

UPX 사용 설명서

Ahn 안철수연구소



1 개요

- ❖ 게임 프로그램을 해커가 직접 수정하여 HackShield 해킹방지 기능을 무력화 시키고 더 나아 가 게임 프로그램의 소스 코드도 수정 할 수 있습니다.
- ❖ 해킹 방지 기능 부분 코드를 직접 수정하는 것을 방지하기 위하여 게임 프로그램에 실행 파일 및 관련된 DLL 파일을 실행 압축을 시켜주는 것이 좋습니다. 이를 통하여 해커가 게임 프로그램을 수정하는 것을 어렵게 합니다.
- ❖ 본 문서는 실행 파일 압축 프로그램 중 변형된 UPX를 가지고 보호하는 방법에 대해 설명합니다.

2 UPX (the Ultimate Packer for eXecutables) 특징

- ❖ 뛰어난 압축률
 - ✓ 기존에 winZip, zip, gzip 보다 뛰어난 압축 알고리즘을 이용하여 파일 사이즈를 줄임
- ❖ 빠른 decompression
 - ✓ Ancient Pentium 133 : ~10 MB/sec, Athlon XP 2000+ : ~200 MB/sec
- No Memory Overhead
 - ✓ in-place decompression를 하기 때문에 실행 시 메모리에 overhead가 발생하지 않음
- ❖ 안정성
 - ✓ compressed and uncompressed file를 내부적으로 CRC를 체크함으로써 안정성을 유지
- Portable
 - ✓ UPX는 C++를 사용하여 작성하였으므로 portable를 높임
- ❖ 거의 대부분에 executable formats을 지원
 - ✓ 예) atari/tos, djgpp2/coff, dos/com, linux/386, dos/exe, dos/sys, win32/pe 등등

3 UPX 사용 설명서

Synopsis

#include "HShield.h"

Command

✓ Compress

▶ Default command로 다음과 같이 압축 레벨을 조절할 수 있습니다.

Command	설명
-1 ~ −9	-1 : compress faster, -9 : compress better
best	Best compress best (can be very slow for big files)

✓ Decompress

▶ 모든 UPX는 "-d" command를 사용하여 unpack 기능을 사용 할 수 있습니다.

✓ Test

▶ "-t" command를 이용하여 데이터에 압축과 압축 해제에 대한 무결성을 테스트 합니



다.

✓ List

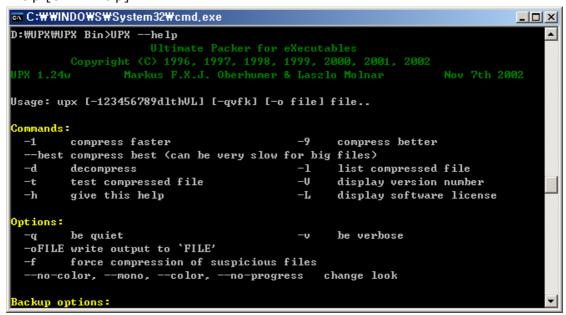
▶ "-I" command는 압축파일에 대한 정보를 command 창에 표시합니다.

Option

Command	설명
	-q : UPX 실행 시 경고를 화면에 표시하지 않는다.
-q	-qq :UPX 실행 시 경고 및 에러를 화면에 표시하지 않는다.
	-qqq : UPX 실행 시 모든 로그를 화면에 표시하지 않는다.
-v	UPX 에 대한 경고, 에러 등에 로그를 화면에 표시한다.
-0	UPX 실행 압축된 output 파일을 설정한다.
no-color,	UPX 실행 시 화면 배경 및 옵션을 설정한다.
mono,	
color,	
no-progress	
help	UPX 관련 도움말을 화면에 표시한다.
version	UPX 버전을 화면에 표시한다

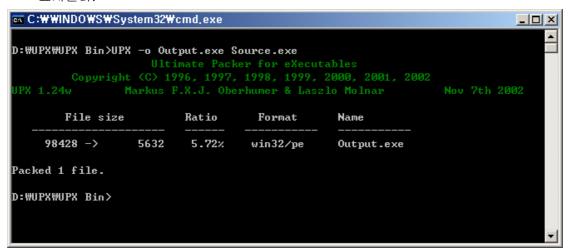
❖ 대표 사용 예제

√ Help [UPX --help]





- ✓ Compress [UPX –o Output.exe Source.exe]
 - ▶ 실제 파일을 압축 시 사용되며 "UPX -o [압축 Output 파일] [압축할 파일]"로 사용한다.
 - ▶ 정상적으로 실행 되었을 경우 파일에 압축 결과와 "Packed 1 File"에 메시지가 화면에 표시된다.



▶ 에러가 발생 시에는 에러 발생 원인과 함께 "Packed 1 File: 0 ok, 1 Error"에 에러 메 시지가 화면에 표시된다

