EE/CprE/SE 491 Weekly Report 4

Report Coverage: 09/24/2018 - 09/30/2018
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 into technical and project feasibility and completed the project plan for the project.

Past Week Accomplishments

Group Accomplishments

- Met in person to conduct brainstorming workshop, gave each group member an opportunity to present ideas, discussed possible technologies to utilize for the project (e.g. Django, AWS, GCP, PowerShell, .NET Framework, etc.) and from this worked to develop the project plan.

Individual Accomplishments

- **Adam Crosser:** Conducted research into the methods presented by Google Project Zero research James Foreshaw into how COM and .NET interopability can be utilized to load arbitrary C# code from JScript/VBScript processes. Reviewed research published by Enigma0x3 (Matt Nelson) on per-user COM hijacking and reviewed his “Windows Operating System Archaeology presentation from BSides Nashville.
- **Daniel Limanowski:** Researched React JS and the implementation of secure APIs. Gained an understanding of API tokens and how to authenticate users of APIs such that no unintended users can access our sensitive information. I researched high performance web servers like Nginx for production settings.

- **Vijay Uniyal:** Conducted further research into utilizing React. Encountered significant problems with re-setting up environment in Ubuntu. A big one being a incorrect install of npm not properly updating, not allowing me to get the proper packages. Fixed majority of problems and continuing with complex javascript.
- **Logan Kinneer:** Wrote a Python script to parse the output of Malice. Researched using Flask to provide a method of requesting a scan remotely, transfering files to be scanned and returning the results of the scan.
- **Paul Chihak:** Further researched Cuckoo to aid in distributing payloads across multiple VMs. Looked into whether or not having multiple versions of microsoft products installed on 1 VM will cause conflicts or unexpected behavior (inconclusive results). Also researched James Foreshaw's COM to load C# code from JScript but the methods he used are detected by windows defender. Still think that we could find other uses of COM objects to load C# code but would have to do some reverse engineering of windows functions.
- **Justin Roepsch:** Researched what Dockerizing the application would entail, got more familiar with Docker, and attempted setting it up for our application.

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.	4	25
Daniel Limanowski	Research application programmer interfaces and how to implement them with security in mind.	6	24
Vijay Uniyal	Fixed significant errors in development environment and continuing research into complex javascript.	5	22
Logan Kinneer		5	22

	Wrote python script to parse malice output, and researched using Flask.		
Paul Chihak	Researched Cuckoo and reviewed published research on published exploits to find new ways to use them.	5	22
Justin Roepsch	Docker research, setup.	4	21

Plan for the Upcoming Week

- **Adam Crosser:** Conduct further project research into red team techniques and methods of implementing them using C# and the .NET framework. Identified open source code on github which I will review for possible use in our implementation
- **Daniel Limanowski:** Meet with frontend subteam to ensure that everyone has working development environments and answer any questions about the existing code. After that, we will distribute the workload and perform detailed planning for all of our desired features. I will continue researching secure APIs.
- **Vijay Uniyal:**. Conduct further research into React book, and contact team member to walk through his steps of the already existing code in React.
- **Logan Kinneer:** Discuss with team the best way to integrate malice into our solution. Determine if our client would like to use Malice. Depending on the outcome of these events I may continue with the development of a api to use Malice through, work on automating the setup of Malice, or move on to evaluating a separate product.
- **Paul Chihak:** Install Cuckoo and look into some possible signed windows functions that we can possible load code into. Try and find a better way to test against multiple versions of microsoft products without needing to have a fresh VM for each one.
- **Justin Roepsch:** Finish research and testing of dockerization. Will probably discuss React progress with other members of team.