TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Reverse Engineering of Android Malware

Date of the online training: **October 21-22, 2021**

Overview

Participants learn how to analyze Android malware.

The majority of sessions consist in hands-on labs, with exercises on recent Android samples we caught. We focus on typical questions for malware analysts:

- How to reverse malware safely?
- How to find out, as quickly as possible, if a given sample is malicious or not?
- How to locate the remote CnC?
- How to deal with obfuscated classes, strings and junk code
- How to unpack malware without pain

Day 1: Reverse engineering of Android Malware - Getting started

- Introduction / Welcome
- Android malware trends
- Contents of Android application: manifest, assets, native libraries...
- Presentation of Reverse Engineering tools
- Setup of tools. A dedicated Docker container is provided to attendees
- Several labs: disassembling an app and patching it, using Smalisca, Quark and MobSF

Day 2: Dynamic load and obfuscation

- Dynamically loaded classes
- Unpacking malware with Dexcalibur, House, MobSF

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

- Decrypting obfuscating strings with Frida
- Implementing a JEB script
- Malware abusing Accessibility Services
- Anti-debug/VM tricks and solutions based
- Detection with APKiD
- Nearly 100% labs!
- Conclusion

Optional content: Network activity and native libraries

- Locating the CnC of a malware
- Reversing the contents of an obfuscated HTTP Post
- Re-activating debug messages with a Frida hook
- Dealing with native libraries
- Training exam

Who should attend this training?

This training is suited to a variety of students, including:

- Security researchers or engineers
- Android developers
- Anti-virus/IPS analysts
- CTF players

Prerequisites

- Be at ease in a Unix environment
- Be autonomous to install development or reverse engineering software on your host: make, git...
- Prior experience in programming, Java being strongly recommended.
- Experience in cybersecurity: malware, trojans, CnC...

- Know how to download and run Docker containers
- A prior experience on disassembly is definitely a plus.

Requirements

- Docker and docker-compose: https://docs.docker.com
- Training's container: `docker pull cryptax/android-re:latest`
- SSH, SCP and/or VNC client
- Recent Java Development Kit (JDK)
- Android Studio: https://developer.android.com/studio/
- Python 3.x
- A programming environment (IDE & build tools) e.g Emacs, Sublime, make...
- Ensure you have a few GB of disk space left...

About the Trainers

Axelle Apvrille is a happy senior researcher at Fortinet, where she hunts down any strange virus on so-called 'smart devices (smartphones, IoT). She is a frequent speaker at several conferences (Virus Bulletin, Insomnihack) and Troopers ;-). She has also given several workshops (Hack.lu, NorthSec...).

She is also the lead organizer of Ph0wn CTF, a CTF located in France and dedicated to security challenges on IoT.

Booking

Recommended online booking of trainings through:

https://tickets.ernw.de/troopers/tr21training/

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

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://www.hm-ts.de