무선백도어 해킹 탐지 시스템

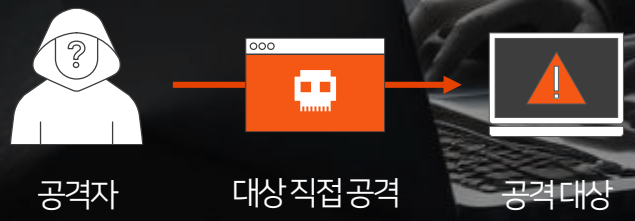
Alpha-H

GITSN (주)지슨
02.852.3560~4 / www.gitsn.com / sales@gitsn.com

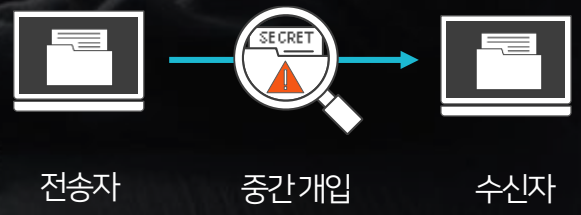
해킹 Hacking

정의 '컴퓨터 시스템에 무단 침입 후 **데이터 탈취, 시스템을 파괴**하는 모든 행위'
정치, 외교, 금융, 산업, 문화 등 정치·경제 사회 전반을 위협

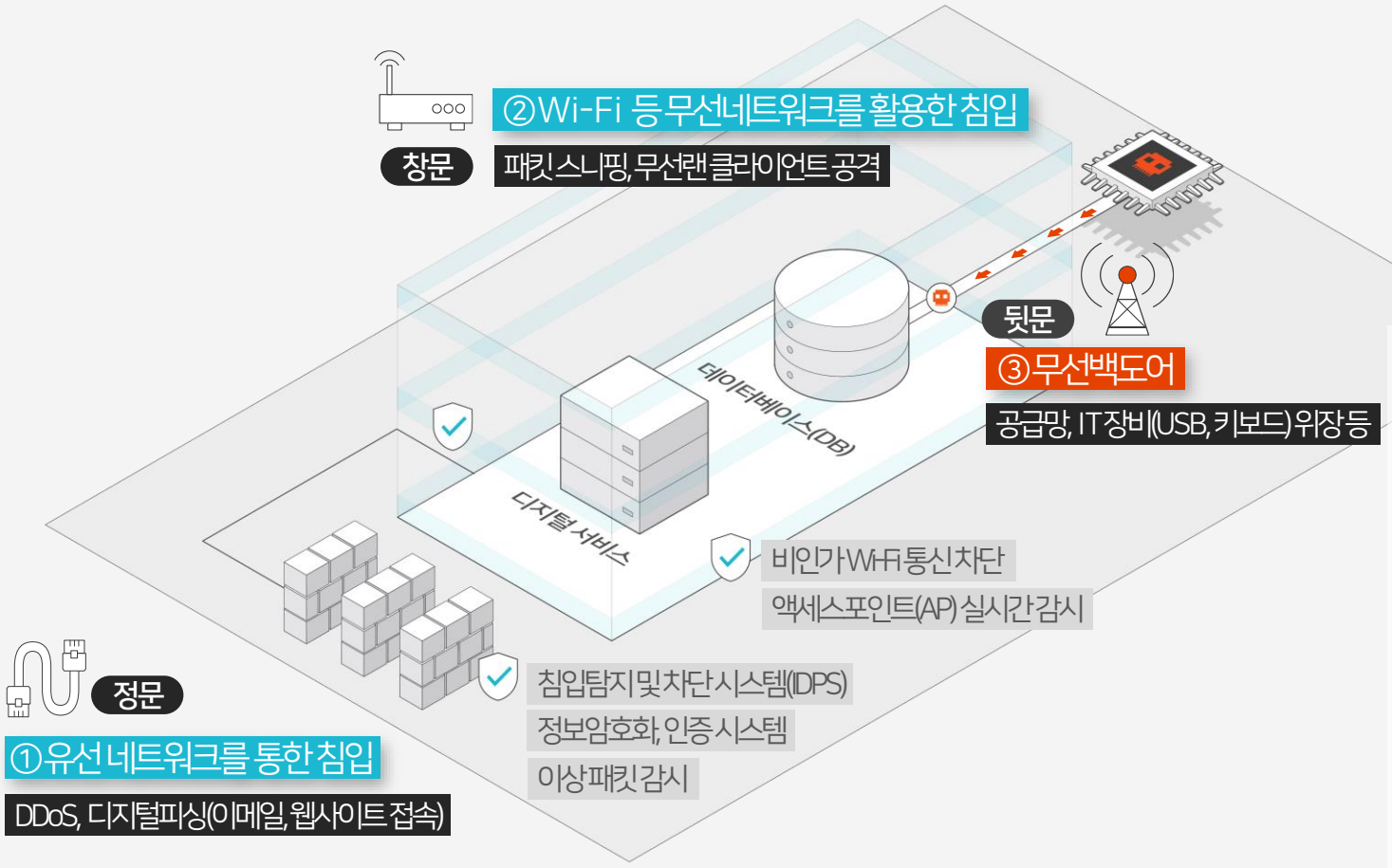
분류 1. 직접 공격



2. 전송중인 데이터를 중간에서 탈취



해킹의 침입 경로



탐지 방어 솔루션 부재

③무선백도어를 이용한 침입

- 무선 주파수(RF) 이용하여 무선 연결통로 확보
- 기존의 솔루션으로는 방어 불가능
- 백도어 설치· 전달· 유포행위 관련 법적 벌칙 ·처벌 규정 미비
- 사례

  NSA가 전세계 10만여대 이상의 PC에 무선백도어 해킹 시도
  (2014년 퀀텀 프로젝트)

  한국군 현역 대위가 무선백도어를 이용하여 북한 해커에게
  한국군 합동지휘통제체계(KJCCS) 서버 자료 전달 시도

무선백도어는 기존 보안체계를 우회합니다.

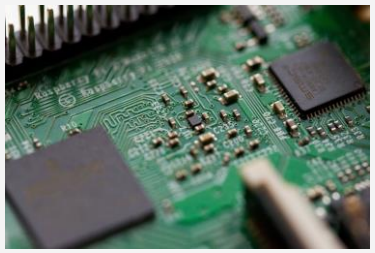
* 타겟 시스템에 무선 주파수(RF)로 연결

step1

공급망 공격 or 평범한 IT장비로 위장

부품 공급 과정에서 컴퓨터 보드에 무선 스파이칩* 탑재

*무선 스파이칩 : 무선 주파수 송·수신 기능을 갖는 초소형 칩



무선 스파이칩을 USB, 키보드 등 IT 장비로 위장

step2

무선 스파이칩을 이용한 무선 주파수(RF) 연결로 기존 보안체계 우회하여 공격

무선백도어 침입 경로

침입 경로	침투 방식
① 컴퓨터 보드 내부 삽입	컴퓨터 보드 안에 무선 스파이칩 탑재 후 구동
	하드웨어 제조사, 유통업체, 배송업체에 의해 삽입 -공급망 공격 (Supply Chain Attack)
② USB, 키보드 등 IT 장비 위장	IT 장비(USB, 키보드 등)로 위장하여 연결 시 구동
	무선 스파이칩이 숨겨진 IT장비를 해당 **컴퓨터**에 **연결**

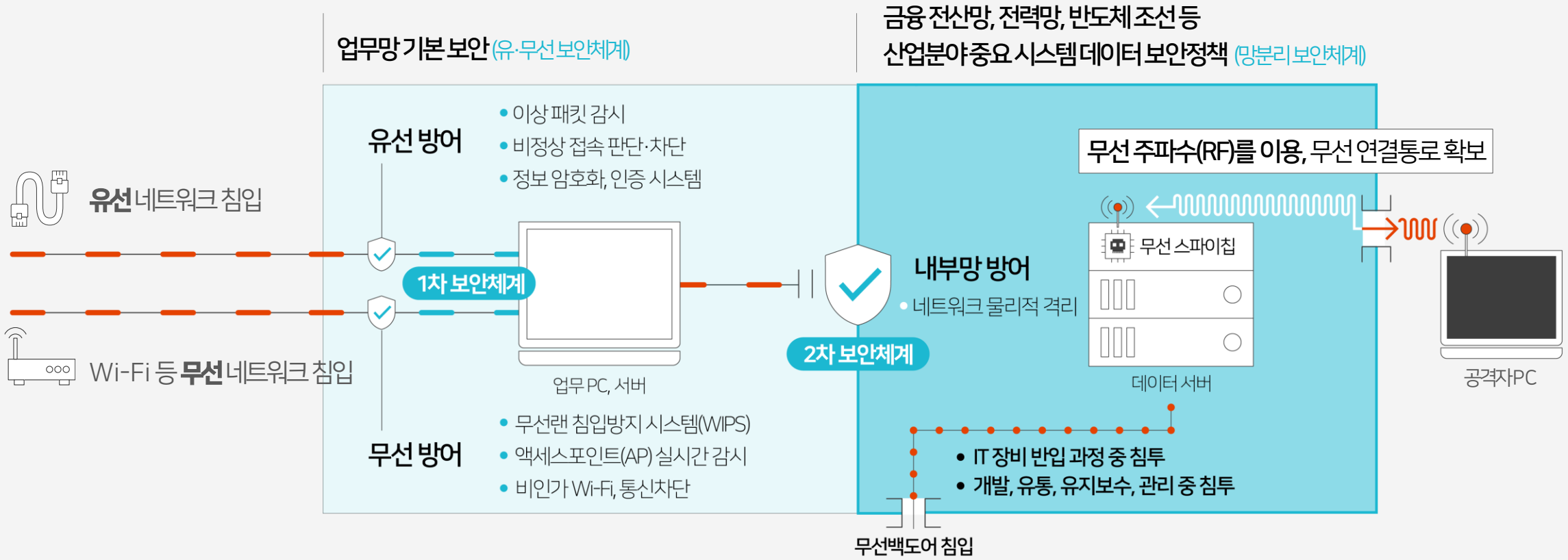
무선백도어 특징

① 타겟 시스템에 **무선 스파이칩**을 심는 등, **무선 연결통로 확보**

② 무선 주파수(RF)로 타겟 시스템 직접 접속 **(수 km밖에서 원격 침입)** **WIPS, 방화벽 등 기존 보안체계 우회**

③ **망분리 시스템 무력화**

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

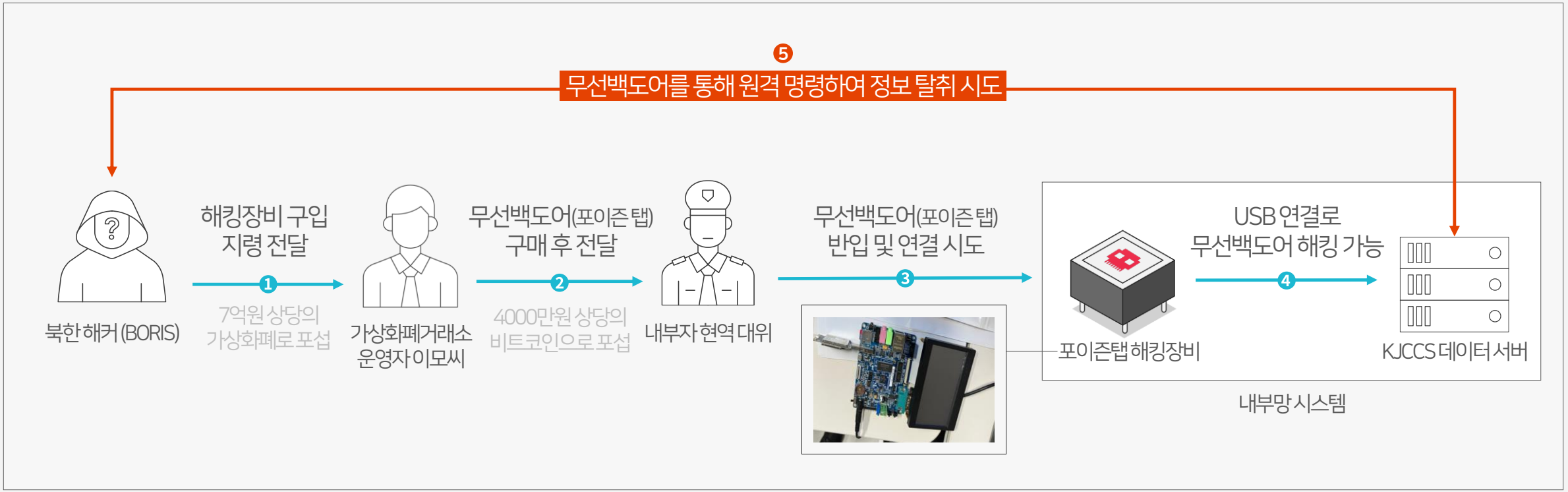


백도어 사례 ❶ 한국군 합동지휘통제체계(KJCCS) 서버 해킹 시도

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

② 가상화폐거래소 운영자 이모씨 군사기밀 탈취에 사용되는 **무선백도어 장비**(포이즌 탭) 구매 후 현역 대위에 전달

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

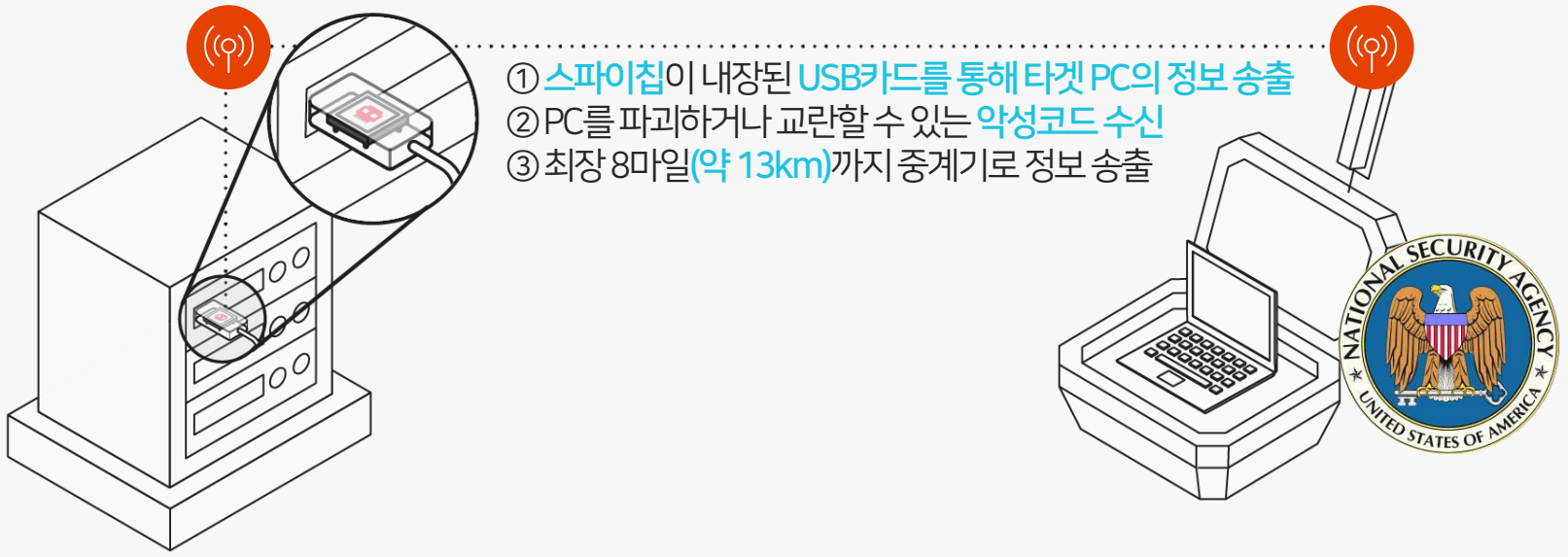


백도어 사례 ❷ NSA(미국 국가안보국) 퀀텀 프로그램

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

② USB포트(제품명 : COTTONMOUTH-1)를 통해 타겟 PC안에 USB카드를 넣거나 소형회로판을 심어 넣고, 이들이 발산하는 무선 주파수(RF)로 무선백도어 실행

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



백도어 사례 ❸ 공공기관 기상관측장비에 악성코드 삽입된 채 납품

① 국내 공공기관에 납품된 **중국산 기상관측장비에서 악성코드 발견**(채널A 2023. 08.21 보도)

② 전형적인 **하드웨어 공급망 공격**(제품의 개발, 유통, 설치, 유지보수 등의 공급 단계 중 해킹, 기존 소프트웨어 기반 탐지 도구 우회하는 전문적인 해킹 공격)

③ "국내 정부기관, 지자체에 공급된 중국산 네트워크 장비, 폐쇄회로 TV(CCTV) 등 유사장비에 대한 전수조사"(국정원) 등 보안 대책 강화 중

④ **무선백도어 공격 가능성**에 대한 전문적인 조사 및 보안책 시급

백도어 사례 ❹ 중국산 CCTV 제품 백도어 해킹 의혹

① **중국산 CCTV 제품의 백도어를 통해 중국으로 정보 유출 의혹**(대표적으로 중국 국영기업인 하이크비전 CCTV)

② 2017년 아프가니스탄 카불 주재 미국 대사관 영상 외부로 전송 의혹(중앙일보 2019.01.21)

③ 백악관과 대사관, 미군 시설 등 중요 정부기관 중요 정보(녹화, 녹음)가 중국 정보당국에 전송될 위험성 인지

④ **중국산 통신·영상 보안장비를 사용하지 못하도록 하는 국방수권법(NDAA) 미 의회 통과 (2019.08)**

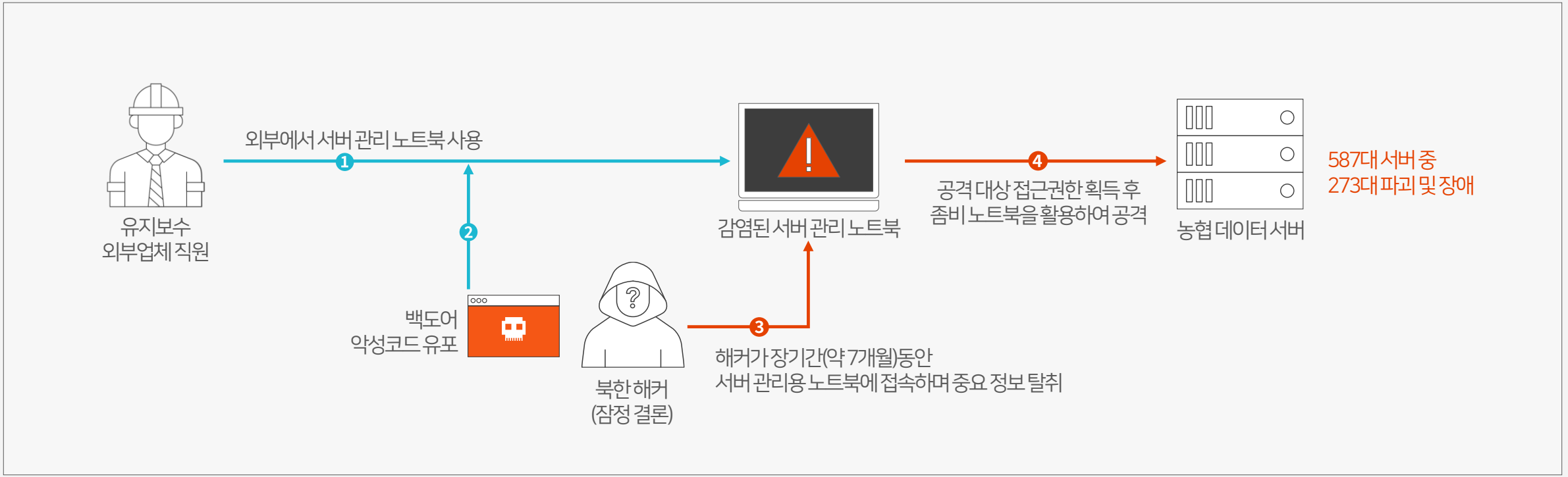
백도어 사례 ❺ 농협 전산망 마비 사태

① **백도어를 이용한 농협 서버시스템 파괴 사건** (연합뉴스 2011.05.03 수사결과 보도 (04.12 서버 마비 사태 발생))

② 유지보수 외주업체(IBM) 직원이 서버 관리 노트북을 외부에서 사용하다 백도어에 감염되어 발생

③ 해커는 백도어를 통해 장기간(약 7개월)동안 들키지 않고 접속하며 공격 대상(농협 서버) IP와 최고접근권한 비밀번호 획득

④ 원격제어를 통해 외부업체 직원 노트북에 악성코드 설치 후 공격 명령 프로그램 실행 – **농협 내부망 및 웹 서버 파괴** (18일간 서비스 마비)



해킹은 보안의 가장 약한 고리를 최우선으로 공격하므로

무선백도어에 대응할 수 있는 상시적 전파환경 감시가

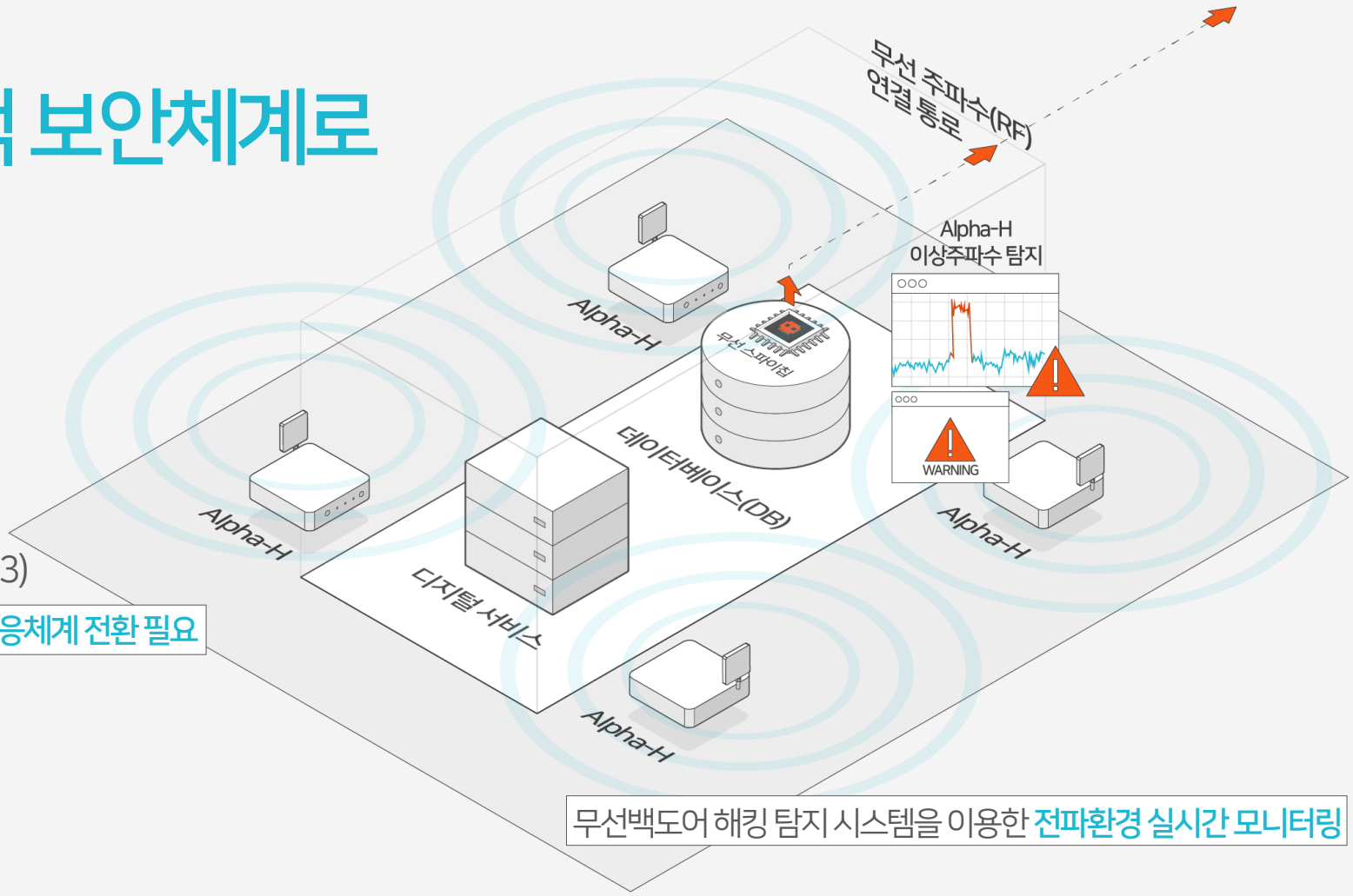
필수적인 보안 요소로 자리잡고 있다.

Alpha-H

무선백도어 해킹 탐지 시스템 Alpha-H

데이터 센터, 집무실 등에 침투되어 망분리 등 기존 방어 시스템을
무력화시키는 무선백도어를 24시간 365일 탐지

전파환경에 대한 상시적 보안체계로 무선백도어 즉각 대응



무선백도어 해킹 탐지 시스템을 이용한 **전파환경 실시간 모니터링**

과학기술정보통신부 '사이버 보안 대응 전략' (2023)

사이버 공격에 효과적 대응을 위한 사이버 **레질리언스 대응체계 전환 필요**

레질리언스 : 피해 발생 후 빠르게 복귀하는 능력, **회복탄력성**

공격 기법이 다양해지면서 완벽한 대응보다 빠른 회복이 중요

빠른 회복의 첫 걸음은 **피해 발생에 대한 신속한 인지**

Alpha-H

① 제품명 : 무선백도어 해킹 탐지 시스템 Alpha-H
② 제품 개요 : 신종 사이버 위협인 백도어 해킹(무선) 사전 예방 솔루션 , 데이터 센터, 집무실 등에 침투된 무선백도어를 24시간 365일 탐지
③ 제품 구성 : ❶ 탐지단말기 ❷ 중앙 컨트롤러 ❸ 통합 관제 솔루션

KTC 산업통상자원부 산하 시험인증기관(한국기계전기전자 시험연구원) 공인 시험 성적서 **적합 판정**

24시간 365일

1초내 전대역 스캔으로
무선백도어 해킹 방어

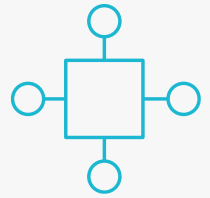
전자동 감시

현장 탐지 인력
불필요

위치 추정 기술 기반

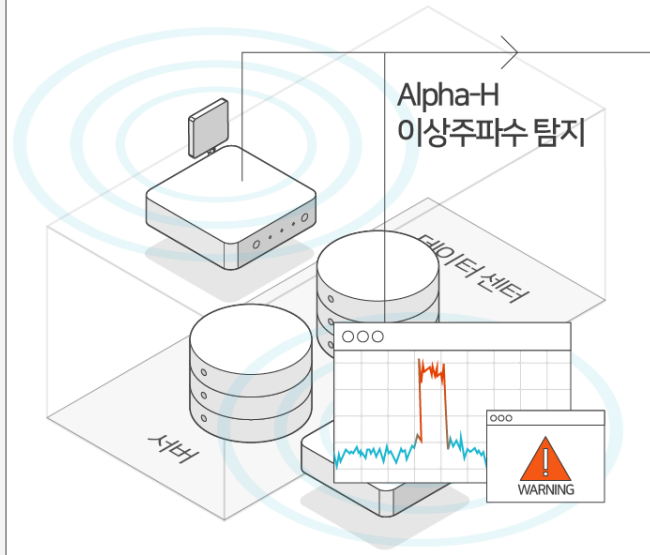
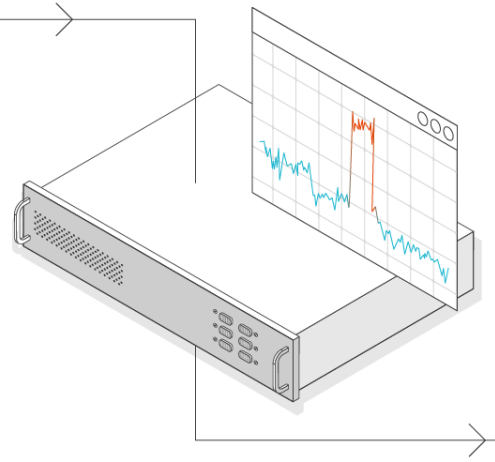
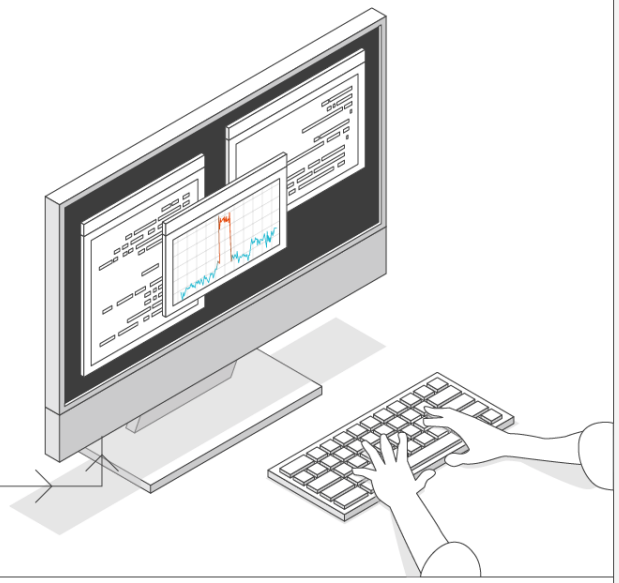
무선백도어
신속 대응

통합 관제



다수 탐지단말기
통합 관리

시스템 구성

탐지·분석 (1 탐지단말기)	관리(2 중앙 컨트롤러)	관제(3 통합 관제 솔루션)
		
실시간 스캔 및 신호 수집·탐지	신호 정보 저장 및 다수 단말기 통합 관리	이상 신호 상시 모니터링, 해킹 여부 판단 후 위치 추정 및 통보

운용 프로세스

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 이상주파수(비정상·비인가)를 **24시간 365일 실시간 탐지**

03 **분석** ③ **이상 주파수 탐지** 시, **탐지단말기** 분석을 거쳐 **중앙 컨트롤러**로 전송

04 **관제** ④ **중앙 컨트롤러**의 데이터를 **통합 관제 솔루션**을 활용한 **무선 주파수(RF) 분석**(해킹 로그 활동 분석) 후 **위치 추정**

05 **대응** ⑤ 위치 추정을 기반으로 무선백도어 해킹 장치 색출

무선백도어 공격에 대한 방어대책 촉구

- 무선백도어 공격에 대한 대비로
금융권 정보 탈취 사전 방지 시스템 주문

김선동 의원 **국내 은행하고 증권사의 무선 네트워크 정보 탈취** 이런 부분들을 무선백도어 침입이라고 편의적으로 말씀드릴 수 있는데 …
실제 무선백도어가 가능하기… 내부 전산실 침입을 하려고 그러면 **스파이칩을 심거나 스파이칩이 내장된 전산장비를 설치하면 무방비 상태로 뚫립니다.**
… 스파이칩이 내장된 키보드나 마우스 같은 것만 교체를 해도 이것이 뚫리게 되어 있습니다. … 그것도 무선 상태에서… 지금 해킹 기술이 굉장히 고도화돼서 발전하고 있는데 방지 시스템은 사실 굉장히 걸음마 수준에 있는 것이 현실입니다…

금융감독원장 윤석헌 예, 저희들이 잘 모니터링을 하도록 하겠습니다.

국정감사 '정무위원회' 금융감독원 감사中 (2019.10.08)

- 군 내부망 해킹 보완을 위해
무선통신 가능 전 주파수 대역 보안 시스템 촉구

백승주 의원 국방부의 군 내부망 해킹에 조금 새로 보안할 요소가 있다고 듣고 있습니다. 무슨 내용인지 아시지요?
무선통신 가능 주파수 전 대역에서 이 보안 시스템을 확인해야 될 부분이 있다. 그것 좀 확인해 주시고.

국방부장관 정경두 예. 알겠습니다.

국정감사 '국방위원회' 국방부 감사中 (2019.10.21)

정보통신망법 일부 개정 발의

(2023.04.21 발의자 : 김영식·정우택·서범수·김희곤·김상훈·서정숙·노용호·이인선·정희용·지성호 의원(10인)

제48조 제4항 신설 **부정 목적 백도어 정보통신망 설치 · 전달 · 유포 금지**

백도어는 하드웨어나 소프트웨어 등의 개발과정이나 유통과정 중에 몰래 탑재되어 정상적인 인증 과정을 거치지 않고 보안을 해제 할 수 있도록 만들어, 정보유출 등 사이버 보안사고를 야기하는 주범으로 꼽히고 있음.

이에 정보통신망에 대한 침해행위 금지 규정에 백도어의 설치와 전달 · 유포 행위를 추가하고, 벌칙 규정에 백도어를 설치하거나 이를 전달·유포한 자에 대한 처벌 규정을 추가하여, 누구든지 부정한 목적으로 백도어를 정보통신망 등에 설치하거나, 이를 전달·유포하지 못하도록 하고자 함(안 제48조제4항 및 제71조제1항제11호).

GITSN

(주) 지슨

핵심 제품

첨단 도청범죄 대응

Alpha-S

상시형 무선도청 탐지 시스템

신종 사이버 위협 대응

Alpha-H

무선백도어 해킹 탐지 시스템

화장실 몰래카메라 대응

Alpha-C

상시형 불법촬영 탐지 시스템

핵심 연혁

2000. 설립

2018. 조달청 우수제품 지정 (광대역 및 저전력 신호탐지가 가능한 도청탐지장치)

2018. 안전산업진흥 유공 안전산업 활성화 및 안전관리 기여부문 행정안전부장관상 수상

2019. 제3회 대한민국 스마트국방 ICT산업박람회 우수제품 평가대회 국방부장관상 수상

2020. 제44회 국가생산성대상 미래유니콘기업부문 대통령 표창 수상

2022. 조달청 혁신제품 선정 (열감지 기반 상시형 몰카 탐지 시스템)

2022. ㈜지슨-LG전자 협력, 글로벌 대상 신제품 출시 (도청 탐지 솔루션 + 디지털 사이니지)

2023. 코넥스 상장

2023. 제3회 조달의 날 '2023 제4회 혁신조달 경진대회' 조달청장 표창

수상내역

대통령 표창

2020 제44회
국가생산성대상
미래유니콘기업부문

국방부장관상

2019 제3회 대한민국
스마트국방ICT산업박람회
우수제품평가대회

행정안전부장관상

2018 안전산업진흥
유공안전산업활성화
및 안전관리기여

산업통상자원부장관 표창

2022 제19회 대한민국
신성장경영대상

방위사업청장상

2018 대한민국 스마트
국방·드론산업대전 전시
참가기업제품평가대회

조달청장 표창

제3회 조달의 날
2023 제4회 혁신조달
경진대회

인증성과

조달청
우수조달물품

중소벤처기업부
성능인증

조달청
혁신제품 지정

품질경영관리시스템
ISO9001 인증

조달청
벤처나라지정

중소벤처기업부
이노비즈 선정