MongoDB VirustotalAPI 데이터베이스 구성

문서 번호 : MDB-001

1 files 컬렉션

업로드된 파일에 대한 메타데이터와 파일 데이터

필드	설명
signature_id	파일의 고유 서명 ID
filehash	MD5 해쉬 정보
filename	파일의 이름
file_data	파일의 전체 내용
upload_time	파일이 업로드된 시간
upload_ip	파일을 업로드한 사용자의 IP 주소

2 info 컬렉션

파일의 details 정보와 파일 behavior 정보

Details

Hash :

필드	설명
md5	파일의 MD5 해시 값
sha1	파일의 SHA1 해시 값
sha256	파일의 SHA256 해시 값
vhash	파일의 VHash 값
auth_hash	인증 해시 값
imphash	Import Hash 값
ssdeep	SSDEEP 해시 값
tlsh	TLSH 해시 값

file_info :

필드	설명
md5	파일의 MD5 해시 값
file_type	파일의 유형 (예: 실행 파일, 문서 파일 등)
magic	파일의 매직 넘버 또는 식별자
file_size	파일 크기 (바이트 단위)
PEID_packer	파일에 사용된 패커 정보
first_seen_time	파일이 처음 발견된 시간
name	파일의 이름

signature : 파일 서명 데이터를 저장, 파일이 디지털 서명되어 있거나 인증된 경우 그 정보를 저장

pe_info : PE(Portable Executable) 파일에 대한 정보 PE 파일은 주로 Windows 운영 체제에서 실행되는 파일, PE 구조와 관련된 추가 정보

dot_net_assembly : .NET 어셈블리 파일에 대한 정보를 저장 .NET 파일이 실행되는 동안 사용되는 메타데이터 및 코드 모듈 정보

behavior

mitre : MITRE ATT&CK 프레임워크에 기반한 공격 기법 분석 정보를 저장 파일의 악성 활동이 MITRE ATT&CK 의 어떤 공격 기법에 해당하는지에 대한 정보

Capabilities : 파일이 실행될 때 수행할 수 있는 기능에 대한 정보 (예 : 파일이 시스템 권한 상승, 키로깅, 백도어 생성 등의 악성 행동을 수행할 수 있는지에 대한 데이터)

tags : 분석된 파일의 행동에 따라 붙여진 태그를 저장 (예 : "ransomware", "spyware")

network_communications : 파일이 실행 중에 수행한 네트워크 통신에 대한 정보 HTTP 대화, IP 주소, 도메인, JA3 지문 등의 데이터를 저장

필드	설명
http_conversations	파일이 서버와 주고받은 HTTP 요청 및 응답 정보

ja3_digests	JA3 지문은 TLS 연결에서 클라이언트 측 정보를 해싱한 값, 특정 네트워크 패턴을 식별하는 데 사용
memory_pattern_domains	메모리에서 발견된 악성 도메인
memory_pattern_ips	메모리에서 발견된 IP 주소
memory_pattern_urls	메모리에서 발견된 URL 정보

file_system_actions : 파일이 시스템에서 실행되면서 수행한 파일 시스템 관련 동작

필드	**설명**
files_opened	파일이 열린 기록
files_written	파일이 작성된 기록
files_deleted	파일이 삭제된 기록
files_attribute_changed	파일 속성(예: 읽기 전용)이 변경된 기록
files_dropped	실행 도중 생성되거나 드롭된 파일에 대한 정보

registry_actions : 파일이 레지스트리와 관련하여 수행한 동작

필드	**설명**
registry_keys_opened	파일이 접근한 레지스트리 키
registry_keys_set	파일이 설정한 레지스트리 키
registry_keys_deleted	파일이 삭제한 레지스트리 키

process_and_service_actions : 프로세스 및 서비스 관련 동작

필드	**설명**
processes_created	파일이 생성한 프로세스 정보
command_executions	파일이 실행한 명령어
processes_injected	파일이 다른 프로세스에 주입한 내용
processes_terminated	파일이 종료한 프로세스
services_opened	파일이 실행한 서비스 관련 정보
processes_tree	파일이 생성한 프로세스 트리 구조

synchronization_mechanisms_signals : 파일이 시스템에서 동기화 메커니즘과 관련하여 수행한 동작

필드	**설명**
mutexes_created	파일이 생성한 mutex 객체
mutexes_opened	파일이 열린 mutex 객체

modules_loaded : 파일이 실행 중에 로드한 모듈을 기록 악성 파일이 추가적으로 로드하는 라이브러리나 코드

highlighted_actions : 분석 중에 강조된 주요 행동

필드	**설명**
calls_highlighted	중요하거나 특이한 시스템 호출
text_decoded	실행 중에 디코딩된 텍스트

system_property_lookups : 파일이 조회한 시스템 속성 정보(예 : 파일이 시스템 버전, 사용자 정보, 설치된 소프트웨어 정보를 확인하려는 시도 등)