- **Course Name :** CodeNext – Malware Development Advanced Program CN103
- **Course Duration :** 120 Days
- **Course Fee :** INR 30,000/participant

- ✓ **Platform:** Windows 7, Linux
- ✓ **Tools (Windows):** Microsoft Visual Studio 2013, Debugging Tools for Windows
- ✓ **Tools (Linux):** GNU C Compiler, NASM Assembler, GNU C++ Compiler, GNU Debugger, Any suitable C++ IDE for Linux
- ✓ **Pre-requisites:** CodeNext-Malware Development Beginner & Intermediate Program CN101 & CN102
- ✓ **Project Work:** Projects will be developed by a group of 3-4 people during the course. Projects will range from pure theoretical work to development of a proof of concept malware technique(s).
- ✓ **Course Module:**

1. **Rootkits**
   a. Introduction to Rootkits
   b. Common Uses of Rootkits
   c. Preparing for Kernel Level Programming
      i. Setting up The Kernel Source Tree
      ii. Creating a Basic Template
   d. Thumb Rules of Kernel Mode Programming
   e. Loadable Kernel Modules
   f. "Hello, Kernel"
      i. The Code Layout
      ii. Inserting the LKM
      iii. Where did my output go?
      iv. Removing the LKM
   g. Virtual Devices

i. Devices in /dev
ii. Devices in /proc
iii. Devices in debugfs

h. Read/Write to Virtual Device
i. Read/Write to device in /dev
ii. Read/Write to device in /proc

i. Syscalls
j. **Practical Stuff:** Hooking the syscalls
k. **Practical Stuff:** Having Fun with Rootkits

2. Introduction to Assembly

a. Assembly Programming with NASM

3. Self-Modifying Codes

a. Self-Modifying Codes
b. Classification of Self Modifying Codes
i. Polymorphic Code
ii. Oligomorphic Code
iii. Metamorphic Code
c. Mutation Engines
d. Position Independent Codes
i. Writing "Hello World" the position Independent Way
ii. Executing Raw Machine Bytes
iii. **Practical Stuff:** Writing a basic Mutation Engine