EE/CprE/SE 492 Weekly Report 4

Report Coverage: 02/25/2019
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 research and development on the project.

Past Week Accomplishments

Group Accomplishments

- Communicating with project stakeholders

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative (for second semester)
Adam Crosser	Reverse engineered malware dropper used by Iranian APT (Advanced Persistent Threat) group to identify delivery mechanisms used. Malware used	4	19

	COM-Scriptlets that were invoked using CMSTP.exe to bypass Microsoft Applocker to decode a malicious powershell module. To bypass monitoring of process trees it used Windows Management Instrumentation (WMI) to spawn a copy of powershell.exe which was used to decode a second stage payload. This payload had three layers of obfuscation before reaching a final stage RAT (remote access trojan) implemented in powershell that supported things such as lateral movement via DCOM, upload/download, invoking arbitrary externally hosted powershell scripts, and taking a screenshot of the users desktop. **BLOCKED:** I need to implement domain fronting using Amazon CloudFront, but cannot do this until the client providers funding for AWS resources. They have agreed to the		

	requested amount of resources and are simply waiting for the proper forms to be completed, etc.		
Daniel Limanowski	Refactored the frontend to reduce complexity. Added first version of User authentication with Django.	4	22
Vijay Uniyal	After much research learned I needed to use nginx to create a web server as apache would not work properly with our project. Starting to get a foothold in nginx.	5	22
Logan Kinneer	Worked on getting the memory dump feature in Cuckoo to work.	4	16
Paul Chihak	Figured out how to create an OVA out of the Proxmox VM however having issues getting it to properly install. I believe it is an issue to do with how I solved the nested virtualization not being transferable into virtualbox but haven’t conclusively determined that yet.	4	20
Justin Roepsch	Started work on logging using new version of the c2 after migration that is being	4	22

	implemented by Daniel. This also included testing of the components as parts of the migration reached completion.		

Plan for the Upcoming Week

- **Adam Crosser:** Continuing to research new payload techniques and implement domain fronting when I obtain access to AWS resources that are required to implement it.
- **Daniel Limanowski:** Finish user authentication and start creating groups and permissions.
- **Vijay Uniyal:** Understood the web development more and am now switching to using nginx to create a front for the web server. Now learning nginx web creation.
- **Logan Kinneer:** Continue to work on getting more functionality in Cuckoo working and getting Cuckoo better integrated with the webapp.
- **Paul Chihak:** Figure out what is going on with the OVA so that I can actually distribute Cuckoo to the rest of the team and then we can integrate it into our web application front end.
- **Justin Roepsch:** Help with completion of migration, before continuing with the logging of user actions.