EE/CprE/SE 491 Weekly Report 8

Report Coverage: 10/22/2018 - 10/26/2018
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 expanded test code for our various development capabilities. We reached out to our university advisor so that we could schedule a meeting with him and keep him up-to-date on our progress. Our team met in person to share our research and help others learn the concepts behind our project. We wrote and expanded on test code.

Past Week Accomplishments

Group Accomplishments

- Group phone meeting with client

Individual Accomplishments

- **Adam Crosser:** Wrote malicious macros to test possible delivery mechanisms for malware. Researched various COM servers which can be used to launch processes without directly spawning them as a child process of WINWORD.exe or EXCEL.exe. Continued to conduct research into binaries which can be used to bypass application whitelisting solutions commonly deployed by organizations. There are a number of documented techniques such as the SquiblyDoo technique (https://blog.conscioushacker.io/index.php/2017/11/17/application-whitelisting-bypass-regsvr32-exe/) and the SquilbyTwo techniques (http://subt0x11.blogspot.com/2018/04/wmicexe-whitelisting-bypass-hacking.html). I put together some proof of concept payloads which exploit these techniques to load

malware. I noticed that some AV software such as Windows Defender will generically block wmic whereas other solutions such as Carbon Black Response will only generate an alert but allow the activity in their default configuration.

- **Daniel Limanowski:** This week I researched the concept of domain fronting so that I could understand the goals and capabilities of our other sub-team. I read papers and watched a technical demo of Domain Fronting by a red teamer who used Amazon's Cloudfront Content Delivery Network (CDN) to proxy his malicious traffic back to him, essentially masking his true identity. In addition, I reached out to our University Advisor, Dr. Doug Jacobson, to schedule a meeting with him in order to keep him up to date.
- **Vijay Uniyal:** Performed various tests utilizing ES6 Object initialization and learned about the importance of Internal Component State. ES6 turned out to be quite technical so still trying to get a grasp on unidirectional Data Flow to manipulate the local state of the application.
- **Logan Kinneer:** Performed further research on Cuckoo and methods malware can use to detect if it is being run in a sandboxed environment. Some of these methods include checking to see if the machine has network connectivity, checking for mouse clicks, and other methods. Looked into methods of reporting that Microsoft Defender can use to report when it has found malware on a system. Looked into using Azure Cloud Services for this purpose.
- **Paul Chihak:** Continued writing simple test scripts to determine a strategy for implementing malleable command and control infrastructure. Found some of the most common topologies are star topology (all bots organized around a central server), multi-server topology (multiple C2 for redundancy), Hierarchical topology (multiple C2 organized into tiered groups), and random topology (P2P botnet). Determined that the most realistic approach for our team will be a star topology because it limits the number of C2 servers that we will require.
- **Justin Roepsch:** Practiced using a React project in a Django server by creating and developing a new project using these technologies during HackISU event. Time recorded is time spent specifically on parts that were not the backend logic for the project.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative

Adam Crosser	Continued to conduct research into red team techniques, tactics, and procedures. Wrote test code to identify techniques we could use for payload delivery.	6	50
Daniel Limanowski	Researched domain fronting and scheduled university advisor meeting.	8	49
Vijay Uniyal		7	43
Logan Kinneer	Researched sandbox detection methods and Microsoft Defender reporting.	7	44
Paul Chihak	Wrote test code for malleable C2 and determined the most realistic topology for our use case and budget.	6	43
Justin Roepsch	Used React and Django in new application for practice	6	44

Plan for the Upcoming Week

- **Adam Crosser:** Continue to conduct research into red team techniques and discuss with PwC for ideas on areas we could research. We have plans to meet with our academic advisor to also begin to leverage their domain expertise to give us research ideas for our project and receive feedback. This feedback will help drive my future research topics and ideas as we continue to write test code and prototype various small elements of our project solution.
- **Daniel Limanowski:** I plan on conducting research into common (ideally free or open source) EDR solutions so that I understand what our other sub-team will be looking to

use in order to solve their problems and goals as we slowly transition away from research and fully into implementation over the next few weeks. Once I hear back from our university advisor I will confirm a time with him to meet and notify the team of our meeting.

- **Vijay Uniyal:** Gain stronger understanding of Unidirectional data flow for the internal state in the App Component. Then look into learning about bindings in Javascript for when I use React ES6 class components.
- **Logan Kinneer:** Continue to look into other methods of reporting on Windows Defender such as Microsoft Intune, the System Center Configuration Manager and others. Find a way that one of these services could communicate with our application in a standard easily replicable way. Determine best way to integrate this into our application.
- **Paul Chihak:** Continue working with Cuckoo Sandbox and start using some sample malware to see what kind of results we can expect to receive from the program. Also should be able to figure out how useful the results will be in a real world scenario where time is crucial.
- **Justin Roepsch:** I plan to stop focusing on just practicing React, and go back to looking at how to implement the technologies required for the frontend requirements.