VirusTotal

2025.11.22 (토)

최병주

VirusTotal이란?

VirusTotal은 Google이 운영하는 무료 악성코드 분석 서비스

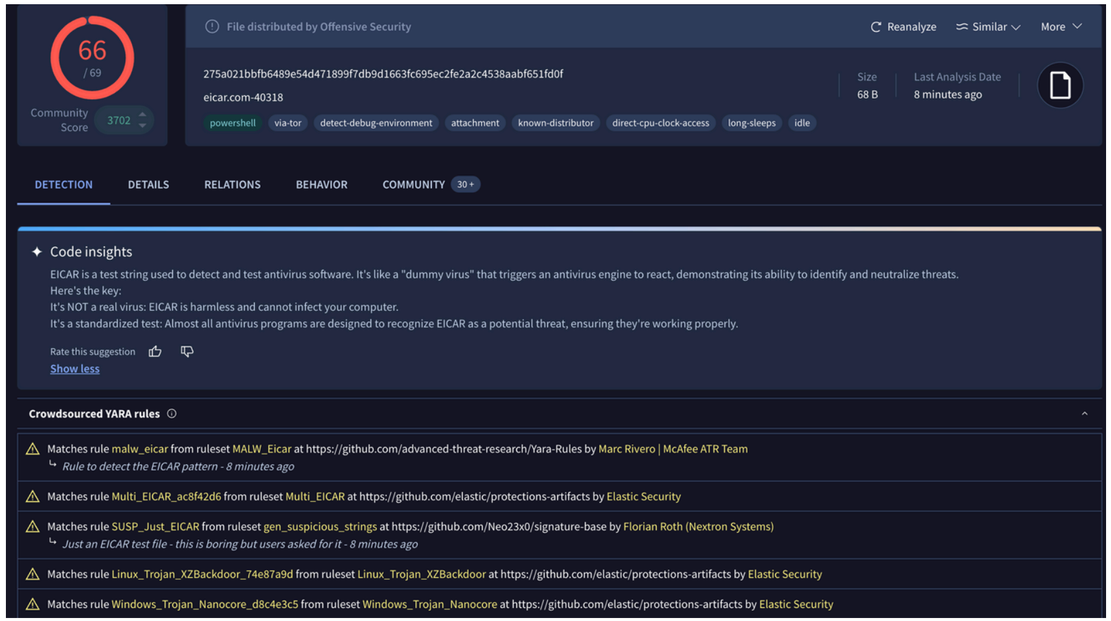
70개 이상의 백신 엔진과 URL/도메인 차단 서비스와 파일, URL, IP, 도메인의 악성 여부 검사 가능

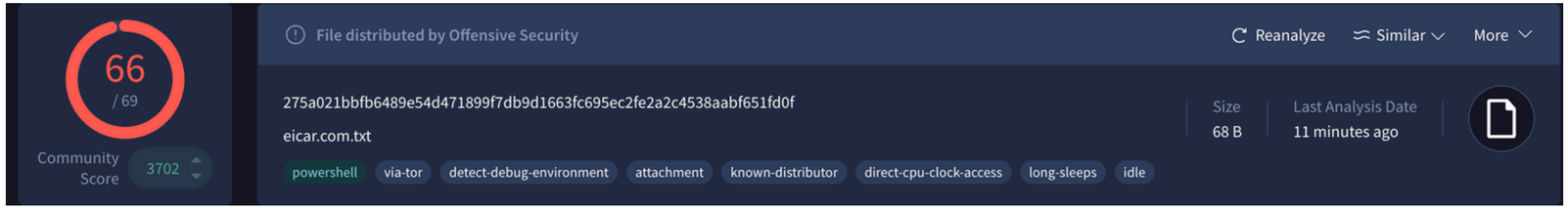
VirusTotal 주요 기능

핵심 스캐닝 기능

- **멀티 엔진 검사** – 70개 이상 백신 엔진의 동시 스캔으로 단일 백신 오탐 방지
- **파일 분석** – 최대 650MB 파일 업로드 지원, 실행 파일·문서·APK 등 모든 형식 지원
- **URL/도메인 검사** – 웹사이트 악성 여부, 피싱 사이트 탐지
- **IP 주소 분석** – IP 평판 정보, 과거 악성 활동 이력 조회
- **Hash 검색** – MD5, SHA-1, SHA-256 해시로 기존 분석 결과 즉시 확인

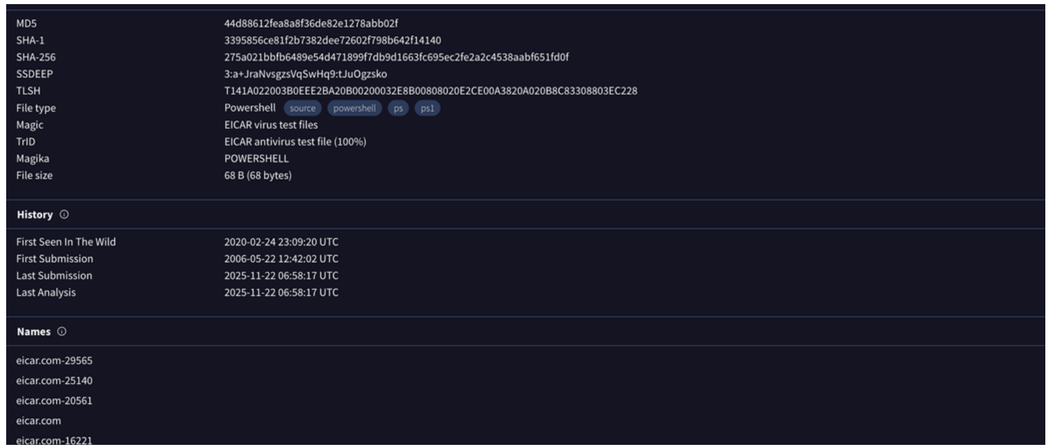
VirusTotal Test(파일 스캔)





파일 분석, 백신 엔진 기반의 악성 파일 분류 확인 가능

VirusTotal Test(파일 스캔 – Details, Relation)



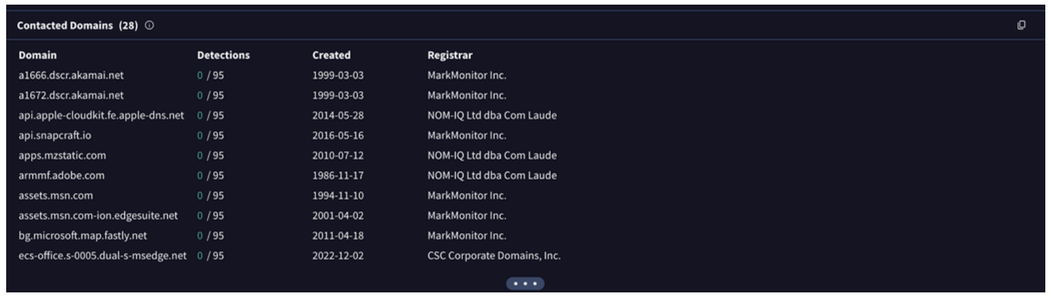
MD5	44d88612fea8a8f36de82e1278abb02f
SHA-1	3395856ce81f2b7382dee72602f798b642f14140
SHA-256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
SSDEEP	3:a+JraNvsgzsVqSwHq9:tJuOgzsko
TLSH	T141A022003B0EEE2BA20B00200032E8B00808020E2CE00A3820A020B8C83308803EC228
File type	Powershell source powershell ps ps1
Magic	EICAR virus test files
TrID	EICAR antivirus test file (100%)
Magika	POWERSHELL
File size	68 B (68 bytes)

History

First Seen In The Wild	2020-02-24 23:09:20 UTC
First Submission	2006-05-22 12:42:02 UTC
Last Submission	2025-11-22 06:58:17 UTC
Last Analysis	2025-11-22 06:58:17 UTC

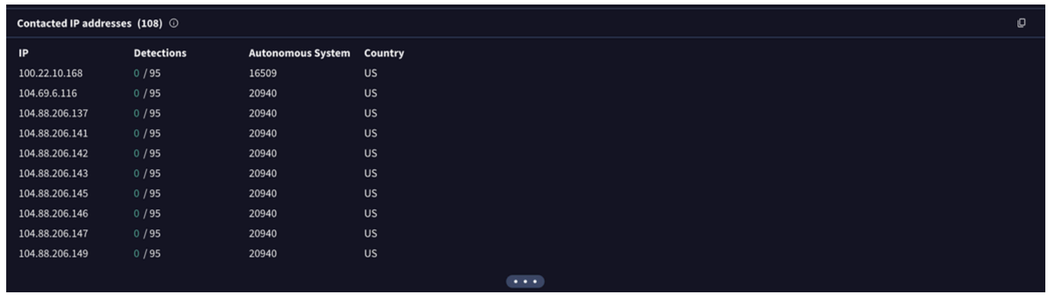
Names

eicar.com-29565
eicar.com-25140
eicar.com-20561
eicar.com
eicar.com-16221



Contacted Domains (28)

Domain	Detections	Created	Registrar
a1666.dscr.akamai.net	0 / 95	1999-03-03	MarkMonitor Inc.
a1672.dscr.akamai.net	0 / 95	1999-03-03	MarkMonitor Inc.
api.apple-cloudkit.fe.apple-dns.net	0 / 95	2014-05-28	NOM-IQ Ltd dba Com Laude
api.snapcraft.io	0 / 95	2016-05-16	MarkMonitor Inc.
apps.mzstatic.com	0 / 95	2010-07-12	NOM-IQ Ltd dba Com Laude
armmf.adobe.com	0 / 95	1986-11-17	NOM-IQ Ltd dba Com Laude
assets.msn.com	0 / 95	1994-11-10	MarkMonitor Inc.
assets.msn.com-ion.edgesuite.net	0 / 95	2001-04-02	MarkMonitor Inc.
bg.microsoft.map.fastly.net	0 / 95	2011-04-18	MarkMonitor Inc.
ecs-office.s-0005.dual-s-msedge.net	0 / 95	2022-12-02	CSC Corporate Domains, Inc.



Contacted IP addresses (108)

IP	Detections	Autonomous System	Country
100.22.10.168	0 / 95	16509	US
104.69.6.116	0 / 95	20940	US
104.88.206.137	0 / 95	20940	US
104.88.206.141	0 / 95	20940	US
104.88.206.142	0 / 95	20940	US
104.88.206.143	0 / 95	20940	US
104.88.206.145	0 / 95	20940	US
104.88.206.146	0 / 95	20940	US
104.88.206.147	0 / 95	20940	US
104.88.206.149	0 / 95	20940	US

파일 분석

- 파일 사이즈, 해시 값, 유형 등
- 파일 분석 히스토리
- 파일 명

네트워크 관계

- Contacted URLs – 파일 실행 시 접속하는 웹 주소 (C2 서버, 다운로드 URL 등)
  - C2 서버 → Command and Control Server
- Contacted IPs – 통신하는 IP 주소
- Contacted Domains – 접속하는 도메인
- DNS Resolutions – 도메인 → IP 변환 기록

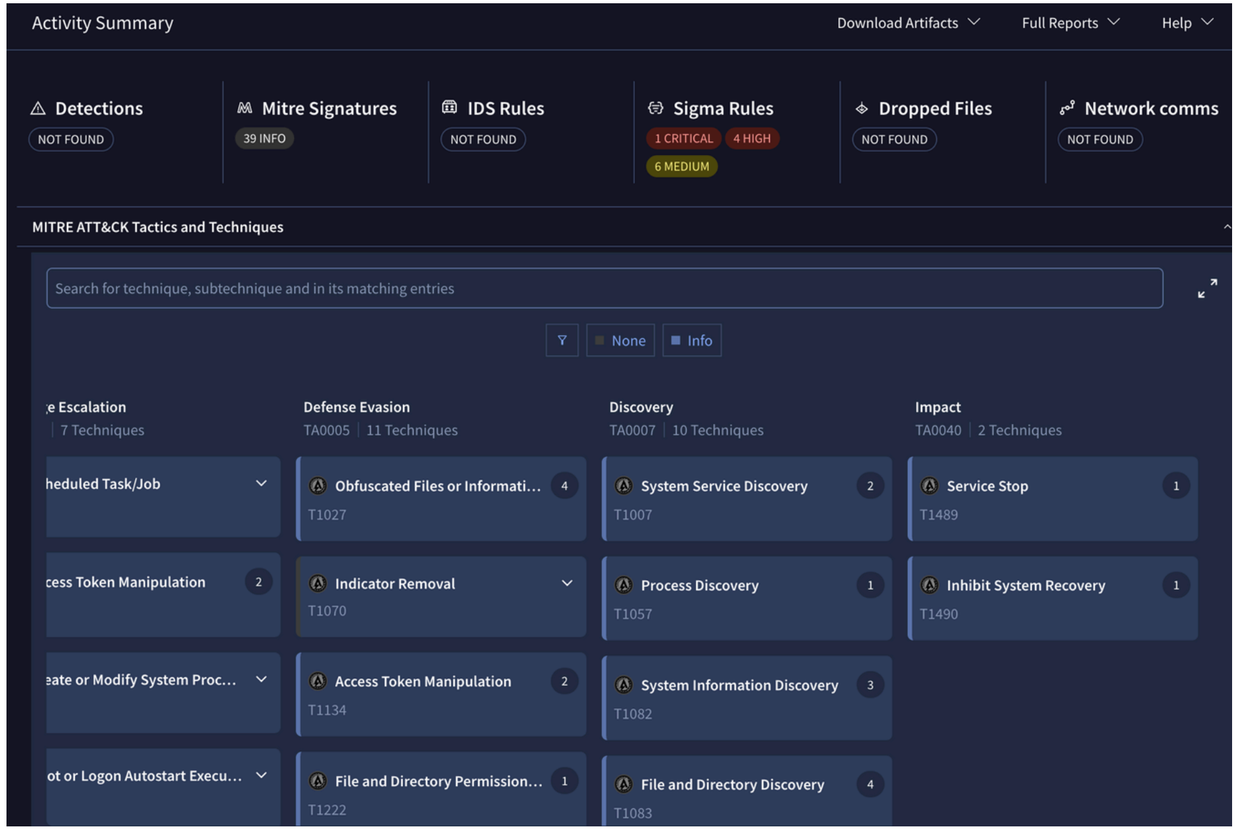
파일 관계

- Dropped Files – 실행 시 추가로 생성하는 파일 (2차 악성코드 등)
- Bundled Files – 압축/설치 파일 내부에 포함된 파일들
- Embedded URLs – 파일 코드 안에 하드코딩된 URL
- Execution Parents – 이 파일을 실행시킨 부모 프로세스

기타 관계

- Itw URLs – In The Wild, 실제 유포된 URL
- Referrer Files – 이 파일을 참조하는 다른 파일
- Similar Files – 코드 구조가 유사한 파일

VirusTotal Test(파일 스캔 – Behavior)

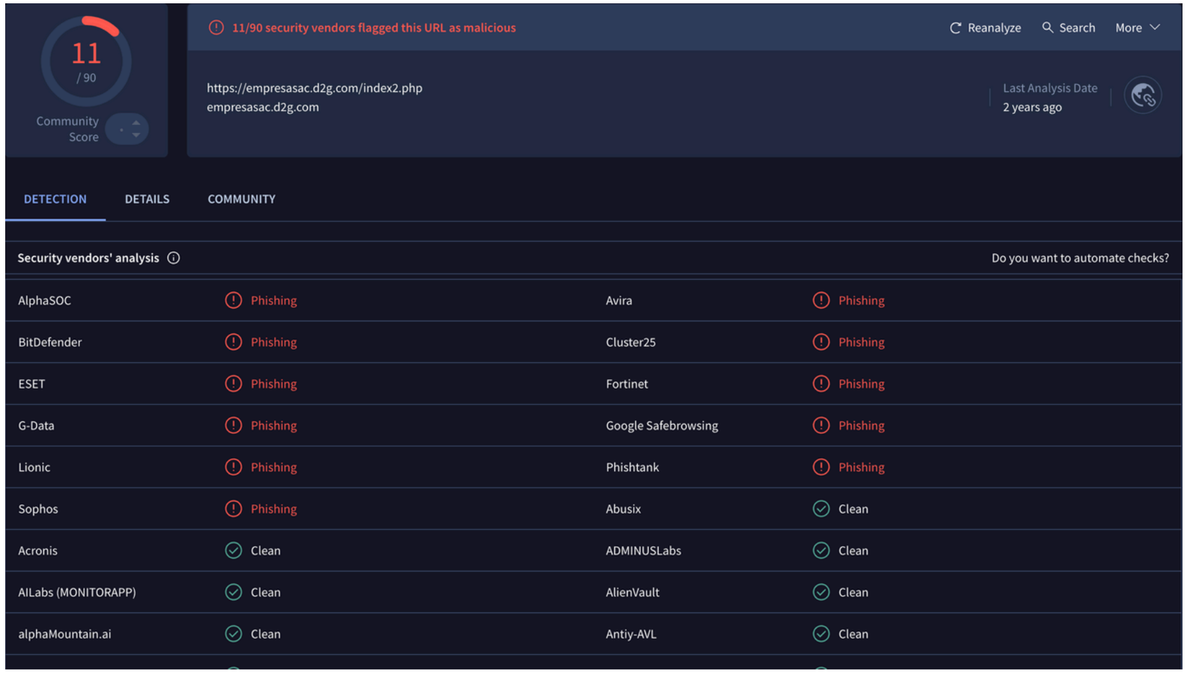


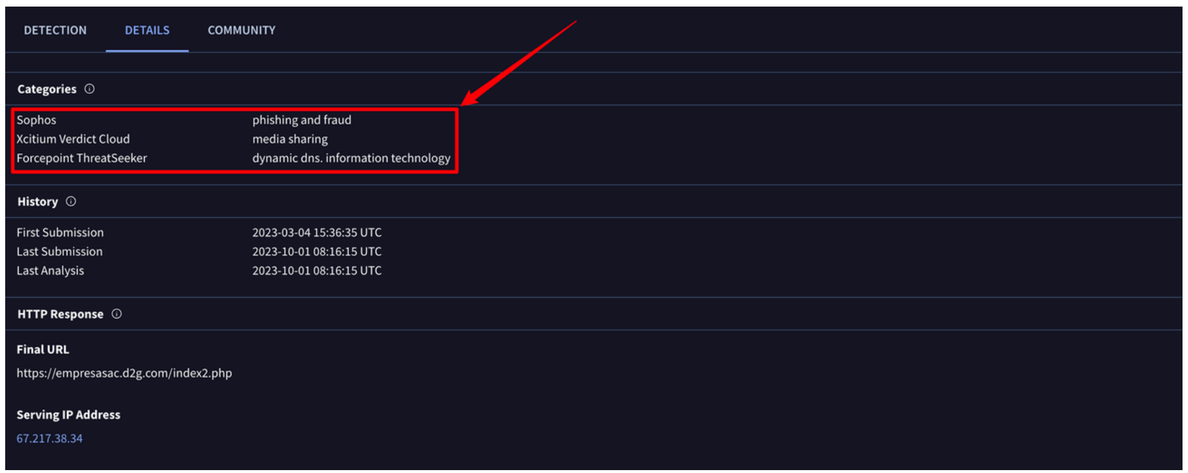
실제 파일의 실행 결과 확인 가능

실행된 샌드박스 환경에서 어떠한 동작을 수행했는지 감지

- Activity Summary 결과
- 실제 행동 기록
- Files Opened (열린 파일)
- 수행된 명령어
- Miter 패턴 여부
- 네트워크 히스토리

VirusTotal Test(URL 스캔)





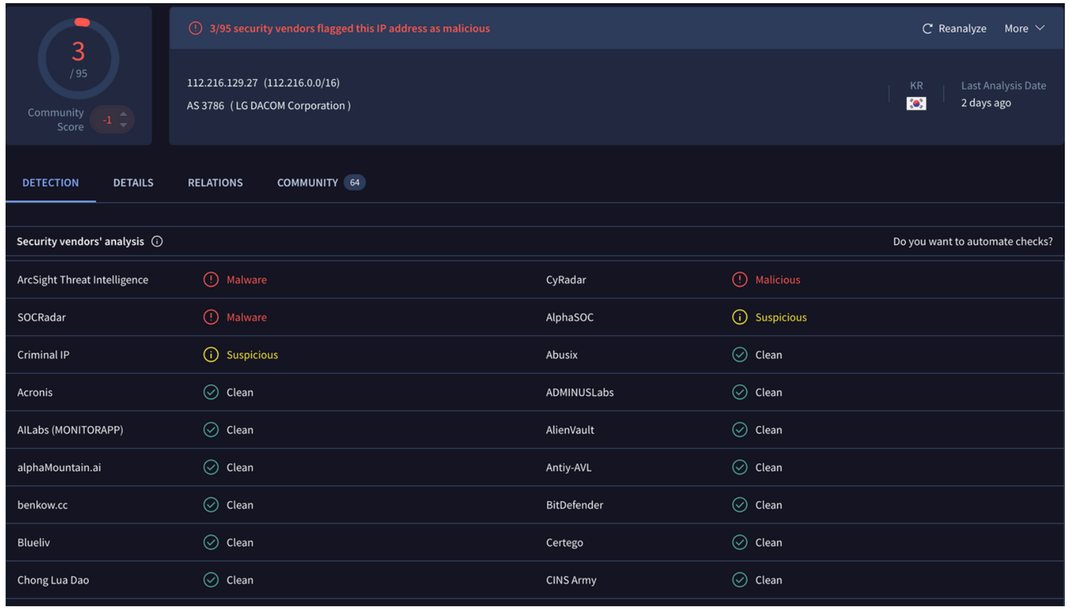
Vendor의 사이트 카테고리 확인

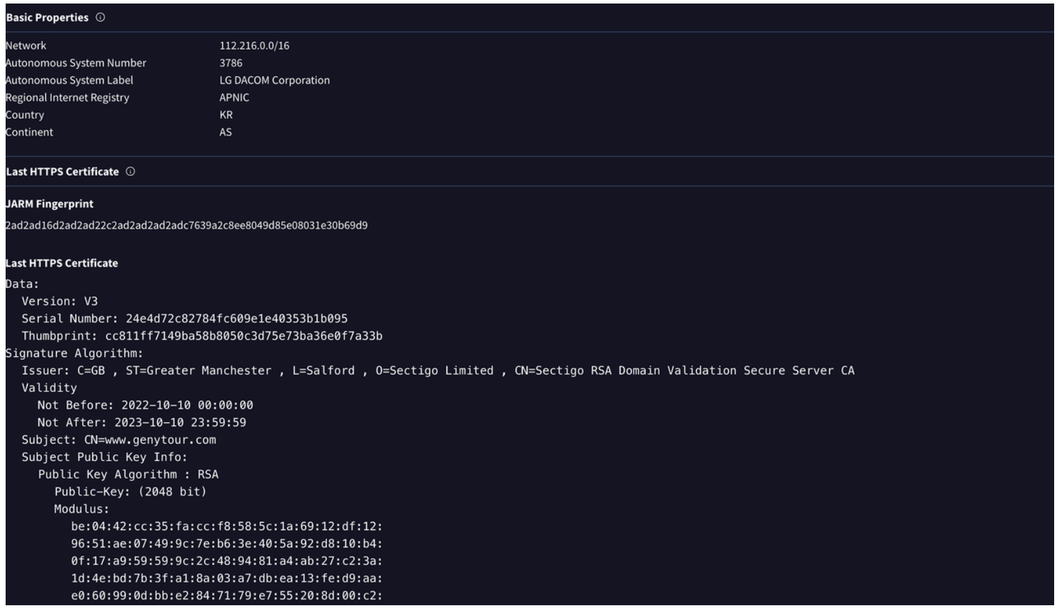
- Sophos → "phishing and fraud" (피싱/사기)
- Xcitium Verdict Cloud → "media sharing" (미디어 공유)
- Forcepoint ThreatSeeker → "dynamic dns, information technology"

기타 사이트 정보

- 최종 Redirection 경로
- IP 주소
- 히스토리 확인 가능

VirusTotal Test(IP 평판)





Passive DNS Replication (9)

Date resolved	Detections	Resolver	Domain
2023-09-26	0 / 95	VirusTotal	genytour.com
2023-09-26	0 / 95	VirusTotal	www.genytour.com
2021-05-21	0 / 95	VirusTotal	momodesign.net
2021-04-20	0 / 95	VirusTotal	msgr3.talknow.co.kr
2020-12-27	0 / 95	VirusTotal	talknow.io
2019-09-29	0 / 95	VirusTotal	rstudy.net
2018-11-03	0 / 95	VirusTotal	www.rstudy.net
2015-04-20	0 / 95	VirusTotal	i11.hanmarket.net
2013-04-01	0 / 95	VirusTotal	www.talknow.co.kr

VirusTotal 분석방법론

1단계 – 정적 분석(파일 조회)

1. Hash 기반 사전 조회

- 이미 분석된 파일인지 확인
- MD5/SHA-256 해시값으로 검색
- 과거 분석 이력 즉시 확인, 시간·비용 절약

2. 멀티 엔진 탐지 결과 검토

- 단일 엔진 오탐 가능성 고려
- 여러 엔진에서 탐지 시 악성 가능성 높음
- 패밀리명 일치 여부 확인 (예: 10개 엔진이 모두 "Trojan.Banker"로 분류)

3. 파일 메타데이터 분석

- 디지털 서명 검증 – 서명 없거나 무효 시 의심
- 컴파일 타임스탬프 – 미래 날짜는 조작 가능성
- 엔트로피 분석 – 높은 엔트로피는 패킹/암호화 의심
- Import 함수 – CreateRemoteThread, WriteProcessMemory 등 위험 API

2단계 – 동적 분석(Details, Relation, Behavior 기반 분석)

프로세스 분석(Details, Behavior)

- 프로세스 인젝션 탐지 – 정상 프로세스에 악성 코드 삽입
- 자가 복제 확인 – Startup 폴더, 레지스트리 Run 키 생성
- 권한 상승 시도 – UAC 우회, 토큰 도용

네트워크 분석(Relation, Details)

- C2 서버 식별 – Contacted IPs/URLs 확인
- DGA(Domain Generation Algorithm) 탐지 – 무작위 도메인 다수 접속
- 데이터 유출 – 대용량 outbound 트래픽

파일 시스템 분석(Behavior)

- Dropped files – 추가 멀웨어 다운로드 여부
- 삭제 파일 – Shadow Copy 삭제 시 랜섬웨어 의심
- 암호화 흔적 – 다수 파일 확장자 변경