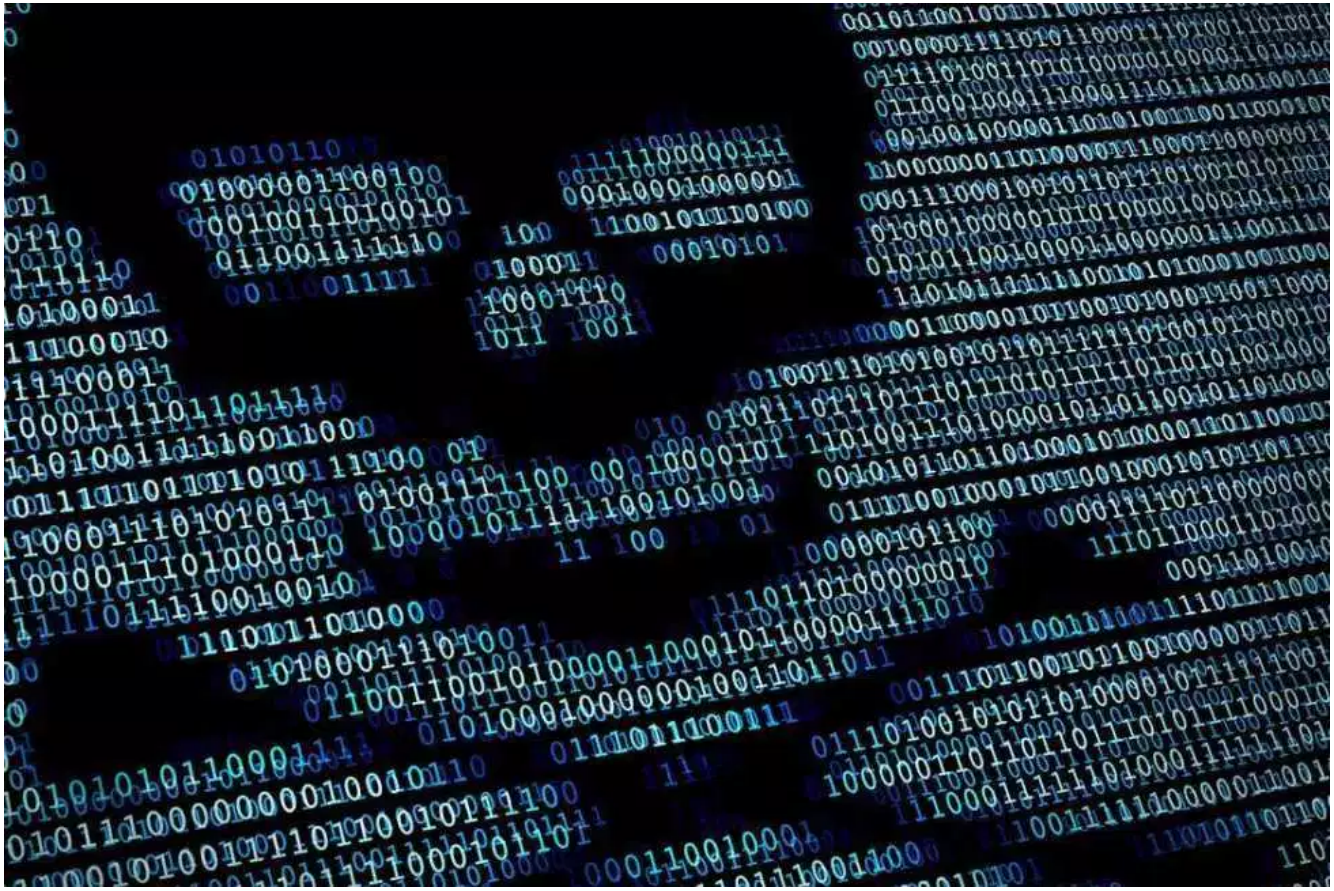
So Long, and Thanks for All the Fish

JUST SOME RANDOM THOUGHTS ABOUT THE MEANING OF LIFE, THE UNIVERSE, AND EVERYTHING

MENU



Malware analysis, my own list of tools and resources

Written by Andrea Fortuna • on August 5, 2016 • in Cybersecurity, Malware Analysis

RECENT POSTS

Reverse engineering and penetration testing on Android apps: my own list of tools

July 18, 2019

Elon Musk unveils Neuralink: tiny wires in the brain to read electrical pulses and let humans 'merge with computers'

July 17, 2019

Commando VM: a full Windows-based penetration testing virtual machine distribution

July 17, 2019

Zoom RCE vulnerability also affects RingCentral and Zhumu

July 16, 2019

A constantly updated list—Last update: August 2, 2018

During my daily activities of analysis and research, often I discover new useful tools.
I collected them in this list (periodically updated).

Enjoy!

Detection

- **AnalyzePE**—Wrapper for a variety of tools for reporting on Windows PE files.
- **chkrootkit**—Linux rootkit detector.
- **Rootkit Hunter**—Detect Linux rootkits.
- **Detect-It-Easy**—A program for determining types of files.
- **hashdeep**—Compute digest hashes with a variety of algorithms.
- **Loki**—Host based scanner for IOCs.
- **MASTIFF**—Static analysis framework.
- **MultiScanner**—Modular file scanning/analysis framework
- **nsrllookup**—A tool for looking up hashes in NIST's National Software Reference Library database.
- **PEV**—A multiplatform toolkit to work with PE files, providing feature-rich tools for proper analysis of suspicious binaries.
- **totalhash.py**—Python script for searching in **TotalHash.cymru.com** database.
- **TrID**—File identifier.
- **YARA**—Pattern matching tool for analysts.

Online scanners and sandboxes

- **NVISO ApkScan** — Dynamic analysis of APKs
- **APK Analyzer** — Dynamic analysis of APKs
- **AndroTotal** — Online analysis of APKs against multiple mobile antivirus apps
- **AVCaesar** — Online scanner and malware repository
- **Cryptam** — Analyze suspicious office documents
- **Cuckoo Sandbox** — Open source sandbox and automated analysis system
- **Malwr** — Free analysis with an online Cuckoo Sandbox instance
- **DeepViz** — Multi-format file analyzer with machine-learning classification
- **detux** — A sandbox developed to do traffic analysis of Linux malwares and capturing IOCs
- **Document Analyzer** — Analysis of DOC and PDF files
- **DRAKVUF** — Dynamic malware analysis system.
- **File Analyzer** — Free dynamic analysis of PE files
- **firmware.re** — Unpacks, scans and analyzes firmware packages
- **Hybrid Analysis** — Online malware analysis tool
- **IRMA** — An asynchronous and customizable analysis platform for suspicious files
- **Joe Sandbox** — Deep malware analysis.
- **Jotti** — Online AV scanner
- **Limon** — Sandbox for Analyzing Linux Malwares
- **Malheur** — Automatic sandboxed analysis of malware behavior
- **MASTIFF Online** — Online static malware analysis
- **Metadefender.com** — Scan a file, hash or IP address for malware
- **PDF Examiner** — Analyse suspicious PDF files

- **SEE**—"Sandboxed Execution Environment", a framework for building test automation in secured environments
- **URL Analyzer**—Dynamic analysis of URL files
- **VirusTotal**—Online analysis of malware samples and URLs
- **NoDistribute**—Scan files with over 35 anti-viruses. The results of the scans are never distributed.

Deobfuscation

- **Balbuzard**—Analysis tool for reversing obfuscation
- **de4dot**—.NET deobfuscator and unpacker
- **FLOSS**—Tool to automatically deobfuscate strings from malware binaries
- **NoMoreXOR**—Guess a 256 byte XOR key using frequency analysis
- **PackerAttacker**—Hidden code extractor for Windows malware
- **unpacker**—Automated malware unpacker for Windows malware
- **unxor**—Guess XOR keys using known-plaintext attacks
- **VirtualDeobfuscator**—Reverse engineering tool for virtualization wrappers
- **JS Beautifier**—JavaScript unpacking and deobfuscation
- **JS Deobfuscator**—Deobfuscation tool for Javascript
- **XORBruteForcer**—A Python script for brute forcing single-byte XOR keys

---

Reverse Engineering and Debugging

- **angr**—Platform-agnostic binary analysis framework
- **bamfdetect**—Identifies and extracts information from bots and malware

- **BARF** — Open source multiplatform Binary Analysis and Reverse engineering Framework.
- **binnavi** — Binary analysis IDE for reverse engineering
- **Capstone** — Disassembly framework for binary analysis and reversing
- **codebro** — Web based code browser with basic code analysis.
- **dnSpy** — .NET assembly editor, decompiler and debugger
- **Evan's Debugger (EDB)** — Modular debugger with a Qt GUI
- **Fibratus** — Windows kernel exploration and tracing tool
- **GDB** — The GNU debugger
- **GEF** — GDB Enhanced Features, for exploiters and reverse engineers
- **hackers-grep** — Uility to search for strings in PE executables
- **IDA Pro** — Windows disassembler and debugger
- **Immunity Debugger** — Debugger for malware analysis
- **ltrace** — Dynamic analysis tool for Linux executables
- **strace** — Dynamic analysis tool for Linux executables
- **objdump** — Static analysis tool for Linux binaries
- **OllyDbg** — Debugger for Windows executables
- **PANDA** — Platform for Architecture-Neutral Dynamic Analysis
- **PEDA** — Python Exploit Development Assistance for GDB
- **pestudio** — Static analysis tool for Windows executables
- **plasma** — Interactive disassembler for x86/ARM/MIPS
- **PPEE (puppy)** — PE file inspector.
- **Process Monitor** — Advanced monitoring tool for Windows programs
- **Pyew** — Python tool for malware analysis
- **Rdare2** — Reverse engineering framework

- **ROPMEMU**—Framework to analyze, dissect and decompile complex code-reuse attacks
- **SMRT**—Sublime Malware Research Tool, a plugin for Sublime Text 3 focused on malware analyis.
- **Triton**—A dynamic binary analysis (DBA) framework
- **Udis86**—Disassembler library and tools
- **Vivisect**—Python tool for malware analysis
- **X64dbg**—Debugger for windows

Memory Forensics

- **Volatility**—Advanced memory forensics framework.
- **DAMM**—Differential Analysis of Malware in Memory, built on Volatility
- **evolve**—Web interface for the Volatility Memory Forensics Framework
- **FindAES**—Find AES encryption keys in memory
- **Muninn**—A script to automate portions of analysis using Volatility, and create a readable report
- **Rekall**—Memory analysis framework (from a Volatility fork).
- **TotalRecall**—Script based on Volatility for automating various malware analysis tasks
- **WinDbg**—Kernel debugger for Windows systems

Packet Analysis

- **PacketTotal**—Online engine for analyzing **.pcap** files and visualizing the network traffic within, useful for malware analysis and incident response. **My review**

- **NetworkTotal**—Online analysis of pcap files to detect viruses, worms, trojans and malware.
- **Network Miner**—A Network Forensic Analysis Tool (NFAT) for Windows
- **Wireshark**—Widely-used network protocol analyzer.

Website Analysis

- **Desenmascara.me**—Tool to retrieve metadata from websites
- **Dig**—Online dig and other network tools
- **dnstwist**—Domain name permutation engine for detecting typo squatting, phishing and corporate espionage
- **IPinfo**—Gather information about an IP or domain by searching online resources
- **TekDefense Automator**—OSINT tool for gathering information about URLs, IPs, or hashes
- **Machinae**—OSINT tool for gathering information about URLs, IPs, or hashes
- **mailchecker**—Cross-language temporary email detection library
- **SenderBase**—Search for IP, domain or network owner
- **SpamCop**—IP based spam block list
- **SpamHaus**—Block list based on domains and IPs
- **Sucuri SiteCheck**—Website Malware and Security Scanner
- **URLQuery**—URL Scanner
- **Malzilla**—Analyze malicious web pages.
- **Whois**—DomainTools free online whois search
- **ZScalar Zulu**—Zulu URL Risk Analyzer
- **Firebug**—Firefox extension for web development.

- **Java Decompiler**—Decompile and inspect Java apps
- **Java IDX Parser**—Parses Java IDX cache files
- **JSDetox**—JavaScript malware analysis tool
- **jsunpack-n**—Javascript unpacker that emulates browser functionality
- **Krakatau**—Java decompiler, assembler, and disassembler
- **RABCDAsm**—ActionScript Bytecode Disassembler
- **swftools**—Adobe Flash decompiler.
- **xxxswf**—Analysis tool for Flash files
- **Spidermonkey**—Mozilla's JavaScript engine, for debugging malicious JS
- **PunkSpider**—Web application vulnerability search engine. **My review**

Resources

- **Practical Malware Analysis**—The Hands-On Guide to Dissecting Malicious Software.
- **The IDA Pro Book**—The Unofficial Guide to the World's Most Popular Disassembler.
- **The Art of Memory Forensics**—Detecting Malware and Threats in Windows, Linux, and Mac Memory
- **APT Notes**—A collection of papers related to Advanced Persistent Threats
- **File Formats posters**—Commonly used file format
- **Honeynet Project**—Honeypot tools, papers, and other resources
- **Kernel Mode** —Malware analysis and kernel development
- **Malware Analysis Search**—Custom Google search engine from **Corey Harrell**.
- **Malware Analysis Tutorials** —Malware Analysis Tutorials

- **Malware Samples and Traffic**—Blog focused on network traffic related to malware infections
- **WindowsIR: Malware**—Harlan Carvey's page on Malware
- **/r/csirt_tools**—Subreddit for CSIRT tools and resources, with a **malware analysis** flair
- **/r/Malware**—The malware subreddit
- **/r/ReverseEngineering**—Reverse engineering subreddit

Related posts

TAGS

CYBERSECURITY DFIR FORENSICS MALWARE ANALYSIS SECURITY TECHNOLOGY

PRINT

Andrea Fortuna

Are you looking for the ideal smartwatch? Do it yourself!

COMMENTS

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.