韓國 컴퓨터情報學會 論文誌
第10卷 第4號, 2005. 9.

2005-10-4-3-2

# 스파이웨어의 위험관리에 대한 연구

김 상 균*

# Risks and Safeguards of the Spywares

Sang-kyun Kim*

## 요 약

스파이웨어는 개인의 동의없이 개인의 인터넷 및 PC사용 현황을 도청하는 소프트웨어를 의미한다. 미시적으로는 개인이 원하지 않는 정보를 개인에게 제공하거나 개인의 정보를 도청하는 것에서부터 거시적으로는 IT의 지향점인 유비쿼터스(Ubiquitous)와 컨버전스(Convergence) 환경으로의 진보를 막고 있는 거대한 위험으로 등장하고 있다. 본 논문에서는 스파이웨어의 정의, 현황, 위험분석 결과 및 현존하는 통제 수단들을 제시한다. 아울러, 향후에 적용 가능한 추가적 통제 수단들을 제시한다. 본 논문에서 제시한 스파이웨어의 위험분석 및 현존하는 통제 수단들에 대한 연구는 개별 기업 및 범국가적 차원의 스파이웨어 통제 체계 구축의 참조자료로 활용될 수 있을 것이다.

## Abstract

Spyware is any software which employs a user's Internet connection in the background without their knowledge or explicit permission. The installation of spywares is generally done in a sneaky, misleading or unannounced manner. It does not only compromise the security and privacy of affected users but also be an obstruction to the digital convergence and ubiquitous computing environments. This paper provides a summary of the definition, status, risk analysis, and security controls of the spywares. Furthermore, this paper suggests additional controls which should be considered at an individual, organizational and national perspective.

▸ Keyword : 스파이웨어(Spyware), 위험분석(Risk Management), 보안통제(Security Control)

---

• 제1저자 : 김상균
• 접수일 : 2005.07.20, 심사완료일 : 2005.09.05
* (주)소만사 이사

# Ⅰ. 서 론

스파이웨어는 바이러스, 웜과 더불어 개인의 정보시스템에 대한 최대의 위협으로 등장하고 있다. 바이러스, 웜에 대한 탐지 및 대응은 정보시스템 사용자의 대다수가 인식하고 있거나 사용 중인 바이러스 백신 프로그램에 의하여 처리가 가능하지만, 스파이웨어의 경우는 아직 침투경로, 피해유형 및 대응 방안에 대한 인식과 처리가 제대로 이루어지지 못하고 있는 상황이다. 또한, 기존의 바이러스 백신 및 유사 프로그램으로 스파이웨어에 대한 기술적 대응이 불가한 경우가 대부분이며, 침해형태가 개인 정보 유출로 직결되는 것이어서 더 큰 문제를 안고 있다.

본 논문에서는 먼저 스파이웨어에 대한 기본 개념을 파악하기 위하여, 스파이웨어의 정의 및 분류 방식에 대하여 정리하였다. 또한, 스파이웨어와 관련된 최신 확산 현황을 통해 스파이웨어가 장기적으로 어느 정도의 사회적 문제로 대두될지를 짚어보았다. 마지막 단계로는 스파이웨어에 대한 위험분석을 실시했다. 이를 통해 스파이웨어의 위험분석 방법론상의 위험목록을 정리했으며, 이에 대한 대응통제로써 현존하는 보안요소 및 향후 수행 가능한 통제요소들을 제시했다. 본 논문에서 제시한 내용을 통해 정보시스템의 개인 사용자들은 스파이웨어의 침투 경로 및 침해 내역을 파악하여 이에 대한 개인 차원의 대응을 할 수 있을 것이며, 기업 및 기관의 책임자는 조직내부의 스파이웨어 확산 및 침해에 대응하기 위한 관리적, 기술적 차원의 대응책을 수립할 수 있을 것이다.

# Ⅱ. 스파이웨어의 개요

## 2.1 스파이웨어의 정의

스파이웨어는 개인 또는 조직에 대한 정보를 그들 스스로 동의하거나 식별하지 못하는 상태에서 수집하도록 지원해주는 소프트웨어를 의미한다[1]. 스파이웨어는 컴퓨터 바이러스나 또는 새로운 프로그램 설치의 결과로서 컴퓨터에 잠입할 수 있다. 만약 그 사용자가 어떠한 데이터가 수집되고 있으며 그것이 누구와 함께 공유되고 있는지 등을 충분히 이해하고 있다면, 즉 사용자가 그 사실을 알고 있는 상태에서 설치된 데이터 수집 프로그램은, 정확히 말하자면 스파이웨어가 아니다[2].

## 2.2 스파이웨어의 설치 형태에 따른 분류

스파이웨어의 설치 형태는 실제 세상에서 산업스파이들이 도청장비를 설치하던 형태와 유사한 양상을 가지고 있다. 실제 세상에서 스파이들이 도청장비를 설치하는 방법은 크게 세 가지로 나눌 수 있다. 이는 잠입설치, 트로이안목마, 근거리 도청으로 나눌 수 있다[3]. 컴퓨터상의 스파이웨어도 이 세 가지 형태로 설치가 된다.

잠입설치의 대표적인 경우는 일반 사용자들이 자신의 배우자나 아이들의 컴퓨터 사용 내역을 감시하기 위해서 스파이웨어를 설치하는 경우이다. 다른 사용자가 자리를 비운 사이에 물리적으로 컴퓨터에 접근하여 수동으로 프로그램을 설치하는 것이다. 실제로 특정 인터넷 사이트 (http://www.spywareonline.org)에서는 일반인들이 구매할 수 있는 스파이웨어 프로그램들이 저가에 판매되고 있다.

대다수의 스파이웨어는 두 번째 방식인 트로이안목마 형태의 설치 방법을 따른다. 이는 프로그램의 원래 기능과 관련이 없는 스파이 기능을 프로그램 내부에 은닉하여 사용자가 자신이 설치하는 프로그램의 세부적인 기능 즉, 스파이웨어 기능이 있다는 것을 인식하지 못하는 상태에서 프로그램을 설치하는 것이다[4].

세 번째 형태인 근거리 도청은 스파이웨어의 형태 중 보편적인 형태는 아니다. 이는 사용자의 컴퓨터에 직접 스파이웨어를 설치하는 것이 아니라 사용자의 컴퓨터가 네트워크 사용을 위해서 경유하게 되는 다른 컴퓨터 또는 네트워크 연결장치 부분에 미리 스니핑 프로그램을 설치하여 사용자의 정보를 도청하거나 사용자가 원하지 않는 정보를 보도록 조작하는 기능을 수행한다.

## 2.3 스파이웨어의 침해 행위에 따른 분류

협의의 스파이웨어란 어떤 사용자에 관한 정보를 수집하여 광고업체나 또는 관심 있는 사람들에게 넘기기 위해 누군가의 컴퓨터에 비밀리에 잠입하는 프로그램을 뜻한다. 그러나 스파이웨어라는 명칭으로 다음과 같은 다른 형태의 악성 프로그램들을 광의적으로 통칭

하는 것이 점차 보편화되고 있다.

에드웨어(Ad-ware)는 사용자의 PC에 임의로 광고를 나타내주는 소프트웨어를 의미한다. 이러한 기능은 일반적으로 공개 또는 쉐어웨어에 포함된 경우가 많은데, 이러한 기능을 제공하며 벌어들이는 수익으로 공개 또는 쉐어웨어 개발자는 개발비용을 충당하게 된다. 일반적인 경우에는 사용자가 공개 또는 쉐어웨어의 설치와 함께 설치, 작동되는 애드웨어를 충분히 인지하고 동의하므로 큰 문제는 없다. 그러나, 문제는 애드웨어가 기본적으로 사용자 PC에 대하여 제작자가 접근할 수 있는 접근경로를 제공하는 것이므로, 이러한 접근경로를 제작자가 광고 표현 이외의 용도로 활용할 수 있다는 것이다[2]. 에드웨어에는 123Messenger, 123Search, 2020Search, A Better Internet, ACXInstall, AdBreak, AdGoblin, Adult Chat Dialer, Adult-Links, Aornum, AproposMedia, ASpam, Aureate, BargainBuddy, BDE, BlazeFind, BonziBuddy, BookedSpace, BrowserAid, BrowserToolbar, Bulla, Clearsearch, ClearStream, Accelerator, Click Till U Win, ClickTheButton 등이 대표적으로 포함된다.

브라우저 하이젝커(Browser Hijacker)는 사용자 PC 브라우저의 설정을 변경하는 소프트웨어를 의미한다. 가장 대표적인 것으로 시작페이지를 제작자가 원하는 사이트로 변경하는 경우이다. 또한, 사용자가 검색 페이지를 방문할 때 원래의 검색 페이지가 아니라 제작자가 설정한 제3의 검색 페이지가 뜨도록 하기도 한다[5]. 브라우저 하이젝커에는 2nd-thought, ActualNames, CoolWebSearch, GoHip, Httper, IETray, iGetNet, ILookup, Ineb Helper, ISTbar, LoadFonts, Masterbar, NavExcel, PRW, Realphx, SafeSearch, Seach Assistant, Searchex, ShopNav, SmartBrowser, Stop Popup Ads Now, Surfairy, Tellafriend, Whazit, Winshow 등이 대표적으로 포함된다.

브라우저 플러그인(Browser Plugin)은 인터넷 브라우저에 툴바 형태로 추가로 설치되는 모듈을 의미한다. 이러한 소프트웨어는 사용자의 인터넷 브라우징 내용을 제작자에게 지속적으로 알려주는 역할을 담당한다[2]. 브라우저 플러그인에는 Alexa Toolbar, Comet Cursor, EasyBar, Fastseeker, FavoriteMan, HotBar, Huntbar, IBIS ToolBar, Internet Marketing Toolbar Pro, Mirar, MySearch, Show Bar, UCmore, W97M_SPY.A, Web Behavior 등이 대표적으로 포함된다.

키로거(Key Logger)는 사용자가 PC에 입력하는 모든 키보드 입력 값을 가로채서 제3자에게 보내주는 소프트웨어를 의미한다. 기업내부에서 직원들의 키보드 입력 값을 로그(Log) 정보 관리 차원에서 보관하는 경우도 있지만, 개인이 해킹을 목적으로 이러한 소프트웨어를 제작, 배포하는 경우도 있어서 문제시 된다[6]. 키로거에는 2Spy!, 3rdEye, AB System Spy, Absolute Keylogger, AceSpy, Actions Monitor, Activity Logger, Activity Monitor 2002, Advanced Keylogger, Apophis, AppsTraka, Ardamax Keylogger, AtomicLog, Belkin PCSpy, BizDefender, Black Box, Boss EveryWare, Call Online Two, Catch Cheat Spy, Chat Watch, Chota, COM, Com Policy, Computer Snooper, ComputerSpy 등이 대표적으로 포함된다.

## III. 스파이웨어의 확산 현황 및 위험

### 3.1 스파이웨어의 확산 현황

뉴스헤럴드의 자료에 따르면 현재 전세계적으로 유포되고 있는 스파이웨어는 총 75,000개가 될 것으로 추산되고 있다[7]. 또한, 스파이웨어에 대한 정보 및 대응툴을 제공해주는 spywareguide.com 사이트에 등록된 잘 알려진 스파이웨어의 종류만해도 총 380여가지가 되며[2], PC Magazine 평가에서 에디터스 초이스에 선정된 스파이웨어 탐지 툴인 Spybot에서 탐지하는 스파이웨어의 종류만 800가지에 이른다[8].

합법을 가장한 전파 유형도 많이 발생하고 있다. 스파이웨어는 EULA(End User Licensing Agreements)에 대한 사용자의 부주의를 통해서 쉽게 전파되는 경우가 많다. 사용자는 새로 구매하거나 또는 인터넷에서 다운로드받은 무료 소프트웨어 설치할 경우 화면에 나타나는 EULA 문구를 세부적으로 읽어보지 않는 경우다. EULA에 동의하겠냐는 물음에 단순하게 동의(Agree)에 체크를 하고 알 수 없는 모듈들을 다운로드 받고 설치하게 되는 것이다[9]. 이 부분에 대한 법률적 해석은 쉬운 문제가 아니다. 법률적으로는 의사표시에 있어 내심의 의사와 표시의 행위가 서로 일치하지 않거나 의사형성과정에 결함이 있다면, 그 정도에

따라 무효(無效)가 되거나 취소(取消)되어질 수 있다. 즉, 사용자가 단순히 표면적으로 들어나는 소프트웨어의 기능만을 보고 해당 소프트웨어를 설치하고자 "동의"버튼을 누른 것이지, 스파이웨어의 설치를 동의했을 가능성은 희박한 것이므로, 법률적으로 "동의"버튼 자체가 사용자의 스파이웨어 설치 수락을 보장하지는 못하는 것이다.

다른 전파 방법은 스파이웨어가 제거될 경우 다른 정상적 소프트웨어의 기능을 마비시켜 사용자 스스로 스파이웨어를 다시 설치하도록 유도하는 것이다. 일예로 Kazaa에는 Brilliant Digital, Cydoor, DouleClick, DownloadWare, New.net, PromulGate, SaveNow 등의 스파이웨어가 포함되어 인스톨되며, 이러한 것을 사용자가 삭제할 경우 Kazaa자체가 작동을 하지 않게 된다. 즉, 사용자가 Kazaa를 다시 인스톨하도록 유도하여 삭제된 스파이웨어들을 복구하도록 구성되어 있다[10].

스파이웨어의 수적 증가 및 급진적인 확산에 따라서 이를 탐지하고 제거해주는 스파이웨어 제거 툴도 많이 개발되고 있다. 그러나 스파이웨어 제거 툴에 대한 제도적 통제와 시장 주도적 제품이 부족한 상황에서 스파이웨어 제거 툴 자체가 스파이웨어의 확산을 위한 수단으로 악용되는 사례도 발생하고 있다. 미국에서는 스파이웨어 제거 프로그램을 판매하는 회사가 자사의 제품 판매량을 늘리기 위하여 허위로 스파이웨어를 제작하여 배포한 사실이 밝혀지기도 했다. 그들은 자신들이 배포한 스파이웨어를 통해 고객 PC에서 팝업창이 뜨게하고, CD롬 드라이브의 트레이를 열거나 웹페이지를 앞서 설명한 브라우저 하이젝커와 유사하게 임의로 포워딩시켜서 사용자들을 불안하게 만든 이후에 자사의 제품인 SpyWiper를 구매하도록 유도한 것이다[11]. 이는 마치 오프라인 상에서 비양심적인 도청탐지업자가 실제로 존재하지 않았던 도청 장비를 고객방에 몰래 숨겨두고 자신이 찾아낸 척을 하며 수입을 올리는 기존 수법과 매우 유사한 것이다[3].

일부 업체들이 스파이웨어 제거 툴에 스파이웨어를 내장시키면서 비난의 표적이 되고도 있다[12]. '스파이밴(SpyBan)'도 스파이웨어 내장 문제로 비난받고 있는 스파이웨어 제거 툴 중 하나이다. CNET 다운로드닷컴에 따르면 스파이밴은 4개월간 4만 4000건의 다운로드 횟수를 기록했다. '스파이봇(Spybot) S&D'를 제작한 페피MK를 비롯해 스웨덴 업체인 캐피닷컴 등 다수의 스파이웨어 제거 툴 개발업체들이 스파이밴에 '룩투미(Look2Me)'로 알려진 스파이웨어가 포함돼 있음을 지적해왔으며, 다운로드닷컴측에서도 사용자들에게 이 같은 사실을 경고한 바 있다.

### 3.2 스파이웨어의 위험 분석

본 논문에서는 전통적인 위험분석 방법의 논리에 따라서 스파이웨어에 대한 위험을 분석했다. 위험은 자산 가치, 취약성 및 위협을 통해 도출될 수 있다. Mayerfeld는 취약성을 자산이 공격에 노출될 수 있는 모든 속성이라고 정의한 바 있다[13]. Stoneburner는 취약성을 시스템의 보안 정책이 위배되도록 이용될 수 있는 시스템 보안 절차, 설계, 구축 및 내부 통제 상의 약점이라고 정의했다[14]. Roper는 위협을 자산을 파괴하거나 가치를 손실시킬 수 있는 징후, 상황 및 이벤트라고 정의했다[15].

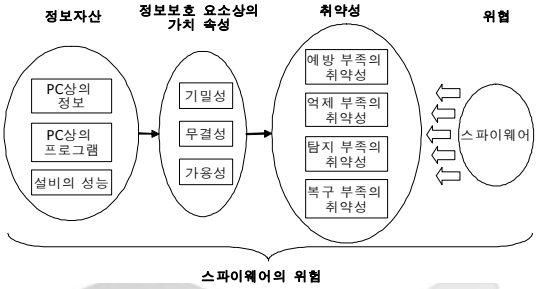


그림 1. 스파이웨어의 위험 분석 방법
Fig. 1. Risk Analysis of the Spywares

본 연구에서는 이러한 내용을 바탕으로 (그림 1)과 같은 형태로 스파이웨어의 위험을 분석했다. 전통적인 위험분석 방법의 주요 논리적 흐름에 따라서 논리전개를 했으나 특정 기업 환경이나 전산 환경에 대한 실제 분석 사례는 아니므로 세부적으로 정성적 또는 정량적인 분석을 통해 수치화나 등급화를 수행하지는 않았다. 즉, 스파이웨어라는 결정된 위협을 대상으로 다양한 상황에 대한 일반적 위험을 정리한 것이다.

스파이웨어라는 위협이 침해할 수 있는 정보자산의 가치를 정의하기 위하여 본 연구에서는 정보자산의 기본적 보안 속성인 기밀성, 무결성, 가용성의 3대 요소를 기준으로 삼았다[16]. 정보자산의 3대 보안 요소를 기준으로 하여 침해 위협이 있는 정보자산의 가치는 <표 1>과 같이 정리된다.

표 1. 침해될 수 있는 정보자산 목록
Table 1. List of Identified Asset

| 정보자산의 보안 속성 | 주요 자산 목록 |
|---|---|
| 기밀성 | - 시스템 레지스트리에 있는 이용자 이름 및 패스워드<br>- 이용자의 IP 주소<br>- 이용자의 컴퓨터에 깔린 소프트웨어 목록<br>- 이용자가 찾아간 URL 목록<br>- 마우스로 누른 배너 광고<br>- 여러 사이트에서 내려 받은 파일<br>- 브라우저를 이용할 때에 나타나는 동작 정보 |
| 무결성 | - 브라우져<br>- 인터넷 억세스<br>- 레지스트리<br>- 운영체계 |
| 가용성 | - 시스템 성능<br>- 네트워크 대역폭 |

이러한 정보자산이 가지고 있는 스파이웨어에 대한 취약성은 <표 2>와 같이 분류 할 수 있다. 통제의 목적은 기존 연구에서 제시하고 있는 보안 통제의 목적을 기준으로 한다[23, 24].

본 연구에서는 별도의 위협 분석은 수행하지 않는다. 본 연구의 주제인 스파이웨어 자체가 위협 요소이므로 <표 1>에서 제시한 관련 자산과 <표 2>에서 제시한 취약성에 대하여 스파이웨어가 야기할 수 있는 위험만 정리하였다. 즉, 앞서 기술한 정보자산의 취약성에 대한 스파이웨어의 위협으로 인한 위험은 다음과 같이 정리된다.

표 2. 스파이웨어에 대한 정보자산 취약성
Table 2. List of Vulnerabilities of the Spywares

| 통제의 목적 | 취약성 항목 |
|---|---|
| 예방 부족의 취약성 | - 대부분의 사용자가 온라인으로 다운로드 및 설치되는 각종 프로그램의 세부적 기능에 대하여 무관심함 |
| 억제 부족의 취약성 | - 법률적인 규제가 세부성이 부족함<br>- 법률적 규제 및 처벌에 대한 사회적 홍보가 부족함<br>- 스파이웨어 배포자 처벌이 보편적으로 발생하지 않거나 처벌의 강도가 미약함 |
| 탐지 부족의 취약성 | - 스파이웨어 탐지 기능을 제공해주는 소프트웨어의 사용이 보편적이지 않음<br>- 바이러스 백신 소프트웨어를 통해서 대부분의 스파이웨어가 탐지될 것으로 오인함 |
| 복구 부족의 취약성 | - 스파이웨어로 인하여 침해받은 정보자산의 내역 및 피해수준의 파악이 어려움<br>- 스파이웨어의 제거가 어려움(제거 기능을 제공하지 않거나 제거될 경우 스파이웨어와 함께 제공된 다른 소프트웨어의 기능을 마비시킴) |

- 인증정보의 도용[17]: 스파이웨어를 통해 유출된 개인 인증정보가 제3자에 의하여 불법으로 악용될 수 있다. 또한, 스파이웨어를 통한 인증정보 유출의 위험이 존재할 경우 개인 컴퓨터를 통한 전자상거래, 협업 및 온라인 투표 등 인증 정보의 중요성이 높은 어플리케이션의 사회적 활용이 어려워지는 위험이 존재한다.

- 프라이버시 침해[18]: 개인의 컴퓨터 운용현황 및 인터넷 사용내역에 대한 비밀을 침해 받을 수 있다. 이는 헌법 제18조에서 보장하고 있는 프라이버시권을 침해하는 것이다.

- 소프트웨어 구성상의 변조[19]: 스파이웨어는 개발업체의 특성상 프로그램이 조악한 경우가 많으며, 프로그램의 내부적 특성상 비일반적인 프로그램 방식을 따르는 경우도 많다. 이러한 소프트웨어적인 특성으로 인하여 스파이웨어는 사용자 컴퓨터의 브라우저와 레지스트리 설정을 포함한 운영체제 전반의 무결성 및 가용성을 침해할 수 있다.

- 의도하지 웹사이트 접근 발생[19]: 사용자가 접근하고자 하는 웹사이트를 스파이웨어가 제3의 사이트로 강제적으로 리디렉션할 수 있다.

- 전산자원 잠식[9]: 사용자 컴퓨터의 리소스(CPU, 램, 하드디스크 및 네트워크 대역)의 용량을 불필요하게 잠식할 수 있다. 특히, 광고 정보를 온라인으로 다운받고 사용자 컴퓨터에 나타내주는 과정에서 네트워크 대역폭을 잠식하고 사용자 PC의 전체적 성능을 저하시키는 경우가 발생할 수 있다.

- 온라인 마케팅 채널의 왜곡[19]: 스파이웨어는 사용자가 특정 사이트를 방문할 경우 경쟁회사의 광고를 띄워줄 수 있다. 이럴 경우 온라인 마케팅 채널을 왜곡할 수 있다.

# Ⅳ. 스파이웨어에 대한 통제 수단

## 4.1 기술적 통제 수단의 현황

표 3. 스파이웨어 컴포넌트 제작사 및 제품명
Table 3. List of Vendors and Products of the Spywares

| 제작사 | 제품명 |
|---|---|
| Belcaro Group | ShopAtHomeSelect |
| BSSCO, Inc. | Black Box |
| CatchCheat | Catch Cheat Spy |
| Coft Software | spyAOL |
| eAcceleration | DownloadReceiver<br>eAnthology |
| Electronic Group | IEAccess<br>StripPlayer |
| Pearl Software | Cyber Snoop |
| SentryCam | SentryCam |
| Spectorsoft | EBlaster<br>Spector |
| Spytech | NetVizor<br>Realtime-Spy<br>SpyAgent<br>SpyAnywhere<br>SpyTech Shadow |
| Spyware Labs, Inc. | Virtual Bouncer |
| WhenU | SaveNow |

스파이웨어 제작 및 배포와 관련된 기술 자체가 불법적인 것은 아니다. 따라서 상당수의 기업이 스파이웨어 제작과 관련된 원천 기술 및 스파이웨어 컴포넌트들을 판매하고 있는 상태이다. <표 3>에 현재 많이 알려진 회사 및 관련 스파이웨어 제품이 정리되어 있다.

이들 스파이웨어에 대한 제거 툴도 국내외적으로 수십 가지가 상용 또는 프리웨어 형태로 배포되고 있다. 이들 중 많이 사용되는 제품들의 주요 기능을 살펴보면 <표 4>와 같다[20]. 현재까지는 이러한 스파이웨어 전용 대응 소프트웨어 이외에 보편적으로 사용되는 기술적 대응 방안을 찾기가 어렵다. 따라서 <표 4>에서 열거한 유형의 제품들을 주요 기술적 통제 수단으로 분류할 수 있다.

표 4. 스파이웨어 제거 툴의 주요 기능 비교
Table 4. Comparison of Key Characteristics of Cleaning Softwares for the Spywares

| 기능 / 제거툴 | 메모리 스캔 | 레지스트리 스캔 | 에드웨어 제거 | 키로거 제거 | 실시간 기능 |
|---|---|---|---|---|---|
| Ad-ware | v | v | v | | v |
| Aluria's Spyware Eliminator | v | v | v | | |
| BPS Spyware/ Adware Remover | v | v | v | v | v |
| Internet Cleanup | | v | v | | v |
| PestPatrol | v | v | v | v | |
| QuickClean | | | v | v | |
| SpyBot Search & Destroy | v | v | v | v | |
| Spy Remover | v | v | v | | v |
| Spy Sweeper | v | v | v | | |

## 4.2 법률적 통제 수단의 현황

미국은 날로 심각해지는 스파이웨어에 의한 개인정보침해를 방지하고자 스파이웨어 금지법안(Spy Block Act)을 의회에 상정했다[21]. 이는 기존의 법률로는 스파이웨어에 의한 개인정보침해를 효과적으로 퇴치할 수 없다는 데에 기인하는 것이다. 본 법안의 발의자는 콘래드 번스(Conrad Burns) 상원위원이며, 법안의 주요 내용은 다음과 같은 항목들을 명시하고 있다.

① 이용자의 컴퓨터에 프로그램 설치 전에 이를 이용자의 컴퓨터 화면상에 명확히 고지

② 이용자가 손쉽게 프로그램 설치를 동의 또는 거절 할 수 있게 구현 및 프로그램 설치 목적(정보 수집, 광고 등)을 명확히 고지

③ 만약, 프로그램의 설치 목적이 다양 할 경우 이용자는 선택적으로 이를 동의 할 수 있어야 함

④ 설치된 프로그램을 이용자는 손쉽게 삭제 할 수 있어야 함

⑤ 프로그램 제공자는 “Add/Remove Program Menu” 또는 이와 유사한 기능을 이용자에게 제공해야 함.

국내 입법 현황을 살펴보면 정보통신망이용촉진및정보보호등에관한법률에서 관련 내용을 언급하고 있다[22]. 본 법 제22조 개인정보의 수집에서는 “정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 당해 이용자의 동의를 얻어야 한다.”고 명시하고 있으며, 이의 대상 항목으로 “인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항”포함하고 있다. 본 법 제50조의5 영리목적의 광고성 프로그램 등의 설치에서는 “정보통신서비스제공자는 영리목적의 광고성 정보가 보이도록 하거나 개인정보를 수집하는 프로그램을 이용자의 컴퓨터 그 밖에 대통령령이 정하는 정보처리장치에 설치하고자 할 때에 이용자의 동의를 얻어야 한다. 이 경우 해당 프로그램의 용도와 삭제할 수 있는 방법을 고지하여야 한다.”고 명시하고 있다. 본 법 제67조 제1항 15의5호에서는 “제50조의5의 규정을 위반하여 이용자의 동의를 얻지 아니하고 프로그램을 설치한 자는 1천만원 이하의 과태료에 처한다.”라고 명시하고 있다.

### 4.3 추가적 통제 수단 제시

대응 방안은 크게 유형에 따라 기술적인 것과 관리적인 것으로 나누어 생각할 수 있다. 또한, 통제의 범위에 따라 개인, 조직(기업 또는 기관) 및 국가라는 3단계의 관점을 나누어 볼 수 있다. 통제 수단에 대한 이러한 분류 및 접근 방식은 Fites et al., Hutt, Vallabhaneni, Krutz and Vines, Schweitzer가 제시하 보안 통제에 대한 분류 관점을 근거로 한다[23, 24, 25, 26].

표 5. 스파이웨어에 대한 추가적 대응 방안
Table 5. Suggestion of Possible Countermeasures for the Spywares

| 범위 | 유형 | 대응 방안 |
|---|---|---|
| 개인 | 기술적 | - 스파이웨어 제거 툴을 설치함[2]<br>- PC에 기록되는 개인 정보에 대한 클리닝 툴을 사용함(예: 레지스트리, 쿠키 값 등에 대한 클리닝)[6] |
| | 관리적 | - 소프트웨어 설치 전 EULA를 면밀하게 검토함[9]<br>- 불필요한 소프트웨어의 설치를 자제함(예: P2P 프로그램, 공개버전 게임 등)[25] |
| 조직 | 기술적 | - 주기적으로 조직내 PC에 대한 스파이웨어 스캐닝을 실시함[6]<br>- 조직의 방화벽을 통해서 알려진 에드웨어 사이트로의 정보 채널을 차단함[27] |
| | 관리적 | - 조직에서 승인해준 소프트웨어 이외의 것을 조직내부 PC에 설치하지 못하도록 관리함[19]<br>- 스파이웨어로 인한 정보자산 피해의 위험성에 대하여 조직 구성원을 대상으로 주기적으로 홍보 및 교육을 실시함[26] |
| 국가 | 관리적 | - 정보통신망이용촉진및정보보호등에관한법률에 스파이웨어의 불법적 설치 및 정보수집에 대한 제재내용을 명시함<br>- 법적으로 명시된 사항의 이행을 감독, 관리하기 위하여 관련 기관의 편제 및 담당 기능을 정의함<br>- 개인용 정보보호 제품에 스파이웨어 제거 관련 기능이 강화되도록 행정적으로 지원, 장려함<br>- ISP, 포털 사이트 등을 통한 공인된 스파이웨어 제거 툴의 확산을 장려함[28]<br>- 스파이웨어 제거 프로그램에 대한 간소화된 인증 제도를 도입하여 스파이웨어 제거 툴 자체에 악성기능이 내장되는 것을 통제함 |

기술적인 요소에는 소프트웨어 및 네트워크 상의 기술적 대응책 등이 포함되며, 관리적인 요소에는 개인의 스파이웨어 대응 지침, 조직의 스파이웨어 관련 정책, 표준, 지침, 절차 및 국가적 제도가 포함된다. 이러한 논리에 근거하여, 4.1과 4.2에서 정리한 현존하는 통제 수단 이외에 추가적으로 제안할 수 있는 스파이웨어에 대한 대응 방안을 <표 5>와 같이 제시된다.

## V. 결론

스파이웨어에 대한 문제를 컴퓨터 바이러스와 유사하게 대응하는 것은 문제가 많다. 바이러스는 본질적으로 정보자

산의 무결성에 대한 침해가 초점이었던 반면에 스파이웨어는 정보자산의 기밀성 침해가 더 큰 문제가 되기 때문이다[6]. 손상된 데이터는 백업을 통해서 복구가 가능하지만 유출된 기밀에 대한 복구 수단은 직접적인 것이 없으며, 법적 해결을 통한 일부의 피해보상 정도가 전부일 뿐이다[25]. 본 논문에서는 이러한 스파이웨어의 최근 확산 현황 및 위험 관리와 관련된 내용을 통하여 장기적으로 참조할 수 있는 스파이웨어에 대한 보안 체계를 제시하였다.

스파이웨어의 현황에 대해서는 기존의 스파이웨어 관련 피해사례 및 공급업체 등의 정보를 통해 해당 내용을 조사하였다. 위험 관리에 대해서는 전통적 위험 분석의 논리에 근거하여 위험요소를 도출하였으며, 이에 대한 대응책으로는 먼저 현존하는 기술적, 관리적 통제 수단을 조사 및 분류하고 추가로 향후 적용 가능한 방안들을 제시하였다.

본 연구에서는 위험분석 방법을 통해 위험 목록을 도출하였으나 이 과정에 정량적인 방법이나 등급 산출과 같은 정성적 방법이 포함된 것은 아니어서 개별 위험의 수준이나 발생 가능성 등에 대해서는 제시하지 못하고 있다. 또한, 현존하는 기술적, 법률적 통제 수단에 대해서는 그 현황을 정리하였으나 그러한 통제 수단들의 위험 요소에 대한 통제 효과나 적용상의 문제점에 대해서는 접근하지 못한 것이 본 연구의 한계점이라고 할 수 있다.

향후에는 이러한 내용들이 추가로 연구되어야 할 것이다.

- **정량적 분석**: 스파이웨어와 관련된 자산의 개별 가치 및 위험의 수준 등에 대한 정량적 지표가 도출되어야 한다.
- **효과 분석**: 스파이웨어의 대응 통제 수단에 대한 투자 효과의 검증 관련 연구가 이루어져야 한다.
- **통제 수단의 세분화 및 상세화**: 본 연구에서 도출된 항목별로 통제 수단의 내용이 세분화되고 세분화된 항목별로 내용이 상세하게 연구되어야 할 것이다.
- **참조 모델(Reference Model)의 구축**: 앞서 열거한 정량적 분석, 효과 분석, 통제 수단의 세분화 및 상세화 등을 통합하여 다양한 기업 환경에서 사례 및 목적별로 적용 가능한 참조 모델을 개발해야 할 것이다.

## 참고문헌


[1] SearchCrm.com, on the Web:www.searchcrm.com, Accessed on May 2005.

[2] SpywareGuide, on the Web: www.spywareguide.com, Accessed on January 2005.

[3] Rustmann, F.W., "Cia, Inc.: Espionage and the Craft of Business Intelligence", Brasseys, 2002.

[4] Webopedia, on the Web: www.webopedia.com, Accessed on February 2005.

[5] Stang, D.J., "Internet Intruders: Spyware, Adware, Hijackers and Other Pests", PestPatrol Research Center, undated.

[6] Harris, S., "CISSP All-in-One Exam Guide", McGraw-Hill Osborne Media, 2003.

[7] Unknown, "Spying Software can Invade Your Computer, Steal Personal Data", The News Herald, March 17, 2004.

[8] Lamb, G.M., "Is Your Computer Spying on You?", The Christian Science Monitor, March 29, 2004.

[9] Choney, S., "Spyware can Put Even Fastest PCs in The Slow Lane", SignOnSanDiego.com, March 8, 2004.

[10] Unknown, "Spyware Delivery Methods", PC Magazine, April 22, 2003.

[11] Unknown, "US: Scare Tactics Used in Adverts to Sell Anti-spyware Software", South China Morning Post, February 17, 2004.

[12] BorlandX, J., "Spyware Cures may Cause More Harm Than Good", CNET News.com, February 4, 2004.

[13] Mayerfeld, H., "Definition and Identification of Assets as the Basis for Risk Management", in Proceedings 1988 Computer Security Risk Management Model Builders Workshop, 1988.

[14] Stoneburner, G., Goguen, A., Feringa, A., "Risk Management Guide for Information Technology Systems", NIST, 2001.
[15] Roper, C.A., "Risk Management for Security Professionals", Butterworth Heinemann, 1999.
[16] Swanson, M., "Guide for Developing Security Plans for Information Technology Systems", NIST Special Publication 800-18, NIST, 1998.
[17] Pescatore, J., Baum, C., "Online Voting Can't Be Trusted on Standard PCs", Gartner, 2004.
[18] 성선제, 류종현, 강장묵, "네티즌을 위한 e-헌법: CyberLaw", 길벗, 2003.
[19] Shaw, G., "Spyware & Adware: the Risks facing Businesses", Elsevier Network Security, 2003.
[20] Dragan, R.V., "Summary of Features: Spywares", PC Magazine, February 17, 2004.
[21] Spy Block Act, Thomas Legislative Information on the Internet, on the Web: thomas.loc.gov, accessed on November 2004.
[22] 정보통신망이용촉진 및 정보보호 등에 관한 법률, 법률 제07142호, 법제처, 일부개정 2004. 1. 29.
[23] Vallabhaneni, R., "CISSP Examination Textbooks", SRV Professional Publications, 2000.
[24] Fites, P.E., Kratz, M.P.J., Brebner A.F., "Controls and Security of Computer Information Systems", Computer Science Press, 1989.
[25] Krutz, R.L., Vines, R.D., "The CISSP Prep Guide: Mastering the Ten Domains of Computer Security", John Wiley & Sons, New York, 2001.
[26] Schweitzer, J.A., "Protecting Information in the Electronic Workplace: A Guide for Managers", Reston Publishing Company, Reston, VA, 1983.
[27] Girard, J., Leong, L., "Seven Steps to Take to Fight Aggressive Internet Ads", Gartner, 2003.
[28] Roberts, P., "AOL Goes After Spyware", PC World, January 6, 2004.

## 저 자 소 개

**김 상 균**

연세대 컴퓨터산업공학 박사 CISSP, CBCP, ISSAP, ISSMP, BS7799 Auditor

현재 (주)소만사 이사 ICCSA 2005, KES 2005 스페셜 세션 좌장