Intro to Windows Malware (Spring 2024)

Instructor: **Bernardini, Kai**
Subject: **CS**
Catalog & Section: **6983 01**
Course ID: **39792**
Objectives:

Enrollment: **13**
Responses Incl Declines: **7**
Declines: **0**

Instructor Related Questions: Kai Bernardini (15 comments)

Q: What were the strengths of this course and/or this instructor?

1. The material is super interesting and the guest lectures take a good class to a great one. I constantly felt like I was learning things that were actually important. Kai's cae for his students and the class in general is very obvious
2. Professor Bernardini is a very knowledgeable, enthusiastic instructor. This course gives students a great oppurtunities to explore the topic and meet with actual professionals.
3. Fantastic course material, very knowledgeable about the subject, assignments (while few) were sufficiently challenging and useful for the course
4. Kai is beyond passionate about the material he teaches. His determination to see his students succeed and grow from the material was one of the strongest points of this class. By the end of the semester, I was fully convinced of any and all hours I put into this class translating in a worthwhile investment into my own education and understanding of cybersecurity / malware concepts.
5. The course material was very interesting and in-depth. The professor clearly has allot of experience in this area and it shows in his lectures. The guest speakers through out the semester were also very interesting and fit well with the material we were learning in class.

Q: What could the instructor do to make this course better?

1. the course needs more organization. The assignments are hard, but they are very useful. If the course were more organized it would make the whole thing a lot more doable. I also think going over the final project earlier would make it easier for students to get it done in time. Check-ins that we could turn in throughout the whole semester would make the whole final less overwhelming.
2. More systematic teaching of internet and windows OS
3. Professor Bernardini could make the syllabus more organized and prepare more hands-on assignments both for homework and in class to prepare for the C2 final project. I can tell the prefessor is a very enthusiastic instructor and eagers to teach the students the most he knows about.

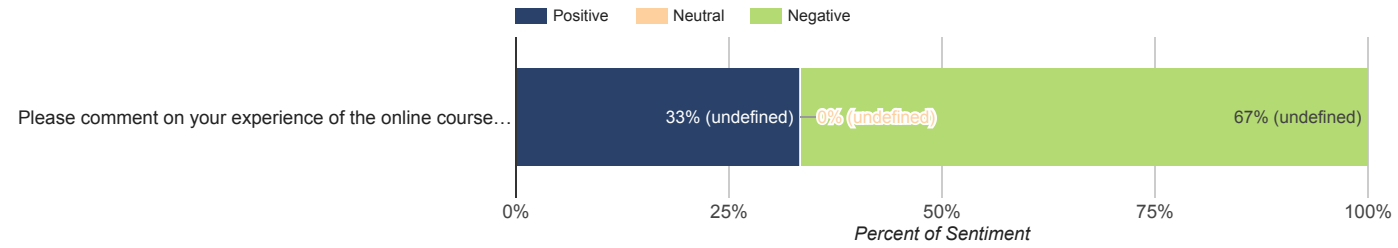
   This course could design more assignments to facilitate learning, and it is better if Prof. Bernardini is more responsive online. Students might feel awkward to ask the same questions again without a respond.
4. The course needs to be more balanced over the whole semester. It's very end-heavy. The current assignments are definitely good: the crackmes, sHELL, epochs. However, there definitely needs to be more actual deadlines and assignments. We should be forced to build a PE Loader ourselves, not just see you build one :D
   In reality, a lot of what you talk about in class can be made into assignments as well to make sure that we practice what we have learned. Like mutexes and named pipes, and cryptography, and calling windows API functions, and learning how PE's are structured, etc. Those can all be small assignments to make sure that we can use the material we learned :)
   Also, we really don't need a lecture on crypto. We all probably know it by now, and if we don't, then we probably shouldn't even be in the class! All your crypto lecture can probably be shortened into like 10 minutes.
   Finally, if you decide to take any of my constructive criticism, please take this last one. The malware can be built over the course of the semester, not the last two weeks.
   Let me explain:
   1. It will still be end-of-semester-heavy. that's fine, because it can be mainly like the implant and other hard stuff.
   2. two of the big parts of the malware, the c2 server and the client, can be built over the course of the semester. You really don't need to know anything about the windows API to build those two, for the most part. You can have a simple lecture about what the final project will look like at the start of the year, and then have assignments like:
   a. build a front end to interact with a c2
   b. build a flask server for the c2
   c. get those two talkin to each other
   d. build a pe loader
   e. etc. etc. etc.
   That way, all group members will know pretty much what they're doing by the time it gets to the final project. And, the malware overall will probably be a lot more impressive! And the students can focus more on the implant and the functionality :)
   If you want anyone to help out next year or anything on course material or assignments or anything, i'd love to :D
5. Restructure the github. There was SO much information in the github that even now, I am not sure of all the information inside. I spent so much time scrambling to understand what I did and did not need to read. For set up of the Azure instance / VM environment, I wasted a lot of time following the set up isntructions in one of the git hub pages before I heard back from a peer days later that I was actually already set from the first time I loaded the azure instance. For assignments, having a PDF summary to hit the bullet points of what is required / how to submit would be amazing. Understanding the exact requirements to get a certain letter grade from the final project would give folks a solider starting ground of what kind of work needs to be put in. For the final project, either dedicate a class or ensure every group meets with Kai after the first week following the announcement of the project in order to confirm everyone has been able to set up some sort of environment in order to actually begin developing and testing their code.
6. The course could have been a bit more organized when it came to the schedule of assignments. There were certain topic that were covered in class and that were part of the final project that I would have been able to internalize a bit better if there was an assignment associated with them that was out around the same time as that lecture. Some of these include pe loading, chrome stealer, process injection, and reflective dlls. The grading of the course could have also been a bit more transparent.

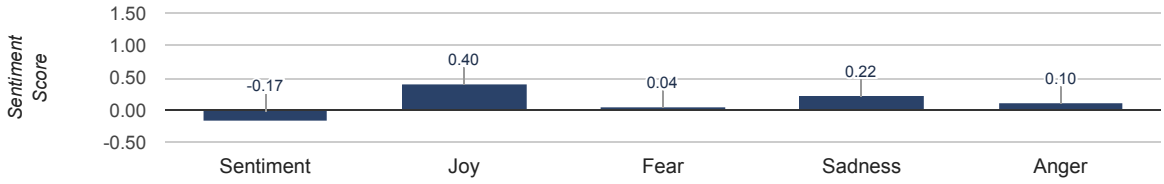
Q: Please expand on the instructor's strengths and/or areas for improvement in facilitating inclusive learning.

1. Kai cares about his students and you can tell that. Making it clear that things like quizzes are used for attendance or that participation is for the betterment of the whole class could make it so that students are more comfortable
2. When you ask a question in class, it is normally a coin flip. 50% chance the question is difficult, and 50% chance the question is incredibly trivial. However, we really don't know which one it is. The way you lead questions makes us terrified to make that coin flip for ourselves lol
   I think it may be difficult for you to kind of get on our level of understanding; you are extremely knowledgeable about it so what's trivial and what's not is sometimes lost in translation between you and the class. In reality, I'm sure that most or many in the class (me included) know the answer to like 80% of your questions. But we are scared to answer and look dumb or something, for one reason or another.
   Maybe it is because you are leagues above us or maybe it is because you word all questions like they are very easy (whether they are super easy for us or not ... lol)
   We would be more confident with more hands on assignments of building stuff i think.
   Last but not least, we need actual office hour times. By-appointment is actually less approachable in my opinion
3. Kai is one of the most phenomenal professors I have been able to experience at Northeastern. His no-bullshit insight into the cybersecurity field reinvigorated my desire to keep learning in this field and not stop trying. The organization of this class kept me from being able to fully enjoy the experience Kai created in-person but the heart and soul of this class is truly redeemed in Kai's unrelenting desire to be an impactful mentor to every person in his class. Also Ghost is the bestest doggo point-blank-period.
4. The instructor did a good job at facilitating a welcoming and inclusive learning environment.

Questions to Assess Students' Online Experience (3 comments)

Q: Please comment on your experience of the online course environment in the open-ended text box.





1	was okay but would be cool if our mics werent muted ★★☆☆☆
2	Github was definitely frustrating to navigate, even towards the end of the semester. Whenever libraries, applications, terminal commands, etc. would be used, I would have to spend time looking up what was actually being discussed in order to understand what the point being made was about 15 minutes ago. It was hard to follow what we were being asked to do when I didn't know about the existence of tools rquired to complete said task. ★★☆☆☆
3	The the online course work (lecture recordings, assignment specs, lecture code) could have been organized better and released in a more timely fashion through the semester. ★★★★☆

Student Self-Assessment of their Effort to Achieve Course Outcomes (5 comments)

Q: What I could have done to make this course better for myself.

1	dedicated more time to assignments
2	Learn more about windows functions calls. More reverse engineering.
3	did more of sHELL
4	I wish I had been much more persistent with asking a lot of questions, especially when the final project came out. I was scared how "stupid" my questions were about not even the structure of the final project but the set up needed to even begin.
5	Do more work earlier in the semester to solidify my understanding of concepts.