MALWARE ANALYSIS & DETECTION ENGINEERING

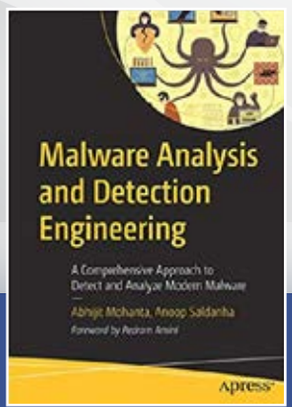
14-17 FEBRUARY 2022 LIVE VIRTUAL TRAINING

Malware analysis and detection engineering are powerful analysis and investigative techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centres, private and public organizations, detecting, responding and investigating such intrusions are essential to information security professionals. Malware analysis have become a must-have skill for fighting advanced malwares, targeted attacks and security breaches.

This hands-on training conducted teaches the concepts, tools, and techniques to analyse, investigate and hunt malwares with the analysis and investigation of various real-world malware samples and infected memory images and contains hands-on labs to gain a better understanding of the subject with successful malware experts

COURSE TRAINERS

Anoop Saldanha is one of the Core-Developers of Suricata Next-Gen Open Source Intrusion Detection & Prevention System, funded by the US Department of Homeland Security and US Navy' Space and Naval Warfare Systems. He has over 13 years of experience in cybersecurity industry & has worked on malware sandbox and IDS development. Anoop holds 9 patents pending in the field of malware analysis and network security.
Abhijit Mohanta has 13+ years of experience in the anti-malware industry and currently works as Senior malware Researcher at Uptycs.". He has several patents, blogs and has presented in well-known security conferences. He has worked in Malware Research labs of well-known organizations which includes Mcafee, Symantec and Juniper Networks. Abhijit specializes in the area of Reverse Engineering, Malware Detection, Vulnerability and Exploit Research. They authored the highly rated book titled "Malware Analysis & Detection Engineering".



Early Bird Participants will receive a copy of the handbook **"Malware Analysis & Detection Engineering"**

4-Day Training provides a hands-on approach to learning how to analyze malware samples with the following skills:

- How to create an isolated lab environment for malware analysis.
- Understand & learn various fundamental OS related concepts specific to malware analysis and advanced topics: file formats, internals of PE File formats, Virtual Memory and dissecting it using various memory analysis tools, Win32 APIs etc.
- Gauge the various components of malware packing & packers, persistence, network CnC, code injection and process hollowing, stealth and rootkits plus learn to identify and dissect these malware components using various static and dynamic analysis techniques.
- Hands-on case-studies, allowing delegates to test the concepts previously learned in malware components, performing both static and dynamic analysis of malwares.
- Study & analyse and dissect Maldocs, including MS Office document and excel malwares, the currently most popular form of malwares used by attackers to infect victims.
- Learn about other types of malwares including Scripting and Fileless malwares.
- Master Memory Forensics and its use for digital forensics
- Discover how to extract a memory dump of a system for the purpose of memory forensics and use the popular open source memory forensic tool Volatility to dissect the memory dump for IoCs.
- Get introduced to using popular debuggers like IDA Pro, Ollydbg and x64dbg.
- Learn to write signatures using Yara, the swiss army knife for analysts & to build a malware signature database to detect malwares both statically and dynamically.

Organised by: THOMVELL international