Course overview

Arvind S Raj
(arvindsraj@am.amrita.edu)

16SN708 Malware Analysis

M.Tech CSN Jul-Nov 2017

Lecture agenda

- Course objectives and topics covered.
- Grading scheme.
- Warm-up task.

Outline

Course objective

- Introduction to malware analysis: tools, techniques and required knowledge.
- Requires knowledge of OS and networks.
- Other stuff needed: patience and an eye for detail.
- Mix of theory and hands-on hopefully. We'll see.

What will you learn?

- **Static analysis**: Techniques to infer information about malware without executing.
- **Dynamic analysis**: Techniques to infer information about malware by executing in controlled environments.
- Focused on Windows for most part but techniques are generic.
- Textbook: Practical Malware Analysis by Michael Sikorski and Andrew Honig.

Outline

Grading scheme(tentative)

- **Periodical 1**: 15%.
- **Periodical 2**: 15%.
- **Assignments**: 30%.
- **Final exam**: 40%.

Assignments

- 6-7 hands-on assignments based on topics discussed in class.
- More if we cover additional topics.
- Regular rules apply: individual work, no plagiarising and no late submissions.
- Malware analysis not theoretical: requires practice. Assignments provide best avenue.

Plagiarism policy

- We do not condone plagiarism. Just don't do it.
- If discovered, everyone involved get a 0 for that assignment.
- If repeated plagiarism occurs, we will make note of it in the department and do any/all of following
  - Assign 0 or less marks for past, current and/future assignments.
  - Assign 0 or less marks for exams.
  - Other creative penalties we think of during the semester.
- Bottomline: Just don't copy or lend your assignments to anyone.

Outline

Warm-up task

- Create 2 VMs(VirtualBox) and install Windows(Windows XP and Windows 7). Run and analyse binaries only in these and nowhere else!
- Tools to install: IDA Pro free 5.0, PEstudio, PEview, Resource Hacker, Dependency Walker, DiE, PEinspector and exeinfo.
- These are standard(and free) tools in malware static analysis.
- More tools will be needed; deferring for later on.

Questions?

If you have any questions,

- Ask now.
- Send an email - arvindsraj@am.amrita.edu.