Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.2, Apr. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.2.331

Sysmon과 ELK를 이용한 산업제어시스템 사이버 위협 탐지*

김 용 준,[1†] 손 태 식[2‡]
[1]아주대학교 정보통신공학과(사이버보안 전공), [2]아주대학교 사이버보안학과

Cyber-Threat Detection of ICS Using Sysmon and ELK*

Yongjun Kim,[1†] Taeshik Shon[2‡]
[1]Department of Information and Communication Engineering, Ajou University
[2]Department of Cyber Security, Ajou University

요 약

국내·외에서 산업제어시스템을 대상으로 한 사이버 위협이 증가하고 있다. 이에 따라 관련 연구와 협력이 활발히 진행되고 있다. 하지만 물리적인 망 분리와 경계선에 대한 보안을 강화에 치중하고 있어 내부에서 발생하는 위협에 대해서는 여전히 취약한 편이다. 왜냐하면, 가장 손쉽고 강력한 대응방법이 경계선 보안을 강화하는 것이며 내부의 보안을 강화하기 위한 솔루션들은 시스템의 가용성 문제로 인하여 적용이 쉽지 않기 때문이다. 특히, 산업제어시스템 전반에 걸쳐 레거시 시스템[1] 이 상당수 잔존하고 있어 취약점이 많이 존재하고 있다. 이러한 취약한 시스템들이 보안 프레임워크에 따라 새롭게 구축되지 않는 한 이에 대한 대응방안이 필요함에 따라 가용성을 고려한 보안 솔루션을 검증하고 활용방안을 제시하였다. Sysmon과 ELK를 이용하는 방법으로 보안 솔루션이 미구축된 산업제어시스템에서 탐지하기 어려운 사이버 위협을 탐지할 수 있다.

ABSTRACT

Global cyber threats to industrial control systems are increasing. As a result, related research and cooperation are actively underway. However, we are focusing on strengthening security for physical network separation and perimeter. Internal threats are still vulnerable. This is because the easiest and strongest countermeasure is to enhance border security, and solutions for enhancing internal security are not easy to apply due to system availability problems. In particular, there are many vulnerabilities due to the large number of legacy systems remaining throughout industrial control systems. Unless these vulnerable systems are newly built according to the security framework, it is necessary to respond to these vulnerable systems, and therefore, a security solution considering availability has been verified and suggested. Using Sysmon and ELK, security solutions can detect Cyber-threat that are difficult to detect in unstructured ICS.

Keywords: ICS/SCADA, Legacy ICS, CTI, Sysmon, ELK

Received(12. 05. 2018), Modified(1st: 02. 11. 2018, 2nd: 03. 19. 2019), Accepted(03. 20. 2019)
* 본 연구는 2018년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 이공분야기초연구 사업임(NRF-2018R1D1A1B07043349)

† 주저자, amuse85@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

1) '레거시 시스템'이란 과거로부터 물려 내려온 시스템을 의미한다. 일반적으로 레거시 시스템은 개발 당시 특정 운영체계 및 플랫폼에서만 운영될 수 있도록 제작되었다.

Ⅰ. 서 론

산업제어시스템은 과거에는 아날로그 방식으로 설치, 구축 운용되었으나 현재는 디지털 방식으로 전환되고 있으며, 정보통신 서비스 연결과 보안을 위해서 주로 제한적인 폐쇄망으로 운용되고 있다.물론, 물리적으로 완전히 독립된 폐쇄망으로 운영되고 있는 제어(정보)시스템도 있기는 하지만 사이버 위협으로부터는 완전히 안전하다고 할 수는 없다. 2010년 이란 원자력 발전소 스턱스넷에서부터 최근에 사례들을 살펴 보면 2015, 2016년 우크라이나에서 발생한 두 차례의 정전사태, 2017년 대만 반도체 공장 가동중단 등 USB나 내부자에 의한 망분리 우회와 국방망 해킹사고와 같이 망연결 접점 존재에 따른 직접 침투 사례가 있었다.

산업제어시스템에는 다양한 시스템과 네트워크가 존재하고 대부분 기존 기구축된 시스템의 보안은 취약한 경우가 많다.[1] 구형 OS로 제작되어 현재까지 패치가 이루어지지 않고 있으며, 제작사의 정책에 의해 보안설정을 확인, 수정할 수 없거나 추가적으로 상용 보안솔루션을 설치시 체계가 미작동되어 가용성 보장을 위해서 보안 솔루션을 미운용하고 있기도 하다.

이에 기구축된 취약한 레거시 제어시스템을 대상으로 위협을 탐지/대응하기 위해 윈도우 기반 모니터링 체계인 Sysmon과 ELK를 이용한 보안 솔루션을 구축해 사이버 위협을 탐지하기 위한 방법을 검증하고 제안하고자 한다.

따라서 본 논문에서는 산업제어시스템의 최근 침해사례와 보안기술 동향을 살펴보고 오래전에 구축되어 마땅한 솔루션이 부재한 레거시 시스템을 위한 보안 솔루션의 효과를 검증하고, 그 필요성과 나아가야 할 방향에 대해서 모색하였다. 본 논문의 2장에서는 연구를 위해 필요한 산업제어시스템의 특성 등 정보들을 취합하고, 현재 주요 보안 트렌드들에 대해 정리하며, 3장에서는 최근 산업제어시스템 사건사고 사례, 대응 보안기술 등 추이를 살펴보고, 주요한 시사점을 도출한다. 4장에서는 레거시 산업제어시스템을 위한 Sysmon과 ELK를 이용한 사이버 위협 탐지방안을 제안하고 5장에서는 실제 실험을 통한 검증 및 분석을 통해 마지막 5장에서는 레거시 산업제어시스템을 위한 솔루션의 필요성과 보안 프레임워크 준수 등 나아가야 할 방향을 제안하고 논문을 마무리 한다.

Ⅱ. 연구 배경 및 관련 기술

2.1 ICS / SCADA 개요

ICS(Industrial Control System)란 통상 산업현장에서 이용하는 제어시스템을 말하며, 센서의 측정값과 현장의 운용 정보를 수집하고, 이 정보들을 처리/표시하며, 원격의 장치로 제어정보를 전달하는 역할을 하는 시스템을 말한다. 이러한 제어시스템의 예로 간단히는 요즘에 스마트폰을 이용하여 가정의 조명, 난방 등을 제어하는 홈 IoT부터 발전소의 다양한 설비들은 운용하는 전력시스템까지 다양하게 들 수 있다.

이러한 제어시스템은 처리영역에 따라 분산제어시스템(DCS, Distributed Control System)과 원방 감시제어 및 데이터 취득시스템(SCADA, Supervisory Control And Data Acquisition)으로 나눌 수 있다. DCS는 보통 작은 지역에서 운영되는 것이며, SCADA는 지역적으로 분산된 시스템의 감시제어와 데이터를 취득하는 시스템을 말하고, 시스템이 대형화되고 복잡해지면서 SCADA와 ICS는 용어적으로 큰 구분 없이 사용되고 있으며,[2] ICS/SCADA로 통칭해서 부르기도 한다. 이것에 대해 정보통신기반보호법은 '국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리 시스템'이라고 정의하고 있다.

국내에서는 2014년 한국수력원자력 사건으로 ICS 보안에 대한 관심이 커진 바가 있으며, 북한과 휴전 중인 우리나라의 경우 안보 관련 ICS 위협과 그 중요성을 간과할 수 없을 것이다. 보통 ICS는 설치 구축 후 오랜 기간 운영되는 특성으로 인해 1/3 이상이 보안 취약점이 존재하지만 패치가 되지 않고 있다.[4] 현재 국내 ICS 보안 기술은 외부와의 경계선 보안에 치우쳐 있는 실정이다.

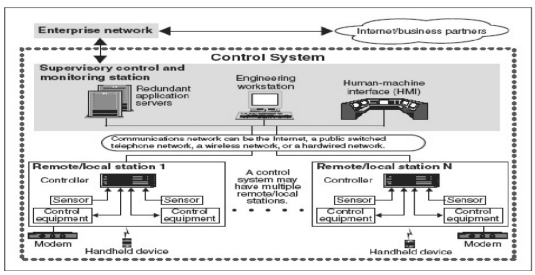

Fig. 1. General structure of CS[3]

ICS/SCADA는 최근 경영·기술 환경의 변화로 비즈니스 시스템과 통합되고 개방형 시스템으로 표준화가 진행되고 있다. 과거에는 폐쇄망으로 망 분리 상태로 구축되었지만, 4차 산업혁명, IoT의 발전과 함께 개방형으로 인터넷과 연결지점이 생겨나고 있다. 이로 인해 사이버 위협 또한 증가하고 있다.

2.2 ICS / SCADA의 특징

ICS/SCADA는 IoT환경과 유사한 부분도 있어 Industrial IoT로 불리기도 하지만 Table 1.에서 보다시피 분명한 차이점 또한 존재한다. ICS는 최신의 IoT 시스템과 달리 이미 수십년 전에 구축되어 운영 중인 레거시 시스템이 존재한다는 것이다. 다양하고 복잡한 시스템 환경이 산재하여 각 체계별로 경험있는 전문 엔지니어가 필요하며, 오래전 환경에 맞춤 제작된 HW와 SW는 변경 및 개선을 어렵게 한다. 또한, 이는 보안 취약점에 대한 조치가 어려운 이유이기도 하다. 그리고 무엇보다도 ICS는 주요 국가 기반 시설에 대한 문제 발생시 생명과 안전 및 국가 경제 전체에 영향을 미칠 수 있는 큰 파급력을 가지고 있다.

Table 1. Comparison "IT System" and "ICS/ SCADA"[5]

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated depending on the system's operational requirements Responses	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive predeployment testing
Risk Management Requirements	Manage data Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Control physical world Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory noncompliance, environmental impacts, loss of life, equipment, or production
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of thirdparty applications such as security solution	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communi-cations	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communicators media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported.
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3 to 5 years	Lifetime on the order of 10 to 15 years
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

Table 2. Function of Sysmon[6]

· Logs process creation with full command line for both current and parent processes. · Records the hash of process image files. And Multiple hashes can be used at the same time (SHA1(the default), MD5, SHA256 or IMPHASH) · Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names. · Detects changes in file creation time to understand when a file was really created. · Rule filtering to include or exclude certain events dynamically.

2.3 Sysmon

Sysmon은 MS에 속한 Sysinternals에서 무료로 제공되는 윈도우 시스템 모니터링 도구이다. Sysmon은 기존의 윈도우 이벤트 로그의 제한된 보안로그 기능을 강화하여 프로세스 생성, 네트워크 연결 등 이벤트를 확인 가능하며, 내부 활동을 추적하여 비정상 행위를 탐지 할 수 있다. 세부 기능은 Table 2.에서 보는 바와 같다.

추출한 해쉬를 이용하여 평판조회 사이트에서 악성코드 여부를 조회하여 확인할 수 있으며, 파일, 프로세스, 네트워크 생성, 수정, 삭제 등 변화를 이벤트로 알려주고, 특정 이벤트에 대해 필터링을 적용할 수 있다.

대부분의 기관과 기업이 소수의 보안업무 인원, 제한된 시간과 정보 또는 너무 방대한 정보를 가지고 위협을 탐지, 분석할 것이다. 이에 따라 호스트 기반으로 위협을 탐지할 수 있는 Sysmon을 이용한 위협 탐지 모델을 공개된 탐지기법들과 실제 경험을 바탕으로 4장에서 제시하였다. Sysmon 로그를 이용한 위협 헌팅이라는 주제로 외국 논문, GitHub, RSA Conference, Botconf, JPCert/CC 등에서 활용방안들이 연구되어 공유되고 있으며,[7][8] 국내에서는 몇몇 보안업체 및 관심있는 개인에 의해서 시험하고 정리 및 소개하고 있다. 확인한 바로는 특정 정보보호솔루션 업체의 경우 자사의 SIEM 솔루션에 Sysmon Agent 설치를 통해서 Sysmon 로그를 수집하여 활용하고 있었다.[9]

2.4 ELK(Elastic Search, Logstash, Kibana)

ELK는 ElasticSearch, Logstash, Kibana 3가지 솔루션을 합쳐 부르는 것이다. Beats가 추가된 것은 ELK Stack이라고 부른다. Logstash와

Beats를 통해서 데이터를 전달, 수집하고, ElasticSearch cluster가 저장, 분석하며, Kibana를 통해 검색 및 시각화한다. 이를 Fig 2.에서 그림으로 쉽게 나타내고 있다.

ElasticSearch는 Apache Lucene을 기반으로 개발한 분산 검색엔진으로 비정형 데이터를 쉽게 저장하고 처리할 수 있으며, 실시간 검색과 플러그인을 이용한 확장을 지원한다. 인덱스 갱신 주기가 빠르며, 운영 중인 스키마 변경도 가능하다. Kibana는 데이터를 시각화하고, Elastic Stack의 모든 기능을 구성 및 관리할 수 있는 확장 가능한 유저 인터페이스 환경의 도구이다. Logstash는 확장가능한 플러그인 에코시스템으로 구성된 동적 데이터 수집 파이프 라인으로, 다양한 소스에서 동시에 데이터를 수집하고 변환하여 자주 사용하는 Stash 보관소로 보낸다. 한마디로 입력값들을 간단하게 원하는 데이터 형태로 변경하여 Elastic Search로 전달한다. Beats는 단말 장치의 데이터를 Logstash 및 Elasticsearch로 전송하는 경량 수집기용 플랫폼으로 단말기 또는 서버에 설치하여 다양한 유형의 데이터를 Logstash를 통하거나 바로 ElasticSearch로 전송하는 오픈소스 데이터 전송 에이전트이다.[10]

이와 같은 도구를 이용한다면 Sysmon 로그를 효율적으로 분석 가능하다.

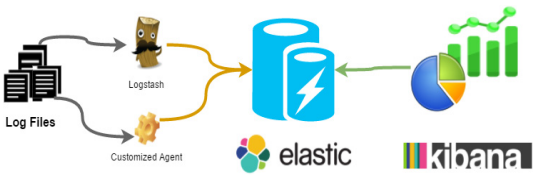

Fig. 2. ELK(Elastic search, Logstash, Kibana)

2.5 CTI(Cyber Threat Intelligence)

2013년 가트너에서는 사이버 위협 인텔리전스에 대해 다음과 같이 정의하고 있다. “사이버 공격으로부터 자산에 대한 위협 대응을 위해 의사 결정에 활용할 수 있는 상황정보, 메커니즘, 지표, 영향 조언 등 증거기반의 지식”. CTI는 사이버 범죄 프로파일링이라고도 볼 수 있다. 과거 사이버 위협들의 정보를 수집하고 이를 침해지표로 정리하여 새로운 위협과 비교 분석하여 연관성을 찾는 것이다. 대표적으로 malware.com(Fig 3.) virustotal.com 등이 있다.

Fig. 3. SaintSecurity, malware.com

급증하고 있는 사이버 위협에 효과적으로 대응하기 위해서는 공격자가 누구인지 파악하고 공격이 이뤄지는 단계별로 방어 전략을 세워야 한다. CTI와 프로파일링의 공통점은 최대한 많은 정보를 수집하여 수집된 침해지표를 기반으로 보안전문가들의 분석을 더해 사건을 조사·판단하는 것이다.[11]

2.6 EDR(Endpoint Detection & Response)

엔드포인트 영역에서 지속적인 모니터링과 대응을 제공하는 보안솔루션을 말한다. 또한, 침해 탐지, 조사와 엔드포인트 영역에서의 보안 통제와 감염 전 상태로 치료 등의 기능을 제공한다. 최근 고도화된 위협에 이용되는 악성코드는 엔드포인트에서 은닉, 우회 등의 기법을 통해 확산되고 있으며, 기존 보안 솔루션으로는 알려지지 않은 위협에 대한 대응에는 한계가 있다. EDR은 엔드포인트에서 발생하는 위협과 관련된 행위 정보(파일, 레지스트리, 프로세스, 네트워크 등)와 위협에 대해 가시성을 제공함으로써 관리자가 네트워크 차단과 같은 즉각적이고 능동적인 대응이 가능하다. 엔드포인트 영역과 네트워크 영역에서 발생하는 정보들을 가지고 연관분석을 한다면 사이버 위협 인텔리전스 정보로는 대응하기 어려운 이상 행위를 조금 더 일찍 발견할 수 있다. 그렇기에 이번 연구에서는 호스트 기반으로 네트워크 영역의 정보와 CTI 연관분석을 통해 위협을 탐지하는 프로세스를 정리하였다.

다크트레이스의 인공지능(AI) 기반 사이버 면역 시스템은 인간의 면역체계의 특징을 차용해 지능적으로 진행되는 공격을 탐지할 수 있다. 머신러닝 기술을 이용해 지속적으로 정상 상태를 학습하고 이상 행위를 분류하면서 진화하고, 사전 학습이 필요 없는 비지도 학습 방식을 이용하며, 실시간으로 흐르는 원시패킷을 분석해 이상행위를 찾아내며, 외부 인터넷 연결 없이도 자율적으로 분석한다. 즉, 사용자·디바

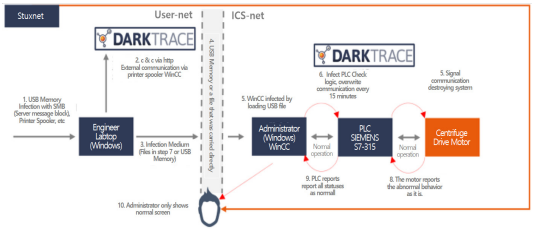

Fig. 4. Darktrace EIS(Enterprise Immune System)

이스·네트워크의 일반성과 특이성을 학습하면서 정상 행위와 다른 이상행위를 찾아낸다.

예를 들어 단 한 번도 접속한 적 없는 PC가 접속 이력이 없는 IP에 비정상적인 시간에 비정상적인 주기로 접속 시도를 하고, 내부 SMB(Server Message Block) 서버에 접속해서 데이터를 다운로드/업로드 하는 등의 행위를 찾아낸다. 탐지룰 없이도 패킷의 이상행위를 탐지하기 때문에 악성코드를 사용하지 않는 공격도 찾아낼 수 있으며, 내부자에 의한 위협도 탐지 가능하다.

다크트레이스의 사이버 면역 시스템(Fig 4.)은 전사 시스템의 위협 가시성을 확보할 수 있으며, 고급 분석 전문가 수준으로 지능형 위협을 탐지할 수 있어 보안조직의 업무를 크게 줄일 수 있다. 이 제품은 금융·공공·제조·통신 등 주요 산업군에 공급돼 성공적으로 사용되고 있다.[12]

Ⅲ. ICS 보안 위협 및 대응기술 분석

3.1 최근 ICS 보안 위협 동향[13]

최근 산업제어시스템은 다양한 산업분야 및 제조, 발전, 가공 등의 산업시설 뿐만 아니라 전력, 자원운

Table 3. Critical attacks cases of Domestic and international ICS[13]

Date	Attack target	Attack type/damage
2001	Australian sewage treatment Systems	A fired employee can manipulate the system using external remote access, Damage caused by unauthorized release of marine sewage.
2003	US Railroad In-house railway system	In-house information system is infected with malware and signal system is stopped being. During the 6 hours of restoration work, Stopped.
2009	US Hospital HVAC system	HVAC(Heating, Heating, Ventilation, Air Conditioning) system is hacked.
2010. 6.	Iran Natanz Nuclear facility	'Stuxnet', a malicious code targeting remote control systems, Found. Stuxnet penetrated the Iran Natanz nuclear facility, To delay the development of nuclear weapons.
2012	The world's largest oil company Saudi Aramco	More than 35,000 computers in my company have been paralyzed, documenting all the work Manually through. Aramco, paralyzed to the payment system, Of the world's oil supply, Free 17 days after the incident.
2014 12	Korea Hydro Nuclear Power	Nuclear plant drawings leaked.
2015. 12.	Ukraine Power Grid	A wide range of 200,000 people can not use electricity for about 6 hours Power outage occurred.
2016. 3.	Seoul KORAIL Railway Traffic Control Center	Exclude your e-mail account and password for employees of railway operators There is an outbreak of phishing e-mail being sent down. At the time of railroad traffic control System is a preliminary stage for cyber terror.
2016. 4.	Michigan Power Plant Water Facilities	Spear phishing attack via e-mail with Ransomware box. If the infection spreads to the internal network, To suspend the company system.
2016. 11.	San Francisco Municipal Railway (MUNI) system	The payment system is a variant of HDD crypto, Mabma Ransomware And more than 2,000 unattended issuers are paralyzed.
2017. 6.	Honda automobile Shiyama Factory	Infected with WannaCry Ransomware, engine production for about 48 hours And assembly is interrupted.

송 등 주요정보통신 기반시설 및 빌딩, 공항 등의 시설에 적용되고 있다. 또한, IT와 ICS 네트워크가 융합되어 실시간 데이터 및 연결성 의존도가 점점 커지고 있으며 이에 따라 사이버 공격 경로는 기하급수적으로 확장되었다.

Table 3, Fig 5. 국내외 ICS 중요 피해 사례를 살펴보면, 표적 맞춤형 APT 공격의 사례가 끊이지 않았으며, 최근에는 랜섬웨어에 의한 산업 전반의 시설 마비와 금전적 피해가 주로 발생하였다.

미국 ICS CERT 보고서에 따르면 ICS에서 발생

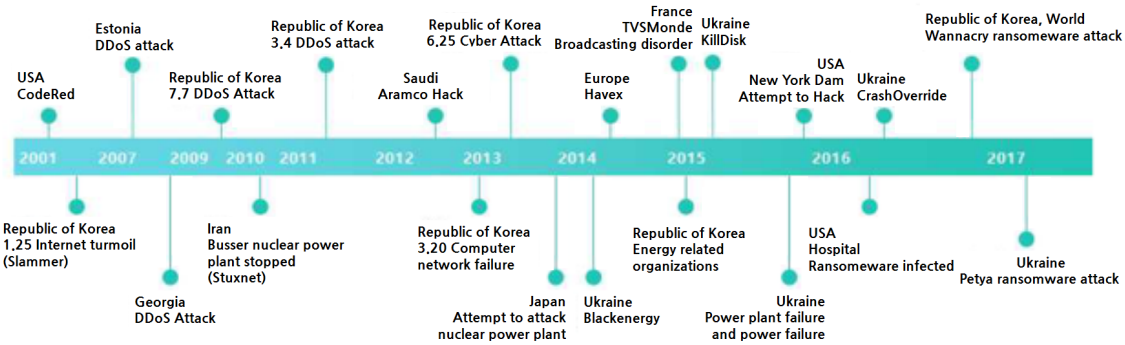

Fig. 5. Major damage cases of Domestic and international ICS[13]

하는 사이버 보안 사고의 55%는 APT (Advanced Persistent Threat) 공격이며, ICS 환경에서 일어나는 모든 사고의 40%는 사람의 부적절한 행동으로 발생한다고 한다. 이를 통해 최근의 보안 위협을 살펴보았을때 단순히 금전 목적으로 산업제어시스템을 공격하였다기 보다는 내부자의 실수로 인한 감염이거나 시설 마비/파괴 목적의 표적형 공격일 가능성이 높다.

제어시스템 대상 사이버 공격은 2011년 140건이었으나 2016년에는 290건으로 크게 증가하였으며, 발견된 취약점 또한 동기간동안 139건에서 187건으로 증가하였다. 2015년 12월 우크라이나 정전사태는 MS 오피스 문서 파일 내 매크로 바이러스 동작에 따른 추가 악성코드 생성 및 실행에 의한 것으로 가장 흔한 이메일을 이용한 APT 공격에서부터 시작된 것이었으나 정확히 1년 후인 2016년 12월 정전사태는 산업제어시스템 내 설비 제조사의 취약점과 원격제어 프로토콜을 사용한 것으로 그 기법의 수준이 고도화되었다.[14]

일반적으로 내부 시스템 침입에서 시스템 파괴까지는 어느 정도 시간이 소요된다. 정찰부터 침투, 내부 시스템을 파악하고 장악해야 하기 때문에 보통 6개월 정도의 시간이 소요된다. 따라서 공격에 의한 피해가 발생하는 것을 방지하기 위해서는 주기적으로 내부 시스템 점검을 통해 이상징후를 빨리 파악할 수 있어야 한다.

3.2 ICS 보안 위협요인[15]

3.2.1 보안 인력 부족

대부분 사고가 발생하지 않는 이상 보안을 중요하게 고려하지 않으며 투자에 소극적이어서 적절한 예산이 편성되지 않는 경우가 많다. 이는 인력 충원을 어렵게 하는 요인이다. 최근에는 보안에 대한 인식이 높아져서 보안 인력 충원이 증가하고 있지만 여전히 전담 인력이 부족하거나 전문성이 떨어지는 경우가 많다.

3.2.2 보안 의식 부족

조직원들의 보안 의식도 중요한 요인이다. 대부분의 경우 보안이 강화되면 불편하게 된다고 생각하며 절차를 지키지 않거나 높은 직책에 있을수록 예외 처리를 종종 요구한다. 보안 절차가 지켜지지 않으면 기존에 알려진 악성코드 조차도 예방하지 못한다. 그러나 여전히 일부 시설의 시스템에서는 오래전에 제작되어 유포된 악성코드가 발견되고 있으며, 백신으로 충분히 진단 및 치료할 수 있는 악성코드가 백신 미설치 또는 업데이트 미실시로 잔존하고 있다.

3.2.3 망분리 허점

대부분의 사회기반시설은 망분리 조치가 되어있다. 망분리가 되어있어 비교적 안전하다고 할 수 있지만 모든 시스템을 망분리할 수 있는 것은 아니다. 시설 내 어딘가에는 인터넷에 연결된 시스템이 존재하며 이를 통해 피해가 발생하기도 한다. 또한, 외부와 연결되면 안되는 중요 시스템임도 미처 인지하지 못하거나 실수로 인터넷에 연결되어 있는 경우도 있으며, 랜카드를 추가로 설치하거나 휴대폰 테더링을 통해 인터넷에 접속하기도 한다. 또한, 업무상 필요에 의해 USB나 공유 폴더를 사용하는 경우도 있다. 이처럼 물리적으로 망분리가 되어있어도 업무상 필요에 의해 인터넷용 컴퓨터에서 다운로드한 파일을 업무용 컴퓨터로 옮길 수도 있다.

게다가 일부의 경우 제대로 된 망분리가 아니라 단순히 시스템의 인터넷 접속을 차단하는 경우도 있다. 또한 사용자들이 불편함을 이유로 망분리 환경을 우회하려는 시도를 하는 경우도 있으며, 그로 인해 외부 공격 경로 및 취약지점이 발생한다. 따라서 여러 망분리 방식 중에서 각자 조직에 적합한 방식을 충분히 검토 후 도입해야 한다. 그리고 내부 시스템과 연결되는 지점이 있다면 이 부분을 제대로 모니터링 해야 한다.

3.2.4 레거시 시스템 운영

여전히 오래된 구형의 레거시 시스템을 이용하고 있는 사회기반 및 산업 시설이 많이 있다. 게다가 해외에서는 1980년대 생산된 구형 컴퓨터를 이용해 난방 제어시스템을 운영하고 있는 사례도 알려진 사실이다. 안정적인 운영이 중요한 사회기반 및 산업 시설의 특성상 시스템 교체가 급박하게 처리해야 할 사안으로 취급되지 않고 있지만, 구형 시스템 상당수가 보안을 고려하지 않고 제작되었거나 이미 알려진 취약점도 해결할 수 없는 경우가 많아 굉장히 취약하다.

3.2.5 협력 업체 관리 미흡

직접적으로 공격하는 방법 외에 협력 업체를 통해서 정보 유출이나 우회 공격을 시도할 수도 있다. 특히 전산망은 외주를 준 유지보수업체를 통해 관리하는 경우가 많아서 협력 업체에 대한 관리 및 보안 강화가 필요하고 중요하다. 그리고 내부에서 사용하는 프로그램 설치시 악성코드가 포함되거나 하드웨어 납품시 백도어가 숨겨져 있을 수도 있다. 특히 펌웨어를 통해 기능을 수정할 수 있는 제품들의 경우 제조업체가 해킹되어 공격 당할 수도 있다.

외부 공격을 방어하기 위해서는 Fig 6.에서 정리된 것처럼 조직 구성원들이 보안정책을 잘 준수할 수 있도록 현실적인 정책을 수립하는 것이 필요하고 내부로 유입되는 위협을 모니터링하고 내부에서 확산되는 악성코드에 대한 적절한 대응과 분석 능력도 필요하다. 하지만 무엇보다도 협력 업체에 대한 강력한 보안 대책을 마련하고 준수토록 해야 한다.

Fig. 6. ICS security threat factor[15]

3.3 ICS 보안 대응방안

2018년 8월 ISEC에서 한국남부발전(주)은 ICS/SCADA 보안의 중요성과 대응방안에 대해서 발표를 하였다. 전력제어시스템은 제어망(PLC, HMI, 서버, 장치설비), 업무망(업무PC, 서버), 인터넷망으로 구성되어 있으며, PLC(Programmable Logic Controller) 제어명령 조작, 전송시 정전 등 이상행위를 발생시키거나 전송되는 정보를 변조하여 혼란을 유발시킬 수 있다. 이에 따라 네트워크 기반으로 제어시스템 내 모든 구간에서 패킷 수집이 필요하고, HMI/PC/서버 구간은 레거시 시스템과 동일한 취약점이 존재하기 때문에 업무망과 동일한 수준의 침입탐지시스템이 필요하다고 발표하였다. 또한, 백신, EDR, HIDS 등 호스트 기반으로 대응하기 위한 솔루션도 장기적으로 마련할 필요가 있다. 하지만 HMI(Human Machine Interface)에서 발생하는 위협을 탐지하기 위한 솔루션들은 제어시스템의 가용성에 따라 제조사가 정하고 있기에 남부발전은 자체적으로 샌드박스를 이용하여 폐쇄망에서 동적/정적분석을 실시하고 모든 네트워크 및 파일/프로세스/레지스트리 변화에 대해 모니터링하여 DB화 하고 있다. 실시간 검사는 제한되지만 가용성을 보장하면서 제어시스템 환경의 가시성을 확보하기 위해 노력하고 있다.[16]

사실 제어시스템을 위한 보안기술은 이미 다양하게 연구, 개발되어 적용되고 있다. 하지만 이처럼 제어시스템의 특성상 가용성이 가장 중요하며, 오래전에 설계, 구축된 레거시 시스템에 대해서는 이러한 보안 대응기술 적용이 제한되는 실정이다.

3.3.1 CTI(위협 인텔리전스) 기반 탐지

인터넷 평판 정보 사이트 또는 각 기관·기업에서 자체적으로 구축한 체계를 이용하여 과거 탐지 이력 정보 및 악성행위 유무 등 평판 정보를 확인하는 방법이다. 이것은 대체로 신뢰할 수 있는 유효한 한가지 방법으로 초기에 위협 판단시 참고사항으로 활용할 수 있다. 이러한 방법의 경우에는 알려진 위협 즉, 침해지표를 보유하고 있을 때에는 효과적이지만 그렇지 않은 경우에는 탐지가 제한된다. 그리고 공급망 공격을 통해서 신뢰하고 있는 체계 및 SW가 자료 유출 등의 악의적인 행위를 수행 할 경우 이상행위를 탐지 할 수 없다는 단점이 있다.

3.3.2 시그니처 기반 탐지

잘 알려진 악성코드 및 취약점 공격과 같은 분석이 완료된 주요 위협 및 공격 탐지에는 매우 효과적이다. 하지만 제어시스템이 사용하는 소프트웨어에 대한 취약점 패치가 나오지 않은 시점의 새로운 제로데이 공격이나 악성코드에 대한 공격에 대해서는 탐지할 수 없으며, 매번 새로운 공격이 발견될 때마다 백신 등 보안솔루션 회사에서 최신의 시그니처를 개발하고 정보보호 담당자는 이를 신속하게 적용해야 하기 때문에 시간과 비용이 지속적으로 발생하며, 탐지 우회를 위한 맞춤형 APT 공격시 대응이 어렵다.

3.3.3 Endpoint 보안로그 분석

Endpoint는 보안의 시작점으로 볼 수 있다. 보안의 모든 정보가 만들어지고 정보가 이동하는 시작점이자, 네트워크와도 연결되어 있다. Endpoint 통합 보안로그 분석기법은 DLP, DRM, 개인정보보호 등 다양한 Endpoint 솔루션들의 보안로그를 통합하여 도출한 단일/연계 시나리오와 4W2H(Who, When, Where, What, How, How much)를 이용한 사용자 행위기반으로 발생하는 보안위협 식별정보들을 위험도 가중치를 부여하여 주의, 경고, 위협 단계로 보안위협을 식별하게 한다. 이외에도 다양한 보안로그 분석기법이 있으며, 보안담당자가 위협수준에 따라 대응할 수 있게 해준다.[17] 이 방법은 기본적인 보안솔루션이 구축되어 있어야 가능하며, 다양한 보안로그를 통합하는 것과 그 데이터에 의미를 부여하여 분석하기가 쉽지는 않다.

3.3.4 비정상행위 기반 탐지

비정상행위 탐지 기법은 정상적인 행위 패턴을 기반으로 평소와는 다른 특이한 행위나 패턴을 식별하는데 사용된다. 네트워크 단계에서 트래픽을 바탕으로 IDS를 구축하거나 신용 카드 거래의 부정행위 탐지를 위해 자주 사용되고 있다. 이 기법은 일반적인 행위 패턴으로부터 벗어난 비정상적인 행위를 탐지하기 때문에 알려지지 않은 침입 방법까지도 탐지할 수 있는 장점이 있으나, 제어시스템의 정상적인 작동 수준 내에서 공격이 이루어지면 탐지하지 못한다는 것과 비정상적인 행위가 아닌데도 비정상적인 행위로 탐지하기도 하는 단점이 있다.[18] 이러한 이상 탐지 기법은 이론상으로는 완벽한 침입탐지가 가능하지만 분석가의 경험과 직관 뿐만이 아닌 지도·비지도 학습에 의한 머신러닝 기법의 연구의 성과가 나와야 신뢰성과 가용성을 중시하는 제어시스템에 적용이 가능하겠다.

3.3.5 White-List 기반 탐지

제어시스템 환경에서의 블랙리스트 기반 보안 탐지 기법의 한계에 따라 화이트리스트 기반 탐지 기법에 대한 검토 및 적용이 증가하고 있다. 화이트·블랙리스트 기반 탐지 기법은 Table 4.과 같이 차이가 있다. 제어시스템에서 화이트리스트 방식은 크게 어플리케이션과 방화벽에 적용되고 있다. 어플리케이션 방식은 각각의 호스트들에서 정상으로 정의한 어플리케이션 이외에는 실행을 막는 것이다. 방화벽에는 기존 MAC, IP, Port 기반 화이트리스트 규칙과 더불어 제어시스템에서 사용하는 제어 통신 프로토콜(Modbus, DNP3, ICCP 등)에 대해 트래픽을 감시하여 세부적으로 적용하고 있다.

Table 4. Comparison of White·Black-List based Detection[20]

	White-List based Detection	Black-List based Detection
Processing method	Prevention	Follow-up action
Program control	Use only allowed programs	Use all programs
Resource Utilization	Lowness	Highness
Security Level	Highness	Lowness
Update cycle	Periodic	Real time
Availability	Limited environment	Universal environment

이러한 화이트리스트 방식은 환경에 의존적이어서 SW 설치 및 업그레이드시 일시적 서비스중단, 성능저하 등의 문제가 야기될 수 있으며, 방화벽의 화이트리스트 규칙 적용은 정상패킷 차단으로 인한 오작동 발생시 확인이 어려워 보안관리자 입장에서 대응이 어려워진다.[19]

Ⅳ. 레거시 ICS를 위한 사이버 위협 탐지 방안

4.1 Sysmon 로그 분석을 통한 위협 탐지

3장에서 언급한 ICS 보안 대응방안들은 나름대로 보안 강화를 위한 대책이기는 하지만 하나의 탐지기법만으로는 지능적인 APT 공격을 탐지하기 어려우며, 레거시 시스템의 경우 기술, 예산, 제조사 정책 등의 문제로 상기 탐지기법을 위한 보안 솔루션이 미적용되어 있는 경우가 많기에 상기 탐지기법 적용조차 어려운 실정이다. 이에 따라 기구축된 이 제어시스템이 윈도우 OS 기반의 환경[2]으로 되어있다면 Sysmon은 레거시 ICS를 위한 가장 최선의 선택이라고 할 수 있다. 먼저, 가용성을 해치지 않으며, 호스트의 각종 행위 정보들을 수집하기 때문이다.

2) SCADA 시스템은 점차 개방형 시스템으로 전환되고 있으며, 과거에는 UNIX 기반이 주류였다면 최근에는 점차 Windows 기반이 증가하고 있다.[21][22]

Table 5. Sysmon Log Event

Category	Event ID
Process Create	1
File Creation Time	2
Network Connection	3
Sysmon Service State Change	4
Process Terminated	5
Driver Loaded	6
Image Loaded	7
CreateRemoteThread detected	8
RawAccessRead detected	9
Process Access	10
File Create	11
RegistryEvent (Object create and delete)	12
RegistryEvent (Value Set)	13
RegistryEvent (Key and Value Rename)	14
File Create Stream Hash	15
Sysmon Configuration Changed	16
Pipe Created	17
Pipe Connected	18
Wmi(Windows Management Instrumentation) Event	19~21
Error	255

Sysmon 로그는 기존 윈도우 XP 이하에서 지원하는 이벤트 로그(보안, 응용프로그램, 시스템 로그)보다 포렌식 및 징후 탐지를 위한 더 많은 아티팩트를 제공한다. Sysmon 로그에서 제공하는 이벤트는 아래 Table 5.에서 보는 바와 같다

Sysmon을 활용해서 윈도우 OS 기반의 단말기의 보안을 손쉽게 강화할 수 있으며, OS에서 지원하기 때문에 만약, 윈도우 OS 환경으로 운영되는 레거시 ICS가 있다면, Sysmon을 활용할 필요가 있다. 단, 제한사항으로 윈도우 XP 이하에서는 지원이 되지 않는 아쉬움이 있으나 윈도우 이벤트 로그에서는 지원하지 않는 대표적인 Sysmon 로그 이벤트를 몇몇 추려서 수집하도록 간단히 개발하거나 호환성 테스트 이후 상용 도구를 사용한다면 동일하게 위협을 헌팅하는데 사용할 수 있을 것이다. 주요한 로그를 백업하고 주기적으로 분석하는 것만으로도 충분히 의미있는 보안 활동이라고 할 수 있다. Sysmon 로그 분석을 통한 위협 탐지는 아래와 같은 방법들이 있다.[23],[24]

4.1.1 Process/File Create 이용 탐지

기존에 존재하지 않았던 새로운 프로세스나 파일이 생성되었을 때, 응용프로그램 사용, 업데이트 등 별다른 사용자 행위가 없다면 확인이 필요하다. 위협 탐지는 물론이고 포렌식 아티팩트로도 사용할 수 있다.

4.1.2 Network Connection 이용 탐지

출발지, 목적지 IP 및 Port 정보를 가진다. 악성코드 감염에 의한 C2 서버 통신을 시도한다면 외부로 네트워크 연결(시도)하는 목적지 IP를 확인한다. 또는 정상적이지 않은 내부 호스트간 네트워크 연결을 분석한다. 네트워크 연결 로그는 중요한 정보이자 확실한 정탐의 증거가 될 수 있으나, 단편적인 로그만 남기 때문에 이 정보로 APT 공격을 탐지하기는 쉽지 않으며, 다른 네트워크 기반 탐지체계의 정보들과 연관분석이 필요하다.

4.1.3 Image, CommandLine 이용 탐지

이 두 가지 로그는 ParentImage, ParentCommandLine와 Parent-Child 관계를 가지며, 함께 Sysmon 로그로 남는다.

Parent-Child Image/CommandLine의 관계가 일치하지 않고 다른 것을 호출하거나 인자값이 특정한 값을 가지거나, 암호화, 인코딩 등의 방법으로 난독화 되어있을 때, Image 이름과 실행되는 경로가 매칭되지 않을 때 악성코드 감염을 의심할 수 있으며, 백신이 탐지하지 못하는 악성코드를 탐지할 수 있을 것이다.

4.1.4 윈도우 명령어 이용 탐지

공격자는 탐지 회피를 위해서 정상적인 툴을 이용하거나 윈도우 명령어를 자주 사용한다. 이러한 윈도우 명령어의 사용 순서나, 사용자가 일반적으로 잘 사용하지 않는 명령어 또는 공격자가 주로 사용하는 명령어 사용 횟수를 통계분석을 통해서 탐지할 수 있다. 정찰을 위한 net 관련 명령어나 자료 검색을 위한 dir 등 주로 사용할 수 밖에 없는 명령어가 있다. 이러한 명령어는 사용자의 정상적인 행위에서도 발생할 수 있기 때문에 사용시간, 횟수, 사용 명령어의 순서 등을 같이 연관분석해야 한다. 외부로 자료 유

출시에는 80, 443port로 위장하기 때문에 단기간에 빼가는 것이 아니라 장기간 서서히 유출시킨다면 특정 목적지 IP들을 식별하고 추적, 분석해야 할 것이다. 침입 흔적을 삭제하는 명령어를 사용해서 로그를 삭제할 수도 있는데, 이는 주기적인 점검을 통해서 로그 삭제가 식별된다면 내부 침해를 인지할 수 있을 것이고, 우리의 보안정책을 알고 지우지 않는다면 로그 분석을 통해 이상징후를 헌팅 할 수 있을 것이다.

4.1.5 File Hash 이용 탐지

Sysmon 로그에서는 파일 생성시 Hash를 로그로 기록한다. 공격을 위해서 사용되는 도구들이나 새로운 악성코드가 발견되었을 때, 해당 Hash를 검색해 볼 수 있다. 호스트가 백신을 설치 할 수 없는 환경이거나 미설치 또는 최신버전으로 업데이트를 수동으로 정기적인 일자에 하고 있다면, 사전에 위협을 탐지할 수 있을 것이다.

4.2 Sysmon과 ELK를 이용한 위협 탐지 제안

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. 위에서 살펴본 Sysmon 로그 분석 방법들을 가지고 ELK를 이용하여 탐지정책으로 제작하여 Sysmon 로그들에 대한 초기 분석을 간편하게 함으로써 위협을 탐지하는 방안을 제안하고자 한다.

호스트에는 Sysmon과 Winlogbeat를 설치·실행한다. Winlogbeat는 Sysmon 로그를 실시간으로 서버의 Logstash로 5044 port를 이용해서 전송한다. Logstash가 데이터를 정제하여 ElasticSearch로 전송하고 수집/저장하면 Kibana를 이용하여 필터링과 Lucene 문법에 따라 검색하여 위협을 헌팅하거나 이를 시각화한 다음, 대쉬보드를 통해서 모니터링 할 수 있다. Sysmon 로그를 Kibana를 이용하여 직접 검색하거나 미리 작성한 탐지정책에 따라 대쉬보드에서 알려주는 비정상적인 프로세스·파일·레지스트리 생성·종료 등 초기분석시 이상징후가 있다면, Fig 7.과 같은 위협 탐지 모델을 이용해 절차에 따라 체계적으로 위협여부를 확인하다. 절차에 대한 세부 설명은 아래와 같다.

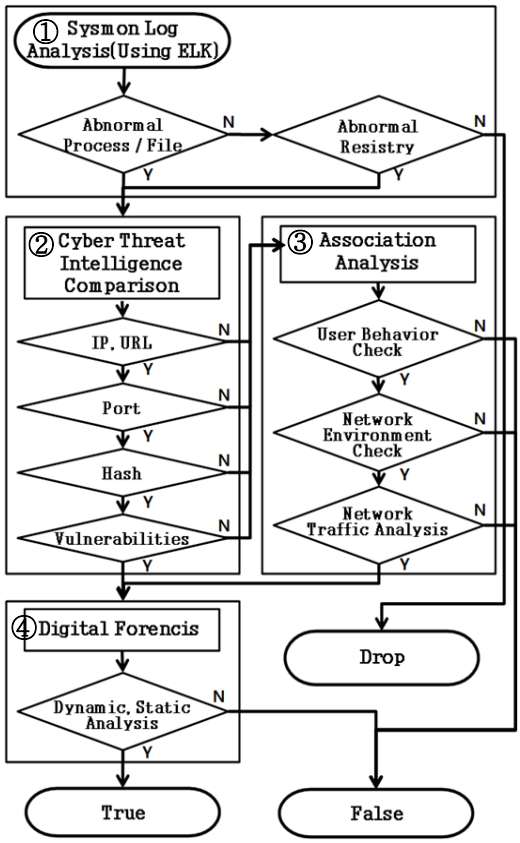

Fig. 7. Sysmon log based threat detection model

① Sysmon 로그 초기 분석

Process Create(Evt. ID 1), File Create (Evt. ID 11), RegistryEvent(Evt. ID 12~14) 등에서 연구·제작한 기본 탐지룰에 의하여 이상징후로 탐지되는 경우 Kibana 대쉬보드로 시각화하여 인지할 수 있도록 한다.(Fig 8.)

Kibana로 시각화하여 일반적으로 잘 사용하지

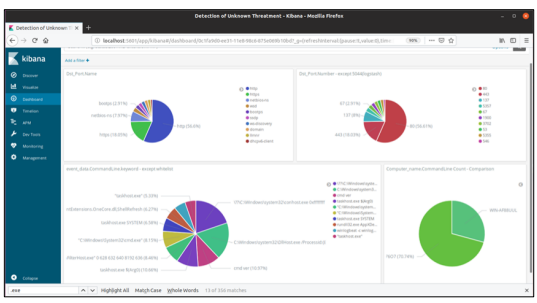

Fig. 8. Screenshot - Kibana Dashboard(Visualize)

않는 윈도우 명령어가 비교적 짧은 시간 안에 다수 실행되는 것을 탐지정책을 통해 통계분석하거나(Fig 9.), 프로세스의 생성과 삭제와 Network Connection을 이용한 C2 통신 시도 및 PID(Process Identification Number)와 PPID (Parent Process Identification Number)[3], Image 로드, 부모 프로세스가 다른 경우 등을 필터링 및 검색을 통해 탐지할 수 있다.

만약 내부에서 악성코드가 전파되고 있다면 감염된 호스트인지 확인하는 과정을 거칠 것이고 확인된 후에 감염되지 않은 다른 호스트를 찾아 나갈 것이다. 오래된 부트 파괴 바이러스인 미켈란젤로 바이러스나 최근 평창 동계올림픽의 올림픽 디스트로이어와 하데스를 예로 들면 악성코드가 드롭되는 특정 위치에 대해 생성된 악성파일 존재 여부를 지정경로에 대한 검사를 하는 과정을 반복할 것이기 때문에 정상적인 명령어로 탐지체계를 우회할지라도 해당 이벤트에 대해서 탐지정책을 제작, 필터링을 통해 Kibana로 시각화한 다음 탐지할 수 있다.

② CTI 침해지표 비교

여러 CTI 정보 관련 사이트를 이용하여 이상징후로 탐지된 호스트의 파일/프로세스의 IP 주소, Domain 이름, Port 번호(Evt. ID 3)와 같이 생성된 파일의 Hash값(Evt. ID 15) 그리고 발표된 취약점 중 해당되는 것이 있는지 확인한다.

위의 사례와 같은 비정상 프로세스, 파일 및 레지스트리로 보인다면 일단 CTI의 침해지표와 비교를 통해서 알려진 위협인지 확인을 해본다. 유해 IP, Domain 여부를 확인하고, 워너크라이 445 port이거나 신뢰받고 있는 공급된 특정한 SW나 시스템의 업데이트나 제어정보 송수신 등에 사용되는 프로토콜이나 Port인지 확인하고 세부적인 화이트리스트 적용 규칙과 차이점을 확인해본다. 또한, 생성된 파일 Hash값을 조회해보는 것이다. OS의 잘 알려진 파일, 드라이브인데 정상, 악성인지 Hash 조회 결과가 없다면 연관분석을 실시하고, 악성으로 확인된다면 해당 SW와 관련하여 최근 발표된 1-Day 취약점이나 가용성으로 인하여 조치하지 못하고 있는 관련된 취약점이 있는지도 확인해 본다.

③ 행위 & 네트워크 연관분석

CTI 침해지표와 비교하였을 때, 일치하는 것이 없다면, 사용자, 관리자 및 SW 제조사 등에게 인터뷰를 통해서 이상징후로 의심되는 행위에 대해서 확인을 하고, 해당 조직의 네트워크 환경과 트래픽 분석을 통해서 추가적인 이상징후가 있는지 연관분석을 실시한다.

연관분석으로는 이상 프로세스, 파일 등의 처리가 발생한 시간대에 관리자 또는 사용자 행위에 대해 인터뷰하고 네트워크 환경과 발생한 트래픽도 같이 살펴본다. 이 과정에서 특이점을 중간에 식별하지 못하였다면 다른 이벤트를 확인하는 과정으로 넘어가고, 뚜렷하게 침해지표와 일치하는 것이 있거나 그렇지 않지만 연관분석 결과 이상징후로 의심되는 경우에는 해당 호스트 대상으로 조사, 채증 및 동적/정적 분석을 실시하여 위협 여부를 최종 판단하게 된다. 이 과정에서 공개된 CTI의 침해지표나 프로파일링 정보 등 지능정보를 이용하여 비교하겠지만, 악성코드의 특징과 탐지룰 등 핵심정보에 대한 공유가 더욱 활발하게 이루어져야 할 것이다. 예를 들어 금융권을 대상으로 하는 공격에 대해서 금융보안원에서는 라이플·도깨비 캠페인이라는 이름으로 적극적으로 공유하고 있으며,[25] MITRE 社의 CARET[4]은공격그룹, 기술과 전술 등 ATT&CK 모델에서 강조된 사항들을 맵핑하여 정보를 무료로 제공하고 있다.[26]

④ 조사 / 분석

이상징후만 발견되고 확실한 판단이 서지 않는다면 전문가를 통해 의심되는 단말기, 프로그램, 파일 등에 대해서 포렌식 및 동적·정적분석을 실시하여 악성코드 여부를 최종적으로 판단한다.

Ⅴ. 가상 시나리오 검증

Sysmon-ELK 이용 호스트 기반 위협 탐지 시험은 가상환경에서 실시하였다. Host OS는

3) PID는 프로세스 각각을 구별할 수 있는 유일한 데이터이고, PPID는 프로세스를 만든 부모 프로세스의 PID를 나타내는 값이다. 프로그램을 실행한 프로세스의 PID가 PPID로 할당된다.

4) 'CARET(Cyber Analytic Repository Exploration Tool)'은 ATT&CK Model에서 강조된 공격 그룹 및 기술을 사이버 분석 저장와 연결, 설계된 GUI형태의 공격 맵핑 Tool이다.

Windows 7으로 Sysmon과 Winlogbeat를 설치하여 Sysmon 로그를 ELK를 설치한 Host인 Ubuntu로 전달하여 Kibana를 이용하여 UI 환경에서 로그 분석 및 대쉬보드로 시각화하였다.

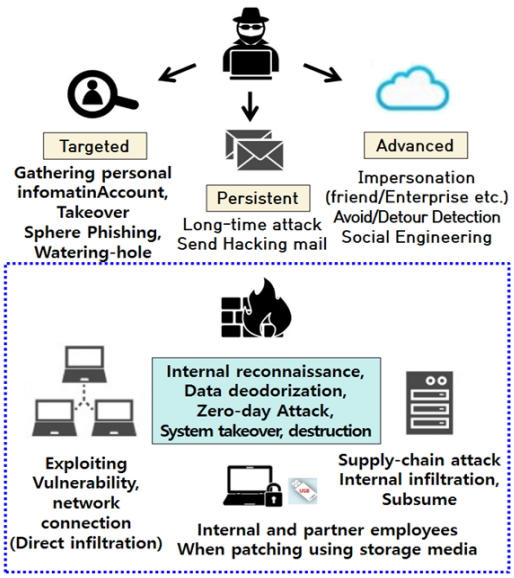

Fig. 9. ICS attack scenario

본 논문에서는 Fig 9.와 같은 공격 시나리오에서 외부 저장장치와 공급망에 의해 악성코드가 유입된 상황을 가정하고, 비정상 프로세스 및 파일 생성과 C2 통신 등을 탐지하기 위한 탐지정책을 작성하였으며, 가상환경에서 악성코드 샘플을 이용하여 시험하였다. 아래에서 시나리오 기반으로 주요 2가지 유형의 위협에 대한 검증 및 분석 결과를 제시한다.

5.1 외부 저장장치에 의한 랜섬웨어 감염

5.1.1 시나리오

Table 6.에서 보는 것과 같이 랜섬웨어 감염에 의한 산업제어시설 피해가 지속 발생하고 있다. 내부 관리자 또는 유지보수 직원이 관리 및 유지보수 목적으로 USB, CD를 이용하여 망분리된 내부 시스템 연결 전에 외부 저장장치를 최신 백신으로 검사하였으나 신종 또는 변형 랜섬웨어로 백신검사 우회한 시나리오를 가정하여 Sysmon 로그 기반의 위협탐지 모델을 검증해보았다.

Table 6. Ransomware infection case

Date	Case
'17. 8.	Korea 'A' Compay, Increased traffic due to Ransomware infection inside service center, delayed business
'17. 10.	Japan Semiconductor Manufacturing Company 'B', Ransomware attack halted some production lines
'18. 8.	Taiwan Semiconductor Manufacturing Company 'C', USB connection for installation of equipment SW WannaCry infection halts production line

5.1.2 검증 및 분석결과

윈도우 디펜더 검사를 중지시켜 백신 미탐지 환경을 모사한 후 정상 파일로 위장한 악성코드로 가정하고 워너크라이 랜섬웨어 악성코드를 실행하였다.

Sysmon 로그를 Kibana 대쉬보드로 확인결과 워너크라이 감염 동작(암호화)이 Process Create/Terminate(Event ID 1, 5)에서 mssecsvc.exe가 식별되었다. 이때, Parent Image/Commandline은 lsass.exe가 실행되었고 외부 C2 서버와 통신을 위한 DNS 질의와 유해 IP를 확인할 수 있었으며,(Event ID 3) 목적지 Port 중 전파 목적의 445port 통신이 다수 탐지되었다.(Fig. 10.)

랜섬웨어 감염시 파일을 암호화하게 되는데, 원래 목적인 금전을 요구하기 위해서 랜섬노트를 띄운다. 워너크라이의 경우 처음에 드롭퍼를 실행하면 추가적으로 악성코드가 다운로드 되고 나서 파일 암호화가 시작된다. 그러다보니 워너크라이는 C2 서버와 통신이 되지 않아서 통신시도만 지속적으로 발생하였다. 그렇기 때문에 외부망과 단절된 내부망에서 USB, CD 등 저장매체에 의해 랜섬웨어 뿐만 아니라 계정/비밀번호 탈취형 바이러스 등 다양한 종류의 악성코드가 유입되고, 감염되어 있을 수 있다. 만약, 백신을 설치할 수 없거나 미설치된 환경이라면 외부망과 단절된 내부망이기 때문에 발생하는 지속적인 통신 시도를 탐지할 수 있을 것이며, 이러한 통신은 상황에 따라서 시스템의 가용성에 영향을 미칠 수도 있기 때문에 Sysmon 로그 분석을 통해서 발견해서 조치할 수 있을 것이다.

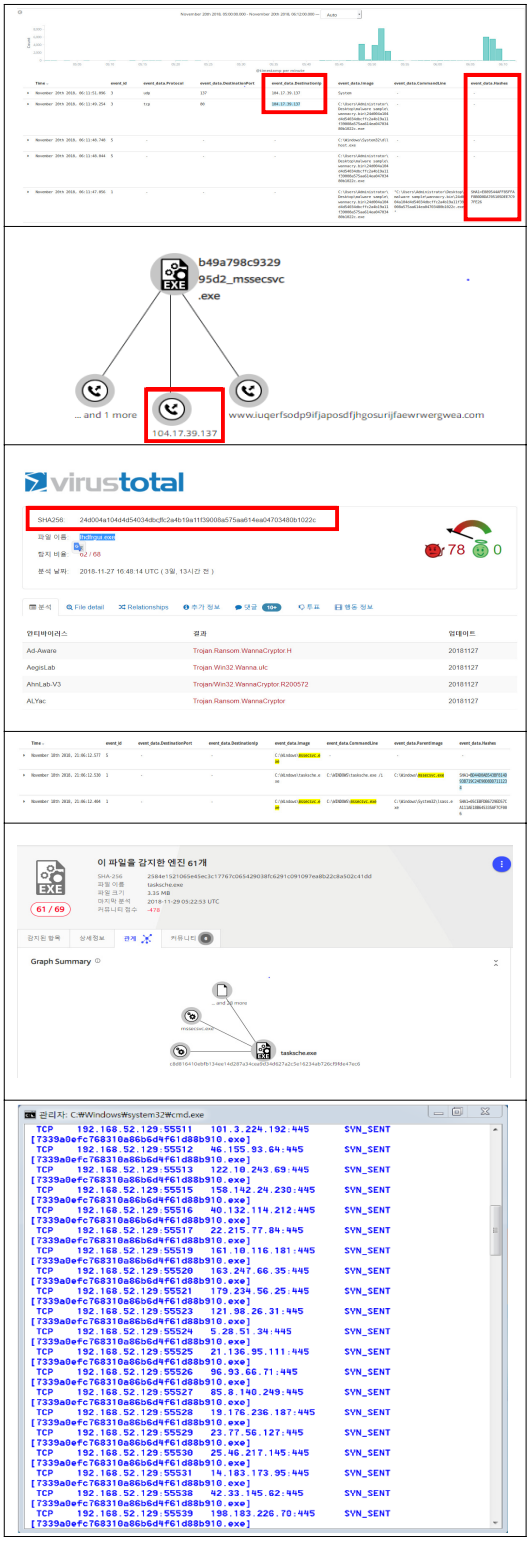

Fig. 10. Screenshot - Ransomeware Detection

5.2 공급망 공격을 통한 악성코드 침투

5.2.1 시나리오

Table 7.에서 보는 것과 같이 최근 공급망 공격 사례를 보았을 때, 공급망을 통한 공격이 지속될 것으로 보인다. 이에 따라서 제어시스템 관련 SW가 제조사 해킹되어 악성코드가 삽입된 변조된 SW(펌웨어, 패치 등)가 설치되어 화이트리스트로 처리되어 탐지 우회한 시나리오를 가정하여 Sysmon 로그 기반의 위협탐지모델을 검증해보았다.

Table 7. Supply Chain Attack cases

Date	Case
'17. 3.	Germany 'D' Company, With control system SW disguised malware found
'17. 8.	Korea 'E' Company, Diffusion with backdoor in server management SW

5.2.2 검증 및 분석결과

서버관리 SW로 위장하였던 "ShadowPad" 악성코드를 가지고 확인하였다. 상기 악성코드는 금융서비스, 교육, 통신, 제조, 에너지, 교통 등 여러 업계 고객이 사용하는 서버 관리 SW의 DLL(Dynamic Linking Library) 파일을 변조하였다.

xshell 5.0 빌드 1325, xftp 5.0 빌드 1218을 가상환경에서 설치 후 Sysmon 로그를 Kibana로 모니터링 및 분석하였다. 하지만 C2 서버가 현재 동작하지 않아서 7일 이상 기간동안 네트워크 패킷을 모니터링 하였으나 특별한 DNS 요청을 발견하지 못하였다. 그렇지만 만약, C2 통신이 발생하였다면 Network Connection(Event ID 3)에서 발견되었을 것이고, "ShadowPad"와 같이 이미 발견된 악성코드라면 CTI 비교를 통해서 확인 가능했을 것이다. 카스퍼스키의 분석보고서[27]에 따르면 C2 서버 통신을 위해 8시간마다 DNS 요청을 보내며, 이때, 감염된 시스템의 사용자명, 도메인명, 호스트명 등 기본정보를 전송한다. 이러한 행위는 네트워크 연결 및 처리를 담당하는 필수 DLL인 nssock2.dll 레지스트리에 의한 것으로, 해커가 해당 시스템에 관심을 가질 경우 명령제어서버가 요청에 응답하고, 백도어 플랫폼을 활성화하면, 피해 컴퓨터에 백도어가 배포된다고 한다. 해당 악성코드가 발견되기 전이라고 하였을 때, 사용자 행위 여부, 네

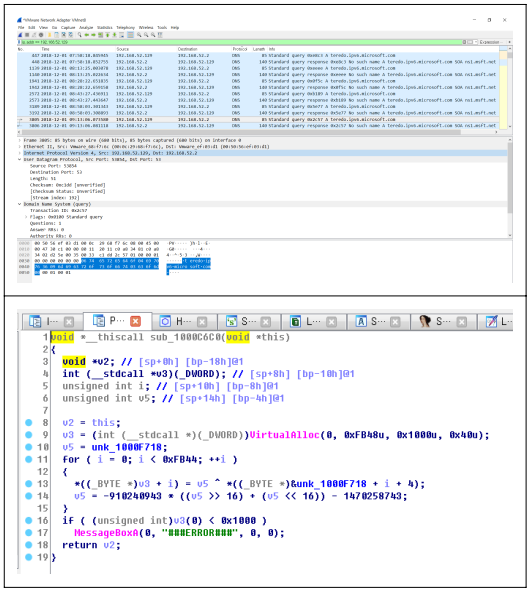

Fig. 11. Screenshot – Network, Static Analysis

트워크 로그 분석을 통해서 DNS 통신을 확인할 수 있을 것이고, SW 제조사에 이상행위에 대한 확인요청 및 동적·정적 분석을 통해서 최종적으로 확인 가능할 것이다. 이상행위를 탐지했다고 가정하고 실제로 와이어샤크, IDA 등 도구를 이용해서 탐지 절차에 따라 nssock2.dll에 대한 분석까지 진행해 보았다.(Fig 11.) 정확한 확인까지 분석보고서와 전문가의 도움이 필요했다.

기본적으로 상용 SW의 경우 제조사 홈페이지로 업데이트 또는 에러상태 보고 등을 위해서 네트워크 통신이 발생하고 이를 위해서 DNS 질의가 발생하는 경우가 많다. 하지만 제어시스템 등 내부 시스템에서 C2 서버와 통신일 수도 있는 네트워크 연결시도에 대해서 목적지 도메인, IP가 어떻게 되는지 확인을 할 필요가 있으며, SW 제조사에 문의하였을 때 인지하지 못하고 있는 행위라면 포렌식 및 동적·정적분석을 통해서 확인을 해야 할 것이다.

검증결과 공급망 공격을 실제로 위협으로 최종 확인 및 판단하기 위해서는 일단 의심가는 행위에 대한 탐지가 있어야 하고, 최종적으로는 전문가에 의한 정밀 분석이 이루어져야 함을 알 수 있었다. 그렇기 때문에 이러한 은닉된 지능형의 APT 공격을 탐지하기 위해서는 호스트 기반으로 로그를 수집·분석하여 위협을 탐지하는 솔루션이 필요함을 알 수 있었다.

Ⅵ. 결론 및 향후 연구방향

본 연구에서는 윈도우 기반의 Sysmon과 ELK를 이용하여 간단한 호스트 기반 위협탐지 체계를 구축할 수 있었다. 특히, Sysmon 로그를 이용해서 호스트에 대한 파일·프로세스·레지스트리 행위 정보 등 다양한 로그를 수집하고 ELK를 이용하여 조회, 시각화 등 분석을 통해서 유입되어 잠재하고 있는 악성코드를 탐지 할 수 있었다. 레거시 제어시스템의 경우 가용성 보장을 위해 패치와 보안솔루션 설치가 제한되기 때문에 Sysmon과 같은 OS에서 지원하는 도구를 사용하여 호스트 기반 위협 탐지체계를 구축한다면 백신 탐지를 우회하는 신·변종 악성코드나 정상적인 파일·프로세스를 악용하는 등 고도화되고 있는 APT 공격을 탐지할 수 있을 것이다.

References

[1] SecurityFocus, “SCADA vulnerabilities”, https://www.securityfocus.com/news/11402, Sep. 2018.

[2] Gyeongyeong Song, “Security technology trend for SCADA system”, The Magazine of the IEEK, pp.1-2, Aug. 2015.

[3] GAO, “Critical Infrastructure Threats”, GAO 04-354, pp.2, Mar. 2004.

[4] MSS, “Technology Roadmap for SME 2018-2020 Information Security”, MSS, pp. 257, Jan. 2018.

[5] NIST, “Guide to Industrial control systems security”, NIST Special Publication 800-82 Revision 2, pp. 29-31, May. 2015.

[6] Microsoft, “Sysmon Setup”, https://docs. microsoft.com/ko-kr/sysinternals/downloads/sysmon, Aug. 2018.

[7] JPCERT Coordination Center, “Sysmon Malware Detection”, https://blogs.jpcert.or.jp /en/2018/09/visualise-sysmon-logs-and-detect-suspicious-device-behaviour-sysmonsearch.html, Sep. 2018.

[8] CISA, “ICS Sysmon”, https://ics-cert.us-cert.gov/Industrial-Control-Systems-

Joint-Working-Group-ICSJWG, Sep. 2018.
〔9〕 Plura Blog, "Windows Sysmon", http://blog.plura.io/?p=9481, Sep. 2018
〔10〕 Elastic, "Elasticsearch Logstash Kibana", https://www.elastic.co/kr/products/, Sep. 2018
〔11〕 "4th Industrial Revolution and 'Cyber Threat Intelligence'", DT, 2. May. 2018. http://www.dt.co.kr/contents.html?article_no=2018050302102351607001
〔12〕 Darktrace Blog, "ICS SCADA EDR", https://blog.naver.com/darktrace-ray/221045454630, Sep. 2018.
〔13〕 MSS, "Technology Roadmap for SME 2018-2020Information Security", MSS, pp. 252-254, Jan. 2018.
〔14〕 DRAGOS, "CRASHOVERRIDE: Analysisof the Threat to Electric Grid Operations", DRAGOS, pp.6-11, Jun. 2017.
〔15〕 Ahnlab, "Critical Infrastructure Threats", Analysis Report, pp. 36-37, May. 2016.
〔16〕 Boannews, "Seungyeon Han, The importance of ICS /SCADA security and counter measures, ISEC 2018", https://www.youtube. com/watch?v=k2oJO-_nkRw, Nov. 2018.
〔17〕 Seonghun Eom, Jaepyo Bag, "A Study on the Security Threats Detection through Analysis of Endpoint Integration Security Log", Soongsil Univ., pp.9-24, Dec. 2016.
〔18〕 Jungchan Na, Hyunsook Cho, "Classification of ICS abnormal behavior in terms of security", Journal of the Korea Institute of Information Security & Cryptology 23(2), pp. 329-33, Apr. 2013.
〔19〕 Hyunguk Yoo, Jeong-Han Yun, Taeshik Shon, "Whitelist-Based Anomaly Detection for Industrial Control System Security", The Journal of The Korean Institute of Communication Sciences 38(8), pp. 642-643, April. 2013.
〔20〕 Younghun Lee, Junghyun Ryu, Jonghyuk Park, "Research Trends and Considerations of Security Technology of Industrial Control System", SeoulNational University of Science and Technology, pp.3, May. 2018.
〔21〕 Procon, "SCADA OS Windows Unix", http://www.procon.co.kr/page/sub.html?main=2&sub=1, DEC. 2018.
〔22〕 Univ. Hoseo, "Analysis of Overseas System based Evaluation Cases and Technology", KISA-WP-2009-0011. pp. 8, Jun. 2009.
〔23〕 Josh Brower, "Using Sysmon to Enrich Security Onion's Host-Level Capabilities", GIAC (GCFA) Gold Certification, pp.6-15, Mar. 2015.
〔24〕 Vasileios Mavroeidis · Audcun Jøsang, "Data-Driven Threat Hunting Using Sysmon", ICCSP 2018, pp.5-6, Mar. 2018.
〔25〕 Financial Security Institute, "Cyber Threat Intelligence", https://www.fsec.or.kr/user /bbs/fsec/163/344/bbsDataView/1139.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=, Sep. 2018.
〔26〕 Mitre Corp, "Mitre ATT&CK", https://mitre-attack.github.io/caret, Sep. 2018.
〔27〕 Kaspersky Lab, "ShadowPad", https://securelist.com/shadowpad-in-corporate-networks/81432/, Oct. 2018.

〈저자소개〉

김 용 준 (Yongjun Kim) 정회원
2008년: 해군사관학교 국제관계학과 졸업(학사)
2019년: 아주대학교 정보통신대학원 졸업(석사)
2008년~현재: 대한민국 해군
〈관심분야〉 Control System, Forensic, CTI, CERT, Big-Data, Machine-Learning

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신· DMC 연구소 책임연구원
2017년~2018년: Illinois Institute of Technology 방문교수
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 교수
〈관심분야〉 ICS/SCADA, DFIR, Anomaly Detection