급증하는 무선백도어 해킹 위협 : 제로트러스트 관점에서 대처하는 방법 및 전략

Rising wireless backdoor hacking threats :
method and strategy to deal with them from a zero-trust perspective

Presenter

한동진(Dong-Jin Han)

㈜지슨 (GITSN, Inc.) 대표이사

전자공학 박사(Ph.D.)

- 前 ISO* 대한민국 전문위원
  (*ISO : International Organization for Standardization)
- 前 금융위원회 주관 금융권 망분리 TF 전문위원
- 現 차세대 교통인프라 융합산업연구조합(NTICA) 초대 이사장
- 現 ㈜지슨(GITSN, Inc.) 대표이사

'광대역 불법 무선신호의 탐지 방법'(특허 10-1641112)

'복수의 전파탐지장치를 이용한 무선해킹 스파이칩 위치 추정 시스템 및 그 방법'(특허10-2271797)등 국내·외 특허 26건

무선백도어를 이용한 해킹 및 대응법(2022) 한국군사과학기술학회 논문

영화 <미션임파서블4> 中 서버실에 잠입해 USB를 꽂아 무선백도어 공격을 시도하는 장면(미션임파서블4, 2011)

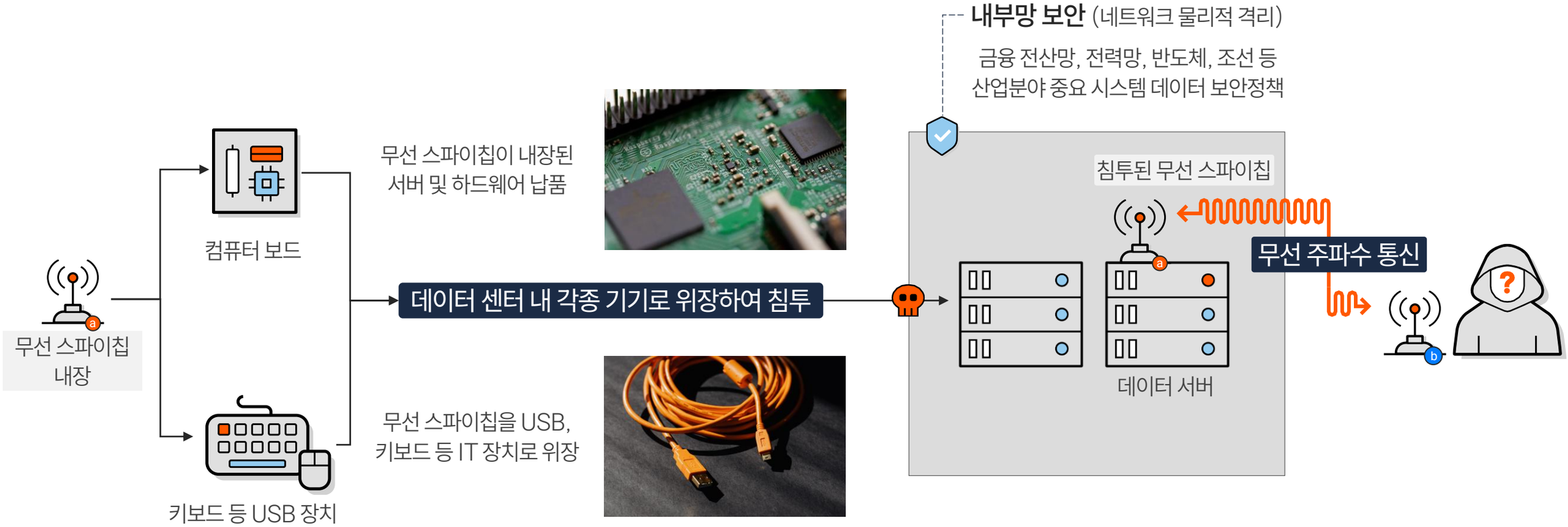
무선백도어 특징

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

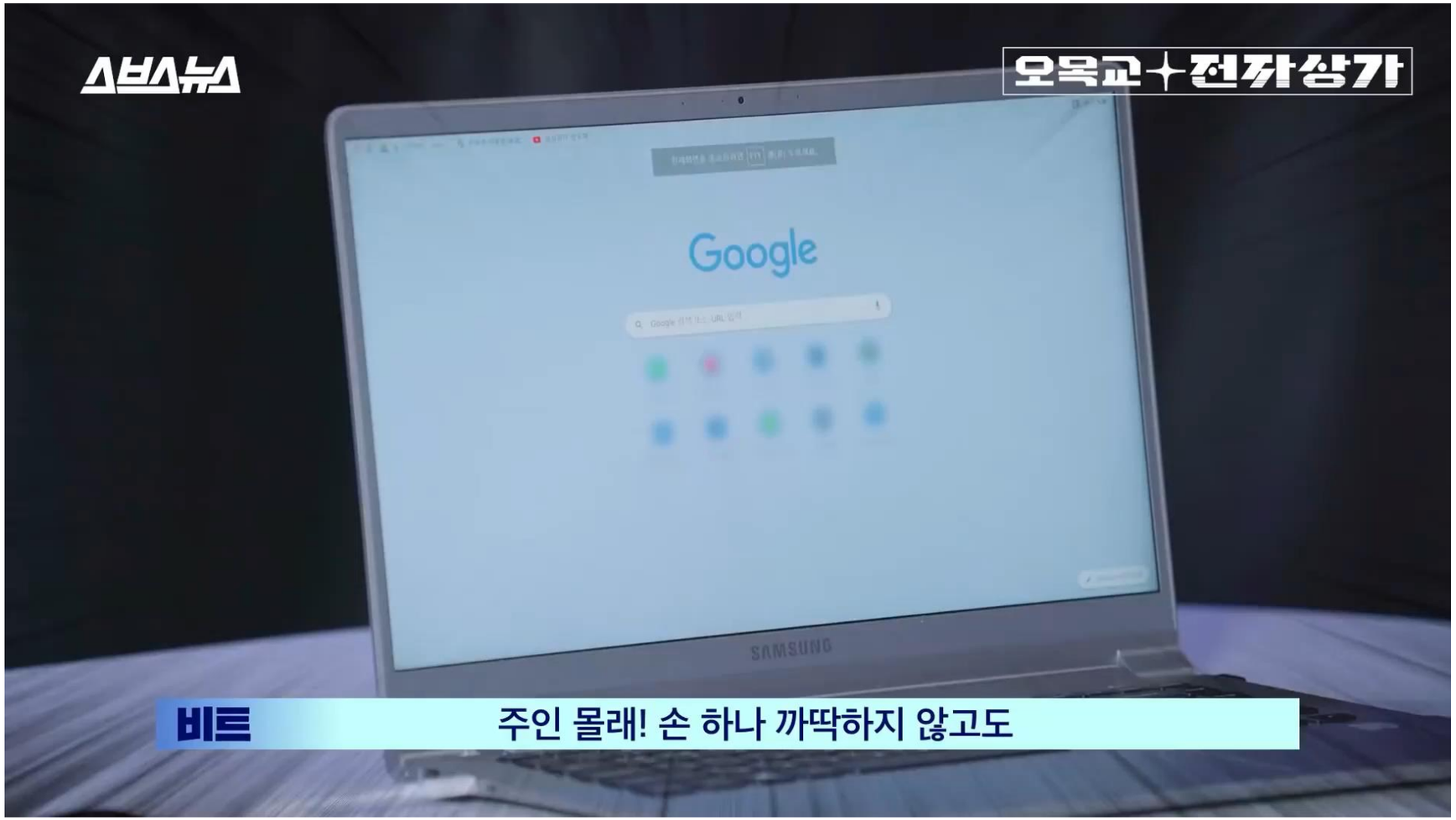
② 무선 주파수 통신으로 타겟 시스템 원격 접속(수 km밖에서 무단 침입)하여 데이터를 탈취하거나 시스템을 붕괴시키는 신종 해킹

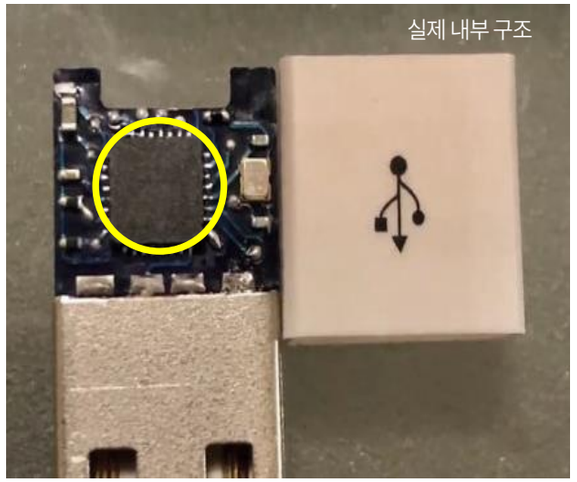
③ 기존의 보안 솔루션으로는 방어 불가능 망분리 시스템(내부망) 무력화 WIPS, 방화벽 등 기존 보안체계 우회

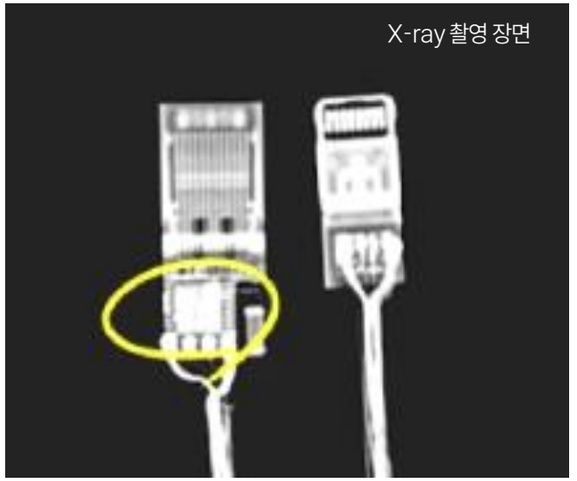
④ 매우 높은 수준의 접속 권한 획득 - 고부가가치 데이터 탈취, 사이버 테러로 인한 혼란 우려



‘해킹 칩’을 숨겨 충전 케이블로 위장한 무선백도어 스파이칩 언론 보도(스브스뉴스, 2021.10.05)







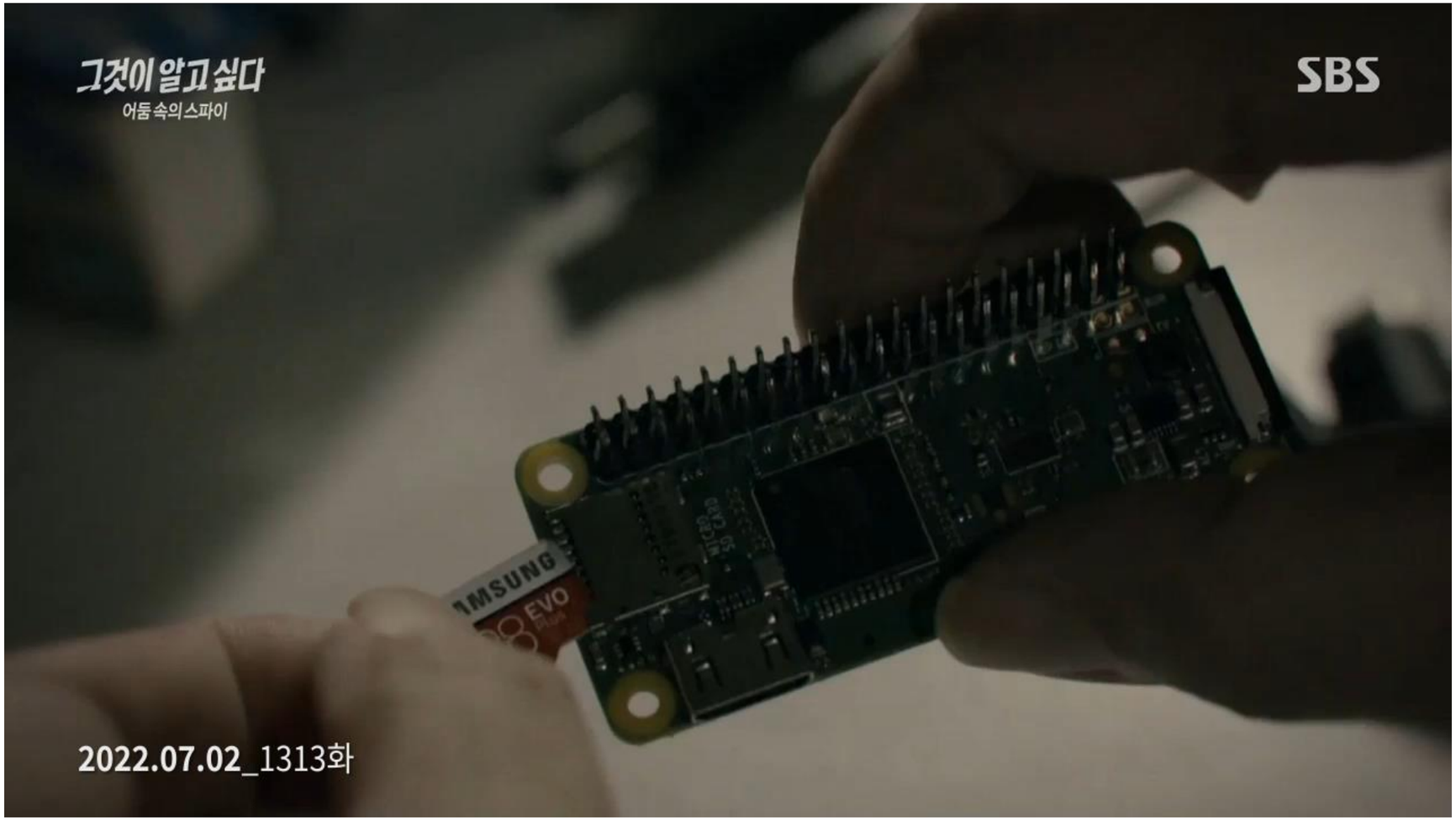
백도어 사례 (USB 장치 : 한국군 합동지휘통제체계 서버 해킹 시도)

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

<그것이 알고 싶다> 1313화 포이즌탭 (SBS 그것이 알고 싶다, 2022.07.02)

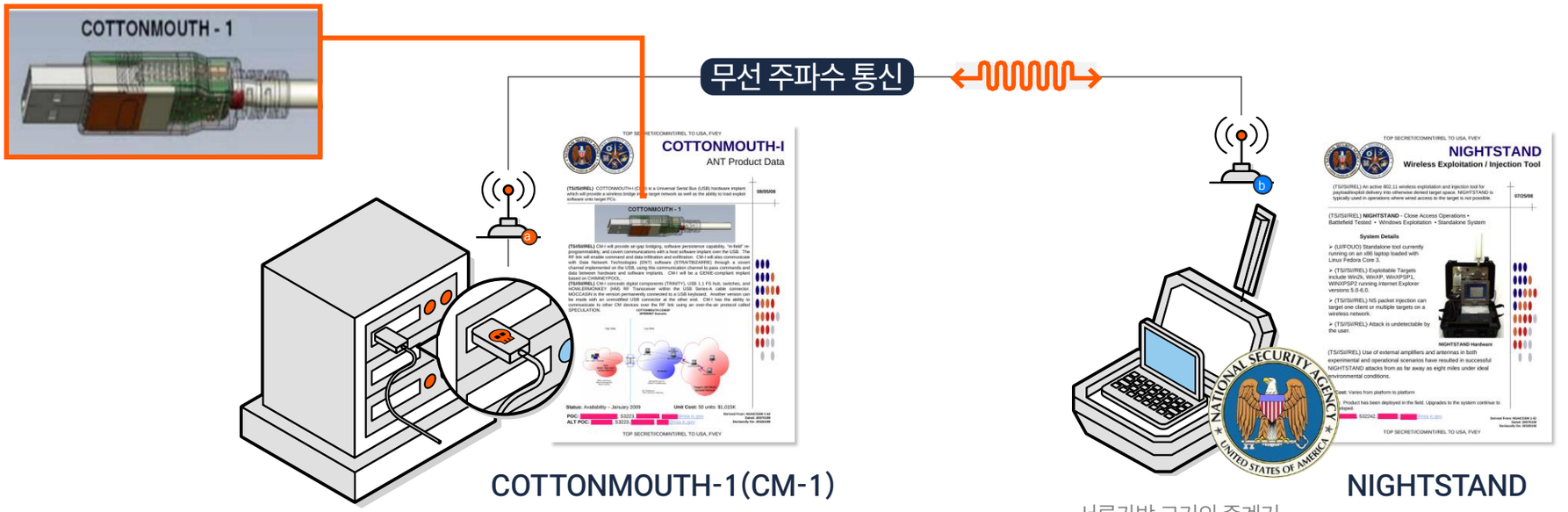


백도어 사례 (USB 장치 : 미국 국가안보국 퀀텀 프로그램)

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

② USB 장치(COTTONMOUTH-1)를 통해 타겟 PC안에 악성소프트웨어를 업로드, 장치가 발산하는 무선 주파수(RF)로 무선백도어 실행 (8 mile,13 km)

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

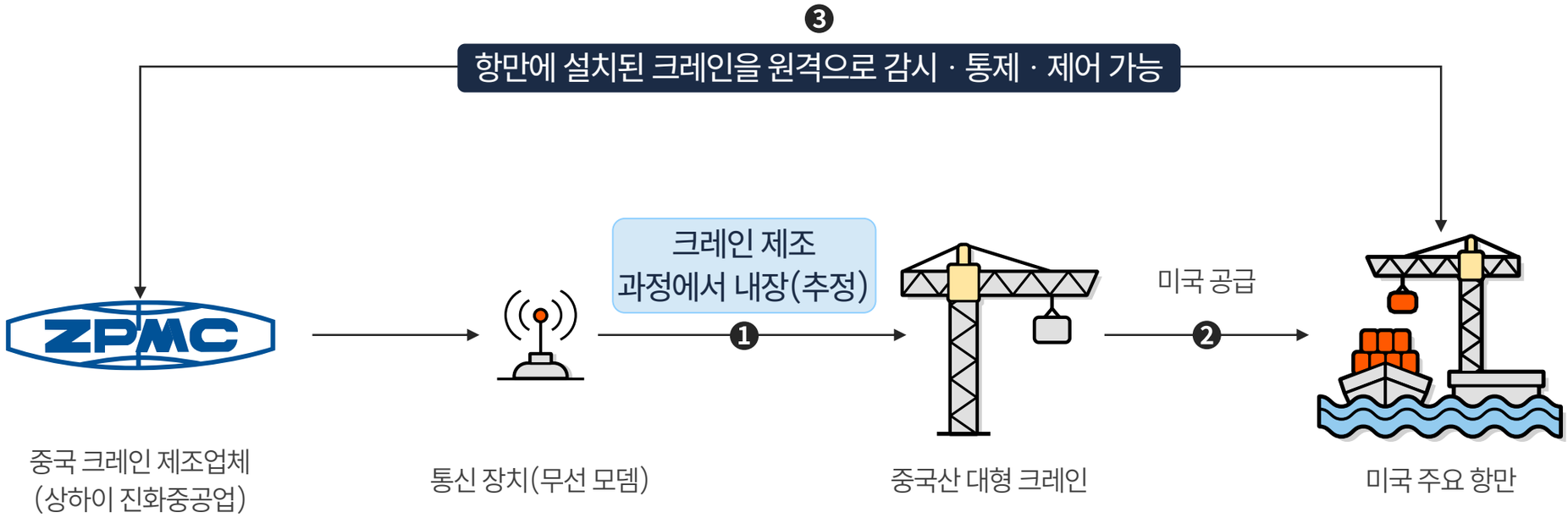
백도어 사례 (공급망, 보드: 중국산 대형 크레인 내 통신장치 발견)

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

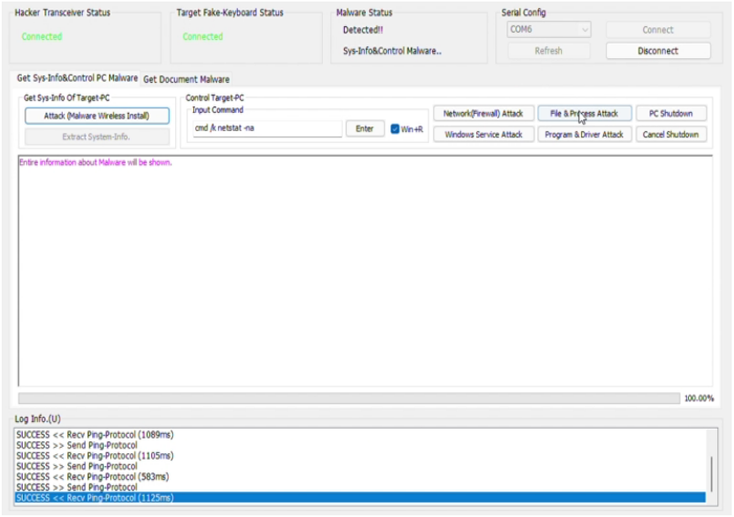
④ 바이든 행정부 외국산 크레인을 미국산으로 대체할 계획 발표

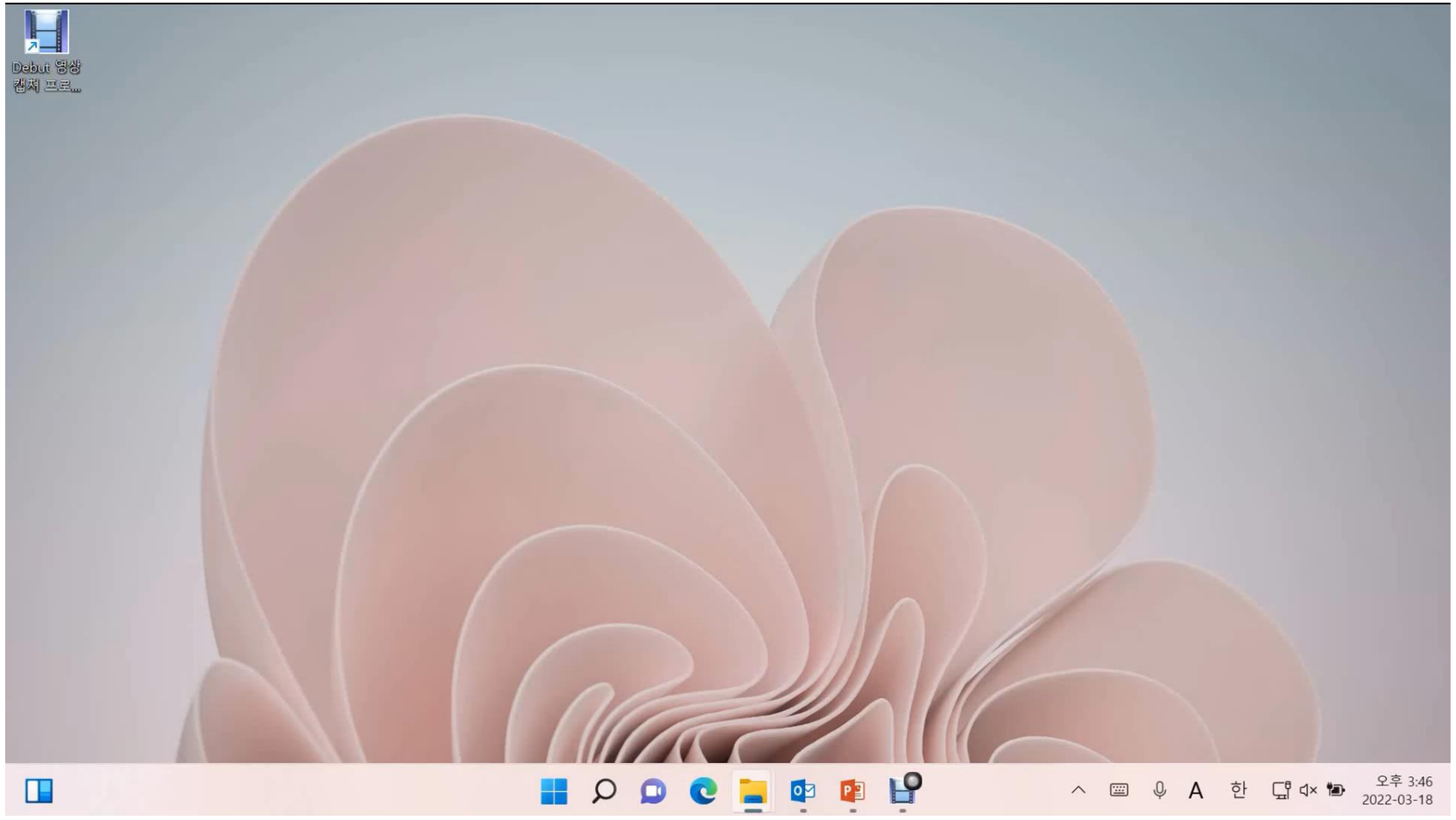


항만 크레인에 기상 관측기까지… 계속되는 중국산 장비 '정보 유출' 논란 (TV조선, 2024.09.26)

시험용 무선백도어 해킹 스파이칩 시료(키보드 위장형) 구동 화면

무선백도어 해킹 스파이칩 시료(키보드 위장형)





무선백도어 해킹으로 인한 치명적 피해

무선백도어 해킹 공격은 다양한 보안기술이 적용된 공간에 침투하여 **수십 킬로미터 떨어진 거리에서도 해킹을 통한 정보 탈취 및 시스템 파괴** 가능

① 내부 전산망 붕괴

주요 서버 공격을 통해 시스템 설정 변경, 네트워크 장비 제어 권한 등을 탈취해 전산망 기능 마비

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

운영체계 변경을 통해 보안설정을 약화시킨 후 고객 개인 정보에 무단 접근 및 수정, 삭제

③ 시스템 침해 및 정보 무단 수정

내부 시스템에 침투하여 정보를 무단으로 수정 및 삭제하는 등 주요 데이터를 조작하여 경영판단에 영향

④ 기업 자산 손실 및 신뢰도 하락

중요 데이터 유출 혹은 시스템 손상으로 인해 재정적 손실 및 기업 신뢰도 하락 발생

제로 트러스트로의 보안 패러다임 전환

치명적인 피해 수준에도 불구하고 무선백도어 해킹 공격은 기존 경계 기반 보안 시스템에서는 탐지조차 어려워

제로 트러스트로의 보안 패러다임 전환이 필요한 시기

제로 트러스트(Zero Trust)의 핵심 개념은 “아무도 신뢰하지 않고 모든 것을 지속적으로 검증한다”

무선 백도어 해킹에 이용될 수 있는 **주파수 전 대역**에 대해 제로 트러스트 개념을 적용하여 **지속적인 감시와 검증 필요**

무선 보안 강화를 통한 제로 트러스트 보안 모델 효과 상승

해킹이 발생할 수 있는 주파수 전 대역의 실시간 감시를 통해 비인가 주파수 신호를 조기에 탐지하고 대응하여 제로 트러스트 모델의 보안 효과 강화

기 운영 중인 무선 방어 시스템(WIPS)의 사각지대를 해소하고, IoT 기반의 초소형 스마트칩을 내장한 무선백도어 칩에 대응

정보 유출 방어 및 컴플라이언스 준수

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제4항* 신설에 따라, 신종 위협인 무선백도어 해킹을 차제에 예방하고 대응

무선백도어 해킹이 발생할 수 있는 주파수 대역(1MHz~3GHz)에서 침해사고 위협 방어

무선백도어 공격에 대한 방어대책 촉구

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부 개정 (2024.1.23)

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 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 금융감독원장 — 예, 저희들이 잘 모니터링을 하도록 하겠습니다.

군 내부망 해킹 보완을 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 국방부장관 — 예. 알겠습니다.

무선백도어 보안 솔루션

무선백도어 해킹 탐지 시스템

Alpha-H

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

무선백도어 해킹 탐지 시스템 Alpha-H

무선 스파이칩 전파 탐지

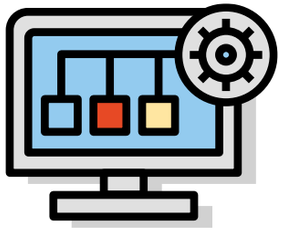
25kHz~3GHz의 주파수 대역을
스캔하여 무선백도어 해킹 탐지

24시간 상시 탐지

보안의 빈틈을 없애는
24시간 365일 상시형 탐지 시스템

위치 추정

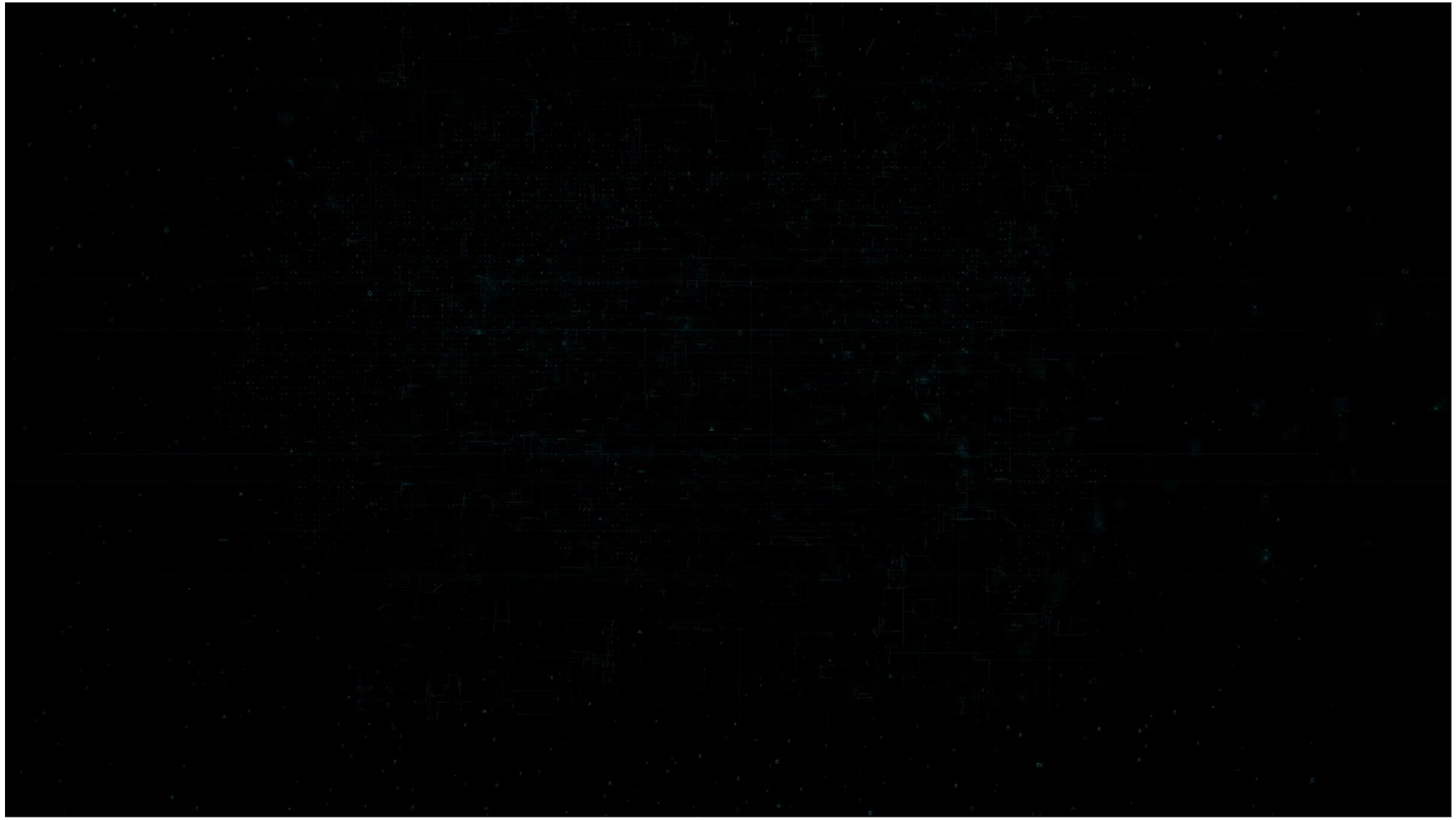
이상 주파수의 신호원 위치 추정으로
무선백도어 해킹에 신속 대응



통합 관제

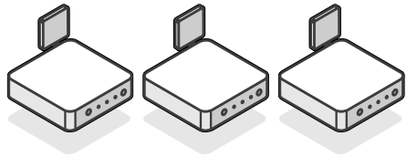
다수 탐지단말기
통합 관리·관제

무선백도어 해킹 탐지 시스템 소개영상



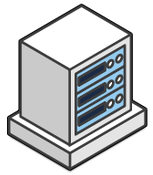
무선백도어 해킹 탐지 시스템 운용 프로세스

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 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

무선백도어 해킹 탐지 시스템 운용 기관

국내 (10개 기관)

국세청 | KDB산업은행 | 한국수출입은행 | KDIC 예금보험공사 | 대한민국해군 REPUBLIC OF KOREA NAVY

우리은행 | 신한은행 | KB 국민은행 | SAMSUNG 삼성SDS | Kdn 한전KDN|주|

해외 (4개국)

보츠와나

미국

영국

싱가포르