What about malware craftsmanship?

CFP 2025 — English version

Speaker: Sonia SEDDIKI

General Information

Duration: 30 minutes.
Preferred language: French.
TLP Classification: TLP: CLEAR.
Recording / Replay: OK for recording and replay.

Short Description

An introduction to malware analysis and the techniques used by malware to evade detection.

Detailed Summary

Behind this buzzword-like expression lies a fact: the characteristics of a good piece of malware are not necessarily those we usually recommend for developing our own software. While their final goal may vary (data exfiltration, system destruction, data encryption for extortion...), malware shares a common constraint: achieving its goal without being caught.

We will present some malware development techniques used to bypass detection tools, before stepping into the shoes of an analyst and dissecting a real specimen!

Et si on parlait de malware craftsmanship ?

CFP 2025 — Version française

Intervenante : Sonia SEDDIKI

Informations générales

Durée : 30 minutes.
Langue souhaitée : Français.
Classification TLP : TLP : CLEAR.
Enregistrement / rediffusion : OK pour l'enregistrement et la rediffusion.

Description concise

Une introduction à l'analyse de malware et aux techniques utilisées par ces derniers pour échapper à la détection.

Résumé détaillé

Derrière cette expression aux faux airs de buzzword, se cache un constat : les caractéristiques d'un bon logiciel malveillant ne sont pas forcément celles que l'on a l'habitude de préconiser pour le développement de nos produits. Si leur objectif final peut varier (exfiltration d'information, destruction de systèmes, chiffrement de données à des fins d'extorsion...), les logiciels malveillants ont bien une contrainte commune : parvenir à leurs fins sans se faire prendre.

Nous vous présenterons quelques techniques de développement de malware utilisées pour contourner les outils de détection, avant de nous mettre dans la peau d'un analyste et de disséquer un vrai spécimen !