제조 설비 PC 의 효과적인 보안위협 대응 방안 연구

김병주
e-mail : supremekb@gmail.com
고려대학교 정보통신대학원

A Study on Effective security threats Defense of Industrial Equipment PC

Byungju Kim
*Dept. of Computer Science, Korea University

요 약

반도체, 디스플레이 등 제조 분야는 환경적인 요소로 인해 고도화된 보안 위협으로부터 적절한 대응을 하지 못하고 있다. 본 논문은 제조 분야에서 사용되는 제조 설비 PC 가 보안 위협에 대해 대응이 어려운 환경적인 요소를 알아보고, Endpoint Level 에서 효과적으로 보안 위협을 대응 할 수 있는 방안에 대해 설명한다.

1. 서론

반도체, 디스플레이 등 제조업 분야에서 사용되는 제조 설비 PC 는 제조 분야의 환경적인 특성으로 인해 고도화된 보안 위협으로부터 노출되어 있다. 제조 분야는 신규 제조 라인 및 제조 설비 PC 교체에는 막대한 금액과 Risk 가 따르게 되며, 이로 인해 노후화된 구형장비를 많이 보유 및 사용하고 있으며, 이 설비들의 운영체제 또한 EOS (End Of Service)되어 취약점 등에 노출되어 있는 상황이다.

제조 산업 분야는 웜(worm), 바이러스 등 다양한 악성코드들로 인한 피해를 비롯하여 최근에는 스턱스넷(Sutxnet)과 같은 APT 공격으로 인한 침해사고가 발생되고 있으며, 제조 라인의 피해로 인한 막대한 금전적인 손실이 발생되고 있다.

2014 년 4 월 8 일 제조업에서 많이 사용되고 있는 Windows XP 에 대한 마이크로소프트의 지원이 종료됨에 따라 OS 취약점을 이용한 피해는 더욱 증가할 것으로 예상된다.

이 논문에서는 제약사항이 많은 제조업 분야 환경의 제조 설비 PC 에 대해 보안 위협을 효과적으로 대응 하는 방법에 대해 설명한다.

2. 제조 생산 시스템의 요구사항

제조업 분야는 제조 라인을 운영하는데 있어 아래와 같은 요구사항을 필요로 한다.

1) 중단 없는 가동

제조 라인을 구성하는 제조 설비 PC 가 계획된 중단 외 이외에 장애로 인한 중단 없이 24 시간 365 일 가동되어 제품을 생산해야 한다.

2) 응용프로그램 사용 제한

제조 설비 PC 는 제품을 생산하는데 필요한 셟비 프로그램에 이외에 다른 응용프로그램은 동작하면 안된다.

3) 제한된 시스템 자원

노후화된 설비 PC 들을 다량 보유 하고 있어, 저사양 PC 들에서 제품을 생산할 때 부하가 없어야 한다.

또한 해당 장비들은 Windows NT , Windows 2000 등 마이크로소프트에서 서비스가 중지된 운영체제를 사용하고 있다.

4) 폐쇄망 환경

폐쇄망 환경에서 운영되어 같은 망의 설비 및 서버 이외에 외부와 통신을 제한한다.

2.1 제조 환경의 보안적 위협 요소

위에서 나열된 제조 생산 시스템의 요구사항으로 인해 적절한 보안 조치를 할 수 없어 제조 설비 PC 는 보안 위협에 노출 되어 있다.

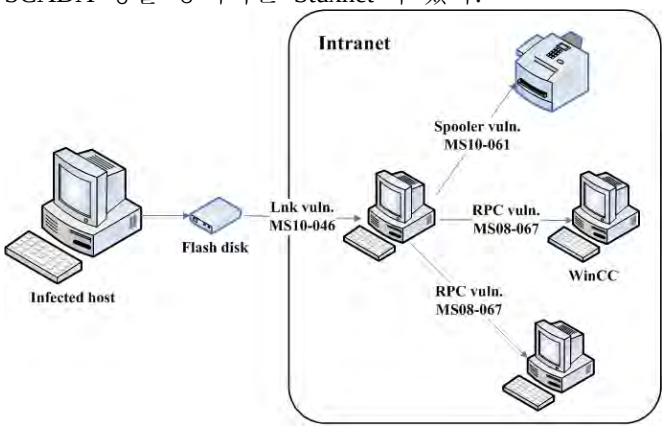
제조 생산 시스템 요구사항으로 인한 보안 취약한 부분은 다음과 같다.

2.1.1 중단 없는 가동 및 폐쇄망 환경

제조 설비 PC 는 중단 없는 가동으로 인해 악성코드 감염 시 즉각적인 대처가 어렵다. 악성코드를 대응하기 위해서는 설비 PM(Planned Maintenance)을 계획해야 하고, 그 기간 동안은 보안 위협에 노출되어 있다. 또한 폐쇄망 환경으로 인해 외부 인터넷과 접속이 되지 않아 윈도우 보안 업데이트 등 보안 패치에 제약사항이 있으며, PMS(Patch Management System)을 통해 패치를 진행하게 될 경우 패치의 특성상 재부팅이 필요하거나, 패치 오류로 인한 롤백 발생 시 중단 없는 가동을 보장 할 수 없어 보안의 취약하다.

이로 인해 제조업 분야는 알려진 보안 취약점으로 통한 악성코드의 공격으로 인해 지속적으로 피해가 발생하고 있으며, 가장 대표적인 예로 MS08-067 취약

점을 이용하여 다량의 네트워크 트래픽 생성을 통해 네트워크 장애를 발생시키는 Conficker.worm 과 프린트스풀러 취약점인 MS10-061 취약점을 이용하여 SCADA 망을 공격하는 Stuxnet 이 있다.



<그림 1> Stuxnet 사용 취약점 및 공격방법

2.1.2 제한된 시스템 자원

노후화된 제조 설비 PC 는 아래 표와 같이 EOS(End of Service)된 운영체제를 많이 사용하고 있다.

제조 설비 PC 는 최근 EOS 된 운영체제인 Windows XP 가 가장 많은 부분을 점유 하고 있으며, 2014 년 4 월 이후로 보안 패치가 제공 되지 않고 있다.

또한 Windows NT 와 Windows 2000 등의 운영체제가 현재까지 사용되고 있으며, 현재 백신업체에서 제공되고 있는 최신 버전의 백신은 Windows NT 와 Windows 2000 운영체제에 대해서는 지원을 하지 않아 보안에 취약하다.

순위	OS 버전	점유량(%)
1	Windows XP	42.0 %
2	Windows 2000	29.0 %
3	Windows Server 2003	25.0 %
4	Windows 7	2.1 %
5	Windows NT 4.0	1.7 %
6	Windows Server 2008 R2	0.2 %

<표 1> A 사 생산설비 OS 설치 현황

3. 기존 제조 환경의 Endpoint 보안 한계점

기존 제조 환경의 블랙리스트 방식을 이용한 Endpoint 보안 백신을 통해 위협을 대응 하고 있다.

기존 보안 백신 제품은 제조 환경에 있어 4 가지 한계점이 있다.

3.1 블랙리스트 방식의 탐지 기법

블랙리스트 방식은 시그니처 기반 탐지 기법으로써 알려지지 않은 악성코드에 대한 유입을 차단이 불가능하다. 따라서 폐쇄망환경을 사용하는 제조 환경에서 엔진 업데이트가 정상적으로 되지 않은 PC 은 알려지지 않은 위협에 대해 노출되게 된다.

3.2 악성코드 분석 및 시그니쳐 업데이트

알려지지 않은 악성코드 샘플을 확보하게 되면 해당 샘플을 분석하여 엔진에 반영한 뒤 백신에 전달하는데 까지 많은 시간이 소요되며, 그 기간 동안 해당 악성코드에 대응이 어렵다. 이로 인해 Zeroday Attack 이나 APT 와 같은 공격에 취약하다.

3.3 과도한 시스템 자원 소모

블랙리스트 보안 제품은 지속적인 시그니쳐 업데이트로 인해 Endpoint 에 엔진사이즈가 지속적으로 증가 하며, 악성코드 검사 및 엔진 업데이트 시 높은 리소스를 사용하게 된다.

현재 제조 시스템은 노후화된 설비가 많이 존재하고 있어, 지속적인 엔진사이즈 증가로 인한 HDD 공간 부족 현상, 높은 리소스 사용 등 AV Strom 이 발생되어 설비 과부화 등 생산에 영향을 주고 있다.

3.4 취약점 패치의 즉각 적용 불가

가용성이 우선인 제조 시스템은 OS 및 소프트웨어 취약점 발생 시 설비 프로그램과의 충돌 이슈로 인하여 즉각 적용을 하지 못한다.

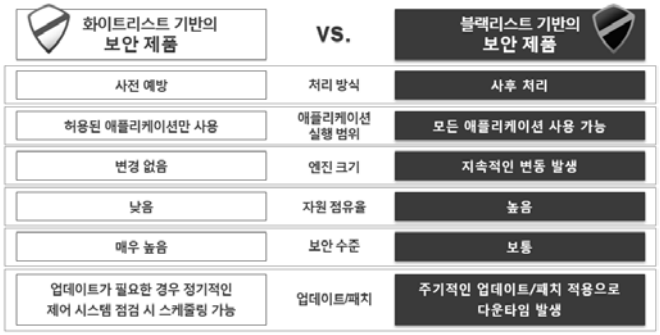
또한 Windows NT, Window 2000, Window XP 와 같이 EOS(End of Service)된 OS 의 경우 취약점 패치가 제공되지 않아 Zeroday Attack 등 취약점을 노리는 보안 위협에 대응 할 수 없다.

4. 효과적인 EndPoint 보안 위협 대응 방안

아래 화이트리스트 기반의 EndPoint 방법을 비롯하여 여러가지 보안기법을 통해 기존 블랙리스트 기반의 보안 한계점을 극복하고, 효과적으로 제조 생산 시스템에서 요구사항을 충족하는 보안 대응을 할 수 있다.

4.1 화이트리스트 기반의 Endpoint 보안 기법

화이트리스트 기반의 EndPoint 보안 기법이란 PC 내부에 있는 파일들에 대해 검증을 통해 화이트리스트를 생성하고 화이트리스트 내부에 파일이 수정, 삭제 되거나 화이트리스트 외에 파일이 유입, 생성되는 것을 차단하게 된다. 즉 블랙리스트 기반의 EndPoint 보안 기법과 다르게 보안 위협에 대해 사전 예방을 한다.



<그림 2> 화이트리스트기반과 블랙리스트기반의 차이점

화이트리스트를 생성하는 방법에는 크게 세가지로 나눌 수 있다.

4.1.1 파일 고유값 기준 화이트리스트 적용

PE 파일의 고유 CRC 값을 수집하여 블랙리스트 엔진과 비교하여 화이트리스트를 생성한다.

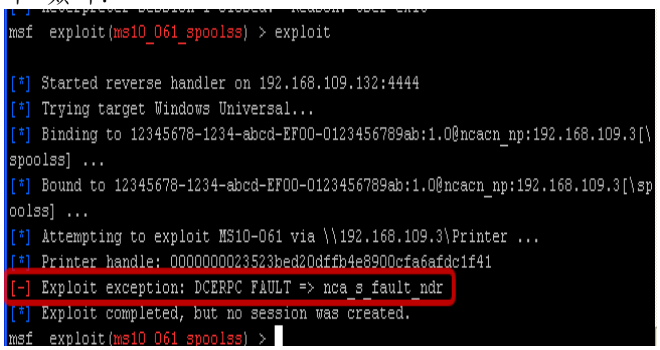
4.1.2 표준시스템 선정 화이트리스트 적용

관리자가 표준시스템을 선정하여 직접 화이트리스트를 생성하여 후 전체 적용 시킨다.

4.1.3 디지털 인증서 기반의 화이트 리스트 적용

소프트웨어 제조사들의 디지털 인증서 기반으로 인증서가 발급된 파일들에 대해 화이트 리스트를 생성한다.

위와 같은 3 가지 방법으로 생성된 화이트리스트들은 알려지지 않은 zero-day attack 이나 APT 등의 공격을 효과적으로 대응 할 수 있으며, AV Strom 등 노후화 된 설비 운용에 문제점을 효과적으로 해결 할 수 있다.



<그림 3> 화이트리스트생성 후 Stuxnet 공격 차단

Endpoint 에 화이트리스트 적용 시 PC 내부에 있는 파일들을 보고하고 외부에서 알려진 윈도우 취약점으로 공격 및 파일 생성이 어렵기 때문에 Exploit Tool 을 이용하여 Stuxnet 이나 Conficker.worm 공격 시 공격이 차단되는 것을 확인 할 수 있다.

4.2 화이트리스트 기반의 network 제어기법

제조 설비 PC 는 CIM PC 와 서브 PC 간의 통신, CIM PC 와 CIM PC 간의 통신 CIM PC 와 내부망 서버 간의 통신 이외에는 외부와 통신을 해서는 안된다.

따라서 사용되는 IP, PORT 이외에 통신이 되지 않도록 EndPoint 에서 방화벽 기능을 통해 차단하여야 한다.

4.3 매체제어 기법

제조 설비 PC 에서 악성코드가 감염되는 가장 큰 이유는 USB 를 통한 악성코드 감염이다. 외부 업체에서 유지보수를 위해 악성코드가 감염된 USB 에 저장되어 있는 파일을 설비 PC 로 이동시켜 악성코드가 감염되는 것이다. 따라서 외부에서 사용되는 USB 가 인식되지 못하도록 보안 USB 나 매체제어를 이용하여 허용된 USB 만 사용되도록 대응이 필요하며, 허용된 USB 도 주기적으로 악성코드 검사를 하여 깨끗한 상태를 유지할 수 있는 내부 정책이 필요하다.

4.4 중요 프로세스 보호 기법

화이트리스트 기법에 추가적인 보안을 위하여 프로세스 보호 기법을 제안한다.

중요 프로세스 보호 기법은 커널에 프로세스 보호 드라이버를 로드 시킨 뒤 설비 PC 에서 사용되는 프로세스가 포함된 파일, 디렉토리, 레지스트리를 담당자가 미리 등록한 정보와 연동시켜 보호함으로써 파일을 무결성을 보장하고, 다른 프로세스로부터 프로세스가 강제로 종료되는 것을 방지 할 수 있어

5. 결론

기존의 최신 기술을 탑재한 EndPoint 보안 제품은 노후화된 제조 환경에서 동작이 불가하거나, 과도한 리소스 사용으로 인해 제조 설비 PC 에서 효과적인 보안 위협을 하는데 한계가 있었다.

본 논문에서 제안하고 있는 화이트리스트 방식을 이용하여 블랙리스트 방식의 보안 제품에서 발생되는 AV Strom 등을 해결하고, 서비스가 중단된 운영체제에서 취약점을 이용한 보안 위협을 대응하고, 중요 프로세스 보호기법을 이용하여 설비 PC 에서 사용되는 프로세스들이 중단 없이 동작될 수 있도록 보호 및 외부 유출을 방지하여 기존의 EndPoint 보안 방식보다 더 효과적으로 보안 위협에 대응할 수 있다.

IoT 가 발전함에 따라 스마트 팩토리 산업이 발전하게 될 경우 외부에서 보안 위협은 더 많아 질 것이다. 향후에는 IoT 가 적용된 제조 환경에서 노후화된 제조 설비 PC 들을 효과적으로 보호 할 수 있는 연구가 필요하다.

참고문헌

<국내문헌>

[1] 허재준, 이상철, “스턱스넷(Stunxet)의 감염 경로와 대응방안”, 정보보호학회지 제 21 권 제 7 호, 2011.11, 23-29

[2] 박세균, “Endpoint Level 의 효과적인 APT 공격 대응방안 연구”, 한국정보과학회 2013 한국컴퓨터종합학술대회 논문집, 2013.6, 732-734

[3] 최재우, “화이트리스트 기법을 이용한 효과적인 보안강화 방안 연구”,석사학위 논문, 동국대학교 국제정보대학원, 2014.8

[4] 이동휘, 최경호, “제어망에서 화이트 리스트 기법을 이용한 이상 징후 탐지에 관한 연구”, 정보·보안논문지 제 12 권 제 4 호 (2012 년 9 월) pp.77-84

[5] 유형욱, 윤정환, 손태식 “제어시스템 보안을 위한 whitelist 기반 이상징후 탐지 기법”, 한국통신학회논문지 제 38 권 제 8 호(네트워크 및 서비스), 2013.8, 641-653

<해외문헌>

[1] Seungwon Shin, Guofei Gu, “Conficker and beyond : a large-scale empirical study”, Proceedings of the 26th Annual Computer Security Applications Conference