애드웨어 및 스파이웨어 대응기법

김배현* · 권문택**

요 약

최근 스파이웨어(Spyware)와 애드웨어(Adware)의 급속한 확산으로 인해, 많은 사용자들이 컴퓨터의 사용에 어려움을 격고 있지만, 애드웨어 및 스파이웨어에 대한 효율적인 대응이 부족한 실정이다. 또한 애드웨어 및 스파이웨어는 앞으로도 더욱 확산될 것으로 전망되며, 이에 따라 보안 솔루션들이 안티-애드웨어(Anti-Adware) 및 안티-스파이웨어(Anti-Spyware) 기능이 추가되고 있고 보안 시장에서 새로운 영역으로 부상하고 있다. 그러나 아직까지 애드웨어 및 스파이웨어에 대한 체계적인 연구가 부족한 실정이다. 본 논문은 애드웨어 및 스파이웨어에 대한 사례 및 기술 분석을 통하여 애드웨어 및 스파이웨어에서 사용되는 악성 기법을 연구하고 이를 바탕으로 애드웨어 및 스파이웨어에 대한 효율적인 대응기법을 제시하고자 한다.

Measures for Adware and Spyware

Baehyun Kim* · Moon Taek Kwon**

ABSTRACT

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. Software designed to serve advertising, known as adware, can usually be thought of as spyware as well because it almost invariably includes components for tracking and reporting user information. A piece of spyware and adware affect computers which can rapidly become infected with large numbers of spyware and adware components. Users frequently notice from unwanted behavior and degradation of system performance, such as significant unwanted CPU activity, disk usage, and network traffic which thereby slows down legitimate uses of these resources. The presence of situation will continue because of rapid expansion of Internet usages. Therefore, security solutions, such as anti-adware and anti-spyware, for recovering these malfunction due to the malicious programs must be developed. However, studies on the malicious programs are still not sufficient. Accordingly, this paper has studied the malicious program techniques, based on the results of analysis of present adware and spyware techniques by employing collected samples, and presents efficient measures for blocking and remedying the malicious programs.

Key words : Spyware, Adware, Malicious Code, Anti-adware, Anti-spyware

* 경희대학교 전자정보대학.
** 경희대학교 테크노경영대학원

1. 서 론

비교적 최근 들어 애드웨어 및 스파이웨어에 의한 피해사례가 급증하고 있다. 애드웨어 및 스파이웨어는 인터넷 이용자의 정보를 감시/수집하는 도구로서 널리 이용되고 있다. 특히, 많은 사람들이 별 의심 없이 사용하고 있는 무료 소프트웨어(freeware)와 부주의한 메일의 첨부파일 개봉은 애드웨어 및 스파이웨어를 확산시키는 주요원인으로 들 수 있다. 스파이웨어는 개인 또는 조직에 대한 정보를 그들 스스로 동의하거나 식별하지 못하는 상태에서 수집하도록 지원해주는 소프트웨어를 의미한다. 이와 같이 스파이웨어의 가장 큰 역기능은 정보 주체의 동의 없이 정보를 수집하고 사용하는데 있으며 이는 인터넷 사용자의 프라이버시를 침해하는 행위이다. 한편 애드웨어는 광고 배너 등이 탑재되어 광고를 보는 것을 전제로 무료로 공급하는 프로그램으로 팝업 윈도우나 툴바를 사용해 광고를 볼 수 있는 프로그램이지만, 사용자도 모르게 개인의 정보가 유출될 수 있기 때문에 컴퓨터 안전과 프라이버시가 침해될 수 있기 때문에 최근에는 애드웨어를 악성 프로그램으로 분류하여 대책을 강구하고 있다. 최근 들어 이처럼 급속히 증가하고 있는 애드웨어 및 스파이웨어의 피해를 줄이기 위한 연구의 필요성이 증가하고 있다. 본 논문은 애드웨어 및 스파이웨어에서 사용되는 악성기법을 분석하여 애드웨어 및 스파이웨어의 대응기법을 제시한다. 본 논문의 구성은 제 2장에서 애드웨어와 스파이웨어를 분류하고 제 3장에서는 애드웨어 및 스파이웨어의 악성기법을 분석하였다. 제 4장에서는 애드웨어 및 스파이웨어 대응기법에 제시하고 제 5장에서 결론을 맺는다.

2. 애드웨어/스파이웨어

일반적으로 스파이웨어에는 개인 또는 조직이 스스로 동의하거나 식별하지 못하는 상태에서 정보를 수집하도록 지원해주는 소프트웨어를 의미한다. 즉, 스파이웨어는 일종의 정보수집모듈을 통칭하는 것으로, 광고효과나 모니터링을 위하여 프로그램 이용자에 대한 개인정보를 특정 서버로 유출하는 소프트웨어를 의미하며, 그 범위와 정의도 광범위하다. 본 논문에서는 애드웨어와 스파이웨어를 구분하여 논의한다.

2.1 애드웨어

사용자에게 임의로 광고를 나타내주는 소프트웨어를 의미한다. 이러한 기능은 일반적으로 공개 또는 쉐어웨어에 포함된 경우가 많다. 일반적인 경우에는 사용자가 공개 또는 쉐어웨어와 함께 설치, 작동되는 애드웨어를 충분히 인지하고 동의하므로 큰 문제는 없다. 그러나, 애드웨어가 기본적으로 사용자 컴퓨터에 대하여 제작자가 접근할 수 있는 접근경로를 제공하는 것이므로, 이러한 접근경로를 제작자가 광고 표현 이외의 용도로 활용할 수 있다는 것이 문제이다. 또한 잦은 광고로 인해 사용자에게 컴퓨터 사용 시 불편함을 줄 수 있다.

2.2 스파이웨어

초기에는 스파이웨어가 애드웨어와 혼용하여 사용되었으나, 최근에는 타인의 컴퓨터에 몰래 침입하여 중요한 개인정보 등을 빼내가는 악의적 프로그램을 지칭한다. 대개 인터넷을 통해 무료로 제공되는 소프트웨어를 다운로드받을 때 함께 설치되어 사용자의 IP 주소, 개인 ID, 패스워드 등 개인정보를 빼낸다. 대표적인 스파이웨어의 종류는 다음과 같다.

- 브라우져 플러그인(Browser Plugin) 형 : 인터넷 브라우져에 툴바 형태로 추가로 설치되는 모듈을 의미한다. 이러한 소프트웨어는 사용자의 인터넷 브라우징 내용을 제작자에게 지속적

으로 알려주는 역할을 담당한다.

- 키로거(Key Logger) 형 : 사용자가 PC에 입력하는 모든 키보드 입력 값을 가로채서 제 3자에게 보내주는 소프트웨어를 의미한다.
- 브라우저 하이젝커(Browser Hijacker) 형 : 브라우저의 설정을 변경하는 소프트웨어를 의미한다. 가장 대표적인 것으로 시작 페이지를 제작자가 원하는 사이트로 변경하는 경우이다. 또한, 사용자가 검색 페이지를 방문할 때 원래의 검색 페이지가 아니라 제작자가 설정한 제3의 검색 페이지를 방문하도록 한다.

3. 애드웨어/스파이웨어 악성기법 분석

3.1 애드웨어 악성기법

시멘텍 사가 애드웨어에 대한 사례를 수집 및 분석한 결과에 따르면, 2005년 기준으로 가장 많이 보고된 애드웨어는 Websearch 으로서 Top 10 애드웨어 중에 19.1%의 비중을 차지하고 있다. 2번째로 자주 등장한 애드웨어는 Hotbar으로 Top 10 애드웨어 프로그램 중 18.5%의 비중을 차지하고 있다. Hotbar는 익스플러러, 마이크로소프트 아웃룩, 아웃룩 익스프레스에 엷은 막을 추가하거나 또는 자체 툴바나 서치버튼을 추가하는 등 기능을 수행하면서 자체 구동된 광고를 디스플레이하기도 한다.

〈표 1〉 Top 10 애드웨어 프로그램 현황

순 위	이 름
1	Websearch
2	Hotbar
3	BetterInternet
4	Istbar
5	GAIN
6	CDT
7	Aurora
8	Lop
9	BargainBuddy
10	IEPlugin

시멘텍은 Top 10 애드웨어 프로그램들을 분류하고 리스크 수준 순위를 정하였다. 이러한 분류와 순위는 다음과 같은 기준으로 평가하였다 (<표 2> 참조).

- 감염된 컴퓨터에 미치는 보안상의 리스크 정도
- 개인 프라이버시에 미치는 영향
- 감염된 컴퓨터로부터 애드웨어를 제거하는 난이도
- 감염여부 탐지의 난이도 수준

〈표 2〉 Top 10 애드웨어의 리스크 현황

순 위	이 름	리스크 수준
1	Websearch	상
2	Hotbar	상
3	BetterInternet	상
4	Istbar	중
5	GAIN	중
6	CDT	중
7	Aurora	중
8	Lop	하
9	BargainBuddy	하
10	IEPlugin	하

3.2 스파이웨어 악성기법 분석

스파이웨어의 기술적 특징은 다음과 같다.

- 일반적인 프로그램
  스파이웨어는 일반적인 프로그램과 동일하므로 프로세스, 레지스트리, 실행 파일등 다수의

객체로 구성된다. 따라서 실행 파일만 제거 시 잔류물 잔존으로 시스템성능을 저하시킬 수 있다. 객체단위가 아닌 프로그램 단위의 완전한 제거가 필요하다.

- 시스템 설정 변경
  특정 스파이웨어는 설치시 시스템 설정을 변경한다. 만약 스파이웨어만 단순히 제거하면 키보드 작동 불능, 인터넷 접속 불능, 시스템 부팅 불능 등 시스템 문제가 발생할 가능성이 있다. 의 현상을 일으킨다. 따라서 스파이웨어 제거와 시스템 설정 복원이 동시에 필요하다.
- 사용자선택
  악성 여부는 사용자가 판단해야한다. 안티-스파이웨어가 탐지한 스파이웨어를 사용자가 사용하길 원할 수 있다. 따라서 안티-스파이웨어는 사용자가 원치 않는 일반프로그램을 탐지하여 제거할 수 있어야한다.

스파이웨어는 이와 같은 기술적 특징뿐만 아니라, 다양성, Grayware 등의 특징을 가진다. 스파이웨어의 다양성은 바이러스 계열 악성코드 이외의 모든 악성코드가 스파이웨어에 포함될 수 있기 때문에 악성광고, 정보유출, 시스템 악용 등 다양한 피해형태와 다양한 침투경로, 동작방법, 프로그램 기법이 존재한다. 또한, 바이러스는 100% 악성 프로그램이지만 다수의 스파이웨어는 악용과 상용의 중간에 위치하기 때문에 Grawareㄹ써의 특징을 가진다. 최근에는 사기성 스파이웨어 백신이 등장하여 일반사용자에게 피해를 주고 있다.

다음은 새로운 스파이웨어의 사례들이다.

- 사기성 안티-스파이웨어
  안티-스파이웨어로 위장하여 사용자 PC가 악성코드에 감염되어 있는 것으로 나타나도록 한 후, 거짓으로 치료하고 금전적인 이득을 취하는 형태이다.
- Grayware형
  - ✓ 인터넷 익스플로러 주소표시줄과 동일한 형태의 툴바
  - ✓ 악성코드 vs 상용코드
    사용자 모르게 설치되어 사용자가 원하지 않는 동작 실행할 경우 악성코드로 분류할 수 있지만, 설치 시 약관 동의 절차 및 사이트에서 Uninstall 프로그램 제공할 경우 상용코드로 분류된다, 그러나 프로그램 성격을 모르게 설치한 경우 사용자들의 불만이 다수이면 악성으로 분류할 수 있다.
- 복수설치형
  실행압축형태로 제작되어 1회의 마우스 클릭으로 다수의 스파이웨어가 설치된다.
- 파일명 변경형
  설치 될 때마다 파일 및 레지스트리 명칭을 불규칙하게 변경하여 안티-스파이웨어의 탐지를 피한다.
- 바이러스 결합형
  스파이웨어 설치 시 다른 악성 코드를 다운로드하여 다른 exe 파일을 찾아서 감염시킨다.
- 삭제 방지형
  시스템 폴더에 파일 명을 불규칙하게 변경하고 실행 시 여러 쓰레드로 실행되어 사용자가 강제로 프로세스를 중지시켜도 다시 바로 다른 프로세스로 실행되어 종료시키기 어렵다.

3.3 악성코드(Malicious Code)의 전파 메커니즘

악성코드의 전파 매카니즘(propagation mechanism)은 다양하다. 대표적인 전파 수단은 SMTP, CIFS, P2P 등 이다. 시기적으로 차이는 있지만 SMTP를 통해 전파되어 가장 많이 사용된 경로로 밝혀졌다. 또한 SMTP는 악성코드 뿐 아니라 트로이 목마를 스팸메일을 통해 전이하는 경로로 활용되고 있다.

〈표 3〉 Top 10 악성코드 분석

순위	악성코드 명	타입	전파수단	피해 효과
1	Sober.X	웜	SMTP	불법 다운로드
2	Netsky.P	웜	SMTP, P2P	계정 자료 도용
3	Mytob.ED	웜, Bot	SMTP	원격 엑세스
4	Mytob.DF	웜, Bot	SMTP	원격 엑세스
5	Spybot	Bot	CIFS, 원격침투, 백도어	원격 엑세스
6	Mytob.EE	웜, Bot	SMTP	원격 엑세스
7	Tooso.L	트로이 목마	-	보안조치 무력화, 원격 다운로드
8	Mytob.KU	웜, Bot	SMTP	원격 엑세스
9	Netsky.Z	웜	SMTP	불법 다운로드
10	Mytob	웜, Bot	SMTP, CIFS, 원격침투	원격 엑세스

4. 애드웨어/스파이웨어 대응 방안

애드웨어 및 스파이웨어에 대한 대응 방안으로 다음과 같은 방법을 고려할 수 있다.

- 안티-스파이웨어의 활용
  안티-스파이웨어는 '스파이웨어 스캐너(Scanner) 방식'과 'Active X 차단 방식이 있다. 스파이웨어 스캐너 방식은 가장 일반적이며, 알려진 스파이웨어의 패턴을 새롭게 설치되는 소프트웨어와 비교하여 스파이웨어로 판단하는 방법이다. 그러나 시그너쳐(Signature) 기반으로 검색함에 따라 새로운 스파이웨어가 등장하고 치료하는 시간차가 발생한다. ActiveX 차단(blockers) 방식은 체크리스트에 근거하여

〈표 4〉 악성 기능에 대한 계층별 방어 매트릭스

구분	안티-바이러스	네트워크 단계			OS단계	
		firewall	IDS	IPS	무결성 체크	stack-guard
네트워크 취약성 공격(감염)		O	O			O
사용자 속이기(감염)		O				
컨피규레이션 취약성 공격 (감염)		O				
사전 설치된 백도어를 이용한 공격(감염)	O	O				
파일시스템 변경				O	O	
시스템 셋팅 변경				O	O	
일부 프로세스 수정				O		
네트워크 접근	O			O		
시스템 권한 획득				O		
변형된 질의 수행				O		
주요 API 침해				O		
네트워크 트래픽 폭주 야기		O		O		
로컬시스템 속도 저하				O		
시그너쳐 포함	O	O	O			

출처 : The Case for Using Layered Defenses to Stop Worms, NSA

ActiveX 콘트롤의 설치와 실행을 통제함으로써 스파이웨어를 차단한다. ActiveX 차단 방식은 체크리스트에 대한 사용자의 관리가 필요하고 ActiveX 유형의 스파이웨어만을 방지한다는 단점이 있다.

- 네트워크 단계 대응 방안
  네트워크 서비스 제공자가 스파이웨어로 의심되는 소프트웨어를 직접 차단하는 네트워크 단계의 대응 방법이다. 그러나 사용자가 악성코드로 인식하지 않을 경우에는 사용자의 권리 침해, 차단 스파이웨어의 범위 등 다양한 문제점이 발생할 수 있다.
- 운영체제 단계 대응 방안
  운영체제 내의 기능을 제한함으로써 스파이웨어의 설치를 제한하는 방법으로 ActiveX 설치를 제한하는 것 등이 포함된다. 운영체제 단계의 대응 방안은 운영체제 개발회사에서 기능을 제공하여야한다.
- 기존 보안제품을 이용한 대응 방안
  스파이웨어도 기술적으로는 바이러스/웜과 같은 악성프로그램의 일종이기 때문에 스파이웨어의 알려진 악성기능에 대해서도 기존의 보안 프로그램을 활용한 기술적 조치는 가능하다.

미국의 NSA(National Security Agency)는 악성 프로그램의 악성기능에 대한 계층별(layed) 방어 가능성을 <표 4>와 같이 분류하였다.

5. 결 론

인터넷과 관련 정보기술의 발전은 기업이나 조직의 업무 패러다임을 획기적으로 개선시키고 개인의 정보 활용 수준도 엄청나게 변화 시켰다. 그러나 정보기술의 이점에는 기존의 해커나 바이러스 이외에도 애드웨어나 스파이웨어와 같은 악성 프로그램의 유포되면서 그 위협이 증가하면서 국가나 사회, 기업과 조직, 개인에게 막대한 피해를 입히고 있다.

본 논문에서는 애드웨어와 스파이웨어의 개념, 기술적 기능 분석을 통해 침해 위협과 피해로부터 기업이나 조직, 개인의 정보를 보호하기 위한 방안을 제시하였다.

향후 본 연구에서 제시된 방안을 기반으로 정보보호 관리체계를 수립하고, 기술적인 정보보호 대책 마련을 위해 정보보호 기술을 연구 및 개발한다면 애드웨어 및 스파이웨어로 인한 침해를 줄일 것으로 기대된다.

참 고 문 헌

[1] 한국정보보호진흥원, "새로운 사이버위협 : 스파이웨어", 2005, 11.
[2] 한국정보보호진흥원, "스파이웨어의 현황분석 및 대응방안",
[3] 정통부, 정보보호진흥원, "스파이웨어 사례집", 2005, 11.
[4] 정통부, "스파이웨어 기준안", 2005, 8.
[5] Symentec, "Symentec Internet Security Threat Report", 2006, 3.
[6] Symantec, "Symantec's Antispyware Approach",
[7] Symantec, "Exploring Spyware and Adware Risk Assessment", 2005, 3.
[8] http://www.symantec.com/
[9] http://home.ahnlab.com/
[10] 김배현, 권문택, "애드웨어 및 스파이웨어 동향에 관한연구", 한국사이버테러정보전학회, 제4회 추계학술대회, 2006, 11.

김 배 현

1995년 호원대학교 전자계산학과 (이학사)
1997년 수원대학교 전자계산학과 (이학석사)
2003년 경희대학교 전자계산학과 (공학박사수료)
2004년~현재 한신대학교 정보통신학과 겸임교수

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa 대학(공학석사)
1987년 미국 University of Wisconsin 대학(경영정보학 박사)
경희대 테크노 경영대학원 종신교수
경희대 정보처리처장
경희사이버 대학교 학장
한국 정보기술응용학회 회장
한국 사이버테러정보전 학회 부회장