Headline

크리덴셜 스터핑 공격과 단계별 대응 전략

ICT 관제사업팀 박남춘 수석

■ 개요

최근 국내기업·기관들을 대상으로 한 크리덴셜 스터핑(Credential Stuffing) 공격이 고도화되면서 관련 사이버 위협이 크게 늘고 있다. 지난해 6~7 월 국내 대표 구인·구직 사이트 한국고용정보원의 '워크넷'은 크리덴셜 스터핑 공격을 받아 23 만 6,000 여 명의 개인정보가 유출됐다. 한국장학재단 홈페이지도 동일한 방식에 의해 3 만 2,000 여 명의 개인정보가 새어 나갔다.

크리덴셜 스터핑은 공격자가 노출 또는 유출된 사용자의 아이디(ID)/비밀번호(PW) 등 계정정보를 대규모 DB(Database)로 구축한 후, 여러 웹(Web)/앱(App) 서비스에 무작위로 대입하여 로그인을 시도해 개인정보나 자료를 유출하는 공격 방식이다. 최근 다수의 기업과 기관에서 자동화 기술을 활용한 크리덴셜 스터핑 공격이 발생하며 사회적으로 중요성이 대두되고 있는 만큼, 이번 헤드라인 리포트에서는 크리덴셜 스터핑 공격 피해사례와 대응 전략에 대해 설명하고자 한다.

크리덴셜 스터핑은 정보통신망법[1]에서 정의한 제 48 조 항목에 따라 불법적인 행위로 판명이 되며, 불법적인 프로그램 사용도 금지된다.

정보통신망법 제 48 조 정보통신망 침해행위 등의 금지
① 누구든지 정당한 접근권한 없이 또는 허용된 접근 권한을 넘어 정보통신망에 침입하여서는 아니 된다 * 5 년 이하의 징역 또는 5,000 만 원 이하의 벌금

크리덴셜 스터핑에서 공격자는 다크웹 등에서 획득한 인증정보를 사용해 여러 사이트에 동시다발적으로 로그인을 시도한다. 대부분의 사용자들이 여러 계정에서 동일한 비밀번호를 사용하는 경향이 있기 때문에, 단 한 곳의 로그인 정보가 유출되어도 문제가 발생할 수 있어 각별한 주의가 필요하다. 특히, 최근 개인정보 유출 사고가 발생하거나 해킹사고가 늘어나면서 크리덴셜 스터핑 공격의 성공 확률도 함께 높아지는 경향을 보이고 있어 더욱 주목할 필요가 있다.

크리덴셜 스터핑은 정상적인 로그인으로 보이기 때문에 공격 패턴을 식별하고, 완벽하게 차단하기 어려운 특성이 있다. 따라서 공격에 의한 데이터 도용, 계정탈취, 기타 부정행위를 막기 위해서는 안전한 비밀번호를 사용하고 악성 소프트웨어에 감염되지 않도록 주의하며, 보안 솔루션을 업데이트하는 등의 조치를 취해야 한다.

[1] 정보통신망법: 정보통신망 이용촉진 및 정보보호 등에 관련 법률

■ 크리덴셜 스터핑 피해사례

아래 표는 최근 국내에서 발생한 크리덴셜 스터핑 공격 피해 사례를 정리한 내용이다. 피해 대상들은 모두 노출 또는 유출된 개인정보를 통해 공격을 당했다. 시스템 오류, 개인정보 유출 등의 1 차 피해와 함께 과징금과 과태료 등 금전적인 피해도 추가로 발생했다.

일자	대상	내용
24 년 01 월	온라인 교육	· 크리덴셜 스터핑 공격과 게시판 내 XSS(Cross-Site Scripting) 공격으로 회원 X 만 X 천 명 개인정보 유출 · 사전에 확보한 아이디, 비밀번호를 악용한 크리덴셜 스터핑 공격으로 회원 A 의 계정탈취, 회원 A 의 계정을 통해 불법이용 신고 게시판에 악성 스크립트를 삽입하여 추가 개인정보 유출
23 년 11 월	복권 사이트	· 회원 비밀번호 변경을 통한 부정 로그인 발생 · 개인정보(이름, 생년월일, 전화번호, 이메일, 가상계좌) 유출 · 피해가 확인된 회원들의 비밀번호 초기화 선 조치 수행
23 년 10 월	스포츠사이트	· 아시안 게임의 한국 vs 중국 축구 8 강전에서, XX 스포츠의 클릭 응원 서비스의 중국팀 응원 90% 이상 · 로그인 없이 응원 클릭 가능하여, 해외 IP 2 곳에서 매크로를 통한 응원 클릭
23 년 07 월	커피전문점	· 크리덴셜 스터핑 공격으로 앱에 무단 로그인하여, 고객(회원)의 충전금 결제 · 현금화가 쉬운 텀블러를 주로 구매, 사측에서는 충전금 전액 보전 · 로그인 혹은 거래 단계에서 별도의 이차인증 없음
23 년 07 월	취업정보 사이트	· 중국 등 해외 IP 에서 XX 만여 건의 무단 로그인을 통한 개인정보 유출 · 이름, 성별, 출생연도, 주소, 일반전화 외 13 개 등록된 개인정보 유출

표 1. 국내 크리덴셜 스터핑 공격사례

■ 크리덴셜 스터핑 예시

최근 크리덴셜 스터핑 공격은 지능화되고 있는 추세다. 기존과 같이 단순히 ID/PW 입력을 통한 해킹뿐 아니라 원하는 정보를 얻기 위해 아래와 같이 다양한 공격을 시도하고 있다.

- 특정한 API 값/페이지/파라미터를 대상으로 다양하게 입력값을 지속적으로 대입하여 응답을 확인하는 공격

- 특정한 목적을 가지고 공격을 하는 형태이며, 다양한 지점을 통해 공격이 시도되고 있음(로그인 전/후 형태, 정상적인 서비스 로직을 악용, 서비스를 위한 지원기능 악용 등)

- 대량의 파라미터 취약점을 이용한 변조 및 SQL Injection 공격 등도 크리덴셜 스터핑 공격으로 분류할 수 있음(반복적인 수행의 응답/결과값을 통해 유니크한 패턴을 인지, 정보의 정합성을 체크)

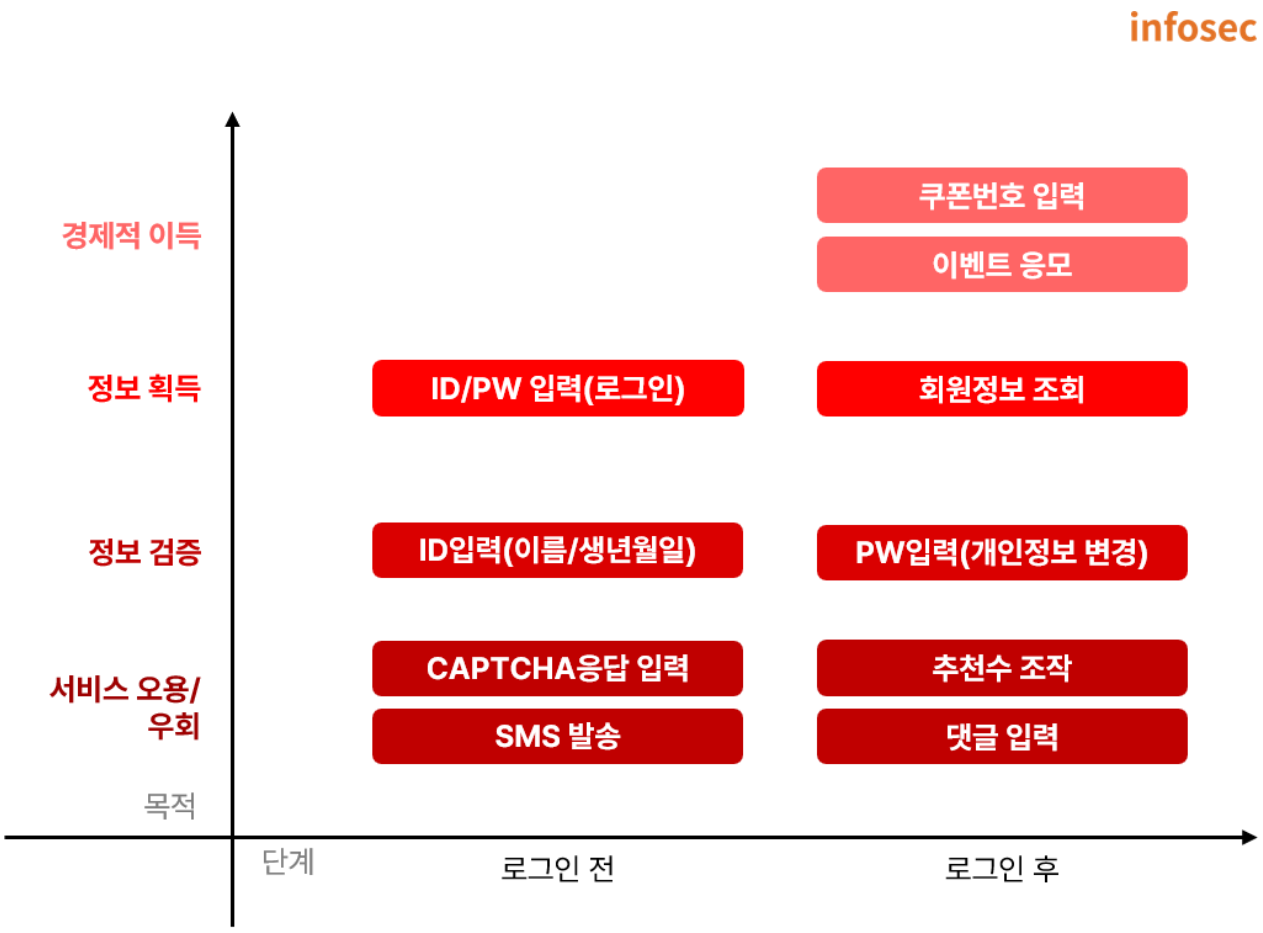

그림 1. 다양한 서비스 지점에 대한 공격 예시

■ 크리덴셜 스터핑 단계별 대응전략

크리덴셜 스터핑 공격 발생 시 보안 담당자가 진행할 수 있는 대응 방안들에 대해 단계적으로 정리했다.

1. 공격자의 목적 및 현황파악
- 크리덴셜 스터핑 공격이 시도되는 페이지의 용도가 무엇인가? : 해당 페이지를 통해 공격자가 확인이 가능한 정보(개인정보) 파악 **- 조작(입력)되는 필드/파라미터, 응답 값은 무엇인가?** : 정합성을 체크하는 정보가 무엇인지 파악 : 입력값의 항목에서 개인정보는 어떠한 것들이 포함되어 있는지 파악 : 응답 값에 포함된 유니크한 정보가 어떤 것들이 있는지를 파악 **- 시도횟수/방식을 파악?** : 크리덴셜 공격인지 단순 공격인지를 파악 : 입력값의 순차적인 증감/문자열 추가 방식은 성공률이 낮음

2. 크리덴셜 스터핑 원천 차단대응 고려
- 사용자별 시도 횟수 제한을 통한 대응을 고려 : 사용자 구분 방법을 통해 시도 횟수를 제한 (로그인 세션, Src_IP, 로그인 전 세션, User-Agent 등) **- 무단 로그인에 대한 피해 방어** : 다중인증/복합인증을 통한 방어

3. 공격자 행위 방해 고려
- 공격 페이지(URL)에 대한 IP 별 접속 제한 방어 : App(서버) 단에서 구현이 어려울 경우, NW 보안 솔루션(ex. 전용장비)을 통해 구현 : AWS/Azure 에서 임계치 접속 차단 대응 기능 지원 : OnPrem 에서는 WAF, SSL 복호화 트래픽을 이용한 대응 **- CAPTCHA 구현을 통한 방어** : 회원가입, 본인인증 등 자주 발생하지는 않지만, 공격/이슈가 많이 발생하는 페이지는 무조건적인 캡챠 적용을 구현 : 일반적인 사용자의 자주 접속하는 페이지(ex.로그인 페이지)는 이상동작 감지 시, 캡챠 적용을 구현

4. 크리덴셜 스터핑 차단 우회 탐지기법 적용
- 차단 우회를 통한 접속 탐지기법 적용 : 자동이 아닌 수동방식을 통한 캡챠 우회 시도 탐지 필요 **- 탐지 및 분석기법 (ex.예시)** : 특정 페이지만 접속하는 경우 : HTTP Header 를 변경하여 접속하는 경우 : 지속적인 대입공격 탐지 (긴 시간 적은 수의 접속) : 필요시 IP 검색 기준을 C/B Class 단위로 확대 모니터링

5. 서비스 안정성 고려하여 대응
- 사용자가 많은 NAT IP 대역 : 1 인이 아닌, 다수 사용자의 정상접속을 인지 및 예외처리 **- 차단 대응 외 추가 대응방법 다양화 모색** : 캡챠 적용/추가 인증 : 사용자/관리자 대상 차단 정보 알림 : 차단 정책에 대해 일정 시간 이후 해제 방식

6. 사전예방 및 사후대응
- App 구현 시 대입공격에 안전하게 서비스 로직 설계 : 사용자 편의 보안기능 구현, 보호 프로세스 구현 **- 크리덴셜 스터핑 공격 시도에 대한 조치 시행** : 불법적인 이벤트 당첨 취소, 사용자 확인을 통한 경고 등 **- 다크웹 노출 계정에 대응** : 필요 시 다크웹 정보 제공 서비스를 활용한 자동화 대응 프로세스 구현 : 노출된 계정들에 대한 로그인 잠금/변경/안내조치

표 2. 크리덴셜 스터핑 단계별 대응전략

■ 맺음말

지금까지 크리덴셜 스터핑 공격 피해사례와 단계별 대응 전략에 대해 알아봤다.

크리덴셜 스터핑 공격을 당할 경우 개인정보 유출로 인해 타 서비스/다른 방식의 해킹 공격에 활용이 될 위험성 커 철저한 대비가 필요하다. 더욱이 피해를 입은 회사 또는 기관도 처벌의 대상이 될 수 있는 만큼 전사 차원에서 각별한 주의가 요구된다.

특히 AI 기술이 점점 발전하면서 이를 활용한 크리덴셜 스터핑 공격도 고도화되고 있다. 기존과 같이 단순 자동화 툴을 통한 공격이 아니라, 사람과 같은 임계치 방식을 적용해 공격할 수 있어 이에 대한 대비가 필요하다. 또한, 다크웹에서 개인정보 판매 및 계정 획득이 활발히 이뤄지고 있어 이와 같은 공격시도는 더욱 증가할 것으로 예상된다.

크리덴셜 스터핑 공격에 대응하기 위해서는 보안 관리자를 비롯해 개발자, 운영자 등 구성원들 간 긴밀한 업무 협업이 필수적이다. 가장 기본적으로는 잦은 비밀번호 교체, 다중 인증 사용 등 강력한 보안 정책을 실시, 확대해야 한다. 또한, 의심스러운 활동 탐지하기 위해 철저한 경계 모니터링을 진행해야 한다.

국내 정보보안 1 위 SK 쉴더스는 보안 사고를 예방하기 위해 맞춤형 보안 컨설팅을 제공하고 있다. 그 중에서도 특히, 모의해킹 컨설팅을 통해 크리덴셜 스터핑 공격을 예방할 수 있다. SK 쉴더스는 국내 최다 모의해킹 전문가를 확보하고 있으며, 차별화된 방법론과 축적된 기술력을 통해 맞춤형 서비스를 제공하고 있다. 최근에는 생성형 AI 챗 GPT 를 활용한 AI 모의해킹 시뮬레이션을 전개해 PC 나 웹 취약점을 파악하고 사이버 공격 활용 가능성을 탐지하고 있다. 이와 자세한 내용은 SK 쉴더스 홈페이지에서 확인할 수 있다.