Forensic Investigator, Part 06 of 10: Malware Forensics

Meet the expert: David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

Prerequisites: Recommended:
Understanding of networking; How data flows from source and destination
Computer security basics such as passwords, encryption and physical security
Basic understanding of computing and computer systems
Experience with various operating systems

Runtime: 57:39

Course description: When was the last time you scanned your system for problems? Did you find anything during a scan? Malware is a serious problem for end systems and networks in general. We are going to look at malware types like rootkits, viruses and Trojans and how we might become compromised. Once we find the malicious software, we as investigators need to know how to analyze the data. We have to ask ourselves are we doing a static or dynamic analysis on the malware. Static versus dynamic, or maybe both, will be a necessary part of our investigation. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Malware
- Introduction
- Malware Forensics
- Malware Parts
- Malware, Virus
- Malware, Trojan
- Malware, Worm
- Malware, Rootkit
- Malware, Ransomware
- Summary

Static Analysis
- Introduction
- Malware Analysis
- Other Malware Analysis Tools
- Static Anlysis
- Static Analysis Techniques
- Statistical Analysis Techniques, Continued
- Summary

Dynamic Analysis
- Introduction
- Dynamic Analysis
- Dynamic Analysis Techniques, Registry Monitors
- Registry Monitoring
- Dynamic Analysis Techiques, Process Monitors
- Dynamic Analysis Techniques, Port Monitors
- Dyamic Analysis Techniques, Network Sniffers
- Wireshark
- Dynamic Analysis Techniques, Mo
- Network or Internet Simulators
- Summary