

무선백도어 해킹 탐지 시스템

Alpha-H

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

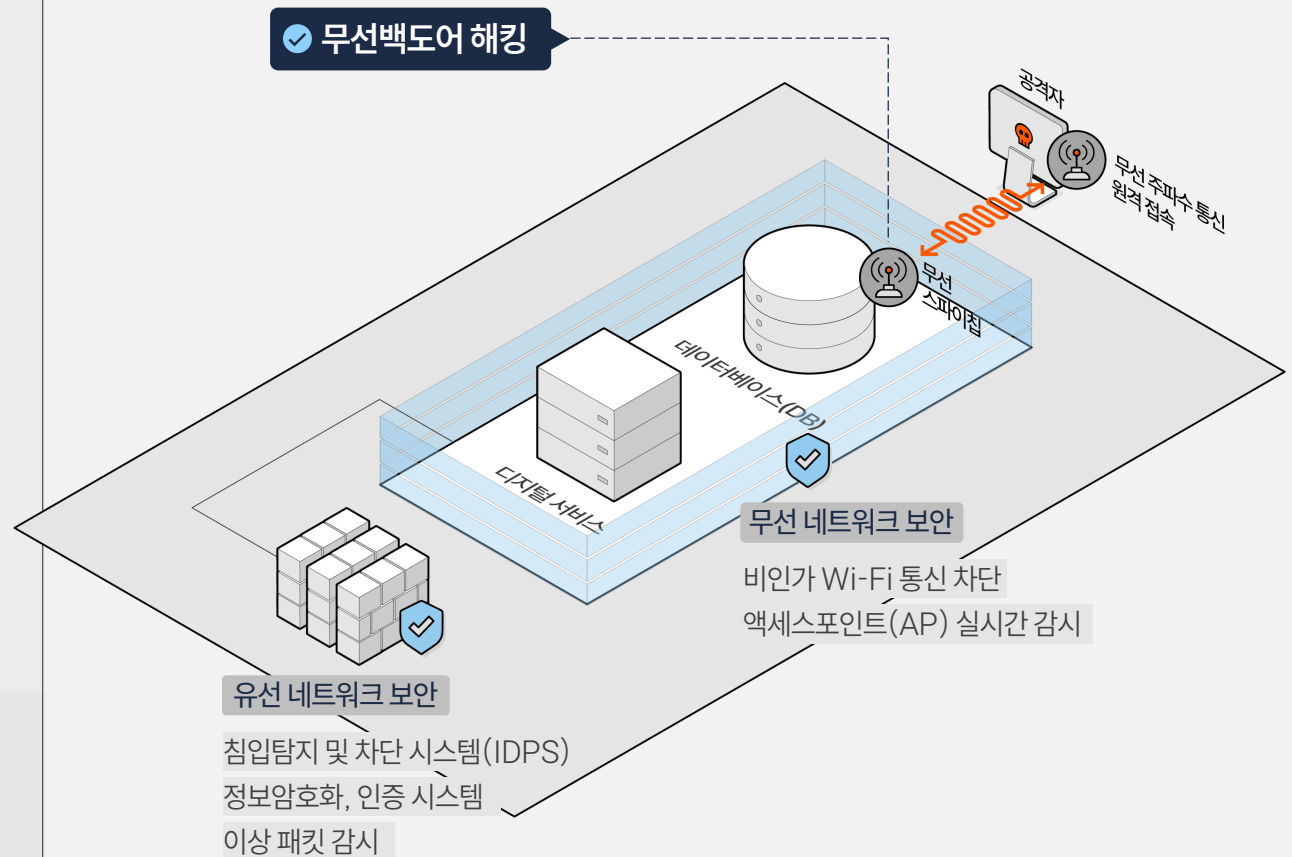
무선백도어 (무선 주파수 통신*)

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

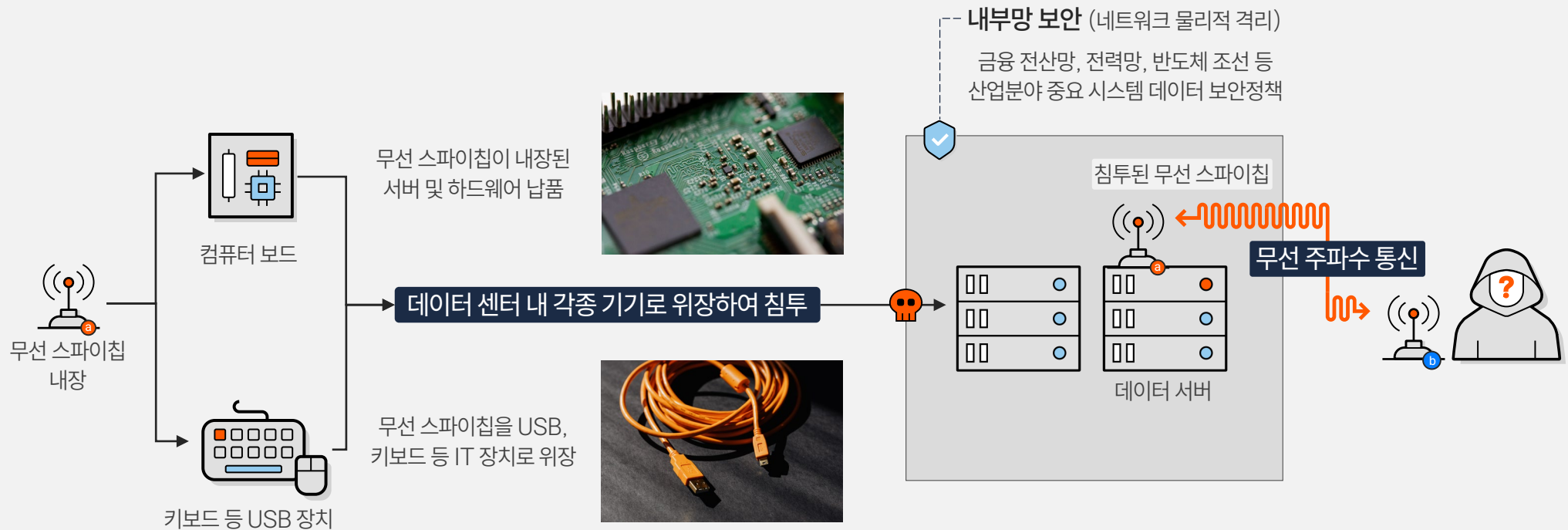
무선 백도어 해킹 사례

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



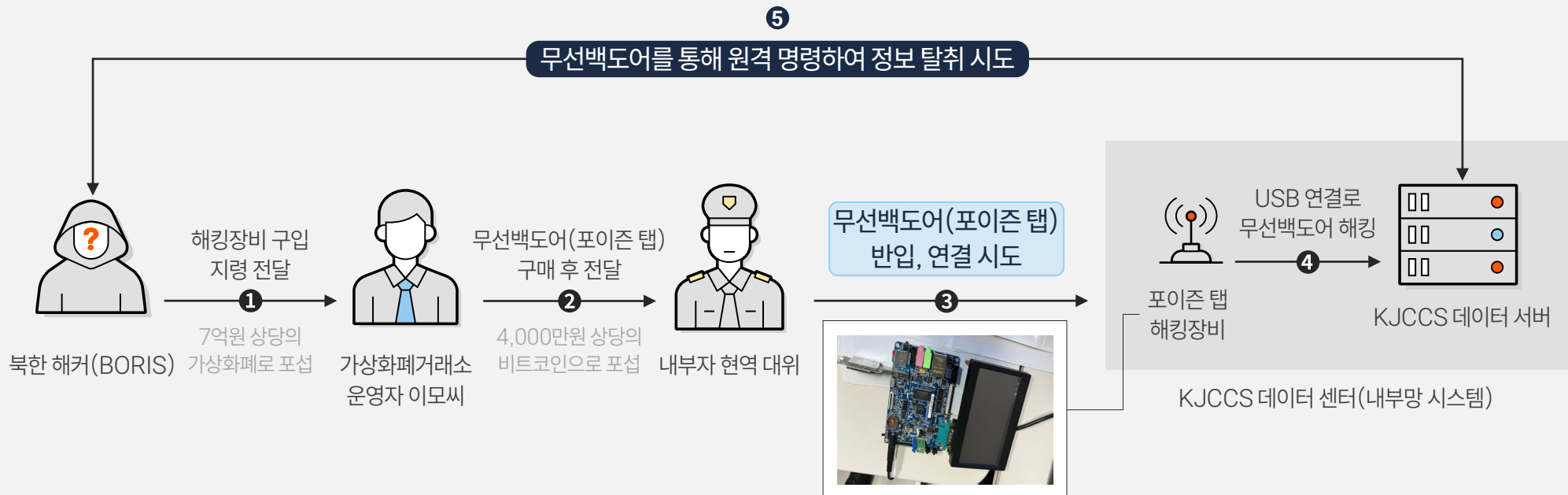
무선백도어 특징

- 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 시스템 원격 접속(수 km밖에서 무단 침입)하여 데이터를 탈취하거나 시스템을 붕괴시키는 신종 해킹
- ③ 기존의 보안 솔루션으로는 방어 불가능 **망분리 시스템(내부망) 무력화** **WIPS, 방화벽 등 기존 보안체계 우회**
- ④ 매우 높은 수준의 접속 권한 획득 - 고부가가치 데이터 탈취, 사이버 테러로 인한 혼란 우려



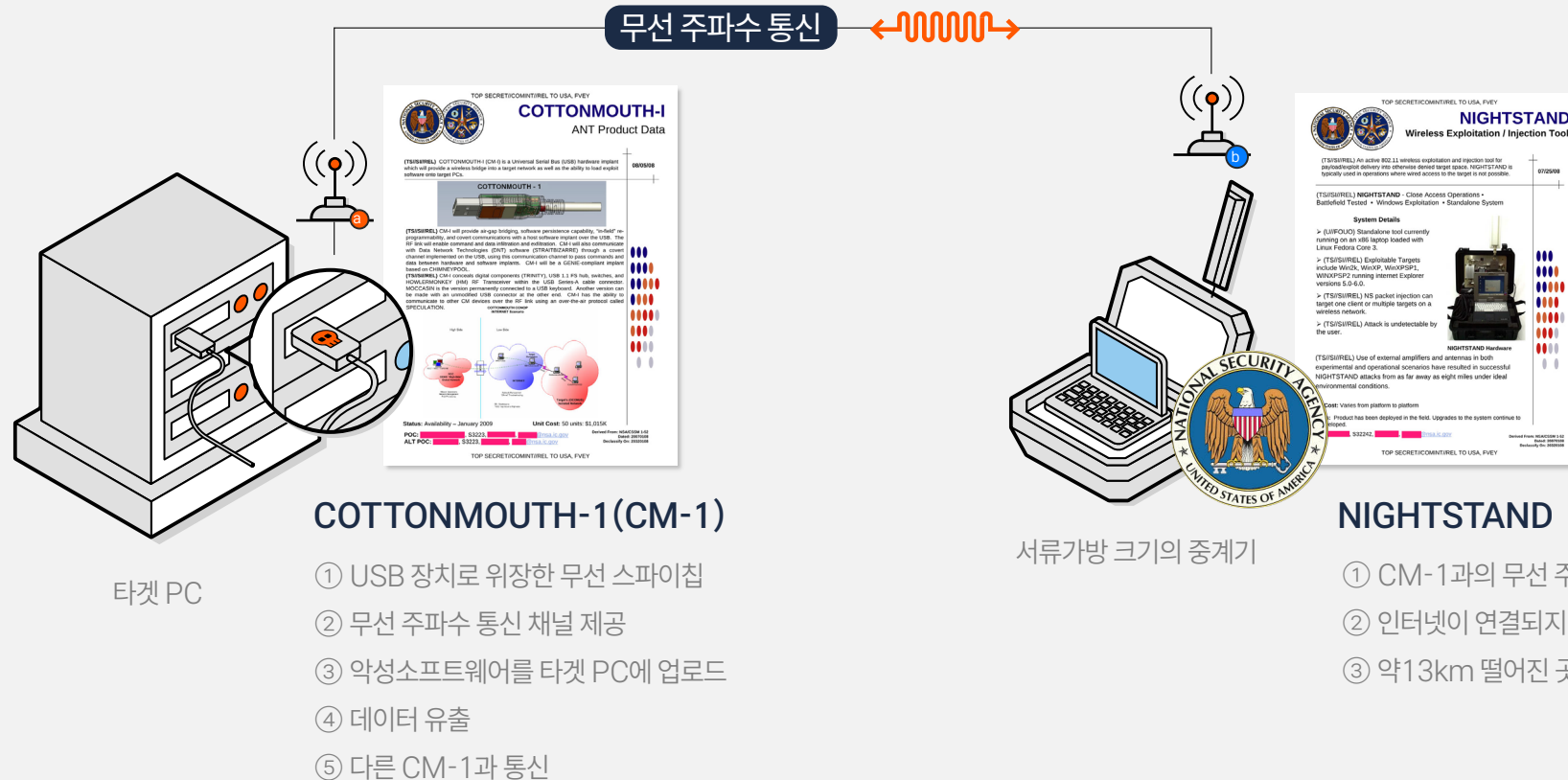
백도어 사례 (USB 장치 : 한국군 합동지휘통제체계 서버 해킹 시도)

- ① 현역 대위가 북한 해커에게 한국군 합동지휘통제체계(KJCCS) 로그인 자료 등을 제공 후 비트코인 수수(매일경제 2022.04.28 보도)
- ② 가상화폐거래소 운영자 이모씨가 군사기밀 탈취에 사용되는 무선백도어 장치(포이즌 탭) 구매 후 현역 대위에 전달
- ③ 무선백도어 장치(포이즌 탭)를 타겟 PC에 연결하면 북한 해커가 원격으로 무선백도어 해킹 가능



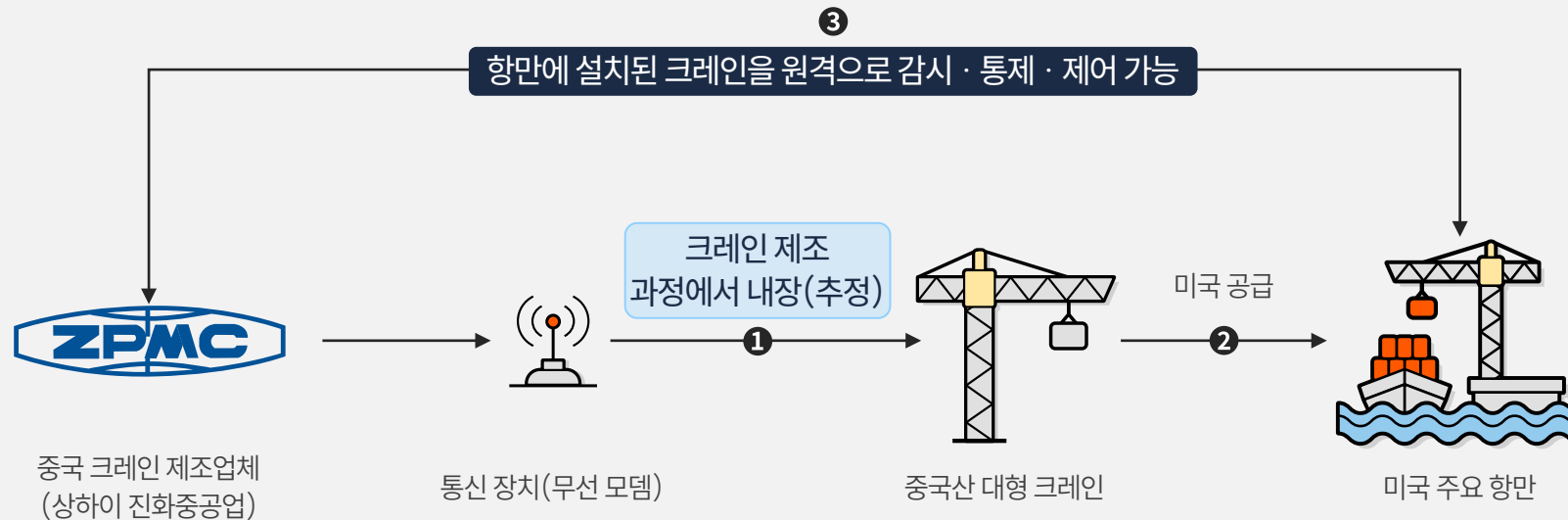
백도어 사례 (USB 장치 : 미국 국가안보국 킴 프로그램)

- ① 미국 국가안보국(NSA)이 전 세계 10만대의 PC에 소프트웨어를 심어 정보를 빼내거나 사이버 공격에 활용(뉴욕타임즈 2014.01.14 보도)
- ② USB 장치(COTTONMOUTH-1)를 통해 타겟 PC안에 악성소프트웨어를 업로드, 장치가 발산하는 무선 주파수(RF)로 무선백도어 실행
- ③ 중국 해킹부서, 러시아군, EU 무역 담당 부처, 멕시코 경찰, 사우디아라비아, 인도, 파키스탄 등의 컴퓨터 네트워크에 설치



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

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



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 (생략)
- ④ 누구든지 정당한 사유 없이 정보통신망의 정상적인 **보호·인증 절차를 우회**하여 정보통신망에 **접근할 수 있도록 하는 프로그램이나 기술적 장치** 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하거나 이를 전달·유포하여서는 아니 된다.

무선백도어 공격에 대한 대비로 금융권 정보 탈취 사전 방지 시스템 주문

국정감사 '정무위원회' 금융감독원 감사中 (2019.10.08)

김선동 의원 국내 은행하고 증권사의 무선 네트워크 정보 탈취 이런 부분들을 **무선백도어 침입**이라고 편의적으로 말씀드릴 수 있는데 ... 실제 무선백도어가 가능하기... 내부 전산실 침입을 하려고 그러면 **스파이칩을 심거나 스파이칩이 내장된 전산장비를 설치하면 무방비 상태**로 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...

윤석현 예, 저희들이 잘 모니터링을 하도록 하겠습니다.
금융감독원장

「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

군 내부망 해킹 보안을 위해 무선 통신 가능 전 주파수 대역 보안 시스템 촉구

국정감사 '국방위원회' 국방부 감사中 (2019.10.21)

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

정경두 예. 알겠습니다.
국방부장관

무선백도어 보안 솔루션



무선백도어 해킹 탐지 시스템

Alpha-H

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

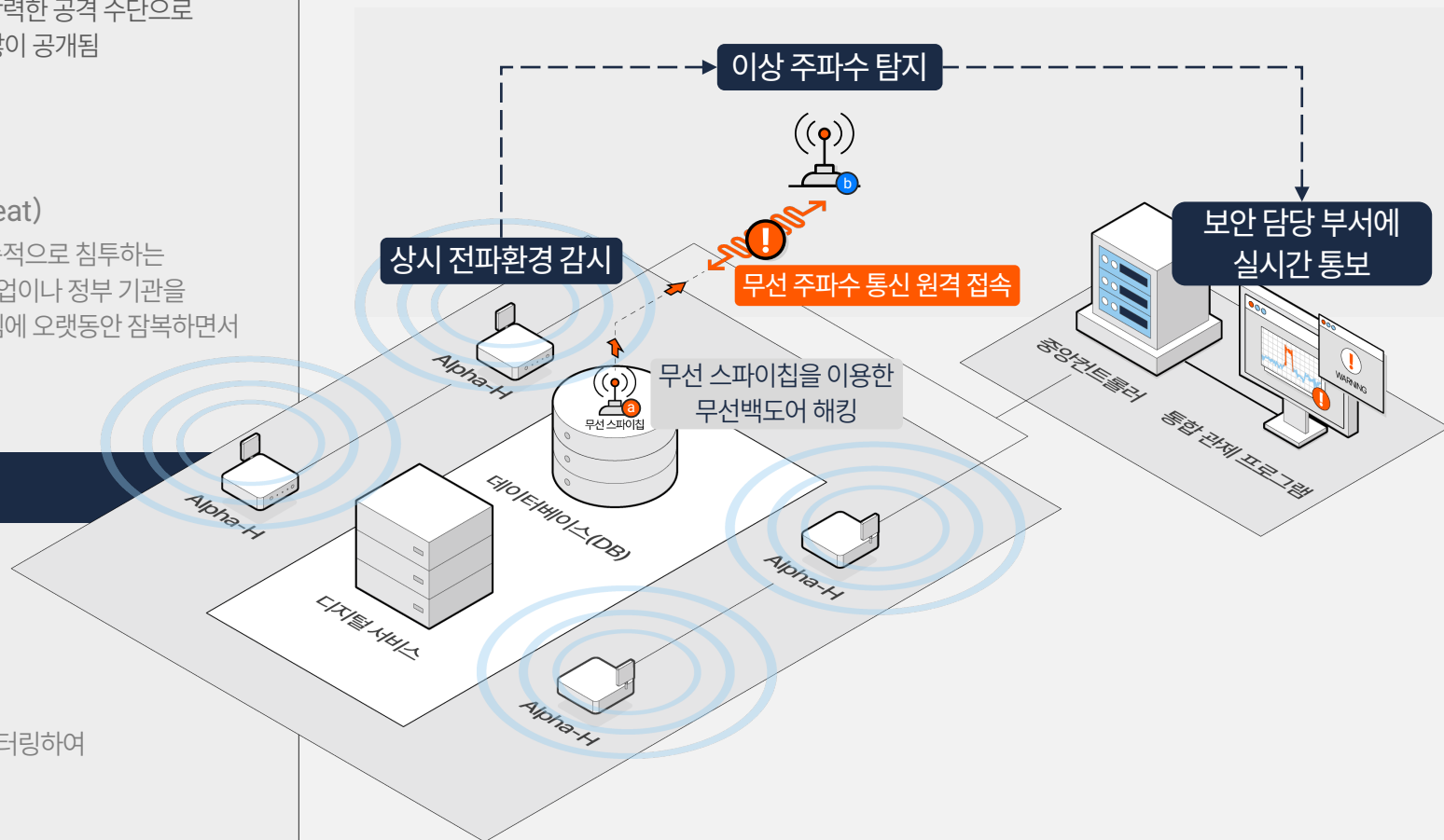
고도로 조직된 그룹이 특정 목표에 장기간 지속적으로 침투하는
사이버 공격. 정치적, 경제적 목적으로 특정 기업이나 정부 기관을
대상으로 하며, 은밀하게 진행하여 목표 시스템에 오랫동안 잠복하면서
데이터 탈취, 중요 서버 공격

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



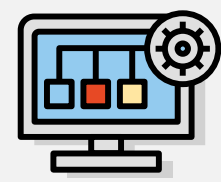
24시간 상시 탐지

보안의 빈틈을 없애는
24시간 365일 상시형 탐지 시스템



위치 추정

이상 주파수의 신호원 위치 추정으로
무선백도어 해킹에 신속 대응

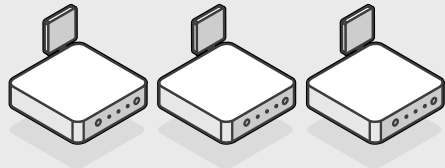


통합 관제

다수 탐지단말기
통합 관리·관제

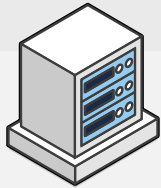
Alpha-H 운용 프로세스

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,
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

제품군

제품 이미지

제품명

제품 소개

무선도청 보안



Alpha-I

스마트 무선도청 상시 방어 시스템

집무실, 회의실, VIP실 등 중요장소에 설치되어
인공지능(AI)으로 침단 도청을 24시간 자동 탐지



Alpha-S

상시형 무선도청 탐지 시스템

집무실, 회의실, VIP실 등 중요장소에 설치되어
24시간 365일 실시간으로 무선도청을 자동 탐지

무선백도어 보안



Alpha-H

무선백도어 해킹 탐지 시스템

서버실, 관제실, 집무실 등에 침투되어 망분리 체계를
무력화시키는 무선백도어를 실시간 탐지

불법촬영 보안



Alpha-C

상시형 불법촬영 탐지 시스템

화장실 등 프라이버시가 중요한 공간에 설치되어
24시간 365일 불법촬영(몰카) 상시 탐지

수상 내역



대통령 표창

2020 제44회
국가생산성대상
미래유니콘기업부문



국방부장관상

2019 제3회 대한민국
스마트국방 ICT 산업박람회
우수제품 평가대회



행정안전부장관상

2018 안전산업진흥
유공 안전산업 활성화
및 안전관리 기여



산업통상자원부장관 표창

2022 제19회 대한민국
신성장 경영대상



방위사업청장상

2018 대한민국 스마트
국방·드론 산업대전 전시
참가기업 제품 평가대회



조달청장 표창

제3회 조달의 날
2023 제4회 혁신조달
경진대회

인증 성과



조달청
우수조달물품



조달청
혁신제품 지정



중소벤처기업부
성능인증



품질경영관리시스템
ISO9001 인증



조달청
벤처나라지정

INNOBIZ
기술혁신형중소기업

중소벤처기업부
이노비즈 선정