****

**파일 초기 분석**

**thugbfmm.exe**

**임 종 철**

**2020. 09. 13.**

**개 정 이 력**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **버전** | **작성일** | **변경내용** | **작성자** | **비고** |
| 1.0 | 2020.09.13. | 파일 초기 분석 및 문서 작성 | 임종철 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

목차

1. 개요 6

1.1 목적 6

1.2 분석 방법 6

1.3 분석 항목 6

2. 총평 6

2.1 총평 요약 6

3. 상세 진단 결과 7

3.1 파일 다운로드 7

3.1.1 파일 상세 설명 7

3.1.2 상세분석 7

3.2 파일 분석 9

3.2.1 알려진 바이러스 정보는? 9

3.2.1 알려진 바이러스 정보는? 10

3.2.2 컴파일 시간은? 11

3.2.3 난독화 또는 패킹 여부는? 11

3.2.4 import된 정보를 통해 얻을 수 있는 부분은? 12

3.2.5 strings 또는 bintext를 이용해서 얻을 수 있는 정보는? 14

3.2.6 리소스 섹션 분석을 통해 얻을 수 있는 정보는? 16

3.2.6 기타 확인 가능한 정보는? 17

2. 개요
3. 1. **목적**

* PE 구조를 가진 프로그램을 분석하므로써, PE구조에 대한 이해를 높이고 분석에 대한 경험을 쌓는것을 목적으로 함
  1. **분석 방법**
* VMware환경에서 PE구조를 가진 어떤한 프로그램을 다운받아, 분석 툴을 활용해 분석함
* 분석 도구
  + PEview
  + PEiD
  + Wiresahark
  + Dependency Walker
  + BinText, Strings
  + Resource Hacker
  1. **분석 항목**
* 알려진 바이러스 정보는?
* 컴파일 시간은?
* 난독화 또는 패킹 여부는?
* import된 정보를 통해 얻을 수 있는 부분은?
* strings 또는 bintext를 이용해서 얻을 수 있는 정보는?
* 리소스 섹션 분석을 통해 얻을 수 있는 정보는?
* 기타

1. 총평

**2.1 총평 요약**

* 초기 분석의 정보를 모아보면 thugbfmm.exe 파일은 키로거의 기능을 가지며, 파일 및 레지스터리를 다루어, 통신과 같은 보조적인 프로그램을 생성할 것으로 보인다.
* 복합 파일을 생성하며, swf같은 파일로 위장할 수도 있을 것 같다.

2. 상세 진단 결과

**3.1 파일 다운로드**

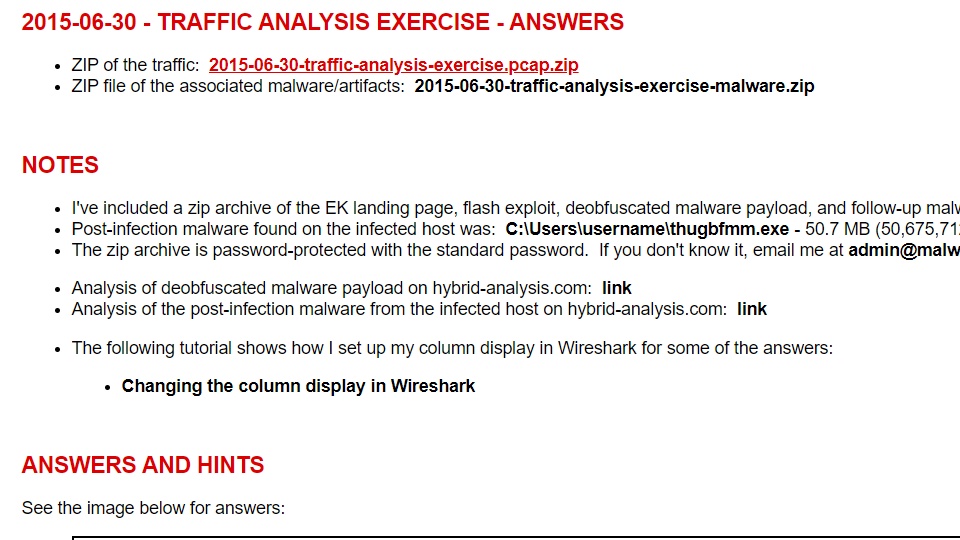
* + 1. **파일 상세 설명**

- 'http://www.malware-traffic-analysis.net/2015/06/30/page2.html'이 사이트에서 '2015-06-30-traffic-analysis-exercise-malware.zip' 파일을 다운로드

- zip파일 해제하여, 여러 내용물 중 'thugbfmm.exe' 파일만을 분석함

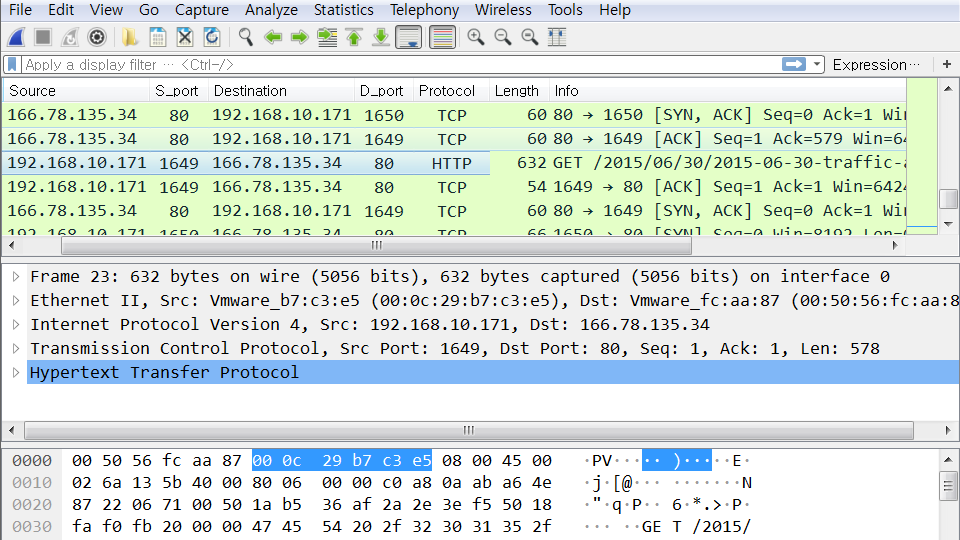
* + 1. **상세분석**

**[Step #1] www.malware-traffic-analysis.net에서 파일을 다운로드함**

****

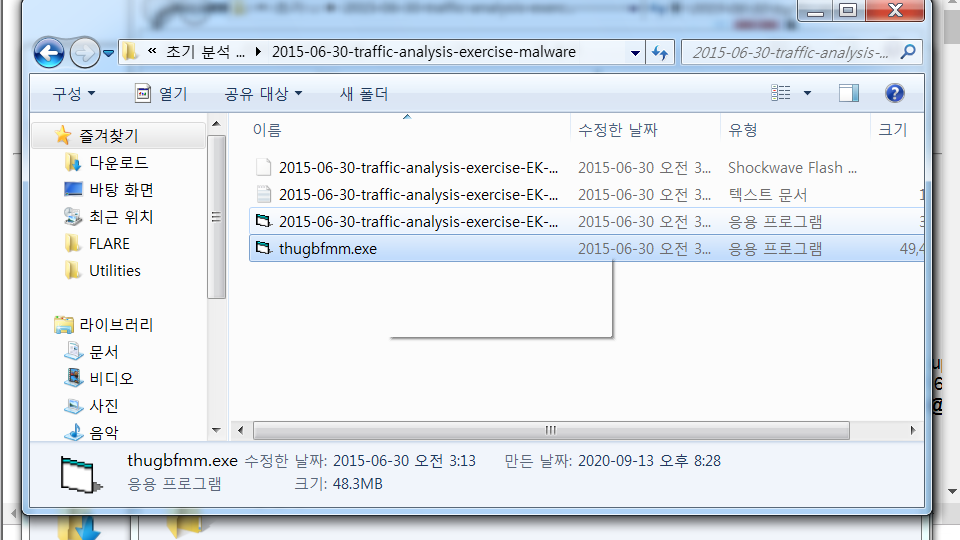
[그림 3 - 1] 파일 다운로드

**[Step #2] 다운로드 과정 패킷 캡처 및 저장함**

****

[그림 3 - 2] traffic-analysis-exercise-malware.pcapng

**[Step #3] 압축 해제 후, 분석할 파일 선택**

****

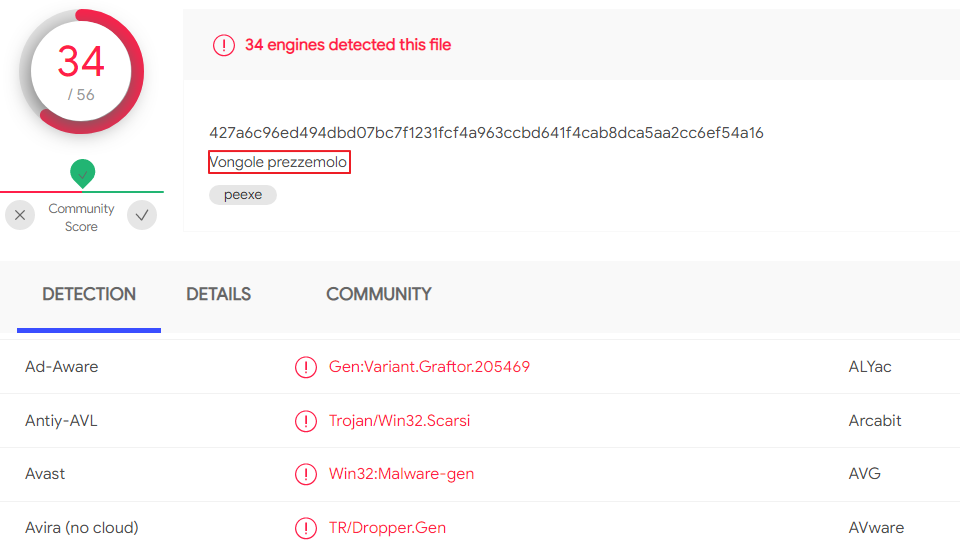
[그림 3 - 3] thugbfmm.exe

**3.2 파일 분석**

**3.2.1 알려진 바이러스 정보는?**

- 해시값 : 2CF1F36F483DD0E316B3DC486171D779

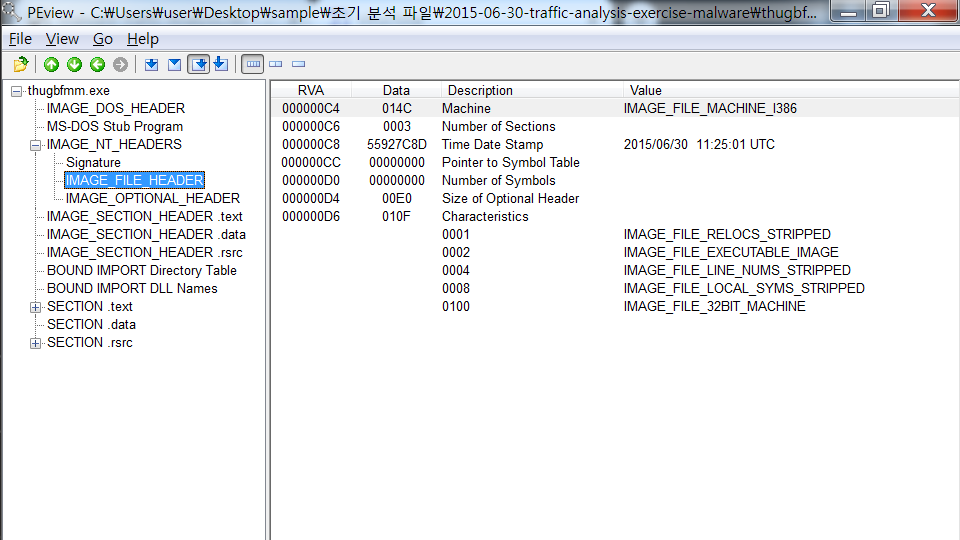
**[Step #1] 바이러스토탈에서 'vongole prezzemolo'라고 알려저 있음**

****

[그림 3 - 4] 34개의 백신에서 악성코드로 알려짐

**3.2.2 컴파일 시간은?**

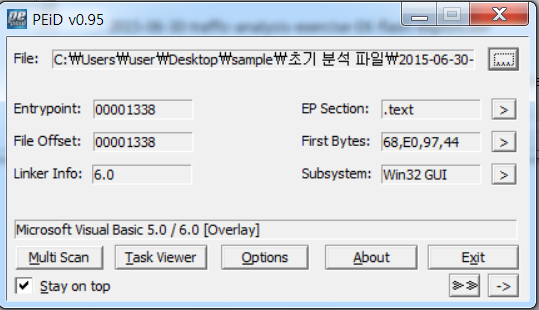
**[Step #1] peview로 보면 2015/06/30 11:25:01 UTC에 컴파일된 걸로 확인됨**

****

[그림 3 - 6] 컴파일 시간 확인

**3.2.3 난독화 또는 패킹 여부는?**

**[Step #1] 난독화 및 패킹은 안된 걸로 확인됨**

****

[그림 3 - 7] 패킹 확인

**3.2.4 import된 정보를 통해 얻을 수 있는 부분은?**

- 사용되는 주요 DLL 이름

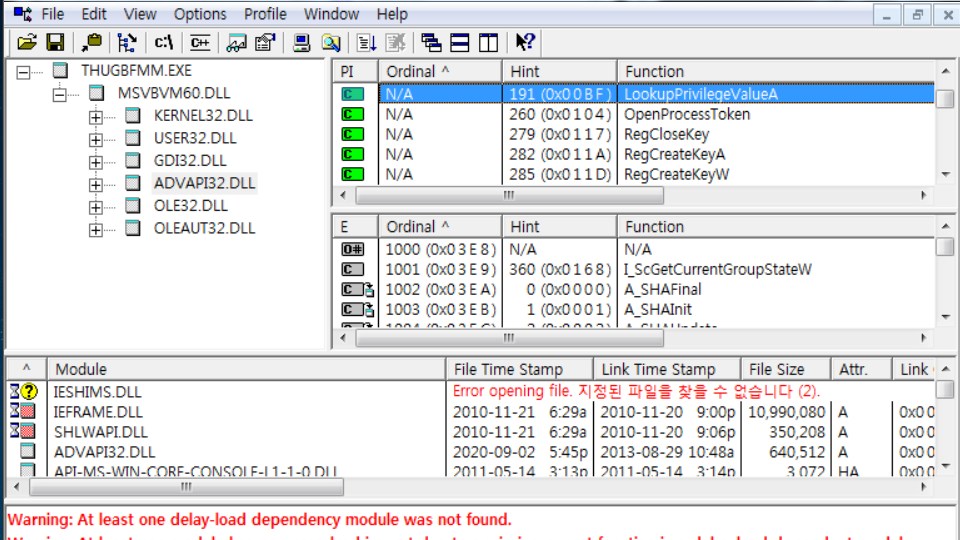
* MSVBM60.DLL, KERNEL32.DLL, USER32.DLL, GDI32.DLL, ADVAPI32.DLL, OLEAUT32.DLL, ETC

- OLE : 복합문서(문서, 달력, 동영상, 소리, 만화, 3D, 계속 갱신되는 뉴스, 콘트롤 등)를 만들거나 전시할 API 집합

- OLEAUT32.DLL : OLE Automation을 위한 동적라이브러리

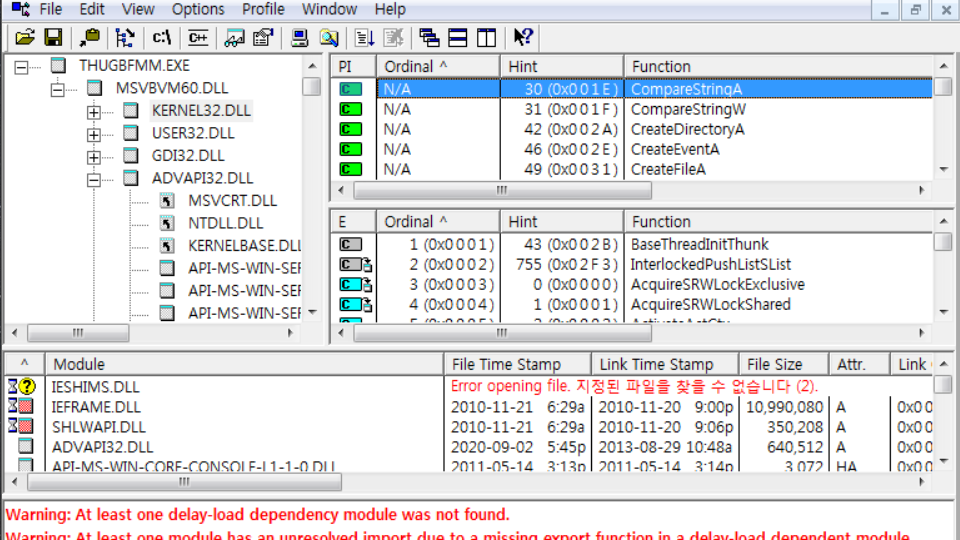
**[Step #1] AdjustTokenPrivileg, RegCreateKeyA와 같은 권한 상승, 레지스터리를**

**다루는 함수를 발견**

****

[그림 3 - 6] ADVAPI32.DLL

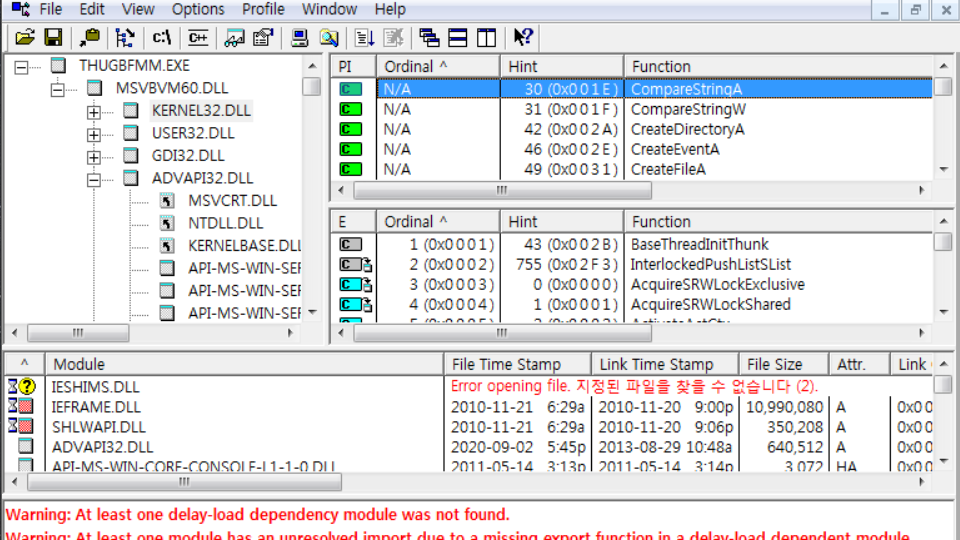
**[Step #2] CreateFileA 등 파일을 찾고, 생성/삭제, 프로세스를 실행하는 함수를 확인**

****

[그림 3 - 6] KERNEL32.DLL

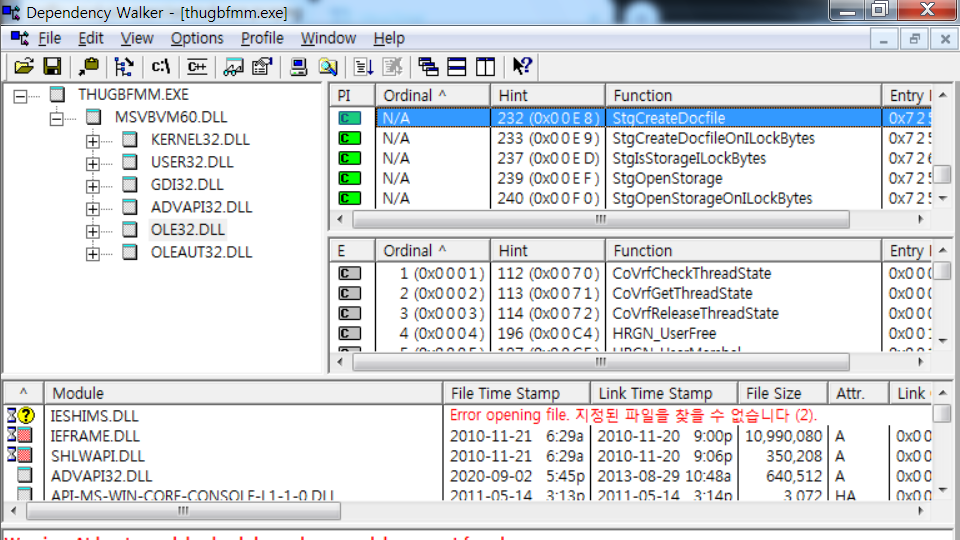
**[Step #3] 키로거에 많이 사용하는 AttachThreadInput, GetAsyncKeyState, GetKeyState**

**함수 사용을 확인**

****

[그림 3 - 6] USER32.DLL

**[Step #2] 복합 문서를 생성하는StqCreateDocfile 함수를 사용하는 것을 확인**

****

[그림 3 - 6] OLE32.DLL

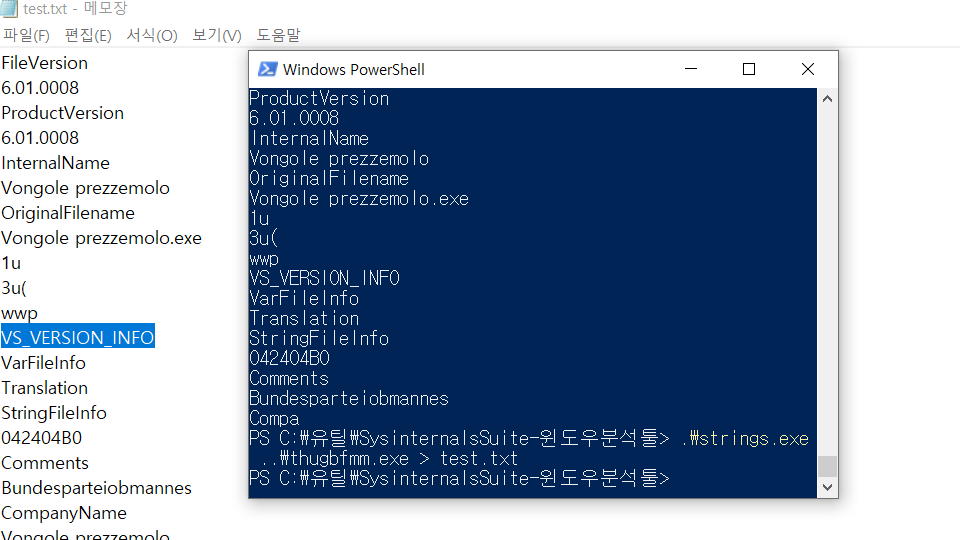
**3.2.5 strings 또는 bintext를 이용해서 얻을 수 있는 정보는?**

- 문자열 내용이 많아 strings를 이용해 'test.txt'파일로 문자열을 추출함

- 일정 구간부터는 문자열이 반복함

|  |
| --- |
| VS\_VERSION\_INFO  VarFileInfo  Translation  StringFileInfo  042404B0  Comments  Bundesparteiobmannes  CompanyName  Vongole prezzemolo  LegalCopyright  Vongole prezzemolo  LegalTrademarks  Vongole prezzemolo  ProductName  Vongole prezzemolo  FileVersion  6.01.0008  ProductVersion  6.01.0008  InternalName  Vongole prezzemolo  OriginalFilename  Vongole prezzemolo.exe  1u  3u(  wwp |

**[Step #1] VS\_VERSION\_INFO 파일 정보가 반복되는 것으로 보임**

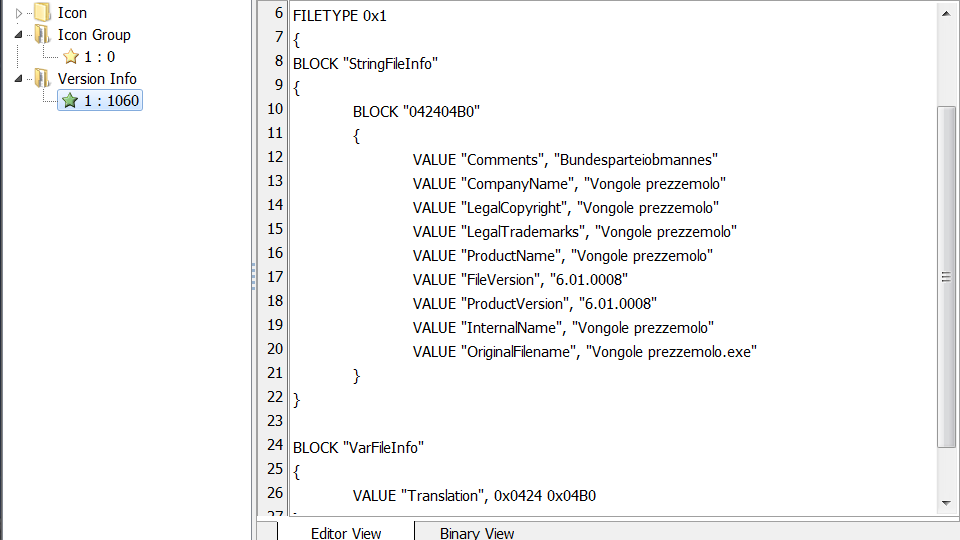
****

[그림 3 - 12] 문자열이 반복됨

**3.2.6 리소스 섹션 분석을 통해 얻을 수 있는 정보는?**

**[Step #1] 아이콘 데이터와 버전관리를 위해 존재는것으로 보이는**

**VS\_VERSION\_INFO를 확인가능**

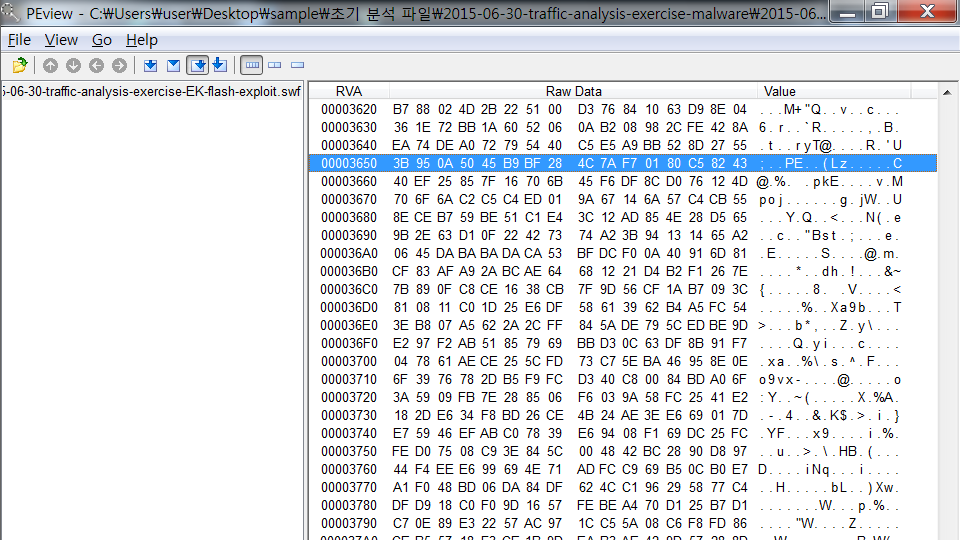
****

[그림 3 - 13] 아이콘과 VS\_VERSION\_INFO 데이터 확인

**3.2.6 기타 확인 가능한 정보는?**

- 같이 첨부된 swf 파일을 PEview로 확인

**[Step #1] 'MZ' 및 'PE' 문자열이 확인되는 것으로 보아, PE파일일수도 있음**

****

[그림 3 - 14] PE문자열 확인