인터넷 뱅킹에서 악성코드를 이용한 피싱에 관한 연구

김지현* · 이동훈*

*고려대학교 정보보호대학원

Survey on Phishing using Malicious Code in Internet Banking

Ji Hyun Kim* · Dong-hoon Lee**

*Graduate School of Information Security,Korea University

E-mail : mmlpl@korea.ac.kr

요 약

피싱 공격의 유형은 역동적으로 변화하며 위협모델도 급속히 변화한다.피싱은 지속적인 변화를 거듭하면서 대응책이 나올 때마다 지능적인 사기범들은 이를 교묘히 피할 수 있는 새로운 공격기법을 개발한다. 최근 그 중 인터넷 뱅킹의 피싱기법이 날로 고도화되고 있으며 인터넷 뱅킹에서의 악성코드를 이용한 피싱기법이 기승을 부리고 있다.본 논문에서는 이에 대한 대응책을 마련하는데 도움이 되기 위하여 2장에서 피싱의 의의와 공격유형에 대해 알아보고3장에서 인터넷 뱅킹에서 악성코드를 이용한 피싱에 관한 구체적인 분석 4장에서 본 논문의 결론을 서술하겠다.

ABSTRACT

The type of phishing changes rapidly and also threat model changes very fastly Accordingly, frauds develop new methods of attacks to avoid the counterparts. Recently, the type of phishing in internet banking is developing specifically..In this paper, to help encounter for it, we first review the meaning of phishing and the types of attacks in phishing in the second chapter,and in the third chapter, we will analyze phishing which is using malicious code in internet banking,and in the fourth chapter, we will describe the conclusion of this paper.

키워드

인터넷 뱅킹에서 악성코드를 이용한 피싱,피싱의 공격유형, 유포경로, 피싱사이트, 악성코드

Ⅰ. 서 론

피싱은 개인정보(Private Data)와 낚시(Fishing)의 합성어로 민감한 개인정보,금융계정 정보를 절도하는 신종 금융사기수법이다.피싱 공격의 유형은 역동적으로 변화하며 위협 모델도 급속히 변화한다. 피싱은 지속적인 변화를 를 거듭하면서 대응책이 나올 때마다 지능적인 사기범들은 이를 교묘히 피할 수 있는 새로운 공격기법을 개발한다. 그 중 인터넷뱅킹의 피싱기법이 날로 고도화되고 있다.최근 악성코드를 이용한 피싱기법이 기승을 부리고 있다. 본 논문에서는 이와 같은 인터넷 뱅킹에서의 악성코드를 이용한 피싱에 대해 분석한다.

논문의 구성은 다음과 같다. 2장에서는 피싱의 의의와 공격유형에 대해 알아보고 3장에서는 악성코드의 정의와 종류 그리고 4장에서는 인터넷 뱅킹에서의 악성코드를 이용한 피싱에 관해 분석해 보겠다.

Ⅱ. 피싱의 의의와 공격유형

피싱은 개인정보를 뜻하는 Private data와 낚시의 의미를 갖는 Fishing의 합성어이다.[1] 피싱은 전자우편

* 본 연구는 지식경제부 및 한국인터넷진흥원의 “고용계약형 지식정보보안 석사과정”지원사업의 연구결과“지원사업의 연구결과로 수행되었음

또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장함으로써 사용자의 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 사회공학의 한 종류이다. 피싱사고에 대한 신고가 늘어남에 따라 피싱을 막으려는 연구가 진행되고 있다. 피싱은 공격 방법에 따라 E-mail피싱 공격, 파밍 공격,숨겨진 공격 등으로 구분된다.

2.1 E-mail 피싱 공격

피싱은 1996년 American Online(AOL)의 메신저를 사용하는 해커들이 일반 사용자에게 조작된 전자우편을 보내는 해킹기법에서 유래되었다. 이 해커들은 자신이 보낸 전자우편을 AOL이 발송한 것처럼 속이고 사용자들은 전자우편을 보고 사용자들의 계정정보를 빼냈다. 이러한 피싱공격을 막지 못하는 이유 중 하나는 웹브라우저나 메일 관리 프로그램의 주소창과 링크 연결에 있어서 취약점들을 가지고 있기 때문이다. 피싱 공격을 당할 때 웹브라우저의 웹브라우저의 주소창의 URL과 링크가 스푸핑되어 실제 기관과 매우 유사한 주소를 보여주기 때문에 메일을 받은 사용자가 웹사이트의 진위여부를 바로 판단하기는 어렵다. 또한 사용자가 URL정보가 맵핑되어 있는 이미지 위로 마우스를 올려놓았을 때 웹브라우저 하단에 보여주는 링크 정보도 악의적인 링크가 아닌 정상적인 링크라고 보여주기 때문에 사용자들이 쉽게 속을 수 있다.[1]

2.1.2 URL스푸핑 공격 및 IP주소 접속 공격

URL주소 스푸핑은 인터넷 브라우저에 표기되어 있는 주소를 속여 특정 악성 사이트를 정상적인 사이트처럼 방문하여 이용할 수 있도록 하는 변조공격의 일종이다. 이 것은 사회공학적 공격기법과 기술적인 기법이 병합되어 있는 방법으로 방어하기가 까다로운 기법이다. 일반적인 피싱 공격 과정과 유사하나, 사용자에게 스푸핑된 URL을 보여주는 악성코드가 들어 있는 메일을 발송한다는 점이 일반적인 피싱공격과는 다르다.

공격자는 피싱 공격에 이용할 목표 사이트를 선정하고,유사 사이트를 제작한다. 그리고, 제3의 서버를 해킹하여 유사사이트를 설치하고,URL을 스푸핑하는 코드가 담긴 악성 메일을 발송하여 피해자의 접속을 유도한다. 피해자가 위조된 사이트로 로그인하거나, 혹은 개인정보 변경화면을 통해 개인정보를 변경하면 이 정보는 공격자에게 전해지고, 피해자는 다시 정상적인 사이트로 이동된다. 공격자는 피해자에게 받은 개인정보 혹은 계정과 패스워드를 통해 정상적인 사이트에 접속하고, 이를 이용해 이득을 취한다.

2.1.3 파밍공격

파밍은 피싱이 사용자나 관리자에 의해 쉽게 탐지되는 점을 보완한 신종 공격 기법이다. 파밍은 다양한 공격방법을 통해 정당한 사용자나 관리자가 특정 도메인에 대한 IP주소 확인 요구시, 해커가 장악하고 있는 악의적인 웹사이트의 주소를 제공하도록 하여 해당 웹사이트로 접속되도록 유도하는 공격기법을 의미한다.[2] 파밍 공격은 URL을 속이는 기법이 아닌 DNS또는 프록시 서버의 주소를 직간접적으로 변조한다. 파밍으로 이용될 수 있는 방법은 DNS주소의 변조, 클라이언트 DNS서버 설정 주소 변경,등록된 도메인의 정보 변경, 프록시 서버 이용, DNS Cache Poisoning등의 방법이 있다. DNS주소를 변경시키게 되면 기존의 피싱 공격보다 사용자의 판단은 더욱 어려워지고 믿고 접속할 가능성이 높아진다.

2.1.4 숨겨진 공격

숨겨진 공격에 가장 일반적으로 사용되는 공격은 숨겨진 프레임 공격과 Overriding Page Content 및 이미지 교체 방법이 있다. DHTML함수(DIV)를 이용하여 페이지에 위장된 페이지를 삽입하는 공격이 가장 많이 사용된다. 이 방법은 공격자가 실제 웹페이지 상단 위에 공격코드를 포함한 하나의 완전한 페이지를 생성하도록 할 수 있다. 그리고 간단한 HTML embedded commands를 사용하면 공격자가 사용자의 세션을 가로챌 수 있다.

이미지 교체 방법은 브라우저의 주소창 및 도구모음을 없애고 동일한 모양의 이미지를 표시함으로서 올바른 URL을 보여주거나 브라우저 좌측 하단의 HTTP통신을 HTTPS암호화 통신처럼 보이도록 이미지를 교체하여 사용자를 속이기도 한다. 이 기법은 인터넷 익스플로러7부터는 팝업창에 강제적으로 URL을 표시하는 기능에 의하여 인식이 가능하지만 인터넷 익스플로러 7이하의 버전을 사용하는 사용자는 피싱 공격을 당하기 쉽게 된다.

Ⅲ. 인터넷 뱅킹에서의 악성코드를 이용한 피싱

1. 유표경로 분석

온라인 뱅킹 정보 탈취 목적의 악성코드는 지금까지 2가지 유형이 확인되었다.

(1)침해사이트+ 응용프로그램의 보안취약점 결합

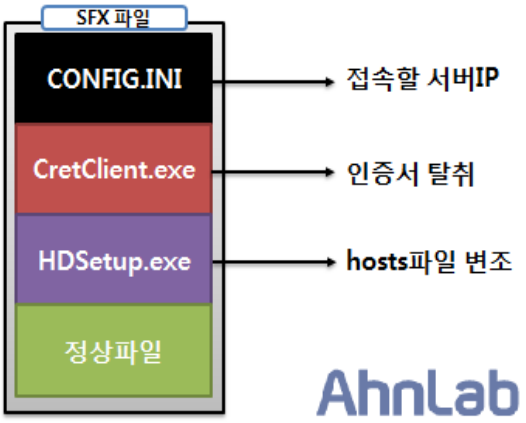
이 온라인 뱅킹 악성코드는 특정 URL을 통해서 유포됐다. 해킹된 국내 웹사이트(31개 사이트, 구글의 안전 브라우징 진단페이지)들의 응용프로그램(Java, IE, Flash Player, Windows Media Player)보안취약점을 이용하여 PC를 감염시켰다. 해킹된 국내 웹사이트들에는 제로보드를 사용한 공지사항 페이지에 악성 스크립트 링크가 삽입되어 있었다.온라인 뱅킹 악성코드의 유포 및 감염은 악성 HTML파일로부터 시작된다. 해당 HTML파일이 실행되면 또 다른 HTML파일을 다운로드 및 실행하는데 어떤 코드인지 확인이 어렵도록 난독화되어 있다. 이 악성HTML파일의 난독화를 해제하면 Java, IE, Flash Player의 취약점을 이용하는 것으로 보이는 코드들이 확인된다. 온라인 뱅킹 악성코드는 가능한 많은 PC를 감염시키기 위해 각 응용 프로그램의 버전을 체크하여 해당 버전에 존재하는 취약점을 사용한다.

응용 프로그램	취약점 ID
Java	CVE-2011-3544 / CVE-2012-0507
Flash Player	CVE-2011-2140 또는 CVE-2012-0754
Windows Media Player	MS12-004
Internet Explorer	MS10-018

(2)정상프로그램과 악성코드 리패키징

온라인뱅킹 악성코드가 특정 인터넷 라이브 방송 프로그램 P2P프로그램인 Torrent와 함께 리패키징된 채로 유포된 사례가 발견되었다. 온라인 뱅킹 악성코드가 유포될 당시에는 인터넷 라이브 방송 플레이어 다운로드 창의 '설치하기'를 클릭하면 악성코드가 포함된 Install_LiveManagerPlayer exe가 다운로드 됐다. 현재는 조치되어 유포되지 않는다.

uTorrent는 흔히 사용되고 있는 P2P프로그램 중 하나이며 누구나 손쉽게 다운로드할 수 있다. 온라인 뱅킹 악성코드 제작자는 이런 점을 이용하여 uTorrent.exe파일 내부에 정상 파일과 온라인 뱅킹 악성코드를 리패키징해 두었다. 이 악성코드는 실행파일인 EXE확장자를 가지고 있지만, 사실 SFX(자동 압축 풀림)형태로 〔그림 1-11〕과 같은 파일구조를 지고 있다.



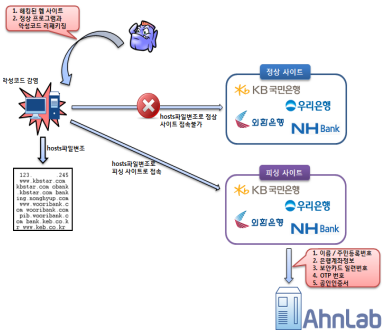
〔그림1-11〕온라인 뱅킹 악성코드의 파일 구조

해당 악성코드 실행 시 SFX옵션도 함께 실행된다. 악성코드가 실행되면 SFX파일에 존재하는 정상 파일이 실행된다. 하지만 백그라운드에서 C: \Windows 폴더에 악성코드가 생성 및 실행되므로 사용자는 악성코드 감염 사실을 인지할 수 없다.

2. 악성코드 분석

온라인 뱅킹 악성코드의 기본적인 형태는 SFX(자동압축 풀림)이나 실제 악의적인 기능은 SFX파일 내부에 존재하는 다음 3개의 파일에 의해서 수행된다. CONFIG.INI, CretClient.exe, HDSetup.exe.dl 세개의 파일은 핵심기능은 각각 나머지 두 파일에서 사용할 서버의 IP를 저장한 환경설정 파일, 특정 경로에서 인증서 존재 여부 검색 및 탈취 기능, 호스트 파일 변조와 삭제, 인터넷 익스플로러의 보안옵션 변경이다.

〔표1-5〕에서 설명된 3개의 파일은 각각 독립된 기능을 가지고 있지만 궁극적인 목표는 〔그림1-13〕과 같다.



〔1-13〕온라인뱅킹악성코드의 감염 흐름

(1)CONFIG.INI

CONFIG.INI는 CretClient.exe.HDSetup.exe가 악의적인 기능을 수행하는 데 필요한 IP를 저장하는 환경설정 파일이다.

(2)CretClient.exe

CretClient.exe는 사용자가 감염된 PC에서 피싱 사이트에 접속 시 실행되는 허위인증서 로그인 파일이다. 해당 파일을 단독으로 실행하면 허위 KB국민은행 인증서 로그인창이 뜨지만,피싱사이트를 통해 실행되면 대상 은행(국민은행, 우리은행, 농협뱅킹, 외환은행 등 총4곳)인증서 로그인 창으로 변경된다. 허위인증서 로그인 프로그램이 실행되면 사용자가 사용중인 인증서 정보를 출력하고 인증서 암호를 입력하도록 유도한다.

(3)HDSetup.exe

HDSetup.exe는 실행시 피싱사이트로 접속되도록 조작된 IP와 URL을 포함한 호스트 파일을 생성한다. HDSetup.exe가 실행되면 기존의 호스트 파일을 삭제하고 호스트 파일을 새로 생성한다. 이후 사용자가 감염된 PC에서 〔그림1-17〕에 명시된 은행으로 접속을 시도할 경우 정상 사이트가 아닌 피싱 사이트로 접속된다.

3. 피싱 사이트 분석

온라인 뱅킹 악성코드에 의해서 피싱대상이 되는 은행은 〔표1-6〕과 같다. 은행마다 조금씩 다르지만 피싱을 통한 사용자의 계좌정보탈취 프로세스는 다음과 같다. 피싱사이트 접속->허위인증서 로그인 입력->보안승급서비스->이름/주민등록번호 입력->계좌정보 입력.피싱사이트는 피싱사이트임을 알아볼 수 있는 증거들을 여러 곳에서 발견할 수 있다. 피싱사이트는 계좌정보를 입력할 때 보안카드에 명시된 모든 번호를 입력하라고 하지 않는다. 또한 공인인증서 로그인 과정에서도 수상한 부분이 많다.

피싱 대상 은행	대상 URL
국민은행	http://www.kbstar.com, http://kbstar.com http://obank.kbstar.com
농협	http://banking.nonghyup.com
우리은행	http://www.wooribank.com, http://wooribank.com http://pib.wooribank.com
외환은행	http://bank.keb.co.kr, http://www.keb.co.kr

또한 피싱사이트들의 보안 승급 서비스는 정상 은행 사이트와는 다르게 사용자에게 계좌의 보안카드의 모든 정보를 입력하라고 요구하지 않는다.〔4〕

Ⅳ.결 론

본 논문에서는 피싱의 의의와 공격유형, 최근 인터넷 뱅킹에 있어서 악성코드를 이용한 피싱기법에 대해 알아보고 분석하였다. 최근 기승을 부리고 있는 온라인 뱅킹 탈취 목적의 악성코드는 지금까지 2가지 유형이 확인되었다. 첫 번째는 피싱공격 유형 중 'URL 스푸핑 공격 및 IP주소 접속 공격'에 해당하는 해킹된 국내 웹사이트들의 응용 프로그램 보안취약점을 이용하여 PC를 감염시킨 유형이 있었고,두번째는 '숨겨진 공격 중 Overriding Page Content방법'유형에 해당하는 온라인 뱅킹 악성코드가 특정 인터넷 라이브 방송 프로그램 Torrent와 함께 리패키징된 채로 유포된 사례가 있었다.인터넷이 발전함에 따라 역기능으로 피싱으로 인한 개인정보 노출이나 금전적 피해 사례는 더욱 늘어나고 있다. 현재 상용 피싱 방지 솔루션들은 DNS스푸핑 및 DNS파밍 공격 등을 방어할 수 있지만 Overriding Page Content과 같은 코드의 변경을 통한 사용자 정보를 가로채는 기법을 방지하는 데에는 부족함이 있다.따라서 향후 과제로는 피싱의 공격유형 중 코드의 변경을 통한 사용자 정보를 가로채는 기법을 방지하는 상용 피싱 방지 솔루션을 개발하는 연구가 필요할 것이다.

참고문헌

[1]김주현, 맹영재, 양대헌, 이경희,"피싱 및 파밍 방지를 위한 인지 기반의 접근 방법", 정보보호학회논문지, 2009.2
[2]고 웅, 이동범, 곽진, "사전 검출을 통한 피싱 및 파밍 예방 시스템", 한국인터넷정보학회, 2008.11
[3]이응용, 김윤정, 조규민, "피싱 위협 및 대응방안", 정보통신연구진흥원
[4]안철수 연구소, "ASEC리포트 [2012년 Vol.30]", 2012-07-24, 2012.07