무선백도어 해킹 탐지 시스템

Alpha-H

www.gitsn.com / sales@gitsn.com / 02.852.3560

해킹의 침투 경로

유선 네트워크

패킷 스니핑, DDoS, SQL 인젝션, 크로스 사이트 스크립팅 등

Wi-Fi 등 무선 네트워크

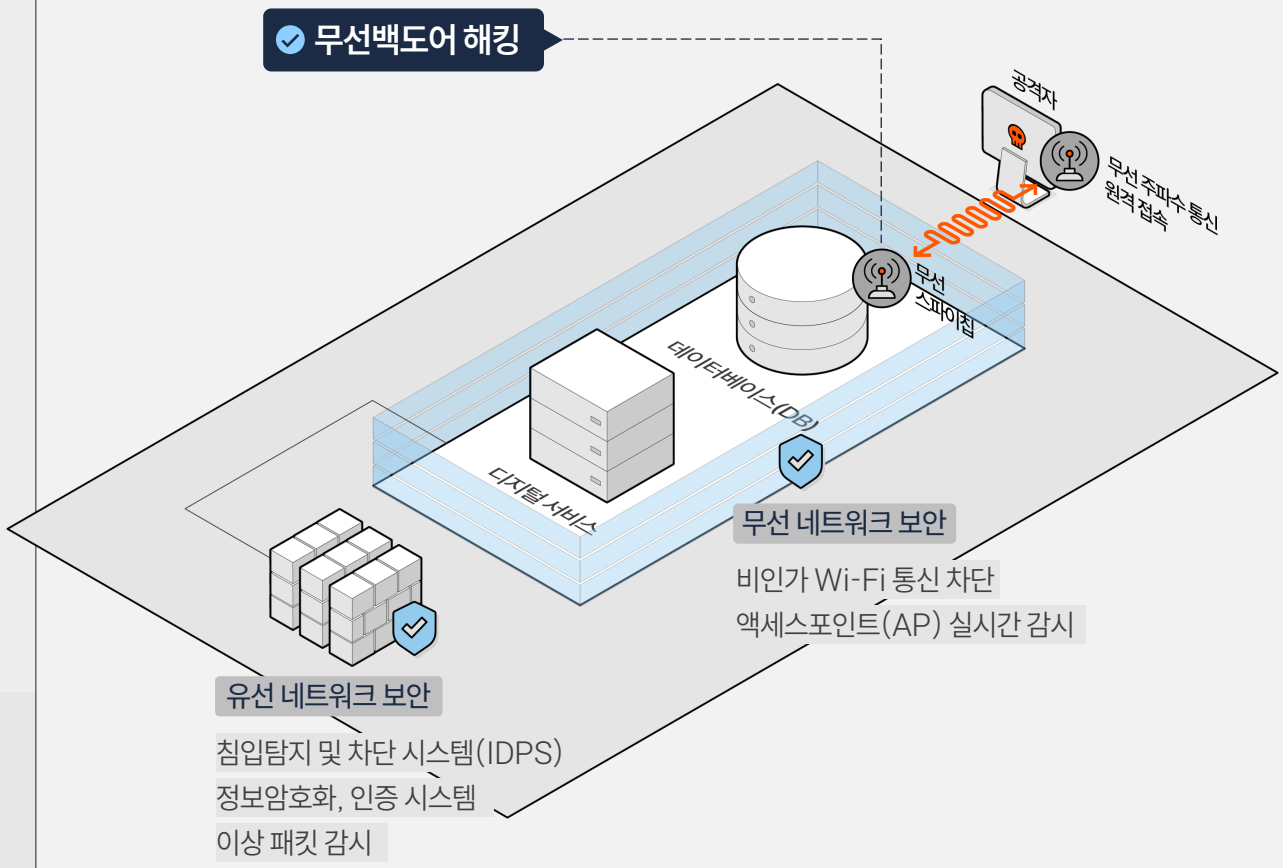
무선 패킷 스니핑, Wi-Fi DoS, 워드라이빙, 불량 액세스 포인트,
무선랜 클라이언트 공격, 무선 네트워크 암호화 해킹 등

무선백도어 (무선 주파수 통신*)

무선 스파이칩*을 IT장치(USB, 키보드)속에 은닉하거나,
공급망 과정 중 탑재하여 이를 거점으로 원격 접속 후 공격

*무선 주파수 통신 : 전파를 사용해 정보를 무선으로 주고받는 방식
무선 스파이칩 : 무선 주파수 송·수신 기능을 갖는 초소형 칩

무선 백도어 해킹 사례
- NSA, 전세계 10만여대 이상의 PC에 무선백도어 해킹 시도(2014)
- 한국군 현역 대위가 무선백도어를 이용하여 북한 해커에게
한국군 합동지휘통제체계(KJCCS) 서버 데이터 탈취 시도(2022)



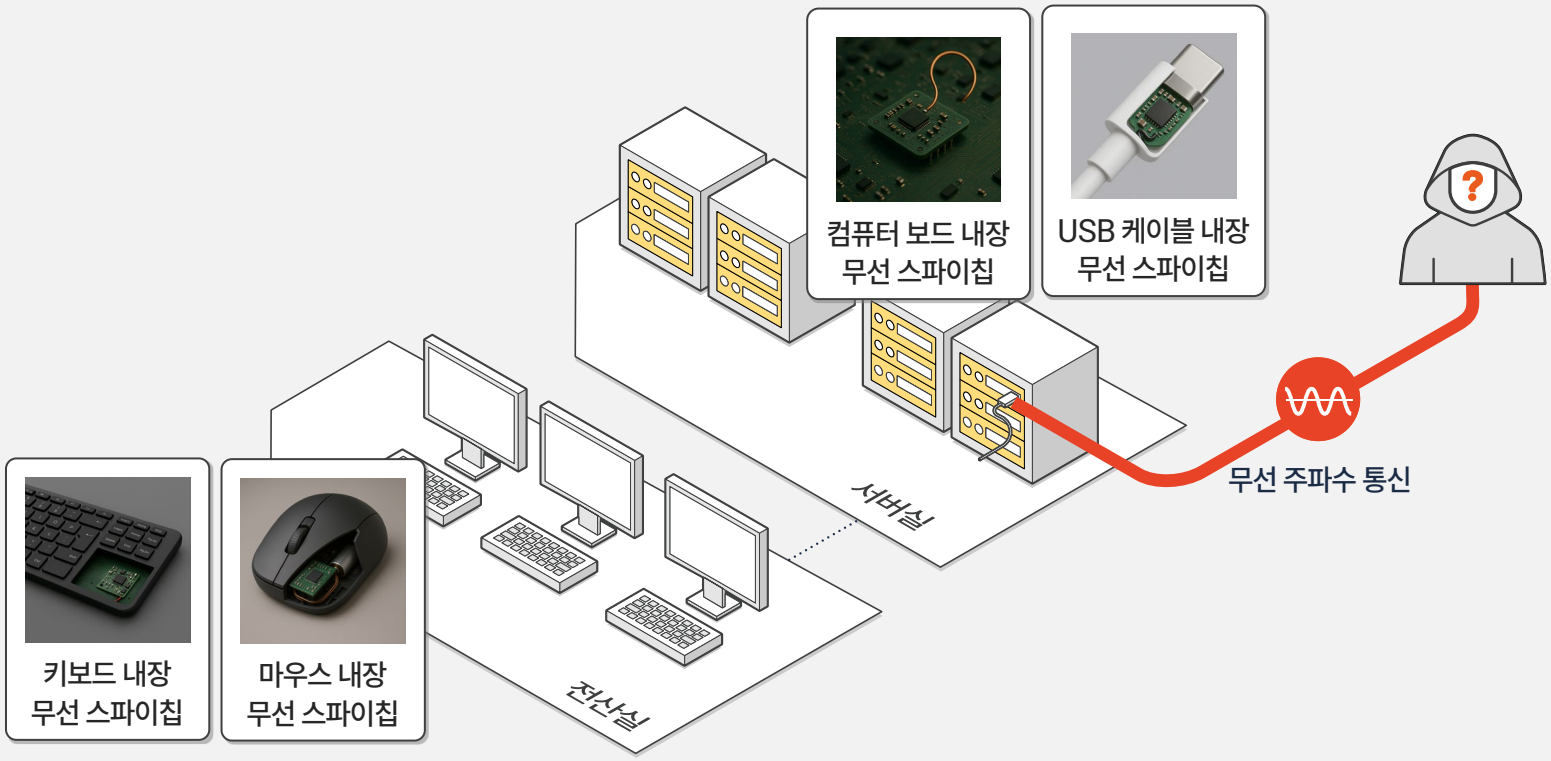
무선백도어 해킹 특징

① 무선 스파이칩을 IT장치(키보드 등 USB 장치) 속에 은닉 또는 공급망 과정 중 탑재하여 내부망으로 분리된 서버 등에 침투

② 무선 주파수 통신으로 타겟 시스템에 원격 접속(수 km밖에서 무단 침입)하여 데이터를 탈취하거나 시스템을 붕괴시키는 신종 해킹 방식

③ 망분리(업무용 내부망과 외부 인터넷망을 분리하여, 정보 유출 및 외부 사이버 공격을 방지하는 네트워크 보안 체계) 보안 무력화, WIPS(무선침입방지시스템) · 방화벽 등 보안체계 우회

④ 매우 높은 수준의 접속 권한 획득 - 고부가가치 데이터 탈취, 사이버 테러로 인한 혼란 우려

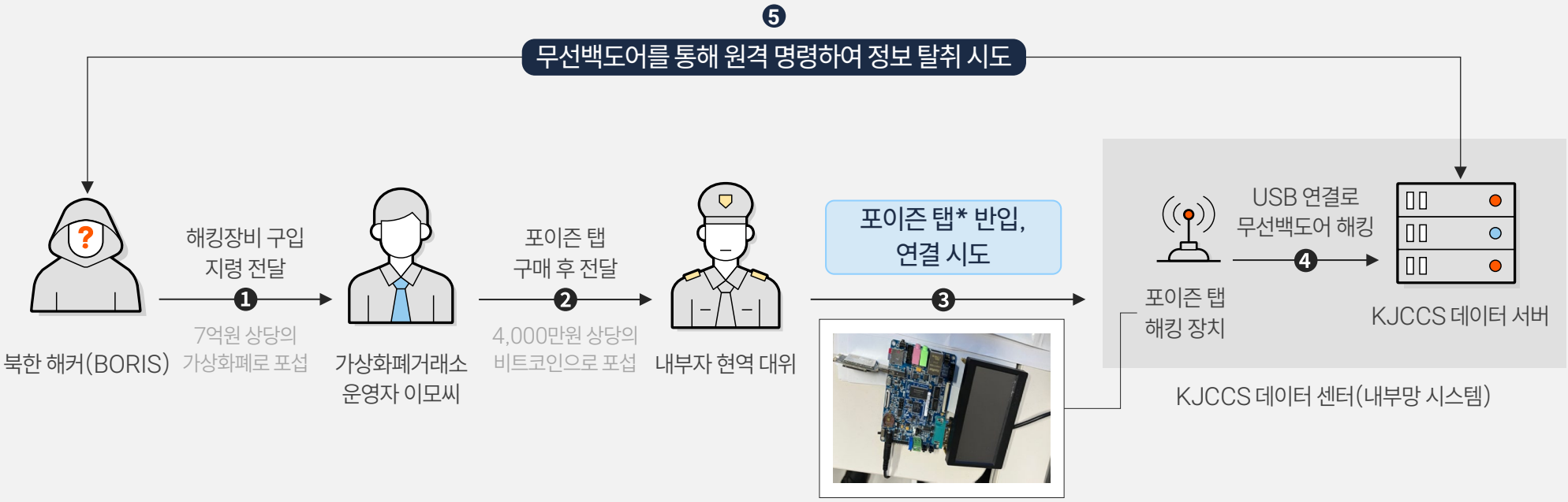


백도어 사례 (USB 장치 : 한국군 합동지휘통제체계 서버 해킹 시도)

① 현역 대위가 북한 해커에게 한국군 합동지휘통제체계(KJCCS) 로그인 자료 등을 제공 후 비트코인 수수(매일경제 2022.04.28)

② 가상화폐거래소 운영자 이모씨가 군사기밀 탈취에 사용되는 무선백도어 해킹 장치(포이즌 탭) 구매 후 현역 대위에 전달

③ 무선백도어 해킹 장치(포이즌 탭)를 타겟 PC에 연결하면 북한 해커가 원격으로 무선백도어 해킹 가능



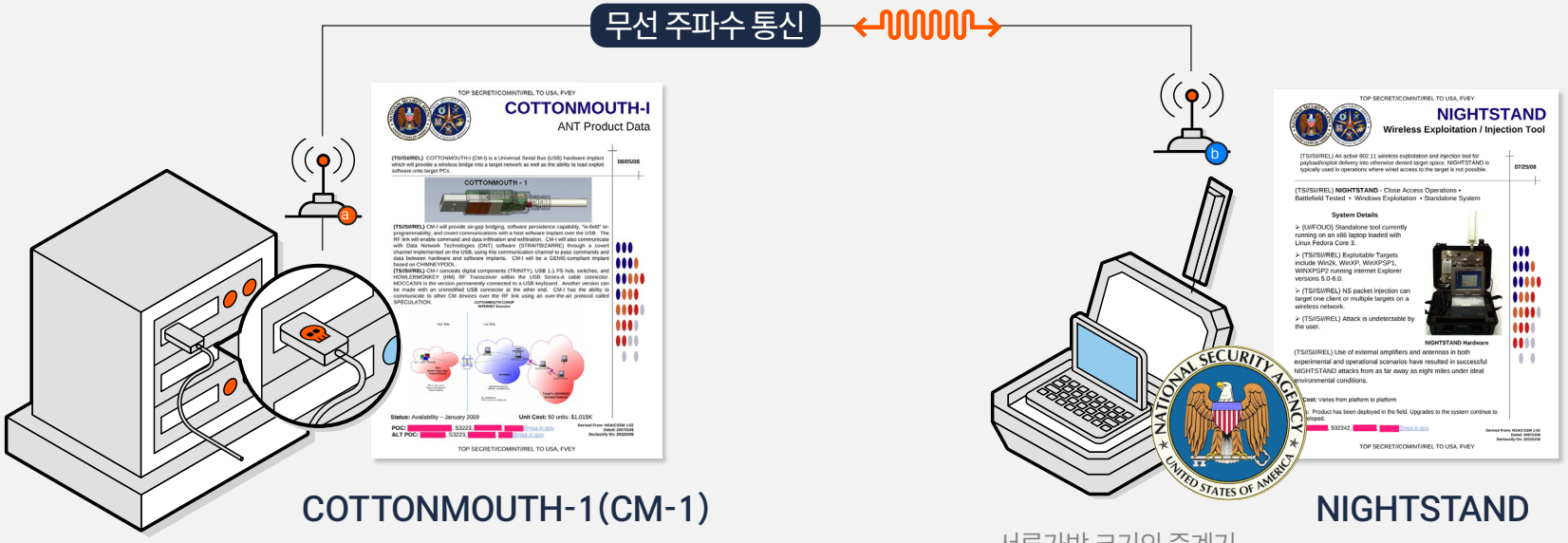
* 포이즌 탭(Poison Tap) : USB 포트를 통해 컴퓨터에 물리적으로 접근하여, 내부망과 외부망이 분리된 환경에서도 웹 세션 정보와 트래픽을 가로채고 원격 조작이 가능한 해킹 장치이자 공격 기법

백도어 사례 (USB 장치 : 미국 국가안보국 퀀텀 프로그램)

① 미국 국가안보국(NSA)이 전 세계 10만대의 PC에 소프트웨어를 심어 정보를 빼내거나 사이버 공격에 활용(뉴욕타임즈 2014.01.14)

② USB 장치(COTTONMOUTH-1)를 통해 타겟 PC안에 악성소프트웨어를 업로드, 장치가 발산하는 무선 주파수(RF)로 무선백도어 실행

③ 중국 해킹부서, 러시아 군, EU 무역 담당 부처, 멕시코 경찰, 사우디아라비아, 인도, 파키스탄 등의 컴퓨터 네트워크에 설치



타겟 PC

COTTONMOUTH-1(CM-1)

① USB 장치로 위장한 무선 스파이칩
② 무선 주파수 통신 채널 제공
③ 악성소프트웨어를 타겟 PC에 업로드
④ 데이터 유출
⑤ 다른 CM-1과 통신

서류가방 크기의 중계기

NIGHTSTAND

① CM-1과의 무선 주파수 통신 및 공격 입력 장치
② 인터넷이 연결되지 않은 대상에 사용
③ 약13km 떨어진 곳에서 수행 가능

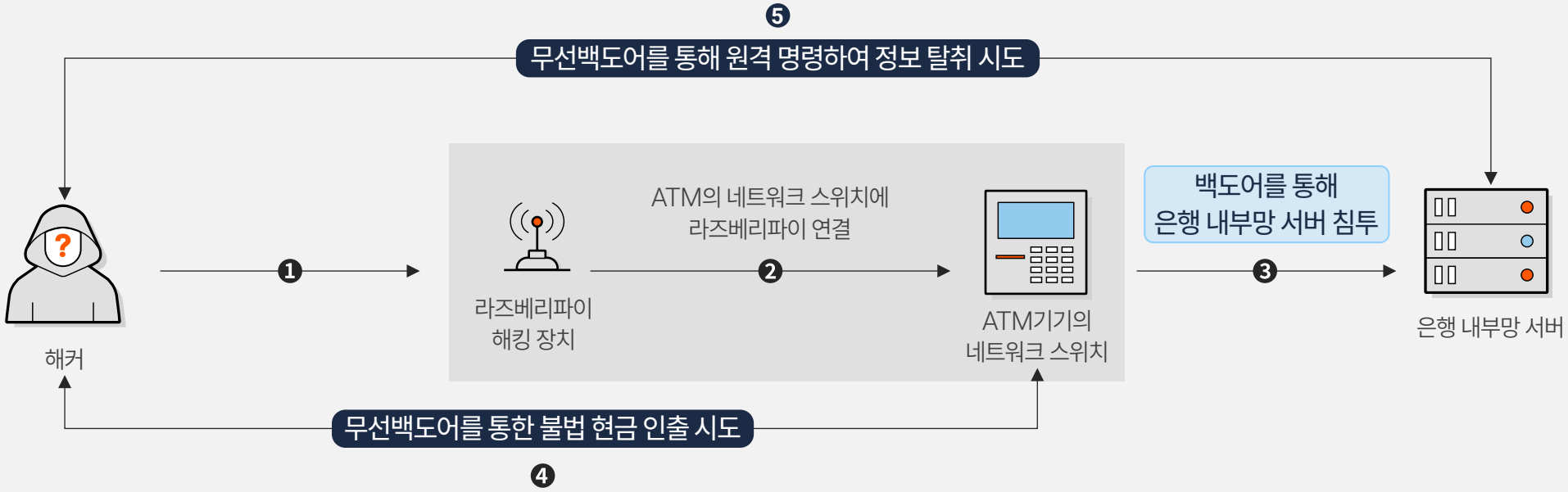
백도어 사례 (LAN카드 : 은행 ATM 네트워크 해킹 시도)

① 해커가 은행 ATM 네트워크에 소형PC인 라즈베리파이* 기기를 연결하여 불법 현금 인출을 노리다 러시아 보안 업체에 발각(보안뉴스 2025.08.01)

② 물리적 접근을 통해 ATM의 네트워크 스위치에 무선 모뎀이 탑재된 라즈베리파이 설치, 백도어를 통해 내부 네트워크 침투

③ 하드웨어 보안 모듈(HSM)의 인증 응답으로 위장하여 ATM에서 불법 현금 인출 및 내부망 장기간 장악을 시도했으나 최종 목표 달성 직전 발각되어 저지

④ 이는 실제 물리적 네트워크를 침투 시작점으로 삼아 무선 통신을 통해 기존 네트워크 방어(방화벽 등)를 우회해 은행 내부망에 침투한 사례



*라즈베리파이(Raspberry Pi) : 개발도상국 학교 등에서 교육용으로 만든 신용카드 크기의 싱글 보드 컴퓨터

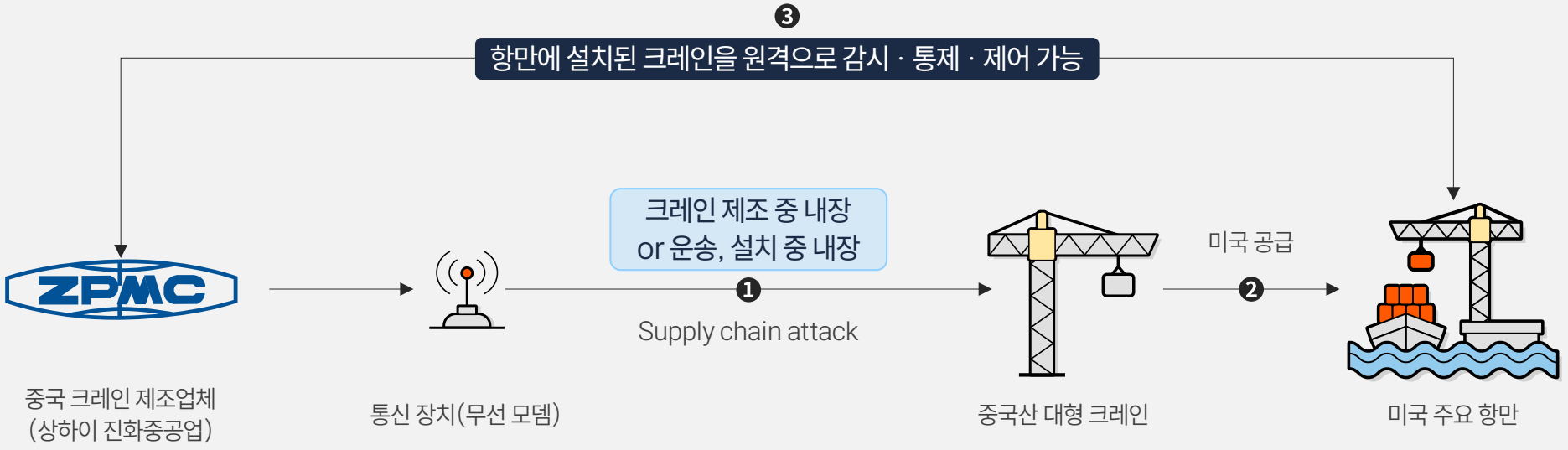
백도어 사례 (공급망, 보드 : 중국산 대형 크레인 내 통신장치 발견)

① 중국산 크레인에서 요청하지 않은 통신장치 발견(월스트리트 저널 2024.03.07)

② ZPMC의 미국 내 크레인 및 기타 해상 인프라에 대한 원격 접근 가능성 제기

③ 미국 항구 내 중국산 장비의 국가안보 위협 가능성에 우려 증폭

④ 바이든 행정부 외국산 크레인을 미국산으로 대체할 계획 발표



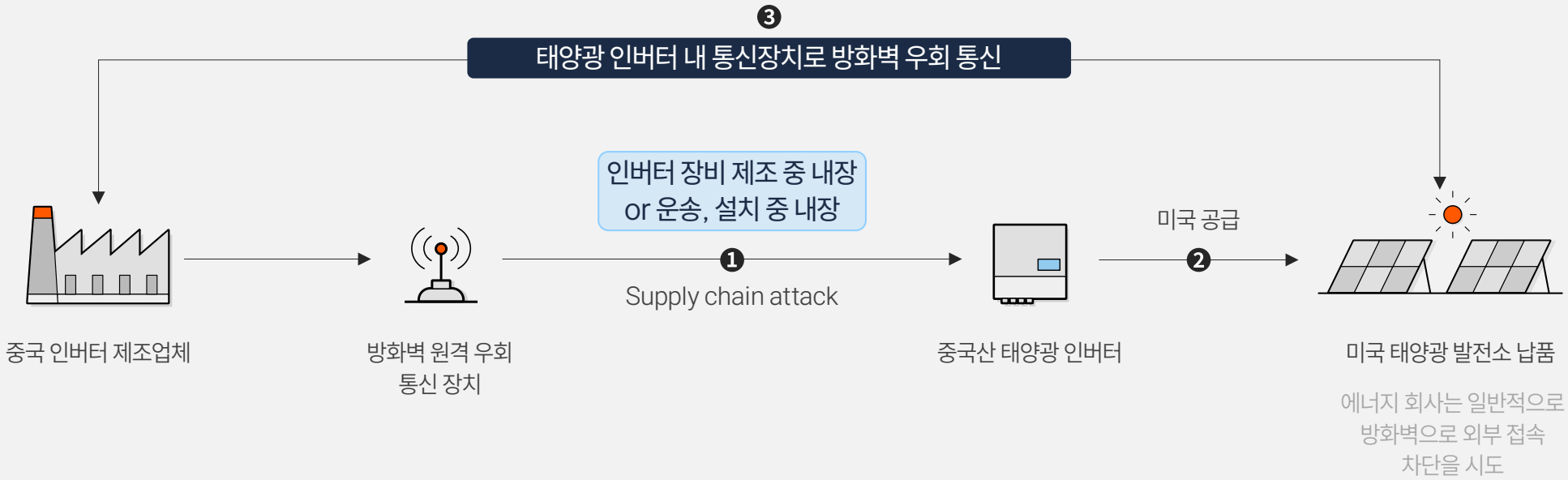
백도어 사례 (공급망, 보드 : 중국산 태양광 인버터 내 통신장치 발견)

① 美 에너지부, 중국산(제조사 미상) 태양광 인버터에서 제품 설명서에 명시되지 않은 통신장치 발견(로이터 2025.05.14)

② 문제 부품은 방화벽을 원격으로 우회하는 추가 통신 채널(백도어 채널)을 제공하면서도 제품설명에는 이를 명시하지 않음

③ 방화벽을 우회해 중국과 직접 통신 가능한 기능을 포함해, 인버터 원격 제어·중단·설정 변경 등을 통한 전력망 교란 가능성 제기

④ 악의적 의도 여부를 떠나 제품 설명에 누락되었다는 것 자체가 공급망 리스크이며, 美 에너지부는 연방정부 전반과 협력해 미 공급망 강화 계획 언급



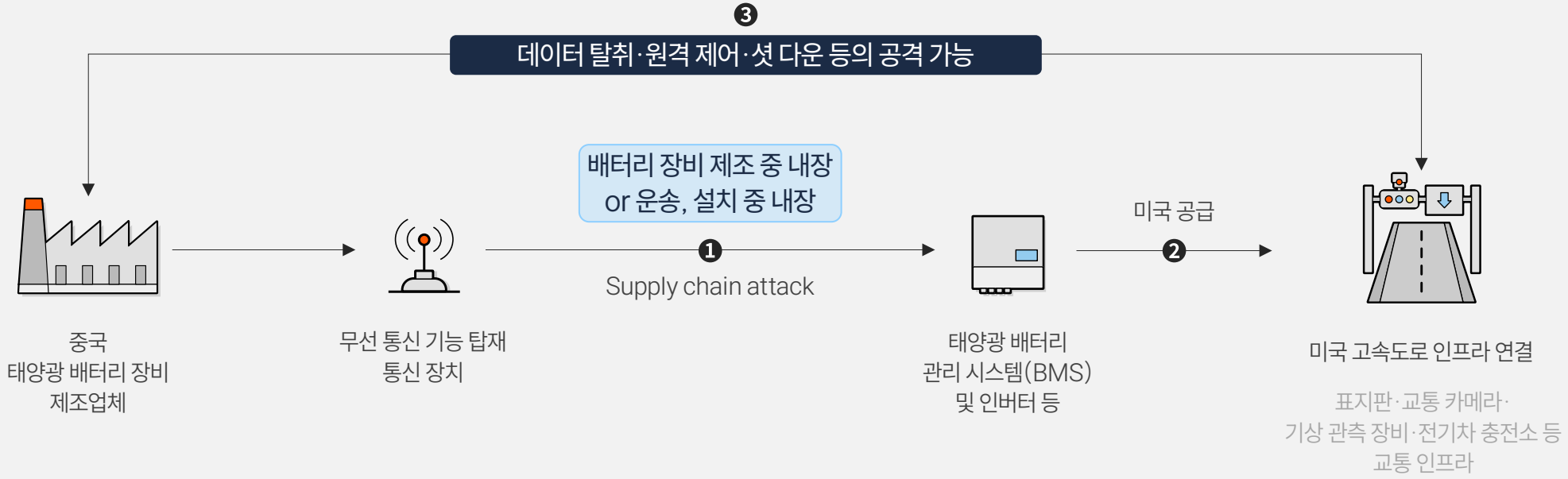
백도어 사례 (공급망, 보드 : 중국산 태양광 배터리 관련 장비 내 통신장치 발견)

① 美 연방고속도로청(FHWA), 중국산(제조사 미상) 태양광 배터리 관리 시스템(BMS)·인버터 내부에서 문서화되지 않은 통신장치 발견(로이터 2025.09.10)

② 해당 장비들은 고속도로 표지판, 교통 카메라, 기상 관측 장비, 전기차 충전소 등 다양한 인프라 시설에 연결되어 있음

③ FHWA는 "무선 통신 기능을 탑재한 이러한 장비들이 악의적으로 활용될 경우 데이터 탈취·원격 작동·셧 다운 등의 공격이 가능하다"고 경고

④ 이에 각 주 정부 및 교통 당국에 모든 태양광 인버터와 배터리 장비에 정기적인 스펙트럼 탐지·분석, 발견 시 즉각 제거 등의 조치 권고



무선백도어 공격에 대한 방어대책 촉구

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부 개정

제48조(정보통신망 침해행위 등의 금지)

① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
② ~ ③ (생 략)
④ 누구든지 정당한 사유 없이 정보통신망의 정상적인 보호 · 인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하거나 이를 전달 · 유포하여서는 아니 된다.

「전자금융감독규정」 제15조(해킹 등 방지대책)

제15조(해킹 등 방지대책)

① 금융회사 또는 전자금융 업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해 행위로부터 방지하기 위하여 다음 각 호의 대책을 수립, 운용하여야 한다.
1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영

2024 국정감사 '정무위원회' 금융감독원 감사中 (2024.10.17)

'무선 백도어 해킹 증가' 우려에 이복현 "방어수단 마련 중"

파이낸셜 뉴스

강명구 의원은 "한국은행에 따르면 지난해 한 해 97건에 달하는 해킹 시도가 있었고 디도스 공격도 있었다"며 "해킹 수법이 나날이 진화하고 있으며 최근에는 망 분리 상태에서도 해킹이 가능한 무선 백도어 해킹이라는 게 늘고 있다"고 지적했다.

국정감사 '과학기술정보방송통신위원회' 과학기술정보통신부 감사中 (2025.10.13)

조인철, 국감용 네트워크망 스파이칩으로 해킹 시연 "무선 백도어 위협 심각"

MBN 뉴스

과기정통부 세종청사에서 열린 국회 국정감사에서 조인철 민주당 의원이 미국 온라인 쇼핑몰을 통해 구매한 USB 케이블 형태의 '스파이칩'으로 직접 국감용 네트워크망을 해킹해 눈길을 끌었습니다.

무선백도어 해킹 보안 솔루션

무선백도어 해킹 탐지 시스템

Alpha-H

데이터 센터, 서버실, 집무실 등에 침투되어
망분리 체계를 무력화시키는 무선백도어를 실시간 탐지

Problem

전파 환경 감시는 무선 보안의 필수 요소

전파 환경 보안 체계 미비로
무선 주파수 통신을 이용한 공격(무선백도어 해킹) 대비가 취약한 상황

APT급 공격*에서 무선 백도어 해킹은 이미 강력한 공격 수단으로
사용되며, 온라인상에서도 관련 해킹 기술이 많이 공개됨

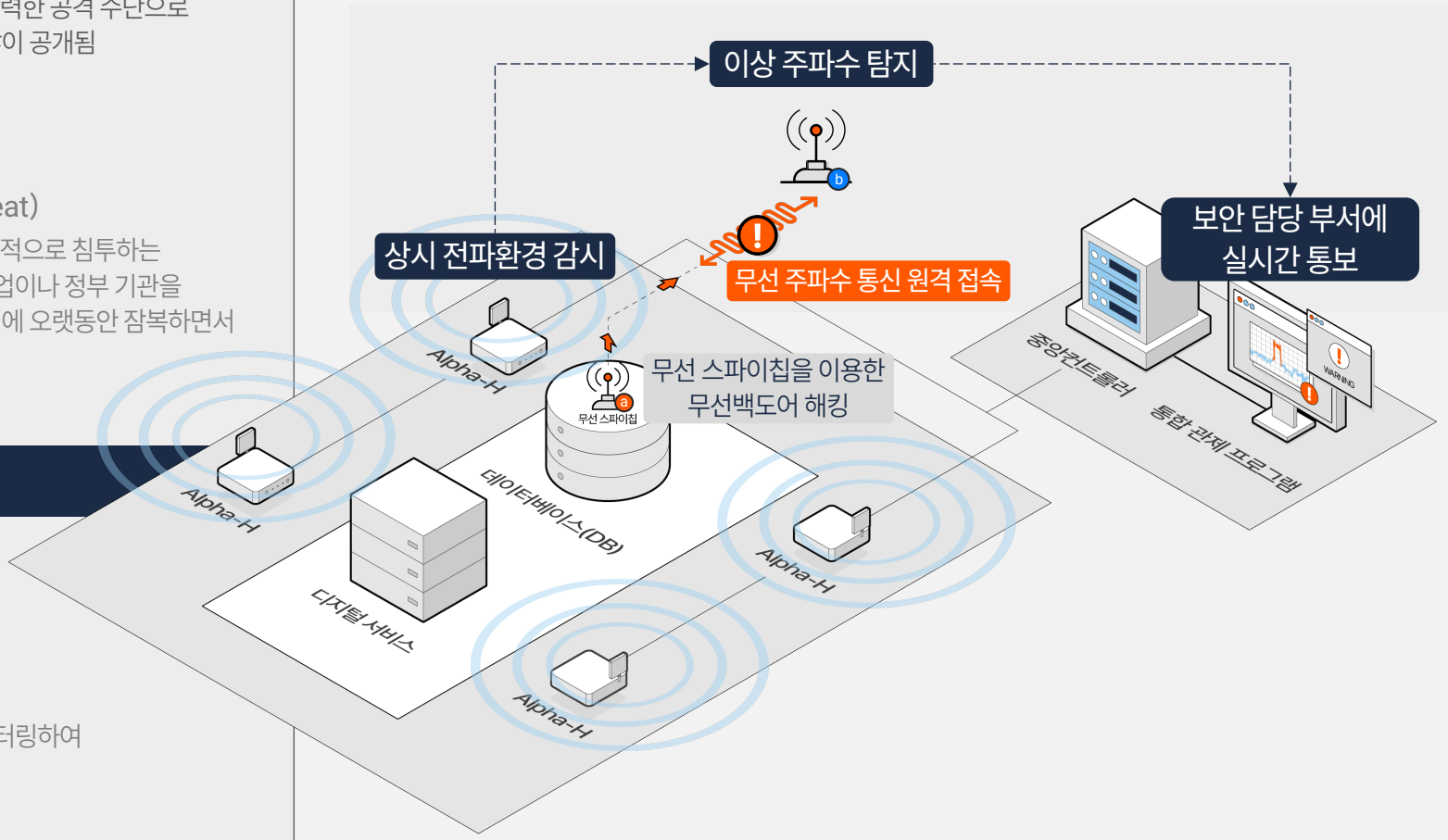
*APT 공격 (Advanced Persistent Threat)
고도로 조직된 그룹이 특정 목표에 장기간 지속적으로 침투하는
사이버 공격. 정치적, 경제적 목적으로 특정 기업이나 정부 기관을
대상으로 하며, 은밀하게 진행하여 목표 시스템에 오랫동안 잠복하면서
데이터 탈취, 중요 서버 공격

Solution

무선백도어 해킹 탐지 시스템

무선백도어 해킹 탐지 시스템 Alpha-H는
25kHz~3GHz 주파수 대역을 24시간 모니터링하여
전파환경에 대한 상시적 보안 제공

무선백도어 해킹 탐지 시스템 운용



무선백도어 해킹 탐지 시스템 Alpha-H

무선 스파이칩 전파 탐지

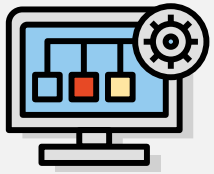
25kHz~3GHz의 주파수 대역을
스캔하여 무선백도어 해킹 탐지

24시간 상시 탐지

보안의 빈틈을 없애는
24시간 365일 상시형 탐지 시스템

위치 추정

이상 주파수의 신호원 위치 추정으로
무선백도어 해킹에 신속 대응

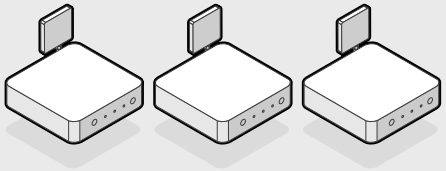


통합 관제

다수 탐지단말기
통합 관리·관제

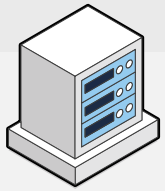
Alpha-H 운용 프로세스

탐지 · 분석 · 관제로 무선백도어 해킹의 사전 예방 및 신속대응



탐지단말기(탐지 · 분석)

실시간 스캔 및 신호 수집 · 탐지



중앙컨트롤러(관리)

신호 정보 저장 및 다수 단말기 통합 관리

통합 관제 프로그램(관제)

이상 신호 상시 모니터링,
무선백도어 해킹 여부 판단 후 위치 추정

01 **학습** ① 탐지 장소에 있는 다양한(정상·인가) 주파수를 탐지·분석하여 분류 및 학습

탐지 범위 : 반경 5~6m

탐지 주파수 범위 : 25kHz~3GHz의 초광대역, 초정밀해상도(※ 탐지 주파수 전 대역 1초 내 스캔)

02 **탐지** ② 학습 완료 후, 탐지단말기는 이상 주파수(비정상·비인가)를 24시간 365일 실시간 탐지

03 **분석** ③ 이상 주파수 탐지 시, 탐지단말기의 분석을 거쳐 중앙컨트롤러로 전송

04 **관제** ④ 통합 관제 프로그램을 활용하여 이상 주파수 분석 및 위치 추정

05 **대응** ⑤ 위치 추정 값을 기반으로 무선백도어 해킹 장치 색출

이동형 전파 탐지기* 활용 시, 이상 주파수의 전파 발생 위치를 정밀 추적하여 색출 시간 단축

*이동형 전파 탐지기 Alpha-P: 무선백도어 해킹 신호를 정밀 추적하는 고감도 휴대형 전파 탐지기

별첨

도청 보안

Product, Service

구매, 렌탈, 방문 탐지 서비스

시장 점유율 1위

Alpha-I
Alpha-S
(상시형)

Alpha-P
(휴대형)

도청 탐지
서비스

무선백도어 해킹 보안

Product

구매, 렌탈

시장 점유율 1위

Alpha-H
(상시형)

Alpha-P
(휴대형)

불법촬영 보안

Product, Service

구매, 렌탈, 방문 탐지 서비스

시장 점유율 1위

Alpha-C
(상시형)

전문 관제
서비스

불법촬영
탐지 서비스

25년 9월 기준 - 도청, 불법촬영 보안 점유율 출처 : 조달데이터 허브·국방전자조달시스템

특허

총 31건

국내(25), 해외(6)

제품 관련 핵심 특허

도청 보안	• 광대역 불법 무선 신호의 탐지 방법 • 광대역 RF신호 수신장치 및 수신방법 • 음성 자동감지 및 주파수를 이용한 도청기 탐지 장치 및 방법
무선백도어 해킹 보안	• 복수의 전파탐지장치를 이용한 무선 해킹 스파이칩 위치 추정 시스템 및 그 방법
불법촬영 보안	• 온도 변화를 이용한 몰래 카메라 탐지기 및 그 방법 • 오탐방지용 몰래카메라 탐지 시스템 • 정상 이용자를 구분하는 몰래카메라 탐지 시스템

인증

- 조달청 우수제품
- 조달청 벤처창업혁신상품
- INNOBIZ 중소벤처기업부 이노비즈 선정
- 조달청 혁신제품
- 중소벤처기업부 성능인증
- 품질경영관리시스템 ISO 9001 인증

수상

- 대통령 표창
- 행정안전부장관 표창
- 조달청장 표창
- 국방부장관상
- 산업통상자원부장관 표창
- 방위사업청장상
- 한국인터넷진흥원장상
- 한국여성단체협의회 전국여성대회 특별상