메신저 해킹을 통한 금융침해(인터넷뱅킹) 공격 분석

류경하* · 박대우*

*호서대학교 벤처전문대학원

Financial violations by messenger hacking (Internet banking) Attack Analysis

kyong-ha Roo* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : freejeus@gmail.com · prof_pdw@naver.com

요 약

본 논문은 네이트온, MSN 등 메신저를 해킹하여 지인처럼 가장하는 방법으로 친밀감을 형성한 다음, 해킹툴(키로그, 원격모니터링 등)을 전송하여 거래은행과 ID, PW, 공인인증서, 보안카드 정보 등 개인의 금융정보를 입수한 뒤 계좌의 잔고를 인출해가는 금융침해 공격을 분석하여 개인의 인터넷뱅킹 거래 취약요소들을 찾아내고, 해당 취약점들과 관련한 대응방안을 모색함으로써 인터넷뱅킹 침해사고 예방 등 보다 안전한 개인의 인터넷뱅킹 거래를 도모하고자 한다.

ABSTRACT

In this paper, Nateon, MSN Messenger, including how to hack into the most intimate acquaintance formed as follows, for hacking (keyloggers, remote monitoring, etc.) by sending a bank and ID, PW, certificate, security card, etc. personal financial information obtained after the withdrawal of the account balance to have a personal financial analysis infringement attack vulnerable elements found in internet banking, the vulnerabilities and countermeasures concerning the prevention of accidents, including violations by seeking a more secure Internet banking personal Internet Banking is to devise a deal.

키워드

Internet Banking, Hacking, Financial breaches, Security card, Messenger (Nateon)

Ⅰ. 서 론

최근의 금융거래는 그림 1과 같이 금융공동망을 이용하여 인터넷이나 스마트폰을 이용한 거래가 급증하고 있다. 그러나 인터넷뱅킹이나 인터넷 거래를 가장한 금융침해사고가 발생하고 있다. 그 중 사회공학적 기법을 이용하여 금품을 요구하거나 상대방의 개인정보를 도난, 해킹하는 사례가 증가하고 있다[1].

따라서 본 논문에서는 최근에 널리 애용되고 있는 메신저를 해킹하여 지인인 것처럼 자연스럽게 접근하여 친근감을 형성한 다음 거부감이 없는 상태에서 키로그, 원격 모니터링 등의 기능을 구현하는 악성코드를 전송, 다운로드하도록 한 다음 개인의 금융거래정보를 입수하여 계좌의 잔고를 인출해가는 이른바 인터넷뱅킹 해킹 사고 발생에 대한 분석과 연구가 필요하다.

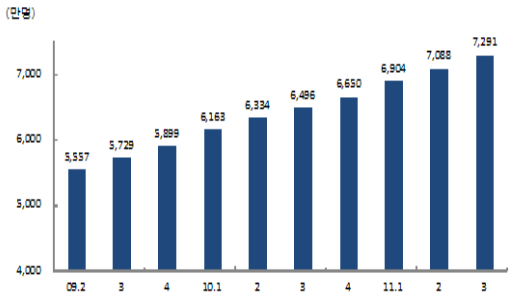

그림 1. 2011년 3/4분기 국내 인터넷뱅킹서비스 이용현황(출처: 한국은행)

Ⅱ. 관련연구

2.1 메신저

메신저(Messenger)는 인터넷을 통하여 실시간으로 대화 및 파일을 주고받는 시스템 어플리케이션으로 활용되고 있다.

악의적 사용자들은 메신저의 특징을 이용하여 사회공학적으로 지인인척 가장하여 금품을 요구하거나, 사용자에게 악성코드가 담긴 파일을 전송하여 위장된 홈페이지로 유인, 또는 키로깅 등의 해킹기법을 이용하여 인터넷 상에 신용카드 번호, 사용자 ID, PW 등 민감한 개인의 금융정보를 획득하는 피싱(Phishing)을 사용한다. 최근에는 피싱의 진화된 형태인 파밍(Pharming)도 출현하고 있다[2].

2.2 인터넷뱅킹 연구

금융거래 수단으로써 인터넷뱅킹 등 전자금융 서비스가 생활화 되었으며 이에 대한 부작용으로서 금융기관, 쇼핑몰, 포털 등의 해킹을 통한 전자금융 접근매체의 유출, 지불결제나 인터넷뱅킹 이체 사고 등 침해사고 또한 함께 증가하고 있다[3]. 금융권은 금융감독원을 중심으로 전자금융 종합보안 대책 수립 및 전자금융거래법 시행 등을 통해 사용자 PC의 해킹방지를 위한 다양한 보안프로그램 제공 의무화, 보안등급에 따른 이체한도 차등화, 금융권 통합 OTP 인증체계 구축 등 전자금융 침해사고 예방을 위한 적극적인 노력을 기울여오고 있으나, 최근 들어 피싱/파밍 등 신종 사이버사기 기법 등 침해사고를 완벽히 차단하지는 못하고 있어, 더욱 강력한 전자금융 침해사고 예방 통제 방안의 수립과 함께 침해사고 발생 시 원인 파악 및 범인 검거를 위한 역추적 시스템의 구축 등 기존 보안체계를 대폭 강화할 필요성이 발생하고 있다[4].

2.3 해킹공격 유형 연구

해커의 해킹공격은 주로 사회공학 기법을 이용한 보안 위협을 발생시킨다. 특히 SNS(Social Network Service)를 통해 온·오프라인에서 이미 형성되어 있는 인간관계를 바탕으로 서로 신뢰관계의 사람들에게 URL주소 및 파일을 전달하여 가짜 웹사이트 접근시켜 사용자의 ID와 PW, 계좌번호 등 개인정보를 빼내는 해킹방법이다[5]. 특히 타인 메신저의 ID와 비밀번호를 해킹해 사기행위를 하는 것이 '메신저 피싱'이라 하며, 이는 사회공학 기법을 이용해 악성파일을 손쉽게 감염 상황을 유발시킬 수 있도록 이메일, SNS 등을 통해 전파하는 방법을 취하는 것이 일반적이다. 이러한 경우 이메일에 특정 악성파일을 첨부하여 유포하는 방법을 취하거나 SNS의 경우 악성파일에 대한 다운로드 및 설치가 가능한 URL 등의 링크를 삽입하는 등의 방법을 취하는 것이 일반적이다[6].

Ⅲ. 메신저 해킹 공격

인터넷뱅킹 침해사고를 발생시키기 위한 전단계 준비작업으로 일반인들이 많이 사용하는 메신저에 대한 해킹공격을 준비한다.

3.1 메신저 설치

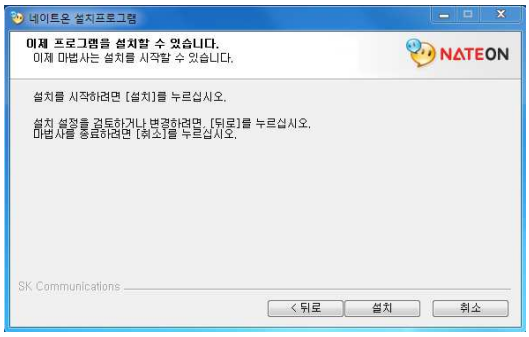

그림 2. 네이트온 설치 화면

그림 2는 일반인들이 많이 사용하는 메신저인 네이트온의 설치 장면이다. 네이트온이 설치된 지인을 파악하여 메신저를 이용하여 대화를 나누거나, 악성코드 파일을 전송한다.

3.2 지인 메신저 해킹

인간 상호 작용의 깊은 신뢰를 바탕으로 정상 보안 절차를 깨트리기 위해 지인에게 이메일을 통해 그들의 약점과 도움을 이용한다. 따라서 악의적 목적으로 악성코드가 담겨있는 파일을 지인에게 보낸다. 이때 악성코드가 인터넷 백신에게 감지되지 않게 하기위해 압축을 하여 감지를 우회하여 전달한다.

그림 3. 악의적인 파일의 전송

3.1 지인 메신저 ID, PW 계정탈취

지인의 메신저 ID, PW 계정을 탈취하기 위하여 이메일을 통해 파일을 전달한다. 파일을 전달받은 사용자는 그림 4와 같이 압축을 풀고 해당 악성코드를 클릭하는 순간 강제적으로 해커가 설정한 해당 포트를 Listen 상태로 동작시켜 세션을 형성 시키게 되고 해커는 지인의 Shell 권한을 획득하게 된다.

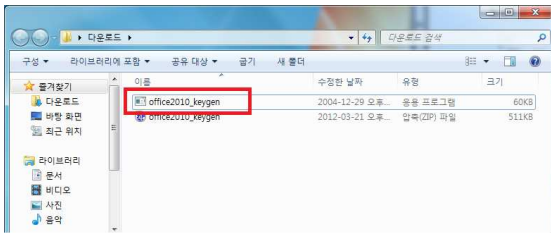

그림 4. 이메일을 통해 전달받은 악성코드 파일

그림 5는 악성코드를 클릭하고 난 후의 서비스 현황이다. 강제적으로 Remote 서비스가 활성화가 된 것을 확인할 수 있다. 해당 remote 서비스는 희생자가 발견하여 강제적으로 종료하기 전까지 활성상태이며 해커는 지속적으로 해당 포트로 접근이 가능하다.

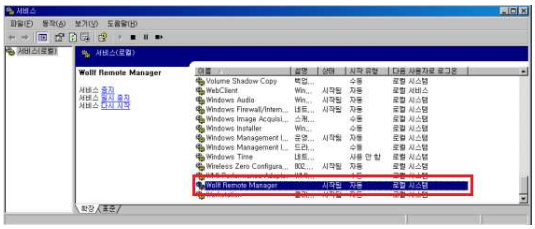

그림 5. 서비스 목록

따라서 그림 6와 같이 Windows의 Command 창이 활성화되고 이 창을 이용해서 지인의 PC에서 동작하고 있는 행동들과 내부 디렉토리로 접근할 수 있다.

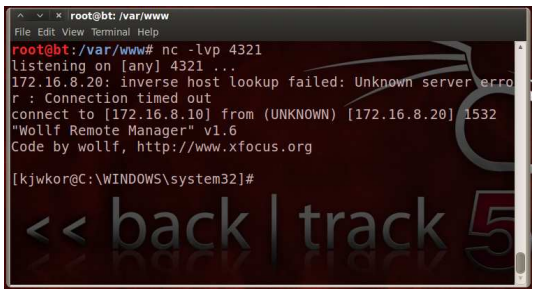

그림 6. 지인 Shell 권환 획득

그림 7에서 희생자는 네이온을 접속하기 위해 아이디, 비밀번호에 해당 자신의 ID, PW를 입력하게 되고 입력된 값은 공격자가 설치해둔 해킹툴로 인해 TXT 파일 형태로 저장되게 된다.

그림 7. 네이트온 설치 화면

해커는 키로깅 프로그램을 통해 희생자가 입력된 값을 원격으로 TXT파일로 저장하게 설정을 하고 저장된 값을 원격지에서 불러들여 접속 시 사용된 ID, PW를 그림 8과 같이 탈취한다.

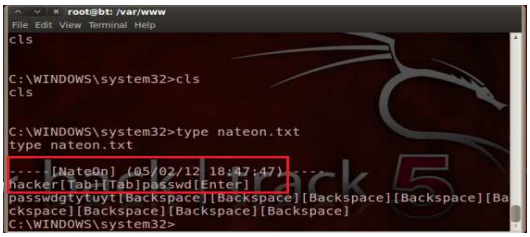

그림 8. 네이트온 계정정보 탈취

Ⅳ. 인터넷뱅킹 해킹 공격

4.1 인터넷뱅킹 해킹 공격 준비

악성코드를 통해 희생자 PC의 OS, IP주소 등의 정보를 확인하고 취약점을 확인하여 PC를 감염시켜 그림 9와 같이 희생자 PC에서 일어나는 이벤트들을 실시간으로 확인한다. 이 때 사용되는 해킹도구는 Backtrack5의 탑제되어 있는 armitage라는 툴을 이용한다.

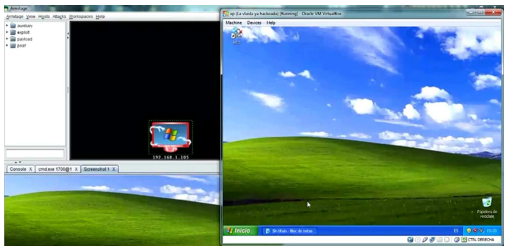

그림 9. 사용자 PC 감염

4.2 보안카드 해킹 공격

그림 10. 보안카드 정보 탈취

현재 해킹 대상의 PC에는 보안카드와 공인인증서가 저장된 상태에서 공격을 시도한다. 따라서 그림 10과 같이 PC에 스캔되어 저장되어 있는 보안카드의 정보를 통해 금융거래 시 입력정보를 확인하도록 한다.

그림 11. 인증서 해킹

그림 11과 같이 지인의 계좌에서 금전적 피해를 발생시키기 위해 PC에 저장되어 있는 인증서와 키로깅 툴을 통해 입력되는 인증서 암호를 획득하여 금융거래를 시도한다.

4.3 인터넷뱅킹 침해사고 공격 분석

그림 12와 같이 희생자가 금융거래 통해 입력한 출금계좌, 계좌비밀번호, 자금이체 비밀번호 등의 획득한 정보들을 입력하고 금액을 인출하여 피해를 발생시킨다.

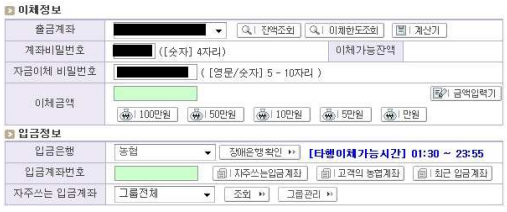

그림 12. 희생자 계좌에서 금액 인출

Ⅴ. 인터넷뱅킹 해킹 공격에 대한 보안대책

5.1 보안대책 제시

사회공학 기법은 이메일, SNS뿐만 아니라 매우 다양한 형태로 일반 사용자에게 악용될 수 있으며, 이렇게 사회공학 기법에 제대로 대처하지 못한다면 악성파일에 감염되어 예측할 수 없는 피해를 입을 뿐만 아니라 본인의 부주의로 인해 다양한 대상에게서 여러 가지 피해 상황이 발생할 수 있다. 이러한 사회공학 기법을 이용한 악성파일의 경우 애초부터 사용자를 속이기 위해 고안되고 제작된 만큼 사용자 스스로 감염되지 않도록 관심을 가지고 아래와 같은 "보안 관리 수칙"을 준수하는 등의 노력이 필요하다.

- 사용 중인 운영체제 및 각종 S/W의 대한 최신 보안패치를 생활화 하도록 한다.
- 신뢰할 수 있는 보안 업체에서 제공하는 백신을 항상 최신 엔진 및 패턴 버전으로 업데이트하여 실시간 감시 기능을 "ON" 상태로 유지해 사용.
- 출처가 불분명한 이메일의 첨부파일에 대한 다운로드를 지양하도록 한다.
- 인터넷 이용 시 출처가 불분명한 링크의 경우 해당 링크 접속 주의한다.
- 연말연시, 명절 등과 같은 사회적 이슈 기간에는 사회공학 기법을 이용한 악성파일 유포에 대한 관심을 갖고 주의하도록 한다.
- 금융거래, 메신저 등 사용되는 ID, PW를 주기적으로 변경한다.
- 알려진 취약점을 이용한 해킹에 대한 지속적인 관리가 필요하다.

5.1.1 패스워드 관리

업무 담당자의 단말기 및 개인용PC는 화면보호기를 설정하고 패스워드를 6자리 이상으로 설정하여 사용하여야 한다. 또한 분기 1회 이상 패스워드를 변경하여 사용하여야 한다.

5.1.2 방화벽시스템의 설치

전자금융거래에 사용되는 시스템이 존재하는 정보통신망(내부망)은 EAL3+ 이상의 CC인증 또는 이에 준하는 침입차단시스템을 설치하여야 하며 개인정보 및 중요 정보가 포함되어 있을 않은 경우(DMZ망)는 EAL2이상의 CC인증 또는 이에 준하는 침입차단시스템을 설치해야 한다. 침입탐지시스템은 전자금융업자의 영위여부 및 규모 등을 고려하여 설치할 수 있으며 설치 시에는 EAL2 이상의 CC인증 또는 이에 준하는 시스템을 설치해야 한다.

5.1.3 웹 서버 취약성 점검

금융거래가 이루어지는 웹 서버는 외부에서 항시 접근이 가능하므로 취약성이 존재할 경우 이용자의 중요 정보가 유출될 수 있으므로 사고가 발생하기 이전에 사전점검 및 취약성을 파악하여 예상되는 공격시나리오와 사고시 대처 방안들을

모색하도록 한다. 또한 금융업자는 다음과 같은 웹 서버에 취약점을 점검하도록 한다.

- 악의적인 명령어 주입 공격(SQL Injection)
- 업로드 취약점
- 취약한 세션 관리(Cookie Injection)
- 악의적인 명령 실행(XSS)
- 부적절한 환경설정 취약점

5.1.4 암호화 전송

금융거래는 공개된 인터넷 망을 통하여 이루어지므로 해커는 이러한 정보를 이용해 침해사고를 발생시킬 수 있다. 따라서 데이터 전송 중 사용자 개인정보 (성명, 주민번호와 같은 개인을 식별할 수 있는 정보) 및 금융거래정보가 유출되거나 변조될 수 있으므로 SSL(Secure Socket Layer)을 이용하거나 상용 암호화 프로그램을 이용하여 암호화하여 전송하도록 한다.

5.1.5 보안프로그램 설치

PC에 설치된 악성코드 및 프로그램이 이용자가 입력하는 비밀번호, 개인정보 등의 중요정보 외부 유출하는 것을 차단하기 위한 개인용 침입차단시스템 및 키보드 해킹방지프로그램을 설치하도록 한다.

5.1.6 금융거래 기록 보존

전자금융업자는 이용자와의 거래 정보가 변조되거나 이상이 없는지에 대한 문제를 해결하기 위하여 금융거래와 관련된 시스템 및 어플리케이션의 기록을 보존하도록 한다.

5.2 보안대책 적용후 해킹공격

보안 백신 사용 및 OS 최신으로 업데이트를 통해 해당 악성코드는 해당 PC에서 압축을 푸는 순간 실시간으로 검출되었다. 또한 OS 업데이트로 인해 해당 OS 취약점이 보완됨으로써 사용자 PC를 보안할 수 있었다.

5.3 보안성 검증

표 1. 보안성 검증

검증 사항	검증 내용
패스워드 관리	패스워드를 주기적으로 관리하여 지속적인 피해를 막고, BruteForce 공격에 대비하여 금융피해 감소
방화벽시스템의 설치	IDS, IPS의 설치 등을 통해 인가되지 않은 외부인으로부터 침입차단 및 침입탐지
웹 서버 취약성 제거	웹 서버에서 존재하고 있는 OS의 취약점, 응용프로그램의 취약점을 제거함으로써 해커의 접근을 통제
암호화 전송	해커가 사용자 PC의 키로깅 프로그램 설치를 통해 입력되는 값의 암호화를 통해 원격지에서 평문 확인 불가능
보안프로그램 설치	보안 프로그램 설치 시 악성코드 및 해킹 툴을 점검하여 사용 불가능
금융거래 기록 보존	침해사고 시 사건에 대한 역추적 및 포렌식 증거자료로 보안·보존

VI 결 론

본 논문에서는 사회공학적 기법을 이용하여 지인에게 악성코드 파일을 전달하여 사용자 ID, PW를 탈취하고 인터넷 뱅킹, 주식거래, 안전결제를 사용할 때, 원격지에서 정보를 탈취하여 침해사고를 발생시키는 해킹 기법에 대해 연구하였다.

따라서 개인정보가 포함되어 있는 내용의 파일들을 PC에 암호화가 되지 않은 상태로 보관하지 않도록 주의해야 하며 해커로부터 침해당하지 않도록 보관하며, 암호는 주기적으로 변경하여 지속적인 피해를 당하지 않도록 주의한다.

향후 연구에서는 금융거래시 SSL 암호화를 스니핑하여, e-mail, 인터넷 뱅킹, 주식거래, 안전결제시 해킹을 하는 연구가 필요하다.

참고문헌

[1] 이규안, 박대우, 고청심, “과학수사를 위한 디지털 포렌식,” GS인터비젼, 2011년 2월.

[2] 이정호, “전자금융 침해사고 예방 및 대응 강화 방안,” 한국정보보호학회, 제18권 제5호, pp.1-20, 2008년 10월.

[3] 고원봉, “윈도우 포렌식 실전 가이드,”한빛미디어, 2010년 10월.

[4] “2011년 3/4분기 국내 인터넷뱅킹 서비스 이용현황,” 한국은행 공보자료, 2011년 8월.

[5] “2012년 3월 인터넷 침해사고 동향 및 분석월보,” 한국인터넷진흥원, 2012년 3월.

[6] 성재모, 이수미, 노봉남, 안승호, “이용자의 금융거래정보 보호를 위한 확장 종단간(End-to-End) 암호화 기술과 보안고려사항,” 정보보호학회논문지, 제20권 제4호, pp.145-153, 2010년 8월.