카드사 사칭 신종 스미싱 분석 결과

('23.10.18., 모바일보안팀)

1. 개요

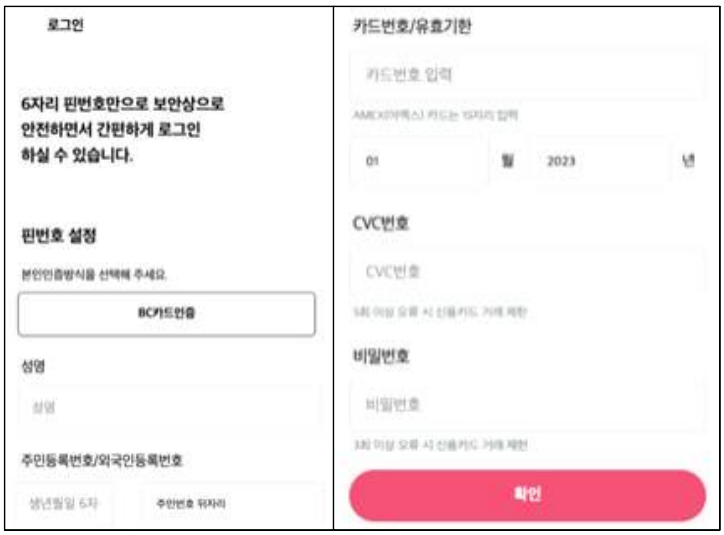
□ 최근 통신사에서 제공받은 스미싱 메시지 분석 과정에서 개인정보와 카드정보를 탈취하는 새로운 유형의 피싱사이트를 발견하여 분석한 결과를 공유

2. 주요 내용

□ **(스미싱 문자)** 문자메시지는 카드사를 사칭해 링크를 클릭하도록 유도하는 문구와 피싱 사이트 링크로 구성됨

스미싱 문자 내역
[Web발신][BC카드] 귀하의 BC 카드가 정지되었습니다. 여기에서 다시 활성화하십시오. https://bc-cardkr.com/s/?i7327
[Web발신][KB 국민카드] 당신의 은행 카드가 정지되었습니다 https://kb-card.com/l/?i5426
[Web발신][BC카드] 계정을 활성화해야 합니다. 그렇지 않으면 카드가 정지됩니다. https://bccardkr.com/s/?i5426

□ **(피싱 사이트)** 메시지에 포함된 링크에 접속할 경우 정보를 입력할 수 있는 페이지가 로드되고, 정보를 입력하고 확인 버튼을 누르게되면 입력된 정보가 공격자에게 전달됨



□ **(예상되는 피해) 모든 정보**(이름, 주민등록번호(외국인등록번호), 카드번호, 유효기간, CVC번호, 비밀번호)를 **입력**하도록 **유도**하고 있어 **부정결제**와 **카드정보를 사용하는 자격증명**에 악용될 **가능성**이 **매우 높음**

3. 스미싱 관련 침해 지표

□ (피싱 사이트)

도메인	도메인 등록일	IP정보
https://bc-cardkr.com	2023.10.16.	Cloud Flare 서비스 사용으로 확인 불가
https://kb-card.com	2023.10.13.	
https://bccardkr.com	2023.10.14.	