Journal of Korea Game Society 2016 Apr; 16(2): 51-60
http://dx.doi.org/10.7583/JKGS.2016.16.2.51

게임 로그분석

로그인 패턴 분석을 통한 대규모 계정도용 차단 방안에 관한 연구 (온라인 게임 IP/계정 차단시스템을 중심으로)

연수권, 유진호
상명대학교 일반대학원 경영학과
skyeon@korea.com, jhyoo@smu.ac.kr

A study on Prevention of Large Scale Identity Theft through the Analysis of Login Pattern(Focusing on IP/Account Blocking System in Online Games)

Soo-Kwon Yeon, Jin-Ho Yoo
Dept. of Business Administration, Sangmyung University

요 약

개인정보가 대량으로 유출되는 사고가 최근 몇 년에 걸쳐 지속적으로 발생하고 있다. 이렇게 외부로 유출된 대량의 개인정보는 명의도용 및 계정도용에 불법적으로 사용되고 있다. 특히 온라인 게임머니·게임아이템 등의 가상의 재화를 현금으로 거래할 수 있는 온라인 게임서비스에서 다수 발생하고 있다. 온라인 게임에서 발생하고 있는 도용 사례를 분석해 보면 몇 가지 특징을 확인 할 수 있는데, 요약해 보면 짧은 시간에 대량으로 발생한다는 것이다. 본 연구에서는 온라인 게임에서 발생하고 있는 도용 공격 사례를 통해 대량의 자동화된 계정 도용 공격의 특징을 정의하고 실시간으로 대응할 수 있는 탐지 및 차단 방안을 제안 하였다.

ABSTRACT

The incidents of massive personal information being leaked are occurring continuously over recent years. Personal information leaked outside is used for an illegal use of other's name and account theft. Especially it is happening on online games whose virtual goods, online game money and game items can be exchanged with real cash. When we research the real identity theft cases that happened in an online game, we can see that they happen massively in a short time. In this study, we define the characteristics of the mass attacks of the automated identity theft cases that occur in online games. Also we suggest a system to detect and prevent identity theft attacks in real time.

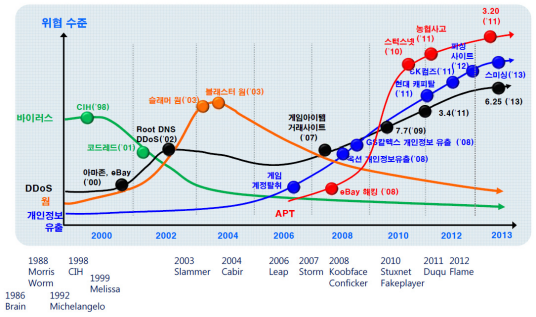
Keywords : Online Game Security(온라인 게임 보안), Identity Theft Detection(신분 도용 탐지), MMORPG(다중 사용자 온라인 롤플레잉 게임)

Received: Mar, 10, 2016 Revised : Apr, 15, 2016
Accepted: Apr, 20, 2016
Corresponding Author: Jin-Ho Yoo(Sangmyung University)
E-mail: jhyoo@smu.ac.kr

ISSN: 1598-4540 / eISSN: 2287-8211

1. 서 론

해킹기술의 발달 및 정보보호 관리체계의 부실로 인해 개인정보 유출은 최근 몇 년간 지속적으로 발생하고 있으며, 개인정보 유출은 여러 공격 유형 중 APT(Advanced Persistent Threat) 공격, DDoS(Distributed Denial of Service)와 같은 유형의 공격들과 함께 지속적으로 상승하고 있는 것으로 나타났다[Fig. 1].



[Fig. 1] Annual Security Users' Festival[1]

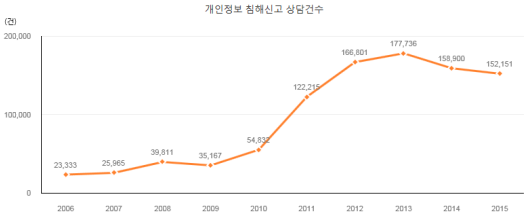
[Table 1]은 2008년부터 2014년까지 언론에 공개된 개인정보 유출 원인과 규모를 조사하여 정리한 표이며, 개인정보 유출 건수를 집계해 보면 대략 2억 건이 넘는 것을 확인할 수 있다.

[Table 1] Theft Scale of Personal Information[2]

발생시기	사업자명	유출규모	원인
2014년 3월	㈜KT	1,170만건	해킹
2014년 1월	카드 3사	10,400만건	외부인력 유출
2012년 7월	㈜KT	873만건	해킹
2012년 5월	EBS	422만건	해킹
2011년 11월	(주)넥슨코리아	1,320만건	해킹
2011년 8월	한국엠손㈜	35만건	해킹
2011년 7월	㈜SK컴즈	3,500만건	해킹
2008년 9월	GS칼텍스	1,151만건	내부자 유출
2008년 2월	옥션	1,863만건	해킹

개인정보가 유출되는 경로는 웹사이트 해킹, 내부자 및 협력업체 인력을 통한 유출, 악성코드에 의한 계정탈취, 피싱(phishing), 스미싱(smishing) 등 다양 하지만 대규모 개인정보 유출은 고도화된 해킹기술로 인한 유출과 관리체계 부실에 의한 내·외부자의 고의적인 유출로 발생한다. 이러한 개인정보 유출 사고는 국민들로 하여금 내 정보가 범죄에 사용될지 모른다는 사회적 불안감을 조성하고 있으며, 실제로 유출된 개인정보는 불법으로 판매되어 명의도용, 계정도용, 불법 마케팅 등에 사용되고 있다.

[Fig. 2]는 한국인터넷진흥원 개인정보침해신고센터에 접수된 개인정보 침해사고 관련 상담 건수로 2009년 까지 서서히 상승하던 상담 건수가 2010년을 기점으로 급속히 증가하고 있는 것을 볼 수 있다.



[Fig. 2] Change of Counseling Number Due to Violation of Personal Information[3]

2010년부터 급속히 증가한 개인정보침해사고 상담 현황을 상세하게 살펴보면, 타인의 명의도용 및 계정도용이 가장 많은 건수를 차지하는 것을 알 수 있다. 이렇게 대량으로 유출된 정보를 이용한 명의도용이나 계정도용이 사회 전반적으로 발생하고 있으며, 특히 온라인 통화 수단으로 사이버 캐시를 사용하거나 게임머니·게임아이템 등의 가상의 재화를 현금으로 거래할 수 있는 온라인 포털이나 온라인 게임서비스에서 다수 발생하고 있다. 명의도용을 통해 온라인 게임서비스에 게임계정을 생성하고, 정상 게임 사용자의 계정을 도용하여 해당 계정으로 가상의 재화를 이동시켜 현금화하는 방식을 사용하고 있으며, 이러한 도용은 이미 유출된 개인정보와 결합하여 빠르고, 지속적이고, 대규모로 이루어지고 있다. 해커들은 수집된 개인정보를 이용해 대규모로 회원가입을 수행하고 있으며, 대부분의 사용자들이 다수의 사이트에서 동일하게 패스

워드를 사용하고 있는 점을 악용하여, 자동화된 도구를 사용하여 계정과 패스워드를 지속적으로 대입해보는 방식으로 계정을 도용하고 있다. 또한 개인정보 유출 이외에 온라인 게임에서의 계정도용은 아래와 같은 다양한 원인으로 발생하고 있다[4].

- 계정 정보 공유
- Phishing Mail
- 게임 내 피싱(Phishing)
- 골드 현금 거래와 캐릭터 육성 대행 서비스
- 악성 애드온악성 웹사이트

[Table 2] Service to Prevent Identity Theft[5]

계정도용방지 서비스	설명
키보드 보안솔루션	악성코드에 의해 인증정보가 가로채기 당하지 않도록 보호하는 서비스
PC등록 서비스	등록된 PC에서만 게임에 접속할 수 있도록 제한하는 서비스
OTP	휴대폰에서 새로운 인증번호를 생성하여 추가 인증하는 서비스
전화 인증	등록된 전화번호로 ARS 안내받아 인증하는 서비스
2차 비밀번호	로그인 후 추가로 비밀번호를 입력받는 서비스
로그인 접속기록 확인	로그인 기록을 제공하여 신고하는 신고하도록 유도하는 서비스
계정 잠금 서비스	사용자가 일정기간 동안 계정/캐릭터/휴면계정을 잠그는 서비스

계정도용은 게임서비스를 제공하는 시스템 자체의 보안취약점으로 발생하는 것은 아니지만, 방치할 경우 게임 서비스에 대한 이미지 하락과 고객과의 심각한 갈등을 초래하여 게임서비스에 상당한 지장을 초래할 수 있기 때문에 게임업체는 많은 인력과 비용 투자하여 대응체계를 마련할 수 밖에 없는 상황이다.

게임업체들은 [Table 2]와 같이 많은 비용을 투자하여 계정도용을 방지하기 위한 다양한 솔루션 및 서비스를 제공하고 있다[4]. 악성코드 감염으로 인해 로그인 인증정보가 해커에게 전송되는 것을 차단하기 위하여 키보드 보안솔루션을 제공하고 있으며, OTP솔루션을 제공하여 로그인시 추가 인증을 받아 인증을 강화하였다[5]. 또한 악성코드에 의해 OTP 번호가 유출되어 인증이 우회되는 사례를 보완하기 위해 통신 채널이 완전히 다른 ARS(전화인증)인증 서비스를 제공하고 있다[5]. 뿐만 아니라 회사에서 수집되는 정보를 활용하여 사용자가 자주 접속할 수 있는 PC에서만 게임에 접속할 수 있도록 PC등록 서비스를 제공하고[5], 캐릭터 창이나 창고 접근시 추가 인증 받는 2차 패스워드 서비스, 본인이 접속한 기록을 검사하여 신고할 수 있는 시스템, 일정기간 게임을 이용하지 않는 경우 접속을 차단하는 계정 잠금 서비스 등 다양한 서비스를 제공하고 있다.

그러나 비즈니스 환경 및 고객환경이 각자 다른 상황으로 인해 개인화된 보안솔루션을 강제하기 어렵고 사용자에게 선택권을 제공할 수밖에 없는 상황이다. 이로 인해 명의·계정도용은 지속적으로 발생하고 있고, 위협을 완전하게 해소하기 어려울 것으로 보인다. 본 논문에서는 국내 온라인 게임회사에서 실제 발생했던 명의·계정도용 사례의 접속 로그를 분석하여 대규모 도용의 특징을 도출하고 기존에 게임사들이 구축해 놓은 시스템을 활용하여 실시간으로 대응할 수 있는 방법을 연구하였다.

2. 관련 연구

인터넷을 기반으로 비즈니스를 하는 기업에서는 계정도용이 지속적으로 발생되고 있다. 특히 계정도용은 온라인 게임에서 사설서버, 게임 봇 등과 함께 다수 발생되는 악의적인 행위이며, 게임 서비스의 성공 여부에 큰 영향을 미치고 있다.

이를 방지하기 위해 다양한 연구가 진행되었으며, [6]에서는 온라인 게임에서 발생할 수 있는 부

정행위를 분류하면서 “Compromising passwords”에 계정도용을 포함시켰으며, 온라인게임에서 발생할 수 있는 부정행위들을 체계적으로 정리하였다. [7]에서는 온라인게임에서 계정도용으로 발생하는 피해사례를 들어 심각성을 확인시켜 주었다. 이렇게 계정도용의 피해가 심각해지고 회사의 비즈니스에 영향을 주기 때문에 다양한 계정도용 탐지 및 차단하는 방안이 연구되고 제안되기 시작했다. [8]에서는 게임접속에 대한 정보를 이용자에게 통보하여 이용자가 계정도용여부를 판단하고 접속을 종료할 수 있도록 하는 시스템을 제안하였다. [9]는 게임캐릭터별 로그를 액션로그, 게임 내 자산의 변동여부 등을 분석하여 계정도용여부를 판단하고 일정 빈도 이상 발생하는 IP Address에 대해 차후에 접속을 제한하는 온라인 게임 도용계정 검출시스템을 제안하였다. [10]에서는 계정도용 사례를 분석하여 계정도용의 유형을 정의하고 유형별로 계정을 분리하는 자동화된 탐지모델을 제안하였고, [11]은 MMORPG 게임 내에서 계정도용 자들의 행위분석을 통한 계정도용 탐지 모델을 제안 하였다.

그러나 지금까지의 연구들은 대부분 이용자에게 추가인증 받은 방식의 불편함으로 인해 사용자의 외면을 받거나 사용자 환경에 따라 사용할 수 없는 경우도 많은 실정이다. 또한 대량의 게임로그를 분석하여 게임 플레이 패턴을 통해 계정도용을 탐지할 수 있는 시스템을 제안하였으나 이렇게 분석된 결과를 토대로 IP를 차단하거나 계정 접속을 제한하는 것은 대부분의 계정도용이 10분 이내의 짧은 시간 이내에 이루어지는 것을 생각해보면 실시간으로 대응해야 하는 환경에서는 한계가 있다. [12][13]에서는 능동형 계정도용 체계를 제안하면서 도용당한 계정들의 특징을 언급하고 정책적인 부분과 기술적인 부분에 대한 전통적인 대응방안을 언급하였다. 또한 로그를 기반으로 한 Blacklist DB 구축 및 차단 시스템에 대해 제안하였다.

[Table 3] Login Attempt Through Account Theft

계정	아이피주소	일시	성공여
p[redacted]	11[redacted]249	12-12 0:49	성공
m[redacted]278	11[redacted]249	12-12 0:49	성공
b[redacted]	11[redacted]249	12-12 0:49	성공
rr[redacted]	11[redacted]249	12-12 0:49	성공
b[redacted]4	11[redacted]249	12-12 0:49	실패
in[redacted]e	11[redacted]249	12-12 0:49	실패
w[redacted]17	11[redacted]249	12-12 0:49	실패
in[redacted]	11[redacted]249	12-12 0:49	성공
al[redacted]	11[redacted]249	12-12 0:49	성공
al[redacted]	11[redacted]249	12-12 0:49	성공
ch[redacted]2	11[redacted]249	12-12 0:49	실패
su[redacted]03	11[redacted]249	12-12 0:49	실패
in[redacted]ioni	11[redacted]249	12-12 0:49	실패
in[redacted]ioni	11[redacted]249	12-12 0:49	실패
in[redacted]ioni	11[redacted]249	12-12 0:49	실패
in[redacted]ioni	11[redacted]249	12-12 0:49	실패
b[redacted]2	11[redacted]249	12-12 0:49	실패
b[redacted]2	11[redacted]249	12-12 0:49	실패
su[redacted]03	11[redacted]249	12-12 0:49	성공
su[redacted]03	11[redacted]249	12-12 0:49	성공
su[redacted]03	11[redacted]249	12-12 0:49	성공

[Table 3]의 내용을 보면 사람이 할 수 없는 짧은 시간에 다수의 로그온 시도를 한 것을 확인할 수 있다. 이는 자동화된 도구를 사용하여 계정 로그온을 수행한 것으로 판단되며 이를 확인하기 위해 실제 온라인게임 계정 생성 기록과 로그인 기록을 분석하여 대규모 명의도용, 계정도용 계정의 특징을 도출해 보았다.

① 패턴이 없는 계정명 : 대량 명의도용 회원가입은 일반 사용자와 다르게 비정형화된 의미 없는 문자열로 계정을 생성하거나 대량의 연속적인 계정명으로 생성이 된다.

② VPN IP 사용 : 대부분의 게임사에서 로그인 가능한 국가 대역을 지정하여 IP기반으로 차단을 수행하고 있으며, 공격자는 접속한 위치나 실제 접속IP를 숨기기 위해 VPN 서비스를 이용한다.

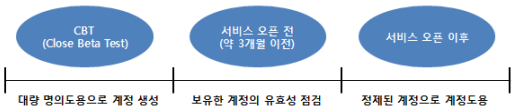
③ 동일한 IP 또는 IP대역 대량으로 시도 : 수십 개에서 수천 개까지 대량으로 회원가입 및 도용을 시도한다.

④ 짧은 시간에 시도 : 1분에 3개에서 50개까지 빠른 속도로 회원가입 및 계정 로그인을 시도한다.

3. 연구 방법

본 연구에서는 온라인 게임의 테스트 및 오픈 단계에서 발생한 도용 사례를 분석하여 기존에 제안된 Blacklist DB 기반 시스템의 단점을 보완할 수 있는 도용 IP 및 계정을 실시간으로 차단 할 수 있는 시스템 구축 모델을 제안한다. 게임에서의 부정행위는 게임해킹, 시스템해킹, 계정도용 등 다양한 방법을 이용할 수 있으나, 고도의 해킹 기술을 요구하는 게임 해킹이나 시스템 해킹보다 계정 도용을 이용할 경우 손쉽게 부정행위를 할 수 있다. 또한 공격자는 기존에 유출된 대량의 개인정보와 이를 자동으로 회원 가입 및 인증을 통과할 수 있도록 제작한 툴을 보유하고 있기 때문에 게임해킹이나 시스템 해킹보다 쉽고 빠르게 재화를 습득하고 현금화 할 수 있는 특징을 가지고 있다.

국내 주요 게임업체 중 한 곳에서 2013년 MMORPG 게임을 런칭하는 단계인 CBT(Close Bata Test) 12일, OBT(Open Beta Test) 및 상용화 전·후 1개월간의 데이터 셋을 얻어 분석한 결과 명의도용과 계정도용이 주로 발생되는 시기가 [Fig. 3]와 같이 다르다는 것이 확인 되었다.



[Fig. 3] Occurrence of Illegal Use of Other's Name and Account Theft

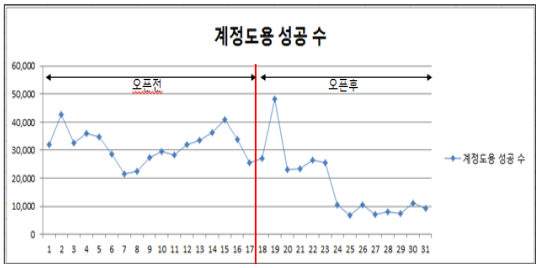
본 논문에서 사용한 게임로그를 분석한 내용을 기반으로 명의도용과 계정도용을 발생시기로 구분해본 보면 명의도용은 통장계정, 작업장 계정 등 불법으로 사용하기 위해 게임서비스가 오픈되기 전 CBT(Close Bata Test) 기간에 집중적으로 이루어지며, 계정도용은 일반사용자가 게임머니, 게임 아이템 등 가상의 재화를 일정기간 모은 이후, 즉 서비스가 정상 제공된 이후에 집중적으로 발생되는 것으로 확인 되었다. 일부 해커들은 게임서비스 정식 오픈 직전 보유하고 있는 계정의 유효성을 체크하기 위해 지속적으로 로그인 시도를 수행하여 최신의 정보로 지속적으로 업데이트하는 치밀한 모습도 확인 되었다.

해당 게임사의 총 12일간의 테스트 기간(CBT) 동안 가입한 회원을 대상으로 명의도용의 특징을 적용하여 분석한 결과, 총 458,499 중 456,523건이 명의도용이 발생한 것으로 확인 되었으며, 해당 계정에 대해 오용 탐지 여부를 분석하기 위해 계정을 삭제하지 않고 본인인증을 적용하여 통과하는 경우 정상적인 가입으로 간주하여 분석한 결과 전체 대상 중 442개의 계정만 본인인증을 통과한 것으로 확인되었다. 또한 본인인증을 통과한 계정을 집중 분석해본 결과 172개 계정만 정상적인 계정으로 확인되었다. 나머지 270개 계정은 명의도용의 특징을 보이고 있으며, 악의적인 목적으로 계정을 사용하기 위하여 대부분 대포폰 등 타인의 개인정보를 이용하여 본인인증을 수행한 것으로 분석되었다. 명의도용 대상으로 확인된 계정 중 오탐으로 확인된 계정은 약 0.06% 정도 인 것으로 확인되었다.

계정도용의 경우 정식 게임서비스 오픈 3개월 전부터 집중적으로 보유 계정의 유효성 점검을 진행하는 것으로 확인되었다.

[Fig. 4] Login Attempt Through Identity Theft

게임서비스의 정식 오픈 전·후로 1개월간의 로그인 기록을 기준으로 위에 언급한 계정도용의 특징을 대입해본 결과 일평균 약 400,000건의 로그인 시도 중 약 25,000건의 계정도용이 발생하고 있다는 사실을 확인할 수 있었다. 또한 게임서비스의 상용화 전·후로 비교해 봤을 때 상용화전 지속적이고 대량으로 계정도용을 시도하고, 게임 서비스 오픈 이후 이후에는 도용 성공 건수가 줄어드는 양상을 보였다. 이러한 양상을 보이는 이유는 게임을 오픈하기 이전에는 계정의 유효성을 점검하고 상용화 이후 계정 제재를 피하기 위해 계정을 분리하여 도용을 시도하는 것으로 판단된다.



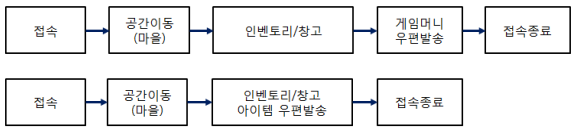
[Fig. 5] Number of Success of Identity Theft Before and After the Game Service

대규모 계정도용 시도에 성공한 계정 20개를 표본으로 추출하여 분석한 결과, 게임 접속 후 게임머니 및 아이템을 탈취하고 접속종료 하는 시간은 3분에서 9분 이내인 것으로 확인되었다.

[Table 4] Identity Theft and Stealing Time of Game Items

계정명	계정 접속	유출 시간(Start)	유출 시간(End)	계정 접속 종료	접속IP	유출(S-E) 소요시간	접속-종료 소요시간
[redacted]	01-15 8:51	01-15 8:55	01-15 8:55	01-15 8:55	101.55.46.121	00:24	03:42
	01-17 19:37	01-17 19:41	01-17 19:44	01-17 19:46	101.55.47.40	03:40	08:43
	01-17 12:03	01-17 12:05	01-17 12:06	01-17 12:06	112.223.56.13	00:35	03:16
	01-15 0:51	01-15 0:53	01-15 0:56	01-15 0:56	101.55.88.250	02:24	04:43
	01-15 10:21	01-15 10:22	01-15 10:28	01-15 10:28	211.189.145.70	05:40	07:04
	01-08 3:04	01-08 3:06	01-08 3:09	01-08 3:10	211.241.203.91	02:49	06:07
	01-15 0:04	01-15 0:10	01-15 0:12	01-15 0:13	115.178.38.171	02:27	08:48
	01-15 16:16	01-15 16:19	01-15 16:22	01-15 16:22	101.55.59.47.87	03:13	06:15
	01-15 19:54	01-15 19:57	01-15 20:00	01-15 20:00	101.55.59.139	03:12	06:11
	01-17 0:09	01-17 0:11	01-17 0:12	01-17 0:13	101.55.47.22.265	01:45	04:25
	01-17 8:14	01-17 8:17	01-17 8:18	01-17 8:18	101.79.174.47	00:57	03:54
	01-14 13:17	01-14 13:20	01-14 13:23	01-14 13:24	101.55.34.20.392	03:31	06:32
	01-14 21:50	01-14 21:52	01-14 21:53	01-14 21:54	110.4.82.38.211	01:43	03:41
	01-15 10:05	01-15 10:08	01-15 10:12	01-15 10:12	101.55.46.67	03:49	07:18
	01-14 11:36	01-14 11:38	01-14 11:39	01-14 11:39	101.55.68.228	00:51	03:31
	01-15 15:20	01-15 15:21	01-15 15:30	01-15 15:25	61.254.33.203	09:02	05:15
	01-15 17:39	01-15 17:41	01-15 17:42	01-15 17:43	101.55.61.161	01:00	03:57
	01-14 16:49	01-14 16:51	01-14 16:52	01-14 16:52	101.55.61.116	00:49	03:34
	01-15 11:00	01-15 11:02	01-15 11:06	01-15 11:07	101.55.58.73	04:47	06:07
	01-14 16:46	01-14 16:49	01-14 16:53	01-14 16:53	101.55.77.69	03:23	06:38

해커들은 게임 내 자산을 불법으로 탈취하기 위한 방법으로 피해 계정이 보유하고 있는 게임머니를 갈취하는 방법을 주로 사용하며, 보유하고 있는 게임 머니를 명의도용으로 생성한 계정으로 전송하거나 아이템을 게임머니로 변환하여 전송하는 방법을 사용한다. 또한 다른 캐릭터로 전송이 가능한 아이템이 존재할 경우 아이템 자체를 해커의 계정으로 전송하여 갈취하는 것으로 확인되었다.



[Fig. 6] Extortion Patterns of Game Money and Items

위 분석 결과를 조합해 보면 해커는 보유하고 있는 계정의 지속적인 유효성 체크를 통해 최신의 계정 정보를 유지하고 자동화된 공격도구를 이용하여 계정을 도용하고 있으며, 짧은 시간에 피해 계정의 재화를 갈취하고 종료하는 것을 확인 할 수 있다. 이렇게 대규모·자동화된 툴을 이용한 공격은 실시간 또는 몇 분 안에 대응해야만 이용자의 중요한 자산을 보호할 수 있다는 사실이 확인되었다. 다음 장에서는 이러한 특징을 기준으로 탐지 및 차단할 수 있는 시스템을 제안하고자 한다.

4. IP/계정 차단시스템 구현

4.1. 제안시스템 구성도

아래 [Fig. 7]는 대량 계정도용을 차단하기 위해 고안된 시스템 구성도이다. 해당 시스템은 총 7가지로 구성되어 있다. 기존 시스템에서는 ⑦ Blacklist DB를 구축하여 공격자 IP에 대해 사후 차단하는 방식을 사용한 반면, 본 시스템에서는 ② 인증서버와 ④ 캐시서버를 이용하여 실시간으로 시도되는 로그인 IP와 시간을 분석하고 계정도용 여부를 판단한다. 또한 ⑤ 인증로그서버에 주기적으로 로그를 분석할 수 있는 시스템을 구축하여 인증을 통과한 계정에 대해 재검증을 수행한다. 각각의 기능은 아래와 같이 정의 할 수 있다.

① Game Client : 정상적인 게임 이용자이거나 불법적으로 계정도용이나 명의도용을 수행하려는 자.

② 인증서버 : 이용자의 로그인 정보를 검증하고 인증해주는 서버로 로그인 시도 회수와 시도 시간을 분석하여 1차 필터링 및 차단을 수행함.

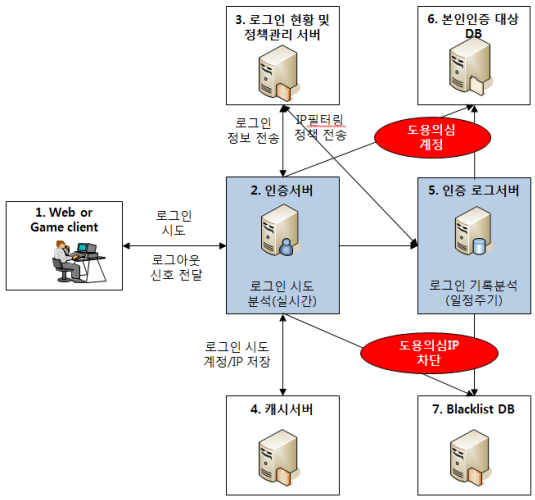
③ 로그인 현황 및 정책 관리서버 : 로그인 시도, 성공, 실패 등 추이를 분석할 수 있도록 현황을 관리해 주는 시스템으로 현황에 따라 필터링 정책을 변경하고 분석 시스템에 정책을 적용하는 시스템.

④ 캐시서버 : 실시간으로 시도되는 로그인 IP와 시간, 로그인 성공한 계정의 정보를 저장하고 있는 서버. 정책 위반이 발생하면 해당 정보를 Blacklist DB와 본인인증 대상 DB에 전송하고 삭제함.

⑤ 인증로그서버 : 로그인 시도IP, 시간, 성공, 실패 여부를 기록하는 로그서버. 저장된 로그를 기반으로 주기적으로 정책위반 여부를 검증할 수 있는 프로그램을 실행시켜 정책 위반이 발생 시 해당 정보를 Blacklist DB와 본인인증 DB에 전송함.

⑥ 본인인증대상DB : 계정도용이 의심되는 계정 중 본인인증을 통과한 계정은 정상적으로 서비스를 이용할 수 있도록 접속을 허용함. Blacklist DB에 저장된 차단IP를 삭제하거나 허용으로 변경함.

⑦ Blacklist DB : 계정도용이 의심되는 IP를 저장하고 있는 DB.



[Fig. 7] Block Diagram of Our Suggested System to Detect Identity Theft

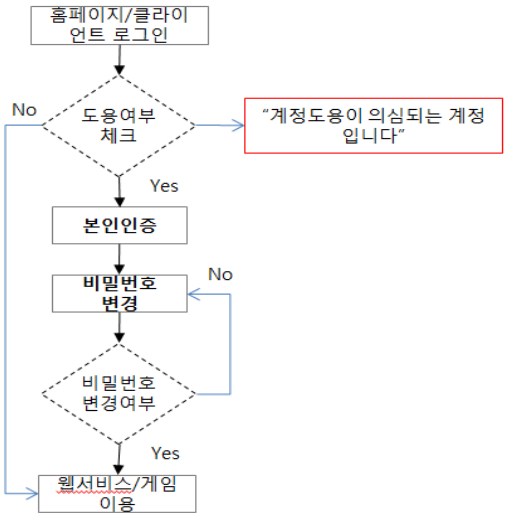
해커가 대량의 계정도용을 시도하면 인증서버에서 캐시서버를 이용하여 로그인 시도 정보를 저장하고 정책 위반이 발생하면 인증서버에서 해당IP를 차단하고 로그인에 성공한 계정에 로그아웃 신호를 전달한다. 또한 해당IP는 로그인을 재시도할 경우 이를 차단하기 위해 Blacklist DB에 정보를 저장한다. 또한 계정도용이 의심되는 계정은 본인인증을 통과해야만 정상 기능을 수행할 수 있도록 본인인증 대상 DB로 이동 시킨다. 인증서버에서는 실시간으로 계정도용 의심 IP 및 계정을 1차 필터링을 수행한다.

인증로그서버에서는 실시간이 아닌 주기적으로 정책 검증을 수행할 수 있는 프로그램을 실행하여 정책 위반 여부를 검증하고 위반된 계정 및 IP는 동일하게 본인인증 대상 DB 및 Blacklist DB에 저장한다. 1차 인증서버, 2차 인증로그서버 검증으로 구분하여 검증을 수행하는 이유는 인증서버의 경우 실시간으로 검증을 수행해야 하므로 성능 이슈가 발생할 수 있기 때문에 여기에 적용하는 정책은 짧은 시간과 적은 시도회수로 정책을 적용해야 한다. 또한 해커들은 검증 정책이 적용되어 있다는 사실을 많은 테스트를 통해 쉽게 감지 할 수 있으며 이를 우회할 수 있는 방법을 찾아 낼 수

있다. 이를 방지하기 위해 인증로그서버에서 로그를 기반으로 다시 한 번 도용 여부 검증을 수행한다.

로그 서버는 실시간으로 차단하지 않고 일정 주기를 가지고 비교적 긴 시간과 많은 시도횟수로 정책을 적용할 수 있다. 이렇게 할 경우 1차 검증에서 탐지하지 못한 도용의심 계정을 추가로 발견할 수 있으며, 검증을 우회하는 해커에게 혼란을 주어 우회할 수 없도록 할 수 있다.

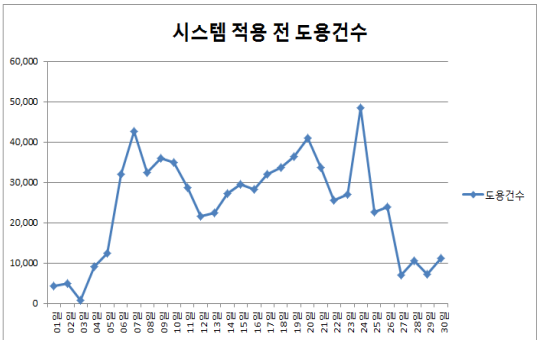
계정도용이 의심되는 계정은 본인인증을 통과하고 비밀번호를 반드시 변경하도록 로그인 프로세스를 수립해야 한다. 비밀번호를 변경하지 않고 기존과 동일하게 사용할 경우 해커가 이미 계정정보를 보유하고 있기 때문에 동일한 공격을 반복적으로 허용하게 된다.



[Fig. 8] Process to Check Identity Theft

4.2 제안시스템을 통한 실험 결과

본 논문에서 제안한 IP/계정 실시간 차단시스템을 적용하기 전 1개월 간의 계정도용 현황을 분석해본 결과 [Fig. 9]와 같이 일일 최저 약 1,000건에서 최고 약 50,000건까지 발생하는 것을 확인할 수 있었다.



[Fig. 9] Number of Identity Theft Before Appling the Identity Theft Prevention System

그러나 제안된 시스템을 구축하여 아래와 같이 1차, 2차 정책을 수립하여 적용한 결과 일평균 약 24,000건에 이르던 계정도용 건수가 [Fig. 10]과 같이 일평균 100건 정도로 줄어든 것을 확인할 수 있었다. 본 시스템은 IP를 기준으로 대량 계정도용을 검증하기 때문에 일반유저가 수동으로 수행하는 적은 건수의 도용을 탐지하고 차단하는 데는 한계가 있지만 수만 건의 계정도용을 100건 이하로 줄이는데 의미가 있다. 차단되지 않은 100건에 대해서는 게임로그를 분석하여 계정도용을 판별하는 기존 탐지방안을 통해 추가 차단할 수 있을 것으로 판단된다.

① 1차 정책(인증서버 : 실시간 IP/계정차단)

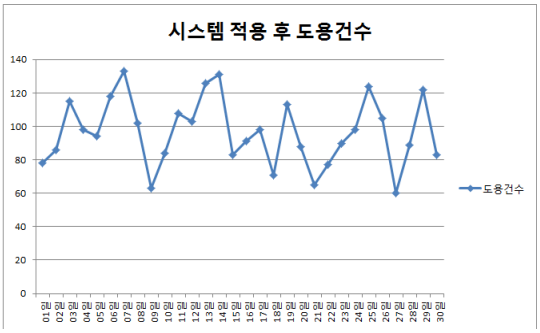
시간	제재기준
10초	6회
15초	8회

② 2차 정책(인증로그서버 : 일정 시간 주기적인 반복으로 IP/계정차단)

시간	제재기준
15초	5회
60초	13회
300초	30회

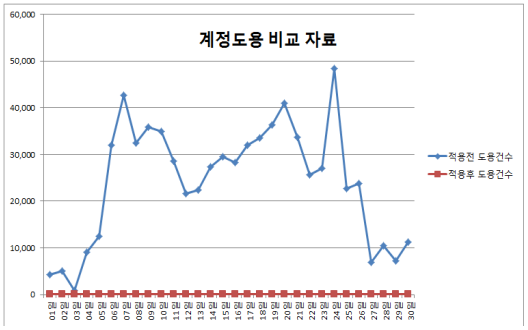
위의 정책은 인증을 시도한 로그를 분석한 결과를 토대로 적용하였다. 해당 정책은 해커의 공격 패턴이 변경될 수 있기 때문에 로그인 시도 현황,

계정도용 차단 IP 현황, 계정도용 차단 계정 수 등의 추이를 지속적으로 모니터링 할 수 있는 시스템을 구성하여 주기적으로 정책을 업데이트 할 필요가 있다.



[Fig. 10] Number of Identity Theft After Applying Identity Theft Prevention System

본 논문에서 제안한 계정도용차단 시스템을 적용하기 전·후를 비교해 보면 [Fig. 11]과 같이 계정 도용 차단 시스템을 적용할 경우 계정도용이 현격하게 줄어든 것을 확인할 수 있다.



[Fig. 11] Comparison of Identity Theft before and after Applying Identity Theft Prevention System

5. 결 론

본 연구는 회원가입 및 계정로그인을 시도하는 로그를 분석하여 [10]에서 언급한 해킹속도, 거래패턴과 패턴이 없는 계정명, VPN IP 사용, 동일한 IP 또는 동일한 IP대역에서 대량으로 시도하는 특징을 도출하여 정의하였다. 이를 통해 대량의 도용 공격은 일반적인 사용자의 로그인과 다른 패턴을 가지고 있다는 것을 알 수 있었다. 계정도용은 짧은 시간에 대량으로 발생하고 있으며, 다양한 게임로그를 활용하면 좀 더 정교하고 명확한 계정도용을 탐지 할 수 있다. 그러나 계정도용은 짧은 시간에 이루어진다는 특성으로 인해 실시간으로 탐지 및 차단할 수 없다면 이미 계정도용이 발생한 이후, 사후 대응으로서의 역할 밖에 수행할 수 없다. 이러한 특성을 고려하여 실시간으로 계정도용 IP 및 계정을 탐지하고 차단할 수 있는 시스템을 제안하였다. 실제 해당 시스템을 구현하여 적용한 결과 대량의 계정도용 시도로 피해가 발생한 계정을 현격하게 줄일 수 있었다. 제안한 시스템은 게임사의 계정도용에 대한 피해를 줄일 수 있는 방안을 제시한다. 계정도용이 의심되는 계정을 회사가 설정한 기준에 따라 실시간으로 제한하고 해당 계정에 대한 보호 조치를 취할 수 있다.

본 논문에서 제시한 실시간 IP 및 계정 차단시스템 수동으로 하나씩 인증정보를 입력하여 계정을 도용하는 공격에는 적합하지 않을 수 있으나 대량으로 신속하게 진행되는 공격을 사전에 차단하는 방안으로는 큰 효과를 볼 수 있다. 대량의 게임로그를 분석하여 계정을 제재하는 기존의 빅데이터 시스템 기반의 계정도용 탐지 연구와 결합하면 계정도용을 효과적으로 탐지 및 차단할 수 있는 시스템으로 활용할 수 있을 것으로 판단되며, 게임이용자의 자산을 보호하는데 도움을 줄 수 있을 것으로 기대한다.

REFERENCES

[1] Sun Tae Park, “2013년 주요 침해사고 사례와 대응”, 2013 Annuual Security User’s Festival, pp. 3, Dec. 2013.

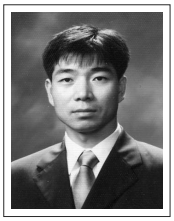
[2] Open Expert Group, http://www.openeg.co.kr/490, 국내 주요 해킹

사례, May 2014.
[3] Statistics Korea, http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366, 2015년 개인정보침해신고 상담 건수 통계, Jan. 2016.
[4] Blizzard Entertainment, “Account Security: General Tips - World of Warcraft (WoW)”, “http://www.vidqt.com/id/nW6SytPikDM?lang=ko”, Sept. 2011.
[5] Myeong Hwan Kim, “이상행위와 Entropy를 이용한 계정도용 탐지 모델”, 고려대학교 정보보호대학원 학위논문, pp. 4, Dec. 2012.
[6] J. Yan and B. Randell, “An Investigation of Cheating in Online Games”, IEEE Security and Privacy, Vol. 7, pp. 37-44, 2009.
[7] Y. C. Chen, P. S. Chen, J. J. Hwang, L.Korba, R. Song, and G. Yee, “An Analysis of Online Gaming Crime Characteristics”, Internet Research, Vol. 15, pp. 246-261, 2005.
[8] Dong Gyu Kim, “온라인게임계정 도용방지 시스템”, 특허청, May. 2007.
[9] Mi Gee Lee, Sung Ho Kim, “온라인 게임에서의 도용계정 검출시스템 및 그 방법”, KIPO, Aug. 2011.
[10] Hwa Jae Choi, Ji young Woo, Huy Kang Kim, “Online Game Identity Theft Detection Model based on Hacker's Behavior Analysis”, Journal of Korea Game Society, Vol.11, No.6, pp. 81-94, Dec. 2011.
[11] Hana Kim, Byung Il Kwak, Huy Kang Kim, “A Study on the Identity Theft Detection Model in MMORPGs”, Journal of The Korea Institute of Information Security & Cryptology, Vol.25, NO.3, Jun. 2015.
[12] Huy Kang Kim, “국내포털, 게임사를 위한 능동형 계정도용 대응 체계”, 정보통신망 정보보호 워크샵 “NETSEC-KR 2011”, pp. 12-25, Apr. 2011.
[13] Hwa Jae Choi, Huy Kang Kim, “온라인 게임의 로그정보를 이용한 계정 도용 방지 방법”, KIPO, Feb. 2013.

연 수 권(Yeon, Soo Kwon)

2001 청주대학교 컴퓨터공학과 학사
2006 건국대학교 정보통신대학원 석사
2016 상명대학교 경영학과 정보시스템보안 박사과정
2006 IZEN 선임 보안컨설턴트
2010 NEXON 보안팀 팀장
2013 XLGAMES 보안팀 팀장
2016 포워드벤처스(쿠팡) 시스템보안팀 팀장

관심분야 : 침해사고대응, 게임보안, 빅데이터 보안



유 진 호(Yoo, Jin Ho)

1992 고려대학교 수학과 졸업
1994 고려대학교 통계학과 석사
2010 고려대학교 정보보호 박사
1999 한국전자통신연구원 연구원
2004 IBM KOREA 전문차장
2012 KISA 인터넷문화진흥단장
2016 상명대학교 경영학과 교수

관심분야 : 정보보호, 개인정보보호, MIS, 인터넷 윤리