이터에 대한 단순한 나열이라고 할 수 있다. 예를 들어 악성코드의 해시 값들 또는 공격자의 IP 주소 및 관련 정보들로만 구성된다. 하지만 이러한 정보들은 과거의 악성코드나 침해사고에 대한 탐지는 가능하지만, 현재 또는 미래 시점에서의 유사 또는 변형된 악성코드 기반 공격에 활용되기에는 어렵고 효율적으로 대응하기에도 힘들다. 또한 이러한 관측 데이터의 나열만으로는 공격자의 의도나 공격을 분석하기에 어렵다. 즉, 기존의 침해지표의 문제는 기존의 공격에 대한 탐지만을 목적으로 한다는 것이다.

따라서 기존의 침해지표의 문제점을 고찰해 보면 단순한 관측 데이터의 나열에 해당하며 침해사고에 대한 능동적 대응 또는 차단 보다는 침해사고 공격 탐지를 주요 목적으로 설정한 것이라 할 수 있다. 그리고 공격자의 관점에서 손쉽게 기존에 작성된 침해지표를 우회하거나 회

피하여 또다른 형태의 공격 수행이 가능하다는 것이다.

물론 이에 대한 해결책으로 기존 방식보다 상대적으로 많은 정보를 침해지표 내에 포함시키는 방법도 생각할 수 있으나, 오히려 너무 많은 정보를 포함할 경우에는 해당 침해지표 내 저장된 정보의 복잡성이 증가함으로써 결과적으로는 수집된 침해지표의 활용도가 떨어진다는 것을 의미한다. 따라서 적당한 정보를 추가로 넣는 방식을 채택해야 하는데, 이때 추가되는 정보는 기존 침해지표가 표현하지 못했던 정보이면서도 침해사고와 관련된 공격자의 목적과 행위를 표현할 수 있어야 한다. 따라서, 이에 맞는 해결책으로 MITRE ATT&CK에서 지원하는 TTP(Tactics, Techniques and Procedures) 정보를 중심으로 표현하는 방식을 적용해 볼 수 있다.

3.3 문제점 해결방안

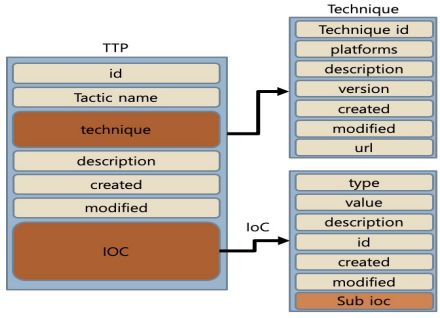
MITRE ATT&CK은 공격자의 공격 전술(Tactic)별로 이를 수행하기 위한 기술(Technique)을 절차에 따라 180여개의 세부 공격 전술을 TTP(Tactics, Techniques and Procedures) 형태로 정의한 표준 프레임워크이다. 각각의 Tactic과 Technique에 id를 부여되어 있으며 해당 id별 설명, 목표 및 해당 기술을 사용하는 공격자의 정보까지 상세하게 정리되어 있다. 따라서 침해지표를 표현할 때 MITRE ATT&CK의 TTP id를 선택적으로 포함할 수 있도록 한다면, 침해사고 발생시 공격자의 의도를 보다 상세하게 정의하고 침해지표 내에 표현 가능하며 추후 공격 자체에 대한 상세 분석 과정 역시 가능하다는 장점이 있다. 또한 각 Technique에 관한 많은 정보는 MITRE ATT&CK에 이미 정의되어 있으니, 침해지표(IoC) 내에는 해당 침해사고에 부합하는 TTP id 정보와 간단한 설명만을 기재하면 된다. 따라서 침해지표 표현을 위해 기존의 IoC 정보와 더불어 아래 그림과 같이 TTP 정보와 Malware에 대한 정보를 각각 연계할 수 있는 방안이 마련되어야 한다.

4. 개선된 침해지표 규격화 방식

4.1 제안하는 침해지표 규격화 구조

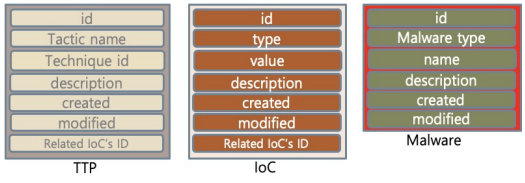
이에 본 연구에서 새롭게 제안하는 침해지표는 기존 침해지표에서 표현 가능한 정보와 함께 추가적으로 각각의 침해사고에 대한 구체적인 TTP 정보와 악성코드에 대한 상제 정보들을 포함하여 저장 및 표현할 수 있도록 구성하였다. 이는 현재 국내외에서 침해사고 정보 교환 표준으로 사용되는 STIX 포맷 구조 내에서도 attack-pattern으로 표현되는 부분이다.

새롭게 제안하는 구조는 아래 그림과 같이 침해지표의 기본 단위는 TTP 형태로 구성되며, TTP 내에 연관되는 IoC 정보를 포함하여 침해지표를 표현하는 구조이다. 상세 내용으로는 아래 그림과 같이 각각의 TTP에 해당하는 공격 기술 정보(technique)와 침해지표(IoC) 정보가 포함되는 구조이다. 이와 같은 방법을 제공할 경우 기존의 침해사고 표현 체계보다도 더욱 더 많은 공격 정보를 포함할 수 있으며 다른 CTI 시스템에게 침해사고 발생 현황 및 상세 정보를 더욱 더 명확하게 전달할 수 있게 된다.



[Fig. 8] TTP based IoC and Malware Representation Structure Diagram

새로운 침해지표 규격은 TTP 중심의 표현 방식과 다르게 TTP, IoC 및 Malware 상세 정보 표현의 3가지 기본 요소로 표현하는 방식이다. 이 경우 TTP만 제외하면 기존의 침해지표 표현 방식과 동일하며, 다만 여기에 TTP만을 추가한 방식이므로, TTP 상세 정보가 포함되지 않은 기존의 침해지표와의 호환도 가능한 방식이다.

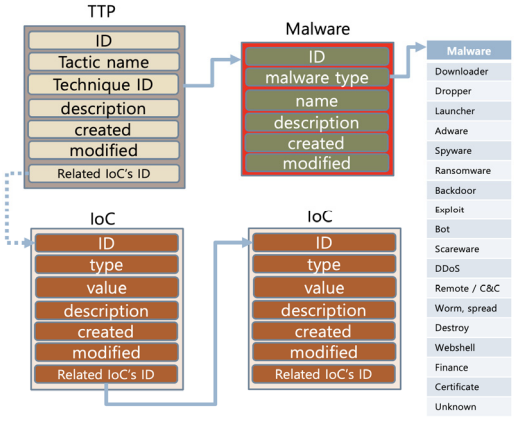


[Fig. 9] TTP, IoC and Malware Date Representation

4.2 개선된 침해지표 규격화 구조

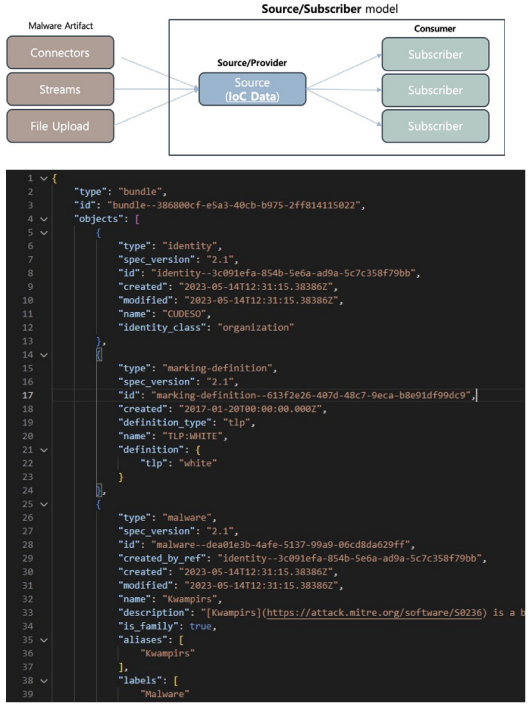
TTP는 전술명(tactic name)과 세부 기술 식별자(technique id) 및 간단한 설명으로 표현되며, IoC는 기존에 방식과 유사하게 type 속성 정보와 각각의 value로 구성된다, Malware는 malware type과 이름, 설명으로 표현되며, 이때의 malware type은 다운로더, 드로퍼 등

이다. 따라서 악성코드를 독립적으로 표현하는 것이 아니라, 직접 IoC에 포함하는 방식으로, 기존의 IoC에 악성코드를 더욱 세분화하여 전체 내용 안에 포함되도록 구성하는 방식이다. IoC에 들어가는 type에 malware-type이 들어가게 되면, IoC에 들어가는 value에는 악성코드를 정의한 객체를 집어넣는 방식으로 악성코드를 더욱 상세하게 표현할 수 있다. 따라서 기존의 침해지표 표현 방식에서는 악성코드를 일일이 자세하게 표현할 수가 없는데 반해서, 제안한 규격은 침해지표 내에 악성코드에 대한 상세 표현이 가능한 방식이다. 이를 그림은 표현하면 아래 그림과 같다.



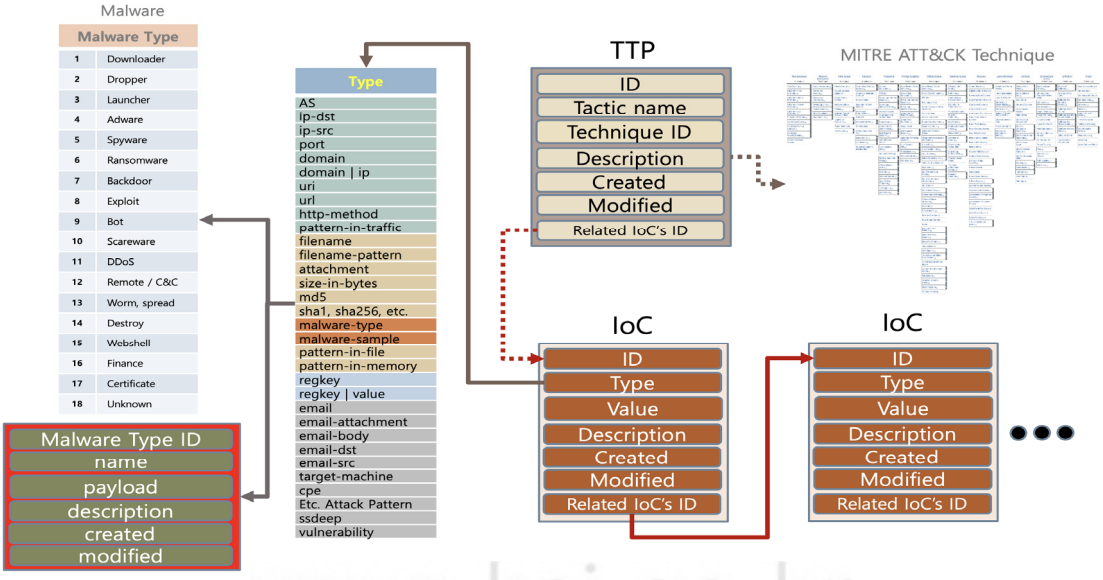
[Fig. 10] Proposed IoC Date Representation Structure

4.3 개선된 침해지표 상세 규격화 구조



[Fig. 12] Proposed IoC Date Representation Structure

본 연구에서 제안하는 개선된 침해지표 상세 구조는 아래 그림과 같다. 각각의 침해사고에 대한 TTP 정보와



[Fig. 11] Advanced IoC Date Representation Structure with TTP and Malware Information

악성코드에 대한 상세 정보들을 포함하여 표현할 수 있도록 규격화하였다. 이는 STIX 포맷 구조로 변형하여 CTI 시스템 간에 위협정보를 공유하는 과정에도 적용 가능한 구조이다. 아래 그림과 같이 CTI 시스템 간에 Source/Subscriber 모델 방식으로 위협정보를 공유하는 과정에 적용할 수 있다. 제안한 IoC 표현 방식을 적용하여 MISP 간에 위협정보를 공유한 결과는 위 그림과 같다.

4.4 기존 기법과의 비교 분석

본 연구에서 제시한 내용에 대해 기존 연구[12-18]와의 비교 분석 과정을 진행하였다. 침해지표 내 포함되는 데이터 형태와 카테고리에 대해 제안한 기법과 기존 방식을 비교하면 아래와 같다.

	type	Malware Related	OpenCTI (STIX2.1)	C-TAS	FSEC
Nwtwork	AS	O	O	X	O
	ip-dst	O	O	O	O
	ip-src	O	O	O	O
	port	O	O	O	O
	domain	O	O	O	O
	domain | ip	O	O	O	O
	uri	O	O	X	O
	url	O	O	O	O
	http-method	O	O	X	X
	pattern-in-traffic	O	X	X	O
File & Payload	filename	O	O	O	O
	filename-pattern	O	X	O	X
	attachment	O	O	O	X
	size-in-bytes	O	O	X	O
	md5	O	O	O	O
	sha1, sha256, etc.	O	O	O	O
	malware-sample	O	O	O	X
	malware-type	O	X	O	O
	pattern-in-file	O	X	O	O
	pattern-in-memory	O	X	X	O
Registry	regkey	O	O	X	X
	regkey | value	O	O	X	X
ETC	email	O	O	O	O
	email-attachment	O	O	X	O
	email-body	O	O	O	X
	email-dst	O	O	O	O
	email-src	O	O	O	O
	target-machine	O	X	X	O
	cpe	O	X	O	X
	기타 탐지 패턴	O	O	X	O
	ssdeep	O	O	O	X
	float	O	X	O	O
	vulnerability	O	O	O	O

[Fig. 13] IoC Type and Category Comparison

또한 아래 그림과 같이 본 연구에서 제시한 침해지표 표현 방식과 기존 관련 연구[16,17,18]와의 비교 분석 과정을 진행하였다. 사이버 침해사고 발생시 위협정보를 침해지표로 표현하는 과정에서의 복잡도, 신뢰도, 확장성, 신규성 및 유연성에 대해 비교하였다. 그리고 침해지표를 통한 위협정보 전파 속도, 중복처리 성능, 위협정보에 대한 관리 및 탐지 성능에 대해 5 단계 척도로 각각 측정하고 이를 종합하여 침해대응 정도를 측정하였다. 비교 결과 제안한 기법이 기존 3개 기법보다 우수한 것으로 나타났다.

Contents	Open IoC	C-TAS	FSEC	Proposed IoC
Complexity	5	4	4	4
Reliability	3	4	5	5
Scalabiity	3	3	4	5
Novelty	2	3	4	5
Flexibility	3	3	4	5
Propagation Speed	3	5	4	4
Duplicate Processing	2	3	4	4
Management Function	3	3	4	4
Detection Performance	2	3	3	4
Incident Response (Comprehensive)	2.8/5 (56%)	3.4/5 (68%)	4.0/5 (80%)	4.4/5 (88%)

[Likert scale (5-poing scale)] : 1 strongly disagree, 2 disagree, 3 neutual, 4 agree, 5 strongly agree

[Fig. 14] Comparative analysis of each IoC Mechanism

5. 결론

최근 사이버 공격이 점차 지능화/고도화됨에 따라 사이버 공격 발생시 해당 공격에 대한 상세 정보를 위협 정보로 생성하여 이를 CTI 시스템 간에 공유하고, 사이버 공격으로 부터 발생한 공격을 위협정보로 전파할 수 있는 시스템이 개발되어야 한다. 피해 상황을 전파하기 위해서는 침해사고 발생시 각각의 공격으로 인해 수집되는 아티팩트 정보를 명확하게 표현할 수 있는 방법이 구축되어야 한다. 하지만, 현재까지 사용가능한 침해지표 표현 구조(표현 방식, 저장구조 및 포맷)인 경우 해당 침해사고에 대해 명확하게 표현하고 있지 못하다는 문제점이 존재한다.

따라서, 본 연구에서는 사물인터넷 기기를 대상으로한 침해사고 공격 발생시 이에 대한 정보를 명확하게 표현할 수 있는 방법 및 규격화 방안을 제시하였다. 제안한 내용은 기존의 방법 보다도 침해사고 공격에 대해서 상세 정보를 포함할 수 있으므로 최근 급증하는 사이버 공격에 능동적으로 대응할 수 있는 기능을 제공한다.

REFERENCES

[1] Abu, S.; Selamat, S.R.; Yusof, R.; Ariffin, A., "An Enhancement of Cyber Threat Intelligence Framework", J. Adv. Res. Dyn. Control. Syst, 10, pp.96-104, 2018.

[2] Harrington, C., "Sharing indicators of compromise: An overview of standards and formats", Emc Crit. Incid. Response Cent. 2013.

[3] Brown, R.; Lee, R.M. The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey; SANS Institute: Bethesda, MA, USA, 2019.

[4] A. Pala and J. Zhuang, "Information sharing in cybersecurity: A review," Decis. Anal., Vol.16, No.3, pp. 172-196, 2019.

[5] S. Ghernaouti, L. Cellier, and B. Wanner, "Information

sharing in cybersecurity : Enhancing security, trust and privacy by capacity building," 2019 3rd Cyber Secur. Netw. Conf. CSNet, pp.58-62, 2019.

[6] Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C., "Guide to Cyber Threat Information Sharing", NIST Special Publication 800-150, 2016

[7] Mavroeidis, V., Bromander, S., "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence", Intelligence and Security Informatics Conference (EISIC), pp.91-98, 2017

[8] Burger, E. W., Goodman, M. D., Kampanakis, P., Zhu, K. A., "Taxonomy model for cyber threat intelligence information exchange technologies", ACM Workshop on Information Sharing & Collaborative Security, pp.51-60. 2017.

[9] Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E., "Cyber threat intelligence sharing: Survey and research directions", Computers & Security Vol.87, pp.1-13, 2019.

[10] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", IEEE Communications Surveys & Tutorials, Vol.22, No.2, pp.1191-1221, 2020.

[11] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. H. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions", Computer & Security, Vol.111, 2021.

[12] H. W. Lee, "Cryptography Module Detection and Identification Mechanism on Malicious Ransomware Software", Journal of Internet of Things and Convergence, Vol.9, No.1, pp.1-7, 2023.

[13] T. Y. Kim, K. Han, S. O. Hwang, "A New Association Rule Mining based on Coverage and Exclusion for Network Intrusion Detection", Journal of Internet of Things and Convergence, Vol.9, No.1, pp.77-87, 2023.

[14] H. W. Lee, "Analysis of Cyber Incident Artifact Data Enrichment Mechanism for SIEM Model Analysis of AI-Based Water Pipeline Improved Decision", Journal of Internet of Things and Convergence, Vol.8, No.5, pp.1-10, 2022.

[15] J. K. Park, J. Kim, "Comparison of encryption algorithm performance between low-spec IoT devices", Journal of Internet of Things and Convergence, Vol.8, No.1, pp.79-85, 2022.

[16] Open IOC: Back to the Basics, Mandiant, https://www.mandiant.com/resources/blog/openioc-basics

[17] C-TAS, Cyber Threat Analysis and Sharing System, https://cshare.krcert.or.kr:8443/index

[18] FSEC, Financial Security Institute API, https://www.fsec.or.kr

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

〈관심분야〉

사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식, 지능형 사이버공격 대응