情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

스파이웨어에 대한 고찰

박 호 진*

요 약

우리는 언제부터인가 개인용 컴퓨터에 개인정보와 같은 민감한 데이터를 사용자의 동의 없이 수집하거나 성가시게 혹은 불쾌한 광고를 출력하는 프로그램들로 가득차 있는 것을 자주 경험하고 있다. 이러한 모든 행동들은 사용자의 적절한 동의 절차 없이 이루어졌다는 것이 가장 근본적인 문제이고 바로 여기서부터 문제를 해결해 나가야할 것이다. 그러나 법적으로 스파이웨어(Spyware)가 명확히 정의되어 있지 않고 그나마 (구)정보통신부에서 발표한 문건은 하루가 멀다 하고 새롭게 변화하는 스파이웨어들에 법적인 구속력을 적용하기 힘든 것이 현실이다. 이 글에서는 현재 국·내외에서 스파이웨어가 어떻게 정의되고 있는지 알아보고 스파이웨어를 정의하기 위해 필요한 기술적인 배경을 살펴봄으로써 보다 효율적인 법안을 마련하는 데 도움이 되고자 한다.

Ⅰ. 서 론

개인용 컴퓨터(Personal Computer, 이하 PC)가 인터넷과 연결되면서 PC 사용자가 할 수 있는 작업은 무수히 많아졌다. 반면 이러한 이유로 PC보안의 취약성은 급격히 높아졌으나 이에 대한 대비책이 미비한 상태이다. 슬래머(Slammer) 웜에 의한 1.25 인터넷 대란 같은 사건을 계기로 보안에 관심을 가지기 시작했지만 최근 국내 최대 오픈 마켓의 회원정보가 유출되는 사건이 발생한 것처럼 아직도 보안에 대한 인식이 미비한 실정이다. 이번 개인정보 유출사건은 고난이도의 기술력을 동원한 것이 아니라 스파이웨어를 유포시켜 타겟 시스템에 접근할 수 있는 아이디와 비밀번호를 얻어 가능했던 것으로 알려졌다.

스파이웨어가 PC에서 발견된 것은 그리 오래전의 일이 아니다. 정보의 위험(Risk)은 단순히 정보의 가치로만 따지는 것이 아니라 정보가 유출되거나 손실되었을 때 입는 피해(Business Impact)에 따라 결정되는 것이기 때문에 스파이웨어가 수집하는 개인정보의 유출이 얼마나 큰 위험을 가지고 올 수 있는지 인식하고 있었더라면 사고를 예방할 수 있었을 것이다.

현재 스파이웨어에 법적 구속력을 발휘하기 위한 정확한 잣대가 없고 (구)정보통신부에서 발표한 "스파이웨어 기준"은 점차 고도화되고 사회공학적 기법이 접목되어가는 스파이웨어들을 효과적으로 대처하지 못하고 있는 것이 현실이다. 이렇다 보니 스파이웨어를 진단, 치료하는 국내외 제품들이 많아 졌지만 사실 이러한 프로그램과 함께 더욱 근본적으로 스파이웨어를 대응할 수 있는 기반을 마련하는 것이 우선시 되어야 할 것이다.

더욱이 안티-스파이웨어 프로그램이 스파이웨어로 진단하는 대부분의 프로그램들은 회사에서 개발된 프로그램이지만 정작 해당 업체에서는 개발한 프로그램이 어떤 이유로 스파이웨어로 진단되는지 인식하지 못하고 있다.

이번 원고에서는 현재 국내·외에서 통용되고 있는 스파이웨어의 정의와 스파이웨어들이 사용하는 기법들에 대해 살펴보고 보다 더 명확한 스파이웨어를 정의하고 관련 법과 제도를 만드는 데 초석이 되었으면 하는 바람이다.

Ⅱ. 스파이웨어의 정의

국내외 또는 안티-스파이웨어 업체에 따라 스파이웨어에 대한 정의나, 스파이웨어 진단 범위, 진단 기준이 서로 다르다. 실제로 스파이웨어라는 용어 이외에도 다

* 안철수연구소 ASEC(Ahnlab Security e-Response Center)팀 선임연구원 (hojinpk@ahnlab.com)

양한 용어들이 사용되고 있기도 하다. 이 장에서는 스파이웨어 관련 용어들을 살펴봄으로써 스파이웨어를 바로 알고 세계적인 동향을 알아보고자 한다.

2.1 국내

현재 스파이웨어에 대한 정의는 국내·외 할 것 없이 다양하게 사용되고 있다. 스파이웨어(Spyware)는 첩자를 뜻하는 스파이(spy) 와 소프트웨어(software) 의 합성어이다. 이 용어는 미국의 인터넷 광고전문회사인 라디에이트(Radiate)에서 개인 사용자의 취향을 파악하기 위해 처음 개발된 프로그램을 일컫는 용어로 사용되었지만 최근에는 개인을 식별할 수 있는 개인정보(IP주소, MAC Address, 개인 아이디나 패스워드 등)를 수집하는 등 점차 악화되고 있는 스파이웨어들을 통칭하는 용어로 사용된다.

미국은 1995년 Usenet 에 올라온 글에서 스파이웨어를 처음 사용하였고, 우리나라의 경우 2000년 한국통신 ADSL 이용자 동호회 홈페이지에 올린 글에서 스파이웨어의 존재에 대해 언급하여 인식하기 시작했다.

스파이웨어는 광의와 협의로 구분되어 사용되고 있다. 광의의 스파이웨어는 위 [표 1]과 같이 적절한 사용자 동의 절차 없이 사용자 PC에 설치되어 불법적인 행동을 하는 것들이다. 대중매체에서 사용하는 스파이웨어는 대부분 광의의 스파이웨어를 말하는 경우가 많다. 협의의 스파이웨어는 일반적인 스파이가 하는 것처럼 개인정보와 같은 정보를 갈취하는 것으로 "스파이웨어류"라고 지칭한다.

〔표 1〕 광의의 스파이웨어 분류

구 분	활 동 목 적
스파이웨어(Spyware)류	개인정보 및 민감한 데이터 수집
애드웨어(Adware)	광고 노출
다운로더(Downloader)	원격지의 특정 파일을 다운로드 및 실행
드롭퍼(Dropper)	실행파일내부에 다른 실행파일을 품고 있다가 떨어뜨린 후 실행
다이얼러(Dialer)	전화접속 연결 설정을 변경하여 비싼 요금을 부과하는 인터넷 연결을 시도
클릭커(Clicker)	주로 사회공학적 기법을 사용하여 마우스 클릭을 유도
익스플로잇(Exploit)	취약점을 이용하여 악성코드를 실행
조크(Joke)	악의성은 적지만 지나친 장난으로 당황하게 만듦.

최근에 "악성코드(Malicious Code)"라는 용어가 사용되고 있는데, 악성코드는 악의적인 행동을 할 수 있는 실행 가능한 파일로써 바이러스, 웜, 스파이웨어 등의 포괄적인 범위를 가진다. 대부분의 허위 안티스파이웨어 업체들은 당사의 제품이 실제로는 바이러스, 웜 등의 악성코드들을 진단할 수 없음에도 악성코드 치료 프로그램으로 소개하면서 이 용어를 남용하고 있다.

2.2 국외

국외에서도 스파이웨어라는 용어 자체는 국내와 거의 동일하게 사용되고 있지만 스파이웨어 이외의 관련 용어들을 많이 사용하고 있는 것이 특징이다. 앞에서 살펴보았던 광의의 스파이웨어를 가리키는 말로 안티-스파이웨어 국제연대기구인 ASC(Anti-Spyware Coalition)[1]에서 사용하는 PUP(Potentially Unwanted Program), StopBadWare[2]의 Badware가 있고, 트렌드마이크로사가 사용하는 그레이웨어(Grayware)가 있다.

또한 얼마 전 중국에서는 '깡패' 소프트웨어라는 용어를 사용하여 퇴치해 달라는 소송을 제기한 적도 있었다. 용어는 서로 다르지만 적절한 사용자 동의 없이 배포되어 사용자 권리를 침해할 수 있는 동작을 수행하는 것이라는 점은 동일하였다.

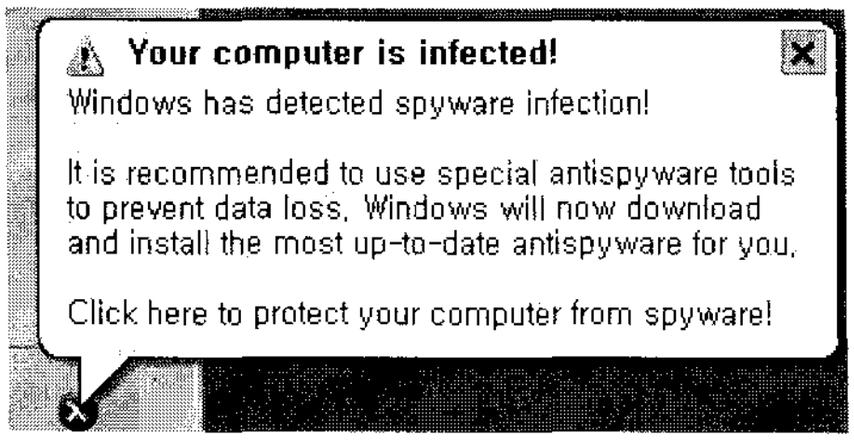
이렇듯 사용자가 원하여 설치했는지 여부 및 스파이웨어적인 행동을 기술적으로 증명할 수 있어야 하고, 이렇게 증명된 디지털 증거 자료들이 법적 증거자료로 인정받을 수 있도록 지속적인 연구 및 개발과 관련 법안도 함께 만들어져야 할 필요가 있다.

Ⅲ. 스파이웨어의 기술적 분석

여기에서는 스파이웨어가 사용하는 많은 기술적인 부분 중에서 특히 스파이웨어가 사용자 권리를 침해할 수 있는 일련의 작업들을 발생하는 순서대로 기술하고 각 부분을 우회하기 위해 사용되는 기술적인 배경과 함께 실제 스파이웨어의 예를 들어 설명하고자 한다.

3.1 프로그램 설치

프로그램이 사용자 PC에 설치되는 경우는 다음과 같이 크게 두 가지로 구분해 볼 수 있을 것이다.

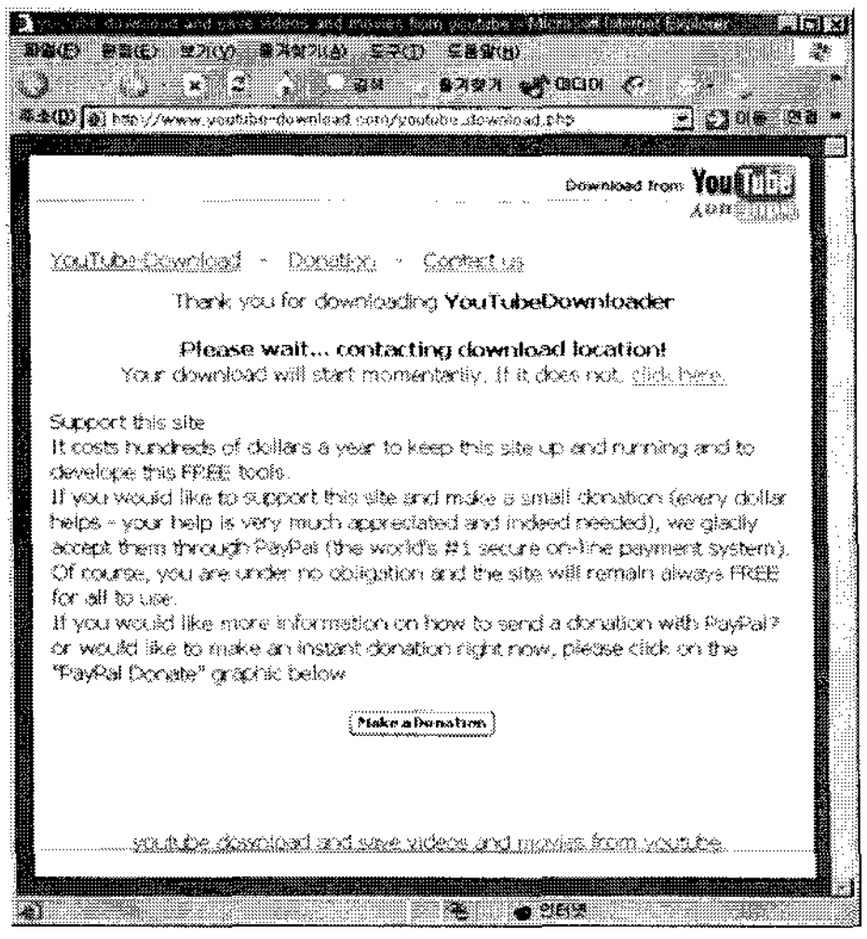


〔그림 1〕 사용자 PC가 스파이웨어에 감염되었다고 허위로 알림풍선을 띄우고 있는 화면

첫 번째로, 사용자의 요구에 의해서 프로그램 설치를 원하는 경우가 있을 것이고, 두 번째로 사용자의 의도와는 다르게 사용자의 PC에 프로그램이 설치되는 경우이다. 첫 번째의 경우 대부분 정상적인 프로그램으로 분류되고 있지만 두 번째의 경우 정상적인 프로그램과 악의적인 프로그램으로 구분해 보아야 한다. 여기서 정상적인 프로그램은 주로 금융권 사이트에서 ActiveX 컨트롤 형태로 설치되는 프로그램과 같이 사용자가 원하는 서비스를 받기 위해 특정 웹 페이지를 방문하게 되었을 때 설치되는 것들로 사용자의 요구에 의해서 프로그램이 설치되는 웹 페이지를 방문한 것만으로도 사용자 동의를 받았다고 볼 수 있다.

〔표 2〕 MS06-13 IE createTextRange 취약점 실행코드

```
<input type="checkbox" id='c'>
<script>
    r=document.getElementById("c");
    a=r.createTextRange();
</script>
```



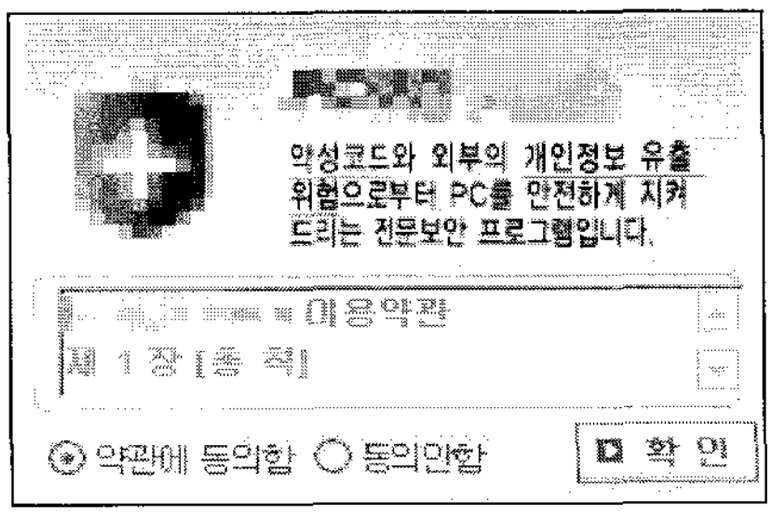
〔그림 2〕 YouTube를 사칭한 사이트

악의적인 프로그램의 경우 사회공학적 기법(Social Engineering)을 사용하는 것과 그렇지 않은 것으로 구분해 볼 수 있다. 먼저 사회공학적 기법이 아닌 것들로, 취약점을 이용하거나 사용자 인터페이스를 제공하지 않고 프로세스로만 동작하여 스파이웨어를 설치하는 경우가 있다. [표 2]는 마이크로소프트사의 인터넷 익스플로러의 특정 함수에서 이전에 사용하던 특정 메모리 지점의 값을 잘못 참조하는 메모리 에러(Corruption Error)가 발생하는 코드로 이러한 코드를 이용해 공격자가 원하는 코드를 실행시켜 스파이웨어를 설치한다.

최근에는 인터넷 검색 사이트에서 제공하는 인기검색어 TOP10 의 키워드를 이용해 불특정 웹 사이트 게시판에 글을 작성하여 검색 사이트 결과 해당 게시판이 노출되고 이를 사용자가 클릭하게 되어 악의적인 코드가 설치되는 등 사회공학적 기법이 많이 사용되고, 더욱 교묘해지고 있어 사용자들의 보안 인식이 더욱 필요해지고 있다.

3.2 사용자 동의

모든 스파이웨어는 적절한 사용자 동의 절차 없이 설치가 이루어진다. 적절한 사용자 동의를 받기 위해 약관을 제시하고 사용자 동의 여부를 확인하여 설치하여야 하지만 약관을 제공하지 않거나 약관을 제공하더라도 대부분의 사용자들이 약관을 정확히 읽어보지 않는 다는 점을 악용하여, 약관의 내용을 어렵게 하거나 약관을 읽기 힘들도록 작은 크기로 제공하는 경우 등이 허다하다.

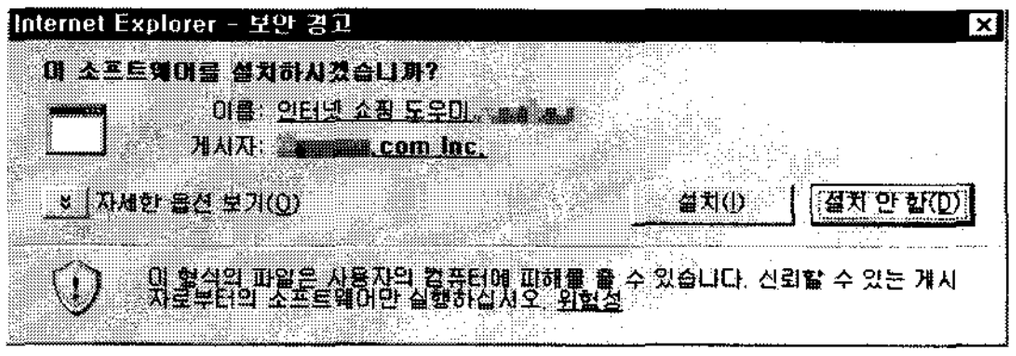


〔그림 3〕 약관을 기술한 윈도우가 너무 작아 약관을 읽어보기 힘든 경우

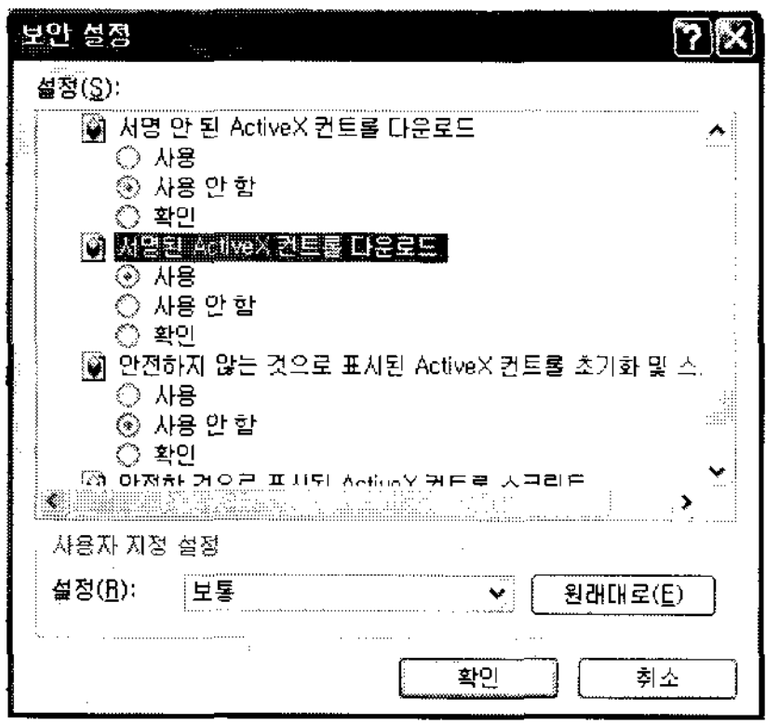
또한, 발견되는 대부분의 스파이웨어들은 웹사이트에서 ActiveX 컨트롤 형태로 배포되고 있다.

ActiveX 컨트롤이 설치될 때 인터넷 익스플로러의

설정에 따라 사용자에게 보안 경고 창이 표시되지 않을 수 있을 뿐만 아니라 ActiveX 컨트롤 보안 경고창 만으로 프로그램을 정확하게 소개하였다고 보기는 힘들다. 정보보호진흥원 에서 발표한 스파이웨어 사례집에서도 이러한 점을 명확하게 명시하고 있다.



〔그림 4〕 ActiveX 보안경고창



〔그림 5〕 ActiveX 보안경고창이 나타나지 않도록 인터넷 익스플로러의 보안 설정을 변경하는 화면

약관에 포함된 개인정보활용에 관한 항목에는 공정한 약관이라고 볼 수 없을 정도로 사용자에게 불리하게 기술되어 있는 것이 태반이다. 개인정보보호를 보호하기위해 국내·외적인 개인정보 강화 기술(Privacy Enhancing Technologies)에 관한 표준화 노력이 활발히 진행되고 있다. 그 중 P3P(Platform for Privacy Preferences) Project 는 웹사이트의 개인정보보호 정책을 표준(W3C P3P)에 의해 표기하면 사용자가 일일이 읽어서 확인할 필요 없이 사용자 에이전트가 자동으로 분석해주는 기술도 개발되고 있다. 2006년 P3Pv1.1가 발표되어 IBM, AT&T 등에서 P3P 표준을 소프트웨어로 구현하여 무료로 보급하고 있으며, W3C에 P3P 채택을 신고한 사이트가 미국, 호주, 영국, 독일 등 영어권 국가 중심으로 약 879여개이다. 국내에서는 현재 다음커뮤니케이션, 옥션, GS홈쇼핑, 야후에서 도입하고 있다. 또한 KISA에서 한국형 P3P 표준을 개발하여 시연회를 개최한바 있으며 홍보를 통해 보급 활성화 계획에 있다.[6]

3.3 설치과정 표시 및 설치 중단 기능

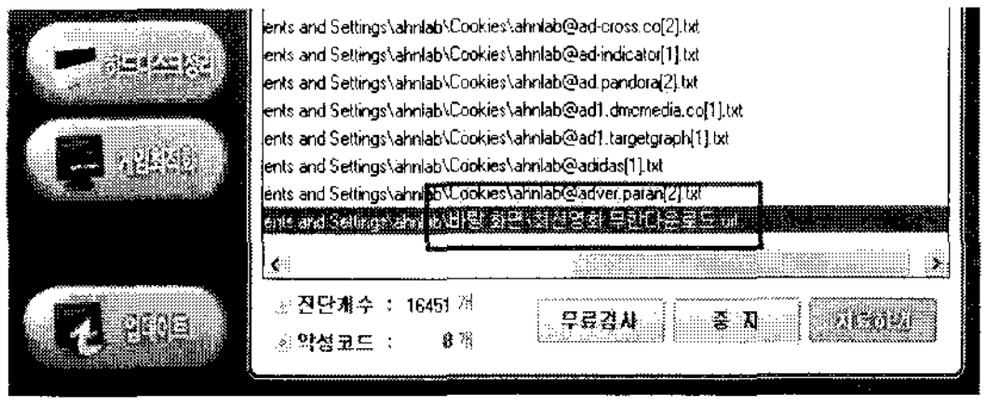
일반적으로 응용프로그램 설치과정에는 설치 진행 상태를 확인할 수 있는 사용자 인터페이스가 제공되어야 하며, 사용자가 중간에 설치 취소를 할 수 있도록 인터페이스를 제공해야 한다.

하지만 대부분의 스파이웨어들은 설치과정을 보여주지 않으며 설치를 중단할 수 없다는 것이 특징이다.

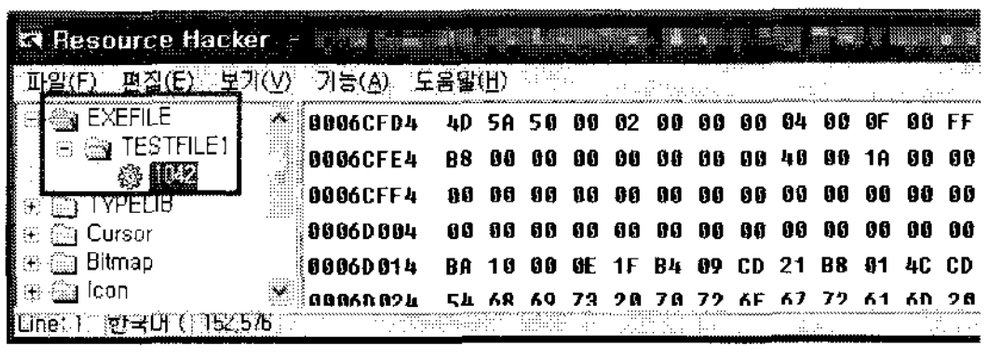
3.4 명시한 기능 수행

정상적인 프로그램들은 약관에서 명시한 기능을 충실히 수행하기 위해 많은 노력을 기울인다. 더욱이 사용자가 동의한 약관 이외의 기능을 추가할 경우 약관 변경을 공지하여 사용자에게 알려줄 의무가 있다.

하지만 악의적인 프로그램들은 약관을 제공하여 사용자 동의를 받고 있지 않을 뿐 아니라 위에서 소개한 허점을 이용하여 약관을 제공하고 있다고 주장하더라도 약관의 내용이 불공정한 약관으로 판단되는 내용이 많아 사용자들은 피해를 입고 있다.



〔그림 6〕 허위 안티-스파이웨어가 설치한 파일을 설치한 허위 안티-스파이웨어가 진단하는 화면



〔그림 7〕 실행 파일 안에 실행 파일을 숨겨서 몰래 떨어트린 후 실행하는 형태

이러한 정보들을 확인하기 위해서는 소프트웨어 역공학을 이용하여 실행 가능한 바이너리 데이터에서 코드를 얻어야 하고 이렇게 얻은 코드를 분석하여 알고리

〔표 3〕 역분석 대상 지정 방식

역분석 방법	설 명
문자열 검색	실행파일 안에 존재하는 문자열을 참고하는 코드 주위의 함수부터 관련된 함수로 이어지는 분석 방법
암호 초기값 검색	암호 알고리즘의 표준 논리는 같지만 구현할 때마다 코드가 달라질 수 있다. 하지만 스트림/블록 암호, 해쉬 알고리즘에서 사용하는 초기 상수 값 설정은 달라지지 않는 점[4]을 이용하는 방법
오픈 라이브러리 사용여부 확인	MS에서 제공하는 API나 오픈소스를 이용하여 스파이웨어를 제작했을 경우 해당 라이브러리 파일을 이용하여 역분석에 도움을 받을 수 있다.
조건 브레이크 포인터 설정	동적 분석 시 사용하는 분석 도구를 이용하여 조건 브레이크 포인터를 설정하여 수많은 경우의 수를 제외하고 분석하고자 하는 조건에서부터 분석하는 방법

즘을 이해해야하는 일련의 작업이 필요하다.

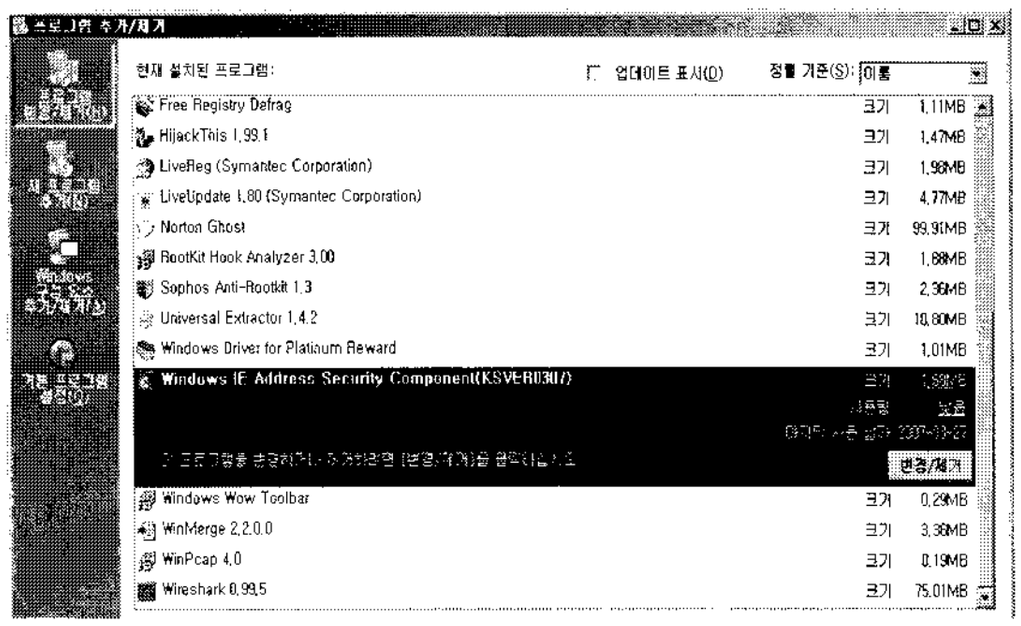
스파이웨어의 기능이 점차 고도화 되고 패키지화 되어가는 추세로 프로그램의 사이즈가 커지고 여러 동적 라이브러리를 사용하고 있어 더욱 많은 시간과 노력이 요구된다. 이런 환경에서 얻고자 하는 정보를 획득하기 위해서는 분석하고자하는 대상을 결정하고 활용할 수 있는 관련 자료를 최대한 활용해서 접근하여야지만 적은 시간과 노력으로 최대의 효과를 얻을 수 있다. [표3]에서는 방대한 양의 코드에서 분석할 대상을 찾기 위해 필자가 경험한 몇 가지 방법에 대해 간단히 소개해 보았다.

그러나 이러한 분석방법을 통해 명시한 기능을 위반하였다는 사실을 일반 사용자가 판단하기에는 상당한 컴퓨터 관련 지식을 필요로 하고 있어 이러한 사실을 꾸준히 관찰할 수 있는 연구기관을 활성화 하는 것 또한 법제도화와 같이 병행되어야 한다.

3.5 설치 제거

사용자 PC에 설치된 프로그램들은 "프로그램 추가/제거"에 기능을 제공하여 사용자가 원할 경우 언제든지 프로그램을 삭제할 수 있어야 한다. 하지만 스파이웨어들은 사용자 또는 안티-스파이웨어 제품들이 자신의 프로그램을 발견하거나 제거하는 것을 방해하기 위해 지속적으로 진화되고 있는 실정이다. 아래에서는 여러 기법 중 최근에 많이 사용되는 것들을 위주로 조사해 보았다.

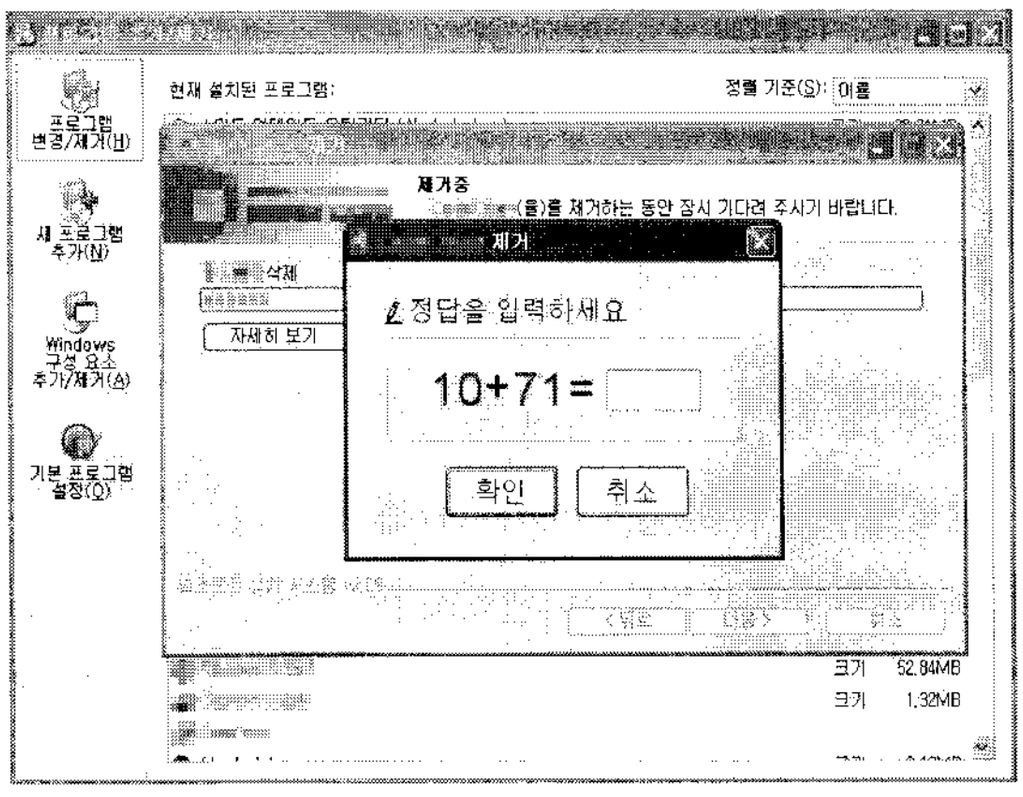
아래 [그림 8]은 스파이웨어가 설치 제거 방법을 제공하고 있지만 일반적인 사용자가 프로그램을 삭제하기 위해 "프로그램 추가/제거" 화면에서 해당 스파이웨어를 찾기 어렵게 만들기 위해 프로그램의 이름을 "Windows IE Address Security Component (KSVER0307)"로 표기한 경우이다.



〔그림 8〕 프로그램 추가/제거 항목에 마치 윈도우 정상 프로그램인 것처럼 프로그램 이름을 설정한 화면

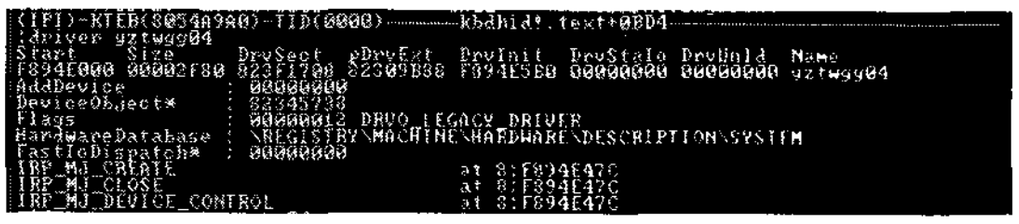
기술적으로 어렵지 않게 적용할 수 있지만 사용자를 속여 프로그램을 제거하는 것을 효과적으로 우회할 수 있을뿐 아니라 프로그램 제거방법을 제공했다는 명분도 챙길 수 있다.

아래 [그림 9]는 스파이웨어가 안티-스파이웨어와 같은 프로그램들에 의해서 기계적으로 삭제되는 것을 방지하기 위해 적용한 기법으로 프로그램을 제거하려고 하는 사용자가 간단한 산술계산의 정답을 맞혀야만 제거할 수 있다.



〔그림 9〕 프로그램 제거 시 덧셈 연산을 요구하는 화면

아래 [그림 10]은 스파이웨어가 삭제되는 것을 우회하기 위해 윈도우 시스템 드라이버로 등록되는 함수가 기본적으로 제공되어야 하는 언로드(Unload) 함수를 제공하고 있지 않아 일반적인 방법으로 시스템 드라이버를 중지하지 못하도록 설정된 화면이다. 이러한 시스템 드라이버를 제거하기 위해서는 특정한 IoControlCode를 해당 시스템 드라이버에 전송을 해야 하고 이 IoControlCode를 알아내기 위해서는 해당 프로그램을 제거하는 모듈을 역분석해야 했다. 물론 이 기능은 정상적인 프로그램에서도 사용되기도 한다.



[그림 10] 윈도우 시스템 드라이버의 언로드(Unload) 함수가 등록되어있지 않은 화면

지금까지 살펴본 것 이외에도 루트킷(Rootkit) 혹은 사회공학적 기법들을 동원하여 설치제거를 고의적으로 방해하고 있다.

Ⅳ. 스파이웨어 관련 법안 마련의 필요성

정부에서는 스파이웨어를 규제할 수 있는 법안으로 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 정보통신망법)을 적용하고 있으며 2005년 8월 (구) 정보통신부에서 스파이웨어 기준안을 발표하였고 이에 이어 2005년 11월 한국정보보호진흥원에서 스파이웨어 사례집[3]을 발표하였다.

내용을 살펴보면 정보통신망법에서 악성코드란 "정당한 사유없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램을 말함" 이라고 정의하였다. 그러나 "3장 스파이웨어의 기술적 분석"에서 살펴보아서 알 수 있듯이 스파이웨어는 다른 프로그램 등을 훼손·멸실·변경·위조하지 않는 경우가 매우 많다. 다른 프로그램의 운용을 방해하는 경우 스파이웨어로 분류되기도 하지만 스파이웨어 정의 영역에 극히 일부분이여서 수많은 스파이웨어들을 정보통신망법에 포함시켜 법적 구속력을 수행하기는 어렵다고 판단된다.

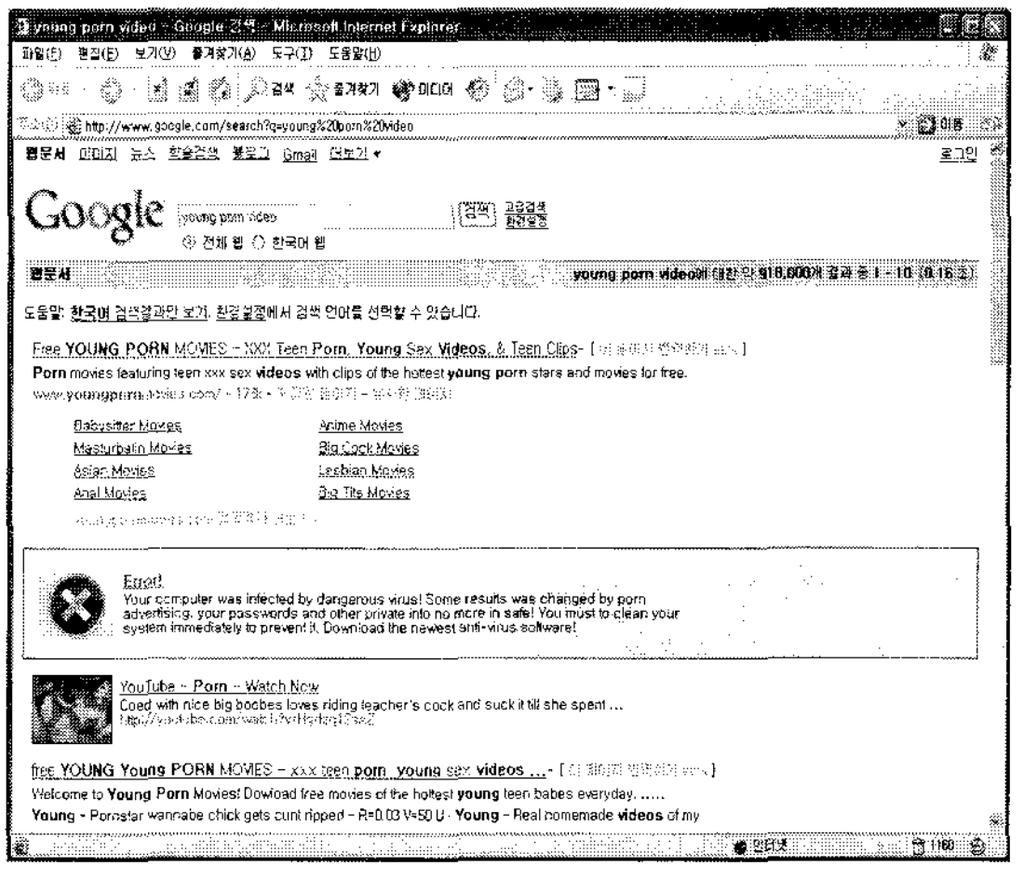
3장에서 살펴본 스파이웨어의 행동패턴들을 기반으로 스파이웨어를 판단하는 데 명확한 기준으로 삼을 수 있을 것이다. 그런데 만약 이러한 기준에 의해 스파이웨어로 판명된 프로그램의 제작 회사가 소송을 걸어 법적 분쟁이 발생할 경우 위에서 살펴본 사실들을 기반으로 증거자료를 준비해야 할 것이며, 이렇게 준비된 디지털 증거자료가 법적으로 인정받을 수 있도록 법안이 마련되어 있어야 할 것이다.

디지털 데이터는 위·변조가 매우 용이해 수집한 스파이웨어의 증거자료가 정말로 해당 스파이웨어에 의해서 발생된 것인지 증명하기 어렵다. 따라서 관련 정부기관에서는 위에서 다루었던 스파이웨어들의 특징들을 기반으로 유효한 증거자료를 수집할 수 있는 신뢰기관을 제공하거나 민간 기업에서도 법적 증거자료를 제작할 수 있는 프로토콜이 개발되어야 할 것이다.

Ⅴ. 스파이웨어가 끊이지 않는 이유

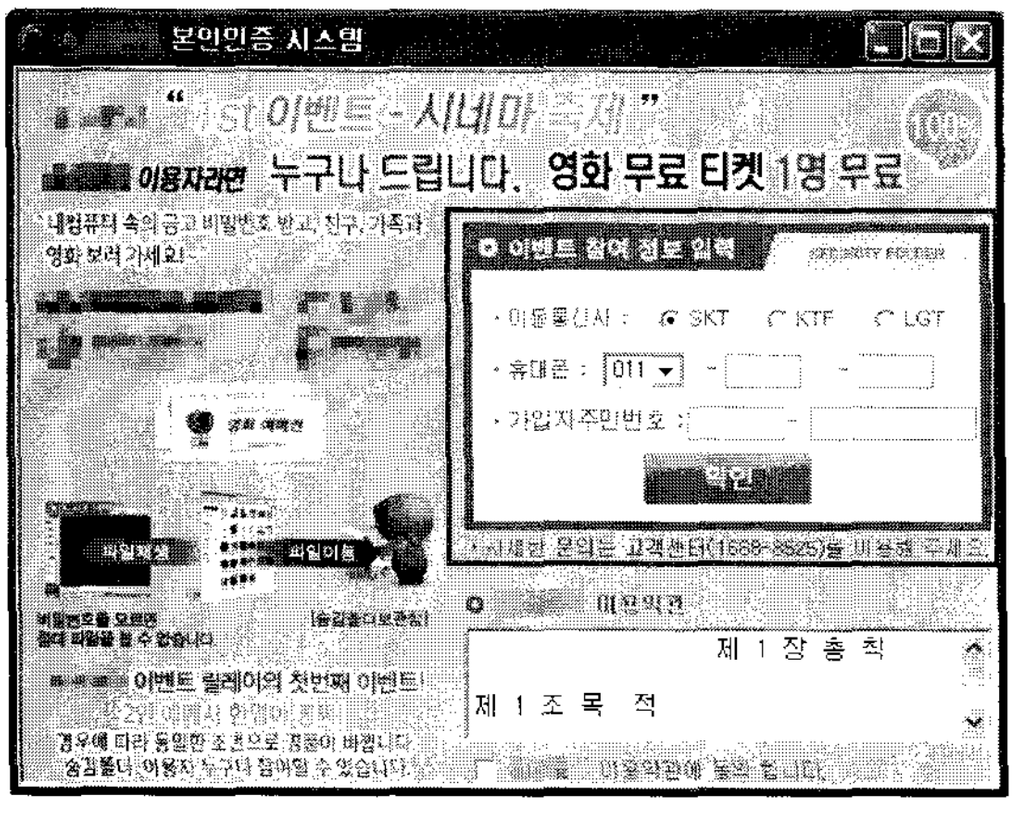
지금까지는 스파이웨어가 사용자 PC에 설치되는 일련의 과정을 살펴보았다. 이렇게 설치된 스파이웨어마다 다른 목적을 가지고 있는데, 이러한 목적들을 살펴보면 스파이웨어가 왜 계속해서 제작되는지 실마리를 찾을 수 있을 것이다.

아래 [그림 11]은 사용자가 검색사이트에서 특정 검색어로 검색했을 때, 검색 결과 상위에 스파이웨어가 원하는 결과를 삽입하여 사용자로 하여금 신뢰도가 높은 결과로 위조하는 화면이다. 사용자 검색을 위해 위조된 사이트링크를 클릭하게 되면 스파이웨어를 설치하도록 유도하는 웹페이지로 이동하게 된다.



[그림 11] 검색사이트의 검색결과를 변조하여 가장 많이 보는 사이트인 것처럼 검색결과 상단에 출력.

아래 [그림 12]는 사용자의 동영상 파일을 하나의 특정 폴더로 이동하고 사용자가 동영상을 보기위해 동영상파일을 클릭하면 유료사용을 요구하는 화면이다. 이렇게 사용자의 중요한 데이터를 볼모로 돈을 요구한 스파이웨어를 랜섬웨어(ransomware)라고 한다.



〔그림 12〕 사용자가 자신의 동영상을 보기위해 스파이웨어가 결제를 요구하는 화면

그 밖에 아래와 같이 다양한 방법으로 스파이웨어가 금전적 이익을 노리고 있다는 것을 알 수 있다.

- 불법적인 방법으로 광고를 출력하는 행위.
- 정상 프로그램에 번들로 설치.
- 프로그램 설치 회당 일정금액 지급.
- 프로그램의 고급 기능을 사용하기 위해 결제를 요구함. 또한 결제를 했을 경우 기본적으로 자동이체가 되어 추가적인 위험이 발생되고 있음.
- 특정 게임의 아이템을 팔아 부당 이득을 챙기기 위해 사용자의 게임 아이디와 패스워드를 수집하는 행위.
- 특정 검색어로 다량의 검색 쿼리를 검색사이트에 전송하여 인기 검색어 관련 사이트로 인식되고 검색사이트 상단에 출력하는 행위.

초기의 바이러스들은 제작자가 자신의 실력을 과시하기 위해 제작되는 경우가 많았으나, 점차 악성코드들이 돈과 관련되기 시작하였고 최근에는 바이러스(Win32/Viking)에 의해서 특정 게임의 계정을 수집하는 스파이웨어(Win-Spy ware/PWS)가 설치되는 경우도 있었다.

Ⅵ. 결 론

지금까지 살펴본 스파이웨어를 한마디로 정의하자면 "적절한 사용자의 동의 절차 없이 설치되고, 사용자가 원하지 않는 동작을 수행하는 소프트웨어"로 정의 할 수 있을 것이다.

지금까지 살펴본 스파이웨어들에서도 알 수 있듯이 점차 발전하는 컴퓨터의 기술과 교묘해지는 사회공학적인 기법들로 무장한 스파이웨어들을 보다 효과적으로 대처하기 위해서는 지속적인 기술적 분석과 함께 스파이웨어 제작자들에게 법적 구속력을 발휘할 수 있는 법안이 만들어져야 된다. 또한 이러한 법안은 스파이웨어 제작자들에게 자율 규제(Self regulation)를 이끌어 낼 수 있도록 강경한 법안을 만든다면 얄팍한 수법으로 법을 교묘히 피해가는 변형된 스파이웨어들을 예방할 수 있을 것이다.

한편 4장에서 간단히 살펴본 봐와 같이 디지털 증거자료가 아날로그 증거들보다 법적 증거로서 높은 허용성을 인정받기 위해서는 엄격하고 세밀한 허용성 판단 기준들이 필요하다. 미국의 경우 연방형사소송절차규칙과 연방증거규칙(FRE)에서 디지털 증거의 허용성에 대한 내용을 담고 있으며, 디지털 증거 수집·분석 절차에 대해 NIST(National Institute of Standard Technology) 에서 최초의 표준화된 디지털 증거 표준 가이드라인을 제시하고 이 가이드라인에 따라 증거 수집 및 분석이 이루어지도록 법적으로 보장하고 있다.[5]

2008년 5월 22일 17대 국회에서 "정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안"이 의결되었다. 이 법률안에는 개인정보를 유출하였을 경우 개인정보를 제공한 측과 제공받은 측 모두 처벌할 수 있는 법안이 마련되어 자율 규제(self regulation)를 유도하기 위한 관련 법안이 포함되어있다. 이번 법률개정안을 시작으로 개인정보 보호 및 안전한 인터넷 세상을 만들기 위해 하루빨리 관련 법안들이 만들어졌으면 하는 바람이다. 이와 동시에 소프트웨어를 제작하여 배포하는 업체에게 관련 법안을 근거로 안전한 소프트웨어를 제작하거나 배포하는 방법에 대해 권고안을 제공하거나 교육 기회가 마련된다면 더욱 바람직할 것이다.

참고문헌

[1] http://www.antispywarecoalition.org

[2] http://www.stopbadware.org

[3] 정보보호진흥원 스파이웨어 사례집 (http://www.boho.or.kr/infor_data/spyware.pdf) 11 page

[4] 김권엽, 최재민, 이산진, 임종인, "소프트웨어에 적용된 암호화 모듈의 역공학 분석에 관한 고찰", 한국방송공학회 동계 학술대회, Feb. 2007

[5] 백승조, 심미나, 임종인, "국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법제 현황", 정보보호학회지, Feb. 2008

[6] 전길수, 개인정보보호정책 설정 및 협상 기술 분석, 한국정보보호진흥원, Oct. 2006

〈著者紹介〉

박 호 진 (HoJin Park)

2001년 10월~2005년 6월 : (주)비씨큐어 암호기술연구소
2005년 6월~현재 : (주)안철수연구소 ASEC팀 선임연구원
2006년 2월 : 한국방송통신대학교 컴퓨터과학과 학사
2008년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 디지털 포렌식, 소프트웨어 역공학, 개인정보보호