Interim Report

TEAM NUMBER:	JMS 58
SCHOOL NAME:	Jackson Middle School
AREA OF SCIENCE:	Computer Science
PROJECT NAME:	Stuxnet
TEAM MEMBERS:	Nancy Avila (nancyavila.lpslover123@gmail.com) Tiffany Chau (doantiffany7418@gmail.com) Laisbiel Garcia(garcialaisbie@gmail.com) Brandon Pham (brandon.pham243@gmail.com)
SPONSORING TEACHER(s):	Ms. Lunsford
PROJECT MENTOR(s):	Mrs. Glennon

PROBLEM DEFINITION: Our project focuses on the workings of the computer worm Stuxnet. Stuxnet is a controlled computer worm. Speculation is that the U.S and Israeli government created Stuxnet, but no one is sure who created it. This computer worm attacked the Iranian nuclear program in the year of 2007. Stuxnet altered Programmable Logic Controllers used in the nuclear program. There are two versions of the worm. Stuxnet will spread with a USB to its chosen target and stops after the third affected computer. The second version is able to spread to many other computers including the chosen target. We are having a difficult time coming up with a question to solve about Stuxnet without doing a simulation.

CODING: We plan to code Stuxnet using NetLogo. The code is going to have a total of six computers and one virus. Because Stuxnet has two versions of throwing the virus, we plan to simulate how both of the versions work. The first version of code will show the worm infecting one computer, spreading to two other computers, and stopping. The actual Stuxnet virus' first version only targets the Programmable Logic Controllers. The coding of the second version display what will happen after pressing the "GO" button. The virus will have no end and spread to all the computers in the simulation. The second version infects the Iranian government's industrial facility systems. Stuxnet also went to infect other places around Iran. The spreading of the virus will show with the diffusion method. The diffusion method will be

PROGRESS: Our progress focuses on our coding and research towards Stuxnet. The information that we plan to have is how it has affected Iran and the truth behind the action of this virus. We will achieve this progress is getting information from books and electronic sources. We have planned on going to a library and get some books about the virus Stuxnet. We are still working on the coding by exploring fields of diffusion that will help us to develop a life like model.

RESULTS EXPECTED: The results we expect to find are how Stuxnet enters a computer system. We expect to learn how Stuxnet neutralizes and reprograms the main system. Another expectation that we have is to see if there is a antivirus capable of stopping Stuxnet. We will discover how the antivirus effects Stuxnet and how it rearranges the coding in the virus. Our coding will show how Stuxnet infiltrates the fire-wall.

REFERENCES:

Is Stuxnet Dead? (2015, July 23). Retrieved November 06, 2017, from https://www.flowcontrolnetwork.com/is-stuxnet-dead/

Landesman, M. (n.d.). What Is the Stuxnet Worm Computer Virus? Retrieved October 09, 2017, from https://www.lifewire.com/stuxnet-worm-computer-virus-153570

Langner, R. (n.d.). Ralph Langnet: Quebrando Stuxnet, un arma cibernética del siglo XXI. Retrieved October 23, 2017, from https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=es#t-328361

(n.d.). Retrieved October 16, 2017, from https://us.norton.com/stuxnet

Posted 26 Feb 2013 | 14:00 GMT By David Kushner. (2013, February 26). The Real Story of Stuxnet. Retrieved October 16, 2017, from https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Schneier, B. (2012, July 11). The Story Behind The Stuxnet Virus. Retrieved December 09, 2017, from https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

Zero Days (2016). (2017, July 22). Retrieved October 23, 2017, from http://watchdocumentaries.com/zero-days/

Zetter, K. (2017, June 03). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved October 23, 2017, from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Pdf:https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf