Teaching Malware Analysis in Challenging Times

Charles Nicholas, Robert "RJ" Joyce
nicholas@umbc.edu, joyce8@umbc.edu
CSEE Department, UMBC

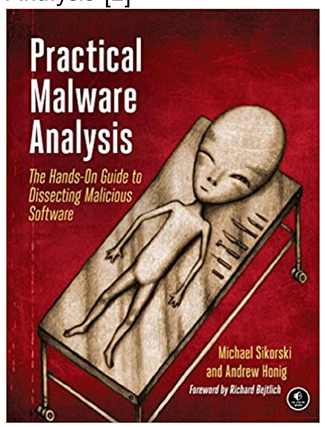
Introduction and Objectives

We summarize our experience in teaching malware analysis, especially in the last two years.

- At MTEM 2013 we presented "Lessons Learned Teaching Malware Analysis" [1]
- After seven years and a pandemic, we have more to share...

Some Things Have Not Changed

- Demand for malware analysts remains strong in the Baltimore-Washington area
- We have stayed with Practical Malware Analysis [2]



- The basic course outline has stayed the same.
- The course remains popular, about fifty students per offering, which is large for an elective course in our program.

Acknowledgements

Presented at the Malware Technical Exchange Meeting, Sandia National Labs, July 13-15, 2021.

Course Topics

- Installing and Using VMs
- Utilities for static analysis
- Basic Windows internals and API
- Network tools, e.g. Wireshark
- Disassemblers: IDA and Ghidra
- Debuggers: Immunity (not Olly)
- Varieties of Malware
- Dealing with packed and obfuscated code

What Have We Changed?

- We used to teach the course in a lecture hall, but we now teach it online, and that's *better*
- We must record our sessions, for the sake of students who participate outside of class hours, but that's quite handy!
- We have no lecture halls that have enough seating, AV capability, and AC power. But with all students being remote, no problem!
- Solutions to exercises are in the back of PMA, which limits the use of those problems
- We no longer require a programming project as such, which was perhaps the only opportunity for students to experience Windows systems programming...

What Would We Change If We Could?

- Still not much time in the course for Android malware, or web-based, or Linux...
- Students often lack sufficient expertise in assembler language, which is annoying

What do students like the most?

- Disclaimer: we have only anecdotal evidence to support these comments
- Guest speakers! Some from local intelligence agencies, more recently from industry, especially FireEye
- Students appreciate having access to recordings of demos, especially tools like Ghidra and Immunity with somewhat complex user interfaces
- Students say that they learn a lot from homeworks!

Some Outcomes

- Three former students in this class have earned Ph.D. degrees! others in the pipeline, and many M.S. thesis students
- Those who finish the course sometimes continue as members of our Malware Research Group
- Many former students hold jobs where these skills are of value
- The course web site is available: `https://bit.ly/3vZYKjH`

References

Charles Nicholas and Andrew Coates.
Lessons learned teaching malware analysis.
In *Malware Technical Exchange Meeting (poster session)*, 2013.

Michael Sikorski and Andrew Honig.
Practical Malware Analysis.
no starch press, 2012.