한국항행학회 논문지 제17권 제 5호 2013년 10월 (JKONI 17(5): 545-551, Oct. 2013)

좀비 클라이언트 차단을 위한 실행 압축 기술에 관한 연구

A Study on Generic Unpacking to Prevent Zombie Client on Mobile Platform

고종빈*, 이상하**, 손태식***

Jong-Bin Ko*, Sang-Ha Lee**and Tae-Shik Shon***

요 약

다양한 악성코드 탐지 및 분석 회피 기술 중 실행 압축 기술은 악성코드의 용량을 줄이고 분석가가 코드를 분석할 때 혼란을 주도록 코드가 변형되기 때문에 악성코드의 확산이 용이해지고 분석하는데 시간이 오래 걸려 신속한 대응이 어렵게 만들고 있다. 본 논문에서는 실행 압축 도구들을 분석하고 엔트로피 값의 변화량을 기반으로 하는 실행 압축 기술 무력화 방법을 제안한다.

Abstract

Packed technique makes difficult to respond quickly because the malicious-code is reduced size that easy to diffusion and changed code that make spend longer time for analysis. In this paper, we analysed the packing tool softwares and we proposed construction and detection methods of the packed technique for easy to analysis of the packed malicious code based on variation of entropy value.

Key words : Packed technique, Malicious code, Zombie client

I. 서 론

최근 봇이나 웜 등의 악성코드로 인한 사이버 공격이 증가하고 있다. 봇이나 웜 등을 이용하여 좀비 PC를 생성하고 이를 통하여 공격자는 일반 사용자의 개인정보를 수집하거나 금전적인 피해를 입히고 있다. 매일 새롭게 발견되는 악성코드의 수와 종류는 지속적으로 증가하고 있기 때문에 그에 대한 신속한 분석 및 대응이 필요하다. 하지만 최근 공격자들은 악성코드를 제작할 때 신속한 분석 및 대응이 어렵게 하도록 다양한 탐지 및 분석 회피 기술들을 사용하고 있어 악성코드로 인하여 사건이 생겼을 때 신속한 대응이 어려워지고 있다. 다양한 탐지 및 분석 회피 기술 중 실행 압축 기술은 악성코드의 용량을 줄이고 분석가가 코드를 분석할 때 혼란을 주도록 코드가 변형되기 때문에 악성코드의 확산이 용이해지고 분석하는데 시간이 오래 걸려 신속한 대응이 어렵게 만들고 있다.

본 논문에서는 이러한 실행 압축된 악성코드의 분석이 용이하도록 실행 압축된 악성코드 자동 분석을 위하여 실행 압축 기술의 현황 및 탐지 방법 그리고 실행 압축 해제 기법을 조사하고 이것을 바탕으로 실

* 아주대학교 컴퓨터공학과 박사과정(Division of Computer Engineering, Ajou University)
** 동서울대학교 정보통신과 교수(Department of Information and Communication, Dong Seoul University)
*** 아주대학교 정보컴퓨터공학부 조교수(Department of Information and Computer Engineering, Ajou University)
· 제1저자 (First Author) : 고종빈(Jong-Bin Ko, TEL : +82-31-219-2531, email : Jongbin.Ko@gmail.com)
· 접수일자 : 2013년 7월 30일 · 심사(수정)일자 : 2013년 7월 31일 (수정일자 : 2013년 9월 11일) · 게재일자 : 2013년 10월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.5.545

행 압축된 악성코드 자동 분석을 위한 무력화 알고리즘을 제안한다.

본 논문은 2장에서 실행 압축 도구의 최신 동향을 알아보고 대표적인 실행 압축 도구들에 대하여 분석한다. 3장에서는 실행 압축 무력화 기술 제안을 위하여 엔트로피를 계산 및 그래프 역 분석을 수행하여 이를 기반으로 오리지널 엔트리 포인트 도출하였다. 4장에서는 결론 및 향후 연구 방향에 대해 시사한다.

Ⅱ. 관련연구

2-1 실행 압축 도구 동향

악성코드 검사 사이트인 바이러스 토탈(Virus Total)에서는 분석됐던 악성코드를 통해 실행 압축 도구에 대한 통계를 제공하고 있다. 통계 자료에서는 분석된 실행 압축 도구 중 가장 많이 사용된 10개의 종류와 수에 대한 통계치를 제공하고 있다. 통계 자료를 살펴보면 12월 26일 하루 동안 UPX가 12,829개로 가장 많은 비중을 차지하고 있었고, PEcompact 4254개, ASPack 2293개로 가장 많은 비중을 차지하는 것을 알 수 있다.

이중 많이 사용되는 UPX와 ASPack의 경우 실행파일을 압축하는 Compressor역할을 한다. Compressor역할을 하는 실행 압축 도구들의 경우 별다른 안티 리버싱의 기법이 적용되지 않고, 실행 압축 해제도 비교적 쉽다. UPX와 ASPack는 순수한 의도로 사용되는 경우가 많으나 이와는 다르게 악의적인 의도로 사용되는 실행 압축 도구에는 UPack, PESpin, NSAnti등이 있다.

UPack은 중국의 Dwing이 만든 실행 압축 도구로 원본 파일을 크게 변형시키고 PE헤더를 심하게 훼손한다. 실제로 UPack이 처음 등장했을 때 여러 PE분석 프로그램들이 정상적으로 작동하지 않았고, 이 특징 때문에 악성코드 제작자들이 UPack을 주로 사용하게 되었다. 이로 인해 현재 대부분의 안티바이러스 프로그램은 UPack으로 실행 압축된 파일은 무조건 삭제한다.

Protector역할을 하는 실행 압축 도구는 안티 리버싱기법이 적용되어 실행 압축 해제가 매우 까다롭다. 상용 Protector에는 ASProtect, Themida, SVKP등이 있고, 공개용 Protector에는 UltraProtect, Morphine등이 있다. 이 중 Themida는 옵션마다 풀기위한 접근 방식이 다르기 때문에 강력한 protector중 하나이고 Themida로 실행 압축된 실행파일을 실행 압축 해제하기가 매우 어렵다. 그렇기 때문에 몇몇 악성코드는 강력한 실행 압축을 위해 Themida를 종종 사용한다.

2-2 실행 압축 도구 분석

○ PEID Signature

PEID는 PE 파일의 실행 압축 도구 및 컴파일러를 탐지하는 가장 일반적인 공개 도구이며, 파일분석, 어셈블링, 디어셈블링을 할 때 도움이 되는 소프트웨어이다. 현재 PEID는 600개 이상의 시그니처를 기반으로 PE 파일의 실행 압축 도구 및 컴파일러를 탐지할 수 있다.

PEID의 실행 압축 파일 탐지 방법은 시그니처를 통한 탐지 방법으로 각 실행 압축 도구에 대한 시그니처 추출 방법은 크게 두 가지로 EP(Entry point)와 Section 정보를 기준으로 Hex Sequence를 시그니처로 사용하는 방법으로 나뉜다.

○ MRC (Mandiant Red Curtain)

MRC는 시스템 침해사고 대응을 위한 공개 소프트웨어이다. 이 도구는 시스템의 침해 여부를 빠르고 효과적으로 조사하기 위한 목적으로 설계되었다. PE 파일의 구조 분석을 통해 악성 파일인지 정상 파일인지 여부를 판단한다.

암호화 또는 압축 등의 회피 기법이 적용된 데이터의 경우 PE 파일의 엔트로피가 구조화된 데이터와 비교해 상대적으로 높다는 점을 이용해 가중치를 주는 방식이다. 침해 여부의 결과는 위협 스코어를 계산하여 조사할 필요가 있는 파일을 Red로 표현하고 의심스러운 것을 Yellow, 정상적인 PE 파일은 Green으로 나타낸다. 그리고 PE 파일의 시그니처 분석을 통해서 실행 압축 여부를 판단한다.

MRC는 Entry Pointer의 Signature를 검사하여 알려진 실행 압축 기술을 탐지한다. 그러나 Armadilo, AcidCrypt, Yoda, MEW와 같은 실행 압축 도구의 경

우는 시그니처를 확인하지 못했다. 그리고 File Virus는 0.764의 점수로 정상파일로 판단하였고, Bot 전파 바이러스의 경우 4.800으로 위협 프로그램으로 판단하는 것을 확인하였다. UPX와 ASpack, ASProtect의 경우 코드 엔트로피를 0으로 계산했는데 이것은 Entry point 섹션을 잘못된 섹션으로 계산하여 이러한 결과가 나온 것으로 추정된다. 또한 MRC는 파일의 Entropy를 결정하는데 슬라이딩 윈도우를 적용한다. 이 방법은 작은 섹션을 가진 큰 블록의 데이터가 랜덤한 데이터를 가지고 있을 때 유용하다.

○ Exeinfo PE

PE 스캔툴로는 PEiD가 가장 널리 알려져 있고 많이 쓰이지만 마지막 업데이트인 2008년 10월 21일 이후 오랫동안 업데이트가 없이 지속적으로 플러그인과 시그니처만 업데이트 되었다. Exeinfo PE는 PEiD와 유사한 인터페이스를 제공하지만 프로그램에서 제공하는 다양한 옵션과 실행 압축 도구의 정보뿐만이 아닌 실행 압축 해제 프로그램 정보와 URL 제공, 다른 프로그램과의 연동 등을 제공한다. 또한 지속적인 업데이트를 통해 최신의 시그니처를 업데이트하기 때문에 많은 사용자들이 이용하고 있다.

ver.0.0.2.7(updated 2010. 3. 26)에서는 564개의 시그니처를 탐지할 수 있으며, Exeinfo PE의 기본 폴더의 readme 파일에서 업데이트된 시그니처 정보를 확인할 수 있다.

또한 Zero-byte 테스트를 통해 UPX와 같은 실행 압축 도구의 경우 섹션의 특징을 확인할 수 있다. 섹션이 Zero-byte로 채워져 있고 복원하는 과정에서 쓰이는 실행 압축 도구의 경우 이러한 테스트를 통해 실행 압축 도구의 특성을 예측할 수 있다.

PEiD는 사용자가 시그니처를 생성하여 사용할 수 있지만 Exeinfo PE는 제작자에 의해 업데이트 되는 시그니처 외에 사용자가 시그니처를 업데이트 할 수 없었다. 동일한 파일에 대해 PEiD와 Exeinfo PE로 탐지를 하였을 때 PEiD는 실행 압축 도구를 찾아낸 반면, Exeinfo PE는 실행 압축 도구를 탐지하지 못하는 경우가 발생 하였다.

○ FastScanner

FastScanner 3(2010년 1월 7일 Updated)는 AT4RE(Arab Team 4 Reverse Engineering)에서 만든 프로그램이다. PEiD를 기반으로 제작되었기 때문에, PE(Portable Executable) 시그니처를 분석하여 결과를 제공한다. AT4RE에서 제작한 플러그인과 추가적인 기능들을 제공하여 PEiD에 비해서 사용자가 보기 쉽고 이용하기 편리하게 제작되었다. 또한, 프로그램이 꾸준히 업데이트 되고 있고, 웹을 통하여 AT4RE에서 제공하는 플러그인을 업데이트 할 수 있어서 최신의 플러그인을 사용할 수 있는 장점이 있다. 시그니처 데이터베이스는 PEiD의 시그니처를 쓰고 있다.

FastScanner 3는 Options 탭에서 인터넷을 통해 쉽게 플러그인과 시그니처 데이터베이스를 업데이트 할 수 있고, 플러그인을 업데이트 하면 AT4RE에서 제작한 플러그인과 PEiD에서 제공하는 플러그인들을 제공받을 수 있다.

플러그인 목록 중 GenOEP와 PEiD Generic Unpacker를 통해 UPX로 실행 압축된 프로그램을 테스트한 결과 정확한 OEP 지점을 찾아내는 것을 확인하였다. 하지만 다른 실행 압축 도구로 실행 압축된 프로그램으로 테스트한 결과 OEP를 못 찾아내는 경우가 발생하였다.

실행 압축된 파일에 대해서는 PEiD나 Exeinfo PE와 유사한 결과를 보여줬다. 하지만 실행 압축 되지 않은 파일에 대해서는 PEiD나 Exeinfo PE는 실행 압축 되지 않았다고 탐지하였지만, Fastscanner는 오탐을 하는 경우가 발생하였다.

Ⅲ. 제안하는 실행 압축 무력화 방법

이전 연구에서는 실행 압축 파일에 쓰레기 값이 들어가서 엔트로피의 값을 변화시킬 경우 실행 압축 탐지와 오리지널 엔트리 포인트 시점을 찾기 어려운 단점이 있다. 하지만 쓰레기 값이 들어가서 엔트로피 값이 변화하여도 그래프의 개형의 변화는 없기 때문에 충분히 오리지날 엔트리 포인트를 찾을 수 있게 된다. 실험에 사용된 UPX로 실행 압축한 구구단 프로그램은 코드섹션에 이용하지 않는 부분에 쓰레기 값을 추가하여 프로그램의 실행에는 영향을 주지 않

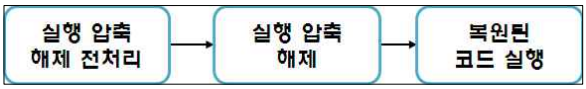

그림 1. 실행 압축 파일 실행 과정
Fig. 1. Operating process of packed file

고 엔트로피 값만 변화 할 수 있게 설정 하였다.

실행 압축 파일을 실행하면 메모리에 값을 읽고 쓰면서 실행 압축 해제 과정을 거치게 된다. 실행 압축 해제가 완료되면 그 다음부터 복원된 실제의 프로그램이 실행되게 된다. 다음 [그림 1]은 실행 압축 파일 실행 과정을 나타내는 그림이다.

실행 압축 파일의 실행 과정에서 엔트로피 값은 초기 실행 부분에서는 아직 실행 압축 해제가 되지 않았기 때문에 랜덤성이 높아 엔트로피의 값이 높게 나온다. 실행 압축 파일이 실행되면서 이후에는 압축 해제 과정이 진행되므로 랜덤성이 떨어져 엔트로피 값이 작아진다. 또한 압축 해제 완료된 시점에서부터는 엔트로피의 값이 크게 변하지 않게 되므로 엔트로피 그래프는 엔트로피의 변화가 일정 범위에서 조금씩 변화하는 모습을 나타내게 된다. 기존의 연구에서의 문제점은 엔트로피의 값으로 실행 압축되어있는지 압축이 풀렸는지 판단한다는 것이다. 일반적으로 실행 압축된 파일의 엔트로피 값은 실행 압축 안된 파일에 비해 크지만 특정 파일의 엔트로피 값은 실행 압축이 되어 있지 않아도 기존 연구에서 주장하는 실행 압축되었다고 판단되는 엔트로피 값의 범위에 들어가는 경우도 있다. 그리고 실행 압축 과정에서 코드 섹션에 쓰레기 값을 넣어 인위적으로 엔트로피 값을 변화 시킬 수도 있기 때문에 문제가 존재한다.

본 논문에서 제안하는 방법은 랜덤성을 측정하기 위하여 엔트로피를 사용하지만 엔트로피의 값만으로 실행 압축 여부 및 오리지날 엔트리 포인트를 찾지 않고 엔트로피의 값의 변화량을 가지고 실행 압축 무력화를 수행한다. 제안하는 방법의 가장 중요한 포인트는 실행 압축 파일 실행 과정 중 실행 압축이 해제되고 복원된 코드가 실행 하게 되면 랜덤성이 크게 변하지 않는 엔트로피 그래프 구간이 생긴다는 것이다. 가상환경에서 실행 압축 프로그램을 실행시켜 종료시점까지의 각 명령어마다의 엔트로피 변화를 그래프로 표현하고 보면 종료 시점 부분에는 복원된 코드가 실행되어 엔트로피 값이 특정 범위 내의 값을 나타낸다. 종료 시점부터 엔트로피 변화량을 역분석하여 특정 범위내의 변화를 넘어서는 부분이 나오면 그 구간은 오리지날 엔트리 포인트가 있는 구간이 된다. 따라서 이 구간에서의 Jump나 call 명령어를 찾고 Jump나 call 명령어 이후의 도착지점이 오리지날 엔트리 포인트가 되게 된다.

3-1 엔트로피 계산

실험 데이터로 사다리 게임 파일(16.5KB) 그리고 악성코드 샘플 하나(12KB), 총 2가지의 PE 파일에 대한 일반적인 엔트로피 측정과 UPX, ASpack, FSG 총 3가지의 실행 압축 도구를 사용하여 실행 압축하고 해당 PE 파일에 대한 엔트로피 측정을 하였다. 실험에 사용된 악성코드는 2007년에 발견된 것으로 악성코드 제거 프로그램을 강제로 설치하고 계속되는 경고 메시지와 팝업, 종료 불가, 강제 검사와 업데이트 등의 현상을 보이는 악성코드이다. 실행 압축 전 각 파일의 엔트로피 값은 다음과 같다.

이전의 엔트로피를 이용한 무력화 연구에서는 실행 압축된 파일의 엔트로피 값이 7.1 ~ 7.2 정도 된다면 실행 압축되었다고 판단하였다. 하지만 일반적인 악성코드 안에서도 7.7 의 엔트로피 값이 측정되는 악성코드가 발견되었다. 따라서 엔트로피 값으로 실행 압축 여부를 판단하는 것은 오탐을 일으킬 가능성이 존재한다는 것이다. 또한 특정 실행 압축 기법이 이러한 엔트로피 값의 탐지를 피하고자 쓰레기 값을 코드에 넣어 엔트로피 값을 변화시킨다면 해당 방법은 많은 오탐을 일으키게 될 것이다.

표 1. 정상 파일의 엔트로피 측정 결과
Table 1. Entropy values of normal files

파일명	엔트로피 값
사다리 게임 프로그램	6.8
악성코드	7.7

표 2. 실행 압축 파일의 엔트로피 측정 결과
Table 2. Entropy values of packed files

파일명	엔트로피 값
사다리 게임 프로그램 (UPX)	7.7
사다리 게임 프로그램 (ASpack)	7.7
사다리 게임 프로그램 (FSG)	7.6
악성코드 (ASpack)	7.8
악성코드 (FSG)	7.9

표 3. 정상적인 실행 파일의 엔트로피 범위 값
Table 3. Entropy variations of normal files

엔트로피 범위의 최대값	엔트로피 범위의 최소값	엔트로피 범위의 평균값
0.005231	0.000064	0.001805696

다음은 실행 압축 후의 엔트로피 값을 측정한 것이다.

악성코드의 크기가 작은 관계로 UPX를 이용한 실행 압축은 불가능하였다. 또한 제안하는 방법의 핵심인 정상적인 프로그램이 실행되었을 때의 엔트로피 값이 얼마나 변화하는지 실험 하였다. 실험에 쓰인 정상적인 프로그램은 Window XP의 System32 내에서 존재하는 여러 실행 파일 중 랜덤하게 100개를 뽑아 측정하였다. 프로그램이 종료하는 시점까지의 매 명령어마다 메모리 덤프를 수행하고 덤프 파일에서 엔트로피 값을 구한다.

표 3은 실험 결과로 나온 정상적인 프로그램의 엔트로피 값 범위를 나타낸다. 범위 값의 측정은 정상 파일의 엔트로피 값의 최대값에서 최소값을 차이를 이용하여 측정하였다.

정상적인 실행 파일의 엔트로피 범위의 최대값은 0.005231로 측정되었고, 최소값은 0.000064로 측정되었고, 엔트로피 범위의 평균은 0.001805696로 측정되었다. 실험에 쓰였던 실행 압축된 사다리 프로그램의 엔트로피 값이 UPX는 0.3, ASpack은 0.8, FSG는 0.4 정도의 범위에서 변화하는 것을 봤을 때 실험 결과에서 보이는 엔트로피 값은 아주 작은 범위 안에서 변화하는 것을 알 수 있었다.

3-2 오리지널 엔트리 포인트 도출

종료 시점부터 엔트로피 변화량을 역분석하여 엔트로피 변화 값이 정상적인 파일의 엔트로피 변화 범위(± 0.0005)를 넘어서는 부분이 나오면 그 구간을 오리지날 엔트리 포인트가 있는 구간으로 추정한다. 따라서 이 구간에서의 Jump나 call 명령어를 찾고 Jump나 call 명령어 실행 후 주소가 오리지날 엔트리 포인트가 되게 된다.

본 논문에서 제안한 방법으로 FSG로 실행 압축된 사다리 게임의 오리지날 엔트리 포인트를 도출하고 이를 검증한다.

제안하는 실험 방법은 다음과 같다.

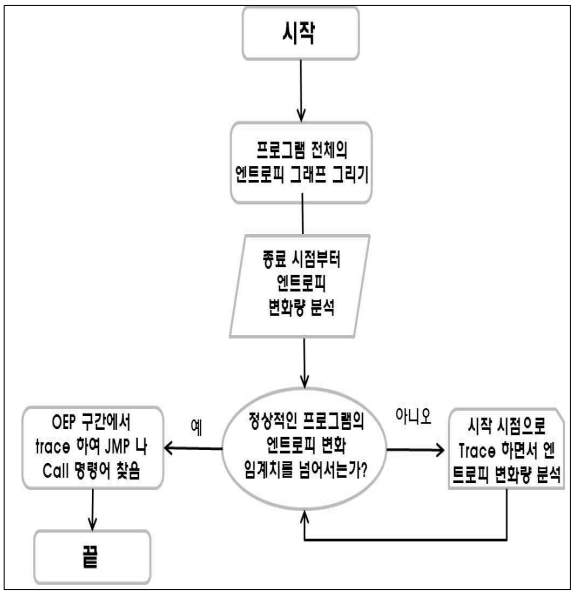

그림 2. 제안하는 기법의 전체 구성도
Fig. 2. Overview diagram of proposed scheme

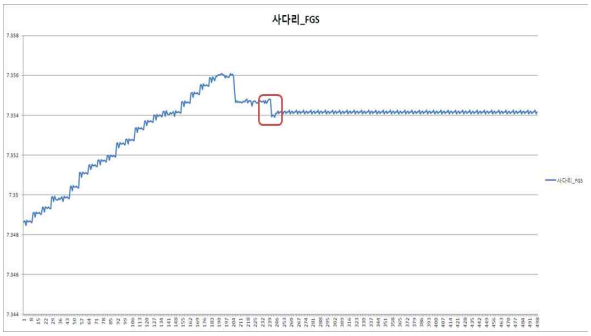

그림 3. 엔트로피 변화량의 초과점
Fig. 3. Overpoint of entropy variation

위 그림과 같이 사다리 게임에 대하여 엔트로피 그래프가 작성되었고, 그래프를 통해 종료시점부터의 엔트로피 변화 값 평균은 약 0.0001이 측정되었다. 이 수치는 그림 3에서 같은 값이 연속으로 발생하는 부분이다. 그래프를 통하여 엔트로피의 변화량이 0.005로 기존의 변화량 보다 5배의 차이를 보이며 정상적인 파일의 변화 범위인 ±0.0005 을 넘어서 변화함을 확인 할 수 있었다. 따라서 OEP 시작점을 추정하고 Jump 명령어를 검색한다. 추정된 OEP 시작점은 그림 3의 붉은 박스 내에서 급격하게 변화량이 감소하는 부분이다. 다음 그림은 추정 시작점부터 Jump 명령어를 찾아 Jump 시점을 찾은 화면이다.

위의 그림에서의 Jump 명령어 지점에서 이동하는 주소는 004026A0 이다. 오리지날 엔트리 포인트라고 확인된 해당 주소에서 덤프 파일을 IAT 테이블을 복원해주는 프로그램을 통하여 IAT 테이블을 복원하였다.

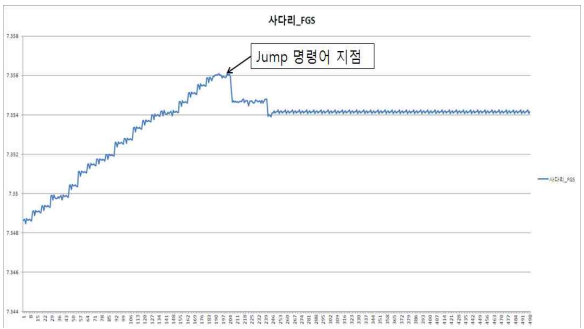

그림 4. Jump 명령어 지점 확인
Fig. 4. Jump command point

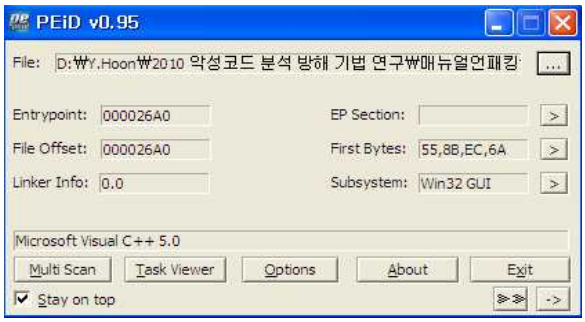

그림 5. 실행 압축 해제 완료 확인 화면
Fig. 5. Completion of unpacking file

PEID에서 확인 한 결과 실행 압축이 해제되었음을 확인 할 수 있다.

Ⅳ. 결 론

본 논문에서는 모바일 플랫폼 환경에서 악성 좀비 클라이언트를 탐지하기 위한 방법으로서 실행 압축 파일에 기반하는 탐지 방법을 제안하였고 엔트로피 기반 탐지를 위한 기초 실험을 수행하였다.

기존의 엔트로피를 이용한 무력화 방법은 엔트로피 값만으로 실행 압축을 무력화하므로 쓰레기 값 등 엔트로피 값에 변화를 주면 오탐이 발생하는 단점이 있다. 본 논문의 제안 방법은 엔트로피 변화량으로 실행 압축을 무력화하므로 기존의 방법의 단점을 보안하고 보다 정확하고 효율적인 분석이 가능할 것으로 기대된다. 향후 엔트로피 변화 값 측정을 위한 알고리즘을 개선하여 보다 효율을 높이는 방법에 대해 연구를 진행할 예정이다.

감사의 글

본 연구는 2012년도 산학협동재단 학술연구비 지원에 의해서 수행된 결과임.

Reference

[1] Virus Total. http://www.virustotal.com/
[2] WildList. http://www.wildlist.org

[3] PEID. http://www.peid.info
[4] AT4RE(Arab Team 4 Reverse Engineering). http://www.at4re.com
[5] Robert Lyda, James Hamrock, "Using Entropy Analysis to Find Encrypted and Packed
[6] Malware,"*IEEE Security and Privacy, Vol. 5, no. 2,* pp. 40-45, Mar/Apr, 2007.
[7] Thomas M. Cover and Joy A. Thomas, "Elements of Information Theory," *Second Edition. Wiley Interscience, New York,* NY, 2006.

고 종 빈(Jong-Bin Ko)

2006년 아주대학교 정보 및 컴퓨터 공학부 공학사
2008년 아주대학교 컴퓨터공학과 석사
2008년 3월~현재: 아주대학교 컴퓨터 공학과 박사과정
관심분야 : 스마트그리드 보안, 보안 위협 평가, 전기자동차 보안, 디지털 포렌식

이 상 하(Sang-Ha Lee)

1987년 울산대학교 전자계산학과 공학사
1991년 아주대학교 컴퓨터공학과 석사
2002년 아주대학교 컴퓨터공학과 박사
1991년~1992년 (주)큐닉스 컴퓨터
1993년~1999년 ㈜케이엔아이시스템
2000년~현재 동서울대학교 정보통신과 교수
관심분야 : 정보통신 Security, 네트워크 관리, IPTV QoS/ QoE

손 태 식(Tae-Shik Shon)

2000년 아주대학교 정보 및 컴퓨터 공학부 공학사
2002년 아주대학교 컴퓨터 공학 석사
2005년 고려대학교 정보보호대학원 박사
2004년 2월~2005년 2월 : University of Minnesota, Research Scholar
2005년 8월~2011년 2월 : 삼성전자 DMC 연구소 책임연구원
2011년 2월~현재 : 아주대학교 정보통신공학부 조교수
관심분야 : 스마트그리드 보안, 디지털 포렌식, 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지