

Malware Analysis Toolkit

Listed below are some of the tools that can be used by the incident handler to perform malware analysis.

Software Tools Required for Malware Analysis	
Category	Tools
YARA Tools	<ul style="list-style-type: none"> ▪ yarGen (https://github.com) ▪ Koodous (https://docs.koodous.com) ▪ YaraRET (https://github.com) ▪ YARA Silly (https://github.com) ▪ Halogen (https://github.com) ▪ Yabin (https://github.com)
Remote Access Trojans (RATs) Detection Tools	<ul style="list-style-type: none"> ▪ SolarWinds Security Event Manager (https://www.solarwinds.com) ▪ Malwarebytes (https://www.malwarebytes.com) ▪ Snort (https://www.snort.org) ▪ OSSEC (https://www.ossec.net) ▪ Zeek (https://zeek.org) ▪ Suricata (https://suricata.io)
Tools for Detecting Malware in Encrypted Network Traffic	<ul style="list-style-type: none"> ▪ Flowmon (https://www.flowmon.com) ▪ Cisco Encrypted Traffic Analytics (https://www.cisco.com) ▪ ThreatEye (https://www.liveaction.com) ▪ Juniper Advanced Threat Prevention (https://www.juniper.net) ▪ Bitdefender Network Traffic Analysis (https://www.bitdefender.com) ▪ ExtraHop Reveal(x) 360 (https://www.extrahop.com)
Fileless Malware Detection Tools	<ul style="list-style-type: none"> ▪ AlienVault USM Anywhere (https://cybersecurity.att.com) ▪ Quick Heal Total Security (https://www.quickheal.com) ▪ Apex One (https://www.trendmicro.com) ▪ Logsign (https://www.logsign.com) ▪ FortiGuard (https://www.fortinet.com) ▪ CYNET EDR (https://www.cynet.com)
Malware Incidents Containment Tools	<ul style="list-style-type: none"> ▪ Infoblox (https://www.infoblox.com) ▪ Rubrik (https://www.rubrik.com) ▪ Microsoft Defender for Endpoint (https://www.microsoft.com) ▪ Illumio (https://www.illumio.com) ▪ Comodo (https://www.comodo.com)

	<ul style="list-style-type: none"> ▪ Netwrix (https://www.netwrix.com)
Virtual Machine Tools	<ul style="list-style-type: none"> ▪ Hyper-V (https://www.microsoft.com) ▪ Parallels Desktop 18 (https://www.parallels.com) ▪ Boot Camp (https://www.apple.com) ▪ VMware Workstation Pro (https://www.vmware.com)
Screen Capture and Recording Tools	<ul style="list-style-type: none"> ▪ Snagit (https://www.techsmith.com) ▪ Jing (https://www.techsmith.com) ▪ Camtasia (https://www.techsmith.com) ▪ Ezvid (https://www.ezvid.com)
Network and Internet Simulation Tools	<ul style="list-style-type: none"> ▪ NetSim Professional (https://tetcos.com) ▪ ns-3 (https://www.nsnam.org) ▪ Riverbed Modeler (https://www.riverbed.com) ▪ QualNet (https://web.scalable-networks.com)
OS Backup and Imaging Tools	<ul style="list-style-type: none"> ▪ Genie Backup Manager Pro (https://www.genie9.com) ▪ Macrium Reflect Server (https://www.macrium.com) ▪ R-Drive Image (https://www.drive-image.com) ▪ O&O DiskImage 10 (https://www.oo-software.com)
Port Monitoring Tools	<ul style="list-style-type: none"> ▪ Netstat (https://learn.microsoft.com) ▪ TCPView (https://learn.microsoft.com) ▪ CurrPorts (https://www.nirsoft.net) ▪ PortExpert (http://www.kcsoftwares.com) ▪ PRTG Network Monitor (https://www.paessler.com) ▪ Port Monitor (https://www.port-monitor.com) ▪ TCP Port / Telnet Monitoring (https://www.dotcom-monitor.com)
Process Monitoring Tools	<ul style="list-style-type: none"> ▪ Process Monitor (https://learn.microsoft.com) ▪ Process Explorer (https://learn.microsoft.com) ▪ Monit (https://mmonit.com) ▪ ESET SysInspector (https://www.eset.com) ▪ System Explorer (http://systemexplorer.net) ▪ OpManager (https://www.manageengine.com)
Registry Monitoring Tools	<ul style="list-style-type: none"> ▪ jv16 PowerTools (https://jv16powertools.com) ▪ regshot (https://sourceforge.net) ▪ Reg Organizer (https://www.chemtable.com) ▪ Registry Viewer (https://accessdata.com) ▪ RegScanner (https://www.nirsoft.net) ▪ Registry Monitoring Tool (https://www.solarwinds.com)

Windows Services Monitoring Tools	<ul style="list-style-type: none"> Windows Service Manager (SrvMan) (https://sysprogs.com) Advanced Windows Service Manager (https://securityxploded.com) Process Hacker (https://processhacker.sourceforge.io) Netwrix Service Monitor (https://www.netwrix.com) AnVir Task Manager (https://www.anvir.com) Service+ (https://www.activeplus.com)
Startup Programs Monitoring Tools	<ul style="list-style-type: none"> Autoruns for Windows (https://www.microsoft.com) HiBit Startup Manager (https://www.hibitsoft.ir) Autorun Organizer (https://www.chemtable.com) Quick Startup (https://www.glarysoft.com) StartEd Pro (https://www.outertech.com) AnVir Task Manager Free (https://www.anvir.com)
Event Logs Monitoring/Analysis Tools	<ul style="list-style-type: none"> Splunk Enterprise Security (https://www.splunk.com) ManageEngine EventLog Analyzer (https://www.manageengine.com) New Relic (https://newrelic.com) Solarwinds Loggly (https://www.loggly.com) Netwrix Event Log Manager (https://www.netwrix.com)
Installation Monitoring Tools	<ul style="list-style-type: none"> Mirekrosoft Install Monitor (https://www.mirekrosoft.com) SysAnalyzer (https://www.aldeid.com) Advanced Uninstaller PRO (https://www.advanceduninstaller.com) Revo Uninstaller PRO (https://www.revouninstaller.com) Comodo Programs Manager (https://www.comodo.com)
Files and Folder Monitoring Tools	<ul style="list-style-type: none"> Sigverif (https://www.microsoft.com) Tripwire File Integrity Manager (https://www.tripwire.com) Netwrix Auditor (https://www.netwrix.com) Verisys (https://www.ionx.co.uk) PA File Sight (https://www.poweradmin.com) CSP File Integrity Checker (https://www.cspsecurity.com)
Device Drivers Monitoring Tools	<ul style="list-style-type: none"> DriverView (https://www.nirsoft.net) Driver Booster (https://www.iobit.com) Driver Reviver (https://www.reviversoft.com) Driver Easy (https://www.drivereasy.com) Driver Fusion (https://treexy.com) Driver Genius 22 (http://www.driver-soft.com)
Network Traffic Monitoring Tools	<ul style="list-style-type: none"> SolarWinds NetFlow Traffic Analyzer (https://www.solarwinds.com) Capsa Network Analyzer (https://www.colasoft.com) Wireshark (https://www.wireshark.org)

	<ul style="list-style-type: none"> ▪ PRTG Network Monitor (https://kb.paessler.com) ▪ GFI LanGuard (https://www.gfi.com) ▪ insightIDR (https://www.rapid7.com)
DNS Monitoring/Resolution Tools	<ul style="list-style-type: none"> ▪ DNSQuerySniffer (https://www.nirsoft.net) ▪ DNSstuff (https://www.dnsstuff.com) ▪ UltraDNS (https://neustarsecurityservices.com) ▪ Sonar Lite Web App (https://constellix.com)
API Calls Monitoring Tools	<ul style="list-style-type: none"> ▪ API Monitor (https://www.apimonitor.com) ▪ APImetrics (https://apimetrics.io) ▪ Runscope (https://www.runscope.com) ▪ AlertSite (https://smartbear.com)
System Calls Monitoring Tools	<ul style="list-style-type: none"> ▪ strace (https://strace.io)
Scheduled Task Monitoring Tools	<ul style="list-style-type: none"> ▪ Monitoring Task Scheduler Tool (MoTaSh) (https://github.com) ▪ ADAudit Plus (https://www.manageengine.com) ▪ CronitorCLI (https://cronitor.io) ▪ Solarwinds Windows Scheduled Task Monitor (https://www.solarwinds.com)
Browser Activity Monitoring Tools	<ul style="list-style-type: none"> ▪ Wireshark (https://www.wireshark.org) ▪ Colasoft Network Analyzer (https://www.colasoft.com) ▪ OmniPeek (https://www.savvius.com) ▪ Observer Analyzer (https://www.viavisolutions.com) ▪ PRTG Network Monitor (https://www.paessler.com) ▪ NetFlow Analyzer (https://www.manageengine.com)
File Fingerprinting Tools	<ul style="list-style-type: none"> ▪ HashMyFiles (https://www.nirsoft.net) ▪ mimikatz (https://github.com) ▪ HashCalc (https://www.slavasoft.com) ▪ hashdeep (https://github.com) ▪ MD5sums (http://www.pc-tools.net) ▪ tools4noobs - Online hash calculator (https://www.tools4noobs.com)
Local and Online Malware Scanning Tools	<ul style="list-style-type: none"> ▪ VirusTotal (https://www.virustotal.com) ▪ Hybrid Analysis (https://www.hybrid-analysis.com) ▪ Cuckoo Sandbox (https://cuckoosandbox.org) ▪ Jotti (https://virusscan.jotti.org) ▪ Valkyrie Sandbo0078 (https://valkyrie.comodo.com) ▪ Online Scanner (https://www.fortiguard.com)

Strings Searching Tools	<ul style="list-style-type: none"> ▪ BinText (https://www.aldeid.com) ▪ FLOSS (https://www.fireeye.jp) ▪ Strings (https://learn.microsoft.com) ▪ Free EXE DLL Resource Extract (https://resourceextract.com) ▪ FileSeek (https://www.fileseek.ca) ▪ Hex Workshop (http://www.hexworkshop.com)
Packing/Obfuscation Tools	<ul style="list-style-type: none"> ▪ PEiD (https://www.aldeid.com) ▪ Detect It Easy (DIE) (https://github.com) ▪ MacroPack (https://github.com) ▪ UPX (https://upx.github.io) ▪ ASPack (http://www.aspack.com) ▪ VMprotect (https://vmpsoft.com) ▪ ps2-packer (https://github.com)
PE Extraction Tools	<ul style="list-style-type: none"> ▪ PE Explorer (http://www.heaventools.com) ▪ Portable Executable Scanner (pescan) (https://tzworks.net) ▪ Resource Hacker (http://www.angusj.com) ▪ PEView (https://www.aldeid.com)
Dependency Checking Tools	<ul style="list-style-type: none"> ▪ Dependency Walker (http://www.dependencywalker.com) ▪ dependency-check (https://jeremylong.github.io) ▪ Snyk (https://snyk.io) ▪ PE Explorer Dependency Scanner (http://www.pe-explorer.com) ▪ Retire.js (https://retirejs.github.io)
Disassembling and Debugging Tools	<ul style="list-style-type: none"> ▪ IDA Pro (https://www.hex-rays.com) ▪ Ghidra (https://ghidra-sre.org) ▪ OllyDbg (http://www.ollydbg.de) ▪ x64dbg (https://x64dbg.com) ▪ radare (https://rada.re) ▪ WinDbg (http://www.windbg.org)
Static Analysis of ELF Files	<ul style="list-style-type: none"> ▪ readelf (https://linux.die.net)
Analyzing String Reuse	<ul style="list-style-type: none"> ▪ Intezer (https://www.intezer.com)
Malicious Mach-O Binaries Analysis Tools	<ul style="list-style-type: none"> ▪ LIEF (https://lief-project.github.io) ▪ otool (https://github.com)
Reverse Engineering Mach-O Binaries	<ul style="list-style-type: none"> ▪ Hopper Disassembler (https://www.hopperapp.com)

Memory Dump Analysis Tools	<ul style="list-style-type: none"> ▪ Volatility Framework (https://www.volatilityfoundation.org)
SSDT Analysis Tools	<ul style="list-style-type: none"> ▪ SSDT View (https://www.novirusthanks.org)
Kernel Filter Drivers	<ul style="list-style-type: none"> ▪ RogueKiller (https://www.adlice.com)
Covert Malware Beaconsing Tools	<ul style="list-style-type: none"> ▪ CapLoader (https://www.netresec.com) ▪ Wireshark (https://www.wireshark.org)
Covert C&C Communication Tools	<ul style="list-style-type: none"> ▪ PRTG Network Monitor (https://www.paessler.com) ▪ GFI LanGuard (https://www.gfi.com)
Malware Alerts Analysis Tools	<ul style="list-style-type: none"> ▪ Microsoft 365 Defender (https://www.microsoft.com)
Antivirus Tools	<ul style="list-style-type: none"> ▪ TotalAV (https://www.totalav.com) ▪ Bitdefender Antivirus Plus (https://www.bitdefender.com) ▪ Kaspersky Anti-Virus (https://www.kaspersky.com) ▪ McAfee® Total Protection (https://www.mcafee.com) ▪ Norton AntiVirus Plus (https://us.norton.com) ▪ Avast Premium Security (https://www.avast.com)
Anti-Trojan Software	<ul style="list-style-type: none"> ▪ Malwarebytes (https://www.malwarebytes.com) ▪ Bitdefender Total Security (https://bitdefender.com) ▪ Norton 360 Premium (https://us.norton.com) ▪ HitmanPro (https://www.hitmanpro.com) ▪ Plumbytes Anti-Malware (https://plumbytes.com) ▪ AVG AntiVirus (https://www.avg.com)
Malware Incident Recovery Tools	<ul style="list-style-type: none"> ▪ EaseUS Data Recovery Wizard (https://www.easeus.com) ▪ Remo Recover (https://www.remosoftware.com) ▪ Stellar Data Recovery Professional (https://www.stellarinfo.com) ▪ Trellix Ransomware Recover (https://www.trellix.com) ▪ NAKIVO (https://www.nakivo.com) ▪ Advanced Disk Recovery (https://www.systweak.com)
Fileless Malware Protection Tools	<ul style="list-style-type: none"> ▪ Microsoft Defender for Endpoint (https://www.microsoft.com) ▪ Kaspersky End Point Security for Business (https://www.kaspersky.com) ▪ SentinelOne (https://www.sentinelone.com) ▪ BlackBerry Spark Suites (https://www.blackberry.com) ▪ Norton 360 (https://us.norton.com) ▪ Sophos Endpoint Detection and Response (https://www.sophos.com)