에너지 기업 산업용 제어시스템(OT/ICS)에 대한 최근 사이버보안 위협과 윈도우OS 기본기능을 통한 탐지 방안

김민규*, 이용구**
* **한국수력원자력 중앙연구원
e-mail:kim.minkyu@khnp.co.kr* , lee.yongku@khnp.co.kr**

Energy Enterprise OT/ICS Security: Cyber Threat Analysis and Detection Using Windows OS Event Log

Min-Kyu Kim*, Yong-Ku Lee**
* **Central Research Institue, Korea Hydro & Nuclear Power Co., Ltd.

요 약

에너지 기업의 산업용 제어시스템(OT/ICS)은 랜섬웨어, 스피어피싱, 이동식 매체를 통한 공격 등 다양한 사이버 위협에 노출되어 있으며, 특히 레거시 시스템 사용과 연속 운전 요구 등의 특성으로 별도 보안 프로그램 설치에 제약이 있다. 이에 본 연구에서는 MITRE ATT&CK 프레임워크를 활용해 에너지 분야에서의 사이버 공격 유형을 분석하고, 공격 단계별 윈도우 OS 기본 이벤트 로그를 활용한 탐지 방안을 제시한다. 추가 보안 솔루션 없이도 윈도우 기본 기능만으로 발전소, 변전소, 송전망 등 핵심 에너지 인프라에 대한 공격 징후를 조기에 발견하여 피해를 예방할 수 있음을 제고하고자 한다.

1. 서론

에너지 기업의 산업용 제어시스템(Operational Technology/Industrial Control System, OT/ICS)에 대한 사이버 공격은 스턱스넷(Stuxnet) 사례 이후 지속적으로 증가하고 있다. MITRE ATT&CK에 따르면 2022년부터 2024년까지 에너지 분야 OT/ICS 환경에 대한 사이버 공격은 30% 이상 증가했으며, 특히 전력망, 송유관, 발전소 등 핵심 에너지 인프라를 대상으로 하는 랜섬웨어 공격이 급증하고 있다.[1] 이러한 공격은 단순한 데이터 유출을 넘어 물리적 설비에 직접적인 영향을 미치는 위험성이 있어 국가 안보와 경제에 심각한 위협이 된다.

2023년 기준 한국 에너지 분야 ICS 시스템의 31.54%에서 멀웨어가 감지되었으며, 이는 글로벌 평균보다 높은 수치이다.[2] 또한 최근 러시아-우크라이나 전쟁과 같은 지정학적 충돌로 인해 에너지 인프라 ICS를 표적으로 하는 국가 간 분쟁으로 의심되는 공격도 증가하고 있어, 에너지 기업의 산업 인프라 보호의 중요성이 더욱 커지고 있다.

따라서 이 연구에서는 발전소 및 에너지 관련 제어시스템 특성상 별도의 보안 프로그램 설치가 어려운 환경에서도 활용 가능한 윈도우 OS 기본 보안 이벤트 로그를 활용한 사이버 공격 탐지 방안을 제시하고자 한다.

2. 본론

2.1 제어시스템의 보안 프로그램 설치 제약 요인

2.1.1 레거시 시스템 및 단종 운영체제 문제

에너지 분야의 산업제어시스템(ICS)은 대부분 장기간 운영을 전제로 설계되어 단종된 윈도우 운영체제에서 운영되고 있다. 발전소 및 변전소의 분산제어시스템(DCS)의 77.5% 이상이 단종된 윈도우 버전(Windows XP, Windows 7)에서 운영되고 있다.[2] 이러한 시스템은 보안 패치나 업데이트가 지원되지 않아 최신 보안 솔루션 설치가 불가능한 경우가 많다.

2.1.2 연속 운전 및 가용성 요구사항

에너지 기업의 OT 환경은 전력 공급, 원유 정제, 가스 관리 등 24시간 연속 운전이 필수적이다. 패치나 업데이트는 몇 년에 한 번씩 실시되는 정비 기간에만 가능하다. 보안 솔루션 설치는 시스템 성능에 영향을 미치거나 예기치 않은 장애를 일으킬 수 있어, 지속적인 에너지 공급이 필요한 현장에서는 새로운 솔루션 도입을 꺼리는 경향이 있다.

2.1.3 다양한 이기종 장비 및 프로토콜 사용

에너지 기업은 발전, 송배전, 변전소, 파이프라인 등 다양한 영

역에서 서로 다른 제조사의 이기종 장비와 프로토콜을 사용하기 때문에, 통합 보안 솔루션 적용이 기술적으로 어렵다. 특히 SCADA, DCS, PLC, RTU 등 다양한 제어 시스템이 혼재되어 있어 표준화된 보안 솔루션 적용이 제한적이다.

2.1.4 신뢰성 보장

에너지 기업은 안정적인 에너지 공급이 최우선 과제로, 안정성과 성능이 최우선시된다. 보안 솔루션 도입 시 시스템 안정성에 영향을 줄 수 있다는 우려가 존재한다. 실제로 보안 프로그램의 오탐으로 인한 발전 중단이나 송전망 이상은 국가 전체의 에너지 공급에 심각한 영향을 미칠 수 있어, 보안보다 연속 운전의 안정성을 우선시하게 된다.

2.2 산업제어시스템에서 탐지되는 주요 사이버 공격

에너지 기업의 산업용 제어시스템을 대상으로 한 최근 주요 사이버 공격은 다음과 같이 분류할 수 있다.

2.2.1 랜섬웨어 공격

최근 에너지 분야 제어시스템을 대상으로 한 공격 중 가장 급증하고 있는 유형은 랜섬웨어 공격이다. 2022년 에너지 분야 ICS를 노린 랜섬웨어 공격은 231건에서 2023년 204건으로 다소 감소했으나, 이는 공격의 효율성이 높아졌기 때문이며 전체 공격 자체가 줄어든 것은 아니다.[2] 주요 사례로는 2016년 미국 미시간 수자원 발전소 랜섬웨어 감염 사태, 2019년 미국 콜로니얼 파이프라인 랜섬웨어 공격 등이 있다.

2.2.2 스피어피싱을 통한 표적 공격

스피어피싱 공격은 에너지 기업 직원을 대상으로 악성 첨부파일을 담은 이메일을 전송하는 방식으로 이루어진다. 2016년 미국 미시간 수자원 발전소 랜섬웨어 감염의 원인이 스피어피싱이었으며, 특히 에너지 분야 엔지니어와 운영자를 대상으로 한 맞춤형 스피어피싱은 공격 성공률이 높은 것으로 나타났다.[3]

2.2.3 이동식 매체를 통한 악성코드 감염

USB와 같은 이동식 저장매체를 이용해 물리적으로 분리된 발전소나 변전소 네트워크에 악성코드를 유입시키는 공격이 지속되고 있다. 이란 부셰르 원전을 대상으로 한 스턱스넷 공격이 대표적인 예이며, 최근에는 이동식 매체를 통해 산업용 제어시스템에 특화된 멀웨어가 유포되는 사례가 증가하고 있다.

2.2.4 원격 서비스 및 취약점 악용 공격

에너지 기업의 OT 환경에 원격 모니터링과 유지보수를 위해 존재하는 원격 서비스(Remote Administration Tool, RAT)를 악용한 공격도 증가하고 있다. 에너지 분야 ICS 중 3분의 1가량이 RAT를 사용하고 있으며, 그 중 20%가 ICS 자체에 연결되어 있어 공격 위험이 높다.[3]

2.2.5 내부 확산 및 권한 상승 공격

초기 침투 이후 SMB 프로토콜 취약점과 같은 내부 네트워크 취약점을 활용해 제어망으로 확산하고, 운영자 권한을 탈취하는 공격이 발생하고 있다. 최근 에너지 기업 대상 랜섬웨어 공격은 초기 침투 후, 제어망을 탐색하며 주요 제어 자산을 식별하고 권한을 획득한 뒤 서비스 중단이나 데이터 암호화를 시도하는 방식으로 진화했다.

2.3 MITRE ATT&CK 프레임워크를 활용한 공격 단계별 분석

MITRE ATT&CK for ICS 프레임워크는 산업제어시스템에 대한 공격을 체계적으로 분류하고, 각 공격의 단계와 기술을 구조화한 지식 기반이다. 이 프레임워크를 활용하여 에너지 기업 대상 주요 공격 유형을 단계별로 분석하면 [표 1]과 같다.

[표 1] 공격 단계별 MITRE ATT&CK 매핑

공격 단계	공격 유형	MITRE 기술코드	주요 공격 사례
초기 접근	랜섬웨어 공격	T0883	발전소 제어 프로젝트 파일 감염
	스피어피싱	T0865	전력회사 엔지니어 대상 피싱
	이동식 매체	T0847	발전소 폐쇄망 USB 침투
	원격 서비스	T0822	변전소 원격 관리 시스템 침투
실행	악성코드 실행	T0807	PLC 명령어 실행
		T0871	SCADA API 악용
지속성 확보	백도어 설치	T0873	발전소 제어 프로젝트 수정
		T0839	변전소 RTU 펌웨어 수정
권한 상승	관리자 권한 획득	T0874	발전 제어 시스템 후킹
		T0890	관리자 권한 탈취
내부 확산	네트워크 확산	T0859	정상 계정 이용 확산
		T0884	프록시를 통한 내부 이동
데이터 수집	정보 수집	T0802	자동화된 발전소 데이터 수집
		T0811	에너지 설비 정보 수집
통제 및 제어	원격 제어	T0869	표준 프로토콜을 통한 명령
		T0885	일반 포트를 통한 C2 통신
보안 회피	탐지 회피	T0849	정상 파일 위장
		T0851	시스템 접근 은닉
공정 제어 방해	제어 시스템 조작	T0806	발전소 I/O 과부하 공격
		T0836	발전 파라미터 변조
대응 기능 방해	알람 제어	T0878	전력망 경보 억제
		T0800	펌웨어 업데이트 모드 강제 전환
영향	시스템 파괴	T0880	발전소 안전 시스템 무력화
		T0826	에너지 서비스 중단
		T0814	송전망 서비스 거부

2.3.1 공격별 공격 특성 분석

에너지 기업에 대한 랜섬웨어 공격은 일반적인 IT 환경의 랜섬웨어 공격과 다른 특성을 보인다. 특히 발전소, 송전망, 변전소, 파이프라인과 같은 핵심 에너지 인프라에 대한 직접적인 영향을 미칠 수 있어 국가 안보와 직결된 심각한 물리적, 경제적 피해를 초래할 가능성이 있다.

스피어피싱 공격은 초기 접근(T0865) 단계에서 발생하며, 에너지 기업 직원들이 악성 첨부파일을 열면 실행(T0807) 단계로 이어진다. 이동식 매체를 통한 공격은 이동식 매체를 통한 복제(T0847)를 사용하여 발전소나 변전소의 격리된 네트워크에 침투한다. 원격 서비스 관련 공격은 외부 원격 서비스(T0822)를 악용하여 원격 관리 시스템을 통해 초기 접근을 시도한다.

내부 확산 및 권한 상승 공격은 유효한 계정(T0859)과 권한 상승을 위한 취약점 악용(T0890)을 활용하여 공격 범위를 제어망으로 확대한다. 최종적으로는 영향 측면에서 가용성 손실(T0826)과 서비스 거부(T0814)를 통해 에너지 서비스 중단이나 랜섬웨어 암호화가 이루어진다.

2.4 윈도우 보안 이벤트 로그를 통한 공격 탐지

에너지 기업의 산업용 제어시스템 환경에서 별도의 보안 솔루션 없이도 윈도우 OS 기본 기능인 이벤트 로그를 활용한다면 사이버 공격을 탐지할 수 있다. [표 2]는 MITRE ATT&CK 공격 코드별로 연관된 윈도우 보안 이벤트 로그 ID와 설명이다.

[표 2] MITRE 공격 코드와 윈도우 보안 이벤트 ID 매핑

MITRE 기술코드	윈도우 이벤트ID	이벤트 설명	공격 탐지 포인트
[초기 접근] T0883 T0865 T0847 T0822	4688	프로세스 생성	제어 시스템 관련 비정상 프로세스
	4624	계정 로그온 성공	비정상 시간대 로그인
	4625	계정 로그온 실패	다수의 로그인 실패
	5156	방화벽 연결 허용	외부 의심 IP 연결
[악성코드 실행] T0807 T0871	4688	프로세스 생성	제어 관련 비정상 명령어
	1006	악성코드탐지 (Windows Defender)	악성코드 탐지
	1007	악성코드설치시도 (Windows Defender)	악성코드 설치 시도
	4697	서비스 설치	비인가 서비스 설치
[지속성 확보] T0807 T0871	4698	예약된 작업 생성	비인가 스케줄 작업
	7045	새 서비스 설치	에너지 설비 관련 조작
	4657	레지스트리 값 수정	제어 시스템 레지스트리 변경
[권한상승] T0874 T0890	4672	특수 권한 할당	제어 관리자 권한 획득
	4670	개체 권한 변경	제어 설정 변경
	4648	다른 사용자 자격 증명을 사용한 로그온	권한 상승 시도
[내부확산] T0859 T0884	4624	로그온 성공	제어망 내부 이동
	5156	방화벽 연결 허용	제어망 내 비정상 통신
	4778	세션 재연결	원격 세션 재연결
[데이터 수집] T0802 T0811	4663	개체 접근	제어 데이터 접근
	4656	개체 접근 실패	보호된 데이터 접근 시도
	5145	공유 개체 접근	중요 문서 접근
[통제 및 제어] T0869 T0885	5156	방화벽 연결 허용	외부 C2 통신
	5157	방화벽에서 차단된 연결	차단된 통신 시도
	4688	프로세스 생성 (외부 통신 시도)	통신 관련 프로세스
[탐지회피] T0849 T0851	4660	개체 삭제	로그 파일 삭제
	1102	감사 로그 정리	감사 로그 삭제
	104	감사 로그 초기화	감사 로그 초기화
[공정 제어 방해] T0806 T0836	4688	프로세스 생성 (제어 SW 대상)	발전/변전 제어 접근
	4663	제어 시스템 파일 접근	제어 시스템 설정 접근
	4657	구성 설정 변경	발전 파라미터 수정
[대응 기능 방해] T0878 T0800	4657	알람 관련 레지스트리 수정	경보 시스템 수정
	6005	이벤트 로그 서비스 시작	로그 서비스 조작
	6006	이벤트 로그 서비스 중지	로그 서비스 중단
[시스템 영향] T0880 T0826 T0814	7036	서비스 시작/중지	발전 제어 서비스 중단
	41	시스템 충돌	제어 시스템 중단
	1074	시스템 종료	비정상 종료
	6008	예기치 않은 종료	강제 종료

2.4.1 초기 접근 및 실행 단계 탐지

이벤트 ID 4688(프로세스 생성)는 시스템에서 새로운 프로세스가 실행될 때 기록된다. 또한 토큰 승격 유형(%%1936, %%1937, %%1938)을 분석하여 권한 상승 시도를 파악할 수 있다. 에너지 기업에서는 발전 제어 관련 비정상적인 명령어 실행을 탐지하는 데 유용하다.[4]

이벤트 ID 4624(계정 로그온 성공)와 4625(계정 로그온 실패)는 로그온 유형을 분석하여 원격 로그온 및 원격 대화형 로그온을 식별할 수 있다. 발전소 정비 기간이 아닌 시점의 원격 접속은 의심스러운 행위로 간주된다.

이벤트 ID 1006, 1007은 Windows Defender에서 악성코드 탐지 및 설치 시도를 나타내므로 초기 실행 단계의 중요한 지표가 된다.

2.4.2 권한 상승 및 지속성 단계 탐지

이벤트 ID 4672(특수 권한 할당)는 PtH(Pass-the-Hash) 공격

이나 권한 상승 시도를 탐지하는 데 유용하다. 특히 일반 운영자 계정에서 발생하는 경우 더욱 주의가 필요하다.
이벤트 ID 4670(개체 권한 변경)은 파일, 레지스트리, 서비스 등의 접근 권한이 변경될 때 기록되며, 발전소 제어 시스템 설정 변경 시도를 탐지할 수 있다.
이벤트 ID 4657(레지스트리 값 수정), 4698(예약된 작업 생성), 7045(새 서비스 설치)는 공격자의 지속성 확보 시도를 탐지하는 데 유용하다.

2.4.3 탐지 회피 및 로그 삭제 탐지
이벤트 ID 1102(감사 로그 정리)는 공격자가 흔적을 지우기 위해 로그를 삭제했음을 나타낸다. 특히 이 이벤트가 발생하면 즉각적인 조사가 필요하다.
이벤트 ID 104(로그 초기화), 1100(이벤트 로깅 중지)는 로그 서비스 자체를 조작하려는 시도를 나타낸다.

2.4.4 시스템 영향 단계 탐지
이벤트 ID 7036(서비스 상태 변경), 41(시스템 충돌), 1074(시스템 종료), 6008(예기치 않은 종료)는 공격으로 인한 실제 시스템 영향을 식별하는 데 도움이 된다.
발전소, 변전소, 송전설비 등의 제어 시스템에서는 특히 제어 관련 서비스의 중단이나 비정상적인 시스템 종료는 즉각적인 조사가 필요한 심각한 이벤트이다.

3. 결론

에너지 기업의 산업용 제어시스템(OT/ICS)에 대한 사이버 보안 위협은 지속적으로 증가하고 있으며, 공격 방식은 더욱 정교해지고 있다. 특히 랜섬웨어, 스피어피싱, 이동식 매체 활용, 원격 서비스 악용, 내부 확산 등의 공격은 발전소, 변전소, 송전망, 파이프라인 등 에너지 인프라에 심각한 위협이 되고 있다.

본 연구에서는 MITRE ATT&CK 프레임워크를 활용하여 에너지 기업 산업제어시스템에 대한 주요 공격 유형을 분석하고, 각 공격 단계별로 윈도우 OS 기본 보안 이벤트 로그를 통한 탐지 방법을 제시하였다. 비록 에너지 분야 제어시스템의 특성상 별도의 보안 프로그램 설치가 어려운 환경이 많지만, 윈도우 운영체제 기본 기능인 이벤트 로그만으로도 주요 공격을 탐지할 수 있음을 확인하였다.

이벤트 ID 4688(프로세스 생성), 4672(특수 권한 할당), 4670(개체 권한 변경), 1102(감사 로그 정리) 등을 중심으로 한 모니터링 체계를 구축함으로써, 추가적인 보안 솔루션 없이도 사이버 공격의 징후를 조기에 탐지하고 대응할 수 있다. 이러한 접근 방식은 특히 보안 프로그램 설치가 제한된 레거시 발전소 및 에너지 인프라 제어시스템 환경에서 큰 의미가 있다.

에너지 기업의 산업제어시스템 보안은 국가 안보와 경제 활동에 직결되는 중요한 문제이다. 따라서 OS 기본 보안 기능을 활용한 공격 탐지와 함께, 네트워크 분리, 접근 통제 강화, 직원 교육 등 종합적인 보안 대책을 마련하는 것이 필요하다. 본 연구가 에너지 기업의 산업제어시스템 보안 강화에 기여하고, 윈도우 기본 기능을 활용한 효과적인 보안 모니터링 구축에 도움이 되기를 기대한다.

참고문헌

[1] MITRE ATT&CK ICS tactics [웹사이트], (2025.4.8.), URL:https://attack.mitre.org/tactics/ics
[2] 보안뉴스-[2024 OT 보안 리포트] 꿈틀대는 OT 보안, 본격 활성화 신호탄 터졌다! [웹사이트], (2024.2.29.), URL:https://m.boannews.com/html/detail.html?mtype=1&idx=127211
[3] 이글루-사례로 보는 산업제어시스템의 랜섬웨어 [웹사이트], (2020.6.1.), URL:https://www.igloo.co.kr/security-information/사례로-보는-산업제어시스템의-랜섬웨어/
[4] ITWORLD-모니터링해야 할 중요한 윈도우 10 보안 이벤트 로그 ID. [웹사이트], (2020.6.19.) URL:https://www.itworld.co.kr/article/3569413