Black-box analysis of malware - LABS

Vít Bukač

CROCS, Faculty of Informatics, Masaryk University

Supervisor IT Security, CIRT, Honeywell Global Security

PV204 Security Technologies

CROCS

Centre for Research on Cryptography and Security

Lab Assignment

- Hands-on experience of manual black-box analysis
- Two malware samples were inserted into study materials. The task is to perform the analysis of at least one sample.
  - In other words, if you provide a perfect analysis of one sample, you don’t have to analyze the other sample. Performing the analysis of both samples increases the chance for perfect score. The results of the analysis should be submitted to IS in the form of a structured textual summary report about one or both samples.
- After the analysis, submit a report about malware sample behavior to information system

Final report

- 1-2 A4 pages, eventually complemented with screenshots
- Report should contain the following:
  - Description of external behavior (e.g., what windows are shown to the user, if any).
  - Created, modified and deleted files. Emphasize what files are critical for the malware. Focus on distinguishing between original malware files and operating system files.
  - Persistence methods. How malware makes sure it is executed again after reboot.
  - Network communication. With whom and how is malware trying to communicate.
  - Defense mechanisms used by the malware to prevent the analysis. Approaches how you were able to circumvent these mechanisms.
  - Changes in Windows registry.
  - Anything relevant and important.

Helpful notes

- Presented samples are real life malware. Be careful.
- Use snapshots for easy restoration of virtual machine clean state.
- You can use any tools and internet sources as you want.
- Focus on observing changes in the operating system just after malware is executed for the first time.
- Execute samples repeatedly, both in clean VM and in already infected VM.
- Check what happens if you restart an infected VM. Verify malware persistence.