恶意软件分析大合集

# 恶意软件集合

## 匿名代理

*对于分析人员的 Web 流量匿名方案*

* [Anonymouse.org](http://anonymouse.org/) - 一个免费、基于 Web 的匿名代理
* [OpenVPN](https://openvpn.net/) - VPN 软件和托管解决方案
* [Privoxy](http://www.privoxy.org/) - 一个带有隐私保护功能的开源代理服务器
* [Tor](https://www.torproject.org/) - 洋葱路由器，为了在浏览网页时不留下客户端 IP 地址

## 蜜罐

*捕获和收集你自己的样本*

* [Conpot](https://github.com/mushorg/conpot) - ICS/SCADA 蜜罐
* [Cowrie](https://github.com/micheloosterhof/cowrie) - 基于 Kippo 的 SSH 蜜罐
* [Dionaea](http://dionaea.carnivore.it/) - 用来捕获恶意软件的蜜罐
* [Glastopf](http://glastopf.org/) - Web 应用蜜罐
* [Honeyd](http://honeyd.org/) - 创建一个虚拟蜜罐
* [HoneyDrive](http://honeydrive.org/) - 蜜罐包的 Linux 发行版
* [Mnemosyne](https://github.com/johnnykv/mnemosyne) - 受 Dinoaea 支持的蜜罐数据标准化
* [Thug](https://github.com/buffer/thug) - 用来调查恶意网站的低交互蜜罐

## 恶意软件样本库

*收集用于分析的恶意软件样本*

* [Clean MX](http://support.clean-mx.de/clean-mx/viruses.php) - 恶意软件和恶意域名的实时数据库
* [Contagio](http://contagiodump.blogspot.com/) - 近期的恶意软件样本和分析的收集
* [Exploit Database](https://www.exploit-db.com/) - Exploit 和 shellcode 样本
* [Malshare](http://malshare.com/) - 在恶意网站上得到的大量恶意样本库
* [MalwareDB](http://malwaredb.malekal.com/) - 恶意软件样本库
* [Open Malware Project](http://openmalware.org/) - 样本信息和下载
* [Ragpicker](https://github.com/robbyFux/Ragpicker) - 基于 malware crawler 的一个插件
* [theZoo](https://github.com/ytisf/theZoo) - 分析人员的实时恶意样本库
* [Tracker h3x](http://tracker.h3x.eu/) - Agregator 的恶意软件跟踪和下载地址
* [ViruSign](http://www.virusign.com/) - 除 ClamAV 外的反病毒程序检出的恶意软件数据库
* [VirusShare](http://virusshare.com/) - 恶意软件库
* [VX Vault](http://vxvault.net/) - 恶意软件样本的主动收集
* [Zeltser's Sources](https://zeltser.com/malware-sample-sources/) - 由 Lenny Zeltser 整理的恶意软件样本源列表
* [Zeus Source Code](https://github.com/Visgean/Zeus) - 2011 年 Zeus 源码泄露

# 开源威胁情报

## 工具

*收集、分析 IOC 信息*

* [AbuseHelper](https://github.com/abusesa/abusehelper) - 用于接收和重新分发威胁情报的开源框架
* [AlienVault Open Threat Exchange](https://otx.alienvault.com/) - 威胁情报的共享与合作
* [Combine](https://github.com/mlsecproject/combine) - 从公开的信息源中得到威胁情报信息
* [Fileintel](https://github.com/keithjjones/fileintel) - 文件情报
* [Hostintel](https://github.com/keithjjones/hostintel) - 主机情报
* [IntelMQ](https://www.enisa.europa.eu/activities/cert/support/incident-handling-automation) - CERT 使用消息队列来处理应急数据的工具
* [IOC Editor](https://www.mandiant.com/resources/download/ioc-editor/) - Mandiant 出品的一个免费的 XML IOC 文件编辑器
* [ioc\_writer](https://github.com/mandiant/ioc_writer) - 开发的用于 OpenIOC 对象的 Python 库
* [Massive Octo Spice](https://github.com/csirtgadgets/massive-octo-spice) - 由 [CSIRT Gadgets Foundation](http://csirtgadgets.org/collective-intelligence-framework)发起，之前叫做 CIF (Collective Intelligence Framework)，从各种信息源聚合 IOC 信息
* [MISP](https://github.com/MISP/MISP) - 由 [The MISP Project](http://www.misp-project.org/) 发起的恶意软件信息共享平台
* [PassiveTotal](https://www.passivetotal.org/) - 研究、链接、标注和分享 IP 与 域名
* [PyIOCe](https://github.com/pidydx/PyIOCe) - 一个 Python OpenIOC 编辑器
* [threataggregator](https://github.com/jpsenior/threataggregator) - 聚合来自多个信息源的安全威胁，包括 [other resources](https://paper.seebug.org/421/#other-resources) 列表中的一些
* [ThreatCrowd](https://www.threatcrowd.org/) - 带有图形可视化的威胁搜索引擎
* [TIQ-test](https://github.com/mlsecproject/tiq-test) - 威胁情报源的数据可视化和统计分析

## 其他资源

*威胁情报和 IOC 资源*

* [Autoshun](http://autoshun.org/) ([list](http://autoshun.org/)) - Snort 插件和黑名单
* [Bambenek Consulting Feeds](http://osint.bambenekconsulting.com/feeds/) - 基于恶意 DGA 算法的 OSINT 订阅
* [Fidelis Barncat](https://www.fidelissecurity.com/resources/fidelis-barncat) - 可扩展的恶意软件配置数据库（必须有请求权限）
* [CI Army](http://www.ciarmy.com/) ([list](http://www.ciarmy.com/list/ci-badguys.txt)) - 网络安全黑名单
* [Critical Stack- Free Intel Market](https://intel.criticalstack.com/) - 免费的英特尔去重聚合项目，有超过 90 种订阅以及超过一百二十万个威胁情报信息
* [CRDF ThreatCenter](http://threatcenter.crdf.fr/) - 由 CRDF 提供的新威胁检出
* [Cybercrime tracker](http://cybercrime-tracker.net/) - 多个僵尸网络的活动跟踪
* [FireEye IOCs](https://github.com/fireeye/iocs) - 由 FireEye 共享的 IOC 信息
* [FireHOL IP Lists](https://iplists.firehol.org/) - 针对攻击、恶意软件的更改历史、国家地图和保留政策的 350+ IP 的跟踪
* [hpfeeds](https://github.com/rep/hpfeeds) - 蜜罐订阅协议
* [Internet Storm Center (DShield)](https://isc.sans.edu/) - 日志和可搜索的事件数据库，并且带有 Web [API](https://dshield.org/api/)([非官方 Python 库](https://github.com/rshipp/python-dshield)).
* [malc0de](http://malc0de.com/database/) - 搜索事件数据库
* [Malware Domain List](http://www.malwaredomainlist.com/) - 搜索和分享恶意软件 URL
* [OpenIOC](http://openioc.org/) - 威胁情报共享框架
* [Palevo Blocklists](https://palevotracker.abuse.ch/blocklists.php) - 蜜罐 C&C 黑名单
* [Proofpoint Threat Intelligence](https://www.proofpoint.com/us/products/et-intelligence) - 以前新兴威胁的规则集
* [Ransomware overview](https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml) - 勒索软件的概述列表
* [STIX - Structured Threat Information eXpression](http://stix.mitre.org/) - 通过标准化的语言来表示、共享网络威胁信息 [MITRE](http://mitre.org/) 相关:
* [CAPEC - 常见攻击模式枚举与分类](http://capec.mitre.org/)
* [CybOX - 网络观测 eXpression](http://cybox.mitre.org/)
* [MAEC - 恶意软件特征枚举与界定](http://maec.mitre.org/)
* [TAXII - 可信的指标信息自动化交换](http://taxii.mitre.org/)
* [threatRECON](https://threatrecon.co/) - 搜索指标，每月最多一千次
* [Yara rules](https://github.com/Yara-Rules/rules) - Yara 规则集
* [ZeuS Tracker](https://zeustracker.abuse.ch/blocklist.php) - ZeuS 黑名单

# 检测与分类

*反病毒和其他恶意软件识别工具*

* [AnalyzePE](https://github.com/hiddenillusion/AnalyzePE) - Windows PE 文件的分析器
* [chkrootkit](http://www.chkrootkit.org/) - 本地 Linux rootkit 检测
* [ClamAV](http://www.clamav.net/) - 开源反病毒引擎
* [Detect-It-Easy](https://github.com/horsicq/Detect-It-Easy) - 用于确定文件类型的程序
* [ExifTool](http://www.sno.phy.queensu.ca/~phil/exiftool/) - 读、写、编辑文件的元数据
* [File Scanning Framework](http://www.sno.phy.queensu.ca/~phil/exiftool/) - 模块化的递归文件扫描解决方案
* [hashdeep](https://github.com/jessek/hashdeep) - 用各种算法计算哈希值
* [Loki](https://github.com/Neo23x0/Loki) - 基于主机的 IOC 扫描器
* [Malfunction](https://github.com/Dynetics/Malfunction) - 在功能层面对恶意软件进行分类和比较
* [MASTIFF](https://github.com/KoreLogicSecurity/mastiff) - 静态分析框架
* [MultiScanner](https://github.com/MITRECND/multiscanner) - 模块化文件扫描/分析框架
* [nsrllookup](https://github.com/rjhansen/nsrllookup) - 查询 NIST's National Software Reference Library 数据库中哈希的工具
* [packerid](http://handlers.sans.org/jclausing/packerid.py) - 跨平台的 PEiD 的替代品
* [PEV](http://pev.sourceforge.net/) - 为正确分析可疑的二进制文件提供功能丰富工具的 PE 文件多平台分析工具集
* [Rootkit Hunter](http://rkhunter.sourceforge.net/) - 检测 Linux 的 rootkits
* [ssdeep](http://ssdeep.sourceforge.net/) - 计算模糊哈希值
* [totalhash.py](https://gist.github.com/malc0de/10270150) - 一个简单搜索[TotalHash.com](http://totalhash.com/) 数据库的 Python 脚本
* [TrID](http://mark0.net/soft-trid-e.html) - 文件识别
* [YARA](https://plusvic.github.io/yara/) - 分析师利用的模式识别工具
* [Yara rules generator](https://github.com/Neo23x0/yarGen) - 基于恶意样本生成 yara 规则，也包含避免误报的字符串数据库

# 在线扫描与沙盒

*基于 Web 的多反病毒引擎扫描器和恶意软件自动分析的沙盒*

* [APK Analyzer](https://www.apk-analyzer.net/) - APK 免费动态分析
* [AndroTotal](https://andrototal.org/) - 利用多个移动反病毒软件进行免费在线分析 App
* [AVCaesar](https://avcaesar.malware.lu/) - Malware.lu 在线扫描器和恶意软件集合
* [Cryptam](http://www.cryptam.com/) - 分析可疑的 Office 文档
* [Cuckoo Sandbox](http://cuckoosandbox.org/) - 开源、自主的沙盒和自动分析系统
* [cuckoo-modified](https://github.com/brad-accuvant/cuckoo-modified) - GPL 许可证的 Cuckoo 沙盒的修改版，由于法律原因作者没有将其分支合并
* [cuckoo-modified-api](https://github.com/brad-accuvant/cuckoo-modified) - 用于控制 cuckoo-modified 沙盒的 Python API
* [DeepViz](https://www.deepviz.com/) - 通过机器学习分类来分析的多格式文件分析器
* [detux](https://github.com/detuxsandbox/detux/) - 一个用于对 Linux 恶意软件流量分析与 IOC 信息捕获的沙盒
* [Document Analyzer](https://www.document-analyzer.net/) - DOC 和 PDF 文件的免费动态分析
* [DRAKVUF](https://github.com/tklengyel/drakvuf) - 动态恶意软件分析系统
* [File Analyzer](https://www.file-analyzer.net/) - 免费 PE 文件动态分析
* [firmware.re](http://firmware.re/) - 解包、扫描、分析绝大多数固件包
* [Hybrid Analysis](https://www.hybrid-analysis.com/) - 由 VxSandbox 支持的在线恶意软件分析工具
* [IRMA](http://irma.quarkslab.com/) - 异步、可定制的可疑文件分析平台
* [Joe Sandbox](https://www.joesecurity.org/) - 深度恶意软件分析
* [Jotti](https://virusscan.jotti.org/en) - 免费在线多反病毒引擎扫描器
* [Limon](https://github.com/monnappa22/Limon) - 分析 Linux 恶意软件的沙盒
* [Malheur](https://github.com/rieck/malheur) - 恶意行为的自动化沙盒分析
* [Malware config](https://malwareconfig.com/) - 从常见的恶意软件提取、解码和在线配置
* [Malwr](https://malwr.com/) - 免费的在线 Cuckoo 沙盒分析实例
* [MASTIFF Online](https://mastiff-online.korelogic.com/) - 在线恶意软件静态分析
* [Metadefender.com](https://www.metadefender.com/) - 扫描文件、哈希或恶意软件的 IP 地址
* [NetworkTotal](https://www.networktotal.com/index.html) - 一个分析 pcap 文件的服务，使用配置了 EmergingThreats Pro 的Suricata 快速检测病毒、蠕虫、木马和各种恶意软件
* [Noriben](https://github.com/Rurik/Noriben) - 使用 Sysinternals Procmon 收集恶意软件在沙盒环境下的进程信息
* [PDF Examiner](http://www.pdfexaminer.com/) - 收集可疑的 PDF 文件
* [ProcDot](http://www.procdot.com/) - 一个可视化恶意软件分析工具集
* [Recomposer](https://github.com/secretsquirrel/recomposer) - 安全上传二进制程序到沙盒网站的辅助脚本
* [Sand droid](http://sanddroid.xjtu.edu.cn/) - 自动化、完整的 Android 应用程序分析系统
* [SEE](https://github.com/F-Secure/see) - 在安全环境中构建测试自动化的框架
* [URL Analyzer](https://www.url-analyzer.net/) - 对 URL 文件的动态分析
* [VirusTotal](https://www.virustotal.com/) - 免费的在线恶意软件样本和 URL 分析
* [Visualize\_Logs](https://github.com/keithjjones/visualize_logs) - 用于日志的开源可视化库和命令行工具（Cuckoo、Procmon 等）
* [Zeltser's List](https://zeltser.com/automated-malware-analysis/) - Lenny Zeltser 创建的免费自动沙盒服务

# 域名分析

*检查域名和 IP 地址*

* [Desenmascara.me](http://desenmascara.me/) - 一键点击即可得到尽可能多的检索元数据以评估一个网站的信誉度
* [Dig](http://networking.ringofsaturn.com/) - 免费的在线 dig 以及其他网络工具
* [dnstwist](https://github.com/elceef/dnstwist) - 用于检测钓鱼网站和公司间谍活动的域名排名网站
* [IPinfo](https://github.com/hiddenillusion/IPinfo) - 通过搜索在线资源收集关于 IP 或 域名的信息
* [Machinae](https://github.com/hurricanelabs/machinae) - 类似 Automator 的 OSINT 工具，用于收集有关 URL、IP 或哈希的信息
* [mailchecker](https://github.com/FGRibreau/mailchecker) - 跨语言临时邮件检测库
* [MaltegoVT](https://github.com/michael-yip/MaltegoVT) - 让 Maltego 使用 VirusTotal API，允许搜索域名、IP 地址、文件哈希、报告
* [Multi rbl](http://multirbl.valli.org/) - 多个 DNS 黑名单，反向查找超过 300 个 RBL。
* [SenderBase](http://www.senderbase.org/) - 搜索 IP、域名或网络的所有者
* [SpamCop](https://www.spamcop.net/bl.shtml) - 垃圾邮件 IP 黑名单IP
* [SpamHaus](http://www.spamhaus.org/lookup/) - 基于域名和 IP 的黑名单
* [Sucuri SiteCheck](https://sitecheck.sucuri.net/) - 免费的网站恶意软件与安全扫描器
* [TekDefense Automator](http://www.tekdefense.com/automater/) - 收集关于 URL、IP 和哈希值的 OSINT 工具
* [URLQuery](http://urlquery.net/) - 免费的 URL 扫描器
* [Whois](http://whois.domaintools.com/) - DomainTools 家免费的 whois 搜索
* [Zeltser's List](https://zeltser.com/lookup-malicious-websites/) - 由 Lenny Zeltser 整理的免费在线恶意软件工具集
* [ZScalar Zulu](http://zulu.zscaler.com/) - Zulu URL 风险分析

# 浏览器恶意软件

*分析恶意 URL，也可以参考*[*domain analysis*](https://paper.seebug.org/421/#domain-analysis)*和*[*documents and shellcode*](https://paper.seebug.org/421/#documents-and-shellcode)*部分*

* [Firebug](http://getfirebug.com/) - Firefox Web 开发扩展
* [Java Decompiler](http://jd.benow.ca/) - 反编译并检查 Java 的应用
* [Java IDX Parser](https://github.com/Rurik/Java_IDX_Parser/) - 解析 Java IDX 缓存文件
* [JSDetox](http://www.relentless-coding.com/projects/jsdetox/) - JavaScript 恶意软件分析工具
* [jsunpack-n](https://github.com/urule99/jsunpack-n) - 一个 javascript 解压软件，可以模拟浏览器功能
* [Krakatau](https://github.com/Storyyeller/Krakatau) - Java 的反编译器、汇编器与反汇编器
* [Malzilla](http://malzilla.sourceforge.net/) - 分析恶意 Web 页面
* [RABCDAsm](https://github.com/CyberShadow/RABCDAsm) - 一个健壮的 ActionScript 字节码反汇编
* [swftools](http://www.swftools.org/) - PDF 转换成 SWF 的工具
* [xxxswf](http://hooked-on-mnemonics.blogspot.com/2011/12/xxxswfpy.html) - 分析 Flash 文件的 Python 脚本

文档和 Shellcode

*在 PDF、Office 文档中分析恶意 JS 和 Shellcode，也可参考[browser malware](https://paper.seebug.org/421/" \l "browser-malware) 部分*

* [AnalyzePDF](https://github.com/hiddenillusion/AnalyzePDF) - 分析 PDF 并尝试判断其是否是恶意文件的工具
* [box-js](https://github.com/CapacitorSet/box-js) - 用于研究 JavaScript 恶意软件的工具，支持 JScript/WScript 和 ActiveX 仿真功能
* [diStorm](http://www.ragestorm.net/distorm/) - 分析恶意 Shellcode 的反汇编器
* [JS Beautifier](http://jsbeautifier.org/) - JavaScript 脱壳和去混淆
* [JS Deobfuscator](http://www.kahusecurity.com/2015/new-javascript-deobfuscator-tool/)- 对那些使用 eval 或 document.write 的简单 Javascript 去混淆
* [libemu](http://libemu.carnivore.it/) - x86 shellcode 仿真的库和工具
* [malpdfobj](https://github.com/9b/malpdfobj) - 解构恶意 PDF 为 JSON 表示
* [OfficeMalScanner](http://www.reconstructer.org/code.html) - 扫描 MS Office 文档中的恶意跟踪
* [olevba](http://www.decalage.info/python/olevba) - 解析 OLE 和 OpenXML 文档，并提取有用信息的脚本
* [Origami PDF](https://code.google.com/p/origami-pdf/) - 一个分析恶意 PDF 的工具
* [PDF Tools](http://blog.didierstevens.com/programs/pdf-tools/) - Didier Stevens 开发的许多关于 PDF 的工具
* [PDF X-Ray Lite](https://github.com/9b/pdfxray_lite) - PDF 分析工具，PDF X-RAY 的无后端版本
* [peepdf](http://eternal-todo.com/tools/peepdf-pdf-analysis-tool) - 用来探索可能是恶意的 PDF 的 Python 工具
* [QuickSand](https://www.quicksand.io/) - QuickSand 是一个紧凑的 C 框架，用于分析可疑的恶意软件文档，以识别不同编码流中的漏洞，并定位和提取嵌入的可执行文件
* [Spidermonkey](https://developer.mozilla.org/en-US/docs/Mozilla/Projects/SpiderMonkey) - Mozilla 的 JavaScript 引擎，用来调试可疑 JS 代码

# 文件提取

*从硬盘和内存镜像中提取文件*

* [bulk\_extractor](https://github.com/simsong/bulk_extractor) - 快速文件提取工具
* [EVTXtract](https://github.com/williballenthin/EVTXtract) - 从原始二进制数据提取 Windows 事件日志文件
* [Foremost](http://foremost.sourceforge.net/) - 由 US Air Force 设计的文件提取工具
* [Hachoir](https://bitbucket.org/haypo/hachoir) - 处理二进制程序的 Python 库的集合
* [Scalpel](https://github.com/sleuthkit/scalpel) - 另一个数据提取工具

# 去混淆

*破解异或或其它代码混淆方法*

* [Balbuzard](https://bitbucket.org/decalage/balbuzard/wiki/Home) - 去除混淆(XOR、ROL等)的恶意软件分析工具
* [de4dot](https://github.com/0xd4d/de4dot) - .NET 去混淆与脱壳
* [ex\_pe\_xor](http://hooked-on-mnemonics.blogspot.com/2014/04/expexorpy.html) 和 [iheartxor](http://hooked-on-mnemonics.blogspot.com/p/iheartxor.html) - Alexander Hanel 开发的用于去除单字节异或编码的文件的两个工具
* [FLOSS](https://github.com/fireeye/flare-floss) - FireEye 实验室的混淆字符串求解工具，使用高级静态分析技术来自动去除恶意软件二进制文件中的字符串
* [NoMoreXOR](https://github.com/hiddenillusion/NoMoreXOR) - 通过频率分析来猜测一个 256 字节的异或密钥
* [PackerAttacker](https://github.com/BromiumLabs/PackerAttacker) - Windows 恶意软件的通用隐藏代码提取程序
* [unpacker](https://github.com/malwaremusings/unpacker/) - 基于 WinAppDbg 的自动 Windows 恶意软件脱壳器
* [unxor](https://github.com/tomchop/unxor/) - 通过已知明文攻击来猜测一个异或密钥
* [VirtualDeobfuscator](https://github.com/jnraber/VirtualDeobfuscator) - 虚拟逆向分析工具
* [XORBruteForcer](http://eternal-todo.com/var/scripts/xorbruteforcer) - 爆破单字节异或密钥的 Python 脚本
* [XORSearch 和 XORStrings](http://blog.didierstevens.com/programs/xorsearch/) - Didier Stevens 开发的用于寻找异或混淆后数据的两个工具
* [xortool](https://github.com/hellman/xortool) - 猜测异或密钥和密钥的长度

# 调试和逆向工程

*反编译器、调试器和其他静态、动态分析工具*

* [angr](https://github.com/angr/angr) - UCSB 的安全实验室开发的跨平台二进制分析框架
* [bamfdetect](https://github.com/bwall/bamfdetect) - 识别和提取奇迹人和其他恶意软件的信息
* [BAP](https://github.com/BinaryAnalysisPlatform/bap) - CMU 的安全实验室开发的跨平台开源二进制分析框架
* [BARF](https://github.com/programa-stic/barf-project) - 跨平台、开源二进制分析逆向框架
* [binnavi](https://github.com/google/binnavi) - 基于图形可视化的二进制分析 IDE
* [Binwalk](http://binwalk.org/) - 固件分析工具
* [Bokken](https://inguma.eu/projects/bokken) - Pyew 和 Radare 的界面版
* [Capstone](https://github.com/aquynh/capstone) - 二进制分析反汇编框架，支持多种架构和许多语言
* [codebro](https://github.com/hugsy/codebro) - 使用 clang 提供基础代码分析的 Web 端代码浏览器
* [dnSpy](https://github.com/0xd4d/dnSpy) - .NET 编辑器、编译器、调试器
* [Evan's Debugger (EDB)](http://codef00.com/projects#debugger) - Qt GUI 程序的模块化调试器
* [Fibratus](https://github.com/rabbitstack/fibratus) - 探索、跟踪 Windows 内核的工具
* [FPort](http://www.mcafee.com/us/downloads/free-tools/fport.aspx) - 实时查看系统中打开的 TCP/IP 和 UDP 端口，并映射到应用程序
* [GDB](http://www.sourceware.org/gdb/) - GNU 调试器
* [GEF](https://github.com/hugsy/gef) - 针对开发人员和逆向工程师的 GDB 增强版
* [hackers-grep](https://github.com/codypierce/hackers-grep) - 用来搜索 PE 程序中的导入表、导出表、字符串、调试符号
* [IDA Pro](https://www.hex-rays.com/products/ida/index.shtml) - Windows 反汇编和调试器，有免费评估版
* [Immunity Debugger](http://debugger.immunityinc.com/) - 带有 Python API 的恶意软件调试器
* [ltrace](http://ltrace.org/) - Linux 可执行文件的动态分析
* [objdump](https://en.wikipedia.org/wiki/Objdump) - GNU 工具集的一部分，面向 Linux 二进制程序的静态分析
* [OllyDbg](http://www.ollydbg.de/) - Windows 可执行程序汇编级调试器
* [PANDA](https://github.com/moyix/panda) - 动态分析平台
* [PEDA](https://github.com/longld/peda) - 基于 GDB 的 Pythton Exploit 开发辅助工具，增强显示及增强的命令
* [pestudio](https://winitor.com/) - Windows 可执行程序的静态分析
* [plasma](https://github.com/joelpx/plasma) - 面向 x86/ARM/MIPS 的交互式反汇编器
* [PPEE (puppy)](https://www.mzrst.com/) - 专业的 PE 文件资源管理器
* [Process Explorer](https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx)- 高级 Windows 任务管理器
* [Process Monitor](https://technet.microsoft.com/en-us/sysinternals/bb896645.aspx) - Windows 下高级程序监控工具
* [PSTools](https://technet.microsoft.com/en-us/sysinternals/pstools.aspx) - 可以帮助管理员实时管理系统的 Windows 命令行工具
* [Pyew](https://github.com/joxeankoret/pyew) - 恶意软件分析的 Python 工具
* [Radare2](http://www.radare.org/r/) - 带有调试器支持的逆向工程框架
* [RetDec](https://retdec.com/) - 可重定向的机器码反编译器，同时有在线反编译服务和 API
* [ROPMEMU](https://github.com/vrtadmin/ROPMEMU) - 分析、解析、反编译复杂的代码重用攻击的框架
* [SMRT](https://github.com/pidydx/SMRT) - Sublime 3 中辅助恶意软件分析的插件
* [strace](http://sourceforge.net/projects/strace/) - Linux 可执行文件的动态分析
* [Triton](http://triton.quarkslab.com/) - 一个动态二进制分析框架
* [Udis86](https://github.com/vmt/udis86) - x86 和 x86\_64 的反汇编库和工具
* [Vivisect](https://github.com/vivisect/vivisect) - 恶意软件分析的 Python 工具
* [X64dbg](https://github.com/x64dbg/) - Windows 的一个开源 x64/x32 调试器

# 网络

*分析网络交互*

* [Bro](https://www.bro.org/) - 支持惊人规模的文件和网络协议的协议分析工具
* [BroYara](https://github.com/hempnall/broyara) - 基于 Bro 的 Yara 规则集
* [CapTipper](https://github.com/omriher/CapTipper) - 恶意 HTTP 流量管理器
* [chopshop](https://github.com/MITRECND/chopshop) - 协议分析和解码框架
* [Fiddler](http://www.telerik.com/fiddler) - 专为 Web 调试开发的 Web 代理
* [Hale](https://github.com/pjlantz/Hale) - 僵尸网络 C&C 监视器
* [Haka](http://www.haka-security.org/) - 一个安全导向的开源语言，用于在实时流量捕获时描述协议、应用安全策略
* [INetSim](http://www.inetsim.org/) - 网络服务模拟。建设一个恶意软件分析实验室十分有用
* [Laika BOSS](https://github.com/lmco/laikaboss) - Laika BOSS 是一种以文件为中心的恶意软件分析和入侵检测系统
* [Malcom](https://github.com/tomchop/malcom) - 恶意软件通信分析仪
* [Maltrail](https://github.com/stamparm/maltrail) - 一个恶意流量检测系统，利用公开的黑名单来检测恶意和可疑的通信流量，带有一个报告和分析界面
* [mitmproxy](https://mitmproxy.org/) - 拦截网络流量通信
* [Moloch](https://github.com/aol/moloch) - IPv4 流量捕获，带有索引和数据库系统
* [NetworkMiner](http://www.netresec.com/?page=NetworkMiner) - 有免费版本的网络取证分析工具
* [ngrep](http://ngrep.sourceforge.net/) - 像 grep 一样收集网络流量
* [PcapViz](https://github.com/mateuszk87/PcapViz) - 网络拓扑与流量可视化
* [Tcpdump](http://www.tcpdump.org/) - 收集网络流
* [tcpick](http://tcpick.sourceforge.net/) - 从网络流量中重构 TCP 流
* [tcpxtract](http://tcpxtract.sourceforge.net/) - 从网络流量中提取文件
* [Wireshark](https://www.wireshark.org/) - 网络流量分析工具

# 内存取证

*在内存映像或正在运行的系统中分析恶意软件的工具*

* [BlackLight](https://www.blackbagtech.com/blacklight.html) - 支持 hiberfil、pagefile 与原始内存分析的 Windows / MacOS 取证客户端
* [DAMM](https://github.com/504ensicsLabs/DAMM) - 基于 Volatility 的内存中恶意软件的差异分析
* [evolve](https://github.com/JamesHabben/evolve) - 用于 Volatility Memory 取证框架的 Web 界面
* [FindAES](http://jessekornblum.livejournal.com/269749.html) - 在内存中寻找 AES 加密密钥
* [Muninn](https://github.com/ytisf/muninn) - 一个使用 Volatility 的自动化分析脚本，可以生成一份可读报告
* [Rekall](http://www.rekall-forensic.com/) - 内存分析框架，2013 年 Volatility 的分支版本
* [TotalRecall](https://github.com/sketchymoose/TotalRecall) - 基于 Volatility 自动执行多恶意样本分析任务的脚本
* [VolDiff](https://github.com/aim4r/VolDiff) - 在恶意软件执行前后，在内存映像中运行 Volatility 并生成对比报告
* [Volatility](https://github.com/volatilityfoundation/volatility) - 先进的内存取证框架
* [VolUtility](https://github.com/kevthehermit/VolUtility) - Volatility 内存分析框架的 Web 接口
* [WinDbg](https://msdn.microsoft.com/en-us/windows/hardware/hh852365) - Windows 系统的实时内存检查和内核调试工具

# Windows 神器

* [AChoir](https://github.com/OMENScan/AChoir) - 一个用来收集 Windows 实时事件响应脚本集
* [python-evt](https://github.com/williballenthin/python-evt) - 用来解析 Windows 事件日志的 Python 库
* [python-registry](http://www.williballenthin.com/registry/) - 用于解析注册表文件的 Python 库
* [RegRipper](https://regripper.wordpress.com/) ([GitHub](https://github.com/keydet89/RegRipper2.8)) - 基于插件集的工具

# 存储和工作流

* [Aleph](https://github.com/trendmicro/aleph) - 开源恶意软件分析管道系统
* [CRITs](https://crits.github.io/) - 关于威胁、恶意软件的合作研究
* [Malwarehouse](https://github.com/sroberts/malwarehouse) - 存储、标注与搜索恶意软件
* [Polichombr](https://github.com/ANSSI-FR/polichombr) - 一个恶意软件分析平台，旨在帮助分析师逆向恶意软件。
* [stoQ](http://stoq.punchcyber.com/) - 分布式内容分析框架，具有广泛的插件支持
* [Viper](http://viper.li/) - 分析人员的二进制管理和分析框架

# 杂项

* [al-khaser](https://github.com/LordNoteworthy/al-khaser) - 一个旨在突出反恶意软件系统的 PoC 恶意软件
* [Binarly](http://www.binar.ly/search) - 海量恶意软件字节的搜索引擎
* [DC3-MWCP](https://github.com/Defense-Cyber-Crime-Center/DC3-MWCP) - 反网络犯罪中心的恶意软件配置解析框架
* [MalSploitBase](https://github.com/misterch0c/malSploitBase) - 包含恶意软件利用的漏洞的数据库
* [Malware Museum](https://archive.org/details/malwaremuseum) - 收集 20 世纪八九十年代流行的恶意软件
* [Pafish](https://github.com/a0rtega/pafish) - Paranoid Fish，与恶意软件家族的行为一致，采用多种技术来检测沙盒和分析环境的演示工具
* [REMnux](https://remnux.org/) - 面向恶意软件逆向工程师和分析人员的 Linux 发行版和 Docker 镜像
* [Santoku Linux](https://santoku-linux.com/) - 移动取证的 Linux 发行版

# 资源

## 书籍

*基础恶意软件分析阅读书单*

* [Malware Analyst's Cookbook and DVD](https://amzn.com/dp/0470613033) - 打击恶意代码的工具和技术
* [Practical Malware Analysis](https://amzn.com/dp/1593272901) - 剖析恶意软件的手边书
* [Real Digital Forensics](https://www.amzn.com/dp/0321240693) - 计算机安全与应急响应
* [The Art of Memory Forensics](https://amzn.com/dp/1118825098) - 在 Windows、Linux 和 Mac 系统的内存中检测恶意软件和威胁
* [The IDA Pro Book](https://amzn.com/dp/1593272898) - 世界上最流行的反汇编器的非官方指南
* [Real Digital Forensics](https://amzn.com/dp/144962636X) - 用于移动取证、恶意软件分析的 Linux 发行版

## Twitter

*一些相关的 Twitter 账户*

* Adamb [@Hexacorn](https://twitter.com/Hexacorn)
* Andrew Case [@attrc](https://twitter.com/attrc)
* Binni Shah [@binitamshah](https://twitter.com/binitamshah)
* Claudio [@botherder](https://twitter.com/botherder)
* Dustin Webber [@mephux](https://twitter.com/mephux)
* Glenn [@hiddenillusion](https://twitter.com/hiddenillusion)
* jekil [@jekil](https://twitter.com/jekil)
* Jurriaan Bremer [@skier\_t](https://twitter.com/skier_t)
* Lenny Zeltser [@lennyzeltser](https://twitter.com/lennyzeltser)
* Liam Randall [@hectaman](https://twitter.com/hectaman)
* Mark Schloesser [@repmovsb](https://twitter.com/repmovsb)
* Michael Ligh (MHL) [@iMHLv2](https://twitter.com/iMHLv2)
* Monnappa [@monnappa22](https://twitter.com/monnappa22)
* Open Malware [@OpenMalware](https://twitter.com/OpenMalware)
* Richard Bejtlich [@taosecurity](https://twitter.com/taosecurity)
* Volatility [@volatility](https://twitter.com/volatility)

## 其它

* [APT Notes](https://github.com/kbandla/APTnotes) - 一个收集 APT 相关文献的合辑
* [File Formats posters](https://github.com/corkami/pics) - 常用文件格式的可视化（包括 PE 与 ELF）
* [Honeynet Project](http://honeynet.org/) - 蜜罐工具、论文和其他资源
* [Kernel Mode](http://www.kernelmode.info/forum/) - 一个致力于恶意软件分析和内核开发的活跃社区
* [Malicious Software](https://zeltser.com/malicious-software/) - Lenny Zeltser 的恶意软件博客和资源
* [Malware Analysis Search](https://cse.google.com/cse/home?cx=011750002002865445766%3Apc60zx1rliu) - [Corey Harrell](https://paper.seebug.org/421/journeyintoir.blogspot.com/) 自定义的用于恶意软件分析的 Google 搜索
* [Malware Analysis Tutorials](http://fumalwareanalysis.blogspot.nl/p/malware-analysis-tutorials-reverse.html) - 由 Xiang Fu 博士提供的恶意软件分析教程，是一个学习恶意软件分析的重要资源
* [Malware Samples and Traffic](http://malware-traffic-analysis.net/) - 此博客重点介绍与恶意软件感染相关的网络流量
* [Practical Malware Analysis Starter Kit](https://bluesoul.me/practical-malware-analysis-starter-kit/) - 此软件包包含 Practical Malware Analysis 书中引用的大多数软件
* [WindowsIR: Malware](http://windowsir.blogspot.com/p/malware.html) - Harlan Carvey 的恶意软件页面
* [/r/csirt\_tools](https://www.reddit.com/r/csirt_tools/) - CSIRT 工具和资源的子版块，讲[恶意软件分析](https://www.reddit.com/r/csirt_tools/search?q=flair%3A%22Malware%20analysis%22&sort=new&restrict_sr=on)的天才
* [/r/Malware](https://www.reddit.com/r/Malware) - 恶意软件的子版块
* [/r/ReverseEngineering](https://www.reddit.com/r/ReverseEngineering) - 逆向工程子版块，不仅限于恶意软件

## 相关 Awesome 清单

* [Android Security](https://github.com/ashishb/android-security-awesome)
* [AppSec](https://github.com/paragonie/awesome-appsec)
* [CTFs](https://github.com/apsdehal/awesome-ctf)
* [Forensics](https://github.com/Cugu/awesome-forensics)
* ["Hacking"](https://github.com/carpedm20/awesome-hacking)
* [Honeypots](https://github.com/paralax/awesome-honeypots)
* [Industrial Control System Security](https://github.com/hslatman/awesome-industrial-control-system-security)
* [Incident-Response](https://github.com/meirwah/awesome-incident-response)
* [Infosec](https://github.com/onlurking/awesome-infosec)
* [PCAP Tools](https://github.com/caesar0301/awesome-pcaptools)
* [Pentesting](https://github.com/enaqx/awesome-pentest)
* [Security](https://github.com/sbilly/awesome-security)
* [Threat Intelligence](https://github.com/hslatman/awesome-threat-intelligence)

转载来源：<https://paper.seebug.org/421/>