Stuxnet

New Mexico Supercomputing Challenge

Final Report

April 4, 2018

Team: JMS58

Jackson Middle School

Team Members - email:

Nancy Avila nancyavila.lpslover123@gmail.com

Tiffany Chau doantiffany7418@gmail.com

Laisbiel Garcia garcialaibie@gmail.com

Brandon Pham brandon.pham243@gmail.com

Sponsoring Teachers:

Karen Glennon

Sharee Lunsford

Project Mentors:

Patty Meyer

Jane Haagensen

Table of Contents

Executive Summary…… p.2

Problem Statement…….. p.3

Method……..... p.4

Code…… p.4

Netlogo Code……..…….. p. 5

Graphs……..... p. 6

Study Results…….. p.7

Conclusions……. p.7

Significant Achievements……... p.8

Acknowledgements……. p.9

Bibliography…… p.10

Executive Summary

Our project is based on Stuxnet. Stuxnet is the controlled computer worm that was released in the year 2009. Stuxnet was believed to be created by the Israeli and the U.S government. However, Stuxnet had a kill date of June 24th, 2012, so not much was able to be discovered during that time. The controlled computer worm had a set of two codes. The first code that was created worked with a flash drive that could only spread on three computers. The second code was a worldwide spread which was the reason for its destruction. To gain this information we used books, internet sources, and documentaries.

Problem Statement

The statement of the problem we have investigated is an attempt to prevent the creation of another version of Stuxnet. Stuxnet is a malicious, controlled computer worm that attacked many computers in the year 2009. Our code will give an example of an antivirus that could neutralize Stuxnet if it did not have a kill date.

While we created pieces of code that created the worm, we had many trials and errors. The first Stuxnet had traveled to only a few computer systems then "killed" itself after infecting its third computer. Then, the second Stuxnet code traveled to more computer systems. Stuxnet spreads with a USB and inside the code it is instructed to go after a certain target. If Stuxnet did not have a kill date, then the U.S or the Israeli government, or maybe someone outside the two governments, would have made a antivirus.

Method

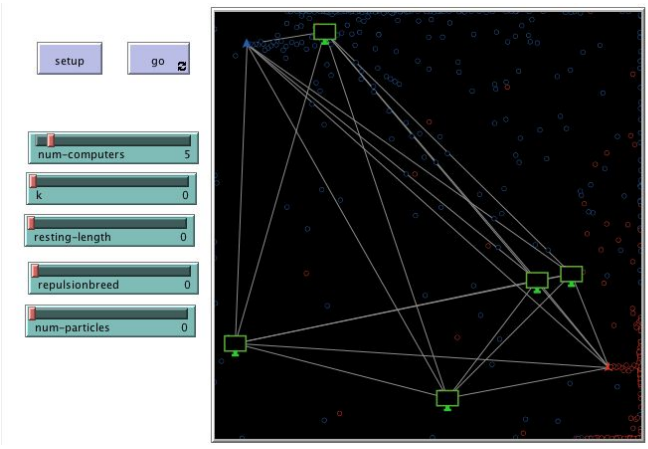
The method we used to solve our problem was to look for information in every form we could. On the weekends we met at one of our teammates house and watched a documentary on our topic. Also, we read some books about the topic and searched for information online.We have contacted coding mentors to help us with our code on the Stuxnet topic.

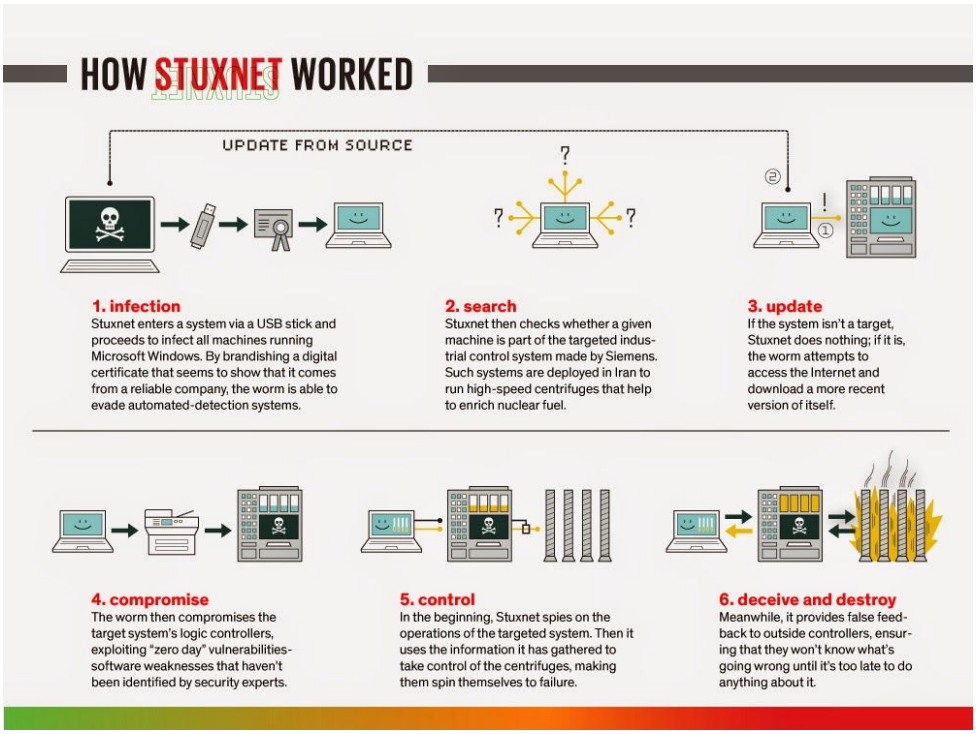
Code

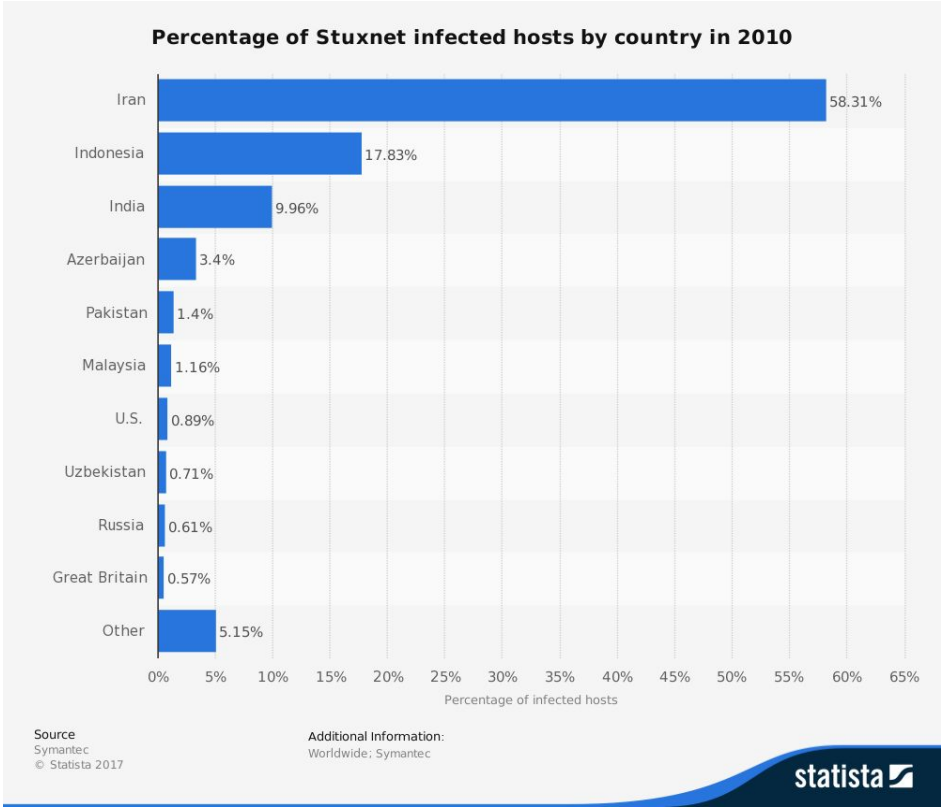
The judges viewed our NetLogo model during the project evaluations. They offered some tips to improve our model. As a result we added the antivirus and made the virus shootout particles which would represent the “virus” and the second code of Stuxnet. We are currently working on trying to get the anti-virus to shoot out the particles which would represent the “anti-virus” and to run along the links that connect the computers to each other. We still have some holes in the code which we need to fix.

Graphs and Netlogo Code

```
breed [ nodes node  ]
breed [emmitters emmitter ]
breed [computers computer]
breed [ virus viruses ]
breed [particles particle]
breed [anti-virus anti-viruses]

to layout
layout-spring computers links k resting-length repulsionbreed
end
to setup
  clear-all
create-turtles num-computers [
   set shape "computer"
    set size 2.5
   set heading 90
    setxy random-xcor random-ycor]

  ask one-of patches [sprout-virus 1]
  ask virus [set color red]

  ask one-of patches [sprout-anti-virus 1]          ;  I think you mean to sprout
  ask anti-virus [set color blue]

  ask virus [create-links-with computers]
  ask turtles [create-links-with other turtles]


end
to go
  ask virus [hatch-particles 1 [
     ;  you create the anti-virus particles below, delete this line of code

    set color red
  set shape "particle"
  set size .4
    set heading 90] ]
  ask particles [                       ; see note below about no need to repeat t
    rt random 10 lt random 10 fd .1
  ]

   ask anti-virus [hatch-particles 1 [   ;  here are your anti-virus particles,
    set color blue
  set shape "particle"
  set size .4
    set heading 90] ]
  ask particles [                     ; these two lines do the same thing as the tw
    rt random 10 lt random 10 fd .1   ;the particles move the same, whether they a
  ]

end
```




HOW STUXNET WORKED
UPDATE FROM SOURCE
1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.
2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.


Percentage of Stuxnet infected hosts by country in 2010
Iran 58.31%
Indonesia 17.83%
India 9.96%
Azerbaijan 3.4%
Pakistan 1.4%
Malaysia 1.16%
U.S. 0.89%
Uzbekistan 0.71%
Russia 0.61%
Great Britain 0.57%
Other 5.15%
0% 5% 10% 15% 20% 25% 30% 35% 40% 45% 50% 55% 60% 65%
Percentage of infected hosts
Source
Symantec
© Statista 2017
Additional Information:
Worldwide; Symantec
statista

Study Results

The information gathered helped us to view different virus constructions. That, in fact, helped us to fully understand and articulate Stuxnet. Stuxnet is complicated to understand and it took us a long time to get information and to summarize its construction. It was difficult to obtain more and in-depth information. It was off limits to the public so we had to improvise.

Conclusion

The conclusion that we have reached by analyzing our results is that if a second version of Stuxnet is created, the world could be in danger. The coding of Stuxnet would be available if your company is one who creates antiviruses since what you were trying to stop would have to be known. The world would be vulnerable to what a virus like Stuxnet might cause.

Significant Achievements

Nancy Avila

My most significant achievement on this team would be learning to write a scientific paper and to articulate what I know. I have not always been good with words and this was a challenge. I'm glad I participated with this team because I was able to learn about something I didn't know and expand on what I already knew and expand my leadership skills. This team has also helped me with my public speaking skills, and it had shaped me into a stronger leader and worker.

Tiffany Chau

My most significant achievement is learning to speak in front of a group of people. I'm not one to speak verbally so talking in front of people always frightened me. When we began to practice for our presentations with the judges at school, it was a challenge for me. I feared that I would say something wrong or I'll speak too quietly. I felt better after presenting the project just by myself, I felt a little better. I came up with techniques to calm my anxiety. When presentations came, I still felt anxious. I managed to pull through and before I knew it, it was over. I felt much better. I feel confident with doing presentations now.

Laisbiel Garcia

My most significant achievement on this team would be learning some personal skills like public speaking and working with other people. The third skill that I think I have improved during this year is on my coding skills. By working with my teammate on the code I think that I have improved a lot since last year.

Brandon Pham

My most significant achievements on this team would be learning to work together in heated situations and to learn more about coding. I have also learned to speak in front of a crowd, I have not liked doing this, but being on this team has helped me with that skill. I am glad I participated with this team because the skills I have learned will help me a lot in the future.

Acknowledgements

We give our thanks to all of our mentors that helped us with this challenge. We thank Mrs. Glennon for all her help. You helped us to improve our project, and you gave us the resources that we might not have had access to. Mrs. Glennon, you gave us everything that we need.

Ms. Lunsford, we thank you for helping us with this enormous project. Without her help and guidance, we would not be able to have come so far. Ms. Lunsford has given us much to improve and much to change. She has given us ideas and information for our project.

Patty Meyer, thank you for all the guidance that you have provided us in this year's Supercomputing Challenge. Thank you for all the help you provided when we worked on our code and on reviewing hard difficult texts. All the help that you have given us.

Jane Haagensen, thank you for all the help you have given us such as: code review, writing, and giving us important information. Your help has been an important impact on our project and your support is what kept us going. Both you and Ms. Patty have helped us understand important difficult information based on Stuxnet. There are not enough words to describe how much gratitude we have towards you and all of our mentors. Once again, thank you all for the help, we could not have done it without you.

Bibliography

Is Stuxnet Dead? (2015, July 23). Retrieved November 06, 2017, from https:// www.flowcontrolnetwork.com/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/white/papers/w32_stuxnet_dossier.pdf

Stuxnet. (n.d.). Retrieved April 03, 2018, from

https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet

Stuxnet - percentage of infected hosts by country | Statistic. (n.d.). Retrieved April 03, 2018, from

https://www.statista.com/statistics/271110/stuxnet-infected-hosts-by-country/