

Basic RCE 05

작성자	koromoon (koromoon@naver.com)
작성일	2011-08
문제	이 프로그램의 등록키는 무엇인가?
정답	GFX-754-IER-954

(1) 설명



시리얼 키를 찾는 문제임.

OlllyDbg를 열어서 들어가보자! 그럼 무슨 경고창이 뜬. OlllyDbg가 자동으로 이 프로그램은 패킹된 걸 감지하고 패킹되어 있는 상태에서 계속 디스어셈블링 하겠냐고 물음.

0045400B	ASCII	"pa?",0	
004541A2	ASCII	"gm"	
004541C9	ASCII	"03vz@2",0	
004542BE	ASCII	"OrH7",0	
00454615	ASCII	"c&i8&e"	
00454741	ASCII	"em"	
00454775	ASCII	";]7eøn?t=u",0	
00454786	ASCII	"-h",0	
00454874	ASCII	"su"	
0045494F	ASCII	"?))",0	
00454B0B	ASCII	"koFok"	
00454D9F	ASCII	"C3",0	
00454EA7	ASCII	"ve",0	
00454F59	ASCII	"Q6",0	
00454FDD	ASCII	"DM"	
00455086	ASCII	"FY",0	
004550B4	ASCII	"P5"	
00455165	ASCII	"V2W"	
00455203	ASCII	"J005/08/20",0	
00455303	ASCII	"oh",0	
0045537F	ASCII	"RAko",0	
004553BB	ASCII	"UnkM",0	
004553E9	ASCII	"G&Vo;F",0	
00455827	ASCII	"6A"	
004558A5	ASCII	"Si"	
004559D0	ASCII	"pl"	
00455B5C	ASCII	"t'.ma",0	
00455BBD	PUSHAD		(Initial CPU selection)

경고창을 무시하고 실행해서 Search for -> All referenced text strings 메뉴로 텍스트를 찾아본 결과 제대로 된 글씨가 안 나옴.

해당 프로그램은 패킹되어 있다는 것으로 추측됨.

(2) 패킹

패킹(Packing)의 정의

패킹이란 실행 파일이 보호를 목적으로 암호화하거나 압축하여 소스코드를 볼 수 없게 만드는 것임. **(실행 파일 포장이라는 개념)**

이와 반대로 언패킹(Unpacking)이란 보호를 목적으로 암호화 및 압축된 실행 파일(패킹된 파일)을 원상태로 해제하는 것을 의미함.

일반 압축과 실행 압축의 차이

항목	일반 압축	실행 압축
대상 파일	모든 파일	PE 파일 (exe, dll, sys)
압축 결과물	압축(zip, rar 등) 파일	PE 파일 (exe, dll, sys)
압축 해제 방식	전용 압축 해제 프로그램 사용	내부의 Decoding 루틴
파일 실행 여부	자체 실행 불가	자체 실행 가능
장점	모든 파일에 대해 높은 압축율로	별도의 해제 프로그램 없이 바로

	압축 가능	실행 가능
단점	전용 압축 해제 프로그램이 없으면 해당 압축 파일을 사용할 수 없음.	실행할 때마다 Decoding 루틴이 호출되기 때문에 실행 시간이 아주 미세하게 느려짐.

패킹을 왜 하는가?

소프트웨어를 그냥 배포한다면 분석이 가능하므로 핵심 기술이 그대로 노출될 위험이 있음. 어셈블리어의 분석이 쉽지 않지만 능숙한 사람이라면 가능함. 그래서 패킹 기술을 이용하여 핵심 기술을 보호하고자 함.

악성코드에서는 '자기가 컴퓨터에서 어떤 일을 수행하는지 모르게 행동해야 한다' 라는 사명감이 있음. 그래서 악성코드 제작자는 직접 제작한 악성 스크립트나 악성 프로그램에 분석가가 분석하지 못하게 패킹하여 악성코드의 활동 기간을 늘리는 것임.

실행 파일을 압축하게 되면 용량이 줄어들기 때문에 다운로드시 걸리는 시간이 줄어듦. 또한 압축된 실행 파일은 파일 시스템의 공간을 덜 차지하기 때문에 파일 시스템으로부터 데이터가 메모리에 전송되는 시간이 덜 걸리므로 더 빨리 실행됨. 즉 실행 속도가 빨라짐. 이러한 장점들로 인해 악성코드가 다른 컴퓨터에 빨리 유포시킬 수 있음.

(3) 패커

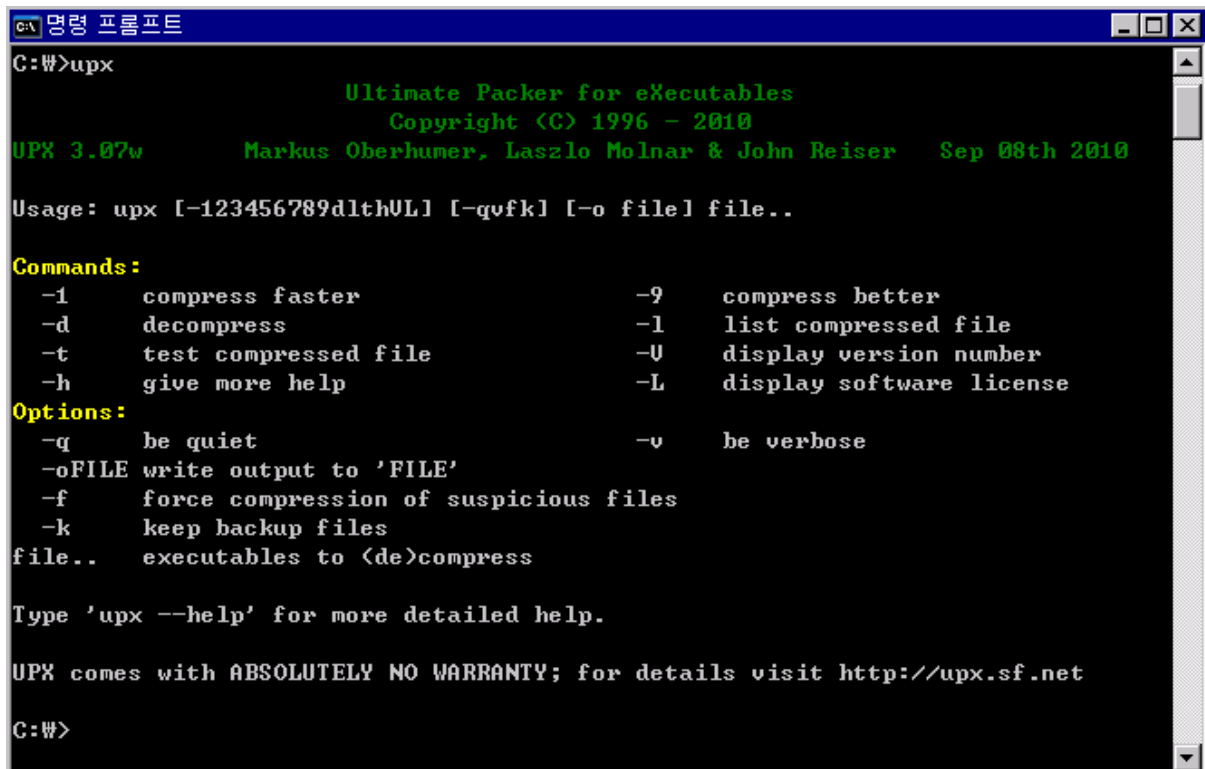


패커(Packer)의 정의

패커는 패킹을 해주는 프로그램으로 실행 파일의 압축과 보호 목적으로 사용됨.

이와 반대로 언패커(Unpacker)는 언패킹을 해주는 프로그램임.

(4) UPX



```
C:\W>upx

      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2010
UPX 3.07w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010

Usage: upx [-123456789dlthUL] [-qvfkl] [-o file] file..

Commands:
  -1      compress faster                -9      compress better
  -d      decompress                    -l      list compressed file
  -t      test compressed file          -U      display version number
  -h      give more help                -L      display software license

Options:
  -q      be quiet                      -v      be verbose
  -oFILE  write output to 'FILE'
  -f      force compression of suspicious files
  -k      keep backup files
file..   executables to <de>compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit http://upx.sf.net

C:W>
```

정의

패커의 일종이며 가장 많이 사용함.

여러 운영체제에서 수많은 파일 포맷을 지원하는 오픈 소스 실행 파일 압축 프로그램이며 GNU 일반 공중 사용 허가서를 통해 공개된 자유 소프트웨어임.

압축, 압축 해제 기능을 모두 담당함.

참고로 암호화 기능이 없음.

다운로드 사이트 : <http://upx.sourceforge.net/>

옵션

-1 ~ -9 : -1이 압축 속도가 제일 빠르고 -9로 갈수록 압축율이 좋음.

-d : 압축 해제

-o : 새로운 파일 생성 (이 옵션이 없을 경우 원본은 사라짐)

참고로 옵션을 생략해도 사용 가능함.

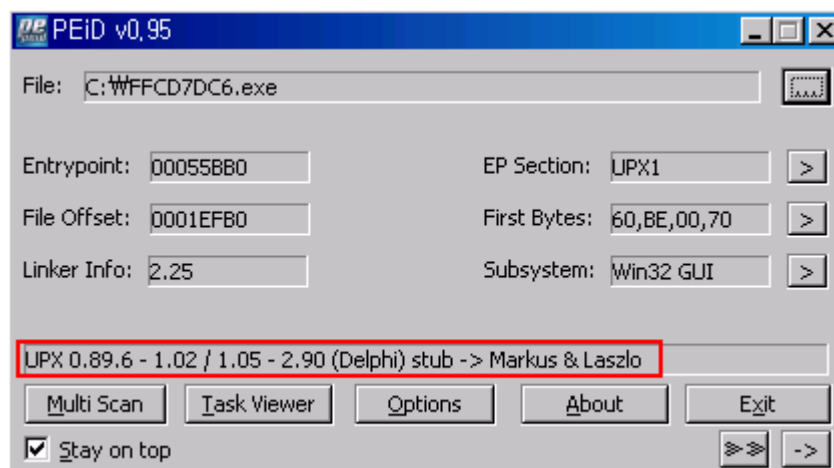
압축할 때

upx filename.exe	<--- 단일 파일 압축시
upx *.*	<--- 폴더 안에 있는 모든 파일을 압축시
upx -9 filename.exe	<--- 압축율을 최대로 하는 압축시 (-1 : 최저, -9 : 최고)
upx -9 *.*	<--- 폴더 안에 있는 모든 파일을 압축하고 압축율을 최고로 하는 압축시

압축 해제할 때

upx -d filename.exe	<--- 단일 파일 압축 해제시
upx -d *.*	<--- 폴더 안에 있는 모든 파일을 압축 해제시

(5) 크랙 방법



PEiD 프로그램 패킹된 프로그램을 찾음.

UPX로 되어 있음을 확인할 수 있음.

```
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>upx -d FFCD7DC6.exe -o u-FFCD7DC6.exe
          Ultimate Packer for eXecutables
          Copyright (C) 1996 - 2010
UPX 3.07w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 08th 2010

      File size      Ratio      Format      Name
      -----
      315392 <- 132608  42.05%    win32/pe    u-FFCD7DC6.exe

Unpacked 1 file.

C:\>
```

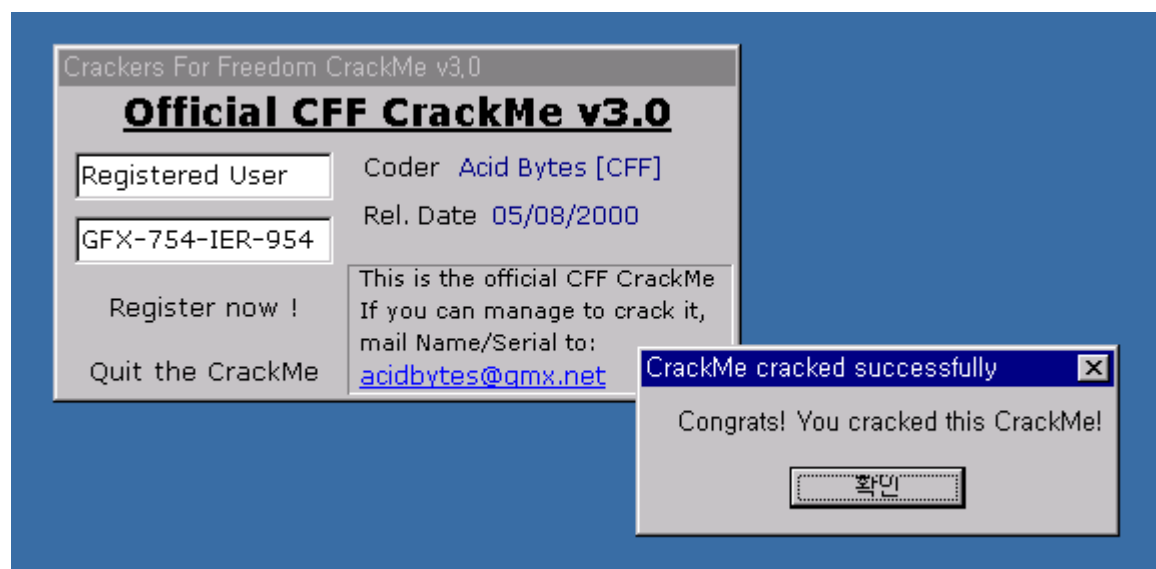
"upx -d FFCD7DC6.exe -o u-FFCD7DC6.exe"명령어를 사용해서 언패킹함.

00440E9C	DD u-FFCD7D.00440CA8	ASCII "4wB"
00440EA7	ASCII "Unit1"	
00440EDC	MOV ECX,u-FFCD7D.00440FC8	ASCII "No Name entered"
00440EE1	MOV EDX,u-FFCD7D.00440FD8	ASCII "Enter a Name!"
00440F08	MOV ECX,u-FFCD7D.00440FE8	ASCII "No Serial entered"
00440F0D	MOV EDX,u-FFCD7D.00440FFC	ASCII "Enter a Serial!"
00440F2F	MOV EDX,u-FFCD7D.00441014	ASCII "Registered User"
00440F4C	MOV EDX,u-FFCD7D.0044102C	ASCII "GFX-754-IER-954"
00440F5A	MOV ECX,u-FFCD7D.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	MOV EDX,u-FFCD7D.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F74	MOV ECX,u-FFCD7D.00441080	ASCII "Beggar off!"
00440F79	MOV EDX,u-FFCD7D.0044108C	ASCII "Wrong Serial,try again!"
00440F8E	MOV ECX,u-FFCD7D.00441080	ASCII "Beggar off!"
00440F93	MOV EDX,u-FFCD7D.0044108C	ASCII "Wrong Serial,try again!"
00440FC8	ASCII "No Name entered",0	
00440FD8	ASCII "Enter a Name!",0	
00440FE8	ASCII "No Serial entered",0	
00440FF8	ASCII "d",0	
00440FFC	ASCII "Enter a Serial!",0	
00441014	ASCII "Registered User",0	
0044102C	ASCII "GFX-754-IER-954",0	
0044103C	ASCII "CrackMe cracked "	
0044104C	ASCII "successfully",0	
0044105C	ASCII "Congrats! You cr"	
0044106C	ASCII "acked this Crack"	
0044107C	ASCII "Me!",0	
00441080	ASCII "Beggar off!",0	
0044108C	ASCII "Wrong Serial,try"	
0044109C	ASCII " again!",0	
004410A9	MOV ECX,u-FFCD7D.004410C8	ASCII "Have a nice day"
004410AE	MOV EDX,u-FFCD7D.004410D8	ASCII "Mail Name/Serial to acidbytes@gmx.net !"
004410C8	ASCII "Have a nice day",0	
004410D8	ASCII "Mail Name/Serial"	
004410E8	ASCII " to acidbytes@gm"	
004410F8	ASCII "x.net !",0	
00441270	PUSH EBP	(Initial CPU selection)
00441293	MOV EDX,u-FFCD7D.004412D0	ASCII "Crackers For Freedom CrackMe v3.0"
004412D0	ASCII "Crackers For Fre"	
004412E0	ASCII "edom CrackMe v3."	
004412F0	ASCII "0",0	

Search for -> All referenced text strings 로 텍스트 파일을 찾아봄.

00440EDA	. 6A 00	PUSH 0	
00440EDC	. B9 C80F4400	MOV ECX,u-FFCD7D.00440FC8	ASCII "No Name entered"
00440EE1	. BA D80F4400	MOV EDX,u-FFCD7D.00440FD8	ASCII "Enter a Name!"
00440EE6	. A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440EEB	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440EED	. E8 76C1FFFF	CALL u-FFCD7D.0043D068	
00440EF2	> 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440EF5	. 8B83 C8020000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440EFB	. E8 20FFFFDFF	CALL u-FFCD7D.00420E20	
00440F00	. 837D FC 00	CMP DWORD PTR SS:[EBP-4],0	
00440F04	~ 75 18	JNZ SHORT u-FFCD7D.00440F1E	
00440F06	. 6A 00	PUSH 0	
00440F08	. B9 E80F4400	MOV ECX,u-FFCD7D.00440FE8	ASCII "No Serial entered"
00440F0D	. BA FC0F4400	MOV EDX,u-FFCD7D.00440FFC	ASCII "Enter a Serial!"
00440F12	. A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F17	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F19	. E8 4AC1FFFF	CALL u-FFCD7D.0043D068	
00440F1E	> 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440F21	. 8B83 C4020000	MOV EAX,DWORD PTR DS:[EBX+2C4]	
00440F27	. E8 F4FEF0FF	CALL u-FFCD7D.00420E20	
00440F2C	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F2F	. BA 14104400	MOV EDX,u-FFCD7D.00441014	ASCII "Registered User"
00440F34	. E8 F32BFCFF	CALL u-FFCD7D.00403B2C	
00440F39	~ 75 51	JNZ SHORT u-FFCD7D.00440F8C	
00440F3B	. 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440F3E	. 8B83 C8020000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440F44	. E8 D7FEF0FF	CALL u-FFCD7D.00420E20	
00440F49	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F4C	. BA 2C104400	MOV EDX,u-FFCD7D.0044102C	ASCII "GFX-754-IER-954"
00440F51	. E8 D62BFCFF	CALL u-FFCD7D.00403B2C	
00440F56	~ 75 1A	JNZ SHORT u-FFCD7D.00440F72	
00440F58	. 6A 00	PUSH 0	
00440F5A	. B9 3C104400	MOV ECX,u-FFCD7D.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	. BA 5C104400	MOV EDX,u-FFCD7D.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F64	. A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F69	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F6B	. E8 F8C0FFFF	CALL u-FFCD7D.0043D068	
00440F70	~ EB 32	JMP SHORT u-FFCD7D.00440FA4	

특정 단어가 있는 코드로 이동해보면 ID와 PW를 확인할 수 있음.



입력하면 크랙 성공함.