Hammerhead

Compile-Time Binary Variant Generator

Assured Information Security · 315.336.3306 · **WWW.AINFOSEC.COM**

ais

Hammerhead

Compile-Time Binary Variant Generator

OVERVIEW

Hammerhead is a compile-time obfuscation tool that aids in creating diversified binaries through manipulation of source and assembly instructions during compilation. Hammerhead uses a blend of open and closed source techniques, called transformations, to create semantically equivalent but syntactically different programs and thus change binary signatures.

How It Works

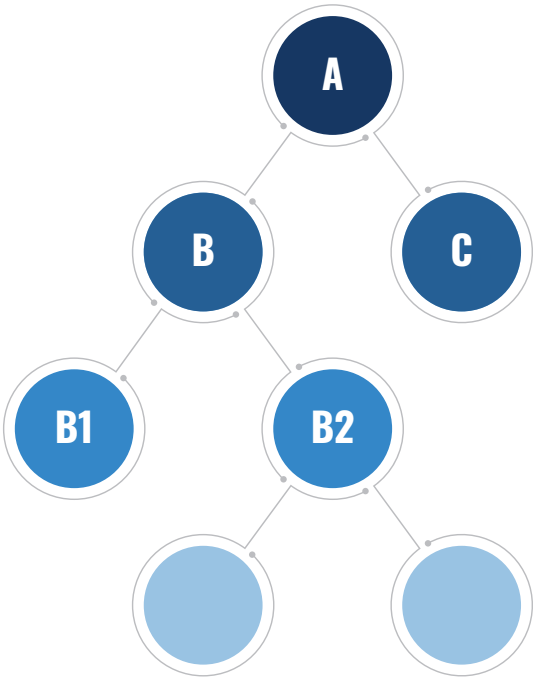
The Hammerhead platform generates binary variants through a model free reinforcement learning algorithm. Developers may specify desired parameters for maximum growth, similarity and number of desired variants to control the algorithm. Hammerhead provides an API for measuring similarity of variants to drive the learning algorithm.

General Facts

- Based on open-source Clang and LLVM (low-level virtual machine) compilers
- Works with C/C++ source code
- Supports x86, X64, MIPS, ARM and PowerPC architectures
- Final compilation supports GCC, Visual Studio, MinGW and embedded system toolchains
- Can be installed on Linux or Windows operating systems
- Provides plugins for similarity measurement using Bindiff/IDA, Bindiff/Ghidra and Radare2
- Machine Learning is used to determine which binaries are most dissimilar based on the requested number of variants

KEY FEATURES

- Compile-time obfuscation tool
- Creates diversified binaries
- Open & closed source techniques
- Changes binary signatures



FOR MORE INFORMATION

bd@ainfosec.com

Assured Information Security
315.336.3306
WWW.AINFOSEC.COM

About Assured Information Security (AIS)

AIS provides critical cyber and information security services, products and operations to commercial and government customers. Founded in 2001 and headquartered in Rome, New York, AIS has multiple operating locations and employees throughout the United States.