EE/CprE/SE 491 Weekly Report 6

Report Coverage: 10/08/2018 - 10/12/2018
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 design plan with the client and updated it from their feedback.

Past Week Accomplishments

Group Accomplishments

- Collectively discussed design plans and shared research. Discussed current research roadblocks and helped each other overcome technical issues we were running into during our research. Created and gave presentation to entire class on our project plan and progress thus far.

Individual Accomplishments

- **Adam Crosser:**Researched tools that could be used to detect our implant when it is installed on a target network. Researched how beaconing for the implant could and reverse engineered how Cobalt Strike malware C2 profile works. One of the techniques a defender could use to detect our malware beaconing is the RITA tool from Black Hills Information Security. It utilizes fast fourier transforms to detect malware beaconing behavior and calculates a total risk score from that. I ran the tool in a test environment and ran a packet capture using Bro IDS. I then installed the RITA tool and ran analysis against the data. From this the beaconing behavior became very clear. I then researched ways you could get around this detection and discovered that you can add a randomized jitter to your beacon which will randomize when it reaches out to the control server. With a sufficient jitter you can lower the confidence score that RITA calculates to a point where you can get lost in the noise. Another technique is to do domain fronting to multiple domains (https://www.blackhillsinfosec.com/projects/rita/)

- **Daniel Limanowski:** Created a diagram of our entire infrastructure (high-level, omitting detailed descriptions) for use in our presentation during class. I helped create the slides for the presentation. I researched production deployment techniques with Docker including the use of volumes versus databases for storing non-volatile, long-term data. We need this because Docker is our deployment framework of choice and we don't want our client losing valuable data such as logs or bot information.
- **Vijay Uniyal:** Researched hot module replacement along with ES6 arrow functions in React. Experimented with a lot of ES6 classes which is the main class for object oriented programming. Bootstrapped my own react application and got basics of classes understood.
- **Logan Kinneer:** Researched Cuckoo and it's built in tools for deploying malware to a variety of VMS. Read over the documentation and analized some of the source code. Found the Python script in the project responsible for analysis of malware and analyzed it to determine how it could be modified to report on the behavior of an EDR solution. Also looked through how to make signatures to automate the process of determining if a EDR solution has detected the malware.
- **Paul Chihak:** Researched ways to automatically generate command and control network traffic. Was not able to find a pre-existing solution that will satisfy our use cases but I believe that I have found a feasible method.
- **Justin Roepsch:** Researched what actions and data should be logged when logging is implemented, compared it with actions possible on our application, and looked for pre-existing solution. Decided that solutions such as Google Analytics will probably not be needed, as we want to only log action-generated events, instead of mouse and screen positioning.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative
Adam Crosser	Research RITA and covert implant C2 channels. Detecting malware beaconing using fast fourier transforms and how to	4	32

	evade the blue team detection mechanism.		
Daniel Limanowski	Researched Docker production best practices. Created diagram of infrastructure for client and class.	5	33
Vijay Uniyal		4	31
Logan Kinneer	Researched signituring in Cuckoo and how it analyzes malware.	5	30
Paul Chihak	Researched ways to automatically generate network traffic.	4	31
Justin Roepsch	Researched logging needs and possible solutions	5	31

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. Writing test code and install and evaluating existing tooling.
- **Daniel Limanowski:** Practice deploying production Docker images and using volumes to store data. I want to use existing images to begin with, and learn how they use either Docker-Compose or Docker Machine to orchestrate stable deployments of microservices. We will eventually be using this for the frontend application even in development scenarios so this tool is of great use to us and will save a lot of time.
- **Vijay Uniyal:**. Research further into react and ES6 Object Initializer along with Unidirectional Data Flow. Will start to analyze source code by the end of the week.
- **Logan Kinneer:** Continue to research Cuck and Malice and determine what the best way to integrate them into our project would be.
- **Paul Chihak:** Create a basic test case for taking a sample network traffic and embedding a command within the network sample. Research ways to allow more than just web traffic to be spoofed.
- **Justin Roepsch:** Create a test database to send basic logs to, and create the log generation to create and send the logs.