**https://krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/#more-69445**

<큰 틀>

**FBI 경고**: 경찰 및 정부 이메일 계정 해킹 증가.

**위조 긴급 데이터 요청(EDR)**: 법적 승인 없이 고객 데이터 요구.

**기업의 딜레마**: 요청 진위 판별 어려움, 높은 응답률.

**사이버 범죄 수법**: 계좌 동결 및 자금 이동 시도.

**취약한 보안**: 피싱, 악성코드로 이메일 해킹.

**Kodex의 역할**: 가짜 EDR 검출 및 예방 강화.

**FBI 권고**: 보안 강화, 피싱 저항형 다중 인증 필요.

**FBI: 해킹된 경찰 이메일과 위조된 긴급 데이터 요청(EDR) 증가**

FBI 전 세계 경찰과 정부 기관에 시스템 보안 강화 촉구

사이버 범죄자들 해킹된 경찰 이메일 계정 이용 => 긴급데이터 요청

미국) => 연방, 주 , 지방의 법 집행 기관 => 기술 제공업체의 계정 정보 요청시 공식적인 법원 명령이나 소환장 제출 필요

대규모 사용자 기반을 보유한 회사들 이런 요청 처리하는 부서 가짐 => 요청이 실제 경찰 도메인 이름처럼 보이고 적법한 서류 제출시 => 대체로 요청 수락

**위조된 EDR과 사이버 범죄**

일부 사이버 범죄자들 => 법원의 승인 받은 소환장 위조 => 해킹된 경찰 or 정부 이메일 계정으로 보냄

But 최근 => 긴급 데이터 요청(EDR) 활용 사례 증가

( EDR : 사람이 신체적으로 해를 입거나 사망할 가능성이 있다고 가정해 계정 데이터 )

그로 인한 문제점 : EDR이 공식적인 검토 절차를 거의 거치지 않음 => 즉각적 미대응시 누군가의 생명 위험 생길 우려 & 잘못된 요청에 응답시 고객 정보 유출 위험성

결과적으론 응답률 높음 ( 90% 이상 )

**사이버 범죄자들의 활동**

‘Pwnstar’ or ‘Pwinpotent’ 라는 별명을 사용하는 영어권 사이버 범죄자 => 범죄 포럼에서 위조된 EDR 서비스 판매 중 ( 25개국 이메일 소유 / 한 번 요청당 1000~ 3000달러 요구)

“주문 100% 성공 보장은 못 해도 에스크로 가능하고 실패시 전액 환불 해드립니다”

다른 범죄자들 => 특정 소셜 미디어 플렛폼으로 위조 능력 판매 / 일부 => 해킹된 이메일 계정 판매 & 구매자가 필요한 문서 위조하도록 함

**Kodex의 역할**

다른 가짜 EDR 서비스 => Kodex라는 스타트업에서 해킹되거나 위조된 계정 판매 주장

Kodex => 가짜 법 집행 데이터 요청 => 더 효과적으로 선별하는 걸 돕는 것이 목표

=>데이터 제공자와 직접 협력 -> 경찰 or 정부 관계자 요청 정보 통함 -> EDR 식별 쉽게 만듦

Ex) 1.고객 기록 요청시 먼저 Kodexglobal.com 계정 등록

2. Kodex 시스템 => 요청자의 과거 기록에 따라 신용 등급 부여ㅑ

3. 정당한 법적 요청 지속적이었으면 높은 점수

Kodex의 성과 => 12개월동안 1,579건의 EDR 처리 / 30%인 485건이 2차 검증 통과 못함 / 4,000명의 법 집행 사용자 계정 중단 시킴

60개 이상의 기술 회사가 법 집행 데이터 요청을 Kodex를 통해 처리 중

Donahue(kodex 창립자 / 2021년 FBI 요원 활동) 의 우려

* 범죄자들 => 가짜 법 집행 요청을 사용해 특정 계좌 동결 or 자금 압류 시도

Ex) 해커 => 해킹된 정부 이메일 계정을 사용해 제공업체에 특정 은행이나 암호화폐 계좌에 대한 동결 요청 보낼 수 있음 / 몇 주 후 같은 범죄자가 다시 계좌 내 자금을 정부 조사관이 통제하는 보관 지갑으로 이체하라고 보냄

소셜 엔지니어링 관점) : 누군가와 관계 맺을수록 당신이 신뢰함 / 동결 명령을 보내는 것은 신뢰를 쌓는 방법

**FBI의 보안 권고**

Donahue – 미국 및 기타 국가의 다수 경찰 기관이 보안 위생이 부족하다고 지적 /

피싱 저항형 다중 인증(MFA)등 기본적인 계정 보안 조치 강화할 것 권고

사이버 범죄자들 => 경찰과 정부 이메일 계정에 접근하는 주요 수단 => 여전히 이메일 피싱 & 악성코드 감염 => 계정 정보 다크웹에서 판매

FBI => 전세계 많은 경찰 기관들 => 사이버 보안 위생 매우 열악한 상태 다시 강조