Hex-Rays IDA Pro and Decompiler

Enterprise IT Solutions (Hardware, Software, Services)
Shared Service and Outsourcing
Technology Products Distribution and Trading

Enterprise Solution
Professionals on Information and Network
Hex-Rays SA

Founded in 2005, privately held, Belgium based, Hex-Rays SA focuses on the binary software analysis technology development for the IT security market. The company’s two flagship product line IDA Pro and Hex-Rays Decompiler work hand in hand to provide malware analysis and reverse engineering (MARE) professionals, researchers and analysts with the industry de facto tools to perform their duties worldwide across enterprise, government and military sectors.

Mr. Guilfanov, the founder and CEO of Hex-Rays SA, holds a BSc in Mathematics from Moscow State University. He is the senior architect of several highly regarded software packages including the widely used IDA, a multi-platform, multi-processor, disassembler and debugger. Mr. Guilfanov is also known for having released, on 31 Dec 2005, a highly publicized unofficial fix for the Windows Metafile (WMF) vulnerability in Microsoft Windows operating system.

Products Overview: Hex-Rays Decompiler and IDA Pro

IDA is the Interactive DisAssembler: the world’s smartest and most feature-full multi processor disassembler and debugger, which many software security specialists are familiar with and highly regard as the industry de facto standard technology and tools. Written entirely in C++, IDA runs on the three major operating systems: Microsoft Windows, Mac OS X, and Linux.

IDA is also the solid foundation on which our second product, the Hex-Rays decompiler, is built. The unique Hex-Rays decompiler delivers on the promise of high level representation of binary executables. It can handle real world code. Hex-Rays Decompiler (a add on/plug in into IDA Pro) is a decompiler that transforms binary applications into a high level C-like pseudo code. Unlike disassemblers, which perform the same task at a lower level, the decompiler output is concise and closer to the way most programmers write applications. This alone can save hours of work because analysts easily map the disassembly output to high-level concepts. The decompiler frees them from this tedious and boring task. Since the decompiler output is similar to high level languages, one does not have to be an expert assembly language programmer to understand it.

E-SPIN and Hex-Rays SA

E-SPIN have actively in promoting Hex-Rays full range of products and technologies as part of the company Vulnerability Management solution portfolio. E-SPIN is active in provide consulting, supply, training and maintenance Hex-Rays products for the enterprise, government and military customers (or distribute and resell as part of the complete package) on the region E-SPIN do businesses. The enterprise range from university teaching reverse engineering to IT security professionals / analysts on the malware analysis or cyber/military defense applications.

Please feel free to contact E-SPIN for your inquiry and requirement, so we can assist you on the exact requirement in the packaged solutions that you may required for your operation or project needs.
IDA Pro

IDA Pro is the most regard and famous software analysis tool, which is a de facto standard in the software security industry, is an indispensable item in the toolbox of any serious software analyst and binary reverse engineer or malware analyst. Hex-Rays will continue to maintain IDA and ensure its continuous evolution along the years for the maintenance subscribed customers.

IDA Pro the official line is: IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment.
IDA Pro is a disassembler

IDA Pro is a disassembler, it use to explores binary programs, for which source code isn't always available, to create maps of their execution. The real interest of disassembler is that it shows the instructions that are actually executed by the processor in a symbolic representation called assembly language. If the friendly screen saver you have just installed is spying on your e-banking session or logging your e-mails, a disassembler can reveal it. However, assembly language is hard to make sense of. That's why advanced techniques have been implemented into IDA Pro to make that code more readable, in some cases, quite close to the original source code that produced the binary program. The map of the program's code then be post processed for further investigations. Some people have used it as the root of a genomic classification of viruses. (digital genome mapping – advanced malware analysis)

IDA Pro is a debugger

But, in real life, things aren't always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms and trojans are often armored and obfuscated. More powerful tools are required. The debugger in IDA Pro complements the static analysis capabilities of the disassembler: by allowing to single step through the code being investigated, the debugger often bypasses the obfuscation and helps obtain data that the more powerful static disassembler will be able to process in depth. IDA Pro can be used as a local and as a remote debugger on various platforms, including the ubiquitous 80x86 (typically windows/Linux) and the ARM platform (typically Windows CE PDAs) and other platforms. Remote debuggers are very useful when one wants to safely dissect potentially harmful programs. Some of IDA debuggers can run the application in a virtual environment: this makes malware analysis even safer.

IDA Pro is interactive

Because no computer can currently beat the human brain when it comes to exploring the unknown, IDA Pro is fully interactive. In sharp contrast with its predecessors, IDA always allows the human analyst to override its decisions or to provide hints. Interactivity culminates in a built-in programming language and an open plugin architecture.

IDA Pro is programmable

IDA Pro contains a complete development environment that consists of a very powerful macro-like language that can be used to automate simple to medium complexity tasks. For more advanced tasks, our open plugin architecture puts no limits on what external developers can do to enhance IDA Pro's functionality. One could, for example, extend IDA Pro with a MP3 player and make malware sing. However, we suspect our governmental customers are involved in more serious projects.
How is IDA Pro useful?

Hostile Code analysis
Given the speed and the complexity of today's hostile code, a powerful analysis solution is required. IDA Pro has become such a standard in the field of malware analysis that information about new viruses is often exchanged under the form of “IDA Databases”. The 2001 “CODE RED” incident is typical of what usually happens in the background. When eEye isolated a new worm whose payload targeted the White House's web site, IDA Pro was used to analyse and understand it: it helped the talented eEye analysts deliver a prompt and accurate warning of the impending attack. 24 hours a day, seven days a week, somewhere in the world, thanks to IDA Pro, anti-virus analysts investigate new virus samples and provide timely solutions.

Vulnerability research
IDA Pro is the ideal tool to investigate why software breaks. While the topic of vulnerability disclosure remains, more than ever, controversial, one cannot ignore the fact that software is unfortunately often vulnerable to outside attacks. It is, without any doubt, a bad idea to let vulnerabilities lurk in essential pieces of software: if they aren't fixed, they could very well be exploited by what we usually call “the bad guys”. The Wisconsin Safety Analyzer is a very interesting project investigating software vulnerability and tamper resistance where IDA Pro plays an important role.

COTS validation
A lot of software is now developed outside the country where it is used. Since programs are incredibly hard to verify, since complete source code audit and rebuilds aren't always practical tools such as IDA provide a convenient means to check if a program really does what it claims to do.

Privacy protection
Software is invading our lives at every level. In some cases, such as in what is known as the “Sony Rootkit” story, IDA Pro helps protect your essential rights.

Who are IDA Pro users?
Virtually all anti-virus companies, most vulnerability research companies, many of the large software development companies and, above everything else, three letter agencies and military organizations.
Hex-Rays Decompiler

Hex-Rays flagship product, the Hex-Rays Decompiler, which brings binary software analysis within reach of millions of programmers. It converts executable programs into a human readable C-like pseudocode text.

In comparison to low level assembly language, high level language representation in Hex-Rays has several advantages:

- concise: requires less time to read it
- structured: program logic is more obvious
- dynamic: variable names and types can be changed on the fly
- familiar: no need to learn the assembly language
- cool: the most advanced decompiler ever built!

The pseudocode text is generated on the fly. The technology is fast enough to analyze 99% of functions within a couple of seconds.

Currently the decompiler supports compiler generated code for the x86, x64, ARM32, ARM64, and PowerPC processors. Hex-Rays plan to port it to other platforms and add a programmatic API. This will allow customers to implement their own analysis methods. Vulnerability search, software validation, coverage analysis are the directions that immediately come to mind.

The decompiler runs on MS Windows, Linux, and Mac OS X. The GUI and text IDA versions are supported. In the text mode, only batch operation is available.
E-SPIN is the leading technology solution and outsourcing vendor in providing enterprise solutions consulting, buying facilitation, network and system integration, software development and customization, product training and certification testing, share service and outsourcing.

More information available at www.e-spincorp.com

Malaysia
No. 21-2, Jalan PJU 8/3B,
Perdana Business Centre,
Damansara Perdana
47820 Petaling Jaya, Selangor
Malaysia
Tel: +603 2168 3687 / +603 7728 2866

Hong Kong
Hong Kong Island
Room 1104, Crawford House, 70 Queen Road Central,
Central,
Hong Kong
Tel: +852 2165 4773, +852 8199 9799

Singapore
10 Anson Road
#18-17 International Plaza
Singapore 079903
Tel: +65 6223 2069 / +65 3158 2203

Indonesia
Office 8, Level 18-A, Jalan Jend Sudirman Kav. 52-53
Sudirman Central Business District (SCBD)
Jakarta Selatan
Daerah Khusus Ibukota Jakarta 12190
Indonesia
Tel: +6221 2960 8334

Thailand
195 Unit 4703, 47th Floor, Empire Tower,
South Sathorn Road, Yannawa, Sathorn, Bangkok 10120
Thailand
Tel: +66 60 002 4168

China
15/F L’Avenue,
99 Xianxia Road, Chang Ning District,
Shanghai 200051
China
Tel: +86 21 60577047

Philippines
Penthouse Level, Mvenue Building,
7844 Makati Avenue,
Makati City, Metro Manila,
1209 Philippines
Tel: +63 (2) 9170256