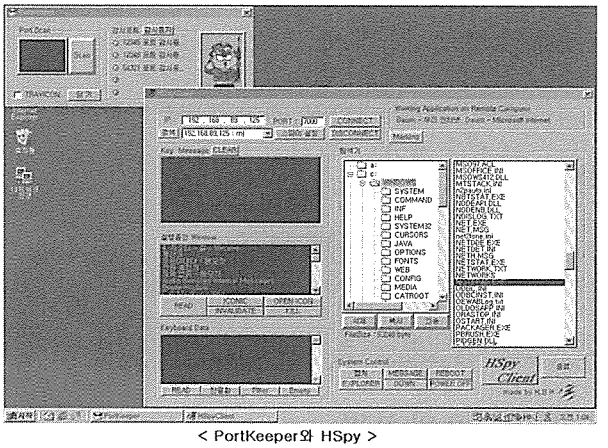
## HSpy와 PortKeeper

# 원거리 PC 제어 / 스파이웨어를 이용한 외부로부터의 접근 감시


< PortKeeper와 HSpy >

HSpy는 Spyware의 이해와 Spyware에서 발전된 원격관리 프로그램으로의 변형이란 두가지 목적을 가지고 개발된 프로그램이다.

HSpy를 이용해 외부에서 집에있는 자신의 PC에 연결하여 특정작업을 하거나 타인이 PC를 사용하는 것을 감시하고 제재를 할수 있다.

가정에서 사용되는 전용선이 대부분 유동IP 이기 때문에 HSpy가 스스로 변경된 IP를 메일로 발송해 줌으로써 외부에서 접속을 가능하게 해준다.

PortKeeper는 Spyware가 가지고 있는 특성을 이용해 개발된 프로그램으로 자신의 PC에 설치된 Spyware의 기능을 마비시키고 외부로부터의 접속을 감시한다. PC에 설치된 Spyware를 단순히 제거하는 것이 아니라 외부에서 Spyware를 이용해 자신의 PC에 접속하는 사람의 정보를 알려주는 것이 PortKeeper의 주된 기능이다.

# HSpy 와 PortKeeper

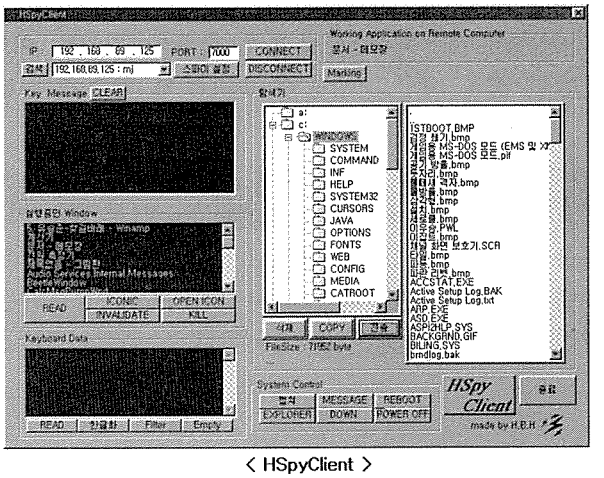
장 려 상

## 1. 작품명 : HSpy/PortKeeper(원격관리툴/Spyware감시툴)

## 2. 제작자 : 한병희


소속 : 명지대학교 전자정보통신공학부
주소 : 경기도 구리시 교문동 801-14호
전화 : 031) 567-9021
휴대폰 : 018) 266-9021
email : hbh2000@hanmail.net


## 3. S/W 요약설명




< HSpyClient >

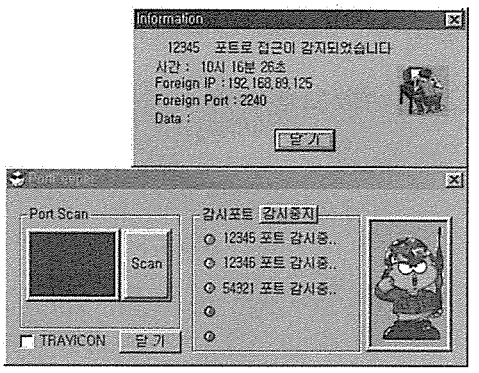
이 프로그램은 PC 원격관리 프로그램인 HSpy 와 Spyware 감시프로그램인 PortKeeper로 구성이 되어 있습니다.

HSpy는 외부에서 집에 있는 자신의 PC를 제어해서 가능한 많은 작업을 할 수 있도록 프로그래밍 되어 있습니다.

HSpy의 기능을 이용해 외부에서도 집에 있는 자신의 PC를 사용하는 사람이

어떤 작업을 하는지 감시하거나 특정한 제재를 할 수 있습니다. 또 어디서든 자유롭게 특정파일을 집에 있는 PC로 보내거나 반대로 가져올 수 있고 외부에서 집에있는 자신의 PC의 화면을 보면서 직접 제어 할 수도 있습니다.

PortKeeper는 공개된 PC (PC방이나 대학PC실 등)에 누군가가 설치해 놓은 Spyware를 탐지하고 그 기능을 마비시킨 뒤 그 Spyware에게 외부로부터 접속이 시도되기를 기다리는 일종의 함정입니다.



<PortKeeper>

누군가가 자신의 PC에서 정보를 유출하기 위해 Spyware를 설치했을 때 단순히 그 Spyware를 찾아 제거하는데 그치지 않고 그 Spyware로 접근하는 사람의 정보를 알려주어 신속한 대응을 할 수 있도록 도와줍니다.

## 3.1 개발 배경

SpyServer와 SpyClient로 구성되어 있는 HSpy는 두 가지 목적을 가지고 개발되었습니다.

첫째는 Spyware의 기능을 구현해 봄으로써 Spyware의 대응책을 모색해보기 위해서 입니다.

요즘은 인터넷을 통해 인터넷뱅킹이나 서신교환 등 많은 일을 하고 있습니다. 인터넷을 통해 할 수 있는 일이 많아지는 만큼 자신의 개인정보가 타인에게 유출되어 악용될 위험도 커지고 있습니다. 그 예로 백오리피스나 넷버스 같은 Spyware를 이용해 타인의 개인정보를 획득하는 사례가 많이 있습니다.

이에 Spyware의 기능을 구현해봄으로써 그 원리를 이해하고 이에 대응 할 수 있는 방법을 강구하는 것이 첫 번째 목적입니다.

두 번째 목적은 어디서든 집에 있는 자신의 PC를 관리/제어 할 수 있는 프로그램의 개발입니다.

누구나 외출했을 때 집에 있는 PC에 저장되어 있는 데이터가 필요할 경우나

어떤 데이터를 집에 있는 PC에 저장해 놓고 싶을 때가 있었을 것입니다. 또 집에 있는 자신의 PC가 무슨 일에 쓰이고 있는지 감시해야 할 경우가 있습니다. 그리고 컴맹인 친구의 컴퓨터에서 어떤 작업을 대신 해주어야 할 경우도 있습니다.
이럴 때 편리하게 사용될 수 있는 프로그램의 개발이 두 번째 목표입니다.

## 3.2 프로그램구성

이 프로그램은 Spyware 감시도구와 PC원격관리 프로그램으로 구성되어 있습니다.

**PC 원격관리 프로그램 (원격 관리)**

- HSpy (SpyServer/SpyClient)
  - SpyServer : PC에 설치되어 메일발송과 메시지후킹을 하며 Client의 접속을 대기
  - SpyClient : Server에 접속하여 Server가 설치된 PC를 원격 제어
  - HookDll : MessageHooking을 수행

**Spyware 감시도구**

- PortKeeper : 자신의 PC에서 Spyware가 사용하는 것으로 의심되는 Port를 빼앗아 스파이웨어의 기능을 마비시키고 지속적으로 포트를 감시 / 외부에서 접속이 시도되는 순간을 알려주어 신속한 대응을 할 수 있게 해줍니다.

## 3.3 프로그램 기능

| | 기능 | 설 명 |
|---|---|---|
| PortKeeper | Scan | 1부터 65535까지의 Port를 체크해서 사용중인 포트 검색 |
| | 감시 | 지정된 포트로부터 접속시도 감지 |
| | 알림 | 외부로부터 Spyware의 접근이 시도 되었을 때 접근 IP를 알려주는 기능 |

| | 기 능 | 설 명 |
|---|---|---|
| SpyServer | 메일 발송 | 자신이 설치된 PC의 IP가 변할때마다 지정된 주소로 mail 발송 |
| | KeyMessage Hooking | 설치된 순간부터 Key값을 저장 / SpyClient의 요구시 내용전송 |
| | 기 타 | 화면캡쳐 / 파일 전송 / Application제어 |

| | 명칭 | 기 능 | 설 명 |
|---|---|---|---|
| SpyClient | 연결 | CONNECT | SpyServer와 연결 |
| | | 검색 | 네트웍망에서 SpyServer가 설치된 PC 검색 |
| | | 스파이 설정 | SpyServer의 기본적인 설정 |
| | KeyMessage | | SpyServer가 설치된 PC에서 발생중인 KeyMessage |
| | System Control | 캡쳐 | SpyServer가 설치된 PC의 캡쳐된 화면/ 마우스 제어 |
| | | MESSAGE | Message 전송 |
| | | REBOOT | 재부팅 |
| | | EXPLORER | 인터넷 Explorer 실행 |
| | | DOWN | SpyServer가 설치된 PC의 resource 감소 |
| | | POWER OFF | Power off |
| | Working Application | | 현재 작업중인 Application의 캡션 |
| | 탐색기 | 삭제 | 파일 삭제 |
| | | COPY | SpyServer로부터 파일 가져오기 |
| | | 전송 | SpyServer로 파일 보내기 |
| | 실행중인 Window | READ | 현재 실행된 Application의 목록 가져오기 |
| | | ICONIC | 선택된 Application의 아이콘화 |
| | | OPEN ICON | 선택된 Application의 확대 |
| | | INVALIDATE | 선택된 Application의 무효화 |
| | | KILL | 선택된 Application의 종료 |
| | Keyboard Data | READ | 저장된 KeyMessage 기록 읽기 |
| | | 한글화 | KeyMessage기록의 변환 |
| | | Fliter | |

## 4. 개발효과

○ TCP/UDP를 이용한 네트워크 프로그램의 인지
- Client / Server의 개념
- File 전송
- PC 원격관리 / 제어

○ MessageHooking을 통해 Window의 이벤트구동방식(Event Driven)의 이해

○ SMTP(Simple Mail Transfer Protocol)의 이해

○ HSpy의 구현을 통해 Spyware의 작동 방식 이해

○ PortKeeper를 이용해 Netbus, SchoolBus 같은 Spyware를 감지/ 정보 유출 차단/ 접근감시

○ HSpy를 원격관리 프로그램으로 자신의 PC에 설치하여 원격제어 (다른 Application 실행/종료, Application 설치, 파일 송수신 등)

○ SpyServer의 메일전송기능을 이용하여 유동 IP사용자도 IP에 구애받지 않고 자신의 PC 제어

## 5. 개발언어, 테스트 프로그램

- 개발 : Microsoft Visual Studio 6.0
  Visual C++ 6.0

- PortKeeper 테스트 프로그램 : Netbus , Schoolbus

## 6. 사용가능 OS

| | |
|---|---|
| PortKeeper | Microsoft Windows 95/98/ME |
| HSpy | Microsoft Windows 95/98/ME/2000/XP |