산업용 사물인터넷을 위한 머신러닝 기반 APT 탐지 기법

주소영 · 김소연 · 김소희 · 이일구*

성신여자대학교

Machine Learning Based APT Detection Techniques for Industrial Internet of Things

Soyoung Joo · So-Yeon Kim · So-Hui Kim · Il-Gu Lee*

Sungshin Women's University

E-mail : 22021603@sungshin.ac.kr / soyeonkim0307@gmail.com / 99rlathgml@naver.com / iglee@sungshin.ac.kr

요 약

엔드포인트를 대상으로 하는 사이버 공격이 표적형, 지능형 공격으로 정교하게 진화하면서 산업용 사물인터넷(IIoT, Industrial Internet of Things)을 겨냥하는 지능형 지속 공격(APT, Advanced Persistent Threat)이 증가하고 있다. APT 공격을 효과적으로 방어하기 위하여 룰 기반으로 악성 행위를 탐지하는 기존의 보안 도구를 결합하고 보완하는 머신러닝 기반의 엔드포인트 탐지 및 대응(EDR, Endpoint Detection and Response) 솔루션이 주목을 받고 있다. 하지만 범용 EDR 솔루션은 오탐률이 높고, 높은 수준의 분석가가 방대한 양의 경보를 모니터링 및 분석해야 하는 문제점이 존재한다. 따라서, IIoT 특성과 취약성을 반영한 머신러닝 기반의 EDR 솔루션 최적화 과정이 필수적이다. 본 연구에서는 IIoT 대상의 APT 공격의 흐름과 영향을 분석하고 머신러닝 기반 APT 탐지 EDR 솔루션을 비교 분석한다.

ABSTRACT

Cyber-attacks targeting endpoints have developed sophisticatedly into targeted and intelligent attacks, Advanced Persistent Threat (APT) targeting the Industrial Internet of Things (IIoT) has increased accordingly. Machine learning-based Endpoint Detection and Response (EDR) solutions combine and complement rule-based conventional security tools to effectively defend against APT attacks are gaining attention. However, universal EDR solutions have a high false positive rate, and needs high-level analysts to monitor and analyze a tremendous amount of alerts. Therefore, the process of optimizing machine learning-based EDR solutions that consider the characteristics and vulnerabilities of IIoT environment is essential. In this study, we analyze the flow and impact of IIoT targeted APT cases and compare the method of machine learning-based APT detection EDR solutions.

키워드

IIoT, Endpoint Security, EDR, APT, Machine Learning

Ⅰ. 서 론

산업용 사물인터넷(IIoT, Industrial Internet of Things)은 사물인터넷(IoT, Internet of Things)을 제조, 운송, 에너지 등의 환경에 도입한 것으로 폭증한 데이터 트래픽을 효율적으로 처리하고 산업 생산성을 획기적으로 개선하고 있다. 산업제어시스템 환경에도 IoT를 융합하여 발전소의 원활한 운영 및 장애 관리를 신속하게 수행할 수 있다. 기존의 산업제어시스템은 네트워크가 분리되어 있고, 특정 용도로만 활용되어 높은 보안성을 유지할 수 있었지만, IIoT의 부상으로 다양한 위협에 노출되었다 [1]. 또한, IIoT에 대한 사이버 공격이 지속적으로

* corresponding author

고도화되면서 제로데이 공격(Zero-day Attack)이 증가하였고, 이에 따라 효과적인 엔드포인트 탐지 및 대응(EDR, Endpoint Detection and Response) 솔루션의 필요성이 대두되었다. 하지만 상용 EDR은 정밀도를 우선시하기 때문에 높은 오탐률을 가지며, 과도한 모니터링 및 분석 업무를 불러일으킨다[2]. 따라서, IIoT 대상의 APT(Advanced Persistent Threat) 공격 및 제로데이 공격에 대한 탐지 및 대응의 효율성을 높이기 위하여 IIoT의 특성과 취약점에 최적화된 머신러닝 기반의 EDR 솔루션이 필수적이다. 본 논문에서는 IIoT를 대상으로 하는 APT 공격의 실제 사례를 바탕으로 IIoT 계층에 대한 공격 흐름 및 영향을 분석하고 머신러닝 기반의 EDR 솔루션을 비교 분석한다.

II. IIoT 계층 아키텍처

표 1. IIoT 계층 아키텍처

Layer		Components
IT	5	Business Application, Cloud Computing, Data Analytics, Internet and Mobile Devices
	4	Data Centers, Office Application, Intranet, Mail and Web Services
Demilitarized Zone		
OT	3	SCADA, HMI, EWS, Control Room and Operator Stations
	2	DCS, PLC(Programmable Logic Controller), Gateways, SIS
	1	Sensors, Motors, Actuators, Transmitters, Embedded Devices

표 1은 IIoT 계층 구조의 아키텍처를 크게 운용 기술(OT, Operation Technology)과 정보 기술(IT, Internet Technology)로 구분한 것이다[3]. 일반적으로 Layer 1은 물리적 프로세스를 수행하는 시스템인 센서, 모터, 액추에이터를 포함하고, Layer 2는 Layer 1의 장치를 제어하는 분산제어시스템(DCS, Distributed Control System), 안전 계측 시스템(SIS, Safety Instrumented System)을 포함한다. Layer 3은 감사 제어 및 데이터 수집(SCADA, Supervisory Control And Data Acquisition) 시스템, 휴먼 머신 인터페이스(HMI, Human Machine Interface), EWS(Engineering Workstation) 등의 모니터링 장치를 사용한다. Layer 4와 5는 정보기술 시스템으로 데이터 센터, 웹 및 메일 서비스와 클라우드 컴퓨팅을 포함한다. IT와 OT 네트워크를 분리하는 DMZ(Demilitarized Zone)는 OT 네트워크에 대한 직접적인 접근을 방지하여 보안성을 유지한다.

III. IIoT 대상 APT 공격 사례 분석

표 2. APT 공격 비교

	Triton	BlackEnergy3[4]	Stuxnet[5]
Initial Attack Vector	Unknown(Spear phishing)	Spear phishing campaign based on documents	Zero-day attack using USB flash drives
Targeted System	Triconex SIS	Legitimate control funtionality via HMIs	ICS under specific conditions
Attack Progress	IT -> Application Server in DMZ -> DCS -> SIS	IT->HMI	IT->SCADA-> PLC
Influence of Attack	Destruction of facilities	Power outage	Destruction of centrifuges

본 장에서는 IIoT 대상의 APT 실제 사례 3가지를 소개한다. 표 2에서 초기 공격 백터, 타겟 시스템, 공격 시나리오, 공격의 영향을 중심으로 각각의 APT 공격을 비교하였다.

첫째, 트리톤(Triton)은 슈나이더 일렉트릭 사의 SIS를 대상으로 한 표적형 공격이다. 실제 사우디 아라비아의 석유 화학 공장을 대상으로 수행한 공격에서는 악성 페이로드의 오류로 버너 관리 시스템을 차단하지 못하여 실패하였지만, MITRE ATT&CK이 제시한 가상 시나리오에 따르면 트리톤은 EWS에서 지속성을 확보한 후, SIS 조작을 통해 가스 폭발을 일으켜 물리적인 파괴를 초래한다.

둘째, 블랙에너지3(BlackEnergy3)는 우크라이나에서 에너지 유통 업체 세 곳의 정보 시스템 손상 및 전기 공급 일시 중단을 목적으로 수행된 APT 공격이다. BlackEnergy3는 피싱 공격을 통하여 공격 대상 식별한 후, 악성 마이크로소프트 오피스 문서를 이메일로 전송하여 네트워크에 침투한다. 이후, HMI (Human Machine Interface) 동작을 모니터링하여 전력 손실을 발생시키는 시나리오로 동작한다.

셋째, 스턱스넷(Stuxnet)은 산업기반 시설을 감시하고 파괴하는 최초의 악성 소프트웨어로, 일부 보조 장치를 사용하여 대상에 접근하여 권한을 얻는 방식으로 초기 침투를 진행한다. 스턱스넷은 SCADA 시스템을 감염시켜, 핵심 라이브러리의 내용을 변경함으로써 PLC를 제어한다.

IV. APT 공격 탐지를 위한 머신러닝 기반 EDR

본 논문에서는 APT 공격 탐지를 위한 대표적인 머신러닝 기반의 EDR (Endpoint Detection and Response) 기법을 비교 분석한다. 표3은 3가지 주요 탐지 방법의 특징을 비교한 것이다.

MLAPT [6]는 머신러닝 기반 APT 공격 탐지 및 예측 시스템으로 위협 탐지, 경고 식별, 공격 예측의 3가지 주요 단계로 구성되며, APT 공격의 각 단계에서 사용되는 기술을 탐지하는 모듈을 융합하여 상관관계 프레임워크를 거쳐 APT 공격을 예측한다.

표 3 머신러닝 기반 EDR 비교

	MLAPT [6]	MOPR [7]	AIDIS [8]
Learning Method	Supervised	Semi-supervised	Supervised
Algorithm	Decision trees, SVM, KNN, Ensemble	Naive Bayes model	Random forest, linear kernel SVM
Technique	Fusion of detection modules and correlation framework	Bayesian network and SOFM	Classification of anomalies by the star depiction of a graph
Process	Threat detection->Alert correlation->Attack prediction	Data collection-> Learning -> classification -> Evaluation	Data collection->Preprocessing->Star Graph Analysis->Meta Model

MOPR [7]은 CPU, RAM 사용 및 네트워크 트래픽 등과 같이 공격 수행 시 생성되는 흔적을 입력으로 하는 머신러닝 기반 멀웨어 분류 시스템이다. 제로데이 공격 데이터로 인한 성능 저하 문제를 해결하기 위해 SOFM(Self Orgnaizing Feature Maps)을 도입하였다.

AIDIS [8]는 베이스라인에서 벗어난 커널 이벤트의 이상 행위를 탐지 및 해석하는 시스템이다. AIDIS는 호스트에서 프로세스 및 네트워크 이벤트 데이터를 수집하여 스타 구조를 통해 비정상적인 이벤트를 분류한다. 또한, 자동으로 식별한 이상 행위를 APT 킬체인에 매핑하여 해석을 제공한다.

세 가지 APT 탐지 방법 모두 머신러닝 기반으로 APT 공격을 탐지하거나, 이상 행위를 분류한다. APT 공격을 세부 단계로 정의하고, 이상 행위를 단계별 동작으로 매핑시켜 APT 공격 탐지 정확도를 향상시킨다. 그러나 APT 공격에 대한 머신러닝 탐지 정확도와 속도의 한계로 인해 효과적인 대응과 IIoT 적용이 어렵다.

Ⅴ. 결 론

산업제어시스템과 IoT의 융합이 활발해지면서 IIoT 엔드포인트를 타겟으로 하는 APT 공격이 급증하고 있다. 또한, IIoT에 대한 사이버 공격이 고도화되면서 IIoT의 특성과 취약점을 고려한 APT 공격 탐지 및 대응 솔루션의 필요성이 부각되고 있다. 이에 따라, 본 논문에서는 IIoT 아키텍처와 공격 사례를 분석하고 머신러닝 기반의 EDR 솔루션을 비교 분석하였다. 후속 연구로 IIoT 네트워크의 정상 패턴과 APT 사이버 킬 체인을 도출하고, 머신러닝 기반의 공격 탐지를 시뮬레이션하여 효과적인 탐지 및 대응 방안을 연구할 계획이다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아 수행된 연구임.

References

[1] Simon D. Duque Anton, et al, “Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests,” International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-6 Sept. 2019.

[2] Wajih UI Hassan, et al, “Tactical Provenance Analysis for Endpoint Detection and Response Systems,” IEEE Symposium on Security and Privacy (SP), pp. 1172-1189, May. 2020.

[3] Panchal, A. C., et al, “Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures,” IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 124-130, Nov. 2018.

[4] M. Geiger, J. Bauer, M. Masuch and J. Franke, “An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems,” 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1537-1543, Sept. 2020

[5] S. Al-Rabiaah, “The “Stuxnet” Virus of 2010 As an Example of A “APT” and Its “Recent” Variances,” 2018 21st Saudi Computer Society National Computer Conference (NCC), pp. 1-5, Apr. 2018

[6] Ghafir, I., et al, “Detection of advanced persistent threat using machine-learning correlation analysis,” Future Generation Computer Systems (FGCS), Vol. 89, pp. 349-359, 2018

[7] Pete Burnap, et al, “Malware classification using self organising feature maps and machine activity data,” Computers & Security, Vol. 73, pp. 399-410, 2018

[8] Luh, R., et al, “AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes,” Computers & Security 2019, Vol. 84, pp. 120-147, 2019