택배 사칭 스미싱 급증과 대응 체계

APK 설치 유도형 공격의 진화

요 약

택배 배송 실패를 사칭한 스미싱 문자가 급증하고 있다. 단축 URL로 연결되는 랜딩 페이지는 정상 택배사 사이트를 그대로 복제한 형태로 육안 구분이 어렵다. 최근에는 APK 설치를 유도해 SMS 수신 권한을 탈취하고 인증번호를 가로채는 사례가 확인됐다.

1. 공격 패턴

발신 번호는 대부분 변작되며, 도메인은 신규 등록된 저가 TLD를 사용한다. 문자 본문은 수취인 이름을 포함해 신뢰도를 높이는 방향으로 정교해지고 있다.

2. 피해 확산 구조

설치된 악성 앱은 주소록을 수집해 동일 문자를 추가 발송하며, 이 과정에서 지인 발신으로 위장되어 클릭률이 크게 상승한다.

3. 이용자 권고

문자 속 링크 대신 공식 앱에서 직접 조회하고, 출처를 알 수 없는 앱 설치를 차단한다. 통신사 번호 도용 방지 서비스와 소액결제 차단을 함께 신청한다.

4. 사고 발생 시

118 또는 112에 신고하고 통신사에 소액결제 차단을 요청한다. 기기 초기화 전 증거 보전이 필요한 경우 전문 기관에 문의한다.