Homework 6

Memory analysis & Blackbox malware analysis

PV204 Security Technologies

CROCS
Centre for Research on Cryptography and Security

Black-box analysis of malware – Outline

- Sixth PV204 homework consists of two parts. The first part is dedicated to the memory analysis, the second part to the blackbox malware analysis.
- Deadline for this homework is **May 12, 23:59**.
- Please put both required reports in a single archive and post the archive in Information system: https://is.muni.cz/auth/el/fi/jaro2019/PV204/ode/90433186/

- Please be aware that you are working with live malware samples. Take caution!

Memory analysis

- **Task:** Analyze a provided sample and create a short report
  - Example report: http://dior.ics.muni.cz/~valor/pv204/bob-vmem-analysis.pdf
- Detailed instructions available at http://dior.ics.muni.cz/~valor/pv204/

Blackbox malware analysis

- **Task:** Analyze two malware samples provided in the virtual machine and create a short report.
  - Samples are encrypted, password is *"infected"*.
  - The samples will probably require external tool to unpack, I recommend 7zip: http://portableapps.com/apps/utilities/7-zip_portable
- Perform the analysis of at least one sample. 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.

Blackbox malware analysis – Notes

- Use snapshots for easy restoration of virtual machine clean state.
- 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.
- Final 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.