산업시설을 겨냥한 악성코드 공격 사례 분석과 대응전략

이세찬[1], 민무홍[1]
[1]성균관대학교 컴퓨터교육과 학부과정
[1]성균관대학교 컴퓨터교육과 조교수
chan1031@skku.edu, iceo@skku.edu

Malware Attacks Targeting Industrial Facilities and Response Strategies

Sechan Lee[1], Moohong Min[1]
[1]Dept. of Computer Education, Sungkyunkwan University

요 약

북한의 사이버 위협은 점점 정교해지고 있으며, 이러한 상황 속 산업시설을 겨냥한 악성코드 공격은 국가 안보에 치명적인 영향을 미칠 수 있다. 본 논문은 스턱스 넷, 에칸스 랜섬웨어, 콜로니얼 파이프라인 랜섬웨어를 분석하고 산업시설 보안 강화 방안을 제시한다. 스턱스 넷은 이란 핵 시설의 PLC 를 조작해 공격을 시도했고, 에칸스는 랜섬웨어 공격을 통해 혼다의 자동차 생산 공장을 마비시켰으며, 콜로니얼 파이프라인 랜섬웨어 또한 감염을 통해 시설을 마비시켰다. 위 공격사례를 분석하고, 이에 대응하기 위한 6 가지 대응 전략을 소개한다.

1. 서론

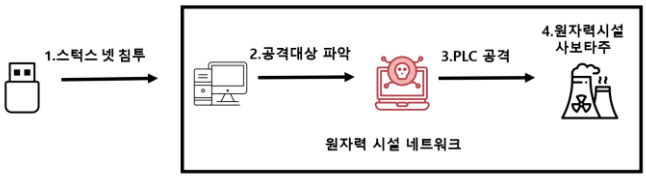
최근 북한의 사이버 위협은 '2022 년 방산업체 해킹 사건', '3.20 전산망 마비', '법원 전산망 해킹' 등 점점 더 정교하고 고도화된 형태로 발전하고 있다. 이와 같은 상황에서 산업시설을 겨냥한 사이버 공격은 데이터 탈취를 넘어 산업, 경제, 물리적 피해까지 초래할 수 있기에 북한의 주요 공격 목표가 될 가능성이 크다. 따라서 산업시설 공격에 대한 사례 분석과 대응 전략 마련이 필요하다. 본 논문에서는 산업시설을 겨냥한 대표적인 악성코드인 '스턱스 넷', '에칸스 랜섬웨어', '콜로니얼 파이프라인 랜섬웨어'를 분석하고, 산업시설 보안강화를 위한 방안을 제시하고자 한다.

2. 스턱스 넷 분석

스턱스 넷은 2010 년 6 월 이란의 핵 프로젝트를 지연시키기 위해 미국과 이스라엘에서 개발한 원자력 시설 공격용 악성코드이며, 최초로 산업시설을 공격한 악성코드라는 점에서 의의가 있다.

또한 스턱스 넷은 무려 4 개의 제로데이 취약점을 보유하고 있었으며, 대만의 Realtek, Jmicron 두개의 회사에서 탈취한 디지털 인증서를 통해 운영체제의 커널에 침투하고, 최초의 산업용 루트 킷을 활용하여 은밀하고 지속적인 APT(Advanced Persistent Threat) 공격을 가했다.

2.1 침투 및 공격 과정



(그림 1) 스턱스 넷 침투, 공격 과정

스턱스 넷은 감염된 USB를 통해 이란의 원자력 시설에 침투했다. 이후 공격을 위해 핵 원심분리기를 제어하는 PLC(제어장치)를 공격해야 했는데, PLC는 이를 제어하는 컴퓨터와 연결되어 있기 때문에 해당 컴퓨터를 공격 대상으로 설정했다. 공격 대상을 감염시킨 이후 PLC를 공격하여 핵 원심 분리기의 회전 속도를 급격하게 증가시켜 원자력 시설의 사보타주를 유도했고 결국 이란의 핵 프로젝트를 지연시키는 데 성공했다 [1].

3. 에칸스 랜섬웨어 분석

에칸스의 이름은 뱀(Snake)을 거꾸로 부른 Ekans 를 지칭한다. 에칸스는 단순한 형태의 랜섬웨어로 산업 제어시스템(ICS)를 공격하며, 2020 년 혼다의 자동차 생산 공장을 공격했었다.

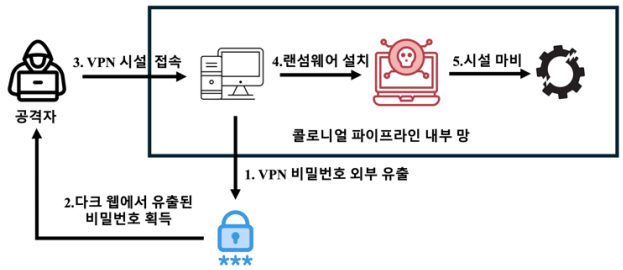
3.1 침투 및 공격 과정

자세한 침투 경로는 알려지지 않았으나 피싱 메일 혹은 코로나 19 로 인해 원격 근무, 공급망 공격을 통해 유입된 것으로 추정된다. 이후 에칸스는 산업 제어시스템에서 실행 중인 프로세스들을 중지시켜 산업시설의 작동을 중단시키고, 다른 랜섬웨어처럼 파일들을 암호화한 후 복호화를 위한 금전을 요구했다 [2].

4. 콜로니얼 파이프라인 랜섬웨어 분석

콜로니얼 파이프라인은 미국 동부 연료 공급의 절반을 담당하는 주요 국가 산업 시설로 2021 년 해킹 조직 Darkside가 유포한 랜섬웨어에 감염되어 5,500 마일이 넘는 연료 파이프라인의 작동 정지, 동부 해안 연료의 45% 공급 차질, 가스 공급 가격 3$ 상승 등 막대한 피해를 받았다. 결국 콜로니얼 파이프라인은 공격자가 제시하는 500 만 달러 상당의 거액을 지불하고 복구키를 받아 시설을 복구 했다.

4.1 침투 및 공격 과정



(그림 2) 콜로니얼 파이프라인 랜섬웨어 침투, 공격과정

우선, 시설 내 VPN 계정의 비밀번호가 외부로 유출되었다. 외부로 유출된 경위는 알려지지 않았지만, 비밀번호는 다크 웹으로 유출되어 공격자의 손에 들어가게 된다. 이후 공격자는 유출된 비밀번호를 통해 VPN 에 접속, 시설에 침투하여 랜섬웨어를 설치하였다. 설치된 랜섬웨어는 콜로니얼 파이프라인의 모든 데이터를 암호화하여 시설을 중지시켰다 [3].

5. 대응방안

우선, 악성코드 유입 방지를 위한 비인가 이동식 저장 장치 연결과 망 혼용 방지를 위한 제도가 마련되어야 한다. 중요 시스템에는 USB Port Blocker 같은 물리적 차단 장치 혹은 비인가 USB 연결을 제한하는 보안 소프트웨어를 설치하고, 외부 인터넷망과 망 혼용되지 않도록 완벽히 구분하여 바이러스가 유입되지 않도록 해야 한다.

두 번째는 지속적인 업데이트이다. 스턱스 넷이 활용한 취약점 중 CVE-2008-425(MS08-067)은 2008 년도에 이미 보안 업데이트가 완료된 취약점이었다. 하지만 업데이트를 미처 하지 못한 컴퓨터를 대상으로 공격이 가해졌다. 그렇기에 지속적이고 즉각적인 보안 업데이트를 통해 취약점을 없애야 한다.

세 번째는 보안 등급별 네트워크의 세분화다. 시설이 바이러스에 감염되더라도 주요 시스템은 시설 내부에 또 다른 독립 네트워크 안에 구축하여, 바이러스가 주요 시스템을 공격하지 못하도록 보안 등급별로 망 분리를 세분화하여야 한다. 예를 들어 PLC 와 같은 주요 장비들은 보안등급을 최고로 설정하고, 따로 독립 망에 구축하여 엄격히 관리하고 통제하여야 한다.

네 번째는 다중 인증(MFA)의 도입이다. VPN 의 특성상 한번 연결되면, 전체 네트워크에 대한 권한을 획득할 수 있기 때문에 비밀번호가 유출되면 보안에 취약하다. VPN 에 연결되더라도 공격자가 내부 시스템에 침입할 수 없도록 접근 권한에 대한 다중 인증 제도가 필요하다. 그 뿐만 아니라 중요시스템에 대한 접근 권한은 한 가지의 권한이 아닌 다중 권한 인증을 통해 접근 하도록 구성한다면 공격을 어렵게 만들 수 있다.

다섯 번째는 주기적인 데이터 백업이다. 랜섬웨어의 등장이후 금전을 목적으로 산업시설을 감염시키는 사례가 많아졌다. 랜섬웨어에 대응하기 위해서는 사전에 데이터를 백업하여, 감염되더라도 시설을 복구할 수 있도록 해야 한다.

마지막으로 가장 중요한 것은 인적 보안이다. 실수 혹은 고의적인 악성 USB 연결은 아무리 강력한 보안 시스템이라도 무용지물로 만들 수 있다. 따라서 인적 보안 강화를 위해선 산업시설 근무자들에게 비인가 USB 사용, 해킹 메일 열람 주의와 같은 지속적인 보안 교육이 필수적이다.

6. 결론

사이버 공격으로부터 100% 안전한 경우는 존재하지 않는다. 북한의 최근 공격 사례를 살펴보면, 앞의 사례보다 더 정교한 악성코드를 개발하여 공격할 가능성이 존재한다. 국가 안보를 위해 우리 스스로 산업시설 보안에 대한 오판을 하는 것은 아닌지, 관련 보안 제도에 허점은 없는지 계속해서 점검하고 대응 방안을 모색해야 한다.

참고문헌

[1]Stamatis Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security", IECON 2011-37th, Annual Conference of the IEEE Industrial Electronics

[2]Ben Hunter and Fred Gutierrez, "EKANS Ransomware: A Malware Targeting OT ICS Systems",Fortiguard,2020.

[3]Jack Beerman, David Berent, Azch Falter, Suman Bhunia,"A Review of Colonial Pipeline Ransomware Attack", 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops