Malware Analysis & CTI

Malware Analysis Platforms

Use these platforms to analyze suspicious files, URLs, or scripts, and identify malicious behavior, network activity, and indicators.

- VirusTotal — Multi-engine malware scanner with IOC and sandbox integrations
- Hybrid Analysis — Dynamic malware analysis platform showing behavior and network calls
- ANY.RUN — Interactive sandbox for live malware execution and observation
- Cuckoo Sandbox — Open-source automated malware analysis system
- Intezer Analyze — Code-reuse and malware lineage analysis
- Joe Sandbox — Advanced commercial sandbox environment
- MalwareBazaar — Repository of malware samples and hashes

Malware Analysis Tools

Toolkits and utilities for static and dynamic analysis of binaries, scripts, and executables.

- Remnux — Linux distribution for reverse engineering and malware analysis
- YARA — Pattern-matching engine for malware detection and classification
- PEStudio — Windows executable analyzer for metadata and indicators
- Capa — Detects capabilities and functionality in executable files
- Die (Detect It Easy) — PE analysis tool for structure, entropy, and packers

Reverse Engineering & Disassembly

Tools for deep binary inspection, debugging, and reverse engineering of malware samples.

- Ghidra — Open-source reverse engineering suite developed by the NSA
- IDA Free — Disassembler and debugger with visual graph analysis
- Binary Ninja — Modern and scriptable reverse engineering platform
- x64dbg — Open-source Windows debugger for malware analysis

Network & Behavior Analysis

Monitor process activity, file system changes, and network communications of suspicious samples.

- Wireshark — Network packet capture and protocol analyzer
- Procmon — Real-time monitoring of file, registry, and process activity
- ApateDNS — DNS redirection tool for malware network simulation
- FakeNet-NG — Network emulation tool for capturing malware traffic

Malware Feeds & Repositories

Live sources of malware samples, indicators, and research materials.

- Malpedia — Structured database of malware families and samples
- VX Underground — Archive of malware source code and research papers
- URLhaus — Database of malicious URLs submitted by the community
- Feodo Tracker — C2 tracking for banking trojans and botnets
- MalShare — Public malware repository with daily sample updates

Threat Intelligence Platforms

Platforms for collecting, structuring, and sharing threat intelligence data.

- MISP — Open-source platform for sharing threat intelligence and IOCs
- OpenCTI — Knowledge graph for cyber threat intelligence management
- YETI — Framework for storing and correlating threat data
- ThreatConnect — Commercial CTI platform with automation and analytics
- EclecticIQ Platform — Enterprise-grade CTI management and analysis platform
- AboutIntel - Freemium TI and AS monitor to deliver relevant, actionable security insights. Without the noise.

IOC Enrichment & Internet Scanners

Tools for IOC enrichment, infrastructure mapping, and exposure analysis of malicious ecosystems.

- SilentPush - Track, monitor and counteract global threat activity.
- Validin - Explore and track threats across key attributes for public infrastructure tracking
- ThreatMiner — Data mining for IOCs, malware, SSL, and related artifacts
- Abuse.ch — Home to ThreatFox, Feodo Tracker, URLhaus, and SSLBL projects
- GreyNoise — Contextual intelligence on internet-scanning IPs
- AlienVault OTX — Community threat intelligence sharing platform
- Maltiverse — IOC enrichment with threat classification and context
- Shodan — Internet-wide search engine for exposed systems
- Censys — Search engine for internet infrastructure and certificates
- BinaryEdge — Real-time internet scanning and asset discovery for threat analysis
- CriminalIP — Attack surface and exposure analysis platform
- FOFA — Cyber asset search engine widely used in China for exposure research
- Censys Workshop — Research environment showcasing Censys experimental tools

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/osint/docs_malware-cti

Last update: **2026/08/07 11:49**