800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Behavioral Malware Analysis Training

Applied Technology Academy

Behavioral Malware Analysis teaches you all the fundamental skills necessary to analyze malicious software from a behavioral perspective. Using system monitoring tools and analytic software, this course teaches how to observe malware in a controlled environment to quickly analyze its malicious effects to the system. From simple keyloggers to massive botnets this class covers a wide variety of current threats from today's Internet with actual samples being analyzed in the training environment. With the majority of the class being hands-on, each student will be issued a computer with a secure environment to learn the skills and essential methodologies.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: Networking TCP/IP**	**$90,103**	**Yes**

Course Overview

Using system monitoring tools and analytic software, you will analyze real-world malware samples in a training environment, giving you hands-on experience building secure lab environments, classifying malware, analyzing behavioral characteristics and their effects to systems, and documenting your findings. You will leave the course with the skills and abilities required to be an effective malware analyst.

After successfully completing this course, students will be able to:

- Set up a secure lab environment in which to analyze malicious software
- Build and maintain a tool set of freely available, trusted tools
- Classify different types of malware and describe their capabilities
- Analyze malware samples of varying types to ascertain their specific behavioral characteristics and their impact on a system
- Determine if a given sample is persistent and, if so, identify and remediate the persistence mechanism(s)
- Identify when a sample is aware of its virtual environment and will require more advanced static or dynamic analysis
- Get Practical Experience That Well Over 95% Of Behavioral Malware Analysis Job Openings Require.

Our training doesn't consist of a set of video lectures followed by unguided work assignments, as is the case with all other Assembly for Reverse Engineers (Classroom) training programs.

Instead, our proprietary Artificial Intelligence-based training platform delivers you bite-sized knowledge that is immediately followed by hands-on exercises, during which the platform watches your every step and helps you with contextual help, hints, and templates, as needed; and you have a personal tutor and coach who help you every step of the way.

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Course Outline

- Malware Analysis
- Static Analysis
- Dynamic/Behavioral Analysis
- Malware Overview
- Definition Of Malware
- Malware Intentions And Motivations
- Malware Types
- Virus
- Worm
- Backdoor
- Trojan
- Malicious Mobile Code
- User-Mode Rootkit
- Kernel-Mode Rootkit
- Combination Malware
- Vulnerabilities
- Malware Threats Research Websites
- Technologies To Fight Malware And Their Limitations
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Anti-Virus Software
- Windows Internals
- Windows Api
- 64-Bit Windows Internals
- Windows Internals Key Components
- Process Monitor And Api
- Building Analysis Environment
- Virtualization
- Vm Snapshots
- Behavioral Analysis Process
- *Initial Autopsy
- *Tool Setup And Startup
- *Malware Execution, Interaction, And Termination
- *Tool Termination

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- *System Log Walkthrough
- *Consolidate Log Reports And Review Findings
- Ba Tools Of The Trade
- Vmware Workstation
- Sysinternals Suite
- Regshot
- Apatedns & Fakenet
- Wireshark
- Peid & Packerbreaker
- Process Hacker
- Lab Exercises
- Ba Process Labs
- Baselining
- Why Baseline A System
- The Windows Registry
- Baselining Tools
- Document-Embedded Malware
- How To Embed A Document
- Hijack Scenario
- Macro Viruses
- Melissa Virus Case Study
- Lab Exercise
- Macro Viruses
- Adware, Spyware, And Ransomware
- Lab Exercise
- Spyware And Ransomware
- Botnet Malware
- Definition Of A Bot
- Botnet Communication Architecture
- Setting Up And Using Irc For Command And Control
- Lab Exercise
- Botnet Malware
- Keyloggers
- Purposes
- Keylogger Types
- Hardware Vs Software

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Remote Access Keyloggers
- Sniffers
- Lab Exercise
- Keylogger Detection
- Malicious Mobile Code (Interactive Web Apps)
- Definition Of Malicious Mobile Code
- Attack Vectors
- Reducing Risk Of Mmc Attacks
- Lab Exercise
- Drive By Download
- Backdoors
- Common Backdoor Types
- Propagation Methods
- Persistence Methods
- Finding Backdoors
- Lab Exercise
- Backdoor
- Trojan Horses
- Definition Of A Trojan Horse
- Backdoor Vs Trojan Horse
- Trojan Horse Infection Methods
- Lab Exercise
- Trojan Horses
- Advanced Persistent Threat (Apt)
- Definition Of Apt
- User-Mode Rootkits
- Definition Of A Rootkit
- Benefit Of Rootkits For Attackers
- Kernel- Vs User-Mode Rootkits
- Detection Methods
- Drop And Execute Malware
- Dropper Vs Injector
- Lab Exercise
- Drop And Execute Malware
- Vmware Detection
- Why Malware Does Vmware Detection

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Honeynets And Honeypots
- Methods Of Vm Detection
- Lab Exercise
- Analysis Detection And Destructive Malware
- Chm Malware
- Normal Chm File Usage
- Advantages And Disadvantages Of Chm Files
- Lab Exercise
- Chm Malware
- Pdf Malware
- Lab Exercise
- Pdf Malware
- Kernel-Mode Rootkits
- Benefits For Hackers
- Disadvantages
- Security And Rootkits
- Hypervisor Rootkits
- Bootkits

Intended Audience

- Threat operation analysts seeking a better understanding of malware
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious software
- Individuals who have experimented with malware analysis and want to expand their malware analysis techniques and methodologies
- Vulnerability Researchers who need to analyze the security of applications

Prerequisites

- Successful completion of Understanding Operating Systems
- or equivalent knowledge of operating system internals
- Experience with C programming in a Windows environment
- Experience with VMware software is an advantage, although not required

Follow-On Courses

- Network Forensics and Investigation I
- Network Forensics and Investigation II

- Endpoint Live Forensics
- Certified Network Defender

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.