보안공부닷컴
http://www.boangongbu.com

개나소나 다하는 해킹 – 원격제어
(NetDevil)

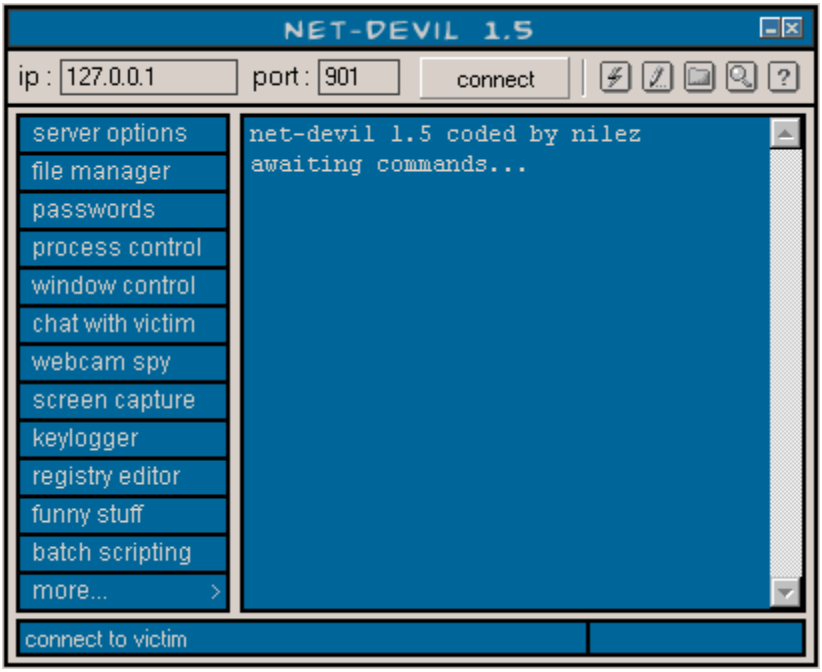
작성날짜: 2010년 4월 29일 목요일

메일주소: boangongbu@naver.com

이번에는 <개나소나 시리즈> 원격제어편 그 첫번째 - 넷데빌편 입니다.

게시판 댓글에 어느분이 뉴스에도 나왔다고 하시는군요. (이런것도 뉴스에… ㅋㅎ)

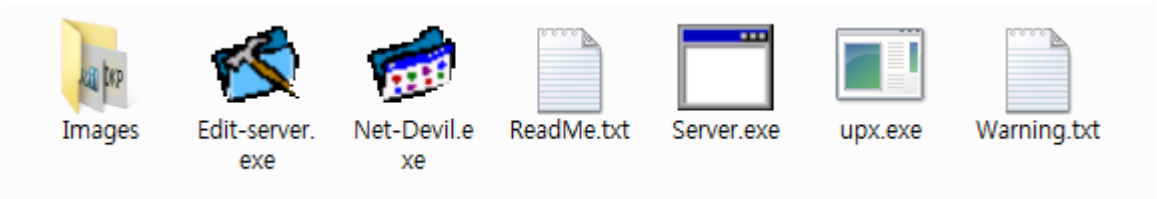
뭐하는 툴인지는 다들 아실테구요. 일단 메인화면을 한번 봐보죠.



(NetDevil 메인창)

인터페이스가 깔끔하고 보기 좋네요. ^^

그럼 파일을 다운받아 압축을 풀어보면 아래와 같은 파일들을 확인가능하구요.

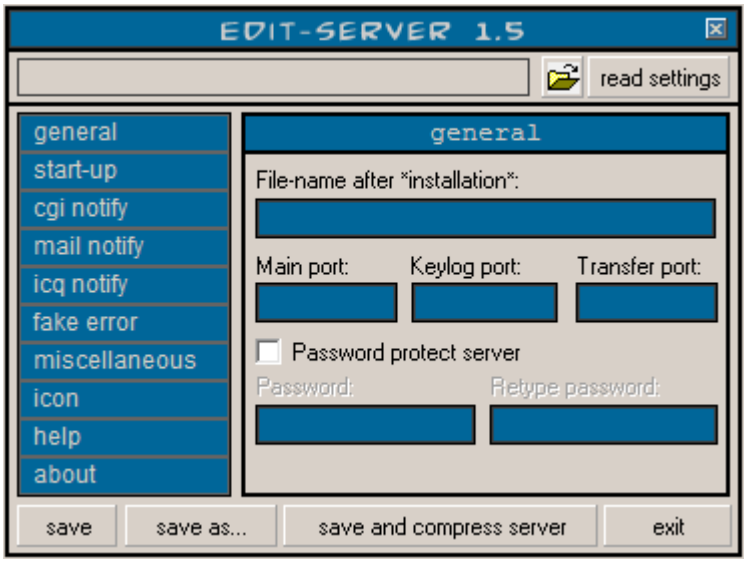


여기서 우리가 필요한 파일은 Edit-server.exe , Net-Devil.exe , Server.exe 이 세개의 파일입니다.

Net-Devil.exe : 메인 프로그램 (클라이언트)

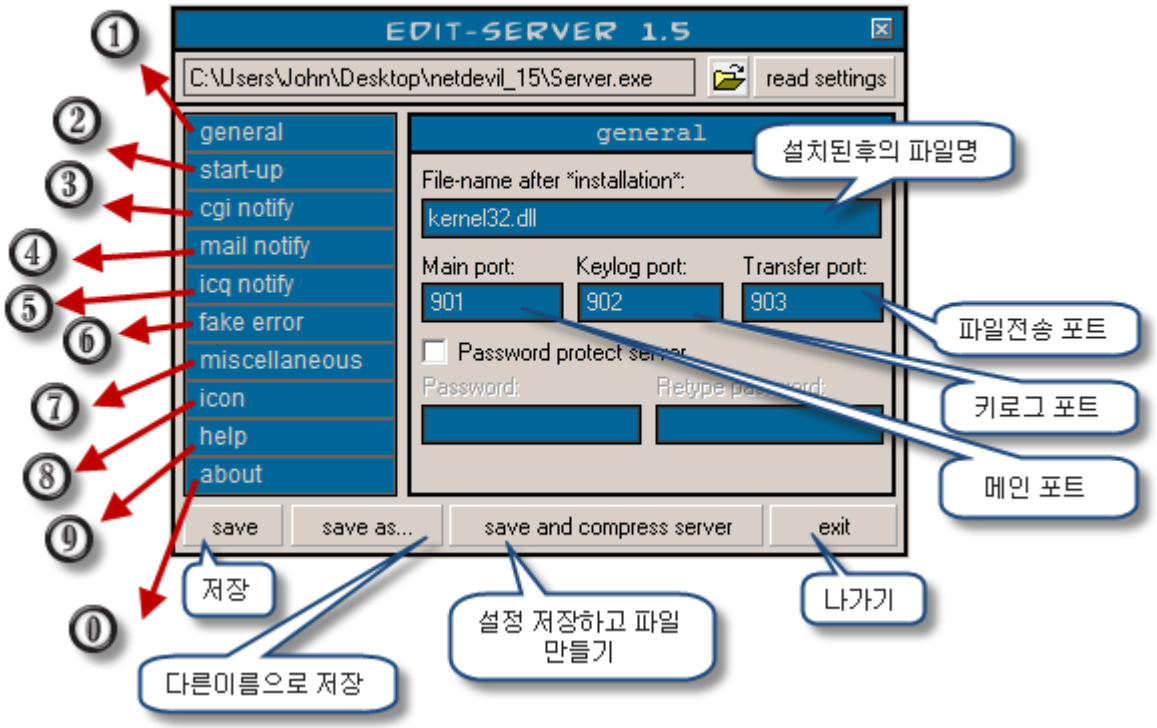
Server.exe : 서버파일 (제어하려는 컴퓨터에 심어줘야 될 파일)
Edit-server.exe : 파일명 그대로 서버파일을 수정하는 프로그램.

먼저 Edit-server 를 실행하여 서버파일설정에 대해 알아보도록 하죠.



여기서 위에  를 클릭하여 서버파일(server.exe)를 불러옵니다.

그럼 아래와같이 기본설정이 나타날거구요

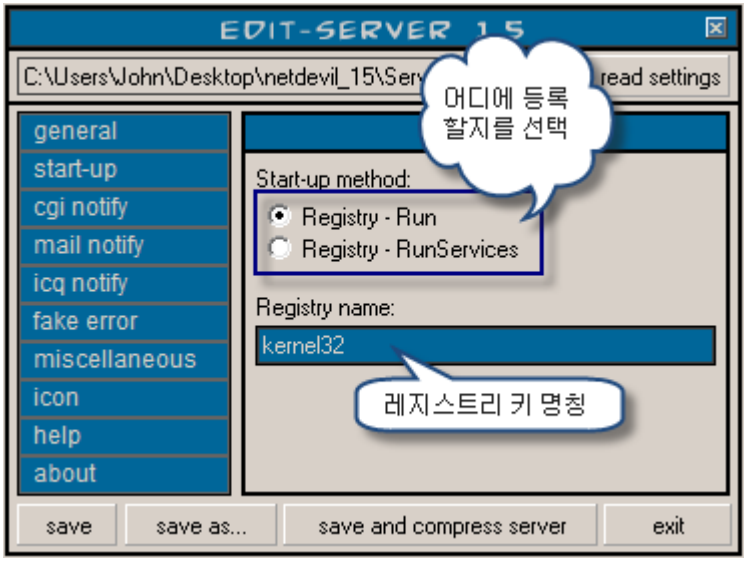


상세하게 하려고 하니 그림이 좀 복잡하게됐네요 ^^;

일단 하나하나씩 설명 드리도록 하겠습니다.

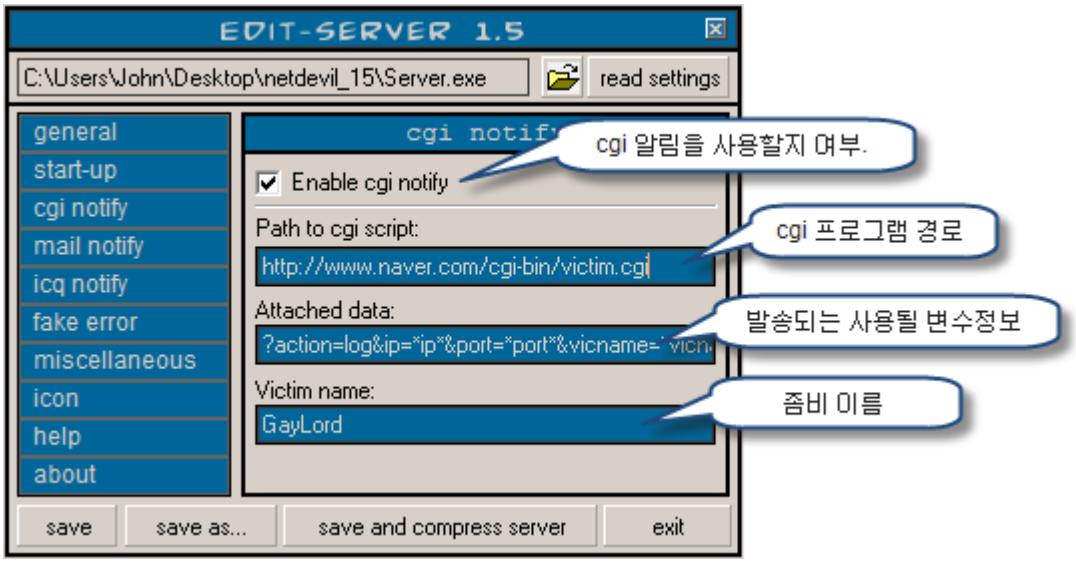
1, general(기본설정): 서버의 기본정보를 설정하는곳인데요 "설치가 되고난후의 파일명" 여기서는 디폴트로 "kernel32.dll" 로 되어있네요. 이건 자신이 원하는 파일명으로 수정하시면 되겠구요. "main port" 는 감염된 컴퓨터를 제어할 때 사용되는 포트, "key log port"는 말 그대로 키로깅을 모니터링하는 포트, "Transfer port"는 역시 말그대로 파일전송에 사용되는 포트구요. 밑에 "password protect server"를 체크하면 감염된 컴퓨터에 접속시 패스워드가 사용되게 되며 다른 넷데빌사용자로부터 자신의 좀비컴퓨터를 보호하게 됩니다. 체크를 하게되면 밑에 패스워드 입력창이 활성화가 될꺼구요 원하는 패스워드를 동일하게 두곳에 입력하시면 되겠습니다.

2, Start-up(자동실행 설정):



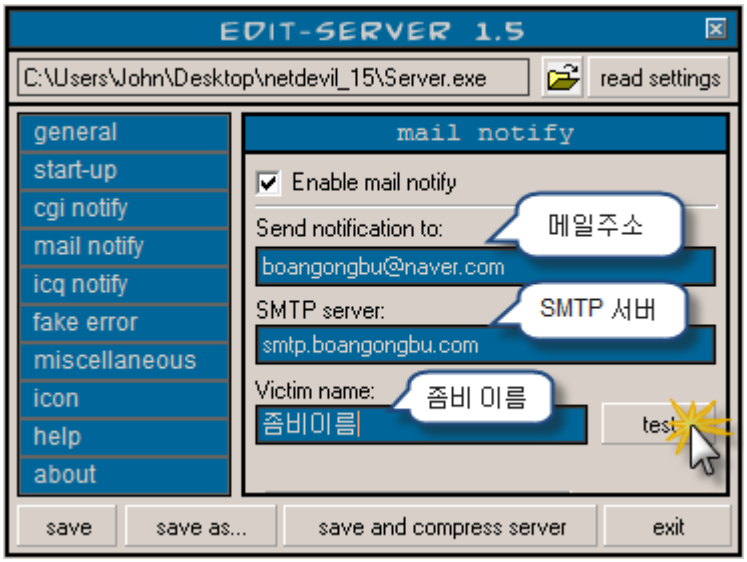
자동실행 설정인데요 키값을 추가할 레지스트리 위치와 키 명칭을 설정하는 곳입니다. 위에 설명대로 설정하시면 되겠구요.

3, cgi notify(CGI알림) :



현재 온라인된 좀비 컴퓨터의 정보를 CGI로 받아보는 기능인데요. CGI파일은 압축파일내에 함께 동봉되어 있다고 하는데 안 찾아지더라구요. ^^;
PERL이나 PHP를 조금 아시는 분이라면 쉽게 제작이 가능하니깐 직접 만들어 사용하시는거도 괜찮을 듯.

4, mail notify(메일알림) :



현재 접속된 좀비 컴퓨터의 정보를 메일로 보내주는 기능.

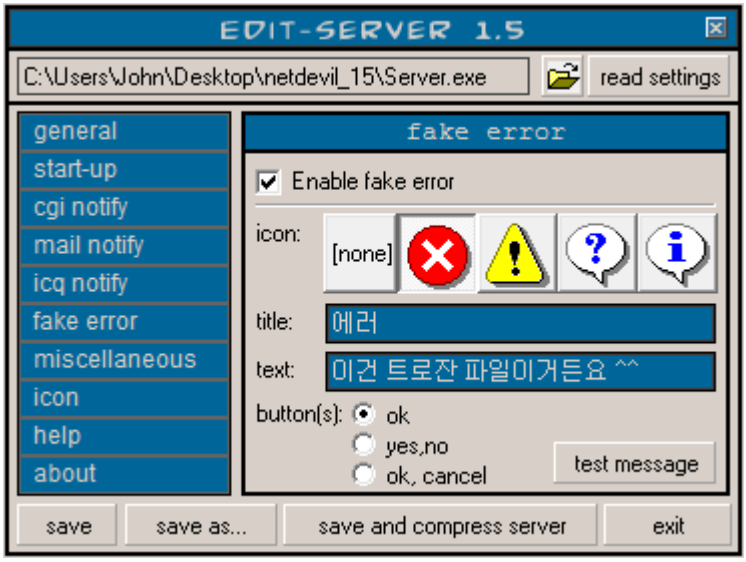
사용하시려면 Enable mail notify 를 체크하시구요 Send notification to: 에는 정보를 받을 메일주소. SMTP server 에는 메일 발송서버 . Victim name 에는 좀비이름을 입력하고 “test” 버튼을 클릭하여 발송이 정상적으로 가능한지를 확인합니다.

5, icq notify(ICQ알림) :

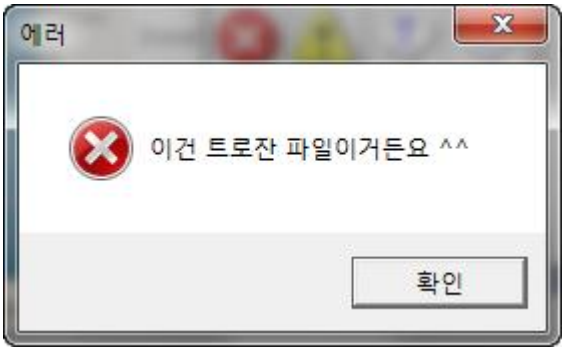
ICQ로 현재 온라인된 좀비서버 정보를 발송하는 기능.

뭐 사용하시려면 http://www.icq.com/ 에 접속하셔서 ICQ를 다운받아 설치를 하시구요 icq 계정을 신청하셔야 되겠죠. 역시 “test” 버튼으로 정상동작 여부를 확인이 가능합니다.

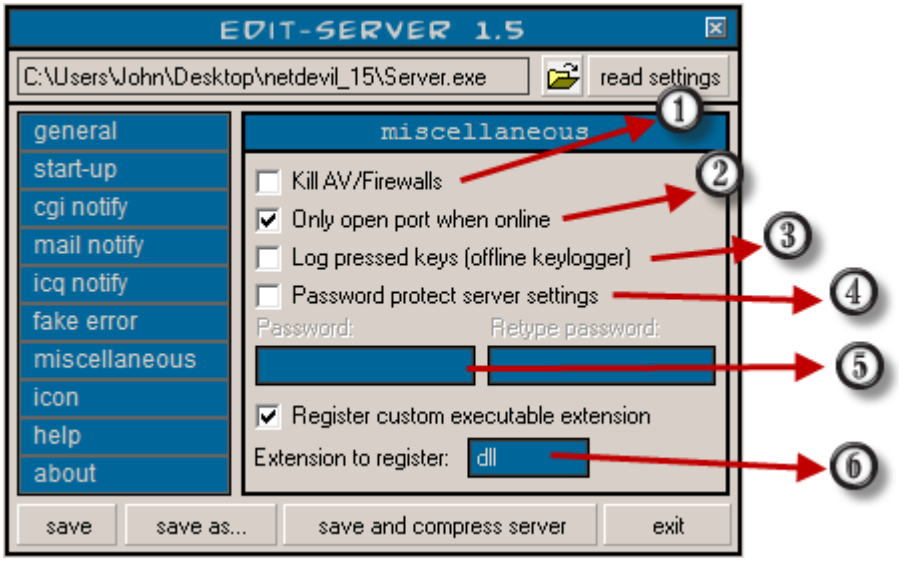
6, fake error (에러위조) :



서버파일 실행시 에러창을 뜨게하여 의심을 피하는 기능을 하죠 ^^
Enable fake error 를 체크하시고 아이콘, 타이틀, 메시지를 입력하신다음. 버튼유형을 선택하시고 “test message”를 클릭하여 미리확인 하시면 됩니다.



7, miscellaneous (기타옵션) :

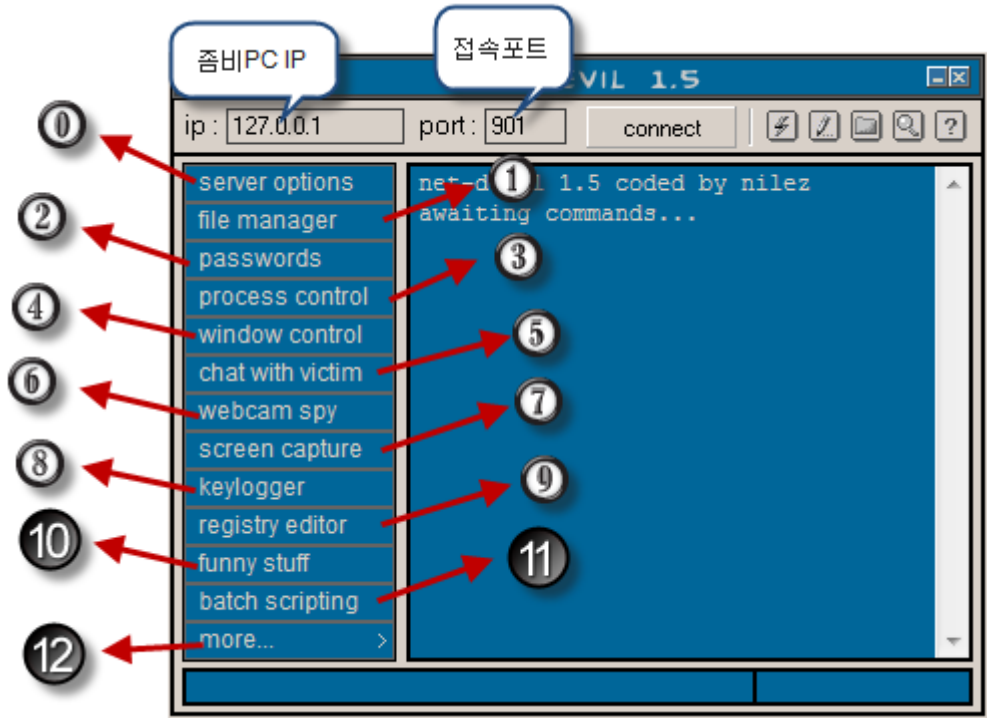


1) **Kill AV/Firewalls**: 체크하시면 10초에 한번씩 프로세스를 확인하여 백신 프로그램과 방화벽을 다운시킵니다.
2) **Only open port when online**: 인터넷에 접속시에만 포트를 열기.
3) **Log pressed keys (offline keylogger)**: 체크하면 오프라인시에도 키로깅실행.
4) **Password protect server settings**: 패스워드를 설정하게되면 패스워드를 아는자만 이 설정을 수정할수있게 됩니다.
5) **Register custom executable extension**: 실행가능한 확장명을 추가하는 기능인데요 밑 입력창에 실행가능 확장명으로 추가를 하고싶은 확장명을 입력합니다. 하지만 이미 존재하는 확장명을 사용하면 안되구요;; 위에 보시면 dll 이라고 적혀져 있는데. 여기 두번째 "L" 는 "엘" 이 아니라 대문자 "i" 를 입력한 것이라고 개발자가 그러네요. 진짜 감쪽같죠? ^^;

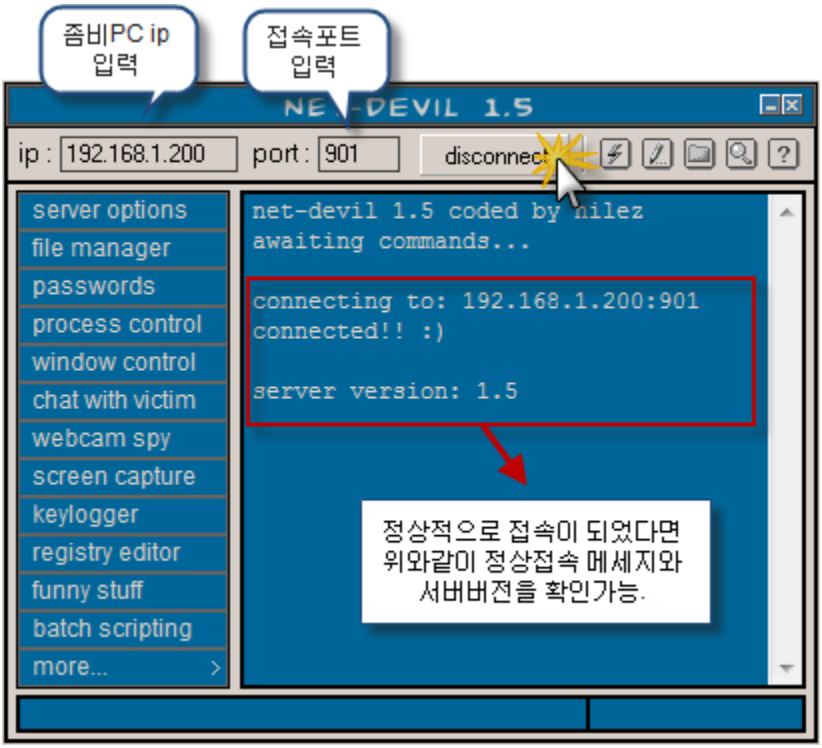
9번과 10번은 도움말과 넷데빌정보이니깐 패스.

이렇게 설정을 다 거쳤다면 밑에 "save and compress server" 를 클릭하면 upx 압축을 거쳐서 설정정보가 server.exe 에 입력되게 되고. 이제 server.exe 파일을 다른 컴퓨터에 설치만 하게 되면 마음대로 제어를 할수있게 되겠죠.

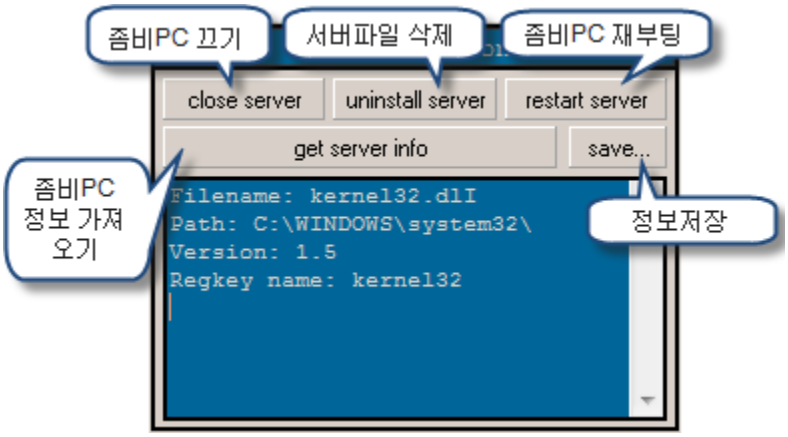
그럼 다음은 클라이언트 프로그램 사용법을 알아보죠.



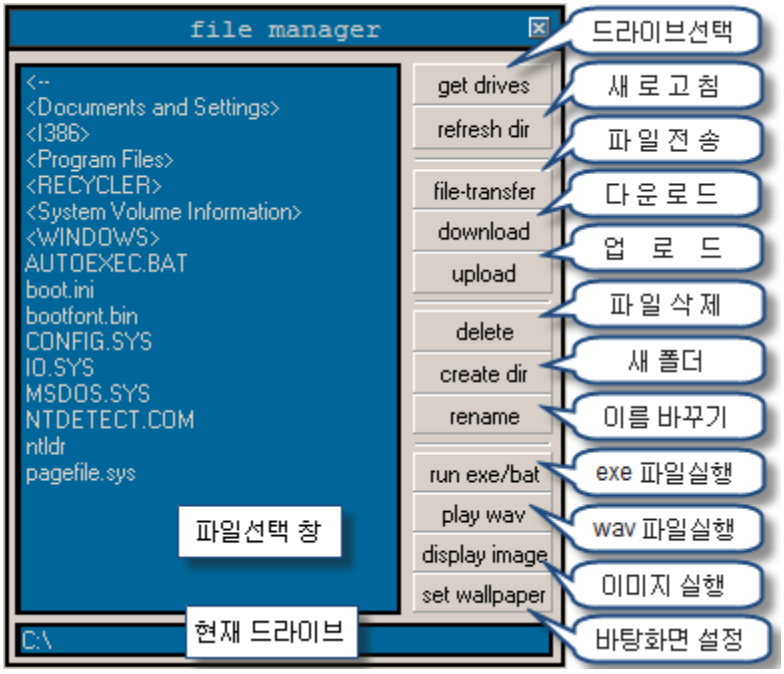
제어프로그램 Net-Devil.exe 창의 뒤에 IP 와 port 는 다 아시는 좀비컴퓨터의 아이피와 포트를 설정하는 곳이구요. 아이피는 아까 위에 설명한 3가지 방법과 포트는 서버파일 설정시 입력한 포트 그대로 써넣으시면 되겠습니다. 정확히 입력한다음 “connect”를 클릭하여 좀비 컴퓨터에 접속.



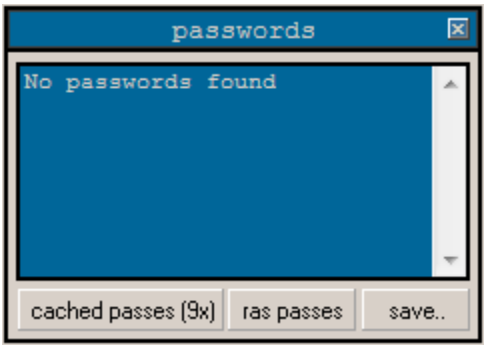
0) **Server options**: 여기서 말하는 서버는 좀비 컴퓨터를 일컷는 말이구요 몇가지 간단한 옵션들을 확인 가능합니다.



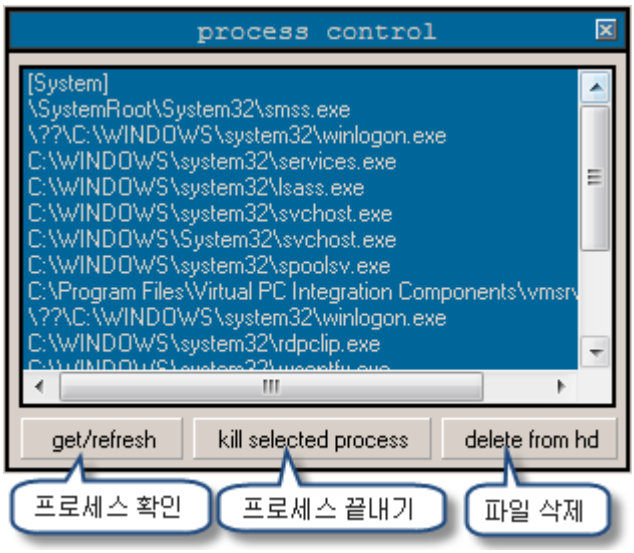
1) **File manager**: 파일 생성/삭제/수정/실행 등 기능



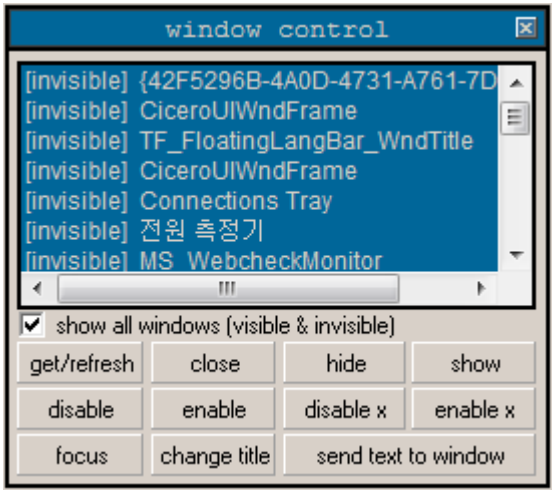
2) Passwords : 시스템에 저장된 패스워드를 읽어들이는 기능인데 현재는 거의 무용지물이죠.



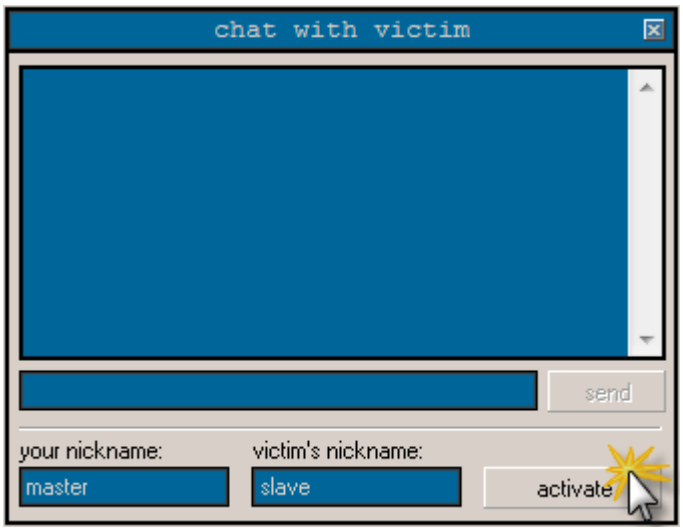
3) Process control(프로세스 제어):



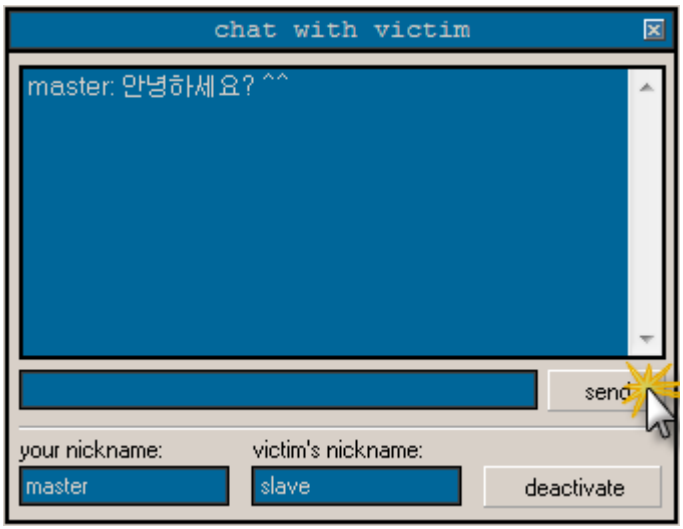
4) **Window control**: 여기서 나오는 윈도우는 그냥 보여지는 그것이 아니구요. 프로그래밍 배우시면 나오는 그 윈도우. 어우~ 잘 사용되지 않으니깐 일단 패스!;;



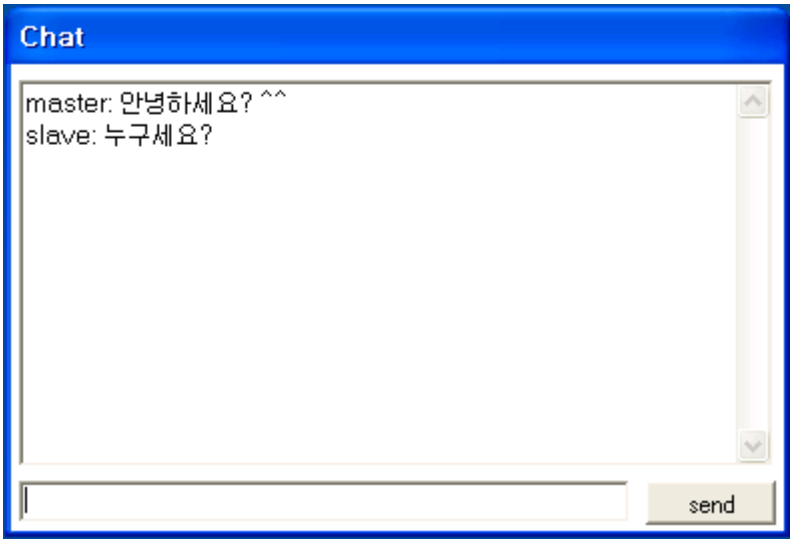
5) **Chat with victim(좀비PC와 채팅을)**: 좀비PC 와 채팅을 즐기는 여유를 보여주세요. ^^



먼저 activete 를 클릭하여 채팅을 활성화.



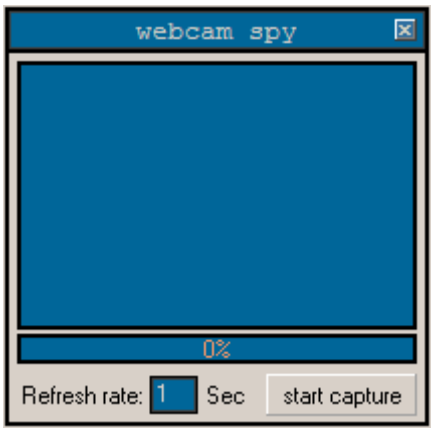
입력창에 말하려는 내용을 입력하고 Send 를 클릭 혹은 엔터키를 누름.



좀비PC 에서 보여지는 화면.

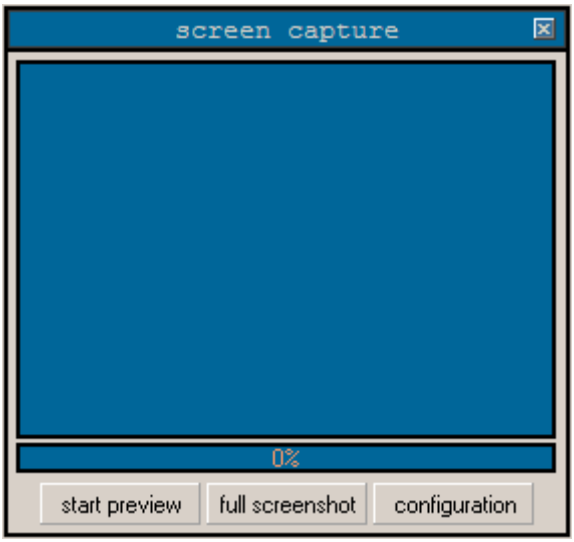
채팅종료시에는 deactivate 를 누르셔야 합니다.

6) **Webcam spy (웹캠 스파이)**: 말그대로 웹캠을 감시하는 기능.



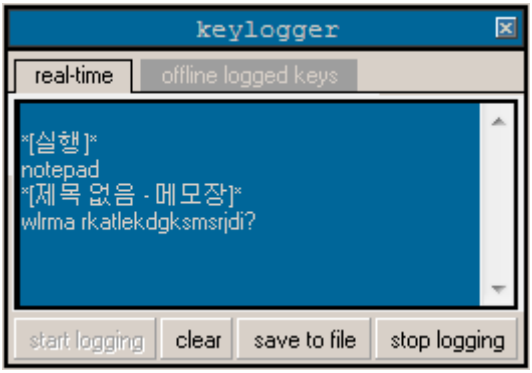
Refresh rate 에 리플래쉬 시간차를 입력하시고 (초 단위). "Start capture"를 클릭하시면 웹캠을 설치한 좀비PC 라면 그쪽 얼굴이 뜨겠죠. ㅎ

7) **Screen capture (스크린캡쳐)**: 좀비PC의 모니터창을 감시가능.

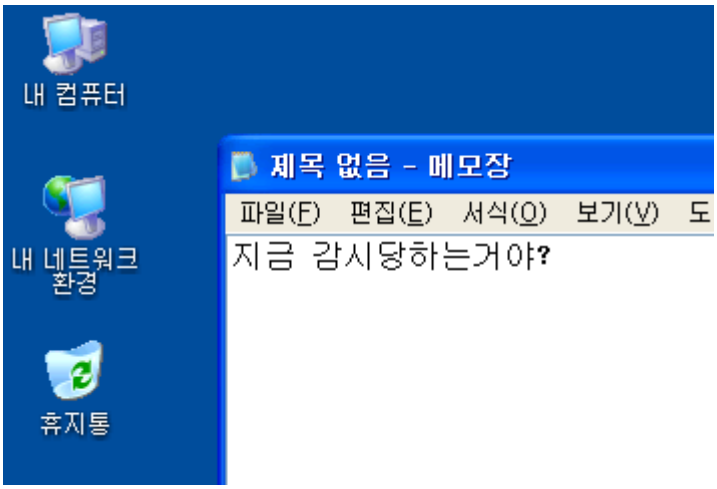


Start preview 를 클릭하면 바탕화면이 떠야되는데… 저의 테스트컴에서는 안뜨더라구요. ㅎㅎㅎ

8) **Keylogger (키로거)**: 설명은 필요없겠죠?



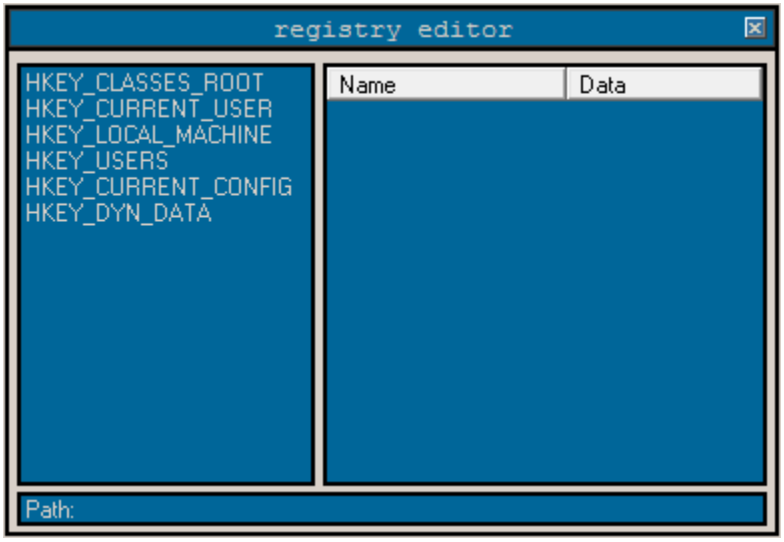
Start logging 을 클릭하여 키로깅 시작.



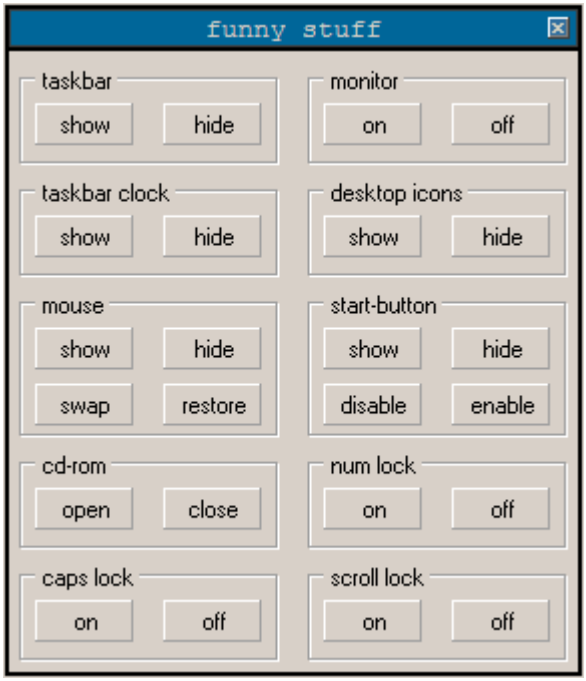
한글은 지원안됨. ^^

Offline logged keys 탭은 오프라인 키로깅 기능을 사용하였을시. 저장된 키보드조작들을 확인하는 기능이구요.

9) **Regstry editor (레지스트리 에디터)**: 그냥 그대로 레지스트리 에디터 ^^;



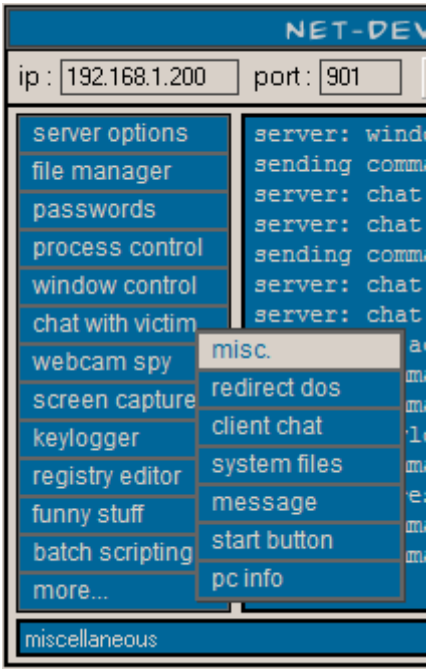
10) **Funny stuff (잼있는 기능들)**:

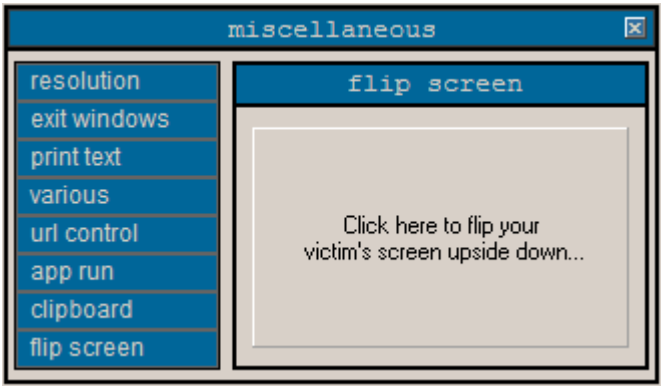


그냥 씨디롬 열고/닫고, 마우스 보여지고/감추고, 모니터 끄고/켜고 하는 잡다한 기능들. 직접 확인하세요 ^^

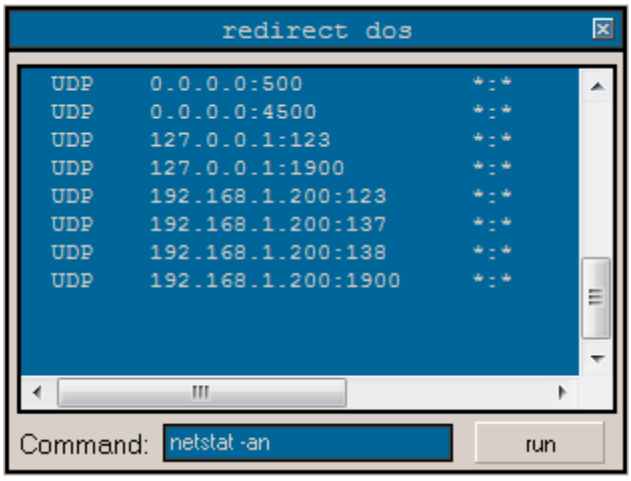
11) **Batch scripting (배치파일 편집)**: 배치파일을 편집하여 실행하고 하는 기능.

12) **Misc** : 잡다한 기능들이 들어있는... 좀비PC에서의 프로그램실행/웹사이트접속, 좀비PC 바탕화면을 거꾸로 돌려놓기. 클립보드확인 등…

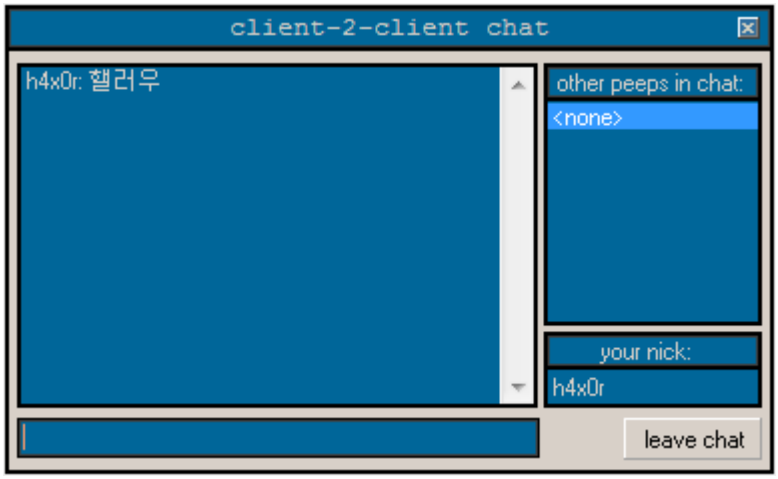




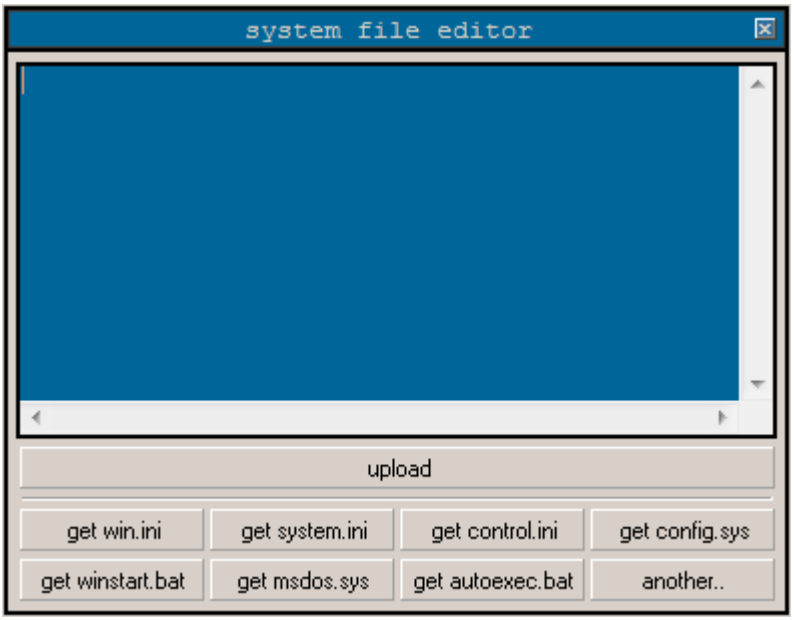
13) **Redirect doc**: 좀비PC에서 dos명령어 실행.



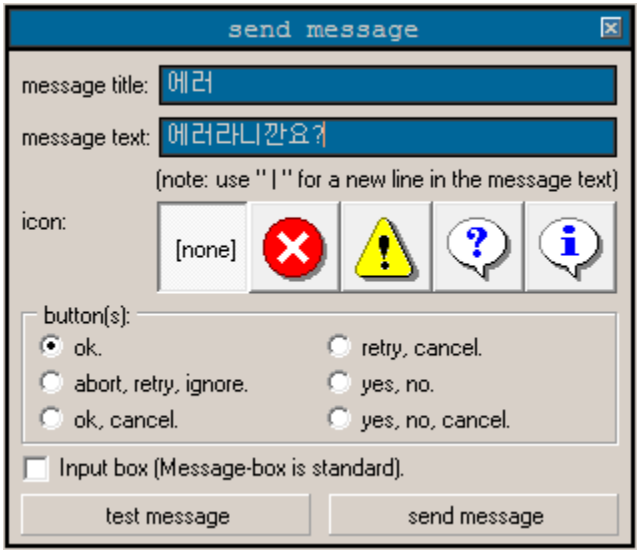
14) **Client chat**: 넷데빌사용자들간의 채팅기능인거 같은데

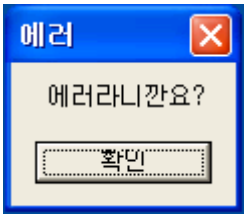


15) **System files**: 시스템파일 편집기.



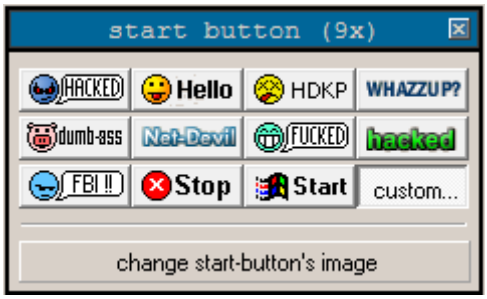
16) **Message**: 에러메세지 작성기



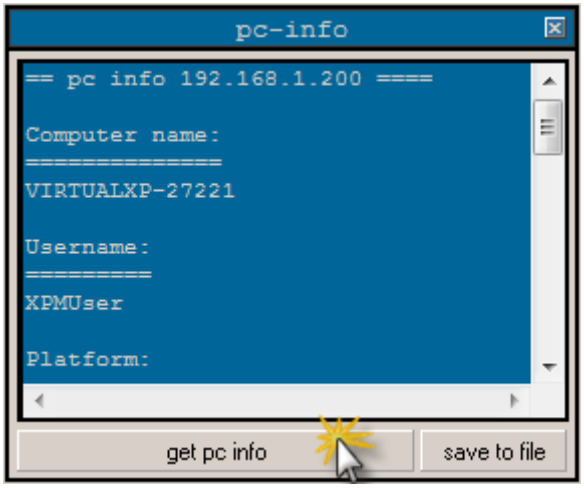


이게 왜 필요할까? ㅡㅡㅋ

17) **Start button**: 시작버튼을 바꿔버리는 잼있는 기능. 하지만 현재는 무용지물. ㅋㅎ 윈도우9x 만 지원되거든요.



18) **PC info**: 좀비PC 정보 확인기능.



어우~ 여기까지. 얼마 안될 것 같던 분량이 이미지 캡쳐까지 하면서 하려니깐 장난 아니네요. ^^

다음강좌는 Sub7…