

VirusTotal

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)

66

/ 69

Community Score

3702

⚠ File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com-40318

powershell

via-tor

detect-debug-environment

attachment

known-distributor

direct-cpu-clock-access

long-sleeps

idle

Size

68 B

Last Analysis Date

8 minutes ago

📄

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 30 +

🔍 Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats. Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.
It's a standardized test: Almost all antivirus programs are designed to recognize EICAR as a potential threat, ensuring they're working properly.

Rate this suggestion

👍

👎

Show less

Crowdsourced YARA rules

⚠ Matches rule **malw_eicar** from ruleset **MALW_Eicar** at <https://github.com/advanced-threat-research/Yara-Rules> by **Marc Rivero | McAfee ATR Team**
↳ Rule to detect the EICAR pattern - 8 minutes ago

⚠ Matches rule **Multi_EICAR_ac8f42d6** from ruleset **Multi_EICAR** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

⚠ Matches rule **SUSP_Just_EICAR** from ruleset **gen_suspicious_strings** at <https://github.com/Neo23x0/signature-base> by **Florian Roth (Nextron Systems)**
↳ Just an EICAR test file - this is boring but users asked for it - 8 minutes ago

⚠ Matches rule **Linux_Trojan_XZBackdoor_74e87a9d** from ruleset **Linux_Trojan_XZBackdoor** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

⚠ Matches rule **Windows_Trojan_Nanocore_d8c4e3c5** from ruleset **Windows_Trojan_Nanocore** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

AhnLab-V3	⚠ Virus/EICAR_Test_File	Alibaba	⚠ Virus:Win32/EICAR.A
AliCloud	⚠ Engtest:Multi/Eicar	ALYac	⚠ Misc.Eicar-Test-File
Antiy-AVL	⚠ TestFile/Win32.EICAR	Arcabit	⚠ EICAR-Test-File (not A Virus)
Avast	⚠ EICAR Test-NOT Virus!!!	Avast-Mobile	⚠ Eicar
AVG	⚠ EICAR Test-NOT Virus!!!	Avira (no cloud)	⚠ Eicar-Test-Signature
Baidu	⚠ Win32.Test.Eicar.a	BitDefender	⚠ EICAR-Test-File (not A Virus)
Bkav Pro	⚠ W32.EicarTest.Trojan	ClamAV	⚠ Win.Test.EICAR_HDB-1
CMC	⚠ Eicar.test.file	CTX	⚠ Txt.virus.eicar
Cynet	⚠ Malicious (score: 99)	DrWeb	⚠ EICAR Test File (NOT A Virus!)
Elastic	⚠ Eicar	Emsisoft	⚠ EICAR-Test-File (A)
eScan	⚠ EICAR-Test-File	ESET-NOD32	⚠ Eicar Test File
Fortinet	⚠ EICAR_TEST_FILE	GData	⚠ EICAR_TEST_FILE
Google	⚠ Detected	Gridinsoft (no cloud)	⚠ Trojan.U.EICAR_Test_File.dd
Huorong	⚠ TEST/AVEngTestFile!EICAR	Ikarus	⚠ EICAR-Test-File
Kingpin	⚠ EICAR-Test-File	K7AntiVirus	⚠ EICAR_Test_File

66

/ 69

Community Score

3702

⚠ File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com.txt

powershell

via-tor

detect-debug-environment

attachment

known-distributor

direct-cpu-clock-access

long-sleeps

idle

Size

68 B

Last Analysis Date

11 minutes ago

📄

Reanalyze

Similar

More

파일 분석, 백신 엔진 기반의 악성 파일 분류 확인 가능

VirusTotal Test(파일 스캔 – Details, Relation)

MD5	44d88612fea8af36de82e1278abb02f
SHA-1	3395856ce81f2b7382dee72602f798b642f14140
SHA-256	275a021bbfb6489e54d471899f7db9d1663fc69Sec2fe2a2c4538aabf651fd0f
SSDEEP	3:a+JraNvsgzsVqSwHq9:tJuOgzsko
TLSH	T141A022003B0EE2BA20B00200032E8B00808020E2CE00A3820A020B8C83308803EC228
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

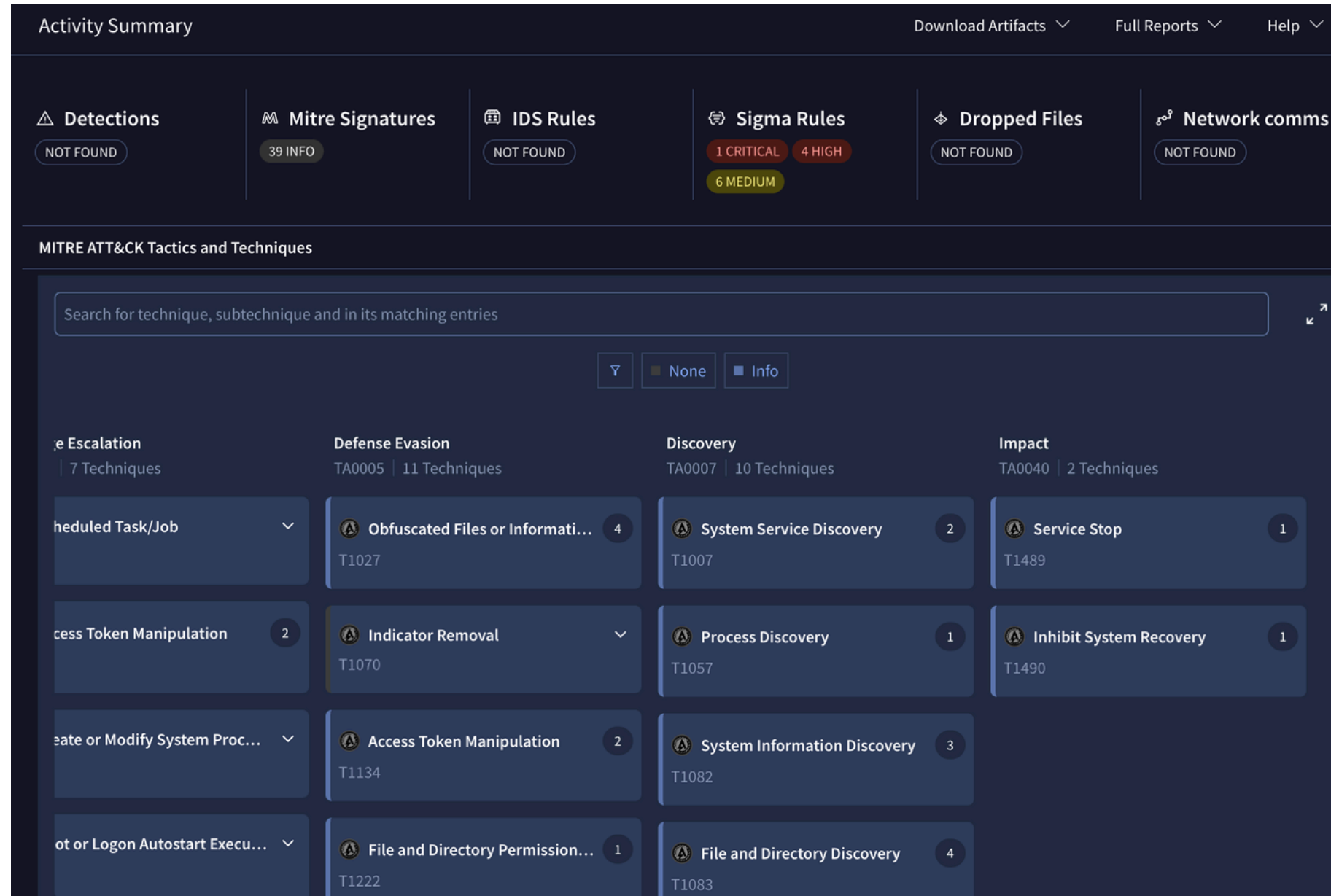
파일 관계

- 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)

11
/ 90

Community Score

11/90 security vendors flagged this URL as malicious

https://empresasac.d2g.com/index2.php
empresasac.d2g.com

Last Analysis Date
2 years ago

Reanalyze Search More

DETECTIONDETAILSCOMMUNITY

Security vendors' analysis ⓘ

Do you want to automate checks?

AlphaSOC	ⓘ Phishing	Avira	ⓘ Phishing
BitDefender	ⓘ Phishing	Cluster25	ⓘ Phishing
ESET	ⓘ Phishing	Fortinet	ⓘ Phishing
G-Data	ⓘ Phishing	Google Safebrowsing	ⓘ Phishing
Lionic	ⓘ Phishing	Phishtank	ⓘ Phishing
Sophos	ⓘ Phishing	Abusix	✔ Clean
Acronis	✔ Clean	ADMINUSLabs	✔ Clean
AlLabs (MONITORAPP)	✔ Clean	AlienVault	✔ Clean
alphaMountain.ai	✔ Clean	Antiy-AVL	✔ Clean

DETECTIONDETAILSCOMMUNITY

Categories ⓘ

Sophos	phishing and fraud
Xcitium Verdict Cloud	media sharing
Forcepoint ThreatSeeker	dynamic dns. information technology

History ⓘ

First Submission	2023-03-04 15:36:35 UTC
Last Submission	2023-10-01 08:16:15 UTC
Last Analysis	2023-10-01 08:16:15 UTC

HTTP Response ⓘ

Final URL
https://empresasac.d2g.com/index2.php

Serving IP Address
67.217.38.34

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)

3

/ 95

Community Score

-1

3/95 security vendors flagged this IP address as malicious

112.216.129.27 (112.216.0.0/16)

AS 3786 (LG DACOM Corporation)

KR

Last Analysis Date
2 days ago

Reanalyze

More

DETECTION

DETAILS

RELATIONS

COMMUNITY 64

Security vendors' analysis

Do you want to automate checks?

ArcSight Threat Intelligence	Malware	CyRadar	Malicious
SOCRadar	Malware	AlphaSOC	Suspicious
Criminal IP	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
ALLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean

Basic Properties

Network

112.216.0.0/16

Autonomous System Number

3786

Autonomous System Label

LG DACOM Corporation

Regional Internet Registry

APNIC

Country

KR

Continent

AS

Last HTTPS Certificate

JARM Fingerprint

2ad2ad16d2ad2ad22c2ad2ad2ad2adc7639a2c8ee8049d85e08031e30b69d9

Last HTTPS Certificate

Data:

Version: V3

Serial Number: 24e4d72c82784fc609e1e40353b1b095

Thumbprint: cc811ff7149ba58b8050c3d75e73ba36e0f7a33b

Signature Algorithm:

Issuer: C=GB , ST=Greater Manchester , L=Salford , O=Sectigo Limited , CN=Sectigo RSA Domain Validation Secure Server CA

Validity

Not Before: 2022-10-10 00:00:00

Not After: 2023-10-10 23:59:59

Subject: CN=www.genytour.com

Subject Public Key Info:

Public Key Algorithm : RSA

Public-Key: (2048 bit)

Modulus:

be:04:42:cc:35:fa:cc:f8:58:5c:1a:69:12:df:12:

96:51:ae:07:49:9c:7e:b6:3e:40:5a:92:d8:10:b4:

0f:17:a9:59:59:9c:2c:48:94:81:a4:ab:27:c2:3a:

1d:4e:bd:7b:3f:a1:8a:03:a7:db:ea:13:fe:d9:aa:

e0:60:99:0d:bb:e2:84:71:79:e7:55:20:8d:00:c2:

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