EE/CprE/SE 492 Weekly Report 5

Report Coverage: 03/04/2019
Project Title: Security Orchestration Platform
Client: “The Company”
Advisor: Doug Jacobson
Team Members:

- Adam Crosser (Implant and EDR Testing Developer)
- Logan Kinneer (Implant and EDR Testing Developer)
- Daniel Limanowski (Frontend Lead)
- Vijay Uniyal (Frontend Developer)
- Justin Roepsch (Frontend Developer)
- Paul Chihak (Implant and EDR Testing Lead)

Weekly Summary

This week our team continued research and development on the project.

Past Week Accomplishments

Group Accomplishments

- Communicating with project stakeholders.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative (for second semester)
Adam Crosser	Have not had much time to do additional research into new TTPs this week. At the end of this week I got access to AWS and will begin working on	1	20

	implementing domain fronting for next week!		
Daniel Limanowski	After our client canceled our meeting I called them individually at night to give them a status update. Additionally, I have finished refactoring frontend code and I worked further on groups and permissions within the C2.	3	25
Vijay Uniyal	Got further into setting up nginx web server. Using free SSL.	4	26
Logan Kinneer	Worked on getting the Memory dump feature in Cuckoo working.	3	23
Paul Chihak	Finished getting OVA to work however had some exams this week and wasn't able to do much more.	2	22
Justin Roepsch	Implementing logging for both regular debugging messages to a file, and user actions to files created for each day using TimedRotatingFileHandler inside of the settings.py file. Actually hooking it up to start logging can't start until the migration started	3	25

	earlier has been completed.		

Plan for the Upcoming Week

- **Adam Crosser:** Begin work on developing domain fronting TTP since we finally have access to AWS.
- **Daniel Limanowski:** Finish user authentication, groups, and permissions for the C2 frontend component. Work with the C2 team to ensure my code can easily be logged and stored away for audit purposes. Write code tests and documentation for my code.
- **Vijay Uniyal:** Understand how to properly utilize certbot acme client to bring together nginx server.
- **Logan Kinneer:** Get Cuckoo's REST API working.
- **Paul Chihak:** Start looking back into malleable C2 since it is looking like Cuckoo will not take as much time as originally anticipated.
- **Justin Roepsch:** Start to import and use the loggers created in the views.py file, and test actual logging.