Unlocking Cybersecurity: Exploring Reverse-Engineering & Malware Analysis Tools

By Dimitar Kostadinov

Published: 2020-02-04 · Archived: 2026-10-25 02:44:13 UTC

Reverse-engineering and malware analysis tools have an important role to play in terms of cybersecurity. For example, app developers and security teams can implement these control mechanisms in their coding practices for detection of reverse-engineering attacks and protection against threat analytics, among other things. Finding the most appropriate tool is not always a simple task, but this article might shed some light on this subject.

In the first corner is the undisputed champion — the IDA, and in the other corner are all of its competitors.



Become a certified reverse engineer!

Get live, hands-on malware analysis training from anywhere, and become a Certified Reverse Engineering Analyst.

IDA

This abbreviation stands for Interactive Disassembler (IDA). There are two versions of IDA:

1. IDA Starter

2. IDA Professional

Hex-Rays, the company that develops IDA, offers also IDA Evaluation Version (a limited version of the disassembler) and the freeware version of IDA v7.0 (free for non-commercial use).

IDA Pro — the primary product — is an excellent tool for malware analysis because of many reasons, and one of them is its ability to extract great amounts of information such as strings, exports, imports, graph flows and more.

IDA Pro is a platform that integrates multiple functions: it can work as a disassembler, debugger and decompiler, all rolled into one.

As a disassembler for computer software, IDA Pro can use a given machine-executable code to generate assembly language source code. The disassembly process can be extended via "IDC scripts." They can be used as a basis for scripts written by users, but mostly for modifications of the generated code. Hex-Rays has equipped their product with an SDK so that users can develop extensions through the Python language.

As a debugger for executables, the IDA Pro supports Windows PE, Mac OS X Mach-O and Linux ELF.

The decompiler plug-in usually comes at an extra price.

IDA Pro can carry out an automatic code analysis based on cross-references between code sections, knowledge of parameters of API calls and other data. Yet not everything is automated — human intervention is needed to calibrate the otherwise natural process of disassembly. IDA Pro's interactive functionality is made for this purpose. As a rule of thumb, one should start with a disassembly listing that is automatically generated and then proceed with transforming code into data (and vice versa). Finally, additional information is to be included until the whole process provides clear results.

Note that upon loading each file, IDA Pro creates a database ("idb").

The main interface has numerous views and windows. For instance:

- A bar called the navigation band depicts how much memory space the binary has consumed
- A graph that illustrates functions

The Function window contains all functions that IDA Pro can perform. "Imports" is for the imported libraries.

When it performs the disassembly function, IDA Pro can work in both text and graph modes. While the text mode displays the entire disassembled program as if it has been mapped into memory, the graph mode shows a single function at a time by singling it out in order to display it into an interconnected block of code.

Users can find other views under View → Open Subviews.

Despite its great capabilities, IDA's high price is a deterrent to many people looking for a malware analysis/reverse engineering tool.

IDA alternatives

Hopper

This tool can work on Linux and macOS. Hopper is designed to decompile and debug 32/64-bit Intel Mac, Windows and iOS (ARM) executables.

Hopper comes with an SDK that allows users to extend features or write their own files. Additionally, most features can be invoked through Python scripts.

x64dbg

Another open-source debugger (x64/x32) for Windows.

Hiew

A disassembler preferred by hackers that can work under three modes: Text, Hexadecimal and Decode (disassembly).

ODA

With its impressive capabilities to support more than 60 architectures and file formats that exist on most popular operating systems and mobile platforms, this free web-based, reverse-engineering disassembler is definitely worth mentioning.

Binary Ninja

If you're looking for a simpler solution, Binary Ninja might be its name. This reverse-engineering tool can operate on Windows, macOS and Linux. Binary Ninja distinguishes itself from its market competitors with an uncomplicated interface in order to allow users perform a multithreaded analysis built on a custom IL that can easily adjust to different compilers, architectures and platforms.

For some reason, however, this tool is not very popular in the reverse-engineering community.

Ghidra

Ghidra is an NSA-sponsored (but free) open-source reverse-engineering platform that can carry out disassembly, assembly, decompilation, graphing and scripting on macOS, Windows and Linux. It is able to process instruction sets and executables that run in automated or interactive mode.

Ghidra can be customized by writing plugins/scripts that use Python or Java. According to Wesley McGrew, director of cyber operations at Horne Cyber, Ghidra "has a complete feature set, and has the best user interface in the market."

Be aware that Ghidra has some bugs that may allow hackers to execute code in vulnerable systems.

radare2

Radare2 is an open-source platform that can perform disassembly, debugging, analysis and manipulation of binary files. The disassembler and debuggers are local and remote.

This reverse engineering framework works on Windows (since XP), iOS, Linux, BSD, OSX, Android, Solaris and Haiku.

Radare2 provides users with a simple way to open multiple input/output sources (such as disks, network connections, kernel drivers, processes under debugging and so on) due to its advanced command-line interface that allows users to analyze data, compare data, patch binaries and programs, disassemble, search, replace and visualize. It can be scripted in Python, JavaScript, Go and more.

This project started as a forensic tool, so it can perform forensics on files and data carving.

Nevertheless, McGrew told TechBeacon that “[radare2 is] more difficult to use compared to Ghidra. That is because it is mostly a command-line-based program.”

In addition, compared to IDA Pro and x64dbg, radare2 does not automatically analyze the binary to reveal functions, code and data (since it does not execute any analysis at startup).

As IDA, radare2 has a command line but it can also run a graphical interface named Cutter, which is also a web interface. This function can visualize structures of a couple of file types.

Radare2 supports numerous architectures:

- architectures (x86{16,32,64}
- Dalvik
- avr
- ARM
- java
- PowerPC
- Sparc
- MIPS

All in all, this software recognizes 15 file formats (e.g., raw binary and WinRAR) and 33 instruction sets (Intel x86 and ARM).

Last but not least, unlike IDA Pro, radare2 is free.

Conclusion

"An IDA Pro license costs thousands and thousands of dollars, but it's worth it. It's a fantastic piece of software," McGrew said.

However, several tools challenge the leading position of IDA Pro. This is mostly because they can be ten times cheaper than the Hex-Rays product.

So for those of you who feel that the price of IDA Pro is just too much, don’t be disheartened — there are alternatives that are good enough.



Become a certified reverse engineer!

Get live, hands-on malware analysis training from anywhere, and become a Certified Reverse Engineering Analyst.

Sources

- Ghidra Explained: A Sophisticated Tool with Far-Reaching Implications, Horne Cyber
- Getting to know IDA Pro, Packt
- Getting started with IDA Pro, Peerlyst
- How to Perform Static Malware Analysis with Radare2, Peerlyst
- Intro to Radare2 for Malware Analysis, Malwology
- Interactive Disassembler, WikiZero
- Is there any disassembler to rival IDA Pro?, StackExchange
- radare2 – Reverse Engineering Framework, CyberPunk
- 9 Best Reverse Engineering Tools for 2019, Apriorit
- 7 tools that have influenced the reversing community, Detectify Labs

---

Source: http://resources.infosecinstitute.com/zeroaccess-malware-part-4-tracing-the-crimeware-origins-by-reversing-injected-code/