Contribution ID: **21** Type: **not specified**

Modern Windows Software Cracking by a GNU Linux hacker

Tuesday 10 June 2025 15:30 (45 minutes)

In this talk, I will walk you through my journey of reverse engineering and cracking a binary protected by a modern licensing software stack named *CryptLion*.

The presentation will be structured into three main sections, going from my first observations (as a hacker more used to exploit Linux binaries than Windows executables) to successfully creating my own version of the program without any kind of license verification.

1. **Reconnaissance**:
   I'll begin by explaining how I identified the protections put in place to protect this program. This includes the techniques I used to analyze the file structure, extract meaningful information, and gather insights from online resources about *CryptLion*. Understanding the binary's composition was the first step in unraveling its secrets.
2. **Understanding the code and CryptLion's SDK**:
   Next, I'll dive into the *CryptLion* SDK to understand how it operates. By comparing the SDK's (and its library) functionality with the binary in hand, I was able to identify a potential vantage point. This phase involved dissecting the code to map out its behaviour and identify vulnerable points.
3. **Binary exploitation : the actual cracking**:
   Finally, I'll share my exploitation strategy, including the techniques I employed. I'll discuss what worked, what didn't, and the lessons learned along the way. This section will also cover some reverse-engineering insights into CryptLion's inner workings and how they were leveraged to achieve the final crack.

This talk will provide a comprehensive look at the methodologies, challenges, and successes of reverse-engineering a CryptLion-protected binary, offering valuable insights for crackers and defenders who'd like to assess their own licensed software.

Length

45 minutes

Optional: Speaker / convener biography

I'm Jérémie, a former web/mobile developer with a long-standing passion for tinkering and free software, who has been an ethical hacker for nearly 7 years. I created my company in 2023, with which I'm trying to bring something new to our two main areas of activity: PenTest and training. I'm ocassionaly speaking at conferences in Paris whenever I have something interesting to the community!

Primary author: A, Jeremie

Presenter: A, Jeremie

Session Classification: Talks

Track Classification: Talks and presentations