사이버 공격 확산 방지 및 신속한 대응을 위한 사이버 위협 인텔리전스 분석 기술

김병익, 이슬기, 김경한, 박순태
한국인터넷진흥원 보안위협대응R&D팀
e-mail:{ kbi1983, sglee, kookie, stpark12 }@kisa.or.kr

Cyber threat intelligence analysis technology to prevent the diffusion of cyber attacks

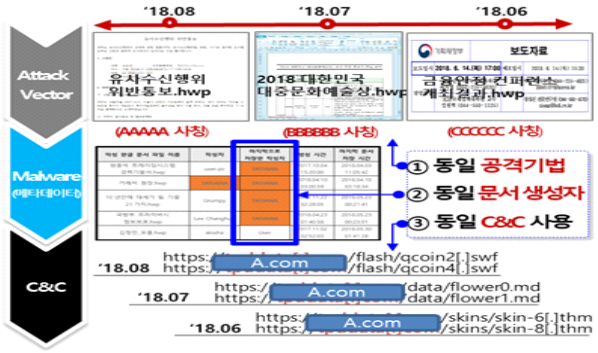
Byung-Ik Kim, Seul-Gi Lee, Kyeong-Han Kim, Soon-Tai Park
Security Threat Response R&D Team, Korea Internet & Security Agency

요 약

최근 국내에서 발생되고 있는 사이버 공격들의 대부분은 기존 보안장비로 탐지가 어려운 지능형 공격으로 2017년 한 해 동안 발생한 사이버 공격의 경제적 피해액은 약 77조원에 달하고 있다. 또한 이러한 공격을 탐지하는데 평균 145일 정도가 소요되고 있으며 국내 기업 중 약 70% 가량은 사이버 공격을 적극적으로 대응하고 있지 않다. 이러한 공격들은 대부분 과거에 발생한 공격의 변형이거나, 특정 공격 집단이 수행하는 유사/변종 공격들이다. 이러한 사이버 공격을 사전에 탐지하거나 이미 발생된 공격의 변형된 공격을 신속하게 탐지하기 위해서 본 논문에서는 기존 사이버 공격에 사용된 다양한 정보들을 능동적으로 수집하여, 이들 간의 연관성을 분석하고, 실시간으로 유입되는 공격 의심정보와 비교분석하는 기술을 제시한다.

1. 서론

최근 국내에서 발생되고 있는 사이버 공격들의 대부분은 APT 공격[1,2], 워터링 홀(Watering Hole)[3] 공격 등 기존 사이버 공격들과 다른 지능형 공격으로 2017년 한 해 동안 발생한 사이버 공격의 경제적 피해액은 약 77조원에 달하고 있다. 또한, 이러한 공격을 탐지하는데 평균 145일 정도가 소요되고 있으며 국내 기업 중 약 70%가량은 사이버 공격을 적극적으로 대응하고 있지 않다[4].



(그림 1) '18년도 주요 E-Mail 기반 APT 공격 분석[5]

이러한 지능화된 공격의 예로 2018년도 6월부터 8월까지 3개월간 정부 기관 3곳을 사칭한 악성 E-Mail 기반의 APT 공격이 발생하였다[5]. 이들 공격은 (그림 1)과 같이 대부분 한글 문서 기반의 악성코드를 첨부한 E-Mail을 발송하였으며, 동일한 공격 기법과 문서 생성자, 동일한 명령 제어(C&C) 서버를 이용한 공격으로 분석되었다. 이들 공격은 기존에 성공한 공격을 변경하거나 수정한 공격들이다. 이러한 공격은 대부분 기존 성공한 공격의 변형된 공격이지만 정확한 공격 탐지 정보(Signature)를 사전에 확보하지 못해 유사 공격들을 탐지하지 못하고 있다. 따라서 본 논문에서는 이러한 문제를 해결하고자 기존 발생된 사이버 공격의 정보들 기반의 유사 공격 정보 분석, 공격에 악용된 자원들 간의 연관성 분석 및 공격 간의 연관성 분석을 통해 알려지지 않은 유사/변종 사이버 공격을 실시간으로 대응하는 시스템을 제안한다.

2. 사이버 위협 인텔리전스 분석 시스템

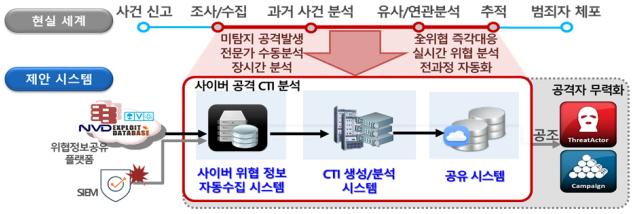
2.1 사이버 위협 인텔리전스 정의 및 동향

가트너에서는 2013년 사이버 위협 인텔리전스(Cyber Threat Intelligence, CTI)에 대해서 '사이버 공격으로부터 자산(Asset)에 대한 위협 대응을 위해 의사결정에 활용할 수 있는 정보'로 정의하고 있으며 세부적으로 CTI 정보를 제공하는 TIS(Threat Intelligence Service)와 CTI 정보를 이용하여 실제 기업/조직에 적용하는 TIP(Threat Intelligence Platforms)로 구분된다. TIS 제품으로는 FireEye사의 iSIGHT와 Symantec의 DeepSight가 대표적이며, TIP 제품으로는 IBM의 Watson Advisor가 대표적이다. 제안하는 시스템은 TIP 제품군에 속하는 기술로 기

존 TIP 제품에서 단순히 과거 사이버 공격과 유사한 공격이 탐지되었을 때 대응할 수 있는 정보를 제공하는 반면, 본 제안 시스템은 단순히 대응 정보를 제공하는 것뿐만 아니라 알려지지 않은 의심 정보 기반으로 공격 여부 및 공격자 추정 정보를 제공하여 사이버 공격 분석가의 분석 부하를 감소시킬 수 있다.

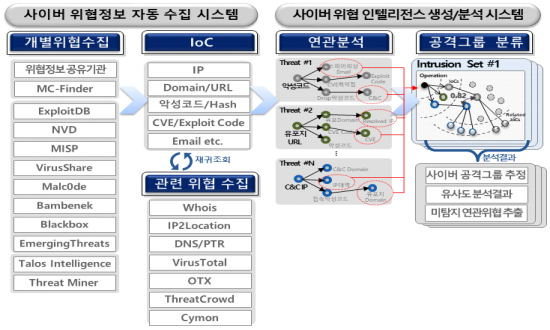
2.2 제안 시스템 개요

현실 세계에서 범죄가 발생하면 범죄에 대한 조사 및 증거 수집이 이루어지고, 과거에 발생한 유사 사건이 있는지 탐지한다. 관련 사건을 탐지한 이후 범죄자를 추정 및 추적하여 범죄자를 체포하게 된다. 사이버 세계에서도 동일한 절차를 거쳐서 공격자 추정 및 탐지를 수행한다. 본 논문에서 제안하는 시스템은 현실 세계에서 이루어지는 과정 중 정보 수집, 수집된 정보와 유사한 과거사건을 조사하는 수집 시스템과 수집된 정보를 분석하여 공격자를 추정하는 분석 시스템으로 구성되어 있다. 본 제안 시스템을 사용할 경우, 기존 미탐지 사이버 공격 대응, 실시간 알려지지 않은 위협 탐지, 전 자동화로 인한 분석 시간 단축 및 사이버 공격 분석 전문가의 업무 경감 등의 효과를 달성할 것으로 사료 된다. (그림 2)는 현실 세계에서의 범죄 조사 과정과 사이버 세계에서의 제안 시스템이 담당하는 범위를 나타내고 있다.[7]



(그림 2) 현실 세계에서의 조사과정과 제안 시스템 범위[7]

(그림 3)은 본 논문에서 제안하는 시스템의 하위 시스템과 해당 시스템이 처리하는 데이터 흐름을 간략하게 나타내고 있다. 그림에서 보는 것과 같이 수집 시스템은 다양한 정보들을 수집하여 관리하고 있으며, 분석 시스템은 수집된 정보를 기반으로 공격자 집단을 추정/분류하는 기능을 가지고 있다.



(그림 3) 제안 시스템 데이터 흐름 요약

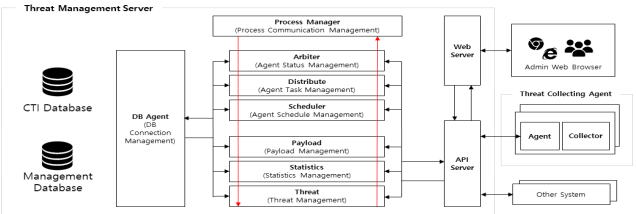
2.3 사이버 위협 정보 자동 수집 시스템

다양한 사이버 공격 정보를 공유하고 있는 서비스(OSINT - Open Source INTelligence)[8]를 통해서 기본적인 공격 정보들을 수집한다. 한국인터넷진흥원의 C-TAS 시스템과 외국에서 운용하고 있는 VirusSare, Bambenek, Cymon 등 총 19개의 채널을 통해 공격 IP, 악성코드 정보, 악성 URL, 악성 E-Mail 등 39종의 데이터를 수집 관리하고 있으며 2016년 10월부터 2019년 8월까지 약 1.5억건의 데이터를 DB화 하였다.

<표 1> 주요 연관정보 수집 및 분석 채널[9]

조회 채널	Whois	분석 채널	VirusTotal
	DNS / PTR record		Anubis
	Google 이력정보		Wepawet
	IP2Location		Cuckoo Sandbox
	SLD (Second Level Domain)		악성코드 유사도 분석시스템(KISA)
	TLD (Top Level Domain)		

대부분의 유사/변종 사이버 공격들은 기존에 사용했던 악성 ICT 정보를 변형하거나 재사용하고 있다. 따라서 본 시스템은 <표 1>의 채널들을 통해서 단순히 기존 공격 정보를 수집하는 것뿐만 아니라 공격에 사용된 유사/연관 정보들을 자동으로 수집하여 인텔리전스 분석에 활용한다.[9] 이러한 유사/연관 정보를 수집하기 위해서 Whois 정보, 동일 대역 IP 정보, 유사 도메인 정보, 유사 악성코드 정보들을 재귀적으로 수집하고 있다.



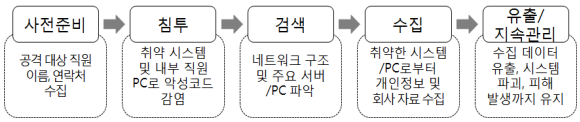
(그림 4) 수집 시스템 세부 구성도

(그림 3)은 제안한 사이버 공격 정보 자동 수집/관리 시스템의 세부 구성을 도식화 한 그림이다. 이렇게 수집된 사이버 공격 정보 및 연관 정보들은 사이버 위협 인텔리전스 분석 시스템으로 전송된다.

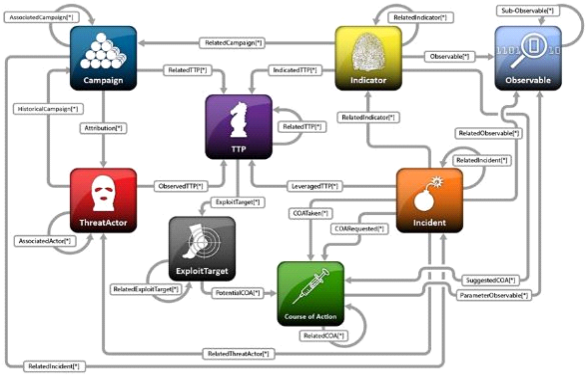
2.4 사이버 위협 인텔리전스(CTI) 생성/분석 시스템

수집 시스템에서 수집된 위협 정보들을 이용하여 각 사이버 공격을 재구성한다. 사이버 공격을 재구성하는 이유는 실제 공격이 수행된 시간을 정확하게 알 수 없으며, 시스템에서 수집된 정보들의 분석 시간 또는 공유 시간이 상이하여 이를 공격 순서에 따라 재정립할 필요가 있기 때문이다. 따라서 사이버 위협 인텔리전스 생성/분석 시스템에서는 수집 시스템에서 수집된 사이버 위협 정보와 연관된 정보들을 공격 순서에 따라 재정리를 하고 있다. 이

를 위해서 본 시스템에서는 공격모델을 설정하고 있으며, 이러한 공격모델은 STIX(Structured Threat Information Expression) 2.0[10,11]과 APT 공격 순서[1,2]를 중심으로 사이버 공격모델을 설정하였다.

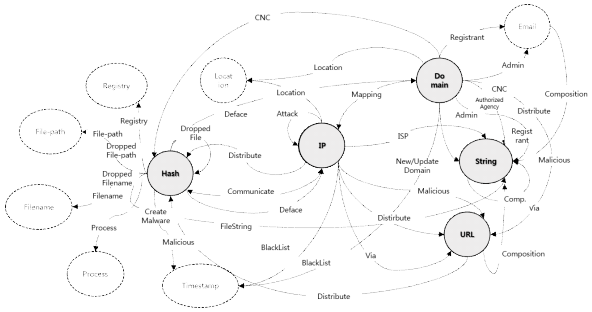


(그림 5) APT 공격 순서 및 흐름

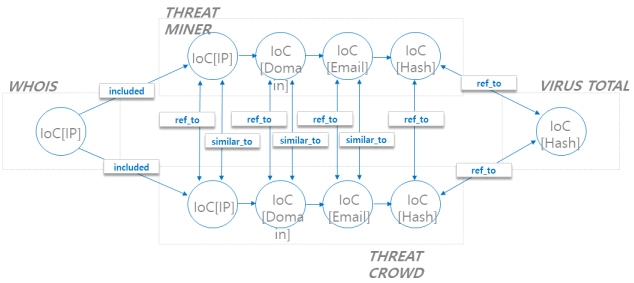


(그림 6) STIX 구조[10,11]

수집된 정보들을 구조화한 이후, 동일 사이버 공격에서 악용된 ICT 자원들과 이들 자원과 유사한 자원 간 연관성에 대해서 분석을 수행한다. 연관성을 분석하는 이유는 대부분의 사이버 공격들은 기존 공격을 그대로 재현하거나 온전히 새로운 공격을 만들어서 수행하는 것이 아니며, 대부분 기존의 성공한 사이버 공격의 주요 정보들을 수정, 변경하여 재사용하기 때문이다. 따라서 기존 사고에서 사용된 정보들과 유사하거나 연관성이 있는 정보 또는 데이터들이 이후 공격에서 사용될 확률이 높기 때문이다. (그림 7, 8)은 분석 시스템에서 사용되고 있는 주요 ICT 자원의 연관성 정보들을 도식한 그림이다.[9] 예를 들어서, 악성 IP의 경우, 해당 IP가 속한 C-Class 정보, 연결된 Domain / URL 정보, 유포된 악성코드 정보, 명령 제어 서버(C&C) 등이 있으며 IP뿐만 아니라 Domain / URL / 문자열 정보 및 악성코드 분석 정보, URL 등 사이버 공격에 사용되는 주요 정보들에 대해서 관련된 연관성 및 유사성을 자동으로 분석하고 있다.

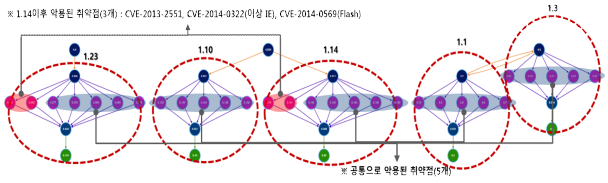


(그림 7) 사이버 위협 간 연관정보 분석 모델[9]



(그림 8) 연관성 연결 정보 예시

이렇게 각개별 사이버 공격의 연관 분석된 정보들은 사이버 공격 간의 연관성 및 유사성 분석에 사용된다. 즉, 개별 사이버 공격에 포함된 자원들이 다른 사이버 공격에 존재하는 ICT 자원과 어떤 연관성과 유사성을 보이는지 확인하여 해당 사이버 공격들이 동일 공격 그룹이 수행한 공격인지 공격 방식이 유사한 공격 그룹에서 수행하는 공격인지 식별할 수 있는 기반정보를 제공할 수 있다.
신규 위협 정보 수집 또는 사이버 공격 분석 정보가 유입될 경우, 주기적으로 연관성 및 유사성 분석을 수행하여 최근에 발생 된 정보들이 과거의 어떤 사이버 공격과 연관이 있는지 확인할 수 있는 기반정보를 제공할 수 있다.



(그림 9) 사이버 공격 연관성 분석 결과(KISA)[9]

(그림 9)는 과거 한 달 사이에 발생한 사이버 공격을 (그림 7, 8)과 같이 각 공격자원에 대한 연관성 분석한 결과이다.[9] 그림에서 나타난 것과 같이 사이버 공격에 사용된 Domain의 문자열이 유사하며 짧은 시간 동안 공격 대상 취약점을 변경하면서 공격을 수행하였다. 이는 최초 발생 된 공격이 분석되어 각종 보안장비에서 탐지/차단됨에 따라 도메인 변경 및 공격 대상 취약점을 변경하면서 공격을 수행한 것으로 추정된다. 이들 5개의 공격은 동일 공격 그룹이 수행했을 것으로 추정되며, 향후 이와 비슷한 공격이 발생 될 경우, 유사한 도메인으로 접근을 금지하고 웹 서버의 취약점을 제거하는 활동이 필요하다는 것을 의미 한다.

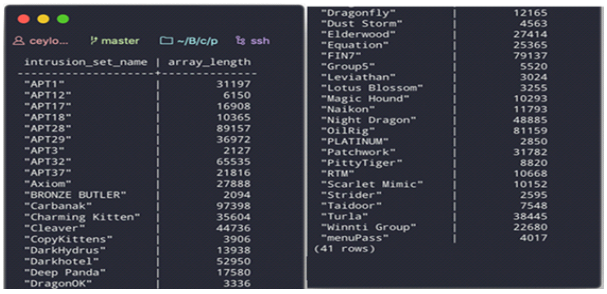
<표 2> 유사 공격 분류 알고리즘 별 분석 속도 및 정확도

사용 알고리즘	수행시간 (s)	클러스터 (건)	정확도 (0-1)
Louvain Method	8.8	571	0.9718
Girvan Newman	611	569	0.9706
Infomap	13.3	599	0.9669

또한, 기존 연구[7,9]는 유사한 공격을 탐지하기 위해 PageRank 분석 알고리즘 및 Betweenness Centrality 알고리즘 을 이용한 공격 분류를 수행했다. 이번 연구에서는 앞선 연구에서 나타난 분석 속도 문제 및 유사공격 그룹 클러스터오류 등을 해결하고자 Louvain Method, Girvan Newman, Infomap 알고리즘을 사용하여 유사 공격 클러스터링 정확도 및 분석 속도를 향상시켰다.

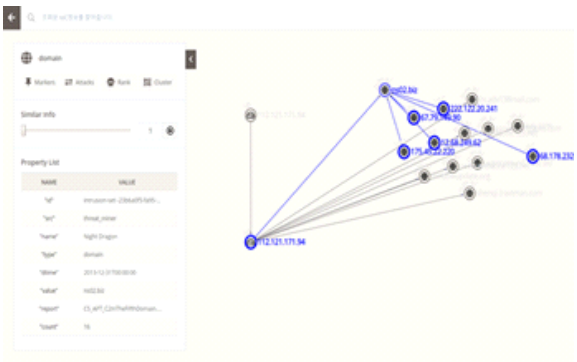
3. 시스템 구현 결과

2장에서 소개한 제안 시스템을 통해 총 41개의 공격 그룹들을 추정하였으며 그 결과는 (그림 10)과 같다. 각 공격 그룹명은 APT 분석 보고서 및 개별 공격 분석 보고서에서 명명한 명칭들이며, 시스템에서 수집된 정보와 동일, 유사한 정보를 가진 공격 그룹의 수를 계산한 결과이다.



(그림 10) 사이버 공격 그룹 추정 결과

또한, 한국인터넷진흥원에서 수집된 악성 E-Mail 정보들을 연관 분석한 결과, 기존 연관성이 없어 보이는 E-Mail 간의 연관성을 실시간으로 확인할 수 있었다. (그림 11)은 악성 E-Mail의 분석 결과 일부이다.



(그림 11) 악성 E-Mail 분석 결과 예시

4. 결론 및 향후 연구

본 논문에서는 기존 탐지나 대응이 어려운 유사/변종 공격을 효과적으로 분석/대응할 수 있는 시스템을 소개하였다. 본 시스템은 사이버 위협 정보 자동수집 시스템과 사이버 위협 인텔리전스 생성/분석 시스템으로 구성되어 있다. 사이버 위협 정보 자동수집 시스템은 사이버 공격에 악용된 ICT 자원을 1차적으로 수집하고 수집된 정보와 유사하거나 관련 있는 정보를 재귀적으로 수집한다. 사이버 위협 인텔리전스 생성/분석 시스템은 수집 시스템에서 수집된 정보에 기반하여 사이버 공격을 재구성하며, 개별 사이버 공격에 악용된 자원 간의 연결성 및 연관성을 자동으로 분석하다. 또한, 서로 다른 사이버 공격의 연관성과 유사성을 분석하여 공격 그룹을 식별하는 기능을 제공한다.

향후, 실제 네트워크 및 시스템 보안장비의 보안 로그를 자동으로 연동시켜, 현재 보안 시스템 및 관제 요원들이 인지하지 못하는 공격을 자동으로 식별 가능한지 실험을 추가로 더 진행하여야 한다. 또한, 이를 위한 보안 로그 자동수집 기능과 각 실험 환경에 맞는 공격 분석 모델을 구축하는 과정이 필요하다.

참고문헌

[1] C. Tankard, "Advanced persistent threats and how to monitor and deter them", Netw. Security , Volume 2011, no. 8, pp. 16-19, 2011.

[2] Zainab Saud and M. Hasan Islam, "Towards proactive detection of advanced persistent threat (APT) attacks using honeypots", 8th International Conference on Security of Information and Networks, pp. 154-157, 2015.09

[3] Khairun Ashikin Ismail et al, "Security Strategies for Hindering Watering Hole Cyber Crime Attack", Procedia Computer Science, Volume 124, pp. 656-663, 2017

[4] Microsoft, "2018 사이버보안 위협보고서", 2018.06.

[5] EST security, "Threat Intelligence Report - OPERATION 'Ghost Puppet'", 2018.09.

[6] Gartner, "Definition : Threat Intelligence", 2013.5.

[7] 박순태, 김병익, 이슬기, "사이버위협인텔리전스(CTI) 기술을 활용한 공격자 프로파일링 및 대응", 국방과 보안, 제1권 제1호, 국방보안연구소, pp. 131-154, 2019.06.

[8] Open-source intelligence, https://en.wikipedia.org/wiki/Open-source_intelligence, WIKIPEDIA

[9] 김병익, 김낙현, 이슬기, 조혜선, 박준형, "기계학습 기반의 잠재적 사이버 위협 자동 분석 시스템", pp. 368-371, 2018년 대한전자공학회 하계학술대회, 2018.06

[10] About STIX,]https://stixproject.github.io/about/

[11] Introduction to STIX, https://oasis-open.github.io/cti-documentation/stix/intro

ACKNOWLEDGMENT

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2017-0-00158, 국가 차원의 침해사고 대응을 위한 사이버 위협 인텔리전스 분석(CTI) 및 정보 공유 기술 개발)