TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Analysis of Malware by Reverse Engineering

Date of the training: **June 26-27, 2023** in Heidelberg, Germany

Book now using the voucher code: **TR23_HMTRAINING** and save an additional 5% of the current valid rate of any package!

Overview

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.

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

ERNW Enno Rey Netzwerke GmbH
George-Boole-Weg 4
69124 Heidelberg
BIC: GENODE61WNM

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
VAT-ID: DE813376919
IBAN: DE40670923000033145934

Managing Director:
Florian Grunow
Michael Schaefer

- 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

Who should attend this training?

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.

Requirements

The attendees should have:

- Own laptop
- A good knowledge of programming as well as the basics of Unix and Windows operating systems are sufficient.
- Some rudiments or basic practice in reverse engineering would be a definite plus - but not a must.

The connection is established via Wifi or Ethernet cable.
We provide the possibility to connect to the virtual test environment via RDP.

About the Trainers:

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…

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR23_HMTRAINING
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.
+49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hm-ts.de
+49 6022 5089999 / https://hm-ts.de