- **Course Name :** CodeNext – Malware Development Beginner Program CN101
- **Course Duration :** 45 Days
- **Course Fee :** INR 12,000/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:** Basic knowledge of C & C++ is required.

✓ **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. **Introduction to Malware**
   a. Computer Malware
   b. Computer Virology
      i. Virology: Art of Writing a Malware
      ii. Cryptovirology: Cryptography in hands of a hacker
      iii. Kleptography: Art of data theft
   c. Classification of Computer Malware

2. **Introduction to Virology**
   a. Formal Definition of Computer Virus
   b. Self-Replicating Codes
   c. Parts of a Computer Virus
      i. Target Hunting
      ii. Self-Replication Mechanisms
      iii. Infection Mechanisms


**Corporate Office:** 3rd Floor, 26 Pusa Road, Adjoint Karol Bagh Metro Station Gate No. 4, New Delhi, India
**Email:** rahul@ignitetechnologies.in **Contact No.:** +91-9599387842,
**Website:** www.ignitetechnologies.in www.rmar.in

- d. Writing a "Hello World" Virus

**3. C and C++ Revisited**

- a. What They Don't Teach You
  - **i.** Variable Declarations
    - **1.** Data Types
      - **a.** What happens behind the curtains?
    - **2.** Conditional and Loops
      - **a.** If…else
      - **b.** Switch
      - **c.** Loop Constructs
      - **d.** What happens behind the curtains?
    - **3.** Function Calls
      - **a.** Function calls without parameters
      - **b.** Function Parameters
        - **i.** Call by value
        - **ii.** Call by reference
      - **c.** What happens behind the curtains?
      - **d.** Calling conventions
    - **4.** Pointers
    - **5.** Functions

**4. Dynamic Link Libraries and Shared Objects**

- a. Dynamic Link Libraries (DLL)
  - **i.** Why DLL?
  - **ii.** Creating a "Hello World" DLL
  - **iii.** Consuming a DLL in C++
  - **iv.** DLL Hijacking
- b. Shared Objects
  - **i.** Creating Shared Object

ii. Consuming Shared Object
iii. Shared Object Hijacking

c. **Practical Stuff:** Injecting malware in programs

5. **Art of Interception**
   a. Intercepting Function Calls
      i. Using LD_PRELOAD
      ii. Using memory hot-patching
      iii. Using Software breakpoints
      iv. Using SHE Hooking
   b. **Parameter Poisoning in Function Calls**
   c. **Practical Stuff:** Spying on other Programs

6. **Art of Interception 2**
   a. Intercepting Events
      i. Intercepting Keyboard Events
      ii. Intercepting Mouse Events
   b. **Practical Stuff:** Creating a keylogger
   c. **Practical Stuff:** Creating a mouse logger
   d. **Practical Stuff:** Controlling the apps from Malware