Special Report

늘어나는 개인 정보 거래,

다크웹을 통한 크리덴셜 스터핑 대응법

■ 개요

다크웹[1]에서의 개인 정보 유출이 크게 증가하면서 크리덴셜 스터핑(Credential Stuffing)[2] 공격이 증가하는 추세이다. 2021년 Fortune 1000대 기업 침해 노출보고서에 따르면 다크웹 개인정보 거래량은 전년 대비 29% 증가했으며 크리덴셜 스터핑 공격 역시 증가하는 양상이다.

다수의 공격자가 크리덴셜 스터핑 공격을 시도하는 이유는 크리덴셜 스터핑이 비용 대비 효율적인 공격 방법이기 때문이다. 공격자가 크리덴셜 스터핑 공격으로 10만 건의 유효한 계정 정보를 탈취하는 비용은 200달러 미만에 불과하고, 이 비용 또한 점차 낮아지고 있어 크리덴셜 스터핑은 앞으로도 증가할 것으로 예상된다.

이번 Special Report에서는 다크웹의 개인 정보 거래 현황과 크리덴셜 스터핑의 위험성 및 대응방안에 대해 알아보고자 한다.

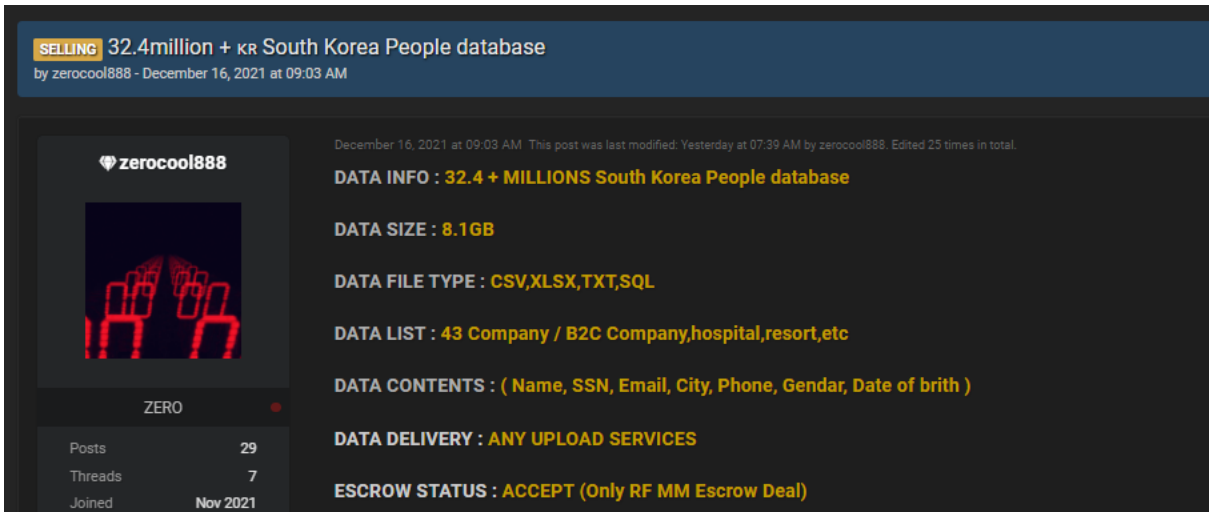
---

[1] 특정 브라우저나 소프트웨어를 통해서만 접근할 수 있는 인터넷 영역

[2] 이용자가 여러 웹사이트에 동일한 계정 정보를 사용하고 있다는 점을 이용, 유출된 계정 정보를 어플리케이션 로그인 폼에 대입하여 인증을 획득하는 공격

■ 다크웹에서 시작되는 크리덴셜 스터핑

개인정보의 거래가 이루어지는 블랙마켓[3] 또는 언더그라운드 포럼에서는 하루 평균 300~600건의 유출 데이터 판매 게시물이 꾸준히 업로드 되고 있다. 이 중에는 43개의 기업, 병원 등에서 탈취한 3,200만 건의 국내 개인 정보 판매 게시물을 포함하여 쇼핑몰, 이동통신사, 공공기관 등을 대상으로 획득한 약 4,000만 건의 판매가 이뤄지는 것을 확인할 수 있다.



[국내 계정 3200만 건 판매 글]

infosec

대상	내용
다수의 웹사이트	43개의 기업, 병원 등에서 탈취한 3,200만 건의 국내 개인정보 판매 글 게시. 이름, 주민등록번호, 이메일, 연락처, 생년월일을 포함(일부 비밀번호)
패션 쇼핑몰	국내 유니콘 기업의 고객정보 700만 건 판매 글 게시. 아이디, 비밀번호, 사진, 이메일 주소 등 포함
이동통신사	이동통신사 데이터베이스의 3만 개의 계정정보를 판매. 고객정보가 아닌 내부 직원의 이메일과 비밀번호로 확인
공공기관	대한민국 350개 공공기관 중 316개 기관, 총 59만 4,242건의 계정정보가 유출. 아이디와 비밀번호 포함

[다크웹 계정정보 유출 내역]

[3] 법에 저촉되는 물건을 암암리에 사고 파는 장소

이처럼 다크웹에서 거래되는 개인정보는 공격자에 의해 크리덴셜 스터핑 공격에 활용된다. 크리덴셜 스터핑의 성공 확률은 0.1~0.2%로 다소 낮은 수치로 보일 수 있지만, 위 사례와 같이 4,000만 건이 유출됐을 경우 그중 0.1 ~0.2%인 400~800만 건이 성공하기 때문에 낮은 수치라고 볼 수 없다.

크리덴셜 스터핑의 위험성은 단순히 개인정보 탈취에 그치지 않고 획득한 정보를 통해 추가적인 공격을 수행할 수 있다는 점에 있다. 크리덴셜 스터핑으로 발생할 수 있는 추가 공격 유형은 데이터 탈취, 사용자 사칭, 악성코드 유포, 피싱 및 스캠 등이 있다.

infosec

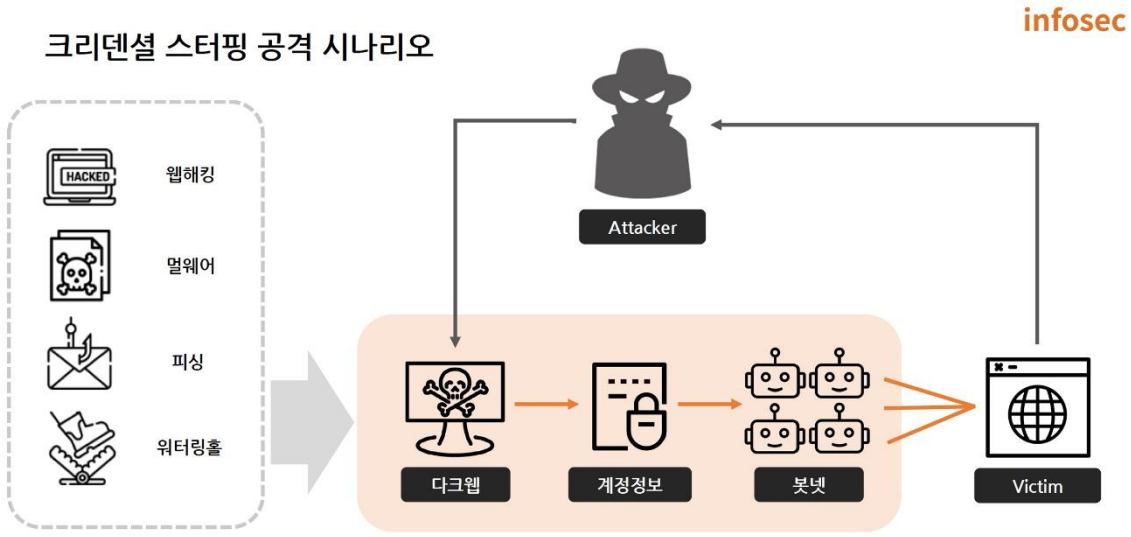
TakeOver	Abuse
A. 추가 개인정보 탈취 B. 사진, 영상 등 개인 데이터 탈취 C. 금전적 자산 남용 D. 사용자 사칭	A. 악성코드 유포 B. 인증 우회(기밀정보 탈취) C. 스피어 피싱 D. 스캠

[다크웹 계정정보 유출 내역]

실제 크리덴셜 스터핑 공격 사례를 살펴보자. 최근 국내 유명 메신저를 대상으로 대량의 크리덴셜 스터핑 공격이 발생한 것으로 추정되는 사건이 있었다. 악성코드에 의해 감염된 PC로부터 PC에 저장돼 있던 계정 7,971건이 다크웹에 유출됐고, 해당 계정 중 중복 계정을 제거 후 바로 활용할 수 있는 계정이 3,696건 존재했다. 그 밖에도 20년에는 유명 배우의 클라우드 계정이 해킹되어 개인적인 자료를 빌미로 금전을 요구하는 사건이 있다. 해커는 다른 웹사이트에서 유출된 계정 정보를 가지고 크리덴셜 스터핑 공격을 시도했고, 동일한 계정 정보를 사용하고 있던 클라우드 계정에 정상적으로 로그인함으로써 이와 같은 범행을 저질렀다고 알려졌다.

■ 크리덴셜 스터핑 공격 시나리오

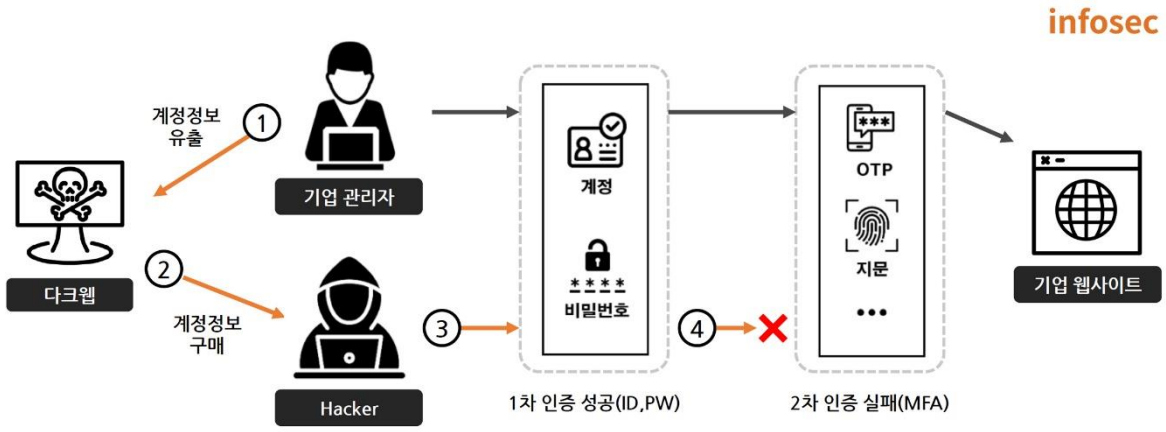
웹 해킹, 멀웨어, 피싱, 워터링홀 등의 방법으로 탈취된 계정 정보는 다양한 경로를 통해 다크웹에 유통되고, 공격 성공률을 높이기 위한 공격자는 다크웹에서 최대한 많은 계정정보를 수집한다. 획득한 계정 정보는 자동화 툴과 봇넷을 통해 희생자 웹사이트의 로그인 폼에 반복하여 대입(Stuffing)이 시도되며, 유출된 계정과 동일한 계정 정보를 쓰는 경우 공격자는 해당 웹사이트에서 추가적인 개인 정보를 획득하거나 악의적인 행위를 수행한다. 이러한 방법으로 획득한 계정 정보는 또 다시 다크웹에 판매되면서 2, 3차 피해로 이어진다.



① 웹해킹, 멀웨어, 피싱, 워터링홀 공격으로 탈취한 계정 정보가 다크웹에 유통
② 공격자(Attacker)가 다크웹에서 유통 중인 계정 정보를 구입
③ 수집한 계정 정보를 봇넷을 이용하여 여러 웹사이트 로그인폼에 무차별 대입(Stuff)
④ 인증된 웹사이트에서 추가 개인정보 획득하며 일부는 다크웹에 재판매

■ 크리덴셜 스터핑 대응 방안

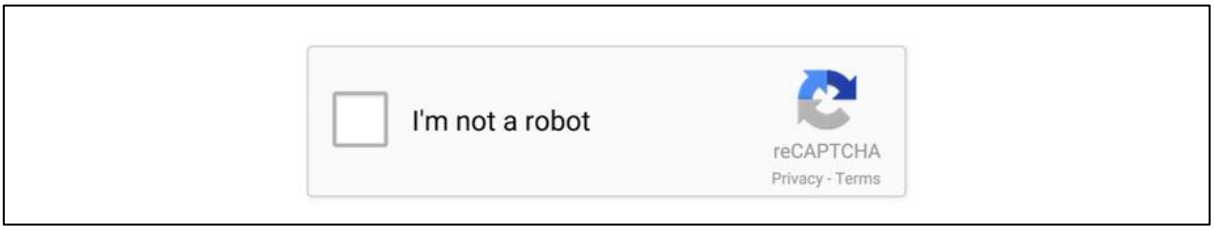
1. 로그인 인증 시 MFA(멀티팩터인증) 사용



[MFA(멀티팩터인증)를 활용한 크리덴셜 스터핑 방어]

로그인 기능에서 MFA(멀티팩터인증)[4]를 사용하면 크리덴셜 스터핑 공격을 방지할 수 있다. 아이디와 비밀번호 입력 후 다른 인증 요소를 사용한 2 차 인증이 추가로 요구되기 때문이다. 따라서 다크웹에 중요 계정이 유출되더라도 비인가자가 도용한 계정 정보로 접근하지 못하게 방어할 수 있다.

2. 로그인 시 CAPTCHA 기능 구현



[구글에서 제공하는 봇 방지 API (reCAPTCHA)]

크리덴셜 스터핑은 해커의 작업 효율성을 위해 악성 봇을 이용해 수행된다. 해커는 다크웹에서 구매한 계정 정보를 봇을 이용해 다수의 웹사이트 로그인 폼에 대입하는 시도를 반복하는데 이 때 봇을 방지하는 CAPTCHA 가 로그인 기능에 구현되어 있을 경우 봇을 이용한 크리덴셜 스터핑을 방지할 수 있다.

[4] MFA(멀티팩터인증): 로그인 시 최소 두가지 이상 인증 요소를 이용하여 본인 여부를 검증

3. 안전한 비밀번호 설정

여러 온라인 서비스에 동일한 ID, 비밀번호를 사용할 경우 크리덴셜 스터핑을 통해 정보 유출 피해가 발생할 수 있기 때문에, 규칙을 정해 온라인 서비스 별 서로 다른 비밀번호를 설정해야 한다. 하나의 안전한 비밀번호를 정하고 사이트마다 도메인의 일부를 조합하여 비밀번호를 설정하는 방법이 가장 기억하기 쉽고 안전하다.

Step 1) 안전한 비밀번호 생성하기

충분히 길고 높은 복잡도의 비밀번호를 설정할 경우 비밀번호를 유추하는데 오랜 시간이 걸리는 것을 알 수 있다. 따라서 최소 10자리 이상, 대소문자, 숫자, 특수문자 중 3종류 조합으로 비밀번호 설정하는 것을 권고한다.

Ex) infosec123!

비밀번호 길이	소문자만 사용 a	대소문자 Aa	대소문자, 숫자 Aa123	대소문자, 숫자, 특수문자 Aa123!@
1	1분 미만	1분 미만	-	-
2	1분 미만	1분 미만	1분 미만	-
3	1분 미만	1분 미만	1분 미만	1분 미만
4	1분 미만	1분 미만	1분 미만	1분 미만
5	1분 미만	1분 미만	1분 미만	1분 미만
6	1분 미만	1분 미만	1분 미만	1분 미만
7	1분 미만	1분 미만	1분	6분
8	1분 미만	22분	1시간	8시간
9	2분	19시간	3일	3주
10	1시간	1달	7달	5년
11	1일	5년	41년	400년
12	3주	300년	2000년	34000년

[비밀번호 복잡도에 따른 크랙 시간]

Step 2) 사이트마다 다른 비밀번호 만들기

각 사이트의 도메인에서 자신만의 규칙을 정해 비밀번호 앞, 또는 뒤에 조합한다.

[비밀번호 생성 규칙]

[예시] 도메인의 앞 3글자를 비밀번호 앞에 붙임

인스타그램인 경우 'ins', 페이스북이면 'fac', 구글이면 'goo', 네이트는 'nat'

Ex) insinfosec123!, facinfosec123!, gooinfosec123!, natinfosec123!

■ 결론

금융권과 정부는 이미 다크웹과 크리덴셜 스터핑의 위험성을 인지하고 발생할 수 있는 피해를 최소화하기 위해 다방면으로 노력하고 있다. 금융보안원은 클롭(Clop) 조직의 카드 정보 유출 사건을 계기로 다크웹에서 발생하는 위협을 지속적으로 모니터링하고 카드 정보 유출에 의한 소비자의 2차 피해를 방지하고 있다. 또한 개인정보보호위원회는 '개인정보 보호 활용 기술 R&D 로드맵('22~'26)'에서 2023년부터 다크웹 접속 및 개인정보 검색 기술 개발에 착수하고 2026년까지 다크웹 개인정보 불법거래 기술을 개발할 계획이라고 밝혔다. 이러한 흐름에 맞춰 기업의 보안 담당자 역시 다크웹과 크리덴셜 스터핑의 위험성을 인지하고 관심을 가져야 할 필요가 있다.

다크웹에서 유통되는 개인 정보는 언제, 어디서 유출되었는지 확인하기 어렵다. 또한 자사의 보안 취약점을 최소화하더라도 타사에서 유출된 개인 정보로 인해 크리덴셜 스터핑의 피해자가 될 수 있다. 개인 정보 거래 시장이 확장함에 따라 크리덴셜 스터핑 공격은 지속해서 증가할 전망이기 때문에 이러한 피해를 방지하기 위해 기업의 보안 취약점을 최소화하려는 노력이 필요하다.

■ 참고 URL

https://m.blog.naver.com/skinfosec2000/222038143450
https://www.f5.com/content/dam/campaign_hubs/shape_attackereconomics/Shape%20Security%20Credential%20Stuffing%202021.pdf
www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/
https://www.cpomagazine.com/cyber-security/about-26-million-fortune-1000-employee-credentials-available-on-the-dark-web-password-reuse-rampant/