

“스파이웨어 통한 개인정보 유출 심각하다”

개인정보 악용할 경우 범죄로 발전 가능성 높아



김연수 | KISA연구원 개인정보침해신고센터
 저서 고도지식정보사회의 개인정보보호와 CyberLaw
 E-mail kimyonsu@kisa.or.kr

▶ 연재순서

- 1 스파이웨어 프로그램(Spyware Program)을 통한 개인정보 유출의 문제
- 2 카니보어 시스템(Carnivore System)과 개인정보보호
- 3 사이버아파트 웹마스터의 개인정보 침해문제에 대한 법적 검토
- 4 콜러 ID(CID : Caller ID) Service와 Privacy
- 5 개인정보 보호 및 활용을 위한 IT 분야의 활성화(Ⅰ)
- 6 개인정보 보호 및 활용을 위한 IT 분야의 활성화(Ⅱ)
- 7 해킹 및 컴퓨터 바이러스에 의한 개인정보 침해(Ⅰ)
- 8 해킹 및 컴퓨터 바이러스에 의한 개인정보 침해(Ⅱ)
- 9 스팸메일의 불법성
- 10 쿠키(Cookies)를 통한 온라인 추적과 개인정보보호
- 11 전자서명과 인증 및 생체인식시스템관련 개인정보보호(Ⅰ)
- 12 전자서명과 인증 및 생체인식시스템관련 개인정보보호(Ⅱ)

최근 개인정보 유출 및 컴퓨터 범죄가 정보 역효과로 대두되고 있다.

이에 본지는 정보보호 및 컴퓨터 범죄에 관해서 국내에서는 앞선 연

구를 하고 있는 한국 정보보호센터의 김연수 연구원의 연재를 통해

정보보호 및 컴퓨터범죄에 관한 기술 및 유형별 동향 법적 대응 등에

관한 폭넓은 고찰을 통해 정보보호 와 사이버 범죄의 실상과 예방에

기여하고자 한다.

다만 연재 순서는 다소 변동이 될 수 있음을 공지한다.

--편집자주--

I. 서설

1. 개인정보보호와 스파이웨어

최근 개인정보 보호에 관심이 집중되면서 스파이웨어에 대한 논란이 일기 시작하였다. '개인 이용자의 정보를 함부로 남에게 알려주기 때문에 불법'이라는 한 백신프로그램 회사의 주장과 '이용자가 정보유출에 대한 동의를 하였기 때문에 법적으로 하자가 없다'는 주장으로 대립되어 컴퓨터 이용자들에게 혼란을 불러일으킨 적도 있다.

개인정보유출 기능이 그동안 트로이목마나 백도어 같은 악의적인 해킹툴에 의해서 도용·유출되어 사회적인 물의를 일으킨 사실은 있지만, 일반인이 자주 사용하는 정품내에 무더기로 개인정보유출 기능이 포함되기는 이번이 처음이다. 또한 많은 일반 사용자들은 자신의 컴퓨터 시스템내에 스파이웨어가 작동하고 있음을 알지 못한 채 자신의 정보가 외부로 유출되고 있음을 감지하지 못하는 경우가 많아 개인정보 보호를 위한 기술적 침해 및 대비의 필요성이 크다고 할 수 있다.

아래에서는 스파이웨어가 무엇이고 그 유포동향과 스파이웨어에 의하여 도용되거나 유출되는 개인정보 및 대처방안 등에 대하여 서술한다.

2. 개인정보유출프로그램 '스파이웨어'

1) 스파이웨어의 의의와 기능

스파이웨어는 무료로 배포되는 공개 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭하는 것으로 광고효과 모니터링을 위하여 컴퓨터 이용자의 이름이나 IP 주소, 방문한 웹사이트 목록, 클릭한 배너 광고 등의 프로그램 이용자에 대한 개인정보를 미리 설정된 특정 서버로 보냄으로써 외부에서 인터넷을 통해 특정이용자의 개인정보를 확인할 수 있도록 해주는 소프트웨어를 의미한다.

스파이웨어는 단지 개인정보를 유출하는 기능을 할 뿐이므로 백오리피스 등의 해킹툴과는 구별된다.

2) 스파이웨어를 통하여 알아내는 정보들

- 시스템 레지스트리에 있는 이용자 이름
- 이용자의 IP 주소

- 이용자의 컴퓨터에 깔린 소프트웨어 리스트
- 이용자가 찾아가는 URL 리스트
- 마우스로 누른 배너 광고
- 여러 사이트에서 내려받은 파일정보
- 브라우저를 이용할 때에 나타나는 동작 정보

II. 스파이웨어 유포 현황 및 문제점

1. 스파이웨어 유포현황

1) 발단과 전개

스파이웨어의 존재는 2000년 6월 2일 한국통신 ADSL 이용자 동호회의 한 회원이 동호회 홈페이지(<http://sig.kor-net.net/adsl>)에 주의를 촉구하는 글을 올리면서 국내 네티즌들 사이에 회자되기 시작하였다.

이러한 스파이웨어는 정품의 무료배포 재원을 마련하기 위하여 소프트웨어 업체가 마케팅정보 조사회사와 계약을 맺고 설치하는 경우가 대부분인데 네티즌들이 많이 사용하는 GetRight, Go!Zilla, CuteFTP 3.0 등 공개프로그램에 '인터넷 스파이웨어(Internet Spyware)'라는 개인정보유출 프로그램을 포함시켜 네티즌의 시스템 정보 및 인터넷 사용 상황을 미국 오리에이트(Aureate, 현재는 Radiate)사로 보고하고 있다는 주장이 제기되었다.

2) 레이디에이트(Radiate)사의 스파이웨어 유포

오리에이트(현재는 레이디에이트)사가 배포하고 있는 스파이웨어에 포함되어 있는 소프트웨어는 인터넷을 사용하기 위하여서 필요한 것들로 300여종(www.radiate.com/advertisers/products.html)이나 되며 주로 웹어웨어나 프리웨어들, 이 중에는 국내 유저들이 애용하는 것들도 많이 있다. 예컨대, 리얼플레이어를 사용하는 경우, 어떤 네티즌이 어떤 노래를 듣는지, 어떤 영화를 보는지 리얼네트워크(RealNetwork)사에 집계된다는 것이다.

3) 국외의 개인정보 유출 프로그램에 대한 심각성 인식 현황

인터넷 상거래 등이 급진장세를 보이고 있는 상황에서 이

1) 이러한 공개 소프트웨어들은 하이텔 공개자료실에서 각각 6,300회, 5,800회, 4,300회 다운로드 회수를 기록하고 있다.

같은 개인정보 유출 문제는 외국에서는 이미 심각한 고민거리로 떠오른 상태이다. 미국 연방거래위원회는 1999년말 이용자의 ID와 패스워드 등이 저장돼 자주 이용하는 웹사이트를 간편하게 이용할 수 있도록 해주는 '키 파일'이 원래 의도와 다르게 비밀정보의 유출 수단으로 사용되어 사생활을 침해할 소지가 있다며 그 위법성을 검토중이다.

또한 2000년 2월 프랑스 국방부 산하 전략문제대표단의 한 고위관료는 전세계 소프트웨어 시장의 90%를 차지하는 MS사의 소프트웨어에 컴퓨터 내의 모든 정보를 미국 국가안보국(NSA)으로 자동 전송하는 비밀 프로그램이 설치돼 있다는 주장을 제기하기도 하였다.²⁾

2. 스파이웨어에 의한 개인정보 유출의 문제점

스파이웨어 프로그램이 있는 제품들은 함께 탑재된 광고를 통해 수익을 올리는 회사에서 광고 효과 모니터링을 위하여 이용자 정보를 빼내가는 것으로 알려져 있으나 이 과정에서 여러가지 악의적인 목적으로 사용되어 질 수 있다.

그동안 웹사이트를 방문할 때 방문기록 등을 알아낼 수 있는 일명 「쿠키」프로그램이 문제가 된 적은 있지만 이같이 개인정보를 무단으로 빼내는 전문 프로그램이 발견되기는 처음이다. 스파이웨어는 단순한 로깅 기록은 물론 유료 콘텐츠를 이용할 때 필요한 패스워드에서 패스워드까지 빼낼 수 있는 것으로 알려졌다.

더욱이 스파이웨어를 찾을 수 있는 검사 프로그램을 실행하거나 빼낸 개인정보가 불법으로 악용되기 전에는 개인정보 유출 여부를 알 수가 없어 정확한 실태 파악조차 힘든 상황이다.

스파이웨어를 포함하고 있는 소프트웨어를 설치할 때에 사용동의서에서 개인정보를 외부로 유출한다는 사실을 표시하는 경우도 있지만 거의 모든 이용자들은 동의서를 읽지도 않을뿐더러 대부분이 영문이므로 내용도 모른 채 함께 설치되는 경우가 많다.

스파이웨어 프로그램의 또다른 문제점은 본 프로그램을 삭제할지라도 첨부되어 있던 스파이웨어는 삭제되지 않으며 본 프로그램을 실행하지 않아도 몰래 작동을 하고 있다는 것이다.

프로그램을 제작한 회사가 정보송출 모듈을 임의로 업그

레이드할 수 있는 것도 문제의 소지가 있다. 이 경우 이용자의 키보드 사용명세까지 알아낼 수 있는 고성능 소프트웨어 설치가 가능하기 때문에 전자상거래나 사이버 बैं킹을 할 때 신용카드 번호나 패스워드가 유출될 가능성은 매우 크다. 게임과 같이 유료 콘텐츠를 이용할 때 예상 밖으로 사용료가 많이 나오거나 자기 신상정보가 가입하지도 않은 인터넷 사업자의 회원 정보에 올라 있을 경우 스파이웨어일 가능성³⁾이 큰 이유도 이러한 스파이웨어의 문제가 있기 때문이다.

개인정보를 빼낼 수 있는 모듈을 무료 소프트웨어에 첨부해 이를 다운로드할 때 자동으로 보내는 방법으로 유포되고 있는 스파이웨어는 엄연히 개인 이용자의 정보를 외부로 알려주고 있는 것이 사실이며 개인 이용자는 이런 사실을 모른다는 것이 가장 큰 문제점이다. 즉, 자기도 모르는 사이에 사생활이 노출될 수 있고, 해커나 악의적인 업체에 의해 피해를 볼 수도 있으며 귀찮은 스팸메일에 시달리게 될 수도 있다.

스파이웨어 기능이 발견된 소프트웨어 1

- 3D-FTP, 123Search, 3D Anarchy:> 3rd block:>
- Abe's FTP Client:> Abe's Image Viewer:> Abe's MP3 Finder:> Abe's Picture Finder:> Abe's SMB Client:>
- Access Diver III:> Acorn E-mail:> AcqURL:> ActionOutline Light 1.6:> Active 'Net:> Add URL:>
- Add/Remove Plus!:> Address Rover 98:> Admiral VirusScanner:> Advanced Call Center:> Advanced Maillist Verify:> AdWizard:> Alive and Kicking:>
- alphaScape QuickPaste:> ASP1-A3:> Auction Explorer:> Aureate Group Mail:> Aureate SpamKiller:> AutoFTP PRO:> AutoWeb:> AxelCD:>
- Beatle:> Binary Boy:> BinaryVortex:> Blue Engine:> BookSmith : Original:> buddyPhone 2:> Calypso E-mail:> CamGrab:> Capture Express 2000:> Cascoly

2) http://iweekly.co.kr/200005/3/iw003_038.asp 참조

3) 전자신문 2000년 5월 29일자 참조

Screensaver:> CDDB-Reader:> CDMaster32:> Chan-
Stat:> Charity Banner:> Cheat Machine:>
Check4New:> ChinMail:> Clabra clipboard viewer:>
Classic Peg Solitaire:> ComTry Music Downloader:>
Crystal FTP:> CSE HTML Validator Lite:> CuteFTP
3.0:> CuteFTP 3.0:> CuteFTP/Tripod:> CuteMX:>
CutePage:> Danzig Pref Engine:> DateTime:> Delphi
Component Test:> Delphi Tester:> Dialer 2000:>
DigiBand NewsWatch:> DigiCams - The WebCam
Viewer:> Digital Postman:> DirectUpdate:> DL-Mail
Pro 2000:> DNScape:> Doorbell 1.18:> Download
Minder 1.5:> Download Wonder:> DownLoader
v.1.1:> Dwyco Video Conferencing:> EasySeeker:>
EmmaSoft ChatCat:> EmmaSoft dBrow:> EmmaSoft
KeepLan:> EmmaSoft Soundz:> EnvoyMail:> EZ-Forms
FREE:> File Mag-Net:> FileSplit:> Folder Guard Jr. :>
FourTimes:> Free Picture Harvester:> Free Soli-
taire:> Free Spades:> Free Submitter Pro:> FreeIm-
ageEditor:> FreeIRC:> FreeNotePad:> FreeSite:>
FreeWebBrowser:> FreeWebMail:> FreeZip!:> FTPEd-
itor:> GetRight:> Go/Zilla:> Go/Zilla WebAttack:> Gov-
ernMail:> Grafula:> Gunther's PasswordSentry:>
HangWeb:> hesci Private Label:> HTML Translator:>
HTTP Proxy-Spy:> Huey v1.8 Color Picker:> Iban
Technologies IP Tools 3.1:> Idle GimmIP:> Idle
GimmIP:> iFind Graphics:> imageN:> Infinite
Patience:> InfoBlast:> InnovaClub:> InstallZIP:>
Internet Tree:> Internetrix:> InterWebWord Com-
panion:> JetCar:> JFK Research:> jIRC:> JOC E-mail
Checker:> JOC Web Finder:> JOC Web Spider:> KVT
Diplom:> LapLink FTP:> LineSoft Download:> LOL
Chat:> LOL Chat:> Mail Them:> Meracl FontMap:>
Meracl ImageMap Generator:> Midnight Oil Soli-
taire:> MirNik Internet Finder:> More Space 99:>
MouseAssist:> MP3 Album Finder:> MP3 Fiend:>
MP3 Groupie:> MP3 Mag-Net:> MP3 Renamer:> Mp3
Stream Recorder:> MP3INFO-Editor:> MultiSender:>
Music Genie:> MX Inspector BIG AD:> My Genie
Patriots:> My Genie SE:> My GetRight:> NeatFTP:> Net
CB:> Net Scan 2000:> Net Vampire:> Net-A-Car Fea-
ture Car Screensaver:> NetAnts:> NetBoard:> Netbus
Pro 2.10:>

스파이웨어 기능이 발견된 소프트웨어 2

NetCaptor 5.0:> Netman Downloader:> NetNak:>
NetSuck 3.10.5:> NetTime Thingy:> Network Assis-
tant:> NeuroStock:> NewsBin:> NewsShark:>
NewsWire:> NfoNak:> NotePads+:> Notificator 1.0b:>
Octopus:> Pattern Book:> People Seek 98:> Personal
Search Agent:> Photocopier:> PicPluck:> Pictures In
News:> Ping Thingy:> PingMaster:> Planet.Bill-
board:> Planet.MP3Find:> PMS:> ProtectX 3:> Proxy-
Checker:> QuadSucker/Web:> Quadzle Puzzles:>
QuikLink Autobot:> QuikLink Explorer:> QuikLink
Explorer Gold Edition:> QuoteWatch:> QWallet:>
Real Estate Web Site Creator:> Recipe Review:> ReGet
1.6:> Resume Detective:> RingSurf:> RoboCam 1.10:>
Rosemary's Weird Web World:> SaberQuest Page
Burner:> SBJV:> SBWcc:> Scout's Game:> ScreenFIRE:>
ScreenFIRE - FileKing:> ScreenFlavors:> Sea Battle:>
Shizzam:> Simple Submit:> SimpleFind:> SimpleSub-
mit v1.0:> SK-111:> Smart 'n Sticky:> SmartBoard
200 FREE Edition:> SmartSum calculator:> Sonic-
Mail:> Sound Agent:> Space Central Screen Saver:>
Splash! Siterave:> StartDrive:> Static FTP:> Stock-
Browser:> Subscriber:> SunEdit 2K:> SuperIDE:>
Sweep:> SweepsWinner:> Text Transmogrifier:> The
Mapper:> TheNet:> TI-FindMail:> TIFNY:> Total Fin-
ger:> Total Whois:> Tracking The Eye:> Trade Site
Creator:> TWInExplorer Standard:> TypeWriter
1.0:> UK Phone Codes:> Vagabond's Realm:> Ver-
iMP3:> Vertigo QSearch:> Virtual Access:> Visual
Cyberadio:> Visual Surfer:> VOG Backgammon
Main:> VOG Backgammon Table:> VOG Chess Main:>
VOG Chess Table:> VOG Reversi Main:> VOG Reversi
Table:> VOG Shell:> VOG Shell:> VOG Shell History:>
W3Filer:> Web Coupon:> Web Page Authoring Soft-
ware:> Web Registrant PRO:> Web Resume:> Web
SurfACE:> WEB2SMS:> WebCamVCR:> WebCopier:>
Web-N-Force:> WebSaver:> Website Manager:> Web-
Stripper:> WebType:> Whols Thingy:> Win A Lotto:>
WinEdit 2000:> Word+:> Wordwright:> WorldChat
Client:> Worm:> www.devgames.com:> xBlock:> Your

ESP Test:> Zion:> Zip Express 2000.
<http://korea.cnet.com/News/2000/06/01/20000601v.html>

램이 집단적으로 발견됨에 따라 국내 PC 이용자들의 개인정보가 무더기로 유출될 것은 자명하다. 특히 이러한 개인정보는 특정 기업의 마케팅정보로 활용되는 것은 물론 다른 악의적인 용도로도 사용될 가능성이 매우 높으므로 정부차원의 대책마련이 시급하다.

III. 스파이웨어에 대한 방지대책

1. 제거물에 의한 검색 및 삭제

이러한 스파이웨어를 제거하기 위하여서는 김슨리서치회사(Gibson Research Corporation)에서 만든 'OptOut'이라는 프로그램(<http://grc.com/optout.htm>)을 이용하면 된다(.). 이 프로그램을 이용하여 제거할 수 있는 스파이웨어는 약 165개 정도라고 알려져 있다.

2. 대체 프로그램 개발

한국통신하이텔(<http://www.hitel.net>)은 제휴사인 애드⁴⁾바이오스(<http://www.adbios.com>)가 개발한 '애드컨트롤'을 이용하여 스파이웨어 프로그램을 차단하고 내려받기 속도를 개선하는 등 대체 프로그램에 의하여 스파이웨어를 방지할 수 있다.

3. 사용동의서에 대한 주의

인터넷에서 무료 소프트웨어를 내려받을 때는 자기 신상 정보를 유출시킬 수 있는 프로그램인지 여부를 먼저 확인하는 것이 좋다. 또한 이용자는 외산 프로그램설치시 사용권 동의서를 자세히 살펴보는 주의를 필요하며 만약 이상한 내용이 있으면 해당 프로그램은 사용하지 않는 것이 안전하다.

4. 이용자의 공개된 장소에서의 인터넷 사용시 주의

이용자가 컴퓨터게임방 등에서 은행거래나 주식거래 등 개인정보를 입력하여야 하는 경우에는 세심한 주의가 필요하다. 유출된 이용자 정보가 악의적인 목적을 가진 해커에게 전달되면, 자신이 사용한 인터넷 사이트의 ID, 패스워드(Password)등이 무방비로 노출될 수 있기 때문이다.

5. 정부차원의 대책마련 시급

국내 네티즌들이 애용하는 외산 SW에 스파이웨어 프로그

OptOut 사용법

1. 스파이웨어를 검색하기 위하여서는 [Deep Scan]버튼을 클릭한다.
2. OptOut이 스파이웨어를 검색하고 스파이웨어를 찾았다면 File Found[화면 중앙의 텍스트 상자]에 적색으로 찾은 개수를 표시하며, [Deep Scan]버튼을 [Press to Continue]버튼으로 변경하여 표시된다.
3. 만약, 스파이웨어가 없다면 File Found[화면 중앙의 텍스트 상자]는 0으로 표시되며 색상 또한 녹색으로 표시된다. 개인정보 누출에 대하여 안전하다는 의미다.
4. 스파이웨어가 없으면 종료하면 되고, 스파이웨어가 있다면 [Press to Continue]버튼을 클릭한다
5. 여기서 어떠한 스파이웨어가 PC에 있는지 확인하려면 [Log]탭을 클릭한다.
6. 스파이웨어 목록을 확인하기 위하여서 [Copy to Clipboard]버튼을 클릭한다. 그리고 메모장[시작]->[실행]-> notepad를 입력하고 [확인]버튼을 클릭한다.)을 실행해서 붙여넣기[Ctrl+v 키]를 한다.
7. 이제 스파이웨어를 삭제하는 방법을 알아보기로 한다. [Status]탭을 클릭한다.
8. 화면에 나타난 대화상자에서 [Delete Them]버튼을 클릭하면 발견된 스파이웨어의 해당 드라이버를 삭제한다.
9. Restart Windows]버튼을 클릭하여 PC를 재부팅하면 된다.

4) 애드바이오스가 개발한 애드컨트롤은 프로그램이 아니기 때문에 따로 설치할 필요가 없고 하이텔 자료실이나 제휴 사이트에서 클릭만 하면 자동으로 인증 화면이 뜨고 자연스럽게 설치되는 플러그인 방식을 채택하고 있다. 따라서 애드컨트롤을 한번만 클릭하면 타 제휴사이트에서도 별도의 인증단계를 거치지 않고 곧바로 자료를 내려받을 수 있다.