**MongoDB 정의**

**JSON**{

    "details": {

        "hash": {

            "md5": "",

            "sha1": "",

            "sha256": "",

            "vhash": "",

            "auth\_hash": "",

            "imphash": "",

            "ssdeep": "",

            "tlsh": ""

        },

        "file\_info": {

            "md5": "",

            "file\_type": "",

            "magic": "",

            "file\_size": "",

            "PEID\_packer": "",

            "first\_seen\_time": "",

            "name": {

                "name1": "",

                "name2": ""

            }

        },

        "signature": {

            "verification": ""

        },

        "pe\_info": {

            ".net\_details": {},

            "header": {},

            "sections": {},

            "imports": {},

            "contained\_resources": {}

        },

        "dot\_net\_assembly": {

            "general": {},

            "streams": {},

            "manifest\_resource": {},

            "external\_assemblies": {},

            "assembly\_data": {},

            "type\_definitions": {},

            "external\_modules": {},

            "unmanged\_method\_list": {}

        }

    },

    "behavior": {

        "behavior\_tags": {},

        "mitre": {

            "privilege\_escalation": {},

            "defense\_evasion": {},

            "discovery": {},

            "collection": {},

            "command\_and\_control": {}

        },

        "capabilities": {},

        "network\_communications": {

            "DNS\_resolutions": {},

            "IP\_traffic": {},

            "JA3\_digests": {},

            "TLS": {}

        },

        "behavior\_similarity\_hashes": {

            "CAPA": "",

            "Microsoft\_Sysinternals": "",

            "Tencent\_HABO": "",

            "Yomi\_Hunter": "",

            "Zenbox": ""

        },

        "file\_system\_actions": {

            "file\_opened": {},

            "files\_written": {},

            "files\_deleted": {},

            "files\_copied": {},

            "files\_dropped": {}

        },

        "registry\_actions": {

            "registry\_keys\_opened": {},

            "registry\_keys\_set": {}

        },

        "process\_and\_serviece\_actions": {

            "processes\_created": {},

            "shell\_commands": {},

            "processes\_terminated": {},

            "process\_tree": {}

        },

        "synchronization\_mechanisms\_signal": {

            "mutexes\_created": {},

            "mutexes\_opened": {}

        },

        "modules\_loaded": {

            "runtime\_modules": {}

        },

        "highlighted\_actions": {

            "calls\_highlighted": {},

            "highlighted\_text": {}

        }

    }

}

**섹션 설명**

**Details 섹션**

**Details.hash 섹션**

* md5: MD5 해시 값
* sha1: SHA-1 해시 값
* sha256: SHA-256 해시 값
* vhash: 가변 해시 값
* auth\_hash: 인증 해시 값
* imphash: 임포트 해시 값
* ssdeep: SSDEEP 해시 값 (유사도 해시)
* tlsh: TLSH 해시 값 (TLSH는 비슷한 파일들을 감지하기 위한 해시 알고리즘)

**Details.file\_info 섹션**

* md5: 파일의 MD5 해시 값
* file\_type: 파일의 유형
* magic: 파일의 매직 넘버 (파일의 식별자)
* file\_size: 파일 크기
* PEID\_packer: 파일의 PEID 패커 정보
* first\_seen\_time: 파일이 처음 발견된 시간
* name: 파일의 이름

**Details.signature 섹션**

* verification: 악성코드 시그니처

**Details.pe\_info 섹션**

* .net\_details: .NET 관련 세부 정보
* header: PE 파일의 헤더 정보
* sections: PE 파일의 섹션 정보
* imports: 파일에서 임포트된 모듈 정보
* contained\_resources: 파일에 포함된 리소스 정보

**Details.dot\_net\_assembly 섹션**

* general: 일반 정보
* streams: .NET 어셈블리 스트림 정보
* manifest\_resource: 매니페스트 리소스 정보
* external\_assemblies: 외부 어셈블리 정보
* assembly\_data: 어셈블리 데이터
* type\_definitions: 타입 정의 정보
* external\_modules: 외부 모듈 정보
* unmanged\_method\_list: 관리되지 않는 메서드 리스트

**behavior 섹션**

**behavior.behavior\_tags 섹션**

* general: 일반 정보

**behavior.mitre 섹션**

* privilege\_escalation: 권한 상승에 대한 정보
* defense\_evasion: 방어 회피 기법
* discovery: 시스템 탐색 기법
* collection: 데이터 수집 기법
* command\_and\_control: 명령 및 제어 기법

**behavior.capabilities 섹션**

* general: 일반 정보

**behavior.network\_communications 섹션**

* DNS\_resolutions: DNS 해석 정보
* IP\_traffic: IP 트래픽 정보
* JA3\_digests: JA3 해시 (TLS 핑거프린팅)
* TLS: TLS 통신 정보

**behavior.behavior\_similarity\_hashes 섹션**

* CAPA: Capa 도구에서 생성된 해시
* Microsoft\_Sysinternals: Microsoft Sysinternals 도구로 생성된 해시
* Tencent\_HABO: Tencent HABO 도구로 생성된 해시
* Yomi\_Hunter: Yomi Hunter 도구로 생성된 해시
* Zenbox: Zenbox 도구로 생성된 해시

**behavior.file\_system\_actions 섹션**

* file\_opened: 열린 파일들
* files\_written: 작성된 파일들
* files\_deleted: 삭제된 파일들
* files\_copied: 복사된 파일들
* files\_dropped: 드롭된 파일들

**behavior.registry\_actions 섹션**

* registry\_keys\_opened: 열린 레지스트리 키들
* registry\_keys\_set: 설정된 레지스트리 키들

**behavior.process\_and\_service\_actions 섹션**

* processes\_created: 생성된 프로세스들
* shell\_commands: 실행된 셸 명령어들
* processes\_terminated: 종료된 프로세스들
* process\_tree: 프로세스 트리

**behavior.synchronization\_mechanisms\_signal 섹션**

* mutexes\_created: 생성된 뮤텍스들
* mutexes\_opened: 열린 뮤텍스들

**behavior.modules\_loaded 섹션**

* runtime\_modules: 런타임에 로드된 모듈들

**behavior.highlighted\_actions 섹션**

* calls\_highlighted: 하이라이트된 호출들
* highlighted\_text: 하이라이트된 텍스트들

**시각적 구조**



**SQL로 정의 했을시**

**테이블 생성문**

CREATE TABLE details (

    id SERIAL PRIMARY KEY

);

CREATE TABLE hash (

    id SERIAL PRIMARY KEY,

    details\_id INT REFERENCES details(id),

    md5 VARCHAR(255),

    sha1 VARCHAR(255),

    sha256 VARCHAR(255),

    vhash VARCHAR(255),

    auth\_hash VARCHAR(255),

    imphash VARCHAR(255),

    ssdeep VARCHAR(255),

    tlsh VARCHAR(255)

);

CREATE TABLE file\_info (

    id SERIAL PRIMARY KEY,

    details\_id INT REFERENCES details(id),

    md5 VARCHAR(255),

    file\_type VARCHAR(255),

    magic VARCHAR(255),

    file\_size VARCHAR(255),

    PEID\_packer VARCHAR(255),

    first\_seen\_time VARCHAR(255)

);

CREATE TABLE name (

    id SERIAL PRIMARY KEY,

    file\_info\_id INT REFERENCES file\_info(id),

    name1 VARCHAR(255),

    name2 VARCHAR(255)

);

CREATE TABLE signature (

    id SERIAL PRIMARY KEY,

    details\_id INT REFERENCES details(id),

    verification VARCHAR(255)

);

CREATE TABLE pe\_info (

    id SERIAL PRIMARY KEY,

    details\_id INT REFERENCES details(id),

    net\_details TEXT,

    header TEXT,

    sections TEXT,

    imports TEXT,

    contained\_resources TEXT

);

CREATE TABLE dot\_net\_assembly (

    id SERIAL PRIMARY KEY,

    details\_id INT REFERENCES details(id),

    general TEXT,

    streams TEXT,

    manifest\_resource TEXT,

    external\_assemblies TEXT,

    assembly\_data TEXT,

    type\_definitions TEXT,

    external\_modules TEXT,

    unmanaged\_method\_list TEXT

);

CREATE TABLE behavior (

    id SERIAL PRIMARY KEY

);

CREATE TABLE behavior\_tags (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id)

);

CREATE TABLE mitre (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    privilege\_escalation TEXT,

    defense\_evasion TEXT,

    discovery TEXT,

    collection TEXT,

    command\_and\_control TEXT

);

CREATE TABLE capabilities (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id)

);

CREATE TABLE network\_communications (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    DNS\_resolutions TEXT,

    IP\_traffic TEXT,

    JA3\_digests TEXT,

    TLS TEXT

);

CREATE TABLE behavior\_similarity\_hashes (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    CAPA VARCHAR(255),

    Microsoft\_Sysinternals VARCHAR(255),

    Tencent\_HABO VARCHAR(255),

    Yomi\_Hunter VARCHAR(255),

    Zenbox VARCHAR(255)

);

CREATE TABLE file\_system\_actions (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    file\_opened TEXT,

    files\_written TEXT,

    files\_deleted TEXT,

    files\_copied TEXT,

    files\_dropped TEXT

);

CREATE TABLE registry\_actions (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    registry\_keys\_opened TEXT,

    registry\_keys\_set TEXT

);

CREATE TABLE process\_and\_service\_actions (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    processes\_created TEXT,

    shell\_commands TEXT,

    processes\_terminated TEXT,

    process\_tree TEXT

);

CREATE TABLE synchronization\_mechanisms\_signal (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    mutexes\_created TEXT,

    mutexes\_opened TEXT

);

CREATE TABLE modules\_loaded (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    runtime\_modules TEXT

);

CREATE TABLE highlighted\_actions (

    id SERIAL PRIMARY KEY,

    behavior\_id INT REFERENCES behavior(id),

    calls\_highlighted TEXT,

    highlighted\_text TEXT

);

**ERD**

