https://doi.org/10.33778/kcsa.2022.22.3.013

ELK 스택과 Sysmon을 활용한 공급망 공격 탐지 기법★

신 현 창*, 오 명 호*, 공 승 준*, 김 종 민**

요 약

IT 기술의 급속한 발전과 함께 기존 산업과의 융합을 통해 4차 산업혁명 기술을 기반으로 프로세스의 간소화 및 생산성을 높일 수 있는 스마트 제조가 증가하고 있으며, 이와 비례하여 공급망 공격에 대한 보안위협도 증가하고 있다. 공급망 공격의 경우 사전 탐지가 힘들고 피해 규모가 매우 크다는 점 때문에 차세대 보안 위협으로 부상하고 있으며 이에 따른 탐지 기법에 대한 연구가 필요하다. 따라서 본 논문에서는 오픈소스 기반 분석 솔루션인 ELK Stack과 Sysmon을 통해 다중 환경에서 실시간으로 로그를 수집, 저장, 분석 및 시각화하여 공급망 공격에 대한 이상 행위 등의 정보를 도출하여 효율적인 탐지 기법을 제공하고자 한다.

Supply chain attack detection technology using ELK stack and Sysmon

hyun-chang Shin*, myung-ho Oh*, seung-jun Gong*, jong-min Kim**

ABSTRACT

With the rapid development of IT technology, integration with existing industries has led to an increase in smart manu facturing that simplifies processes and increases productivity based on 4th industrial revolution technology. Security threat s are also increasing and there are. In the case of supply chain attacks, it is difficult to detect them in advance and the sc ale of the damage is extremely large, so they have emerged as next-generation security threats, and research into detectio n technology is necessary. Therefore, in this paper, we collect, store, analyze, and visualize logs in multiple environments i n real time using ELK Stack and Sysmon, which are open source-based analysis solutions, to derive information such as abnormal behavior related to supply chain attacks, and efficiently We try to provide an effective detection method.

Key-words: Supply Attack, ELK stack, Sysmon, Log Anlysis, Infringement response

접수일(2022년 08월 31일), 수정일(2022년 09월 13일), 게재확정일(2022년 09월 30일)

★이 논문은 2021년도 동신대학교 학술연구비에 의하여 연구되었음

* 동신대학교 정보보안학과

** 동신대학교 정보보안학과(교신저자)

1. 서 론

IT 기술의 급속한 발전과 함께 4차 산업혁명 기술을 기반으로 프로세스의 간소화 및 생산성을 높일 수 있는 스마트 제조가 증가하고 있으며, 이와 비례하여 공급망 공격에 대한 보안위협도 증가하고 있다.

공급망 공격의 대부분의 시작점은 엔드포인트로서 악성코드로 인한 공격이 주를 이루고 있다. 악성코드로의 공격기법은 계속해 진화하고 있지만 엔드포인트에 대한 보안의 대표적인 안티바이러스는 시그니처 기반 탐지 방법을 사용함으로써, 파일을 비교하여 제거 또는 격리하는 방식을 통해 악성코드 탐지에 대해 한계점이 존재한다.

따라서 본 논문에서는 ELK Stack 및 Sysmon을 활용하여 엔드포인트에서 발생하는 로그들을 실시간으로 수집하고 분석하여 위협 가능성이 있는 행위를 실시간으로 판단함과 동시에 보안위협을 대해 가독성을 높힐 수 있게 로그 시각화를 하여 보안 담당자들에게 있어 보안 위협을 신속하게 파악할 수 있는 탐지 기법을 구현하였다.

2. 관련연구

2.1 공급망 공격

2.1.1 솔라윈즈(Solar Winds) 공급망 공격

솔라윈즈 공급망 공격은 2020년 12월 13일, C미국 대형 네트워크 관리 소프트웨어가 해킹공격을 받아, 악성코드가 포함된 채 1만개 이상의 기업과 정부기관에 유포되어 피해를 준 사례이며, 2020년 3월~6월까지 정부수준의 해커가 업데이트 프로그램에 악성코드를 심어 업데이트 프로그램을 니려받은 이용자가 시스템에 백도어를 퍼뜨린 사건이다[1].

2.1.2 ASUS 공격

2019년도 ASUS 공격 사례는 해외 보안업체인 카스퍼스키(Kaspersky)사에 의해 발견되어 셰도우해머 작전(Operation ShadowHammer)이라 명명된 공격사건이다. 공격자는 ASUS의 업데이트 서버를 공격하고 업데이트 파일을 변조하여, 전 세계적으로 100만 대 이상의 PC를 감염시킨 것으로 추정되고 있다[2][3].

공격에 사용된 변조 업데이트 파일은ASUS의 정상적인 인증서로 서명되어 있어 변조 여부의 파악이 어려우며, 변조 파일에 하드 코딩된MAC(Media Access Control) 주소 리스트에 의해 추가 악성코드가 다운로드되도록 구현되었다[3].

2.1.3 Avast 공격

Avast 서버 공격은 2017년 발생한 사건으로, 공격자는 Avast가 만든 씨클리너 CCleaner) 소프트웨어의 공식 서버에 침투하여 해당 소프트웨어에 악성코드를 은닉하여 이를 다운로드한 대략 220만 사용자의 PC를 감염시킬 수 있었다. 해당 공격으로 일반 사용자 PC가 주로 감염되었지만, 공격자가 실제로 노린 건 시스코, 마이크로소프트, 구글, 소니, HTC와 같은 대형 IT 기업들이었던 것으로 분석되었다[3][4].

2.1.4 MeDoc 공격

MeDoc은 회계 관리 소프트웨어로서 우크라이나 정부 기관과 자국 내 90%의 기업이 사용하던 것으로 알려져 있다. 공격자는 MeDoc의 업데이트 서버를 해킹하여 업데이트 요청 시 랜섬웨어가 포함된 제품이 배포되도록 변조하였으며, 이로 인한 경제적 피해 규모가 대략 10조 원대로 추정되는 대규모 사태를 야기하였다[3][5][6][7].

2.2 탐지 기법

2.2.1 시그니쳐(Signature)기반 탐지 방법

시그니쳐기반 탐지방법은 오용 탐지(misuse detection)라고도 하며 시그니쳐 혹은 패턴을 이용하여 매치되는 모든 알려진 공격을 탐지하는 방법론이다. 이 방법은 패턴으로 정의된 모든 알려진 공격을 정확히 탐지할 수 있는 장점이 있으나, 일반적으로 제어시스템에 대한 공격패턴이 거의 알려져 있지 않은 사이버 위협 상황에서는 탐지가 어렵고, 무엇보다 제로데이 공격(zero-day attack)과 같은 새로운 형태의 공격에 대해서는 상세분석을 통해 탐지패턴을 지속적으로 개발하여 시스템에 적용하기 전까지는 탐지가 불가능하다는 문제점이 존재한다. 따라서 최근의 산업 제어시스템에 적용하기에는 다소 한계가 존재하는 탐지 방법이다[8].

2.2.2 이상행위(Anomaly) 기반 탐지 방법

이상행위기반 탐지방법은 네트워크상의 트래픽이나 시스템 자원의 사용이 정상적인 범주를 벗어나는 경우를 탐지하는 방법론이다[9]. 이 방법은 제로데이 공격(zero-day attack)과 같은 알려지지 않은 취약점을 이용한 공격이나 정보보호시스템을 우회하여 탐지되지 않는 지능적이고 새로운 공격까지도 탐지 할 수 있는 장점이 있다. 일반적으로 제어시스템에 대한 공격패턴이 거의 알려져 있지 않은 사이버위협 상황에서는 이상행위 탐지를 수행하는 것이 더 적합하게 고려되어 최근의 제어시스템 보안을 위한 많은 연구에서 활용되고 있다[8].

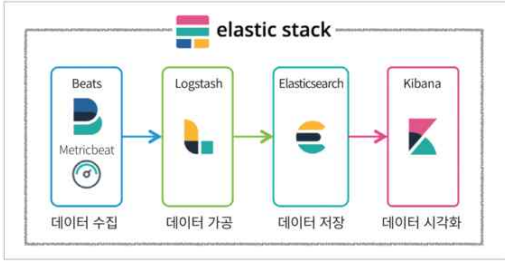
일반적으로 대부분의 침해성 데이터는 정상적인 형태로 가장하여 접속하며, 침해 패턴을 우회하는 접속은 악성코드를 내려받게 만드는 C&C(Command and Control) 서버로의 접속을 유도하고 C&C 서버와 접속되는 순간 악성코드가 다운로드 되면서 정보탈취 등 일련의 해킹이 이루어진다[10]. 이러한 일련의 과정들을 실시간으로 모니터링하며 침해 행위를 파악하고 이상행위에 대한 로그들을 수집, 분석하여 정/오탐의 결과를 도출해 낼 수 있는 침해대응체계 구축이 필요하다.

<표 1> 네트워크 및 정보보호 모니터링 체계[10]

Index		Monitoring System	Etc.
Network		Network monitoring system	Traffic, Devices
Info Security	DDoS	Dedicated management system	Effective control of cyber threats with the operation of information protection integrated monitoring system
	Firewall	Dedicated management system	
	IDS/IPS	Dedicated management system	
	Spam	Dedicated management system with limited monitoring function	
	Server	Using monitoring tools like server availability	
	Terminal	Antivirus and using separated terminal management solution	

2.3 ELK Stack 및 Sysmon

본 논문에서 사용된 ELK Stack은 Elasticsearch, Logstash, kibana를 병행하여 구현한 로그 수집 프로그램이며 이를 활용하여 공급망 공격 탐지 기법을 구현하고자 한다. (그림 1)은 세 가지 모듈을 이용하여 로그 저장 및 검색, 로그 수집 엔진, 로그 시각화 및 관리로 구성된 ELK Stack의 구조를 나타낸 것이다.



(그림 1) ELK 스택의 구조

Elasticsearch는 Shay Banon에 의해 개발된 Lucene 기반의 오픈소스 분산시스템으로 text, 숫자, 위치기반정보, 정형 및 비정형 데이터 등 모든 유형의 데이터를 검색 및 분석 해주는 엔진이다[11].

Logstash는 수집할 데이터를 선정 후 지정된 대상 서버에 전송하고 분석하는 역할을 담당하고, Elasticsearch는 분산 시스템으로써 수신된 데 이터를 저장소에 저장 및 쿼리문을 사용하여 저장된 데이터들을 실시간 검색하는 역할을 담당한다[11].

Kibana는 도식화를 목적으로 사용자에게 Elasticsearch에 저장된 데이터를 시각화해주는 역할을 한다[11].

ELK Stack의 데이터 흐름은 데이터를 Logstash로 수집 및 분석 후 Elasticsearch에 저장하게 된다. Elas

ticsearch에 저장된 데이터들은 Kibana를 통해 사용자들이 보기 편한 그래프나 숫자 등으로 표시되게 된다[11].

Sysmon은 Sysinternals에서 제작한 도구로 기본 윈도우 이벤트 로그와 마찬가지인 시스템 모니터링 툴이다. Sysmon에서 제공하는 로그 이벤트 중에서 특히, 프로세스·파일·레지스트리·WMI 이벤트를 이용하여 파워쉘 등에 의한 악성코드 감염이나 정상적인 윈도우 명령어 사용을 통한 네트워크 탐색 및 내부 파일·프로세스 목록 검색 등 Lateral Movement를 탐지할 수 있다[12].

<표 2> Sysmon eventlog Category

Event ID	Tag
1	Process Create
2	FileCreatTime
3	Network Connection
5	ProcessTerminate
10	ProcessAccess
11	Filecreate
12	RegistryEvent (Object create and delete)
13	RegistryEvent (Value set)
14	RegistryEvent (Key and Value Rename)
22	DNSQuery
23	FileDelete
255	Error

3. 제안하는 방법

3.1 구현 환경

<표 3>은 공급망 공격 탐지를 위한 ELK Stack 분석 환경이다.

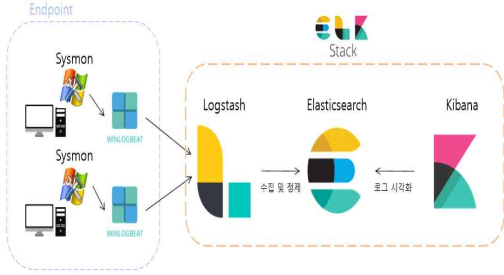
<표 3> 구현 환경

구분	version
OS	Ubuntu 18.04
Elasticsearch	7.17.5
Logstash	7.17.5
Kibana	7.17.5
Sysmon	14.0

3.2 EDR(Endpoint Detection and Response)

본 논문에서는 엔드포인트 보안중 하나인 EDR(Endpoint Detection and Response)을 사용한다. EDR은 PC, 노트북 등 네트워크의 모든 엔드포인트 영역에서 지속적으로 모니터링하고 데이터를 수집한 뒤 이를 실시간으로 분석하여 보안 위협에 대한 탐지 및 분석, 대응할 수 있게 하는 엔드포인트 보안 방법 중 하나이며, 위협에 대한 분석·가시성을 제공하기 때문에 시스템 및 네트워크 차단과 같은 즉각적이고 능동적인 대응이 가능하다.

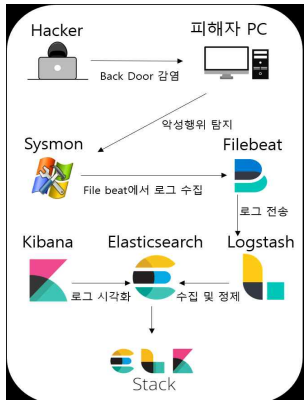
(그림 2)는 EDR 로그 수집 및 탐지 구성도이다.



(그림 2) EDR 로그 수집 및 탐지 구성도

3.3 ELK Stack 및 Sysmon 구성 방안

(그림 3)은 ELK Stack과 Sysmon을 활용하여 로그 수집 및 분석하는 구성도 이며, Sysmon에서는 로그를 필터링 및 수집하여 ELK Stackt에 전송하고, ELK Stack에서는 로그들을 수집·저장·필터·분석·가시화하여 공급망 공격에 대한 위협에 대해 탐지 가능하도록 구성하였다.



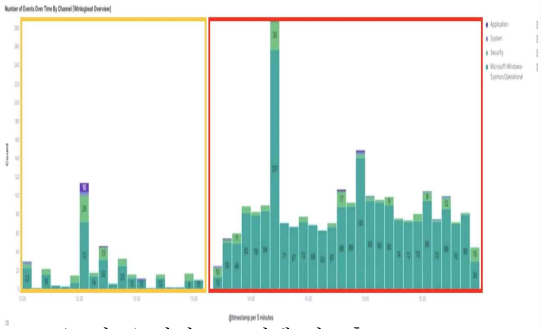
(그림 3) ELK Stack&Sysmon 연동 구성

4. ELK Stack 및 Sysmon을 이용한 탐지 기법

(그림 4) Backdoor:Win32/Wabot.A VirusTotal result

(그림 4)는 공급망 공격 탐지 기법에 사용할 악성코드이며, Win32/Wabot.A를 사용하였다.

먼저, 해커가 특정 기업의 공급망을 해킹하여 인증된 S/W에 Backdoor 악성코드를 삽입하였다는 시나리오를 가정하였으며, 사용자들이 해당 S/W를 실행시켰을 때 발생하는 로그를 Sysmon으로 탐지하고, 이를 ELK Stack을 이용해 실시간으로 분석하였다.



(그림 5) 악성코드 실행 전・후 DashBoard

(그림 5)는 악성코드를 실행시키기 전과 후의 DashBoard 화면이며, 악성코드가 실행되고 나서 확연하게 로그들이 급격하게 증가한 것을 볼 수 있다.

(그림 6) 악성코드 실행 전・후 DashBoard

(그림 6)은 악성코드가 실행하여 192.168.200.96 IP의 시스템에 대하여 dll.host.exe 등 프로세스들을 활성화 하고 공격이 수행되는 로그들이 나타나는 것을 볼 수 있다.

이처럼 ELK Stack 및 Sysmon을 이용해 공격이 진행되는 과정을 실시간으로 탐지를 하게되면 악성코드에서 실행하는 행위들과 공격의 유형 등에 대해 빠르게 분석이 가능하고 대응을 할 수 있다.

5. 결 론

본 논문에서는 ELK Stack 및 Sysmon을 이용하여 침해 대응 체계를 구축하였고 가상의 시나리오를 통해 이상행위 기반 탐지 방법으로 탐지 기법에 대해 제안하였다. 공급망 공격의 경우 개발 및 배포 단계에서 악성코드가 삽입되어진 형태를 유지하여 정상 업데이트 서버로 배포되기 때문에 업데이트 수행하는 사용자는 파일이 변조되어 실행이 되는지를 알 수 없으며, 기업의 입장에서는 공격이 발생하였음을 인지하기 전까지 피해가 계속해서 수행되기 때문에 그 규모는 클 수밖에 없다. 이와 같은 특성 때문에 공급망 공격은 보안 위협에 있어 계속해서 증가할 것으로 예상된다.

본 연구에서는 이런 공급망에 대한 탐지 기법에 대해 필요성을 판단하고

따라서 공급망 프로세스에 대한 전반적인 보안 강화의 필요성을 인지하고 침해대응 체계 구축 시 안티바이러스 솔루션 탐지를 우회하는 신·변종 악성코드 및 정

상적인 파일·프로세스를 악용하는 등 시그니처 기반의 탐지 방법으로는 발견하기 어려운 신종 악성코드들에 대비해 이상행위 기반 탐지 기법을 함께 사용하거나 AI, 빅데이터 기반의 탐지 체계 구축도 하나의 방안이 될 것이다.

참고문헌

[1] 홍병진, “항공무기체계 소프트웨어 사이버공격에 대한 작전영향성평가 방안”, 아주대학교 대학원 박사논문, 2021.

[2] “Operation ShadowHammer”, Kaspershy, Mar. 2019. https://securelist.com/operation-shadow-hammer/89992/.

[3] 김대원, 강동욱, 최용제, 이상수, 최병철, “공급망 보안기술 동향”, 한국전자통신연구원, pp. 149-157, 2020.

[4] OndrejVIckk, "CCleaner APT Attack: A TechnicalLook Inside", RSAConference2018.

[5] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, Oct. 2019. https: // www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[6] "2017 cyberattacks on Ukraine, "Wikipedia, Oct. 2019. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine.

[7] 손효현, 김광준, 이만희, “미국 공급망 보안 관리 체계 분석”, 정보보호학회논문지, 29권 5호, pp 1089-1097, 2019.

[8] 장정우, 김우석, 윤지원, “에너지 기반보호시설의 보안관제 방안에 관한 연구”, 정보보호학회논문지, 25권 2호, pp. 279-292, 2015.

[9] 박형민, “공격라이프사이클에 기반한 발전제어시스템 보안강화 방안 연구”, 고려대학교 정보보호대학원, 석사학위논문, 2018.

[10] 현정훈, 김형중, “오픈소스 ELK Stack 활용 정보보호 빅데이터 분석을 통한 보안관제 구현”, 디지털콘텐츠학회지, 19권 1호, pp. 181-191, 2018.

[11] 홍성대, “Sysmon과 ELK Stack를 이용한 윈도우 시스템 사이버 위협 탐지 및 가시성 증대에 관한 연구 ”, 동국대학교 대학원 석사논문, 2020. 02.

[12] 김용준, 손태식, “Sysmon과 ELK를 이용한 산업제어시스템 사이버 위협 탐지”, 정보보호학회논문지, 29권 2호, pp. 331-346, 2019.

〔저자소개〕

신 현 창 (hyun-chang Shin)
현 재 동신대학교 정보보안학과 학부생 재학

email : tlsgusckd124@gmail.com

오 명 호 (myung-ho Oh)
현 재 동신대학교 정보보안학과 학부생 재학

email : dhajd44@naver.com

공 승 준 (seung-jun Gong)
현 재 동신대학교 정보보안학과 학부생 재학

email : szkong@naver.com

김 종 민 (Jong-Min Kim)
2015년 산업보안학박사
현 재 동신대학교 정보보안학과 교수

email : dyuo1004@dsu.ac.kr