

ISSN 1738-9593
제20권 1호

www.ksii.or.kr



2019 춘계학술 발표대회

논문집

4월 26일(금) ~ 27일(토)

동국대학교 서울캠퍼스 사회과학관



주최: 사단법인 한국인터넷정보학회

주관: 동국대학교 서울캠퍼스

후원: SK스토아(주), (주)카카오, (주)LGCNS, (주)아이티센

www.ksii.or.kr



KOREAN SOCIETY FOR INTERNET INFORMATION
사단법인 한국인터넷정보학회

B. 인터넷보안 (좌장 : 조규상 교수(동양대))

B-1 IoT 환경에 적합한 경량 블록암호 성능 분석	53
김의진, 곽진(아주대)	
B-2 의료정보접근을 위한 IoT 상황정보기반으로한 자동인증시스템의 서비스 모델 구현	55
함규성, 주수중(원광대)	
B-3 ☆ ICS 사이버 공격 동향 분석	57
고영민, 김득훈, 곽진(아주대)	
B-4 Frida를 이용한 안드로이드 악성앱 분석기술 연구	59
이석훈, 류재철(충남대)	
B-5 ☆ 악성코드 작성자 그룹 식별을 위한 저자 클러스터링을 적용한 특징 추출	61
신건윤, 한명묵(가천대)	
B-6 최신 핀테크 서비스 현황 및 보안 동향 분석	63
고주성, 곽진(아주대)	
B-7 웹 브라우저 취약점 사례 분석 및 대응 방안	65
이민경, 최슬기, 곽진(아주대)	

C. 인터넷미디어 (좌장 : 이우찬 교수(인천대))

C-1 Conditional GAN을 이용한 단일 영상에서의 그림자 제거 방법	71
윤희진, 전준철(경기대)	
C-2 빅데이터 분석과 AHP를 이용한 악성 댓글 분류	73
김진우, 조혜인, 이봉규(연세대)	
C-3 U-Net을 이용한 간 분할 방법	75
김강직, 전준철(경기대)	
C-4 인터넷 먹방 프로그램의 긍정적 및 부정적 효과	77
지양슈에진, 황하성(동국대)	

B. 인터넷보안

ICS 사이버 공격 동향 분석

고영민*, 김득훈**, 꺾 진***

***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과 정보보호응용및보증연구실

e-mail : *science8810@ajou.ac.kr, **dhkim.isaa@gmail.com, ***security@ajou.ac.kr

Analysis of ICS Cyber Attack Trend

Young-Min Ko, Deuk-Hun Kim**, Jin Kwak***

***Department of Cyber Security, Ajou University

**ISAA Lab., Department of Computer Engineering, Ajou University

요 약

IT 기술의 발전에 따라 산업 제어 시스템(ICS)은 원자력 발전소나 자동차 생산시설과 같은 사회기반시설의 제어에 사용되고 있다. 이러한 사회기반시설에 해당하는 인프라는 전력, 수도 등 높은 가치의 자원을 지니고 있고, 침해사고 발생 시 비가역적인 손실이 발생할 수 있다. 또한, ICS는 산업 규모의 증가로 제어의 효율성을 증가시키기 위해 네트워크 기반으로 제어되고 있어, 공격 빈도와 침해 심각성이 증가하고 있다. 이에 따라 ICS의 보안 요구 수준 또한 높아지고 있으며, 공격에 대한 선제적 대응방안의 수립이 필요한 실정이다. 따라서 본 논문에서는 ICS에 대한 사이버 공격 동향을 분석하고 이에 대한 대응방안을 제시한다.

1. 서 론

산업 제어 시스템(ICS:Industrial Control System)은 주요 사회기반시설 인프라에 이용되고 있으며, 이러한 인프라들은 높은 가치를 지니고 있다. 미국의 홈랜드 시큐리티 산하기관 ICS-CERT의 자료를 분석한 Positive Technologies사의 연간보고서에 따르면, ICS에 대한 공격의 빈도와 침해사고의 심각성은 지속적으로 증가하고 있다[1]. 2015년 Black energy에서 2016년 Industroyer를 거쳐 2017년 TRITON에 이르기까지 ICS를 대상으로 하는 멀웨어들은 지속적으로 제작되고 있으나, 국내에는 ICS를 공격 대상으로 하는 멀웨어들의 분석자료가 많지 않은 실정이다.

따라서 본 논문에서는 공격에 대한 선제적 대응방안의 수립을 위해 ICS를 대상으로 하는 멀웨어들의 라이프 사이클과 작동 메커니즘을 기반으로 ICS공격 동향에 대해 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 ICS의 구성요소에 대해 설명한다. 3장에서는 ICS를 대상으로 하는 멀웨어들과 라이프 사이클을 기반으로 각각의 작동 메커니즘을 분석하고, 4장에서 결론을 맺는다.

2. 관련 연구

ICS에 대한 공격은 제어 시스템에 대한 제어 수치 조작으로 공격자에 의해 원하는 결과를 유도하는 방식으로 이루어진다. ICS에서 자동화 설비를 제어하는 시스템은 다수의 단순 작업들을 직접 제어하는 분산 제어 시스템(DCS:Distributed Control System)인 원격 터미널 유닛(RTU:Remote Terminal Unit) 및 프로그래머블 로직 컨트롤러(PLC:Programmable Logic Controller)와, 이를 제어 및 관리하는 관리 제어 및 데이터 수집(SCADA:Supervisor

Control And Data Acquisition)시스템으로 구성되어있으며, 이에 대한 설명은 아래와 같다[2].

2.1 분산 제어 시스템(DCS)

DCS란 산업기기용 프로세서의 제어 시스템으로, 컨트롤러 기능과 필드 연결 모듈이 시스템 전체에 분산되어 있다. 프로세서는 입력 모듈에서 정보를 수신하고 처리하며 출력 모듈에서 수행할 제어 작업을 결정하게 된다. DCS에는 PLC, RTU 등이 활용되고 있다.

2.2 관리 제어 및 데이터 수집(SCADA)

SCADA시스템은 컴퓨터, 네트워크 데이터 통신 등을 이용하여 프로세스 감독 관리를 수행하는 제어 시스템 아키텍처이다. 컨트롤러 수치 조정과 같은 조작 명령을 수행하나, 실질적 제어는 DCS 레벨에서 이루어진다.

3. ICS 멀웨어 분석

ICS에 대한 대표적인 공격으로는 2010년 이란의 핵 설비를 공격한 스텍스넷이 있다. 스텍스넷의 경우 PLC의 작동주기 및 제어 수치의 조정을 통해 설비 동작불능을 유도했다[3]. ICS를 대상으로 한 치명적 공격 사례 중 하나인 스텍스넷은 이후 ICS를 대상으로 하는 멀웨어의 파생에 영향을 미치게 된다. 본 장에서는 스텍스넷 이후 ICS대상 멀웨어들 중 Black energy, Industroyer, TRITON에 대하여 분석한다.

3.1 Black energy

2015년 우크라이나의 발전소를 공격한 Black energy는 마이크로소프트 XLS 문서를 통한 사회공학적 공격기법을 사용하였다. 이 문서를 열람하게 되면 Black Energy3 멀웨어가 설치되며, win32/KillDisk 멀웨어를 다운받게 된다. 이후, 멀웨어가 동작하여 시스템 파일을 파괴하고 프로세스를 종료하게 된다. Black energy의 모듈은 표 1과 같은 구조를 가진다[4].

(표 1) Black energy 멀웨어 모듈

모듈	기능
Malicious XLS file	악성 매크로를 내재한 BE3제작용 파일
Black energy3	감염 PC에서 KillDisk를 다운받는 멀웨어
Killdisk	시스템 파일 파괴 및 프로세스 강제 종료

3.2 Industroyer

2016년 하반기 우크라이나의 발전소를 목표로 한 공격으로, Black energy의 경우 단순 시스템 파일 파괴 및 프로세스 강제 종료에 그친 반면 Industroyer는 사전에 하드코딩 해둔 프록시 주소로 C&C서버와 추가적인 명령을 받는 등 발전된 모습을 보인다. Industroyer는 기본적으로 모듈형 멀웨어로, 표 2와 같은 구조를 가진다[5].

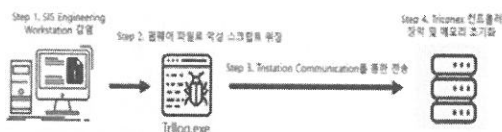
(표 2) Industroyer 멀웨어 모듈

모듈	기능
메인 백도어	메인 백도어를 제외한 컴포넌트 제어 및 C&C 서버와의 통신 제어
추가 백도어	메인 백도어의 비활성화시를 대비한 지속 동작 메커니즘
런처 컴포넌트	멀웨어 동작 시작 내재 및 페이로드&데이터 와이핑 구동 컴포넌트
페이로드 컴포넌트	IEC 60870-5-101, IEC 60870-5-104, IEC 61850, Open Platform Communication Data Access의 ICS 프로토콜 대상 4가지 페이로드로, 네트워크 매핑과 제어 장치에 대한 명령 내재
데이터 와이퍼 컴포넌트	시스템 데이터 삭제 컴포넌트

또한, 공격이 익스플로잇 된 이후에는 공격자가 자체적으로 개발한 포트 스캐너를 통해 얻은 내부 주소를 대상으로 CVE-2015-5374 취약점으로 ICS보안 설비에 대한 서비스 거부 공격을 진행하여 ICS보안체계를 무력화한다.

3.3 TRITON

TRITON은 2017년 중동 지역을 공격 목표로 하는 ICS 멀웨어로, 스틱스넷과 유사하게 특정 기기에 영향을 미친다. 스틱스넷의 공격대상이 PLC인 반면, TRITON은 Triconex사의 안전계장시스템(SIS:Safety Instrumented Systems)을 대상으로 한다. 해당 기기 운영체제의 제로데이를 이용하여 공격하였으며, 공격 시나리오의 구성도는 아래 그림 1과 같다[6].



(그림 1) TRITON 공격 시나리오

공격 시나리오를 단계별로 나타내면 다음과 같다.

Step 1. SIS Engineering Workstation이 이에 접속한 감염된 사용자 단말을 통해 감염된다.

Step 2. 펌웨어 파일로 위장한 악성스크립트 제작용 라이브러리와 컨트롤러 간 통신용 Tristation communication 모듈을 다운로드한다.

Step 3. 펌웨어로 위장한 악성스크립트를 Tristation communication을 이용해 컨트롤러에 전송한다.

Step 4. Triconex OS 제로데이를 이용해 메모리에 백도어를 설치한 후, 권한을 기존 상태로 복구하고 사용한 메모리를 초기화한다.

3.4 멀웨어 비교 및 분석

위에서 분석한 멀웨어들의 특징 및 공격 대상을 각각 비교 및 분석하여 나타내면 아래 표 3과 같다.

(표 3) 멀웨어별 특징

멀웨어	공격 대상	주요 공격 내용	위험 종류
Black energy	SCADA 시스템	데이터 와이핑	데이터 변조
Industroyer	SCADA 시스템 및 보안체계	데이터 와이핑 및 DoS	데이터 변조, 서비스 거부
TRITON	SCADA 시스템 및 SIS	DCS 제어 수칙 조작	데이터 변조, 권한 상승

4. 결론

ICS기술이 발전함에 따라 다양한 공격 가능성이 생겨났고, 3장에서 분석한 바와 같이 ICS 멀웨어는 지속적으로 발전해왔다. 또한 ICS기술은 IoT환경의 등장과 함께 빌딩 에너지 제어 시스템과 스마트 홈 제어 기술로 발전하고 있는 추세이며, 해당 기술의 대용적 사용 가능성을 고려하였을 때 보안 대책 수립의 필요성이 존재한다.

본 논문의 ICS 멀웨어 주요 공격 대상 및 라이프사이클 분석을 통해 DCS나 SCADA시스템을 사용하는 설비에서의 멀웨어 대응방안을 마련할 수 있다. 향후 연구에서는 ICS에서 영역을 확장하여 가상 물리 시스템(CPS : Cyber Physical System)에서의 보안 및 정보 이벤트 관리 시스템과 침입 탐지 시스템, 사용자 행위분석 시스템을 이용한 지능형 행위 분석 아키텍처 설계에 대해 연구하고자 한다.

참고 문헌

- [1] Positive Technologies, "ICS Security: 2017 in review", <https://www.ptsecurity.com/ww-en/analytics/ics-security-2017/>, Positive Technologies, pp. 4-13, Feb. 2018.
- [2] Tyson Macaulay and Bryan L. Singer, "Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS", Auerbach Publications, pp. 45-46, Dec. 2011.
- [3] Karnouskos and Stamatidis, "Stuxnet worm impact on industrial cyber-physical system security", IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, IEEE, pp.2-4, Nov. 2011.
- [4] Lee, Robert M., Michael J. Assante and Tim Conway, "Analysis of the cyber attack on the Ukrainian power grid", SANS Industrial Control Systems 23, pp. 4-5, Mar. 2016.
- [5] Cherepanov and Anton, "WIN32/INDUSTROYER A new threat for industrial control systems", https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, ESET, pp. 2-15, June. 2017.
- [6] Fireeye, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>, Fireeye, Dec. 2017.