

# KicomAV 가이드

## 목차

---

|       |                       |    |
|-------|-----------------------|----|
| 1     | 개요.....               | 3  |
| 1.1   | 프로젝트 주제 .....         | 3  |
| 1.2   | 프로젝트 추진 배경 및 목표 ..... | 3  |
| 1.3   | 프로젝트 요약 .....         | 3  |
| 2     | 키콤백신 .....            | 4  |
| 2.1   | 키콤백신이란? .....         | 4  |
| 2.2   | 키콤백신 설치 방법.....       | 5  |
| 2.3   | 키콤백신 사용법 .....        | 6  |
| 2.3.1 | 키콤백신 검사.....          | 6  |
| 2.3.2 | 키콤백신 패턴 추가 .....      | 11 |

# 1 개요

---

## 1.1 프로젝트 주제

|                   |
|-------------------|
| 1. 키콤백신 오픈소스 프로젝트 |
|-------------------|

표 1-1 프로젝트 주제

## 1.2 프로젝트 추진 배경 및 목표

|                           |
|---------------------------|
| 키콤백신 사용법 이해 및 패턴 추가 방법 숙지 |
|---------------------------|

표 1-2 프로젝트 추진 배경 및 목표

## 1.3 프로젝트 요약

- |  |
|--|
| <ol style="list-style-type: none"><li>1. 키콤백신 설치</li><li>2. 키콤백신 사용법</li><li>3. 키콤백신 패턴 추가</li></ol> |
|--|

표 1-3 프로젝트 요약

## 2 키콤백신

### 2.1 키콤백신이란?

키콤백신은 하우리 창업자(바이로봇 개발 및 악성코드 분석 총괄)이자 현재 누리랩 대표이신 최원혁씨가 만든 안티 바이러스이다. 또한 키콤백신은 현재 오픈소스로 공개되어 있으며, 꾸준히 업데이트 진행중이다.

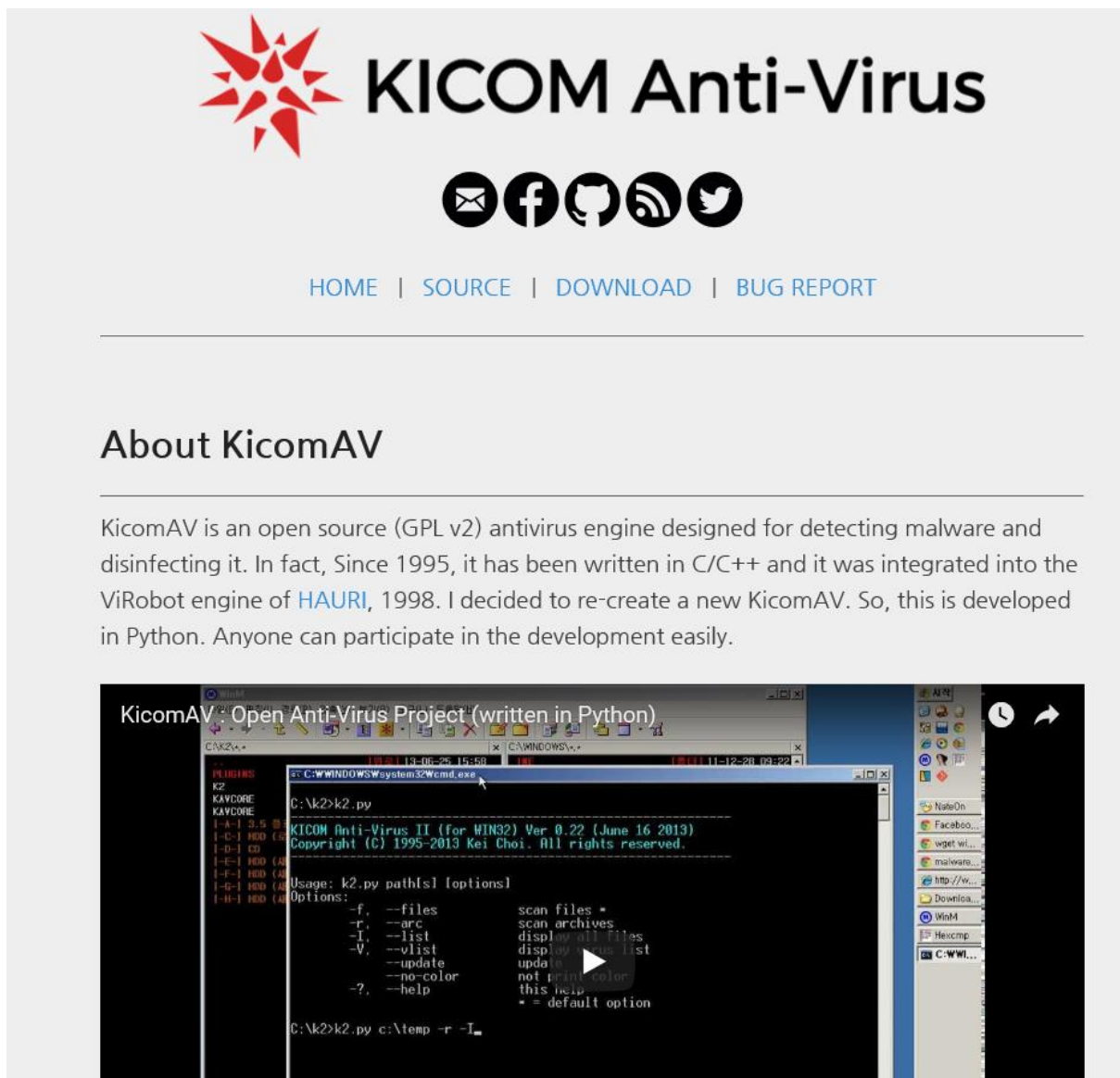


그림 2-1 키콤백신 홈페이지 메인 화면

## 2.2 키콤백신 설치 방법

키콤백신은 현재 0.28버전까지 업데이트되어 공개되어 있다. 키콤백신 설치 방법은 다음과 같다. 키콤백신(<http://www.kicomav.com/>)사이트에 들어가 아래로 조금 내리면 그림 2-2와 같이 다운로드 링크가 보인다. 해당 링크를 클릭하면 kicomav-master.zip이라는 압축파일을 다운로드 받게 된다.

○ Download the latest release and unzip it.

그림 2-2 키콤백신 다운로드

압축을 풀고 들어가게 되면, 아래 그림 2-3과 같은 파일들이 보인다. 키콤백신 설치 후 압축을 풀었다면, 이제 키콤백신을 동작시키기 위한 몇가지 모듈을 설치해야 한다.

|              |                  |               |      |
|--------------|------------------|---------------|------|
| Engine       | 2017-10-10 오후... | 파일 폴더         |      |
| Tools        | 2017-10-10 오후... | 파일 폴더         |      |
| build.bat    | 2017-09-04 오전... | Windows 배치 파일 | 2KB  |
| build.sh     | 2017-09-04 오전... | SH 파일         | 2KB  |
| CHANGELOG.md | 2017-09-04 오전... | MD 파일         | 2KB  |
| LICENSE      | 2017-09-04 오전... | 파일            | 18KB |
| README.md    | 2017-09-04 오전... | MD 파일         | 7KB  |

그림 2-3 키콤백신 압축 해제

키콤백신은 파이썬2.7로 만들어졌으며, Pylzma와 yara 모듈을 사용한다. 키콤백신을 구동시키기 위해서는 아래 3가지를 설치해야 한다. 파이썬은 아래 링크를 클릭하여 설치하면 되며, Pylzma 및 yara는 파이썬의 pip 명령어를 통해 설치하면 된다.

1. 파이썬 2.7 (<https://www.python.org/ftp/python/2.7.14/python-2.7.14.msi>)
2. Pylzma (<http://www.lfd.uci.edu/~gohlke/pythonlibs/#pylzma>)
3. yara (<https://pypi.python.org/pypi/yara-python>)

ex) pip install pylzma-0.4.9-cp27-cp27m-win32.whl

위 과정을 모두 거쳤다면 윈도우상에서 KICOM AV를 사용하기위한 마지막 절차로 빌드과정을 거쳐야 한다. 빌드 과정을 거치게 되면 다음과 같은 화면이 출력된다. (그림 2-4) 해당 과정까지 모두 거쳤다면 키콤백신을 사용할 준비를 모두 마친 것이다.

```

C:\Users\%[redacted]\kicomav-master\kicomav-master>build.bat build
-----
KICOM Anti-Virus II (for WIN32) Build Tool Ver 0.11
Copyright (C) 1995-2017 Kei Choi. All rights reserved.
-----
[+] Delete all files in Release

[*] Engine file copy to the Release folder...
[*] Make key : key.pkr, key.skr
[*] Build Engine files...
Success : kicom.lst      -> kicom.kmd
Success : alz.py        -> alz.kmd
Success : attach.py     -> attach.kmd
Success : cab.py        -> cab.kmd
Success : cryptolib.py  -> cryptolib.kmd
Success : dummy.py      -> dummy.kmd
Success : eicar.py      -> eicar.kmd
Success : elf.py        -> elf.kmd
Success : emailware.py  -> emailware.kmd
Success : html.py       -> html.kmd
Success : hwp.py        -> hwp.kmd
Success : kavutil.py    -> kavutil.kmd
Success : kernel.py     -> kernel.kmd
Success : macro.py      -> macro.kmd
Success : nsis.py       -> nsis.kmd
Success : ole.py        -> ole.kmd
Success : olenative.py  -> olenative.kmd
Success : pdf.py        -> pdf.kmd
Success : pe.py         -> pe.kmd
Success : rtf.py        -> rtf.kmd
Success : script.py     -> script.kmd
Success : unpack.py     -> unpack.kmd
Success : upx.py        -> upx.kmd
Success : yaraex.py     -> yaraex.kmd
Success : zip.py        -> zip.kmd
Success : __init__.py   -> __init__.kmd
[*] Build Success

```

그림 2-4 키콤백신 빌드

## 2.3 키콤백신 사용법

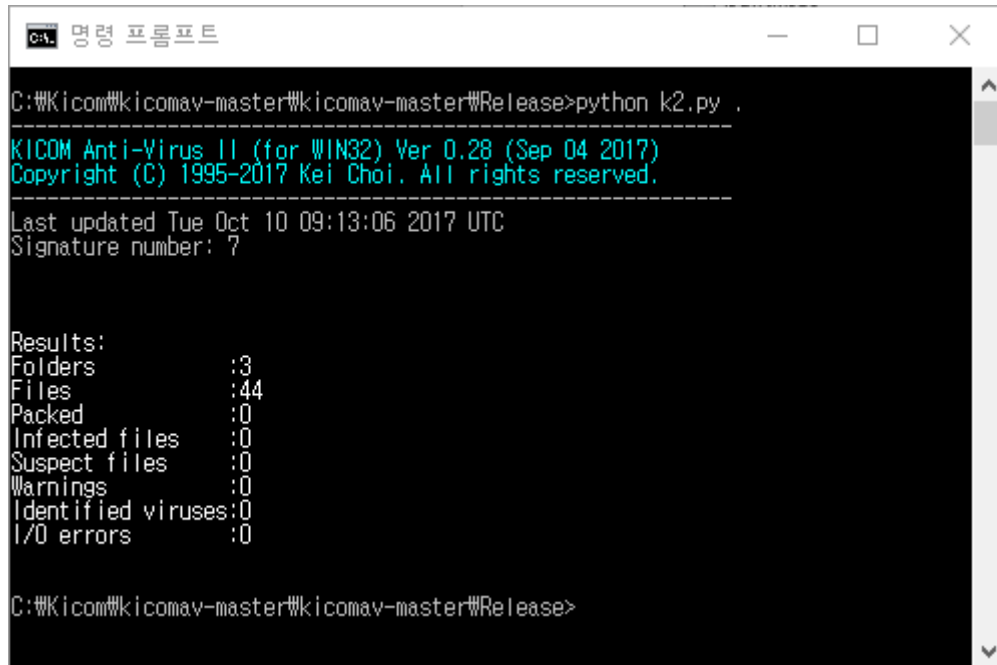
### 2.3.1 키콤백신 검사

키콤백신은 현재 커맨드라인 버전으로만 개발되어 있다. 그렇기에 명령 프롬프트를 이용해 동작 시켜야 한다. 바로 이전에 빌드 과정을 거친 후 다시 키콤백신 폴더로 가보면 Release라는 폴더가 있는 것을 확인할 수 있다. (그림 2-5)

|              |                  |               |      |
|--------------|------------------|---------------|------|
| Engine       | 2017-10-10 오후... | 파일 폴더         |      |
| Release      | 2017-10-10 오후... | 파일 폴더         |      |
| Tools        | 2017-10-10 오후... | 파일 폴더         |      |
| build.bat    | 2017-09-04 오전... | Windows 배치 파일 | 2KB  |
| build.sh     | 2017-09-04 오전... | SH 파일         | 2KB  |
| CHANGELOG.md | 2017-09-04 오전... | MD 파일         | 2KB  |
| key.pkr      | 2017-10-10 오후... | PKR 파일        | 1KB  |
| key.skr      | 2017-10-10 오후... | SKR 파일        | 1KB  |
| LICENSE      | 2017-09-04 오전... | 파일            | 18KB |
| README.md    | 2017-09-04 오전... | MD 파일         | 7KB  |

그림 2-5 빌드 후 키콤백신 폴더

Release폴더에 들어가면 k2.py보게 되는데 이 파일이 백신을 구동시키는 파일이다. 백신을 실행시키는 방법은 “python k2.py [path] [options]”이다. 간단한 악성코드 검사를 위해 아래 그림 2-6과 같이 “python k2.py .” 를 실행하면, 현재 폴더를 검사하게 된다.



```
C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py .

-----
KICOM Anti-Virus II (for WIN32) Ver 0.28 (Sep 04 2017)
Copyright (C) 1995-2017 Kei Choi. All rights reserved.
-----

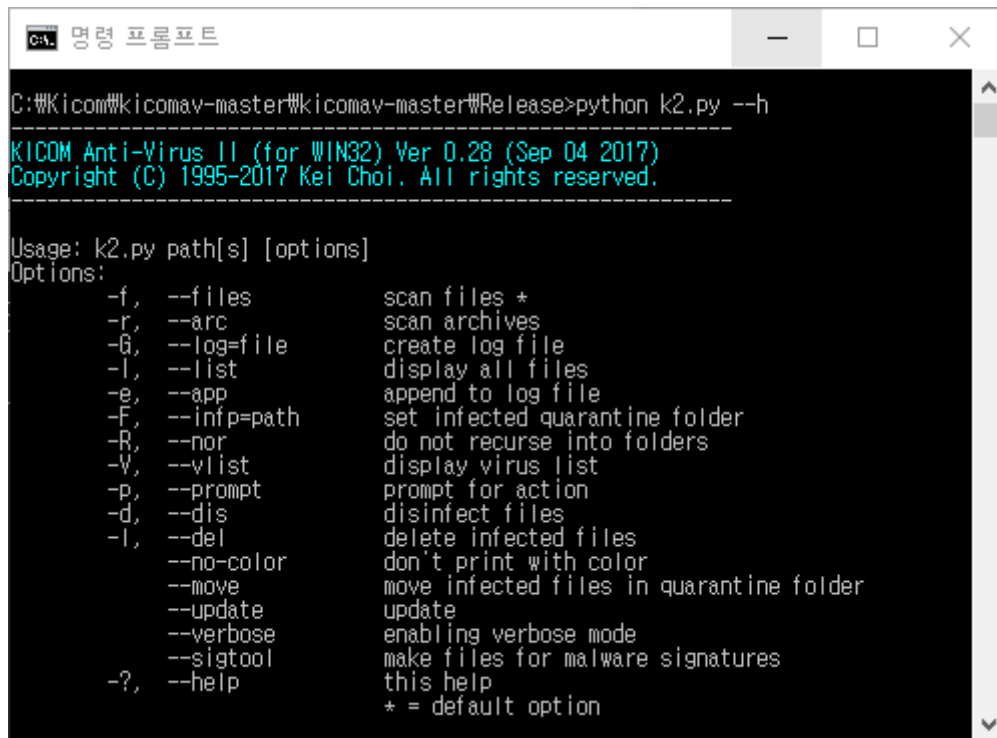
Last updated Tue Oct 10 09:13:06 2017 UTC
Signature number: 7

Results:
Folders      :3
Files       :44
Packed      :0
Infected files :0
Suspect files :0
Warnings    :0
Identified viruses:0
I/O errors  :0

C:\Kicom\kicomav-master\kicomav-master\Release>
```

그림 2-6 k2.py 실행

다음으로 키콤백신에서 사용 가능한 옵션들은 아래 그림 2-7과 같다.



```
C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py --h
-----
KICOM Anti-Virus II (for WIN32) Ver 0.28 (Sep 04 2017)
Copyright (C) 1995-2017 Kei Choi. All rights reserved.
-----

Usage: k2.py path[s] [options]
Options:
  -f, --files          scan files *
  -r, --arc            scan archives
  -l, --log=file       create log file
  -l, --list           display all files
  -e, --app            append to log file
  -F, --infp=path      set infected quarantine folder
  -R, --nor            do not recurse into folders
  -V, --vlist          display virus list
  -p, --prompt         prompt for action
  -d, --dis            disinfect files
  -l, --del            delete infected files
  --no-color           don't print with color
  --move              move infected files in quarantine folder
  --update            update
  --verbose            enabling verbose mode
  --sigtool            make files for malware signatures
  -?, --help           this help
  * = default option
```

그림 2-7 k2.py 옵션 목록

키콤백신의 옵션은 악성코드 발견 시에만 검사 결과를 출력한다. 필자는 임의의 악성파일을 Release에 옮겨놓았다. 이제 해당 파일에 대한 검사를 실시 해보았다. 사용한 옵션은 다음과 같다.

- 모든 결과를 보고 싶을 경우 : -l 옵션
- 압축 파일 내부 검사를 하고 싶을 경우 : -r 옵션

**오류! 참조 원본을 찾을 수 없습니다.**은 압축 파일에 숨은 악성코드 검사를 실시한 것이다. 검사 결과 virus.zip 이라는 폴더가 있고 그안에 00e80...~ 라는 파일이 있고, eb3a6..~ 라는 파일이 Attached 되있는 것을 알 수 있다. 이렇게 키콤백신을 이용해 압축파일 내부까지 확인 할 수 있다. 또한 키콤 백신의 또 다른 기능은 한글 파일 같은 문서에 숨겨져 있는 파일까지 검사가 가능하다.



```
명령 프롬프트
C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py virus.zip -r -l
-----
KICOM Anti-Virus II (for WIN32) Ver 0.28 (Sep 04 2017)
Copyright (C) 1995-2017 Kei Choi. All rights reserved.
-----
Last updated Tue Oct 10 09:13:06 2017 UTC
Signature number: 7

C:\Kicom\kicomav-master\kicomav-master\Release\virus.zip ok
C:\Kicom\kicomav-master\kicomav-master\mas ... (00e80edeb3a6f51fc53e800dd8110dff) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... eb3a6f51fc53e800dd8110dff/Attached) ok

Results:
Folders      :0
Files        :3
Packed       :1
Infected files :0
Suspect files :0
Warnings     :0
Identified viruses:0
I/O errors   :0

C:\Kicom\kicomav-master\kicomav-master\Release>
```

그림 2-8 압축 파일에 숨은 악성코드 검사

아래 그림은 바로 위에서 설명한 한글 파일내에 virus.zip이라는 파일이 숨겨져 있을 경우의 검사 결과이다. 위에서 검사한 virus.zip 파일을 그림 2-9와 같이 word문서에 숨긴 후 검사를 실시한 결과 그림 2-10에서 처럼 검사 결과가 나오는 것을 확인할 수 있다. 검사 결과를 보면 특이점을 발견할 수 있는데, 타 백신과 달리 키콤 백신은 문서파일 또한 압축파일로 생각하기 때문에 상세하게 검사를 하는 것을 확인할 수 있다.

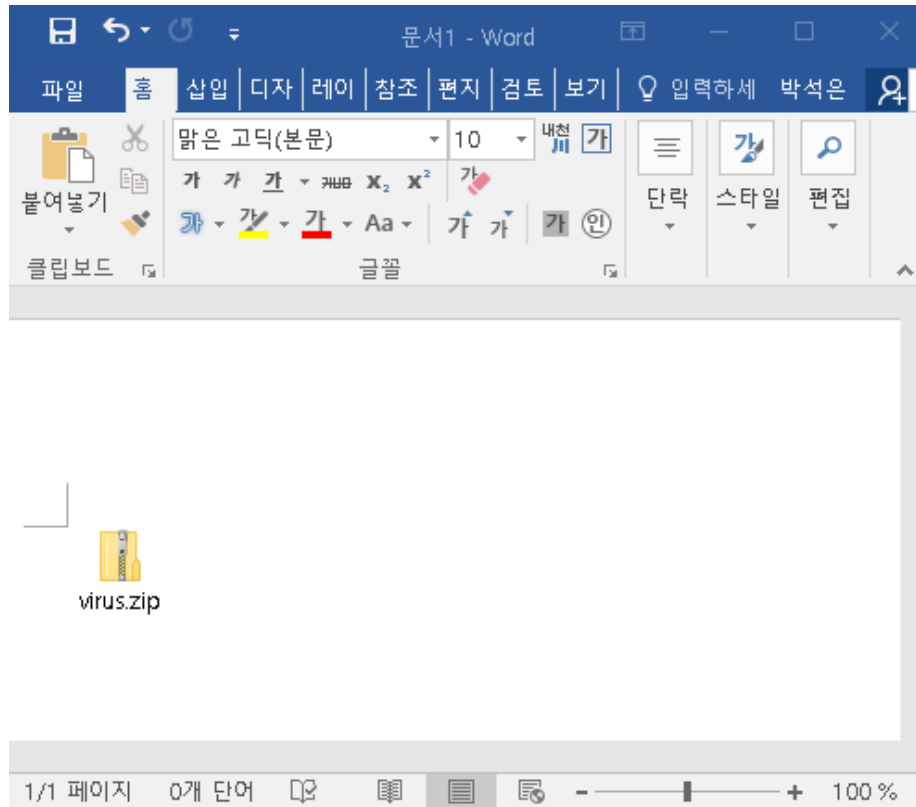


그림 2-9 한글 파일내 숨겨진 악성파일

```

C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py 문서1.docx -r -l
-----
KICOM Anti-Virus II (for WIN32) Ver 0.28 (Sep 04 2017)
Copyright (C) 1995-2017 Kei Choi. All rights reserved.
-----
Last updated Tue Oct 10 09:13:06 2017 UTC
Signature number: ?

C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py 문서1.docx ok
C:\Kicom\kicomav-master\kicomav-master\mas ... se\문서1.docx ([Content_Types].xml) ok
C:\Kicom\kicomav-master\kicomav-master\Release>python k2.py 문서1.docx (_rels/.rels) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... docx (word/_rels/document.xml.rels) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... ease\문서1.docx (word/document.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... \문서1.docx (word/media/image1.emf) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... cx (word/embeddings/oleObject1.bin) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... embeddings/oleObject1.bin/CompObj) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... /embeddings/oleObject1.bin/4EPRINT) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... embeddings/oleObject1.bin/40bjInfo) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... eb3a6f51fc53e800dd8110dff/Attached) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... \문서1.docx (word/theme/theme1.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... ease\문서1.docx (word/settings.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... e\문서1.docx (word/webSettings.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... ease\문서1.docx (docProps/core.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... ease\문서1.docx (word/styles.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... ase\문서1.docx (word/fontTable.xml) ok
C:\Kicom\kicomav-master\kicomav-master\mas ... lease\문서1.docx (docProps/app.xml) ok

Results:
Folders      :0
Files        :22
Packed       :2
Infected files :0
Suspect files :0
Warnings     :0
Identified viruses:0
I/O errors   :0

```

그림 2-10 한글 파일내 악성파일 검사

## 2.3.2 키콤백신 패턴 추가

다음은 키콤백신에 악성코드 패턴을 추가하는 방법이다. 가장 먼저 악성코드의 이름을 하나로 통일하기 위해 모든 파일명을 SHA256 형태의 이름으로 변경하는 작업을 실시한다. 해당 작업을 위해 사용하는 파일은 xsha.py라는 파일이다. Xsha.py 사용법은 다음과 같다.

- xsha.py [src 폴더명] [target 폴더명]

위 명령어에 대한 설명을 하자면, src폴더에 존재하는 악성코드를 target 폴더명으로 이름을 변경하여 복사한다. 그림 2-11은 malware\_md5폴더를 1폴더로 이름을 변경해서 복사하는 모습이다.

```

C:\kicomav\sample>python xsha.py malware_md5 1
c8fcd0de624d15d7a4dfe02930eabc7650124c04d6085a65a8660b18eeb794a60
368db5f35043ed13f2b5b015ed1636b94798e0691bc34957b8b09dd75fa67e55
d36a0aec1aaa7a8a1639e4c46d8775536cf0199d1506835369fe872c9cc38913
045b52901994cae1f75bbcb6bf00f5894e659ded9cee12dc25ea5f29c82e481a
6052800081a686e2620880c8e3f49c7aab8210ac34db58fe8f7192a6965d2812
1a8a669b9a21dd065f1a4e6ef19bf38c649f012e5ba5667dcea844ce02dc695
f7a2199cfef18b4367b524dff527a51435079b567e3d6e2d552851e30210c9f9
1f82a962f438b4c1a1fe19c3d532b609c3e9d54efe35536477f1032b50d45e7f
53ddb1b7ca9599e5ae9f4182b95b46687aad0c933c5d15970f7b4f9f7d4e4a0
b4d96fca9262cddf3765b6e343dd1ba3bc23b17ca3857fbf82ff2e4d705eb1ef
4ad7dbee63bdb1d246a9352aafb5a94c76fec57e3671dbcd744c6be3ea9feae
03307bb9e3f5204ec97435e5bd2678e2c2465125cc1247c80f62af99ac6b38fe
a1e7e0ca59f3e91a682e20ac4c4b3134821e808863aa2fe15a0297ce4007b536
c5e232802e7783a0afae9c71fe33e32baf12af75c7b858fd38a74dee2ac39bb
7a9d53ed4d24997d66b3377b5e25ee3cde0114d4bdb66afe2dca2e4a4ebfaa80
b6103d8a1b270319535b10001e34e739fbf436ef2317227c6a40911b7c4670a3
e3dbcf5455fda34f842ee361c8871eb13dffdc5ff84076b4c2c0d01138d9116f
3df29c8fa724c75f4892126d60565ba527008cf147cf08e4660d55a9858dc4df
b5cc40ee5f4b6f2a958c9b029ffda14d133cda8646f28d45dbd9afedd2f6df43
b612b4d31b700f652fe2040725ff0c87de1d3b7f2e81687a7f672ee1afdd191e

```

그림 2-11 xsha.py

내 PC > Windows (C:) > kicomav > sample > 1

| 이름                                   | 수정된 날짜           | 유형 | 크기       |
|--------------------------------------|------------------|----|----------|
| 1a8a669b9a21dd065f1a4e6ef19bf38c...  | 2017-10-13 오후... | 파일 | 728KB    |
| 1be910beb719837667af466031d729e...   | 2017-10-13 오후... | 파일 | 165KB    |
| 1f82a962f438b4c1a1fe19c3d532b609c... | 2017-10-13 오후... | 파일 | 1,087KB  |
| 2ffb1994c9b4ff4e1dfab3b80011df752... | 2017-10-13 오후... | 파일 | 15,394KB |
| 3d6e3da40ffeb71e2c5ce05c955d9bc0...  | 2017-10-13 오후... | 파일 | 760KB    |
| 3d49e07cca34e0b6bab3b2010028949...   | 2017-10-13 오후... | 파일 | 269KB    |
| 3df29c8fa724c75f4892126d60565ba5...  | 2017-10-13 오후... | 파일 | 1,812KB  |
| 4ad7dbee63bdb1d246a9352aafb5a94c...  | 2017-10-13 오후... | 파일 | 10,823KB |
| 4bd4dc9ff544ea050f710748f5bd36df...  | 2017-10-13 오후... | 파일 | 183KB    |
| 4ddefce0173cd320d0c903774cc3fe0bb... | 2017-10-13 오후... | 파일 | 2,607KB  |
| 6b57dc8997c19a7e475acf99938447e4...  | 2017-10-13 오후... | 파일 | 3,545KB  |
| 6b385df18da9a17892d8133a0da5e6d5...  | 2017-10-13 오후... | 파일 | 409KB    |
| 6ca2169bc3a368cc1ddd5f54c7c8bf59d... | 2017-10-13 오후... | 파일 | 3,987KB  |
| 7a9d53ed4d24997d66b3377b5e25ee3...   | 2017-10-13 오후... | 파일 | 23KB     |
| 7bf6a681ba94215a08a985e77ccfb30d...  | 2017-10-13 오후... | 파일 | 6,686KB  |
| 7dbe42c091bd616fdc61a14fcd23bc83...  | 2017-10-13 오후... | 파일 | 1,012KB  |

그림 2-12 1폴더로 복사된 모습

다음은 fileformat.exe를 이용해 1폴더에 있는 파일들을 파일 포맷별로 분류하여 각 포맷에 맞는 폴더로 복사한다.

```

C:\kicomav\sample>fileformat.exe 1
1#\03307bb9e3f5204ec97435e5bd2678e2c2465125cc1247c80f62af99ac6b38fe : UPX_Attached_PE
1#\045b52901994cae1f75bbcb6bf00f5894e659ded9cee12dc25ea5f29c82e481a : UPX_Attached_PE
1#\1071a2b09ae6d4cacdd70bf62e9306a94b8a825831ff35fa729504b06ba4f69f : BobSoftMiniDelphi_PE

1#\1127a71586ff24f2f2c4a626bb0abf8b8264627b9eadbeb0e4590e3e77acec97 : PE
1#\12576c07bf03dd8548974ef71d1a74a78bf1e6745ec398ed4f533abc5151ebd : Attached_PE
1#\13819559f4333687826fd115934424dd4b22327b072bba0d3c4c235d1fd382be : Attached_PE
1#\13b4a02e207e59b68aac3a3e01031cc75009e2192fe0457d0e49622c6277284 : UPX_Attached_PE
1#\17f371c2cc72dd333e49b6532e2b55b9cf7e9f055835e7e7b4ac969b64183fee : UPX_PE
1#\190526c3b1e06c3b4661556c5164f1c4db8f2bfeefa42d384d1ecadb195beae3 : Attached_PE
1#\1a8a669b9a21dd065f1a4e6ef19bfb38c649f012e5ba5667dcea844ce02dc695 : Attached_PE
1#\1be910beb719837667af466031d7d29ee4798c92eac67e8af14c36176a73037d : PE
1#\1f82a962f438b4c1a1fe19c3d532b609c3e9d54efe35536477f1032b50d45e7f : Attached_PE
1#\24333645a04db5c98c17ed875b983fb6734de339581682c79cdd000146b6d11e : Attached_PE

```

그림 2-13 fileformat.exe

다음은 분류된 파일 중 pe파일을 분석하여 악성파일 패턴을 등록해야 한다. 키콤백신의 옵션 중 -verbose를 이용해 주요 정보를 확인해야 한다. 아래 그림 2-14를 보면 pe파일의 주요 정보가 보인다. 분석 결과 악성파일로 판단될 경우 검사할 섹션의 크기와, 그 섹션의 md5를 추가해줘야 한다. 추가하는 방법은 다음과 같다. emalware.mdb 파일에 패턴을 작성하면 되는데, 그림 2-15처럼 섹션의 크기:md5:악성코드 이름 #주석문을 작성한 후 저장하면 된다. 만약 계속해서 패턴을 추가하고자 할 때는 sort를 해줘야 한다. 이유는 악성코드 패턴의 파편화를 막기 위해서이다. (키콤백신의 속도가 빨라진다.)

마지막으로 패턴을 빌드하는 방법이다. Sigtool\_md5.py를 이용해 emalware.mdb파일을 빌드하면 된다. 패턴 빌드를 하면 그림 2-16과 같이 4개의 파일이 생긴다.(emalware.c01, i01, s01, n01) 생성된 파일을 키콤백신 plugins 폴더로 이동하면 키콤백신이 인식을 한다. 검사 결과는 그림 2-17을 통해 확인 가능하다.

```

C:\w\kicomav\source\Engine>python k2.py 1be910beb719837667af466031d7d29ee4798c92eac67e8af14c36176a73037d --verbose
KICOM Anti-Virus II (for WIN32) Ver 0.28 (Sep 04 2017) Copyright (C) 1995-2017
Kei Choi. All rights reserved.
Last updated Fri Oct 13 08:21:08 2017 UTC
Signature number: 9

[*] Engine
[-] Engine : pe.kmd
[-] File name : 1be910beb719837667af46 ... c67e8af14c36176a73037d
[-] MD5 : 6956e414d03d460eea465cb0b64719e6

[*] PE
[-] EntryPoint : 00001456
[-] EntryPoint (Section): 0

[*] Section Header
Name VOFF VSIZE FOFF FSIZE EXEC
-----
.text 00001000 000021AA 00000400 00002200 True
.rdata 00004000 00000F4A 00002600 00001000 False
.data 00005000 000025AB 00003600 00002560 False
.reloc 0000B000 000005CC 000028C0 00000600 False

[*] Section MD5
Name FSIZE MD5
-----
.text 8704 dbb3a06f6a52345c8bb2acf249ad4db3
.rdata 4096 d3c784c1d4db42d20e0304152c41410b
.data 153088 1f43ae87ae8e21b7c98bcf2d39758b2c
.reloc 1536 e81f92c8705655865a53347aa511137f

[*] Entry Point (Raw)
00000850 : 55 8b ec 56 68 04 01 00 00 68 U..Vh...h
00000860 : 08 a4 42 00 33 f6 56 ff 15 90 40 40 00 6a 01 ff ..B.3.V...@.j..
00000870 : 15 ac 40 40 00 e8 37 0c 00 00 e8 79 09 00 00 a3 ..@...7...y...
00000880 : 0c a5 42 00 e8 a3 11 00 00 e8 34 ff ff ff e8 6d ..B.....4....m
00000890 : fb ff ff 85 c0 75 55 e8 5a fc ff ff 39 35 5c a5 .....uU.Z...95w.
000008A0 : 42 00 74 2e e8 0b fe ff ff 85 c0 75 25 6a 14 58 B.t.....uXj.X
000008B0 : e8 21 1c 00 00 8b c4 3b c6 74 11 68 84 00 00 00 .!.....;t.h....
d 40 00 e8 91 14 00 00 50 e8 e4 09 j..0]@.....P...
000008D0 : 00 00 e8 19 fd ff .....
000008C0 : 6a 11 ba 30 5

```

그림 2-14 pe파일 분석

```

emalware.mdb - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
8704:dbb3a06f6a52345c8bb2acf249ad4db3:Trojan.Win32.Shifu # PE

```

그림 2-15 emalware.mdb에 패턴 추가

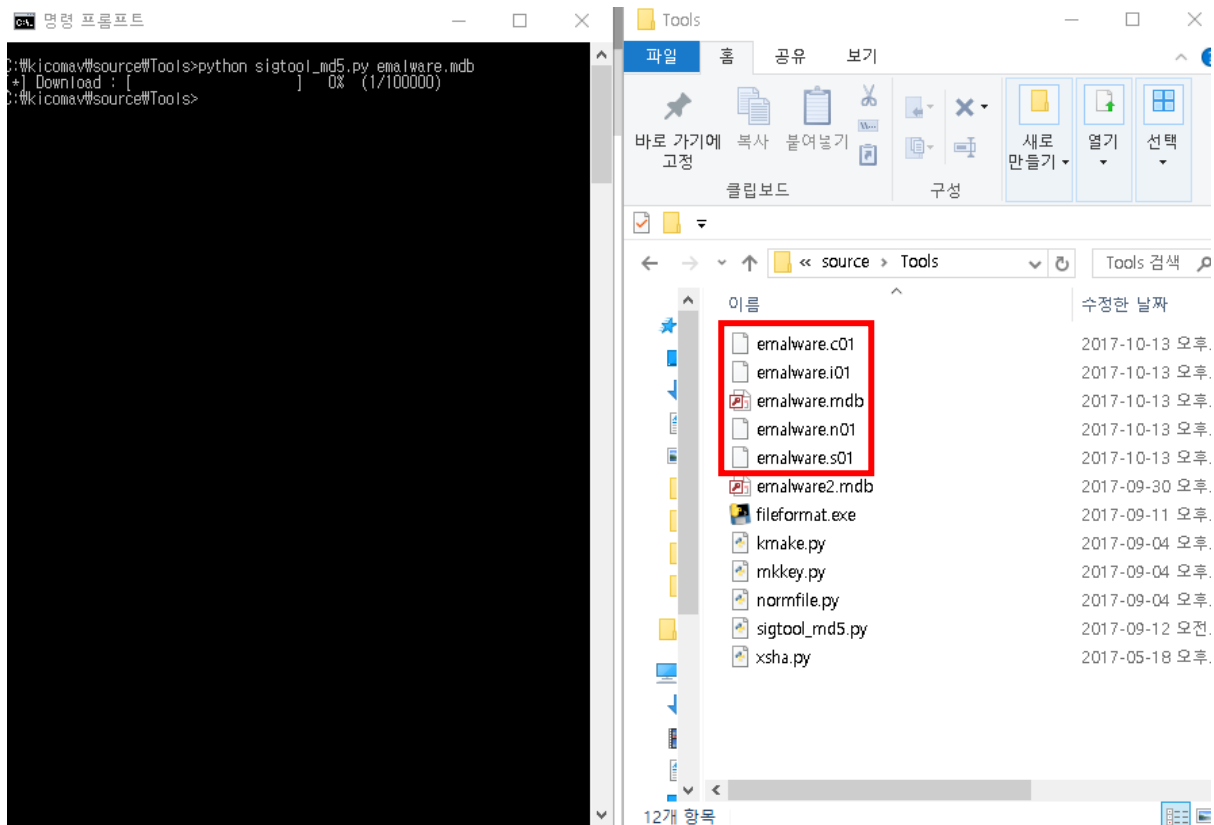


그림 2-16 패턴 빌드



그림 2-17 검사 결과

### 3 참고 자료

---

1. <http://www.kicomav.com/>
2. 키콤백신 DB 과정.pdf
3. <https://github.com/hanul93/kicomav>