사회공학적 이메일 공격 대비 모의훈련 시스템 설계

임일권*, 김영혁*, 이재필*, 이재광*, 남궁현*, 이재광*
*한남대학교 컴퓨터공학과
{iklim, yhkim, jplee, leejk, ghnam}@netwk.hnu.kr, jklee@hnu.kr

A Study on Tools for Agent System Development

Il-kwon Lim*, Young-Hyuk Kim*, Jae-Gwang Lee*, Jae-Pil Lee*,
Hyun Nam-Gung*, Jae-Kwang Lee*
*Dept of Computer Engineering, Hannam University

요 약

사회공학적 공격이란 인간의 심리를 이용하여 보안 위협 상황을 갖게 하는 공격을 말한다. 그렇기 때문에 사회공학적 공격을 막기 위한 보안 솔루션은 그 한계가 있기 마련이다. 그리하여 본 논문에서는 사회공학적 공격에 대비하는 보안훈련시스템을 제안한다. 스팸 및 피싱 이메일을 수집하여, 시그니처 기반 필터링을 이용하여, 최신의 사회공학적 공격 이메일을 분석한 후, 가상으로 사회공학적 이메일 공격을 실시하여 훈련대상자들이 최신의 사회공학적 공격에 대비하는 능력을 갖추게 하는 보안 훈련 시스템을 설계하였다.

1. 서론

사회공학적 공격이란 고도의 기술이 접목된 해킹기술과는 전혀 무관한 인간의 심리를 이용하여 민감한 개인정보 및 금융정보를 갈취하는 행위를 말한다. 그렇기 때문에 사회공학적 공격은 시스템이나 네트워크의 취약점을 이용한 해킹방식이 아니다. 최근 이슈가 되는 사건 사고나, 인기 가수의 신곡 발표 등의 인간 심리를 이용하여, 피싱 사이트로 유도하거나, 악성코드 등을 첨부하여 불법적인 행위를 시도한다. 이러한 예로 미국 팝 가수 마이클 잭슨의 사망 소식을 악용하여 유포된 전자 메일을 들 수가 있다. 미국의 유명한 팝 가수 마이클 잭슨이 2009년 6월 26일 심장 마비로 사망하였다는 소식이 언론을 통해 전 세계로 퍼지자 만 하루가 채 지나기도 전에 악성코드 다운로드를 유도하는 전자 메일이 유포되었다. 해당 전자 메일은 마이클 잭슨이 심장 마비로 사망하기 직전의 모습들을 유튜브 동영상으로 볼 수 있다는 메일 내용을 가지고 있어 전자메일 수신자들의 호기심을 자극하였다. 그러나 이 메일은 본문에 포함되어 있는 뱅커(Win-Trojan/Banker) 트로이 목마를 다운로드 하는 웹 사이트의 링크를 클릭하도록 유도하고 있다[1-4].

또한, 국내의 보안 위협 통계를 보면 <표 1>과 같이 지난 2013년 한해 국내의 해킹사고 접수처리는 10,600건, 악성코드 감염탐지현황은 2,415,046건, 국내피싱사이트 차단 현황은 7,999건, 월별 악성코드 은닉사이트 탐지/조치 현황은 17,750건이다. 국외를 살펴보면, 보안업체 McAfee의 2013년 3분기 Threats Report에 따르면, 전세계 2012년 3분기에 위협 URL의 총 수는 전 분기에 비해 14%가 증가되는 85,000,000건으로 집계되었다. 이러한 URL은 이전 기간에 최대 30,000,000건의 도메인 이름이 증가되었으며, 이전 대비 최대 3%가 증가했다[5-6].

위와 같은 보안위협의 근간에는 사회공학적 공격으로 이루어진다. 2010년 시만텍 자료에 따르면 사회공학적 공격이 전체 공격에 60%를 차지한다고 밝혔다[7]. 시만텍, 안철수연구소 등 국내·외 보안업체들은 이러한 사회공학적 공격(social engineering attacks)으로 전파되는 악성메일이 강력한 위협으로 대두 된다고 말하고 있다[8].

그리하여 본 논문에서는 이러한 사회공학적 공격으로 이루어지는 이메일 공격에 대비한 보안훈련시스템을 설계한다. 사회공학적 이메일 공격을 시도하는 이메일을 수집하여, 메일을 파싱 후, 특정 문구나 내용의 사회공학적 공격 이메일을 파악한다. 이메일을 파악하면, 관리자는 특정 문구와 내용의 이메일을 대상 훈련자에게 가상의 공격 이메일을 송신한다. 이렇게 송신한 이메일을 열게 되면, 신고, 또는 수신한 내용의 이메일 공격이 이뤄진다는 경고메시지를 훈련대상자에게 알린다. 이러한 일련의 과정을 통해 훈련대상자들은 최근 이슈가 되는 사회공학적 이메일 공격에 대비하는 능력 갖추게 된다.

구 분	2012년 총계	2013년 1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	2013년 합계
해킹사고접수 처리현황	19,570	1,258	992	991	947	868	1,090	831	612	532	846	764	869	10,600
악성코드 감염탐지현황	-	68,101	240,325	272,246	226,892	229,743	203,715	92,083	188,207	135,316	155,936	176,759	125,723	2,415,046
국내피싱사이트 차단현황	6,944	1,024	805	1,039	1,032	478	345	554	995	778	205	299	445	7,999
• 정부/공공	2,646	169	73	161	181	132	144	165	144	125	148	196	312	1,950
• 금융기관	4,242	848	729	868	844	345	199	376	832	638	46	89	126	5,940
• 기타	56	7	3	10	7	1	2	13	19	15	11	14	7	109
월별 악성코드 은닉사이트 탐지/조치 현황	13,018	1,550	993	1,844	1,586	2,964	2,556	1,121	1,064	1,156	680	797	1,439	17,750
• 유포지	3,270	353	208	355	397	429	527	415	508	466	256	318	240	4,472
• 경유지	9,748	1,197	785	1,489	1,189	2,535	2,029	706	556	690	424	479	1,199	13,278

자료출처: 2013년 12월 인터넷 침해사고 대응통계월보, 한국인터넷진흥원, 2013. 12

<표 1> 2013년 인터넷 침해사고 대응통계

2. 관련연구

기술의 발전과 더불어 정보보호기술 온라인 학습이 이루어지고 있다. 보안 훈련 시스템의 기반에는 e-Learning이라 하는 정보통신기술을 이용하여 시간과 장소에 구애됨이 없이 수준별 교수·학습이 가능한 교육활동을 기반으로 한다.

우리나라의 경우 e-Learning은 직업훈련 분야에 '인터넷 원격 훈련' 제도를 통해 1999년에 처음 도입되었다. 처음 도입 후 지속적인 증가를 통해 2006년 말에는 기업의 총 교육비 예산액 대비 e-learning을 통한 교육비 지출액 비율은 14.3%를 차지하고 있다. 이는 현업을 수행하면서 훈련을 받을 수 있고, 훈련비용이 절감되는 등의 장점이 기업의 지식경영 방침과 맞물려 지속적인 성장을 이어 왔다고 볼 수 있다[9]. 이러한 e-Learnig은 현재 한국인터넷진흥원에서 정보보호기술 온라인학습장이라는 이름으로 기초 이론 학습, 가상서버에 접속하여 모의상황 훈련, 해킹방어훈련 등의 서비스를 제공하고 있다. (그림 1)은 정보보안 학습에 대한 화면이다.

(그림 1) 한국인터넷진흥원에서 제공하는 정보보호 교육 시스템

하지만 이러한 온라인학습장에는 '주니어 정보보호 교육', '청소년 인터넷 윤리', '모바일 인터넷 보안', '정보보호 기초과정', '정보보호 실무과정', '웹호스팅 보안과정', '개인정보보호 담당자 과정', '안전한 홈페이지 개발', '실력테스트' 등의 단순 보안 학습 과정과 '시스템 보안', '네트워크 보안', '어플리케이션 보안', '윈도우 보안', '중소기업 보안', '디지털 포렌식' 등의 사이버 훈련 공간, 그리고 해킹방어 훈련장 등의 기본적인 보안학습과 전문적인 보안전문가 훈련시스템으로 이루어지며, 일반 사용자들에 효과적인 훈련시스템은 부족하다[10]

한국인터넷진흥원 인터넷침해대응센터는 인터넷 침해사고에 신속하고 효율적으로 대응하기 위해 2004년 이후 국내외 유관기관과 공동 모의훈련을 실시하고 있다. 지난 2011년 2월, APCERT(아시아태평양 침해사고대응팀협의회, Asia Pacific Computer Emergency Response Team) 주관으로 실시한 국제 공동모의훈련의 경우 한국, 일본, 홍콩 등 15개국 20개 침해사고대응팀과 국내 5개의 주요 인터넷서비스제공사업자가 훈련에 참여하였으며 이메일이나 SMS로 유포되는 악성코드로 인해 사회 주요 기반시설이 공격받고 대응하는 형태의 국제 공동모의훈련이 진행하였다. 또한 침해사고 대응능력강화를 위해 6월에 실시한 모의훈련의 경우, ISP, 백신사 등 12개 국내기관이 참여하였으며, 대응능력 향상을 위해 사전 시나리오가 공개 되지 않는 블라인드 드릴 훈련으로 실시하였다. 훈련과정에서 영세한 사업자를 DDoS 공격으로 부터 보호하기 위한 DDoS 사이버 대피소 운영, 좀비PC 감염자를 치료하기 위한 감염PC치료체계 시스템 운영 등 침해사고에 대비한 실전형 훈련을 실시하였다. 2012년 8월에 실시한 전시대비를 위한 을지훈련에서도, 국정원 및 교과부(정보보호팀) 주관으로 사이버테러 대응연습을 실시하는 등의 사이버테러나 보안 훈련에 대비한 훈련은 이루어지고 있지만, 그리하여 악성코드 유포나 위협 URL 주소 등을 사회공학적 기법을 이용하여 이메일 등으로 유포하는 사례는 더욱 다양해지고 그 수법이 교활해지고 있으나, 공공기관의 일반 사용자 등은 이에 따른 훈련의 필요성에도 불구하고, 실제 훈련은 보안 강습이나, 교육자료 배포 등으로 한정되고 있는 실정이다[11-12].

3. 시스템 설계

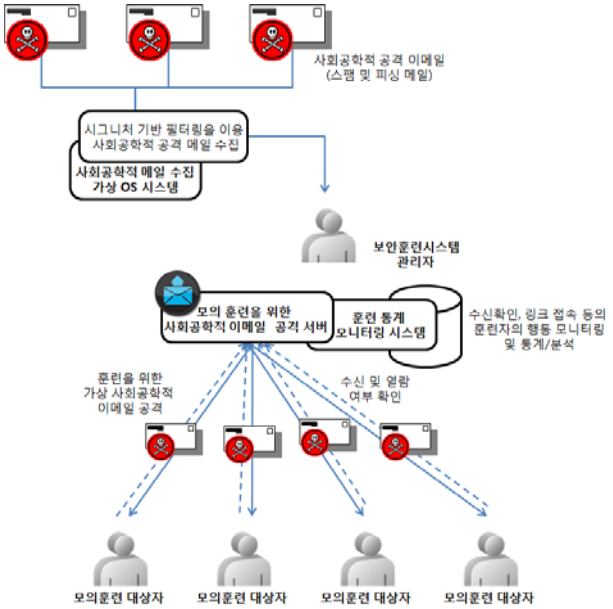
스팸 및 피싱 메일에 대응할 수 있는 기술시스템은 표 1과 같이 시그니처 기반 필터링, 자동차단, 레퓨테이션 (Reputation) 시스템 등이 존재한다.

유형	방법
시그니처 기반 필터링	컨텐츠 필터링 휴리스틱 필터링 베이지안 필터링
네트워크 필터링	SMTP 연결 차단 트래픽 모티너링 및 속도 제한
자동 차단	대량 메일 발송기를 이용해 전송되는 스팸메일 차단 최초 발송된 이메일 인증 같은 형태의 이메일이 일정 시간 내에 연속적으로 발송될 경우 차단
레퓨테이션 시스템	실시간 스팸 차단 리스트(RBL) 넬(Sender Policy Framework)

<표 2> 스팸 및 피싱 메일 대응 기술

시그니처 기반 필터링은 기본적으로 특정 시그니처에 대한 필터를 적용하고 매치 여부를 판단한다. 그중에서도 컨텐츠 필터링은 수신하려는 이메일의 헤더 정보, 본문, 첨부파일의 정보를 읽어 제목 또는 본문 중에 특정 내용, 키워드, 문자열을 포함하고 있거나 발송자의 주소가 특정한 이메일 주소일 경우 컨텐츠 필터가 이러한 스팸메일의 수신을 차단하는 기능을 가지는데, 이러한 컨텐츠 필터링 기능을 이용하여 스팸 및 피싱 메일을 수집하여 관리한다 [3]. 이렇게 수집된 메일들의 특정 내용, 키워드, 문자열을 분석하여 모의 훈련 시스템 관리자는 특정 패턴의 이메일을 분석한다. 이때 보안을 위해 피싱 위협 URL이나, 보안 위협 첨부파일은 가상 OS에서 메일 확인을 한다. 이렇게 수집된 메일 패턴을 분석하면, 유행하는 패턴의 사회공학적 공격파악이 가능하다. 보안훈련시스템 관리자는 이렇게 수집된 사회공학적 공격 메일 유형을 분석하여 훈련대상자들에게 비슷한 유형으로 모의 훈련 메일을 송신한다. 전체 시스템은 (그림 2)와 같다.

이렇게 최신 유행하는 사회공학적 공격 이메일을 훈련대상자들에게 송신함으로써, 훈련대상자들은 이메일에 대한 특정행동을 취하게 되는데, 이는 이메일을 열람하거나, 이메일에 있는 피싱 URL로 접속을 하거나, 첨부파일을 실행을 할 것이다. 싱행을 하게 되면, '모의 보안 이메일 훈련입니다'와 '최근 이러한 사회공학적 이메일 공격이 유행입니다' 라는 안내문을 보여준다. 그리고 이렇게 훈련대상자가 취한 행동을 훈련 통계 모니터링 시스템에서 저장·관리하여, 보안훈련시스템 관리자는 통계와 분석이 가능하게 된다.



(그림 2) 사회공학적 이메일 공격 대비 모의훈련 시스템 전체 구성도

4. 결론

사회공학적 공격 이메일을 통해, 피싱이나 스팸 이메일을 통한 애드웨어나, 악성코드를 유포한다. 이러한 사회공학적 공격은 APT(Advanced Persistent Threat) 공격이나, 사용자 PC를 좀비PC로 만들어 DDoS (Distributed Denial of Service)공격으로 이루어지기 마련이다. 최근에는 스마트폰의 발달로 사회공학적 공격이 스미싱 (smishing)으로 확대되어 극성을 부리고 있다.

그리하여 본 논문에서는 이러한 사회공학적 공격을 대비하기 위해, 보안 훈련 시스템을 제안한다. 단순한 이메일을 송신하여, 훈련을 하는 것이 아닌, 최신 유행하는 사회공학적 이메일을 분석하여, 훈련에 이용함으로써, 더욱 사회공학적 이메일 공격에 대비가 가능하도록 하였다.

하지만 본 논문에서 제안하는 시스템은 악성코드나 스팸메일을 막는 솔루션이 아니기 때문에, 보안 솔루션과 같이 운용을 해야 할 것이며, 최근 유행하는 스마트폰의 스미싱 공격에 대한 보안 훈련 시스템의 연구도 필요할 것이다.

참고문헌

[1] 최양서, 서동일, "사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석", 정보보호학회논문지, 제16권 제1호, pp.40-48, 2006년 2월.

[2] 박기홍, 이준환, 조한진, "개인정보 입력 감지를 이용한 사회공학적 공격 대응방안", 한국콘텐츠학회논문지, 제12권 제5호, 32-39, 2012년 5월

[3] 한경수, 신윤호, 임일규, "스팸메일로 전파되는 악성코드의 분석 및 대응 프레임워크", 보안공학연구논문지, 제 7권, 제 4호, 2010년 8월

[4] 안랩, 보안이슈 & 이슈, “전자 메일을 악용하는 악성 코드의 발전”, 2010년 7월 22일, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16442

[5] 2013년 12월 인터넷 침해사고 대응통계 월보, 한국인터넷 진흥원, 2014.2.17
[6] McAfee® Labs Threats Report: Third Quarter 2013
[7] Symantec, “시만텍 인터넷 보안 위협 보고서 2010년 동향“, 제 16호, 2011년 4월
[8] 한국인터넷진흥원 보도자료, “독해진 해커, 취업준비생 두 번 울린다”, http://www.kisa.or.kr/notice/pressView.jsp?mode=view&p_No=8&b_No=8&d_No=415
[9] 이현정, 전종호, 이정의, 신선미, 박형국, 김한별, “e-Learning 훈련 정책 국제 비교”, 한국인력개발학회 논문지, Vol.10, No.3, pp. 249-264. 2008년
[10] 한국인터넷진흥원 “정보보호기술 온라인학습장”, http://sis.or.kr/

[11] 보안뉴스, “KISA, 아·태지역 사이버공격 대응훈련 참여”, 2012년 2월 15일, http://www.boannews.com/media/view.asp?idx=30095&page=1&kind=1&search=title&find=APCERT
[12] 2012 을지연습실시계획, 2012년 7월, http://goo.gl/YeCh9P
[13] 한경수, 신윤호, 임을규, “스팸메일로 전파되는 악성 코드의 분석 및 대응 프레임워크”, 보안공학연구논문지, 제7권 제4호, pp. 363-384, 2010년 8월.