효과적인 Credential Stuffing 공격 방지 방안

김충배O
O대한상공회의소
e-mail: cbkim@korcham.netO

An Effective Prevention to Credential Stuffing Attacks

Choungbae KimO
OThe Korea Chamber of Commerce & Industry

● 요 약 ●

본 논문에서는 사용자 계정 탈취인 1차 공격을 통해 수행되는 2차 공격인 크리덴셜 스터핑 공격을 효과적으로 대응할 수 있는 방안을 제안한다. 사전파일을 통해 공격을 시도하는 사전 공격보다 공격 성공 확률이 더욱 높은 이 공격은 최근 다크웹에서 거래되는 사용자 계정 정보를 구매하여 공격자가 적은 노력으로 손쉽게 계정을 탈취할 수 있어 정보화 시대에서 다양한 온라인 계정을 사용하는 사용자를 위협하고 있다. 본 논문에서는 기존에 알려진 대응 방안인 2-Factor 인증, 서비스별로 다른 패스워드 사용 방식을 응용하여 사용자가 암기하기 쉬운 특정 패턴을 활용하여 시스템별 상이한 패스워드를 더욱 쉽게 설정할 수 있도록 제안하여 크리덴셜 스터핑 공격으로부터 사용자 계정을 보호할 수 있음에 더 우수함을 보인다.

키워드: 크리덴셜 스터핑(credential stuffing), 계정 보안(account security), 사전 공격(dictionary attack)

I. Introduction

4차 산업혁명 시대가 진행되며 인류의 삶에 정보시스템이 차지하는 비중이 매우 높아졌다. 전자상거래, 사물인터넷, 금융, 민원업무 등 다양한 일상생활이 온라인으로 가능하게 되었으며, 코로나19 팬데믹 이후 일상생활의 비대면화가 급속도로 발전하며 직장, 교육 등 직업분야까지 온라인으로 전환되고 있다. 정보시스템 사용 범위가 넓어질수록 공격자들의 공격대상 범위가 넓어지고 있다.

최근 다크웹에서 시스템 침투 후 사용자 계정 데이터베이스를 탈취하여 거래하는 정황이 포착되었다.[1] 정보시스템 사용자들이 계정정보를 대부분 동일하게 사용한다는 가정하에 크리덴셜 스터핑 공격을 통해 손쉽게 다른 시스템 계정정보를 획득하여 2차 공격으로 이어지고 있다. 특히 VPN 등을 활용해 조직 내부 시스템을 사용하는 사례의 경우 이와 같은 공격으로 인해 발생할 피해는 더욱 클 것이다. 본 논문에서는 이러한 취약성을 효과적으로 예방할 수 있는 사용자 패스워드 설정 방안을 제안하고 있다.

II. Preliminaries

1. Related works

1.1 Credential Stuffing 공격 원리

Fig 1과 같이 크리덴셜 스터핑 공격은 사전 파일을 이용해 계정을 탈취하는 사전 공격과 방식은 유사하지만, 불특정 정보시스템에서 사용자 ID와 패스워드를 탈취한 1차 공격을 성공한 후, 해당 계정정보를 사전 파일로 재구성하여 타 정보시스템에 접속을 시도, 사전 공격에 비해 공격이 성공할 확률이 매우 높다는 점이 사전 공격과의 차이점이라 할 수 있다.

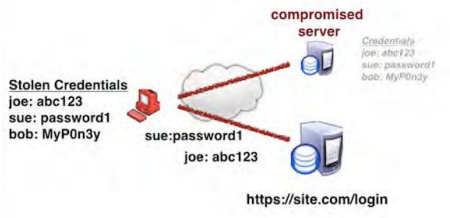

Fig. 1. Credential Stuffing Attack[2]

사용자 계정을 탈취해 다양한 정보시스템에서 개인정보를 탈취하거나, VPN(Virtual Private Network) 계정을 탈취해 기업이나 기관 내부망을 접속해 내부정보를 탈취하는 2차, 3차 공격이 크리덴셜 스터핑 공격의 가장 위협적인 특징이다.

III. The Proposed Scheme

특정 시스템에서 유출된 계정정보를 재사용할 수 없도록 사용자 입장에서 다양한 시스템의 패스워드를 모두 상이하게 사용하기란 매우 어려운 일이다. 이에 사용자가 이용하는 시스템의 도메인네임 앞자리와 도메인네임 자릿수를 패스워드에 함께 삽입하는 방법을 제안한다.

사용자 계정 ID가 banana이고, 패스워드가 P@ssw0rd!라고 가정할 때, Table 1과 같이 시스템별 패스워드를 설정하여 크리덴셜 스터핑 공격을 쉽고 효과적으로 예방할 수 있다.

Table 1. improve password set of prevention credential stuffing attack

System domain	ID	Password
www.delta.net	banana	d5P@ssw0rd!
www.echo.com		e4P@ssw0rd!
www.carrot.net		c6P@ssw0rd!
www.fox.com		f3P@ssw0rd!

만약 공격자가 www.delta.net 시스템의 사용자 계정 정보를 탈취하고, 공격자는 해당 시스템에서 탈취한 사용자 계정 정보를 다른 시스템인 www.fox.com 시스템에 대입하여 로그인을 시도하는 크리덴셜 스터핑 공격을 시도한다고 가정할 때, banana라는 ID에 대한 패스워드 d5P@ssw0rd!는 f3P@ssw0rd와 일치하지 않아 시스템에서 로그인에 실패하게 된다.

Table 1과 같이 기존 패스워드 앞부분이 아닌 뒷부분, 특정 자릿수 위치에 이과 같은 패턴으로 패스워드를 설정하면 크리덴셜 스터핑 공격을 효과적으로 예방할 수 있다.

IV. Conclusions

본 연구를 통해 제안한 패스워드 관리 방안으로 크리덴셜 스터핑 공격을 효과적으로 대응할 것으로 예상한다. 정보시스템 사용자 계정으로 인간의 삶의 활동반경이 점차 늘어나는 시대에 본 연구에서 제안한 패스워드 설정 방안을 응용하여 단순 공격으로 인한 막대한 피해를 손쉽게 대응할 수 있을 것으로 기대한다.

본 연구를 토대로 정보시스템에서 사용자가 패스워드 설정 시, 시스템상에서 패스워드를 응용하여 특정 값을 임의로 입력할 수 있는 패턴을 만들어 사용자가 직접 규칙을 설정하지 않아도 제안한 방안으로 입력이 가능하도록 할 수 있도록 연구할 계획이다.

REFERENCES

[1] Thebn Co., Ltd., "It sold account information to 134,698 people on 31 Korean websites on the Deep Web.", https://www.boannews.com/media/view.asp?idx=96906&page=1&kind=1

[2] Jeong-Seok Jo, and Jin Kwak, "Improvement of Authentication Protocol for Preventrion of Credential Stuffing in Cloud Environment", *Proceedings of the Korea Information Processing Society Conference*, Korea Information Processing Society, pp. 196-199, 2018.