HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE INTERNATIONAL

LIVE ONLINE COURSE

M 10

A two day newly developed course in English
Malware Techniques 101
Your trainer is Dr. Baptiste David

The workshop is in English (The speaker's languages are English and French). 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.

Abstract:

This training is about the analysis of different malware techniques. The goal is to enhance the analysis concerning malware samples in a context of a CERT/CSIRT/SOC teams. This training is an introduction to the world of malware and the strategies used by them to compromise a system. The content of this training is focused on the current version of Windows operating system since a large part of the threats is there.

The first part of this training focuses on the technical and conceptual presentation of the different forms of malware threats, from (brief samples of) historical viruses to the most recent and modern ones. The purpose of this part is to cover the different tools, tactics, and procedures (TTPS) used by malware to propagate or execute itself as well as to cover their malicious nature through relevant examples. By discovering advanced techniques (stealthiness, polymorphic, metamorphic, lateral movement, code injection, hook, …), this technical background aims to better understand resultant threats.

In addition to general concepts, different technologies in Windows are covered concerning different possibilities to execute malicious code. That way, we cover script malware (PowerShell, JavaScript) and malicious documents (Microsoft Office and Libre Office), discussing how these different cases work in practice.

The second part of this training is driven by practice across different Labs. The first one is about analyzing different techniques of malware compromise through different tools. Especially, automatic triggers of malware are considered, and different code execution means are analyzed through a toolset, including Sysinternals software suite, Windbg debugger from Microsoft (just to track specific behaviors observed during runtime) and ProcessHacker which is open source.

4-5 June 2025 - live online   11-12 November 2025 - live online

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

The second Lab is dedicated to scripts analysis, including an introduction to remove some script obfuscation. In the end, a third Lab concerns regular malicious document analysis, taking care of macro execution and associated analysis techniques.

Concerning the different malicious threats observed, an introduction concerning detection techniques will be proposed for each one when applicable. From a general point of view, this conceptually explains how the antivirus or EDR software can track malicious behavior and how it is possible to detect them (when it is detectable) on a given system. Also, possibilities of mitigation regarding specific cases (scripts and documents) will be explored.

In the end, all participants will have a better understanding of what is possible in the field of malware techniques, through a didactic approach and practical Labs whose contents are always based on current and representative (real) samples. The participants will have the opportunity to expand their knowledge of malware and associated threats by observing technical details from different types of malwares over two intensive days.

Requirements:

Required Knowledge: In this training, the knowledge required for a good understanding of the concepts exposed is low. Knowledge in programming (compiled and scripting languages) as well as the basics of Unix and Windows operating systems is a definitive plus must – but not a must.

Required Hardware:

-       Own laptop

-       We provide the possibility to connect to the virtual test environments via RDP

-       The connection is established via Wifi or Ethernet cable

In-House Presentations

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

Training plan:

Day 1:
- Basic concept definition: program, virus, worm, malware, antivirus software …
- Technical refresher on the operating system
  - File system, network interface, process, memory, access rights
- Computer malware Fundamentals
  - Life cycles of a malware
  - Different kinds of malware
- Malware, including a technical description illustrated with real cases
  - Trojan / RAT
  - Spyware / Adware
  - Worms / Bots
  - Rootkits
  - Keyloggers
  - Ransomware / Wiper
- Threats, tactics, and techniques through malware
  - Malware concepts dealing with Threats concerning confidentiality, integrity & availability.
  - Technical means concerning:
    - Initial Access, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Command and Control, and Exfiltration
    - Polymorphism and Packer software, Fileless Malware, Reinfection, Code Injection & Hooks
  - Illustrated examples based on malware (WannaCry, NotPetya, German Parliament)
- Lookout on MZ-PE malware detection techniques
  - Detecting code infection
  - Detecting code injection and hooks
  - General considerations about antivirus / EDR
- **Lab:**
  - Identifying different malicious techniques (lateral movement, infection, dll injection, hooks, automatic execution, …) with runtime toolset
  - Analysis of real malware features (ransomware techniques, C&C communication, …)

Day 2:
- Script malware (VBScript, PowerShell, JavaScript)
  - Concepts, tactics, and techniques
    - Problematic to detect threats based on language interpretation
    - Obfuscation and writing style
    - System integration and interface with the native API
    - Self-evaluation and self-modifying code
    - Propagation vectors
  - Example of malware through different languages
    - PowerShell
    - JavaScript
  - Deobfuscation basics / AMSI
  - **Lab:** Deobfuscate a PowerShell script
- Lookout regarding malicious script mitigation
  - Limits regarding regular execution policy
  - Just enough administration
  - Constrain language mode
- Malicious documents
  - Microsoft and LibreOffice documents
  - Interface documents and access macros
  - Handling such documents in a secure environment
  - **Lab:** Analyzing a malicious document
- Lookout regarding malicious documents mitigation
  - Environment configuration restrictions
- Lookout on malicious document and script detection
  - Detection of script execution
  - Detection of malicious document
- Conclusion

▛▛▛ 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] Alexey Kleymenov, Amr Thabet, Mastering Malware Analysis - Second Edition: A malware analyst's practical guide to combating malicious software, APT, cybercrime, and IoT attacks Paperback, No Starch Press, 30/09/2022, 978-1803240244.

[5] Monnappa K A, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware Paperback, 29/06/2018, 978-1788392501.

▛▛▛ Why should you participate?

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) by elements issued from reverse engineering?
- What are the strategies used by malware authors and how to manually analyze them with free software (Sysinternals software suite, ProcessHacker, and Windbg)?
- What are the different technical means used by malware to perform malicious actions?
- How malicious scripts and documents are composed and how to analyze it?
- How to remove some obfuscation techniques from scripts or documents.
- How to check different specific malicious behaviors.

▛▛▛ Intended audience:

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 for analyzing malware. It can be an introduction to the world of malware for beginners or an update for more experienced participants.

▛▛▛ Trainer bio:

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

▐▐▐ *In-House Presentations*

All HM Training Solutions seminars are available as in-house 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

Malware Techniques 101

- ☐ **4 - 5 June 2025 – online Workshop**
- ☐ **11 - 12 November 2025 – 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 _____