

Advanced Malware Analysis Using Responder™ Professional (3-day Instructor-led Course)

This hands-on course provides a challenging and deep level of understanding through using HBGary Responder Professional and HBGary REcon to discover methods used by malware authors to inject code into running processes, detect and reverse-engineer backdoor implants, reverse-engineer drivers and Botnets, and assess the capabilities of virtual machine-based obfuscation techniques used by malware authors. The course concludes with a capture the flag (CTF) team competition, that encompasses the skills and techniques taught during both the Basic and Advanced Malware Analysis courses.

CPE Credits: 24

Level: Advanced

Prerequisites:

- Successfully completed the Basic Malware Analysis Using Responder Professional (3-day Instructor-led Course)
- Minimum of 2-year of computer forensics, or 1-year network intrusion investigation experience
- Minimum of 1-year software reverse-engineering experience
- Minimum of 1-year Assembly Language experience

Course Objectives:

By the end of the course, students will be able to:

- Describe methods malware authors use to inject code
- Examine backdoor implants
- Discover backdoor commonalities, as well as unique traits
- Reverse-engineer drivers and identify their capabilities
- Analyze virtual machine obfuscation
- Use REcon and Responder Pro to analyze code injection techniques, identify backdoor program capabilities, reverse engineer malicious Windows drivers, and analyze virtual machine obfuscation techniques

Course Outline:

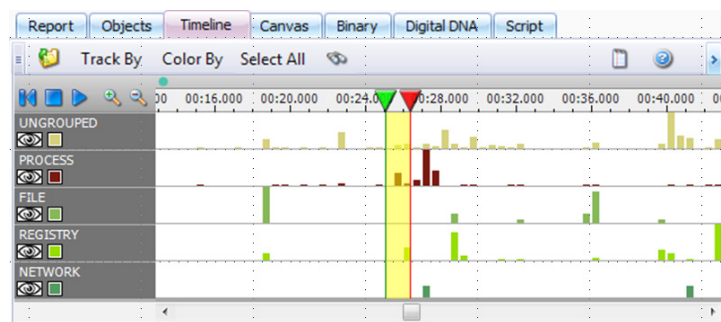
Day 1

Code Injection: Beyond the Basics – Most modern malware used in advanced attacks use some form of code injection. Upon successful completion of this module, students will:

- discover methods that malware authors use to inject code into running processes
- use REcon and Responder Pro to identify samples that use code injection techniques

Reversing Backdoors - Zero-days are hard to come by, which is why attackers only want to compromise a machine once. Attackers install a backdoor so they can come back at will, without having to re-exploit the machine. Upon successful completion of this module, students will:

- examine backdoor implants used by malicious actors
- discover what backdoors share in common, and what makes a very few unique
- use REcon and Responder Pro to identify capabilities in backdoor programs



Day 2

Reversing Drivers – Attackers use Windows device drivers to hide deep in the kernel and avoid detection. Upon successful completion of this module, students will:

- develop a background in Windows driver development to successfully reverse engineer drivers, and identify capabilities
- use REcon and Responder Pro to reverse engineer malicious Windows drivers used in recent attacks

Reversing Bots – Botnets are a huge threat in the modern cyber-landscape, with some botnets having more than 100,000 zombies. With numbers that large, students are likely to deal with bot software in incident response sooner or later. Upon successful completion of this module, students will use REcon and Responder Pro to identify bot software, assess key capabilities, and extract key information to mitigate specific bot attacks in the enterprise.

Day 3

Protected malware (virtual machine based obfuscation) – Some top-of-the-line malware uses virtual machine-based obfuscation to make the reverse engineer's job much more difficult. While this incurs a performance penalty, attackers are using your processor cycles (they don't care). Upon successful completion of this module, students will learn how virtual machine obfuscation works and how to assess some capabilities using REcon and Responder Pro.

Guided reverse engineering of suspect binaries (CTF) - Students will use REcon and Responder Pro to analyze suspect binaries in an instructor proctored environment. Most labs in the course are written with step-by-step instructions. CTF labs questions are written as open-ended questions without specific instructions, allowing students to test their comprehension of the material, while still having an instructor present to address specific questions on the material. Students may also bring their own malware (executables, livebins, or memory images) to work on in the instructor proctored environment during this period.

