가상키보드에 대한 스크린 키로거 구현 및 그 대응방안

조진우, 양환석, 이병천

중부대학교 정보보호학과

Implementation of screen key-logger for virtual keyboard and its countermeasures

Jinwoo Joe, Hwan Seok Yang, Byoungcheon Lee

Department of Information Security, Joongbu University

요 약

가상키보드는 키로거를 이용한 키보드 해킹을 방지하기 위하여 도입된 기술로 우리나라에서는 금융권을 비롯하여 많은 웹사이트들에서 널리 사용되고 있다. 이 논문에서는 가상키보드를 사용하는 환경에서도 키로깅이 가능한 이미지 캡처 기능을 이용한 스크린 키로거를 설계하고 직접 구현해 보았다. 이것을 국내외 여러 웹서비스들에 적용해본 결과 대부분의 사이트들이 이러한 스크린 키로거에 취약함을 알 수 있었다. 이러한 공격에 대처하기 위해서는 스크린 키로거의 위험성을 인지하고 이러한 악성코드에 감염되지 않도록 조심해야 하며 이미지 캡처를 방지할 수 있는 솔루션의 사용 등의 대응책이 필요하다고 생각된다.

I. 서론

키로거(keylogger)는 사용자의 키보드 이용 내역을 기록하고 공격자에게 전달하는 기능을 갖는 악성코드로서 사용자의 패스워드 해킹 등에 사용될 수 있어서 오늘날의 전자상거래 환경에서 큰 위협이 되고 있다. 키로거는 계정 탈취를 위한 다른 기법들과 비교했을 때, 많은 정보를 손쉽게 탈취할 수 있으며, 피해자가 알아차리기 어렵기 때문에, 공공장소와 같이 많은 사람들이 사용하는 공간에서는 피해가 커질 수 있다.

키로거는 원리상 하드웨어 키로거와 소프트웨어 키로거로 나누어볼 수 있다. 하드웨어 키로거는 키보드와 본체 사이에 하드웨어 제품을 설치하여 사용하는 방식으로서 백신이나 안티 키로거 제품으로 탐지가 어려운 실정이다. 소프트웨어 키로거는 DLL Injection, 메모리 해킹, 키보드 드라이버 해킹 등의 기법을 이용하여 사용자의 키보드 사용내역을 기록하고 공격자에게 전달하는 방식이다.

우리나라의 인터넷뱅킹, 전자상거래 환경에서는 안티 키로거 제품을 설치하여 사용하도록 운영되는 경우가 많은데 키로거에 의한 공격을 완벽하게 방어하는 것은 어려운 실정이다. 백신 프로그램은 알려진 키로거만 탐지할 뿐 키로거의 행위자체를 탐지하지는 못하며, 안티 키로거 제품들은 하드웨어 키로거를 탐지하지 못하는 단점이 있다.

키로거의 위협에 대응하기 위해 중요한 정보는 마우스로 입력하게 하는 그래픽 기술 기반의 가상키보드(virtual keyboard) 기술을 사용하기도 하는데, 해커들은 키로거에 원격뷰어 기능을 추가하여 가상키 입력값을 실시간으로 볼 수 있게 하여 이를 무력화하였다.

우리는 원격뷰어기능이 공격자가 실시간으로 보고 있어야 한다는 점이 불편하다고 생각하여 이를 좀 더 효율적으로 구현하기 위해 가상키보드를 사용하는 순간을 이미지 캡처하는 방식

으로 스크린 키로거를 설계하였고 이를 구현하였다. 이를 이용하여 국내외 주요 웹사이트들의 취약성을 분석한 결과 대부분의 웹사이트들의 키보드 사용내역을 추출할 수 있었다. 이러한 위협을 방지하기 위한 대응방법에 대한 의견을 제시하였다.

II. 관련 기법

키로거는 하드웨어 키로거와 소프트웨어 키로거로 나누어 볼 수 있다.

하드웨어 키로거는 키보드의 USB 단자와 본체의 USB포트 사이에 끼워 넣어서 하드웨어 단에서 키입력 값을 가로채는 기법으로 백신이나, 안티 키로거 등 소프트웨어적인 방법으로는 검출이 불가능하며, 비교적 쉽게 구할 수 있으므로 큰 위협이 된다.

〈그림 1〉. 하드웨어 키로거 제품인 '타입 세이프'

소프트웨어 키로거에서는 사용자의 키입력을 추출하기 위해 주로 다음의 4가지 기법이 활용되는데, 메모리 해킹, DLL Injection, 드라이버 해킹, 특정 프로세스 함수를 후킹해 SSL 암호화 전 데이터를 훔치는 기법이 있다.

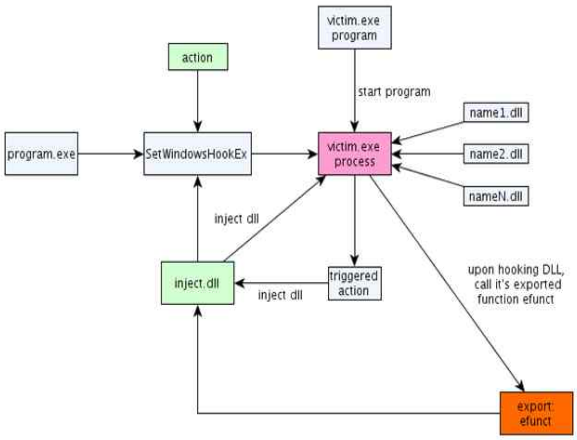
1) 메모리 해킹 기법은 실행중인 프로세스의 메모리속의 키입력 값을 탈취하는 기법으로, 현재는 메모리속의 값을 암호화하거나, 접근불가능하게 만드는 기법으로 대응이 가능하다.

2) DLL Injection을 이용하는 기법에서는 SetWindowsHookEx라는 함수를 이용하여 활성화된 프로세스들에게 DLL을 Injection 시키고, OS 메시지큐가 어플리케이션 메시지 큐로 전달하는 중간 과정을 가로챔으로서 전달되는 값을 변조, 차단, 기록하는 등의 기법을 이용한다. DLL Injection 기법을 활용한 키로거는 독립된 키 입력경로를 사용하거나, 키보드 값을 변조, 암호화하는 방법으로 대응이 가능하다.

3) 드라이버 해킹 기법은 기존 키보드 드라이버를 드라이버 형태의 키로거로 대체하거나, 우선순위를 조작하여 먼저 실행되도록 하여 키입력 값을 가로채는 기법으로, 별도의 보안드라이버를 사용하는 방식으로 대처할 수 있다.

4) SSL 후킹을 이용한 기법은 특정 프로세스의 소켓 관련 함수를 후킹하여 SSL 암호화 전의 HTTP 데이터를 훔치는 기법이다.

아래의 그림은 DLL 인젝션 기법을 사용한 키로거가 실행될 때 호출되는 과정을 보여주고 있다.



〈그림 2〉. SetWindowsHookEx 원리

III. 키로거 구현

3.1 키로깅 프로그램 구현

키로깅 기능은 DLL Injection 방식을 이용한 기법으로 구현하였으며, SetWindowsHookEx 함수를 이용해 운영체제와 어플리케이션 사이의 메시지큐를 Hooking 하여 키값이 전송될 때마다 이것을 저장하도록 하였다.

이를 위해 우리는 DLL 파일을 두 개 제작하였는데 KeyHook.dll 파일은 키보드의 키 값을 읽어와 저장하는 역할을 하며 MouseHook.dll 파일은 화면 캡처를 담당한다.

또한 키로깅 데이터를 수집하기 위해 원격명령전송서버(C&C)도 구현하였다. 키로거는 두 DLL의 Export 함수를 읽어와 실행해 후커를 설치하고, C&C와의 통신을 담당하여 명령수신, 파일전송 등의 역할을 담당한다. C&C 서버의 주요 기능은 키로거에게 탈취한 파일 수신요청

을 하거나, Process Block 명령을 전달하는 등의 역할을 한다. 그리고 감염된 해당 클라이언트에서 특정 프로세스의 실행을 방지하기 위해 Process Block 기능을 추가하였다.

그리고 SSL 후킹으로 키로깅 가능한 툴을 제작하였는데 여기에서는 SSL 함수를 후킹하여 SSL 암호화 전의 데이터를 추출해내는 기능을 한다.

3.2 가상키보드 스크린 캡처 기능 구현

우리는 사용자의 가상키보드 사용 순간을 화면 캡처하는 방식으로 키로거를 구현하기로 하였다. 이를 위해 Mouse Hooking 기법을 이용하기 위해 SetWindowsHookEx 함수로 Hooker를 설치한 후, 운영체제와 응용프로그램 사이의 마우스 메시지를 감시할 수 있도록 하였고, 화면 캡처와 관련된 모든 행위는 Injection 되는 DLL내에서 동작하도록 구현하였다.

실행중인 응용프로그램은 설치된 Hooker로 인해 마우스 인터럽트가 발생할 때 마다 DLL이 Injection 되고, Injection 된 DLL 내에서는 WM_LBUTTONDOWN 메시지가 도착할 때마다 현재 Foreground 프로세스의 캡션을 확인하고 특정 캡션을 포함하는(예 : 로그인, 은행 등) 문자열을 가지고 있다면, 순간 화면의 DC(Device Context)를 얻어 BITMAP형태로 변환하고 마우스 포인터를 메모리 DC에 추가한 후 BMP 파일로 저장하도록 구현하였고, 저장된 파일에 순번을 붙여서 순서를 알기 쉽도록 하였다.

키로거 프로그램은 DLL Injection 기법을 이용한 것과 SSL 후킹 기법을 이용한 것의 2가지 툴을 제작하였는데, 화면 캡처 기능을 추가한 스크린 키로거는 DLL Injection 기법을 사용한 툴에 포함되어 C&C 와의 통신이 가능하게 하였고, SSL 후킹 기법을 이용한 툴은 실험을 위해 별도로 제작하였다.

3.3 실험 및 결과

이러한 키로거 프로그램은 악성코드 형태로 사용자 컴퓨터에 감염시켜야 할 것인데 기존의 백신 프로그램에서 검출이 가능한지 확인해보아야 한다. 우리가 제작한 키로거 프로그램들과 DLL Injection에 사용되는 DLL들을 Virus Total[6]에 업로드하여 테스트해 본 결과 61개 백신 중 탐지율은 1~2건에 불과하였으며, 그 탐지원인도 인증서명이 없는 경우에 대한 경고였다. 그러므로 시그니처 기반으로 동작하는 기존의 백신 프로그램으로는 우리가 제작한 새로운 키로거의 탐지가 어렵다는 것을 알 수 있었다.

〈그림 3〉,Virus Total에서의 DLL 탐지 결과

다음의 <표 1>은 키로거 프로그램을 테스트한 실험 대상을 사용한 Browser, 적용한 웹사이트로 정리한 것으로, 가상키보드 기능을 이용하는 웹사이트를 위주로 가용한 모든 브라우저를 이용하여 테스트하였다. 이 중에서 키보드 보안모듈이 적용되지 않은 웹사이트는 G 사와 N2 사이다.

〈표 1〉. 실험 대상

브라우저	웹사이트
FireFox	G 사
Chrome	P 사
iExplorer	B 사
Safari	W 사
Opera	K 사
	N1 사
	N2 사

P사 같은 경우는 키보드 보안 모듈이 존재하였지만, DLL Injection 기법이 유효했다.

B사의 경우는 키보드 보안 모듈이 설치되어 있으며, 로깅은 되지만 값이 변조되어 로깅되는 특징이 있었다. 그러나 SSL 후킹을 적용하면 정상적으로 탈취가 가능하였고, 화면 캡처 공격 역시 유효하였다.

W사는 DLL Injection 기법으로는 공격이 되지 않았고, SSL Hooking 기법을 적용하면 계속해서 브라우저가 강제 종료되는 현상이 일어나 정확한 확인이 불가능하였지만, 에러 내용을

분석해본 결과 별도로 메모리를 차단하는 솔루션이 작동하는 것으로 추측되었다. 그러나 화면 캡처 공격을 이용하면 탈취가 가능하였다.

다음의 <표 2>는 DLL Injection, SSL Hooking, 화면 캡처 기법으로 7개의 웹사이트를 대상으로 공격해본 뒤 해당 기법으로 키로깅이 가능한지 여부를 정리한 것이다.

〈표 2〉. 실험 결과

	DLL Injection	SSL Hooking	화면캡처
G사	O	O	O
P사	O	O	O
B사	X	O	O
W사	X	X	O
K사	X	X	O
N1사	X	X	O
N2사	O	O	O

실험 결과 키보드 보안 모듈이 없는 게임이나, 웹사이트의 경우는 DLL Injection 기법으로 쉽게 키로깅이 가능했다. 키보드 보안 모듈이 적용된 일부 은행이나 카드사와 같은 경우에는 로깅이 되더라도 값이 바뀌거나 혹은 쓰레기 값이 저장되어 키로깅이 실패하는 경우도 볼 수 있었다.

가상키보드를 사용하는 환경에서는 우리가 구현한 화면 캡처를 이용한 스크린 키로거를 적용해 보았는데 모든 경우에 키로깅이 가능하였으며 화면 캡처를 방지하는 별도의 모듈은 감지되지 않았다.

아래의 <그림 4>는 키보드 보안 모듈이 적용된 W사의 가상키보드 입력시 화면 캡처 기반의 스크린 키로거를 적용하여 공격한 결과 가상키보드 입력화면이 캡처되어 공격자의 컴퓨터로 전송된 것을 보여준다.

〈그림 4〉. 캡처된 가상키보드 입력화면

IV. 대응 방안

4.1 키로거 감염 예방

스크린 키로거가 공격에 널리 이용될 수 있는 환경이라면 일반 사용자 입장에서는 키로거 감염에 주의를 기울여야 한다. 무엇보다 보안이 의심스러운 사이트의 접속 및 출처가 불분명한 파일을 다운로드하지 않는 등의 주의가 필요하다.

공공장소에서의 컴퓨터 사용시 중요한 정보 입력은 자제하는 것이 좋으며, 사용 전 컴퓨터의 뒷면의 키보드 포트를 관찰하여 하드웨어 키로거가 설치되어 있는지 여부를 관찰할 필요성이 있다.

4.2 화면 캡처 방지 기능의 이용

이러한 화면 캡처 기반의 스크린 키로거를 방지하기 위해서는 화면 캡처를 방지하는 솔루션을 사용할 필요가 있다고 생각된다. 현재 화면 캡처 방지는 고려되지 않고 있으므로, 웹서비스 제공사에서는 해당 보안솔루션 설치를 안내할 필요가 있다.

화면 캡처 방지 솔루션 구현에 관한 이종혁의 논문[5]에서는 윈도우 키입력을 감시하여 특정키를 차단하거나, Black List방식으로 알려진 캡처 프로그램이 감지된다면 강제 종료하도록 구현하였는데, 이는 알려진 화면 캡처 프로그램은 막을 수 있겠지만, 새로운 캡처 프로그램이나, 앞서 우리가 구현한 화면 캡처 기능이 자동으로 수행되게 내장된 프로그램에는 유효하지 않다.

캡처 방지 솔루션의 원리를 조사해본 결과 주로 사용하는 기법은 API Hooking 기법을 이용해 비트맵 저장에 사용되는 함수 BitBlt 함수를 이용하여 GetObjectType 함수를 호출, 반환값이 OBJ_DC (Device Context)일 경우에만 원본 함수를 호출하지 않은 방식을 택하고 있다.

하지만 일부 솔루션은 캡처에 사용되는 또 다른 함수인 PrintWindows 함수를 후킹하지 못하는 경우도 있고, DirectX를 활용하거나 Media API를 활용하는 등의 여러 가지 방식의 캡처 방법이 있기 때문에 이를 모두 방지해야 한다.

이러한 원인들로 인해 화면 캡처 방지 솔루

션은 어느 정도는 방어가 가능하지만, 화면 캡처 공격을 완전히 차단하는 것은 어려울 수 있다. 오히려 스크린 키로거의 화면 캡처 기능을 방지하기 위해 운영체제의 기본기능인 화면캡처 기능을 동작하지 못하도록 운영한다면 사용자에게 큰 불편을 끼칠 수도 있음을 고려해야 한다.

4.3 가상키보드 대체 기술 이용

취약성이 존재하는 가상키보드 기능을 사용하지 않는 것도 좋은 해결 방법이다. 가상키보드에 입력하는 대신 별도의 신뢰할 수 있는 통신채널을 통해 정보를 전달하는 멀티채널 통신 기능을 이용할 수 있다. 또는 일회용패스워드(OTP) 기술을 이용하면 입력하는 값이 매번 바뀌기 때문에 키로거를 이용하여 정보를 수집하더라도 재활용이 불가능하게 된다. 보다 근본적인 대책으로는 고급 암호 및 인증기술을 사용하여 암호키를 보유해야만 인증정보를 보낼 수 있도록 운영할 필요가 있다. 이러한 대체기술은 별도의 절차와 비용이 필요하다는 단점이 있다.

V. 결론

지금까지 가상키보드 사용에 대한 취약성을 제시하기 위하여 스크린 키로거를 직접 설계, 구현하였고, 제작한 프로그램을 이용하여 가상키보드를 사용하는 웹사이트들의 취약성을 분석해 보았다. 그 결과 모든 실험 대상 웹사이트에서 사용자가 가상키보드를 사용하는 순간을 이미지 캡처하여 주요 정보를 획득하는 것이 가능하다는 것을 보였다.

이러한 공격을 방지하기 위해서는 별도의 화면 캡처 방지 솔루션을 사용할 수 있겠는데 운영체제에 화면 캡처 방법이 다양하게 존재하여 모든 경우를 방지하는 것은 어려울 수 있으며, 오히려 운영체제의 기본 편의기능인 화면캡처 기능을 사용하지 못하도록 하여 사용자의 불편을 초래할 수 있다는 단점이 있다. 화면캡처 공격에 의한 위험성이 커진다면 가상키보드 기능의 사용을 중지하고 대체 보안기술을 사용할 필요가 있다고 사료된다.

향후 이미지 캡처 기능을 이용하는 다양한 공격의 가능성 및 시스템의 취약성에 대해 지속적인 연구개발을 수행할 계획이다. 특히 크게 확대되고 있는 모바일 환경에서도 이러한 취약점이 있을 수 있는지 조사해 볼 계획이다.

[참고문헌]

[1] 김상형, Windows API Conquest, 2013

[2] Choi,In-Young, “Real-Time Detection of Information Leakage by Kelogger&Design and Implementation of Keylogger Detection Solution”, 2015

[3] 금융ISAC, “키보드 해킹 기법 및 대응기술 분석”, Nov 2005

[4] 신영진, “개발자를 위한 후킹테크닉“, 2007

[5] 이종혁, “개인 정보 보호를 위한 화면 캡처 방지 모듈 구현”, 한국정보통신학회논문지, Vol. 18, No. 1, pages 91-96, 2014

[6] 바이러스토탈, https://www.virustotal.com/