

악성코드 탐지, 암호화 및 패키징

테스트 결과 보고서

문서번호 : TMD-001

VER1.0

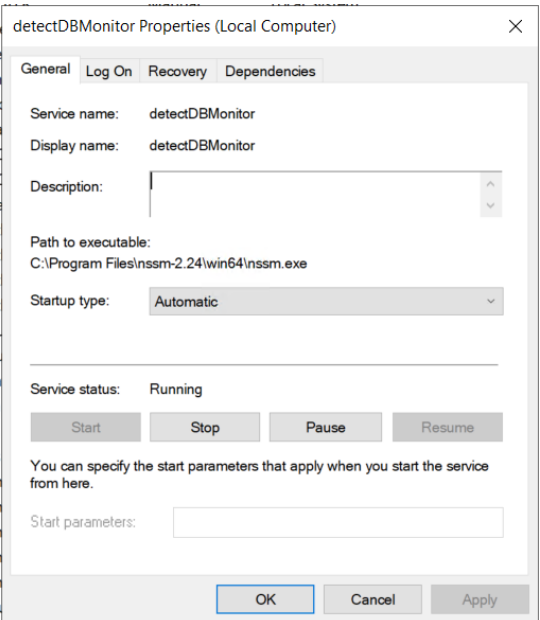
프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

변경 이력서

변경일자	적용범위	버전	변경내용	작성자
2024.10.01	VTAPI MODULE	1.0	VTAPI PROCESS_NEW_FILE MODULE 최초 작성	우건희
2024.10.01	VTAPI MODULE	1.0	VTAPI PROCESS_HASH MODULE 최초 작성	우건희

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

1. 제목 VTAPI process_new_file 테스트

시스템 명	VTAPI MODULE	작성일	2024-10-01
테스트 대상	VTAPI process_new_file	작성자	우건희
테스트 책임자	우건희	테스트 완료일	2024-10-01
번호	테스트케이스/예상결과	개발	검증
1	MongoDB의 vsapi DB의 files collection 모니터링	O	<div>1. files collection 모니터링</div> 
2	처리한 해시값 저장	O	
3	처리된 해시값 불러오기	O	
4	새로운 파일 업로드 됐을때 파일 내용 도큐먼트 추출	O	
5	Virustotal API 해시 검색	O	
6	Virustotal API upload url 생성	O	
7	Virustotal API file upload	O	
8	5번 기능 후 나온 JSON 파일 규격에 맞게 변환	O	
9	JSON 파일 vsapi DB의 info collection에 업로드	O	
10	업로드 된 파일의 해시 값으로 vsapi DB의 info collection에 검색	O	
11	7번 이후 5번 기능을 반복적으로 수행	O	
12	1번 기능 반복 수행	O	

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

시스템 명	VTAPI MODULE	작성일	2024-10-01
테스트 대상	VTAPI process_new_file	작성자	우건희
테스트 책임자	우건희	테스트 완료일	2024-10-01

검증

2. 처리한 해시 기록 json

```

processed_hashes.json X
C: > Users > SEOLT > Documents > Pre-Vision > 2. MODULE > VirusTotal API > processed_hashes.json >
1  [ "dd4bd9f1a4a23f3d04bee332b1c5a124", "2bffa08ec892c53c4ce6e36709b7fd2cf",
    "be1a4eb4abfa66c168b8b947afbfa6ca", "6daeccad61a0c7a6343226aebc2f5991",
    "a95aa166567f9946940a6015d9c5ebd9", "e63943693d426b7360277c344d887756",
    "19c4c9a7719c34a8ec0bdfdc687e64ea", "3977f99d25b05899eac55bcc92d40cbf",
    "d8c1e3d95b1091fe2736ab13b6a1f551", "9fefdc75634dacd9a1cbf4b8fc833d0f",
    "4bfebdcf04ca30126f19f5c99edd0a9c", "f5b00636853231785277e324d4dc8403",
    "2d62bc45fdb61f802129df3fd20c0b47", "f7f4bfc8d83d9987631beb58d27d1d30e",
    "4ed09e048949521321f0369d2e908971", "25e1487c5e0c2104411e5685cebcef84",
    "d64bcc000feb58a339000dc069a02efa", "80a20c307904ed98007d5c6716839ab5",
    "5b1b10d16308f61ac598822de806e827", "00c8b60cc6c51b7c4c93405ebf9237ad",
    "6c951396c8a600f3954f02724204e6ce", "1135e17339577c5144553ae78797789b",
    "3a81013ee762a47909c88c078cc1747c", "16618e636158684100bc4765ab67e0e4",
    "438c7a93f853a732c1934512f4ae125d", "6e28eac6bad78b5757c5b57edbc379b2",
    "a64e374945845aaec6ad063e8be450db", "4d64dc26add3df7d8fbe10f48e8eda25",
    "c14bc74c048972b3eed2073ae3cdc8c1", "4b90b9879e014140ac5aa1f75fa616c6",
    "3ccfea6abb70ee274c1389946793ade4", "821e219f3bcece9cf0a01f414a86fce4",
    "551977703bd64d8f12e66626ae00ffd5", "3b6501feef6196f24163313a9f27dbfd",
    "8ae4605ae214af3ba375ad58263ca707", "34c1dcf5ae13cf8bb19dd4238d1a69eb",
    "8e41d2107579afb2911dccffeab97f1c", "b14ef85a60ac71c669cc960bdf580144",
    "9f88234068d7abad65979eb1df63efb5", "4d86c48b5d9f043b6e0b1ef3d2c7bdd4",
    "836818e56aec7caf282287d9cac4663b", "c7e47553b94c0d18ecf9e03b5ffec68b",
    "0e3dacf8e6b3cafd219a55bce552b66", "0b182aef2380479423dc14220756aa7a",
    "7f0bde5df6ebbdceeda83413fc738320", "365c7243259666885e6d322d0527786a",
  ]

```

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

3. 데이터 변환 및 DB 업로드

```

2024-10-01 14:51:37,210 - INFO - de9fb2ae1eb3ed922602b1c1667553ed 데이터 변환 중...
2024-10-01 14:51:37,215 - INFO - de9fb2ae1eb3ed922602b1c1667553ed MongoDB에 저장 완료.
2024-10-01 14:51:37,216 - INFO - de9fb2ae1eb3ed922602b1c1667553ed 처리된 해시 기록에 추가.
2024-10-01 14:51:38,266 - INFO - 922797db0e0e3ef07b7d56948c7c9df9 데이터 변환 중...
2024-10-01 14:51:38,271 - INFO - 922797db0e0e3ef07b7d56948c7c9df9 MongoDB에 저장 완료.
2024-10-01 14:51:38,272 - INFO - 922797db0e0e3ef07b7d56948c7c9df9 처리된 해시 기록에 추가.

```

4. DB 파일 업로드 감시 및 저장

```

2024-09-12 00:02:06,096 - INFO - 파일 업로드 감시 시작
2024-09-12 00:03:44,084 - INFO - 새로운 파일 업로드 감지: 9f1d169fa26cf0d709b414245e69eaeef
2024-09-12 00:03:44,722 - INFO - 9f1d169fa26cf0d709b414245e69eaeef VirusTotal에 없음, 파일 업로드 중...
2024-09-12 00:04:49,552 - INFO - 9f1d169fa26cf0d709b414245e69eaeef 데이터 변환 중...
2024-09-12 00:04:49,559 - INFO - 9f1d169fa26cf0d709b414245e69eaeef 분석 및 행동 분석 완료 후 MongoDB에 저장.

```

5. 새로운 파일이 Virustotal에 등록되어 있는 파일일 경우(해시 값으로 VTAPI 검색이 가능한 경우)

```

2024-09-12 00:01:41,307 - INFO - 파일 업로드 감시 시작
2024-09-12 00:02:01,362 - INFO - 새로운 파일 업로드 감지: 14f22266cceb3a4d1a554471dc2be3c6
2024-09-12 00:02:02,007 - INFO - 14f22266cceb3a4d1a554471dc2be3c6 이미 VirusTotal에 존재함. 데이터 가져오는 중...
2024-09-12 00:02:03,107 - INFO - 14f22266cceb3a4d1a554471dc2be3c6 데이터 변환 중...
2024-09-12 00:02:03,118 - INFO - 14f22266cceb3a4d1a554471dc2be3c6 분석 및 행동 분석 완료 후 MongoDB에 저장.

```

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

6. 새로운 파일이 Virustotal에 등록되지 않은 파일일 경우

```
2024-09-12 00:02:06,096 - INFO - 파일 업로드 감시 시작
2024-09-12 00:03:44,084 - INFO - 새로운 파일 업로드 감지: 9f1d169fa26cf0d709b414245e69eaeef
2024-09-12 00:03:44,722 - INFO - 9f1d169fa26cf0d709b414245e69eaeef VirusTotal에 없음, 파일 업로드 중...|
2024-09-12 00:04:49,552 - INFO - 9f1d169fa26cf0d709b414245e69eaeef 데이터 변환 중...
2024-09-12 00:04:49,559 - INFO - 9f1d169fa26cf0d709b414245e69eaeef 분석 및 행동 분석 완료 후 MongoDB에 저장.
```

7. 새로운 파일이 vsapi DB의 info 정보가 있는경우

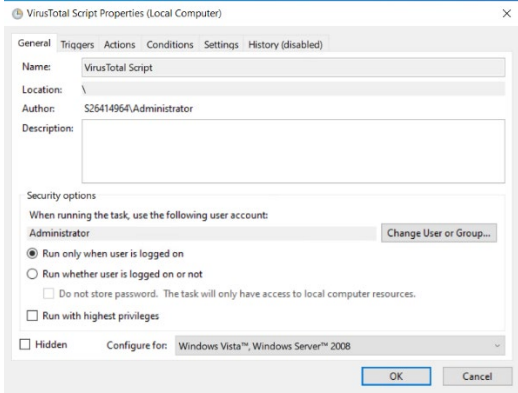
```
2024-09-24 19:49:13,624 - INFO - 파일 업로드 감시 시작
2024-09-24 20:12:09,468 - INFO - 새로운 파일 업로드 감지: 9f1d169fa26cf0d709b414245e69eaeef
2024-09-24 20:12:09,473 - INFO - 9f1d169fa26cf0d709b414245e69eaeef 이미 DB에 존재함. 처리 종료.
```

8. VTAPI 해시 검색을 통해 데이터값 추출 후 format에 맞게 데이터 변환

```
2024-10-01 14:51:40,491 - INFO - Behavior 데이터가 없음
2024-10-01 14:51:41,523 - INFO - 데이터 변환 시작
2024-10-01 14:51:41,524 - INFO - Behavior 데이터가 없음
2024-10-01 14:51:42,833 - INFO - 데이터 변환 시작
2024-10-01 14:51:42,834 - INFO - 데이터 변환 완료
2024-10-01 14:51:43,863 - INFO - 데이터 변환 시작
2024-10-01 14:51:43,863 - INFO - Behavior 데이터가 없음
2024-10-01 14:51:44,925 - INFO - 데이터 변환 시작
2024-10-01 14:51:44,925 - INFO - 데이터 변환 완료
2024-10-01 14:51:47,524 - INFO - 데이터 변환 시작
2024-10-01 14:51:47,524 - INFO - 데이터 변환 완료
2024-10-01 14:51:48,738 - INFO - 데이터 변환 시작
2024-10-01 14:51:48,738 - INFO - 데이터 변환 완료
```

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

2. 제목 VTAPI process_hash 테스트

시스템 명	VTAPI MODULE	작성일	2024-10-01
테스트 대상	VTAPI process_hash	작성자	우건희
테스트 책임자	우건희	테스트 완료일	2024-10-01
번호	테스트케이스/예상결과	개발	검증
1	Dataset.csv에서 MD5 해시값 추출	○	<p>1. dataset에서 해시 로드 후 처리된 해시 저장</p> <p>2024-10-01 14:50:27,017 - INFO - CSV 파일 C:\VTAPImodules\dataset.csv에서 해시 값 로드 성공 2024-10-01 14:50:28,550 - INFO - 처리된 해시 기록 저장 성공 2024-10-01 14:50:30,604 - INFO - 처리된 해시 기록 저장 성공 2024-10-01 14:50:31,597 - INFO - 처리된 해시 기록 저장 성공 2024-10-01 14:50:34,059 - INFO - 처리된 해시 기록 저장 성공 2024-10-01 14:50:35,658 - INFO - 처리된 해시 기록 저장 성공 2024-10-01 14:50:37,403 - INFO - 처리된 해시 기록 저장 성공</p> <p>2. 매달 3일동안 반복 실행</p> 
2	처리된 해시값 제외	○	
3	VTAPI를 통해 해시 검색	○	
4	VTAPI 검색으로 나온 결과값 변환	○	
5	변환된 결과값 vsapi DB의 info collection에 저장	○	
6	매달 3일 동안 반복	○	
7	API 한계만큼 리미트 설정	○	

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우

3. 하루 사용량 처리 로직

```
# 설정
MAX_EXECUTIONS_PER_MINUTE = 2 # 분당 최대 2번 실행
MAX_EXECUTIONS_PER_DAY = 250 # 하루 최대 250번 실행

# 분당 5번 실행을 위한 제한 함수
def rate_limiter():
    time.sleep(30) # 30초마다 1번 실행 -> 분당 2번 실행 가능
    logger.info("Rate limiter: 30초 대기")

if __name__ == "__main__":
    logger.info("처리된 해시 로드 시작")

    # 처리된 해시 로드
    processed_hashes = load_processed_hashes()

    # 해시값 처리
    execution_count = 0
    hashes = read_hashes_from_csv()

    for hash_value in hashes:
        if execution_count >= MAX_EXECUTIONS_PER_DAY:
            logger.info("오늘의 최대 실행 횟수에 도달했습니다.")
            break

        if process_hash(hash_value, processed_hashes):
            execution_count += 1 # 실제로 처리된 경우에만 증가
```

프로젝트 명	Pre-vision	단 계	1
버 전	1.0	작성일	2024-10-01
작성자	우건희	검토자	김효진, 김선우