# Hacking Lab Primer

Super cool Hacking Lab TAs

## 1 Introduction

Congratulations! You are now the proud owner of your own malware sample! Your aim in the next few weeks will be to try and understand what these samples do and to use some methods to try and understand more about the infrastructure with which these samples interact. These are live samples and we have not examined them completely, so please take the necessary precautions. If in doubt, Google is your best friend, and you can always reach out to us.

### 1.1 Do's and Dont's

Since the samples we will be providing are actual malware samples, some quick guidelines on what (not) to do with them.

- If you want to run the samples, make sure that you run it in a virtual machine. We don't know what these samples do, so **absolutely** make sure to run it in an isolated environment. **These samples could break your computer.** Also, do not let these samples connect to the Internet (also not from the Virtual environment), as you will then likely be performing DDoS attacks. You probably do not need to run the sample in an isolated environment to do the project as it involves mainly static decompilation.
- Do **NOT** run these samples or the communication program you are building on TUD networks! Doing this usually results in a very angry call from the TUD security team (speaking from experience).

### 1.2 Tools to use

You may use any tools that you are familiar or comfortable with. If you haven't used any reverse engineering tools before, these might be a good starting point:

- Ghidra (Disassembler)
- IDA Pro (Disassembler)
- Any.run (Online sandbox)
- GDB (dynamic analysis)
- Virustotal (Commmunity info)
- Urlhaus (IP activity information)
- Our in-house network telescope (IP activity and samples) to (hopefully) be able to enumerate the devices infected or adversarial loading infrastructure

## 1.3 Interesting places to start looking

- The Mirai botnet is one of the most popular botnets out there. Since the source code got leaked in 2016, many samples we see today are Mirai spinoffs. A good way to understand the basic setup of a botnet sample would be to go through this source code [1].
- Look at the plain text within the samples to get a rough idea of what is going on (you can use `strings`).
- Check online sources to see if samples have been reported elsewhere. These sources might provide you interesting hints on how to proceed.
- Find system calls in the samples to quickly jump to interesting parts of the code. For example, look at system calls related to network interactions to find the part where a sample might make contact with external sources.

## 1.4 Artifacts that we would look for

- Try to figure out the capabilities of the sample itself, Does it:
  - Encrypt the device files itself, perhaps as a ransomware?
  - Have DDoS or Distributed Denial of Service capabilities? If so, what?
  - Maybe it also has the ability to behave as a proxy or VPN?
  - Do they mine cryptocurrency?
- Usually these samples would try to initiate contact with a C&C or Command and Control Server, try to identify the address that they reach out to.
- Is the sample active? Is there a two-way communication with the C&C server? If not, maybe check sources such as malware bazaar or urlhaus to find newer samples of the same strain.

## 1.5 Milestones

Some milestones that we would like to see over the course.. of this course. We will judge on the basis of the difficulty of your individual sample, some tasks might be not possible with your sample. Please indicate then why this is not possible.

- Gaining an understanding of the functionalities provided by the malware
- Identifying the infrastructure behind this particular strain of malware
- Additional capabilities of the malware
- Enumerating devices in the botnet based on indicators you might have found
- Understanding the communication among bots or between the bots and the C2 server and capturing the commands sent.
- Creating a standalone script that emulates the bot communication and "joins" the botnet.

[1] https://github.com/jgamblin/Mirai-Source-Code

You are welcome to discuss your methods with other groups as each of you have unique samples, however do not compare progress as some breakthroughs may depend on luck, which samples are still active, and so on. It is not allowed to look at, use, or help write the code of another group, similar to any other coding assignment. You are, as a group, responsible for the code you write. If you get stuck, you can always come to us for advice on how to proceed! Each group will be graded separately depending on the nature of the binary they are provided.