OT 환경 랜섬웨어 감염 사례가 주는 교훈

ASEC(AhnLab SEcurity intelligence Center)은 최근 OT(Operation Technology) 환경에서 발생한 랜섬웨어 감염 사례를 확인했다. OT 환경은 기반 시설, 제조업 등 운영 기술에 중점을 둔 분야로 설비 및 장비들의 유형에 따라 네트워크를 구분하고 단절된 폐쇄망 환경으로 운영한다. 과거에는 OT 환경이 특유의 폐쇄성으로 인해 안전하다고 여겨졌지만, 최근 IT 환경 및 외부 연결이 확대되면서 침해 사례들도 늘어나고 있다. 이번 랜섬웨어 감염 사례 역시 폐쇄되어 있는 OT 환경이 IT망과 연결되면서 시작되었다.

이번 글에서는 본 사례의 랜섬웨어 감염 경로와 시사점을 살펴본다.

기존 OT 환경에서 발생한 침해 사례들은 대부분 내부 폐쇄망 침입을 위해 외부망에서부터 내부 폐쇄망까지 치밀하게 준비된 APT 공격으로 인한 것이었다. 하지만 이번 사례는 논리적 망 분리로 운영된 OT 환경에서 생산 설비 점검을 위해 직접 인터넷에 연결하면서 문제가 발생했다.

공격자가 OT 환경을 직접 노린 APT 공격은 아니었지만, 부적절한 네트워크 연결로 인해 외부 인터넷에 생산 설비 자산이 노출됐고, 결국 랜섬웨어에 감염되어 생산 라인이 멈추는 피해가 발생했다. 생산 설비로는 동일 제조사의 장비가 다수 있었으며, 제조사의 초기 패스워드가 그대로 사용되어 더 큰 피해로 이어졌다.

이번 랜섬웨어 감염 사례의 주요 내용을 요약하면 [표 1]과 같다.

구분	내용
주요 공격 내용	• 랜섬웨어 감염
피해 현황	• 랜섬웨어 감염으로 인한 생산 설비 장애 발생
피해 환경	• Windows 10
사건 TAG	#Phobos #ransomware #lateralmovement #RDP #windowsdefender #netpass #dcontrol #OT

[표 1] 본 침해 사례 주요 내용 요약

OT 환경 이해하기

(1) IT와 OT 환경의 차이

본격적으로 사례를 분석하기에 앞서, OT가 무엇인지 또 환경은 어떻게 구성되어 있는지 살펴보자.

OT(Operation Technology) 환경은 산업의 운영기술 환경으로, 일반적으로 산업제어시스템(ICS: Industrial Control System)이 포함된다. 최근에는 IT와 연결되거나 함께 사용되는 영역까지 범위가 확장되고 있다.

IT(Information Technology)는 데이터의 처리 및 전송을 주 목적으로 '정보'를 중점으로 하는 기술이다. 물리 장치를 모니터링하고 제어하는 '운영'을 중점으로 하는 OT(Operation Technology)와 다소 차이가 있다.

IT 기술과 OT 기술의 차이처럼 IT 보안과 OT 보안 역시 차이점이 있다. 정보 보안의 3요소로 불리는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에서도 IT는 기밀성, 무결성, 가용성의 순서대로 중요도를 평가한다. OT 보안에서는 IT 보안과 다르게 가용성, 무결성, 기밀성의 순서대로 중요도를 평가한다.

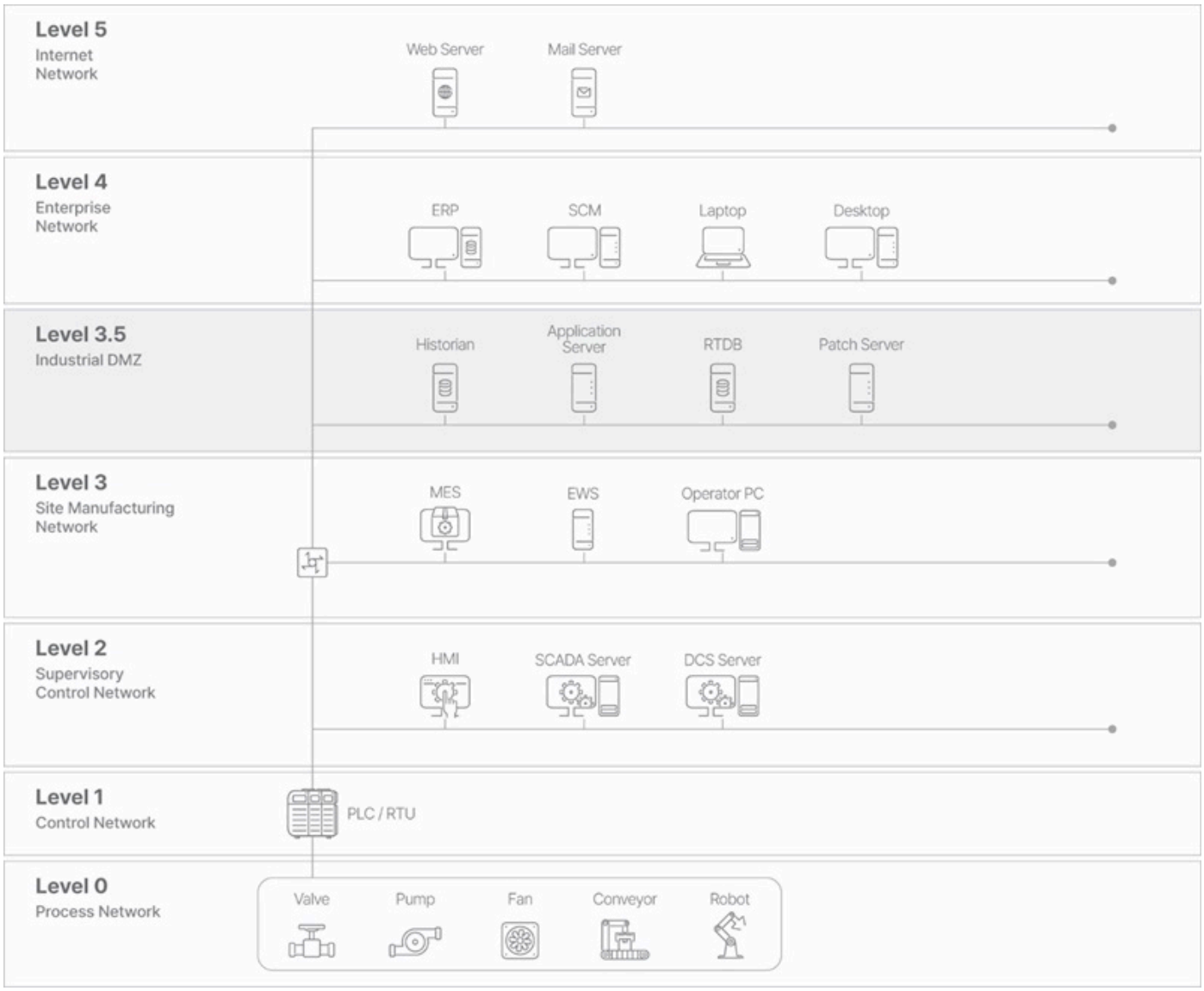
예를 들어, IT 환경에서는 자산(PC, 노트북, 모바일, 서버 등)에 문제가 발생했을 때 문제 해결을 위해 재부팅, 자산 교체 조치가 가능하다. 하지만, OT 환경에서는 자산의 재부팅, 교체 등의 조치는 생산 설비의 중단으로 이어지기 때문에 기밀성 보다 가용성과 무결성을 더 높게 평가하고 있다.

IT 보안의 보안 요소 우선순위	OT 보안의 보안 요소 우선순위
1. 기밀성(Confidentiality)	1. 가용성(Availability)
2. 무결성(Integrity)	2. 무결성(Integrity)
3. 가용성(Availability)	3. 기밀성(Confidentiality)

[표 2] 보안의 3요소로 보는 IT 보안과 OT 보안 우선순위

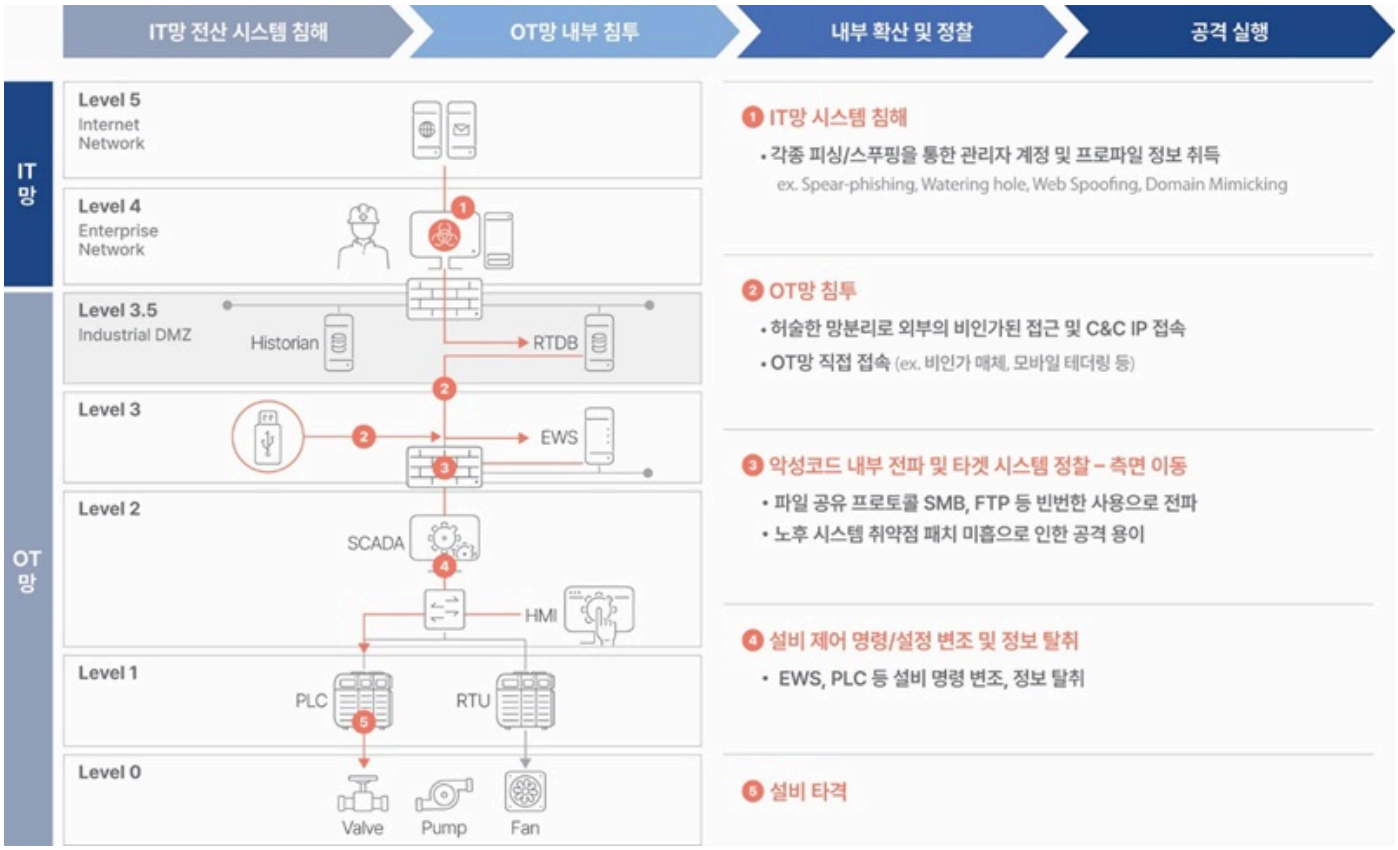
(2) OT 보안 구성

일반적으로 OT 보안을 설명할 때 '퍼듀 모델(Purdue Model)'을 이용해 네트워크 보안 계층을 구분한다. 퍼듀 모델은 네트워크 환경을 Level 0부터 Level 5까지 총 7개 계층으로 나눈다. 7개의 계층에는 IT 환경인 Level 4/5와 OT 환경을 의미하는 Level 0 ~ Level 3의 폐쇄망 환경이 있다. OT 환경에 대해서도 제어망(Level 0 ~ Level 2)과 운영망(Level 3 ~ Level 3.5)으로 구분해서 보기도 한다. Level 3.5는 IT망과 OT망이 맞닿는 영역으로 'Industrial DMZ'라 부른다.



[그림 1] 퍼듀 모델(Purdue Model)

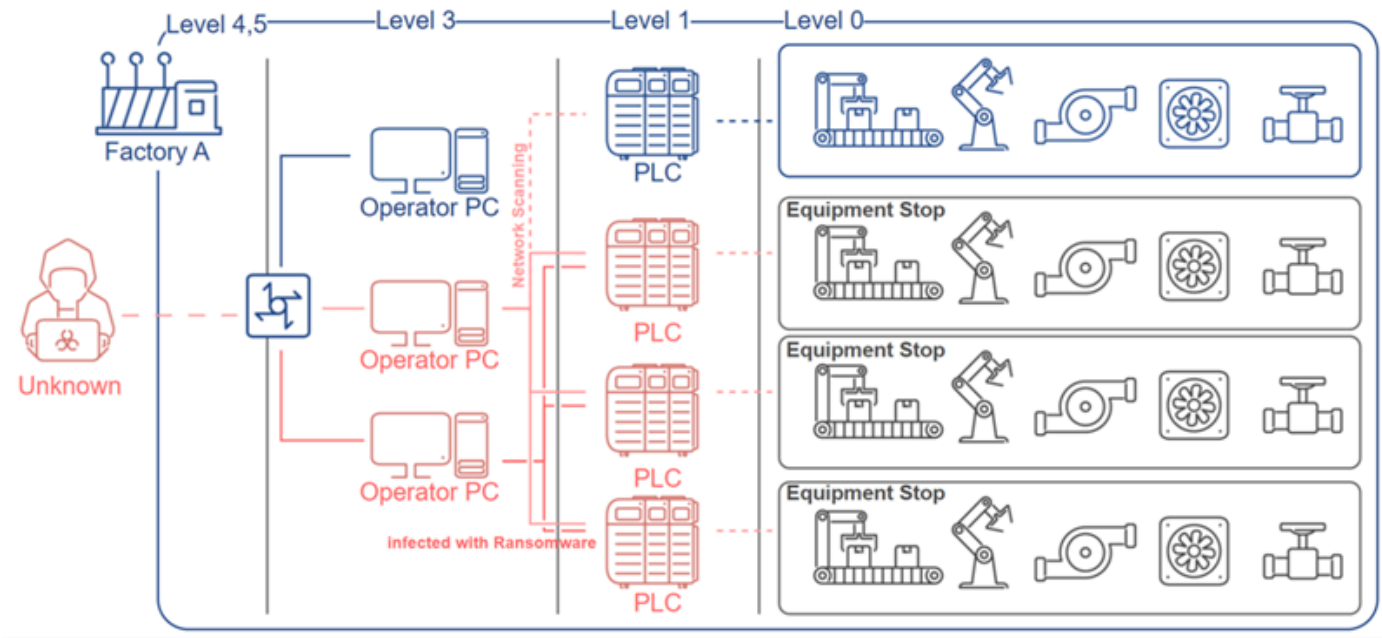
하지만 실제 생산 설비 장비들이 동작 중인 현장에서는 퍼듀 모델과 같은 형태로 네트워크가 체계적으로 구분되지 않거나, 네트워크는 구분했으나 취약한 관리로 인해 침해가 발생하는 경우들이 있다.



[그림 2] OT 환경 침해 흐름 예시

OT 환경에서 발생하는 침해 사고들은 Level 4(Enterprise Network), Level 5(Internet Network)의 IT망으로부터 시작되는 경우가 많다. IT망이 침해되면 내부 네트워크 구조가 노출되고, 공격자가 폐쇄된 OT망으로 침입할 수 있는 빌미를 제공한다. OT망 침해는 보통 잘못 관리된 접근 제어 정책, 네트워크 세그멘테이션(network segmentation) 부족 등으로 인해 IT망에서부터 시작된다. 또한, 감염된 저장매체 사용 혹은 모바일 테더링을 통해 OT 환경을 직접 노리는 경우도 있다. OT망이 침해되면, 노후화되고 취약한 시스템들이 내부로 유입된 악성코드에 감염되면서 피해가 급속도로 확산될 수 있다.

피해 시스템의 OT 환경 구성



[그림 3] 침해 흐름도

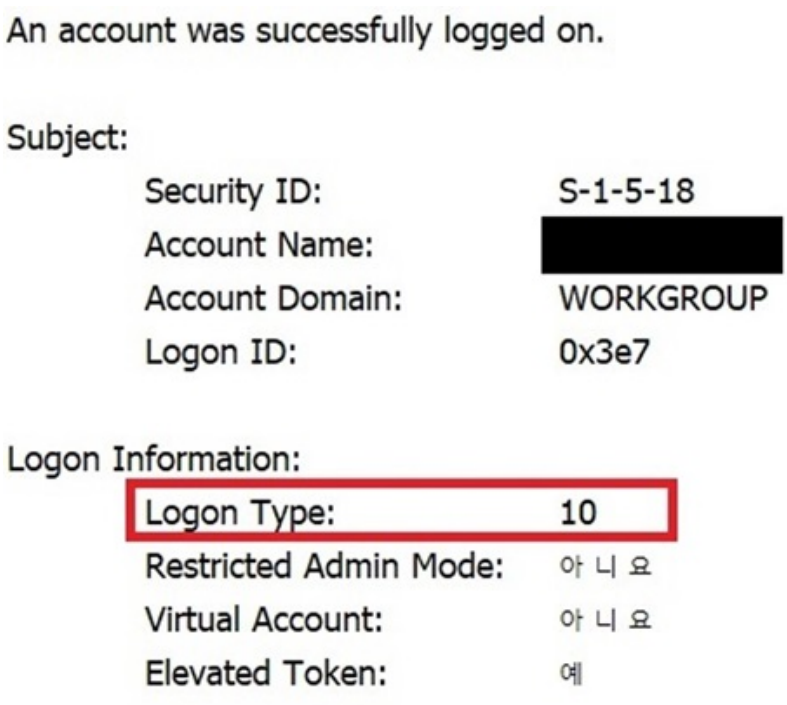
(1) 인터넷 환경에 연결된 폐쇄망

이번 침해 사례는 OT 환경 내 생산 설비를 통제하는 시스템을 점검하는 과정에서 랜섬웨어 감염이 발생했다. 시스템 점검 중 외부 인터넷과 연결했고, 이로 인해 OT 환경의 자산들이 인터넷 환경에 노출되어 랜섬웨어 감염 피해로 이어졌다.

OT 환경은 폐쇄망으로 구성됐으나, 논리적 망분리로 구성되어 운영 시스템 점검을 위한 인터넷 연결이 가능했다. 관리자는 침해 시점에 논리적 망분리가 적용된 라우터에 외부 인터넷과 연결 가능한 네트워크 대역을 설정했다. 이후, 인터넷이 가능한 네트워크 대역을 내부 운영 시스템들에 순차적으로 할당해가면서 점검을 진행했다.

점검을 진행하는 동안 운영 시스템들은 외부 인터넷에 노출됐으며, 이 중 보안 업데이트가 누락되는 등 취약한 상태로 관리된 시스템들이 있었다.

(2) 관리자 계정 로그온



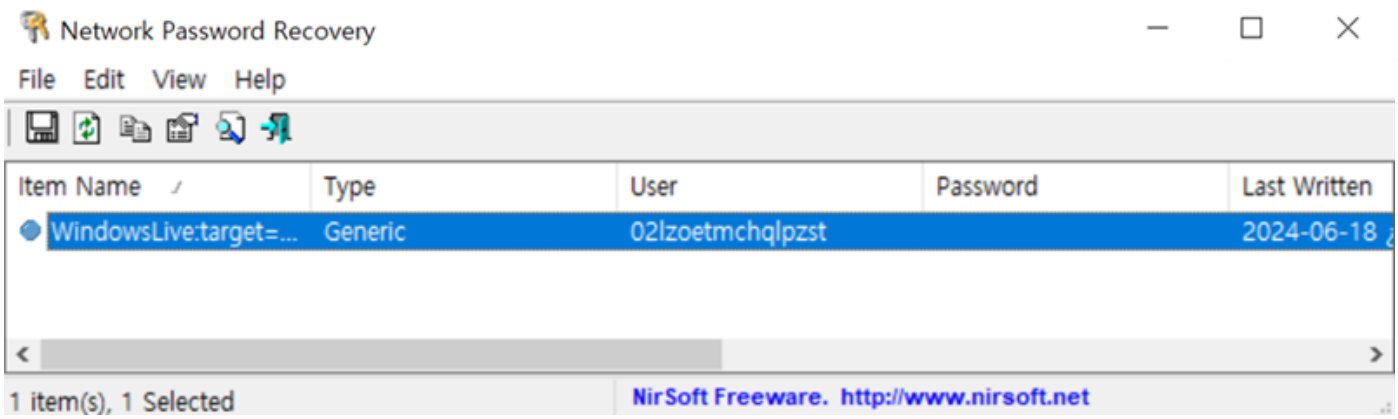
[그림 4] 관리자 계정으로 로그온한 이벤트 로그

외부에 노출된 운영 시스템들은 관리자 계정(Administrator) 로그온 공격 시도를 받았다. 이 중 취약한 패스워드로 관리된 운영 시스템이 침해당했다. 침해된 시스템은 이후 내부 네트워크 대역으로 스캔 공격이 수행됐다.

(3) 내부 이동(Lateral Movement)

공격자는 운영 PC를 침해한 후, PLC 시스템으로 내부 이동(lateral movement)을 수행했다.

네트워크 스캔 과정에서 윈도우 OS 기반 PLC(Programmable Logic Controller) 시스템들이 공격자에게 노출됐다. PLC 시스템은 시스템 명이 제품 명으로 설정되어 있어 공격자가 어떤 시스템인지 유추할 수 있었다. 또한, 패스워드가 제조사의 초기 패스워드로 설정되어 있어 로그온 공격에도 보안이 취약했다. 피해 조직은 같은 제조사의 동일 제품 다수를 동일한 패스워드로 관리하고 있었으며, 이로 인해 피해 규모가 커졌다.

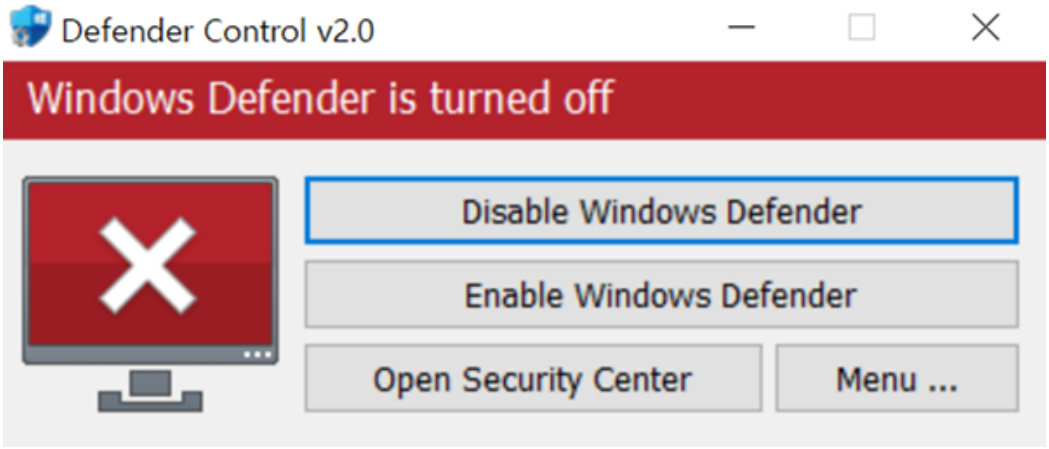


[그림 5] netpass 이미지

이 과정에서, 관리자 계정 로그온 스캔 공격의 흔적은 확인되지 않았다. 공격자가 피해 시스템의 계정 정보를 알고 있었던 것으로 보인다. 계정 정보를 수집한 경로는 확인되지 않았으나, 공격자가 외부에서 계정 정보를 수집했거나 내부 이동을 위한 정보 수집 단계에서 PLC 시스템들의 계정 정보를 수집한 것으로 보인다.

(4) 탐지 우회

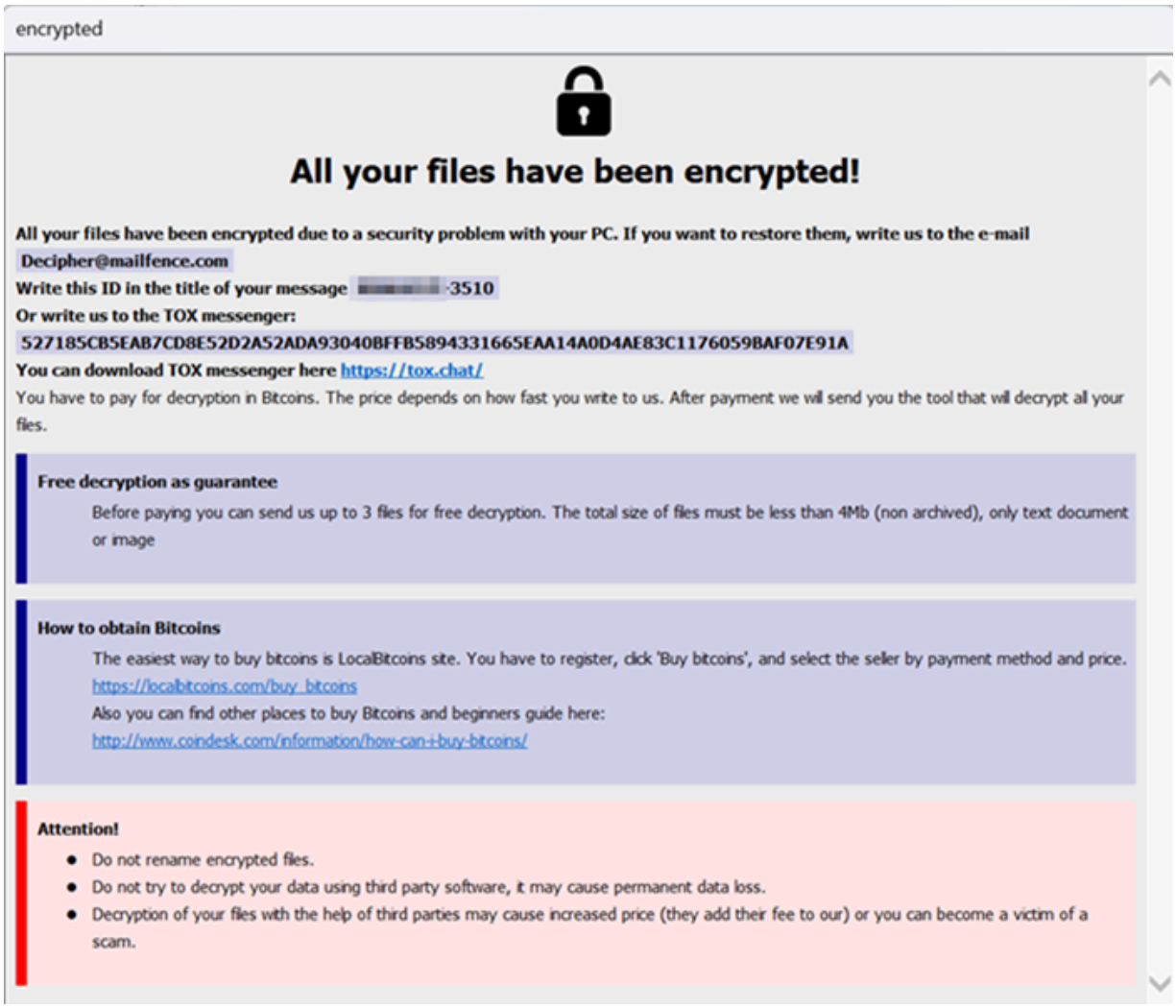
PLC 시스템에는 별도 백신 프로그램이 설치되지 않았으나, Windows Defender가 동작 중이었다. 공격자는 Windows Defender 무력화 도구를 이용해 백신 프로그램으로 인한 랜섬웨어 악성 파일 탐지를 우회했다.



[그림 6] 윈도우 디펜더 무력화

(5) 랜섬웨어 감염

Windows Defender를 무력화한 공격자는 운영 PC 및 PLC 시스템들에 랜섬웨어를 유포했다.



[그림 7] 포보스(Phobos) 계열 랜섬웨어의 랜섬노트

피해 시스템에서 확인된 랜섬노트는 포보스(Phobos) 계열 랜섬웨어의 랜섬노트와 동일하다. 랜섬웨어에 감염된 파일 확장자의 형식 또한 포보스 계열 랜섬웨어와 같다. 즉, 피해 조직은 포보스 계열 랜섬웨어에 감염된 것으로 확인했다.

시사점

가용성이 중시되는 OT 환경에서는 IT 환경과 동일한 수준의 보안을 적용하기 어렵지만, OT 환경의 구조와 IT-OT 연결성을 이해하고 이에 부합하는 보안 태세를 갖춰야 한다. 이 관점에서 본 침해 사례를 통해 얻을 수 있는 시사점은 [표 3]과 같다.

문제점	대응 방안
• 폐쇄망 환경에 인터넷 연결로 내부 시스템 인터넷 노출	• 예외 상황(시스템 점검)이 증가할수록, 폐쇄망 환경에 대한 공격 표면 증가 – 체계적 관리 필요 • 폐쇄망 인터넷 연결 제한 혹은 인터넷 연결 없이 점검을 진행할 수 있는 방안 고려
• 폐쇄망 내 자산이 취약한 상태 (보안 업데이트 및 보안 프로그램 설치 누락)로 관리	• (가용성을 보장하는 선에서) 보안 프로그램 운영 • 최신 보안 업데이트 적용

• 제품 명으로 등록된 시스템 명과 초기 패스워드 사용으로 인한 침해 발생	• 시스템 유추가 어렵도록 시스템 명 변경 • 제품의 초기 패스워드는 반드시 변경 후 사용

본 침해 사례 관련 침해지표(IOC) 등 보다 자세한 내용을 담은 보고서 원문은 AhnLab TIP 구독 서비스를 통해 확인할 수 있다.

안랩

A-FIRST팀 이권왕 선임연구원