EE/CprE/SE 491 Weekly Report 9

Report Coverage: 10/29/2018 - 11/02/2018
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 team our continued to engage in research and development and early prototyping.

Past Week Accomplishments

Group Accomplishments

- Our group continued to work with the client and presented our updated project plan.

Individual Accomplishments

- **Adam Crosser:** Conducted research into alternative payload delivery mechanisms such as using HTML Applications with DotNetToJScript to load arbitrary C# code into mshta.exe. Researched lateral movement techniques we could integrate into the implant. Will need to discuss with the client if this is something they would be interested in pursuing as part of the project or if it would be in scope for development.
- **Daniel Limanowski:** Conducted research into secure user authentication development, including using third-party providers (such as single-sign-on, or SSO services). Determined that a local user authentication service would work best given the context of the application (it will be built/destroyed all the time). Determined the application, when built, should just have a default admin user that requires a password change at the first login. Read documentation on Django’s provided authentication modules.
- **Vijay Uniyal:** Gained stronger understanding of Unidirectional dataflow to help me manipulate local internal state.Learned few interesting functionalities such as onDismiss and render. Made a sizeable entry into learning about bindings as it’s quite big.

- **Logan Kinneer:** Worked on learning how to create a new page in the webapp. Researched more C sharp. Brainstormed a way to create an interface between Cuckoo and the webapp. Installed the webapp on my local machine machine.
- **Paul Chihak:** Worked with cuckoo sandbox to determine that it will be able to handle the different payloads that we want to use, trace API calls to determine what endpoints are being activated which is the main use case of this portion of the platform. However if we decide to implement a malleable C2 infrastructure then we will be able to also follow any HTTP/S traffic that is being beaconed by the implant and then we can determine whether or not the malleable C2 is implemented properly.
- **Justin Roepsch:** Researched and worked with the requirement for https. If we want to test our server in a local environment while using https, we will need to use something like django-sslserver with self-signed certificates. This requires adding it to the project, creating a certificate, which can be partially automated, and making including the location of the certificate in the "python manage.py makemigrations..." command used to run the server.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative
Adam Crosser	Primary researched new payload delivery techniques and developed prototypes. I had an exam for COMS311 this week so I didn't have as much time to work on the project as I normally would.	4	54
Daniel Limanowski	Research user authentication and applied it to our project. Played with local user	6	55

	authentication on the Django web framework.		
Vijay Uniyal	Learned how to utilize Unidirectional dataflow and various functionalities. Started on learning bindings also.	6	49
Logan Kinneer	Learned about how to create new page in webapp. Researched C sharp and methods to create an interface between cuckoo the webapp. Installed webapp on local machine.	7	51
Paul Chihak	Worked with cuckoo sandbox to help determine what kind of results we can expect to receive and to determine how useful the results will be in a real world scenario.	5	48
Justin Roepsch	Researched and worked with technologies to implement the https requirement, for local testing	6	50

Plan for the Upcoming Week

- **Adam Crosser:** Continue to conduct research into how our client conducts red team operations and writing test code

- **Daniel Limanowski:** I plan to reassign project plan tasks for the team as well as conduct research into database systems for the command-and-control server.
- **Vijay Uniyal:** Will continue and finish research into Bindings so I can combine my knowledge of React ES6 Class components.
- **Logan Kinneer:** Continue to find ways to integrate cuckoo with the webapp.
- **Paul Chihak:** Start using cuckoo sandbox with different payloads to see what payloads retrieve more effective results. Also try and determine if the program will still give effective results regardless of how the payload is compiled and deployed. Such as if the HTTP traffic can still be monitored when using domain fronting, etc.
- **Justin Roepsch:** Continue testing technologies needed for the frontend environments.