HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE ONLINE COURSE

M 10

A two day course in English ONLINE

Analysis of Malware by Reverse Engineering

Your trainer is Dr. Baptiste David

The workshop is in English. As the speaker´s mother tongue is French, in-company trainings can also be held in the French language. Our workshops take place online. In-company presentations are possible against surcharge. A workshop particpation is possible from any PC/lap top with a stable internet connection.
You don´t need additional software. An up-to-date browser is sufficient (current Microsoft Edge, Google Chrome or Firefox). Access to the training lab will also take place via your browser. Exercises can be implemented without additional software. The workshop will of course be transmitted live from the ERNW studio. The workshop material as well as possible demos and of course the trainer are always visible and will be shown depending on the requirements or will be emphasized. We will provide the training material electronically before the start of the course. The trainer will answer questions live. The microfone and/or camera are optional. You can also ask questions via chat.

Course Description

This training is about the analysis of malware by reverse-engineering. When automatic analysis tools can no longer work as expected (malware escaping their analysis environment, unknown threat, need to answer specific questions...), it becomes necessary to analyze the malware manually. Therefore, we offer an initiation training for malware analysis going from a novice level to an initiated one. For the sake of understanding, malware analysis is done at pseudo code level with a Windows-API focus approach.
The first part of the course focuses on the technical and conceptual presentation of the different forms of malware threats, from historical viruses to the most recent and modern ones. The purpose of this part is to cover the different technologies used by malware to propagate or execute itself as well as to cover their malicious nature through numerous examples. This approach aims to better understand the threat to analyze it more efficiently.
The second part of the course focuses on the practical application of the previously learned concepts presented through a series of practical exercises and it ends with an operational real case study. For this purpose, analyze will be driven by practicing reverse engineering at a pseudo-code level, close to C/C++ programming. The goal is to be able to understand simple malware in an efficient way and to be able to identify some malware threat intelligence elements. In the end of the training, an unpublished and special crafted for this training malware will be provided to the participant.
Note that the content of this training is mainly focused on the Windows operating system (since a large part of the threat is there) but it also presents threats in the Linux environment. In fact, the most important is to understand the algorithms used by malware and how to find them via reverse engineering before focusing on the specifics of a given technique or an operating system.
In the end, all participants will have a better understanding of what is possible and of what is not possible in the field of malware, through a didactic and practical introduction to reverse engineering, based on relatively simple but particularly representative examples. The participants will have the opportunity to expand their knowledge of malware and associated threats by observing technical details from more than ten different types of malwares over two intensive days.

03 – 04 May 2023 – online Workshop

Various institutions will acknowledge this course as a re-certification measure.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

Analysis of Malware by Reverse Engineering

A two day course in English

M 10

Course Agenda

Day 1

Introduction to malware

- Basic concept definition: program, virus, worm, malware, antivirus software …
- Technical refresher on the operating system
  - Microsoft & Posix API
  - Useful API: File, Network, Crypto, Process, …
- Computer virus Fundamentals
  - Life cycles of a virus
  - Different kinds of virus
- Malware and technical description illustrated with real cases
  - Trojan / RAT
  - Spyware / Adware
  - Worms / Bots
  - Rootkits
  - Keyloggers
  - Ransomware / Wiper
- Other technologies used by malware
  - Polymorphism and packer software
  - Fileless Malware & reinfection
  - Script malware (VBScript, PowerShell, other)
- Presentation of a secure analysis environment for malware
  - Introduction to sandboxing environment
  - Tooling for malware analysis
- Conclusion & practice
  - IDA: analysis of simple samples

Day 2

Exercises and practice

Exercises with malware samples:

- WannaCry: Ransomware (2017) by exploiting a vulnerability (EternalBlue) leaked from the NSA.
- NotPetya: Ransomware/Wiper (2017) infected hundreds of thousands computer in the world by reusing the EternalBlue vulnerability.
- German Parliament: RAT (2015) targeting German institution that might be of Russian origin.

Workshop:

- Full analysis of an unknown malware (for half a day)
  - Analysis of an unknown malware specifically written for this training and based on real cases
  - Network, system interaction, and propagation analysis (malware analysis tooling)
  - Introduction to possible remediation

HM TRAINING SOLUTIONS ON-SITE SERVICE

All HM Training Solutions Seminars are available as On-Site presentations, tailored to meet the specific requirements of your organisation. For details please telephone +49 (0) 6022 508 200 (international).

Analysis of Malware by Reverse Engineering

M 10

A two day course in English

Bibliographic references

[1] Eric Filiol, Les virus informatiques : théorie, pratique et applications, 2nd ed., Springer Verlag France, 14/05/2009, 978-2287981999.
[2] Pavel Yosifovich & al., Windows Internals, Part 1, ⁋ Microsoft Press, 03/05/2017, 978-0735684188.
[3] Andrea Allievi & al., Windows Internals, Part 2, ⁋ Microsoft Press, 01/10/2021, 978-0135462409.
[4] Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Paperback, No Starch Press, 01/03/2012, 978-1593272906.
[5] Chris Eagle, The IDA Pro Book, 2nd Edition: The Unofficial Guide to the World's Most Popular Disassembler, 2nd ed., No Starch Press, 14/07/2011, 978-1593272890.

Why you should attend

The training aims to allow you to answer the following questions in a qualified manner:

- What are the different kinds of malware and how to recognize them (ransomware/trojan/keylogger/rootkit/bot) with reverse engineering?
- What are the strategies used by malware authors and how to identify then in malware?
- What are the different technical means used by malware to perform malicious actions?
- How did some famous malware work?
- How do we manage a real malware in an operational context?

Target Groups

With this training, the following participant are addressed in particular:

- Analysts in CERT/CSIRT/SOC
- Junior malware analysts
- Threat intelligence analysts
- Cyber security engineer

More generally, this training is designed for anyone wishing to have a rigorous and efficient methodological approach, including an intensive experience to practice of reverse engineering at pseudo-code level on malware. It can be an introduction to the world of malware for beginners or an intensive update for more experienced participants.

Speaker Biography

Dr. Baptiste David is an IT security specialist at ERNW, specialized in Windows operating system. His research is mainly focused on malware analysis, reverse engineering, security of the Windows operating system platform, kernel development and vulnerabilities research. He has given special courses and trainings in different universities in Europe. Also, he gives regularly talks on different conferences including Black Hat USA, Defcon, Troopers, Zero Night, Cocon, EICAR, ECCWS…

REGISTRATION DETAILS

Three Ways to Register

By Post: Please complete and return this form to HM Training Solutions.
By e-Mail: **Info@hm-ts.de**
Per Webseite: https://www.hm-ts.de/

Registration Fees

€ 2,290 + VAT 19%

Joining Instructions

Your booking will be confirmed by e-mail containing full event details. The price includes the course documentation as pdf, access to the online platform and the issuing of a certificate.

Change of Terms

It may be necessary for reasons beyond our control to alter the venue, timetable or content of this seminar or to appoint another speaker alternatively or to cancel the event. We accept no liability for any other cost.

Cancellations

Should you need to cancel your booking please confirm in writing either by email (info@hm-ts.de) or post. No refunds will be considered for cancellations occurring withing six weeks of the start of the event. However, we are happy to accept substitutions at any time; prior notice is appreciated

On-Site Presentations

All HM Training Solutions seminars are available as on-site presentations tailored to meet the specific requirements of your organisation. For more information please call +49 (60 22) 508200.

The number of delegates is limited. Therefore please immediately return this booking form

REGISTRATION FORM

Analysis of Malware by Reverse Engineering

❒ **03 – 04 May 2023 – online Workshop**

❒ Please reserve _____ places at a cost of 2**,290 €** + VAT 19% per participant

Mr/Mrs/Miss/Other First Name Last Name

Job Title _____

Company _____

Address _____

Postcode _____ City _____

Country _____

Telephone _____

Mobile number _____

E-Mail _____

Signature _____

BOOKING REFERENCE: M10eng

You will receive the course documentation as pdf before the beginning of the course.

Payment

❒ Please invoice my company _____

Invoice address (if different) _____

Purchase order no. _____

Additional Registrations

1. Mr/Mrs/Miss/Other First Name Last Name

Job Title _____

email _____

2. Mr/Mrs/Miss/Other First Name Last Name

Job Title _____

email _____

3. Mr/Mrs/Miss/Other First Name Last Name

Job Title _____

email _____