EE/CprE/SE 491 Weekly Report 5

Report Coverage: 10/01//2018 - 10/05/2018
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 to conduct research and started writing test code to learn various development capabilities. We reviewed our project plan with the client and updated it from their feedback.

Past Week Accomplishments

Group Accomplishments

- Collectively discussed project plans and shared ideas.

Individual Accomplishments

- **Adam Crosser:** Conducted research into usage of malicious browser extensions as a command and control and proxying solution. Reviewed presentation from DerbyCon covering usage of this red team TTP. Reviewed possible alternative delivery mechanisms for malware such as malicious PDF files and Excel DDE (Dynamic Data Exchange) delivery mechanism used by various APT groups (e.g. FIN7)
- **Daniel Limanowski:** Performed design thinking analysis and development training with Justin. Developed and tuned Gantt charts to plan out the timeline for the next two semesters. Researched the concept of domain fronting.
- **Vijay Uniyal:** Finished researching into complex javascript with practice and now researching into hot module replacement and ES6 arrow functions in React.

- **Logan Kinneer:** Performed research on Cuckoo to determine how it could be used to distribute malware to group of hosts . Reviewed code for the malware segment of the project.
- **Paul Chihak:** Researched methods to allow generic command and control traffic that can be modified to look like any application using a command tag. Also worked to do analysis of our project idea so far and further refine the big picture ideas to ensure that everyone is on the same page.
- **Justin Roepsch:** Continued research into dockerization of applications, logging of user actions, and went through more example react applications.

Individual Contributions

Brief summary of individual red team contributions given below.

Name	Individual Contributions	Hours this week	HOURS cumulative
Adam Crosser	Continued to review published research on red team tactics, techniques, and procedures.	3	28
Daniel Limanowski	Researched domain fronting, created project timelines, met with client.	4	28
Vijay Uniyal	Finished research into complex Javascript within react, moving onto next goal.	5	27
Logan Kinneer	Performed research on Cuckoo and malware	3	25
Paul Chihak	Reviewed options for a generic command and control traffic generator and refined big picture goals	5	27

Justin Roepsch	Researched dockerization, logging, and React	5	26

Plan for the Upcoming Week

- **Adam Crosser:** Continue to work on researching and designing implant and improving understanding of client requirements and red team TTPs
- **Daniel Limanowski:** Research EVR solution to understand the work required for that part of the project. Make changes to project plan as requested by our client.
- **Vijay Uniyal:**. Going to continue research and focus on learning hot module replacement along with ES6 arrow functions in React.
- **Logan Kinneer:** Continue to work on integrating Malice with the rest of the project and evaluate the pros and cons of Malice and Cuckoo.
- **Paul Chihak:** See if there are any existing solutions that will allow us to generate network traffic that we can inject our command and control traffic into. That way we don't have to completely develop the idea ourselves and it will be maintained outside of the scope of the project.
- **Justin Roepsch:** Will test out possible methods of logging user actions for both ease of implementation and value of information.